DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

č.j. DIA- 799-9/SEP-2026
ev. číslo smlouvy: 014/2026

SMLOUVA O POSKYTOVÁNÍ SLUŽEB PRO NÁRODNÍ CERTIFIKAČNÍ SCHÉMA EUDIW

uzavřená
dle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník,
ve znění pozdějších předpisů, (dále jen „**občanský zákoník**“)
(dále jen „**Smlouva**“)

ČLÁNEK I.
SMLUVNÍ STRANY

Česká republika – Digitální a informační agentura

Sídlo:	Na Vápence 915/14, 130 00 Praha 3
IČ:	17651921
DIČ:	Není plátce DPH
Bankovní spojení:	Česká národní banka
Číslo účtu:	6326001/0710
Zastoupená:	Mgr. Bohdanem Urbanem, ředitelem
ID dat. schránky:	yukd8p7

(dále jen „**Objednatel**“ nebo „**DIA**“)

a

MONET+,a.s.

se sídlem:	Za Dvorem 505, Štípa, 763 14 Zlín
IČO:	26217783
DIČ:	CZ26217783
Bankovní spojení:	Komerční banka, a.s., pobočka Zlín
Číslo účtu:	1547260257/0100
Zastoupená:	Ing. Břetislavem Endrysem, předsedou představenstva a Ing. Janem Vavrysem, členem představenstva
ID dat. schránky	g4xe86t

(dále jen „**Zhotovitel**“)

(Objednatel a Zhotovitel dále společně také jako „**smluvní strany**“ a jednotlivě jako „**smluvní strana**“)

ČLÁNEK II.
ÚVODNÍ USTANOVENÍ

1. Účelem této smlouvy je realizace veřejné zakázky „Národní certifikační schéma EUDIW, jeho údržba, rozvoj a monitoring jeho uplatňování II“.

2. Zhotovitel bere na vědomí, že předmět plnění dle této Smlouvy je spolufinancován z fondů Evropské unie, z programu Národní plán obnovy, z projektu ROPIM s registračním číslem CZ.31.5.0/0.0/0.0/23_106/0008503. Zhotovitel bere na vědomí, že je povinen označit veškeré účetní doklady informací o projektu ROPIM, jak je stanoveno dále ve Smlouvě.

3. Předmětem veřejné zakázky je vytvoření národního certifikačního schématu pro evropské peněženky digitální identity (dále jen „**EUDIW**“) v České republice (dále také jako „**NCS**“ nebo „**NCS EUDIW**“), včetně jeho následné údržby, rozvoje a monitoringu jeho uplatňování, a to v souladu se všemi relevantními právními předpisy, především s Nařízením Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, ve znění pozdějších předpisů (dále jen jako „**eIDAS**“) a veškerými jeho prováděcími předpisy .

4. Zhotovitel uzavřením Smlouvy bere na vědomí, že DIA jako budoucí vlastník NCS v České republice bude odpovídat za činnosti vlastníka certifikačního schématu vyplývající z Prováděcího nařízení Komise (EU) č. 2024/2981 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla eIDAS, pokud jde o certifikaci EUDIW, a k tomuto účelu bude také využívat služeb Zhotovitele; v českém překladu uvedeného prováděcího nařízení je NCS označeno jako „*vnitrostátní systém certifikace*“.

5. V průběhu plnění této Smlouvy bude DIA spolupracovat se Zhotovitelem a bude ho informovat o aktuální situaci a případných výstupech a výsledcích vzešlých ze spolupráce členských států EU či expertních skupin v oblasti budování certifikačních schémat pro EUDIW tak, aby tyto výstupy mohly být v případě potřeby a kdykoli v průběhu trvání této Smlouvy inkorporovány také do NCS. Spolupráce mezi DIA a Zhotovitelem je blíže rozvedena v následujících článcích této Smlouvy.

6. Objednatel je ústředním orgánem státní správy ve smyslu zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů, jehož působnost a zásady činnosti jsou stanoveny zákonem č. 12/2020 Sb. o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky z ní vyplývající.

7. Zhotovitel splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené, a ke dni uzavření této Smlouvy není vůči němu vedeno řízení dle zákona č.182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (dále jen „**Insolvenční zákon**“), a zavazuje se Objednatele bezodkladně informovat o hrozícím úpadku, popř. o prohlášení úpadku jeho podniku.

8. Touto Smlouvou se Zhotovitel zavazuje realizovat pro Objednatele vytvoření, údržbu, rozvoj a monitoring NCS, v souladu s požadavky eIDAS a s jeho prováděcími akty.

9. Zhotovitel uzavřením Smlouvy bere na vědomí, že primárním účelem, pro který je tato Smlouva uzavírána, je zajištění plnění ze strany Zhotovitele (vytvoření NCS, jeho údržba, rozvoj a monitoring), a to tak, aby DIA jako budoucí vlastník NCS v České republice mohla řádně a spolehlivě plnit své povinnosti vlastníka certifikačního schématu vyplývající z eIDAS a jeho prováděcích aktů, a zejména z Prováděcího nařízení Komise (EU) č. 2024/2981 ze dne 28. listopadu 2024.

ČLÁNEK III.
PŘEDMĚT SMLOUVY

1. Předmětem této Smlouvy je závazek Zhotovitele poskytovat pro Objednatele služby spočívající v zajištění vytvoření, údržby, rozvoje a monitoringu NCS EUDIW, jejichž rámcové vymezení je uvedeno v čl. III odst. 2 této Smlouvy (dále souhrnně jen „**Služby**“) a závazek Objednatele uhradit za poskytnuté Služby Zhotoviteli sjednanou cenu.

2. Zhotovitel se na základě této Smlouvy zavazuje zajistit pro Objednatele především tyto Služby:

   2.1. vytvoření NCS pro certifikaci EUDIW, jehož obsahové náležitosti a jiné požadavky jsou blíže specifikovány v Příloze č. 1 této Smlouvy (dále jen „**Služby vytvoření NCS**“). Služby vytvoření NCS zahrnují i naplnění akceptačních milníků popsaných v příloze č. 1 Smlouvy v souladu s čl. VI této Smlouvy; a

   2.2. údržbu, rozvoj a monitoring NCS EUDIW na základě jednotlivých požadavků Objednatele, učiněných v souladu s čl. VI. Smlouvy (dále jen „**Ad-hoc služby**“).

ČLÁNEK IV.
DOBA A MÍSTO PLNĚNÍ

1. Místem plnění je sídlo Objednatele a jeho jednotlivých pracovišť.

2. Není-li smluvními stranami dohodnuto jinak, veškeré písemné výstupy související s plněním této Smlouvy a/nebo jeho části bude Zhotovitel předávat Objednateli elektronicky na adresu osoby k tomu určené dle čl. XIV Smlouvy. Listinné výstupy budou Zhotovitelem předávány v sídle Objednatele na adrese uvedené v záhlaví této Smlouvy.

3. Plnění vymezené v článku III. odst. 2.1 této Smlouvy – **Služby vytvoření NCS,** se Zhotovitel zavazuje předat Zadavateli k akceptaci nejpozději do dvou (2) měsíců ode dne účinnosti této Smlouvy. Lhůty relevantní pro akceptační proces jsou upraveny v čl. VI Smlouvy, přičemž je výslovně sjednáno, že po dobu trvání akceptačního procesu neběží lhůta pro poskytnutí Služby vytvoření NCS dle první věty tohoto odstavce.

4. Plnění vymezené v článku III. odst. 2.2 této Smlouvy - **Ad-hoc služby,** se Zhotovitel zavazuje plnit po dobu dvou let od akceptace plnění vymezené v článku III. odst. 2.1 této Smlouvy **.**

ČLÁNEK V.
CENA A PLATEBNÍ PODMÍNKY

1. Souhrnná celková cena za plnění na základě této Smlouvy činí maximálně 2 989 500,- Kč bez DPH (slovy: dva miliony devět set osmdesát devět tisíc pět set korun českých) bez DPH, tedy 3 617 295,- Kč včetně DPH (slovy tři miliony šest set sedmnáct tisíc dvě stě devadesát pět korun českých) včetně DPH (dále též jako „**Celková cena**“ nebo „**finanční limit**“). Celková cena je maximální, nepřekročitelná a nejvýše přípustná za celé období trvání této Smlouvy a jsou v ní zahrnuty veškeré náklady Zhotovitele související s plněním dle této Smlouvy. Zhotovitel se zavazuje informovat Objednatele o skutečnosti, že byl finanční limit vyčerpán.

2. Smluvní strany se dohodly, že Celková cena je rozdělena na dvě části, odpovídající rozdělení plnění dle čl. 2 Smlouvy, a sice:

   2.1 Cena za plnění dle ustanovení článku III. odst. 2.1 této Smlouvy (Služby vytvoření NCS), je stanovena ve výši 2 650 000,- Kč bez DPH, tedy 3 206 500,- Kč včetně DPH.

   2.2 Cena za plnění dle ustanovení článku III. odst. 2.2 této Smlouvy (Ad-hoc služby), činí souhrnně maximálně částku ve výši 339 500,- Kč bez DPH, tedy 410 795- Kč včetně DPH.

3. Cena plnění konkrétně požadovaných Ad-hoc služeb dle ustanovení článku III. odst. 2.2 této Smlouvy (údržba, rozvoj a monitoring NCS na základě jednotlivých požadavků Objednatele) bude naceněna **cenou za 1** (jeden) **člověkoden** (dále také jako „**MD**“) podle zúčastněných rolí pracovníků Zhotovitele. Jeden MD znamená 8 (osm) hodin (nikoliv nutně po sobě jdoucích) práce jednoho pracovníka. Zhotovitel se zavazuje vždy uvádět rozklad MD na jednotlivé role dle následujícího odst. 4.

4. Smluvní strany se dohodly, že Služby budou poskytovány v jednotkových cenách za jednotlivé role v následující výši:

Název role	**Cena v Kč za 1 MD bez DPH**	**Popis činností role**
Analytik	11 500,-- Kč	Expertní práce týkající se certifikací procesů, produktů a služeb, včetně tvorby certifikačního schématu ve vztahu k plnění této Smlouvy
Expert v oblasti kybernetické a informační bezpečnosti	11 500,-- Kč	Expertní práce v oblasti kybernetické nebo informační bezpečnosti ve vztahu k plnění této Smlouvy
Expert informačních systémů	11 500,-- Kč	Expertní práce v řízení bezpečnosti informací ve vztahu k plnění této Smlouvy
Expert pro budování a správu důvěryhodných digitálních identit	12 500,-- Kč	Expertní práce promítající zkušenosti týkající se budování či správy důvěryhodných digitálních identit a související infrastruktury ve vztahu k plnění této Smlouvy

Název role	**Cena v Kč za 1 MD bez DPH**	**Popis činností role**
Projektový manažer	11 500,-- Kč	Řízení projektu, prostřednictvím kterého bude plněna tato Smlouva

5. Cena za příslušná plnění Služeb bude hrazena na základě faktury (daňového dokladu) vystavené Zhotovitelem. Zhotoviteli vzniká právo na úhradu ceny a vystavení daňového dokladu (faktury) následovně:
   a) pro Služby vytvoření NCS dle čl. III. odst. 2.1 Smlouvy, okamžikem zhotovení, předání a akceptace celých Služeb vytvoření NCS v souladu s čl. VI. této Smlouvy;
   b) pro jednorázová dílčí plnění požadovaná v rámci Ad-hoc služeb dle čl. III odst. 2.2 Smlouvy, okamžikem zhotovení, předání a akceptace dílčího plnění v souladu s čl. VI. této Smlouvy;
   c) pro kontinuální dílčí plnění požadovaná v rámci Ad-hoc služeb dle čl. III. odst. 2.2 Smlouvy, okamžikem skončení příslušného kalendářního měsíce poskytování kontinuálního dílčího plnění. Nebude-li dílčí plnění poskytováno po celou dobu příslušného kalendářního měsíce, budou měsíčně fakturované částky poměrně sníženy tak, aby částka fakturovaná v kalendářním měsíci byla přímo úměrná skutečnému počtu dní poskytování dílčího plnění v tomto měsíci.

6. Faktura (daňový doklad) vystavená Zhotovitelem musí obsahovat náležitosti stanovené právními předpisy, číslo jednací této Smlouvy a celkovou cenu plnění bez a včetně DPH. Dále musí faktura obsahovat název projektu „ROPIM“ “ a registrační číslo projektu: CZ.31.5.0/0.0/0.0/23_106/0008503 a text: „projekt je financován z programu Národní plán obnovy, komponenta 1.7 Digitální transformace veřejné správy“.

7. Smluvní strany se dohodly na lhůtě splatnosti faktury (daňového dokladu) v délce třiceti (30) kalendářních dnů ode dne doručení faktury Objednateli do datové schránky Objednatele uvedené v záhlaví Smlouvy. V případě doručení faktury (daňového dokladu) v období od 8. 12. do 28. 2. příslušného kalendářního roku činí splatnost faktury (daňového dokladu) šedesát (60) kalendářních dnů. V případě pochybností se má za to, že dnem doručení se rozumí třetí den ode dne odeslání faktury (daňového dokladu). Faktury budou zasílány do datové schránky Objednatele, uvedené v záhlaví Smlouvy.

8. Objednatel nebude poskytovat Zhotoviteli jakékoliv zálohy na úhradu plnění nebo jeho části.

9. Objednatel je oprávněn před uplynutím lhůty splatnosti fakturu (daňový doklad) vrátit bez zaplacení faktury (daňového dokladu), která neobsahuje náležitosti stanovené touto Smlouvou, nebo budou-li tyto údaje uvedeny chybně. Zhotovitel je povinen podle povahy nesprávnosti fakturu (daňový doklad) opravit nebo nově vyhotovit. V takovém případě není Objednatel v prodlení se zaplacením fakturované částky. Okamžikem doručení náležitě doplněné či opravené faktury (daňového dokladu) začne běžet nová lhůta splatnosti faktury (daňového dokladu) v délce dle odst. 5 tohoto článku Smlouvy.

10. Součástí faktury bude akceptační protokol potvrzený oprávněným zástupcem Objednatele nebo jeho prostou kopií.

ČLÁNEK VI.
AKCEPTAČNÍ PROCES SLUŽEB A OBJEDNÁVKY AD-HOC SLUŽEB

1. Plnění musí být Zhotovitelem realizováno vždy řádně a včas, v odpovídající kvalitě a bez vad. Za vadné se považuje takové plnění, které nebude odpovídat smluvené, předepsané či obvyklé kvalitě plnění. Plnění musí být v souladu s aplikovatelnými právními předpisy České republiky a Evropské unie.

2. Výstupy zpracované dle této Smlouvy či Ad-hoc objednávek Zhotovitelem musejí být vždy vypracovány v českém jazyce, přičemž NCS pro certifikaci EUDIW a jeho případné změny musejí být vypracovány rovněž v anglickém jazyce. Jednotlivá jednání mezi Objednatelem a Zhotovitelem a součinnost poskytovaná Zhotovitelem Objednateli v rámci plnění Smlouvy či Ad-hoc Objednávek budou probíhat v českém jazyce s výjimkou případné komunikace na mezinárodní úrovni, kde komunikačním jazykem je anglický jazyk. Splněním podmínky dle předchozí věty je také situace, kdy člen realizačního týmu Zhotovitele komunikuje během jednání ve slovenském jazyce. V případě, že jednotliví členové realizačního týmu neovládají dostatečně český nebo slovenský jazyk, je Zhotovitel povinen zabezpečit pro jejich komunikaci s Objednatelem překladatele/tlumočníka do českého jazyka, kterým může být i jiný člen realizačního týmu. Jakékoliv náklady na překladatele/tlumočníka ve smyslu tohoto článku hradí v plné výši Zhotovitel.

3. V průběhu poskytování Služeb vytvoření NCS je Zhotovitel povinen plnit jednotlivé akceptační milníky popsané v příloze č. 1 této Smlouvy, přičemž výstupy jednotlivých milníků je povinen předat/zpřístupnit Objednateli.

4. K jednotlivým výstupům akceptačních milníků dle předchozího odstavce je Objednatel oprávněn (nikoliv povinen) uplatnit námitky, pokud tyto výstupy (i) nesplňují požadavky Objednatele dle této Smlouvy a jejích příloh, (ii) jsou vnitřně rozporné či zavádějící, (iii) jsou v rozporu s účelem této Smlouvy nebo (iv) nesplňují požadavky zadávací dokumentace veřejné zakázky. V takovém případě je Zhotovitel povinen oprávněné námitky Objednatele vypořádat a zohlednit namítnuté vady předmětného výstupu při plnění následujících akceptačních milníků dle přílohy č. 1 Smlouvy. Pokud výstup Zhotovitele v některém z následujících akceptačních milníků bude mít tytéž podstatné vady (tj. již jednou Objednatelem namítané podstatné vady), je Objednatel oprávněn odstoupit od Smlouvy.

5. O řádném dokončení a předání celých Služeb vytvoření NCS bude smluvními stranami vyhotoven akceptační protokol, a to za podmínek blíže specifikovaných v tomto článku VI. Smlouvy (dále jen „**Akceptační proces**“).

6. Účelem Akceptačního procesu je zejména ověření, zda Zhotovitelem poskytnuté plnění odpovídá výsledku, ke kterému se Zhotovitel touto Smlouvou či na jejím základě zavázal.

7. Po dokončení Služeb vytvoření NCS bude NCS předán či jinak zpřístupněn Objednateli k akceptaci. Objednatel je povinen vyjádřit se k NCS (akceptovat nebo odmítnout jeho akceptaci) ve lhůtě deseti (10) pracovních dnů ode dne jeho prokazatelného předání Objednateli k akceptaci.

8. Objednatel je oprávněn odmítnout akceptaci NCS, pokud obsahuje vady, čímž se zejména rozumí že (i) nesplňuje požadavky a/nebo náležitosti plynoucí z této Smlouvy a jejích příloh, (ii) je vnitřně rozporný či zavádějící, (iii) je v rozporu s účelem této Smlouvy nebo (iv) nesplňuje požadavky zadávací dokumentace veřejné zakázky. Při

odmítnutí akceptace sdělí Objednatel Zhotoviteli konkrétní důvody (vady), pro které odmítl NCS akceptovat a je povinen poskytnout Zhotoviteli na jeho žádost veškeré dodatečné informace týkající se povahy a specifikace vytknutých vad.

9. Zhotovitel je povinen Objednatelem vytknuté vady NCS bez zbytečného odkladu nejpozději však do pěti (5) pracovních dnů odstranit, a předat NCS znova k akceptaci (tj. k dalšímu kolu Akceptačního procesu), která se za stejných podmínek opakuje do doby, než jsou splněny všechny podmínky pro jeho akceptaci.

10. Pokud Objednatel NCS ve stanovené lhůtě od jeho předání k akceptaci (srov. odst. 7. výše) ani neakceptuje, ani ho neodmítne akceptovat, je Zhotovitel povinen po marném uplynutí této lhůty písemně vyzvat Objednatele k tomu, aby se k NCS vyjádřil (tj. aby ji akceptoval či aby ho odmítl akceptovat). Za tímto účelem mu poskytne dodatečnou lhůtu k plnění, která nebude kratší než deset (10) pracovních dnů od doručení výzvy Objednateli. Nevyjádří-li se Objednatel ani v této dodatečné lhůtě, je NCS považován za akceptovaný Objednatelem, a to dnem marného uplynutí lhůty.

11. Jakmile dojde k akceptaci NCS, jsou smluvní strany o této skutečnosti povinny vyhotovit akceptační protokol. Vzor akceptačního protokolu tvoří přílohu č. 2 této Smlouvy. Vyhotovením akceptačního protokolu nejsou dotčena práva z vadného plnění Objednatele, a to ani pokud jde o vytknutí zjevných vad; Objednatel má právo vytknout vady a uplatnit práva z vadného plnění do 24 měsíců od vyhotovení akceptačního protokolu.

12. Je výslovně ujednáno, že trváním (opakováním) Akceptačního procesu za podmínek této Smlouvy není jakkoliv dotčena povinnost Zhotovitele poskytnout plnění řádně a ve sjednaných lhůtách. Podmínky pro uplatnění případných námitek jsou stanoveny odst. 4 tohoto článku.

13. Smluvní strany se dohodly, že Akceptační proces sjednaný v tomto čl. VI se obdobně uplatní i na jiná plnění požadovaná v rámci Ad-hoc služeb.

14. Smluvní strany se dohodly, že Ad-hoc služby uvedené v čl. III odst. 2.2 Smlouvy budou u Zhotovitele objednávány na základě písemných požadavků Objednatele postupem uvedeným dále v tomto článku. Je výslovně sjednáno, že Objednatel není povinen čerpat během trvání této Smlouvy žádné Ad-hoc služby.

15. Objednatel je oprávněn vznést požadavek k čerpání Ad-hoc služeb prostřednictvím e-mailu zaslaného Zhotoviteli na adresu příslušné kontaktní osoby Zhotovitele uvedené v čl. XIV Smlouvy. Zhotovitel je povinen písemně potvrdit přijetí požadavku do dvou (2) pracovních dnů od jeho přijetí.

16. Nedohodnou-li se smluvní strany jinak (s ohledem na kapacity Zhotovitele), je Objednatel oprávněn vznést požadavek na čerpání Ad-hoc služeb nejdříve po akceptaci NCS v souladu s čl. VI Smlouvy.

17. Zhotovitel je povinen v návaznosti na požadavek Objednatele zaslat Objednateli bez zbytečného odkladu nabídku, která bude obsahovat alespoň: (i) celkovou cenu požadované Ad-hoc služby s uvedením rozsahu pracnosti v člověkodnech (dále jen jako „**MD**“) s rozpadem na jednotlivé role příslušných pracovníků (srov. čl. V. odst. 4 Smlouvy) a (ii) časování realizace požadavku (dále jen „**Nabídka**“). Nabídka nesmí být v rozporu s touto Smlouvou nebo s výzvou Objednatele k podání nabídky. Zhotovitel je povinen

Objednatele informovat, pokud by realizace Nabídky překročila Celkovou cenu dle čl. V odst. 1 Smlouvy.

18. Smluvní strany se dohodly, že Objednatel je povinen ve lhůtě deseti (10) pracovních dnů od obdržení Nabídky Zhotoviteli sdělit, zda Nabídku akceptuje či zda má k Nabídce jakékoliv připomínky, popř. že o Nabídku Zhotovitele nemá zájem. Pokud se Objednatel v uvedené lhůtě k Nabídce nevyjádří, pak platí, že Objednatel o návrh realizace nemá zájem.

19. Po akceptaci Nabídky Zhotovitele ze strany Objednatele je tento návrh závazný pro obě smluvní strany.

20. Pro vyloučení jakýchkoli pochybností je stanoveno, že v případě rozporu mezi Nabídkou Zhotovitele akceptovanou Objednatelem a touto Smlouvou má přednost vlastní text Smlouvy.

ČLÁNEK VII.
SOUČINNOST

1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si součinnost nezbytnou pro řádné plnění Smlouvy. Smluvní strany jsou povinny informovat bezodkladně druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění. Objednatel předpokládá, že pro účely plnění vymezeného v článku III. odst. 2.1 a odst. 2.2 této Smlouvy bude nutné vést jednání s příslušnými stakeholdery, v rámci kterých bude průběžně komunikován aktuální stav plnění a diskutovány otázky důležité pro samotné plnění. Zhotovitel je povinen zajistit účast alespoň jednoho příslušného zástupce na těchto jednáních.

2. V případě prokazatelného prodlení povinné smluvní strany s poskytnutím součinnosti není oprávněná smluvní strana v prodlení s plněním svých závazků podle této Smlouvy, pro jejichž splnění je poskytnutí dané součinnost nezbytné, a veškeré lhůty (včetně lhůt pro navazující plnění) se o prokazatelné prodlení povinné smluvní strany prodlužují; to neplatí v případech a do té míry, v jaké prodlení v poskytnutí součinnosti ze strany povinné smluvní strany bylo vyvoláno v přímé příčinné souvislosti s prokazatelným neposkytnutím součinnosti nebo prodlením ze strany oprávněné smluvní strany. Objednatel je v prodlení, jestliže v rozporu se svými povinnostmi vyplývajícími ze smluvního vztahu nepřevezme řádně nabídnuté plnění, nebo neposkytne součinnost nutnou k tomu, aby Zhotovitel mohl splnit svůj závazek. Zhotovitel je v prodlení, jestliže v rozporu se svými povinnostmi vyplývajícími z dohodného vztahu neposkytne součinnost nutnou k tomu, aby Objednatel mohl splnit svůj závazek.

3. Zhotovitel je povinen informovat Objednatele o věci či zvláštní součinnosti potřebné pro dosažení účelu požadovaného plnění, která má být zajištěna ze strany Objednatele (a to i např. prostřednictvím třetí osoby), a to bez zbytečného prodlení poté, kdy se Zhotovitel o potřebě dané věci či zvláštní součinnosti mohl a měl dozvědět. Za takovou věc či zvláštní součinnost je považováno zejména: přístup do určitých prostor, zpřístupnění či úpravy dokumentace, úpravy či dodání software, úpravy či dodání hardware, zajištění kompatibility jiného systému, poskytnutí certifikace, nebo jiné součinnosti bránící naplnění účelu Smlouvy.

4. Nesplní-li Zhotovitel povinnost včas informovat Objednatele dle předchozího odstavce, smluvní strany se písemně dohodnou na dodatečném způsobu zajištění součinnosti, který nemá dopad na termín plnění ani náklady Objednatele. Nedohodnou-li se smluvní strany v přiměřené době na postupu dle předchozí věty, pak:

   a) je Zhotovitel povinen zajistit si danou věc či součinnost sám a na své náklady v rámci plnění; nebo
   b) nemůže-li Zhotovitel z objektivních důvodů postupovat dle předchozího bodu (i) nebo doloží-li Zhotovitel Objednateli s ohledem na okolnosti případu, že by postup dle předchozího bodu (i) byl nepoměrně obtížnější či vyžadoval podstatně vyšší náklady, než kdyby danou věc či součinnost zajistil Objednatel, pak danou věc či součinnost zajistí Objednatel. Zhotovitel však Objednateli nahradí dodatečné účelně vynaložené náklady na zajištění dané věci či součinnosti. Lhůty k plnění Zhotovitele z důvodu nesoučinnosti Objednatele se pak prodlužují pouze o takovou dobu, po kterou Objednatel nečiní pro zajištění dané věci či součinnosti kroky, které po něm lze v dané situaci rozumně požadovat.

5. Pokud smluvní strana neposkytne na výzvu druhé smluvní strany součinnost nezbytnou pro plnění jejích povinností, bude postupováno následovně:

   a) Smluvní strana bez zbytečného prodlení písemně vyzve oprávněnou osobu druhé smluvní strany k poskytnutí součinnosti, a to listině, e-mailem nebo ústně s vyhotovením zápisu;
   b) pokud smluvní strana vyzvaná k součinnosti v přiměřené lhůtě po první výzvě neposkytne součinnosti ani nepodnikne konkrétní kroky k poskytnutí takové součinnosti, smluvní strana, která vyzývá k součinnosti, opětovně vyzve druhou smluvní stranu, a to písemně v listinné podobě (včetně zprávy doručené do datové schránky).

6. Výzvy k poskytnutí součinnosti musí obsahovat nezbytné informace, a to zejména: (i) vymezení povinnosti (např. konkrétního plnění), kterou není možné z důvodu nedostatku součinnosti plnit, (ii) dostatečné určitý popis součinnosti, která je vyžadována. Splní-li oprávněná smluvní strana postup pro informování dle tohoto odstavce, okamžik informování podle tohoto odstavce nemá vliv na počátek prodlení povinné smluvní strany s poskytnutím součinnosti. Naopak, pokud oprávněná strana tento postup nedodrží, počátek prodlení povinné smluvní strany s poskytnutím součinnosti nastává až k okamžiku dodatečného zaslání výzvy dle odst. 5 písm. b) tohoto článku Smlouvy.

7. Zhotovitel není oprávněn si bez souhlasu Objednatele podle ustanovení § 2591 a § 2597 odst. 2 občanského zákoníku při nedostatku součinnosti Objednatele obstarat náhradní plnění na náklady Objednatele od třetí osoby; ani uplatnit ustanovení § 2609 občanského zákoníku o svépomocném prodeji.

8. Pokud Objednatel poskytne Zhotoviteli pokyn nebo věc, které jsou nevhodné pro dosažení řádné dodávky plnění a Zhotovitel mohl a měl vzhledem ke své odbornosti tuto nevhodnost zjistit, pak:

   a) Zhotovitel bez zbytečného prodlení oznámí oprávněné osobě Objednatele nevhodnost pokynu nebo věci, a to listině, e-mailem nebo ústně s vyhotovením zápisu;
   b) pokud Objednatel v přiměřené době po prvním oznámení trvá na svém pokynu nebo použití věci (o čemž listině, e-mailem nebo ústně s vyhotovením zápisu vyrozumí

Zhotovitele), nebo se v přiměřené době k oznámení nevyjádří, Zhotovitel je povinen oznámit Objednateli nevhodnost pokynu nebo věci písemně v listinné podobě (včetně zprávy doručené do datové schránky Objednatele).

9. Oznámení Zhotovitele o nevhodnosti pokynu či věci musí obsahovat nezbytné informace, a to zejména: (i) označení nevhodného pokynu nebo věci (ii) konkrétní vysvětlení nevhodnosti pokynu nebo věci, a (iii) možné nežádoucí důsledky při dodržení pokynu nebo použití věci. Pokud Zhotovitel nedodrží zde stanovený postup pro oznámení nevhodnosti pokynu nebo věci, Zhotovitel řádně neupozornil na nevhodnost.

ČLÁNEK VIII.
POVINNOST MLČENLIVOSTI, OCHRANA OSOBNÍCH ÚDAJŮ

1. Smluvní strany se zavazují zachovávat ve vztahu ke třetím osobám mlčenlivost o informacích, které při plnění této Smlouvy získají (dále jen „**důvěrné informace**“), ledaže se jedná o:

   a) informace, které jsou veřejně přístupné,
   b) informace, které již byly smluvní straně po právu známé předtím, než jí byly zpřístupněny druhou smluvní stranou;
   c) informace, ke kterým smluvní strana dospěla nezávisle na jejich zpřístupnění od druhé smluvní strany a je schopna tuto skutečnost doložit svými záznamy; nebo
   d) informace, které byly zpřístupněny třetí osobou, aniž by tím byla porušena zákonná či smluvní povinnost mlčenlivosti této třetí osoby.

2. Smluvní strany nejsou oprávněny důvěrné informace zpřístupnit bez předchozího písemného souhlasu druhé smluvní strany třetí osobě ani je použít v rozporu s účelem této Smlouvy, ledaže se jedná:

   a) o případ, kdy je zpřístupnění informace vyžadováno právními předpisy, nebo rozhodnutím soudu nebo orgánu veřejné moci;
   b) zpřístupnění informací třetí osobě v nezbytném rozsahu výhradně za účelem plnění této Smlouvy, bude-li tato třetí osoba zavázána k dodržování mlčenlivosti nejméně v rozsahu stanoveným touto Smlouvou a nedojde-li k porušení právních předpisů chránících důvěrné informace.

3. Smluvní strany jsou povinny zavázat povinností mlčenlivosti podle odstavce 1 všechny osoby, kterým zpřístupní důvěrné informace, zejména pokud se jedná o poddodavatele Zhotovitele, kteří se budou podílet na poskytování plnění dle této Smlouvy.

4. Za porušení povinnosti mlčenlivosti osobami, kterým byly zpřístupněny důvěrné informace, zejména osoby, které se budou podílet na poskytování plnění dle této Smlouvy, odpovídá strana, která takovou důvěrnou informaci zpřístupnila, jako by povinnost porušila sama.

5. Smluvní strany se zavazují chránit informace tvořící předmět obchodního tajemství jedné ze smluvních stran ve smyslu ustanovení § 504 občanského zákoníku ve stejném rozsahu jako je sjednána ochrana důvěrných informací v tomto článku.

6. Povinnost mlčenlivosti trvá patnáct (15) let po skončení platnosti a účinnosti této Smlouvy.

7. Pro vyloučení jakýchkoli pochybností se smluvní strany výslovně dohodly, že ujednání tohoto článku VIII. Smlouvy týkající se důvěrnosti informací se nevztahují na Objednatele

ve vztahu k NCS a jakýmkoli jeho částem a informacím s nimi souvisejícím. Objednatel je oprávněn NCS nebo jakoukoli jeho část, včetně souvisejících informací, zveřejnit či zpřístupnit jakýmkoli způsobem, a to i bez předchozího souhlasu Zhotovitele.

8. Zhotovitel je povinen dodržovat zákon č. 110/2019 Sb., o zpracování osobních údajů (dále jen „**ZZOÚ**“), a Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „**GDPR**“) a zabezpečit splnění všech povinností z ZZOÚ a GDPR vyplývajících a zachovávat mlčenlivost o všech osobních údajích, se kterými se v souvislosti s plněním dle této Smlouvy jakkoliv seznámí nebo se v souvislosti s plněním dle této Smlouvy dostanou do sféry jeho dispozice nebo mu budou jakkoliv zpřístupněny a o organizačních a technických bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo bezpečnost osobních údajů. Povinnost mlčenlivosti o osobních údajích, o organizačních a technických bezpečnostních opatřeních a povinnost dle předchozí věty trvá i po zániku Smlouvy.

9. Bude-li v souvislosti s činnostmi Zhotovitele dle této Smlouvy nebo Ad-hoc objednávek docházet ke zpracování osobních údajů na systematické, pravidelné, a nikoliv pouze nahodilé bázi pro Objednatele, zavazují se Strany uzavřít smlouvu o zpracování osobních údajů, která bude splňovat veškeré požadavky podle platných právních předpisů týkajících se ochrany osobních údajů.

ČLÁNEK IX.
SMLUVNÍ POKUTY A UKONČENÍ

1. V případě nedodržení termínu zhotovení a předání předmětu plnění dle Smlouvy či akceptované Nabídky ze strany Zhotovitele (vč. případu nepřevzetí plnění ze strany Objednatele z důvodů vad) je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 3.000,-- Kč (slovy tři tisíce korun českých) za každý započatý den prodlení (počítáno od počátečního prodlení), pokud Zhotovitel své prodlení nenapraví ani v dodatečné přiměřené lhůtě stanovené Objednatelem, která nebude kratší než pět (5) pracovních dnů. Pro účely tohoto článku se stanovuje limit možné smluvní pokuty do výše 50 % ceny daného plnění.

2. Jestliže je Zhotovitel v prodlení s poskytnutím informace o stavu plnění a písemnou informaci neposkytne ani do dvou (2) dnů od dodatečné výzvy Objednatele, zavazuje se Zhotovitel uhradit Objednateli smluvní pokutu ve výši 0,02 % z ceny daného plnění bez DPH, nejvýše však 2.000,-- Kč (slovy: dva tisíce korun českých), a to za každý započatý den prodlení (počítáno od počátečního prodlení).

3. Jestliže smluvní strana poruší povinnost mlčenlivosti dle této Smlouvy, zavazuje se uhradit druhé smluvní straně smluvní pokutu ve výši 100.000,- Kč (slovy: sto tisíc korun českých) za každé jednotlivé porušení povinnosti.

4. V případě prodlení Objednatele s úhradou řádně vystavených a doručených faktur (daňových dokladů) je Objednatel povinen uhradit Zhotoviteli úrok z prodlení v zákonné výši dle platných právních předpisů.

5. Smluvní pokuta a úrok z prodlení jsou splatné ve lhůtě třiceti (30) kalendářních dnů ode dne doručení faktury s jejich vyúčtováním příslušné smluvní straně. V případě doručení faktury v období od 8. 12. do 28. 2. příslušného kalendářního roku činí splatnost faktury šedesát (60) dnů. V případě pochybností se má za to, že dnem doručení se rozumí třetí den ode dne odeslání faktury (daňového dokladu). Faktury budou zasílány do datové schránky druhé smluvní strany, uvedené v záhlaví Smlouvy.

6. Uplatněním smluvní pokuty a úroku z prodlení není dotčen nárok smluvních stran na náhradu škody v plném rozsahu ani povinnost Zhotovitele řádně poskytnout plnění.

7. Za podstatné porušení, které zakládá právo Objednatele na odstoupení od Smlouvy, se považuje zejména:

   a) prodlení Zhotovitele s předáním plnění k akceptaci o více než třicet (30) kalendářních dnů. V případě výroku „neakceptováno“ je pro potřeby tohoto podstatného porušení za počátek prodlení považováno ukončení akceptační procedury; při opakovaném výroku „neakceptováno“ je za počátek prodlení považován stále okamžik ukončení první akceptační procedury s výrokem „neakceptováno“;
   b) prodlení s řádným odstraněním vad plnění ve lhůtě stanovené podle článku VI. Smlouvy o více než třicet (30) kalendářních dnů;
   c) postup Zhotovitele při zhotovení plnění v zásadním rozporu s požadavky na plnění uvedenými ve Smlouvě, jestliže Zhotovitel nepodnikne kroky potřebné k uvedení postupu provádění plnění do souladu se Smlouvou ani ve lhůtě deseti (10) kalendářních dnů od výzvy Objednatele k napravení postupu; nebo
   d) případy uvedené níže v odst. 8, písm. a), b).

8. Objednatel je oprávněn tuto Smlouvu vypovědět s okamžitým účinkem doručením písemné výpovědi Zhotoviteli v následujících případech:
   a) po dobu trvání Smlouvy dojde alespoň třikrát (3x) k některému z následujících porušení:
      (i) prodlení s předáním plnění k akceptaci o více než patnáct (15) dní;
      (ii) prodlení s odstraněním vad (nebo jediné vady) jednotlivého plnění bránících v užívání delšímu než patnáct (15) dní,
      (iii) prodlení s odstraněním vad (nebo jediné vady) jednotlivého plnění nebránících v užívání (vyjma kosmetických) delšímu než šedesát (60) dní,
      (iv) porušení povinnosti mlčenlivosti dle této Smlouvy,

      Pro účely bodů (ii) a (iii) platí následující: V případě, že bude ve vztahu k plnění vytčeno více vad, prodlení dle předchozí věty se počítá jednotně pro veškeré vady vytčené současně nebo jinak vzájemně související, nikoli pro každou jednotlivou vytčenou vadu. Délka prodlení se počítá pro každý případ prodlení Zhotovitele samostatně a v případě více jednotlivých případů prodlení Zhotovitele v rámci jednoho plnění se nesčítá.

   b) Objednatel nenabude Licenci ve smyslu článku XI. této Smlouvy – zejména pokud Zhotovitel nebyl oprávněn Licenci poskytnout – a Zhotovitel tuto situaci nenapraví ani do šedesáti (60) kalendářních dnů od výzvy Objednatele.

9. Zhotovitel je oprávněn od Smlouvy odstoupit pro podstatné porušení pouze v případě, že:

a) Objednatel bude v prodlení s úhradou svých peněžitých závazků vyplývajících ze Smlouvy po dobu delší než šedesát (60) kalendářních dnů;
b) Objednatel bude v prodlení s poskytnutím součinnosti vyžádané Zhotovitelem v souladu s článkem VII. této Smlouvy a toto pochybení nenapraví ani ve lhůtě šedesáti (60) kalendářních dnů, kterou mu Zhotovitel poskytne;
c) Objednatel v rozporu se Smlouvou nepodepíše Akceptační protokol nebo bez závažného důvodu jinak brání ukončení Akceptační procedury nebo je v prodlení se zahájením Akceptační procedury déle než šedesát (60) kalendářních dnů.

10. Účinky odstoupení nastávají okamžikem doručení písemného projevu vůle odstoupit druhé smluvní straně. Odstoupení se nedotýká zejména nároku na náhradu škody, smluvní pokuty a povinnost mlčenlivosti.

11. Strany si ujednaly, že Objednatel je oprávněn při svém odstoupení odstoupit pouze částečně, a to:

a) pouze ve vztahu k části plnění, která je funkčně oddělitelná od zbylé části plnění;
b) s účinky ex nunc, tzn. do budoucna – tyto účinky odstoupení je Objednatel oprávněn jednostranně vyvolat i při odstoupení ze strany Zhotovitele, a to písemným oznámením zaslaným Zhotoviteli ve lhůtě třiceti (30) dnů od doručení odstoupení Zhotovitele; nebo
c) kombinací částečných odstoupení podle předchozích písm. a) a b) tohoto odstavce.

12. Ustanovení § 1912 odst. 2, § 2591, § 2595 a § 2627 odst. 2 občanského zákoníku se pro účely odstoupení od Smlouvy neuplatní.

ČLÁNEK X.
OSTATNÍ UJEDNÁNÍ, POJIŠTĚNÍ

1. Smluvní strany jsou povinny bez zbytečného odkladu oznámit druhé smluvní straně změnu údajů v záhlaví Smlouvy.

2. Zhotovitel není bez předchozího písemného souhlasu Objednatele oprávněn postoupit práva a povinnosti z této Smlouvy na třetí osobu.

3. Zhotovitel je oprávněn plnit tuto Smlouvu prostřednictvím poddodavatelů, přičemž za plnění poddodavatele vždy odpovídá Zhotovitel, jako by plnil sám.

4. Zhotovitel je povinen dokumenty související s poskytováním plnění dle této Smlouvy uchovávat po dobu nejméně deseti (10) let ode dne a) schválení závěrečné zprávy o projektu ROPIM s registračním číslem CZ.31.5.0/0.0/0.0/23_106/0008503 s tím, že o datu jejího schválení bude Objednatelem informován po skončení projektu ROPIM, anebo b) po dobu deseti (10) let od konce účetního období, ve kterém došlo k zaplacení poslední části ceny plnění, popř. k poslednímu zdanitelnému plnění dle této Smlouvy, podle toho, která z uvedených skutečností bude v čase později; a to zejména pro účely kontroly oprávněnými kontrolními orgány.

5. Zhotovitel je povinen umožnit kontrolu dokumentů souvisejících s předmětem plnění dle této Smlouvy ze strany Objednatele a jiných orgánů oprávněných k provádění kontroly, a to zejména ze strany Ministerstva financí ČR, územních finančních orgánů, Nejvyššího kontrolního úřadu, případně dalších orgánů oprávněných k výkonu kontroly a ze strany třetích osob, které tyto orgány ke kontrole pověří nebo zmocní.

6. Zhotovitel je povinen ve smyslu ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), spolupůsobit při výkonu finanční kontroly.

7. Zhotovitel bez jakýchkoliv výhrad souhlasí se zveřejněním své identifikace a dalších údajů uvedených ve Smlouvě včetně ceny plnění; vyjma obchodního tajemství, ledaže je Objednatel povinen obchodní tajemství zveřejnit na základě příslušných právních předpisů.

8. Zhotovitel prohlašuje, že ke dni uzavření Smlouvy má sjednanou pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Zhotovitelem třetí osobě s limitem pojistného plnění na jednu škodní událost minimálně **2.500.000,- Kč** (slovy: dva miliony pět set tisíc korun českých) s výší spoluúčasti nejvýše 10 %. Zhotovitel se zavazuje, že bude platnost tohoto pojištění udržovat po celou dobu trvání práv a povinností ze Smlouvy. Zhotovitel je povinen předložit kopii pojistné smlouvy nebo pojistku na vyžádání Objednatele. Škoda, kterou je případně Zhotovitel povinen nahradit Objednateli nebo třetím osobám, není omezena výší nebo rozsahem podmínek pojištění odpovědnosti. Porušení povinnosti mít sjednanou pojistnou smlouvu dle tohoto odstavce je považováno za podstatné porušení Smlouvy.

9. Zhotovitel se zavazuje poskytovat plnění dle této Smlouvy za aktivní účasti členů realizačního týmu uvedeného v Příloze č. 3 této Smlouvy, jimiž Zhotovitel prokázal svou kvalifikaci ve výběrovém řízení. Jakákoliv dodatečná změna členů realizačního týmu je možná pouze s předchozím písemným souhlasem Objednatele. Zhotovitel se v takovém případě zavazuje v souladu s požadavky zadávací dokumentace nahradit osobu realizačního týmu osobou, která bude splňovat minimálně stejnou kvalifikaci jako nahrazovaná osoba. Realizační tým je možné ze strany Zhotovitele doplňovat dále i o další členy nad rámec členů realizačního týmu uvedeného v Příloze č. 3 při splnění obdobných požadavků na znalosti a odbornou kvalifikaci takových členů.

ČLÁNEK XI.
PRÁVA DUŠEVNÍHO VLASTNICTVÍ

1. Pro účely následujících ustanovení tohoto článku se Zhotoveným dílem, resp. jeho částí rozumí takové součásti plnění Zhotovitele, které naplňují znaky autorského díla nebo jsou předmětem zvláštních práv pořizovatele databáze ve smyslu ustanovení § 2 a § 88 a násl zákona č. 121/2000 Sb., o právu autorském (dále jen „**Autorský zákon**“) a které byly v rámci plnění a ke splnění této Smlouvy Zhotovitelem či kterýmkoli jeho poddodavatelem zhotoveny, resp. vytvořeny jako dílo vytvořené na objednávku ve smyslu Autorského zákona dle této Smlouvy (výše a dále pro účely tohoto článku Smlouvy jako „**Zhotovené dílo**“).

2. Zhotovitel se zavazuje poskytnout Objednateli veškerá práva související s ochranou duševního vlastnictví vztahující se ke Zhotovenému dílu, a to v rozsahu nezbytném pro řádné užívání Zhotoveného díla Objednatelem po celou dobu trvání příslušných práv. Zhotovitel se zejména zavazuje poskytnout a příp. zajistit, aby Objednatel nabyl, v souladu s Autorským zákonem, oprávnění k výkonu práva užití ke Zhotovenému dílu, a to formou výhradní a neomezené licence ke všem způsobům užití Zhotoveného díla. Povinnost Zhotovitele dle předchozí věty platí i v případě zhotovení části Zhotoveného díla poddodavatelem.

3. Zhotovitel se zavazuje poskytnout Objednateli nejpozději při předání Zhotoveného díla (resp. jeho části mající povahu Zhotoveného díla dle příslušné etapy plnění), ve smyslu ustanovení § 2358 a násl. občanského zákoníku, oprávnění k výkonu práva Zhotovené dílo užít (dále jen „**Licence**“), a to Licenci

   a) výhradní,
   b) neomezenou (zejména není omezena územním rozsahem, množstevním rozsahem, způsobem nebo rozsahem užití),
   c) neodvolatelnou, převoditelnou, postupitelnou;
   d) k veškerým známým způsobům užití Zhotoveného díla (resp. jeho části dle příslušné etapy plnění);
   e) na dobu určitou – po dobu trvání autorských práv ke Zhotovenému dílu.

4. Z důvodu právní jistoty se sjednává, že Licence je udělena v maximálním rozsahu povoleném platnými právními předpisy.

5. Licence nabývá účinnosti dnem předání a převzetí Zhotoveného díla, či jeho funkčně oddělitelné části. Licence se nevztahuje na předem existující know-how, metodiky, šablony a další materiály, které Zhotovitel nebo jeho poddodavatel vlastnili nebo oprávněně užívali před uzavřením této Smlouvy (dále jen „**Předchozí práva**“). Na Předchozí práva poskytuje Zhotovitel Objednateli nevýhradní, nepřevoditelnou licenci pouze v rozsahu nezbytném pro řádné užívání poskytnutého plnění**.**

6. Odměna za Licenci je zahrnuta v ceně dle této Smlouvy.

7. Zhotovitel se zavazuje udělit Objednateli nejpozději při předání plnění souhlas k tomu, aby Objednatel byl oprávněn (dále jen „**Souhlas**“), bez ohledu na to, zda jde o způsob užití ve smyslu Autorského zákona či nikoliv, Zhotovené dílo nebo jeho část zveřejnit, upravovat, zpracovávat, překládat, měnit jeho název, spojit s dílem jiným a zařadit jej do díla souborného.

8. Odměna za udělení Souhlasu je zahrnuta v ceně dle této Smlouvy.

9. Strany sjednávají, že ve vztahu k součástem plnění Zhotovitele podle této Smlouvy, k němuž se vztahuje ochrana duševního vlastnictví, ale nemají povahu Zhotoveného díla a jde o produkty třetích stran či Zhotovitele (obecně standardní softwarové produkty) platí, že se práva a povinnosti Objednatele (a případně Zhotovitele) řídí licenčními podmínkami jejich výrobců, které takové produkty doprovázejí. Zařazení takových součástí do plnění podle této Smlouvy je možné pouze na základě výslovného písemného požadavku anebo výslovného písemného souhlasu Objednatele.

10. Pokud třetí osoba uplatní vůči Objednateli nárok vyplývající z porušení práv z duševního vlastnictví v souvislosti s užíváním Zhotoveného díla, jiného díla nebo věci předané Zhotovitelem Objednateli, Zhotovitel v plném rozsahu odškodní a nahradí Objednateli újmu a náklady vzniklé v souvislosti s řešením a případným uspokojením takového nároku, včetně nákladů na právní zastoupení. To neplatí, vznikl-li nárok v důsledku porušení ujednaných licenčních podmínek Objednatelem.

ČLÁNEK XII.
KYBERNETICKÁ BEZPEČNOST

1. Zhotovitel se zavazuje naplnit všechny bezpečnostní požadavky dle této Smlouvy a je povinen tyto požadavky dodržovat po dobu plnění dle této Smlouvy. V této souvislosti Zhotovitel bere na vědomí, že ve vztahu k plnění dle této Smlouvy:

   a) Objednatel je subjektem kritické infrastruktury ve smyslu příslušných ustanovení zákona č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (dále jen jako „**Zákon o kritické infrastruktuře**“) a souvisejících právních předpisů ve znění pozdějších předpisů;

   b) Objednatel je správcem informačního systému kritické informační infrastruktury podle příslušných ustanovení zákona č. 264/2025 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen jako „**Zákon o kybernetické bezpečnosti**“), ve znění pozdějších předpisů.

ČLÁNEK XIII.
ZÁVĚREČNÁ USTANOVENÍ

1. Kontaktní osoby smluvních stran uvedené v následujícím čl. XIV. této Smlouvy jsou oprávněny k poskytování součinnosti dle této Smlouvy včetně podepisování akceptačních protokolů. Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím osob oprávněných jednat jménem stran, kontaktních osob, popř. jimi pověřených pracovníků.

2. Tato Smlouva nabývá platnosti dnem jejího podpisu poslední smluvní stranou a účinnosti dnem jejího zveřejnění v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), v registru smluv. Zveřejnění v registru smluv zajistí Objednatel.

3. Tato Smlouva se řídí právním řádem České republiky, zejména příslušnými ustanoveními občanského zákoníku. Ustanovení § 131 a násl. zákona č. 134/2016 Sb., o zadávání veřejných zakázek, upravující rámcové dohody se použijí přiměřeně.

4. Tato Smlouva může být změněna pouze dohodou stran prostřednictvím písemných dodatků podepsaných oběma smluvními stranami, pokud se nejedná o změnu kontaktních osob dle čl. XIV. této Smlouvy, která může být činěna jednostranným písemným oznámením smluvní strany, která změnu oznamuje.

5. Veškeré spory mezi smluvními stranami vzniklé z této Smlouvy nebo v souvislosti s ní budou řešeny, pokud možno, nejprve smírnou cestou – dohodou. Smluvní strany se dohodly, že nedojde-li k dohodě, místně příslušným soudem pro řešení případných sporů bude soud příslušný dle místa sídla Objednatele.

6. Smluvní strany tímto prohlašují, že neexistuje žádné ústní ujednání, dohoda či řízení některé strany, které by nepříznivě ovlivnilo výkon jakýchkoliv práv a povinností dle této Smlouvy. Zároveň potvrzují svým podpisem, že veškerá ujištění a dokumenty dle této Smlouvy jsou pravdivé, platné a právně vymahatelné.

7. Jestliže se ukáže jakékoliv ustanovení této Smlouvy jako neplatné, nevymahatelné nebo neúčinné, nedotýká se tato neplatnost, nevymahatelnost nebo neúčinnost ostatních ustanovení této Smlouvy. Smluvní strany se zavazují nahradit do patnácti (15)

pracovních dnů od doručení výzvy jedné smluvní strany druhé smluvní straně neplatné, neúčinné nebo nevymahatelné ustanovení ustanovením platným, účinným a vymahatelným se stejným nebo obdobným smyslem.

8. Tato Smlouva je podepsána elektronicky.

9. Každá ze smluvních stran prohlašuje, že tuto Smlouvu uzavírá svobodně a vážně, že považuje obsah této Smlouvy za určitý a srozumitelný, a že jsou jí známy veškeré skutečnosti, jež jsou pro uzavření této Smlouvy rozhodující, na důkaz čehož připojují smluvní strany k této Smlouvě své podpisy.

ČLÁNEK XIV.
KONTAKTNÍ OSOBY

1. Kontaktní osoby pro jednání ve věcech Smlouvy, ve věcech technických, ve věcech kybernetické bezpečnosti a ve věcech ochrany osobních údajů jsou:

a) za Objednatele ve věcech Smlouvy (včetně akceptací plnění, podepisování akceptačních protokolů a Ad-hoc objednávek):

[redacted]

b) za Objednatele ve věcech technických:

[redacted]

nebo

[redacted]

c) za Zhotovitele ve věcech Smlouvy:

[redacted]

d) za Zhotovitele ve věcech technických:

[redacted]

2. Obě smluvní strany jsou oprávněny jednostranně změnit kontaktní osoby bez nutnosti uzavření dodatku k Smlouvě, přičemž změna je účinná doručením písemného oznámení o takové změně druhé smluvní straně.

Přílohy:

Příloha č. 1 – Specifikace předmětu plnění - vytvoření NCS, údržba, rozvoj a monitoring NCS
Příloha č. 2 – Vzor Akceptačního protokolu
Příloha č. 3 – Seznam členů realizačního týmu

V Praze dne [*dle el. podpisu*]

[redacted]……………………..
agentura
Mgr. Bohdan Urban
ředitel

V Praze dne [*dle el. podpisu*]

[redacted]
MONET+, a.s.
Ing. Břetislav Endrys
předseda představenstva

[redacted]
MONET+, a.s.
Ing. Janem Vavrysem
člen představenstva

Technická specifikace veřejné zakázky „Národní certifikační schéma EUDIW, jeho údržba, rozvoj a monitoring jeho uplatňování II”

Obsah

1. Použité zkratky

Zkratka	Vysvětlení
EUDIW	Evropská peněženka digitální identity ve smyslu čl. 3 odst. 42 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění
ARF	Architecture and Reference Framework, https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/
nařízení eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění. Konsolidované (informativní) znění: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:02014R0910-20241018
CIR 2024/2981	Prováděcí nařízení Komise (EU) 2024/2981 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o certifikaci evropských peněženek digitální identity, https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32024R2981
Návrh adaptační legislativy	Návrh zákona, kterým se mění zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, a další související zákony, https://odok.gov.cz/portal/veklep/material/ALBSDHZA32NV/

Zkratka	Vysvětlení
WSCD	Wallet Secure Cryptographic Device - „bezpečný kryptografický prostředek peněženky“ je prostředek odolný proti neoprávněné manipulaci, který poskytuje prostředí propojené s bezpečnou kryptografickou aplikací peněženky a používaný touto aplikací k ochraně kritických aktiv a poskytování kryptografických funkcí pro bezpečné provádění kritických operací
WSCA	Wallet Secure Cryptographic Device Application - „bezpečná kryptografická aplikace peněženky“ aplikace, která spravuje kritická aktiva prostřednictvím propojení s kryptografickými a nekryptografickými funkcemi poskytovanými bezpečným kryptografickým prostředkem peněženky a jejich využívání
PID	Person identification data - „osobní identifikační údaje“ soubor údajů vydaných v souladu s právem Unie nebo vnitrostátním právem a umožňujících určit totožnost fyzické či právnické osoby nebo fyzické osoby zastupující jinou fyzickou či právnickou osobu
HSM	Hardware Security Module - hardwarový bezpečnostní modul
CSA	Cybersecurity Act - Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“). Konsolidované znění: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:02019R0881-20250204
ENISA (AHWG)	Ad Hoc Working Group zřízená na základě čl. 49 odst. 4 CSA
CIR 2025/848	Prováděcí nařízení Komise (EU) 2025/848 ze dne 6. května 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o registraci stran spoléhajících se na peněženku

Zkratka	Vysvětlení
NCCA	Vnitrostátní orgán certifikace kybernetické bezpečnosti podle článku 58.1 nařízení CSA
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost

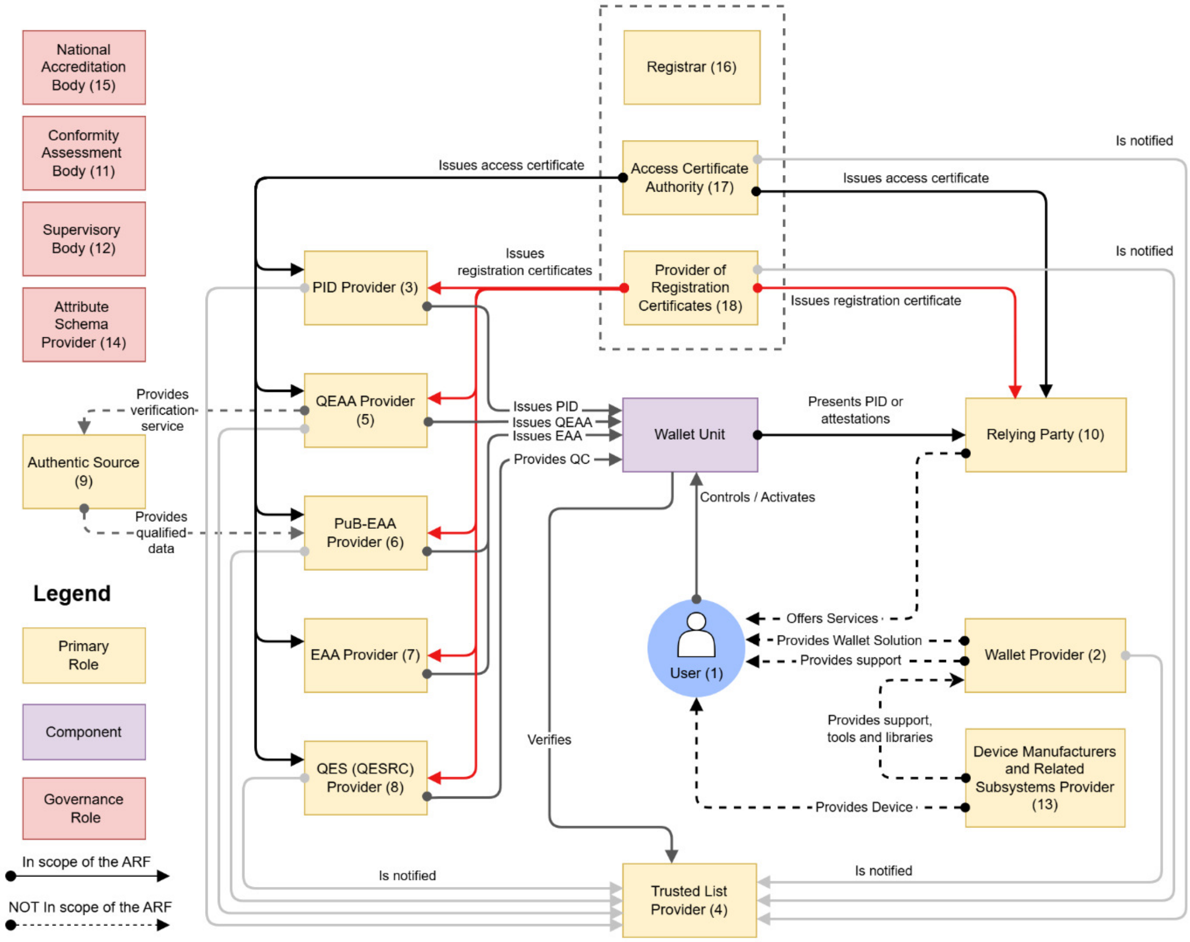
2. Předmět veřejné zakázky

Veřejná zakázka má dvě základní plnění:

1. vytvoření národního certifikačního schématu pro certifikaci evropské peněženky digitální identity (dále jen „EUDIW“)
2. údržba, rozvoj a monitoring národního certifikačního schématu EUDIW na základě jednotlivých požadavků Digitální a informační agentury (Objednatele).

3. Základní informace

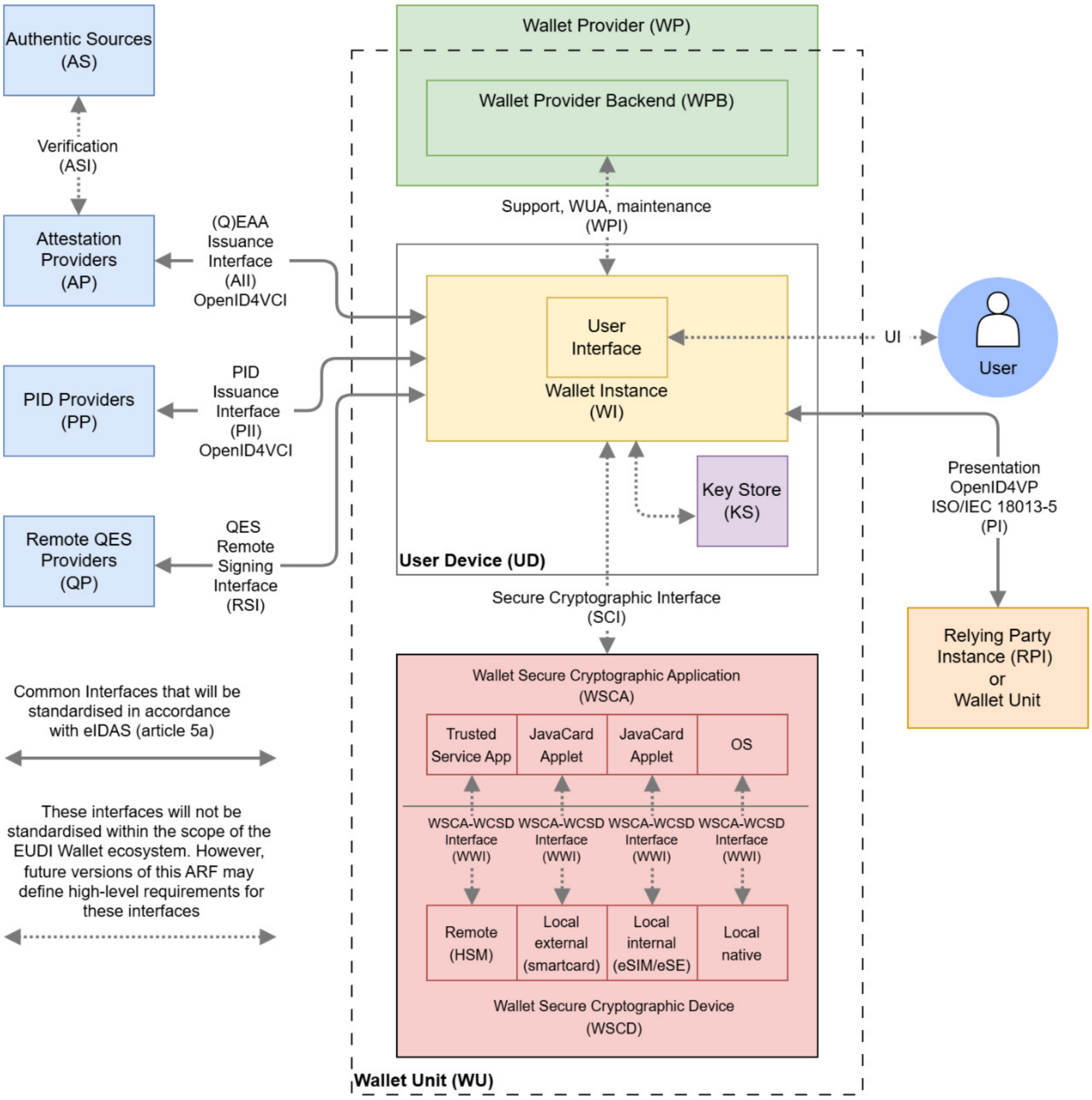
Ekosystém budovaný kolem EUDIW lze vyjádřit následujícím schématem:



Obr. 1 - ekosystém EUDIW, zdroj: ARF

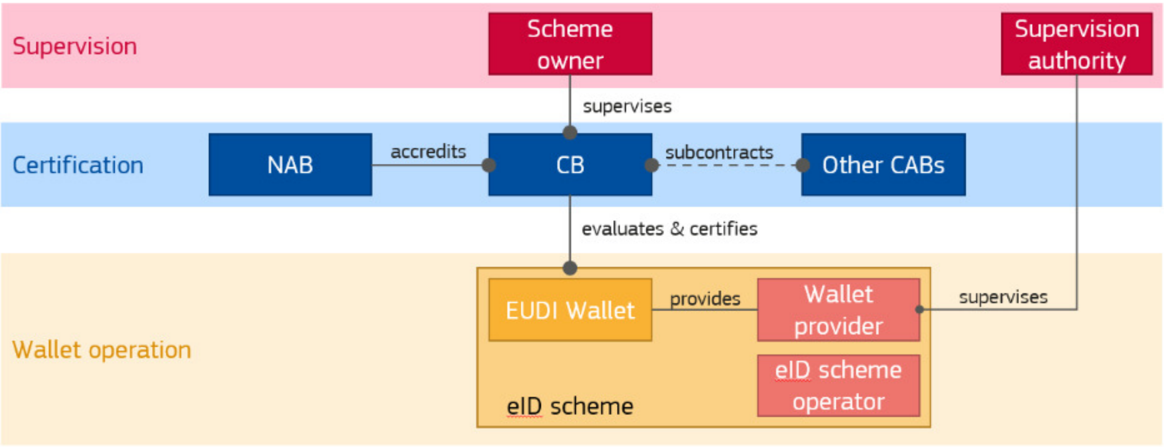
Certifikační schéma bude používáno ze strany certifikačního subjektu (conformity assesment body - 11) pro certifikaci EUDIW a systému elektronické identifikace, v rámci kterého je EUDIW vydávána. Certifikační schéma je rovněž nutné pro účely akreditace certifikačního subjektu ze strany národního akreditačního orgánu (National Accreditation Body – 15).

Wallet unit (jednotka peněženky) představuje jedinečnou konfiguraci řešení peněženky, která zahrnuje instance peněženky, bezpečné kryptografické aplikace peněženky a bezpečné kryptografické prostředky peněženky, které poskytovatel peněženky (Wallet Provider - 2) poskytuje jednotlivému uživateli peněženky. Graficky vyjádřeno:


Authentic Sources (AS)
Verification (ASI)
Attestation Providers (AP)
(Q)EAA Issuance Interface (AII) OpenID4VCI
PID Providers (PP)
PID Issuance Interface (PII) OpenID4VCI
Remote QES Providers (QP)
QES Remote Signing Interface (RSI)
Common Interfaces that will be standardised in accordance with eIDAS (article 5a)
These interfaces will not be standardised within the scope of the EUDI Wallet ecosystem. However, future versions of this ARF may define high-level requirements for these interfaces
Wallet Provider (WP)
Wallet Provider Backend (WPB)
Support, WUA, maintenance (WPI)
User Interface
Wallet Instance (WI)
Key Store (KS)
User Device (UD)
UI
User
Presentation OpenID4VP ISO/IEC 18013-5 (PI)
Relying Party Instance (RPI) or Wallet Unit
Secure Cryptographic Interface (SCI)
Wallet Secure Cryptographic Application (WSCA)
Trusted Service App
JavaCard Applet
JavaCard Applet
OS
WSCA-WCSD Interface (WWI)
WSCA-WCSD Interface (WWI)
WSCA-WCSD Interface (WWI)
WSCA-WCSD Interface (WWI)
Remote (HSM)
Local external (smartcard)
Local internal (eSIM/eSE)
Local native
Wallet Secure Cryptographic Device (WSCD)
Wallet Unit (WU)

Obr. 2 dekompozice jednotky peněženky a její rozhraní s dalšími entitami, zdroj: ARF

Role v rámci certifikace EUDIW lze vyjádřit pomocí následujícího schématu:



Obr. 3 - role v rámci certifikace, zdroj: EK – EUDI Wallet Certification: Roles and Responsibilities

Digitální a informační agentura bude předávat informace a případné výstupy vzešlé ze spolupráce členských států v oblasti vytváření certifikačních schémat, ke který bude mít přístup. V případě, že se Česká republika rozhodne spolupracovat s jinými členskými státy v oblasti budování národních certifikačních schémat, tak Digitální a informační agentura zapojí do této spolupráce rovněž vybraného Zhotovitele.

Digitální a informační agentura zároveň nevylučuje možnost spolupráce na vytvoření národního certifikačního schématu s potencionálními certifikačními orgány či subjekty posuzování shody.

4. Vytvoření národního certifikačního schématu

Předmětem této části veřejné zakázky je vytvoření národního certifikačního schématu pro EUDIW v České republice v českém a anglickém jazyku, a to v souladu se všemi relevantními právními předpisy, zejména:

- nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění (dále jen „nařízení eIDAS“)
- prováděcí nařízení Komise (EU) 2024/2981 ze dne 28. listopadu 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o certifikaci evropských peněženek digitální identity (dále jen „CIR 2024/2981“),
- prováděcí akty, které blíže definují a upřesňují příslušné technické standardy, specifikace, a postupy týkající se zajištění fungování evropských peněženek digitální identity (dále jen „EUDIW“)

Národního certifikační schéma pro EUDIW musí reflektovat rovněž Architektonický a referenční rámec[1] („ARF“).

Podle čl. 5c odst. 1 shodu EUDIW a systému elektronické identifikace, v jehož rámci jsou poskytovány, s požadavky stanovenými v čl. 5a odst. 4, 5 a 8 nařízení eIDAS, s požadavkem na

[1] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/

logické oddělení stanoveným v čl. 5a odst. 14 nařízení eIDAS a případně s normami a technickými specifikacemi uvedenými v čl. 5a odst. 24 certifikují subjekty posuzování shody určené členskými státy. Národní certifikační schéma dle CIR 2024/2981 má stanovit požadavky a postupy pro certifikaci evropských digitálních peněženek prováděné akreditovanými orgány pro posuzování shody na národní úrovni.

Požadavky na národní certifikační schéma vychází z čl. 5c nařízení eIDAS a jsou primárně uvedeny v CIR 2024/2981. Vlastníkem národního certifikačního schématu by měla být Digitální a informační agentura dle připravované adaptační legislativy[2] (dále jen „návrh adaptační legislativy“), která je aktuálně v legislativním procesu.

Zhotovitel rovněž musí poskytovat plnou spolupráci včetně účasti na jednání skupiny pro evropskou spolupráci v oblasti digitální identity zřízené podle čl. 46e odst. 1 nařízení eIDAS v souvislosti s požadavkem uvedeném ve čl. 5c odst. 3 podle kterého musí členské státy předat své návrhy vnitrostátních schémat certifikace skupině pro evropskou spolupráci v oblasti digitální Tato skupina pro spolupráci může vydávat stanoviska a doporučení, které by měl členský stát reflektovat, respektive zapracovat.

4.1. Předmět a rozsah certifikace

Podle čl. 5c odst. 1 shodu EUDIW a systému elektronické identifikace, v jehož rámci jsou poskytovány, s požadavky stanovenými v čl. 5a odst. 4, 5 a 8 nařízení eIDAS, s požadavkem na logické oddělení stanoveným v čl. 5a odst. 14 nařízení eIDAS a případně s normami a technickými specifikacemi uvedenými v čl. 5a odst. 24 certifikují subjekty posuzování shody určené členskými státy.

Certifikační schéma má dle čl. 4 CIR 2024/2981 pokrývat požadavky na funkčnost, kybernetickou bezpečnost a ochranu údajů. Předmětem certifikace podle národního certifikačního schématu je tak dle čl. 3 odst. 2 CIR 2024/2981 poskytování a fungování řešení peněženky („wallet solution“) a systému elektronické identifikace, v jejichž rámci se poskytují a zahrnuje:

- softwarové komponenty, včetně nastavení a konfigurace řešení peněženky a systému elektronické identifikace, v jehož rámci jsou řešení peněženky poskytována;
- hardwarové komponenty a platformy, na kterých běží softwarové komponenty nebo se na ně spoléhají při kritických operacích v případech, kdy jsou poskytovány přímo nebo

[2] https://odok.gov.cz/portal/veklep/material/ALBSDHZA32NV/

nepřímo řešením peněženky a systémem elektronické identifikace, v jehož rámci je poskytováno, a kdy jsou vyžadovány pro splnění požadované úrovně záruky těchto softwarových komponentů. Pokud hardwarové komponenty a platformy neposkytuje poskytovatel peněženky, vnitrostátní systémy certifikace stanoví předpoklady pro hodnocení hardwarových komponentů a platforem, podle něhož lze zajistit odolnost proti útočníkům s vysokým potenciálem útoku v souladu s prováděcím nařízením (EU) 2015/1502, a stanoví hodnoticí činnosti k potvrzení těchto předpokladů, jak je uvedeno v příloze IV CIR 2024/2981

- procesy, které podporují poskytování a fungování řešení peněženky, včetně procesu onboardingu uživatelů, a které zahrnují alespoň přihlášení, správu prostředků pro elektronickou identifikaci a organizaci podle oddílu 2.1, 2.2 a 2.4 přílohy I prováděcího nařízení (EU) 2015/1502,

Obecné požadavky na národní certifikační schéma jsou stanoveny ve čl. 4 CIR 2024/2981. Národní certifikační schéma musí rovněž obsahovat popis konkrétní architektury řešení peněženky a systému elektronické identifikace, v jehož rámci je poskytováno. Pokud vnitrostátní systémy certifikace pokrývají více než jednu konkrétní architekturu, musí obsahovat profil pro každou jednotlivou architekturu. Pro každý profil musí vnitrostátní systémy certifikace stanovit alespoň tyto požadavky:

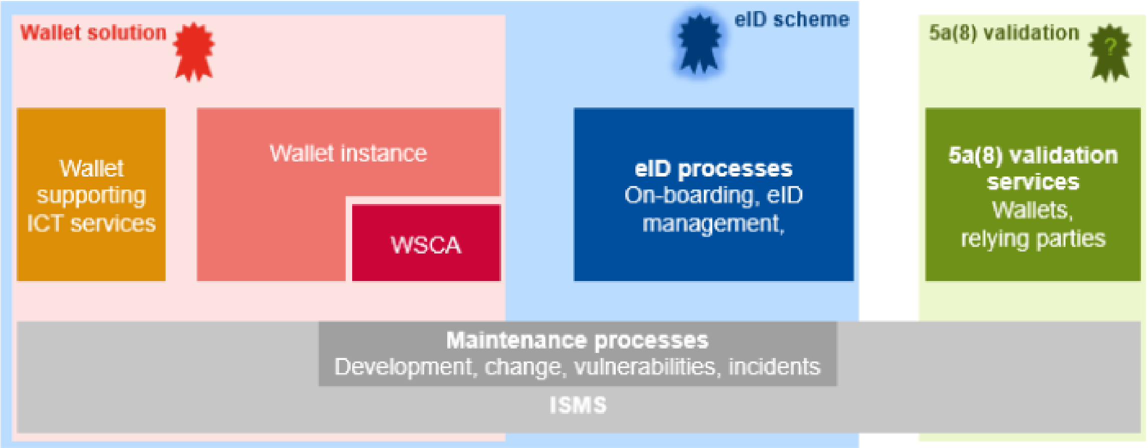
a) konkrétní architekturu řešení peněženky a systému elektronické identifikace, v jehož rámci je poskytováno;
b) bezpečnostní kontroly spojené s úrovněmi záruky stanovenými v článku 8 nařízení eIDAS;
c) plán hodnocení vypracovaný v souladu s oddílem 7.4.1 normy EN ISO/IEC 17065:2012 (má obsahovat seznam hodnoticích činností, které mají být zahrnuty do hodnocení řešení peněženky a systému elektronické identifikace, v jehož rámci jsou poskytována), v rámci hodnoticí činnosti se od poskytovatelů řešení peněženky a systému elektronické identifikace, v jehož rámci se poskytují, se bude požadovat, aby poskytli informace splňující požadavky uvedené v příloze II CIR 2024/2981
d) bezpečnostní požadavky nezbytné k řešení kybernetických bezpečnostních rizik a hrozeb uvedených v registru rizik stanoveném v příloze I tohoto nařízení, a to až do požadované úrovně záruky, a případně ke splnění cílů vymezených v článku 51 nařízení (EU) 2019/881;

e) přiřazení kontrol uvedených v písmenu (b) tohoto odstavce ke komponentům architektury;

f) popis toho, jak bezpečnostní kontroly, přiřazení kontrol, bezpečnostní požadavky a plán hodnocení uvedené v písmenech (b) až (c) umožňují poskytovatelům řešení peněženek a systému elektronické identifikace, v jehož rámci jsou poskytována, odpovídajícím způsobem řešit kybernetická bezpečnostní rizika a hrozby identifikované v registru rizik podle písmena (d), a to až do požadované úrovně záruky na základě posouzení rizik s cílem upřesnit rizika a hrozby uvedené v registru a doplnit je o rizika a hrozby specifické pro architekturu.

Architekturu EUDIW lze rozdělit do čtyř hlavních komponent:

- řešení peněženky sestávající z ICT služeb podporující EUDIW a instance peněženky
- systém elektronické identifikace sestávající z procesů jako je onboarding či správa prostředku pro elektronickou identifikaci,
- ověřovací služby pro peněženky a spoléhající se strany dle čl. 5a(8) nařízení eIDAS,
- systém řízení bezpečnosti informací (ISMS) a procesy údržby, jako je vývoj, správa změn, správa zranitelností a správa incidentů.


Wallet solution
eID scheme
5a(8) validation
?
Wallet supporting ICT services
Wallet instance
WSCA
eID processes
On-boarding, eID management,
5a(8) validation services
Wallets, relying parties
Maintenance processes
Development, change, vulnerabilities, incidents
ISMS

Obr. 4 - typy certifikátů, zdroj: EK – EUDI Wallet Certification: TopicIII: Ad Hoc Working Group Conclusions

S ohledem na skutečnost, že v rámci poskytování a fungování řešení peněženky a systému elektronické identifikace, v jejichž rámci se poskytuje, bude zapojeno několik subjektů, bude nutné, aby národní certifikační schéma umožnilo vydání několika certifikátů pro jednotlivé dílčí části. Certifikát pro systém elektronické identifikace je nejvyšší a zahrnuje jednak systém elektronické identifikace sestávající z procesů jako je onboarding či správa prostředků pro elektronickou identifikaci tak i samotné řešení peněženky. Národní certifikační schéma musí umožnit, aby řešení peněženky bylo certifikováno zvláště s ohledem na to, že řešení peněženky může být poskytováno různými subjekty. S ohledem na to, že poskytovatelem EUDIW nebude s největší pravděpodobností přímo stát, bude potřebné vydat dva různé certifikáty.

Povinnost zajistit ověřovací služby pro peněženky a spoléhající se strany dle čl. 5a(8) nařízení eIDAS je stanovena pro členské státy, nikoliv pro poskytovatele EUDIW.

4.2. Hodnocení rizik a zranitelností

Při vytváření certifikačního schématu je nutné provést posouzení rizik a zranitelností s cílem upřesnit rizika a hrozby uvedené v registru rizik dle CIR 2024/2981 a doplnit je o rizika a zranitelnosti (hrozby) specifické pro architekturu nebo zavádění daného řešení peněženky. Posouzení rizik by mělo zvážit, jak lze příslušná rizika a hrozby vhodně ošetřit. Poskytovatelé peněženek a systému elektronické identifikace by měli doplnit posouzení rizik systému s cílem určit veškerá rizika a hrozby specifické pro jejich zavádění a navrhnout vhodná opatření pro jejich řešení, která vyhodnotí certifikační subjekt. Národní certifikační schéma musí obsahovat požadavky na řízení incidentů a zranitelností v souladu s požadavky uvedenými ve čl. 5 CIR 2024/2981.

Z nařízení eIDAS (čl. 5c odst. 4) rovněž vyplývá požadavek, aby certifikační orgán každé dva roky prováděl hodnocení zranitelnosti, viz rovněž harmonogram povinných hodnocení dozoru uvedený v příloze IX CIR 2024/2981. Posouzení zranitelnosti každé dva roky má zajistit, aby řešení peněženky i nadále vhodně krylo kybernetická bezpečnostní rizika a hrozby identifikované v registru rizik, včetně případného vývoje v oblasti hrozeb. Z čehož plyne, že je nutné v rámci certifikačního schématu definovat požadavky na toto hodnocení zranitelnosti.

4.3. Národní architektura

Jak bylo uvedeno výše, národní certifikační schéma musí reflektovat také národní architekturu řešení peněženky a systému elektronické identifikace, v jehož je řešení poskytováno, přičemž základní požadavky či předpoklady jsou shrnuty v následujících podkapitolách. Zhotovitel si vyhrazuje právo tyto předpoklady požadavky změnit či upravit, pokud to okolnosti budou vyžadovat.

4.2.2 Forma EUDIW

První verze národního certifikačního schématu musí obsahovat požadavky a postupy týkající se certifikace EUDIW reflektující skutečnost, že instance EUDIW bude realizována ve formě mobilní aplikace instalované na zařízení uživatele (pro Android a iOS), při následném rozvoji certifikačního schématu může být na základě požadavku Digitální a informační agentury doplněn další profil týkající se jiných forem instance EUDIW (např. cloudová aplikace).

Digitální a informační agentura bude poskytovat Zhotoviteli součinnost pro účely popisu národní architektury řešení peněženky a systému elektronické identifikace, v jehož rámci je řešení poskytováno. V případě, když by došlo ke změnám výše popsané základní architektury, bude Digitální a informační agentura bez odkladu informovat Zhotovitele.

4.2.3 Vydávání PID

Vydávání osobních identifikačních údajů (dále jen „PID“) do EUDIW bude zajištěno příslušným státním orgánem, přičemž tímto státním orgánem by měla být dle návrhu adaptační legislativy Digitální a informační agentura, která bude vydávat tyto osobní identifikační údaje do EUDIW uživatele, u kterého byla předtím ověřena totožnost v souladu s požadavky nařízení eIDAS a jeho prováděcími akty na úroveň záruky vysoká. Pro účely zajištění podpůrných procesů týkající se pečetění vydaných PID, se počítá s využitím služeb poskytovaných Správou státních služeb vytvářejících důvěru, s. p. o.

Předpokládáme, že ověření totožnosti před vydáním PID do EUDIW bude umožněno několika způsoby:

a) ověření totožnosti prezenčně
b) ověření totožnosti vzdáleně pomocí prostředku pro elektronickou identifikaci s úrovní záruky vysoká
c) ověření totožnosti vzdáleně pomocí prostředku pro elektronickou identifikaci splňující značnou úroveň záruky plus dodatečná opatření ve smyslu čl. 5a odst. 24 nařízení eIDAS (příslušný prováděcí akt zatím nebyl vydán, probíhá příprava tohoto prováděcího aktu na úrovni EU)

Ověření totožnosti před vydáním PID by měl provádět budoucí poskytovatel EUDIW, který bude vybrán na základě probíhající veřejné zakázky (https://nen.nipez.cz/verejne-zakazky/detail-zakazky/N006-25-V00006605) a to jak pro EUDIW, který bude sám poskytovat, tak i pro účely případných jiných EUDIW, které by byly v České republice poskytovány.

Konkrétně by vybraný subjekt měl zajistit prezenční ověřování totožnosti a dále ověřování totožnosti pomocí prostředku pro elektronickou identifikaci splňující značnou úroveň záruky plus dodatečná opatření ve smyslu čl. 5a odst. 24 nařízení eIDAS v souladu s budoucím prováděcím aktem.

Dále není vyloučeno, že v České republice by mohly existovat také další subjekty, které by ověřovaly totožnost (zejména prezenčně) pro účely vydání PID do EUDIW a to např. v průběhu procesu žádosti o vydání nového občanského průkazu nebo cestovního pasu. V takovém případě musí certifikační schéma reflektovat rovněž tuto možnost – opět by takovýto způsob byl využitelný pro účely všech EUDIW, které by v České republice byly do budoucna poskytovány.

4.2.4 Architektura WSCD

Bezpečný kryptografický prostředek peněženky (dále jen „WSCD“) je zásadní součástí řešení EUDIW, protože tato komponenta provádí kryptografické funkce, včetně ukládání a správy kryptografických klíčů. Je proto jedním z hlavních určujících faktorů úrovně zabezpečení EUDIW. ARF definuje čtyři odlišná architektonická řešení pro WSCD: vzdálený WSCD (Remote WSCD), lokální externí WSCD (Local external WSCD), lokální interní WSCD (Local internal WSCD) a lokální nativní WSCD (Local native WSCD). S ohledem na potřebu zajistit vydání EUDIW do konce roku 2026, možnost použití EUDIW u širokého okruhu uživatelů, a zároveň „certifikovatelnost“ takového řešení, je logickou volbou aktuálně architektura vzdáleného WSCD spočívající ve využití vzdálených HSM. Nevýhodou tohoto řešení je, že ho lze využívat jen v rámci online scénáře, tj. když EUDIW uživatele je on-line.

Za účelem zajištění také možnosti využívat EUDIW v off-line scénářích, poskytovatel EUDIW může umožnit uživatelům využívat také lokální externí WSCD, které by uživatelům vydával poskytovatel EUDIW.

První verze certifikačního schématu tak musí pokrývat následující architekturu WSCD:

- vzdálený WSCD (Remote WSCD),
- lokální externí WSCD (Local external WSCD).

V rámci budoucí aktualizace národního certifikačního schématu předpokládáme podporu pro lokální interní WSCD (Local internal WSCD) nebo lokální nativní WSCD (Local native WSCD), jakmile bude na trhu existovat dostatek zařízení a bude možné tyto varianty architektury WSCD certifikovat.

4.2.5 Registrace spoléhajících se stran na peněženku

Nezbytnou součástí ekosystému budovaného kolem EUDIW, je rovněž registr stran spoléhajících se na peněženku. Povinnost zajistit tento registr vyplývá ze samotného nařízení eIDAS (čl. 5b), přičemž další podrobnosti jsou uvedeny v prováděcím nařízení Komise (EU) 2025/848 ze dne 6. května 2025, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o registraci stran spoléhajících se na peněženku (dále jen „CIR 2025/848)“

Spoléhající se strana, které hodlá spoléhat na evropské peněženky digitální identity pro účely poskytování veřejných nebo soukromých služeb prostřednictvím digitální interakce, má být zaregistrována v členském státě, v němž je usazena. Správcem tohoto registru by měla být dle návrhu adaptační legislativy Digitální a informační agentura. Tento registr je klíčovou součástí pro podporu umožnění autentizace a identifikace stran spoléhajících se na peněženku a zavedení bezplatného mechanismu ověřování platnosti s cílem umožnit uživatelům EUDIW ověřit pravost a platnost totožnosti stran spoléhajících se na peněženku registrovaných v souladu s článkem 5b nařízení eIDAS (viz čl. 5a odst. 8 nařízení eIDAS).

Mechanismus ověřování pravosti a platnosti evropských peněženek digitální identity a totožnosti registrovaných stran spoléhajících se na peněženku je rovněž v rámci předmětu certifikace.

Vydavatelem přístupových certifikátů strany spoléhající se na peněženku by měla být Správa státních služeb vytvářejících důvěru, s. p. o., vydavatelem registračních certifikátů strany spoléhající se na peněženku by měla být Digitální a informační agentura.

4.4. Struktura národního certifikačního schématu

V rámci pracovní skupiny AHWG organizované agenturou ENISA vznikl dokument „draft National Certification Scheme Template“, který je ve své aktuální verzi uveden jako příloha I těchto technických specifikací. Dokument je ve fázi návrhu a tak dokument nelze považovat za finální, bude se postupně vyvíjet.

Dokument obsahuje předběžný návrh šablony pro národní certifikační schéma pro certifikace EUDIW. Je přímo inspirován návrhem evropského schématu certifikace kybernetické bezpečnosti, který vyvíjí agentura ENISA s pomocí pracovní skupiny AHWG. Hlavním cílem tohoto dokumentu je identifikovat oblasti, které je třeba upravit tak, aby splňovali specifické požadavky národních schémat certifikace EUDIW. Cílem je však maximalizovat společné rysy mezi národními schématy a budoucím evropským schématem pro certifikaci kybernetické bezpečnosti, což minimalizuje následné úsilí potřebné k přechodu z jednoho schématu na druhý.

Šablona se pokouší jasně identifikovat, jaké rozhodnutí musí vlastníci schémat učinit při definici svého certifikačního schématu. Každý článek je doplněn poznámkami a diskusními body a eventuálními příklady.

Obsah dokumentu bude ještě pře-uspořádán následně, aby se snáze používal jako základ pro schéma a akreditaci subjektů posuzování shody, respektive certifikačních orgánů. Ve své současné podobě je tento dokument zejména určen jako základ pro výměnu názorů s členskými státy a jako úložiště nápadů či myšlenek pro členské státy, které vyvíjejí své národní certifikační schémata.

Dokument lze tak použít jako podklad pro tvorbu národního certifikačního schématu v České republice. Případné další verze tohoto dokumentu bude objednatel sdílet se zhotovitelem.

Při vytváření národního certifikačního schématu Zhotovitel musí rovněž reflektovat relevantní požadavky dokumentu „EA-1/22 A-AB: 2023 - Postup a kritéria pro hodnocení schémat posuzování shody akreditačními orgány - členy EA“[3], IAF MD25:2023 - Kritéria pro hodnocení schémat posuzování shody[4] a MPA 70-01-24 - Postup pro přezkoumání podkladů u sektorových certifikačních schémat a nestandardních inspekčních metod[5], nebo jejich případné aktualizace.

4.5. Požadovaný scénář dodávky národního certifikačního schématu

Objednatel požaduje po Zhotoviteli, aby se při tvorbě národního certifikačního schématu nejdříve zaměřil na oblast vybudování a provozu řešení peněženky, vydávání PID, onboardingu uživatelů (tj. ověření totožnosti za účelem vydání PID do peněženky), mechanismu umožňující identifikaci a autentizaci stran spoléhajících se na peněženku, mechanismu ověřování pravosti a platnosti evropských peněženek digitální identity a funkci elektronické identifikace a autentizace prostřednictvím peněženky, při kterém se předávají údaje z PID. Výše uvedené může být dále upřesněno na základě pokynů zhotovitele.

[3] https://www.cai.cz/wp-content/uploads/2024/02/01_08-P043-EA-01_22-A_2023_20240223.pdf

[4] https://www.cai.cz/wp-content/uploads/2023/09/01_08-P062-IAF-MD25_2023_20230904.pdf

[5] https://www.cai.cz/wp-content/uploads/2025/11/02_03-MPA-70-01-24-Postup-pro-prezkoumani-sektorovych-schemat-a-inspekcnich-metod_20240223o.pdf

5 Údržba, rozvoj a monitoring národního certifikačního schématu

Druhá část plnění veřejné zakázky spočívá v průběžné aktualizaci národního certifikačního schématu na základě požadavků Digitální a informační agentury jakožto vlastníka certifikačního schématu, která podněty na rozvoj či úpravu certifikačního schématu může získat například na základě vlastní činnosti, nebo od certifikačních subjektů, akreditačního orgánu, ze stanovisek či doporučení skupiny pro evropskou spolupráci v oblasti digitální identity zřízené podle čl. 46e odst. 1 nařízení eIDAS nebo od jiných relevantních stakeholderů. Jednotlivé požadavky na rozvoj či údržbu certifikačního schématu budou před zadáním požadavku na úpravu certifikačního schématu nejdříve dohodnuty mezi Zhotovitelem a Objednatelem (a případnými dalšími stakeholdery), před jejich formálním zadáním na realizaci. V rámci údržby národního certifikačního schématu bude nutné pravidelně přezkoumávat provoz schématu, přičemž cílem tohoto procesu je potvrdit přiměřenost schématu a určit aspekty, které vyžadují zlepšení, s přihlédnutím ke zpětné vazbě od stakeholderů.

5.2 Předpokládané budoucí změny certifikačního schématu

V budoucnu bude nutné národní certifikační schéma upravit v souvislosti s předpokládaným přijetím společného certifikačního schématu pro certifikaci kybernetických požadavků vytvořeného na základě nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) – dále jen „CSA“. Nicméně pro certifikaci funkčních požadavků, národní certifikační schéma by se mělo používat nadále.

Vnitrostátní orgán certifikace kybernetické bezpečnosti (dále jen „NCCA“) v ČR NÚKIB - bude následně odpovědný za dohled nad evropským schématem pro certifikaci EUDIW a jeho vymáhání (podle článku 58.1 nařízení CSA 2019/881).

Pokud jde o příklady dalšího možného budoucího rozvoje certifikačního schématu, jedná se například o rozvoj certifikačního schématu s ohledem na možnou potřebu certifikace EUDIW pro právnické osoby, či přidání profilu pro certifikaci jiných forem instance EUDIW (např. cloudová aplikace).

5.3 Údržba schématu

Povinnosti Zhotovitele týkající se údržby schématu budou specifikovány v jednotlivých Ad-hoc objednávkách. Objednatel předpokládá, že odpovědností Zhotovitele bude provádět periodickou revizi certifikačního schématu alespoň 1x ročně a také při změně příslušné legislativy (včetně implementačních aktů) či technických standardů a doporučení. Objednatel předpokládá, že v Ad-hoc objednávce bude stanovena povinnost Zhotovitele vést dokumentaci změn a jednotlivých verzí, archivovat starší verze a za tímto účelem využívat vhodný systém pro sledování změn a organizaci požadavků.

Požadavky na údržbu vnitrostátních systémů certifikace jsou stanoveny ve čl. 6 CIR 2025/848.

5.4 Rozvoj schématu

Rozvoj certifikačního schématu reaguje na požadavky zadavatele (podněty na rozvoj či úpravu certifikačního schématu může získat zadavatel například na základě vlastní činnosti, nebo od certifikačních subjektů, akreditačního orgánu či jiných relevantních stakeholderů), které reflektují požadované architektonické nebo funkční změny v ekosystému EUDIW a eGovernmentu v ČR. Zadavatel předpokládá, že v Ad-hoc objednávce bude stanoveno, že požadavky a podněty budou ve formě žádostí o změny zaznamenávány v systému pro správu požadavků (viz kap. 5.2), a budou přístupné zadavateli a dodavateli ve strukturované formě tak, aby bylo možné rovněž sledovat proces řešení požadavků nebo podnětů. Zadavatel si vyhrazuje právo před schválením realizace požadavků na rozvoj či úpravy tyto změny konzultovat s relevantními stakeholdery.

Zadavatel předpokládá, že součástí aktivit na rozvoji certifikačního schématu bude vytvoření a aktualizace roadmapy rozvoje (Strategická plánovací mapa vývoje a rozšíření na základě priorit podle potřeb zadavatele, trhu a legislativy).

Jak je uvedeno v kap. 5.1, po schválení společného evropského certifikačního schématu EUDIW pro certifikaci kybernetických požadavků vytvořeného na základě CSA, bude potřeba národní certifikační schéma upravit tak, aby obsahovalo pouze funkční požadavky na certifikaci a dále zajistit případnou harmonizaci národního schématu s evropským schématem. Národní úřad pro kybernetickou bezpečnost (dále jen „NÚKIB“) bude následně odpovědný za dohled nad tímto evropským schématem pro certifikaci EUDIW a jeho vymáhání na základě článku 58.1 nařízení CSA. Zadavatel předpokládá, že také tato část plnění bude předmětem Ad-hoc objednávky.

Platí, že Národní certifikační schéma bude rozvíjeno s ohledem na výstupy aktivit mezinárodní spolupráce v příslušných pracovních skupinách ENISA (AHWG), Evropské komise (working group on certification zřízené v rámci skupiny pro evropskou spolupráci v oblasti digitální identity zřízené podle čl. 46e odst. 1 nařízení eIDAS) nebo stanoviska a doporučení skupiny pro evropskou spolupráci v oblasti digitální identity zřízené podle čl. 46e odst. 1 nařízení eIDAS), aj. a s ohledem na rozvoj souvisejících evropských a obdobných národních schémat.

5.5 Monitoring a dozor

Monitoring a dozor bude vykonáván zadavatelem ve spolupráci se Zhotovitelem, a to na základě Ad-hoc objednávky (či objednávek). Monitoring bude probíhat alespoň na základě těchto informací:

- informací od certifikačních subjektů, vnitrostátních akreditačních orgánů a příslušných orgánů dozoru nad trhem;
- informací vyplývajících z vlastních auditů a šetření nebo auditů a šetření jiného orgánu;
- stížností a odvolání podle čl. 15 CIR 2025/848.

Účelem monitoringu bude rovněž vyhodnocování účinnosti a efektivity schématu.

Pokud jde o dozorové činnosti, tak národní certifikační schéma musí dle čl. 16 CIR 2025/848 obsahovat požadavky na vlastníka schématu (Objednatel), aby monitoroval soulad certifikačních subjektů s povinnostmi vyplývajícími z nařízení eIDAS a případně z vnitrostátních schémat certifikace. Monitoring by měl rovněž zahrnovat případné výskyty incidentů a bezpečnostních problémů, získávání zpětné vazba z auditů a její vyhodnocení, spolupráci s akreditačním orgánem pro kontrolu provádění schématu, a řešení sankčních opatření nebo pozastavení platnosti certifikací při porušení pravidel.

6 Přehled akceptačních milníků

Akceptační milníky pro Vytvoření národního certifikačního schématu

Milník	Název fáze	Hlavní výstupy	Akceptační kritéria
M1	Zahájení projektu	Projektový plán a vytvoření roadmapy pro vytvoření národního certifikačního schématu, komunikační matice	Stanovený a odsouhlasený plán a řízení projektu Objednatelem
M2	Analýza a návrh struktury	Vytvoření návrhu struktury certifikačního schématu,	Předání a odsouhlasení návrhu struktury schématu a

Milník	Název fáze	Hlavní výstupy	Akceptační kritéria
	certifikačního schématu	definování rozsahu certifikace a identifikace systémů / komponent / subjektů. ,	návrhu rozsahu certifikace a identifikace systémů / komponent / subjektů.
M3	Vytvoření prvního návrhu certifikačního schématu	Návrh obsahu první verze schématu včetně metodiky hodnocení a hodnotících kritérií a návrhu doplněného registru rizik.	Dodání a odsouhlasení prvního návrhu certifikačního schématu
M4	Ověření, validace a úpravy prvního návrhu certifikačního schématu	Testování návrhu schématu (např. simulace certifikace na modelovém příkladu) , interní validace a zapracování případných úprav do návrhu certifikačního schématu.	Předání výsledků testování a odsouhlasení upraveného návrhu certifikačního schématu
M5	Akceptace první verze certifikačního schématu a školení	První verze certifikačního schématu a související dokumentace čimetodiky, školení pracovníků, provozní záznamy	Akceptační protokol

Výše uvedené může být dále upřesněno na základě pokynů zhotovitele.

Akceptační milníky pro Údržbu, rozvoj a monitoring národního certifikačního schématu

Akceptační milníky budou stanoveny v jednotlivých Ad-hoc objednávkách. Zadavatel předpokládá, že budou mít následující podobu:

Milník	Název fáze	Hlavní výstupy	Akceptační kritéria
M6	Monitoring a údržba	Zprávy o provozu, aktualizace schématu, evidence změn	Schválená pravidelná zpráva o činnosti a zajištěné mechanismy údržby, upravené certifikační schéma, aj.

7 Závěr

Příprava certifikačního schématu akceptuje a předpokládá využití dokumentů „state-of-the-art (SOTA)“, které umožní flexibilní aktualizaci technických požadavků. Zadavatel si vyhrazuje právo provést odborné oponentní hodnocení výstupů v kterékoli fázi procesu tvorby a aplikace certifikačního schématu.

8 Přílohy

- draft National Certification Scheme Template - National-Scheme-Template-0.2.pdf

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TEMPLATE

Towards national schemes

AUGUST 2025

DOCUMENT HISTORY

//DRAFT ONLY - DELETE THIS SECTION AND PAGE UPON FINAL PUBLICATION

Date	Version	Modification	Author
11/07/2025	0.1	Creation	Eric Vetillard
14/08/2025	0.2	Update after first round of feedback	Eric Vetillard

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union’s agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act ,the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services, and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union’s infrastructure, and, ultimately, to keep Europe’s society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use certification@enisa.europa.eu

For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

ENISA

ACKNOWLEDGEMENTS

TBD

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

ISBN SHOULD BE PLACED HERE, DOI SHOULD BE PLACED HERE (IF APPLICABLE)

TABLE OF CONTENTS

1. INTRODUCTION

1.1 PURPOSE OF THE DOCUMENT

The present document is the first draft of a template for a national scheme for the certification of EUDI Wallets. It is directly inspired from the draft European cybersecurity certification scheme under development at ENISA with the assistance of the AHWG.

The main focus of this document is to identify where the content will be adapted to meet the specific requirements of national schemes. However, the objective is here to maximise the commonalities between the national schemes and the European scheme, which will minimise the effort required to migrate from one to the other.

The template will attempt to clearly identify the choices that remain to be made by the scheme owners in the definition of their scheme. Each article is complemented with notes and with discussion items, and examples have been added where relevant.

Finally, the focus of this document is the content, so the form remains very close to an EU scheme (*i.e.*, a legal text with annexes). The content will be reorganised when it will be more mature, in order to be easier to use as a basis for a scheme and for the accreditation of CABs.

In its current form, this document is intended to be used (1) as a basis for exchanges with Member States, and (2) as a repository of ideas for Member States who are developing their national schemes. More decisions will come later.

1.2 HISTORY OF THE DOCUMENT

This document is adapted from the first draft of the European cybersecurity certification scheme for EUDI Wallets, which has been developed by ENISA with the support of a dedicated Ad Hoc Working Group (EUDIW AHWG).

This document is itself based on EUCC, the first European cybersecurity certification scheme that has been adopted. For this reason, there are some references to the EUCC Implementing Act throughout the document.

1.3 STATUS OF THE DOCUMENT

The document is far from complete, and it has undergone very limited review.

The first category of missing information is the information that is still work in progress in the development of the European scheme, including:

- Security requirements, which are currently under definition in various standards at CEN and ETSI.
- Evaluation methods, which are currently under definition in the EUDIW AHWG for the European scheme.

In addition, a few items that are required in the scheme by Regulation (EU) 2024/2981 or by section 6.5 of EN ISO/IEC 17067 are still missing or incomplete, mostly because they are not covered by default, and it would be preferable to have an exchange on these topics through the EDICG before to make a final proposal. This includes in particular:

- Requirements for the management of complaints and appeals
- Requirements on contracts between the different stakeholders
- Requirements on the references to the certificates
- Requirements on the maintenance of the scheme
- Requirements on responsibilities and legal actions in case of fraudulent use

One category, about requirements to guarantee the consistency of the results, is not directly covered in CSA schemes, but we are currently investigating how we could cover it in national schemes.

Finally, the requirements for accreditation need to be further discussed, in particular to identify the status of that document, which could also be a harmonised document shared by all national schemes.

1.4 PRESENTATION OF THE DOCUMENT

The document is split in chapters that correspond to Chapters in the scheme (or sections for the largest chapters). Each chapter begins with a short introduction that presents the most important focus of the chapter, and points to the relevant Annex(es) that should be considered together with the chapter.

Then, each section corresponds to an article, which starts by a formal text, with notes on every paragraph. In the formal text, elements that need to be replaced with specific national content is outlined in red.

Where relevant, for each article, there is a discussion, as well as a description of remaining action items.

2. GENERAL PROVISIONS

This chapter focuses on the scope of certification, which is outlined here, and defined in greater details in Annex I.

This is Chapter 1 of the scheme.

2.1 SUBJECT MATTER AND SCOPE

The article mostly lists the elements for which certificates may be delivered:

Article 1	Notes on Article 1
(1) This scheme sets out the [EUDIW] certification scheme for European digital identity wallets.	This is mostly about identifying the scheme, modify the [EUDIW] name as needed.
(2) This scheme applies to all information and communication technologies ('ICT') services, including their documentation, which are submitted for certification under the EUDIW, including in particular: (a) services for the provision of European digital identity ('EUDI') wallets and the electronic identity ('eID') schemes under which they are provided; (b) [more things to be certified].	This is the list of items for which certificates will be delivered.

Discussion

This article lists the items that may be certified under the national scheme. It needs to contain at least one item, which is the overall "wallet and eID scheme", as required by eIDAS Article 5c(1). However, it may contain more items, for instance:

- A validation service[1], an ICT service used to verify the validity of wallet units and relying parties.
- A wallet solution, which may be an ICT service or an ICT product, depending on the components that it includes.
- Any component of the wallet that need to be certified separately.
- A specific focus, for instance the cybersecurity of the EUDI Wallet, or the protection of personal data[2].

This list depends on the target architecture and on the capabilities of the certification bodes. Note in particular that the reason why the wallet solution is not identified as a mandatory component to be certified, and that it is defined as being a product or a service, is that its scope and nature depends greatly on the target architecture and on the split of the components between the various stakeholders. A minimal wallet solution could be mostly an ICT product, with minimal support processes, leaving most of the processes to the eID scheme. On the other hand, a comprehensive wallet solution could be a full-fledged ICT services, including most of the processes required to manage the wallet and PID.

[1] Such validation service are defined in eIDAS Article 5a(8), and they are required to be included in the scope of certification in Article 5c(1). Because this service may be provided by another entity, it may be practical to have it certified independently of the other components.

[2] Such certification is mentioned in eIDAS Article 5c(5), but it is not mandatory, so it is not currently covered in the present document.

***NOTE**: In the rest of the formal text, the reference is to an "ICT service" as the object of certification, but this may need to be modified if a scheme considers to issue other kinds of certificates, for instance to ICT products.*

You need to think carefully before deciding to include many more certificates. By introducing too many certificates, the complexity of the national scheme (and of related certification activities) increases, as well as the possibility of wrongfully assigning requirements to a given component (and realising later that it is covered by another component).

You should not list in here the certification of components that rely on other schemes. For instance, if your WSCA is to be certified with EUCC, it should not be listed here, since that certificate will not be issued under the present scheme.
See article 5(3) below for details.

EXAMPLE

If we consider one of the simplest configurations, which corresponds to the certification of the EUDI Wallet by using a dedicated cybersecurity scheme, we would have the following certificates:

- service for the provision of European digital identity ('EUDI') wallets and the electronic identity ('eID') scheme under which they are provided;
- cybersecurity of a service for the provision of EUDI wallets and the eID scheme under which they are provided;
- cybersecurity of services for the verification of the validity of EUDI wallet units and relying parties;

In this example, the process for getting certified is as follows:

1. Get a certificate for the cybersecurity of the EUDI wallet and associated eID scheme
2. Get a certificate for the cybersecurity of the validation services
3. Get the overall certificate, by performing functional testing on the wallet, eID scheme and validation services, and by ensuring that the two cybersecurity certificates are appropriate and complement each other well (in particular, that they do not include contradictory elements in their guidance).

A slightly more complex model would add two additional certificates relative to the functional testing. In that case, almost all evaluation activities would be performed in secondary certifications, and the overall certification would consist of a few overall activities, mostly to verify the consistency of the different subcertificates.

This last model could be particularly interesting if you only have a CB with limited cybersecurity skills. In that case, this CB could issue the "main" certificate only, only performing limited evaluation activities, while the more complex activities (evaluation and review) would be delegated to private CBs or to CBs from another Member State.

2.2 DEFINITIONS

See the Annex on terminology. You will need to select a subset of these definitions into Article 2.

3. SPECIFIC STANDARDS AND REQUIREMENTS FOR EVALUATION

This chapter is mostly a pointer to the annexes that define the criteria (Annex X) and methods (Annex XI) to be used in the certification process. However, the criteria are still TBD, and the methods remain incomplete.

This is Section I of Chapter 2, *Certification of EUDIW services*.

3.1 CERTIFICATION CRITERIA

This section is clearly the missing one for national schemes. The EU scheme will rely on standards and technical specifications that are for most of them under development or not developed yet.

The recommendation would be to develop the criteria to be met by the object of certification in an Annex or in a separate document, which may need to be updated. In that case, the article would be very simple.

Article 3	Notes on Article 3
1. A wallet service submitted for certification shall, as a minimum, be evaluated to be in conformity with the criteria defined in Annex X.	Since there is no pre-existing specifications, the easiest is to define a distinct set of requirements for each type of certificate to be issued.

Discussion

The lack of requirements is a significant issue for national schemes. As a reminder, there are obligations[3] to define requirements that cover the risks and threat scenarios identified in the risk register defined in (EU)2024/2981, and to specialise the requirements for a specific architecture.

This issue will be addressed separately, as we will provide some guidance for the development of requirements that could be harmonised between at least some Member States. In addition, there may be possibilities to simplify the way requirements are defined in some specific cases.

For instance, when a MS intends to use an EUDI Wallet developed by the private sector, they may require the EUDI Wallet to be already certified in another Member State, and to only specify the requirements related to the adaptation that they would require, for instance about adapting to their national eID scheme (which will be specific to every Member State).

3.2 METHODS FOR CERTIFYING EUDIW ICT SERVICES

This article refers to the methods defined in an Annex, and set rules for the reuse of evaluation reports in the case of composition, in particular within the scheme, and with an EU cybersecurity certification certificate.

Article 4	Notes on Article 4

[3] Article 3(5) of (EU)2024/2981 defines these obligations, which may need to apply to several profiles.

1. An ICT service submitted for certification shall, as a minimum, be evaluated in accordance with the methods defined in Annex XI.	This is mostly about identifying the scheme, modify the [EUDIW] name as needed.
2. In the case of an ICT service undergoing a composite service evaluation, the CB that carried out the evaluation of the underlying ICT service shall share the relevant information with the CB performing the evaluation of the composite ICT service.	This paragraph is optional, and needed only when composition is possible. In that case, the “relevant” documents mostly consist of the ETR. Also, there is no plan to develop a composition annex now, most likely a set of guidelines, which will need to be adapted from the corresponding EUCC document.
3. In the case of an ICT service including a component that has been certified with a European cybersecurity certification scheme, the CAB that carried out the evaluation of the component shall share the relevant information with the CB performing the evaluation of the ICT service.	This is mostly dedicated to EUCC[4], and a reminder that we expect the CAB to share the ETR with the CB performing the evaluation of the EUDI Wallet based on a CC-certified component.

Discussion

The EUDIW AHWG has started to work on some of these methods, which are included in the proposed annex. Our intention also is to reference CEN TS 18072, which is to be revised soon, and which should be modified to cover any type of IT service (and not just cloud services like today). In the absence of this revision, some of the content from CEN TS 18072 may need to be adapted in the annex defining methods.

Regarding composition, the text can be extended to cover other (national) schemes where composition would be relevant, to ensure that the relevant information will be made available to the CB in charge of the certification.

[4] The references to the EUCC scheme as defined in (EU)2024/482, are motivated by the direct reference made to it in (EU)2024/2981 in Article 4(1) and others.

4. ISSUANCE, RENEWAL AND WITHDRAWAL OF EUDIW CERTIFICATES

This chapter defines the conditions for certification as well as the lifecycle of certificates. It also points to a number of annexes, and all of the elements defined here need to be defined in a certification scheme.

This is Section II of Chapter 2, *Certification of EUDIW services*.

4.1 INFORMATION NECESSARY FOR CERTIFICATION

Paragraph 1 lists all the information that the applicant for certification needs to provide, and it also defines how results from previous conformity assessment work may be provided for reuse. Finally, it defines how long the applicant needs to retain the documentation used in the certification process.

Article 5	Notes on Article 5
1. An applicant for certification under [EUDIW] shall provide or otherwise make available to the certification body all information necessary for the certification activities.	This is mostly about identifying the scheme, modify the [EUDIW] name as needed.
2. The information referred to in paragraph 1 shall include the information listed in Annex IV.	This Annex lists the long list of required information, inspired from several sources, including EUCC, EUCS, and the CRA.
3. Applicants for certification may provide to the certification body appropriate evaluation results from prior certification pursuant to: (a) the present scheme; (b) a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881; (c) qualification and certification by conformity assessment bodies accredited according to the requirements of CIR (EU) 2025/xxx; (c) certification under any scheme by a CAB accredited to issue such certificates by the national accreditation body of an EU Member State, according to regulation (EU)765/2008. (d) [to be completed].	The objective is here to allow the reuse of many different schemes. This is here quite wide, covering any CSA scheme (for now, EUCC), all eIDAS-related certifications and qualifications, and even all certifications based on accreditation. There is no issue to accept even more exotic certificates or assurance, since there is an evaluation activity dedicated to the assessment of the relevance of this information. There is no specific mention of composition, since this is covered by point (a).
4. Where the evaluation results are pertinent to its tasks, the certification body may reuse the evaluation results provided that such results conform to the applicable requirements and their authenticity is confirmed.	This paragraph (from EUCC) encourages the reuse of evidence based on previous conformity assessments.
5. Applicants for certification shall also provide the certification body with the link to their website containing the information to be made publicly available, as defined in Annex III	Part of the information needs to be made publicly available, so this link is used to verify that the information available publicly is consistent with the information provided to the CB.
6. All relevant documentation referred to in this Article shall be retained by the certification body and the applicant for a period of 5 years after the expiry of the certificate.	There is no specific rationale for the 5 years, except that this is the figure used in EUCC, so it is possible to change it if required.

Discussion

In paragraph 2, the inspiration for the required documentation listed in Annex IV partly comes from CRA. Although CRA will only be applicable to product components that are placed on the market, the elements of the CRA technical file are generic enough to be used as a basis to describe the documentation here.

The objective is also to maximise reuse and to avoid “reinventing the wheel”, so our requirements are designed to be compatible with the requirements of other regulations, helping wallet providers to comply with all these regulations.

Paragraph 3 introduces the certificates that may be reused in this scheme. Because the objective of the present scheme is to focus on the integration and to use other schemes for the evaluation of the components (both for product and process components). It is therefore recommended to reuse as much external evidence as possible, as long as there is an evaluation activity to assess the quality of this evidence.

***NOTE**: The assessment of the quality of the evidence can be greatly simplified for a well-known scheme, where certificates are issued by trusted CABs, following a trusted methodology. In such cases, the assessment mostly consists in verifying the relevance of the certificate in terms of its scope of certification (object and requirements). See details in the discussion in the next section.*

The proposed wording is very inclusive, in particular point (c), which allows reuse from any conformity assessment which relies on accreditation of the CABs. This can be restricted if needed, or even extended, in particular to private schemes that may bring specific value.

The one limiting factor may be the complexity of combining too many different certifications. At the end, the wallet provider may end having to demonstrate conformity to many individual requirements (if they are not covered by the provided evidence), which could be costly, and also lead to additional costs during the maintenance, in particular if the scope of the underlying certificates evolves.

4.2 CONDITIONS FOR ISSUANCE OF AN EUDIW CERTIFICATE

Article 6 defines the conditions for certification, including a list of commitments that needs to be taken by the ICT service provider:

Article 6	Notes on Article 6
1. The certification bodies shall issue an [EUDIW] certificate where all of the following conditions are met: (a) the categories of the ICT service and of its components fall within the scope of the accreditation, and where applicable of the authorisation, of the certification body issuing the certificate; (b) the applicant for certification has signed a statement undertaking all commitments listed in paragraph 2; (c) the certification body has concluded the evaluation without objection in accordance with the evaluation criteria and methods referred to in Articles 3 and 4; (d) the certification body has concluded the review of the evaluation results without objection.	The conditions are strongly inspired from EUCC. The specific requirement on verifying the ETR has been removed, since this is part of the review from subparagraph (d).
2. The applicant for certification shall undertake the following commitments: (a) to provide the certification body with all the necessary complete and correct information, and to provide additional necessary information if requested; (b) not to promote the ICT service as being certified under the [EUDIW] before the [EUDIW] certificate has been issued;	These commitments are quite standard. The first one, in particular, is intended to reinforce the fact that the applicant is responsible for ensuring that the information provided to the CB is complete and correct.

(c) to promote the ICT service as being certified only with respect to the scope set out in the [EUDIW] certificate; (d) to cease immediately the promotion of the ICT service as being certified in the event of the suspension, withdrawal or expiry of the [EUDIW] certificate; (e) to ensure that the ICT service provided with reference to the [EUDIW] certificate is the ICT service subject to the certification;	
3. If the certificate applies to services for the provision of European digital identity ('EUDI') wallets and the electronic identity ('eID') schemes under which they are provided, then the applicant for certification shall satisfy the requirements of Article 5a(2) of regulation (EU)No.910/2014.	This guarantees that such certificates are only delivered to entities authorized by governments[5]. This only applies for the high-level certificate.

Discussion

These requirements are quite classic and minimalistic, but they indirectly raise some questions.

The CB has an obligation to review the evaluation, which means that they need to be able to understand whether or not the evaluation was done according to the scheme's rules. In some case, this may require very specific competencies (*e.g.*, for the WSCA). We propose here to take an approach where a CB may not be required to have these competencies, in which case they would be forced to use an external certificate for some components (*e.g.*, for a SE-based WSCA, they would be forced to use an EUCC certificate). In such a case, they simply need to verify that the certificate has the expected scope, plus a few other activities that do not require an advanced evaluation expertise.

The commitments of the ICT service provider are very important, because they represent strict obligations that the provider has explicitly agreed to follow. The first one is in particular very important, as it refers to the completeness and accuracy of the information provided to the CB. If the scheme is a legal text, then violating these commitments is a legal non-compliance, not just a nonconformity to the scheme's requirements.

These commitments could form the basis for defining legal action in case of fraudulent use of the certificates, as required in Article 4(4)(e) of regulation (EU)2024/2981.

4.3 ISSUANCE OF AN EUDIW CERTIFICATE

This is directly adapted from EUCC's Article 10, and it raises limited issues:

Article 7	Notes on Article 7
1. An [EUDIW] certificate shall include at least the information set out in Annex V.	We recommend to align the information required for certificates in the different national certificates.
2. The scope and boundaries of the certified ICT service shall be unambiguously specified in the [EUDIW] certificate or the certification report.	The certificate is likely to focus on the commercial name of the certified EUDI Wallet, but a more precise description of the object of certification needs to be provided in the certification report.
3. The certification body shall provide the applicant with the [EUDIW] certificate at least in electronic form.	
4. The certification body shall produce a certification report in accordance with Annex VI for each [EUDIW] certificate it issues. The certification report shall be based on the evaluation technical report. The certification report shall indicate the specific evaluation criteria and methods referred to in Articles 5 and 6 used for the evaluation.	The certification report contains very basic information about the certification, without getting into the details of the evaluation. It includes a detailed description of the wallet and of its security model, but only a summary of the evaluation activities.

[5] As required in Article 4(4)(a) of regulation (EU) 2024/2981.

5. The certification body shall produce a certification assessment report in accordance with Annex VII for each [EUDIW] certificate it issues.	The certification assessment report is not a classical report in certification. The current proposal is to make it a version of the evaluation technical report with a detailed description of the evaluation activities, but only limited information about the results, and in particular, no information about exploits.
6. The certification body shall provide the [scheme owner] and the supervisory body referred to in Article 46a(1) of Regulation (EU) No 910/2014 [and other] with every [EUDIW] certificate, certification report and certification assessment report it issues in electronic form.	The certificate and associated reports are distributed to the national supervisory body, and if needed to another entity, who will then forward the information to other entities (see below).
7. The [member state] shall provide the Commission and the Cooperation Group established pursuant to Article 46e(1) without undue delay with every [EUDIW] certificate, certification report and certification assessment report it issues in electronic form, together with the information required in Article 5d(2) of Regulation (EU) No. 910/2014 and in the annex of Regulation (EU) 2025/849.	The "member state" has this obligation, so it should be replace by the organization in charge of this, which as indicated above, could be the supervisory body or another entity. Note that we also require the provision of the Certification Report, which may be made publicly available (contrarily to the Certification Assessment Report.

Discussion

It would be preferable to use the same mandatory content for the certificate and associated reports across all national schemes, in particular since these documents will be provided to the EDICG for review.

The certification assessment report is specific to the eIDAS regulation, so its content may be subject to further discussions The initial guiding principles (from Annex VIII of the 5c IA) are to use it as a way to provide additional information about the evaluation activities, including in particular a full list of the evaluation activities performed and a summary of their results. but the limit of the information to be provided remains to be clarified, in particular regarding the level of details provided about the results of the evaluation activities.

NOTE: The conformity assessment report is not the full Evaluation Technical Report (ETR), so it is expected to contain less information). In particular, it should not contain any sensitive information about nonconformities that have been identified, in particular if they include the description of vulnerabilities that could be exploited.

We will also consider mandating the use of English as main language for the conformity assessment report, since it is intended to be shared with all Member States. For the certificate and certificate report, there may be recommendations to require the inclusion of an English translation if the main language is not English.

Publication of Certificates, References to Certificates

In an EU scheme, the reference for the publication of certificates is ENISA's Web site. CBs and NCCAs can of course publish the certificates, but it's not an obligation. In addition, in EUCC, the label includes a QR-code that links to the ENISA Web page for the certificate, allowing a product's potential customer to check its status.

For EUDI Wallets, the Commission has this role, and Member States have an obligation to transmit to the Commission information about certified EUDI Wallets, as described in Article 5d of eIDAS and in Regulation (EU) 2025/849, the implementing regulation dedicated to this topic.

NOTE*: Part of the information required in (EU)2025/849 is not available in the certificate itself, but in the certification report, which is not required in that regulation. We therefore propose to make it mandatory to also send the certification report.*

***NOTE**: The notification of certificates concerns only wallets that are certified and provided, and it includes a description of the eID scheme under which the wallet is provided. This means that the notification of the Commission and od the EDICG only applies to high-level certificates of an EUDI Wallet and the eID scheme under which it is provided. If components, including wallet solutions, can be certified under this scheme, these certificates do not need to be notified to the Commission and the EDICG.*

The issue of the reference to the certificate is not fully resolved here. Ideally, each certificate should be associated with a URL, which ideally could be created from basic information available on the certificate (CB identifier and certificate identifier). For interoperability reasons, it would be better to point to the Commission's global storage, but this may not be suitable, so this remains to be discussed.

4.4 MARK AND LABEL

The proposal is to not support the use of marks or labels:

Article 8	Notes on Article 8
1. The holder of a certificate shall not affix any mark or label to related to certification issued according to the present scheme to documentation relative to a certified ICT service.	Th recommendation is to not use marks and labels[6].

DISCUSSION

The recommendation not to use marks and labels mostly comes from two reasons:

1) First, the main use of the certificate is to support the notification of a full solution to the Commission, including an EUDI Wallet and the eID scheme under which it is provided, not to be used as a differentiating means for companies.
2) Then, having many different marks and labels in every country may be confusing, and the harmonisation may not be sufficient to use a single mark or label.

In addition, the EUDI Wallet Trust Mark is supposed to have this role towards the end user, with additional guarantees.

If a national scheme defines additional certificate types, for instance for wallet solutions, then it may make sense to use a dedicated mark or label specifically for these certificates, but its usage needs to be carefully considered, to ensure that it does not introduce any confusion for citizens that could be exploited by malevolent actors.

4.5 PERIOD OF VALIDITY OF AN EUDIW CERTIFICATE

Article 9 defines how long the certificates can be:

Article 9	Notes on Article 9
1. The certification body shall set a period of validity for each [EUDIW] certificate issued taking into account the characteristics of the certified ICT service.	The CB may decide to set a period of validity that is shorter than the maximum period. This may for instance occur in particular if the EUDI Wallet has many non-material nonconformities or residual vulnerabilities, or if it is incomplete and needs to undergo revisions.
2. The period of validity of the [EUDIW] certificate shall not exceed 4 years.	The 4-year limit is intended to be lower than the legal 5-year limit set in the eIDAS regulation, and to be aligned with the vulnerability assessment to be conducted every two years.

[6] Also, Article 4(4)(b) of(EU) 2024/2981 does not allow marks of conformity other than the Trust Mark.

3. By derogation from paragraph 2 that period may be extended up to 5 years, subject to the prior approval of the [scheme owner]. The [scheme owner] shall notify the Cooperation Group referred to in Article 46e(1) of Regulation (EU) No 910/2014 of the granted approval without undue delay.	An extension is possible, in particular if a certificate holder experiences difficulties for re-certification, but this extension can only be granted after approval by the scheme owner (the NCCA in the EU scheme). Of course, the extension needs to be notified to the EDICG.

Discussion

The proposal is to limit by default the validity of a certificate to four years, in order to keep a buffer with the legal 5-year limit. The 4-year validity is also optimised for the execution of the vulnerability assessment every two years.

There is no obligation to use the same limit, but if the limit in paragraph 2 is set to 5 years, then no derogation (according to paragraph 3) will be available for certificates issued with a 5-year validity period. Upon reaching the 5-year limit set in the eIDAS regulation, the certificate will have to be considered expired, possibly followed by the issuance of a new certificate (following a full initial evaluation). Because of the required mutual recognition of EUDI Wallets between Member States, our recommendation is to steer clear of the eIDAS limits whenever possible, to avoid legal issues.

4.6 MAINTENANCE OF AN EUDIW CERTIFICATE

The certificate needs to be associated to a maintenance schedule.

Article 10	Notes on Article 10
1. Following the schedule defined in Annex II, upon request of the holder of the certificate or for other justified reasons, the certification body shall regularly perform a maintenance conformity assessment and review the [EUDIW] certificate for an ICT service. The maintenance conformity assessment shall be carried out in accordance with Annex II.	The annex defines a schedule[7] of evaluation activities over a 4-year period, as well as a list of the activities to be performed in every periodic assessment[8].
2. Following the results of the maintenance conformity assessment and review, the certification body shall: (a) confirm the [EUDIW] certificate; (b) withdraw the [EUDIW] certificate in accordance with Article 11; (c) append an amendment to the [EUDIW] certificate that defines an updated scope; or (d) withdraw the [EUDIW] certificate in accordance with Article 11 and issue a new [EUDIW] certificate with an identical or updated scope and an extended validity period.	At the end of the periodic assessment, several things can happen, depending first on the information provided by the certificate holder and on the results of the activities performed by the CB, with many possible consequences on the certificate, discussed below.
3. The certification body may decide to suspend, without undue delay, the [EUDIW] certificate in accordance with Article 19, pending remedial action by the holder of the [EUDIW] certificate.	Suspension is another option if an issue has been identified that can be fixed by the certificate holder.
4. When an amendment is added to an [EUDIW] certificate, the CB shall notify the supervisory body referred to in Article 46a(1) of Regulation (EU) No 910/2014, the Commission and the Cooperation Group referred to in Article 46e(1) of Regulation (EU) No 910/2014 of the amendment without undue delay, and share with them the amended certificate, certification report and certification assessment report.	Like every event on certificates, the supervisory body, the Commission and the EDICG needs to be notified of amendments.

[7] Article 18 of (EU)2024/2981 defines a certification lifecycle as well as a number of activities, in Annex IX of the same regulation.

[8] Such maintenance activities are mandated for Type 6 schemes (as defined in EN ISO/IEC 17067 and as required by Article 4(3) of (EU)2024/2981.

Discussion

In addition to the reviews that exist in EUCC (which are here called special evaluations), we here propose to have a schedule with yearly activities, defined in Annex II.

The object of certification is here an ICT service, which includes some processes, so the first goal of these regular activities is to ensure that these processes (which have been deemed appropriate in the initial certification) are implemented as they are defined. In addition, because the object of certification is complex, regular update are likely, and a yearly evaluation will ensure that the actual service does not deviate too far from the service that was initially certified. Finally, the eIDAS regulation mandates a vulnerability assessment every two years, which is integrated in the proposed maintenance schedule.

After the evaluation, a number of outcomes are possible, including

- The activities are successful, so the certificate remains valid, and there is no update to be made to the description of the service in the certificate (or certificate report).
- The activities fail in a way that cannot be fixed, so the certificate is withdrawn.
- The activities succeed, so the certificate remains valid, but there are changes in the description of the wallet that require an update. The update is added to the certificate in an amendment. Note that this differs from EUCC (see details below).
- The activities succeed after a full recertification evaluation, so the certificate is withdrawn and replaced with another one with another expiration date. This typically happens just before the certificate expires, or when the wallet underwent significant changes.
- Suspending the certificate, when most activities have been successful, but some activities have uncovered issues that can be fixed rapidly.

NOTE*: The description provided here does not define precisely the extent of failure that will lead to the suspension or withdrawal of the certificate. We will make a proposal in an Annex, but the decision ultimately lies with the CB.*

NOTE*: These rules should satisfy the need of performing a vulnerability assessment at least every two years. The normal schedule includes such an assessment every two years, and the only type of maintenance evaluation that may lead to a change of expiration date and schedule is the recertification evaluation, which includes a vulnerability assessment.*

In other schemes, the operation of the processes over a period of time (typically, 6 to 12 months) is evaluated before to issue a certificate. Here, it is difficult to include such an assessment, because the initial certification is a prerequisite for the operation of the service. This means that the first yearly assessment could lead to significant challenges regarding the verification of the compliance to the processes that have been validated during the initial certification assessment.

Example

When performing a surveillance evaluation, the certificate holder informs the CB that they are in the process of replacing the HSMs that they are using, so the WSCA is completely new.

During the evaluation, the CB needs to verify that the WSCD is properly certified to meet all requirements. Then, they need to perform a new evaluation of the WSCA to ensure that it meets all requirements. Finally, they will update the description and issue an amendment to the certificate that will be attached to the certificate as the new HSM and WSCA are deployed.

Note that this is not an issue because the service rendered remains the same, and only its implementation has been modified. In this matter, services differ greatly from products, also because the new version of the service usually replaces the old one, so there is one active version of the service, whereas products may be deployed in different versions at a given time.

4.7 WITHDRAWAL OF AN EUDIW CERTIFICATE

Article 11 defines the conditions for withdrawing certificates:

Article 11	Notes on Article 11
1. An [EUDIW] certificate shall be withdrawn by the certification body that issued that certificate, or by the [scheme owner] when an [EUDIW] certificate does not comply with the present scheme.	The EU scheme has a reference to CSA Article 58(8)(e), which gives NCCAs the power to withdraw certificates that do not comply with the CSA or with a scheme. We propose to give this power to the scheme owner, but this is to be appreciated by every Member State[9].
2. The certification body referred to in paragraph 1 shall notify the [scheme owner] and the supervisory body referred to in Article 46a(1) of Regulation (EU) No 910/2014 [and other] of the withdrawal of the certificate. The [scheme owner] shall notify other relevant market surveillance authorities.	Withdrawal of certificate needs to be notified to the same entities to which the issuance of certificates is notified.
3. The [member state] shall notify the Commission and the Cooperation Group established pursuant to Article 46e(1) without undue delay of the withdrawal of the certificate.	This is the obligation from eIDAS Article 5d, which is on the Member State. This could be done by the scheme owner, supervisory body or any other body (in that case, add the “and other” above.
4. The holder of an [EUDIW] certificate may request the withdrawal of the certificate.	A certificate holder should always have the power to request the withdrawal of a certificate.

Discussion

The certification of EUDI wallets is a legal requirement, so the withdrawal of the certificate of a deployed EUDI wallet has real consequences, disturbing the interactions between the citizen and the Member State, since the loss of certification triggers an interdiction to use the wallet.

The objective of this article is to define very basic conditions for the withdrawal of certificates, but this remains a difficult decision for a CB, in particular for such an important certificate. It is therefore very important to also grant the power to an authority to withdraw certificates.

We here propose to give to the scheme owner this power to appreciate whether a certificate does not comply with the rules of the scheme and withdraw if needed, but this power may be assigned to another entity, in particular if the scheme owner does not have the competence and authority to take such important decisions.

This article is a reminder that there is a clear interest to get the NCCA involved in the operation of the scheme. Beyond the fact that this would ease the transition to the EU scheme, the expertise of the NCCA can be very useful when decisions as important of the withdrawal of a certificate need to be taken.

[9] Rules relative to the withdrawal of certificates are required by Article 18(5) of regulation (EU)2024/2981.

5. CONFORMITY ASSESSMENT BODIES

This chapter defines he requirements to be met by conformity assessment bodies, which will be verified through accreditation and, if required, through authorisation (a notion introduced in the CSA).

This is Chapter 3, *Conformity Assessment Bodies*.

5.1 SPECIFICATION OF REQUIREMENTS FOR ACCREDITATION OF CONFORMITY ASSESSMENT BODIES

Article 12 makes a reference to an external document:

Article 12	Notes on Article 12
1. Certification bodies shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008 in accordance with EN ISO/IEC 17065:2012.	This is the basic requirement.
2. The accreditation of conformity assessment bodies shall take into account the specification of requirements for accreditation of certification bodies as laid down in [AccredDoc].	The scheme does not define how accreditation is to be performed, but it defines some requirements that need to be taken into consideration. In a national scheme, the accreditation requirements may be defined in an Annex to the scheme or another document.

Discussion

In the present proposal, the only role that is defined is the certification body. It is here a certification body in the ISO/IEC 17065 sense, who issues certificates and is also in charge of performing all evaluation activities[10].

In particular, we have not proposed to define an ITSEF role, or other roles like an auditor. However, in a national scheme, there may be good reasons to define such a role, either by defining it in the scheme (the EUCC IA can be used as reference, or by referring to the EUCC ITSEFs or other bodies performing evaluation tasks.

In the current proposal, a CB may subcontract some evaluation activities, but subcontractors will be included in the CB's own accreditation rather than being accredited themselves. This may be a sensible choice in a scheme where few CBs and subcontractors are foreseen.

Accreditation is costly, and in these national schemes, it is seen as a significant obstacle by CABs, in particular from the private sector. It is therefore important to consider this issue and to minimise the effort required from CABs involved in the implementation of national schemes.

[10] Article 10 of regulation (EU)2024/2981 provides additional details, with reference to other harmonised standards related conformity assessment for testing (EN ISO/IEC 17025), inspection (EN ISO/IEC 17020), and for certification of management systems (EN ISO/IEC 17021-1). These references are also included in EN ISO/IEC 17065, so they will necessarily end up in the accreditation requirements. However, note that although subcontractors are required to meet the requirements of these standards, there is no requirement to have them accredited separately.

EXAMPLE

One of the tasks to be performed is the evaluation of the WSCA to a level equivalent to AVA_VAN.5. This is a complex task, so several options are feasible:

- The CB may perform the evaluation themselves, using a team that fulfils the requirements to perform such an evaluation. In addition, an independent team will need to be able to review the evaluation work (and therefore will need to have an in-depth understanding of the required evaluation activities).
- The CB subcontracts the evaluation to another body who performs the evaluation. In that case, during accreditation, the subcontractor needs to meet the requirements to perform the evaluation. However, the CB still needs to be able to perform an independent review of the work performed by the subcontractor.
- Another solution is to ask an EUCC-accredited CB (and ITSEF) to certify the WSCA. In that case, the entire responsibility of that evaluation lies with the EUCC CB. The EUDI Wallet CB only needs to validate the adequation of the certified WSCA.

To recap, the more components are evaluated independently and outside of the wallet scheme, the lighter the Wallet CB's responsibility. This may be an interesting direction for Member States who want to have a CB but do not have a local CB with the required competencies to perform or review all the evaluation tasks related to the components.

This decision of the organisation of certification is essential in the scheme, because it conditions the level of competences required for the certification body. In addition to the options mentioned above, the Cybersecurity Act introduces a notion of delegation from the NCCA to private CBs, which could be adapted here: A Member State could allow private CBs to issue certificates, while controlling their activities as part of a delegation.

5.2 ADDITIONAL OR SPECIFIC REQUIREMENTS FOR A CERTIFICATION BODY

The Cybersecurity Act defines an additional mechanism through which the NCCA can check some competences of the CABs in complement to accreditation. A similar mechanism may be defined here:

Article 13	Notes on Article 13
1. A certification body shall be authorised by the [scheme owner] to issue [EUDIW] certificates where that body demonstrates that, in addition to meeting the requirements laid down in [ISO17065] regarding accreditation of conformity assessment bodies, it meets the following: (a) it has the expertise and competences required for the certification decision; (b) it has the necessary expertise for performing the evaluation activities to determine the resistance to state-of-the-art cyberattacks carried out by actors with significant skills and resources; and (c) it has the requisite competences and put in place appropriate technical and operational measures to effectively protect confidential and sensitive information required for the evaluation, in addition to the requirements set out in Article 31.	The EUCC Article makes a reference to CSA Article 60(1) and Annex, as well as level of assurance 'high'. The article has been modified to remove these references, but it is not strictly equivalent.
2. The [scheme owner] shall assess whether a certification body fulfils all the requirements set out in paragraph 1. That assessment shall include at least structured interviews and a review of at least one pilot certification performed by the certification body in accordance with this Regulation. In its assessment, the national cybersecurity certification authority may reuse any appropriate evidence from prior authorisation or similar activities granted pursuant to:	This paragraph is more independent of the CSA.

(a) this scheme; (b) a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881	
3. The [scheme owner] shall specify the ICT service and component categories to which the authorisation extends. The authorisation shall be valid for a period no longer than the validity of the accreditation. It may be renewed upon request provided that the certification body still meets the requirements set out in this Article. For the renewal of the authorisation, no pilot evaluations are required.	This has been adapted from EUCC to mention "component categories", but the idea remains to list the scope of the authorisation.
4. The [scheme owner] shall withdraw the authorisation of the certification body where it no longer meets the conditions set out in this Article. Upon withdrawal of the authorisation, the [scheme owner] shall inform without delay the supervisory body referred to in Article 46a(1) of Regulation (EU) No 910/2014, and the certification body shall cease immediately promoting itself as an authorised certification body.	

Discussion

The notion of authorisation is defined in the CSA. It may be used outside of the CSA context, but some adaptation is required. In particular, some entity (here assumed to be the scheme owner) needs to take the role of evaluator, who will verify the competences of the CAB.

In addition, it is also difficult to make a reference to the CSA assurance level 'high'. This may not be a big issue here, since all certificates are issued at that level. It is therefore possible to use excerpts of the definition, as suitable, like in paragraph 1(b).

Since there is no mention of authorisation in regulation (EU)2024/2981, we would recommend not to use this mechanism unless an organisation has clearly been identified (e.g., the NCCA) that can undertake the verification of the competences.

6. COMPLIANCE MONITORING

For every certificate issued, the scheme owner, certification body and certificate holder need to monitor the compliance of the EUDI Wallet and eID scheme to the requirements of the certificate.

This is Section I of Chapter 4, *Monitoring, nonconformity and non-compliance.*

6.1 MONITORING ACTIVITIES BY THE SCHEME OWNER

A scheme owner typically centralises information from CBs and samples certificates for additional scrutiny:

Article 14	Notes on Article 14
1. The [scheme owner] shall monitor the compliance of: (a) the certification bodies with their obligations pursuant to Regulation (EU) No 910/2014 and to this scheme; (b) the holders of an [EUDIW] certificate with their obligations pursuant to this scheme; (c) the certified ICT services with the requirements set out in the [EUDIW]; (d) the assurance expressed in the [EUDIW] certificate addressing the evolving threat landscape.	The EUCC Article makes a reference to CSA Article 58(7), and several times to the requirements of the CSA. The references have been removed and replaced by references to eIDAS or less precise references. Point (d) addresses the evolution of the threat landscape, although it's not fully clear (point raised to the EUCC team).
2. The [scheme owner] shall perform its monitoring activities in particular on the basis of: (a) information coming from certification bodies, national accreditation bodies and relevant market surveillance authorities; (b) information resulting from its own or another authority's audits and investigations; (c) complaints and appeals received.	This remains entirely valid[11].
3. The [scheme owner] shall select the sample of certified ICT services to be checked using objective criteria, including: (a) service category; (b) holder of a certificate; (c) certification body; (d) specific points of attention defined by the [scheme owner]; (e) any other information brought to the authority's attention.	Point (d) has been added to focus on specific points instead of doing a full review.
4. The [scheme owner] shall inform the holders of the [EUDIW] certificate about the selected ICT services and the selection criteria.	
5. The certification body that certified the sampled ICT service shall, upon request of the [scheme owner], conduct additional review in accordance with the procedure laid down in Annex II and inform the [scheme owner] of the results.	The "additional review" is described in detail in an Annex, but it clearly is a review task, to perform verifications on the evaluation activities performed. After analysis of the additional review results, the scheme owner and CB may decide to perform additional evaluation activities.
6. Where the [scheme owner] has sufficient reason to believe that a certified ICT service is no longer in compliance with this scheme or Regulation (EU) No 910/2014, it may carry out investigations or [other powers].	We have removed the reference to CSA Article 58(8), which give the NCCA authority to investigate, take measures, access the premises of CABs, withdraw certificates and impose penalties.

[11] The same items are mentioned in Article 7(3) of (EU)2024/2981 that defines monitoring requirements for scheme owners.

	Depending on the scheme owner, national law may grant them some or all of these powers.
8. The [scheme owner] shall inform the certification body concerned about ongoing investigations regarding selected ICT services.	
9. Where the [scheme owner] identifies that an ongoing investigation concerns ICT services that are certified by certification bodies established in other Member States, it shall inform thereof the [scheme owner] of the relevant Member States in order to collaborate in the investigations, where relevant. Such [scheme owner] shall also notify the Cooperation Group referred to in Article 46e(1) of Regulation (EU) No 910/2014 of the cross-border investigations and the subsequent results.	This may be questionable. However, it is quite likely that at least some components will be certified in other Member States, so there is an interest to have such a rule in place. The EDICG is mentioned instead of the ECCG.

Discussion

Compliance monitoring is an important component of the CSA certification framework, and it has been included in CIR (EU)2024/2981 with a limitation of monitoring to CBs. The proposal above goes beyond, directly adapted from EUCC. It is relevant when the scheme owner is in a position (availability of technical competences, in particular) to perform these oversight tasks, but it may be preferable to remove or simplify these requirements if the scheme owner is not in position to implement this monitoring.

Paragraph 3 is the central paragraph that defines the criteria for deciding on which certificate(s) to perform the monitoring. We have added point (d) here to make sure that if there are very few certificates issued (possibly, just 1), then the monitoring will focus on specific aspects rather than perform an overall review of the certificate.

It is nevertheless important to give enough power to the scheme owner, because of the need to handle complaints and other issues appropriately.

NOTE*: In schemes where a single CB is accredited to issue certificates, the monitoring activities of the scheme owner are less relevant, since their main objective is to harmonise the performance between several CBs. In addition, that single CB may be the scheme owner. With national schemes, this situation (a single CB) is likely to occur, so this simplification can be considered as well.*

NOTE*: There is here a mention to appeals, which did not appear in EUCC but is explicitly listed in (EU)2024/2981. The notion of appeal is defined in EN ISO/IEC 17065, so we have so far refrained to define additional requirements in the scheme.*

Open Topics

Because the security of EUDI Wallets may rely on the security on devices provided by the user (and therefore not in scope of the certification), there is a potential issue related to harmonisation between Member States regarding the identification and analysis of such issues.

This is outside of the scope of both national and European certification schemes, and should rather be under the responsibility of the EDICG or similar group, but we may need to introduce into the scheme an obligation for CBs and/or scheme owners to notify the relevant stakeholders when they become aware of an issue with a particular type of user devices. This is at least partly covered by vulnerability management, but some of the issues may be nonconformities rather than vulnerabilities.

NOTE*: The current draft, in line with (EU)2024/2981, assumes that each certificate for an EUDIW wallet and eID scheme will define a set of hypotheses to be met by the components to be provided by end users, as well as mechanisms to check that these hypotheses are verified in* *practice. This is difficult to implement for mobile devices, in particular, which most likely will not be the subject of any cybersecurity assessment. The proposal above is intended to address this specific issue, and needs to be discussed further.*

6.2 MONITORING ACTIVITIES BY THE CERTIFICATION BODY

Article 15 defines activities to be performed by the certification body:

Article 15	Notes on Article 15
1. The certification body shall monitor the compliance of: (a) the compliance of the holders of a certificate with their obligations under this scheme and Regulation (EU) No 910/2014 towards the [EUDIW] certificate that was issued by the certification body; (b) the compliance of the ICT services it has certified with their respective security requirements.	The requirements are minimalistic, and very classical for CBs.
2. The certification body shall undertake its monitoring activities on the basis of: (a) the information provided on the basis of the commitments of the applicant for certification referred to in Article 6(2); (b) information resulting from activities of other relevant market surveillance authorities; (c) complaints and appeals received; (d) vulnerability information that could impact the ICT services it has certified.	Similarly, this is very basic[12].

Discussion

The requirements in this article are very classical, and reflect obligations of the CBs accredited to ISO/IEC 17065.

6.3 MONITORING ACTIVITIES BY THE HOLDER OF THE CERTIFICATE

Article 16 defines activities for the certificate holder:

Article 16	Notes on Article 16
1. The holder of an [EUDIW] certificate shall perform the following tasks to monitor the conformity of the certified ICT service with its security requirements: (a) monitor vulnerability information regarding the certified ICT service, including known dependencies by its own means but also in consideration of: (1) a publication or a submission regarding vulnerability information by a user or security researcher through the contact provider to that avail; (2) a submission by any other source; (b) monitor the assurance expressed in the [EUDIW] certificate, and in particular the evolution on the status of any certificate or assurance report used as objective evidence in the evaluation of the ICT service.	The requirements are focused on the monitoring of vulnerabilities and on the surveillance of the certificates of the different components.
2. The holder of an [EUDIW] certificate shall work in cooperation with the certification body and, where applicable, the [scheme owner] to support their monitoring activities.	
3. The holder of an [EUDIW] certificate shall notify the certification body without undue delay when the following events occur: (a) any breach or compromise of the ICT service they provide; (b) any material change to the ICT service.	This is an addition to satisfy requirements from Article 5 of the 5c IA. We propose not to mention materiality of breaches and compromises, because it’s not clear how a breach

[12] Article 9(3) of (EU)2024/2981 defines requirements about the monitoring activities to be undertaken by CBs, and the list of source information has been extended.

	could not be likely to impact conformity to the scheme’s requirements.

DISCUSSION

The two first paragraphs do not correspond to any specific requirement in CIR (EU) 2024/2981, but this presents the advantage of putting an obligation on the certificate holder, in addition to the operation of a vulnerability management process that complies with the scheme’s requirements. They may therefore be removed without significant prejudice, since the monitoring of composite certifications is also an implicit requirement.

The last paragraph, on the other hand, reflects obligations from the eIDAS regulation.

***NOTE**: The notion of materiality for changes is mentioned by not defined here, but materiality is addressed in Annex I, including for changes. There is no such mention for breaches, because any actual breach should be considered as material.*

7. CONFORMITY AND COMPLIANCE

Once a nonconformity or non-compliance has been detected, it has consequences, which are defined in this chapter.

This is Section II of Chapter 4, *Monitoring, nonconformity and non-compliance.*

7.1 CONSEQUENCES OF NONCONFORMITY OF A CERTIFIED ICT SERVICE

Article 17 defines the possible consequences of a nonconformity.:

Article 17	Notes on Article 17
1. When the certification body becomes aware of a material nonconformity of a certified ICT service with the requirements laid down in this Regulation and in Regulation (EU) No 910/2014, the certification body shall inform the holder of the [EUDIW] certificate about the identified nonconformity and request remedial actions, and inform. without delay the supervisory body referred to in Article 46a(1) of Regulation (EU) No 910/2014	The notion of materiality is discussed below, but this means that some nonconformities may be minor enough for the CB to ignore at first[13]. The supervisory body is also informed, since the nonconformity has been deemed material[14].
2. Upon receipt of the information referred to in paragraph 1, the holder of the [EUDIW] certificate shall within the time period set by the certification body, which shall not exceed 30 days, propose to the certification body the remedial action necessary to address the non-conformity.	The 30-day limit for a response is only indicative. For a significant nonconformity, the CB should set a much shorter time limit for the response.
3. The certification body may suspend, without undue delay, the [EUDIW] certificate in accordance with Article 19 in case of emergency, or where the holder of the [EUDIW] certificate does not duly cooperate with the certification body.	The CB has means to “convince” the certificate holder to comply with the request.
4. The certification body shall carry out a validation to assess whether the remedial action addresses the nonconformity.	The CB then will then analyse the proposed remedial actions, to understand whether or not it could remediate the nonconformity if executed effectively.
5. Where the holder of the [EUDIW] certificate does not propose appropriate remedial action during the period referred to in paragraph 2, the certificate shall be suspended in accordance with Article 19 or withdrawn in accordance with Article 11.	Note that this paragraph includes an automatic suspension in case of non-response within the required timeframe.
6. This Article shall not apply to cases of vulnerabilities affecting a certified ICT service, which shall be handled in accordance with Chapter V.	This process is only for nonconformities, vulnerabilities are processed according to other rules.

Discussion

This article described the possible consequences of a nonconformity. Paragraph 2 from the EUCC version, relative to presumption of conformity, has been removed, because it didn’t seem relevant here.

Because of the composite nature of the object of certification, it is very difficult to set a single process. Instead, the article sets a loose time limit in paragraph 2 and then gives the CB means

[13] Article 17(1) of regulation (EU)2024/2981 defines a similar requirement, without the reference to materiality. Also, although it is not explicitly mentioned here, one of the ways for a CB to become aware of a nonconformity is a notification from the certificate holder (one of the obligations under certification).
[14] Article 17(2) of regulation (EU) 2024/2981 mandates such a notification “where the nonconformity concerns relevant Union legislation”, which would require it at best for material nonconformities.

to influence the response of the certification holder in paragraph 3. For instance, for a significant operational issue, the CB may warn from the beginning that they immediately suspend the certificate and that they will withdraw it without response within 48 hours (mixing the urgency and non-cooperation reasons from paragraph 3).

Because the nonconformities may be operational, requiring urgent remediation, the certification holder is not supposed to wait for the confirmation to perform the proposed remediation action. However, if the remedial actions are not validated by the CB, additional actions may be required.

This matter may be very delicate to handle, because of the need to balance the risk of leaving an infringing solution in use and the risk of abruptly removing access to the wallet, which could leave many citizens in a difficult situation.

***NOTE**: For this exact reason, there are no automatic actions here, and the decision to suspend or withdraw a certificate is left to the professional judgment of the CB, because the decision may be very impactful.*

Materiality

Paragraph 1 refers to “material nonconformities”, and materiality is a concept used in auditing. It is quite difficult to find a precise definition, but the one proposed for financial statements can be adapted to our context:

> An information is material if it could reasonably be expected to influence the decisions that the primary users of [a certificate] make on the basis of those [certificates].

We then apply this definition to nonconformities, to the impact of vulnerabilities, and to changes on the object of certification. This notion replaces the notion of “minor” and “major”, “material” being a replacement for “major”, but with a better semantics.

We will need to provide a better description of material nonconformities, but the definition above provides a framework for determining whether or not a nonconformity is material, and this notion is already familiar to auditors.

7.2 CONSEQUENCE OF NON-COMPLIANCE BY THE HOLDER OF THE CERTIFICATE

Article 18 defines the consequences of non-compliance for certificate holders:

Article 18	Notes on Article 18
1. Where the certification body finds that: (a) the holder of the [EUDIW] certificate or the applicant for certification is not compliant with its commitments and obligations as set out in Articles 6(2), 16 and 31; or (b) the holder of the [EUDIW] certificate does not comply with Chapter VI of this scheme; it shall set a time period of not more than 30 days within which the holder of the [EUDIW] certificate shall take remedial action.	This is about the obligations of the certificate holder, with a special mention for the requirements related to vulnerabilities[15].
2. Where the holder of the [EUDIW] certificate does not propose appropriate remedial action during the time period referred to in paragraph 1, the certificate shall be suspended in accordance with Article 19 or withdrawn in accordance with Article 11.	Like for nonconformities, the CB has means to force the certificate holder to act
3. Continued or recurring infringement by the holder of the [EUDIW] certificate of the obligations referred to in paragraph 1 shall trigger	Unlike nonconformities, multiple infringements will lead directly to withdrawal.

[15] There is no direct reference to this non-compliance of the provider in regulation (EU)2024/2981.

the withdrawal of the [EUDIW] certificate in accordance with Article 11.	
4. The certification body shall inform the [scheme owner] of the findings referred to in paragraph 1. The [scheme owner] shall immediately notify the supervisory body referred to in Article 46a of Regulation (EU) No 910/2014.	In EUCC, this paragraph is about presumption of conformity. It was replaced by a reference to the eIDAS supervisory body.

Discussion

This article sounds a lot like the previous one, but the main difference is that a non-compliance is generally considered more serious than a nonconformity, because non-compliance is about a certificate holder not fulfilling its contractual obligations, whereas a nonconformity may be related to a technicality that the certificate holder strives to address.

The main differences are in paragraph 3, which indicates that “continued or recurring” non-compliance leads to withdrawal of the certificate, and in paragraph 4, since non-compliance needs to be reported to supervision authorities, as they may indicate an issue with the behaviour of the certificate holder.

Also, there is no notion of materiality, as non-compliance is always material.

Finally, Regulation (EU) 2024/2981 requires sanctions to be defined in case of fraudulent use, which could fall around paragraphs 1 (if sanctions are considered immediately for some violations) or 3 (if sanctions come with sustained violations, more or less associated with the withdrawal of the certificates).

***NOTE**: Non-compliance is specific to a given certificate, but it impacts the service provider rather than the service itself. For this reason, if a service provider has been issued several certificates, non-compliance with respect to one of the certificates should trigger at least specific monitoring actions on all certificates held by the same provider. In addition, the supervision authority would be expected to notify their counterparts in other Member States in case of non-compliance.*

7.3 SUSPENSION OF THE EUDIW CERTIFICATE

Article 19 defines the initial conditions for suspension:

Article 19	Notes on Article 19
1. Where this Regulation refers to suspension of an [EUDIW] certificate, the certification body shall suspend an [EUDIW] certificate concerned for a period appropriate to the circumstances triggering suspension, that does not exceed 42 days. The suspension period shall begin on the day following the day of the decision of the certification body. The suspension shall not affect the validity of the certificate.	Suspension is intended to indicate that there is an issue with the certificate, but that the expectation is that the certificate holder will address the issue, and that the CB is monitoring the situation.
2. The certification body shall notify the holder of the certificate and the [scheme owner] of the suspension without undue delay and shall provide the reasons for the suspension, the requested actions to be taken and the suspension period.	Suspension is decided by the CB, but the owner of course needs to be notified, as well as the scheme owner.
3. The holder of the certificate shall notify the users of the ICT services concerned about the suspension and the reasons provided by the certification body for the suspension, except those parts of the reasons the sharing of which would constitute a security risk or which contain sensitive information, as well as guidance for users of the ICT service. This information shall also be made publicly available by the holder of the certificate.	Users need to be notified, but here, the users should be understood as the authorities in charge of managing the wallet, not the end users. We have added an obligation for the certificate holder to provide guidance, so the users can use it to decide how to best protect the end users.
4. The [scheme owner] may inform the supervisory body referred to in Article 46a(1) of Regulation (EU) No 910/2014 about the suspension.	The proposal is to let the scheme owner decide whether or not to notify the supervisory body

5. In duly justified cases, the [scheme owner] may authorise an extension of the period of suspension of an [EUDIW] certificate. The total period of suspension may not exceed 1 year.	Because the default maximum length is short, such a clause is necessary, but the body making the decision may be another one.

DISCUSSION

Suspension of a certificate is a mechanism to be used when there is an issue that could be material, but is expected to be remediated rapidly. Users of the certificate have to be notified, and to be provided guidance on how to handle the issue, and they can decide on the way to handle the suspension.

We have proposed not to systematically notify the supervisory body, and to leave this decision to the scheme owner (the NCCA in EUCC), because suspension is an event related to certification, which may be difficult to interpret, and also because Regulation (EU)2025/849 does not make it mandatory to notify the Commission and EDICG about suspension of certificates. However, this may be reconsidered if the scheme owner does not have the required cybersecurity expertise, or if there is an interest from EDICG to receive notifications of certificate suspensions.

Once again, this topic outlines the essential role of the scheme owner, in particular when issues arise after the issuance of a certificate. The scheme owner has a significant role here, in deciding whether or not to notify the supervision authority, and also how to describe the issue to them.

7.4 CONSEQUENCES OF NON-COMPLIANCE BY THE CB

When a CB is non-compliant, the consequences may be quite significant, depending on the reason for non-compliance. In particular, if the non-compliance is related to competences or to the execution of conformity assessment activities, then the validity of certificates issued by the CB may be compromised.

Article 20 defines these rules:

Article 20	Notes on Article 20
1. In case of non-compliance by a certification body with its obligations, the [scheme owner] shall, without undue delay: (a) identify the potentially affected [EUDIW] certificates; (b) where necessary to support that identification, request conformity assessment activities to be performed on one or more ICT services by either the certification body which issued the certificate, or any other accredited and authorised certification body that may be in a better technical position to perform these activities; (c) analyse the impacts of non-compliance by the certification body; (d) notify the holders of the [EUDIW] certificates affected by non-compliance by the certification body.	There may be a great variety of reasons for the non-compliance of a certification body. However, the main issue is when conformity assessment activities have not been appropriately performed, for instance because of a lack of competences, because this may lead the authorities to reconsider the validity of the certificates issued by the CB[16].
2. For every certificate affected by non-compliance of the certification body, the [scheme owner] shall, without undue delay: (a) identify the conformity assessment activities that have to be reperformed, if required with the support of the non-compliant certification body or of or any other accredited and authorised certification body that may be in a better technical position to perform these activities; (b) for every such conformity activity, request the activity to be performed by either the certification body which issued the certificate, or any other accredited and authorised certification	When this happens, conformity assessment activities have to be done again. In some cases, they may have to be performed by another CB.

[16] Article 17(6) of regulation (EU)2024/2981 requires the definition of these consequences.

body that may be in a better technical position to perform this activity.	
3. Any nonconformity of a certified ICT service identified while reperforming conformity assessment activities shall be processed according to Article 17.	Nonconformities may be discovered while performing these activities, which have to be managed like any nonconformity found after certification (with potential consequences up to the withdrawal of the certification).
4. The non-compliant certification body shall be responsible for the costs related to the activities in paragraph 2.	The costs related to these additional activities are the responsibility of the non-compliant CB, including when another CB is performing the actions.
5. On the basis of the measures referred to in paragraph 1, the [scheme owner] shall: (a) where necessary, report the non-compliance of the certification body to the national accreditation body; (b) where applicable, assess the potential impact on the authorisation.	In addition to the impact on certificates, the accreditation and authorisation of the CB may need to be reconsidered.

DISCUSSION

CABs operate under the authority of the NAB, so most of their supervision is out of scope of the scheme. Nevertheless, the NCCA/scheme owner has a responsibility towards the certificates and towards the authorisation of the CABs that may lead them to identify issues with CBs (if authorisation is implemented in the scheme).

This article mostly covers the impact of such issues on the certificates issued by the non-compliant CB, and organises the re-evaluation of the services that have been certified by the non-compliant CB.

This is a key role for the scheme owner, who needs to have the required expertise to organise this re-evaluation, especially if there is a risk that the non-compliance may have hidden material nonconformities about the certified service.

Note that we propose to include in the scheme a requirement for the non-compliant CB to be financially liable for the extra work to be performed due to their non-compliance, but we stop short of requiring a financial compensation for the provider of the certified service, as this could be handled in contracts between the CB and the provider.

8. VULNERABILITY MANAGEMENT

This chapter covers vulnerability management rules, which are quite limited here, since they mostly constrain the vulnerability management policy that every provider of certified services is required to implement.

This is section I of Chapter 5, *Vulnerability Management and Disclosure*.

8.1 SCOPE OF VULNERABILITY MANAGEMENT

Article 21 is very short , and it also applies to the following chapter, on vulnerability disclosure:

Article 21	Notes on Article 21
This Chapter applies to ICT services for which an [EUDIW] certificate was issued.	This may sound obvious, but it is better to state it.

8.2 VUNERABILITY MANAGEMENT PROCEDURES

Article 22 defines the basic rules.

Article 22	Notes on Article 22
1. The holder of an [EUDIW] certificate shall establish, maintain and operate all necessary vulnerability management procedures in accordance with the rules laid down in this Section and, where necessary, supplemented by the procedures set out in EN ISO/IEC 30111.	The reference is to a very generic standard, which provides interesting guidance on the management of risks.
2. For all relevant components of the ICT service, the vulnerability management procedures mentioned in paragraph 1 shall include: (a) the use of a software bill of materials in a commonly used and machine-readable format, covering at the very least the top-level dependencies of the component; (b) the use of security updates to remediate vulnerabilities, and when technically feasible, separate from functional updates; (c) mechanism to securely distribute updates, including a mechanism to ensure that the vulnerabilities are remediated without delay, where applicable, an automated distribution of security updates, and where applicable, a mechanism to disable the operation of a wallet unit until required security updates have been applied; (d) the distribution in relation to updates of advisory messages providing users with the relevant information, including on potential action to be taken.	Paragraph 2 adds some details from CRA, which apply to all “relevant components” of the ICT service. This at least including the software product components. This paragraph can be removed, but it is also an interesting reminder that CRA will apply to at least some of the wallet components, and that the CRA requirements are rather standard requirements, so they provide a good basis. In addition, harmonised standards will be developed, which should help for their assessment.
3. The holder of an [EUDIW] certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their products from external sources, including users, certification bodies and security researchers.	This is a bit redundant for CSA schemes, since it is an obligation stemming from CSA’s Article 55. But in the context of a national scheme, this is a strong requirement.
4. Where a holder of an [EUDIW] certificate detects or receives information about a potential vulnerability affecting a certified ICT service, it shall record it and carry out a vulnerability impact analysis.	The identification of a vulnerability triggers a vulnerability impact analysis, which I defined in the following article.
5. In response to a reasonable request by the certification body that issued the certificate, the holder of an [EUDIW] certificate shall transmit all relevant information about potential vulnerabilities to that certification body.	The CB also has the possibility to inquire about a vulnerability, typically when a vulnerability is identified in one of components on which they depend (identified from the Software Bill Of Materials (SBOM)).

Discussion

This article can be simplified, but it is important to keep an explicit requirement for a vulnerability management procedure, and also for the requirement to establish means for researchers and users to report potential issues.

8.3 VULNERABILITY IMPACT ANALYSIS

Article 23 describes the analysis, and is much less specific in its description than the original EUCC article:

Article 23	Notes on Article 23
1. The vulnerability impact analysis shall refer to the description of the object of certification and the assurance statements contained in the certificate. The vulnerability impact analysis shall be carried out in a timeframe appropriate for the exploitability and criticality of the potential vulnerability of the certified ICT service.	There is no precise deadline, but some vulnerabilities would need to be investigated and fixed in a very short time, especially when related to operational issues.
2. The materiality of the impact shall be determined in accordance with the relevant methodology defined in Annex XI, in order to determine the exploitability and impact of the vulnerability.	We again use the notion of materiality.

Discussion

It is very important here to differentiate between the vulnerability and its impact. The urgency of the vulnerability analysis is likely to be determined by the criticality of the vulnerability itself, estimated with a system like CVSS.

The goal of the impact analysis is to determine the level of the impact on the certified service. In some cases, a critical vulnerability may have a negligible impact, if the vulnerable feature is not used or not accessible in the implementation. In other cases, a vulnerability with a lower rating may have greater impact, for instance if it impacts the security of the cryptography behind the WSCD implementation.

Here, what needs to be determined is the materiality of the impact of the vulnerability. A threshold will need to be defined, and we propose to use existing ones when available. For instance, on a product component that has been evaluated using EUCC, the attack rating would be the proper tool. Additional information will be made available in an annex.

The objective is here to limit the interactions between the certificate holder and the certification body to the essential ones. In a complex system, there may be a large number of vulnerabilities to manage, but most of them should have limited impact and be easily managed, not requiring the involvement of the CB. These vulnerabilities will be considered at the end of the year, during the surveillance evaluation, as part of the evaluation of the effectiveness of the vulnerability management process.

8.4 VULNERABILITY IMPACT ANALYSIS REPORT:

Article 24 defines the conditions for producing a vulnerability impact analysis report:

Article 24	Notes on Article 24
1. The holder shall produce a vulnerability impact analysis report where the impact analysis shows that the vulnerability has a material impact on the security of the ICT service, as defined in Annex XI, which in turn has a likely impact on the conformity of the ICT service with its certificate.	The report must be produced for vulnerabilities where the impact analysis shows the materiality of the potential impact. However, this doesn't mean that other vulnerabilities should not be covered by some kind of impact analysis, just that there are no specific requirements for these.

2. The vulnerability impact analysis report shall contain an assessment of the following elements: (a) the impact of the vulnerability on the certified ICT service; (b) possible risks associated with the proximity or availability of an attack; (c) whether the vulnerability may be remedied; (d) where the vulnerability may be remedied, possible resolutions of the vulnerability.	The report needs to contain the information that the CAB needs to take an informed decision about the continuing validity of the certificate.
3. The vulnerability impact analysis report shall, where applicable, contain details about the possible means of exploitation of the vulnerability. Information pertaining to possible means of exploitation of the vulnerability shall be handled in accordance with appropriate security measures to protect its confidentiality and ensure, where necessary, its limited distribution.	If exploitation means are known, they have to be described in the report, but specific precautions then need to be taken in order to avoid disclosure of that information.
4. The holder of an EUDIW certificate shall transmit a vulnerability impact analysis report to the certification body, without undue delay.	There is no precise definition of the "undue delay" because it depends greatly on the type of vulnerability.
5. Where the vulnerability impact analysis report determines that the vulnerability has a material impact on the security of the ICT service, and that it can be remedied, Article 25 shall apply.	Remediation requirements are defined in the following article.
6. Where the vulnerability impact analysis report determines that the vulnerability has a material impact on the security of the ICT service and that it cannot be remedied, the [EUDIW] certificate shall be withdrawn in accordance with Article 11.	If a material vulnerability cannot be remedied, withdrawal is unavoidable.
7. The holder of the EUDIW certificate shall monitor any residual vulnerabilities to ensure that they cannot be exploited in case of the changes in the operational environment.	See the discussion below on residual vulnerabilities.
8. Residual vulnerabilities shall be considered in the periodic vulnerability assessments.	

Discussion

This section, like other sections on vulnerability management, does not provide very strong timing guidelines, due to the different nature of vulnerabilities that may be encountered.

For product vulnerabilities, handling is expected to be quite similar to what it is in EUCC, with relatively long delays, as required to ensure that the update is properly performed (commensurate with the complexity of the update). This is complex, so you should not attempt to define and enforce delays without carefully thinking of all consequences. In all cases, we would recommend to include "loopholes", by allowing delay extensions under the authority of the scheme owner, to avoid having to withdraw a certificate when other solutions would be possible.

For vulnerabilities on services, the fixes are often simpler. Some testing is required, but the deployment of the fix is much simpler as it is deployed on a system that is under the control of the wallet provider. Also, the relative ease of exploitation of such vulnerabilities is likely to lead to much faster procedures and delays between the identification of the vulnerability and its remediation.

Residual vulnerabilities

A residual vulnerability is a vulnerability that has not yet been fixed (or cannot be fixed), but that has been remediated by other measures.

In such cases, specific monitoring is required, because the adequacy of the measures depends on the threat environment. As the threats evolve, the mitigation measures may need to be reinforced, or in the worst case, could not be sufficiently effective. The wallet provider therefore has an obligation to monitor the threat environment, and these residual vulnerabilities need to be considered by the CB in the vulnerability assessment that is performed every two years.

8.5 VULNERABILITY REMEDIATION

Remediation is here covered for all vulnerabilities, not only for vulnerabilities with major impact:

Article 25	Notes on Article 25
1. The holder of an [EUDIW] certificate shall design and implement a remediation plan in a timely manner for all vulnerabilities that may impact the certified ICT service.	A remediation plan needs to be available for all vulnerabilities.
2. Where the holder of an [EUDIW] certificate has submitted a vulnerability impact assessment report to their certification body, the holder of an [EUDIW] certificate shall also submit a proposal for an appropriate remedial action to the certification body. The certification body shall review the certificate in accordance with Article 10. The scope of the review shall be determined by the proposed remediation of the vulnerability.	In the case of a vulnerability with material impact, about which a report has been shared with the CB, a remedial action plan also needs to be shared, although not necessarily together with the initial report. Depending on the remediation, the CB then needs to review the certificate.

Discussion

Once again, the objective is here to limit the interactions with the CB to the essential ones, related to the most impactful vulnerabilities. Nevertheless, a remediation plan needs to be available for all vulnerabilities, and evidence of the impact assessment and of the preparation and execution of the remediation plan need to be kept for the CB to verify the effectiveness of the vulnerability management process.

9. VULNERABILITY DISCLOSURE

Vulnerability disclosure needs to be implement responsibly, following a coordinated vulnerability disclosure policy, and some collaboration needs to be organised as well.

This is section I of Chapter 5, *Vulnerability Management and Disclosure*.

9.1 COORDINATED VULNERABILITY DISCLOSURE

This is presently missing, so we propose to introduce another Article at the beginning of this chapter:

Article 26	Notes on Article 26
1. The holder of an [EUDIW] certificate shall establish, maintain and operate a coordinated vulnerability disclosure policy and related procedures, in accordance with the rules laid down in this Section and, where necessary, supplemented by the procedures set out in EN ISO/IEC 29147.	A coordinated vulnerability disclosure policy ensures that key stakeholders are informed of a potentially impactful vulnerability before it is made public, allowing them to apply the recommended measures before the vulnerability becomes known to the general public.
2. The holder of an [EUDIW] certificate shall make their coordinated vulnerability disclosure policy and procedures publicly available.	Since this is a policy for external stakeholders, it has to be made public.

Discussion

This is not mandatory in EUCC, but the EUCC guidance strongly recommends using such a coordinated vulnerability disclosure policy. We decided to make it mandatory here because security issues in EUDI wallets may have significant impact, so it is mandatory to have processes available to manage complex situations.

9.2 INFORMATION SHARED WITH THE SUPERVISORY BODIES

Article 27 describes the sharing of information to and between supervisory bodies:

Article 27	Notes on Article 27
1. The information provided by the certification body to the [scheme owner] shall include all elements necessary for the [scheme owner] to understand the impact of the vulnerability, the changes to be made to the ICT service and, where available, any information from the certification body on the broader implications of the vulnerability for other certified ICT services.	The scheme owner needs to be mentioned in the CVD policy, and this paragraph provides details of the information that needs to be sent to them.
2. The information provided in accordance with paragraph 1 shall not contain details of the means of exploitation of the vulnerability. This provision is without prejudice to the investigative powers of the [scheme owner].	This may need to be revised depending of the nature of the scheme owner (who may not have any investigative powers).
3. The [scheme owner] shall share the relevant information received in accordance with Article 27 with national supervisory bodies established in their country pursuant to Article 46a(1) of eIDAS.	Like for nonconformities, the scheme owner is supposed to filter the vulnerability disclosures and only forward the most relevant ones to the supervisory body.
4. The national supervisory bodies established in their country pursuant to Article 46a(1) of eIDAS shall share the relevant information received in accordance with Article 27 with the national supervisory bodies established in other Member States.	This last paragraph from EUCC's Article 38, which is very much simplified

DISCUSSION

Paragraph 4 requires supervisory bodies to share “relevant” information between each other. Each supervisory body is responsible for assessing what constitutes relevant information.

There may be a need for a harmonised procedure here, to ensure that the criteria used by the different supervisory bodes are harmonised between Member States.

Once again, in the absence of the NCCA, the scheme owner may not have all the skills required to decide which information is relevant for the eIDAS supervisory body. In that case, this responsibility needs to be assigned to another stakeholder, possibly the CB.

9.3 PUBLICATION OF THE VULNERABILITY

Article 28 defines basic rules for publication:

Article 28	Notes on Article 28
Upon withdrawal of a certificate or upon remediation of a vulnerability, possibly including the addition of an amendment to a certificate, the holder of the [EUDIW] certificate shall disclose and register any publicly known and remediated vulnerability in the ICT service or its components on the European vulnerability database, established in accordance with Article 12 of Directive (EU) 2022/2555 of the European Parliament and of the Council or other online repositories referred to in the description of the certified service.	Vulnerabilities need to be published whenever a vulnerability has been handled, or the certificate has been withdrawn because the vulnerability could not be handled.

DISCUSSION

***WARNING**: This article needs additional work, because the situation is here quite different from EUCC, since many vulnerabilities will be handled without modifying the certificate.*

In addition, many of the vulnerabilities handled are expected to be on third-party components, so there may not need to publish them specifically. This issue will be raised to the horizontal thematic group on vulnerabilities.

Ideally, the rules for publication of vulnerabilities should be harmonised between Member States, and discussed in the EDICG, together with the rules on information sharing between supervisory bodies.

10. RETENTION, DISCLOSURE AND PROTECTION OF INFORMATION

The rules defined here are mostly related to the management of documentation, to ensure that it remains available in case of technical issue or legal challenge.

This is Chapter 6, *Retention, disclosure and protection of information*.

10.1 RETENTION OF RECORDS BY CERTIFICATION BODIES

Article 29 defines delays and other requirements on retention of records by CBs:

Article 29	Notes on Article 29
1. The certification bodies shall maintain a record system, which shall contain all documents produced in connection with each evaluation and certification they perform.	This is a basic requirement.
2. Certification bodies shall store the records in a secure manner and shall keep those records for the period necessary for the purposes of this Regulation and for at least 5 years after the withdrawal of the relevant EUDIW certificate. When the certification body has issued a new EUDIW certificate in accordance with Article 10(2), point (c), it shall retain the documentation of the withdrawn EUDIW certificate together with and as long as for the new EUDIW certificate.	Unless there are specific national requirements to be considered, we recommend to keep the timeframe used in EUCC (5 years after withdrawal).

Discussion

The period may end up being quite long, since a service may be kept in service for quite a long time, despite its evolution over the years.

We may need to update this in the future in order to slightly reduce the length during which information needs to be kept, but the approximation is sufficient for now.

10.2 INFORMATION MADE AVAILABLE BY THE HOLDER OF A CERTIFICATE

Article 30 defines obligations for the certificate holder:

Article 30	Notes on Article 30
1. The information identified in Annex III as being made available publicly shall be available in a language that can be easily accessible to users.	The mention of CSA Article 55 has been extended to all publicly available information.
2. The holder of an [EUDIW] certificate shall store the following securely for the period necessary for the purposes of this Regulation and for at least 5 years after the withdrawal of the relevant [EUDIW] certificate: (a) records of the information provided to the certification body during the certification process; (b) specimen of the product components of the certified ICT service.	Once again, the 5 years should be sufficient. There are ongoing discussions about “specimens”, so this specific detail may need to be updated.

3. When the certification body has issued a new [EUDIW] certificate in accordance with Article 10(2), point (c), the holder shall retain the documentation of the withdrawn [EUDIW] certificate together with and as long as for the new [EUDIW] certificate.	The documentation needs to be kept independently of the evolution of the wallet service.
4. Upon request by the certification body or the [scheme owner], the holder of an [EUDIW] certificate shall make available the records and copies referred to in paragraph 2.	Naturally, the scheme owner or CB have the right to access this information if they need to investigate something.

Discussion

It is not clear how the "specimens" need to be kept by the certificate holder. In some cases, because of change management, there may be different versions of the software available on a given hardware, so this should not be interpreted as keeping a version of each hardware and software combination, which would be too difficult, but only as keep ing a version of each hardware, together with a way to reconstruct every version of software running on that hardware.

10.3 PROTECTION OF INFORMATION

Article 31 is inspired from EUCC to require the implementation by CBs of sufficient security measures in their own information systems where client information is stored.

Article 31	Notes on Article 31
Conformity assessment bodies, [scheme owner], supervisory bodies, the Commission and all other parties shall ensure the security and protection of business secrets and other confidential information, including trade secrets, as well as the preserving intellectual property rights, and take the necessary and appropriate technical and organisational measures.	The objective is here to protect the intellectual property of the wallet provider.

11. MUTUAL RECOGNITION AND PEER ASSESSMENT

This chapter covers mutual recognition and peer assessment. These topics should be discussed together, but the scope remains unclear, depending on the way in which Member State will rely on each other (or not).

This is Chapter 7, *Mutual recognition and peer assessment of conformity assessment bodies.*

11.1 CONDITIONS FOR MUTUAL RECOGNITION

Mutual recognition with third countries may not be very relevant for national schemes, but on the other hand, there may be a need to define conditions for mutual recognition between Member States, which could be based on Article 32:.

Article 32	Notes on Article 32
1. Countries willing to certify their products in accordance with this Regulation, and who wish to have such certification recognised within [MSName], shall conclude a mutual recognition agreement with [MSName].	This is the first paragraph, but we are not providing the rest. See discussion below..

Discussion

***WARNING**: The present discussion presents some elements to be considering when establishing mutual recognition between national certification schemes, but such agreements should be considered based on many considerations that are not covered here. In all cases, mutual recognition terms should be discussed between members of a group.*

Typically, the minimum requirements for mutual recognition would be twofold. First, the schemes should use the same annexes, which define the technical framework of certification (requirements, methods, content of certificates and reports, maintenance schedules, etc.). Then, the schemes should have similar rules regarding important topics such as monitoring and continuity of compliance, and also about the lifecycle of certificates, including in particular the conditions for suspension and withdrawal.

In addition, mutual recognition should come with some kind of mutualised control, which is typically organised as peer assessment of CBs. Note that this should be complemented with peer evaluation of scheme owners, which could be inspired in part from the rules for the peer review of NCCAs under the CSA.

This MRA may include the following information:

- participants to the MRA;
- purpose and spirit of the Agreement;
- membership;
- scope;

- exceptions;
- definitions;
- conditions for recognition of certificates;
- peer assessments;
- publications;
- sharing of Information;
- acceptance of new participants and compliant authorities or bodies;
- administration of this Agreement;
- disagreements;
- costs of this Agreement;
- revision;
- duration;
- voluntary termination of participation;
- commencement and continuation;
- effect of this Agreement.

Conditions for recognition of certificates by participants to such an MRA should include at a minimum the following conditions:

- the participants shall commit themselves to recognise applicable conformant certificates by any accepted Participant;
- acceptance of participants shall confirm that the evaluation, review, decision and certification activities have been carried out in a duly professional manner:
  - on the basis of commonly accepted ICT security evaluation criteria;
  - using commonly accepted ICT security evaluation methods;
  - in the context of an evaluation and certification scheme managed by a compliant certification body in the accepted participant's country;
  - the conformant certificates and certification reports issued satisfy the objectives of this Agreement;
- certificates which meet all these conditions shall be termed as conformant certificates for the purposes of this Agreement;
- ICT security evaluation criteria are to be those laid down in Annex X of this document;
- ICT security evaluation methods are to be those laid down in Annex XI of this document;
- minimum requirements for Certification Reports are laid down in Annex VI to this document;
- minimum requirements for Certification Assessment Reports are laid down in Annex VII to this document;
- the scheme of the participants or to which the participants adhere shall be organised with a proper National Authority and conformity assessment bodies (CABs), in accordance with the following requirements:
  - the National Authority supervises the certification activities, notifies and, where applicable, authorises CABs, and reports any vulnerability of certified cloud services to the scheme owners of the other participants;
  - the CAB has been accredited in its respective country by a recognised Accreditation Body in accordance with ISO/IEC 17065 and has been authorised where necessary by the National Authority;
  - the CAB is accepted as compliant by the Participants through a peer assessment mechanism installed for the MRA;
  - the CAB has been where necessary subject to an assessment by the National Authority in order to confirm its competence to perform evaluations, in accordance with Article 13 of this document;
- in order to assist the consistent application of the criteria and methods between evaluation and certification schemes, the participants plan to work towards a uniform interpretation of the currently applicable criteria and methods and commit to accept the supporting

documents that results from this work. In pursuit of this goal, the participants also plan to conduct regular exchanges of information on interpretations and discussions necessary to resolve differences of interpretation;

- in further aid to the goal of consistent, credible and competent application of the criteria and methods, the certification bodies shall undertake the responsibility for the monitoring of all evaluations in progress within the MRA at an appropriate level, and carrying out other procedures to ensure that all CABs:
  - perform evaluations impartially;
  - apply the criteria and methods correctly and consistently;
  - have and maintain the required technical competencies;
  - adequately protect the confidentiality of sensitive or protected information.

Note that these conditions are quite stringent, and basically required the use of an equivalent scheme. The recommendation is to go as far as possible in requiring all mechanisms to be identical or equivalent.

11.2 PEER ASSESSMENT PROCEDURE

Article 33 defines peer assessment procedures, which typically complement mutual recognition agreements to ensure that the criteria are met by all signatories of the MRA:

Article 33	Notes on Article 30
1. A certification body issuing [EUDIW] certificates shall undergo a peer assessment on a regular basis and at least every 5 years. The different types of peer assessment are listed in Annex VIII.	The frequency may depend on the number of states and CABs in the mutual recognition agreement.
2. The [mutual recognition group] shall draw up and maintain a schedule of peer assessments ensuring that such periodicity is respected. Except in duly justified cases, peer assessments shall be performed on-site.	References to the ECCG are replaced by a more neutral “mutual recognition group”.
3. The peer assessment may rely on evidence gathered in the course of previous peer assessments or equivalent procedures of the peer-assessed certification body, provided that: (a) the results are not older than 5 years; (b) the results are accompanied by a description of the peer assessment procedures established for that scheme where they relate to a peer assessment conducted under a different certification scheme; (c) the peer assessment report referred to in Article 40 specifies which results were reused with or without further assessment.	Evidence that is less than 5 years old can be reused if it meets simple conditions.
4. The peer-assessed certification body shall ensure that all relevant information is made available to the peer assessment team.	
5. The peer assessment shall be carried out by a peer assessment team set up in accordance with Annex VIII.	

Discussion

This is a very basic setup that should meet the requirements of most mutual recognition agreements, and can at least be used as a checklist of things to think about when setting up a peer assessment procedure.

11.3 PEER ASSESSMENT PHASES

This article is directly inspired from EUCC:

Article 34	Notes on Article 34

1. During the preparatory phase, the members of the peer assessment team shall review the certification body's documentation, covering its policies and procedures, including the use of state-of-the-art documents.	
2. During the site visit phase, the peer assessment team assesses the body's technical competence.	
3. The duration of the site visit phase may be extended or reduced depending on such factors as the possibility of reusing existing peer assessment evidence and results.	
4. In the reporting phase, the assessment team shall document their findings in a peer assessment report including a verdict and, where applicable, a list of observed nonconformities, each graded by a criticality level.	
5. The peer assessment report must be first discussed with the peer-assessed certification body. Following those discussions, the peer-assessed certification body establishes a schedule of the measures to be taken to address the findings.	

Discussion

All the items above are very basic, there isn't much to add…

11.4 PEER ASSESSMENT REPORT

This article is directly inspired from EUCC:

Article 35	Notes on Article 35
1. The peer assessment team shall provide the peer-assessed certification body with a draft of the peer assessment report.	
2. The peer-assessed certification body shall submit to the peer assessment team comments regarding the findings and a list of commitments to address the shortcomings identified in the draft peer assessment report.	
3. The peer assessment team shall submit to the [mutual recognition group] a final peer assessment report, which shall also include the comments and the commitments made by the peer-assessed certification body. The peer assessment team shall also include their position on the comments and on whether those commitments are sufficient to address the shortcomings identified.	
4. Where non-conformities are identified in the peer-assessment report, the [mutual recognition group] may set an appropriate time limit for the peer-assessed certification body to address the non-conformities.	
5. The [mutual recognition group] shall adopt an opinion on the peer assessment report: (a) where the peer-assessment report does not identify nonconformities or where nonconformities have been appropriately addressed by the peer-assessed certification body, the [mutual recognition group] may issue a positive opinion and all relevant documents shall be published on [transparency website]; (b) where the peer-assessed certification body does not address the nonconformities appropriately within the set time limit, the [mutual recognition group] may issue a negative opinion that shall be published on [transparency website], including the peer assessment report and all relevant documents.	The "transparency website" replaces "ENISA's certification website", and is intended to be a website where the entities involved in the mutual recognition group publish information.
6. Prior to the publication of the opinion, all sensitive, personal or proprietary information shall be removed from the published documents.	

Discussion

The requirements are quite basic, and suitable for any kind of peer assessment group, but some adaptation may be required depend on the nature of the group.

We do recommend to keep the transparency requirements, unless there is an agreement between the Member States involved in the mutual recognition group to make the remarks in a peer assessment binding.

12. MAINTENANCE AND FINAL PROVISIONS

12.1 MAINTENANCE OF THE NATIONAL EUDIW SCHEMES

It is difficult to propose text for these final provisions, but the following issues most likely need to be considered:

- Depending on the legal status of the scheme, it may be easier to move some of the documentation outside of the scheme (and its annexes), and into “state-of-the-art documents”, to be endorsed by the signatories of the mutual recognition agreement and published somewhere.
- There could also be a mandate to revise the National scheme after adoption of a European Cybersecurity Certification Scheme, since the cybersecurity aspects will be transferred to the EU scheme, whereas the functional aspects will remain in the scope of the national schemes.

EUCC’s Articles 48 and 49 can provide some inspiration for this, but they would need to be significantly updated.

NOTE*: The CSA typically considers rather long delays during which national schemes are allowed to issue certificates that cover the aspects also covered by the EU scheme, but of course, national schemes would have the possibility to shorten these delays in order to encourage a quick transition to the European schemes for relevant aspects.*

13. ABOUT ANNEXES

13.1 PROPOSED ANNEXES

The annexes that we propose for a national EUDIW scheme are inspired from several sources, including the EUCC Implementing Act Annexes, the EUCC state-of-the-art (SOTA) documents, and the Annexes to the 5c Implementing Act (EU)2024/2981.

For national EUDIW schemes, we will not differentiate between annexes and SOTA documents, so the list of annexes could be as follows (including some that are strongly inspired from documents adopted as SOTAs for EUCC).

- Annex I: Scope of certification
- Annex II: Assurance continuity and certification lifecycle
- Annex III: List of publicly available information
- Annex IV: List of information required upon application for certification
- Annex V: Content of a certificate
- Annex VI: Content of a certification report
- Annex VII: Content of a certification assessment report
- Annex VIII: Scope and team composition for peer assessment
- Annex IX: Criteria to assess the acceptability of assurance information
- Annex X: Security requirements for EUDI Wallets and the eID schemes under which they are provided
- Annex XI: Methods and procedures for evaluation activities

Finally, we would propose to adapt some of the guidelines available for EUCC, possibly adding them as annexes:

a) Composition of certificates
b) Accreditation of CABs for EUDIW
c) EUDIW guidelines on the authorization of CABs

WARNING*: The work on these annexes is only starting at the moment. They have been added because they are critical in the definition of the schemes. Also, for some annexes, the content may be suitable for both the European cybersecurity certification scheme and for the national schemes, which may pave the way for harmonisation.*

14. ANNEX I: SCOPE OF CERTIFICATION

WHAT? This annex is intended to define the scope of certification, based on the discussion held in TG2.

HOW? The annex should define the scope of certification, composed of the object of certification and of a high-level view of the requirements on each component of the service.

This Annex still is work in progress, as there are significant questions that are still being addressed, in particular regarding the definitions of the basic components of the EUDI Wallet. Also, we have kept in this annex the distinction between the EUDI Wallet and the eID scheme under which it is provided.

In addition, in the context of national schemes, the scope of certification should include one or more profiles, as discussed in the last section.

***NOTE**: Many of the requirements are taken or inspired from other regulations, in particular NIS2 and CRA. Although these regulations do not necessarily apply to all services to be certified under the present scheme, we have chosen to use the requirements that they define as baselines for the requirements of the present scheme where applicable, in order to avoid the definition and maintenance of another set of requirements.*

***NOTE**: some essential definitions are inserted as notes in this Annex as a reminder.*

14.1 OVERALL SCOPE

1. Certificates are issued under the present scheme to ICT services related to European Digital Identity wallets and to the electronic identity schemes under which they are provided, including as defined in Article 1 of the present regulation:

(a) services for the provision of European digital identity ('EUDI') wallets;
(b) services related to the provision of an electronic identity ('eID') scheme;
(c) services related to the validation of EUDI Wallets and Relying Parties.

We here provide as a reminder the definition of a component that we have adopted, which is essential for the rest of this Annex:

***component** smallest selectable set of elements on which requirements may be based*
[From ISO/IEC 15408-1:2022(en), 3.17]

2. Each certified service is built by combining components, which may themselves be ICT products, ICT services, information security management systems (ISMS), or processes.

***NOTE**: We made the choice to include an ISMS as mandatory component, because it is mentioned in (EU)2015/1502, but it would be possible to consider the mention of ICT systems instead, in order to leave more freedom on the means available to demonstrate the conformity*

of ICT systems to requirements.
NOTE*: The mention of processes (without an ICT qualifier) is voluntary, since some of the processes used may not strictly be ICT processes, but human-based processes supporting the provision of an ICT service.*

3. Each ICT service certified under the present scheme shall include at least the following components, which shall be demonstrated in conformity with the listed requirements:

ICT system	The ICT system on which the ICT service relies for its provision. Note that the IT system is covered as a "full stack", so evidence of conformity is expected to be available for the entire system.	**Reference**: - NIS2 IA Annex - (CIR)2015/1502, level 'high' (for eID schemes) **Other** - CEN TS 18026, level 'substantial' - ISO/IEC 27001
Development process	The process operated by the ICT service provider for the development of its ICT service.	**Reference**: - NIS2 IA Annex **Other** - CEN TS 18026, level 'substantial' - ISO/IEC 27001
Change management process	The process operated by the ICT service provider for the management of the changes in the ICT service.	**Reference**: - NIS2 IA Annex **Other** - CEN TS 18026, level 'substantial' - ISO/IEC 27001
Vulnerability management process	The process operated by the ICT service provider for the management and handling of vulnerabilities in the ICT service.	**Reference**: - NIS2 IA Annex - CRA Annex I, Section 2 **Other** - CEN TS 18026, level 'substantial' - ISO/IEC 27001 - Upcoming CRA-related standards
Incident management process	The process operated by the ICT service provider for the management and handling of cybersecurity incidents in the ICT service.	**Reference**: - NIS2 IA Annex **Other** - CEN TS 18026, level 'substantial' - ISO/IEC 27001
Fraud management process	The process operated by the ICT service provider for the management of fraud in the ICT service.	Still under investigation in TG2

4. The ICT service provider shall define assumptions on the environment used by components of the ICT service that allow the components to meet the requirements applying to them.

5. The ICT service provider shall demonstrate the validity of the assumptions defined on the environment used by components of the ICT service:

a) if the environment is provided by the ICT service provider, then the provider shall provide evidence that the environment satisfies all the assumptions defined for it;
b) if the environment is provided by the wallet user, then the ICT service provider shall define appropriate controls to verify the assumptions on the environment, and they shall validate the sufficiency of these measures and verify their effectiveness.

NOTE*: The notion of "supplied by the ICT service provider" does not preclude environments that are provided by a third-party contracted by the ICT service provider (e.g., cloud service provider).*

14.2 SERVICES RELATED TO THE PROVISION OF AN EUDI WALLET

eID means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service
[SOURCE: From eIDAS, Article 3(2)]

1. In order to be certified under the present scheme, an ICT service used to provide EUDI wallets shall be in conformity with Article 5c(4) and 5c(5) of eIDAS, and shall in particular satisfy the requirements of an eID means for an eID scheme at assurance level 'high'.

critical assets assets within or in relation to a wallet unit of such extraordinary importance that where their availability, confidentiality or integrity are compromised, this would have a very serious, debilitating effect on the ability to rely on the wallet unit
[SOURCE: From CIR (EU)2024/2981 (eIDAS 5c IA), 2.11

wallet instance application installed and configured on a wallet user's device or environment, which is part of a wallet unit, and that the wallet user uses to interact with the wallet unit
[SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(5)]

WSCA application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the wallet secure cryptographic device
[SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(4)]

2. Each ICT service related to the provision of EUDI wallets certified under the present scheme shall include at least the following components, which shall be demonstrated in conformity with the listed requirements:

Wallet instance	The application (ICT product) running on the user's device or environment and that the wallet user uses to interact with.	**Reference**: • CIR (EU)2015/1502 (for the eID means) • TO BE DEFINED FOR OTHER FUNCTIONS
WSCA	application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the wallet secure cryptographic device.	**Reference**: • CIR (EU)2015/1502 (for the eID means) • TO BE DEFINED FOR OTHER FUNCTIONS
Loading and update process	The process(es) operated by the ICT service provider for the loading and update of the wallet instance and WSCA.	**Reference**: • TO BE DEFINED
Wallet provisioning and management service	The ICT service operated by the ICT service provider for the provisioning of the EUDI wallet and for its management throughout its lifecycle.	**Reference**: • TO BE DEFINED

NOTE*: The definition of the wallet instance is slightly different than the one from the CIR, since in some cases (Web application), the wallet instance may not be installed on the wallet user's device.*

3. Depending on the architecture of the EUDI Wallet solution, an ICT service related to the provision of EUDI wallets certified under the present scheme may include the following components, which shall be demonstrated to be in conformity with the listed requirements:

WSCD	tamper-resistant device that provides an environment that is linked to and used by the wallet secure cryptographic application to protect critical assets and provide cryptographic functions for the secure execution of critical operations.	**Reference**: • CIR (EU)2015/1502 (for the eID means) • TO BE DEFINED FOR OTHER FUNCTIONS
Wallet instance service	ICT service provisioned by the wallet provider to support the execution of the wallet instance.	**Reference**: • CIR (EU)2015/1502 (for the eID means) • TO BE DEFINED FOR OTHER FUNCTIONS

4. When a WSCA from the ICT service relies on a WSCD that is not included as a component of the ICT service, the ICT service provider shall define assumptions as defined above about that WSCD that are sufficient for the WSCA to meet all applicable requirements, and the validity of the assumption shall be demonstrated.

NOTE*: This paragraph is intended to indicate that the scheme does not define any direct requirements on the WSCD, but only constrains the WSCD through the needs of the WSCA.*

14.3 SERVICES RELATED TO THE PROVISION OF AN EID SCHEME

NOTE*: The requirements are defined to support the certification of any eID scheme, but the certificate can only be used for the notification of an "EUDI wallet and the eID scheme under which it is provided" when the eID means used to certify the eID scheme is a certified EUDI wallet.*

eID scheme a system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons [SOURCE: From eIDAS, Article 3(4)]

1. In order to be certified under the present scheme, an ICT service used to provide an eID scheme shall satisfy the requirements for an eID scheme at assurance level 'high'.

2. Each ICT service used to provide an eID scheme that is certified under the present scheme shall include at least the following components, which shall be demonstrated to be in conformity with the listed requirements:

eID means	A material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service, which may be a wallet solution	**Reference**: • CIR (EU)2015/1502 (for the eID means) • MORE?
User on-boarding and management	The process(es) operated by the ICT service provider for the on-boarding of the users and for the management.	**Reference**: • CIR (EU)2015/1502 (for the eID means) • TO BE DEFINED
eID provisioning and management service	The ICT service operated by the ICT service provider for the provisioning of person identification data and for its management throughout its lifecycle.	**Reference**: • CIR (EU)2015/1502 (for the eID means) • TO BE DEFINED

***NOTE**: the user on-boarding and management processes are about the management of the information that is held about users independently of the wallet in an IT system, whereas the eID provisioning and management service is about the data that is managed within the wallet.*

14.4 SERVICES RELATED TO THE VALIDATION OF WALLETS AND RELYING PARTIES

1. In order to be certified under the present scheme, an ICT service used to verify the authenticity and validity of EUDI wallets and of the identity of relying parties shall be in conformity with Article 5c(8) of eIDAS.

2. Each ICT service used to validate EUDI Wallets and relying parties that is certified under the present scheme shall include at least the following component, which shall be demonstrated to be in conformity with the listed requirements:

ICT System	An ICT system used to provide an ICT service to verify the authenticity and validity of EUDI wallets and of the identity of relying parties	**Reference**: • TO BE DEFINED

***NOTE**: One (simple) way to demonstrate that this ICT system complies to the scheme's security requirements would be to demonstrate that it is covered by the ISMS component.*

14.5 WALLET PROFILES

***NOTE**: No profile has been defined so far, since this document is directly inspired from a similar document developed for the European scheme, where there is no mention of such profiles.*

DISCUSSION

Article 3(4) of CIR (EU) 2024/2981 requires the definition of profiles, based on the targeted architectures. The objective of this requirement is to allow national schemes to be specialized for a given architecture, and therefore to simplify the conformity assessment by avoiding the definition of generic certification activities that can fit any possible architecture.

The article does not include a strict definition of architecture and profile. So, the level of detail provided will depend greatly of the situation in a given Member State:

- If a Member State has already decided on a solution, the architecture can be very close to the selected solution, in order to only include the relevant requirements and evaluation activities. However, it is important to leave enough flexibility in the scheme to support the evolution of the solution and of its components, and of the underlying standards, technical specifications.
- If a Member State has decided to procure a wallet without mandating the use of a given architecture, they may propose a single architecture that would cover their procurement requirements, in particular those that limit the architectural choices of the respondents.
- If a Member State has already decided on a solution but remains open for the emergence of other wallets in the future, then it is recommended to combine both approaches, by defining a profile that will closely guide the evaluation of the known solution, and to complement it with an "open" profile that will not restrict the addition of wallets in the future.

15. ANNEX II: ASSURANCE CONTINUITY AND CERTIFICATION LIFECYCLE

WHAT? This annex is intended to define the measures to put in place in order to guarantee that certified services remain in conformity with the scheme requirements after the issuance of the certificate.

HOW? The annex should define a lifecycle for certificates, including the definition of activities to be performed by the certificate holder and by the CB throughout the lifecycle of the certificate.

15.1 SURVEILLANCE EVALUATIONS

The objective of surveillance evaluations is to ensure the ongoing validity of the demonstration of fulfilment of the scheme requirements, which shall cover three aspects:

a) operation of the certified service over a period of time;
b) changes in the certified service over a period of time;
c) changes in the threat environment over a period of time.

The present scheme uses four different types of evaluations for the maintenance of the certificate: core surveillance evaluation, extended surveillance evaluation, recertification evaluation and special evaluation.

15.1.1 Core surveillance evaluation

The purpose of the core surveillance evaluation is to confirm the continued conformity and effectiveness of the certified service over a period of time.

The evaluation team shall:

a) perform an analysis of the changes since the last evaluation in the service including
   - assessment of the suitability of the design of the modified controls;
   - verification of the existence and implementation of modified controls;

b) select a subset of requirements, considering:
   - requirements where observations or non-conformities were identified in previous evaluations;
   - potential new threats or guidance identified by the certification body or provided by the ECCG;

c) evaluate the suitability of the design of the controls associated to the previously selected requirements;

d) evaluate the operating effectiveness of a subset of the controls to be determined at each evaluation since the last evaluation.

***NOTE**: In the case of composition, changes may have occurred in components that are certified in other schemes and have undergone surveillance activities on their own. In such a case, the evaluation team should ensure that the component continues to meet the requirements of the* *scheme, and that any updates in the user guidance have been considered in the implementation of the service.*

15.1.2 Extended surveillance evaluation

The purpose of the extended surveillance evaluation is to add to the core surveillance evaluation a vulnerability assessment as required by the eIDAS regulation every two years.

In addition to the tasks required for a surveillance evaluation, the evaluation team shall:

a) identify the vulnerabilities that have been published since the last vulnerability assessment was performed and that could impact the service;
b) analyse how these vulnerabilities have been handled by the service provider, and how they may have affected the service;
c) where needed, perform further evaluation activities to ensure that the vulnerabilities have been properly mitigated, for instance by performing penetration testing on select components of the service.

15.1.3 Recertification evaluation

The purpose of the recertification evaluation is to confirm the continued conformity and effectiveness of the service as a whole, and its continued relevance and applicability for the scope of certification. A recertification evaluation shall be planned and conducted to evaluate the continued fulfilment of all of the evaluation criteria. This shall be planned and conducted in due time to enable for timely renewal before the certificate expiry date.

The recertification activity shall include the review of previous surveillance evaluation reports and consider the performance of the client's service over the most recent certification cycle.

***NOTE**: This is straight from CEN TS 18072, but it may need further details.*

15.1.4 Special evaluation

If a special evaluation is necessary then the certification body shall determine any evaluation activities necessary to decide about the potential termination, reduction, suspension or withdrawal of the certification.

A special evaluation shall be performed when a certificate has been suspended, before the suspension is lifted and the certificate is fully restored.

***NOTE** The objective of a special evaluation is to perform an evaluation focused on the measures taken by the client to fulfil the requirements for which nonconformities have been detected or on the changes made by the client to their service or to their control framework.*

The evaluation team shall

a) perform an analysis of the changes and nonconformities identified since the last evaluation of the client's service including:
   - assessment of the suitability of the design of the affected controls;
   - verification of the existence and implementation of affected controls.
b) evaluate the operating effectiveness of affected controls over the period since the previous evaluation.

15.2 SURVEILLANCE SCHEDULE

Surveillance activities shall be performed at least once a year, with the following rules:

a) At least a core surveillance evaluation shall be performed every year;
b) An extended surveillance evaluation or recertification evaluation shall be performed every two years;
c) A recertification evaluation shall be performed the months before the certificate is set to expire, in due time for timely renewal before the certificate expiry date;
d) A special evaluation shall be performed when decided by the certification body, following material changes or a material nonconformity.

***NOTE**: With these rules, and since the reference duration of the certificates is four years, the reference schedule is as follows:*

- Year 1: Surveillance evaluation
- Year 2: Extended surveillance evaluation
- Year 3: Surveillance evaluation
- Year 4: Recertification evaluation

In addition, after each evaluation, a review and certification decision shall take place, with the following possible outcomes:

a) continuation of the certificate, without any change;
b) suspension of the certificate, with guidance for users and requirements for the client to fix the identified nonconformities in the defined timeline;
c) cancelation of the certificate in case of nonconformities that cannot be addressed;
d) addition of an amendment to the certificate with a new description and guidance but the same end date.

In the case of a recertification evaluation, the following outcome is also possible:

e) addition of an amendment to the certificate with a new description and guidance, and with an updated end date, which shall not be more than four years after the certification decision.

15.3 PARAMETERS FOR MAINTENANCE PROCESSES

The providers of ICT services certified in the present scheme are required to implement processes related to the day-to-day maintenance of their services (see Annex I). One of the key objectives of these processes is to reduce the number of interactions between the ICT service provider and the certification body, by establishing a distinction between material events and other events, and by assigning different ways to process these events:

- A material event (nonconformity, change or vulnerability, see the following subsections for details) shall be notified to the certification body without waiting for the end of the year, and the certification body shall follow up and provide feedback on the handling of the event by the ICT service provider.
- Oher events shall be handled directly through the process defined by the ICT service provider, with an assessment of the effectiveness of this process performed every year by the certification body.

The assessment of the effectiveness of these processes shall include an assessment of the process used to determine the materiality of events. In the case where the certification body identifies a nonconformity in this assignment, the certification body shall take appropriate measures to ensure that the nonconformity is addressed, including where necessary an obligation to notify all events to the certification body over a given period, so the certification body can determine whether the event was assigned to the appropriate category.

The rest of this section provides definitions for the materiality of nonconformities, and of events in the following processes: change management and vulnerability management.

Overall, the definition of material is “capable of influencing the decisions of intended users”. The rationale therefore is that materiality is determined by considering the consequences of an event towards the intended users.

15.3.1 Materiality of nonconformities

A nonconformity is considered material if it makes a measure or control used to meet a requirement ineffective. A nonconformity may be considered as not material if it simply leads to a decreased effectiveness of the measure or control.

In addition, a nonconformity that is not considered material by itself may lead to a material nonconformity if it is repeated too often, actually making a measure or control ineffective.

EXAMPLE

In a control that implements a backup system to guarantee the availability of data:

- the loss of backup data or the inability to restore it is very likely to be considered material;
- a failure to perform the backup of a system once may not be considered material;
- the same failure repeated over several days is very likely to be considered material.

When assessing materiality, more than a parameter is taken into account, such as the amount of data concerned, its sensitivity, and the effectiveness of the provider to identify the issue and mitigate it.

15.3.2 Materiality of changes

Since the materiality of changes needs to be estimated by the certificate holder, a detailed procedure needs to be defined in the change management policy and evaluated by the CAB.

The following principles should be followed:

- A change should be considered material if it may lead to a material nonconformity.
- Functional changes that do impact the security of the ICT service or impact the implementation of its interfaces should be considered material.
- Changes to the architecture underlying the ICT services should be considered material.
- Changes to critical components such as the WSCD or WSCA should be considered material.

***NOTE**: Because the national schemes also include functional testing, it makes it more likely that a change should be considered material. This may need to be discussed further, in order to avoid unnecessary exchanges between the CB and the certificate holder.*

15.3.3 Materiality of the impact of vulnerabilities

Like changes, the materiality of the impact of vulnerabilities needs to be estimated by the certificate holder, a detailed procedure needs to be defined in the vulnerability management policy and evaluated by the CAB.

***NOTE**: We are talking about the impact of vulnerabilities, not of the vulnerabilities themselves. A vulnerability may be critical, but its impact minor if a patch is available to mitigate it and the* *patch is easy to apply and has been applied timely while ensuring that the vulnerability has not been exploited (which actually happens regularly on complex IT systems).*

***CAUTION**: The principles still need to be defined, but they are likely to be different for product component and for process components, because the criteria are different. For instance, a vulnerability in the operation of an ICT process exposed to internet is more likely to be material because of the availability of an interface, and of the potential global impact.*

16. ANNEX III: LIST OF PUBLICLY AVAILABLE INFORMATION

WHAT? This Annex should list all the information that the certificate holders need to make available publicly.

HOW? The list has been built from the CSA requirements and some of the CRA requirements. None of these are of mandatory application for a national scheme, but they are a good basis.

NOTE*: The requirements are inspired from the CRA and from the CSA. Most of them only apply to the EUDI wallet solution (which is centered around the wallet instance, a product with digital elements):*

1. The provider of a certified EUDI wallet shall make the following publicly available:

(a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the EUDI wallet, including:
- (i) any known or foreseeable circumstance, related to the use of the Wallet solution in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;
- (ii) a description of the measures necessary to secure the initial commissioning of the wallet solution (configuration, installation and deployment instructions);
- (iii) a description of the measures necessary to secure the use of the wallet solution throughout its lifetime;
- (iv) a description of the measures necessary to secure the decommissioning of the wallet solution, including information on how user data can be securely removed;
- (v) a description of the way in which the security of data may be impacted by changes in the wallet solution;
- (vi) a description of the procedures to install security updates to the wallet solution;
- (vii) a description of the procedure to disable automatic security updates to the wallet solution;

(b) the intended purpose of the wallet instance, as well as the EUDI Wallet's essential functionalities, including:
- (i) the security environment provided by the manufacturer;
- (ii) all the Wallet solution's essential functionalities, with an identification of the functionalities not used in the context of EUDI Wallet, and information about the security properties;
- (iii) The identification of all components of the certified Wallet solution (software and hardware products, services, processes). For each component:
  - (1) The name and nature of the component;
  - (2) The provider of the component;
  - (3) For products component, it must include the versions of software affecting compliance with essential cybersecurity requirements, and the versions of hardware with photographs or illustrations showing external features, marketing and internal layout;

(iv) any limitations on the use of a wallet solution for every certified EUDI Wallet.

(c) One or several product security information documents including at minima:

(i) the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website at which the manufacturer can be contacted;

(ii) If the manufacturer decides to make available the software bill of materials to the user, information on where the software bill of materials can be accessed;

(iii) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;

(iv) a reference to online repositories listing publicly disclosed vulnerabilities related to the Wallet solution and to any relevant cybersecurity advisories;

(v) the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;

(d) the source code of the application components of the EUDI Wallet that run on the user's device, as part of an open source program:

2. The information referred to in paragraph 1 shall be made available in a clear, comprehensive and easily accessible manner, in a publicly accessible space, to any person seeking to use a wallet solution.

NOTE*: The list is still being consolidated in the context of TG4*

Discussion

Some of the information that is required to be made public includes detailed user guidance. There may be an ongoing debate about the definition of a user. End user documentation should definitely be publicly available, but EUCC considers that the documentation to be used by a customer who is not the end user (*e.g.*, the government entity deploying an eID into the wallet) should not be shared as it contains sensitive information.

These discussions are ongoing, as the eIDAS regulation also includes a requirement to make the Wallet's application code available as open source, which would mean that this documentation would be available too. This is why the proposal is to make public all documentation, and to make the source available.

Compliance to CIR (EU) 2024/2981

The articles cover all the elements mandated in the CIR's Annex V.

17. ANNEX IV: LIST OF INFORMATION REQUIRED UPON APPLICATION FOR CERTIFICATION

WHAT? This Annex should list all the information that the certificate holders need to make available at the beginning of the certification process.

HOW? This list is mostly derived from the activities to be performed by the CAB, and the input required by the CAB to perform them.

1. The provider of an EUDI wallet shall make the following information available to the CAB when initiating the evaluation of an EUDI Wallet[17]:

(a) all elements described in Annex III as elements to be provided publicly at the end of the certification process;

(b) an architecture description of the wallet, including:

(1) a description of the solution, indicating the role of every component;

(2) a description of the interfaces, including the external interfaces and the internal interfaces between components;

(3) a description of the assumptions (for example on components provided by the end user);

(c) a certification plan, including:

(1) a list of the components certified or planned to be certified with certificates or potential dates when the components will be certified

(2) security targets (certified/draft) or equivalent documents describing the scope of certification for each component;

(3) associated guidance or any kind of integration document (certified/draft). Any certification should be performed taking into account some integration requirements. These requirements must be provided to the evaluator to check that the integration has been correctly performed.

(d) a risk assessment[18] describing the cybersecurity risks against the wallet solution is designed, developed, produced, delivered and maintained, as defined in Annex XI. It must include a mapping between this risk assessment and the risk register as provided in Commission Implementing Regulation (EU) 2024/2981.

Discussion

The list is quite minimal, only including elements that are clearly known to be mandatory. It may be expanded in the future.

[17] This list is strongly inspired from the list of documentation required in Article 8(5) of regulation (EU)2024/2981.

[18] This risk assessment is required in Article 4($)(d) of (EU)2024/2981, and their transmission to the CAB by Article 4(5) of the same regulation.

For instance, elements required to the lifecycle of the wallet may be required. One example would be an “exit plan”, which could be activated if a technical issue impacts the wallet solution, and its certification has to be withdrawn or limited (*e.g.*, by not allowing its deployments on devices that have been found vulnerable to an attack). In such cases, this plan would minimise the impact to citizens.

18. ANNEX V: CONTENT OF A CERTIFICATE

WHAT? This Annex should list the required content of certificates.

HOW? The content of the certificate was built from the lists in the EUCC IA and in the 5c IA.

1. An EUDIW certificate shall at least contain:

(a) a unique identifier allocated by the certification body issuing the certificate of conformity;
(b) information related to the certified wallet solution and the electronic identification schemes under which they are provided, and about the holder of the certificate of conformity, including the following:
(1) name of the ICT service;
(2) type of the ICT service (*e.g.*, EUDI Wallet, eID scheme or verification service);
(3) version of the ICT service that was evaluated;
(4) name, address and contact information of the holder of the certificate of conformity;
(5) link to the website of the holder of the certificate of conformity containing the information that is required to be made publicly available, as defined in Annex III.
(c) Information related to the evaluation and certification of the ICT service, including the following:
(1) name, address and contact information of the certification body that issued the certificate of conformity;
(2) where applicable, name of the subcontractors that contributed to the evaluation;
(3) name of the [scheme owner];
(4) references to regulation (EU) No 910/2014 and to the present scheme;
(5) a reference to the certification report associated with the certificate of conformity;
(6) a reference to the certification assessment report associated with the certificate of conformity;
(7) a reference to the standards used for the evaluation, including their versions;
(8) the date of issuance of the certificate of conformity;
(9) the period of validity of the certificate of conformity.

2. The information shall be provided in an official language of the EU, and an English translation shall be available within the certificate.

***NOTE**: Typically, the front page would be provided in national language, with an English translation made available in the subsequent pages (e.g., for a one sheet certificate, the national information would be in the front and the English translation in the back).*

DISCUSSION

The content of a certificate is quite standardised. There is here no reference to the accreditation of the CB, but this is another information that is commonly present in certificates (accreditation number and validity date).

COMPLIANCE TO CIR (EU) 2024/2981

The list is very close to the list in Annex VII of the CIR, and it includes all required elements.

19. ANNEX VI: CONTENT OF A CERTIFICATION REPORT

WHAT? This Annex should list the required content of a certification report (to be made publicly available together with the certificate).

HOW? This Annex should start from the lists in the EUCC IA and in the 5c IA.

NOTE: This content is structured from the 5c IA's Annex VIII and strongly inspired from the 5c the EUCC IA's Annex V and from the EUCS draft candidate scheme.

19.1 CERTIFICATION REPORT

1. On the basis of the evaluation technical reports resulting from the evaluation, the certification body establishes a certification report to be published together with the corresponding EUDIW certificate.

2. The certification report is the source of detailed and practical information about the ICT service and about the ICT service's secure deployment and shall therefore include all publicly available and sharable information of relevance to users and interested parties. Publicly available and sharable information can be referenced by the certification report.

3. The certification report shall at least contain the following sections:

(a) executive summary;
(b) identification of the ICT service;
(c) description of the ICT service;
(d) the security information to be made publicly available, as listed in Annex III;
(e) a summary of the preliminary audit and evaluation plan, including a summary of the results of the evaluation;
(f) summary of the review and certification decision;
(g) when available, the mark or label associated to the scheme;
(h) bibliography.

4. The executive summary shall be a brief summary of the entire certification report. The executive summary shall provide a clear and concise overview of the evaluation results and shall include the following information:

(a) name of the certified ICT service, enumeration of the service's components that are part of the evaluation and the ICT service version;
(b) the name of the certification body issuing the certificate and, where applicable, the list of subcontractors who contributed to the evaluation;
(c) completion date of evaluation;
(d) reference to the evaluation technical report established by the evaluation team;
(e) brief description of the certification report results, including:
(1) the name and version of all components evaluated in the context of the certification;

(2) the name and version of all components that have been evaluated prior to the certification, together with a reference to their certificate or other relevant assurance information;
(3) assumptions about the operating environments;
(4) special configuration requirements;
(5) disclaimer(s).

NOTE*: All the information in the executive summary is duplicated, as it appears later in the document in a more detailed version. This is voluntary, as the idea is to allow a reader to get a first impression of the content by simply reading the executive summary..*

5. The evaluated ICT service shall be clearly identified, including the following information:

(a) the name and version number of the evaluated ICT service;
(b) the type of ICT service (EUDI wallet, eID scheme, or validation service);
(c) an enumeration of the ICT service's components that are part of the evaluation, including their version number at the time of the evaluation;
(d) an enumeration of the ICT service's components that are have been evaluated prior to the evaluation, including their version number at the time of the evaluation, a reference to the certificate or assurance information provided, and the date of issuance of that information;
(e) name and contact information of the holder of the EUDIW certificate;
(f) link to the website of the holder of the EUDIW certificate where publicly available information is provided, including the supplementary cybersecurity information for the certified ICT service in accordance with Article 55 of Regulation (EU) 2019/881.

6. The information included in the section defined in paragraph 5 shall be as accurate as possible in order to ensure a complete and accurate representation of the ICT service that can be re-used in future evaluations.

7. The description of the ICT service shall include:

(a) a description of the ICT service's architecture and components, including required hardware, software and ICT subservices;
(b) a description of the ICT service's security policies that are relevant for the ICT service's users, which may refer to the description of the information security management system component and of other components that define such security policies and processes;
(c) a description of the ICT service's control framework, including a mapping between the controls, the components in which they are implemented and the risks identified on the ICT service;
(d) the list of additional assumptions and requirements to the operating environments of the certified ICT service for the compliant provision of the ICT service;

8. A complete listing of the information to be made publicly available, as listed in Annex III shall be provided. All relevant documentation shall be denoted by the version numbers.

9. The summary of the evaluation shall include:

(a) a description of the initial audit and its results;
(b) a description of the resulting evaluation plan, including a list of the evaluation activities;
(c) the results of the evaluation activities;

(d) in the case of a maintenance evaluation, a summary of the nonconformities encountered since the previous evaluation.

10. The summary of the review and certification decision shall include the following information:

(a) confirmation of the attained assurance level, including when available a reference to the levels defined in Article 52 in Regulation (EU) 2019/881 or in Article 8 of Regulation (EU) No 910/2014;
(b) detailed description of the assurance requirements, as well as the details of how the ICT service meets each of them;
(c) date of issuance and period of validity of the certificate;
(d) unique identifier of the certificate.

***NOTE**: Point (c) most likely needs to be revised, but we kept it as a reference that the review is expected to ensure that the scheme requirements regarding evaluation have been met.*

17. The bibliography section shall include references to all documents used in the compilation of the certification report. That information shall include the following:

(a) the security evaluation criteria, state-of-the-art documents and further relevant specifications used and their version;
(b) the evaluation technical report;
(c) the evaluation technical reports for composite evaluation, where applicable;
(d) technical reference documentation;
(e) developer documentation used in the evaluation effort.

18. In order to guarantee the reproducibility of the evaluation, all documentation referred to has to be uniquely identified with the proper release date, and proper version number.

Discussion

This certification report is already quite extensive, in particular regarding the information made available about the ICT service being certified. There have not been extensive discussions about this Annex in the EUDIW AHWG yet, but no specific comments have been raised about it either.

Coverage of the CIR (EU) 2024/2981 requirements

The Annex above covers all the requirements for certification reports from Annex VIII of the CIR, and actually describes the same items in greater details.

20. ANNEX VII: CONTENT OF A CERTIFICATION ASSESSMENT REPORT

WHAT? This Annex should list the required content of a certification assessment report (a specific report to be made available only to the EDICG).

HOW? This Annex starts from the lists in Annex VIII of the 5c IA.

1. The certification assessment report shall at least contain:

(a) a description of the ICT service's design, including all product and process components, together with the risk assessment and the specific validation plan;
(b) a description of how the ICT service meets the requirements of assurance level high as defined in Article 8 of Regulation (EU) No 910/2014 and of how this is demonstrated by the results of the certification assessment of the ICT service conducted in accordance with this scheme;
(c) a description of the result of assessment of the conformity of the ICT service with, in particular the conformity with the following:
— the requirements set out in Article 5a(4), (5), and (8) of Regulation (EU) No 910/2014;
— the requirement for logical separation set out in Article 5a(14) of Regulation (EU) No 910/2014;
— where applicable, the standards and technical specifications referred to in Article 5a(24) of Regulation (EU) No 910/2014, while describing how these requirements relate to the corresponding normative requirements specified by this scheme;
(d) a summary of the result of the performance of the validation plan, including all identified nonconformities.

NOTE*: The certification assessment report should be based on the certification report, with additional information about the evaluation activities, about the ICT service's risk assessment and about mapping between the controls in the ICT service and the risks identified in the risk assessment.*

2. The description of the ICT service's design should include the elements from the description provided in the Certification Report, augmented with information related to the risk assessment for each component, and with the specific evaluation plan that is being proposed for each component and for the overall object of certification.

3. The justification that the wallet solution meets the requirement of assurance level 'high' shall be based on the evidence available from the evaluation activities performed in this scheme, including the analysis of the assurance information made available from other schemes. A link also needs to be established with the risk register defined in Annex I of Regulation (EU) 2024/2981.

4. The description of the assessment results shall establish that the ICT service complies with the relevant requirements from Regulation (EU) No 910/2014, so where standards and technical specifications are used that include a mapping to these requirements, a demonstration that the requirements from these standards and technical specifications are met shall be deemed sufficient.

5. The summary of the performance of the validation plan shall include a description of every conformity assessment activity performed, as well as a summary of its results, including a description of the nonconformities identified during the evaluation, as well as a description of the mitigation actions that have been implemented, and of the conformity assessment actions to be performed in subsequent conformity assessments.

Discussion

This is only a stub, which will need to be extended. Paragraph 1 is very strongly inspired from paragraph 2 of Annex VIII of CIR (EU) 2024/2981, and the subsequent paragraphs provide additional information about the content of the section, which will most likely be extended in the future.

Coverage of the CIR (EU) 2024/2981 requirements

The Annex above covers all the requirements for certification reports from paragraph 2 of Annex VIII of the CIR, and actually describes the same items in greater details.

21. ANNEX VIII: SCOPE AND TEAM COMPOSITION FOR PEER ASSESSMENT

WHAT?	**This Annex should complement the articles on peer assessment by more detailed requirements.**
HOW?	**This Annex should start from the corresponding Annex in the EUCC IA, changing it only as required.**
AND?	**This work should also analyse how much of the peer assessment requirements should be considered as a part of the certification framework, to be shared by all schemes.**

***NOTE**: Work in progress*

22. ANNEX IX: CRITERIA TO ASSESS THE ACCEPTABILITY OF ASSURANCE INFORMATION

WHAT? This Annex should define the specific criteria to assess the acceptability of different kinds of assurance information.

HOW? There will be two parts in the content, the first part should be inspired from the corresponding Annex VI in the 5c IA to define a generic method, and the second part by the content developed in TG3 for specific schemes.

***NOTE**: Sections 1 and 2 are copied from Regulation (EU) 2024/2981*

1. Assessing the availability of assurance documentation

Evaluators shall list the assurance documentation available for every relevant component of the wallet solution and the electronic identification scheme under which they are provided. Then, evaluators shall assess the overall relevance of each piece of assurance documentation for the dependency review.

The following aspects shall be considered in the analysis:

(1) about the assurance documentation itself:
(a) the type of assurance documentation, with all required details,
(examples of such documents are certificates of conformity according to EN ISO/IEC 27001:2022 or Type 1 or Type 2 for ISAE reports);
(b) the period covered or period of validity,
(this period may be supplemented with a bridge letter (a document to cover a period of time between the end date of the reporting period of the current ISAE report and the release of a new ISAE report) or similar a statement);
(c) the applicable framework (e.g. existing standard);
(d) whether the assurance documentation includes a mapping to the scheme's requirements;
(2) about the assurance report issuer's professional competence and impartiality:
(a) name of the certification body and, if available, name of the lead evaluator;
(b) evidence of the certification body's and the evaluator's competence (e.g. accreditation, personal certification, etc.);
(c) evidence of the certification body's and the evaluator's impartiality (e.g. accreditation, etc.).

2. Assessing assurance related to individual requirements

Evaluators shall verify that the assurance documentation available for the wallet solution and the electronic identification scheme under which they are provided is adequate to determine that the wallet solution meets the expectations relative to the certification scheme's individual requirements.

This assessment shall be performed for every relevant component of the wallet solution and the electronic identification scheme under which they are provided, by formulating an assumption on the wallet solution's security controls.

For each such assumption, the evaluation team shall determine whether or not the assurance provided in the available assurance documentation is adequate.

The determination that the assurance is adequate shall be based on the following:

(1) the required information is available, with the expected assurance level, in the assurance documentation;
(2) the information available in the assurance documentation does not cover the full scope of the requirement, but additional controls or compensating controls (i.e., internal controls that reduce the risk of existing or potential control weakness) implemented in the wallet solution or in the electronic identification scheme under which they are provided allow the evaluators to determine that the information is adequate;
(3) the information available in the assurance documentation does not offer the expected assurance level but the controls implemented to assess and monitor the wallet provider allow the evaluators to determine that the information is adequate;
(4) if the assurance documentation mentions nonconformities on the design or implementation of the controls used to meet an assumption, the remedial actions proposed and implemented by the wallet provider and reviewed by its evaluators shall be adequate to guarantee that the assumption is indeed met.

3. Certified components

When a component has been certified in a component certification scheme recognized by the present scheme, the processes defined above shall be simplified by defining specific criteria:

(1) the CAB's competence and impartiality do not need to be assessed if the component certification scheme mandates accreditation;
(2) the report can be considered as being fully compliant with the rules of the component certification scheme for the assurance level of the report, as defined in the component certification scheme;
(3) the mapping of the component certification scheme's security requirements to the present certification scheme's security requirements may be performed once and reused for all certificates.

If the certification scheme includes specific requirements for composition, and if the service and its subservice both satisfy these requirements, the assessment may be simplified further.

NOTE*: This last paragraph will need to be updated if we define a specific set of requirements for composition, or removed if we don't.*

3.1 EUCC

NOTE*: The present section is provided as example only, as its content still needs to be discussed by the EUDIW AHWG, specifically its TG3.*

When a product component has been certified with EUCC (the European cybersecurity certification scheme established by Regulation (EU) 2024/482, the consequences are as follows:

(1) The CAB's competence and impartiality do not need to be assessed, since EUCC requires accreditation for all CABs, and authorization for the CABs who perform conformity assessment activities at assurance level 'high' from Regulation (EU) 2019/881.
(2) The EUCC report can be considered as sufficient, and the AVA_VAN level of vulnerability assessment used can provide additional indication to determine to which degree the EUCC-certified component meets the requirements of the assurance levels from Regulation (EU) No 910/2014.
(3) When the EUCC certificate relies on one of the Protection Profiles listed in Annex X, then no specific mapping needs to be performed to the present scheme's security requirements, since the mapping will be available for the Protection Profile.
(4) When the EUCC certificate does not rely on a Protection Profile listed in Annex X, then a specific mapping needs to be established between the SFRs listed in the EUCC Security Target and the present scheme's security requirements.

In addition, for every component certified with EUCC, the following activity shall be performed by the ICT service provider and by the certification body:

(1) The ICT service provider shall provide a justification that their ICT service follows the guidance provided with the EUCC-certified component (Operational user guide and Preparative procedures).
(2) The certification body shall verify the justification provided by the ICT service provider.
(3) The certification body shall verify the content of the ETR of the EUCC-certified product to ensure that no issue has been identified during the evaluation that may be problematic when the component is used to support the operation of the ICT service.

Discussion

This Annex is strongly inspired from Annex B in CEN TS 18072, which defines a dependency analysis conformity assessment activity for the certification of cloud services. This Technical Specification may be updated later this year to support all kinds of services.

The objective is here to explain for each "recognized" scheme or evaluation methodology how we may simplify the general methodology. This is still under development in TG3, but we have here provided an example for EUCC, which is one of the cases where the dependency analysis will be most simplified.

Coverage of the CIR (EU) 2024/2981 requirements

Since we copy-pasted the content of Annex VI from the CIR, this is very much compliant. The main interest of this Annex will be the development of the simplified procedures for various schemes.

23. ANNEX X: SECURITY REQUIREMENTS FOR EUDI WALLETS AND THE EID SCHEMES UNDER WHICH THEY ARE PROVIDED

WHAT? **This SOTA document should define the requirements that apply to all the services that can be certified in the context of this scheme.**

HOW? **Most of the requirements should be defined in standards (to be listed and referenced), and some additional requirements may be defined in the document itself.**

NOTE: **This SOTA document may need to be defined in an Annex of the scheme, although it may need to be updated regularly.**

NOTE*: Content currently under definition in TG1*

24. ANNEX XI: METHODS AND PROCEDURES FOR EVALUATION ACTIVITIES

WHAT? This Annex defines the specific methods and procedures to be used in the evaluation activities.

HOW? This Annex starts by grouping the required methods and later move on to defining them with the required details.

NOTE: This Annex, or some of its content, may need to be eventually integrated in a formal standard or technical specification.

***NOTE**: Content currently under definition in TG4. This Annex only contains one activity, as an example, and for further discussions.*

***NOTE**: We are considering to refer to the CEN TS 18072 technical specification, once it will be revised to remove the explicit reference to cloud services. Doing so would allow us to start from a framework in which we could add the activities defined below.*

24.1 INTRODUCTION

This annex is not intended to be exhaustive, and certification will use many activities that are not defined here. However, the methods described in this Annex are either specific to the scheme or have a specific definition in the context of the scheme.

24.2 OVERALL EVALUATION ACTIVITIES

These evaluation activities are global for a certificate, aiming at considering all the components together and demonstrating that they meet the requirements for certification.

24.2.1 Risk assessment

***NOTE**: The presentation is loosely inspired from the definition of the assurance components in the Common Criteria standard.*

24.2.1.1 Developer actions

The developer shall perform a risk assessment of the proposed ICT service, including the following steps:

(1) Relevance check
- (a) Review each risk scenario from the risk register and evaluate its applicability for the ICT service architecture and components.
- (b) If a risk scenario is not applicable, provide a rationale to explain why (e.g., this risk scenario is applicable only if the WSCD is remote).
- (c) If a risk scenario is applicable but can be difficult to interpret depending on the architecture, propose a new formulation for this risk and explain how it could apply.

(2) Completeness check
- (a) Regarding this specific ICT service, check that all the risks are covered, especially the risks related to the specific interfaces, assumptions, and security mechanisms.

(b) Complete by adding risks specific to the ICT service architecture if necessary.

(3) Risk evaluation

(a) For each risk, evaluate the impact and the likelihood.

(b) Determine the risk level according to Impact and Likelihood.

(4) Security controls

(a) For each risk, identify the controls in place for the ICT service. These controls can be implemented by a component or a set of components of the ICT service.

(b) For each control, explain how the control effectiveness is checked (component certified, service/process audited, etc.).

(c) Determine the residual risks and how they are monitored.

24.2.1.2 Developer deliverables

The risk assessment deliverable shall include at least the following elements:

(1) List of relevant risks and risk scenarios, including relevance justification for all risks and risk scenarios from the risk register and for the risks specific to the ICT service

(2) Evaluation of the impact and likelihood for each relevant risk

(3) A list of the controls, including assurance information available to control the sufficiency and effectiveness of each control (or a reference to the same list in the ICT service description)

(4) A mapping of controls to risks, with a justification of the coverage, identification of residual risks

24.2.1.3 Evaluator actions

The evaluator shall perform the following actions:

1. Check the coverage of the risk register

For each risk scenario of the risk register, check that:

   a. It has a direct equivalent.
   b. Or it is not applicable, and the rationale is consistent with the ICT service architecture.
   c. Or it is replaced by a more specific risk and the rationale is consistent with the ICT service.

2. Check the completeness of the risk assessment
   a. Check if risks have been added from the risk register. If yes, these risks may be applicable to other solutions and should be communicated to the organisation in charge of the risk register maintenance.
   b. Check if the risks covered correctly the interfaces of the ICT service.
   c. Check if the risks are consistent with the assumptions.
   d. Check if the risks are complete regarding the ICT service.
3. Assess the quality of the risk level evaluation
   a. Check the evaluation of the risk level of each risk.
4. Security controls
   a. Check that each risk is suitably covered by controls.
   b. Check the relevance, *i.e.* the necessity, and the completeness, *i.e.* the sufficiency of the controls for the risk.
   c. Check the effectiveness of the control. If the control is covered by assurance information, assess how the effectiveness of the control is covered. If the control is not covered or partially covered by assurance information, identify it in a list of controls to check during the evaluation.
   d. Check the list of residual risks to verify that it corresponds to the risk assessment and that the monitoring process is relevant and in place.

24.2.2 Vulnerability assessment

24.3 COMPONENT EVALUATION ACTIVITIES

These evaluation activities are specific to a given component of the object of certification.

24.3.1 WSCA evaluation

24.3.2 Wallet instance evaluation

24.3.3 IT system evaluation

24.3.4 Process evaluation

24.4 SURVEILLANCE EVALUATION ACTIVITIES

These activities are specific to surveillance evaluations and to the maintenance of assurance throughout the certification lifecycle.

24.4.1 Service change impact assessment

24.4.2 Threat environment change impact assessment

24.4.3 Process effectiveness assessment

25. COMPOSITION IN EUDIW

WHAT? This SOTA document is supposed to provide guidelines on the composition in the EUDIW schemes, which is going to be very limited (only about composition between an EUDI Wallet (used as eID means) and an eID scheme).

HOW? The corresponding SOTA for EUCC can be used as a basis, although significant changes will be required, because of the much more specific use of composition.

***NOTE**: No work has been performed on this topic at the time.*

26. ACCREDITATION OF CABS FOR EUDIW

WHAT? This document (status to be confirmed) will define the requirements for the accreditation of CABs in the context of the national scheme.

HOW? The document has drawn inspiration from the proposed SOTA for the accreditation of CABs for EUCC, which is itself strongly inspired from the same SOTA for EUCC, by mixing some content about CBs and ITSEFs. The CEN TS 18072 Annex on competences is also a source.

***CAUTION**: This first version has not been updated, because there have been only limited exchanges about the proposed EUDIW version, which is included here **for reference only**. This document will need to be updated for national schemes, also because there may be an interest to harmonize the requirements.*

***NOTE**: This first version is based on a "copy-paste" version of the corresponding SOTA for EUCC, so the color code is 'black' for content that comes from the EUCC SOTA on accreditation of CBs, 'purple' for the content that comes from the EUCC SOTA on accreditation of of ITSEFs, 'blue' for changes, and 'red' for points that still need to be revised.*

26.1 INTRODUCTION

This draft state-of-the-art document as defined under Article XX point YY of EUDIW IA is a legal supporting document under Implementing Regulation EUDIW IA on establishing the European Digital Identity Wallet cybersecurity certification scheme (EUDIW). It provides an overview of the requirements for the accreditation of Certification Bodies (CBs). As mentioned in the Annex to the EU Cybersecurity Act, the conformity assessments performed in the context of the EUDIW must follow the requirements of the relevant standard that is harmonized under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing conformity assessment activities for the purpose of cybersecurity certification of ICT services.

This document specifically covers the accreditation of CBs as defined under Article 2 point 12 of the EUDIW. 'Certification body' means a conformity assessment body as defined in Article 2, point (13), of Regulation (EC) No 765/2008, which performs certification activities.

The activities of a CB, including such certification activities, cover:

- the evaluation of the ICT service according to the methods and procedures defined in the EUDIW.
- the review of the evaluation results and the verification of the evaluation technical report[19] in line with Article XX of the EUDIW;
- the issuance, renewal and withdrawal of EUDIW certificates in line with Article XX of EUDIW;
- monitoring activities, as defined in Article XX of the EUDIW;
- conformity and compliance activities, as defined in Article XX of the EUDIW;

[19] As defined under Article XX point YY of EUDIW: 'evaluation technical report' means a document produced by an ITSEF to present the findings, verdicts and justifications obtained during the evaluation of an ICT service in line with the rules and obligations set out in this Regulation.

- vulnerability management and disclosure activities, as defined in Article XX of the EUDIW.

The standard selected for the accreditation of CBs under the EUDIW is EN ISO/IEC 17065:2012 in line with point 19 of the Annex to Regulation (EU) 2019/881. Among the requirements defined for CBs in that standard, many are related to the methodology to be applied by the CB during a conformity assessment.

These methodological elements are broad, and this state-of-the-art document provides the necessary interpretations to the necessary competences to perform conformity assessment activities for the purpose of cybersecurity certification of ICT services related to European digital identity wallets and the electronic identification schemes under which they are provided.

Next to the requirements provided by the standard EN ISO/IEC 17065:2012, the Annex to Regulation (EU) 2019/881 sets out the main requirements for accreditation of conformity assessment bodies in general. Under paragraph 8.1 of this document, a mapping of these annexed requirements and the applicable standard of EN ISO/IEC 17065:2012 is provided.

The formal accreditation statement provided by the National Accreditation Body (NAB) to the CB sets forth that the CB complies with the conformity assessment requirements and that it is technically competent to carry out their related tasks.

This document must be used by NABs to accredit the CBs for EUDIW, with the active support of the National Cybersecurity Certification Authority (NCCA)[20] in their monitoring and supervising role established in the respective Member State.

26.1.1 RESPONSIBILITIES OF THE NATIONAL ACCREDITATION BODY

The NAB that is established in a Member State in line with Regulation (EC) 765/2008, is the body that is responsible to perform the accreditation for a conformity assessment body (Article 60(1) CSA).

Since the CB needs to certify for the assurance level high, the NCCA and the NAB should pay attention to the fact that the CB may want to avoid duplication of effort and to use the work undertaken during the accreditation process as much as possible in the authorisation process. Therefore, the accreditation body should use technical assessors (TAs) and technical experts (TEs) who can also be accepted by the NCCA and should consult with the NCCA if they are interested in including a suitable technical expert to participate in the accreditation process. Tas and TEs used by the NAB must however operate under the sole responsibility of the NAB for their accreditation activities.

In addition, the following tasks need to be performed by the NAB:

- report the results of the accreditation assessment to the NCCA, including assessment reports and decisions on granting, extending, reducing, suspending, or withdrawing of accreditations for EUCC;
- apply an assessment programme to assess that the accredited conformity assessment bodies meet the requirements of accreditation;
- take appropriate measures to reduce the scope, suspend or withdrawn the accreditation of conformity assessment bodies where they are not compliant with the accreditation requirements, including those from the CSA.

[20] NCCAs mentioned in this document are acting on their monitoring and supervising role.

In the case of possible infringements of the CSA, particularly related to the requirements in Annex of the CSA, the collaboration with the NCCA is important since the NCCA has the monitoring and supervising powers under Article 58(8) CSA that can support the NAB in this task.

26.1.2 RESPONSIBILITIES OF THE NATIONAL CYBERSECURITY CERTIFICATION AUTHORITY

Based on the accreditation decision taken by the NAB, the NCCA must notify the European Commission in accordance with Article 61 CSA and relevant implementing regulation[21].

ENISA will make the information regarding the notified conformity assessment bodies available on its dedicated website on European cybersecurity certification schemes referred to in Article 50(1) of Regulation (EU) 2019/881.The monitoring and supervising national cybersecurity certification authorities (NCCAs) have the responsibility to actively assist and support the NAB in their monitoring and supervising tasks and need to share information and report to the NAB. This cannot obstruct the handling of complaints performed by the CB in line with EN ISO/IEC 17065:2012 concerning any:

- (potential) non-compliance of the CB related to the accreditation requirements annexes in Regulation (EU) 2019/881 (Cybersecurity Act- Article 58(7), point (c) and Article 58(7), points (h) and (i) CSA);
- (potential) non-compliance of the CB that is a public body (Article 58(7), point (d) CSA);
- complaints received related to the authorisation of a CB that may have an impact on the accreditation of the CB (for assurance level ‘high’ Article 58(7), point (f) CSA).

The NCCA needs to include the active assistance and support provided to the NAB for the monitoring and supervision of the CABs (CBs and ITSEFs) activities and the monitoring and supervision of the CB that issues certificates of protection profiles, in line with Article XX of EUDIW IA in an annual summary report and send this to the ECCG and ENISA[22].

26.2 NORMATIVE REFERENCES

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council.

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

***NOTE**: This is a placeholder, which needs to be complemented by many more references.*

[21] Implementing Regulation …/…. establishing the circumstances, formats and procedures for notifications pursuant to Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification

[22] See Article 58(7), point (g) CSA.

26.3 ACRONYMS AND DEFINITIONS

26.3.1 Acronyms

CB	Certification Body
CSA	Cybersecurity Act
ENISA	European Union Agency for Cybersecurity
ETR	Evaluation Technical Report
EUDIW	European Digital Identity Wallet cybersecurity certification scheme
ICT	Information and Communications Technology
NAB	National Accreditation Body
NCCA	National Cybersecurity Certification Authority
TA	Technical Assessor
TE	Technical Expert

26.3.2 Definitions

The definitions used under Article 2 of Regulation (EU) 2019/881 (CSA) and under Article XX of the EUDIW IA apply to this document. The following definitions also apply to this document.

Certifier
'Certifier' means CB personnel performing activities such as review or certification decision.

Evaluator
'Evaluator' means CB personnel performing evaluation activities.

26.4 SCOPE AND OBJECTIVE

CBs, including their staff, must be technically competent, impartial and perform their duties in a consistent manner when certifying an ICT service under the EUDIW.

EN ISO/IEC 17065:2012 applies to a very general and wide range of certification activities. This document is intended to be used for the accreditation of CBs for the EUDIW. It includes interpretations of EN ISO/IEC 17065:2012 applicable to the cybersecurity certification of ICT products, and further EUDIW requirements for CBs whose conformity is to be assessed during their accreditation.

26.5 APPLICABILITY OF EUROPEAN AND INTERNATIONAL STANDARDS TO THE ACCREDITATION OF CBS

The Cybersecurity Act requires that schemes refer to international, European or national standards that are to be applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme.

In this respect the following standard must apply to the accreditation of CBs:

- EN ISO/IEC 17065:2012 – Conformity assessment – Requirements for bodies certifying products, processes and services.

***NOTE**: We may add to the list CEN TS 18072 if it is revised in a way that makes it applicable beyond cloud services and if it is deemed suitable for the present scheme.*

QAC-01 Are there other standards that we should mention here, similar to the ISO/IEC 19896 series and ISO/IEC TS 23532 used for evaluation laboratories?

We may actually mention these standards, but they are tied to specific methodologies (ISO/IEC 19790, ISO/IEC 15408), so may not be easy to apply.

26.6 SCOPE OF THE ACCREDITATION OF A CB

The scope of accreditation must at least specify:

- The certification field:
  - ICT Cybersecurity Evaluation
- The certification object:
  - Information and Communication Technology Services, within the following categories:
    - Services providing an EUDI Wallet
    - Services providing an eID scheme
    - Services for the verification of properties of EUDI Wallets and relying parties
- The assurance information types in which the CB has proven technical competence to review the assessments and reports established by other CABs:
  - IT security certification in the EUCC scheme up to EAL 3 augmented with ALC_FLR.2
- The evaluation activities for which the CB has proven technical competence to evaluate ICT services and their components, for example:
  - Evaluation of a WSCA up to assurance level eIDAS-'high'
  - Evaluation of an ISMS up to assurance level eIDAS-'high'
- The reference to the scheme:
  - EUDIW.

Technology and evaluation types from the Annex in which the CB has proven technical competence must be referred to in the accreditation assessment report.

***NOTE**: We here make a difference between the activities for which the CB has the ability to review a assurance information obtained through another scheme, and those for which the CB has the ability to perform the evaluation tasks themselves. Note that the CB may use subcontractors, in which case these subcontractors are include in the scope of accreditation and the activities they perform are considered to be competences of the CB (and fall under the responsibility of the CB).*

26.7 ACCREDITATION REQUIREMENTS

The CB accreditation requirements are as follows:

- those that need to be met by conformity assessment bodies as set out in the Annex to the CSA. These are provided in Section 7.1 'General accreditation requirements from the CSA';
- those applicable to CBs as indicated in the EUDIW, in particular monitoring activities by the certification body (Article XX);
- those for bodies certifying services defined in ISO/IEC 17065:2012;
- those mentioned in Section 7.2 'Specific accreditation requirements' of this document.

26.7.1 General accreditation requirements from the CSA

Conformity assessment bodies that wish to be accredited must meet the requirements set out in the Annex to the CSA (see the table below).

For information purposes, links to related requirements in EN ISO/IEC 17065:2012 that may support compliance of the CSA requirements are set out in the second column of the table below.

Requirements from the CSA Annex	Supporting requirements from EN ISO/IEC17065:2012
1. A conformity assessment body shall be established under national law and shall have legal personality.	4.1.1
2. A conformity assessment body shall be a third-party body that is independent of the organisation or the ICT products, ICT services or ICT processes that it assesses.	4.2
3. A body that belongs to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products, ICT services or ICT processes which it assesses may be considered to be a conformity assessment body, provided that its independence and the absence of any conflict of interest are demonstrated.	4.2
4. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product, ICT service or ICT process which is assessed, or the authorised representative of any of those parties. That prohibition shall not preclude the use of the ICT products assessed that are necessary for the operations of the conformity assessment body or the use of such ICT products for personal purposes.	4.2
5. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, manufacture or construction, the marketing, installation, use or maintenance of the ICT products, ICT services or ICT processes which are assessed, or represent parties engaged in those activities. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to their conformity assessment activities. That prohibition shall apply, in particular, to consultancy services.	4.2
6. If a conformity assessment body is owned or operated by a public entity or institution, the independence and absence of any conflict of interest shall be ensured between the national cybersecurity certification authority and the conformity assessment body, and shall be documented.	4.2
7. Conformity assessment bodies shall ensure that the activities of their subsidiaries and subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.	4.2.3; 4.2.6; 4.2.7; 4.2.8 and 6.2.2
8. Conformity assessment bodies and their staff shall carry out conformity assessment activities with the highest degree of professional integrity and the requested technical competence in the specific field, and shall be free from all pressures and inducements which might influence their judgement or the results of their conformity assessment activities, including pressures and inducements of a financial nature, especially as regards persons or groups of persons with an interest in the results of those activities.	4.2.2; 4.2.3; 4.2.5; 4.2.12; 6.1.1.2; 6.1.2 and 6.1.3
9. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. Any subcontracting to, or consultation of, external staff shall be properly documented, shall not involve any intermediaries and shall be subject to a written agreement covering, among other things, confidentiality and conflicts of interest. The conformity assessment body in question shall take full responsibility for the tasks performed.	6.1.1.1; 6.1.1.2 and 6.2.1
10. At all times and for each conformity assessment procedure and each type, category or sub-category of ICT products, ICT services or ICT processes, a conformity assessment body shall have at its disposal the necessary: (a) staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks; (b) descriptions of procedures in accordance with which conformity assessment is to be carried out, to ensure the transparency of those procedures and the possibility of reproducing them. It shall have in place appropriate policies and procedures that distinguish between tasks that it carries out as a body notified pursuant to Article 61 and its other activities; (c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the technology of the ICT product, ICT service or ICT process in question and the mass or serial nature of the production process.	6.1.1.1; 6.1.1.2; 6.2.1; 4.4; 4.6a); 5.1.2; 7.1.1; 7.1.2; 7.1.3; 7.3; 7.4.4; 7.10.1 7.10.2

Requirements from the CSA Annex	Supporting requirements from EN ISO/IEC17065:2012
11. A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner, and shall have access to all necessary equipment and facilities.	4.3.2; 6.2 and 7.3.1
12. The persons responsible for carrying out conformity assessment activities shall have the following: (a) sound technical and vocational training covering all conformity assessment activities; (b) satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate authority to carry out those assessments; (c) appropriate knowledge and understanding of the applicable requirements and testing standards; (d) the ability to draw up certificates, records and reports demonstrating that conformity assessments have been carried out.	6.1.1.2; 6.1.2 and 6.2.1
13. The impartiality of the conformity assessment bodies, of their top-level management, of the persons responsible for carrying out conformity assessment activities, and of any subcontractors shall be guaranteed.	4.2.3; 4.2.4 and 5.2
14. The remuneration of the top-level management and of the persons responsible for carrying out conformity assessment activities shall not depend on the number of conformity assessments carried out or on the results of those assessments.	
15. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the Member State in accordance with its national law, or the Member State itself is directly responsible for the conformity assessment.	4.3
16. The conformity assessment body and its staff, its committees, its subsidiaries, its subcontractors, and any associated body or the staff of external bodies of a conformity assessment body shall maintain confidentiality and observe professional secrecy with regard to all information obtained in carrying out their conformity assessment tasks under this Regulation or pursuant to any provision of national law giving effect to this Regulation, except where disclosure is required by Union or Member State law to which such persons are subject, and except in relation to the competent authorities of the Member States in which its activities are carried out. Intellectual property rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this point.	4.5 and 6.1.1.3
17. With the exception of point 16, the requirements of this Annex shall not preclude exchanges of technical information and regulatory guidance between a conformity assessment body and a person who applies for certification or who is considering whether to apply for certification.	7.2
18. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of SMEs in relation to fees.	4.4; 7.1 and 7.4.4
19. Conformity assessment bodies shall meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing certification of ICT products, ICT services or ICT processes.	
20. Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of laboratories performing testing.	

26.7.2 Specific accreditation requirements

The requirements set out in CSA Annex and EN ISO/IEC 17065:2012 regarding independence, personnel and resources as specified below, shall apply to the accreditation of a CB.

26.7.2.1 Independence

The independence criteria set out in CSA Annex point 2 must apply to the ICT product, ICT process, ICT service under evaluation.

The CB must inform its clients of any activity of its legal entity including being a designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product, ICT service or ICT process that might be related to the type of services of the clients.

26.7.2.2 Certification body personnel

NOTE*: The EUCC SOTA requires compliance to a Common Criteria-specific set of requirements [ISO/IEC 19896] for “competence, competency levels, knowledge, skills, experience and education”, which may be relevant here, but only for evaluators. In addition, they refer to a list of products and attack types that are listed in annexes.*

This leads to at least two questions

QAC-02 Should we attempt to reuse the requirements from 19896, or shall we focus on the competences from CEN TS 18072?

We need to perform a comparison, and to possibly make a mix of these two.

QAC-03 Should we reuse and extend the tables defined in EUCC for technologies and evaluation techniques, or should we rather build a similar but dedicated table for this scheme (reusing the same)?

This is more of a strategic question for ENISA, about whether we would like to build a single table, extending it over time, or to build a dedicated table for each scheme. The EUDI Wallet may establish a bridge between different kinds of certification, since it includes different kinds of components.

26.7.2.3 Resources for the evaluation

NOTE*: For EUCC, they add a mandate to strictly separate the ITSEF activities from the certification activities, which may be linked to the fact that these two entities are accredited separately. There is no such explicit separation in EUDIW, so it may not be necessary to be so strict. Nevertheless, we may need to define some rules in addition to the basic ones when there is subcontracting.*

QAC-04 Do we want to define rules that are stronger than those from ISO/IEC 17065 and the CSA Annex? Should we treat subcontracting as a specific case?

The basic rules are already quite strict, so we are not sure that we need anything specific. However, there may be some precautions needed for some activities, like pen testing.

27. EUDIW GUIDELINES ON THE AUTHORISATION OF CABS

WHAT? **This SOTA document will define the requirements for the authorisation of CABs in the context of this scheme.**

HOW? **The corresponding SOTA for EUCC can be used as inspiration, most likely by mixing some content about CBs and ITSEFs. The basic competence requirements will need to be defined in the scheme itself.**

A TERMINOLOGY

A.1 MAIN TERMINOLOGY

Term	Definition
access control	means to ensure that physical and logical access to assets is authorised and restricted based on business and information security requirements [SOUCE: From ISO/IEC 27002:2022, 3.1.1]
access right	permission for a subject to access a particular object for a specific type of operation [SOURCE: From ISO/IEC 2382:2015, 2126298]
accreditation	third-party attestation related to a conformity assessment body, conveying formal demonstration of its competence, impartiality and consistent operation in performing specific conformity assessment activities [SOURCE: From ISO/IEC 17000:2020(en), 7.7]
accreditation body	conformity assessment body that performs accreditation Note 1 to entry: The authority of an accreditation body is generally derived from government. [SOURCE: From ISO/IEC 17000:2020(en), 2.6]
administration actions	set of actions for installing, deleting, modifying and consulting the configuration of a system participating in the service's information system and likely to modify its operation or security [SOURCE: From SecNumCloud Version 3.2, paragraph 1.3.2. Definitions (March 8, 2022)]
anonymisation	process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party [SOURCE: From ISO/IEC 29100:2011(en), 2.2]
application capabilities type	cloud capabilities type in which the cloud service customer can use the cloud service provider's applications [SOURCE: From ISO/IEC 22123-1:2023(en), 3.5.2]
application document	the document provided by a CSP to the CAB when applying for certification, which provides information about the cloud service to be certified
appropriate level of management	person or group of persons to whom top management has delegated a task or responsibility with the required mandate and authority Note 1 to entry: In security controls, the appropriate level of management would typically be responsible for topic-specific policies and procedures. [SOURCE: From CEN-CENELC TS 18026:2024, 3.8]
appropriateness of evidence	The measure of the quality of evidence [SOURCE: From ISAE3000: 12.i.ii]
asset	anything that has value to the organisation Note 1 to entry: In the context of information security, two kinds of assets can be distinguished: — the primary assets: — information;

Term	Definition

	— business processes and activities;
	— the supporting assets (on which the primary assets rely) of all types, for example:
	— hardware;
	— software;
	— network;
	— personnel;
	— site;
	— organisation's structure.
	[SOURCE: From ISO/IEC 27002:2022(en), 3.1.2]

asset life	period from asset creation to asset end-of-life [SOURCE: From ISO 55000:2014(en), 3.2.2]
assumption	a factor in the conformity assessment process that is considered to be true, real, or certain, without proof or demonstration [From ISO/IEC/IEEE 24765:2017(en), 3.276]
assurance	grounds for justified confidence that a product, service or process meets specified requirements [SOURCES: Inspired from ISO/IEC 15408-1:3(2009).1.4 and from ISO/IEC/IEEE 15026-1(2019):3.1]
assurance information	information including a claim about a system, evidence supporting the claim, an argument showing how the evidence supports the achievement of the claim, and the context for these items [SOURCE: From ISO/IEC/IEEE 15026-1(2019):3.4]
assurance level	a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned Note 1 to entry: A scheme often defines discrete assurance levels, and each such discrete level defines a degree of confidence in the fulfilment of requirements by the ICT product, ICT service, or ICT process. [SOURCE: From EC 881/2019, 2.21]
attack	successful or unsuccessful unauthorized attempt to destroy, alter, disable, gain access to an asset or any attempt to expose, steal, or make unauthorized use of an asset. [SOURCE: From ISO/IEC 27002:2022, 3.1.3]
attestation	issue of a statement, based on a decision, that fulfilment of specified requirements has been demonstrated Note 1 to entry: The resulting statement (…) is intended to convey the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, afford contractual or other legal guarantees. Note 2 to entry: First-party attestation and third-party attestation are distinguished by the terms declaration, certification, and accreditation, but there is no corresponding term applicable to second-party attestation. [SOURCE: From ISO/IEC 17000:2020(en), 7.3]
attribute	a characteristic, quality, right or permission of a natural or legal person or of an object [SOURCE: From eIDAS, Article 3(43)]
audit	process for obtaining relevant information about an object of conformity assessment and evaluating it objectively to determine the extent to which specified requirements are fulfilled Note 1 to entry: The specified requirements are defined prior to performing an audit so that the relevant information can be obtained. Note 2 to entry: Examples of objects for an audit are management systems, processes, products and services.

Term	Definition
	Note 3 to entry: For accreditation purposes, the audit process is called “assessment”. [SOURCE: From ISO 17000:2020(en), 6.4]
audit conclusion	outcome of an audit, after consideration of the audit objectives and all audit findings [SOURCE: From ISO 9000:2015, 3.13.10]
audit criteria	set of requirements used as a reference against which objective evidence is compared Note 1 to entry: Requirements may include policies, procedures, work instructions, legal requirements, contractual obligations, etc. [SOURCE: ISO 19011:2018(en), 3.7]
audit evidence	records, statements of fact or other information, which are relevant to the audit criteria and verifiable [SOURCE: FROM ISO/IEC 19011:2018, 3.9]
audit findings	results of the evaluation of the collected audit evidence against audit criteria [SOURCE: FROM ISO/IEC 19011:2018, 3.10]
audit plan	description of the activities and arrangements for an audit [SOURCE: From ISO 19011:2018, 3. 6]
audit programme	arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose [SOURCE: ISO 19011:2018, 3.4]
audit team	one or more persons conducting an audit, supported if needed by technical experts Note 1 to entry: One auditor of the audit team is appointed as the audit team leader. [SOURCE: ISO 9000:2015(en), 3.13.14]
audit time	time needed to plan and accomplish a complete and effective audit of the client’s service [SOURCE: From ISO/IEC 17021-1:2015, 3.16]
auditor	person who conducts an audit Note 1 to entry: In the schemes and related documents, 'the auditor' is typically used as the subject of requirements related to audit of the form "the auditor shall (...)". [SOURCE: From ISO/IEC 17021-1:2015(en), 3.6]
authentic source	a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice [SOURCE: From eIDAS, Article 3(47)]
authentication	[cybersecurity] provision of assurance that a claimed characteristic of an entity is correct [SOURCE: From ISO/IEC 27022:2022, 3.1.4 [identity] an electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form [SOURCE: From eIDAS, Article 3(5)]
authenticity	property that an entity is what it claims to be [SOURCE: From ISO/IEC 27000:2018(en), 3.6]
authorisation	activity performed by a NCCA to verify that an accredited CAB meets the specific or additional requirements define in a European cybersecurity certification scheme [SOURCE: From EUCSA, Article 60(3)]

Term	Definition
automated monitoring **monitor with automation**	Gather and pre-process data to analyse some aspects of the activity being monitored at discrete intervals at a sufficient frequency by non-human means Note 1 to entry: Automated monitoring and monitor with automation have the same meaning in this document
bridge letter	A document made available by a service organisation to cover a period of time between the reporting period end date of the current ISAE report and the release of a new ISAE report. Note to entry: bridge letters are needed in complements to ISAE reports that do not make forward-looking statements, to provide some guarantee that the vendor still operates the controls that have been audited in the previous reports, and declares any changes to its control framework [SOURE: ISAE]
business continuity	capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption [SOURCE: From ISO 22301:2019(en), 2019, 3.3]
business continuity plan	documented information that guides an organisation to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives [SOURCE: From ISO 22301:2019(en), 2019, 3.4]
business impact analysis	process of analysing the impact over time of a disruption on the organisation Note 1 to entry: The outcome is a statement and justification of business continuity requirements. [SOURCE: From ISO 22301:2019(en), 2019, 3.5]
capacity management	process for monitoring, analysis, reporting and improvement of capacity [SOURCE: From ISO/IEC TS 22237-7:2018(en), 3.1.2]
carve-out method	Method of dealing with the services provided by a subservice organisation, whereby the service organisation’s description of its system includes the nature of the services provided by a subservice organisation, but that subservice organisation’s relevant control objectives and related controls are excluded from the service organisation’s description of its system and from the scope of the service auditor’s engagement. The service organisation’s description of its system and the scope of the service auditor’s engagement include controls at the service organisation to monitor the effectiveness of controls at the subservice organisation, which may include the service organisation’s review of an assurance report on controls at the subservice organisation. [SOURCE: From ISAE3402: 9.a]
certification	third-party attestation related to an object of conformity assessment, with the exception of accreditation [SOURCE: From ISO/IEC 17000:2020(en), 7.6]
certification audit **joint audit** **combined audit** **integrated audit**	audit carried out by an auditing organisation independent of the client and the parties that rely on certification, for the purpose of certifying the client's service Note 1 to entry: Unless specifically qualified (e.g., “internal audit”), in the definitions which follow, the term “audit” has been used for simplicity to refer to third-party certification audit. Note 2 to entry: Certification audits include initial, surveillance, re-certification audits, and can also include special audits. Note 3 to entry: A joint audit is when two or more auditing organisations cooperate to audit a single client. Note 4 to entry: A combined audit is when a client is being audited against the requirements of two or more standards together. Note 5 to entry: An integrated audit is when a client has integrated the application of requirements of two or more standards into a single service and is being audited against more than one standard. Note 6 to entry: Removed references to management systems and the original Note 3. [SOURCE: From ISO/IEC 17021-1:2015, 3.4]

Term	Definition
certification body	third-party conformity assessment body that performs review and certification activities.
certification report	the document that accompanies the certificate, and provides a simple presentation of the cloud service and a summary of the conformity assessment activities
certification requirement	specified requirement, including service requirements, that is fulfilled by the client as a condition of establishing or maintaining certification Note to entry: This is the most high-level definition, which covers all kinds of requirements that need to be met in order to be certified. [SOURCE: From ISO/IEC 17065:2012, definition 3.7]
certification scheme	conformity assessment scheme that includes a certification activity Note 1 to entry: In a certification scheme, a successful assessment leads to the issuance of a certificate.
change management	process for recording, coordination, approval and monitoring of all changes [SOURCE: From ISO/IEC TS 22237-7:2018(en), 3.1.3]
characteristic	distinguishing feature Note 1 to entry: A characteristic can be inherent or assigned. Note 2 to entry: A characteristic can be qualitative or quantitative. [SOURCE: From ISO 9000:2015(en), 3.10.1]
claim	information declared by the client (3.13) Note 1 to entry: The claim is the object of conformity assessment by validation (3.2)/verification (3.3). Note 2 to entry: The claim can represent a situation at a point in time or could cover a period of time. Note 3 to entry: The claim should be clearly identifiable and capable of consistent evaluation or measurement against specified requirements by a validation body (3.4)/verification body (3.5). Note 4 to entry: The claim can be provided in the form of a report, a statement, a declaration, a project plan, or consolidated data. [SOURCE: From ISO/IEC 17029:2019(en), 3.1]
client	organisation whose service is being audited for certification purposes Note 1 to entry: “management system” has been replaced by “service” [SOURCE: Adapted from ISO/IEC 17021-1:2015(en), 3.5]
code of conduct	document specifying the ethical or personal behaviour required by a CSP from its employees [SOUCE: Adapted from ISO/IEC TS 17027:2014, 2.23]
compensating control	an internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions [SOURCE: SOC2]
competence	ability to apply knowledge and skills to achieve intended results [SOURCE: From ISO/IEC 17021:2015(en), 3.7]
complaint	expression of dissatisfaction by any person or organisation to a CAB or accreditation body or to the CAB’s NCCA, relating to the activity of that CAB, where a response is expected [SOURCE: Adapted from ISO/IEC 17000:2020, 8.7]
complementary user entity control **CUEC**	a control that the CSP assumes that their CSCs will have in place in order for them to securely use their cloud service NOTE: The term originates from the audit community, which is why it refers to a user entity instead of a customer, but the meaning is the same.

Term	Definition
	[SOURCE: SOC2]
complementary service organisation control **CSOC**	a control that the CSP assumes that their subservice providers will have in place in order for them to securely operate their cloud service NOTE: The term originates from the audit community, which is why it refers to a subservice organisation instead of a subservice provider, but the meaning is the same. [SOURCE: SOC2]
compliance	conformity in the context of the rules and requirements defined in a certification scheme that apply to the provider of the certified product, service or process Note 1 to entry: This is a refinement of ISO19011, which defines compliance as conformity in the context of a statutory requirement or regulatory requirement. In this case, compliance is conformity in the context of a given scheme. Note 2 to entry: The term is used to differentiate between compliance of a cloud service provider to the requirements defined in the scheme and conformity of a cloud service to the requirements on controls defined in the scheme. [SOURCE: Inspired from ISO 19011:2018(en), 3.7]
component	smallest selectable set of elements on which requirements may be based [SOURCE: From ISO/IEC 15408-1:2022(en), 3.17]
compromise	loss of confidentiality, integrity, or availability of information, including any resultant impairment of (1) processing integrity or availability of systems or (2) the integrity or availability of system inputs or outputs [SOURCE: TSC]
configuration management	management activity that applies technical and administrative direction over the life cycle of a product and service, its configuration identification and status, and related product and service configuration information [SOURCE: From ISO/IEC TS 10007:2017(en), Introduction]
conformity	fulfilment of a requirement Note 1 to entry: when used in opposition with compliance, conformity relates to the requirements related to the object of conformity assessment rather than to the requirements related to the certification scheme. [SOURCE: From ISO/IEC 19011:2018(en), 3.20]
conformity assessment	demonstration that specified requirements are fulfilled Note 1 to entry: The process of conformity assessment (…) can have a negative outcome, i.e. demonstrating that the specified requirements are not fulfilled. Note 2 to entry: The subject field of conformity assessment includes selection activities, determination activities such as testing, inspection and audit, review activities, and attestation activities such as certification, as well as the accreditation of conformity assessment bodies. Note 3 to entry: EN ISO/IEC 17000 does not include a definition of "conformity". "Conformity" does not feature in the definition of "conformity assessment". Nor does EN ISO/IEC 17000 address the concept of compliance. [SOURCE: From ISO/IEC 17000:2020(en), 4.1, some modifications in notes]
conformity assessment body **CAB**	body that performs conformity assessment services, excluding accreditation [SOURCE: From ISO/IEC 17000:2020(en), 4.6]
conformity assessment scheme	set of rules and procedures that describes the objects of conformity assessment, identifies the specified requirements and provides the methodology for performing conformity assessment Note 1 to entry: A conformity assessment scheme can be managed within a conformity assessment system. Note 2 to entry: A conformity assessment scheme can be operated at an international, regional, national sub-national, or industry sector level. Note 3 to entry: A scheme can cover all or part of the conformity assessment functions.

Term	Definition
	[SOURCE: From ISO/IEC 17000:2020(en), 4.9]
conformity self-assessment	first-party conformity assessment activities, which evaluate whether those ICT products, ICT services or ICT processes meet the requirements of a specific European cybersecurity certification scheme Note 1 to entry: The original definition from EC 881-2019 has been reworded to make the link with the definition of a first-party conformity assessment activity, but the meaning remains unchanged. [SOURCE: From EC881/2019:2.22]
consultancy	participation in a) the designing, manufacturing installing, maintaining or distributing of a certified product or a product to be certified, or b) the designing, implementing, operating or maintaining of a certified process or a process to be certified, or c) the designing, providing or maintaining of a certified service or a service to be certified [SOURCE: From ISO/IEC 17065:2012, 3.2]
control	measure that maintains and/or modifies risk Note 1 to entry: Controls include, but are not limited to, any process, policy, device, practice or other conditions and/or actions which maintain and/or modify risk. Note 2 to entry: Controls may not always exert the intended or assumed modifying effect. [SOURCE: From ISO 31000:2018, 3.8 / ISO/IEC 27002:2022(en), 3.1.8]
control objective	statement describing what is to be achieved as a result of implementing controls [SOURCE: ISO/IEC 27000:2018(en), 3.15]
control risk	the risk that an event that prevents a security requirement from being met will not be prevented or detected and corrected on a timely basis by the controls
Coordinated Universal Time **UTC**	time scale based on the second as defined in Recommendation ITU-R TF.460-6. [SOURCE: EN 319 401]
credential	representation of an identity Note 1 to entry: A credential is typically made to facilitate data authentication of the identity information in the identity it represents. Note 2 to entry: The identity information represented by a credential can be printed on paper or stored within a physical token that typically has been prepared in a manner to assert the information as valid. EXAMPLE: A credential can be a username, a username with a password, a PIN, a smartcard, a token, a fingerprint, a passport, etc. [SOURCE: From ISO/IEC 24760-1:2011, 3.3.5]
criteria	rules on which a judgment or decision can be based, or by which a product, service, result, or process can be evaluated [SOURCE: From ISO/IEC/IEEE 15289:2019(en), 3.1.6]
critical assets	assets within or in relation to a wallet unit of such extraordinary importance that where their availability, confidentiality or integrity are compromised, this would have a very serious, debilitating effect on the ability to rely on the wallet unit [SOURCE: From CIR (EU)2024/2981 (eIDAS 5c IA), 2.11
cyber risk	risk caused by a cyber threat Note 1 to entry: Cyber risks include risks associated with the loss of confidentiality, integrity and availability of information
cybersecurity	the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats

Term	Definition
	[SOURCE: From Regulation (EU) 2019/881, Article 2(1)]
Cybersecurity Act **EUCSA**	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
cyber threat	any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons [SOURCE: From Regulation (EU) 2019/881, Article 2(8)]
data at rest	structure, or group of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network telecommunications equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control together with the necessary levels of resilience and security required to provide the desired service availability Note 1 to entry: A structure can consist of multiple buildings and/or spaces with specific functions to support the primary function. Note 2 to entry: The boundaries of the structure or space considered the data centre, which includes the information and communication technology equipment and supporting environmental controls, can be defined within a larger structure or building. [SOURCE: From ISO/IEC 30134-1:2016(en), 3.6]
data in motion **data in transit**	data being transferred from one location to another Note 1 to entry: These transfers typically involve interfaces that are accessible and do not include internal transfers (i.e., never exposed to outside of an interface, chip, or device). [SOURCE: From ISO/IEC 27040:2015(en), 3.8]
data record	electronic data recorded with related meta- data supporting the processing of the data [SOURCE: From eIDAS, Article 3(56)]
decision	conclusion, based on the results of review, that fulfilment of specified requirements has or has not been demonstrated [SOURCE: From ISO/IEC 17000:2020(en), 7.2]
declaration	first-party attestation [SOURCE: From ISO/IEC 17000:2020(en), 7.5]
de-identification process	process of removing the association between a set of identifying attributes and the data principal [SOURCE : From ISO/IEC 20889:2018(en), 3.6]
design effectiveness	Refers to the suitability of the control as of a specified date or for a specified period (typically 6 to 12 months), based on the auditor's conclusion on whether (i) the risks that threaten the achievement of the control objectives have been identified by management; (ii) the controls would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives from being achieved. [SOURCE: Inspired from ISAE3402]
detective control	A control that detects and reports when errors, omissions and unauthorised uses or entries occur [SOURCE: SOC2]
determination	activities undertaken to develop complete information regarding fulfilment of the specified requirements by the object of conformity assessment or its sample [SOURCE: From ISO/IEC 17000:2020(en), A.3.1]

Term	Definition
development environment	The environment in which changes to software are developed NOTE: The environment may be local to an individual developer's workstation or distributed, possibly based on external services
disruption	incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organisation's objectives [SOURCE: From ISO 22301:2019(en), 2019, 3.10]
document	recorded information or material object, which can be treated as a unit [SOURCE: From ISO 5127:2001, 1.2.02]
effectiveness	extent to which planned activities are realised and planned results achieved [SOURCE: ISO Supplement:3.6]
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
electronic attestation of attributes **EAA**	an attestation in electronic form that allows attributes to be authenticated [SOURCE: From eIDAS, Article 3(44)]
electronic identification **eID**	the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person [SOURCE: From eIDAS, Article 3(1)]
electronic identification means **eID means**	a material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service [SOURCE: From eIDAS, Article 3(2)]
electronic identification scheme **eID scheme**	a system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons [SOURCE: From eIDAS, Article 3(4)]
electronic signature	data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign [SOURCE: From eIDAS, Article 3(10)]
employee	a person under contract with the provider to whom human resource management controls apply
EU statement of conformity	declaration produced by a vendor of ICT product, ICT process, or ICT service after performing a conformity self-assessment in the context of an European cybersecurity certification scheme, that states that a specific ICT product, ICT service or ICT process complies with the requirements of the European cybersecurity certification scheme
European Cybersecurity Certification group **ECCG**	A group composed of representatives of national cybersecurity certification authorities or other relevant national authorities [SOURCE: Adapted from Cybersecurity Act, Article 62]
European cybersecurity certification scheme	a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes Note 1 to entry: This definition is a refinement of the definition of a certification scheme. [SOURCE: From EC 881/2019:2.9]

Term	Definition
European Digital Identity Wallet **EUDI Wallet** wallet	an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals [SOURCE: From eIDAS, Article 3(42)]
EU Digital Identity Wallet Trust Mark	a verifiable, simple and recognisable indication which is communicated in a clear manner that a European Digital Identity Wallet has been provided in accordance with this Regulation [SOURCE: From eIDAS, Article 3(50)]
evaluation	combination of the selection and determination functions of conformity assessment activities [SOURCE: From ISO/IEC 17065:2012(en), 3.3]
evaluation level	a combination of assurance components within an evaluation methodology that corresponds to an assurance level and appropriate level of depth and rigour, corresponding to a category of security problems [SOURCE: From EC 881/2019, 52.8]
evaluation report	the document written by the CAB to describe the evaluation activities and their results, including the audit and the dependency analysis
events log	log which records audit trail data related to the system operations [SOURCE: From ISO 14641:2018, 3.2]
expiry	ending of the validity of the statement of conformity after a specified period [SOURCE: From ISO/IEC 17000:2020(en), 8.4]
extended requirement	a service requirement defined in a CSEP
fair presentation	accurate, truthful and transparent description Note: This is typically applied to the client's description of its service [SOURCE: Inspired from
feature	abstract functional characteristic of a system of interest that end-users and other stakeholders can understand Note 1 to entry: In systems engineering, features are syntheses of the needs of stakeholders. These features will be used, amongst others, to build the technical requirement baselines. [SOURCE: From ISO/IEC 26550:2015(en), 3.14]
first-party	the person or organisation that provides the object of conformity assessment [SOURCE: From ISO/IEC 17000:2020(en), 2.2]
first-party conformity assessment activity	conformity assessment activity that is performed by the person or organisation that provides the object of conformity assessment [SOURCE: From ISO/IEC 17000:2020(en), 4.3]
functional component	functional building block needed to engage in an activity, backed by an implementation [SOURCE: From ISO/IEC 22123-1:2023(en), 3.3.9]
guide	person appointed by the client to assist the audit team [SOURCE: From ISO/IEC 17021-1:2015, 3.8]

Term	Definition
ICT process	a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service Note 1 to entry: This term is to be used when a process is intended to be the object of a cybersecurity certification. The term 'process' is more general and should be used in other situations. [SOURCE: From EUCSA, Article 2(14)]
ICT product	an element or a group of elements of a network or information system Note 1 to entry: In the definition of certification schemes, the use of 'ICT product' follows this definition from EC 881-2019, and will mostly be used to refer to certification schemes and products certified using such schemes. It is a subset of the more general term product, whose definition originates in ISO9000. [SOURCE: From EUCSA, Article 2(12)]
ICT service	a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems Note 1 to entry: In the definition of certification schemes, the use of 'ICT service' follows this definition from EC 881-2019, and will mostly be used to refer to certification schemes and products certified using such schemes. For a more general use, it is preferable to use the term 'service'. [SOURCE: From EUCSA, Article 2(13)]
identity matching	a process where person identification data, or electronic identification means are matched with or linked to an existing account belonging to the same person [SOURCE: From eIDAS, Article 3(55)]
impact	outcome of a disruption affecting objectives [SOURCE: From ISO 22301:2019(en), 3.10]
impartiality	presence of objectivity [SOURCE: From ISO/IEC 17065:2012, 3.13]
incident	any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. [SOURCE: EN 319 401]
incident handling	actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents [SOURCE: From ISO/IEC 27035-1:2023, 3.1.8]
incident response	actions taken to mitigate or resolve an information security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it [SOURCE: From ISO/IEC 27035-1:2023, 3.1.9]
inclusive method	Method of dealing with the services provided by a subservice organisation, whereby the service organisation’s description of its system includes the nature of the services provided by a subservice organisation, and that subservice organisation’s relevant control objectives and related controls are included in the service organisation’s description of its system and in the scope of the service auditor’s engagement [SOURCE: From ISAE3402: 9.g]
information	meaningful data [SOURCE: ISO 9000:2015, 3.8.2]
information security	preservation of confidentiality, integrity and availability of information [SOURCE: From ISO/IEC 27000:2016, 2.33]

Term	Definition
information security breach	compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed. [SOURCE: From ISO/IEC 27002:2022, 3.1.13]
information security event **security event**	occurrence indicating a possible breach of information security or failure of controls [SOURCE: From ISO/IEC 27035-1:2023, 3.1.4]
information security incident **security incident** **incident**	one or multiple related and identified information security events that can harm an organisation's assets or compromise its operations [SOURCE: From ISO/IEC 27035-1:2023, 3.1.5]
information security incident management **incident management**	exercise of a consistent and effective approach to the handling of information security incidents [SOURCE: From ISO/IEC 27002:2022, 3.1.16]
information security management system **ISMS**	part of the overall management system, based on a business risk approach, used to establish, implement, operate, monitor, review, maintain and improve information security [SOURCE: From ISO/TS 12812-2:2017(en), 3.11]
information service	any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. Note 1 to entry: For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request. [SOURCE: From EC1535/2015:1.b]
inquiry	activity consisting of seeking information of knowledgeable persons, within the entity or outside the entity [SOURCE: From IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, 2017 Edition, Glossary of Terms]
inspection	an activity involving the examination of records or documents, whether internal or external, in paper form, electronic form, or on other media, or a physical examination of evidence [SOURCE: From IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, 2017 Edition, Glossary of Terms]
interested party **stakeholder**	person or organisation that can affect, be affected by, or perceive itself to be affected by a decision or activity [SOURCE: ISO Supplement:3.2]
internal audit	audit conducted by, or on behalf of, an organisation itself for management review and other internal purposes, and which can form the basis for an organisation's self-declaration of conformity Note 1 to entry: In many cases, particularly in smaller organisations, independence can be demonstrated by the freedom from responsibility for the activity being audited. [SOURCE: From ISO 22300:2021(en), 3.1.134]
large scale cybersecurity incident	incident whose disruption exceeds a Member State's capacity to respond to it or with a significant impact on at least two Member States [SOURCE: From NIS2]
life cycle	stages involved in the management of an asset

Term	Definition
	Note 1 to entry: The naming and number of the stages and the activities under each stage usually vary in different industry sectors and are determined by the organisation. [SOURCE: From ISO 55000:2014(en), 3.2.3]
limited assurance	assurance type where the nature and extent of the evaluation activities have been designed to provide a reduced level of assurance. Note 1 to entry: The evaluator's conclusion is expressed in a form that conveys whether, based on the evaluation activities performed and evidence obtained, a matter(s) has come to the evaluator's attention to cause the evaluator to believe the object of conformity assessment presents nonconformities. Note 2 to entry: The evaluator's conclusion in a limited assurance engagement is framed in a negative sense, for instance: " Based on the procedures performed, nothing came to our attention to indicate that the cloud service XYZ does not satisfy the certification requirements of the **Error! Unknown document property name.** at assurance level LLL." [SOURCE: Inspired from ISO 14064-3:2019, 3.6.7]
major change	change of a technical, physical, procedural or organisational nature that can impact security system integrity Note 1 to entry: This definition is based on the definition of management of change as included in ISO 19345-2:2019, 3.1.22 ("management of change -process that systematically recognises and communicates to the necessary parties changes of a technical, physical, procedural or organisational nature that can impact system integrity").
major nonconformity	nonconformity that affects the capability of the management system to achieve its intended results Note 1 to entry: Nonconformities could be classified as major in the following circumstances: - if there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements; - a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity. [SOURCE: Adapted from ISO/IEC 17021-1:2015(en), 3.12]
malware malicious software	Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability Note 1 to entry: Viruses and Trojan horses are examples of malware. [SOURCE: ISO/IEC 27033-1:2015, 3.22]
management system	set of interrelated or interacting elements of an organisation to establish policies and objectives, and processes to achieve those objectives Note 1 to entry: A management system can address a single discipline or several disciplines. Note 2 to entry: The system elements include the organisation's structure, roles and responsibilities, planning and operation. Note 3 to entry: The scope of a management system may include the whole of the organisation, specific and identified functions of the organisation, specific and identified sections of the organisation, or one or more functions across a group of organisations. [SOURCE: From ISO/IEC 27000:2018(en), 3.41]
minor nonconformity	nonconformity that does not affect the capability of the management system to achieve its intended results [SOURCE: Adapted from ISO/IEC 17021-1:2015(en), 3.12]
monitoring	determining the status of a system, a process or an activity Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe. [SOURCE: ISO/IEC 27000:2018(en), 3.46]

Term	Definition
multi-factor authentication	authentication mechanism consisting of two or more of the independent categories of credentials (knowledge, possession, and inherence factor) to verify the user's identity for a login or other transaction [SOURCE: EN 319 401
national cybersecurity certification scheme **national scheme**	a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes falling under the scope of the specific scheme Note 1 to entry: This definition is a refinement of the definition of a certification scheme. [SOURCE: From EC 881/2019:2.10]
national accreditation body **NAB**	the sole body in a Member State that performs accreditation with authority derived from the State [SOURCE: From EC765/2008:2.1]
near miss	event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but was successfully prevented from transpiring or did not materialize. [SOURCE: From NIS2]
non-compliance	nonconformity in the context of the rules and requirements defined in a certification scheme Note 1 to entry: This is a refinement of ISO19011, which defines non-compliance as nonconformity in the context of a statutory requirement or regulatory requirement. Here, compliance is conformity in the context of a given scheme. [SOURCE: Inspired from ISO 19011:2018(en), 3.7]
nonconformity	non-fulfilment of a requirement Note 1 to entry: when used in opposition with non-compliance, conformity relates to the requirements related to the object of conformity assessment rather than to the requirements related to the certification scheme. [SOURCE: From ISO Supplement:3.19]
object of conformity assessment **object**	entity to which specified requirements apply EXAMPLE: Product, process, service, system, installation, project, data, design, material, claim, person, body or organisation, or any combination thereof. [SOURCE: From ISO/IEC 17000:2020(en), 4.2, Note 2]
objective	result to be achieved Note 1 to entry: An objective can be strategic, tactical, or operational. Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels [such as strategic, organisation-wide, project, product and process]. Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an information security objective or by the use of other words with similar meaning (e.g. aim, goal, or target). Note 4 to entry: In the context of information security management systems, information security objectives are set by the organisation, consistent with the information security policy, to achieve specific results. [SOURCE: From ISO/IEC 27000:2018(en), 3.49]
objective evidence **evidence**	data supporting the existence or verity of something Note 1 to entry: Objective evidence can be obtained through observation, measurement, test, or by other means. Note 2 to entry: Objective evidence for the purpose of audit generally consists of records, statements of fact or other information which are relevant to the audit criteria and verifiable. [SOURCE: From ISO 9000:2015(en), 3.8.3]

Term	Definition
observation	activity consisting of looking at a process or procedure being performed by others [SOURCE: From IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, 2017 Edition, Glossary of Terms]
observer	person who accompanies the audit team but does not audit [SOURCE: From ISO/IEC 17021-1:2015(en), 3.9]
offline mode	as regards the use of European Digital Identity Wallets, an interaction between a user and a third party at a physical location using close proximity technologies, whereby the European Digital Identity Wallet is not required to access remote systems via electronic communication networks for the purpose of the interaction [SOURCE: From eIDAS, Article 3(57)]
operating effectiveness	A control is operating effectively, if (i) it was consistently applied as designed throughout the specified period, and (ii) in case of manual controls, they were applied by individuals who have the appropriate competence and authority. [SOURCE: Inspired from ISAE3402]
operational requirement	requirement that relates directly to the operation of a service, specified in standards or in other normative documents identified by the certification scheme [SOURCE: Inspired from ISO/IEC 17065:2012(en), 3.8]
operational risk	A risk arising from execution of a company's business functions
organisation	person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives Note 1 to entry: The concept of organisation includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private. [SOURCE: From ISO/IEC 27000:2018(en), 3.50]
output	result of a process Note 1 to entry: Whether an output of the organisation is a product or a service depends on the preponderance of the characteristics involved, e.g. a painting for sale in a gallery is a product whereas supply of a commissioned painting is a service, a hamburger bought in a retail store is a product whereas receiving an order and serving a hamburger ordered in a restaurant is part of a service. [SOURCE: From ISO 9000:2015(en), 5.6]
outsourcing	acquisition of services (with or without products) in support of a business function for performing activities using supplier's resources rather than the acquirer's Note 1 to entry: For the purposes of this document the terms "outsourcing" and "subcontracting" are considered to be synonyms. [SOURCE: From ISO/IEC 27036-1:2015, 3.6] [SOURCE Note 1: From ISO/IEC 17065:2012(en), $ 6.2.2.1]
peer assessment	assessment of a body against specified requirements by representatives of other bodies in, or candidates for, an agreement group Note 1 to entry: This entry is not satisfactory for several reasons, and in particular because it refers to concepts that are not currently defined (agreement group) and have little interest for us, and also mentions of a "body", which is unclear. Note 2 to entry: On the other hand, this could cover both CABs at level 'high' and NCCAs, but some rewriting is required. [SOURCE: From ISO/IEC 17000:2020(en), 4.5]
penetration testing	Authorised simulated cyberattack on a computer system, performed to evaluate the security of the system. [SOURCE: Adapted from Wikipedia]

Term	Definition
persistent data	data which is retained in the information system for more than one data management session [SOURCE: From ISO/IEC TR 10032: 2003(en), 2.54]
person identification data	a set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person [SOURCE: eIDAS, Article 3(3)]
personnel	persons doing work under the CSP's direction Note 1 to entry: The concept of personnel includes the CSP's members, such as the governing body, top management, employees, temporary staff, contractors and volunteers. [SOURCE: Adapted from ISO/IEC 27002:2022, 3.1.20]
point of contact	defined organisational function or role serving as the coordinator or focal point of information concerning incident management activities [SOURCE: From ISO/IEC 27035-1:2023, 3.1.10]
policy	intentions and direction of an organisation, as formally expressed by its top management [SOURCE: From ISO/IEC 27000:2018(en), 3.53]
pre-production environment	Mirror of production environment used for final testing or debugging
preventive control	An internal control that is used to avoid undesirable events, errors and other occurrences that an enterprise has determined could have a negative material effect on a process or end product [SOURCE: SOC2]
procedure	specified way to carry out an activity or a process Note 1 to entry: In this context, a process is defined as a set of interrelated or interacting activities that use inputs to deliver an intended result. [SOURCE: From ISO/IEC 17000:2020(en), 5.2]
process	set of interrelated or interacting activities which transforms inputs into outputs [SOURCE: From ISO Supplement:3.12]
product	result of a process Note 1 to entry: Four generic product categories are noted in ISO 9000:2005: — services (e.g. transport) (see definition in 3.6); — software (e.g. computer program, dictionary); — hardware (e.g. engine, mechanical part); — processed materials (e.g. lubricant). Many products comprise elements belonging to different generic product categories. Whether the product is then called service, software, hardware or processed material depends on the dominant element. Note 2 to entry: Products include results of natural processes, such as growth of plants and formation of other natural resources. Note 3 to entry: Adapted from ISO/IEC 17000:2004, definition 3.3. [SOURCE: From ISO/IEC 17065:2012(en), 3.4]
production environment	The environment that serves customers
qualified electronic attestation of attributes	an electronic attestation of attributes which is issued by a qualified trust service provider and meets the requirements laid down in Annex V [SOURCE: From eIDAS, Article 3(45)]

Term	Definition
qualified electronic signature	an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures [SOURCE: From eIDAS, Article 3(12)]
qualified trust service	a trust service that meets the applicable requirements laid down in this Regulation [SOURCE: From eIDAS, Article 3(17)]
qualified trust service provider	a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body [SOURCE: From eIDAS, Article 3(20)]
reasonable assurance	assurance type where the nature and extent of the evaluation activities have been designed to provide a high but not absolute level of assurance. Note 1 to entry: The evaluator's conclusion is expressed in a form that conveys the evaluator's opinion on the outcome of the evaluation of the object of evaluation against applicable criteria. Note 2 to entry: The evaluator's conclusion in a reasonable assurance engagement is framed in a positive sense, for instance: "Based on the activities performed, in our opinion, the cloud service XYZ satisfies the certification requirements of the **Error! Unknown document property name.** at evaluation level LLL." [SOURCE: Inspired from ISO 14064-3:2019, 3.6.6]
relying party	natural or legal person that relies upon an electronic identification or a trust service [SOURCE: From eIDAS, Article 3(6)]
reperformance	The auditor's independent execution of procedures or controls that were originally performed as part of the customer's internal controls [SOURCE: From IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, 2017 Edition, Glossary of Terms]
requirement	need or expectation that is stated, generally implied or obligatory Note 1 to entry: "Generally implied" means that it is custom or common practice for the organisation and interested parties that the need or expectation under consideration is implied. Note 2 to entry: A specified requirement is one that is stated, for example in documented information. Note 3 to entry: A qualifier can be used to denote a specific type of requirement, e.g. product requirement, service requirement, customer requirement. [SOURCE: From ISO/IEC 27000:2018(en), 3.56]
residual risk	risk remaining after risk treatment Note 1 to entry: Residual risk can contain unidentified risk. Note 2 to entry: Residual risk can also be known as "retained risk". [SOURCE: From ISO Guide73:2009(en), 3.8.1.6]
restoration	reinstatement of the full or partial statement of conformity [SOURCE: From ISO/IEC 17000:2020(en), 8.5]
review	determination of the suitability, adequacy or effectiveness of an object to achieve established objectives EXAMPLE: Management review, design and development review, review of customer requirements, review of corrective action and peer review. Note 1 to entry: Review can also include the determination of efficiency. [SOURCE: From EN ISO 9000:2015, 3.11.2]

Term	Definition
review	<certification> consideration of the suitability, adequacy and effectiveness of selection and determination activities, and the results of these activities, with regard to fulfilment of specified requirements by an object of conformity assessment [SOURCE: From ISO/IEC 17000:2020(en), 7.1]
review report	the document written by the CAB after performing the review of the evaluation performed by the audit team
risk	effect of uncertainty on objectives Note 1 to entry: An effect is a deviation from the expected — positive and/or negative. Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product and process). Note 3 to entry: Risk is often characterised by reference to potential events and consequences, or a combination of these. Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. [SOURCE: From ISO 31073:2022(en), 3.1.1]
risk analysis	process to comprehend the nature of risk and to determine the level of risk Note 1 to entry: Risk analysis provides the basis for risk evaluation and decisions about risk treatment. Note 2 to entry: Risk analysis includes risk estimation. [SOURCE: From ISO 31073:2022(en), 3.3.1]
risk assessment	overall process of risk identification, risk analysis and risk evaluation [SOURCE: From ISO 31073:2022(en), 3.3.8]
risk evaluation	process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable Note 1 to entry: Risk evaluation assists in the decision about risk treatment. [SOURCE: From ISO 31073:2022(en), 3.3.2]
risk identification	process of finding, recognising and describing risks Note 1 to entry: Risk identification involves the identification of risk sources, events, their causes and their potential consequences. Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs. [SOURCE: From ISO 31073:2022(en), 3.3.9]
risk management	coordinated activities to direct and control an organisation with regard to risk [SOURCE: From ISO 31073:2022(en), 3.2.1]
risk of material misstatement	The risk that the subject matter information is materially misstated prior to the start of the engagement [SOURCE: From ISAE3000: 12.w]
risk owner	person or entity with the accountability and authority to manage a risk [SOURCE: From ISO 31073:2022(en), 3.3.14]
risk treatment	process to modify risk (1.1) Note 1 to entry: Risk treatment can involve: • avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; • taking or increasing risk in order to pursue an opportunity;

Term	Definition
	• removing the risk source; • changing the likelihood; • changing the consequences; • sharing the risk with another party or parties [including contracts and risk financing]; and • retaining the risk by informed decision. Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”. Note 3 to entry: Risk treatment can create new risks or modify existing risks. [SOURCE: From ISO 31073:2022(en), 3.3.32]
role	set of activities that serves a common purpose [SOURCE: From ISO/IEC 22123-1:2023(en), 3.3.10]
role-based access control **RBAC**	security technique for authentication that authorises operations or allows access to resources based upon the user's identity and his/her relationship to other users and entities EXAMPLE 1: A teacher has read/write access to the grades for his/her students (role: "the teacher of the student"), but no access to other students' grades EXAMPLE 2: A principal has read-only access to the grades of all of his/her teachers' students (role: "the principal of the teachers of the students"), but the principal is not permitted to change any grades [SOURCE: From ISO/IEC 20944-1:2013(en), 3.21.20.2]
sampling	selection and/or collection of material or data regarding an object of conformity assessment Note 1 to entry: Selection can be on the basis of a procedure, an automated system, professional judgement etc. Note 2 to entry: Selection and collection can be performed by the same or different persons or organisations. [SOURCE: From ISO/IEC 17000:2020(en), 6.1]
scope of certification	identification of — the service(s) for which the certification is granted, — the applicable certification scheme and scheme options, and — the standard(s) and other normative document(s), including their date of publication, to which it is judged that the service(s) comply Note to entry: The definition has been altered to include “scheme options”, which may in the context of the EUCS cover in particular the selected evaluation level and extension profiles. [SOURCE: Adapted from ISO/IEC 17065:2012(en), 3.10]
security area	an area delimited by security perimeters, within which access is not controlled
security assurance	grounds for justified confidence that a claim about meeting security objectives has been or will be achieved [SOURCE: From ISO/IEC/IEEE 15026-1(2019):3.4]
security perimeter	the physical border surrounding locations hosting CSP equipment and personnel, for which access is controlled
security problem	statement which in a formal manner defines the nature and scope of the security that the object of conformity assessment is intended to address Note 1 to entry: This statement consists of a combination of: — threats to be countered by the object of conformity assessment, — the OSPs enforced by the object of conformity assessment, and — the assumptions that are upheld for the object of conformity assessment and its operational environment. [SOURCE: Adapted from ISO/IEC 15408-1:2009(en), 3.1.61]
security zone	area of a network in which limited data exchange with areas outside is allowed

Term	Definition
	[SOURCE: From ISO/TR 11636:2009(en), 2.13]
selection	planning and preparation activities in order to collect or produce all the information and input needed for the subsequent determination function Note 1 to entry: Selection activities vary widely in number and complexity. In some instances, very little selection activity may be needed. [SOURCE: From ISO/IEC 17000:2020(en), A.2.1]
service	output of an organisation with at least one activity necessarily performed between the organisation and the customer Note 1 to entry: This definition from ISO9000 echoes the definition of a product, and is refined into the notion of information service from European Regulation 1535/2015. [SOURCE: From ISO 9000:2000, 3.7.7]
service requirement	requirement that relates directly to a service, specified in standards or in other normative documents identified by the certification scheme [SOURCE: Adapted from ISO/IEC 17065:2012(en), 3.8]
specified requirement	need or expectation that is stated Note 1 to entry: Specified requirements may be stated in normative documents such as regulations, standards and technical specifications. Note 2 to entry: Specified requirements can be detailed or general Note 3 to entry: In the context of a European cybersecurity certification scheme, the specified requirements typically correspond to the requirements specified in the scheme, either directly or indirectly (in normative documents referred to in the scheme). [SOURCE: From ISO/IEC 17000:2020(en), 5.1]
Stakeholder Cybersecurity Certification Group **SCCG**	Advisory group composed of members selected from among recognised experts representing the relevant stakeholders [SOURCE: Adapted from Cybersecurity Act, Article 22]
state-of-the-art	developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience Note 1 to entry: The state of the art embodies what is currently and generally accepted as good practice in technology and medicine. The state of the art does not necessarily imply the most technologically advanced solution. The state of the art described here is sometimes referred to as the "generally acknowledged state of the art". [SOURCE: From ISO/IEC Guide 63:2019, 3.18]
state-of-the-art document	a document which specifies evaluation methods, techniques and tools that apply to the certification of cloud services, or security requirements of a generic cloud service category, or any other requirements necessary for certification, in order to harmonise evaluation [SOURCE: Adapted from (EU) 2024/482 (EUCC), Article (2)(14)]
strategy	planned activities to achieve a long term or overall objective [SOURCE: ISO 9000:2015, 3.5.12]
strong	not easily defeated, having strength or power greater than average or expected, able to withstand attack or solidly built [SOURCE: From ISO/IEC 19790:2012, 3.123]
strong user authentication	an authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inherence, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data [SOURCE: From eIDAS, Article 3(51)]

Term	Definition
subsystem	a set of elements, which is a system itself, and a component of a larger system [SOURCE: Wikipedia]
sufficiency of evidence	The measure of the quantity of evidence [SOURCE: From ISAE3000: 12.i.i]
supplementary cybersecurity information	Information related to cybersecurity to be made publicly available by any manufacturer or provider of certified ICT products, ICT services or ICT processes or of ICT products, ICT services and ICT processes for which an EU statement of conformity has been issued NOTE: The information includes guidance and recommendations, the period during which security support will be offered, contact information for receiving vulnerability information and a reference to online repositories listing vulnerabilities. [From Cybersecurity Act, Article 55]
supplier	organisation or an individual that enters into agreement with the acquirer for the supply of a product or service Note 1 to entry: Other terms commonly used for supplier are contractor, producer, seller, or vendor. Note 2 to entry: the term “service provider” is typically used in this scheme for suppliers of services Note 3 to entry: when opposed to “service provider”, the term “supplier” refers to a supplier of products [SOURCE: Adapted from ISO/IEC 27036:1-2014, 3.9]
support	set of activities necessary to ensure that an operational system or component fulfils its original requirements and any subsequent modifications to those requirements. NOTE: Examples include software or hardware maintenance, user training. [SOURCE: From ISO/IEC/IEEE 24756:2017, 3.4054]
surveillance	systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity Note 1 to entry: We may not want to keep this term, because of possible confusion with market surveillance, but it is kept for now, as some term needs to cover that concept. [SOURCE: From ISO/IEC 17000:2020(en), 8.1]
suspension	temporary restriction of the statement of conformity by the body that issued the statement, for all or part of the specified scope of attestation [SOURCE: From ISO/IEC 17000:2020(en), 8.2]
system	A distinct entity that consists of a number of interacting parts such that the removal or failure of one part may incapacitate the entity as a whole [SOURCE: From www.oxfordreference.com]
system component	a functional component required for the information security of the cloud service during the creation, processing, storage, transmission, deletion or destruction of information in the cloud service provider's area of responsibility NOTE: system components may include software, hardware, or both. EXAMPLES: firewalls, load balancers, web servers, application servers, database servers. [Source: Adapted from C5:2020]
technical expert	person who provides specific knowledge or expertise to the audit team [SOURCE: From ISO/IEC 17021-1:2015(en), 3.14]
tenant	one or more cloud service users sharing access to a set of physical and virtual resources [SOURCE: From ISO/IEC 22123-1:2023(en), 3.4.2]
test environment	The environment in which new and changed code is tested

Term	Definition
test	<development>activity in which a system or component is executed under specified conditions, the results are observed or recorded, and an evaluation is made of some aspect of the system or component [SOURCE: IEEE Std 610.12-1990]
testing	<conformity assessment>determination of one or more characteristics of an object of conformity assessment, according to a procedure Note 1 to entry: The procedure can be intended to control variables within testing as a contribution to the accuracy or reliability of the results. Note 2 to entry: The results of testing can be expressed in terms of specified units or objective comparison with agreed references. Note 3 to entry: The output of testing can include comments (e.g. opinions and interpretations) about the test results and fulfilment of specified requirements. [SOURCE: From ISO/IEC 17000:2020(en), 6.2]
third-party	a person or body that is independent of the person or organisation that provides the object of conformity assessment, and of user interests in that object [SOURCE: From ISO/IEC 17000:2020(en), 2.2]
third-party conformity assessment activity	conformity assessment activity that is performed by a person or organisation that is independent of the provider of the object of conformity assessment, and has no user interest in the object [SOURCE: From ISO/IEC 17000:2020(en), 4.5]
threat	potential cause of an unwanted incident, which can result in harm to a system or organisation [SOURCE: From ISO/IEC 27000:2018, 3.74]
top management	person or group of people who directs and controls an organisation at the highest level Note 1 to entry: Top management has the power to delegate authority and provide resources within the organisation. Note 2 to entry: If the scope of the management system covers only part of an organisation, then top management refers to those who direct and control that part of the organisation. [SOURCE: ISO Supplement:3.5]
trust service	an electronic service normally provided for remuneration which consists of: (a) the issuance of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; (b) the validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; (c) the creation of electronic signatures or electronic seals; (d) the validation of electronic signatures or electronic seals; (e) the preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals; (f) the management of remote electronic signature creation devices or remote electronic seal creation devices; (g) the issuance of electronic attestations of attributes; (h) the validation of electronic attestation of attributes; (i) the creation of electronic timestamps; (j) the validation of electronic timestamps; (k) the provision of electronic registered delivery services; (l) the validation of data transmitted through electronic registered delivery services and related evidence; (m) the electronic archiving of electronic data and electronic documents; (n) the recording of electronic data in an electronic ledger; [SOURCE: From eIDAS, Article 3(16)]

Term	Definition
trust service provider	a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider [SOURCE: From eIDAS, Article 3(19)]
tunnel	data path between networked devices which is established across an existing network infrastructure Note 1 to entry: Tunnels can be established using techniques such as protocol encapsulation, label switching, or virtual circuits [SOURCE: From ISO/IEC 27033-1:2015(en), 3.40]
undertaking	entities engaged in an economic activity, regardless of their legal status and the way in which they are financed including all linked enterprises or connected undertakings that form a group through the direct or indirect control of an enterprise or undertaking by another. [SOURCE: Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), Article 2(27)]]
user	a natural or legal person, or a natural person representing another natural person or a legal person, that uses trust services or electronic identification means provided in accordance with this Regulation [SOURCE: eIDAS, Article 3(5a)]
validation	[conformity assessment] confirmation of plausibility for a specific intended use or application through the provision of objective evidence that specified requirements (5.1) have been fulfilled Note 1 to entry: Validation can be applied to claims to confirm the information declared with the claim regarding an intended future use. [SOURCE: From ISO/IEC 17000:2020(en), 6.5] the process of verifying and confirming that data in electronic form are valid in accordance with this Regulation [SOURCE: From eIDAS, Article 3(41)]
verification	confirmation of truthfulness through the provision of objective evidence that specified requirements (5.1) have been fulfilled Note 1 to entry: Verification can be applied to claims to confirm the information declared with the claim regarding events that have already occurred or results that have already been obtained. [SOURCE: From ISO/IEC 17000:2020(en), 6.6]
version control	establishment and maintenance of baselines and the identification and control of changes to baselines that make it possible to return to the previous baseline [SOURCE: From ISO/IEC/IEEE 24765:2017(en), 3.4546]
vulnerability	weakness of an asset or control that can be exploited by one or more threats [SOURCE: From ISO/IEC 27000:2018(en), 2018, 3.77]
wallet instance	application installed and configured on a wallet user's device or environment, which is part of a wallet unit, and that the wallet user uses to interact with the wallet unit [SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(5)]
wallet provider	natural or legal person who provides wallet solutions [SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(8)]
wallet secure cryptographic application **WSCA**	application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the wallet secure cryptographic device [SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(4)]

Term	Definition
wallet secure cryptographic device **WSCD**	tamper-resistant device that provides an environment that is linked to and used by the wallet secure cryptographic application to protect critical assets and provide cryptographic functions for the secure execution of critical operations [SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(4)]
wallet solution	combination of software, hardware, services, settings, and configurations, including wallet instances, one or more wallet secure cryptographic applications and one or more wallet secure cryptographic devices [SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(1)]
wallet unit	unique configuration of a wallet solution that includes wallet instances, wallet secure cryptographic applications and wallet secure cryptographic devices provided by a wallet provider to an individual wallet user [SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(10)]
wallet user	user who is in control of the wallet unit [SOURCE: From CIR (EU) 2024/2981 (eIDAS 5c IA), Article 2(12)]
withdrawal **cancellation**	revocation of the statement of conformity by the body that issued the statement [SOURCE: From ISO/IEC 17000:2020(en), 8.3]

B COMPLIANCE TO REGULATION (EU)2024/2981

The present Annex is intended to describe how the present document meets the requirements of Regulation (EU)2024/2981 on the certification of EUDI Wallets.

Article	Coverage	Comments
Article 3: Establishment of national schemes	Article 1: Subject matter and scope Annex I: Scope of certification	Article 1 sets the big picture, with additional details provided in Annex I. Paragraph 4 requires architecture-specific information, which is not covered in the current template.
Article 4: General requirements 1.-2. Other schemes	Annex IX: Criteria to assess the acceptability of assurance information	Annex IX will include a list of schemes and standards that may be used to support the EUDIW schemes. As of today, only an example based on EUCC is provided, so this is mostly not covered.
Article 4.3 ISO 17067	Everywhere	The scheme includes all activities of a Type 6 scheme, including surveillance activities. A dedicated table is provided below for Article 6.5.
Article 4.4 (a) Restriction on providers	Not covered	This one could be an issue, since a recommendation is to issue certificates for partial coverage of the requirements, in particular for 5a(8), whose providers may not meet this requirement.
Article 4.4 (b) Trust Mark	Article 8: Marks and labels	Marks and labels are not allowed.
Article 4.4 (c) Scheme references	Throughout the scheme	In certificates and reports, the references to the scheme and regulation are mandatory.
Article 4.4 (d) Risk assessment	Article 4: Methods Annex XI: Methods	This is only covered in part as the method is not finalised. In addition, the chapter on methods may not be specific enough.
Article 4.4 (e) Responsibilities	Chapter 6: Conformity and compliance	This is not covered, as it needs to rely on national law.
Article 5.1 Policies	Annex I: Scope of certification	The incident and vulnerability management policies are listed as part of the object of certification, so they have to be present
Article 5.2 Incident notification	Article 16(3)	This is one of the monitoring
Article 5.3 Vuln management	Article 22(1)	This is the same requirement.
Article 5.4 Vuln/change notification	Article 16(3) Article 24(4)	Both changes and vulnerabilities need to be transmitted when they are material.
Article 5.5 Impact assessment	Article 24	The terms are nearly identical.
Article 5.6 Vuln report to CB	Article 24(4)	The notification of the vulnerability occurs with the transmission of the report.
Article 5.7 CRA	Article 22(2)	The CRA requirements have been adapted, but they are covered.
Article 5.8 Vuln disclosure	Article 27	CBs have obligations to share with scheme owners.

Article	Coverage	Comments
Article 5.9 Vuln public disclosure	Article 28	Publication is mandatory.
Article 6 Scheme maintenance		Not covered yet. Coverage will be added soon, drawing inspiration with rules adopted for EUCC maintenance.
Article 7 Scheme owners		Not applicable, as these obligations do not need to be stated in the scheme.
Article 8 Requirements	Annex X	Not covered yet.
Article 9 Accreditation	Article 12(1) Separate document on accred.	Covered, with requirements in an external document.
Article 10 Subcontracting	EN ISO/IEC 17065	This is covered by the basic standard, so no specific coverage is required.
Article 11 Supervisory body	Article 7(6) Article 10(4) Article 11(2) Article 19(4)	Notification of the supervisory body is required on all events on certificates.
Article 12 Consequences	Article 17 Article 24	The consequences of a nonconformity (including breaches) are covered, as well as the consequences of unmitigated vulnerabilities.
Article 13 Evaluation activities	Annex XI	Not covered yet, as the Annex is under development.
Article 14 Certification	Article 7 Annexes V, VI and VII	The requirements are in Article 7 and the content of the reports in three distinct annexes.
Article 15 Complaints & appeals		This is partially covered in EN ISO/IEC 17065, and could be complemented by references to national law. Consider adding specific text.
Article 16 Surveillance	Article 14 (scheme owber) Article 15 (CB) Article 16 (holder)	Monitoring obligations are defined.
Article 17 Consequences	Article 17 (nonconformity) Article 18 (non-compliance) Article 20 (CB non-compliance)	All aspects are covered in the articles.
Article 18 Lifecycle	Annex II: Lifecycle	All aspects are covered in the Annex.
Article 19 Retention of records	Article 29: Retention of records	All aspects are covered in the article.
Article 20 Protection of info	Article 31: Protection of info	All aspects are covered in the article.

As required in Article 4(2), point (a), national schemes also need to specify the elements listed in section 6.5 of EN ISO/IEC 17067:2013:

Element	Coverage	Comments
a) scope	Article 1: Subject matter and scope Annex I: Scope of certification	Article 1 sets the big picture, with additional details provided in Annex I.
b) requirements	Annex X	Requirements are still missing
c) activities	Annex XI	The activities are described, as well as their mandatory status
d) client obligations	Article 7(2) Article 16 Article 30	Several articles define obligations for service providers.

Element	Coverage	Comments
e) CB requirements	Article 13	Dedicated requirements, still missing a more detailed description.
f) accreditation	Article 12	Accreditation is required
g) consistency methods	Article 33 (peer assessment) Annex IX (peer assessment) Annex XI (methods)	Consistency is ensured by the definition of common methods, and also by the proposal of a peer assessment, although this may be an issue if there aren't enough CBs involved in the same peer assessment group.
h) required information	Article 5	Extensive list available
i) certificate content	Article 7 Annex V	Extensive description available
j) conditions of use	Article 7(2)	Clients have to agree on limitations on how they can use the certificate
k) marks of conformity		Not applicable, no marks of conformity
l) resources	EN ISO/IEC 17065	Covered by accreditation and accreditation requirements
m) use of results		Partly covered by EN ISO/IEC 17065, maybe some additions would be needed
n) nonconformities	Article 17	Nonconformities need to be reported and mitigated.
o) surveillance	Article 14 Article 15	Extensive requirements are defined, to monitor the certificate as well as the CBs.
p) access	Regulation (EU) No 910/2014	The access requirements (conditions for vendors, notification for CBs) are defined in the regulation.
q) publication	Article 7 (issuance) Article 11 (withdrawal)	Publication is mostly performed through the Commission.
r) contracts		This is not covered yet, to be discussed with scheme owners.
s) maintenance	Article 10	Many maintenance options are covered.
t) complaints records		Complaints are not covered yet
u) scheme references	Article 7(2)	Very simple obligations provided, should be enhanced by defining a unique reference to certificates across MS.
v) retention of records	Article 29 (CB) Article 30 (holder)	Obligations are clearly defined, including timelines

XX-00-00-000-XX-X

ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector, and Europe’s citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe’s critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 000-00-0000-000-0
doi: 0000.0000/000000

Příloha č. 2 – Vzor akceptačního protokolu

AKCEPTAČNÍ PROTOKOL_ Č.

Zhotovitel:

Objednatel:

Smlouva/Objednávka (název, číslo, datum uzavření):

Datum akceptačního řízení:

PŘEDMĚT AKCEPTACE:

Č.		Akceptační kritéria	
	Plnění (popis)/Přehled činnosti		Výrok Objednatele (splnění akceptačních kritérií)
1.			☐ Akceptováno bez výhrad ☐ Neakceptováno
2.			☐ Akceptováno bez výhrad ☐ Neakceptováno

Počet MD jednotlivých rolí poskytnutých pro splnění předmětu akceptace:

Role	Popis činnosti a datum	Počet MD celkem

(Pozn.: Počet MD se vyplňuje pouze, pokud je to relevantní s ohledem na předmět Objednávky.)

Přílohy:
BUDE DOPLNĚNO

Pozn. pro řádné splnění předmětného plnění musí být u všech položek k akceptaci uveden výrok Objednatele „Akceptováno bez výhrad“

Za Objednatele:	**Za Zhotovitele:**
Dne dle elektronického podpisu	Dne dle elektronického podpisu

Příloha č. 3 – Seznam členů realizačního týmu

	Role člena realizačního týmu	Titul, jméno a příjmení	Pracovně vztah právní k dodavateli (zaměstnanec/ poddodavatel)
1	*Analytik*	[redacted]	Zaměstnanec
2	*Expert v oblasti kybernetické a informační bezpečnosti*	[redacted]	Poddodavatel
3	*Expert informačních systémů*	[redacted]	Poddodavatel
4	*Expert pro budování a správu důvěryhodných digitálních identit*	[redacted]	Zaměstnanec
5	*Projektový manažer*	[redacted]	Zaměstnanec