Česká republika – Ministerstvo životního prostředí

• • •

INISOFT s.r.o.

SMLOUVA

NA REALIZACI VEŘEJNÉ ZAKÁZKY S NÁZVEM

„Nastavení nového způsobu aplikační identifikace uživatelů pro vybrané agendy odpadového hospodářství“

TATO SMLOUVA NA REALIZACI VEŘEJNÉ ZAKÁZKY (dále jen „**Smlouva**“) je uzavřena ve smyslu ustanovení § 1746 odst. 2 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“),

MEZI

Českou republikou – Ministerstvem životního prostředí

se sídlem:	Vršovická 1442/65, 100 10 Praha 10
zastoupenou:	Ing. Janou Vodičkovou, ředitelkou odboru informatiky
IČO:	00164801
bankovní spojení:	ČNB Praha 1
číslo účtu:	7628001/0710
zástupce pro věcná jednání:	Mgr. Jaromír Adamuška, vedoucí oddělení rozvoje, odbor informatiky

DÁLE JEN „**Objednatel**“ či také „**MŽP**“
NA STRANĚ JEDNÉ,

A

INISOFT s.r.o.

se sídlem:	Rumjancevova 696/3, Liberec 1, 460 01
zastoupenou:	Ing. Davidem Marečkem, jednatelem
IČO:	25417657
DIČ:	CZ25417657 (je plátcem DPH)
zapsanou:	obchodní rejstřík vedený Krajským soudem v Ústí nad Labem, spisová značka C 16913
bankovní spojení:	ČSOB a.s.
číslo účtu:	1805806583/0300
zástupce pro věcná jednání:	Ing. David Mareček

DÁLE JEN „**Poskytovatel**“
NA STRANĚ DRUHÉ,

POSKYTOVATEL A OBJEDNATEL SPOLEČNĚ JEN „**Smluvní strany**“
NEBO JEDNOTLIVĚ „**Smluvní strana**“.

Preambule

Tato Smlouva je uzavírána mezi Objednatelem a Poskytovatelem na základě výsledků zadávacího řízení na veřejnou zakázku malého rozsahu na služby s názvem **„Nastavení nového způsobu aplikační identifikace uživatelů pro vybrané agendy odpadového hospodářství“**, systémové číslo NEN: N006/21/V00029510 (dále jen „**Veřejná zakázka**“), zadávanou v souladu s ustanovením § 27 písm. a) zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále také jen jako „**ZZVZ**“), mimo působnost ZZVZ v souladu s ustanovením § 31 ZZVZ formou uzavřené výzvy. Nabídka Poskytovatele podaná v rámci zadávacího řízení na Veřejnou zakázku byla vyhodnocena jako nejvýhodnější (dále jen „**Nabídka**“).

Předmětem této Smlouvy je zabezpečení nového způsobu identifikace, autentizace a získávání oprávnění uživatelů u vybraných webových aplikací a služeb Informačního systému odpadového hospodářství (dále jen „**ISOH**“; viz níže) pro bezproblémovou komunikaci s centrálními systémy MŽP (CRŽP[1]/EnvIAM[2]). Ty umožní uživatelům ISOH využívat nové služby registrace, autentizace a autorizace tak, aby bylo možné pracovat s ISOH i po ukončení provozu systému ISPOP[3], který končí k datu 31. 12. 2021 a doposud služby autentizace a autorizace (v rámci modulu SSO a Registr ISPOP) systému ISOH poskytuje. Konkrétně půjde o poskytnutí služby rekonfigurace a nezbytného nastavení v rámci procesů přihlašování, ověřování rolí a ověřování IČO v ISOH.

Rekonfigurace se bude týkat vybraných webových částí ISOH, k nimž mj. Objednatel disponuje nevýhradním oprávněním je rozvíjet třetími stranami, zdrojovými kódy a základní technickou dokumentací, které budou dostupné Poskytovateli po podpisu této Smlouvy. Tvůrcem těchto částí ISOH a poskytovatelem aplikační podpory[4] je firma INISOFT s.r.o. (dále také „**zhotovitel ISOH**“).

Konkrétně se jedná rekonfiguraci a reparametrizaci v rámci níže uvedených webových částí ISOH (dále také „**předmětné části ISOH**“), tj. pro:

- webové aplikace:
  1. VISOH – Veřejný informační systém odpadového hospodářství (https://isoh.mzp.cz/visoh),
  2. Registr zařízení, obchodníků a spisů (https://isoh.mzp.cz/RegistrZarizeni);
- webové služby (SOAP):
  3. Datový sklad ORP – v části příjem/poskytování dat (https://isoh.mzp.cz/HlaseniOrpWS/HlaseniOrp.svc),
  4. Registr zařízení, obchodníků, skladů u původců a spisů – v části příjem dat (https://isoh.mzp.cz/RegistrZarizeniWS/RegistrZarizeni.svc),
  5. Seznam dopravců – v části příjem dat (https://isoh.mzp.cz/SeznamDopravcuWS/SeznamDopravcu.svc).

[1] https://crzp.mzp.cz
[2] https://iam.env.cz/cas/login
[3] https:/www.ispop.cz
[4] https://smlouvy.gov.cz/smlouva/16008011

Předmětné části ISOH jsou naprogramovány v jazyce C# ASP.NET, webové služby jsou na bázi SOAP/XML. Dosavadní nastavení autentizace uživatelů a strojová komunikace uvedených aplikací a služeb ISOH je dle standardu SSO (https://dev.ispop.cz/sso/README.html) a autorizace prostřednictvím registru ISPOP (https://dev.ispop.cz/ispop/ispop-ws/wsdl-doc/README.html).

Předmětné části ISOH ve stávající verzi jsou, a po rekonfiguraci Poskytovatelem budou, provozovány na infrastruktuře Objednatele.

Nový způsob autentizačních a autorizačních mechanismů potřebných pro nastavení nového způsobu autentizace a autorizace pro předmětné části ISOH popisuje dokumentace EnviIAM a CRŽP, které jsou přílohou č. 1 a č. 2 této Smlouvy.

Poskytovatel si je vědom, že předmětné části ISOH jsou nyní, a i po provedení plnění dle této Smlouvy Poskytovatelem budou dostupné v prostředí internetu, a že předmětné části ISOH jsou provozovány na infrastruktuře správce významného informačního systému dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**Zákon o KB**“). Poskytovatel se zavazuje, že po celou dobu trvání této Smlouvy bude jednat v souladu s výše citovaným Zákonem o KB a dále v souladu s vyhláškou č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**Vyhláška o KB**“). Poskytovatel prohlašuje, že při realizaci Veřejné zakázky zohlední bezpečnostní opatření k zajištění dostupnosti, důvěrnosti a integrity dat minimálně v rozsahu standardu OWASP.

Čl. 1
Účel a předmět Smlouvy

1.1 Účelem této Smlouvy je zajištění realizace Veřejné zakázky.

1.2 Předmětem této Smlouvy je závazek Poskytovatele zajistit pro Objednatele poskytnutí služby reparametrizace nastavení u funkcionality autentizace a autorizace pro předmětné části ISOH spočívající v poskytnutí níže uvedených služeb:

1.2.1. Nastavení nového způsobu autentizace a autorizace webových aplikací v procesu přihlášení, ověření role, ověření IČO dle technické specifikace EnviIAM a CRŽP (viz příloha č. 1 a č. 2 této Smlouvy) pro:

a) VISOH,

b) Registr zařízení, obchodníků a spisů;

1.2.2. Nastavení nového způsobu autentizace a autorizace webových služeb v procesu přihlášení, ověření role, ověření IČO[5] dle technické specifikace EnviIAM a CRŽP (viz příloha č. 1 a č. 2 této Smlouvy) pro:

a) Datový sklad ORP – v části příjem dat,

b) Datový sklad ORP – v části poskytnutí dat,

[5] Pro všechny služby vyjma pododst. 1.2.2 písm. a).

c) Registr zařízení, obchodníků, skladů u původců a spisů – v části příjem dat,

d) Seznam dopravců – v části příjem dat.

Vše shora uvedené dále souborně nebo jednotlivě – dle kontextu také jako „**Plnění**“, a to v rozsahu a za podmínek stanovených dále v této Smlouvě. Specifikace východisek a podklady potřebné pro realizaci Plnění jsou uvedeny v Příloze č. 1 a č. 2 této Smlouvy.

V rámci Plnění budou Poskytovatelem poskytnuty služby jako je analýza stávajícího nastavení předmětných částí ISOH, analýza rozhraní CRŽP/EnviIAM, návrh nového nastavení předmětných částí ISOH, ověření nového nastavení a finální přenastavení předmětných částí ISOH.

1.3 Poskytovatel prohlašuje, že je (i) oprávněn poskytovat Plnění v souladu a za podmínek stanovených touto Smlouvou, (ii) že je schopen řádně plnit veškeré povinnosti, ke kterým se touto Smlouvou zavázal, (iii) že svým plněním a poskytováním Plnění dle této Smlouvy neporušuje jakákoliv práva třetích osob.

1.4 Objednatel se zavazuje za řádně a včas poskytnuté Plnění zaplatit Poskytovateli ujednanou odměnu, a to za podmínek dále stanovených.

Čl. 2
Doba a místo plnění, trvání Smlouvy

2.1 Poskytovatel se zavazuje zahájit poskytování Plnění dle Čl. 1 odst. 1.2 pododst. 1.2.1 a 1.2.2 této Smlouvy ihned po nabytí účinnosti této Smlouvy. Povinností Poskytovatele je řádně realizovat Plnění dle Čl. 1 odst. 1.2 pododst. 1.2.1 a 1.2.2 této Smlouvy (tedy výstupy Plnění) nejpozději do 15. 12. 2021.

2.2 Tato Smlouva se uzavírá na dobu určitou, a to do 15. 12. 2021, resp. do splnění všech závazků z ní vyplývajících. Poskytovatel bude Objednateli poskytovat Plnění po celou dobu trvání této Smlouvy.

2.3 Místem plnění této Smlouvy je sídlo Objednatele uvedené výše v této Smlouvě, nebude-li Objednatelem během trvání této Smlouvy určeno písemně jinak.

2.4 Pro potřeby ověření, resp. zahájení akceptační kontroly, musí být Plnění Objednateli předáno a prezentováno nejpozději do 02. 12. 2021.

Čl. 3
Cena za Plnění

3.1 Cena za celkovou realizaci předmětu této Smlouvy činí dle Nabídky Dodavatele podané v rámci zadávacího řízení na Veřejnou zakázku 744.00,- Kč bez daně z přidané hodnoty (dále jen „**DPH**“). DPH činí v souladu s aktuálně platnou a účinnou právní úpravou 21 %, tedy 156.240,- Kč. Celková cena včetně DPH tedy činí 900.240,- Kč (dále jen „**Cena**“). Poskytovatel je plátcem DPH.

3.2 Cena dle odst. 3.1 tohoto článku je cenou konečnou, závaznou a nepřekročitelnou a zahrnuje veškeré případné náklady Poskytovatele související s poskytováním Plnění včetně všech úkonů, poplatků, služeb, dodávek apod., byť nebyly v Nabídce Poskytovatele výslovně uvedeny.

3.3 Cenu dle odst. 3.1 tohoto článku je možné změnit či překročit pouze v případě změny příslušných právních předpisů upravujících výši DPH. V takovém případě bude účtována DPH ve výši platné k datu uskutečnění zdanitelného plnění.

Čl. 4
Platební podmínky a fakturace

4.1 Cena dle Čl. 3 odst. 3.1 této Smlouvy bude Poskytovateli uhrazena na základě jediného daňového a účetního dokladu – faktury vystaveného Poskytovatelem (dále jen „**faktura**“) formou jednorázové úhrady. Podmínkou fakturace je Objednatelem schválený akceptační protokol, který bude přílohou faktury (viz dále).

4.2 Faktura bude obsahovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a bude mít náležitosti obchodní listiny dle § 435 Občanského zákoníku. Jedná se zejména o tyto náležitosti:

a) označení faktury a její číslo,

b) identifikační údaje Smluvních stran,

c) bankovní spojení, číslo účtu Poskytovatele,

d) předmět Smlouvy,

e) fakturovanou částku bez/včetně DPH,

f) evidenční číslo Smlouvy přidělené z Centrální evidence smluv Objednatele: 210205.

4.3 Přílohou faktury musí být Objednatelem schválený akceptační protokol o kvalitě poskytnutého Plnění. Objednatelem odsouhlasený akceptační protokol o kvalitě poskytnutého Plnění musí předcházet fakturaci. Oprávněná osoba Objednatele ve věcech smluvního plnění (viz Čl. 7 odst. 7.5 této Smlouvy) si bude moci vyžádat doplňující informace, kterými je Poskytovatel povinen doplnit akceptační protokol. V případě sporných údajů v akceptačním protokolu, které nebyly uspokojivě vysvětleny, budou tyto sporné údaje řešeny na úrovni signatářů této Smlouvy.

4.4 V návaznosti na odsouhlasení akceptačního protokolu Objednatelem (viz odst. 4.3 tohoto článku) bude oprávněnou osobou Objednatele ve věcech smluvního plnění (viz Čl. 7 odst. 7.5 této Smlouvy) vypočtena výše případných sankcí (smluvních pokut), které budou uplatněny vůči Poskytovateli způsobem dle Čl. 5 této Smlouvy.

4.5 Faktura bude zaslána buď v listinné podobě v jednom vyhotovení na adresu Objednatele ve tvaru: Ministerstvo životního prostředí, Odbor informatiky, Vršovická 1442/65, 100 10 Praha 10 nebo elektronicky na elektronickou podatelnu Objednatele: posta@mzp.cz, příp. datovou schránkou: 9gsaax4.

4.6 Lhůta splatnosti faktury činí 21 kalendářních dnů ode dne jejího doručení Objednateli. Fakturovaná částka bude uhrazena bezhotovostním převodem na účet Poskytovatele uvedený výše v této Smlouvě. Povinnost Objednatele zaplatit fakturovanou částku je splněna odepsáním příslušné částky z účtu Objednatele. Objednatel neposkytuje zálohy. Platby budou probíhat výhradně v Kč (CZK), rovněž veškeré cenové údaje na faktuře budou v této měně.

4.7 V případě, že faktura nebude obsahovat potřebné údaje a náležitosti dle odst. 4.2 tohoto článku a příslušných právních předpisů, je Objednatel oprávněn takovou fakturu vrátit Poskytovateli k doplnění či opravě. V takovém případě není Objednatel v prodlení s plněním svého závazku a nová lhůta splatnosti faktury začne plynout ode dne doručení doplněné či opravené faktury Objednateli.

Čl. 5
Smluvní pokuty

5.1 Poskytovatel se zavazuje poskytnout Objednateli na Plnění dle Čl. 1 odst. 1.2 pododst. 1.2.1 a 1.2.2 této Smlouvy (tedy výstupy Plnění) záruku za jakost v délce 24 měsíců, a to počínaje dnem jejich převzetí Objednatelem v souladu s příslušnými ustanoveními této Smlouvy.

5.2 Vady výstupů Plnění, které se vyskytnou v záruční době, musí Objednatel uplatnit u Poskytovatele bez zbytečného odkladu poté, co je zjistil nebo při náležité péči zjistit měl. Oznámení o výskytu vady bude Objednatelem učiněno písemně a doručeno Poskytovateli. V písemné oznámení o výskytu vady Objednatel vadu popíše a uvede požadovaný způsob odstranění vady. Poskytovatel je povinen vadu výstupů Plnění odstranit nejpozději do 10 kalendářních dnů ode dne doručení písemného oznámení Objednatele o výskytu vady, nebude-li dohodnuto mezi Smluvními stranami písemně jinak.

5.3 V případě prodlení Poskytovatele s řádným dokončením realizace Plnění dle Čl. 1 odst. 1.2 pododst. 1.2.1 a 1.2.2 této Smlouvy v termínu uvedeném v Čl. 2 odst. 2.1 této Smlouvy je Objednatel oprávněn požadovat po Poskytovateli uhrazení smluvní pokuty ve výši 200.000,- Kč. Tato pokuta nebude uplatněna, pokud dojde k akceptaci Plnění s výhradou, a zároveň do 10 pracovních dní proběhne akceptace Plnění bez výhrad. V případě, že by k této akceptaci bez výhrad ve výše uvedené lhůtě nedošlo, je Poskytovatel povinen uhradit k výše specifikované jednorázové pokutě návaznou pokutu 2.000,- Kč za každý i započatý den prodlení počínaje termínem dle Čl. 2 odst. 2.1 této Smlouvy (tedy zpětně), a to až do doby akceptace tohoto Plnění bez výhrad.

5.4 V případě porušení závazků vyplývajících z Čl. 6 této Smlouvy je Objednatel oprávněn požadovat po Poskytovateli smluvní pokutu ve výši 50.000,- Kč za každý jednotlivý případ takového porušení.

5.5 V případě prodlení Poskytovatele s odstraněním záručních vad dle odst. 5.2 tohoto článku o více než 7 kalendářních dní je Objednatel oprávněn požadovat po Poskytovateli smluvní pokutu ve výši 2.000,- Kč za každý i započatý den prodlení.

5.6 V případě porušení jakékoliv další povinnosti Poskytovatele vyplývající z této Smlouvy je Objednatel oprávněn požadovat po Poskytovateli smluvní pokutu ve výši 5.000,- Kč za každý jednotlivý případ takového porušení/den prodlení.

5.7 Zaplacení uvedené smluvní pokuty dle odst. 5.1 až 5.6 tohoto článku nemá vliv na případné uplatnění náhrady škody, a to v její plné výši.

5.8 Smluvní pokuta je splatná do 21 kalendářních dnů ode dne doručení výzvy k jejímu zaplacení Poskytovateli. Dnem splatnosti se rozumí den připsání příslušné částky na účet Objednatele, který je uveden výše v této Smlouvě.

5.9 Při nedodržení termínu splatnosti jakékoli faktury dle Čl. 4 odst. 4.6 této Smlouvy je Poskytovatel oprávněn požadovat po Objednateli úrok z prodlení ve výši stanovené příslušnými právními předpisy.

Čl. 6
Ochrana informací

6.1 Smluvní strany jsou povinny zajistit utajení získaných důvěrných informací. Tato povinnost platí bez ohledu na trvání této Smlouvy a vztahuje se rovněž na všechny zaměstnance obou Smluvních stran.

6.2 Právo užívat, poskytovat nebo zpřístupnit důvěrné informace mají obě Smluvní strany pouze v rozsahu a za podmínek nezbytných pro řádné plnění práv a povinností vyplývajících z této Smlouvy či jiných právních předpisů.

6.3 Smluvní strany sjednávají, že důvěrnými informacemi jsou veškeré vzájemně poskytnuté informace, podklady a dokumenty, pokud nejsou běžně dostupné ve veřejných zdrojích (např. obchodní rejstřík). Tím není dotčeno ustanovení odst. 6.4 tohoto článku.

6.4 Poskytovatel uzavřením této Smlouvy výslovně souhlasí, aby tato Smlouva a/nebo její jakákoliv část byla Objednatelem zveřejněna způsobem umožňujícím neomezenému počtu třetích osob dálkový přístup a/nebo jiným vhodným způsobem v souladu s příslušnými právními předpisy.

6.5 Smluvní strany jsou si vědomy povinností vyplývajících zejména z nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), (dále jen „**GDPR**“), popř. ze zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (dále jen „**Zákon o zpracování**“). Vzhledem ke skutečnosti, že při plnění předmětu této Smlouvy může docházet ke zpracování osobních údajů, zavazuje se Poskytovatel uzavřít s Objednatelem před zahájením zpracování osobních údajů v souvislosti s plněním předmětu této Smlouvy smlouvu o zpracování osobních údajů (dále jen „**Smlouva o zpracování**“) s náležitostmi a v souladu s příslušnými ustanoveními GDPR a Zákona o zpracování. Návrh Smlouvy o zpracování předkládá Objednatel a Poskytovatel se zavazuje uzavřít Smlouvu o zpracování nejpozději do 5 kalendářních dnů ode dne předložení jejího návrhu.

Čl. 7
Součinnost a vzájemná komunikace

7.1 Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění závazků vyplývajících z této Smlouvy, zejména pak vzájemně se informovat o skutečnostech, které jsou nebo mohou být významné pro plnění této Smlouvy.

7.2 Poskytovatel se též zavazuje k poskytnutí veškeré případné součinnosti při plnění povinností vyplývajících ze ZZVZ.

7.3 Poskytovatel je dále povinen umožnit kontrolu v místě plnění i kontrolu všech dokladů souvisejících s plněním této Smlouvy, a to zejména v souladu se zákonem č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, zákonem č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů. Tyto povinnosti trvají i po ukončení této Smlouvy.

7.4 Pro komunikaci mezi Objednatelem a Poskytovatelem ve věcech plnění této Smlouvy bude sloužit primárně e-mail nebo telefon.

7.5 Veškerá komunikace mezi Smluvními stranami bude probíhat prostřednictvím zástupců Smluvních stran (dále jen „**Oprávněné osoby**“). Oprávněné osoby budou zastupovat Smluvní strany v záležitostech souvisejících s plněním této Smlouvy, zejména co se týče kladení požadavků ze strany Objednatele a řešení těchto požadavků Poskytovatelem. Pro účely této Smlouvy se má za to, že Oprávněnými osobami jsou:

Oprávněné osoby Objednatele:

a) Ve věcech smluvního plnění a akceptace:

Mgr. Jaromír Adamuška (kontaktní údaje: jaromir.adamuska@mzp.cz, 267 122 277).

Oprávněné osoby Poskytovatele:

a) Ve věcech technické realizace smluvního plnění:

b) Ve věcech akceptace smluvního plnění:

Ing. David Mareček (kontaktní údaje: 

7.6 Oprávněné osoby je přípustné v průběhu trvání této Smlouvy měnit na základě písemného oznámení druhé Smluvní straně (není tedy potřeba uzavřít dodatek k této Smlouvě). Pro podání tohoto oznámení je přípustná e-mailová cesta. Kontaktními osobami oprávněnými provádět tato oznámení jsou za Objednatele: Mgr. Jaromír Adamuška (jaromir.adamuska@mzp.cz), případně Objednatelem jiná delegované osoba a za Poskytovatele: Ing. David Mareček,  .

Čl. 8
Povinnosti Smluvních stran

8.1 Objednatel se zavazuje spolupracovat se Poskytovatelem v rozsahu nezbytném k řádnému splnění závazků vyplývajících Poskytovateli z této Smlouvy.

8.2 Poskytovatel se zavazuje plnit předmět této Smlouvy s odbornou péčí, řádně a včas v souladu s pokyny a zájmy Objednatele, a dále se zadávacími podmínkami na Veřejnou zakázku, Nabídkou a touto Smlouvou.

8.3 Poskytovatel odpovídá Objednateli v plném rozsahu (bez omezení) za škodu, kterou mu způsobí v souvislosti s plněním předmětu této Smlouvy, zejména pokud způsobí nevratnou ztrátu nebo poškození významnější části informačního obsahu (dat) ISOH. Této odpovědnosti se zprostí, pokud prokáže, že škodu nezavinil. Poskytovatel se vždy zprostí odpovědnosti za škodu také v případě, pokud Objednatele upozorní na nevhodnost jeho pokynů a Objednatel přesto postupuje způsobem, který byl Poskytovatelem označen za rizikový.

8.4 Poskytovatel se zavazuje poskytovat:

a) Plnění související s realizací úprav předmětných částí ISOH, jakožto významného informačního systému dle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů, v souladu s požadavky Zákona o KB a navazující Vyhlášky o KB,

b) součinnost při kontrole plnění požadavků Zákona o KB Národním bezpečnostním úřadem (dále jen „**NBÚ**“) a Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**“) a auditory Objednatele, a

c) odstranit bezúplatně nedostatky související s poskytováním Plnění zjištěné při kontrole plnění požadavků Zákona o KB, NBÚ, NÚKIB nebo auditory Objednatele, vznikly-li z důvodů na straně Poskytovatele.

8.5 Poskytovatel se zavazuje umožnit Objednateli kdykoliv k jeho žádosti provedení zákaznického auditu. Požadavek Objednatele o provedení zákaznického auditu musí být doručen alespoň 5 pracovních dnů před požadovaným termínem provedení zákaznického auditu. Nebudou-li to vyžadovat okolnosti zvláštního zřetele hodné, je Objednatel oprávněn doručit požadavek na provedení zákaznického auditu vždy maximálně jednou v každém roce trvání této Smlouvy. Zákaznický audit může být proveden pouze osobami k jeho provedení vydaným osobou oprávněnou jednat za Objednatele ve věcech smluvních (viz Čl. 7 odst. 7.5 této Smlouvy). Rozsah zákaznického auditu bude předmětem dohody Smluvních stran.

8.6 Dojde-li v souvislosti s plněním této Smlouvy ke kybernetickému bezpečnostnímu incidentu ve smyslu Zákona o KB, je Poskytovatel povinen informovat Objednatele písemně o výskytu kybernetického bezpečnostního incidentu a písemné oznámení doručit Objednateli bezodkladně, nejpozději však do 24 hodin od výskytu kybernetického bezpečnostního incidentu. Poruší-li Poskytovatel tuto povinnost, je povinen zaplatit Objednateli smluvní pokutu ve výši 1.000,- Kč za každou hodinu prodlení.

8.7 Poskytovatel se zavazuje po celou dobu trvání této Smlouvy naplňovat Zákon o KB a jednat v souladu s Vyhláškou o KB.

8.8 Poskytovatel je povinen informovat Objednatele o způsobu řízení rizik na straně Poskytovatele ve smyslu § 4 Vyhlášky o KB. Řízením rizik se rozumí činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik.

8.9 Poskytovatel se zavazuje k součinnosti při výkonu finanční kontroly dle § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů. Poskytovatel se dále zavazuje umožnit všem oprávněným subjektům provést kontrolu dokladů souvisejících s plněním Veřejné zakázky, a to po dobu určenou k jejich archivaci v souladu s příslušnými právními předpisy.

8.10 Poskytovatel se zavazuje k dodržování bezpečnostních politik Objednatele, s nimiž byl seznámen před podpisem této Smlouvy, což potvrzuje v samostatném protokolu, který je vyhotoven Objednatelem k datu podpisu této Smlouvy včetně specifikace jednotlivých bezpečnostních politik. Poskytovatel se zavazuje i k dodržování veškerých jejích následných změn, s nimiž musí být rovněž Objednatelem prokazatelně seznámen.

8.11 Poskytovatel se dále zavazuje, že po dobu trvání této Smlouvy bude mít sjednáno a platně uzavřeno pojištění odpovědnosti za škodu způsobenou Objednateli či třetí osobě Poskytovatelem, jeho zaměstnanci, nebo osobami v obdobném postavení, přičemž pojistná smlouva bude mít limit pojistného plnění na jednu pojistnou událost ve výši nejméně 1.000.000,- Kč. Poskytovatel je povinen umožnit Objednateli kdykoliv nahlédnout do originálu pojistné smlouvy. Poskytovatel je dále povinen Objednatele bezodkladně (nejpozději do 2 pracovních dnů) informovat o jakékoliv změně pojistné smlouvy.

8.12 Poskytovatel je dále povinen informovat Objednatele o významné změně ovládání Poskytovatele (viz § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů) a to bez zbytečného odkladu poté, co dojde k takové změně ovládání. Nastane-li skutečnost uvedená v předchozí větě tohoto odstavce, je Objednatel oprávněn od této Smlouvy odstoupit v souladu s Čl. 9 této Smlouvy.

8.13 Poskytovatel nesmí, vyjma na písemnou žádost Objednatelem vyžádaných a řádně zdůvodněných případů, zasahovat do obsahu dat ISOH či jakýchkoliv jiných dat Objednatele.

8.14 Poskytovatel nesmí provést zásah, který by ovlivnil či mohl ovlivnit funkcionalitu HW Objednatele či jiného SW provozovaného na HW Objednatele, včetně pracovních stanic.

Čl. 9
Ukončení Smlouvy, řešení sporů

9.1 Tuto Smlouvy lze ukončit písemnou dohodou Smluvních stran, písemnou výpovědí nebo odstoupení od této Smlouvy.

9.2 Objednatel je oprávněn ukončit tuto Smlouvu písemnou výpovědí bez uvedení důvodu s výpovědní dobou v délce 7 kalendářních dní. Výpovědní doba počíná běžet prvním dnem následujícím po dni, ve kterém byla výpověď doručena druhé Smluvní straně.

9.3 Poskytovatel je oprávněn vypovědět tuto Smlouvu písemnou výpovědí s výpovědní dobou v délce 14 kalendářních dní. Výpovědní doba počíná běžet prvním dnem následujícím po dni, ve kterém byla výpověď doručena druhé Smluvní straně.

9.4 Smluvní strany jsou oprávněny odstoupit od této Smlouvy z důvodů uvedených v § 2002 Občanského zákoníku, tj. z důvodu porušení této Smlouvy podstatným způsobem.

9.5 Za podstatné porušení této Smlouvy ze strany Objednatele se považuje prodlení s úhradou faktury po dobu delší než 60 kalendářních dnů po její splatnosti.

9.6 Za podstatné porušení této Smlouvy ze strany Poskytovatele se považuje, realizuje-li Poskytovatel plnění předmětu této Smlouvy v rozporu s ustanoveními této Smlouvy a/nebo ustanoveními jiných závazných dokumentů či příslušných obecně závazných právních předpisů, a neodstraní-li takové porušení ani v dodatečné přiměřené lhůtě poskytnuté mu Objednatelem v písemné výzvě.

9.7 Objednatel je dále oprávněn odstoupit od této Smlouvy v případě:

a) bude-li Poskytovatel v prodlení s realizací Plnění oproti termínům stanoveným touto Smlouvou či na základě této Smlouvy a/nebo bude-li v prodlení s odstraněním záručních vad či s jakýmkoli jiným termínem daným touto Smlouvou o více než 7 kalendářních dní;

b) jestliže prohlášení Poskytovatele uvedené v Čl. 1 odst. 1.3 této Smlouvy se ukáže jako nepravdivé jako celek, popř. v kterékoliv jeho části,

c) nebude-li mít Poskytovatel platné a účinné pojištění odpovědnosti za škodu v souladu s Čl. 8 odst. 8.11 této Smlouvy;

d) poruší-li Poskytovatel povinnost ochrany důvěrných informací dle této Smlouvy,

e) na majetek Poskytovatele je prohlášen úpadek nebo Poskytovatel sám podá dlužnický návrh na zahájení insolvenčního řízení, nebo vstoupí-li Poskytovatel do likvidace.

9.8 Objednatel je dále oprávněn odstoupit od této Smlouvy, jestliže zjistí, že Poskytovatel:

a) nabízel, dával, přijímal nebo zprostředkovával určité hodnoty s cílem ovlivnit chování nebo jednání kohokoliv, ať již státního úředníka nebo někoho jiného, přímo nebo nepřímo, v zadávacím řízení nebo při provádění Smlouvy; nebo

b) zkresloval jakékoliv skutečnosti za účelem ovlivnění zadávacího řízení nebo provádění Smlouvy ke škodě Objednatele, včetně užití podvodných praktik k potlačení a snížení výhod volné a otevřené soutěže; nebo

c) nedodržoval povinnosti vyplývající z předpisů práva životního prostředí, sociálních nebo pracovně právních předpisů nebo kolektivních smluv vztahujících se k předmětu plnění Veřejné zakázky.

9.9 Bude-li Poskytovatel poskytovat plnění dle této Smlouvy v rozporu s touto Smlouvou a jejími přílohami, zadávacími podmínkami na Veřejnou zakázku, Nabídkou, popř. v rozporu s platnými právními předpisy a normami a nenapraví-li Poskytovatel takové vadné plnění ani v dodatečné lhůtě stanovené mu Objednatelem v písemné výzvě ke sjednání nápravy, je Objednatel oprávněn po marném uplynutí této dodatečné lhůty od této Smlouvy odstoupit.

9.10 Odstoupení od této Smlouvy musí být učiněno v písemné formě a doručeno druhé Smluvní straně. Odstoupením se závazek založený touto Smlouvou zrušuje od počátku a Smluvní strany se vypořádají podle příslušných ustanovení Občanského zákoníku o bezdůvodném obohacení. Účinky odstoupení od této Smlouvy nastávají okamžikem doručení písemného oznámení o odstoupení od této Smlouvy druhé Smluvní straně. Odstoupení od této Smlouvy se nedotýká práva na zaplacení smluvní pokuty a úroku z prodlení, pokud již dospěl, práva na náhradu škody a ani ujednání, které má vzhledem ke své povaze zavazovat Smluvní strany i po odstoupení od této Smlouvy, tj. zejména ani ujednání o způsobu řešení sporů a volbě práva. Obdobné platí i pro předčasné ukončení této Smlouvy jiným způsobem.

9.11 Součástí plnění Poskytovatele dle této Smlouvy je pro případ skončení účinnosti této Smlouvy (výpovědí, odstoupením od Smlouvy, dohodou Smluvní stran, jak je uvedeno v příslušných ustanoveních této Smlouvy) poskytnutí (i) veškeré potřebné součinnosti, (ii) předání všech SW komponent, dat a metadat, (iii) poskytnutí informací a (iv) účast na jednáních s Objednatelem a třetími osobami za účelem plynulého nahrazení všech dosavadních činností Poskytovatele dle této Smlouvy vlastní činností Objednatele nebo činností jiného poskytovatele určeného Objednatelem v souvislosti s ukončením účinnosti této Smlouvy. Dosavadními činnostmi Poskytovatele se rozumí zajištění realizací Plnění.

9.12 S odkazem na skutečnosti uvedené odst. 9.11 tohoto článku se Poskytovatel zavazuje poskytovat veškerou součinnost do doby úplného převzetí výstupů Plnění Objednatelem nebo novým poskytovatelem. V případě, že dojde k uzavření nové smlouvy týkající se rozvoje výstupů Plnění s novým poskytovatelem odlišným od Poskytovatele, zavazuje se Poskytovatel po skončení účinnosti této Smlouvy poskytovat Objednateli nebo jím určeným třetím stranám veškerou součinnost potřebnou pro účely plynulého a řádného poskytování rozvoje a podpory výstupů Plnění novým poskytovatelem.

9.13 Bude-li požadována součinnost dle odst. 9.12 tohoto článku ze strany Objednatele nebo jím určené třetí osoby, zavazuje se Poskytovatel reagovat na požadavek Objednatele nebo jím určené třetí osoby a zahájit poskytování součinnosti nejpozději do 3 pracovních dnů ode dne doručení takovéhoto požadavku. Bude-li Poskytovatel v prodlení se splněním této povinnosti poskytnout součinnost, je povinen zaplatit Objednateli smluvní pokutu ve výši 1.000,- Kč za každý i započatý den prodlení.

9.14 Dojde-li z jakéhokoli důvodu, spočívajícího na kterékoli Smluvní straně, k potřebě migrace výstupů Plnění do nástupnického systému, je Poskytovatel povinen poskytnout Objednateli veškerou potřebnou součinnost k tomuto převodu, a to i po datu ukončení této Smlouvy.

Čl. 10
Součinnost a záruka k výsledkům poskytování Plnění

10.1 Objednatel umožní Poskytovateli řádnou realizaci Plnění dle této Smlouvy poskytnutím potřebných licencí, dokumentace, informací a součinnosti pro napojení na stávající informační systémy (zejména EnviAIM, CRŽP), které jsou pro plnění dle této Smlouvy potřebné.

10.2 Poskytovatel tímto poskytuje Objednateli záruku za to, že výstupy Plnění budou po dobu nejméně 2 let od ukončení trvání této Smlouvy v souladu s touto Smlouvou a v souladu s právními předpisy České republiky, kterými jsou zejména (nikoliv však výlučně): zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, zákon č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, zákon č. 123/1998 Sb., o právu na informace o životním prostředí, ve znění pozdějších předpisů, zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů, zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších

předpisů, zákon č. 499/2004 Sb., o archivnictví a spisové službě a změně některých zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), vyhláška o 317/2014 Sb., vyhláška o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů, zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, Nařízení (EU) 2016/679 (GDPR), zákon č. 110/2019 Sb., o zpracování osobních údajů, zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů a zákon č. 261/2021, zákon, kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci.

Čl. 11
Závěrečná ustanovení

11.1 Práva a povinnosti Smluvních stran, pokud nejsou upraveny touto Smlouvou, se řídí Občanským zákoníkem a souvisejícími právními předpisy.

11.2 Veškeré případné spory vzniklé mezi Smluvními stranami na základě nebo v souvislosti s touto Smlouvou budou primárně řešeny jednáním Smluvních stran. V případě, že tyto spory nebudou v přiměřené době vyřešeny, budou k jejich projednání a rozhodnutí příslušné obecné soudy České republiky.

11.3 Poskytovatel bezvýhradně souhlasí se zveřejněním své identifikace a celého znění této Smlouvy včetně Ceny v souladu s příslušnými právními předpisy.

11.4 Tato Smlouva může být měněna nebo doplňována pouze (vyjma případu uvedeném v Čl. 7 odst. 7.5 a 7.6 této Smlouvy) formou písemných vzestupně číslovaných dodatků podepsaných oběma Smluvními stranami. Ke změnám či doplnění neprovedeným písemnou formou se nepřihlíží.

11.5 V případě, že některé ustanovení této Smlouvy je nebo se stane v budoucnu neplatným, neúčinným či nevymahatelným nebo bude-li takovým shledáno příslušným orgánem, zůstávají ostatní ustanovení této Smlouvy v platnosti a účinnosti, pokud z povahy takového ustanovení nebo z jeho obsahu anebo z okolností, za nichž byla tato Smlouva uzavřena, nevyplývá, že jej nelze oddělit od ostatního obsahu této Smlouvy. Smluvní strany se zavazují bezodkladně nahradit neplatné, neúčinné nebo nevymahatelné ustanovení této Smlouvy ustanovením jiným, které svým obsahem a smyslem odpovídá nejlépe ustanovení původnímu a této Smlouvě jako celku.

11.6 Smluvní strany na sebe přebírají nebezpečí změny okolností v souvislosti s právy a povinnostmi Smluvních stran vzniklými na základě této Smlouvy. Smluvní strany vylučují uplatnění ustanovení § 1765 odst. 1, § 1766 a § 2620 Občanského zákoníku na svůj smluvní vztah založený touto Smlouvou.

11.7 Tato Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem jejího uveřejnění v Informačním systému Registr smluv (dále jen „**IS RS**“), za podmínek stanovených zákonem č. 340/2015 Sb., zákon o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Poskytovatel bezvýhradně souhlasí s uveřejněním celého znění této Smlouvy v IS RS a na profilu Objednatele, jakožto zadavatele, popř. dalších místech v souladu s příslušnými právními předpisy. Uveřejnění této Smlouvy na právními předpisy požadovaných místech provede Objednatel.

11.8 Je-li tato Smlouva uzavřena v listinné podobě, pak je vyhotovena ve 3 stejnopisech, z nichž každý bude považován za prvopis, a Objednatel si ponechá 2stejnopisy a Poskytovatel obdrží 1 stejnopis. Je-li tato Smlouva podepsána elektronicky, pak je podepsána v 1 originále elektronicky pomocí uznávaných elektronických podpisů osob oprávněných jednat za Smluvní strany.

11.9 Nedílnou součástí této Smlouvy jsou její přílohy:

a) Příloha č. 1: Dokumentace EnviIAM,

b) Příloha č. 2: Dokumentace CRŽP.

Smluvní strany prohlašují, že tuto Smlouvu prostudovaly, rozumějí jí a souhlasí se závazností všech ustanovení. Toto znění Smlouvy vyjadřuje jejich svobodné, vážné, určitě a srozumitelně míněné vůle.

Za Objednatele:	Za Poskytovatele:
V Praze, dne ……	V Liberci, dne ……
Ing. Jana Vodičková Digitálně podepsal Ing. Jana Vodičková Datum: 2021.11.23 08:17:44 +01'00'	Ing. David Mareček Digitálně podepsal Ing. David Mareček Datum: 2021.11.22 15:24:42 +01'00'
……	……
Česká republika – Ministerstvo životního prostředí	**INISOFT s.r.o.**
Ing. Jana Vodičková ředitelka odboru informatiky	Ing. David Mareček jednatel

Příloha 1: Specifikace – Dokumentace EnviIAM

(následuje)

Integrace aplikací na EnviAM – AM

v 2.0

Ministerstva životního prostředí České republiky

Název projektu	**EnviIAM**
Objednatel	**Česká republika – Ministerstvo životního prostředí** IČ: 00164801 Vršovická 1442/65, 100 10 PRAHA 10
Dodavatel	**AMI Praha a.s.** IČ: 25715909 Hanusova 29, 140 00 Praha 4

VERZE	DATUM	POPIS ZMĚN	AUTOR	STATUS
0.1	14. 2. 2021	První verze k připomínkování	Jan Smutný	draft
0.2	24. 2. 2021	Úprava na základě komentářů, odpovědi na komentáře	Jan Smutný	draft
0.3	1. 3. 2021	Doplnění úvodní části (kap. 3.1)	Jan Smutný	draft
1.0	2. 3. 2021	Finalizace	Jan Smutný	final
1.1	29. 6. 2021	Úprava kapitoly 5 Odhlášení – doplnění parametru služby odhlášení *service*	Jan Smutný	final
1.2	13. 7. 2021	Doplnění kapitoly Doporučení	Petr Jančík	draft
2.0	19. 7. 2021	Schválení nové verze	Jan Vácha	final

Obsah

Seznam obrázků

1 ÚVOD

EnviAM je systém poskytující autentizační službu pro uživatele IS/AIS systémů Ministerstva životního prostředí ČR registrovaných v systému CRŽP. EnviAM provádí buď interní vícefaktorovou autentizaci uživatelů vůči systému CRŽP nebo umožňuje delegovat autentizaci na externí poskytovatele identit, aktuálně jsou to tyto: NIA, mojeID a JIP/KAAS. Počítá se však s připojením dalších externích poskytovatelů identit. Autentizační služba je poskytována pouze prostřednictvím webového uživatelského rozhraní.

IS/AIS systémy MŽP tak používají EnviAM k autentizaci uživatelů přistupujících prostřednictvím webového rozhraní. V případě, že jsou služby IS/AIS systémů MŽP využívány prostřednictvím dalších Aplikací, tj. systémů externích subjektů, je nutné, aby tyto systémy externích subjektů v případě volání služeb IS/AIS použily též identitu uživatele získanou z EnviAM. Z tohoto důvodu je nutné, aby tyto Aplikace využívající služeb IS/AIS systémů MŽP (ISPOP v2, CRŽP, …) byly s EnviAM integrovány, tj. uměly přesměrovat uživatele na EnviAM k autentizaci, převzít identitu daného uživatele a předat ji volané službě IS/AIS systému MŽP.

2 POUŽITÉ ZKRATKY A POJMY

Zkratka	Význam
Aplikace	Systém externího subjektu, který z důvodu komunikace s IS/AIS MŽP musí být integrován s EnviAM.
Autentizace uživatele	Ověření identifikačních údajů uživatele, např. zadáním hesla, případě vícefaktorovou autentizací, tj. zadáním dalších informací. Zpravidla se v rámci procesu autentizace počítá i procesem identifikace.
CRŽP	Agendový informační systém (AIS) Centrální registr životního prostředí. CRŽP poskytuje služby a data ostatním agendovým informačním systémům MŽP (IS/AIS), které primárně zabezpečují služby elektronického podání (hlášení) k dotčeným agendám.
EnviAM	Poskytovatel identity (IdP), který poskytuje službu autentizace uživatele a získání jeho identity pro IS/AIS MŽP a systémy externích subjektů, které chtějí volat systémy IS/AIS.
EnviIAM	Projekt, jehož cílem je dodávka autentizačního systému (poskytovatele identity) EnviAM-AM a systému pro správu identit EnviIAM - IdM.
Externí IdP	Externí poskytovatel identity (IdP – Identity Provider), jedná se o systémy třetích stran, které poskytují služby autentizace a které umí EnviAM využít k autentizaci uživatele.
Externí uživatel	Uživatel, který přistupuje k systémům IS/AIS MŽP, buď přímo prostřednictvím webového rozhraní těchto systémů nebo nepřímo prostřednictvím systému externího subjektu, který používá služby těchto IS/AIS.
Externí subjekt	Subjekt, který používá systémy IS/AIS MŽP (ISPOP v2, CRŽP).
HNVO	Systém IS/AIS – systém Hodnocení nebezpečných vlastností odpadů.
IdP (Identity provider)	Obecně poskytovatel identity, představuje buď aplikaci EnviAM nebo externí poskytovatel identity (NIA, mojeID, JIP/KAAS).
IPO	Systém IS/AIS – informační Portál odborně způsobilých osob
IS	Informační systém
ISOH	Systém IS/AIS – informační systém odpadového hospodářství.
ISPOP	Systém IS/AIS – agendový informační systém Integrovaného systému plnění ohlašovacích povinností v oblasti životního prostředí.
ISDS	Informační systém datových schránek
ISZR	Informační systém základních registrů
MFA (vícefaktorová autentizace)	Zvýšení důvěryhodnosti procesu autentizace poskytnutím dvou nebo více důkazů (faktorů) potvrzujících identitu uživatele: znalost (něco, co ví pouze uživatel, např. heslo), vlastnictví (něco, co má pouze uživatel - telefon, email) a charakteristika (něco, čím je pouze daný uživatel - biometrie). V rámci tohoto projektu se zatím uvažuje o dvoufaktorové autentizaci, kdy prvním faktorem je heslo uživatele a druhým faktorem je jednorázové heslo s omezenou časovou platností (OTP) zaslané uživateli prostřednictvím SMS nebo email zprávy.
MŽP	Ministerstvo životního prostředí ČR
OIDC (OpenID Connect)	Ověřovací protokol postavený na protokolu OAuth 2.0, který je používán k bezpečné výměně autentizačních a autorizačních dat mezi zúčastněnými stranami, tj. poskytovatelem služeb a poskytovatelem identity. Je vyvíjen organizací OpenID.
SAML	Standard založený na XML poskytující mechanismus pro výměnu autentizačních a autorizačních dat mezi zúčastněnými stranami, tj. poskytovatelem služeb a poskytovatelem identity. Je vyvíjen organizací OASIS.
SEPNO	Systém IS/AIS – systém evidence přepravy nebezpečných odpadů.
SLO	Single logout – jednotné odhlášení, pokud je zavolána tato služba, dojde k odhlášení ze všech aplikací, ke kterým je uživatel přihlášen a které podporují SLO.
SSO	Single sign-on – jednotné přihlášení, uživatel zadává přihlašovací údaje pouze jednou, pokud přejde do jiných aplikací, použije se aktuální přihlášení uživatele.
Systém externího subjektu	Subjekt, který používá systémy IS/AIS systémovým způsobem, tj. nepřistupuje k nim uživatel, ale jsou volány externím systémem.
Systémy IS/AIS	Jedná se o systémy Objednatele, které budou s aplikací EnviAM integrovány, tj. budou využívat její služby poskytování identity. Jedná se o systémy ISOH, IPO, EnviHELP, HNVO, SEPNO, ISPOP v2 a CRŽP.

Zkratka	Význam
UUID	Globálně jednoznačný identifikátor, 128bitové číslo zapisované jako 32 šestnáctkových číslic, zobrazených v 5 skupinách oddělených spojovníky, ve tvaru 8-4-4-4-12 pro celkem 36 znaků. Bude sloužit jako jednoznačný identifikátor uživatele.

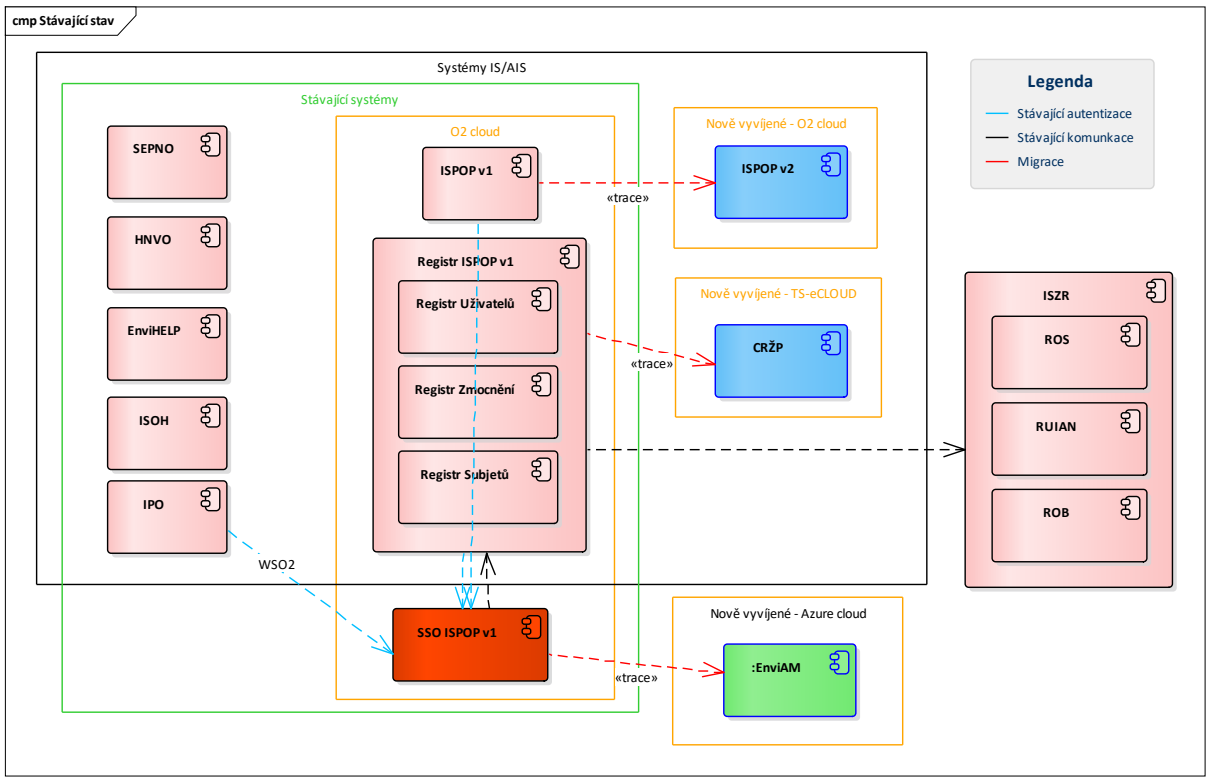
3 POPIS AUTENTIZAČNÍ INFRASTRUKTURY PRO EXTERNÍ UŽIVATELE

3.1 STÁVAJÍCÍ ARCHITEKTURA AUTENTIZAČNÍ INFRASTRUKTURY

Stávající architektura řešené domény zachycená na následujícím obrázku 1 se skládá se ze současných systémů IS/AIS MŽP, které používají externí uživatelé k vykonávání předepsaných (legislativních) agend. Jedná se zejména o systémy ISPOP v1, ISOH, IPO, HNVO, SEPNO a EnviHELP.

V rámci modernizace infrastruktury MŽP probíhá v současnosti implementace nové architektury, která postupně nahradí stávající řešení ISPOP v1. V rámci této modernizace bude ve zjednodušeném pohledu Registr ISPOP v1 nahrazen Centrálním registrem životního prostředí (CRŽP) a systém ISPOP v1 bude nahrazen systémem ISPOP v2. Vzhledem k tomu, že MŽP poskytuje externím uživatelům několik aplikací (systémů), ke kterým se musí uživatelé řádně autentizovat, je nutné doplnit novou architekturu centrálním autentizačním systém. Ten umožní externím uživatelům jednotné přihlašování (SSO) k poskytovaným systémům (uživatel se přihlásí/autentizuje jen jednou a následně může přecházet mezi systémy bez opakovaného přihlášení). Současně zavedení centrálního autentizačního systému umožní zavedení a prosazení jednotné politiky přihlášení včetně (s ohledem na požadavky na zabezpečení a úroveň autentizace uživatelů) zavedení vícefaktorové autentizace (MFA). Klíčovou úlohou centrálního autentizačního systému je také jednotná a řízená integrace na vybrané externí poskytovatele identit (JIP/KAAS, NIA, mojeID a v budoucnu další), kteří poskytnou externím uživatelům možnost identifikovat se a autentizovat pomocí sofistikovaných autentizačních metod (např. certifikáty).

Tento centrální autentizační systém, který je předmětem této specifikace (viz též obrázek) je nazýván EnviIAM – část AM (EnviAM).



Obrázek 1: Stávající architektura autentizační infrastruktury

3.2 ARCHITEKTURA AUTENTIZAČNÍ INFRASTRUKTURY ENVIAM

Autentizační infrastruktura EnviAM slouží jako poskytovatel identity pro systémy IS/AIS MŽP a systémy externích subjektů (Aplikace), které s těmito IS/AIS komunikují, viz následující Obrázek 2: Architektura autentizační infrastruktury.

Pokud chce uživatel používat nějaký ze systémů IS/AIS MŽP prostřednictvím webového rozhraní a nemá vytvořeno s tímto systémem uživatelské aplikační sezení, přesměruje systém uživatele na EnviAM. EnviAM provede autentizaci buď přímo, prostřednictvím zadaných autentizačních údajů od uživatele a jejich ověřením

vůči CRŽP, včetně ověření dalším faktorem, anebo nepřímo delegací uživatele na některého z podporovaných externích IdP (aktuálně NIA, mojeID, JIP/KAAS). Následně EnviAM předá původnímu IS/AIS, ke kterému uživatel přistupoval, identitu autentizovaného uživatele. Zprostředkování žádosti o identitu a její vrácení je provedeno jedním z podporovaných protokolů SAML2 nebo OIDC.

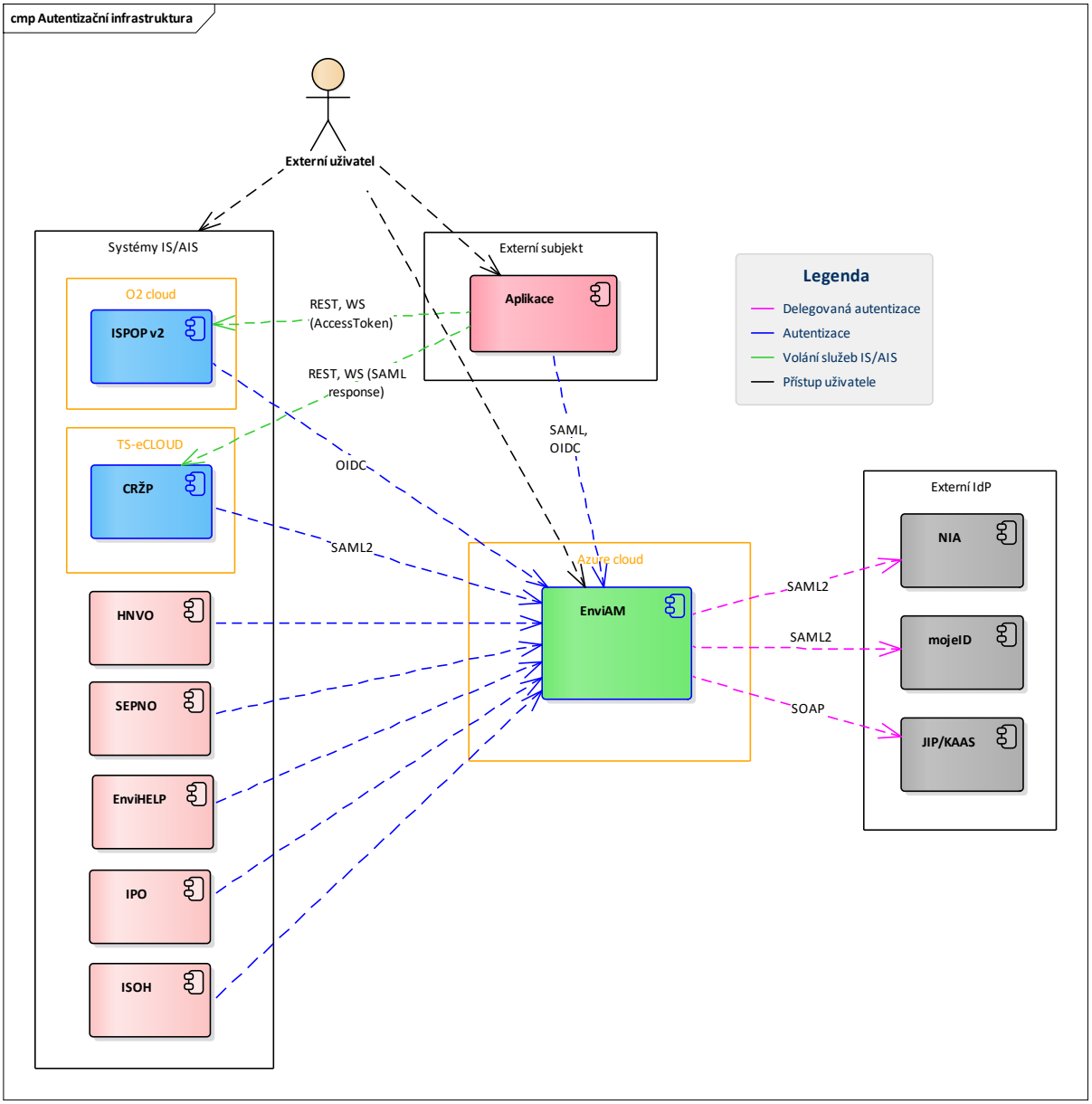
Pokud chce Aplikace zavolat službu IS/AIS MŽP, musí získat identitu uživatele z EnviAM a následně tuto identitu předat příslušným způsobem volané službě IS/AIS. Vzhledem k tomu, že existují dva typy autentizačních protokolů SAML2 a OIDC, které jsou používané systémy IS/AIS, je nutné při integraci na konkrétní IS/AIS MŽP zjistit, jaký autentizační protokol daný IS/AIS podporuje a tento protokol použít pro získání identity od EnviAM.

Detaily integrace prostřednictvím těchto protokolů jsou popsány v následující kapitole 4 Integrace s EnviAM.

Základními vlastnostmi EnviAM jsou:

- Provádí autentizaci uživatele prostřednictvím autentizačních údajů v CRŽP, včetně vícefaktorové autentizace zasláním ověřovacího kódu prostřednictvím SMS nebo e-mail zprávy na kontaktní údaje zadané v CRŽP; v případě chybějících informacích pro odeslání druhého faktoru informuje uživatele o nutnosti jejich doplnění v CRŽP,
- poskytuje možnost delegované autentizace prostřednictvím externích IdP NIA, mojeID, JIP/KAAS,
- poskytuje SSO (single sign on) a SLO (single logout),
- podporuje protokoly SAML a OIDC pro systémy IS/AIS a systémy externích subjektů,
- provádí autorizaci přístupu uživatele k IS/AIS,
- poskytuje identitu přihlášeného uživatele a jeho základní atributy IS/AIS a systémům externích subjektů.

Externí uživatel (v tomto dokumentu jen zkráceně uživatel) představuje uživatele, který přistupuje k systémům IS/AIS Ministerstva životního prostředí. Uživatel tedy v tomto kontextu představuje uživatele, který má v CRŽP definovány role pro přístup k systémům IS/AIS MŽP. Fyzicky takovým uživatelem může být interní pracovník (zaměstnanec) MŽP, osoba spolupracující s MŽP nebo uživatel externího subjektu, který v rámci přidělené činnosti přistupuje k systémům IS/AIS.



Obrázek 2: Architektura autentizační infrastruktury

4 INTEGRACE S ENVIAM

EnviAM jako poskytovatel identity (IdP) poskytuje rozhraní standardizovaných protokolů SAML 2.0 a OpenID Connect 1.0 (OIDC) ke zprostředkování žádosti o autentizaci uživatele a předání jeho identity včetně dalších atributů. Každá Aplikace, která chce používat služby systémů IS/AIS musí při volání těchto služeb předat i identitu aktuálně přistupujícího uživatele získanou právě od EnviAM.

Autorizace nebude pro systémy externích subjektů (Aplikace) prováděna.

V rámci poskytování identity poskytuje EnviAM i službu jednotného přihlášení (SSO). Uživatel se v rámci definovaného intervalu platnosti SSO sezení přihlašuje prostřednictvím EnviAM pouze jednou. Po přihlášení uživatele do EnviAM je vytvořeno SSO sezení s uživatelem a v případě dalších požadavků na získání identity tohoto uživatele již není požadována opakovaná autentizace. EnviAM poskytne identitu uživatele získanou v rámci vytvořeného SSO sezení.

4.1 ATRIBUTY UŽIVATELE

V rámci předávání identity uživatele mezi EnviAM a systémem IS/AIS nebo Aplikací, jsou předávány atributy uživatele z registračních údajů uložených v CRŽP, kromě atributu *JIP/KAAS role*, který bude předán pouze v případě autentizace uživatele prostřednictvím IdP JIP/KAAS. Konkrétní podoba atributů pro dané protokoly a jejich výčet je uveden v kapitolách 4.3.4 a 4.4.4 Identifikátor a atributy uživatele.

Seznam základních (společných) atributů je následující:

Atribut	Název atributu	Poznámky
Jednoznačný identifikátor uživatele	Závisí na použitém protokolu viz kapitoly 4.3.4 a 4.4.4	Představuje jednoznačnou identifikaci uživatele v CRŽP.
Login jméno	login	Přihlašovací jméno, bude k dispozici v případě autentizace prostřednictvím CRŽP a dále při autentizaci prostřednictvím externího IdP, jen v případě, že bude poskytnuto.
Jméno uživatele	given_name	
Příjmení uživatele	family_name	
Celé jméno uživatele včetně titulů	full_name	
E-mail uživatele	email	Email uživatele, který je použit při registraci jako kontaktní údaj (tj. nikoli email pro zasílání ověřovacího kódu MFA).
Telefonní číslo	phone	Telefonní číslo uživatele, které je použito při registraci jako kontaktní údaj (tj. nikoli telefonní číslo pro zasílání ověřovacího kódu MFA).
JIP/KAAS role	role_rpp	Seznam JIP/KAAS rolí uživatele z RPP, bude k dispozici pouze v případě autentizace uživatele prostřednictvím externího IdP JIP/KAAS a uživatel bude mít v RPP tyto role přiděleny.
Úroveň ověření uživatele	loa	Úroveň ověření uživatele u externího IdP (NIA, mojeID).

4.2 URL ADRESY ENVIAM

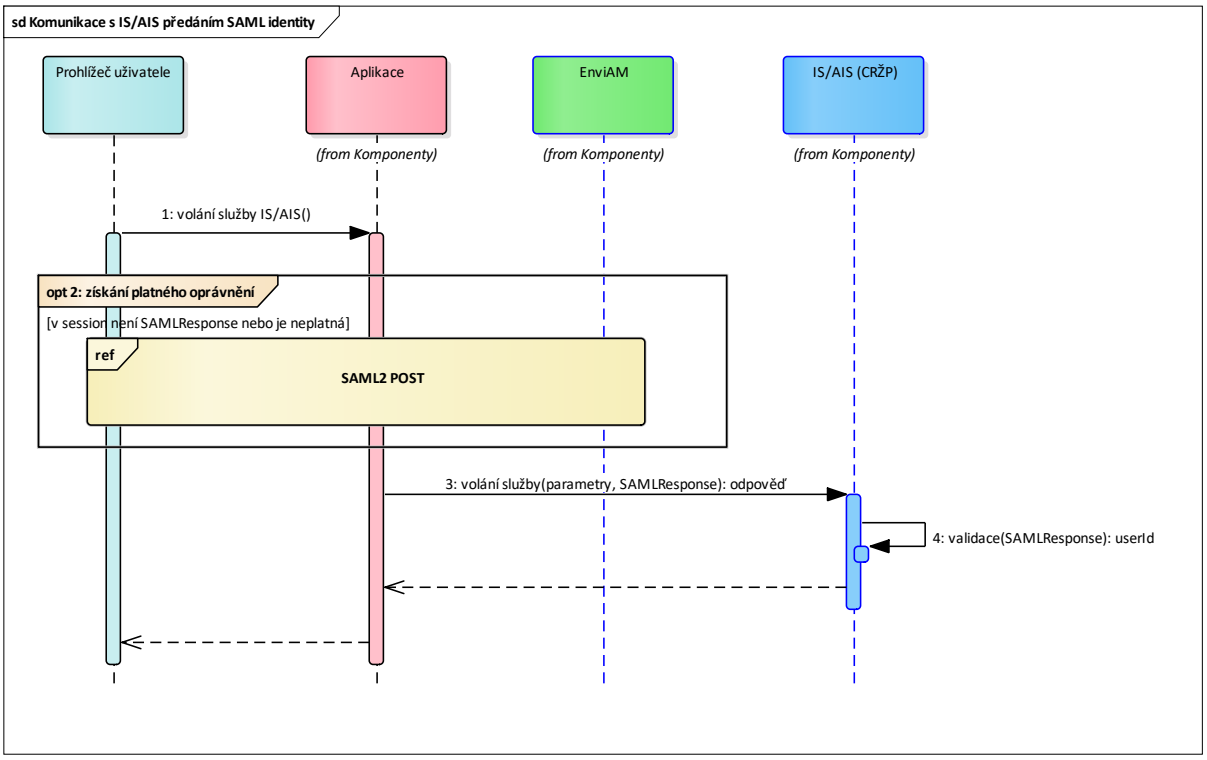
V následujícím popisu je základní URL adresa systému EnviAM nahrazena řetězcem *{ENVIAM_SERVER}*. Tento řetězec je nahrazen v testovacím prostředí řetězcem https://t-iam.env.cz/cas v produkčním prostředí https://iam.env.cz/cas

4.3 VOLÁNÍ SLUŽBY IS/AIS POUŽÍVAJÍCÍHO SAML2

EnviAM poskytuje služby autentizace s použitím protokolu SAML2. Klíčovým systémem využívajícím tento protokol je CRŽP.

4.3.1 POPIS ZPŮSOBU INTEGRACE

V případě, že IS/AIS volaný Aplikací požaduje předání identity uživatele ve formě SAMLResponse, je nutné provést komunikaci s EnviAM pro získání identity uživatele prostřednictvím protokolu SAML, viz následující Obrázek 3.



Obrázek 3: Volání IS/AIS vyžadujícího identitu SAMLResponse

Scénář komunikace (integrace) je následující:

1. Uživatel v Aplikaci chce provést operaci, která vyžaduje volání služby IS/AIS MŽP.
2. Aplikace se podívá, zda je v aplikačním sezení uživatele uložena platná identita uživatele ve formě SAMLResponse, tj. kde datum a čas nepřekročil hodnotu `//SubjectConfirmationData/@NotOnOrAfter`. Pokud SAMLResponse neexistuje nebo není platná, získá aktuální SAMLResponse uživatele od EnviAM prostřednictvím protokolu SAML2. Scénář získání SAMLResponse je popsán v kapitole 4.3.3.
3. Aplikace zavolá službu IS/AIS a SAMLResponse předá v HTTP hlavičce volání `Authorization: SAML <SAML Response>` kódovanou prostřednictvím BASE64.
4. IS/AIS ověří SAMLResponse a získá z ní identitu uživatele, který daný IS/AIS volá. Pokud má uživatel oprávnění na danou službu, provede požadovanou operaci a vrátí výsledek.

4.3.2 POPIS SAML2 SLUŽEB ENVIAM

EnviAM poskytuje SAML2 službu *{ENVIAM_SERVER}/idp/metadata*, která vrací metadata (konfiguraci) SAML2 protokolu v EnviAM, jako např. certifikát, kterým je podepsána SAML odpověď, URL jednotlivých služeb, jméno IdP apod. Parametry jednotlivých služeb jsou definovány v příslušném standardu http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.

EnviAM podporuje protokol SAML 2.0. V rámci tohoto protokolu podporuje tyto typy profilů (binding) pro SSO a SLO:

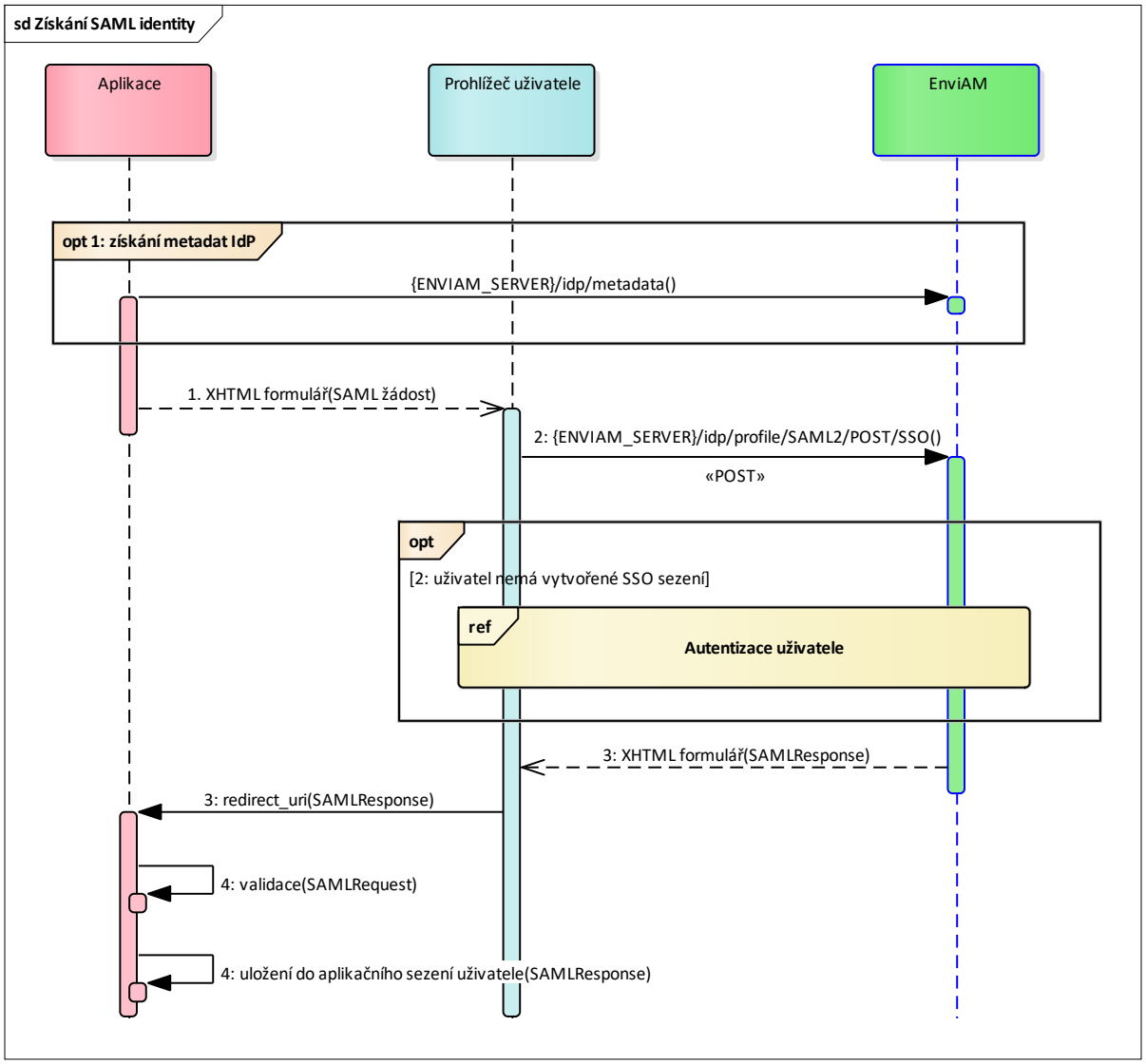
- HTTP Redirect Binding
- HTTP POST Binding.

Vzhledem k možným rizikům (bezpečnostním a technickým) při předávání SAML žádosti a odpovědi přes HTTP Redirect – tj. metodou HTTP GET, je preferována varianta HTTP POST Binding.

4.3.3 *Získání SAML identity*

Aplikace pro získání SAML identity ve formě SAMLResponse musí provést komunikaci s EnviAM prostřednictvím SAML2 protokolu dle standardu http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.

Z pohledu bezpečnosti je nejvhodnější použít metodu HTTP POST Binding, jelikož předání SAML požadavku a odpovědi probíhá v těle požadavku, nikoli v URL. Postup volání prostřednictvím této metody je následující:



Obrázek 4: Získání identity uživatele prostřednictvím SAML2 HTTP POST.

1. Aplikace může získat od EnviAM metadata IdP, která obsahují podepisovací a šifrovací certifikáty (jejich veřejné části), URL adresy jednotlivých endpointů (služeb) a další důležité informace se kterých vytvoří SAML žádost.
   Aplikace vytvoří SAML žádost (AuthhRequest), kterou elektronicky podepíše, viz příklad:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="identifier_1"
    Version="2.0"
    IssueInstant="2004-12-05T09:21:59Z"
    AssertionConsumerServiceIndex="0">
    <saml:Issuer>{SERVICE_URL}</saml:Issuer>
    <samlp:NameIDPolicy
      AllowCreate="true"
```

```
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
</samlp:AuthnRequest>
```

SAML žádost vrátí prohlížeči uživatele ve formě formuláře. Ve formuláři je cílové URL EnviAM.

```
<form method="post" action="https://t-iam.env.cz/cas/idp/profile/SAML2/POST/SSO" ...>
    <input type="hidden" name="SAMLRequest" value="SAML žádost" />
    <input type="hidden" name="RelayState" value="token" />
    ...
    <input type="submit" value="Submit" />
  </form>
```

Formulář je okamžitě odeslán (prostřednictvím JavaScriptu) na zadané URL EnviAM a v těle požadavku je předán obsah SAML požadavku v kódování Base64.

2. Na EnviAM jde HTTP POST požadavek se SAML žádostí:

```
POST /cas/idp/profile/SAML2/POST HTTP/1.1
Host: {ENVIAM_SERVER}
Content-Type: application/x-www-form-urlencoded
Content-Length: nnn

SAMLRequest=saml žádost&RelayState=token
```

EnviAM obdrží požadavek a ověří, zda je již uživatel přihlášen – tj. je vytvořeno SSO sezení s uživatelem. Pokud neexistuje platné SSO sezení s uživatelem, je uživatel autentizován a je vytvořeno sezení. Vlastní průběh autentizace je definován v samostatném diagramu. Pokud byl již autentizován a SSL sezení je platné, je identita uživatele automaticky získána z tohoto sezení.

Následně je vytvořena SAML odpověď, do které je vložena identita uživatele, viz příklad odpovědi včetně atributů v příloze 7.1. Důležitým atributem je NameID, což je UUID identifikátor uživatele v CRŽP. V rámci odpovědi jsou předány i další základní atributy uživatele (např. jméno, příjmení, email). SAML odpověď je podepsána certifikátem EnviAM.

3. Uživatel je pomocí formuláře přesměrován na Aplikaci společně se SAML odpovědí (SAMLResponse), která je v těle požadavku.
4. Aplikace provede validaci SAML odpovědi a uloží ji do sezení uživatele po dobu platnosti, jejíž datum je v atributu SAMLRespose `//SubjectConfirmationData/@NotOnOrAfter`.

4.3.4 *IDENTIFIKÁTOR A ATRIBUTY UŽIVATELE*

Jednoznačný identifikátor uživatele UUID v CRŽP je předán prostřednictvím standardního elementu `<saml2:NameID>`, viz příklad:

```
<saml2:NameID                    Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
NameQualifier="crzp.inqool.cz"       SPNameQualifier="crzp.inqool.cz">123e4567-e89b-12d3-a456-
426655440000</saml2:NameID>
```

Ostatní atributy budou předány v SAML odpovědi v bloku `<saml2:AttributeStatement>`, ukázka atributů SAML odpovědi je v příloze 7.1 Ukázka SAML odpovědi. Seznam základních atributů je definován v kapitole 4.1 Atributy uživatele.

4.3.5 *CHYBOVÉ SITUACE A JEJICH ŘEŠENÍ*

Uživatel je přesměrován na daný IS/AIS pouze v případě, že dojde k úspěšné autentizaci uživatele. V případě jakékoli chyby je její zpracování a informování uživatele plně v režii EnviAM.

4.3.6 *POSTUP PŘIPOJENÍ K ENVIAM*

1. Dodavatel Aplikace prozkoumá SAML metadata IdP testovacího EnviAM na adrese https://t-iam.env.cz/cas/idp/metadata. Z nich zjistí potřebné informace, jako URL jednotlivých endpointů služeb IdP, veřejné části klíčů určených k podepisování a případně šifrování SAML odpovědí, profily, apod.
2. Dodavatel Aplikace předá správci EnviAM:
    a. URL testovací aplikace, na které bude uživatel přesměrován z testovacího EnviAM,

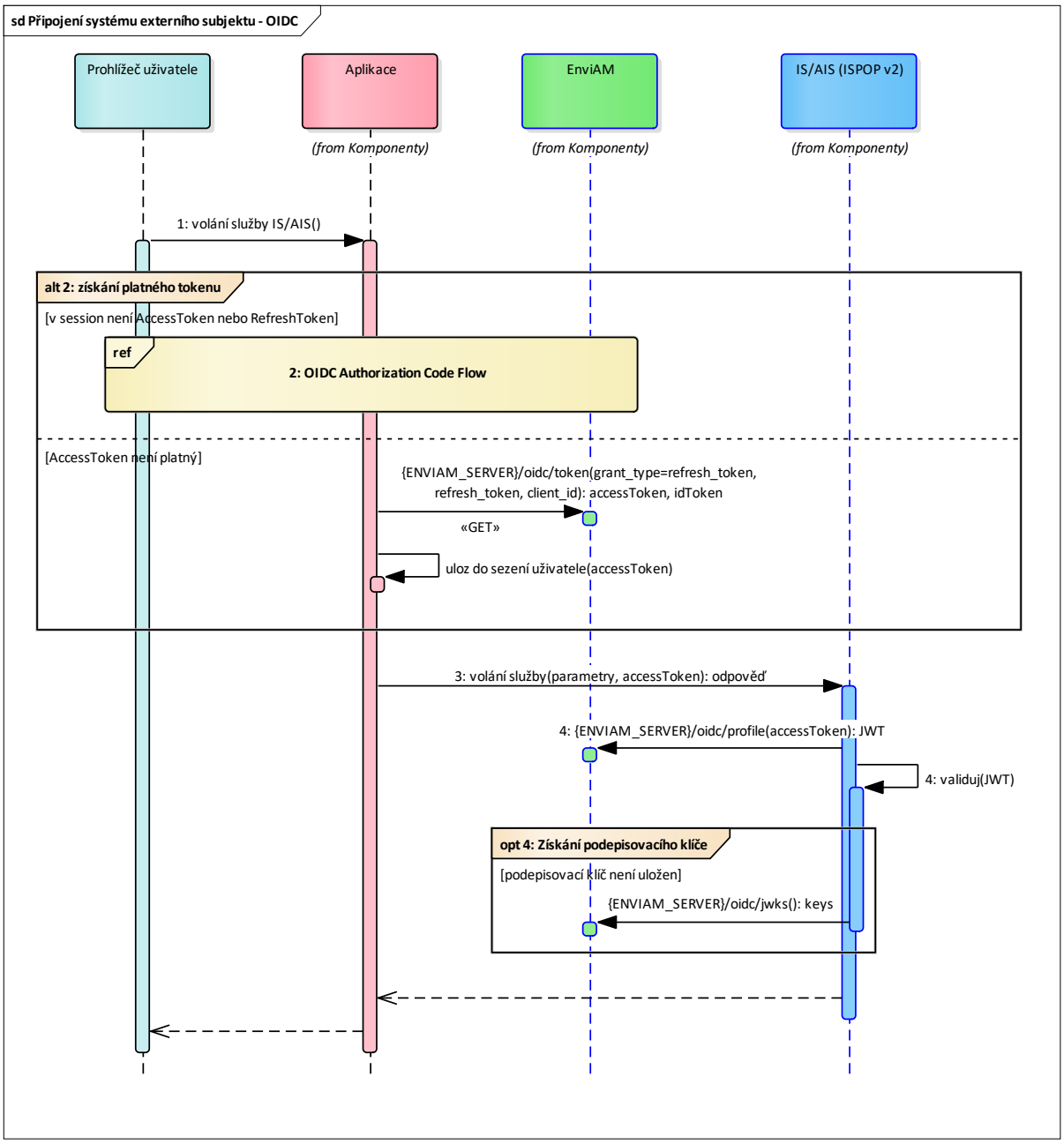
   b. veřejnou část certifikátu, která bude sloužit k podepisování SAML požadavku.
3. Správce EnviAM provede registraci aplikace v testovacím EnviAM.
4. Dodavatel otestuje komunikaci a v případě problémů kontaktuje správce EnviAM a sdělí mu odpověď, která mu byla od EnviAM vrácena (http response) a přesný čas provedení testu.
   a. Správce analyzuje problém a provede buď opravu vlastní konfigurace nebo sdělí důvod, proč nebyl požadavek akceptován.
   b. Případně může proběhnout vzájemná intenzivnější komunikace a spolupráce na odhalení příčiny problému.
5. Dodavatel provede otestování své Aplikace, zejména integraci na IS/AIS a správnou autentizaci volaných služeb IS/AIS.
6. Dodavatel zopakuje kroky 1 – 4 pro produkční prostředí Aplikace a EnviAM.

4.4 VOLÁNÍ SLUŽBY IS/AIS POUŽÍVAJÍCÍHO OIDC

EnviAM poskytuje služby autentizace s použitím protokolu OIDC. Klíčovým systémem využívajícím tento protokol je ISPOP2.

4.4.1 POPIS ZPŮSOBU INTEGRACE

V případě, že volaný IS/AIS požaduje v rámci volání služby předání identity uživatele ve formě OIDC Access tokenu, je nutné provést komunikaci s EnviAM pro získání identity uživatele ve formě Access tokenu prostřednictvím protokolu OpenID Connect (OIDC), viz následující Obrázek 5: Volání IS/AIS vyžadujícího OIDC Access token.



Obrázek 5: Volání IS/AIS vyžadujícího OIDC Access token

Scénář komunikace (integrace) je následující:

1. Uživatel v Aplikaci chce provést operaci, která vyžaduje volání služby IS/AIS MŽP.
2. Aplikace zjistí, zda je v aplikačním sezení uživatele uložen platný Access token a Refresh token. Pokud ne, odešle EnviAM žádost o Access token a Refresh token prostřednictvím OIDC protokolu. Scénář komunikace je popsán v následujících kapitolách. Pokud je Access token neplatný, ale je k dispozici Refresh token, zavolá službu EnviAM */oidc/token*, která na základě předaného Refresh tokenu a dalších parametrů, vydá nový, platný Access token, který uloží do sezení uživatele.
3. Aplikace zavolá službu IS/AIS a předá Access token v HTTP hlavičce volání `Authorization: Bearer <AccessToken>`.
4. IS/AIS zavolá službu EnviAM, které předá Access token a získá identitu uživatele ve formátu JWT. Provede validaci JWT a případně, pokud nemá klíč k ověření JWT, může ho od EnviAM získat prostřednictvím služby */oidc/jwks*. Pokud je validace úspěšná a uživatel smí volat danou službu, provede služba příslušnou operaci a vrátí příslušná data.

4.4.2 *POPIS OIDC SLUŽEB ENVIAM*

EnviAM poskytuje službu *{ENVIAM_SERVER}/oidc/.well-known*, která vrací metadata (konfiguraci) OIDC protokolu, tj. informace o IdP, URL jednotlivých služeb, podepisovací a šifrovací klíče apod.

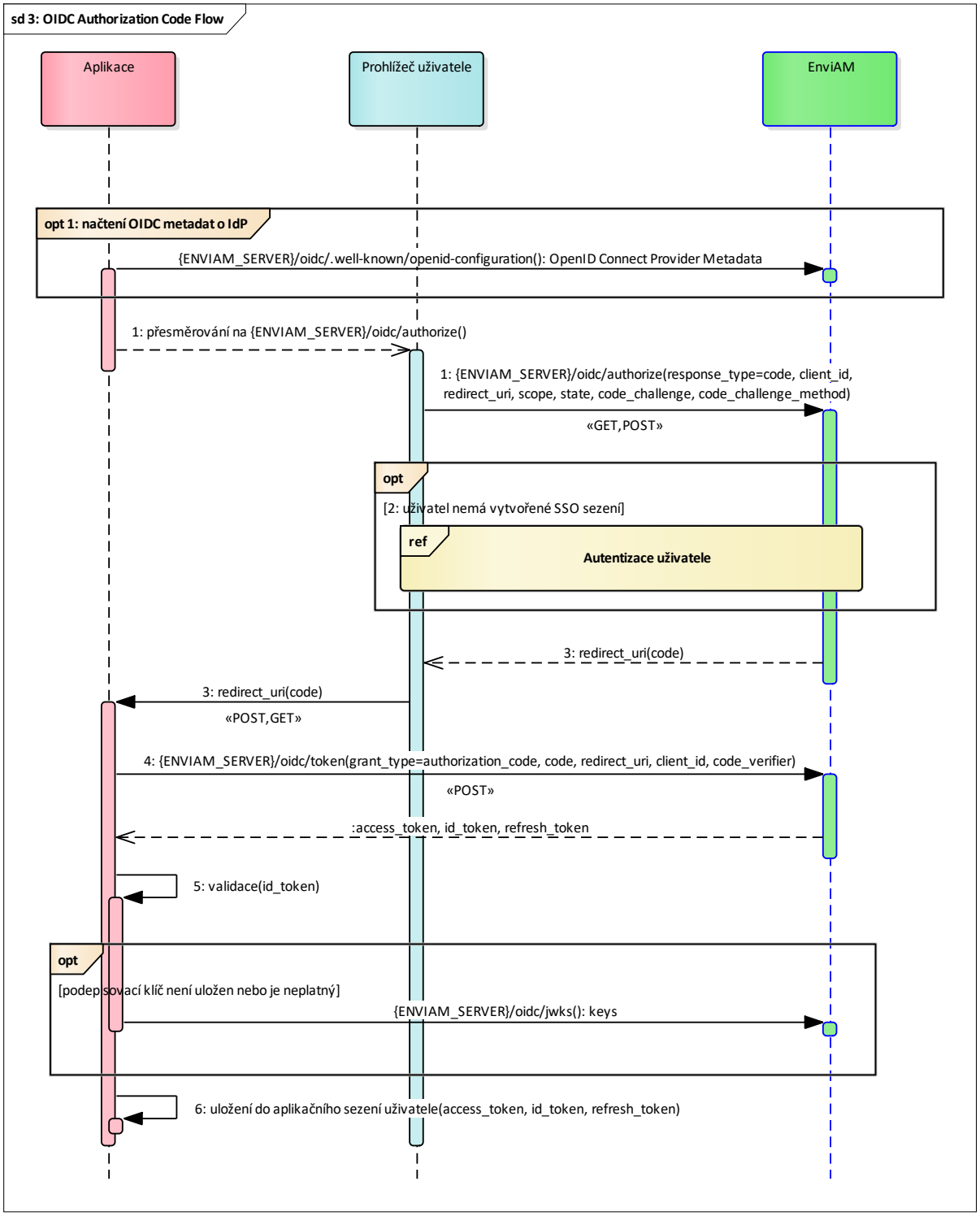
EnviAM podporuje protokol OIDC 1.0. V rámci tohoto protokolu podporuje tyto způsoby předání identity uživatele:

- Authorization Code Flow
- Implicit Flow

Z důvodu bezpečnosti doporučujeme používat pouze metodu Authorization Code Flow rozšířenou o **PKCE** (Proof Key for Code Exchange), což je bezpečnostní rozšíření proti některým útokům na protokol. Parametry jednotlivých služeb jsou definovány v příslušném standardu https://openid.net/specs/openid-connect-core-1_0.html.

4.4.3 *Získání OIDC identity metodou Authorization Code Flow*

Předání identity uživatele prostřednictvím standardizovaného způsobu OIDC Authorization code flow probíhá níže uvedeným způsobem:



Obrázek 6: Získání identity uživatele a Access tokenu prostřednictvím OIDC Authorization Code Flow.

1. Aplikace může získat od EnviAM voláním služby *{ENVIAM_SERVER}/oidc/.well-known* metadata IdP, která obsahují podepisovací a šifrovací certifikáty (jejich veřejné části), URL adresy jednotlivých

endpointů a další důležité informace.
Aplikace přesměruje uživatele (POST nebo GET) na službu EnviAM */oidc/authorize*, které předá tyto parametry:

- *response_type=code* – definuje metodu předání identity Authorization Code Flow,
- *client_id* – identifikace klienta (externího IS/AIS),
- *redirect_uri* – URL externího IS/AIS, na které bude uživatel přesměrován po autentizaci,
- *scope* – identifikace, jaký rozsah atributů uživatele aplikace vyžaduje,
- *state* – náhodně vygenerovaný identifikátor,
- *code_challenge, code_challenge_method* – hodnoty PKCE rozšíření.

2. EnviAM v případě, že uživatel není autentizován nebo je SSO sezení neplatné, provede jeho autentizaci. V případě, že je uživatel autentizován, tj. existuje platné SSO sezení, autentizace se již neprovádí.
3. EnviAM přesměruje uživatele zpět na Aplikaci na URL dané v parametru *redirect_uri* a předá autorizační kód *code*.
4. Aplikace zavolá službu EnviAM */oidc/token*, které předá parametry:
   - *grant_type=authorization_code* – definuje metodu předání identity Authorization Code Flow,
   - *code* – autorizační kód, který aplikace obdržela v předchozím kroku,
   - *redirect_uri* – URL externího IS/AIS, na které bude uživatel přesměrován po autentizaci, musí být stejné jako předané při volání služby */oidc/authorize* v předchozím kroku,
   - *client_id* – identifikace klienta (externího IS/AIS),
   - *code_verifier* – hodnota PKCE rozšíření.

   Služba vrátí Access token, Id token, Refresh token. Id token obsahuje informace a atributy uživatele ve formátu JWT. Access token slouží k volání služeb IS/AIS, Refresh token slouží pro obnovu neplatného Access tokenu.
5. Aplikace ověří podpis JWT Id token, v případě potřeby může získat podepisovací klíč voláním služby EnviAM */oidc/jwks*.
6. Aplikace uloží získaný Access token, Refresh token do sezení uživatele pro příští volání služby nebo pro obnovu Access tokenu.

4.4.4 ATRIBUTY A IDENTIFIKÁTOR UŽIVATELE

Atributy uživatele jsou předávány v ID tokenu, viz seznam atributů v kapitole 4.1 Atributy uživatele. ID token je ve formě JWT tokenu. Jednoznačný UUID identifikátor uživatele v CRŽP je předán v atributu `sub`, viz následující příklad obsahu JWT tokenu:

```
{
 "jti": "TGT-1-4O9CBh6guln9I68I9JEAZwghncsrXYs9euQeFQz-cWuGjncw8uezv-VzbD9X3IPsJVc-jsmhtpc",
 "sid": "4ffa860b8aaf130a206cd83c2b4b7457ff1a3421",
 "iss": "https://jsmhtpc:8443/cas/oidc",
 "aud": "clientId",
 "exp": 1606268378,
 "iat": 1606264683,
 "nbf": 1606264383,
 "sub": "123e4567-e89b-12d3-a456-426655440000",
 "client_id": "clientId",
 "auth_time": 1606264683,
 "state": "tIV9vWZGZKQOS4hMO-cXek0XAMwTzAm6rIqFkHwGI4o",
 "nonce": "VXdfcK8GA2mpE89jx9B744zuGO5ZFnw78VTdAPiuYiM",
 "at_hash": "Scn8LW8wH8QfP6R0KS4Sdg",
 "login": "custuser",
 "email": "oto.klus@org.cz",
 "phone": "+420777666555",
 "family_name": "Klus",
 "given_name": "Otto",
 "full_name": "Ing. Otto Klus",
 "role_crzp": "A100, A101",
 "role_rpp": "A100:A001,A101:A002",
 "loa": "high"
}
```

JWT token je dle standardu OIDC předáván v kódované formě (base 64), společně s hlavičkou a kontrolním součtem (podpisem).

4.4.5 CHYBOVÉ SITUACE A JEJICH ŘEŠENÍ

Uživatel je přesměrován na aplikaci pouze v případě, že dojde k úspěšné autentizaci uživatele. V případě jakékoli chyby je její zpracování a informování uživatele plně v režii EnviAM.

4.4.6 POSTUP PŘIPOJENÍ K ENVIAM

1. Dodavatel Aplikace prozkoumá OIDC metadata IdP testovacího EnviAM na adrese https://t-iam.env.cz/oidc/.well-known. Z nich zjistí potřebné informace, jako URL jednotlivých endpointů služeb IdP, použité šifrovací a podepisovací algoritmy apod.
2. Dodavatel Aplikace předá správci EnviAM URL testovací aplikace, na které bude uživatel přesměrován z testovacího EnviAM.
3. Správce EnviAM provede registraci aplikace v testovacím EnviAM a předá dodavateli hodnotu atributu **ClientID**.
4. Dodavatel otestuje komunikaci a v případě problémů kontaktuje správce EnviAM a sdělí mu odpověď, která mu byla od EnviAM vrácena (http response) a přesný čas provedení testu.
    a. Správce analyzuje problém a provede buď opravu vlastní konfigurace nebo sdělí důvod, proč nebyl požadavek akceptován.
    b. Případně může proběhnout vzájemná intenzivnější komunikace a spolupráce na odhalení příčiny problému.
5. Dodavatel provede otestování své Aplikace, zejména integraci na IS/AIS a správnou autentizaci volaných služeb IS/AIS.
6. Dodavatel zopakuje kroky 1 – 4 pro produkční prostředí Aplikace a EnviAM.

4.5 INTEGRACE NE-WEBOVÝCH APLIKACÍ (TLUSTÝCH KLIENTŮ)

EnviAM nabízí pouze webové uživatelské rozhraní pro autentizaci uživatele. V případě, že Aplikace nevyužívá webové uživatelské rozhraní, tj. uživatel nepřistupuje k aplikaci prostřednictvím webového prohlížeče, ale grafického rozhraní založeného na jiné technologii, nejčastěji ve formě tlustých klientů, nemůže aplikace přímo využít autentizaci uživatele prostřednictvím webového rozhraní EnviAM.

Tyto aplikace bývají přímo nainstalovány na počítačích jednotlivých uživatelů, případně se přistupuje na tyto aplikace prostřednictvím vzdálených (virtuálních) ploch. V takových případech je nutné provést integraci Aplikace s webovým rozhraním EnviAM.

Základní dva způsoby integrace:

1. simulace webového prohlížeče,
2. integrace komponenty webového prohlížeče.

4.5.1 SIMULACE WEBOVÉHO PROHLÍŽEČE

Aplikace bude simulovat prohlížeč, tj. bude zasílat HTTP požadavky, přijímat HTTP odpovědi a příslušně je zpracovávat (reagovat na ně). Na stejném principu pracuje např. automatizované testování webových stránek. Aplikace zašle HTTP požadavek a počká na odpověď, odpovědí je buď formulář, informační stránka nebo http přesměrování na jinou stránku. Pokud se jedná o formulář, bude to buď formulář pro zadání uživatelského jména a hesla nebo formulář pro zadání ověřovacího kódu MFA. V případě informační stránky se bude jednat o informaci o chybně zadaných autentizačních údajích nebo o chybném ověřovacím kódu. V případě přesměrování, zašle Aplikace nový požadavek na cílové URL přesměrování (hodnota v hlavičce Location). V případě, že se jedná o přesměrování zpět do Aplikace, převezme si Aplikace předaný autentizační token (SAML Response nebo OIDC autorizační kód).

Výhody:

- jednoduchá realizace prostřednictvím základních technologií (protokol HTTP),
- možno volání automatizovat – tj. uživatel nemusí fyzicky interagovat s rozhraním EnviAM.

Nevýhody:

- náročnější integrace s externími IdP (pokud jsou vyžadovány),

- závislost na IdP – v případě aktualizace stránek a jejich výraznější změny nebo např. při přidání nové funkcionality, např. ošetření pomocí captcha může způsobit nefunkčnost tohoto řešení a nutnost aktualizace.

4.5.2 INTEGRACE WEBOVÉHO PROHLÍŽEČE

Další možností je integrace webového prohlížeče pro přihlášení přímo do aplikace. Existuje několik technologií, z nichž nejznámější a běžně používané jsou tyto:

1. Integrace CEF (Chromium Embedded Framework) do aplikace. CEF je poskytován pro celou řadu technologií (Delphi, Java, .NET, C#, Python, Swift, VB, Ruby, Visual Studio .NET, …)
2. CefSharp – založeno na CEF, zjednodušené použití CEF v C# a C++.
3. Standardní komponenta VisualStudio WebBrowser.

V tomto případě je integrace provedena tak, že komponenta do aplikace vložena a na základě specifické události (volání služby, stisknutí tlačítka) otevřeno okno komponenty s prohlížečem a předáno URL na EnviAM s požadavkem na autentizaci. Následně komponenta monitoruje událost přesměrování, a pokud se jedná o přesměrování zpět na aplikaci (fiktivní URL), tak převezme informace z přesměrování, které obsahují SAML Response nebo OAuth autorizační kód a uzavře okno.

Výhody:

- může být poměrně jednoduché na implementaci v případě dostupnosti příslušné komponenty v dané technologii Aplikace.
- nezávislé na změnách webového rozhraní EnviAM nebo externích IdP.

Nevýhody:

- specifická technologie (komponenta),
- komponenty nemusí být k dispozici na některých platformách či technologiích, na kterých je Aplikace postavena,
- někteří externí IdP mohou tyto externí komponenty identifikovat a zabránit jejich použití pro přístup na stránky. IdP bohužel tyto informace neuvádějí, jelikož je to součástí zabezpečení autentizačního procesu – bránit přihlášení pomocí jiných prostředků než standardních prohlížečů. Pokud se komponenta tváří jako běžný prohlížeč (tj. v hlavičkách posílá stejné informace jako prohlížeče) IdP toto nemusí identifikovat, pokud však posílá jiné informace nebo některé informace chybějí, IdP toto může klienta identifikovat jako nestandardního a znepřístupnit autentizaci. (zatím byla nalezena pouze informace, že Google jako IdP se snaží tyto nestandardní komponenty identifikovat)

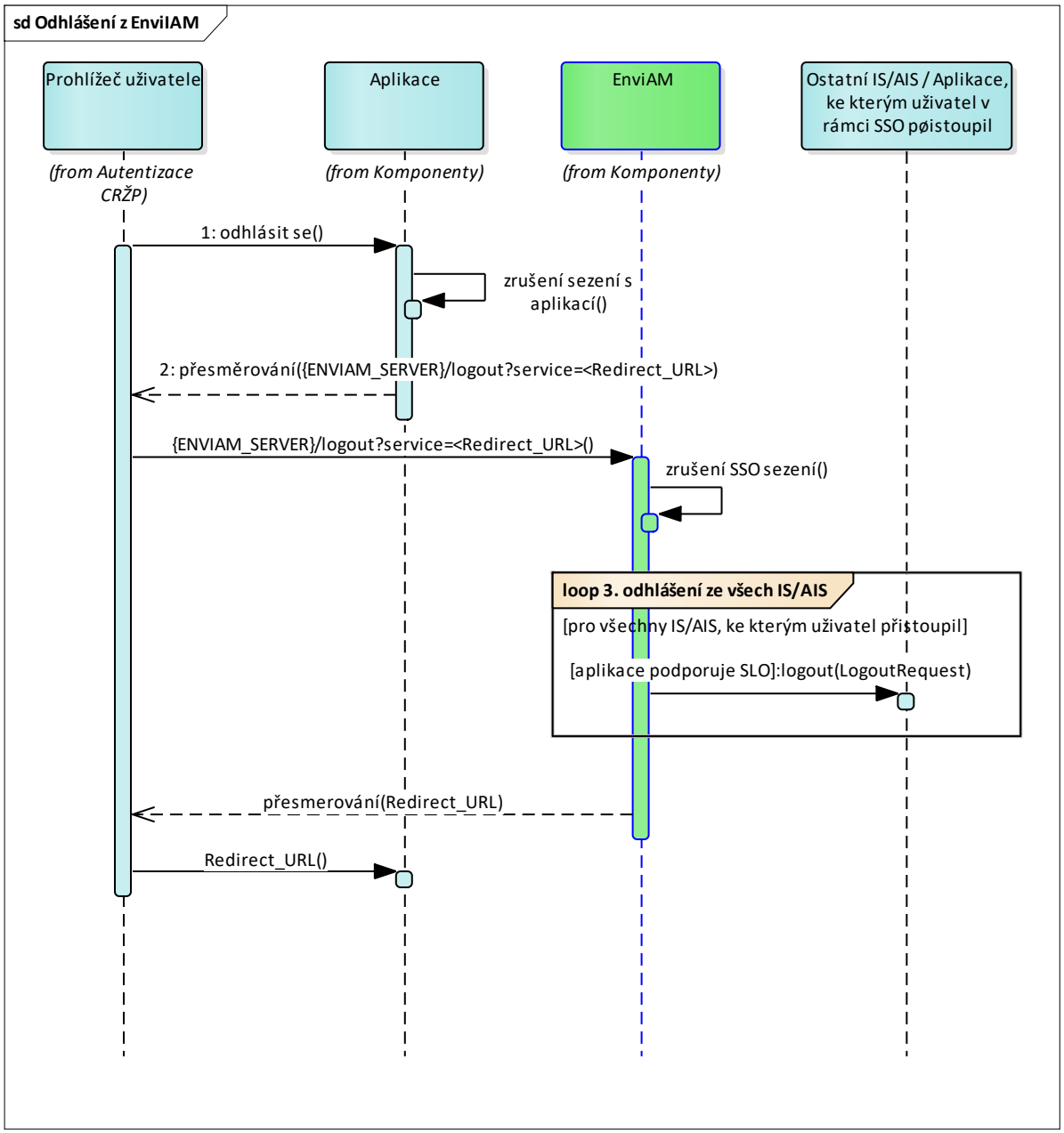
5 ODHLÁŠENÍ

5.1 POPIS

Pokud se uživatel odhlašuje z Aplikace nebo systému IS/AIS integrovaného k EnviAM, musí vyvolat odhlášení uživatele v EnviAM a tím zrušení SSO sezení uživatele. EnviAM po zrušení SSO sezení uživatele zavolá službu odhlášení ve všech IS/AIS nebo Aplikacích, ke kterým v rámci SSO sezení uživatel přistoupil a které mají implementovánu/realizují službu jednotného odhlášení (SLO).

Aktuálně nebudou integrované IS/AIS službu SLO implementovat. Tato funkcionalita je v EnviAM obecně k dispozici a systém IS/AIS nebo Aplikace může v případě potřeby kdykoli tuto službu dodatečně implementovat. Záleží na konkrétní Aplikaci, zda chce být informována o ukončení SSO sezení uživatele či nikoli.

Scénář průběhu odhlášení je zachycen na následujícím Obrázek 7.



Obrázek 7: Odhlášení z EnviAM – zrušení SSO sezení.

1. Uživatel v Aplikaci, která je integrována s EnviAM, použije funkcionalitu „Odhlásit se“. Aplikace zajistí nezbytné činnosti, např. uloží rozpracovanou práci a zruší sezení uživatele v aplikaci.
2. Aplikace provede přesměrování uživatele prostřednictvím metody http GET na službu EnviAM *logout*, která provede zrušení SSO sezení s uživatelem. Volitelně může Aplikace předat v parametru *service* URL, na které bude uživatel po odhlášení automaticky přesměrován.
3. EnviAM zavolá službu jednotného odhlášení ve všech integrovaných IS/AIS, ke kterým uživatel v rámci rušeného sezení přistoupil a které implementují požadovanou službu jednotného odhlášení, viz dále popis služby SLO.
4. Uživateli je zobrazena informace, že byl úspěšně odhlášen v případě, že nebyl předán parametr *service*, nebo přesměruje uživatele na URL předané v tomto parametru.

5.2 Služba EnviAM pro zrušení SSO sezení (odhlášení v EnviAM)

EnviAM poskytuje službu odhlášení uživatele z EnviAM, a tedy zrušení SSO sezení. Služba se volá přesměrováním uživatele, tj. zasláním HTTP GET, na následující URL:

{ENVIAM_SERVER}/cas/logout?service={Redirect_URL}

URL parametr *service={Redirect_URL}* specifikuje URL, na které je uživatel po odhlášení automaticky přesměrován – musí obsahovat URL aplikace (domovské / úvodní stránky), pro které byla služba definována.

5.3 Služba jednotného odhlášení SLO

Jednotné odhlášení je způsob, jak se může uživatel během odhlašování z jedné aplikace odhlásit najednou ze všech aplikací, ke kterým v rámci konkrétního SSO sezení přistoupil.

Každá aplikace, která se chce účastnit jednotného odhlášení, tj. být notifikována v případě, že se uživatel odhlásil z EnviAM, musí vystavit službu (endpoint), na kterém akceptuje následující žádost zaslanou prostřednictvím HTTP POST požadavku.

```
<samlp:LogoutRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="[generovaný ID]"
    Version="2.0"
    IssueInstant="[aktuální datum a čas]">
    <saml:NameID>[CRŽP UserId]</saml:NameID>
    <samlp:SessionIndex>[Identifikace sezení]</samlp:SessionIndex>
</samlp:AuthnRequest>
```

Po obdržení tohoto požadavku by měla (asi ne v případě, že uživatel aktuálně v aplikaci pracuje) aplikace buď na základě obdrženého uživatelského jména nebo identifikace sezení (viz níže) zrušit aplikační sezení uživatele. Problém s rušením aplikačního sezení na základě uživatelského jména je ten, že může být vytvořeno více aplikačních sezení pro jedno uživatelské jméno, v tom případě nelze rozlišit na základě jména, kterého SSO sezení se odhlášení týká. EnviAM nekontroluje výsledek volání této služby, zda aplikace skutečně uživatele odhlásila či nebylo sezení nalezeno.

Identifikace sezení je předána daným autentizačním protokolem, v případě SAML se jedná o hodnotu atributu `SessionIndex` elementu `AuthnStatement`, OIDC protokol předává identifikaci sezení v JWT v atributu `sid`.

5.4 Expirace SSO sezení

Uživatel nemusí být v EnviAM odhlášen jen prostřednictvím služby odhlášení, ale také automaticky po expiraci definované doby SSO sezení.

SSO sezení v EnviAM má dvě doby expirace:

5.4.1 Doba života SSO sezení

TTK (time to kill) – doba života SSO sezení je doba, po kterou když uživatel nepoužije aplikaci EnviAM, dojde k expiraci a tj. odhlášení uživatele.

Vzhledem k tomu, že uživatel pracuje v integrované aplikaci, nikoli EnviAM, je tato doba restartována v případě, že uživatel znovu přistupuje k EnviAM, např. z důvodu zahájení práce v nové aplikaci nebo v případě, že stávající aplikace, ve které uživatel pracuje, pravidelně obnovuje identitu, tj. v rámci daného protokolu znovu žádá o zaslání identity uživatele.

5.4.2 MAXIMÁLNÍ DOBA ŽIVOTA SSO SEZENÍ

TTL (time to live) – definuje maximální dobu života SSO sezení, tj. i v případě, že uživatel pravidelně prodlužuje standardní dobu života SSO sezení, dojde po této době k expiraci SSO sezení. Tj. doba SSO sezení nemůže být delší než tato definovaná doba.

EnviAM předává v atributech uživatele i atribut SSOExpiration, který obsahuje datum a čas expirace SSO sezení. Pokud uživatel intenzivně pracuje v aplikaci před koncem této doby, měla by aplikace dát uživateli vědět, že v brzké době dojde k expiraci SSO přihlášení a že se bude muset znovu přihlásit. Záleží pak na aplikaci, jaký vhodný způsob odhlášení použije. Základním dělením těchto variant je, zda bude uživatel dále pokračovat v práci, zda si bude muset práci uložit a znovu otevřít aplikaci nebo dojde k ukončení aplikace včetně ztráty rozpracované práce. Vhodný způsob obnovy přihlášení závisí na způsobu práce v aplikaci (uživatel se jen na něco dívá, uživatel vyplňuje dlouhé formuláře apod.)

6 DOPORUČENÍ

Pro zvýšení bezpečnosti přístupů a užívání AIS systému doporučujeme do uživatelské příručky AIS systému doplnit informaci pro koncové uživatele, aby se vždy při ukončení práce v AIS systému odhlásili a uzavřeli okno prohlížeče.

7 PŘÍLOHY

7.1 UKÁZKA SAML ODPOVĚDI VČETNĚ UŽIVATELSKÝCH ATRIBUTŮ

```
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://
http://crzp.env.cz/saml/" ID="_4263239398302973952" InResponseTo="z787c7d14-3638-459b-931d-
9b9d6c21e8fe" IssueInstant="2020-11-25T00:00:51.262Z" Version="2.0">
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://iam.env.cz/cas/idp</saml2:Issuer>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </saml2p:Status>
    <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_8561768784470691840" IssueInstant="2020-11-25T00:00:51.228Z" Version="2.0">
        <saml2:Issuer>https://iam.env.cz/cas/idp</saml2:Issuer>
        <saml2:Subject>
            <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
NameQualifier="crzp.inqool.cz" SPNameQualifier="crzp.inqool.cz">123e4567-e89b-12d3-a456-
426655440000</saml2:NameID>
            <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml2:SubjectConfirmationData InResponseTo="z787c7d14-3638-459b-931d-
9b9d6c21e8fe" NotOnOrAfter="2020-11-25T00:01:06.217Z" Recipient=" http://crzp.env.cz/saml/"/>
            </saml2:SubjectConfirmation>
        </saml2:Subject>
        <saml2:Conditions NotBefore="2020-11-25T00:00:36.255Z" NotOnOrAfter="2020-11-
25T00:01:06.255Z">
            <saml2:AudienceRestriction>
                <saml2:Audience>crzp.inqool.cz</saml2:Audience>
            </saml2:AudienceRestriction>
        </saml2:Conditions>
        <saml2:AuthnStatement AuthnInstant="2020-11-25T00:00:51.217Z" SessionIndex="ST-2-jbcI-
mTJz7dhSGywqkBxPSfSIFU-jsmhtpc">
            <saml2:SubjectLocality Address="10.1.1.140"/>
            <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport<
/saml2:AuthnContextClassRef>
            </saml2:AuthnContext>
        </saml2:AuthnStatement>
        <saml2:AttributeStatement>
            <saml2:Attribute FriendlyName="isFromNewLogin" Name="isFromNewLogin"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml2:AttributeValue>false</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="authenticationDate" Name="authenticationDate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml2:AttributeValue>2020-11-24T23:58:14.349058200Z</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="successfulAuthenticationHandlers"
Name="successfulAuthenticationHandlers" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">
                <saml2:AttributeValue>CustomAuthenticationHandler</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="role_rpp" Name="role_rpp"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml2:AttributeValue>A100:ACR01,A100:ACR02,A110:ACR06</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="given_name" Name="given_name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml2:AttributeValue>Otto</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="login" Name="login"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml2:AttributeValue>oklus</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="credentialType" Name="credentialType"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml2:AttributeValue>UsernamePasswordCredential</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="full_name" Name="full_name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml2:AttributeValue>Ing. Otto Klus</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="phone" Name="phone"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
```

```
                <saml2:AttributeValue>+420777666555</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="authenticationMethod" Name="authenticationMethod"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml2:AttributeValue>CustomAuthenticationHandler</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="role_cizp" Name="role_cizp"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml2:AttributeValue>C100,C101,C102,C202,C110:C206</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="longTermAuthenticationRequestTokenUsed"
Name="longTermAuthenticationRequestTokenUsed"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml2:AttributeValue>false</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="userUUID" Name="userUUID"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml2:AttributeValue>123e4567-e89b-12d3-a456-
426655440000</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="family_name" Name="family_name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml2:AttributeValue>Klus</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute FriendlyName="email" Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                <saml2:AttributeValue>oto.klus@org.cz</saml2:AttributeValue>
            </saml2:Attribute>
        </saml2:AttributeStatement>
    </saml2:Assertion>
</saml2p:Response>
```

Příloha 2: Specifikace – Dokumentace CRŽP

Předmětná příloha je dostupná neomezeným a přímým dálkovým přístupem v Národním elektronickém nástroji v detailu Veřejné zakázky – viz odkaz:

https://nen.nipez.cz/Zadavaci_postup/N006-21-V00029510.