Příloha č. 5 Zadávací dokumentace

Příloha A Smlouvy

Požadavky na technická řešení

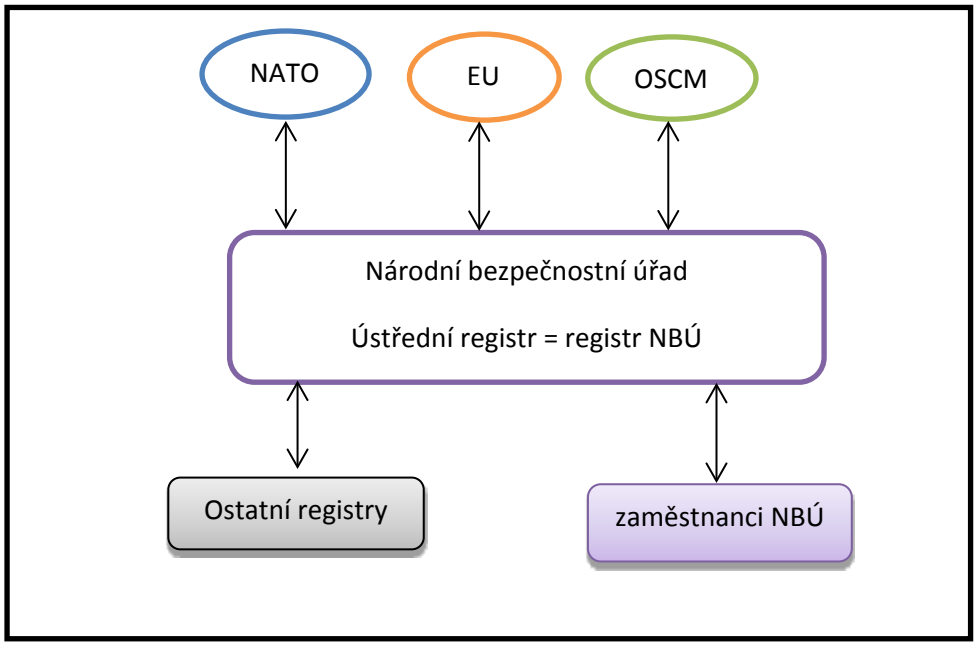
„Vybudování informačního systému ústředního registru“

1 Úvod

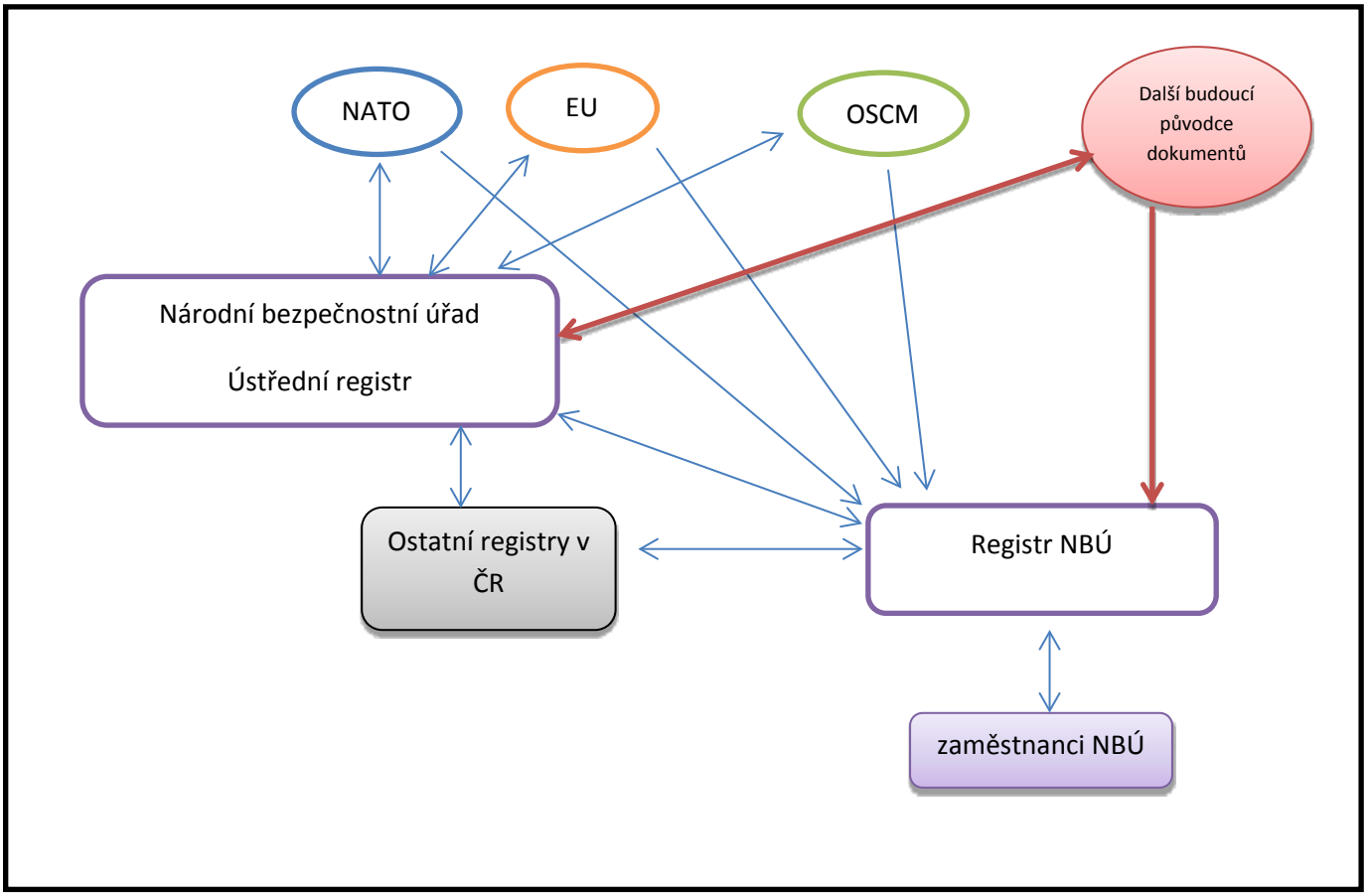
Ústřední registr byl zřízen Národním bezpečnostním úřadem v souladu s ustanovením § 79 odst. 2 zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon“). V ústředním registru se přijímají, vytvářejí, evidují, odesílají a ukládají utajované i neutajované informace poskytované v mezinárodním styku.

V souladu s ustanovením § 79 odst. 3 zákona zřizuje a vede Národní bezpečnostní úřad registr utajovaných i neutajovaných informací poskytovaných v mezinárodním styku pro výkon svojí činnosti.

Obrázek č. 1 - postavení ústředního registru – současnost



obrázek č. 2 - postavení ústředního registru a registru NBÚ – po zavedení řešení



2 Jmenné konvence a definice

Administrativní pomůcka	§ 3 vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů
AthenA	eSSL zadavatele
eSSL	Elektronický systém spisové služby
NBÚ	Národní bezpečnostní úřad
ÚR	Ústřední registr
NATO	Severoatlantická aliance
EU	Evropské unie
OSCM	Ostatní subjekty cizí moci
cizí moc	Souhrnný název pro dokumenty NATO, EU a OSCM (§ 2 písm. g zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, dále jen „zákon“).
Číselník	Předdefinovaný seznam pro automatický a manuální výběr (např. původců, adresátů…)
Distribuce	Odeslání příchozího dokumentu cizí moci dalším registrům

NSESSS	Národní standard pro elektronické systémy spisové služby (VMV čá. 57/2017)
IS	Informační systém
IS UR	Informační systém ústředního registru
Datové formáty	TXT, XML, PDF, HTML, DOC, DOCX, XLS, XLSX, PPT, PPTX, GIF, JPEG, BMP, ODP, ODS, ODT, PNG, RTF, TIFF, BMP, JPG, RAR, DBF, GIF, MP3, MP4 a další audio a video formáty
SIP	Informační balíček („Submission Information Package“) určený k exportu nebo přenosu entit z eSSL do digitálního archivu
ISDS	Informační systém datových schránek
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
GDPR	Nařízení Evropského parlamentu a rady (EU) č. 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)
JP	Jednací protokol
č. j.	Číslo jednací
UI	Utajované informace
Dokument	Každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální. Formy dokumentu: listinná, nelistinná, digitální.
Datová zpráva	Obecný objekt popisující známou datovou strukturu (zfo, xml, eml, apod.)
ISSD	Informační systém spravující dokumenty (utajované i neutajované)
VIS	Vnitřní informační systém NBÚ
Objektem IS	Pasivní prvek informačního systému, který obsahuje nebo přijímá informaci
Subjektem IS	Aktivní prvek informačního systému, který způsobuje předání informace mezi objekty informačního systému nebo změnu stavu systému
Řízený přístup	Prostředky pro omezení přístupu subjektů informačního systému k objektům

	informačního systému, zajišťující, že přístup k nim získá jen autorizovaný subjekt informačního systému
Kryptografický prostředek	Hardwarový nebo softwarový produkt určený ke kryptografické ochraně anebo jejich kombinace
Heslový materiál	Utajovaný znakový řetězec na nosiči, ze kterého je odvozován kryptografický klíč nebo který je použit k autentizaci
Původce	Orgán státu, právnická osoba nebo podnikající fyzická osoba, u nichž utajovaná informace vznikla (§ 2 písm. f) zákona
Uživatel	Každý, kdo má identifikační a autentizační prvky pro přístup k dodávanému řešení.

3 Legislativní požadavky

- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
- Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů
- Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb., ve znění pozdějších předpisů
- Vyhláška 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů
- Vyhláška č. 432/2011 Sb. o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb., ve znění pozdějších předpisů
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě, a to ve znění pozdějších předpisů
- Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby ve znění vyhlášky č. 283/2014 Sb., ve znění pozdějších předpisů
- Národní standard pro elektronické systémy spisové služby (VMV čá. 57/2017)
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů

- Zákon č. 301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů
- Zákon č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů
- 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
- Rozhodnutí rady ze dne 23. září 2013 o bezpečnostních pravidlech na ochranu utajovaných informací EU (2013/488/EU)
- Rozhodnutí komise (EU, Euratom) 2015/444 ze dne 13. března 2015 o bezpečnostních pravidlech na ochranu utajovaných informací EU
- Nařízení rady č. 3, kterým se provádí článek 24 Smlouvy o založení Evropského společenství pro atomovou energii
- AC/35-D/2001-REV2 NATO SECURITY COMMITTEE DIRECTIVE on PHYSICAL SECURITY
- AC/35-D/2002-REV4 SECURITY COMMITEE DIRECTIVE on the SECURITY of INFORMATION AC/35-D/2004-REV3 SECURITY COMMITTEE Primary Directive on CIS Security
- AC/35-D/2005-REV3 SECURITY COMMITTEE MANAGEMENT DIRECTIVE ON CIS SECURITY
- C-M(2002)49 SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION, v platném znění
- 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
- a případně další právní předpisy, které tuto problematiku upravují.

4 Popis současného stavu

NBÚ v současné době spravuje UI cizí moci v evidenčním systému Agile, který není eSSL a nesplňuje požadavky podle NSESSS. Evidenční systém Agile je certifikovaným systémem a zajišťuje celý životní cyklus utajovaných i neutajovaných dokumentů cizí moci do stupně utajení Tajné (včetně).

4.1 Funkcionality evidenčního systému AGILE

Evidenční systém Agile je galvanicky odděleným systémem pracujícím v offline režimu, umožňující přihlášení do systému a souběžnou práci více uživatelů na různých počítačových stanicích, změnu uživatelského hesla pro přístup do systému a zaznamenává všechny činnosti uživatele. Evidenční systém Agile pracuje s číselníky.

Evidenční systém Agile slouží k evidenci dokumentů cizí moci (včetně vložení souborů), které jsou vedeny odděleně dle jednotlivých původců a stupňů utajení, dále k přidělování, odesílání, ukládání a provedení skartačního řízení (odděleně dle jednotlivých původců, stupňů utajení a ročníku evidence). Dále umožňuje zaznamenání poznámek a provedení oprav v evidenci, které zapíše do historie příslušného dokumentu.

Jednací protokoly jsou vedeny odděleně dle původce dokumentů, stupně utajení a ročníku s možností jejich průběžného tisku dle vybraných kritérií, a to i opakovaně.

Evidenční systém Agile umožňuje vyhledávání v evidenčních záznamech dle vybraných kritérií.

5 Poptávané řešení

Zadavatel poptává ISSD, které musí zajistit životní cyklus utajovaných i neutajovaných dokumentů cizí moci v souladu s platnými právními předpisy, NSESSS a mezinárodními smlouvami, kterými je Česká republika povinna se řídit (dále jen „řešení“).

Dodavatel doloží jako součást akceptačního protokolu „Prohlášení o shodě s příslušnou legislativou a Národním standardem“ a „Prohlášení o shodě implementace s Národním standardem a další legislativou“. Dodavatel zajistí po dobu požadované podpory shodu s platnými právními předpisy.

Provozní prostředí požadovaného řešení tvoří certifikovaná síť na stupeň utajení Tajné (NATO SECRET, SECRET UE/EU SECRET) včetně (dále jen „síťové prostředí Registru“), v bezpečnostním módu „s nejvyšší úrovní“.

V síťovém prostředí Registru budou provozovány dva ISSD, které budou zajišťovat životní cyklus dokumentů cizí moci v oddělených evidencích.

ISSD ústřední registr – bude spravovat dokumenty cizí moci pro celou Českou republiku.

ISSD registr NBÚ – bude spravovat dokumenty cizí moci pro potřeby NBÚ.

ISSD registr NBÚ bude současně provozován i ve VIS, který je certifikovaný pouze do stupně „Důvěrné“ včetně (dále jen „síťové prostředí VIS“), v bezpečnostním módu „s nejvyšší úrovní“.

„Síťová prostředí“ je společný pojem pro síťové prostředí Registr a síťové prostředí VIS.

Zadavatel požaduje, aby řešení zajišťovalo logické oddělení dokumentů podle původce v jakékoli fázi životního cyklu včetně jejich uložení. Zadavatel požaduje ukládání dokumentů do výše stupně utajení v souladu s certifikací daného síťového prostředí.

Řešení musí umožnit převedení dokumentu v souladu s § 69a zákona č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů, včetně všech textových vrstev.

Řešení musí spravovat informace o jednotlivých objektech řešení, které ukládají utajované informace (dokumenty), a to s ohledem na stále platné oprávnění přístupu subjektů k objektům. Pokud takové platné oprávnění k přístupu již není, musí řešení takový přístup zakázat. tzv. řízený přístup je definován ve vyhlášce č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění pozdějších předpisů.

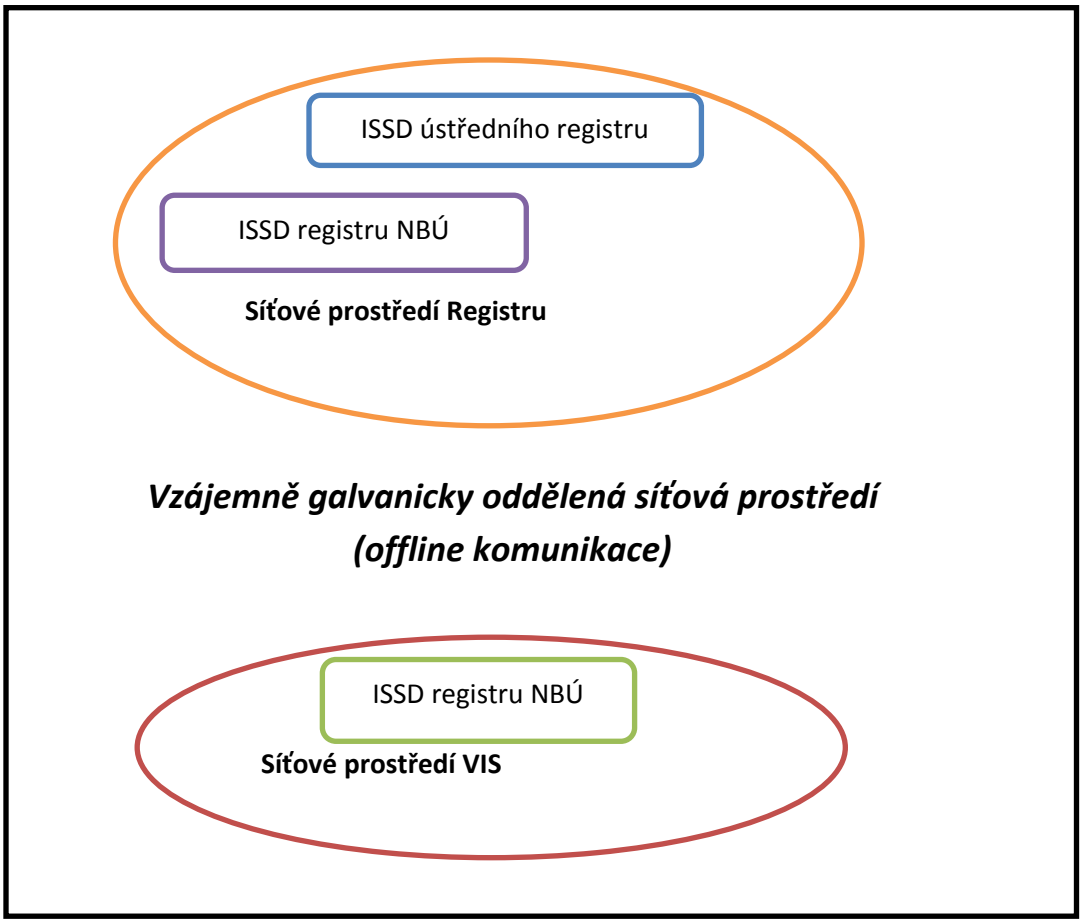
Zadavatel definuje, že stávající certifikované sítě (viz obrázek č. 3) pro provoz řešení jsou galvanicky oddělené od ostatních síťových prostředí a přenos informací a dat je realizován přenosnými vyměnitelnými nosiči (USB, CD, apod.). Zároveň požaduje, aby dodávané řešení architektonicky počítalo s dalším možným budoucím bezpečným propojením certifikovaných sítí zadavatele s ostatními IS. Bezpečné propojení IS je definováno v § 9a vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.

Zadavatel zajistí vlastními prostředky síťová prostředí až do úrovně operačních systémů a serverových aplikací od společnosti Microsoft.

Síťová prostředí jsou uzavřená a nemají žádné přímé propojení na jiné informační a komunikační systémy. Přenos informací a dat je zabezpečen prostřednictvím přenosných vyměnitelných médií (USB, CD, apod.).

ISSD ústředního registru a ISSD registru NBÚ jsou provozovány v síťovém prostředí Registru. Výměna dat nebude probíhat prostřednictvím přenosných vyměnitelných médií, ale prostředky síťových prvků, kterými je síťové prostředí Registru tvořeno.

obrázek č. 3 – certifikované sítě



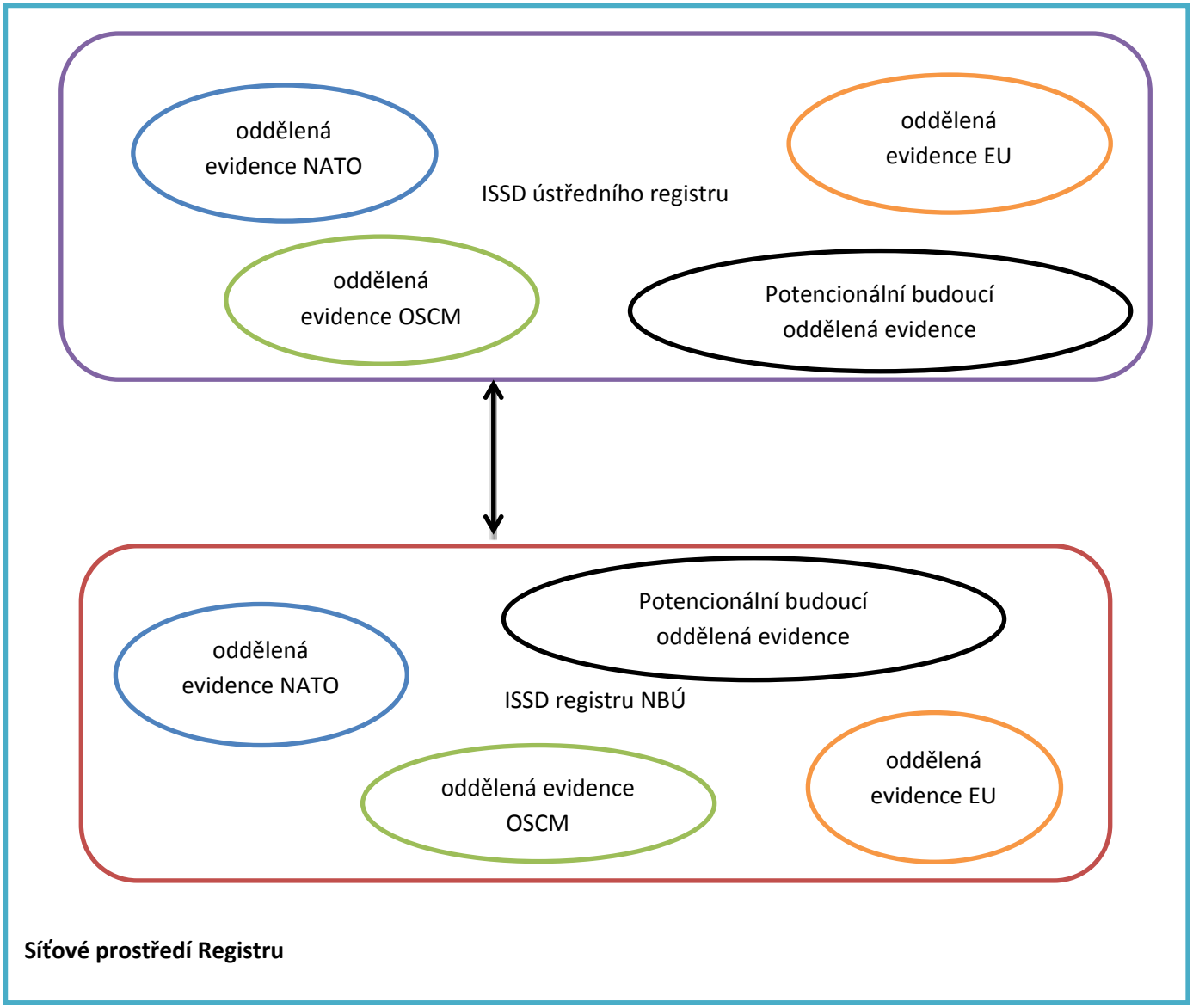
5.1 Požadavky na komunikaci

Zadavatel v rámci síťového prostředí požaduje komunikaci referenčním rozhraním, při přenosech dat mezi síťovými prostředími a při přenosech do informačních a komunikačních systémů třetích stran bude komunikace offline datovou dávkou pomocí přenositelných vyměnitelných médií (USB, CD,…).

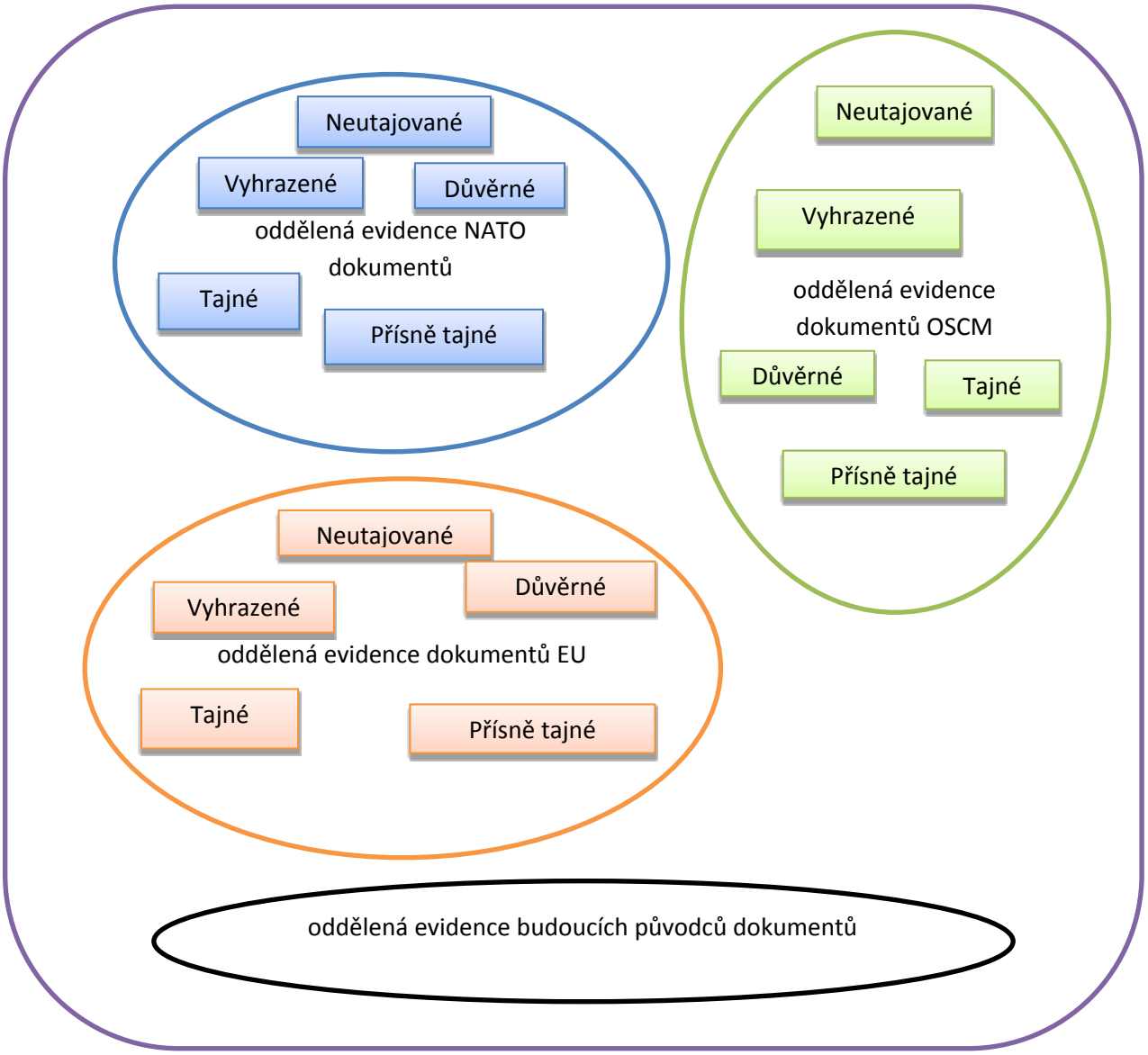
5.2 Oddělená evidence v síťovém prostředí Registru

V síťovém prostředí Registru budou provozovány dva ISSD, každý s oddělenou evidencí dokumentů rozdělených podle původců dokumentů (viz obrázek č. 4). V současné době jsou tři původci (NATO, EU, OSCM), ale mohou být určeni další, pro které bude možno rozšířit řešení o nové samostatné plně funkční oddělené evidence v obou ISSD.

obrázek č. 4 – oddělené evidence



obrázek č. 5 – oddělené evidence v jednotlivých ISSD



Každý ISSD v síťových prostředích bude obsahovat oddělenou evidenci pro každého původce dokumentů (v obrázku č. 5 barevně odlišenými buňkami: modrá = původce dokumentů NATO, oranžová barva = původce dokumentů EU, apod.). V každé z oddělených evidencí jsou vedeny odděleně dokumenty pro každý stupeň utajení, včetně neutajovaných.

Struktura oddělených evidencí pro budoucí původce dokumentů (další samostatná evidence) bude stejná jako u výše uvedených původců dokumentů.

Zadavatel požaduje, aby pracovník registru vždy jednoznačně rozeznal, v jaké evidenci aktuálně pracuje (např. na grafické úrovni, na úrovni textové identifikace, apod.). Dále požaduje, aby odlišnost mezi oddělenými evidencemi byla stejná pro každý ISSD (pokud oddělená evidence NATO bude mít např. modré pozadí oken, tak jej bude mít i v dalším ISSD).

Zadavatel požaduje, aby řešení mezi ISSD registru v síťovém prostředí Registru a síťovém prostředí VIS provádělo transakční výměnu dat a informací, čímž bude zajištěna aktuálnost obou ISSD. Výměna dat bude zabezpečena prostřednictvím vyměnitelných přenosných médií, interval si určí zadavatel.

Řešení musí umožňovat volbu jazykové mutace čeština a angličtina.

5.3 Požadavky na fáze životního cyklu dokumentu

Společnost ICZ a.s., IČO 25145444, pod vedením pánů V. Dinuše, R. Urbana, J. Krtila a paní K. Klanicové, se podílela na předběžné tržní konzultaci ve smyslu § 36 odst. 4 zákona č. 134/2016, o zadávání veřejných zakázek.

5.3.1 Příjem

Příjem probíhá pouze v síťovém prostředí Registru (viz obrázek č. 6).

Pokud dokument nebude při příjmu ve výstupním datovém formátu, bude do něj převeden a opatřen kvalifikovanou elektronickou pečetí a časovým razítkem.

Při příjmu bude určena oddělená evidence dokumentů podle původce (NATO, EU, OSCM). Okamžikem určení původce dokumentu musí být zajištěno logické oddělení dokumentů jednotlivých původců.

K určení původce budou využívány číselníky. Pokud bude automaticky určen původce z číselníku, řešení nabídne k zaevidování příslušnou samostatnou evidenci (pracovník registru potvrdí správnost), pokud původce určen nebude, dojde k jeho manuálnímu určení pracovníkem registru.

5.3.1.1 Příjem dokumentu v analogové podobě:

Dokumentu je při příjmu přidělen ID, který se vytiskne a nalepí na doručený dokument v analogové podobě (štítek s grafickým kódem). Následně bude dokument skenován.

Při příjmu dokumentu v nelistinné podobě, bude postupováno tak, aby byl zajištěn soulad s platnými právními předpisy.

5.3.1.2 Příjem dokumentu v digitální podobě:

Zdrojem příjmu ISSD je AthenA (zajišťuje příjem ISDS, elektronické pošty, úplné elektronické podání, apod). Příjem bude probíhat offline prostřednictvím přenosného vyměnitelného média (USB, CD, apod). Dalším zdrojem příjmu jsou pro ISSD certifikované informační systémy ostatních stran. V současné době bude probíhat příjem offline prostřednictvím přenosného vyměnitelného média (USB, CD, apod).

Technologie datových zpráv z:

AthenA

- ISDS – formát zfo
- Elektronická pošta – email
- Plné elektronické podání - XML

Certifikované informační systémy třetích stran

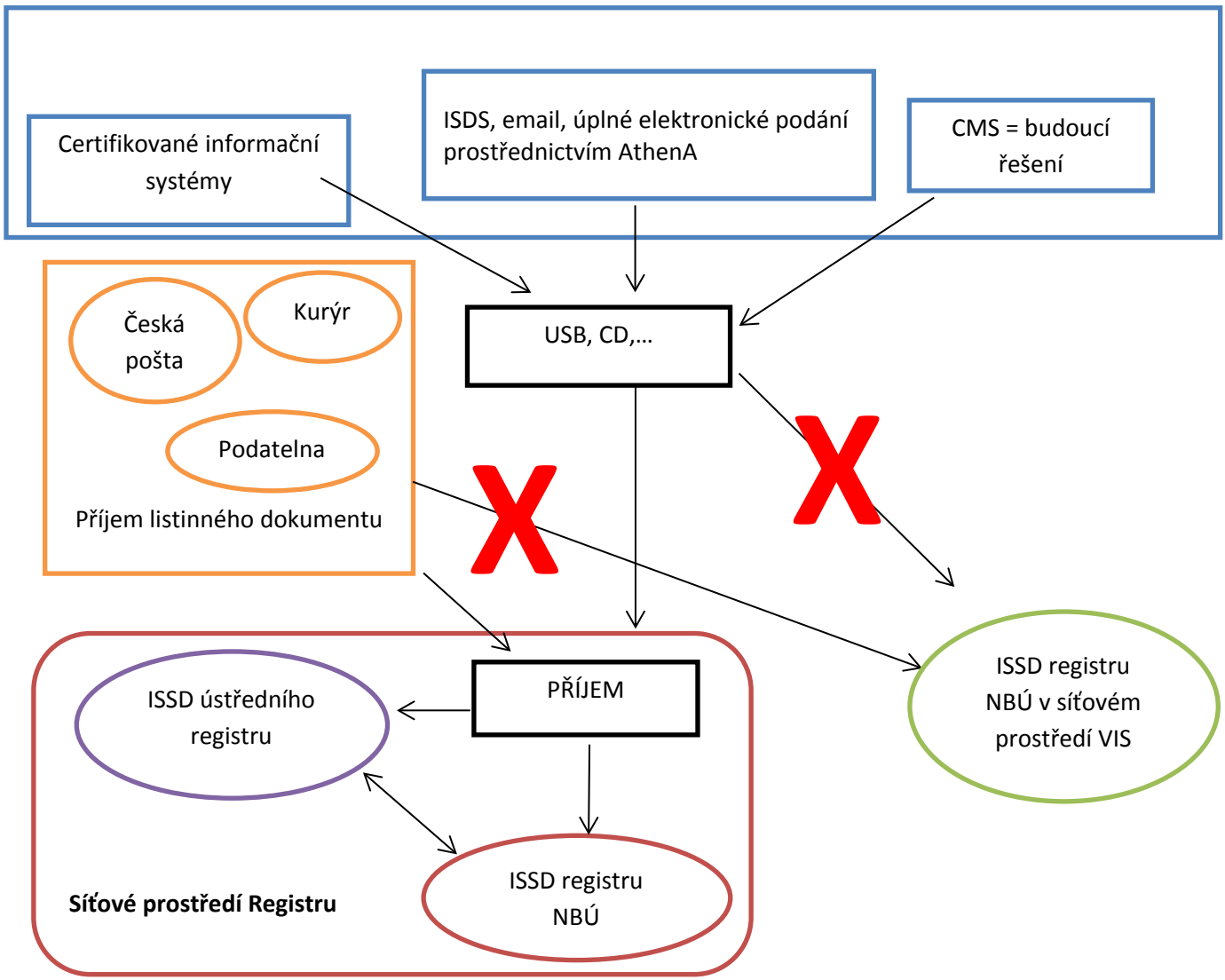
- Technologie typu email společnosti Microsoft (MS Exchange, MS Outlook, MS Office).

V případě, že datová zpráva bude obsahovat více dokumentů, řešení umožní práci s jednotlivými dokumenty a podrobnosti budou předmětem předimplementační analýzy.

U každého dokumentu či datové zprávy musí řešení zajistit jejich důvěryhodnost a integritu.

Pokud datová zpráva obsahuje metadata využitelná k automatizaci příjmu a evidenci, musí řešení tato metadata použít, přičemž pracovník každého ISSD musí mít možnost výsledek automatizace ověřit.

obrázek č. 6 – příjem



Zadavatel přijímá dokumenty v analogové nebo digitální podobě v datových formátech, ve kterých lze dokumenty zobrazit uživatelsky vnímatelným způsobem.

Prvotním přijímacím místem je zpravidla ISSD ústředního registru.

ISSD registru NBÚ přijímá dokumenty od ISSD ústředního registru - Odesílání vlastního dokumentu /distribuce. V rámci síťového prostředí Registru budou data přijímána přímo, včetně všech metadat. Příklad: ISSD ústředního registru v oddělené evidenci zaeviduje dokument NATO stupně utajení Důvěrné, předá tento dokument do ISSD registru NBÚ, kde bude zaevidován v oddělené evidenci dokumentů NATO a předvyplní shodná metadata. Pracovníkovi registru bude umožněno ověření správnosti údajů a bude přiděleno č. j. registru NBÚ.

Pokud bude datová zpráva nebo její část šifrovaná, řešení automaticky nabídne použití některého z kryptografických prostředků v předem definovaném číselníku, dle původce a stupně utajení.

Zadavatel požaduje, aby řešení umožnilo implementaci dalších kryptografických prostředků.

Zadavatel v současné době požaduje implementaci kryptografického prostředku HCryptC na stupeň utajení „Vyhrazené“.

Jedná se o aplikaci běžící pod operačním systémem Windows, která je určená k šifrování-dešifrování a mazání souborů nebo složek. Aplikace se spouští a ovládá pomocí příkazového řádku. Je určena zejména pro dávkové zpracování. Činnost aplikace se řídí pomocí vstupních parametrů zadaných v příkazovém řádku.

Kryptografický prostředek má tento tvar zápisu HCryptC.exe <***operace***> [***parametry***] <***data***>, přičemž sekce operace má tři typy, sekce parametry má cca do 20 možných parametrů a sekce data jsou vlastní data (dokument/ty) k některé z typu operací.

K použití správného kryptografického prostředku (dále jen „KP“) a heslového materiálu, hesla, PINu, certifikátu apod. je nutné vést číselník, který spravuje role Správce aplikace. Určuje jaký KP a jaký klíč, apod. použít při znalosti zdroje a identifikace kategorie dokumentu (stupeň utajení, oddělená evidence).

KP může navodit několik stavů:

- Úspěšně dešifrováno – použili jsme správný heslový materiál, přejdi na další krok v rámci příjmu.
- Neúspěšně dešifrováno
    - Špatný klíč
        - Dokument není určen pro ÚR, uloží se v původním formátu k další distribuci
        - Použij další klíče určené pro daný stupeň utajení a KP

- Dokument byl cestou k ÚR modifikován

Zadavatel požaduje integraci s tímto kryptografickým prostředkem.

Kryptografický prostředek požaduje zadání heslového materiálu k šifrování/dešifrování dokumentu/ů. Heslový materiál je soubor obsahující vygenerovaná data.

Zadavatel definuje, že pokud bude heslový materiál uložen přímo v systému řešení, bude opatřen prvky důvěry a integrity. Tyto prvky se musí vždy ověřovat před použitím heslového materiálu.

Řešení musí zajistit řízený a logovaný přístup k heslovému materiálu dle přesně definovaného seznamu uživatelů a aplikace. Zadavatel neřeší uložení heslového materiálu, způsob uložení je součástí této veřejné zakázky.

Další detaily použití KP budou předmětem předimplementační analýzy.

Zadavatel požaduje integraci s antivirovým řešením buď voláním funkcí API nebo voláním antivirové aplikace z příkazového řádku.

Při příjmu bude provedeno ověření elektronických podpisů, elektronických pečetí a elektronických časových razítek. Výsledkem této kontroly bude protokol o vyhodnocení datové zprávy (nově vzniklá komponenta přijatého dokumentu), který nebude mít vliv na evidenci dokumentů přijaté datové zprávy. V případě, že je digitální dokument neúplný, poškozený nebo že jej nelze zobrazit uživatelsky vnímatelným způsobem, oddělená evidence nabídne možnost vytvoření informační zprávy odesílateli, jejíž přílohou bude protokol o vyhodnocení datové zprávy. Pracovník registru rozhodne, zda bude tato informační zpráva odeslána či nikoliv. Při výskytu škodlivého kódu oddělená evidence vymaže veškeré soubory a zachová jen metadata.

5.3.2 Skenovací linka s OCR

Proces skenování bude probíhat v souladu s NSESS se zajištěním čitelné textové vrstvy, se kterou bude možno dále pracovat (např. vyhledávání v obsahu dokumentu). Současný statistický průměr jeden dokument = 21 stránek ve formátu papíru A4.

Zadavatel zde požaduje následující.

5.3.2.1 Hardware

- Spolehlivý barevný síťový skener pro formát papíru A3
- Rozlišení od 100 do 600 dpi pro text a pro foto až do 1200 dpi
- Snadná a rychlá obsluha
- Centralizovaná správa a bezproblémová integrace do provozovaných aplikací a řešení
- Snadné přizpůsobení pomocí webové verze sady pro vývoj softwaru SDK
- Univerzálních umístění, jako jsou e-mail, síťová složka, server FTP, paměťové zařízení USB, tisk

- Přidáním skeneru do sítě nebude třeba žádný další hardware či software a k jeho provozu není třeba instalovat žádný serverový software
- Indexové soubory metadat (ve formátu CSV nebo XML) lze přenášet při každém skenování a tyto informace lze použít také k pojmenování obrazových souborů, což usnadňuje snazší klasifikaci pro potřeby systémů
- Ověřování identifikačních přihlašovacích údajů a hesla zařízení a automatické odhlášení po určité době nečinnosti
- Jakákoliv činnost musí být logovaná
- Dokumenty různých původců musí být ukládány odděleně na úrovni např. složky na file systému. Uložení jen na dobu nezbytně nutnou.

5.3.2.2 Software

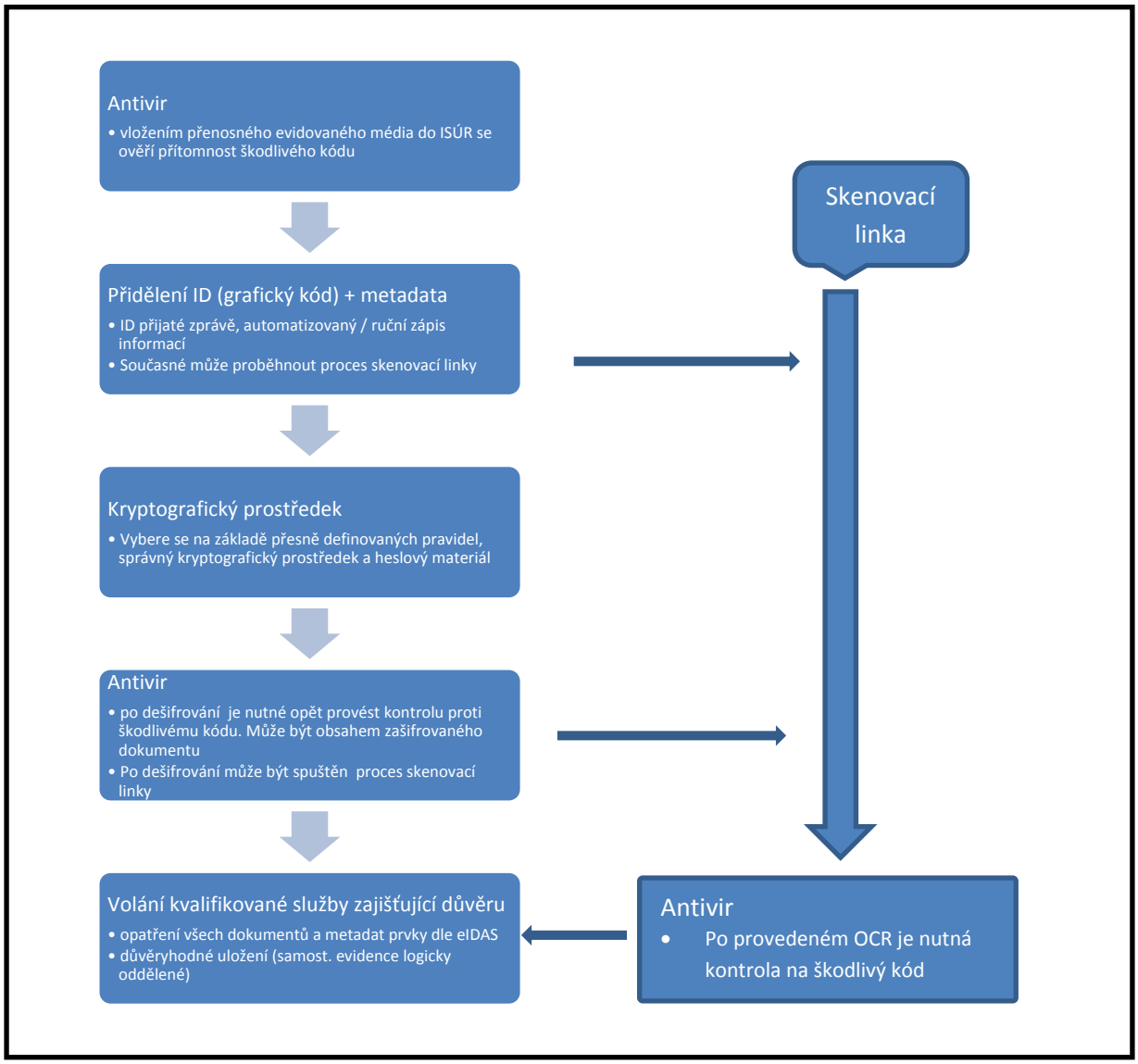
Zadavatel požaduje takové řešení, které bude provozu schopné v prostředí zadavatelem popisované

- Software musí být dostupný pro více aplikací
- Musí mít popsané referenční rozhraní
- Musí mít kompletní sadu technologií rozpoznávání:
  - Optické rozpoznávání znaků (OCR)
    - Evropské jazyky (latinská, cyrilika, arménská, řecká abeceda)
    - Min. 40 jazyků má podporu slovníku / morfologie, což výrazně zlepšuje přesnost OCR
    - Funkce pro rozpoznávání vícejazyčných dokumentů umožňuje rozpoznávání několika jazyků ve stejném dokumentu
    - Rozpoznávání psaných dokumentů
    - Rozpoznávání písem OCR-A, OCR-B, MICR (E13B) a CMC7
  - Inteligentní rozpoznávání znaků (ICR)
    - Technologie ICR pro více jazyků
    - Rozpoznávání ručně vytištěných znaků v polích a rámech - podtržené pole, rámečky, pole hřebenového stylu atd.
  - Optické rozpoznávání značek (OMR)
    - zaškrtnutí v čtvercovém rámečku
    - zaškrtnutí políčka na prázdném pozadí
    - nestandardní typy zaškrtnutí
  - Optické rozpoznávání čárových kódů (OBR)
    - 1D a 2D typy čárových kódů více typů
    - Rychlá extrakce čárových kódů. Funkce umožňuje automatickou detekci a rozpoznávání čárových kódů v libovolném úhlu dokumentu. Pracuje jak pro 1D, tak pro 2D čárové kódy
- Paralelní zpracování – využití více vláken
- Profily technologie rozpoznávání
- Předzpracování obrazů - deskewing, otočení, korekce zkreslení, textový řádek rovnání, rozdělení protilehlých stran, adaptivní binarizace, apod.

- Konverze do výstupních formátů
- Podrobná dokumentace k SDK i s ukázkovým kódem
- Podpora

Skenovací linka musí zajistit rozpoznávání a automatizaci přiřazení jednotlivých dokumentů do určené oddělené evidence, např. na základě štítků s grafickým kódem, který si před skenováním vytiskne a nalepí na dokument. Výsledek OCR bude uložen jako další verze dokumentu, popř. paralelní vedení dokumentu s patřičnými prvky zajišťujícími integritu a důvěryhodnost. Tento bude využit jen pro potřeby registru v modulu vyhledávání přímo v dokumentech (např. fulltext).

Obrázek č. 7 – jednotlivé kroky příjmového modulu



Obrázek č. 7 značí proces příjmu elektronického dokumentu. V případě, že elektronický dokument neobsahuje strojově čitelný text, vyvolá proces digitalizace s OCR. Výsledek je automaticky přiřazen jako další verze dokumentu nebo paralelní vedení s patřičnými prvky zajišťujícími integritu a důvěryhodnost.

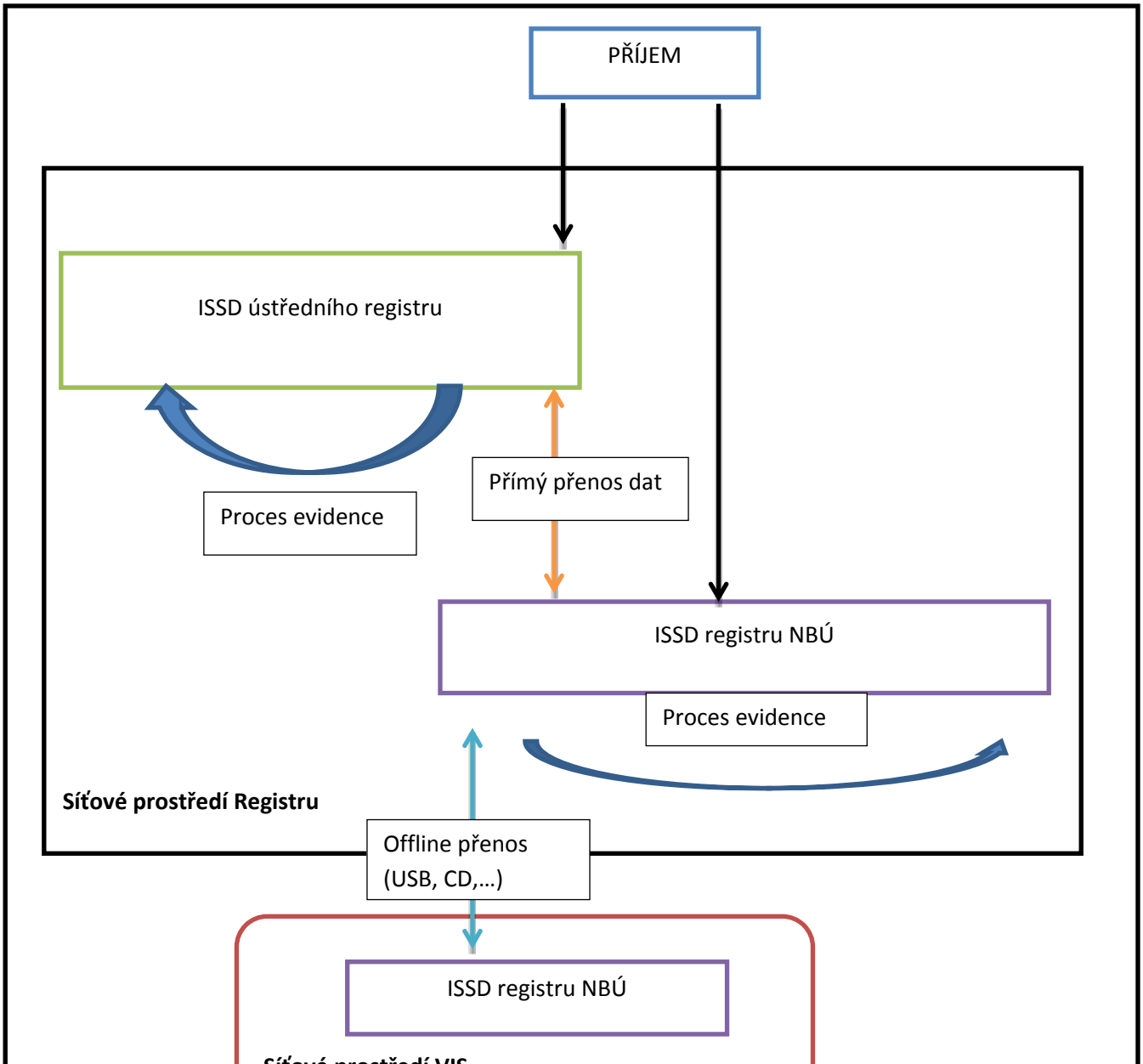
5.3.3 Evidence

V každé oddělené evidenci je vlastní i doručený dokument řádně zaevidován podle stupně utajení.

Evidence (viz obrázek č. 8) probíhá pouze v oddělených evidencích vedených v síťovém prostředí Registru až do stupně utajení Přísně tajné včetně. Oddělené evidence v síťovém prostředí VIS pouze přebírají evidenční údaje z oddělených evidencí vedených v síťovém prostředí Registru, a to až do stupně utajení Přísně tajné včetně.

Vkládání komponent utajovaných dokumentů je závislé na aktuální certifikaci síťového prostředí. Při změně stupně utajení certifikace dojde ke změně možnosti vkládání komponent utajovaného dokumentu.

obrázek č. 8 - evidence



Prvotním evidenčním místem je zpravidla ISSD ústředního registru. Dokumentu je přiděleno číslo jednací z příslušné oddělené evidence pro ÚR.

Po zaevidování dokumentu bude přidána textová vrstva k dokumentu s evidenčními údaji a českým ekvivalentem stupně utajení (pokud nebude již obsahovat – rozhodne pracovník registru). Tyto údaje nesmí překrývat samotný text dokumentu a pracovník registru umožní určit jejich umístění na dokumentu (jako otisk razítka). V případě, že takové umístění nebude možné, budou evidenční údaje na další stránce (samostatném listu).

Struktura čísel jednacích v oddělených evidencích bude upřesněna v rámci předimplementační analýzy.

5.3.4 Vyhotovení dokumentu

Oddělená evidence umožní vyhotovení vlastního utajovaného i neutajovaného dokumentu včetně rozdělovníku a zajištění prvků dle eIDAS s tím, že číslo jednací je přiděleno v oddělené evidenci v síťovém prostředí Registru a přeneseno do VIS.

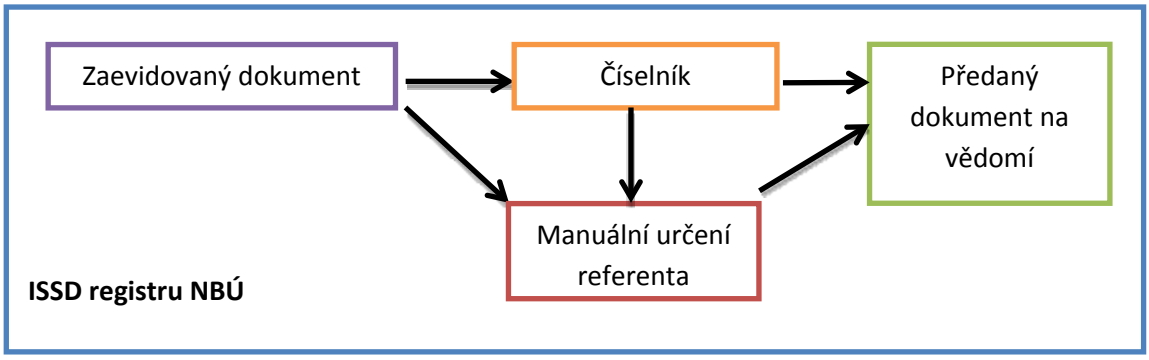
Vyhotovení dokumentu musí být v souladu s dotčenou platnou legislativou.

Detaily budou upřesněny v rámci předimplementační analýzy.

5.3.5 Předání dokumentu na vědomí v ISSD registru NBÚ

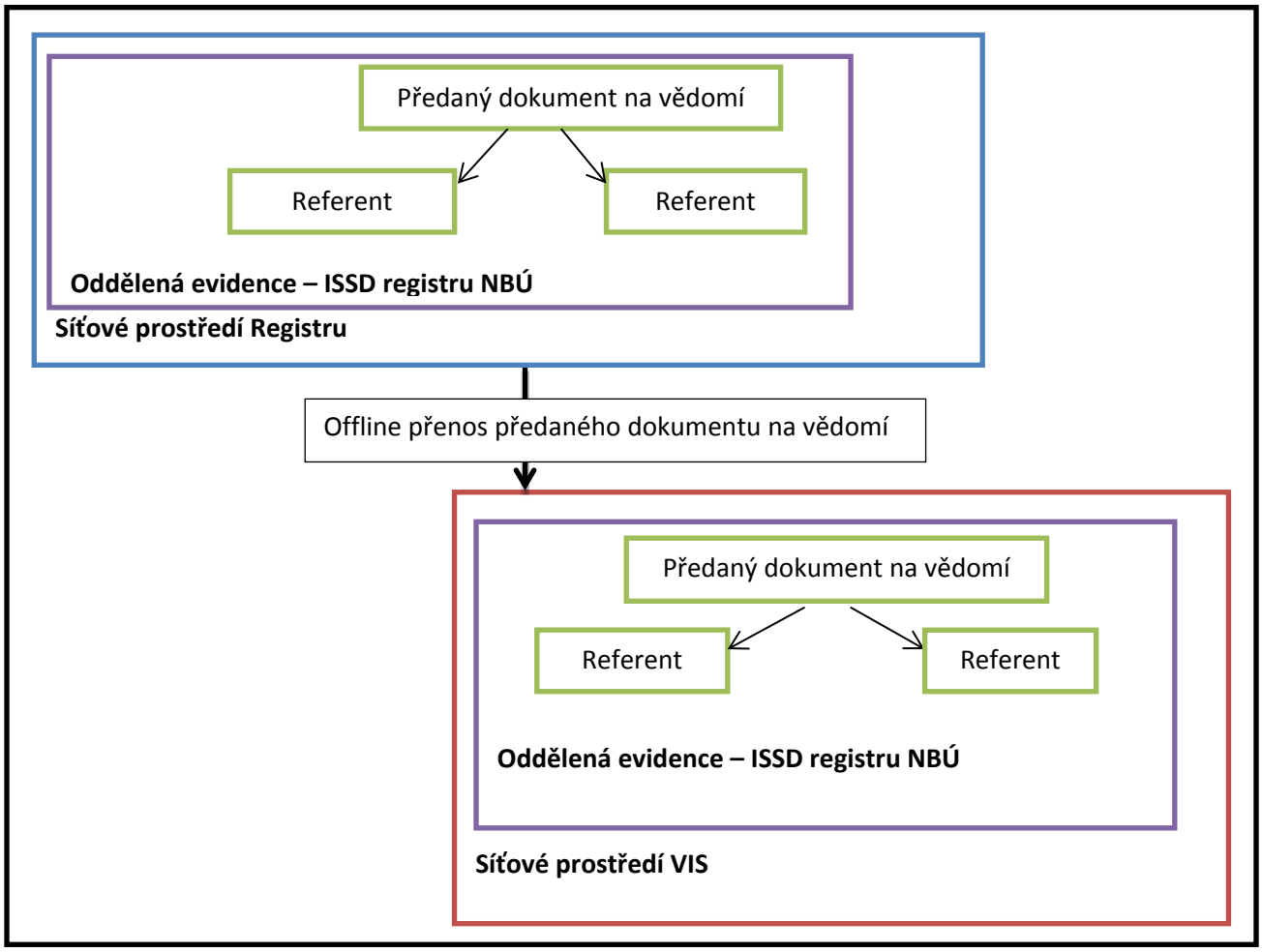
Dokument v oddělené evidenci ISSD registru NBÚ bude automaticky nebo manuálně předán jednomu nebo více referentům na vědomí na základě číselníku referentů.

obrázek č. 9



Dokument může být předán na vědomí v rámci ISSD registru NBÚ v obou síťových prostředích s ohledem na stupeň utajení.

obrázek č. 10



Řešení musí ve stavu na vědomí umožnit referentovi NBÚ nastavit návrh skartačního znaku a lhůty, při předání dokumentu na vědomí více referentům se do evidence zaznamená návrh nejvyššího skartačního znaku a nejdelší skartační lhůty. Stanovením skartačního znaku a lhůty se referentovi ukončí oprávnění přístupu k dokumentu. Skartační lhůta se počítá od data stanovení návrhu nejvyššího skartačního znaku a nejdelší skartační lhůty.

Detaily procesu předání dokumentu na vědomí budou specifikovány v předimplementační analýze.

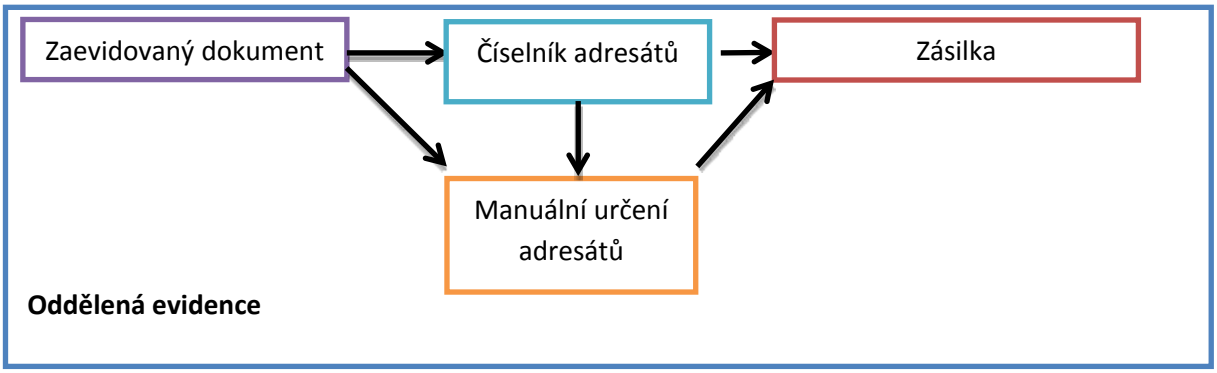
Oba ISSD v síťovém prostředí Registru umožní:

- Zobrazení a tisk všech administrativních pomůcek.
- Ke každému dokumentu (doručenému i vytvořenému) bude možno připojit novou textovou vrstvu (např. při změně nebo zrušení stupně utajení,…), ve které bude manuálně určeno umístění nového textu na dokumentu tak, aby nedošlo k překrytí obsahu dokumentu. Pokud se nový text nevejde na dokument, připojí se na další stránku, která se stane součástí dokumentu).
- Přílohy dokumentu lze odpojit s jejich následným zaevidováním nebo připojením k již zaevidovanému dokumentu (včetně přidání textových vrstev).

5.3.6 Odesílání vlastního dokumentu /distribuce

Pokud bude ze zaevidovaného dokumentu a číselníku jednoznačně určen adresát, dokument bude zařazen do fronty a bude vytvořena zásilka k odeslání (viz obrázek č. 11). Metadata zásilky budou upřesněna v rámci předimplementační analýzy. Každá zásilka bude vložena do dávky, dávky budou rozděleny dle původců. Jeden dokument může mít i více adresátů. Řešení musí umožnit ověření, opravu a manuální přidání určených adresátů, které provede pracovník registru.

obrázek č. 11

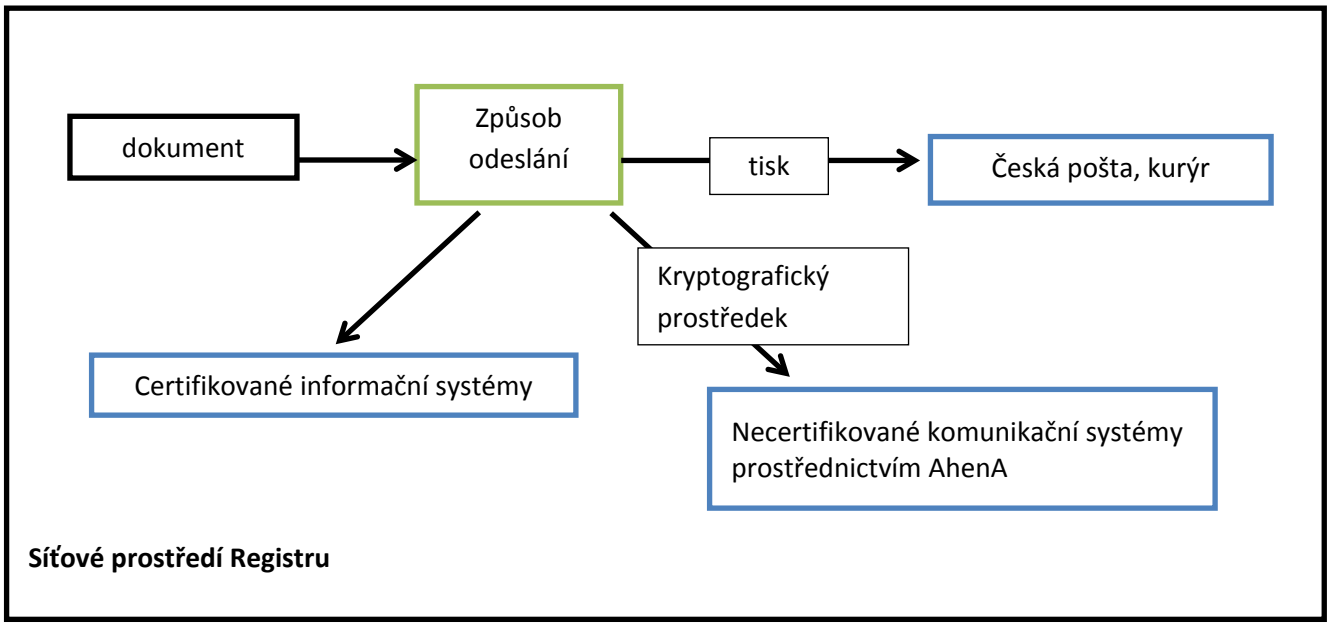


V oddělené evidenci jsou dokumenty k odeslání určeny na základě číselníku a budou zařazeny do dávek podle způsobů odeslání (certifikovaný informační systém, ISDS, kurýr,…).

Odesílání bude probíhat offline prostřednictvím přenosného vyměnitelného média (USB, CD, apod.).

V případě způsobu odeslání utajovaných dokumentů necertifikovaným systémem (viz obrázek č. 12), např. ISDS, musí řešení automaticky upozornit pracovníka registru na tuto situaci a na základě jeho potvrzení nabídnout příslušný kryptografický prostředek s ohledem na stupeň utajení.

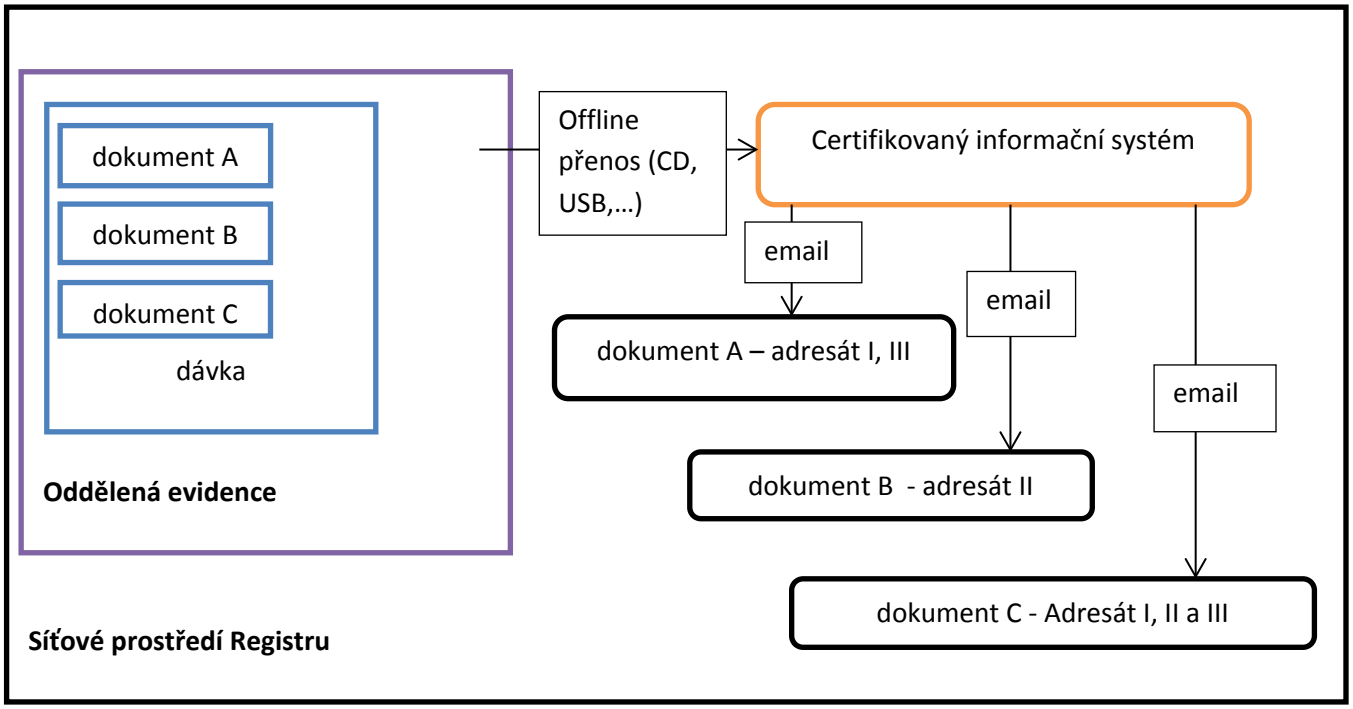
Obrázek č. 12



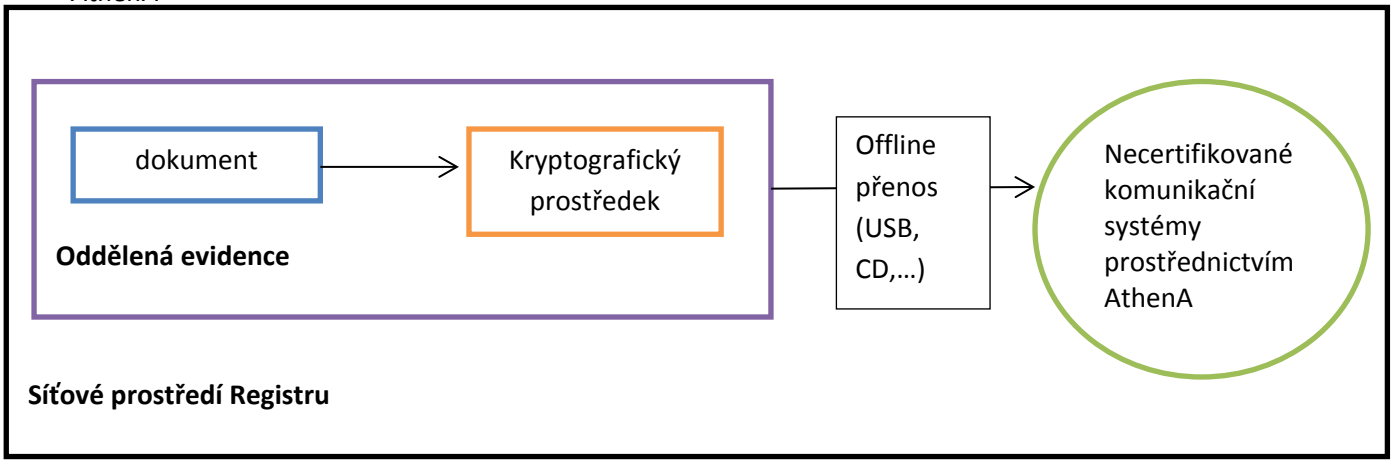
V současné době probíhá komunikace prostřednictvím třech certifikovaných informačních systémů třetích stran - jde o technologie typu email. Všechny systémy používají ke komunikaci elektronickou poštu postavenou na technologiích společnosti Microsoft (MS Exchange, MS Outlook, MS Office). Zadavatel požaduje, aby řešení vytvořilo datovou zprávu ve finální podobě s tím, že připraví programový kód, který na straně certifikovaného systému zajistí automatizaci distribuce. Zároveň pokud systém posílá informaci o převzetí datové zprávy adresátem (doručenka), bude přenesena k dokumentu do příslušné oddělené evidence.

Zadavatel v rámci předimplementační analýzy zajistí součinnost třetích stran při tvorbě komunikačního rozhraní s certifikovanými informačními systémy.

Obrázek č. 13 - Odeslání dokumentu prostřednictvím certifikovaných informačním systémem různým adresátům:



Obrázek č. 14 - Odeslání dokumentu necertifikovaným informačními systémy prostřednictvím AthenA



Odeslání dokumentu bude umožněno pouze z oddělených evidencí v rámci síťového prostředí Registru. Data potřebná pro odeslání dokumentu zadaná v oddělených evidencích v síťovém prostředí VIS budou přenášena do oddělených evidencí v síťovém prostředí Registru.

Při distribuci ISSD ústředního registru umožní po celou dobu uloženého dokumentu jeho odeslání dalšímu adresátovi s přidáním adresáta do seznamu zásilek.

Řešení při odeslání vlastního dokumentu musí být v souladu s platnými právními předpisy.

5.3.7 Ukládání a zapůjčování dokumentu

Ukládání a zapůjčování dokumentu musí být v souladu s platnou legislativou. Řešení umožní u zapůjčeného dokumentu vložení dalšího údaje (např. poznámky).

Řešení musí splňovat podmínky dlouhodobého důvěryhodného ukládání v souladu s platnými právními předpisy.

Detaily budou upřesněny v rámci předimplementační analýzy.

5.3.8 Změna/zrušení stupně utajení

Při změně nebo zrušení stupně utajení se přeeviduje dokument do nového JP (zápisy v JP musí být provedeny v souladu s přílohou č. 1 vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů). Informace o přeevidování včetně změny/zrušení (přeškrtnutí původního stupně utajení včetně odůvodnění) stupně utajení budou uvedeny v další textové vrstvě, kterou určí pracovník registru.

5.3.9 Stanovení skartační lhůty

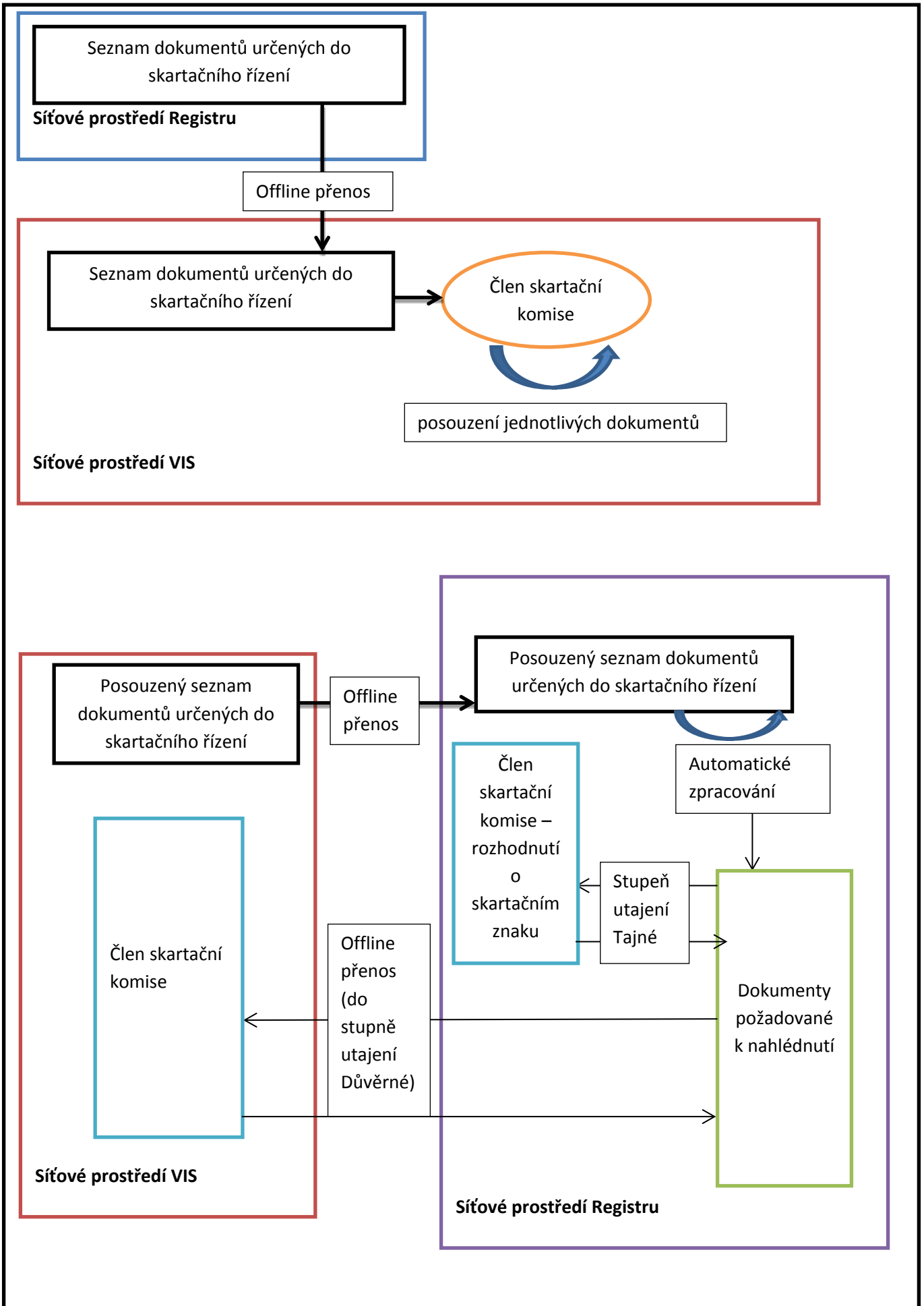
ISSD ústředního registru – dokumenty, které jsou určeny k uložení v ústředním registru, budou automaticky označeny skartačním znakem a lhůtou podle interního spisového a skartačního plánu.

ISSD registru NBÚ – dokumenty určené k uložení v registru NBÚ budou označeny skartačním znakem a lhůtou dle kapitoly Předání dokumentu na vědomí v ISSD registru NBÚ.

5.3.10 Skartační řízení

Řešení automaticky vytvoří v oddělených evidencích seznam dokumentů určených do skartačního řízení (obsah shodný se skartačním návrhem) pro posouzení skartační komisí a umožní přidání dalších dokumentů do seznamu. Seznam bude předán do síťového prostředí VIS, kde bude umožněno každému členovi skartační komise změnit skartační znak a lhůtu a označit dokument, který bude požadovat k náhledu. Doplněný seznam bude přenesen zpět do síťového prostředí Registru. Řešení umožní po posouzení poskytnutého dokumentu odsouhlasit, popř. změnit skartační znak a lhůtu, a pronést změnu k dokumentu. V případě změny skartačního znaku a lhůty musí být změna (nejvyšší skartační znak a nejdelší skartační lhůta) pronesena ke každému dokumentu s poznámkou, kdo, kdy a jakou lhůtu (skartační znak) určil.

obrázek č. 15 – skartační řízení



Řešení dále umožní provedení skartačního řízení v oddělených evidencích v souladu s platnými právními předpisy a NSESSS.

Po provedeném skartačním řízení řešení umožní vytvoření seznamu zničených dokumentů a seznam dokumentů předaných do archivu specializovaného/bezpečnostního.

Detaily procesu skartačního řízení budou upřesněny v rámci předimplementační analýzy.

5.3.11 Tisk

Řešení umožní tisk:

- administrativních pomůcek a jednacích protokolů dle zadaných kritérií
- dokumentu včetně všech přidaných textových vrstev během jeho celého životního cyklu
- všech vytvořených sestav
- štítků na obálky
- statistik
- aktuálního nastavení parametrů bezpečnostních a uživatelských práv pro oddělené evidence a ISSD
- seznamu uživatelů s uvedením role

Detaily budou upřesněny v rámci předimplementační analýzy.

5.3.12 Vyhledávání

Řešení umožní fulltextové vyhledávání dle zadaných kritérií (např. kombinace evidenčních údajů a obsahu, dle data přidělení dokumentu,…) napříč metadaty a obsahem dokumentů s možností použití přednastavených filtrů včetně použití booleovských operátorů. Dále umožní export vyhledaných dat do sestav (tabulkový program, např. excel) a jejich následné vytisknutí. Řešení umožní filtrovat v evidenci dokumentů (JP), řadit dle určených kritérií (např. vzestupně,…).

Detaily budou upřesněny v rámci předimplementační analýzy.

5.3.13 JP a podací deníky

V souladu s NSESS a platnými právními předpisy.

Detailní informace budou předmětem předimplementační analýzy.

5.3.14 Administrativní pomůcky

Řešení umožní ztvárnit, zobrazit a vytisknout všechny legislativou a NSESSS požadované administrativní pomůcky.

6 Požadavky na provozní prostředí

6.1 Specifikace prostředí systému

- systém bude provozován na serverech Windows Server 2016 ve virtualizovaném prostřední na platformě Hyper-V cluster Windows Server 2016.
- databázová platforma Microsoft SQL Server 2016 nebo novější
- klientská část musí umožňovat provoz v prostředí Remote Desktop Services na Windows Server 2016.

6.2 Škálovatelnost provozního prostředí

- Architektura musí být navržena tak, aby podporovala výkonnostní a kapacitní škálovatelnost, a to nejen na úrovni provozované infrastruktury, ale i na serverové a aplikační úrovni, několikanásobnou duplikací webových, databázových a souborových služeb.

6.3 Licence a limity

- dodávané řešení nebude zavádět další limity na množství zpracovávaných a ukládaných dat a dokumentů nad rámec limitů daných použitým HW a softwarovou platformou, dále nebudou omezeny limity na počet uživatelů i administrátorů.
- zadavatel zajistí na vlastní náklady pouze licence produktů společnosti Microsoft. Licence jiných výrobců musí zajistit na minimálně smluvní období dodavatel řešení.
- dodavatele poskytne zdrojové kódů řešení včetně jejich aktualizace při každém upgrade, zadavatel se zavazuje, že nebude tyto kódy měnit ani používat po dobu trvání smlouvy na servisní podporu poskytovanou dodavatelem .
- zadavatel požaduje, aby nabízené řešení při případném ukončení podpory bylo bez aktualizací, dále plně funkční bez jakýchkoliv omezení i dílčích funkcionalit

6.4 Produkční prostředí

- produkční prostředí bude zřízeno za účelem provozování systému, který bude poskytovat svou funkcionalitu nad standardními dokumenty, které vznikají běžným provozem NBÚ.

6.5 Testovací prostředí

- testovací prostředí bude zřízeno za účelem otestování funkcionality systému před jeho zprovozněním v produkčním prostředí. Testovací prostředí bude využíváno také při dodávce nové verze systému a pro účely školení zaměstnanců. Testovací prostředí bude sloužit pro ověřování nových funkcionalit řešení, případně nových technologií.

6.6 Zálohování systému a dat

- zálohování bude prováděno stávajícími prostředky NBÚ a není součástí požadovaného řešení. Zadavatel požaduje dokumentaci s popisem komponent a dat, které je nezbytné zálohovat. Dále dodavatel dodá dokument pro obnovení celého dodávaného řešení do stavu k datu zálohy. Zálohy a obnovu dat provádí zadavatel dle dokumentace dodavatele.

6.7 Požadavky na bezpečnost

- Řešení musí splňovat požadavky zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, včetně všech prováděcích předpisů.
- Detailní popis požadavků je uveden v Příloze č. 1 této specifikace.

6.8 Identifikace, autorizace a autentizace přístupů

- Zadavatel požaduje identifikaci a autorizaci uživatelů pro přístup do dodávaného řešení přes Active Directory, dodávané řešení musí podporovat Single sign-on až na úrovni remote desktop serveru.
- Autentizace přístupů se bude logovat do vlastního úložiště dodávaného řešení. Specifikace struktury logu je uvedena v sekci Bezpečnostní monitoring.
- Uživatelé řešení jsou v obou síťových prostředích stejní. Řešení identifikuje uživatele v každém síťovém prostředí na základě těchto atributů v Active directory : sAM Account name a osobního čísla (Employee ID). SID uživatelského účtu bude v každém síťovém prostředí rozdílné.
- Zadavatel rozšíří schéma uživatelského účtu v Active directory o informace týkající se osvědčení fyzické osoby a osvědčení fyzické osoby pro cizí moc, tedy o stupeň utajení a platnost osvědčení. Tyto atributy musí vždy řešení ověřovat, pokud se bude řešit přístup uživatele (referenta NBÚ) k dokumentům. Pokud uživatel (referent NBÚ) nesplňuje podmínky na seznámení, musí řešení zakázat přístup takovému uživateli.
- Řešení na základě číselníků musí vést informace zajišťující přehled oprávnění jednotlivců k dokumentům při jejich distribuci.

6.9 Bezpečnostní monitoring

Řešení musí splňovat požadavky na logování dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů a zároveň zadavatel požaduje, aby řešení zaznamenávalo a logovalo minimálně události typu:

- akce uživatelů
- akce administrátorů
- změny konfigurace,
- nestandardní stavy systému.

Dodané řešení musí umožňovat zpracování logů v systému SCOM.

Log musí být ve strukturovaném formátu s dostatečným popisem v dokumentaci, kterou poskytne Dodavatel řešení.

6.10 Provozní monitoring

Zadavatel poskytne technologii SCOM od společnosti Microsoft.

7 Integrace s ostatními řešeními

Zadavatel specifikuje další řešení, která budou integrována do dodávaného řešení a zároveň nejsou předmětem této veřejné zakázky.

7.1 Antivirová ochrana

- Antivirová ochrana bude zajištěna stávajícími prostředky NBÚ (antivirový systém ESET) a není součástí požadovaného řešení. Zadavatel požaduje integraci se stávajícím antivirovým systémem.

7.2 Kryptografický prostředek

- Zadavatel požaduje integraci s řešením, které je popsáno detailněji v sekci Příjem.
- Zadavatel požaduje, aby dodávané řešení umožňovalo využití více kryptografických prostředků, v současné době zadavatel požaduje integraci pouze s jedním kryptografickým prostředkem, tzv. HCryptC.

7.3 Komplexní systém integračních služeb pro implementaci nařízení eIDAS

Zadavatel zajistí v síťovém prostředí Registru implementaci řešení kvalifikovaných časových razítek a pečetí.

7.4 Skenovací linka s OCR

Společnost ICZ a.s., IČO 25145444, pod vedením pánů V. Dinuše, R. Urbana, J. Krtila a paní K. Klanicové, se podílela na předběžné tržní konzultaci ve smyslu § 36 odst. 4 zákona č. 134/2016, o zadávání veřejných zakázek.

- Zadavatel požaduje integraci. Skenovací linka s OCR je předmětem této veřejné zakázky. Zadavatel požaduje, skenování ovládat minimálně přímo ze skenovacího zařízení. OCR bude prováděn jak u analogových tak i u digitálních dokumentů, které nemají strojově čitelnou textovou vrstvu.
- Specifikace Skenovací linky s OCR je popsána v sekci Příjem.

8 Požadavky na vytvoření rolí

Pracovník registru – pracovník registru ÚR a registru NBÚ – všechny funkcionality kromě vytváření a změny formulářů, číselníků, přidávání, odebírání uživatelských práv a zřizování účtů

Referent NBÚ – náhled na přidělené dokumenty, možnost vyhledávání bez znázornění obsahu dokumentu (najde dokument, který hledá a požádá pracovníka registru o přidělení/zapůjčení dokumentu)

Správce aplikace – všechny funkcionality, včetně správy číselníků, vytváření jednoduchých formulářů, přidávání a odebírání uživatelských práv ze seznamu uživatelů, které řešení načítá z AD.

Provozní správce aplikace – má k dispozici funkcionality uvedené v roli Správce aplikace a dále, nastavování logů, rolí, konfigurace aplikace vůči technologiím, které využívá k provozu či s nimi jinak komunikuje, atd.

Bezpečnostní správce – nahlížení do nastavení logů a nahlížení do nich. Nesmí mít možnost logy žádným způsobem modifikovat.

Člen skartační komise – náhled na dokumenty zařazené do skartačního řízení.

Archivář – náhled na přidělené dokumenty, předání do digitálního archivu (příprava SIP balíčků), posouzení dokumentů ve skartačním řízení.

Mezinárodní kontrola – pouze náhled bez oprávnění jakékoli modifikace dané agendy podle původce (kontrola z NATO náhled jen do NATO agendy), nastaví administrátor, jazyková mutace AJ.

9 Automatizované procesy

Společnost ICZ a.s., IČO 25145444, pod vedením pánů V. Dinuše, R. Urbana, J. Krtila a paní K. Klanicové, se podílela na předběžné tržní konzultaci ve smyslu § 36 odst. 4 zákona č. 134/2016, o zadávání veřejných zakázek.

Řešení bude využívat šablony, číselníky a formuláře.

Řešení umožní centrálně evidovaný oběh dokumentu v celém životním cyklu, pevné spojení dat, která byla vygenerována na základě oběhu s dokumentem a ad hoc definování oběhu, tj. možnost předem neplánovaného předání dokumentu referentovi NBÚ.

Dále umožní definování souběžných i následných kroků (paralelní či postupné zpracování).

Dokumenty určené referentem NBÚ (určeno v síťovém prostředí VIS) pro odeslání mimo NBÚ budou offline přeneseny do síťového prostředí Registru, který zabezpečí odeslání dokumentu.

Řešení umožní zastupování.

Ke každému dokumentu zobrazí informace z transakčního protokolu, které budou možné následně filtrovat (např. zobrazení dokumentu, předání dokumentu, …)

Detaily budou upřesněny v rámci předimplementační analýzy.

10 Kapacitní požadavky

V současné době jsou v síťovém prostředí 4 pracovníci registru, v síťovém prostředí VIS cca 30 referentů.

Objem přijímaných dat je cca 1GB/měsíc = cca 1 000 dokumentů/měsíc (1 dokument cca 2 soubory).

11 Požadavky na dokumentaci

Dokumentace předávaného stavu – popis kde, jak a v jaké konfiguraci bylo řešení implementováno

Dokumentace Administrátorská - pro roli Provozní správce a Bezpečnostní správce aplikace

Dokumentace Zálohování a obnovení řešení

Dokumentace uživatelská s ohledem na jednotlivé role

Ke každé roli požaduje zadavatel vlastní dokumentaci, včetně jazykové mutace v angličtině

12 Migrace dat z Agile do nového řešení

Společnost ICZ a.s., IČO 25145444, pod vedením pánů V. Dinuše, R. Urbana, J. Krtila a paní K. Klanicové, se podílela na předběžné tržní konzultaci ve smyslu § 36 odst. 4 zákona č. 134/2016, o zadávání veřejných zakázek.

Migrace – převod dat ze stávajícího evidenčního systému při zachování stávající evidence. Při migraci bude Zadavatel koordinovat spolupráci nového Dodavatele se stávajícím Dodavatel řešení. Náklady vůči stávajícímu Dodavateli budou hrazeny Zadavatelem.

Časový plán Migrace je uveden v Harmonogramu prací.

Další detailní postupy a rozsah migrace bude předmětem předimplementační analýzy.

13 Certifikace – schválení řešení pro provoz v síťovém prostředí registru

Certifikace IS proběhne dle zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Certifikace IS proběhne ve dvou fázích ve vztahu k příslušným etapám.

- Etapa I. - po implementaci řešení před předáním do pilotního provozu. Je nutné, aby dodavatel předal v části Akceptace navrhovaného řešení dokumentaci s informacemi popsanými v příloze č.8 ZD. Současně Zadavatel musí předat Projektovou a provozní bezpečnostní dokumentaci. Vlastní proces certifikačního řízení proběhne na konci etapy B2 Etapa I. projektu.

Etapa II. - certifikačního řízení proběhne ve Fázi II. Projektu v etapě A, část Předání etapy A.

Při jakékoli změně v řešení (upgrade) předá zhotovitel objednateli dokumenty nezbytné k posouzení certifikačním orgánem.

14 Harmonogram implementace

Společnost ICZ a.s., IČO 25145444, pod vedením pánů V. Dinuše, R. Urbana, J. Krtila a paní K. Klanicové, se podílela na předběžné tržní konzultaci ve smyslu § 36 odst. 4 zákona č. 134/2016, o zadávání veřejných zakázek.

Zadavatel požaduje implementaci řešení ve dvou fázích. Přičemž předmětem první fáze (Etapa I.) je implementace celého řešení v rámci komunikační a systémové infrastruktury do stupně utajení „Tajné“ a předmětem fáze (Etapa II.) je implementace v rámci komunikační a systémové infrastruktury do stupně utajení „Důvěrné“. Migrace dat z původního řešení do nového bude probíhat již v Etapě I. a bude ukončena před předáním Etapa II. do pilotního provozu.

Etapa II. Musí začít nejpozději do 2 pracovních týdnů od ukončení Etapy I.

V tabulce níže Zadavatel ve sloupci Ukončení uvádí číselné hodnoty. Hodnota „1“ odpovídá pracovnímu týdnu.

Aktivity	Ukončení	Základní výstupy	Provádí
Etapa I.			
Podpis smlouvy	D	Smlouva	Zadavatel, Dodavatel
Inicializační schůzka	D+1	Zápis	Zadavatel, Dodavatel
Krok A – Předimplementační analýza			
Analýza požadavku na řešení	D+8	Zápis	Zadavatel, Dodavatel
Představení návrhu s možností připomínkování	D+11	Pracovní dokument nabízeného řešení	Zadavatel, Dodavatel
Akceptace navrženého řešení	D+14(A)	Finální dokument nabízeného řešení Začátek certifikačního řízení, na základě předané dokumentace dle přílohy č. 1 specifikace VZ	Dodavatel Zadavatel
Krok B – Instalace, konfigurace, testování			
Příprava infrastruktury	A+6	technické zabezpečení	Zadavatel
Instalace, konfigurace řešení a akceptační testování	A+21	instalační a konfigurační	Zadavatel, Dodavatel

		sada, instalační příručka, protokol o instalaci a akceptačním testování	
Integrace s aplikacemi třetích stran	A+24	instalační a konfigurační sada, instalační příručka, protokol o instalaci a akceptačním testování	Zadavatel, Dodavatel
Předání etapy B1	A+26 (I)	předávací protokol	Zadavatel, Dodavatel
Krok C – Integrace, testování			
Analýza integrace a migrace	A	popis migrace a integrací	Dodavatel, Impromat
Vývoj řešení a testování	A + 4	integr. rozhraní, migrační skripty - **migrace je postupná finalizace je před předáním do pilotního provozu Etapa II.**	Dodavatel
Implementace pro účely pilotního provozu	I	protokol o akceptačním testování	Zadavatel, Dodavatel
Implementace pro účely rutinního provozu	O	předávací protokol	Zadavatel, Dodavatel
Předání etapy B2	1	předávací protokol Certifikace IS	Zadavatel, Dodavatel
Krok D – Školení			
školení uživatelů	1	prezenční listiny, uživatelská příručka, administrátorská příručka, školící texty	Zadavatel, Dodavatel
školení administrátorů			
Předání etapy C	S	předávací protokol	Zadavatel, Dodavatel
Krok E – Pilotní provoz			

Pilotní provoz	S+7	evidence poruch, evidence požadavků	Zadavatel, Dodavatel
Vyhodnocení pilotního provozu	S+9	návrh rozvoje	Zadavatel, Dodavatel
Předání etapy D	S+10 (P)	předávací protokol	Zadavatel, Dodavatel
Předání Etapa I.	**P**	předávací protokol zakázky + dokumentace popisující stav implementovaného řešení	Zadavatel, Dodavatel
Fakturace za Etapa I.	**P+2**	Platba po akceptaci implementovaného řešení	Zadavatel,
Konec Etapa I. a začátek Etapa II.			
Krok F – Instalace, konfigurace, testování			
Příprava infrastruktury	F+2	technické zabezpečení	Zadavatel
Instalace, konfigurace řešení a akceptační testování	F+10	instalační a konfigurační sada, instalační příručka, protokol o instalaci a akceptačním testování	Zadavatel, Dodavatel
Předání Kroku F	F+11	předávací protokol + Certifikace IS	Zadavatel, Dodavatel
Krok G – Školení			
školení uživatelů	1	prezenční listiny, uživatelská příručka,	Zadavatel, Dodavatel
školení administrátorů		administrátorská příručka, školící texty	
Předání Kroku G	H	předávací protokol etapy + ukončení migrace dat z Etapa I.	Zadavatel, Dodavatel

Krok H – Pilotní provoz			
Pilotní provoz	H+5	evidence poruch, evidence požadavků	Zadavatel, Dodavatel
Vyhodnocení pilotního provozu	H+6	návrh rozvoje	Zadavatel, Dodavatel
Předání Kroku H	H+6 (P)	předávací protokol	Zadavatel, Dodavatel
Předání Etapa II.	**P**	předávací protokol zakázky + dokumentace popisující úplný stav implementovaného řešení	Zadavatel, Dodavatel
Fakturace Etapa II.	**P+2**	Platba po akceptaci implementovaného řešení	Zadavatel

15 Softwarová maintenance

Dodavatel poskytne maintenance na kompletní řešení na dobu 5 let od podpisu smlouvy, přičemž platby budou probíhat ročně ve výši rovnoměrného rozložení do jednotlivých let.

Zadavatel nepožaduje maintenance na produkty uvedené v kapitole 6.1. „Specifikace prostředí systému“.

Dodavatel bude implementované řešení udržovat v souladu s dotčenou legislativou, bez nutnosti vyzvání objednatele, bude v souladu s termínem účinnosti legislativní změny nasazovat nové verze řešení.

Bude zajištěna pravidelná údržba celého nabízeného řešení.

Součástí maintenance bude i aktualizace dokumentace skutečného stavu a tvorba podkladů pro certifikaci schvalování upgrade.

Požadavek na rozdílovou příručku – po určitém počtu rozdílových příruček vydat jednu verzi, která obsahuje zapracované změnové příručky v jednom dokumentu.

Zadavatel požaduje na úpravy – změny funkcionalit požadované zadavatelem v prvním roce podporu 30 MD a ve čtyřech následujících letech podporu 10MD/rok. Zadavatel požaduje, aby nevyčerpaná podpora byla převedena do následujících let platnosti smlouvy.

Dále Zadavatel požaduje do cenové nabídky zahrnout cenu za 150 MD, které budou čerpány v případě dalších úprav nad rámec MD uvedených v odstavci výše, formou samostatného plnění na základě objednávek.

16 Servisní podpora

Zadavatel požaduje uzavřít servisní smlouvy na 5 let od předání celého díla. Dodavatel rovnoměrně rozloží platbu za servisní podporu do každého roku. Zadavatel zaplatí každý rok jednorázově platbu ve výši 1/5 z celkové ceny servisní podpory.

Podpora bude zahrnovat:

- řešení uživatelských i administrátorských problémů s provozem nabízeného řešení – v souladu s tabulkou priorit níže
- uživatelské i provozní konzultace k používání nabízeného řešení,
- Součinnost při obnově nabízeného řešení po havárii,
- používání telefonické podpory formou Hotline

Uvedené činnosti budou poskytovány formou přítomnosti v prostorách zadavatele a telefonickou konzultací.

Podpora bude zadavateli poskytována prostřednictvím systému Help Desk dodavatele a telefonní konzultací.

Dodavatel v nabídce uvede kontakt na Helpdesk a Hotline.

Tabulka priorit (dle jednotlivých kategorií):

Priorita	*Charakteristika problému*	*Reakční doba od nahlášení problému*
Vysoká	• řešení nelze spustit nebo dochází ke ztrátě dat, • nebo řešení lze spustit, ale nefunguje některá z klíčových funkcí a neexistuje dočasné náhradní řešení • nebo existují zásadní problémy s výkonem klíčových funkcí nabízeného řešení	4 pracovní hodiny s fixem do 8 hodin v pracovních dnech v době od 8:00 do 16:00 hodin
Střední	• nefunguje některá z méně důležitých funkcí nabízeného řešení • problémy s výkonem u důležitých funkcí nabízeného řešení	8 pracovních hodin s fixem 16 hodin v pracovních dnech v době od 8:00 do 16:00 hodin
Nízká	• ostatní problémy	40 pracovních hodin v pracovních dnech v době od 8:00 do 16:00 hodin

17 Školení

Školení proběhne dle Etap v jednotlivých fázích v harmonogramu prací. Školení Administrátorů a uživatelů proběhne zvlášť, přičemž Administrátoři musí být obeznámeni se základními principy funkcionalit celého řešení, aby byli schopni reagovat na všechny vzniklé situace v provozu řešení.

Zadavatel dále požaduje v každém roce trvání smlouvy školení uživatelů i administrátorů v sídle zadavatele v celkové délce 4h/rok.