Příloha č. 1 – Specifikace a rozsah předmětu plnění

Obsah

Předmět zadávacího řízení

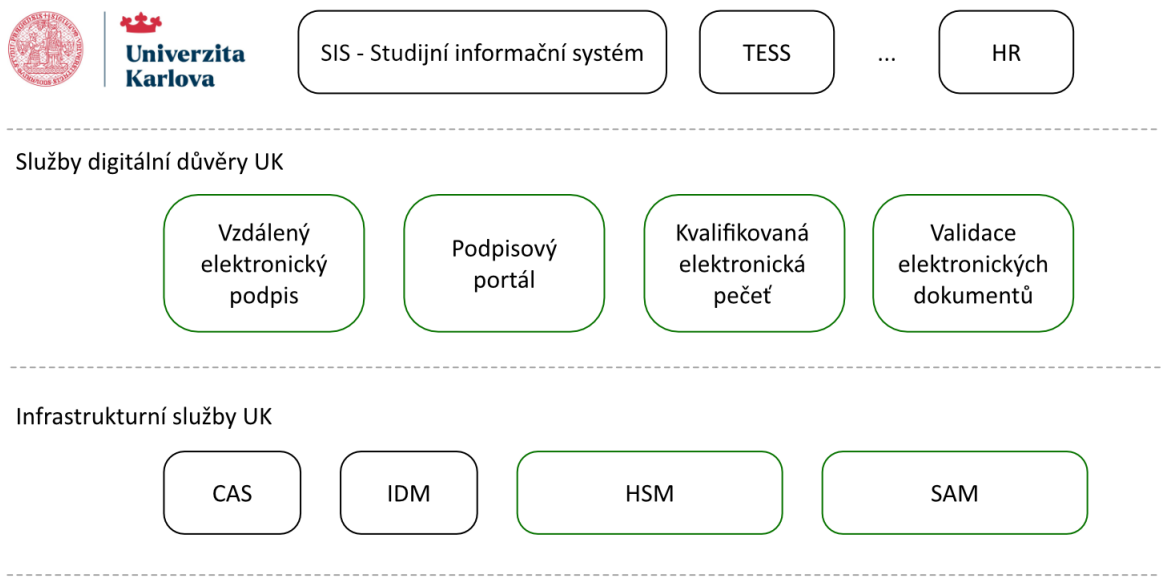
Univerzita Karlova (dále jen UK) vystupuje v rámci vybraných procesů souvisejících se studiem (např. přijímací řízení) jako orgán veřejné moci, a proto musí mimo jiné splňovat požadavky zákona č. 297/2016 o službách vytvářejících důvěru pro elektronické transakce (dále také služby digitální důvěry), resp. nařízení eIDAS. Díky tomu musí UK v dotčených procesech studijního systému využívat kvalifikovaný el. podpis, kvalifikované el. pečeti a všechny související dokumenty opatřovat kvalifikovaným el. časovým razítkem.

Tyto požadavky vyžadují realizovat nejenom významné změny v samotném studijním systému, ale vybudovat i příslušné centrální služby vytvářející důvěru, které budou novým studijním informačním systémem využívány. Dále bude nutné tyto služby integrovat do dalších částí informačního systému UK jako je např. spisová služba TESS a další. Jedná se o následující služby:

- vzdálený kvalifikovaný elektronický podpis včetně podpisového portálu,
- kvalifikovaná elektronická pečeť,
- validace elektronických dokumentů.

Součástí předmětu veřejné zakázky je integrace dodaných služeb se stávající spisovou službou TESS. eSSL TESS bude integrována jako pilotní aplikace, pomocí které bude možné ověřit jednotlivé služby, které budou následně implementovány i do nového studijního systému.

Záměrem UK je v budoucnu tyto služby dále poskytovat i jiným univerzitám, které již nyní využívají, nebo budou využívat i jiné části informačního systému UK.



Obrázek 1 / Logické schéma nově budované vrstvy služeb vytvářejících důvěru.

Služby vytvářející důvěru

Služba	Význam
Vzdálený elektronický podpis	Služba elektronického podpisu, která využívá centrálně spravované klíče pod ochranou HSM a SAM. • Certifikáty pro zaručený podpis vydává CESNET. • Certifikáty pro kvalifikovaný podpis vydává vybraný kvalifikovaný poskytovatel dle požadavků UK.
Podpisový portál	Zajišťuje jak aplikační služby pro objednání podpisu informačním systémem UK, tak i grafické uživatelské rozhraní pro vyřizování podpisů uživateli.
Kvalifikovaná elektronická pečeť	Poskytuje aplikační rozhraní pro vytváření kvalifikovaných elektronických pečetí.
Validace elektronických dokumentů	Validace prvků elektronického zabezpečení dokumentu (elektronický podpis, pečeť, časové razítko) a integrity dokumentu na základě přednastavených politik prostřednictvím aplikačního i uživatelského rozhraní.

Infrastrukturní služby

Služba	Význam
Hardware Security Module (HSM)	Zajistí bezpečné prostředí pro práci s privátními klíči, na nichž bude založen elektronický podpis a pečeť. Zařízení musí splňovat QSCD certifikaci, aby jej bylo možné použít pro službu vzdáleného kvalifikovaného podpisu.
Signature Activation Module (SAM)	Certifikovaný kvalifikovaný prostředek pro vyváření el. podpisů a pečetí (QSCD) nezbytný pro vytváření kval. el. podpisů uživatelů a pro vytváření kval. el. pečetí pro další univerzity.

Implementační služby

Služba	Význam
Implementace řešení	Implementační služby minimálně v rozsahu • Vstupní analýza, cílový koncept • Implementace testovacího a produkčního prostředí • Školení a dokumentace
Integrační služby	• Podpůrné služby a konzultace pro integraci jednotlivých systémů prostřednictvím aplikačních rozhraní

	• Integrace se spisovou službou TESS
Podpora řešení	• Produktová podpora dodaných řešení • Servisní podpora související s provozem řešení včetně částečné správy ze strany QTSP pro kvalifikované části řešení

Tento dokument obsahuje definici služeb vytvářejících důvěru v souladu s legislativními požadavky a podrobnou specifikaci požadavků na jejich praktickou implementaci odpovídající velikosti organizace, jejím potřebám, aktuálnímu stavu a komplexnosti IT prostředí UK.

Interoperabilita s ČVUT

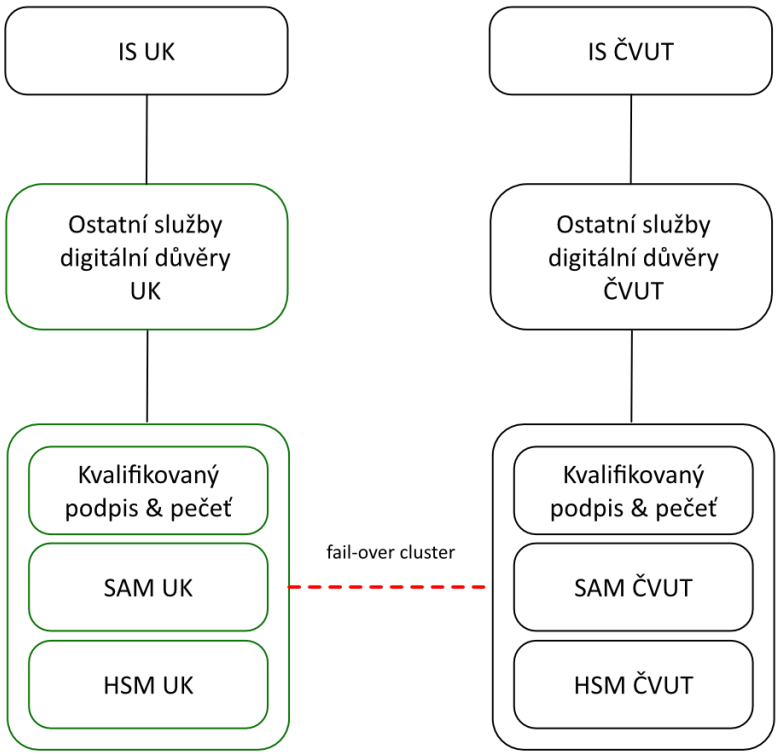
ČVUT již několik let provozuje obdobnou sestavu služeb digitální důvěry a uvažovaných technologií, která aktuálně postupuje aktualizaci na nejnovější verze technologií plně kompatibilní s připravovanými standardy dle novelizovaného nařízení eIDAS 2.0. Jedná se o řešení postavené na komponentách vyhovujících výše uvedeným technologickým požadavkům

- Síťové HSM moduly certifikované dle EN 419 221-5
- SAM moduly certifikované dle CEN 419 241-2
- Řešení vzdáleného kvalifikovaného podpisu certifikované dle CEN 419 241-2 s podporou CSC API
- Řešení kvalifikované el. pečeti využívající výše uvedené certifikované HSM a SAM moduly

Vzhledem k tomu, že i ČVUT poskytuje výše uvedené služby digitální důvěry i pro další univerzity, plánují proto UK společně s ČVUT vytvoření mezi univerzitního fail-over clusteru, který zvýší dostupnost řešení. Cluster je v této etapě budování služeb vytvářejících důvěru především na úrovni vzdáleného kvalifikovaného el. podpisu a kvalifikované el. pečeti včetně souvisejících podkladových HW/SW komponent (HSM, SAM).

Vytvoření tohoto fail-over clusteru umožní oběma univerzitám garantovat dostupnost kritických služeb s minimálními dopady na stávající služby a aplikace a zajistit tyto služby ve vysoké dostupnosti nejenom pro jejich vlastní potřebu, ale i pro další propojené univerzity.

Provozování služeb vytvářejících důvěru pracujících přímo s el. dokumenty, včetně jejich ověřování, archivace a ukládání bude zajištěn jednotlivými univerzitami. Cílovým záměrem UK Praha je vybudování fail-over clusteru s využitím řešení na ČVUT i pro tyto služby. Technické řešení poptávaných služeb vytvářejících důvěru musí vybudování fail-over clusteru umožnit.



Obrázek 2 / Logické schéma fail-over clusteru

Podrobné informace o aktuálně používaných/nasazovaných technologiích v prostředí ČVUT budou případnému zájemci poskytnuty na základě uzavřeného NDA.

Specifikace služeb vytvářejících důvěru

Vzdálený elektronický podpis

V rámci modernizace interních procesů směřujících k plné digitalizaci UK doporučujeme vybudování služby vzdáleného kvalifikovaného a zaručeného el. podpisu, aby bylo možné tyto služby podpisů využívat v libovolném prostředí koncových uživatelů – různé OS, různé webové prohlížeče a různé mobilní platformy.

Vzhledem k legislativním a praktickým požadavkům požaduje UK podporu nejenom pro zaručené el. podpisy založené na interních certifikátech, ale i pro menší skupinu uživatelů kvalifikované el. podpisy od zvoleného kvalifikovaného poskytovatele.

Z důvodů zpětné kompatibility bude minimálně po přechodnou dobu nezbytně nutné, aby bylo možné služby vzdáleného podpisu využívat i klasickými aplikacemi, které standardně podporují práci s čipovými kartami a tokeny.

Vzhledem k tomu, že takováto služba je především pouze podpisovou metodou, musí být rovněž zajištěna příslušná integrace a uživatelské rozhraní pro její využívání, viz následující položka Podpisový portál.

Požadavky

#	Požadavek
VEP01	Řešení vzdáleného podepisování musí splňovat certifikaci EN 419 241-2: Protection Profile for QSCD for Server Signing.

VEP02	Řešení musí obsahovat systém komponent pro řízení životního cyklu certifikátů, v takové formě, aby uživateli (na základě oprávnění) s minimálním množstvím interakce zprostředkovalo:
	• vydání certifikátu:
	  ○ vygenerování privátního klíče na HSM,
	  ○ vytvoření žádosti o certifikát,
	  ○ odeslání žádosti o certifikát na certifikační autoritu,
	  ○ import certifikátu,
	• obnovování certifikátu,
	• zneplatnění certifikátu.

VEP03	Součástí řešení musí být zajištění procesu komunikace s kvalifikovanou certifikační autoritou za účelem automatické práce s certifikátem (žádost, obnova, příp. další poskytované operace) pro kvalifikované certifikáty vydané tímto poskytovatelem služeb.
VEP04	Řešení zajistí uživatelům prvotní vydání kvalifikovaného certifikátu prostřednictvím SAM modulu ve spolupráci s HSM na základě platného kvalifikovaného certifikátu od zvoleného kval. poskytovatele uloženého na certifikovaném nebo systémovém úložišti.
VEP05	Uživatel musí mít oprávnění operovat pouze s vlastními certifikáty a klíči.
VEP06	Řešení musí obsahovat komponenty pro aplikace, které kvalifikovaný certifikát využívají, jako jsou aplikace pro el. podepisování, ověřování identity uživatele apod.
VEP07	Řešení zprostředkuje uživateli možnost elektronicky podepsat dokument v rámci jeho počítače skrze standardní systémové prostředky (platforma MS Windows).
VEP08	Řešení musí být integrovatelné s IDM UK pro synchronizaci uživatelů
VEP09	Řešení musí být schopno provést autentizaci za pomocí externího ověření za pomoci AD/Radius, SAML 2.0, nebo Web Browser SSO (NTLM/Kerberos, apod).
VEP10	Autentizace uživatele vůči řešení probíhá minimálně pomocí SSO, certifikátem, uživatelské jméno + další faktor.
VEP11	Pro potřeby autorizace požadavků na kvalifikovaný el. podpis bude využíváno stávající řešení více faktorové autentizace/autorizace.
VEP12	Autorizace uživatele pro provedení operací s certifikátem vůči řešení pomocí minimálně uživatelem definovaného PINu, uživatelem definovaného hesla (zaručený el. podpis) nebo prostřednictvím 2FA autorizace (kvalifikovaný el. podpis).
VEP13	Řešení poskytne veškeré své služby prostřednictvím API rozhraní.
VEP14	Základní služba el. podpisu musí být dostupná prostřednictvím standardizovaného API dle specifikace CSC (Cloud Signature Consortium) resp. dle ETSI TS 119 432

VEP15	Licenčně musí být veškerá funkcionalita dostupná nejméně pro 1000 uživatelů nebo zařízení. Licence musí být přenositelná v rámci prostředí zadavatele.

Podpisový portál

Pro zajištění komfortního podepisování el. dokumentů uživateli v rámci UK (personál, studenti, …) různými podpisovými metodami v závislosti na potřebách konkrétních procesů či dokumentů, je třeba zajistit jednoduché a zároveň intuitivní uživatelské rozhraní – jednotný podpisový portál.

Dále je třeba zajistit inteligentní řízení jednotlivých podpisových procesů v souladu s podpisovým řádem UK, ale i adhoc, včetně uchovávání auditních údajů nezbytných pro případné budoucí prokazování průběhu procesu.

Role podpisového portálu není tedy jenom o uživatelském rozhraní pro koncové uživatele, ale i o řízení procesů podepisování a také zpřístupnění různých podpisových metod jednotlivým aplikacím pomocí jednotného aplikačního rozhraní (API).

Požadavky

#	Požadavek
PP01	Řešení musí disponovat uživatelskou částí ve formě grafického uživatelského rozhraní (GUI) dostupného přes internetový prohlížeč (bez závislosti na konkrétním operačním systému, nebo použitém prohlížeči) optimalizované i pro mobilní zařízení, která zajistí dále uvedené funkce:

PP01a	• podpisové workflow, které uživatelům nabídne minimálně funkce:
	  ○ podepsání dokumentů
	  ○ odmítnutí podepsání dokumentu (s nutností napsat komentář)
	  ○ odvolání požadavku na podpis zadavatelem
	  ○ náhled na dokumenty k podpisu (včetně zobrazení příloh dokumentu)
	  ○ možnost stažení dokumentů

PP01b	• podepisování dokumentů jednotlivě i hromadně
PP01c	• definice termínu, kdy nejpozději musí k podpisu dojít
PP01d	• evidenci podepsaných dokumentů
PP01e	• uživatelské notifikace
PP02	Řešení musí být schopno produkovat elektronické podpisy v úrovních: • Kvalifikovaný elektronický podpis • Zaručený elektronický podpis založený na kvalifikovaném certifikátu • Zaručený elektronický podpis • Prostý elektronický podpis
PP03	Řešení musí nabízet množinu podpisových metod, kterými umožní vytvářet elektronické podpisy minimálně v rozsahu: • QSCD čipové karty a tokeny (minimálně v rozsahu zařízení uznaných jako QSCD v ČR) • Lokální keystory operačních systémů

	• Služby vzdáleného kvalifikovaného podpisu buď hostované a provozované on-site, nebo v podobě služby třetí strany • BankID Sign • Podpis stylusem (případně prstem) na displej mobilního zařízení (mobilního telefonu, tabletu apod.) • Prostý podpis typu Click-to-sign
PP04	Řešení musí být schopno dle metadat automaticky vybrat nejvhodnější podpisovou metodu pro přihlášeného uživatele a konkrétní dokument, tak aby výsledkem byl elektronický podpis v dostatečné kvalitě / úrovni, dle požadavku žádajícího o podpis
PP05	Řešení musí nabízet služby prostřednictvím webových rozhraní API pro automatizaci zadávání dokumentů k podpisu
PP06	Řešení musí umožnit dokument k podpisu zadat ručně přímo z GUI
PP07	Řešení musí být schopno dokumenty k podpisu třídit do logických adresářů
PP08	Řešení musí být integrovatelné s IDM UK pro synchronizaci uživatelů
PP09	Řešení musí podporovat minimálně režimy podpisu: • Okamžitý – vyvolání podepsání konkrétního uživatele přímo z externího systému a okamžité vyřízení podepsání • Odložený – předání dokumentu k podepsání do řešení, uživatel má možnost podpis vyřídit později („až se mu to hodí“)

PP10	Řešení musí být schopno vytvářet vizualizované i nevizualizované podpisy. Pro vizualizace musí být splněno:
	• Jsou konfigurovatelné každým uživatelem, uživatel může mít vytvořeno více různých vizualizací
	• Obsahují minimálně jméno a příjmení podepisujícího, informaci, že se jedná o elektronický podpis a datum podpisu
	• Do vizualizace lze vložit i grafické prvky (např. logo společnosti)
	• Vizualizace jsou do dokumentu umísťovány:
	  ○ Na určené místo, dle požadavku zadavatele
	  ○ Do předpřipravených podpisových polí (dle PDF specifikace)
	  ○ Libovolně v dokumentu podepisujícím, pokud není využité ani jedno z předchozích

PP11	Řešení umožňuje využívat služby vzdáleného el. podpisu podporující standardní API dle specifikace CSC (Cloud Signature Consortium) resp. ETSI TS 119 432
PP12	Řešení si ukládá auditní log operací prováděných jednotlivými uživateli
PP13	Řešení umožňuje na podpis uživatele navázat dodatečným automatickým zpracováním za využití dalších služeb z této specifikace, konkrétně: přidání el. pečetě na dokument či časového razítka.
PP14	Řešení umožňuje podpis dokumentu i externím uživatelem mimo uživatelskou bázi UK.

Kvalifikovaná elektronická pečeť

V závislosti na konkrétních procesech vyžaduje UK pečetění vybraných dokumentů kvalifikovanou elektronickou pečetí. Z tohoto důvodu UK požaduje dodání řešení, které podporuje vytváření kvalifikovaných el. pečetí jménem UK s rozšiřitelností na možnost vytváření kvalifikované el. pečeti i pro jiné subjekty (univerzity).

Vytváření kvalifikované el. pečeti musí dále podporovat přidávání kvalifikovaných časových razítek k vytvářeným pečetím.

V případě zpřístupnění služby kvalifikované el. pečeti i pro další subjekty mimo UK bude vyžadovat využití certifikovaného SAM modulu, obdobně jako v případě služeb vzdáleného el. podpisu.

Požadavky

#	Požadavek
EP01	Podpora vytváření el. pečetí ve formátu PAdES v profilech -BES a -T
EP02	Podpora vytváření el. pečetí ve formátu CAdES v profilech -BES a -T
EP03	Podpora vytváření el. pečetí ve formátu XAdES v profilech -BES a -T
EP04	Podpora vytváření el. pečetí ve formátu ASiC v profilech -BES a -T
EP05	Podpora vytváření el. pečetí ve formátu JAdES v profilech -BES a -T
EP06	Podpora vytváření el. pečetí ve formátu S/MIME v profilech -BES a -T
EP07	Podpora vložení kvalifikovaného elektronického časového razítka od externích kvalifikovaných poskytovatelů služeb vytvářejících důvěru
EP08	Kontrola platnosti používaných certifikátů
EP09	Práce s více různými klíči / certifikáty
EP10	Podpora využití technologií pro bezpečné ukládání kryptografických klíčů pomocí kvalifikovaného prostředku pro vytváření pečetí typu HSM
EP11	Možnost auditu vykonávaných operací a změn konfigurace
EP12	Vytváření vizualizovaných i nevizualizovaných pečetí v PDF
EP13	Možnost konfigurovat vizualizace pečeti (včetně možnosti parametricky ovlivnit podobu výsledné vizualizace při volání webové služby pečetění)
EP14	Podpora využití certifikovaného SAM modulu pro sdílení služby kvalifikované el. pečeti

Validace elektronických dokumentů

V UK vzniká velké množství vlastních dokumentů (týká se i doručených), u kterých je zapotřebí v případě, že obsahují certifikát (el. podpis, pečeť, časové razítko), validovat, a tak potvrdit platnost a správnost vložení certifikátu do dokumentu.

Ačkoliv jsou služby obvykle využívány v rámci procesu archivace el. dokumentů, je samostatná služba validace el. dokumentů nutná především pro správné zpracování a vyhodnocení všech příchozích el. dokumentů.

Tato služba bude využívána primárně přes aplikační rozhraní z jednotlivých IS UK, ale je třeba zajistit i jednoduché uživatelské rozhraní pro případně adhoc validace el. dokumentů.

Požadavky

#	Požadavek
VAL01	Validace elektronických podpisů, pečetí a časových razítek vytvořená na základě certifikátů, vydaných v kterékoli členské zemi EU, dle platných seznamů důvěryhodných služeb TSL
VAL02	Je možné přidat vlastní důvěryhodné certifikační autority mimo evropské seznamy TSL
VAL03	Ověřování platnosti elektronických podpisů, pečetí a časových razítek je prováděno dle principů stanovených v technické normě ETSI EN 319 102-1
VAL04	Ověřování platnosti musí být schopné rozlišit úroveň elektronického podpisu a elektronické pečetě dle ustanovení zákona č. 297/2016 Sb.
VAL05	Výstupem validace je validační report v lidsky čitelné podobě (ve formátu PDF). Webová služba navíc vrací i strojově čitelné validační reporty ve formátu XML
VAL06	Validační software disponuje jak integračním rozhraním webových služeb, tak i grafickým uživatelským rozhraním pro ruční validace dokumentů a prohlížení validačních reportů
VAL07	Chování validačního softwaru lze konfigurovat a parametrizovat definicí validačních politik
VAL08	Validační software musí být schopen provádět validace zpětně k důvěryhodnému času buď přečteného z časového razítka, nebo specifikovaného v rámci validace (např. při volání webové služby), včetně ověření odvolání certifikátů k danému času. A to i po vypršení platnosti podpisových / pečetících certifikátů

Specifikace infrastrukturních služeb

Hardware Security Module (HSM)

Pro potřeby implementace služby kvalifikované el. pečeti v infrastruktuře UK vyžaduje takovéto řešení certifikované kvalifikované prostředky pro vytváření el. pečetí (QSCD). Z důvodů požadavků na výkon, dostupnost a implementaci systému více očí je vyžadován QSCD v podobě samostatných HW prostředků typů HSM (Hardware Security Module) v síťovém provedení použitelném v prostředí virtualizace.

Požadavky

#	Požadavek
HSM01	Certifikace zařízení pomocí ISO15408 (Common Criteria) dle profilu CEN 419 221-5
HSM02	Implementace kryptografických algoritmů RSA pro elektronický podpis s délkou klíčů minimálně 2048 a 4096 bitů
HSM03	Zajištění nezávislého přístupu ke kryptografickým prostředkům pro platformy MS Windows a Linux
HSM04	Musí být zajištěno, že vygenerované kryptografické klíče nikdy neopustí kvalifikovaný prostředek v otevřené podobě
HSM05	Zpřístupňování více klíčů nezávisle na sobě – možnost separace správy klíčů pro jednotlivé organizační celky
HSM06	Aktivace kryptografických klíčů pro jednotlivé části řešení v kvalifikovaných prostředcích v režimu „více očí“ (nutnost přítomnosti více než jednoho správce)
HSM07	Podpora generování žádostí o kvalifikované certifikáty pomocí kvalifikovaného prostředku
HSM08	Nástroje pro zálohování a přenos konfigurace a klíčů na nové zařízení musí být součástí dodávky
HSM09	Podpora montáže zařízení do standardního rozvaděče o velikosti 19“
HSM10	Podpora zapojení do 2 nezávislých síťových segmentů
HSM11	Vyměnitelný duální zdroj napájení
HSM12	Nabízené řešení musí poskytovat minimálně následující integrační rozhraní: • PKCS#11 • OpenSSL • Java (JCE) • Microsoft CAPI a CNG
HSM13	Kompatibilita HSM modulů se zvolenou platformou SAM modulu – viz samostatná infrastrukturní komponenta
HSM14	Licence pro připojení minimálně 5 připojených nezávislých serverů

HSM15	Součástí řešení musí být nástroje a licence umožňující vzdálenou správu a administraci HSM modulů bez nutnosti přístupu do datového centra
HSM16	Použité HSM moduly musí být možné využít i pro jiné účely než pouze pro pečeť a podpis

Signature Activation Module (SAM)

Pro případ služeb vzdáleného el. podpisu v kvalifikované úrovni, nebo pro využívání služby kvalifikované el. pečeti i dalšími subjekty mimo UK, musí plnit roli kvalifikovaného prostředku pro vytváření el. podpisů a pečetí tzv. SAM (Signature Activation Module), který pro svoji správnou činnost musí využívat odpovídající certifikovaný HSM modul – viz předchozí infrastrukturní komponenta.

Součástí dodávky SAM modulu musí být i veškerý nezbytný HW nutný pro jeho provoz.

Dalším typickým požadavkem v souvislosti se SAM moduly a vytvářením kvalifikovaných el. podpisů a pečetí je správa příslušného certifikovaného SAM ze strany kvalifikovaného poskytovatele. Jedná se o standardní podmínku provedené certifikace.

Požadavky

#	Požadavek
SAM01	Certifikace zařízení pomocí ISO15408 (Common Criteria) dle profilu CEN 419 241-2, ideálně včetně uvedení na seznamu QSCD dle nařízení eIDAS
SAM02	Dodávka SAM modulu včetně veškerého potřebného HW dle požadavků certifikace zvoleného SAM modulu
SAM03	Podpora aktivačních dat (SAD) pro vytváření podpisů a pečetí včetně podpory vícefaktorové autorizace – buď součástí dodávky SAM nebo integrace s řešením UK
SAM04	Zajištění podpory správy a provozu SAM modulu ze strany kvalifikovaného poskytovatele
SAM05	Podpora nabízeného SAM modulu ze strany alespoň jednoho kvalifikovaného poskytovatele vydávajícího kvalifikované certifikáty působícího v ČR

Obecné požadavky

Tato část obsahuje obecné požadavky související s celkovým řešením služeb vytvářejících důvěru a obecným legislativním prostředím. Bližší upřesnění jednotlivých požadavků je rozvedeno níže v rámci této kapitoly.

Základní požadavky

#	Požadavek
ZOP01	Řešení bude možné provozovat na vlastní infrastruktuře UK
ZOP02	Řešení musí umožnit současný provoz řešení pro různé subjekty s datovým a konfiguračním oddělením pro tyto subjekty (multitenantní provoz) v rámci dodané licence
ZOP03	Řešení bude splňovat obecné bezpečnostní standardy a také interní bezpečnostní předpisy UK
ZOP04	Řešení úspěšně projde výkonovými a penetračními testy ze strany UK
ZOP05	Soulad s nařízením Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
ZOP06	Soulad se zákonem č. 297/2016 Sb., Zákon o službách vytvářejících důvěru pro el. transakce
ZOP07	Soulad se zákonem č. 499/2004 Sb., Zákon o archivnictví a spisové službě a o změně některých zákonů
ZOP08	Řízení práv a přístupů na základě rolí
ZOP09	Řešení musí mít potvrzení o absolvovaných plug-testech dle ETSI EN 319 132 části 1 a 2, ETSI EN 319 122 části 1 a 2, ETSI EN 319 142 části 1 a 2, ETSI EN 319 162 části 1 a 2.
ZOP10	Dodavatel má minimálně 5-ti leté zkušenosti s vývojem produktů a implementací řešení pro důvěryhodnost dokumentů.
ZOP11	Dodavatel je kvalifikovaným poskytovatelem služeb vytvářejících důvěru
ZOP12	Dodávka rozhraní a dokumentace pro integraci jednotlivých služeb do prostředí studijního systému UK, využitelné pro integraci i dalších IS UK

IT prostředí

Produkční prostředí

- Služby běžící ve dvou aktivních instancích pro zajištění vysoké dostupnosti.
- HSM/SAM běžící ve dvou aktivních instancích pro zajištění vysoké dostupnosti.

Testovací prostředí

- Služby běžící v jedné instanci.
- HSM/SAM, pokud to umožňují, mohou být sdílené s produkčním prostředím. Jinak jedna dedikovaná instance pro testovací prostředí.

Infrastruktura UK

- Podporované běhové prostředí
    - virtualizace (VMWare vSphere pro virtuály na platformě Windows, Linux KVM pro virtuálny na platformě Linux),
    - kontejnery (na platformě Kubernetes, Docker nebo Podman)
    - aplikační servery (s OS MS Windows Server Standard 2022 nebo OS RockyLinux, OracleLinux ve verzích 8 nebo 9 nebo Debian 12),
    - databázové platformy (Oracle Database Standard Edition 2 verze 19c nebo MS SQL Server)
- Řešení bude poskytovat informace o stavu systému pro monitoring (celkový stav, informace o stavu jednotlivých komponent).
- Musí být dostupný popis a postup zálohování (přes zálohu databáze, snapshoty, souborová záloha apod.) a obnovy systému.
- V dokumentaci musí být popsány potřebné síťové prostupy mezi komponentami řešení.
- Integrace na Identity Provider (CAS).
- Integrace na IdM (MidPoint).

Multitenantnost

Jednotlivé služby i HSM musí podporovat současný provoz s více oddělenými konfiguracemi v rámci jednotlivých tenantů. Tyto tenanty mohou být určeny buď pro samostatné části UK nebo mohou být využívány dalšími subjekty, které mohou v budoucnu tyto služby využívat.

Škálovatelnost

Řešení musí být schopné škálovat v řádu desítek tisíc uživatelů bez nutnosti upgradu hardware a software. Přípustné je dokoupení potřebných uživatelských licencí.

Rozhraní

Řešení musí mimo jiné poskytovat následující technologická či aplikační rozhraní:

Rozhraní	Oblast
CSC API (JSON)	Vzdálený elektronický podpis

OASIS DSS (XML)	Kvalifikovaná elektronická pečeť
OASIS DSS (XML)	Validace elektronických dokumentů
SCIM (JSON)	Výměna identit s IDM
PKCS#11	Komunikace s HSM moduly
MS CAPI/CNG	Komunikace s HSM moduly
Grafické uživatelské prostředí	Primárně pro podpisový portál, validaci dokumentů a autorizaci služeb vzdáleného el. podpisu

Standardy

Řešení musí být v souladu s následujícími standardy.

Standard	Oblast
ETSI TS 119 432	Vzdálený elektronický podpis
ETSI EN 319 102	Vytváření a validace AdES podpisů
ETSI EN 319 122	Elektronické podpisy ve formátu CAdES
ETSI EN 319 132	Elektronické podpisy ve formátu XAdES
ETSI EN 319 142	Elektronické podpisy ve formátu PAdES
ETSI EN 319 162	Elektronické podpisy ve formátu ASiC
ETSI EN 319 182	Elektronické podpisy ve formátu JAdES
CEN 419 221-5	Certifikace HSM jako kvalifikovaného prostředku (QSCD)
CEN 419 241-2	Certifikace SAM modulu jako kvalifikovaného prostředku (QSCD)

Řešení musí mít potvrzení o provedených plug-testech dle ETSI EN 319 132 části 1 a 2, ETSI EN 319 122 části 1 a 2, ETSI EN 319 142 části 1 a 2, ETSI EN 319 162 části 1 a 2.

Použité řešení kryptografických prostředků musí splňovat požadavky na kvalifikované prostředky dle nařízení eIDAS v režimu správy ve jménu třetí osoby (nutné pro kvalifikovaný vzdálený podpis a pečetění pro více subjektů).

Rozsah služeb

Vlastní dodávka řešení by měla obsahovat minimálně služby v následujícím rozsahu:

- Vstupní analýza a cílový koncept řešení jako základ pro nasazení v prostředí UK
- Implementace produkčního prostředí (v HA) a testovacího prostředí všech komponent (SW, HW) v prostředí UK
- Podpora pro integraci aplikací:

    - Dokumentace, vzory integračních volání, konzultace
    - Integrace implementovaných služeb vytvářejících důvěru do SIS nebude z důvodu časové náročnosti předmětem této veřejné zakázky.
- Pilotní projekt
    - Správnost implementace bude ověřena na integraci do spisové služby TESS na všechny implementované služeb vytvářejících důvěru:
        - vzdálený kvalifikovaný el. podpis
        - kvalifikovaná pečeť
        - ověřování podpisů a pečetí
    - Startovací počet uživatelů pro služby vzdáleného el. podpisu - 1000
- Školení a dokumentace provedeného řešení

Produktová a servisní podpora

Tato část obsahuje požadavky na podporu dodaného řešení.

Produktová podpora by měla obsahovat

- podporu (maintenance) licencí SW poskytovanou výrobcem,
- podporu dodaného hardware poskytovanou výrobcem.

Předmětem servisní podpory by mělo být poskytování služeb pro zajištění provozu dodaného řešení včetně

- odstraňování havarijních stavů, provozních problémů a vad řešení;
- instalace aktualizací, konfigurace, customizace a rozvoje řešení dle požadavků zadavatele v celkovém rozsahu 20 MD / rok;
- správy kvalifikovaných prostředků (QSCD) ze strany QTSP.

Požadavky na reakční dobu a dobu vyřešení

Úroveň hlášení	Popis	Reakční doba	Doba vyřešení
Vysoká	Standardní procesy jsou vážně ovlivněny a nezbytné úlohy nemohou být plněny. Některé nebo všechny systémy podporující hlavní firemní procesy selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je kritickým způsobem ovlivněna informační podpora činnosti objednatele.	1 hodina	Následující pracovní den
Střední	Jsou dotčeny firemní procesy v míře způsobující ztěžování výkonu konkrétní činnosti. Podporované činnosti jsou výrazně ovlivněny z důvodu selhání nebo omezení některé ze systémových funkcí podporující důležité procesy. V případě současného výskytu více vad kategorie B může nastat situace, kdy vzájemné působení těchto vad způsobí kumulaci	4 hodiny	Následující pracovní den +1

	negativního dopadu na firemní procesy, pak budou i jednotlivé vady způsobující tuto kumulaci hodnoceny kategorií A.		
Nízká	Stav služby, kdy nejsou ohroženy hlavní funkce systému/aplikace. Po dobu výpadku lze nahradit nefunkční část náhradním řešením.	Následující pracovní den	Následující pracovní den +5

Reakční doby se počítají v pracovních dnech v čase od 9 do 17 hodin od času oznámení incidentu. Doba vyřešení se počítá od doby reakce Dodavatele na nahlášený incident zadavatelem.