Příloha č. 1 – Technická specifikace a popis předmětu plnění

Předmět zakázky

Předmětem plnění je rozšíření stávající aplikace o novou funkcionalitu zajišťující bezpečné a spolehlivé ukládání logů v souladu s legislativními požadavky a standardy v oblasti kybernetické bezpečnosti. Toto pilotní řešení realizované v návaznosti na aplikaci výdeje studentských a zaměstnaneckých průkazů musí být v souladu s nařízeními týkající se kybernetické bezpečnosti a realizovat garantované úložiště logů vytvořených v rámci portálu. Jednotlivé záznamy budou ukládány ve formátu Xades. Systém musí být koncipován s ohledem na možnosti rozšíření bezpečného ukládání záznamů z dalších aplikací informačního systému UK.

Funkční a věcné požadavky na Důvěryhodné úložiště logů (dále jen „DÚL“):

1. Inventarizace a kategorizace dotazů
2. Bude podporovat formáty AdES (PAdES, CAdES, XAdES) a ASIC kontejnery.
3. Musí vůči okolním systémům vystupovat tak, že každému uloženému objektu přiřadí jedinečné a neměnné ID. S jeho pomocí lze objekt identifikovat jednoznačně v rámci IS organizace.
4. Musí podporovat ukládání a zpřístupňování objektů ve formě textových, grafických, audiovizuálních, digitálních nebo jiných obdobných záznamů.
5. Systém obsahuje uživatelské rozhraní pro přístup k uloženým objektům provozované ve webovém prohlížeči bez nutnosti instalovat přídavné moduly či rozšíření. Toto uživatelské prostředí umožňuje vyhledávání dle různých vyhledávacích kritérií.
6. Dlouhodobé zajištění integrity archivovaných dokumentů i na úrovni datového úložiště po dobu technické životnosti úložiště. Možnost budoucí migrace na nové datové úložiště plnící podmínky kladené na takové úložiště bez ztráty integrity archivovaných objektů a zajištění integrity archivovaných objektů na další období.
7. Systém musí umožňovat řízenou skartaci.
8. Systém musí umožňovat nastavení a řízení přístupových práv dle rolí uživatele a jeho organizačního zařazení.
9. Nesmí být licenčně omezen na počet archivovaných objektů; počet uživatelů nebo zobrazovacích stanic.
10. Systém umí dynamicky reagovat na dodatečné informace, které mohou dodatečně ovlivnit a změnit skartační plán a zohlednit tyto změny do skartační lhůty pro konkrétní archivované objekty.
11. Musí umožňovat do budoucna zvýšení výkonu formou škálování aplikačních serverů stávajícího úložiště, nikoliv dodávkou dalšího HW.
12. Auditování a logování provozu jednotlivých prvků systému a možnost vyhodnocování minimálně 1 rok zpětně a logy musí být důvěryhodně pečetěny a uloženy.
13. Aplikační servery musí podporovat běh ve vysoké dostupnosti v režimu Active-Active a Active-Pasive ve dvou lokalitách a loadbalacing na úrovni aplikačních serverů.
14. Systém musí podporovat multitenantní konfiguraci, tj. pro různé typy objektů musí jít v rámci jedné instance vytvořit zcela samostatně konfigurovatelné úložiště jak z pohledu metadat, uživatelských oprávnění a dalších parametrů.
15. Má používat úložiště MS SQL nebo PostgreSQL.

16. Nad rámec běžného pečetění při zpracování objektů, musí v rámci svého integračního rozhraní poskytovat funkcionalitu pečetění pro objekty ve formátech AdES a ASIC kontejnery.
17. Nesmí být omezen množstvím uložených dat ani počtem uživatelů přistupujících přímo nebo prostřednictvím dalších systémů k DÚL.

Služby vytvářející důvěru (konektory)

1. Musí obsahovat konektor alespoň na jednoho kvalifikovaného poskytovatele služeb vytvářejících důvěru zajišťující kvalifikované pečetění a uvedeného na stránkách Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru – Ministerstvo vnitra České republiky (mvcr.cz)
2. Musí obsahovat konektor alespoň na jednoho kvalifikovaného poskytovatele služeb vytvářejících důvěru zajišťující službu Kvalifikovaného ověřování platnosti kvalifikovaných elektronických podpisů a pečetí a uvedeného na stránkách Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru – Ministerstvo vnitra České republiky (mvcr.cz)
3. Musí nativně podporovat alespoň jeden kryptografický prostředek pro ukládání elektronických podpisů a pečetí (HSM) uvedený na seznamu SSCD a QSCD zveřejňovaném Evropskou komisí (Compilation of Member States notification on SSCDs and QSCDs).
4. Nad rámec standardních validačních mechanismů musí na integračním rozhraní DEA poskytovat funkci pro všechny formáty AdES a ASIC kontejnery a „zvaliduj a vrať“, kde výstupem je validační report v podobě PDF nebo XML.
5. Jako pilotní projekt bude na svém rozhraní poskytovat metody pro vzdálené podepisování a pečetění (pro účely tohoto funkčního požadavku se za vzdálené podepisování nebo pečetění považuje situace, kdy uživatel nemá svůj token nebo vlastní úložiště a využívá pro podepisování nebo pečetění síťový kryptografický prostředek nebo služeb některého z kvalifikovaných poskytovatelů zajišťující službu vzdáleného pečetění nebo podepisování) – tento bod je výhodou, nikoliv podmínkou.

Specifikace aplikace pro výdeje studentských a zaměstnaneckých průkazů

Aplikace Výdej studentských a zaměstnaneckých průkazů používá pro frontend webové prostředí. Na pozadí systému Windows je spuštěná nativní komponenta (Java), která zajišťuje komunikaci se všemi připojenými zařízeními (tiskárna, čtečky karet, platební terminál, fotoaparát, podpisová destička). Na serveru aplikace výdeje průkazů běží služba, která aktivně komunikuje s WS informačního systému UK.

Aplikace je rozdělena do několika funkcionalit. Ty lze provozovat i jednotlivě nastavením oprávnění (Výdej průkazů, generování počáteční hesel LDAP, registrace čipových přívěšků pro vstupní systémy, platba za prodloužení licencí ISIC, zápis certifikátu SALTO pro šatní skříňky).

Ověření osoby v aplikaci je napojeno na LDAP UK pro nastavování příslušného oprávnění na jednotlivé funkcionality aplikace.

Tato aplikace slouží i pro výdej průkazů jiných VŠ (AMU a VŠUP), kdy používá webové služby přímo příslušných VŠ.