Otázka č. 1:

Otázka k vkladaniu časových pečiatok do výstupných správ kvalifikovaných služieb validácie.

Požaduje obstarávateľ, aby boli pri do výstupných správ z kvalifikovaných služby validácie KEP/KEPe vkladané časové pečiatky? Ak áno, je ich počet už započítaný v požiadavke na počty časových pečiatok (REQ_SNCA_6), alebo potrebné ich celkový počet navýšiť o spotrebu v rámci validačných služieb?

Vysvetlenie:

Podľa dokumentu Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu v1.4, s. 33: ,,Spoliehajúcej sa strane je poskytnutá podpísaná alebo zapečatená správa validácie".

Podľa [ETSI 119 441] SVR-8.4-18: "When validation reports are signed the signature may be in a basic form; it does not need to be time-stamped or further augmented. See also annex F."

Pri počte ,,minimálne 60.000.000 požiadaviek na validáciu/rok" (REQ_SNCA_50) ide o nezanebateľnú položku.

Odpoveď č. 1:

Verejný obstarávateľ upresňuje, že v predpokladanom počte ročne vydaných kvalifikovaných elektronických časových pečiatok, ktorý je uvedený v súťažných podkladoch verejného obstarávateľa, konkrétne v Prílohe č. 18 - Katalóg požiadaviek – KDS, požiadavka REQ_SNCA_6, nie sú zahrnuté počty časových pečiatok, ktoré využijú ostatné služby. Z uvedeného dôvodu je potrebné, aby uchádzač pri návrhu riešenia zohľadnil navýšenie predpokladaného počtu ročne vydaných kvalifikovaných elektronických časových pečiatok o počet časových pečiatok, využitých v rámci ostatných služieb. Verejný obstarávateľ predpokladá, že celkový počet ročne vydaných kvalifikovaných elektronických časových pečiatok pre všetky poskytované služby nepresiahne hodnotu 600 miliónov vydaných časových pečiatok.

Otázka č. 2:

Otázka k formátu výstupných správ kvalifikovaných služieb validácie.

Požaduje obstarávateľ aby výstupom jedného volania kvalifikovanej služby validácie bola vždy výstupná správa v jednom formáte?

Vysvetlenie:

Podľa dokumentu Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu v1.4, s. 25: ,,Výsledkom kvalifikovanej dôveryhodnej služby validácie kvalifikovaných elektronických podpisov a pečatí je správa z validácie v textovom dokumente v UTF8 kódovaní, ..".

Zároveň je v ETSI TS 119 102-2 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report štandardizovaný iný, strojovo spracovateľný formát.

Vyhotovovanie výstupnej správy v dvoch formátoch má dopad na počet vyhotovených pečatí (pečatenie výstupnej správy) a v prípade vkladania časových pečiatok, aj na ich spotrebu.

Odpoveď č. 2:

Verejný obstarávateľ požaduje, aby uchádzač navrhol také riešenie, ktoré umožní vrátenie validačného reportu aj v dvoch rôznych formátoch (PDF ako vizuálna podoba a XML ako strojovo spracovateľná podoba), pričom presný rozsah bude určený vo fáze detailného návrhu riešenia.

Otázka č. 3:

Otázka k formátu výstupných správ a vkladaniu časových pečiatok do nekvalifikovaných služieb validácie.

Požaduje obstarávateľ, aby boli výstupné správy z nekvalifikovaných služieb validácie pečatené rovnako ako v prípade kvalifikovaných služieb a aby boli do nich vkladané časové pečiatky?

Odpoveď č. 3:

Verejný obstarávateľ konštatuje, že výstupy z nekvalifikovaných služieb validácie nemusia byť povinne pečatené, teda verejný obstarávateľ požaduje možnosť konfiguračne alebo cez parameter určiť potrebu zapečatenia. Verejný obstarávateľ predpokladá, že v produktívnej prevádzke dodaného riešenia / informačného systému predvolene nastaví pečatenie aj nekvalifikovaných validačných reportov.

Otázka č. 4:

Otázka k požiadavkám na testovacie prostredie.

Vyžaduje obstarávateľ, aby testovacie prostredie bolo identické s produkčným (1:1), vrátane troch lokalít a počtu hardvérových a softvérových komponentov? Alebo je prípustné testovacie prostredie optimalizovať z hľadiska finančnej efektívnosti (napríklad zdieľaním prvkov medzi jednotlivými testovacími uzlami) za predpokladu, že budú splnené minimálne požadované výkonnostné požiadavky?

Odpoveď č. 4:

Verejný obstarávateľ uvádza, že testovacie prostredie musí umožniť overenie všetkých funkčných aj nefunkčných požiadaviek prostredníctvom otestovania všetkých potrebných scenárov, vrátane testov nefunkčných požiadaviek (dostupnosť, update a upgrade dodaného softvéru a firmvéru dodaných hardvérových zariadení, DR), kapacitne však nie je potrebné dosahovať úroveň produkčného prostredia. Môže existovať viacero inštancií testovacieho prostredia vznikajúcich a zanikajúcich podľa potreby – v automatizovanom DevSecOps kontajnerizovanom prostredí v závislosti od dostatočnej infraštruktúrnej rezervy. Testovacie scenáre môžu byť závislé na konkrétnom riešení, zodpovednosťou uchádzača je navrhnúť konfiguráciu testovacieho prostredia tak, aby všetky potrebné testy v celom životnom cykle riešenia bolo možné spoľahlivo vykonávať. Verejný obstarávateľ predpokladá, že minimálne na otestovanie redundancie a bezpečného pravidelného aktualizovania dodaného softvéru a firmvéru dodaných hardvérových zariadení je potrebné, aby konfigurácia testovacieho prostredia bola, z pohľadu geografie, zhodná s produkčným prostredím (testovacie prostredie na viacerých lokalitách).

Otázka č. 5:

Otázka k rozsahu GRC platformy.

Chceli by sme si objasniť požiadavku na dodanie GRC platformy (REQ_SNCA_200). Hľadáte riešenie, ktoré pokrýva všeobecné riadenie rizík, politík, compliance a auditu v rámci organizácie a jej procesov (vrátane ne-IT aspektov), alebo riešenie špecificky zamerané na technickú správu a bezpečnosť Kubernetes prostredí?

Odpoveď č. 5:

Verejný obstarávateľ konštatuje, že GRC platforma bude slúžiť pre potreby dodaného riešenia a z tohto dôvodu musí pokrývať všeobecné riadenie rizík, politík, compliance a auditu v rámci dodaného riešenia a jeho procesov (vrátane ne-IT aspektov). Zároveň musí byť GRC platforma schopná efektívne spravovať a zabezpečovať Kubernetes prostredia dodaného riešenia. Verejný obstarávateľ požaduje, aby GRC platforma poskytovala:

1. Riadenie rizík, politík, compliance a auditu pre dodané riešenie: Zabezpečenie súladu s regulačnými požiadavkami, riadenie interných politík a procesov vyplývajúcich pre dodané riešenie a vykonávanie auditov.

2. Technickú správu a bezpečnosť Kubernetes prostredí riešenia: Automatizované monitorovanie, riadenie prístupu, zabezpečenie konfigurácií a ochranu pred bezpečnostnými hrozbami v Kubernetes prostredí.