



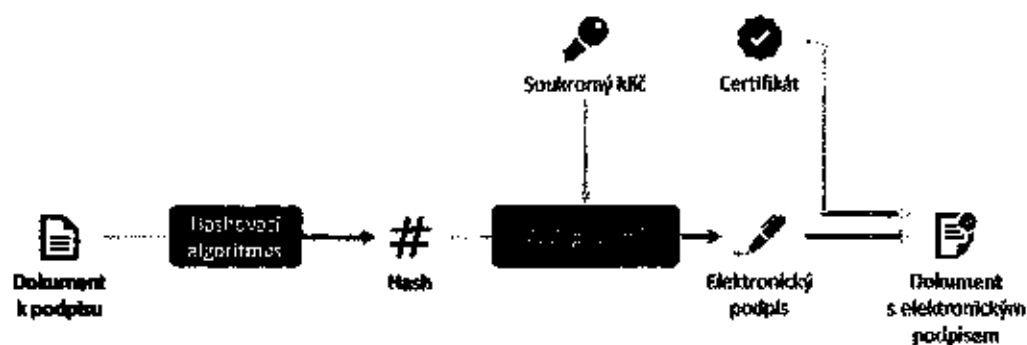
MHMP09KQPM3

POKYN č.2 – ke smlouvě DIL/31/04/000102/2021

Zhotovitel	Asseco Central Europe, a.s. IČO: 27074358,
Objednatel	Hlavní město Praha Mariánské náměstí 2/2, PSČ 11001 Praha 7 IČO: 00064581
Zakázka (č. smlouvy Objednatele, název)	Číslo smlouvy Objednatele DIL/31/04/000102/2021 <i>Centrální Systém Pečetění elektronických dokumentů v souladu s nařízením eIDAS a jeho integrace do IS MHMP, MČ a městských organiz</i>
Odpovědný pracovník Objednatele	Ing. Milan Krch
Odpovědný pracovník Zhotovitele	Ing. David Šindelář
Číslo pokynu	Pokyn č.2

Specifikace plnění

- **Popis stávajícího stavu ze smlouvy**
 - V rámci projektu CESYP bylo dodáno rozhraní pro asynchronní režim pečetění dokumentů.
 - V rámci požadavku na pečetění dokumentu kvalifikovanou pečeti se pomocí definovaného API rozhraní odesílá celý dokument a opečetěn se vrací zpátky.
- **Cíl řešení – čeho chceme tímto požadavkem dosáhnout**
 - Zavést novou možnost pečetění dokumentu pomocí metody Hash, jelikož služba poskytující elektronické podpisy dle EU direktivy eIDAS musí zajišťovat neměnnost dokumentu po okamžiku podpisu (viz eIDAS, oddíl IV, článek 26 d), někdy se též mluví o "časovém ukotvení dokumentu".
 - Mít k dispozici možnost, jak volat požadavek na pečetění hash jak asynchronním tak i synchronním způsobem, tedy napřímo. Tedy mít na výběr obě varianty, které bude možné rozlišit díky parametru metody webové služby.
 - Při pečetění hash není nutno přenášet celý dokument, ale konzumující systém služby provede podle definovaného matematického výpočtu pečetění pouze hashe daného dokumentu. Při jeho tvoření se nejprve vypočte otisk dokumentu, který se nazývá hash (jde malé číslo o velikosti několik stovek bitů).



- Mezi vlastnosti hashe patří to, že pokud vstupní dokument třeba jen nepatrně upravíte, výsledný hash se výrazně změní. Navíc je matematicky zcela nepravděpodobné, že by dvě zprávy měly stejný hash, takže podle něj snadno identifikujete právě jeden dokument. Jakmile se hash vytvoří, systém ho zašifruje autorovým privátním klíčem, čímž vzniká elektronický podpis.
 - Rozhraní bude obsahovat i funkci vyžádání si časového razítka, které zajistí společně s el. podpisem důvěryhodnost el. pečeti.
 - Vstupním bodem pro poskytovanou službu pečetění hash bude Integrovaná platforma.
 - Podle parametru ve volání služby bude Integrovaná platforma směřovat požadavek na příslušnou skupinu aplikačních serverů. Skupiny serverů budou rozděleny (samostatné virtuální servery) tak, aby funkce pro asynchronní a synchronní služby nebyly poskytovány na stejném serveru, tedy aby se jednalo o realizaci v robustním řešení.
 - Logování systémových a uživatelských požadavků pro hash službu
 - Bude proveden výkonostní test pro synchronní i asynchronní metodu, na jehož základě budou nastaveny limity na Integrovanou platformě i CESYPU, jež zabrání zahájení systému CESYP.
 - Rozšíření této funkčnosti je požadováno projektem spisové služby eSpis. Jako další vhodné využití je důvěryhodné uchovávání bezpečnostních logů IT systémů, které využívají pouze hash a to zejména z důvodu velikosti souboru.
- **Důvody a popis toho co se bude měnit (práce)**
 - Na základě požadavku projektu eSpis, který bude využívat služby pečetění systému CESYP je nutno zavést novou službu pro pečetění dokumentů pomocí Hash.
 - Služba bude realizována rozšířením metody webových služeb současného řešení založeného na akceptovaném Detailním návrhu a schválených akceptačních testech. Současné řešení bude rozšířeno o požadovanou funkčnost pro synchronní a asynchronní způsob komunikace, kdy bude možné parametricky zvolit typ volání pro vyřizování požadavků. SW produkt eSpis nedokáže využívat pečetění dokumentů a podporuje pouze práci s Hash.
 - Další využití funkčnosti Hash je pro zajištění důvěryhodné práce s bezpečnostními logy, kdy IT systémy podporují využití funkce hash.
 - **Způsob předvedení – např. dle akceptačního scénáře + příložený návrh**
 - Předvedení funkčnosti řešení prostřednictvím prezentace/ukázky na základě akceptačního scénáře
 - Doplnění technické dokumentace k popisu webových služeb a provozní dokumentaci.

Požadovaný termín zahájení a případně ukončení poskytování Plnění:

Datum zahájení je považován datum podpisu Pokynu (= T), datum ukončení je T+ 90dní.

Celková předpokládaná cena za Plnění

Objednatelem předpokládaný rozsah Plnění a cena:

Cena v Kč bez DPH za jednotku (člověkden)	Počet MD (8h)
8.000,-	26
Celkem bez DPH:	208 000
Celkem s DPH:	251 680



Ing. David Šindelář

ASSECO
CENTRAL EUROPE
Budějovická 778/3a, 140 00 Praha 4

22 -09- 2021



Ing. Milan Krch

Hlavní město Praha
Magistrát hl.m. Prahy
Jungmannova 35/29
111 21 Praha 1 /43/