

Anonymní		Odpověď						Závěr
Otázka ▼ / Účastník ▶		Účastník 1	Účastník 2	Účastník 3	Účastník 4	Účastník 5	Účastník 6	
D.1	Rozdělení projektu na uvedené fáze dle kapitoly 1.1 je vhodné a odpovídá našim zkušenostem z podobných projektů	Ano	Ano	Ano	Ano	Částečně	--	
D.2	Zajištění zdrojů pro provoz dodávaných systémů (kapitola 1.3) dle specifikací Platforma 2.0 (příloha č. 5) je dostačující	Částečně	Ano	Ano	Ano	Ano	--	
D.3	Jste schopni splnit celý předpokládaný rozsah plnění? (zejména dodávka a podpora SW správy certifikátů a karet, SW koncových stanic, dodávka čipových karet a jejich personalizace a další).	Ano	Ano	Ano	Ano	Ano	--	
D.4	Jste ochotni poskytnout SŽ zdrojové kódy části SW vyvíjeného nebo upravovaného na základě specifických potřeb SŽ za účelem zajištění budoucí kompatibility a otevřenosti řešení a za účelem bezpečnostní analýzy kódu?	Ano	Ne	Ano	Ano	Ano	--	Zohledněno v zadávací dokumentaci
D.5	Prosíme o úvodní návrh segregace rolí v procesech vydávání a správy životního cyklu uživatelských certifikátů.						--	Zohledněno v zadávací dokumentaci
D.6a	Podle Vašich zkušeností s obdobnými projekty: jakou technologii personalizace smart karet doporučujete a proč?						--	Zohledněno v zadávací dokumentaci v souladu s požadavky Zadavatele na kompatibilitu se současným řešením personalizace nosičů
D.6b	Jaká je typická životnost personalizace karty (potisk, polep) při běžném používání uživateli (několikanásobné použití karty ve čtečce denně)?						--	Zohledněno v zadávací dokumentaci
D.7a	V případě dodávek již personalizovaných (potištěných) karet: jaká je běžná doba dodání personalizované karty od jejího objednání?	--					--	Zohledněno v zadávací dokumentaci
D.7b	Jaké minimální množství personalizovaných karet je možné objednat?						--	Zohledněno v zadávací dokumentaci
D.8	Jaká je typická životnost kontaktní části karty při běžném používání uživateli (několikanásobné použití karty ve čtečce denně)?						--	
D.9a	Je Vámi uvedená smart karta kompatibilní a akceptovaná uvedenou akreditovanou CA (I.CA) jako QSCD dle eIDAS pro generování příslušných certifikátů?	Ano	Ano	Ano	Ne	Ne	--	Nerelevantní pro zadávací dokumenaci
D.9b	Pokud je Vaše odpověď na 9a NE, prosím, uveďte, jak navrhujete danou situaci řešit.	--	--	--			--	Nerelevantní pro zadávací dokumenaci
D.10	Splňuje Vaše řešení požadavky na middleware a služební software koncových stanic (kap. 2.2)?	Ano	Ano	Ano	Ano	Ano	--	
D.11	Jak odhadujete délku trvání fází 1 – 6 (např. v týdnech nebo měsících)?						--	Zohledněno v harmonogramu
D.12	Jaký je Váš odhad ceny plnění v uvedené struktuře? (označeno jen zda účastník poskytl cenové odhady)						--	Zohledněno v předběžné hodnotě
D.13	Je uvedený rozsah informací poskytnutých v rámci PTK (doplňný o informace, které jsou předmětem dotazování v PTK) dostačující pro zpracování nabídky? V případě, že by byl rozsah informací nedostatečný, specifikujte prosím, které informace jsou pro zpracování Vaší nabídky nezbytné.	Částečně	Ano	Částečně	Částečně	Částečně	--	Zohledněno v zadávací dokumentaci (poskytnuty požadované informace)
E.1	Jste schopni doložit alespoň 2 referenční zakázky za posledních 5 let? (zakázka: 3000+ zaměstnanců; eIDAS kompatibilní; systém správy ŽC; celkové řešení 10+ mil.Kč, popř. systém správy ŽC 2+ mil. Kč	Ano	Ne	Částečně	Částečně	Ano	--	Zohledněno v zadávací dokumenaci
E.2	Schopnost doložit realizační tým (garant celkového řešení, seniorní produktový specialista, seniorní specialista pro čipové karty, specialista MS AD/AAD; infrastrukturní specialista)	Ano	Ano	Ano	Ano	Ano	--	
E.3	Realizační tým: naplněním požadavků na odborné/produktové znalosti u každého člena týmu dosaženými certifikacemi?	Ano	Ano	Ne	Ano	Částečně	--	Zohledněno v zadávací dokumentaci

Legenda:	Ano	Účastník odpověděl kladně (jeho řešení vyhovuje uvedeným podmínkám)
	Částečně	Řešení účastníka částečně v yhovuje podmínkám (s případným upřesněním)
	Ne	Účastník odpověděl záporně (jeho řešení nevyhovuje podmínkám, s případným upřesněním)
		Účastník poskytl odpověď
	--	Účastník poskytl neúplnou dpověď
		Účastník neodpověděl

			Technické požadavky na nosič certifikátů							
ID	Požadavek	Požadováno?	Účastník 1 Splňuje	Účastník 2 Splňuje	Účastník 3 Splňuje	Účastník 4 Splňuje	Účastník 5 Splňuje			
Základní požadavky na smart karty	Základní požadavky na smart kartu									
	A.1	Karta musí být certifikována jako QSCD (kvalifikovaný prostředek pro vytváření elektronických podpisů) podle 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)	Požadováno	Ano	Ano	Ano	Ne	Ano		
	A.2	Certifikace karty jako QSCD musí být platná nejméně další 3 roky od dodávky	Požadováno	Ano	Ano	Ano	Ne	Ano	Nerelevantní pro zadávací dokumentaci	
	A.3	Čipová karta musí být podporována minimálně u dvou vydavatelů kvalifikovaných certifikátů (akreditovaných CA) na území České republiky, karta musí být podporována u současného dodavatele kvalifikovaných certifikátů SŽ	Požadováno	Ano	Ano	Ano	Ne	Ano	Nerelevantní pro zadávací dokumentaci	
	A.4	Privátní PKI klíč bude uložený na kartě nelze z karty vyexportovat	Požadováno	Ano	Ano	Ano	Ano	Ano	Nerelevantní pro zadávací dokumentaci	
	A.5	Ke klíčovým párom lze na kartu uložit i příslušné certifikáty X.509	Požadováno	Ano	Ano	Ano	Ano	Ano		
	A.6	PKI aplikace v čipu karty musí splňovat Common Criteria úrovně minimálně EAL5+ (alt. EAL 6+)	Požadováno	Ano	Ano	Ne	Ano	Ano	Zohledněno v zadávací dokumentaci	
Požadavky na PKI čip smart karty a související PKI aplikaci	Požadavky na PKI čip smart karty a související PKI aplikaci									
	B.1	Podpora vytváření elektronických podpisů (včetně podpisů dle eIDAS)	Požadováno	Ano	Ano	Ano	Částečně	Ano	Nerelevantní pro zadávací dokumentaci	
	B.2	Podpora vícefaktorové autentizace na bázi certifikátů X.509 do PC (prostředí Microsoft Active Directory / Smartcard Logon), webových služeb, VPN, aplikací, apod.	Požadováno	Ano	Ano	Ano	Ano	Ano		
	B.3	Možnost uložení certifikátů X.509 různých certifikačních autorit. (tedy nejen certifikáty z interních CA SŽ, ale také certifikáty veřejných CA – např. kvalifikovaných poskytovatelů služeb vytvářejících důvěru)	Požadováno	Ano	Ano	Ano	Ano	Ano		
	B.4	Pro generování kryptografických klíčů pro kvalifikovaný elektronický podpis karta podporuje mechanismus vzniku kryptografického důkazu o původu kryptografického klíče v dedikovaných kontejnerech na kartě za tímto účelem uložených. Vygenerovaný kryptogram je následně schopen akreditovaný kvalifikovaný poskytovatel při žádosti o certifikát kryptograficky ověřit a vydat podpisový certifikát držitelé karty	Požadováno	Ano	Ano	Ano	Ano	Ano		
	B.5	Uložení minimálně 16 klíčovými párů s certifikáty (8 kontejnerů pro RSA, 8 kontejnerů pro ECC), včetně definice jiného rozdělení před výrobou karty	Požadováno	Ano	Ano	Částečně	Ano	Ano	Vysvětleno	
	B.6	Šifrovací algoritmy RSA: 2048, 3072 a 4096 bitů; RSA OAEP, RSA PSS; včetně generování párů klíčů v čipu	Požadováno	Ano	Ano	Ano	Částečně	Ano	V zadávací dokumentaci byly zohledněny aktuální požadavky NÚKIB	
	B.7	Šifrovací algoritmy ECC: P-256, P-384, P-521 bitů, včetně generování párů klíčů v čipu	Požadováno	Ano	Ano	Částečně	Ano	Ano	V zadávací dokumentaci byly zohledněny aktuální požadavky NÚKIB	
	B.8	Podpora RSA OAEP a RSA PSS	Požadováno	Ano	Ano	Ano	Ne	Ano	V zadávací dokumentaci byly zohledněny aktuální požadavky NÚKIB	
	B.9	Hashovací algoritmy: SHA-1, SHA-256, SHA-384, SHA-512	Požadováno	Ano	Ano	Ano	Ano	Ano	V zadávací dokumentaci byly zohledněny aktuální požadavky NÚKIB	
	B.10	Podpora algoritmů ECDSA a ECDH	Požadováno	Ano	Ano	Ne	Ne	Ano	V zadávací dokumentaci byly zohledněny aktuální požadavky NÚKIB	
	B.11	Podpora symetrické kryptografie AES (128, 192, 256 bits) a 3DES (ECB, CBC)	Požadováno	Ano	Ano	Ano	Ano	Částečně	Ano	V zadávací dokumentaci byly zohledněny aktuální požadavky NÚKIB
	B.12	Import klíčů s certifikáty do čipu, např. ze standardizovaného souboru PKCS#12	Požadováno	Ano	Ano	Ano	Ano	Ano		
	B.13	Podpora PIN; podpora PUK pro odblokování PIN, včetně zablokování PIN resp. PUK po opakovaném chybném zadání PIN, resp. PUK	Požadováno	Ano	Ano	Ano	Částečně	Ano	Ano	
	B.14	Podpora změny PIN pomocí standardního logon desktopu MS Windows	Požadováno	Ano	Ano	Ano	Ne	Ano	Ano	Upraveno podle potřeb Zadavatele
	B.15	Uchování dat v paměti min. 10 let	Požadováno	Ano	Ano	Ano	Ano	Ano	Ano	
	B.16	Přepis paměti: minimálně 500 000 cyklů	Požadováno	Ano	Ano	Ano	Ano	Ano	Ano	
Požadavky na bezkontaktní část	Požadavky na bezkontaktní část karty									
	C.1	Bezdrátová komunikace na 13.56MHz	Požadováno	Ano	Ano	Ano	Ano	Ano		
	Podpora komunikačních protokolů									
	C.2	MIFARE Ultralight® C	Požadováno	Ano	Ano	Ano		Ano	Nerelevantní pro zadávací dokumentaci	
	C.3	MIFARE Ultralight® EV1	Požadováno	Ano	Ano	Ano		Ano	Nerelevantní pro zadávací dokumentaci	
	C.4	MIFARE Classic® 1K EV1	Požadováno	Ano	Ano	Ano		Ano	Nerelevantní pro zadávací dokumentaci	
	C.5	MIFARE Classic® 4K EV1	Požadováno	Ano	Ano	Ano		Ano	Nerelevantní pro zadávací dokumentaci	
	C.6	MIFARE® DESFire® 256B EV1	Volitelné	Ano	Ano	Ano		Ano	Nerelevantní pro zadávací dokumentaci	
	C.7	MIFARE® DESFire® 2K EV1/EV2	Požadováno	Ano	Ano	Ano		Ano	Nerelevantní pro zadávací dokumentaci	
	C.8	MIFARE® DESFire® 4K EV1/EV2/EV3	Požadováno	Ano	Ano	Ano		Ano		
	C.9	MIFARE® DESFire® 8K EV1/EV2/EV3	Požadováno	Ano	Ano	Ano	Ano	Ano		
	C.10	MIFARE Plus® SE	Volitelné	Částečně	Ano	Ano		Ano	Nerelevantní pro zadávací dokumentaci	
	C.11	MIFARE Plus® S 2K	Požadováno	Částečně	Ano	Ano		Ano	Nerelevantní pro zadávací dokumentaci	
	C.12	MIFARE Plus® S 4K	Požadováno	Částečně	Ano	Ano		Ano	Nerelevantní pro zadávací dokumentaci	
	C.13	MIFARE Plus® X 2K	Požadováno	Částečně	Ano	Ano		Ano	Nerelevantní pro zadávací dokumentaci	
	C.14	MIFARE Plus® X 4K	Požadováno	Částečně	Ano	Ano		Ano	Nerelevantní pro zadávací dokumentaci	
	C.15	MIFARE Plus® EV1 2K	Požadováno	Částečně	Ano	Ano		Ano	Nerelevantní pro zadávací dokumentaci	
	C.16	MIFARE Plus® EV1 4K	Požadováno	Částečně	Ano	Ano		Ano	Nerelevantní pro zadávací dokumentaci	
	C.17	i-Code® SLIX	Volitelné	Částečně	Ano	Ne		Částečně	Nerelevantní pro zadávací dokumentaci	
	C.18	NTAG213	Volitelné	Částečně	Ano	Ano		Částečně	Nerelevantní pro zadávací dokumentaci	
	C.19	NTAG215	Volitelné	Částečně	Ano	Ano		Částečně	Nerelevantní pro zadávací dokumentaci	
	C.20	NTAG216	Volitelné	Částečně	Ano	Ano		Částečně	Nerelevantní pro zadávací dokumentaci	
	C.21	SmartMX (JCOP)	Volitelné	Částečně	Ano	Ne		Částečně	Nerelevantní pro zadávací dokumentaci	

⁷⁾ Minimální požadavky na kryptografické algoritmy ze dne 5.2.2025

Legenda:	Ano	Účastník odpovídek kladně (jeho řešení vyhovuje uvedeným podmínkám)
	Částečně	Řešení účastníka částečně vyhovuje podmínkám (s případným upřesněním)
	Ne	Účastník odpovídek záporně (jeho řešení nevyhovuje podmínkám, s případným upřesněním) Účastník neodpovídek

		Odhad délky implementace					
Délka implementace ▼	/ Účastník ►	Účastník 1	Účastník 2	Účastník 3	Účastník 4	Účastník 5	Účastník 6
Celkový čas		8 - 12 měsíců	3 měsíce	4 měsíce	12 - 18 měsíců	7 měs. (min)	--

			Cenový odhad				
Ceny ▼	/	Účastník ►	Účastník 1	Účastník 2	Účastník 3	Účastník 4	Účastník 5
Celkem bez nosičů certifikátů			16 520 000	28 520 000	20 600 000	98 074 000	13 320 600
Celkem nosiče			11 220 000	17 600 000	19 800 000	25 300 000	12 628 000
Odhad ceny celkem			27 740 000	46 120 000	40 400 000	123 374 000	25 948 600
Účastník 1: bez ceny implementace							

