Pomáhat a chránit

Vybudování Národní kontrolní autority (NKA)

Technicko-organizační zadání

Verze 1.03

Praha 2016

Obsah

Vybudování Národní kontrolní autority (NKA) **1**

Technicko-organizační zadání **1**

1 Úvod **4**

1.1 Rozsah implementace projektu *5*

1.2 Blokové schéma *5*

2 Požadavky na realizaci dodávky NKA **7**

2.1 Požadavky na hardware *7*

2.2 Požadavky na software a funkce *7*

2.2.1 Registrační procedury (P1) 8

2.2.2 Žádost o certifikát DVCZE, import certifikátu DVCZE (P2) 10

2.2.3 Žádost o certifikát ISY, vydání certifikátu ISY (P3) 11

2.2.4 Doba platnosti certifikátů (P4) 14

2.2.5 Práce s řetězci certifikátů CVCA cizího státu (P5) 14

2.2.6 Práce s certifikáty a CRL CSCA 15

2.2.7 Implementace všech potřebných kryptografických algoritmů (P6) 15

2.2.8 Požadavky na uživatelské rozhraní (P7) 16

2.2.9 Požadavky na nastavení a kontrolu času (P8) 16

2.2.10 Podpora pro více typů dokladů (P9) 16

2.2.11 Podpora více profilů certifikátů (P10) 16

2.2.12 Autentizace uživatelů (P11) 17

2.2.13 Auditní záznamy (P12) 17

2.2.14 Zálohování, obnova, replikace dat (P13) 18

2.2.15 Možnosti konfigurace (P14) 19

2.3 Požadavky na bezpečnost a kryptografii *19*

2.3.1 Volba kryptografického modulu pro uložení a manipulaci s klíči (P15) 19

2.3.2 Správa klíčů a kryptografická bezpečnost (P16) 19

2.3.3 Bezpečnost kryptografických klíčů (P17) 19

2.3.4 Správa ochranných klíčů (P18) 19

2.3.5 Správa pracovních klíčů DVCZE (P19) 20

2.4 Požadavky na komunikaci a interoperabilitu *21*

2.4.1 Komunikace s NIMS (P20) 21

2.4.2 Komunikace s ISY (P21) 21

2.5 Požadavky na spolehlivost a výkon (P25) *23*

2.6 Požadavky na role a procesy *23*

2.7 Požadavky na dokumentaci 23
2.8 Požadavky na certifikaci a akceptaci funkčnosti (P26) 25
3 Požadavek na dodávku IT infrastruktury 27
3.1 Serverová část (P27) 27
3.2 Požadavky vybavení pracovišť (P28) 33
3.2.1 Minimální požadavky na stacionární administrátorské stanice NKA 34
3.2.2 Minimální požadavky na testovací stanici NKA 35
3.2.3 Minimální požadavky na přenosnou stanici ve formě notebooku 36
3.2.4 Minimální požadavky na testovací inspekční systém (TEST ISY) 36
3.2.5 Multifunkční zařízení 39
3.2.6 Skartovací zařízení 39
3.3 Požadovaná úroveň podpory na dodané technologie: (P29) 39
4 Požadavky na uživatelské rozhraní aplikace NKA *(P30)* 41
5 Další požadavky a plnění 42
5.1 Požadavky na školení 42
5.2 Prokázání referencí (P31) 42
5.3 Záruka (P32) 42
5.4 Informační povinnost a publicita (P33) 42
6 Harmonogram projektu 43
7 Projektové řízení a organizace *(P34)* 44
8 Použité reference 47
9 Seznam pojmů a zkratek 49
10 Tabulka naplnění požadavků projektu 55

1 Úvod

Přechod ke strojově čitelným veřejným dokladům s biometrickými prvky je budován etapovým způsobem, tak jak postupně vznikaly nutné specifikace a pokrok v čipových technologiích.

Základním normalizačním dokumentem je specifikace strojově čitelného cestovního dokladu, vydaná Mezinárodní organizací pro civilní letectví ICAO. Dle tohoto dokumentu byla řešena první etapa budování a implementace biometrických dokladů v České republice. Cílem této etapy bylo vytvoření národního Public Key Infrastructure (dále jen „PKI“) systému pro zabezpečení a možnost ověření pravosti dokladu.

V současné době se řeší i zabezpečení přístupu k datům v biometrickém cestovním dokladu (otisky prstů). Doklad obsahuje primárně jako biometrický prvek fotografii držitele a od roku 2009 rovněž otisk prstu.

Uložení tak citlivého osobního údaje, jakým je otisk prsu, ve veřejném dokladu vyžaduje také užití silnějšího zabezpečení přístupových práv k těmto datům.

Státy EU přistoupily k tomuto požadavku koordinovaně a vydaly specifikaci označovanou jako EAC (Extended Access Control). Opět se jedná o PKI systém určený pro vydávání oprávnění pro přístup k biometrickým datům ve veřejném dokladu.

V současné době je vybudována vydavatelská infrastruktura pro cestovní biometrické doklady vyhovující oběma specifikacím.

Pro ověřování dokladů orgány státní správy, které mají zákonné oprávnění žádat prokázání totožnosti, však požadovaná infrastruktura chybí.

Zákon č. 197/2009 Sb., o certifikaci veřejných dokladů s biometrickými údaji, ve svém § 3, odst. 2 ukládá Policii České republiky: „*v rozsahu potřebném pro výkon její působnosti a za podmínek stanovených tímto zákonem“* mj. *„vést seznam obdržených certifikátů pravosti a certifikátů přístupu a používat certifikáty pravosti a certifikáty přístupu pro určení totožnosti držitele veřejného dokladu“*.

Zákon č. 329/1999 Sb., o cestovních dokladech, ve svém § 3, odst. 3, říká že *„kontrola cestovního dokladu přísluší Policii české republiky“*.

Zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky, udává v § 5 *„Při vstupu na území je cizinec při hraniční kontrole povinen“ … „strpět ověření pravosti cestovního dokladu a ověření své totožnosti pomocí osobních údajů zapsaných v cestovním dokladu, popřípadě porovnání biometrických údajů zpracovaných v nosiči dat prostřednictvím technického zařízení umožňujícího srovnání aktuálně zobrazených biometrických údajů cizince s biometrickými údaji zpracovanými v nosiči dat cestovního dokladu, jde-li o cestovní doklad, který obsahuje nosič dat s biometrickými údaji“.*

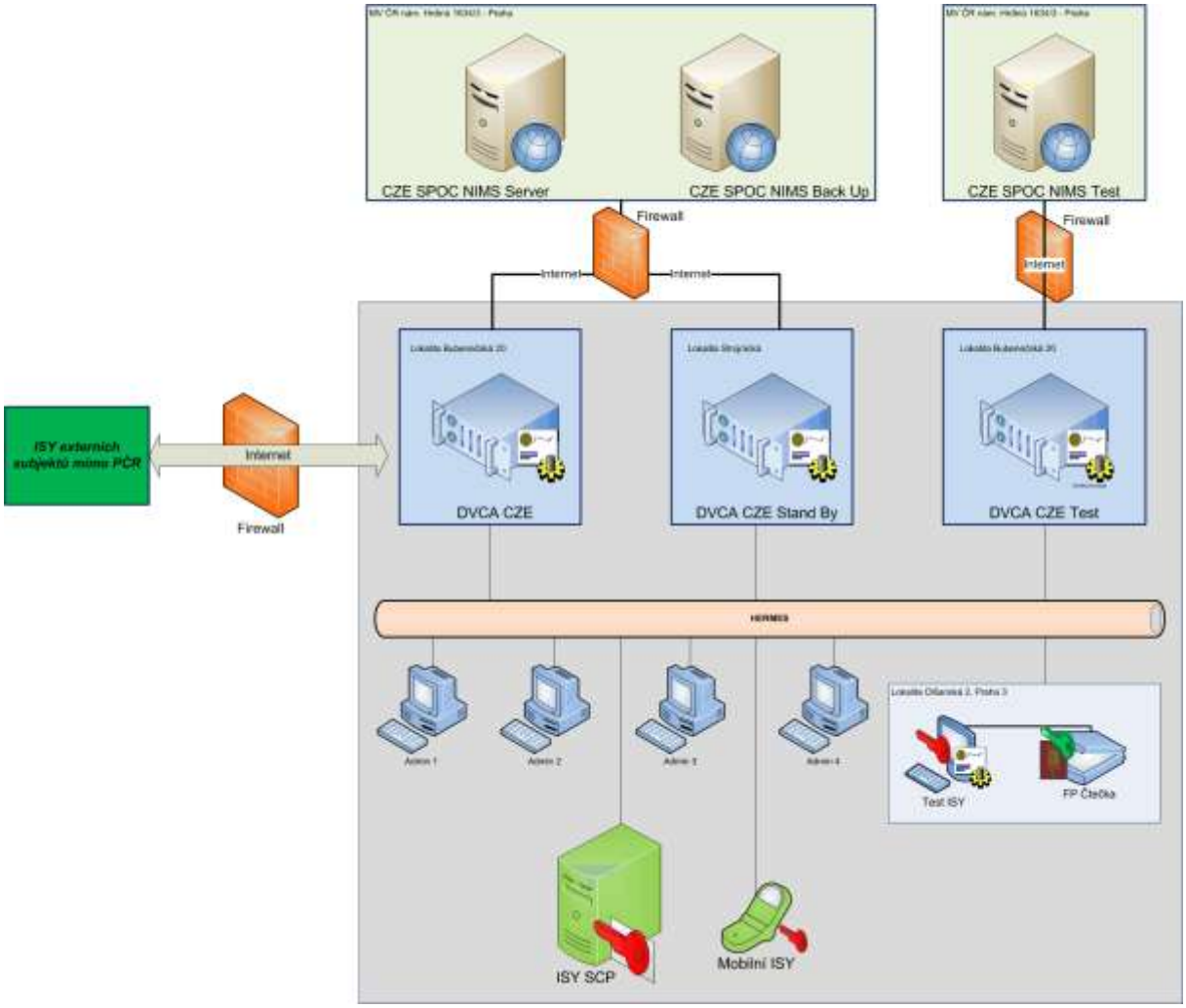
Zákon č. 273/2008 Sb., o Policii České republiky, ve svém § 63 říká, že *„Policista je oprávněn vyzvat k prokázání totožnosti osobu…“* a dále popisuje způsob a podmínky prokazování totožnosti.

Výše uvedené zákony zakládají Policii České republiky povinnost vybudovat technické prostředky s infrastrukturou pro potřeby kontroly pravosti veřejného dokladu s biometrickými prvky a kontroly totožnosti jejich držitelů. Tento systém je dále označován jako NKA – Národní kontrolní autorita a ISY – Inspekční systém.

Účelem tohoto dokumentu je specifikovat zadání pro vývoj a dodávku, vztahujících se k vybudování NKA v prostředí Policie české republiky.

1.1 Rozsah implementace projektu

Rozsah implementace projektu je definován jako komplexní dodávka centrálních komponent NKA a ovládacích konzol, kde kromě všech instancí NKA budou dodánu rovněž administrátorské stanice, přenosné administrátorské stanice, a pro účely testování i jeden inspekční systém (Test ISY).



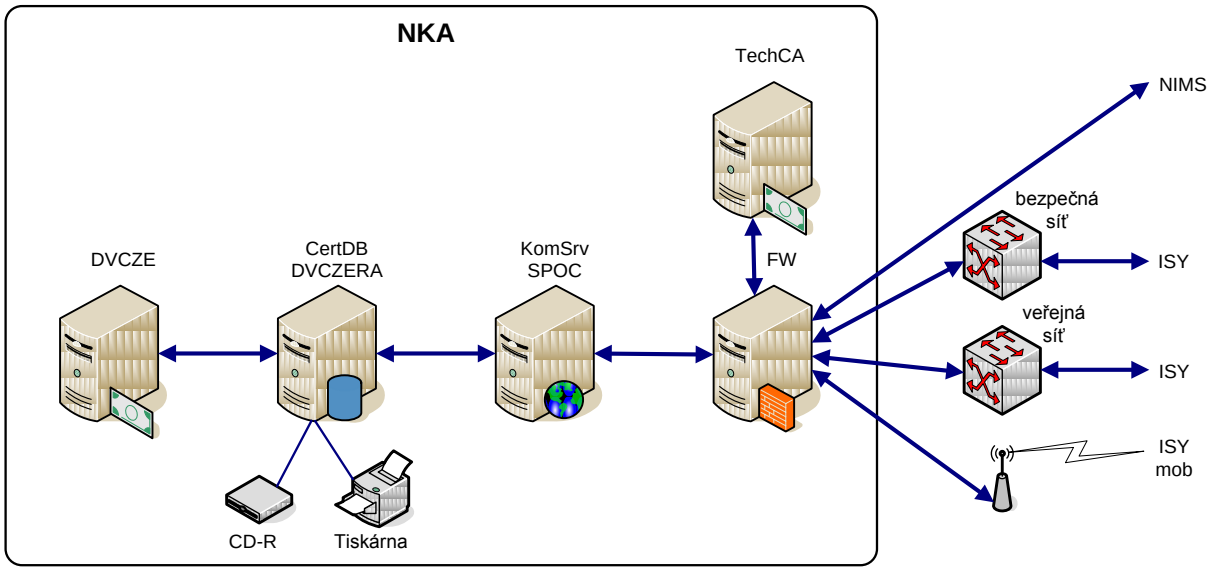
Obrázek 1: Navrhované schéma implementace projektu

Uvedené schéma představuje návrh logického uspořádání cílového stavu, kde nově dodané soubory jsou označený modře.

Klienty NKA se během implementace stanou již existující stacionární a i mobilní inspekční systémy Ředitelství služby cizinecké policie.

1.2 Blokové schéma

Pro účely tohoto dokumentu je vlastní NKA tvořen následujícími funkčními bloky. Toto schéma slouží pro znázornění činností NKA a nepředstavuje závazný model pro výstavbu NKA.



Obrázek 2: Blokové schéma NKA

Legenda:

DVCZE je vlastní certifikační autorita Document Verifier České republiky.

CertDB je úložiště certifikátů CVCA, DV a ISY, certifikátů a CRL CSCA a DS, tuzemských i zahraničních, pro potřeby ISY.

DVCZERA je Registrační autorita DVCZE.

KomSrv je zařízení, realizující komunikaci s ISY a prostřednictvím NIMS s CVCA, DV, CSCA a DS, tuzemskými i zahraničními, včetně zápisu CD-R pro iniciální navázání spojení. Realizuje protokol SPOC.

FW je firewall, realizuje bezpečné komunikační kanály s ISY a NIMS.

TechCA je technologická certifikační autorita pro bezpečné komunikační kanály.

2 Požadavky na realizaci dodávky NKA

2.1 Požadavky na hardware

NKA v uspořádání v principu odpovídajícím kap. 1.2 bude realizována ve třech identických instancích, nazývaných Hlavní, Záložní a Testovací / Školící NKA. Instalace Hlavní a Záložní instance bude prováděna na geograficky odlišných lokalitách. Testovací / Školící NKA bude obsahovat navíc i jeden kompletní testovací systém stacionárního ISY. Tomu musí odpovídat návrh hardwarového řešení.

Předpokládá se, že každá NKA bude řešena jako sada serverů a jiných zařízení, umístěných ve společné 21U přístrojové skříni. Tato skříň bude umístěna v technologických prostorách s fyzickým a režimovým zabezpečením (zajistí provozovatel). Obsluha a dohled NKA budou prováděny vzdáleně, pomocí pracovních stanic a napojením na funkce dohledového střediska. Komunikace mezi servery NKA a pracovními stanicemi musí být řešena tak, aby data mohly být přenášena po sdílené síti. V oprávněných, výjimečných případech, jako je například oprava zařízení nebo záloha pracovních klíčů DVCZE, je možné provádět úkony přímo na serverech NKA v technologických prostorách. Další možností přístupu k serverům NKA pro obsluhu a dohled, bude vzdálená správa z přenosné administrátorské stanice ve formě notebooku, a to skrze veřejnou síť Internet. Notebooky k tomuto určené budou vybaveny čtečkou identifikačních karet, aby jednoznačně určili uživatele vzdáleně přistupujícího k serveru NKA. Notebook musí splňovat celkově vysoké nároky na bezpečnost. Dodavatel zajistí přístup z přenosné stanice, a to ze sítě Internet do sítě HERMES, pomocí již stávajícího řešení, jež je tvořeno zařízením Barracuda F600, umístěného v objektu PČR – Bubenečská 20, Praha.

Nároky na obnovu provozu NKA po výpadku nejsou mimořádně vysoké. Časově nejkritičtější je nutnost vydávat následné certifikáty mobilním ISY, u nichž se předpokládá platnost **3 dny** a obnova certifikátu každý den. Z toho vyplývá, že činnost NKA po výpadku by měla být obnovena do **12-24 hodin**. Takovýto termín nevynucuje, aby Záložní NKA byla trvale v provozu a obsahovala aktuální data. Postačující bude provést přenos dat na zálohovacím mediu a Záložní NKA zprovoznit. Dodavatel musí navrhnout procesy pro přenos vlastních klíčů NKA do Záložní instance.

Třetí, Testovací / Školící instance NKA bude užívána pro vývoj software a pro školení obsluhy.

Umístění a instalace HW se předpokládá v těchto lokalitách:

a) Hlavní instance - objekt PČR - Bubenečská 20, Praha. Prostory OIPIT PP ČR.
b) Záložní instance - objekt PČR - Strojnická 27, Praha. Prostory OIPIT PP ČR.
c) Testovací/školící instance - objekt PČR - Bubenečská 20, Praha. Prostory OIPIT PP ČR.
d) Administrátorské pracoviště a testovací ISY - objekt PČR - Olšanská 2, Praha 3. Prostory ŘSCP.
e) Přenosná stanice ve formě notebooku

2.2 Požadavky na software a funkce

Systém NKA je chápán jako komponenta kontrolní a verifikační části systému pro práci s elektronickými veřejnými doklady s biometrickými prvky. Představuje platformu DV určenou

pro mezinárodní provoz a rozšířenou o podporu správy dat nezbytných pro verifikaci dokladů a autentizaci jejich držitelů na podřízených inspekčních systémech.

Oproti dosud existujícím systémům DV v ČR jsou požadavky na NKA výrazně náročnější. NKA musí být schopna podpory všech povolených kryptografických algoritmů a být klientem všech kooperujících států.

Subsystém DVCZE představuje Document Verifier v České republice určený pro mezinárodní provoz. Tato skutečnost vynucuje schopnost DVCZE pracovat s certifikáty přístupu k biometrickým údajům v elektronických pasech pro domácí i zahraniční doklady. Základním určením DVCZE je získat certifikát od nadřízených CVCA a následně na základě identifikace a autentizace žádostí od ISY vydávat certifikáty oprávnění pro podřízené ISY.

Subsystém CertDB je komponenta podporující správu certifikátů pravosti a certifikátů přístupu pro domácí i zahraniční veřejné doklady. Subsystém CertDB získává aktuální data národních CSCA, CVCA a DV systémů (uložené na NIMS) a tato data na základě požadavků přeposílá podřízeným systémům ISY pro potřeby kontroly pravosti dokladu a přístupu k biometrickým údajům. Subsystém CertDB zároveň plní funkce registrační autority DVCZE. Tato podpora se předpokládá pro stejnou množinu ISY, které pokrývá DVCZE.

Specifikace ČSN 36 9791 definuje rozhraní pro komunikaci národních systémů SPOC mezi sebou. Toto rozhraní je pro propojení systému NKA a NIMS (CVCA, CSCA) vyžadováno na základě schválené implementace SPOC.

2.2.1 Registrační procedury (P1)

DVCZE bude klientem všech nadřízených CVCA systémů (domácích i zahraničních). Sama DVCZE je nadřízenou certifikační autoritou spravovaných systémů ISY. Komunikační infrastruktura se zabezpečením odvozeným ze systému SPOC vyžaduje registraci u národní SPOC CA před vydáním certifikátu pro zabezpečení komunikace.

Registrační procedury DVCZE realizuje subjekt DVCZERA (součást CertDB).

2.2.1.1 Registrace DVCZE u domácí CVCA

Kompletní registrační procedura musí vynutit sekvenci těchto činností. Bez registrační procedury nesmí být povoleno vydat žádost o certifikát u domácí CVCA

a) DVCZERA připraví podklady pro registraci, viz CCP [9]:
   I. Certifikát pro DVCZE o shodě s CCP;
   II. Seznam zastřešujících systémů ISY.
b) DVCZERA přebere od CVCA Rozhodnutí o registraci, která definuje PKI identitu DVCZE (Country Code a Holder Mnemonic) a kořenový certifikát CVCA;
c) Na DVCZE se nastaví vlastní identita systému (z Rozhodnutí o registraci);
d) Na DVCZE se zavede kořenový certifikát CVCA.

2.2.1.2 Registrace DVCZE u cizích CVCA

Identitu DVCZE definuje domácí CVCA v Rozhodnutí o registraci. Tuto identitu předává DVCZE v registračních procedurách prostřednictví CVRA k zahraničním CVCA.

CCP [9] vyžaduje předání registračních údajů, oboustranně schváleným bezpečným kanálem.

Výstupem registrační procedury v systému DVCZE je zavedení identity spolupracující CVCA a jejího kořenového certifikátu.

Vlastní způsob registrace musí být v souladu s CCP [9].

2.2.1.3 Registrace subjektů SPOC NKA u SPOC CA

CVRA přebere od SPOC CA Rozhodnutí o registraci pro klienta a server SPOC systému NKA. SPOC NKA tak získá svou PKI identitu.

2.2.1.4 Registrace klientů ISY

O registraci a následně o certifikát mohou žádat ISY, provozované složkami bezpečnostních sborů ČR a jinými orgány státní správy ČR, oprávněnými žádat prokázání totožnosti osob.

Otázka registrace klientů je úzce spjata s problematikou prvotní žádosti o certifikát Vzhledem k množství očekávaných klientů bude jejich registrace prováděna dávkově. Oprávněný zástupce provozovatele ISY dodá registrační autoritě DVCZE seznam klientů, kteří budou registrováni, ve formě:

a) Unikátní jméno (kód) pro stacionární ISY;

b) Identifikátor zařízení pro mobilní ISY.

Za správnost seznamu ručí provozovatel ISY.

Z těchto údajů vytvoří registrační autorita DVCZE jedinečný kód každého ISY, který bude obsažen v poli CHR jeho certifikátu. DVCZE vydá Rozhodnutí o registraci pro podřízené ISY klienty. V rozhodnutí o registraci je uvedena CAR identita systému DVCZE a CHR identita klienta ISY, CHR identita ISY je tvořena podle následujícího schéma, podle specifikace TR-03110 [2]:

Délka	Pole	Popis
2	ISO 3166-1 country code	Dvoupísmenový kód státu, do nějž subjekt definovaný CHR náleží
max. 9	Holder code	Identifikátor držitele certifikátu
2	SqNum - state	Sekvenční číslo – kód státu, jež bude vydávat certifikát. Je generováno CA.
3	SqNum - serial	Sekvenční číslo – třímístný serial z množiny číslic a písmen anglické abecedy

Pro ISY v ČR bude naplnění polí následující:

Pole	Hodnota	Popis
Country code	CZ	ISO 3166-1 kód pro Českou republiku
Holder code	ISABCXXXX	IS = Inspekční systém A = alfanumerický znak pro orgán státní správy provozující ISY B = alfanumerický znak pro složku orgánu státní správy C = alfanumerický znak pro systém, jehož součástí je dané ISY XXXX = čtyřmístný sekvenční čítač, kde každá pozice čítače je obsazena znakem z uspořádané množiny číslic a velkých

Pole	Hodnota	Popis
		písmen anglické abecedy (X je prvkem (0,1,2, ...,9,A,B, ... ,X,Y,Z)), přiděluje DVCZERA při registraci ISY.
SqNum - state	CZ	ISO 3166-1 kód pro Českou republiku
SqNum - serial	XXX	Třímístný sekvenční čítač, kde každá pozice čítače je obsazena znakem z uspořádané množiny číslic a velkých písmen anglické abecedy (X je prvkem (0,1,2, ...,9,A,B, ... ,X,Y,Z))

Pro podporu registrace klientů musí být implementovány tyto postupy:

a) Registrace klienta – prvotní zavedení registračních údajů;

b) Prohlížení klienta – zobrazení registrovaných dat;

c) Editace klienta – možnost změnit registrační data klienta.

Vzhledem k očekávanému počtu klientů, zejména mobilních ISY, musí být DVCZE, resp. její registrační autorita, vybavena uživatelsky přívětivými nástroji pro správu velkého počtu klientů, jako seskupování, hromadné editace, dávkové příkazy, importy-exporty aj.

2.2.2 Žádost o certifikát DVCZE, import certifikátu DVCZE (P2)

2.2.2.1 Prvotní žádost o certifikát

Postupy při podání prvotní žádosti musí respektovat požadavky nadřízené infrastruktury, tj CVCA a systém SPOC:

a) Úspěšně ukončená registrační procedura u domácí CVCA;

b) Úspěšně ukončená registrační procedura u SPOC CA.

Žádost o prvotní certifikát musí být doručena komunikačním kanálem SPOC nebo manuálně kurýrem.

Při manuálním způsobu doručení je součástí žádosti o certifikát Předávací protokol k žádosti, který drží kryptografický otisk SHA2 žádosti.

Generování žádosti o certifikát je spojeno se vznikem párových dat. V této souvislosti se požaduje stanovení postupu pro identifikaci příslušného veřejného klíče označovaného jako CHR. Jedná se především o způsob generování a správy položky Sequence Number (TR-03110 A.3.1).

Zadavatel požaduje dodání funkcionalit podporujících oba způsoby doručení žádosti o certifikát.

2.2.2.2 Následná žádost o certifikát

Následná žádost o certifikát musí být generována automatizovaně. Vyžaduje se návrh postupů vedoucích k optimalizovanému stanovení data generování následné žádosti. V tomto postupu musí být zohledněna doba platnosti aktuálního certifikátu, doba platnosti podřízených klientských certifikátů a režie komunikačních kanálů na doručení žádosti, vydání certifikátu a doručení certifikátu. Dále musí být zohledněna doba na zpracování žádosti CVCA od DV a to 7 dní.

Automatizované zpracování předpokládá odeslání žádosti a přijetí certifikátu rozhraním SPOC.

2.2.2.3 Import vlastního certifikátu od CVCA

Pro import vlastního certifikátu musí být implementovány tyto postupy:

a) Manuální import certifikátu – v případě doručení certifikátu kurýrem, případně formou e-mailu;

b) Automatizované přijetí certifikátu – v případě doručení certifikátu rozhraním SPOC.

Po přijetí nového vlastního certifikátu se veškeré podpisové operace realizují s využitím nových párových dat náležejících tomuto certifikátu

2.2.2.4 Žádost o certifikát k SPOC CA

Postup vydání žádosti o certifikát pro komunikační subsystém SPOC systému NKA musí odpovídat požadavkům SPOC CA. Prvotní žádosti o vydání certifikátu musí předcházet registrace SPOC NKA u SPOC CA. Systém SPOC NKA musí vygenerovat žádost o certifikát ve formátu PKCS#10. Profil certifikátu je stanoven ve specifikaci SPOC[8].

Následnou žádost o certifikát musí vytvořit obsluha před vypršením platnosti starého certifikátu.

2.2.2.5 Import certifikátu SPOC CA

Import certifikátu SPOC CA je realizován manuálním postupem. Předpokládaná doba platnosti klientského certifikátu je 18 měsíců, kořenového 10 let.

2.2.3 Žádost o certifikát ISY, vydání certifikátu ISY (P3)

2.2.3.1 Správa klientů ISY

DVCZE musí disponovat softwarovými nástroji na správu dat většího počtu registrovaných klientů. Ve správě klienta musí být zahrnuty tyto postupy:

a) Registrace klienta – nástroj na zavedení nového klienta ISY;

b) Prohlížení klientů;

c) Editace klienta – úprava registračních údajů;

d) Blokování klienta – zablokování klienta musí znemožnit vydání certifikátu pro klienta;

e) Odblokování klienta.

Předmětem správy klienta jsou především tyto údaje:

a) Jméno klienta;

b) Identifikátor klienta (CHR - Country Code + Holder Code);

c) Odkaz na profil certifikátu;

d) Oprávnění pro přístup k datům (DG3, DG4);

e) Blokovací příznaky.

Profil certifikátu by měl zohledňovat především časovou platnost certifikátu, který musí být stanoven dle charakteru ISY.

2.2.3.2 Zpracování žádosti o certifikát od ISY, vydání certifikátu

Po registraci klienta ISY, viz kap. 2.2.1.4 je možno zpracovávat žádosti o certifikát od ISY. Důležitou otázkou je ověření identity žadatele a pravosti žádosti při prvotní žádosti o certifikát, a to zejména u mobilních ISY.

Zadavatel bude akceptovat také takové řešení, které bude zcela konformní se standardem BSI TR-03129, a zároveň zaručí akceptaci NKA zahraničními subjekty a úspěšné provedení certifikace ISO/IEC 27001.

2.2.3.2.1 Žádost v listinné podobě

V tomto případě je použit postup obdobný jako při přidělování přístupových oprávnění. Žádost o prvotní certifikát ISY má podobu formuláře, obsahujícího

a) Jedinečný identifikátor ISY (viz kap. 2.2.1.4);

b) Jméno a podpis žadatele;

c) Jméno a podpis nadřízeného žadatele.

Za pravost žádosti odpovídá oprávněná osoba, zastupující provozovatele ISY.

Následně ISY vygeneruje svůj klíčový pár a žádost o certifikát dle specifikace TR-03110. Žádost zašle elektronicky na NKA. Registrační autorita DVCZE porovná údaje v žádosti se seznamem registrovaných klientů. Pokud žádost splňuje všechny požadavky, žádající ISY je registrována a o vydání prvotního certifikátu je podána žádost v listinné podobě, DVCZE vygeneruje certifikát a NKA jej odešle žádajícímu ISY. Zároveň mu odešle aktuální řetězce zahraničních certifikátů a CRL.

2.2.3.2.2 Žádost s použitím kódové knihy

V této verzi NKA vydá přiměřený počet obálek pro utajený tisk, které budou obsahovat jeden kódový řetězec čitelný zvenčí a jeden kódový řetězec čitelný jen po otevření obálky. Tyto obálky se kurýrní službou PČR, dokumentovaným způsobem, distribuují provozovatelům ISY. Přitom je dodrženo určení obálek do orgánů státní správy a jejich organizačních jednotek souhlasné se znaky A a B identifikátoru CHR, viz kap. 2.2.1.4. Při prvotní žádosti o certifikát ISY pak obsluha dokumentovaným způsobem odebere jednu z uložených obálek a zadá do zařízení oba kódy, které pak ISY odešle jako součást žádosti. Registrační autorita DVCZE porovná údaje v žádosti se seznamem registrovaných klientů, vyhodnotí shodu a platnost kódových řetězců a místo, kam byly doručeny proti CHR žadatele. Pokud žádost splňuje všechny požadavky, žádající ISY je registrována a kódy souhlasí, DVCZE vygeneruje certifikát a NKA jej odešle žádajícímu ISY. Zároveň mu odešle aktuální řetězce zahraničních certifikátů a CRL. Použité kódy jsou na straně NKA označeny jako neplatné, na straně žadatele dokumentovaným způsobem zlikvidovány.

2.2.3.2.3 Žádost na nosiči dat

V této verzi ISY vygeneruje svůj klíčový pár a žádost o certifikát dle specifikace TR-03110. Žádost uloží na datový nosič (zapisovatelné CD nebo DVD) a doprovodí formulářem s uvedením údajů o žádající ISY a kryptografickým klíčem ke kontrole správnosti obsahu datového nosiče. Datový nosič a formulář doručí důvěryhodný kurýr na NKA. Registrační autorita DVCZE porovná údaje v žádosti se seznamem registrovaných klientů. Pokud žádost splňuje všechny požadavky a žádající ISY je registrována, DVCZE vygeneruje certifikát a NKA jej uloží na datové medium a doprovodí předávacím formulářem. Zároveň na datové

medium uloží aktuální řetězce zahraničních certifikátů a CRL. Důvěryhodný kurýr doručí datové medium zpět k žádajícímu ISY.

2.2.3.2.4 Žádost podepsaná čipovou kartou

V této verzi NKA vydá přiměřenému počtu odpovědných osob čipové karty nebo zaregistruje jejich existující osobní čipové karty (například vydané pro identifikaci k jiným systémům). Při prvotní žádosti o certifikát ISY pak odpovědná osoba vloží čipovou kartu do čtečky ISY. ISY vygeneruje svůj klíčový pár a žádost o certifikát dle specifikace TR-03110. Žádost navíc podepíše soukromým klíčem obsaženým na čipové kartě. Žádost zašle elektronicky na NKA. Registrační autorita DVCZE porovná údaje v žádosti se seznamem registrovaných klientů a seznamem registrovaných čipových karet. Pokud žádost splňuje všechny požadavky, žádající ISY je registrována a žádost o vydání prvotního certifikátu je podepsána soukromým klíčem registrované čipové karty, DVCZE vygeneruje certifikát a NKA jej odešle žádajícímu ISY. Zároveň mu odešle aktuální řetězce zahraničních certifikátů a CRL.

Každá žádost odeslaná z mobilního ISY offline musí být podepsána, jak je uvedeno ve specifikacích TR 03129 a TR 03129-2. NKA musí podpisy ověřovat. Podrobný návrh realizace žádosti o certifikáty a jejího ověření bude dále předmětem analýzy řešení.

Aktuálně Zadavatel používá 1 konkrétní systém mobilního ISY Offline a má k dispozici nástroj na personalizaci SAM modulů. Předpokládá se úprava personalizačního procesu podle společného návrhu Zhotovitele NKA a ISY offline, který zajistí Zadavatel.

2.2.3.2.5 Žádost podepsaná SAM modulem

V této verzi se používá k identifikaci žadatele tzv. SAM modul, což je malá čipová karta, kterou lze namontovat do mobilního ISY. NKA vydá SAM moduly pro registrované mobilní ISY. Při prvotní žádosti o certifikát ISY pak ISY vygeneruje svůj klíčový pár a žádost o certifikát dle specifikace TR-03110. Žádost navíc podepíše soukromým klíčem obsaženým na SAM. Žádost zašle elektronicky na NKA. Registrační autorita DVCZE porovná údaje v žádosti se seznamem registrovaných klientů a seznamem vydaných SAM. Pokud žádost splňuje všechny požadavky, žádající ISY je registrována a žádost o vydání prvotního certifikátu je podepsána soukromým klíčem vydaného SAM, DVCZE vygeneruje certifikát a NKA jej odešle žádajícímu ISY. Zároveň mu odešle aktuální řetězce zahraničních certifikátů a CRL. Při tom také dojde ke spojení identity zařízení a SAM, což může být využito ke kontrole při vydávání následných certifikátů.

Výše uvedené postupy lze pro zvýšení bezpečnosti kombinovat.

U stacionárních ISY je možné použít všechny postupy kromě 2.2.3.2.5. U mobilních ISY je možné použít všechny postupy kromě 2.2.3.2.3.

V procesu zpracování žádosti musí být provedeny tyto kontroly:

a) Ověření CAR žádosti – zda je určena DVCZE;

b) Ověření identity klienta proti databázi registrovaných klientů (CertDB);

c) Ověření příznaku blokování klienta;

d) Ověření integrity žádosti (ověření vnitřního podpisu žádosti);

e) Ověření kompatibility algoritmu a doménových parametrů směrem k CAR;

f) Ověření správnosti CAR (zda odkazuje na aktuální klíčový pár).

U následných žádostí o certifikát je nutné ověřit, zda je vnější podpis žádosti ověřitelný starým certifikátem

Vydání certifikátu je spojeno s přiřazením správného profilu certifikátu k danému klientu (především s ohledem na časovou platnost vydaného certifikátu). Pokud došlo k aktualizaci položky CAR, je s vydaným certifikátem pro ISY odeslán i aktuální certifikát DV.

Způsob vydání prvotního certifikátu může být ovlivněn koncepcí systému ISY.

2.2.4 Doba platnosti certifikátů (P4)

Doba platnosti vlastního certifikátu DVCZE je **70** dnů. Tento časový údaj bude vyznačen v datovém objektu Certificate Effective Date a po uplynutí této doby certifikát ztrácí platnost.

Po vypršení platnosti certifikátu DVCZE a tedy i uplynutí doby použitelnosti soukromého klíče DVCZE k vystavování certifikátů je tento klíč zničen. Generování žádosti o následný certifikát DVCZE bude provedeno s minimálním předstihem 14 dnů, obvykle 39 dnů před vypršením platnosti starého certifikátu.

Doba platnosti vydaných certifikátů stacionárních ISY je **14 dní**. Vydání následného certifikátu ISY je provedeno s předstihem 7 dní před vypršením platnosti starého certifikátu.

Doba platnosti vydaných certifikátů mobilních ISY je **3 dny**. Vydání následného certifikátu ISY je provedeno s předstihem 2 dny před vypršením platnosti starého certifikátu.

Časová pravidla pro vydávání certifikátů DVCZE v období obnovy certifikátu DVCZE:

a) Přijme-li DVCZE žádost o certifikát v době před vydáním svého nového certifikátu, vydá DVCZE certifikát právě platným klíčem. Pokud obsahovala žádost položku CAR (specifikace požadovaného klíče autority) a její hodnota neodpovídá hodnotě ve vydaném certifikátu, bude součástí výstupních dat i aktuální certifikát DVCZE;

b) Přijme-li DVCZE žádost o certifikát v době, kdy jsou platné dva certifikáty DVCZE (v době překryvu platností certifikátů), bude pro vydání certifikátu ISY použit novější certifikát DVCZE (respektive odpovídající privátní klíč) i pokud žádost obsahovala CAR a požadovala použití staršího klíče DVCZE. Součástí dat odpovědi směrem k ISY bude také aktuální certifikát DVCZE;

c) Pokud do termínu vypršení platnosti certifikátu DVCZE zbývá méně než 14 dnů a DVCZE nemá platný novější certifikát, DVCZE nevydá certifikát ISY;

d) Počátek platnosti certifikátu bude dán dnem vydání certifikátu, konec platnosti bude vypočten z doby platnosti certifikátu.

2.2.5 Práce s řetězci certifikátů CVCA cizího státu (P5)

DVCZE spravuje kořenové a link certifikáty všech nadřízených systémů CVCA. Pro podporu této činnosti byl navržen protokol SPOC. Modifikovaný protokol SPOC pro vnitrostátní použití musí být schopen rozlišovat mezi typy certifikátů CVCA.

Pro potřeby DVCZE a podřízených systémů ISY musí být v systému spravovány pro každý registrovaný systém CVCA tyto údaje:

a) Stát;

b) Typ certifikátu (identifikuje určení certifikátu – ePas, ePKP,eID, ...);

c) Řetězec platných kořenových a link certifikátů.

Pro daný stát může být v systému registrováno více CVCA subjektů, dle toho, jaké typy certifikátů daná autorita podporuje.

Pro potřeby správy by měly být implementovány tyto operace:

a) Import aktuálních kořenových a link certifikátů daného státu a typu;

b) Prohlížení kořenových a link certifikátů.

DVCZE musí zajišťovat správu vlastních certifikátů:

a) Import vlastních certifikátů (manuální, automatizovaný rozhraním SPOC);

b) Prohlížení vlastních certifikátů, případně žádostí o certifikát.

DVCZE musí zajišťovat správu klientských certifikátů:

a) Správa profilů klientských certifikátů;

b) Prohlížení klientských žádostí o certifikát;

c) Prohlížení klientských certifikátů.

2.2.6 Práce s certifikáty a CRL CSCA

Subsystém CertDB zajišťuje správu dat systému CSCA sloužících pro bezpečné ověření pravosti veřejného dokladu. Tato data jsou určena především pro podřízené systémy ISY.

Subsystém CertDB musí spravovat pro každý podporovaný systém CSCA tyto údaje (jsou odrazem evidovaných systémů v NIMS):

a) Stát;

b) Typ certifikátu (ePas, ePKP, eID ...);

c) Sada platných kořenových certifikátů pro daný systém;

d) Sada platných certifikátů CDS vydaných příslušnou kořenovou autoritou;

e) Sada aktuálních seznamů zneplatněných certifikátů vydaných příslušnými kořenovými autoritami.

Pro daný stát může být v systému evidováno více CSCA subjektů, kteří vydávají certifikáty pro zabezpečení pravosti různých typů dokladů (ePas, ePKP, eID).

Některé státy (včetně ČR) sdílí společnou CSCA pro více typů dokladů.

Správa dat systému CSCA musí být založena na využití modifikovaného protokolu SPOC pro přístup k příslušným datům na systém NIMS.

Zadavatel bude akceptovat, řešení, které podporuje práci s Master Listem a Defect Listem. Podmínkou je nastolení shody se standardem ICAO 9303 a BSI TR-03129.

2.2.7 Implementace všech potřebných kryptografických algoritmů (P6)

DVCZE musí být schopna pracovat se všemi přípustnými druhy a modifikacemi kryptografických algoritmů, přicházejících v úvahu. Jedná se o skupiny algoritmů RSA, DSA a EC-DSA. Závazný seznam přípustných kryptografických algoritmů a délek klíčů je uveden v ICAO Doc 9303, Part 1, Vol. 2, kapitola 8 [3]. Určitá upřesnění se nacházejí rovněž v jednotlivých Supplement to ICAO Doc 9303 a dále v TR-03110 [2] a TR-03111 [4] (speciálně pro algoritmy eliptických křivek).

2.2.8 Požadavky na uživatelské rozhraní (P7)

Správa a užívání systému by mělo být u často prováděných činností realizováno prostřednictvím grafického uživatelského rozhraní. Složitější činnosti, které vyžadují sekvenční řazení elementárních operací, musí být řešeny softwarovým nástrojem, který poskytuje obsluze podporu pro správné provedení řetězce operací s maximální mírou automatizace.

2.2.9 Požadavky na nastavení a kontrolu času (P8)

DV certifikáty obsahují položky vymezující časové údaje označované jako:

a) Certificate Effective Date – datum generování certifikátu;

b) Certificate Expiration Date – datum vypršení platnosti certifikátu.

Elektronický pas, jakožto subjekt bez zdroje vlastního reálného času, musí být schopen omezeně vyhodnocovat časovou platnost certifikátů. Tento požadavek byl implementován tak, že čip po zavedení kryptograficky ověřeného certifikátu porovná vlastní časový údaj s hodnotou Certificate Effective Date. Pokud je tento údaj v budoucnu proti drženému údaji, čip si jej zavede jako nový aktuální čas.

Pokud by se stalo, že časový údaj v certifikátu je proti reálnému času posunut do budoucnosti a byl by zaveden do čipu, takový doklad nebude nadále funkční s certifikáty s reálnými časovými údaji, neboť tyto certifikáty vyhodnotí jako exspirované.

Chybné nastavení času v systému, z nějž se odvozuje časový údaj do certifikátu, může mít kritické dopady do další funkčnosti dokladu.

Systém DVCZE vyžaduje násobnou kontrolu časového údaje (více NTP serverů, dohledové centrum, kontrola času v podřízeném systému ISY).

2.2.10 Podpora pro více typů dokladů (P9)

DVCZE musí být připraven pro podporu více typů strojově čitelných dokladů s biometrickými prvky např. ePKP. Tento typ dokladu také používá CV certifikáty pro ověření oprávnění pro přístup k biometrickým údajům. Technologicky se jedná o stejný systém jako pro strojově čitelné cestovní doklady s biometrickými prvky.

Skutečnost, že některá státy vybudují nový CVCA systém, jiné budou sdílet existující CVCA pro více typů dokladů, bude mít dopad do CertDB pro správu certifikátů CVCA

Pro DVCZE je zdrojem registrovaných CVCA systém NIMS. DVCZE s využitím protokolu SPOC aktualizuje obsah své CertDB údaji o CVCA a typech podporovaných certifikátů.

2.2.11 Podpora více profilů certifikátů (P10)

Dle charakteru podřízených ISY, systém musí mít možnost přiřadit ISY profil certifikátu, který odpovídá jeho vlastnostem.

Za podstatnou vlastnost se pokládá charakter správy privátního klíče systému ISY. Bude-li spravován centrálně, nehrozí nebezpečí jeho zneužití zcizením, a proto platnost příslušného certifikátu může být delší. Pokud budou u např. mobilních zařízení klíče drženy lokálně, musí být platnost příslušného certifikátu zkrácena na minimum. Navrhujeme dobu platnosti certifikátů pro mobilní ISY na **3** dny, přičemž po uplynutí jednoho dne by ISY žádal o následný certifikát.

2.2.12 Autentizace uživatelů (P11)

K identifikaci a autentizaci oprávněných uživatelů je vyžadována dvou faktorová autentizace, například autentizační prostředek (čipová karta, token apod.) a PIN, nikoliv pouhé jméno a heslo. Výjimky jsou možné v oprávněných případech, např. přihlášení administrátora při inicializaci nového systému.

2.2.13 Auditní záznamy (P12)

Systém musí zaznamenávat do auditního logu údaje, vážící se k bezpečnosti provozu.

V rámci provozu DVCZE jsou zaznamenávány provozní události následujících typů:

a) Události spojené s operacemi v rámci životního cyklu certifikátu;

b) Události spojené s řízením přístupu k systému DVCZE;

c) Události spojené se změnami konfigurace systémů DVCZE;

d) Události spojené s životním cyklem klienta;

e) Jiné významné události spojené s provozem systémů DVCZE.

V rámci událostí, spojených s operacemi životního cyklu certifikátu, jsou zaznamenávány:

a) Zavedení certifikátu;

b) Generování vlastní žádosti o certifikát;

c) Zpracování žádosti o certifikát klienta;

d) Vydání certifikátu;

e) Export certifikátů;

V rámci událostí, spojených s řízením přístupu k systému DVCZE, jsou zaznamenávány:

a) Zavedení uživatele;

b) Správa uživatele (zneplatnění, atd.);

c) Úspěšné přihlášení uživatele;

d) Neúspěšný pokus o přihlášení;

e) Odhlášení uživatele.

V rámci jiných významných událostí, spojených s provozem systému DVCZE, jsou zaznamenávány zejména:

a) Spuštění systému DVCZE;

b) Ukončení / přerušení provozu systému DVCZE;

c) Provedení záloh;

d) Vytvoření ochranných klíčů;

e) Použití ochranných klíčů;

f) Generování párových dat DVCZE a certifikátů;

g) Zálohování soukromého klíče z HSM;

h) Vložení soukromého klíče ze zálohy do HSM,

i) Provozní chyby.

Pro všechny události jsou zaznamenávány identifikace události, čas výskytu události a uživatele, závažnost události.

Události jsou zaznamenávány:

a) Elektronicky, v databázi nebo logovacím souboru;

b) Případně současně v papírové formě (provozní deníky).

V rámci událostí, spojených se změnami konfigurace systému DVCZE, jsou zaznamenávány zejména:

a) Změny politiky DVCZE (událost vedena v provozním deníku);

b) Změny konfigurace systémů DVCZE (událost vedena v provozním deníku).

Auditní záznamy jsou ukládány v textové podobě s následující strukturou:

a) Závažnost události;

b) Datum a čas vzniku události;

c) Kategorie typu události (skupina a typ);

d) Zdroj – komponenta generující auditní záznam;

e) Identifikace uživatele;

f) Identifikace role;

g) Unikátní číslo události;

h) Data – údaje blíže popisující zaznamenanou událost (vstupní údaje, výsledek operace a pod).

Integritu auditních záznamů garantuje jejich uložení se zabezpečením přístupových práv. Po exportu auditních záznamů do archivu bude zachována struktura dat v textové podobě, data bude možno prohlížet standardními editory.

2.2.14 Zálohování, obnova, replikace dat (P13)

Záložní instance DVCA bude trvale v provozu a zároveň se budou provádět zálohy, jak je uvedeno níže v této kapitole.

Přepnutí hlavního uzlu na záložní musí být realizováno automaticky. Zadavatel požaduje, aby všechny další procesy přechodu na záložní řešení byly realizovány automaticky

Zadavatel očekává, že uchazeč navrhne takové řešení, které naplní požadavky na dostupnost NKA a to při zachování principu bažící záložní instance NKA

Dodavatel musí v rámci vývoje systému navrhnout procesy pro:

2.2.14.1 Replikace kryptografických klíčů

Při návrhu koncepce správy klíčů zvážit metody automatické replikace kryptografických klíčů, které by garantovaly sdílení stejných kryptografických klíčů ve všech HSM pracujících ve společném clusteru.

2.2.14.2 Replikace obsahu databáze

Za provozu musí být replikována databáze na oba uzly clusteru, případně bude cluster pracovat nad sdíleným diskovým polem.

Při ukončení činnosti na aktivním systému NKA daného dne musí být provedena replikace (záloha) obsahu relevantních tabulek databáze pro přenos na Záložní systém.

2.2.14.3 Archivace dat a klíčů pro obnovu systému

Archivace dat a klíčů slouží pro uchování stavu databáze a kryptografických klíčů na zálohovacím datovém nosiči. Smyslem jejího provádění je zachovat právě aktuální obraz systému pro případ katastrofy, kdy by mohlo dojít k fyzické likvidaci jak hlavního tak záložního systému.

2.2.15 Možnosti konfigurace (P14)

NKA musí být konfigurovatelná pro použití všech přípustných kryptografických algoritmů. NKA musí být konfigurovatelná pro správu většího množství různých typů ISY. NKA musí mít konfigurovatelná uživatelská oprávnění. NKA musí být vybavena konfigurovatelným **firewallem pro vytváření bezpečných komunikačních kanálů** k NIMS a ISY. NKA musí být konfigurovatelná pro případ existence více systémů CSCA a CVCA v rámci jednoho státu. NKA musí mít možnost ručně korigovat nastavení systémového času. NKA musí mít možnost konfigurovat profil vydávaného certifikátu. NKA musí mít možnost konfigurovat vytváření záznamů o provozu systému a činnostech uživatelů.

2.3 Požadavky na bezpečnost a kryptografii

2.3.1 Volba kryptografického modulu pro uložení a manipulaci s klíči (P15)

CCP [9], Dodatek B. 1, vynucuje pro správu kryptografických klíčů (generování klíčů, jejich uložení a použití) v „certifikačních orgánech“, tj. CVCA a DVCA nebo Inspekčních systémech využívat bezpečné zařízení, které splňuje některý z těchto požadavků:

a) Certifikaci FIPS PUB 140-1 (140-2) level 3 nebo vyšší;

b) PP-SSCD (CEN/TC 224: prEN 14169-1:2009 - Protection profiles for Secure signature creation device — Part 2: Device with key generation);

c) BSI-PP-0045-2009: Cryptographic Modules Security Level "Enhanced" Version 1.01.

2.3.2 Správa klíčů a kryptografická bezpečnost (P16)

Z hlediska správy kryptografických klíčů je nutné specificky přistupovat k různým typům klíčů:

a) Ochranné klíče – slouží pro vytváření kryptografických záloh pracovních klíčů

b) Pracovní klíče – jsou klíče zabezpečující základní funkčnosti DV – slouží pro vydávání / podepisování certifikátů

V rámci správy kryptografických klíčů budou podporovány dále uvedené funkčnosti.

2.3.3 Bezpečnost kryptografických klíčů (P17)

Technická ochrana kryptografických klíčů bude realizována použitím zařízení viz kap. 2.3.1.

2.3.4 Správa ochranných klíčů (P18)

Ochranné klíče slouží ke kryptografickému zabezpečení ostatních klíčů v systému, které mají být bezpečně zálohovány a uloženy mimo prostředí HSM. Tento klíč musí existovat také

mimo prostor HSM a nikdo jej nesmí znát. Je tedy zřejmé, že způsob manipulace a uložení samotných záloh ochranných klíčů je bezpečnostně citlivou záležitostí.

Uložení Ochranných klíčů mimo prostředí HSM musí být realizováno s respektováním zásady rozdělení znalostí. Klíč musí být rozdělen na více částí, každá část klíče musí být ve správě jiné důvěryhodné osoby. Komponentu klíče je vhodné držet na alespoň na dvou nezávislých médiích (např. čipová karta a PIN obálka).

Kompromitace ochranného klíče je tak možná jen za současného selhání všech držitelů komponent klíče.

Pro správu ochranných klíčů musí být definovány tyto procesy:

2.3.4.1 Generování ochranného klíče

Proces generování klíčů, při kterém jsou klíče zároveň uloženy na nosiče, viz výše, spouští role Správce klíčového hospodářství, vyžaduje však účast rolí, které zajišťují bezpečné uložení komponent ochranného klíče na záložních mediích.

Ke každé komponentě klíče musí existovat Protokol o generování komponenty klíče a jejich převzetí.

2.3.4.2 Obnovení ochranných klíčů ze zálohy

Proces obnovy ochranných klíčů ze zálohy provádí role Správce klíčového hospodářství, vyžaduje však účast držitelů jednotlivých komponent klíče. Tato operace může být provedena jen na příkaz krizového štábu (při obnově systému po poruše nebo katastrofě).

2.3.5 Správa pracovních klíčů DVCZE (P19)

Pracovními klíči DVCZE se rozumí klíčový pár (privátní a veřejný klíč), určený pro vytvoření vlastní žádosti o certifikát a podepisování klientských certifikátů DVCZE. Mezi pracovní klíče dále patří také klíče páry TechCA, kdy jejich uložení je požadováno v HSM modulu obdobně jako u klíčových párů DVZCE.

2.3.5.1 Generování pracovního klíče

Generování pracovního klíče je součástí procesu vydání vlastního certifikátu a probíhá v posloupnosti operací:

a) Generování vlastní prvotní / následné žádosti o certifikát;

b) Odeslání vlastní žádosti protokolem SPOC do CVCA;

c) Přenos vydaného certifikátu na DV;

d) Import vlastního certifikátu;

e) Zálohování;

f) Zrušení pracovních klíčů (smazání starých již neplatných klíčů).

Správa klíčů dále vyžaduje implementaci těchto procesů:

a) Zálohování pracovních klíčů;

b) Obnovení pracovních klíčů ze zálohy;

c) Zrušení klíčů.

2.4 Požadavky na komunikaci a interoperabilitu

2.4.1 Komunikace s NIMS (P20)

NKA musí navazovat komunikaci s NIMS a jeho prostřednictvím podávat žádost a obdržet certifikáty DVCZE od CVCA. Dále musí prostřednictvím NIMS žádat o a získat certifikáty (řetězce certifikátů) a CRL tuzemské a zahraničních CSCA a zahraničních CVCA a DV. Tato komunikace bude probíhat on-line a musí být zabezpečena tak, aby mohlo být využito veřejné sítě. Lze doporučit použití rozhraní a protokolu SPOC nebo odvozeného.

Registrace DVCZE u CVCA musí proběhnout důvěryhodným, protokolárním způsobem, viz Certifikační politika CVCA [5]. Následné certifikáty je možno předávat elektronicky, v automatickém režimu. Certifikáty zahraničních entit budou rovněž předávány v automatickém režimu.

2.4.2 Komunikace s ISY (P21)

Komunikace NKA s ISY bude probíhat prostřednictvím datových sítí. Převážně se bude jednat o neveřejné sítě MV, nelze však vyloučit ani komunikaci prostřednictvím veřejných datových sítí. V době tvorby tohoto dokumentu nejsou ještě známy technické specifikace nebo jiná závazná doporučení pro tento druh komunikace. Dodavatel NKA musí technické podrobnosti komunikace navrhnout ve spolupráci s dodavateli ISY. Navržený způsob komunikace bude splňovat následující požadavky:

a) Komunikace mezi NKA a ISY probíhá zásadně šifrovaně. Pro vzájemnou identifikaci a navázání šifrovaného spojení je zřízena v rámci NKA certifikační autorita TechCA, které vydává v automatickém režimu serverové certifikáty pro KomSrv a registrované ISY (ISY v žádosti o certifikát uvádí svoje UID).

b) Komunikace mezi NKA a ISY probíhá předáváním zpráv. K tomu je využit protokol a rozhraní SPOC (viz [6]), modifikovaný doplněním nových typů zpráv pro potřeby této komunikace. Komunikaci protokolem a rozhraním SPOC realizuje na straně NKA komponenta KomSrv prostřednictvím web services (SOAP nad HTTPS).

c) Komunikace je zahajována vždy dotazem či požadavkem ze strany ISY. NKA nemá možnost iniciovat spojení s ISY.

V infrastruktuře PKI-EAC v ČR je uvažováno s následujícími typy a počty ISY:

2.4.2.1 Stacionární ISY (P22)

V současné době Policie ČR disponuje již vybudovaným jedním ISY. Toto ISY je vybudováno v rámci systému hraniční kontroly KODOX a jeho účelem je zabezpečit služby ISY pro všechny odbavovací stanoviště hraniční kontroly na Inspektorátech cizinecké policie umístěné na mezinárodních letištích v České republice Toto ISY je provozováno Ředitelstvím služby cizinecké policie.

Zátěž, kterou budou generovat stacionární ISY na DVCZE, nebude vysoká. Jejich počet bude nejvýše asi 100 kusů a jejich certifikáty ISY budou obnovovány typicky jednou týdně. Stejně tak zátěž na CertDB bude nízká, jelikož lze předpokládat, rovněž z důvodu udržení provozu v případě přerušení spojení mezi NKA a ISY, že řetězce certifikátů zahraničních entit budou uloženy v jejich paměti a jen čas od času synchronizovány s CertDB.

2.4.2.2 *Mobilní ISY on-line* (P23)

Použití mobilních ISY, které by pro každou operaci navazovaly bezdrátové spojení s NKA, je významně limitován možnostmi datového přenosu v radiové síti Pegas, která jako jediná je pro tento účel v ČR schválena. Z důvodu kapacitních omezení sítě nemohou tato zařízení, provozovaná v počtu desítek kusů, způsobit významnou zátěž DVCZE ani CertDB. Systém NKA však tuto funkcionalitu musí podporovat s ohledem na vývoj nových mobilních zařízení komunikující prostřednictvím GSM brány. GSM branou je myšlena komunikační brána na bázi technologie APN/VPN u Policie ČR.

Dodavatel z tohoto důvodů navrhne řešení propojení NKA a ISY dostupných prostřednictvím mobilních bezdrátových sítě (např. prostřednictvím APN, VPN).

NKA musí podporovat komunikaci s ISY prostřednictvím rozhraní HTTPS (TCP/IP), která bude použita při komunikaci s komunikační branou na bázi technologie APN/VPN. Zadavatel požaduje v rámci nabídky návrh na úrovni obecné technické architektury a následně dodávku řešení.

Rozhraní stávajících inspekčních systémů jsou realizovány v souladu se specifikací BSI TR-03129 a TR-03129-2 a podle této specifikace se také předpokládá komunikace mezi ISY a NKA. Podrobnější návrh komunikace je předmětem zadání této VZ a zadavatel předpokládá, že dodavatel navrhne přesný způsob komunikace ve spolupráci s dodavateli ISY.

Rozhraní všech stávajících mobilních ISY jsou realizována v souladu se specifikací TR-03129. Aktuálně všechna provozovaná mobilní ISY budou registrovány přímo v NKA bez realizované komunikace prostřednictvím TCC. TCC není předmětem této VZ.

Dodávka NKA musí obsahovat vybudování rozhraní HTTPS tak aby jakékoliv online ISY splňující specifikaci TR-03129 mohlo být využité. NKA musí mít vybudované rozhraní tak aby nebylo závislé na konkrétním operátorovi mobilní sítě. Počáteční počet mobilní ISY je cca 100 ks. NKA však musí být vybudováno tak aby garantovalo služby minimálně pro 10 000 mobilní ISY. Typy mobilních zařízení nejsou rozhodující, pro všechny budoucí mobilní ISY bude vyžadována komunikace dle specifikace TR 03129. Dodávka mobilního ISY není součástí této zakázky. Koordinaci součinnosti mezi dodavateli ISY a NKA bude provádět Zadavatel. Všichni zhotovitelé musí dodržet závazný rámec rozhraní dle citovaných specifikací

2.4.2.3 *Mobilní ISY off-line* (P24)

Jedná se o zařízení, která jsou vybavena vlastní pamětí, do níž lze uložit s určitou mírou zabezpečení jak certifikát ISY, tak i řetězce certifikátů zahraničních entit. Tato data je možno dávkově synchronizovat při připojení zařízení k interní síti MV, což nastává typicky třikrát denně. Vzhledem k charakteru zařízení, která jednak neumožňují uložení klíčů a certifikátů s tak dokonalým zabezpečením jako má HSM stacionárních zařízení, jednak existuje možnost jejich ztráty či zcizení, je nanejvýš vhodné vystavovat jim certifikáty ISY s minimální dobou platnosti cca 2-3 dny, přičemž k výměně by docházelo denně. Těchto zařízení je v současnosti v provozu do 100 ks. Cílový stav počtu registrovaných systémů může být až 10 000. Zadavatel vychází z předpokladu, že ne všechny ISY budou žádat o certifikáty v jeden čas. Zadavatel předpokládá, že bude aplikován adekvátní management odbavovacích požadavků. Tato četnost obnovy certifikátů, spolu s počtem zařízení, může generovat nárazově vysoké nároky na přenosovou kapacitu a odezvu DVCZE a CertDB.

Koordinaci součinnosti mezi dodavateli ISY a NKA bude provádět Zadavatel. Všichni zhotovitelé musí dodržet závazný rámec rozhraní dle citovaných specifikací

2.4.2.4 Ostatní

Na základě dosud dostupných informací lze očekávat, že další útvary PČR (dopravní policie, pořádková policie) a další orgány státní správy (Ministerstvo vnitra, Ministerstvo zahraničních věcí, Celní správa) budou budovat vlastní ISY. Tím se celkový počet ISY, obsluhovaných NKA, zhruba zdvojnásobí.

2.5 Požadavky na spolehlivost a výkon (P25)

Faktory ovlivňující spolehlivost:

a) Systém NKA bude budován na značkových komponentách se zakoupenou servisní podporou, která garantuje:

   a. dostupnost náhradních dílů,

   b. dostupnost servisní podpory s definovanou odezvou.

b) Použití zdrojů nepřerušitelného napájení;

c) Použití zálohovací páskové jednotky pro vytváření kopií.

Vzhledem k předpokladu vyšší nárazové zátěže systému musí být navrženy všechny subsystémy, tj. DVCZE, CertDB a KomSrv jako zdvojené (clustery), přičemž každá instance (včetně testovací) musí mít vlastní HSM modul

a

a) Oba uzly clusteru CertDB budou sdílet společné diskové pole, nebo

b) každý uzel clusteru CertDB bude mít vlastní disky nebo diskové pole a dodavatel vyřeší proces synchronizace obsahu databází obou uzlů.

2.6 Požadavky na role a procesy

Dodavatel NKA navrhne:

a) strukturu důvěryhodných rolí pro obsluhu NKA,

b) jejich náplň činnosti,

c) požadavky na slučitelnost a neslučitelnost rolí,

d) procesy vyžadující součinnost více rolí

Dále dodá odhad pracovního vytížení pro jednotlivé role.

2.7 Požadavky na dokumentaci

Dokumentace systému NKA, provozní i bezpečnostní, bude mít strukturu dle následujícího schéma.

Dodavatel NKA **vytvoří**:

a) Analytickou dokumentaci, tj.:

   a. Analýza technického řešení NKA;

   b. Analýza rizik;

c. Analýza bezpečnostních požadavků;

d. Bezpečnostní projekt;

e. Systémová bezpečnostní politika

f. Projekt technického řešení NKA;

b) Provozní dokumentaci, tj.

a. Systémová příručka;

b. Uživatelské příručky pro jednotlivé role;

c) Bezpečnostní dokumentaci, tj.

a. Směrnice pro technickou bezpečnost;

b. Směrnice pro netechnickou bezpečnost;

c. Směrnice pro reakci na incidenty;

d. Směrnice pro kontinuitu činností;

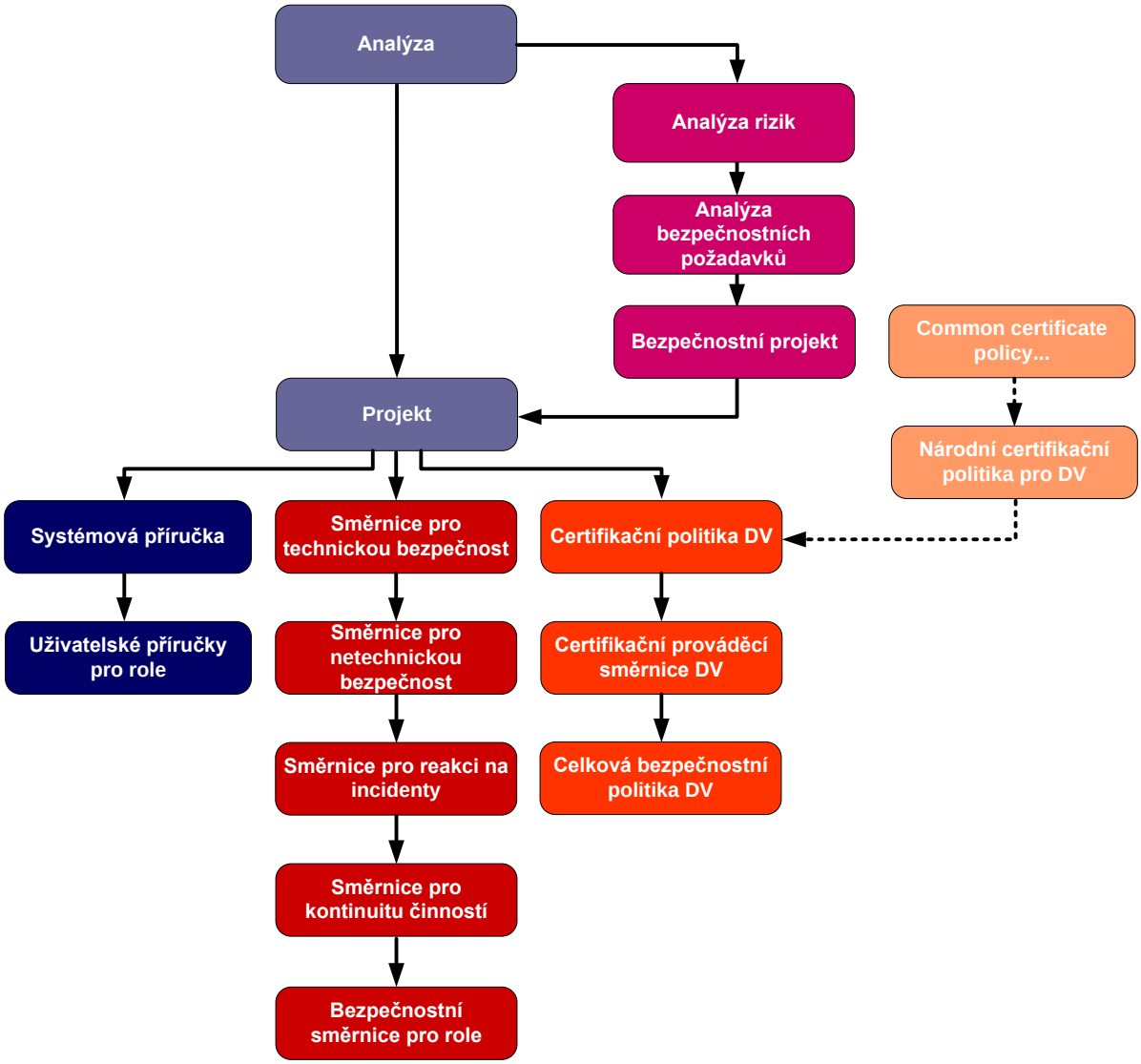
e. Bezpečnostní směrnice pro jednotlivé role.

Dokumentace NKA může být provedena jako samostatná nebo jako návrh revize existující dokumentace zadavatele.

Dodavatel **dále zajistí revizi a doplnění,** v souvislosti se zvoleným technickým řešením, těchto dokumentů

a. Certifikační prováděcí směrnice DVCZE;

b. Celkové bezpečnostní politiky DVCZE v souvislosti se zvoleným technickým řešením.



Obrázek 3: Povinná struktura provozní a bezpečnostní dokumentace

Pro případ, že by v budoucnu byl považován NKA za obecný (nikoliv policejní) informační systém veřejné správy ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy, je pro splnění požadavků tohoto zákona požadováno:

1. Systémová příručka popisuje způsob instalace, uvedení do provozu, pravidelné údržby a administrátorských úkonů na systému. Plní zároveň úlohu Systémové příručky ve smyslu zákona č. 365/2000 Sb., a vyhlášky č. 529/2006 Sb.
2. Uživatelské příručky pro jednotlivé role popisují provádění jednotlivých úkonů v běžném provozu NKA pracovníky v příslušných rolích. Pro každou roli je zpracována samostatná příručka. Plní zároveň úlohu Uživatelské příručky ve smyslu zákona č. 365/2000 Sb., a vyhlášky č. 529/2006 Sb.

2.8 Požadavky na certifikaci a akceptaci funkčnosti (P26)

Dodavatel poskytne podporu aktivit, které souvisí s registrací DVCZE u národní CVCA a zároveň u jedné zahraniční CVCA v součinnosti s národním PKI koordinátorem viz kap. 1.4.1 a 3.2 BSI TR-03139

V rámci nabídky bude uveden popis jednotlivých kroků. Zadavatel si vyhrazuje právo ověřit navržený postup.

Je-li součástí procedury provedení vybraných auditů nebo procesů ověření shody, jsou tyto aktivity součástí ceny dodávky dodavatele.

Dodavatel zajistí:

1. Certifikace a vydání Prohlášení o shodě Certifikační politiky DVCZE s CCP.
2. Součástí dodávky bude provedení certifikačního auditu dodaného řešení dle normy **ISO/IEC 27001**. Náklady na provedení auditu nese dodavatel NKA.
   a. Fyzické hranice pro certifikaci: Zadavatel předpokládá umístění hlavní a testovací instance NKA v budově PČR Bubenečská 20 a záložní instance v budově PČR Strojnická 27. Prostory pro administraci systému budou umístěny v objektu PČR Olšanská 2. Vše je definováno v kap. 2.1. Technicko-organizačního zadání. Přesné počty místnosti a jejich charakter budou určeny až na základě navrženého řešení uchazeče
   b. Zadavatel požaduje, aby certifikace zahrnovala všechny potřebné role navržené uchazečem. Uchazeč musí stanovit strukturu rolí, náplň jejich činnosti, a jiné. Zadavatel požaduje maximální úsporu počtu osob provádějící obsluhu NKA. Návrh počtu nutný zaměstnanců očekává zadavatel od uchazeče v nabídce.

3 Požadavek na dodávku IT infrastruktury

3.1 Serverová část (P27)

Jako součást dodávky dodavatel navrhne řešení nezbytné IT infrastruktury pro všechny komponenty NKA. Pro její návrh je závazné umístění jednotlivých instancí NKA v konkrétních lokalitách:

a) **Hlavní instance** - objekt PČR - Bubenečská 20, Praha. Prostory OIPIT PP ČR

b) **Záložní instance** - objekt PČR - Strojnická 27, Praha. Prostory OIPIT PP ČR

c) **Testovací instance** - objekt PČR - Dr. Bubenečská 20. Praha. Prostory OIPIT PP ČR.

Tato kapitola zadávací dokumentace definuje požadavky na dodávky IT infrastruktury nezbytné pro zajištění provozu systému na serverové úrovni potřebného hardware, software a konektivity LAN.

Parametry jednotlivých technických prostředků jsou definovány jako minimální a jejich naplnění v rámci dodávky je povinné.

Policie ČR běžně používá síťové spojení oddělené od internetu (vnitřní síť) s přenosovou kapacitou nejméně 1Gb. Pro aplikaci je množné vytvořit VPN, nicméně zabezpečení komunikace je třeba řešit i na aplikační úrovni a jeho návrh se očekává od uchazeče.

PČR dále v této lokalitě disponuje dedikovanými optickými trasami, které je také možné využít. Zadavatel je schopen poskytnout buď několik vyhrazených vlnových délek (to pak vyžaduje speciální DWDM transceivery v připojovaném systému) anebo je možné DWDM zařízení osadit příslušnými transpondéry. Tyto optickými zařízení by musela být součástí ceny projektu NKA

Hardwarová podpora provozu spočívá v požadavku Zadavatele na dodávku dvou racků do dvou geograficky oddělených lokalit (serveroven) zákazníka. Lokalita 1 je produkční. Lokalita 2 slouží jako záložní. V racku v lokalitě 1 budou umístěny dva produkční servery včetně zálohovacího média. V lokalitě 2 bude umístěn záložní server. Záložní HW bude veden formou horké zálohy. Zálohování dat, operačního systému a aplikace je požadováno na páskovou mechaniku LTO. Provedení zálohy požadujeme konzistentním způsobem pro databáze, operační systémy a aplikace. Zadavatel požaduje zálohování pouze v lokalitě1., tedy zálohovat produkční systém. Pro lokalitu č. 2 není zálohování požadováno. Vzhledem k možnosti snížení ceny software doporučujeme využití free a open source software u databází a operačních systémů např. na bázi produktů LINUX, (předpoklad Linux Postgre) OS (předpoklad CentOS v6.5 nebo vyšší). Předpokládaný objem dat není objemově významný a z těchto důvodů se nepředpokládá použití diskových polí. Servery budou dodány včetně OS, ethernet switchů, kabeláže, datového rozvaděče s vnitřním vybavením, dopravou a instalací do serverových místností zadavatele a to vše s bezplatnou zárukou na zařízení min. 24 měsíců a podporou na zařízení a aplikace min.24 měsíců. HSM musí podporovat všechny požadované kryptografické algoritmy EAC.

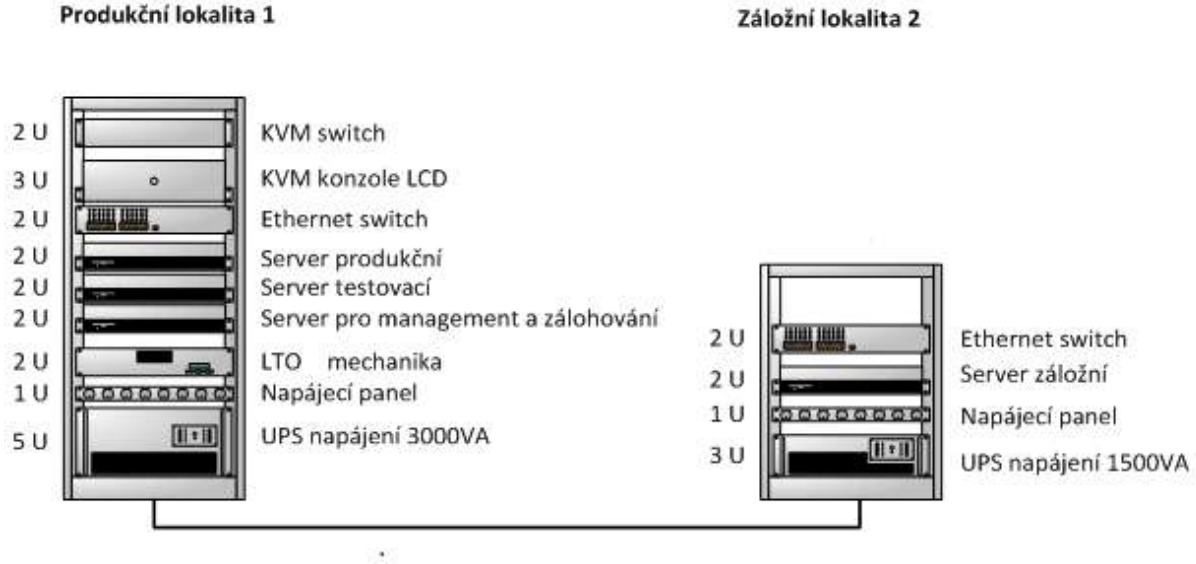
Virtualizace a přepínání mezi lokalitami. Aby bylo možno zajistit dostupnost dat ze záložní lokality v případě výpadku produkčního serveru při zachování konzistence dat,

požadujeme použití softwarové virtualizace a softwarové přepínání mezi serverem produkčním a záložním. Virtualizaci požadujeme na úrovni virtuálního stroje nebo formou hypervisoru nad fyzickým serverem a server pro správu virtualizace. Požadovanými funkcemi pro zajištění dostupnosti dat z lokalit jsou snapshoty, klony a synchronní replikace již na dvounodovém řešení. Připojení uživatele k záložnímu serveru po výpadku produkční lokality je doporučeno pomocí softwarových nástrojů, například použitím softwarového arbiteru. Z důvodu již investovaných prostředků do školení pracovníků zadavatele v oblasti správy produktů společnosti VMware a snížení ceny pro virtualizaci, doporučujeme použití řešení na bázi VMware vSphere Essential Plus nebo podobné.

Zadavatel předpokládá využití pouze interních mechanismů virtualizační platformy, nicméně Zadavatel připouští asynchronní replikace dat s maximálním definovaným od RPO 15 min.

Předmětem dodávky musí být plně funkční, nový, nepoužitý hardware včetně propojovací kabeláže a připojení do LAN zadavatele. Součástí dodávky musí být i dokumentace k zařízení, manuály, prohlášení o shodě.

Příklad obsazení technologii v jednotlivých lokalitách:



Příklad minimálního požadavku na vybavení lokalit:

Lokalita 1

1ks Rack stojanový pro produkční prostředí včetně vybavení o rozměrech (š)600 x (h)1200 x (v) min. 21U
1ks Produkční server (ostrý server s PCI + HSM), výška 2U)
1ks Testovací server (server s PCI + HSM, výška max. 2U)
1ks Management server pro administraci a zálohování (výška max. 2U)
1ks 24x 1 Gb Ethernet switch x 2x 10Gb porty
3ks Operační systém (např. Linux CentOS v6.5, nebo dle návrhu dodavatele. Licence OS musí být součástí dodávky)
2ks Databáze (dle návrhu dodavatele. Licence OS musí být součástí dodávky)
1ks Vmware Essential Plus
1ks KVM konzole

1ks KVM switch (včetně příslušenství a kabelů)
1ks Zálohovací zařízení – pásková knihovna LTO včetně zálohovacího software
1ks Záložní napájení - UPS 3000 VA
1ks Kompletní kabeláž
1ks Doprava
1ks Instalace,
1ks Zajištění konektivity k místní LAN

Lokalita 2 – záložní
Záložní HW bude veden formou horké zálohy

1ks Rack pro záložní včetně vybavení o rozměrech (š)600 x (h)1200 x (v) 15U
1ks 2U server záložní (geografický cluster s PCI + HSM)
1ks 24x 1 Gb Ethernet switch x 2x 10Gb porty
1ks Operační systém (např. Linux CentOS v6.5, nebo dle návrhu dodavatele. Licence OS musí být součástí dodávky)
1ks Databáze (např. SQL nebo dle návrhu dodavatele. Licence OS musí být součástí dodávky)
1ks UPS 1500 VA
1ks Kompletní kabeláž
1ks Doprava
1ks Instalace
1ks Zajištění konektivity k místní LAN (zjistit u IT k jakému switchi LAN je možno se připojit)

Minimální požadavky na RACK

- Svařovaný ocelový rozvaděč s odnímatelnými bočnicemi a zadním krytem, IP20
- Rozměry (š)600 x (h)1200 x (v)27U lokalita 1
- Rozměry (š)600 x (h)1200 x (v)15U lokalita 2
- Bezpečnostní kalené sklo tloušťky min 4 mm
- Univerzální rozvaděč pro datové a telekomunikační účely a s dostatečnou nosností pro požadované vybavení a vystrojení.
- Svařovaná konstrukce
- Flexibilní otevírání dveří pod úhlem min 170°
- Dveře demontovatelné s možností přemístění a otvírání na opačnou stranu
- Otvírání na kliku
- Uzamykatelný rack
- Nastavitelné vertikální lišty 19“ vertikální lišty s možností plynulého nastavení v libovolné hloubce rozvaděče pro snadnou organizaci a montáž propojovacích kabelů.
- Odnímatelné bočnice a zadní kryt se zámkovým uchycením a jednotným klíčem

- Vylamovací záslepky pro kabelové vstupy v zadní části rozvaděče proti pronikání prachu
- Ventilační jednotka musí být součástí vybavení racku
- Zemnění všech oddělitelných částí a vzájemné propojení dle příslušných norem
- Vybavení k montáži (matice, šrouby, záslepky, klíče, kryty, vodící lišty…)

Minimální požadavky na servery

- Počet serverů činí celkem 4ks

Z těchto čtyř kusů serverů budou tři servery umístěny v produkční/hlavní lokalitě 1 a jeden server jako záloha v lokalitě 2 takto:

Lokalita 1:

1. Produkční server
2. Testovací server
3. Management server – bude obsahovat zálohovací management software a softwarový „arbiter“, pro zajištění zálohování a přepínání dostupnosti serverů při výpadku.

Lokalita 2:

4. Záložní server

- Rackmount bude součástí dodávky
- Výška jednoho serveru – maximálně 2U
- Minimální počet CPU patic 2ks
- Minimální počet osazených patic 2ks
- Minimální počet jader – 6 jader
- Výkon v testu SPEC CFP2006 rates Result Published by SPEC – minimálně 380 bodů (požadovaný výkon musí splňovat minimálně procesor osazený v dodaném serveru)
- Paměti – minimálně 24x dostupných DIMM slotů s možností osazení až 768 GB
- Velikost osazené RAM – minimálně 128 GB pomocí registered 1333HHZ Low voltage DIMM modulu, pro Produkční, Záložní server, Management server, Testovací server
- RAM – minimálně 8 volných slotů pro pozdější rozšíření
- Napájecí zdroje s požadovaným příkonem, který zajistí i možnost dalšího rozšíření serverů

- Účinnost napájecích zdrojů – minimálně 92%
- Interní USB konektor
- Interní SD slot osazený 4GB kartou pro hypervisor
- Prediktivní analýza poruch minimálně pro RAM, CPU, napájecí zdroje a ventilátor
- Integrovaný informační panel LED/LCD s identifikací chybových hlášení CPU, RAM, zdrojů, ventilátorů
- Minimálně 3 dostupné PCI-e sloty s možností rozšíření na 6 PCI-e slotů
- Síťová karta – minimálně 4 portová, 1Gb, typ LOM (nezabírající místo v PCI-e slotech)
- Síťová karta – možnost upgrade na minimálně 2 portovou 10GB síťovou kartu typu LOM
- Síťová karta – 2 portová 10GB síťová karta s rozhraním SFP+
- HDD – minimálně 8 pozic pro osazení HDD s možností rozšíření na 16 SFF HDD nebo až 25 SFF HDD
- HDD - 8x HDD 600GB, 15k RPM SAS
- RAID – integrovaný HW RAID s podporou RAID 1/1/1+0 s možností rozšíření o 2GB cache včetně podpory RAID 5, 5+0, 6, 6+0, včetně read/write zálohované cache o velikosti min 512GB
- Podpora – minimálně 2 letá podpora 24 hodin, 7 dní v týdnu, se zaručenou dobou opravy do 6hod
- Integrovaný nezávislý procesor pro vzdálenou správu umožňující: vzdálené vypínání a zapínání serveru, plně integrovanou grafickou konzoly s možností sdílení více uživateli současně, připojení virtuálních médií (FDD, DVD, ISO i jejich image, USB klíče, adresář pro čtení), možnost záznamu a následného přehrání videozáznamu chybové obrazovky a následného restartu, podpora standardu SNMP/SSL/SSH/IPMI/ integrovaný nástroj pro instalaci operačního systému s možností automatické aktualizace od výrobce HW, integrovaný nástroj pro upgrade firmware s možností automatické aktualizace od výrobce HW, nástroj pro plnohodnotnou konfiguraci RAID řadiče v grafickém prostředí, integrované logování stavu server, včetně konfiguračních změn pro případné rychlé vyřešení chybových stavů.
- Požadujeme dodávku management software, který bude umožňovat minimálně centrální sledování stavu více serverů, nástroj pro deployment OS a SW včetně podpory bootování, nástroj na migraci instalovaného serveru mezi fyzickým a virtuálním prostředím, monitorování logování zátěže jednotlivých serverových komponent (CPU, RAM, HDD, LAN atd.) pro fyzické i virtuální servery s podporou Windows a Linux, integraci správy serverů do nástrojů pro správu virtualizačních řešení Microsoft System Center a VMware vCenter, centrální sledování spotřeby serveru.

Minimální požadavky na Ethernet switch

Počet kusů Ethernet switchů bude činit minimálně 2ks. Ethernetové switche musí zajišťovat 1Gb konektivitu ke všem serverům. Každý ethernet switch bude vybaven 24x 1Gbit porty a musí mít minimálně 2x 10Gb XFP externí porty. Rozhraní SFP+ pro 10-Gbit je přípustné. Podmínkou umožnění dodávky je, že veškerý dodávaný hardware bude nový a nepoužitý.

Požadavky na výkon:

Přenosová rychlost	8,8 Gbit/s
Forwarding rate	6.6Mpps
Plně duplexní režim	Ano
Typ přepínače	managed
	Switch layer L3 (Pro L3 funkcionalitu switchů je dostačující manuální konfigurace routování pro IPv4 a IPv6 a podpora služeb ARP a DHCP
Správa protokolů	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP
Přepínací protokol	Ethernet
Protokol datového spoje	Ethernet, Fast Ethernet, Gigabit Ethernet
Podporované síťové prot.	IEEE 802.1D (STP), IEEE 802.1p QoS, IEEE 802.1Q VLANs / VLAN, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.3 Ethernet, IEEE 802.3ad, IEEE 802.3ae 10-Gigabit Ethernet IEEE 802.3i 10BASE-T IEEE 802.3u Fast Ethernet IEEE 802.3x Flow control IEEE 802.3z Gigabit Ethernet 1000BASE-X.
Počet portů	24
Porty	20 x 10BASE-T/100BASE-TX/1000BASE-T (MDI/MDIX), 4 x Gigabit (1000BASE-T / SFP),

	2 x 10-Gigabit XENPAK(XFP).
Konektor	RJ-45

Minimální požadavky na KVM konzole

1ks KVM konzole musí umožňovat montáž do 19“ racku a musí být dodána jako jeden kus obsahující zobrazovací jednotky (LCD panel preferován), klávesnice a polohovacího zařízeni (myš nebo touchpad). KVM konzole ve složeném stavu nesmí přesáhnout 2U.

Minimální požadavky na KVM switch (včetně příslušenství)

1 ks KVM switch do 19“ racku musí umožňovat současné připojení až 4 ks serverů a možností přepínání mezi nimi. KVM switch může být integrován do KVM konzole.

Minimální požadavky na Zálohovací zařízení

- 1ks Páskové zálohovací zařízení LTO 5 (knihovna)
- Min počet založených pásek 10 (9 produkčních a jedna čistící)
- min. SCSI rozhraní, možné i s SAS konektivitou
- Provedení – rackové
- Kapacita min. 1TB přirozená / 2 TB komprimovaná
- Podpora pásek LTO 5
- Standard záznamu LTO 5
- Přenosová rychlost přirozená min 130 MBps (min 250GBph)
- Průměrný čas hledání záznamu, max. 70 sec
- Velikost rezervy 128 MB
- Zálohovací software
- Zálohovací mechanika musí být připojena k serveru se zálohovacím software
- Operační systém – Windows Server 2012 R2, Postgre SQL
- Záruka 2 roky

Minimální požadavky na Záložní napájení - UPS 3000 VA

1 ks UPS racková 19“ je požadována s kapacitou minimálně 3000 VA.

1 ks UPS racková 19“ je požadována s kapacitou minimálně 1500 VA.

3.2 Požadavky vybavení pracovišť (P28)

Jako součást NKA dodavatel dodá koncové stanice a sestavu testovacího inspekčního systému s dalším vybavením. Všechny níže uvedené komponenty budou umístěny a

instalovány ve vybraných prostorách Ředitelství služby cizinecké policie, Olšanská 2, Praha 3.

3.2.1 Minimální požadavky na stacionární administrátorské stanice NKA

Dodavatel dodá 4 kusy administrátorských stanic v minimálním požadovaném provedení:

- Minimální parametry procesor PassMark CPU min 9000, (http://www.cpubenchmark.net)
- RAM 16GB DD3,
- Grafická karta - min rozlišení 1920X1200/85Hz, podpora DirectX10,2 X DVI výstup – slotové provedení samostatné výstupy na min. dva monitory,
- HDD 2000GB 7.2k,
- mechanika DVD-RW,
- klávesnice, myš – bezdrátové,
- Windows 7 Pro 64-bit (včetně medií)
- Dvakrát monitor - LCD monitor LED 24", 16:10, 1000:1, 300cd/m2, 5ms, 1920x1200 FullHD, TCO,
- Síťová karta - integrovaná, 10/100/1000 Mbps, konektivita 1 RJ45
- DVI, DisplayPort, 6 X USB Hub, min 2 USB z přední strany PC skříně,
- Reproduktory 2.0, min výkon 2 X 5W,
- Celostránková čtečka dokladů
  - Rozměry snímací plochy: pro doklady konformní v souladu se specifikací ICAO 9303 - ve formátu ID1, ID2 a ID3., antireflexní úprava snímací plochy (např. anti-glare), min 120X85 mm, odolná proti poškrábání
  - Rozlišení: min 400 dpi
  - Hloubka barev:true-color 24 bit
  - Komunikace s PC: USB 2.0
  - Dekódování strojově čitelné zóny dokladů vydaných dle normy ISO/IEC 7501-1 a ICAO 9303 (ID-1, ID 2, ID 3)
  - Dekódování čárových kódů (1D, 2D) vytištěných na papíře nebo zobrazené na displeji mobilního telefonu
  - RFID doklady dle normy ISO 14443 (A/B), ISO 7816, ICAO 9303, PKI 1.1
  - Detekce čipu v jakékoliv části dokladu
  - Čtečka musí být podporovány OS s tím, kterým bude dodána stanice a dále Windows 7 a novější
- kancelářský balík MS Office Profesional (v posledních verzích
- SW pro expertní elektronickou kontrolu dokladu, kde požadované vlastnosti jsou uvedeny v kapitole ***3.2.4.1 Konfigurace lokálního ISY***
- Zařízení pro identifikaci a autentizaci oprávněných uživatelů, je-li dle návrhu uchazeče nutný (např. čtečka čipových karet)

3.2.2 Minimální požadavky na testovací stanici NKA

Dodavatel dodá jeden kus pracovní stanice pro testovací provoz v minimálním požadovaném provedení:

- Minimální parametry procesor PassMark CPU min 9000, (http://www.cpubenchmark.net)
- RAM 16GB DD3,
- Grafická karta - min rozlišení 1920X1200/85Hz, podpora DirectX10,2 X DVI výstup - slotové provedení,
- HDD 2000GB 7.2k,
- mechanika DVD-RW,
- klávesnice, myš - bezdrátové
- Windows 7 Pro 64-bit (včetně medií)
- Monitor - LCD monitor LED 24", 16:10, 1000:1, 300cd/m2, 8ms, 1920x1200 FullHD, TCO,
- Síťová karta- integrovaná, 10/100/1000 Mbps, konektivita 1 RJ45
- DVI, DisplayPort, 6 X USB Hub
- Celostránková čtečka dokladů
  - Rozměry snímací plochy: pro doklady konformní v souladu se specifikací ICAO 9303 - ve formátu ID1, ID2 a ID3., antireflexní úprava snímací plochy (např. anti-glare), min 120X85 mm, odolná proti poškrábání
  - Rozlišení: min 400 dpi
  - Hloubka barev:true-color 24 bit
  - Komunikace s PC: USB 2.0
  - Dekódování strojově čitelné zóny dokladů vydaných dle normy ISO/IEC 7501-1 a ICAO 9303 (ID-1, ID 2, ID 3)
  - Dekódování čárových kódů (1D, 2D) vytištěných na papíře nebo zobrazené na displeji mobilního telefonu
  - RFID doklady dle normy ISO 14443 (A/B), ISO 7816, ICAO 9303, PKI 1.1
  - Detekce čipu v jakékoliv části dokladu
    - Čtečka musí být podporovány OS s tím, kterým bude dodána stanice a dále Windows 7 a novější
- kancelářský balík MS Office Professional (v posledních verzích)
- SW pro expertní elektronickou kontrolu dokladu, kde požadované vlastnosti jsou uvedeny v kapitole ***3.2.4.1 Konfigurace lokálního ISY***
- Zařízení pro identifikaci a autentizaci oprávněných uživatelů je-li dle návrhu uchazeče nutný (např. čtečka čipových karet)

3.2.3 Minimální požadavky na přenosnou stanici ve formě notebooku

Dodavatel dodá 4 kusy přenosné stanice ve formě notebooku v minimálním požadovaném provedení:

- Úhlopříčka displeje 13,3“ až 14“
- Rozlišení displeje min 1920x1080 FHD
- Typ procesoru Intel Core i7 min řada Broadwell
- Operační paměť RAM min 16GB DDR3
- Harddisk typu SSD min 500GB
- Minimálně tři USB 3.0 porty
- Integrovaná čtečka identifikačních karet SmartCard
- Integrovaný TPM čip
- Integrovaný modem pro 3G sítě
- Maximální hmotnost notebooku 1,5 kg
- Minimální udávaná výdrž baterie min 10 hodin
- Operační systém min Windows 7 Professional 64b
- kancelářský balík MS Office Professional (v posledních verzích)
- Bezdrátová myš s laserovým snímačem
- USB Token – hardwarový klíč do USB portu
- Odpovídající brašna pro přenášení
- Externí USB DVD mechanika
- Polarizační folie na displej

3.2.4 Minimální požadavky na testovací inspekční systém (TEST ISY)

S ohledem na rozsah a konfiguraci inspekčních systémů v prostředí Policie ČR požaduje zadavatel dodat testovací instanci centralizovaného řešení ISY a zároveň lokálního řešení v podobě aplikace instalované na úrovni testovací stanice, ze které pro účely testování bude přístupný rovněž centralizovaný systém.

3.2.4.1 Konfigurace lokálního ISY

Dodavatel dodá jeden kus pracovní stanice s uvedenými periférierniemi jako testovací inspekční systém v minimálním požadovaném provedení:

- Minimální parametry procesor PassMark CPU min 9000, (http://www.cpubenchmark.net)
- RAM 16GB DD3,
- Grafická karta - min rozlišení 1920X1200/85Hz, podpora DirectX10,2 X DVI výstup, slotové provedení,
- HDD 1000GB 7.2k,

- mechanika DVD-RW,
- klávesnice, myš - bezdrátové
- Monitor - LCD monitor LED 24", 16:10, 1000:1, 300cd/m2, 8ms, 1920x1200 FullHD, TCO,
- Síťová karta- integrovaná, 10/100/1000 Mbps, konektivita 1 RJ45
- DVI, DisplayPort, 6 X USB Hub
- kancelářský balík MS Office Profesional
- Celostránková čtečka dokladů
  - Rozměry snímací plochy: pro doklady konformní v souladu se specifikací ICAO 9303 - ve formátu ID1, ID2 a ID3., antireflexní úprava snímací plochy (např. anti-glare), min 120X85 mm, odolná proti poškrábání
  - Rozlišení: min 400 dpi
  - Hloubka barev:true-color 24 bit
  - Komunikace s PC: USB 2.0
  - Dekódování strojově čitelné zóny dokladů vydaných dle normy ISO/IEC 7501-1 a ICAO 9303 (ID-1, ID 2, ID 3)
  - Dekódování čárových kódů (1D, 2D) vytištěných na papíře nebo zobrazené na displeji mobilního telefonu
  - RFID doklady dle normy ISO 14443 (A/B), ISO 7816, ICAO 9303, PKI 1.1
  - Detekce čipu v jakékoliv části dokladu
- Čtečka musí být podporovány minimálně tím OS, který bude dodán na testovací ISY Čtyřprstá čtečka otisků prsů
  - Komunikace s PC:USB 2.0
  - Snímání otisku prstů v rozlišení min 500ppi
  - Vysoká rychlost snímání (min 15 fps)
  - Ochrana proti vodě a prachu
  - Čtečka musí být podporována minimálně tím OS, který bude dodán na testovací ISY Funkce snímání otisků Auto capture, FlexFlats, FlexRolls
- SW pro testovací ISY, který umožní scénář funkcionality v podobě lokálního ISY a zároveň nastavení role jako klienta centralizovaného ISY (v normách označovaného jako TCC), kde základní povinné požadavky jsou:

  <u>Vymezení základní funkcionality</u>

  Provedení všech bezpečnostních procedur a protokolů implementovaných pro:

  - E-PAS – elektronický cestovní pas,
  - E-PKP – elektronické povolení k pobytu,
  - E-OP – elektronický občanský průkaz,

  Podpora bezpečnostních protokolů:

  - Definovaných podle ICAO – BAC, PA, AA

- Specifikace BSI – EAC 1.11 + EAC 2.1 včetně PACE, CA a TA při napojení na testovací ISY (TCC).

Práce s certifikáty a klíči:

- CV-certifikáty a sestavení řetězce z CVCA/CVCA-Link-/DV/IS certifikátů s využitím privátního klíče
- X.509-certifikáty & sestavení řetězce z CSCA/DS certifikátů
- Práce s CRL (Certificate Revocation Lists for X.509-certificates) v tomto případě budou veškeré krypto-operace realizovány lokálně.

Logování výsledků až na úroveň jednotlivých APDU příkazů s možností následného exportu do XML.

Podpora prostředků pro čtení osobních a cestovních dokladů

Vzhledem k tomu, že zadavatel disponuje řadou čteček elektronických cestovních dokladů, požaduje, aby dodaný SW podporoval práci s následujícím typem čteček:

- 3M AT9000

Podpora práce s biometrickými prvky

Aplikace musí být dodána s biometrickým software, který umožňuje:

- pořídit aktuální biometrický obraz otisku prstu nebo obličeje a to formou:
- auto enroll – automatické nabrání včetně aplikace algoritmu pro ověření kvality,
- manuální pořízení – obraz bude pořízen manuálně na základě rozhodnutí operátora.
- pro otisky prstů platí podmínka možnosti snímání formou jednoho otisku prstu a pomocí procesu 442p – (levá ruka, pravá ruka a palce).
- během pořízení musí být zhodnocena kvalita snímaného otisku prstu nebo obličeje.
- po pořízení biometrických dat, musí být systém schopný zrealizovat porovnání těchto dat vůči datům vyčteným z DG2 nebo DG3 čipu elektronického cestovního dokladu.
- Stejně jako v případě čteček elektronických cestovních dokladů disponuje zadavatel sadou hardware pro pořízení otisku prstu, pro který požaduje podporu postavenou na rozhraní definovaném podle ISO/IEC 19784-1 BioAPI Biometric application programming interface. Zadavatel požaduje, aby dodaný SW podporoval práci i s následujícími čtečkami. Čtečky otisku prstu:
    - Cross Match Technologies – LSCAN 100
    - Cross Match Technologies – řada L SCA GUARDIAN
- Systém musí umožňovat pořízení fotografie
    - řada fotoaparátů řady Cannon PowerSHOT

3.2.4.2 Konfigurace centralizovaného řešení testovacího ISY

Centralizované řešení ISY (TCC) bude registrováno u testovací instance nadřízené řídící autority, kterou je NKA.

Testovací instance Národní kontrolní autority bude poskytovat služby pro testovací inspekční systémy, kde v této fázi implementace NKA se jedná o lokální testovací stanici.

Testovací instance centralizovaného ISY (TCC) musí být v souladu se specifikací BSI TR-03129 a TR-03129-2.

Pro účely testování centralizovaného ISY (TCC) bude sdílen HSM modul testovací instance NKA.

Testovací koncová aplikace musí být implementována v souladu se specifikací BSI-03105.

3.2.5 Multifunkční zařízení

Dodavatel dodá 2 multifunkční kancelářské zařízení (tiskárna, scanner, kopírka) v minimálním požadovaném provedení:

- Podpora formátu papíru min. A3
- Barevný laserový tisk
- Zatížení na min. denní tisk 200 listů, duplexní/oboustranný tisk
- automatické podávání dokumentů
- LAN,
- Samostatně stojící
- Rozlišení tisku min 1200X600 dpi
- Barevný scanner s automatickým podavačem dokumentů, min 1200 dpi
- Náhradní sada tonerů

3.2.6 Skartovací zařízení

Dodavatel dodá jedno skartovací zařízení v minimálním požadovaném provedení:

- Skartace CD
- Skartace min 10 listů (70 gramového papíru) najednou
- Křížový řez,
- Odolnost proti sponkám
- Obsah koše min 15 litrů

3.3 Požadovaná úroveň podpory na dodané technologie: (P29)

- Implementace, instalace
- Záruka na zařízení min 2 roky
- Podpora na zařízení min. 2 roky

Veškeré komponenty NKA (HW a SW) musí být dodány s plnou zárukou na dobu min 2 let ode dne protokolárního uvedení NKA do provozu. Záruka se vztahuje na konfiguraci, která byla zadavatelem od uchazeče předána do ostrého provozu.

Pro veškeré HW komponenty musí být zajištěna technická podpora na dobu minimálně dvou let, s ohledem na technickou udržitelnost systému, případně v době záruky musí uchazeč přijmout takové nápravné opatření, které nepovedou ke snížení výkonu a provozních parametrů NKA.

4 Požadavky na uživatelské rozhraní aplikace NKA *(P30)*

Správa aplikace NKA musí být v plně grafickém rozhraní. Všechny aktivity musejí být realizovány z jedné softwarové platformy, nejlépe webové rozhraní. Všechny základní části aplikace musejí být v českém jazyce. Aplikace musí být jednoduchá na ovládání (intuitivní) a maximalizovat uživatelský komfort (definování pracovních postupů), workflow. Uchazeč v rámci nabídky představí návrhy 3 obrazovek aplikace.

Systém musí umožnit identifikovat chybové stavy (události) a tyto přiřadit konkrétním rolím v uživatelském rozhraní, pro účely zabránění odhalení kritických informací neautorizovaným uživatelům. Notifikace musejí být doručeny s použitím různých komunikačních mechanismů.

5 Další požadavky a plnění

5.1 Požadavky na školení

Součástí dodávaného systému bude příprava a provedení školení 10 uživatelů a 5 administrátorů jednotlivých částí dodávaného systému.

Součástí přípravy školení bude vytvoření dokumentace pro účastníky jednotlivých školení. Veškerá školení budou provedena v dohodnutých termínech před zahájením testovacího provozu.

Dodavatel poskytne drobné pohoštění pro školené policisty (nápoje, občerstvení)

5.2 Prokázání referencí (P31)

Zadavatel požaduje jako prokázání kvalifikace dodavatele k plnění projektu poskytnutí následujících referencí:

1. Zadavatel požaduje prokázání realizace minimálně jedné dodávky komponenty DV v rámci EU. Reference bude potvrzena koncovým uživatelem s uvedením kontaktních údajů.

2. Reference alespoň z jednoho projektu, kde dodavatel v rámci procesu inspekce dokladu realizoval procedury definované v EAC 2.1.

5.3 Záruka (P32)

Zadavatel požaduje komplexní záruku na všechny dodané soubory po dobu min 24 měsíců od doby uvedení systému do provozu.

Dnem uvedením systému do provozu je myšleno jeho protokolární předání (akceptace) po odstranění všech vad a nedodělků.

5.4 Informační povinnost a publicita (P33)

Dodavatel vytvoří pro zadavatele fotobanku dostupnou na internetu, kde bude dodavatel průběžně ukládat fotografie o realizaci projektu ve formátu vhodném pro webovou prezentaci. Fotografická dokumentace projektu bude také provedena vždy po dokončení konkrétního milníku (viz. kap. 7). O dokončeném milníku dodavatel dále sepíše zprávu o její realizaci a to v českém a anglickém jazyce.

Po dodavateli se dále požaduje, poskytnou nezbytnou informační podporu a součinnost zadavateli při realizaci ostatních aktivit za účelem realizace publicity tohoto projektu (např. tvorba informační, tiskové konference), tvorby monitorovacích zpráv nebo ověření realizace na místě.

Všechny dokumenty a výstupy, které budou v rámci projektu realizovány, musí splňovat podmínky stanovené v Nařízení - Annex IV. – Information and Publicity Requirements,Communication and Design Manual), které jsou dostupné na webových stránkách www.eeagrants.com, www.norwaygrants.com.

6 Harmonogram projektu

Zadavatel garantuje, že uchazeči bude poskytnuta minimální lhůta 8 měsíců od podpisu smlouvy pro plnění zadání.

Termín ukončení projektu 30. 04. 2017 je nepřekročitelný.

7 Projektové řízení a organizace *(P34)*

Zadavatel požaduje po uchazeči jako součást nabídky zpracování obecného způsobu a metodiky projektového řízení, kterým se bude uchazeč v rámci implementace projektu řídit a postupovat, včetně přístupu k organizaci účastníků projektu.

Zadavatel požaduje zpracování a předložení návrhu, který bude obsahovat:

a) Organizace účastníků projektu
b) Popis implementace
c) Popis testování
d) Požadavky na součinnost zadavatele
e) Popis identifikace možných rizik a návrh jejich eliminace a vypořádání
f) Návrh postupu předání provozu provozovateli, popis součinnosti dodavatele v tomto procesu.

Zadavatel očekává návrh řešení, které:

a) bude obsahovat obecnou metodiku organizace projektu, včetně účinné kontroly a navržených opatření k zajištění cílů projektu;
b) bude obsahovat metodiku postupu odpovídající charakteru plnění zakázky;
c) bude obsahovat srozumitelně popsaný přístup k testům;
d) rozpracovaný průběh plnění této veřejné zakázky dle jednotlivých závazných projektových milníků;
e) bude vyžadovat nižší požadavky na součinnost zadavatele v průběhu plnění celého předmětu veřejné zakázky;
f) nabídne návrh konkrétních opatření a přístupů pro zajištění realizovatelnosti projektu (v termínech, kvalitě a za daných technických podmínek cílových prostředí).

Příklad:

Milník	Cíle milníku	Výstupy
1.) Rozpracování – systémový projekt	Nastavení řízení projektu, práce na všech úrovních – procesní, systémové, komunikační, klientské, bezpečnostní.	Plán projektu Analýza rizik Analýza systémového a integračního řešení
2.) Rozpracování – Technicko – implementační projekt	Návrhové práce na všech úrovních - procesní, systémové, komunikační, klientské, bezpečnostní.	Návrh infrastruktury Návrh systémového a integračního řešení Návrh bezpečnostního projektu
3.) Realizace technického řešení	Zajištění HW infrastruktury, zabezpečení infrastruktury u Zadavatele, instalační a konfigurační práce, příprava testování, dokumentace.	Instalace, konfigurace Plán testování Testování Dokumentace

4.) Nasazení a testovací provoz	Testovací provoz, oprava chyb a dolaďování všech procesů a aplikačního prostředí. Ověřování provozních parametrů. Zvýšená podpora uživatelů.	Vyhodnocení testovacích fází Akceptační testování Předání dokumentace

8 Použité reference

Legislativa ID	Zákon, regulace, dokument vždy v posledním znění
[1]	Společná pravidla pro vydáváni certifikátů pro infrastrukturu rozšířeného řízení přístupu pro cestovní pasy a cestovní doklady vydávané členskými státy EU (Rozhodnutí Komise K(2008) 8657)
[2]	Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1 - Version 2.10
[3]	Technical Guideline TR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents -Part 2 – Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI) - Version 2.10
[4]	Technical Guideline TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents Part 3 – Common Specifications
[5]	ICAO Doc 9303 Machine Readable Travel Documents, Part 1 Machine Readable Passports, Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability
[6]	Technical Guideline TR-03111 - Elliptic Curve Cryptography
[7]	Certifikační politika CVCA České republiky
[8]	ČSN 36 9791 Informační technologie – Protokol pro správu klíčů Národní ověřovací certifikační autority používaný SPOC
[9]	BSI TR-03139 COMMON CERTIFICATE POLICY FOR THE EXTENDED ACCESS CONTROL INFRASTRUCTURE FOR PASSPORTS AND TRAVEL DOCUMENTS ISSUED BY EU MEMBER STATES – Version 2.1 – 27.5.2013
[10]	Nařízení Rady (ES) č. 2252/2004
[11]	Rozhodnutí Komise K (2006) 2909
[12]	Rozhodnutí Komise K (2008) 8657
[13]	Nařízení Evropského parlamentu a Rady (ES) č. 562/2006
[14]	Zákon č. 329/1999 Sb., o cestovních dokladech
[15]	Zákon č. 197/2009 Sb., o certifikaci veřejných dokladů s biometrickými údaji
[16]	ISO/IEC 7816
[17]	Certifikační politika CVCA ČR
[18]	Nařízení Rady (ES) č. 380/2008
[19]	Rozhodnutí Komise C(2009) 7476
[20]	Zákon č. 325/1999 Sb., o azylu
[21]	Zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky
[22]	ČSN 36 9791
[23]	ICAO PKD Memorandum of Understanding
[24]	Usnesení o zavedení cestovního pasu jednotného typu (2004/C 245/01)
[25]	Nařízení Evropského parlamentu a Rady (ES) č. 444/2009

Legislativa ID	Zákon, regulace, dokument vždy v posledním znění
[26]	Zákon č. 28/1999 Sb., o občanských průkazech
[27]	Zákon č. 101/2002 Sb., o ochraně osobních údajů
[28]	Zákon č. 273/2008 Sb., o Policii České republiky
[29]	Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
[30]	Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
[31]	Zákon č. 121/2000 Sb., o právu autorském
[32]	FIPS PUB 140
[33]	ČSN ISO/IEC 15408
[34]	IETF RFC 3647
[35]	Rozhodnutí Komise K(2013) 6181, K(2011) 5499 (k pasům) a Rozhodnutí Komise K(2013) 6178 a K(2011) 5478 (k PKP)
[36]	ISO/IEC 27001 - Systém managementu bezpečnosti informací

9 Seznam pojmů a zkratek

Pojem / Zkratka	Plný text	Vysvětlení
BAC	Basic Access Control	Slouží k zabezpečení dat menší důležitosti, které lze jednoduše získat i jinými kanály než vyčtením z čipu pasu (např. fotografie).
CA	Certifikační autorita	Souhrn technických a organizačně-administrativních prostředků, které umožňují vystupovat jako poskytovatel certifikačních služeb
CP	Certifikační politika	Dokument specifikující postupy související s vydáváním certifikátů
CAR	Certificate Authority Reference	Identifikátor veřejného klíče CA, kterým je možno verifikovat certifikát
Certifikát		Elektronicky podepsaná datová zpráva, vydaná certifikační autoritou, která spojuje data pro ověřování elektronického podpisu nebo pro šifrování zprávy s identifikačními údaji osoby držitele certifikátu a stvrzuje ověření identity této osoby
Certifikát přístupu		Certifikát, umožňující přístup k biometrickým údajům o otiscích prstů rukou. Je vydán CVCA na žádost DV. Pojem je zaveden zákonem o certifikaci veřejných dokladů s biometrickými údaji (zákon č. 197/2009 Sb.)
CHR	Certificate Holder Reference	Identifikátor veřejného klíče držitele certifikátu, tedy klíče jenž je obsažen v certifikátu
CBP	Celková bezpečnostní politika	Položka dokumentační základny CA
CP	Certifikační politika	Položka dokumentační základny CA
CCP	Common certificate policy	Common certificate policy for the extended access control infrastructure for passports and travel documents issued by EU member states. Společná pravidla pro vydávání certifikátu pro infrastrukturu rozšířeného řízení přístupu pro cestovní pasy a cestovní doklady vydávané členskými státy EU
CDBP		Cestovní doklad s biometrickými prvky (strojově čitelný)
CIS	Cizinecký informační systém	Hlavní produkční systém SCP PČR.
CPS	Certifikační prováděcí směrnice	Položka dokumentační základny CA
CRL	Certificate Revocation List	Seznam zneplatněných certifikátů.

Pojem / Zkratka	Plný text	Vysvětlení
CSCA	Country Signing Certification Authority	Kořenová certifikační autorita v rámci národní infrastruktury pro vydávání e-cestovních dokladů.
CVC	Card Verifiable Certificate	Zjednodušený formát certifikátu, užívaný pro autentizaci čipových karet. Viz ISO/IEC 7816. Specifikace pro CDBP viz Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)
CVCA	Country Verification Certification Authority	Neveřejný poskytovatel certifikačních služeb pro potřeby systému elektronického pasu v České republice – pro potřeby terminálové autentizace.
Čipová karta		Nosič párových dat, prostředek pro vytváření elektronických podpisů a dešifrování zpráv a k autentizaci držitele
Data pro ověřování elektronického podpisu		Jedinečná data, která se používají pro ověřování elektronického podpisu, dále též uváděna jako veřejný klíč
Data pro vytváření elektronického podpisu		Jedinečná data, která se používají pro vytváření elektronického podpisu, dále též uváděna jako soukromý klíč
DBMS	Database Management System	Databázový systém. Obvykle je to program nebo soustava programů, které řídí vytváření, údržbu a užívání databáze. Tvoří mezivrstvu mezi aplikacemi a uloženými daty.
Držitel certifikátu		Klient CA vlastnící párová data, který požádal o vystavení certifikátu a certifikát mu byl vystaven
Důvěryhodný kurýr		Osoba, pověřená osobním doručením zásilky (např. předávací protokol a datový nosič) od Odesílatele k Příjemci. Identita Důvěryhodného kurýra je Odesílateli i Příjemci známá; Důvěryhodný kurýr požívá důvěry Odesílatele i Příjemce. Důvěryhodný kurýr garantuje autenticitu přenášených dat.
DS	Document Signer	Zařízení digitálně podepisující osobní data uložená v čipu dokladu
DV	Document Verifier	Kontrolní systém, kontrolní jednotka – subjekt, spravující inspekční systémy, přistupující k otiskům prstů. DV je klientem CVCA a sám představuje certifikační autoritu pro ISY, které spravuje.
DVCZE	Document Verifier České republiky	Neveřejná certifikační autorita pro potřeby kontroly a ověřování strojově čitelných veřejných dokladů s biometrickými prvky v České republice.
DVCZERA	Registrační autorita DVCZE	Orgán pověřený prováděním identifikačních a autentizačních procesů pro potřeby DVCZE
CVRA	Registrační autorita CVCA	Orgán pověřený prováděním identifikačních a autentizačních procesů pro potřeby CVCA.

Pojem / Zkratka	Plný text	Vysvětlení
EAC	Extended Access Control	Rozšířená kontrola přístupu; podle ICAO se jedná o kombinaci prokázání důvěryhodnosti čipu (CA) a terminálu (TA). Slouží k zabezpečení citlivých biometrických dat držitele pasu (např. otisk prstu)
EAL	Evaluation Assurance Level	Úroveň zajištění bezpečnosti. Viz ČSN 15408.
EK	Evropská komise	
Elektronický podpis		Údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě
EPS	Elektrická požární signalizace	
EU	Evropská unie	
HTTPS	Hypertext Transfer Protocol over SSL	HTTPS je nadstavba síťového protokolu HTTP, která umožňuje zabezpečit spojení mezi webovým prohlížečem a webovým serverem před odposloucháváním, podvržením dat a umožňuje též ověřit identitu protistrany.
HSM	Hardware Security Module	Česky obvykle „kryptografický modul“. Samostatně stojící nebo do počítače montované zařízení pro bezpečné uložení klíčů a provádění kryptografických operací.
CA	Chip Authentication	Slouží k ověření pravosti pasu a vytváří šifrovaný komunikační kanál mezi čipem pasu a inspekčním místem.
ICAO	International Civil Aviation Organization	Mezinárodní organizace pro civilní letectví.
ISY	Inspekční systém	Místo pro ověřování pravosti pasu, jeho autentizace a integrity a identifikace jeho držitele s využitím biometrických údajů (otisk prstu)
Klient CA		Subjekt využívající certifikačních služeb CA
Klientský certifikát		Certifikát vystavený klientu, který u CA požádal o vystavení certifikátu k vlastním párovým datům
Kontext důvěry		Vztah mezi DV a ISY, umožňující automatizované vydávání následných certifikátů.
MOBLUST		IS PČR pro kombinovanou online a offline lustraci – dotazy do centrálních registrů bezdrátovým spojením + vyhledávání v lokálních databázích na mobilním zařízení.
MRTD	Machine Readable Travel Document	Strojově čitelný cestovní doklad

Pojem / Zkratka	Plný text	Vysvětlení
MV	Ministerstvo vnitra České republiky	
Následný certifikát		Certifikát, který byl vydán držiteli v době platnosti již vydaného certifikátu, který má stejné údaje uvedené v tomto certifikátu a liší se v datech pro ověřování elektronického podpisu a sériovém čísle certifikátu
NCA	Národní certifikační autorita	Komplex certifikačních autorit (CSCA,CVCA,SPOCCA,SPOCCA) a komunikačního a databázového systému SPOC/NIMS provozovaný MV
SPOC/NIMS	Single Point of Contact/National ICAO Management System	Systém zabezpečující distribuci certifikátů na národní úrovni a podporu pro výměnu certifikátů a CRL mezi zúčastněnými státy (zabezpečení pasivní autentizace) rozšířený pro zabezpečení potřeb EAC především jako zprostředkovatel žádostí o certifikát u CVCA a odesílatel vydaných certifikátů.
NIST	National Institute of Standards and Technology	Standardizační organizace USA.
NKA	Národní kontrolní autorita	
OID	Object identification number	Jedinečný identifikátor objektu. Struktura OID se skládá z uzlů v hierarchicky přiřazeném jmenném prostoru. Formálně je definován v normě ITU-T ASN.1.
Oprávněná osoba		Osoba zastupující daný subjekt ve svěřené roli.
Organizační složky PČR		Organizační složky PČR dle aktuální organizační struktury PČR (např. CIAP)
OS		Operační systém
Párová data		Tvoří data pro vytváření elektronického podpisu a jim odpovídající data pro ověřování elektronického podpisu, nebo data pro šifrování datové zprávy a jim odpovídající data pro dešifrování datové zprávy. Párová data jsou tvořena dvojicí soukromého a veřejného klíče
PČR	Policie České republiky	
PIN	Personal Identification Number	Osobní identifikační číslo. Jedná se o identifikátor, pomocí kterého je možné se autorizovat např. u platební karty, mobilního telefonu, vstupních kódů apod.
PKI	Public Key Infrastructure	Infrastruktura veřejných klíčů
Předávací protokol		Textový dokument zabezpečující evidenci přenosu dat na datovém nosiči. Obsahuje identifikaci datového nosiče, kryptografický otisk zprávy a podpis osob zodpovědných za odeslání, distribuci a příjem zprávy mezi systémy

Pojem / Zkratka	Plný text	Vysvětlení
Soukromý klíč		Data pro vytváření elektronického podpisu nebo data pro dešifrování datové zprávy
RA	Registrační autorita	Registrační orgán
RIA	Regulatory Impact Assesment	Hodnocení dopadů vládních regulací na soukromý a veřejný sektor zahrnuje soustavu metod směřujících k systematickému hodnocení negativních a pozitivních dopadů navrhovaných či existujících právních předpisů v oblasti hospodářské, sociální a environmentální. Hodnoceny mohou být rovněž dopady na různé ekonomické a sociální skupiny. Podklady získané v rámci procesu hodnocení dopadů regulace slouží jako podklad pro politické rozhodování o přijetí či nepřijetí navrhované právní úpravy nebo přehodnocení/úpravu či zrušení stávající.
Root certifikát / kořenový certifikát		Certifikát vystavený CA pro svůj veřejný klíč, podepsaný odpovídajícím privátním klíčem (self-signed certifikát)
SCP	Služba cizinecké policie	Organizační složka Policie České republiky
SIS	Schengenský informační systém	Jeden z hlavních produkčních systémů PČR.
SLC	Smart Logon Card	Čipové karty, sloužící jako prostředek k identifikaci a autentizaci osob v prostředí se zvýšenými bezpečnostními nároky.
SOAP	Simple Object Access Protocol	Protokol pro výměnu zpráv přes síť. Formát SOAP tvoří základní vrstvu komunikace mezi webovými službami a poskytuje prostředí pro tvorbu složitější komunikace.
SPOC	Single Point of Contact	Entita odpovědná za odesílání a přijímání dat při operacích správy klíčů EAC-PKI mezi státy. Jediné rozhraní poskytnuté daným státem pro komunikaci EAC-PKI s cizími státy. Definováno v ČSN 36 9791.
TA	Terminal Authentication	Slouží k ověření oprávnění inspekčního místa k vyčtení citlivých dat držitele pasu.
TechCA		
UID	Unique Identifier	Jedinečný nezměnitelný identifikátor objektu ve formě řetězce alfanumerických znaků.
UPS	Uninterruptible Power Supply	Nepřerušitelný zdroj napájení elektrickým proudem.
Veřejný klíč		Data pro ověřování elektronického podpisu nebo data pro šifrování datové zprávy

Pojem / Zkratka	Plný text	Vysvětlení
VIS	Vízový informační systém	Jeden z hlavních produkčních systémů Ř SCP PČR.
Závislá strana		Klient CA spoléhající na využití certifikátu.
KODOX	Informační systém hraniční kontroly KODOX	Informační systém KODOX je hlavní produkční systém k podpoře provádění hraniční kontroly na vnějších hranicích České republiky. IS KODOX je provozovaný ŘSCP.

10 Tabulka naplnění požadavků projektu

Níže uvedená tabulka je pouze prvotní informací pro zadavatele, kde je jasně uvedeno, zda konkrétní specifické požadavky označené jako (Px) jsou naplněny. Detailní znění každého požadavku je vždy uvedeno v textu zadávací dokumentace a končí buď nově označeným požadavkem, nebo koncem konkrétní kapitoly.

U každého bodu požadavku bude jasně uvedeno, jakým způsobem je naplněn, případně bude uvedena reference do technické části zadávací dokumentace, kde bude popsán ve větší míře detailu.

Pozn:

Tabulka požadavků obsahuje pouze výpis zásadních kapitol zadávací dokumentace a slouží zejména Zadavateli k usnadnění zajištění splnění požadavků. Zadavatel v rámci hodnocení prostuduje a vyhodnotí celou nabídku.

ID požadavku	Popis požadavku	Naplněn Ano / Ne
P1	**Požadavek:** Registrační procedury **Popis způsobu naplnění:**	
P2	**Požadavek:** Žádost o certifikát DVCZE, import certifikátu DVCZE **Popis způsobu naplnění:**	
P3	**Požadavek:** Žádost o certifikát ISY, vydání certifikátu ISY **Popis způsobu naplnění:**	
P4	**Požadavek:** Doba platnosti certifikátů **Popis způsobu naplnění:**	
P5	**Požadavek:** Práce s řetězci certifikátů CVCA cizího státu **Popis způsobu naplnění:**	
P6	**Požadavek:** Implementace všech potřebných kryptografických algoritmů **Popis způsobu naplnění:**	
P7	**Požadavek:** Požadavky na uživatelské rozhraní	

ID požadavku	Popis požadavku	Naplněn Ano / Ne
	Popis způsobu naplnění:	
P8	**Požadavek:** Požadavky na nastavení a kontrolu času **Popis způsobu naplnění:**	
P9	**Požadavek:** Podpora pro více typů dokladů **Popis způsobu naplnění:**	
P10	**Požadavek:** Podpora více profilů certifikátů **Popis způsobu naplnění:**	
P11	**Požadavek:** Autentizace uživatelů **Popis způsobu naplnění:**	
P12	**Požadavek:** Auditní záznamy **Popis způsobu naplnění:**	
P13	**Požadavek:** Zálohování, obnova, replikace dat **Popis způsobu naplnění:**	
P14	**Požadavek:** Možnosti konfigurace **Popis způsobu naplnění:**	
P15	**Požadavek:** Volba kryptografického modulu pro uložení a manipulaci s klíči **Popis způsobu naplnění:**	
P16	**Požadavek:** Správa klíčů a kryptografická bezpečnost **Popis způsobu naplnění:**	
P17	**Požadavek:** Bezpečnost kryptografických klíčů **Popis způsobu naplnění:**	

ID požadavku	Popis požadavku	Naplněn Ano / Ne
P18	**Požadavek:** Správa ochranných klíčů **Popis způsobu naplnění:**	
P19	**Požadavek:** Správa pracovních klíčů DVCZE **Popis způsobu naplnění:**	
P20	**Požadavek:** Komunikace s NIMS **Popis způsobu naplnění:**	
P21	**Požadavek:** Komunikace s ISY **Popis způsobu naplnění:**	
P22	**Požadavek:** Stacionární ISY **Popis způsobu naplnění:**	
P23	**Požadavek:** Mobilní ISY on-line **Popis způsobu naplnění:**	
P24	**Požadavek:** Mobilní ISY off-line **Popis způsobu naplnění:**	
P25	**Požadavek:** Požadavky na spolehlivost a výkon **Popis způsobu naplnění:**	
P26	**Požadavek:** Požadavky na certifikaci a akceptaci funkčnosti. **Popis způsobu naplnění:**	
P27	**Požadavek:** Požadavek na dodávku IT infrastruktury - serverová část **Popis způsobu naplnění:**	

ID požadavku	Popis požadavku	Naplněn Ano / Ne
P28	**Požadavek:** Požadavky na pracovní stanice a testovací ISY **Popis způsobu naplnění:**	
P29	**Požadavek:** Požadovaná úroveň technické podpory na dodané technologie. **Popis způsobu naplnění:**	
P30	**Požadavek:** Požadavky na uživatelské rozhraní aplikace NKA **Popis způsobu naplnění:**	
P31	**Požadavek:** Prokázání referencí **Popis způsobu naplnění:**	
P32	**Požadavek:** Záruka **Popis způsobu naplnění:**	
P33	**Požadavek:** Informační povinnost a publicita **Popis způsobu naplnění:**	
P34	**Požadavek:** Projektové řízení, organizace a harmonogram projektu **Popis způsobu naplnění:**	