



Pomáhat a chránit

**Automatická evaluace dat PA pro ML tvořené
NKA**

Technické zadání

verze 1.00

Praha 2016

OBSAH

1	Úvod	3
2	Popis aktuálního stavu – výchozí podmínky	5
2.1	<i>Systém automatického odbavení cestujících EasyGO</i>	<i>5</i>
2.2	<i>Národní kontrolní autorita NKA</i>	<i>5</i>
2.3	<i>Systémy stacionární a mobilní kontroly</i>	<i>6</i>
3	Technické zadání.....	8
3.1	<i>Doplnění funkcí evaluačního modulu EasyGO aplikačního serveru.....</i>	<i>9</i>
3.2	<i>Realizace interface mezi systémem EasyGO a sub-modulem NKA – N-PKD</i>	<i>12</i>
3.3	<i>Doplnění serveru do infrastruktury systému EasyGO.....</i>	<i>13</i>
3.4	<i>Výčet dodávek uchazeče</i>	<i>14</i>

Seznam obrázků a schémat

Obrázek 1: Národní kontrolní autorita – rozsah implementace	6
---	---

1 Úvod

S ohledem na stále větší nároky na správu inspekčních systémů pro kontrolu elektronických cestovních dokladů a jejich interoperabilitu je nutné aplikovat rozšíření systému Národní kontrolní autority (dále jako NKA). Rozšířením je myšlena její intenzivnější integrace s aktuálními provozovanými inspekčními systémy na úrovni hraniční kontroly s cílem zapojení České republiky do aktivit Evropské unie a agentury Frontex v rámci vytváření tzv. Schengen Master Listu.

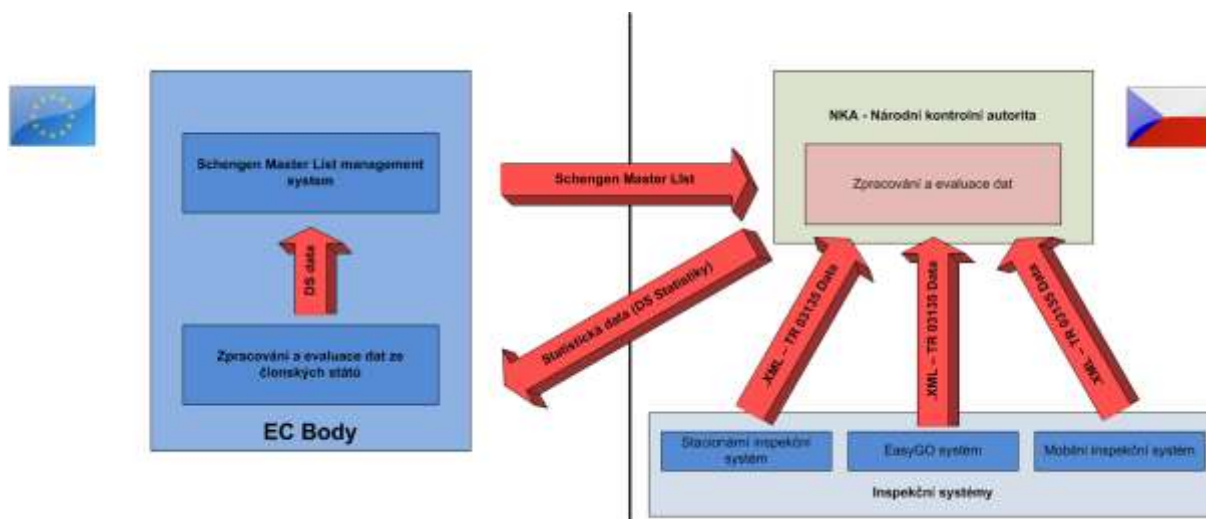
Schengenský Master List (SML) je připravován jako centrální řešení pro sdílení dat nezbytných pro provedení Pasivní Autentizace, pro který je nezbytná spolupráce všech států Evropské unie.

SML bude spravován Evropskou komisí, která pro jeho správu předpokládá úzkou spolupráci se všemi členy Evropské Unie a to zejména Schengenského prostoru.

Uvedená spolupráce je postavena na sdílení dat, které musí být předány v definovaném formátu a předpřipraveny pro jejich následné zpracování. Jedná se o data z každé inspekční procedury na úrovni elektronické hraniční kontroly (stacionární hraniční místa, automatický systém odbavení cestujících), která budou automaticky posunuta NKA, která provede následnou automatickou evaluaci dat a reporting vůči Evropské komise.

Pro naplnění výše uvedených cílů musí být data ze všech inspekcí poskytnuta ve formátu .XML jak je definován standardem TR-03135 pro další zhodnocení v systému NKA. Data neobsahují žádné osobní údaje. Jejich hlavní součástí jsou informace o Document Signer certifikátu, které jsou následně v požadovaném formátu zpracovány.

Systém NKA bude tedy doplněn o modul pro evaluaci a reportování včetně doplnění vybraných automatických pracovních postupů, v rámci nichž je řízen provoz NKA.



Po odeslání dat do modulu Národní kontrolní autority budou data připravena podle definovaného formátu a postoupena orgánu Evropské komise, který je určený vydávání Schengen Master Listu.

V momentě, kdy je vydán nový Schengen Master List, je tento postoupen všem členským státům, kde kontaktním bodem na národní úrovni ČR bude pracoviště Národní kontrolní autority, která jej bude distribuovat všem registrovaným inspekčním systémům.

Implementací výše uvedeného bude posílena role České republiky a zároveň její schopnost pro ještě vyšší schopnost kontroly elektronických cestovních dokladů.

Požadavek na realizaci projektu je definován následujícími soubory dodávek souvisejících s rozšířením funkcionality systému EasyGO a NKA:

- Doplnění funkcí evaluačního modulu EasyGO aplikačního serveru včetně migrace modulu Bioserver na nově dodaný server,
- Realizace interface mezi EasyGO aplikačním serverem a sub-modulem NKA – N-PKD,
- Implementace automatických pracovních postupů na úrovni NKA a zpracování logů z inspekčních systémů ve formátu BSI TR-03135

2 Popis aktuálního stavu – výchozí podmínky

Aktuální stav vychází z konfigurace již provozovaných systémů EasyGO, NKA a systémů mobilní/stacionární kontroly.

Systémy poskytující potřebná data pro účely požadované funkcionality jsou EasyGO a KODOX (stacionární a mobilní), kde jimi vytvořená data budou dále zpracována v sub-modulu NKA, kterým je N-PKD.

2.1 Systém automatického odbavení cestujících EasyGO

Systém EasyGO je provozován nad sedmnácti automatickými branami - eGATE, které jsou instalovány v prostoru hraniční kontroly na terminálu 1 na úrovni první kontrolní linie, kde 9 automatických bran je instalováno v lokalitě PŘÍLET a 8 automatických bran v lokalitě ODLET.

Provoz všech nových automatických bran (17) je realizován prostřednictvím terminálové klientské aplikace, která je nainstalována na Monitorovacích stanicích (M-STATION) umístěných v odbavovacích stanovištích policie v obou lokalitách. Všechny stanice na platformě PC ve formě terminálu komunikují s EasyGO APP Server jehož součástí je evaluační modul, který zpracovává tzv. transakční záznamy podle specifikace BSI TR-03135.

Veškeré kryptografické operace jsou realizovány komponentou EasyGO ISY (TCC), která je implementována zcela v souladu se specifikací BSI TR-03129 a BSI-03129-2.

Výrobce klíčových komponent v podobě automatické brány, aplikačního serveru EasyGO APP Server (včetně evaluačního modulu Bioserver) a inspekčního systému EasyGO ISY (architektura TCC) je společnost secunet Security Networks AG – Německo (www.secunet.com).

Uvedená společnost již byla zadavatelem kontaktována za účelem podání nabídky všem uchazečům.

2.2 Národní kontrolní autorita NKA

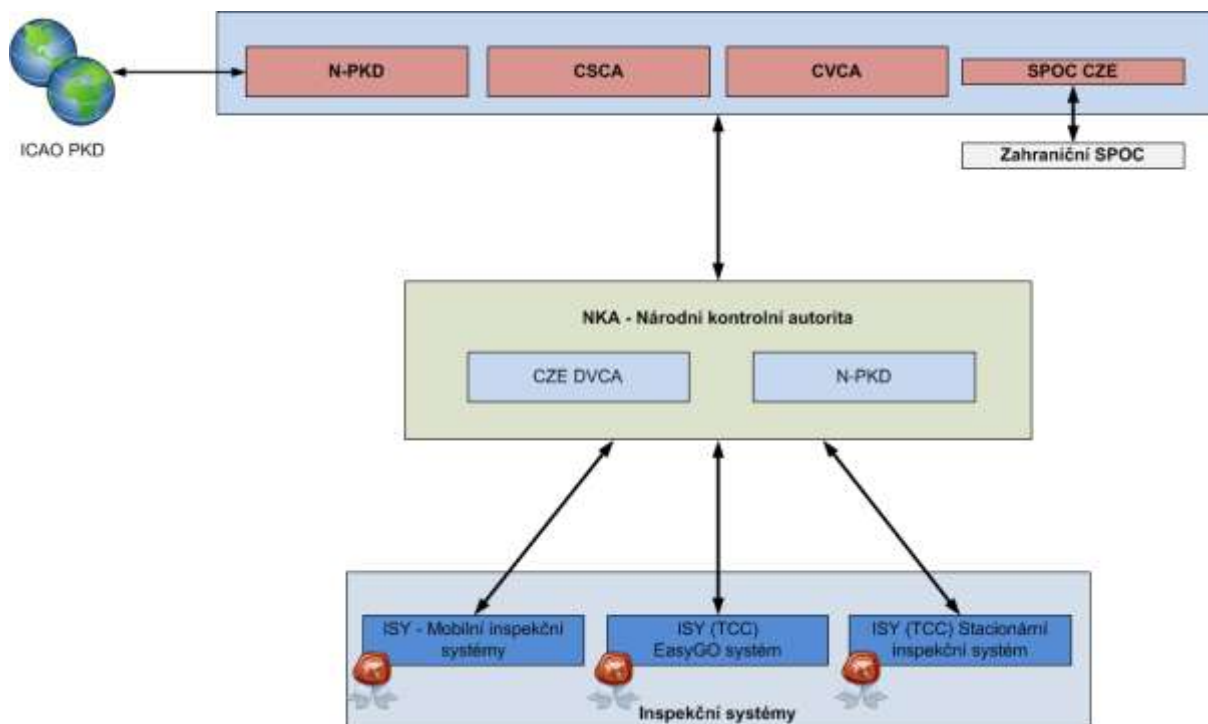
Národní kontrolní autorita – NKA (rovněž jako DVCA4) je řešení postavené na technologii komplexního systému poskytujícího PKI infrastrukturu pro kontrolu a vydávání elektronických cestovních a osobních dokladů COTS produktu secunet eID PKI Suite.

NKA komunikuje v prostředí České republiky prostřednictvím rozhraní SPOC_AUX s nadřízenými autoritami a následně i se zahraničními CVCA autoritami.

Jako taková poskytuje jak data pro řízení přístupu v rámci Terminálové autentizace, tak data pro provedení Pasivní autentizace na registrovaných inspekčních systémech (TCC, IS...)

NKA je provozována na třech instancích:

- Primární instance,
- Hot StandBy instance,
- Testovací prostředí včetně testovacího inspekčního systému v provedení TCC spolu s klientem postaveném na technologii referenčním řešením pro kontrolu a čtení eMRTD Golden Reader Tool (elektronických cestovních a osobních dokladů).



Obrázek 1: Národní kontrolní autorita – rozsah implementace

Specifickým modulem provozovaným v systému NKA je integrovaný modul **N-PKD**.

Tento modul realizuje v rámci provozu NKA následující procesy:

- Import certifikátů CSCA, DS a CRL,
- Správa importovaných certifikátů,
- Vytvoření Mater Listu a Defect Listu,
- Export dat Master a Defect listu,
- Podepsání Master Listu a Defect Listu certifikátem.

Současně N-PKD poskytuje funkcionalitu ve formě vytváření a správy Master a Defect listů, které jsou následně připraveny a distribuovány pro provedení Pasivní Autentizace v rámci kontrolních procesů elektronických cestovních a osobních dokladů distribuovány dále komponentou DVCA pro registrované inspekční systémy.

Výrobce softwarových komponent systému NKA jako komplexního řešení eID PKI Suite je společnost secunet Security Networks AG – Německo (www.secunet.com).

Uvedená společnost již byla zadavatelem kontaktována za účelem podání nabídky všem uchazečům.

2.3 Systémy stacionární a mobilní kontroly

Kromě výše uvedených systémů zadavatel provozuje stacionární a mobilní kontroly, které jsou obsluhovány při realizaci kontroly elektronického cestovního dokladu dedikovanými inspekčními systémy podle standardu BSI TR-03135.

Tyto inspekční systémy poskytují možnost vytváření transakčních záznamu podle standardu TR-03135.

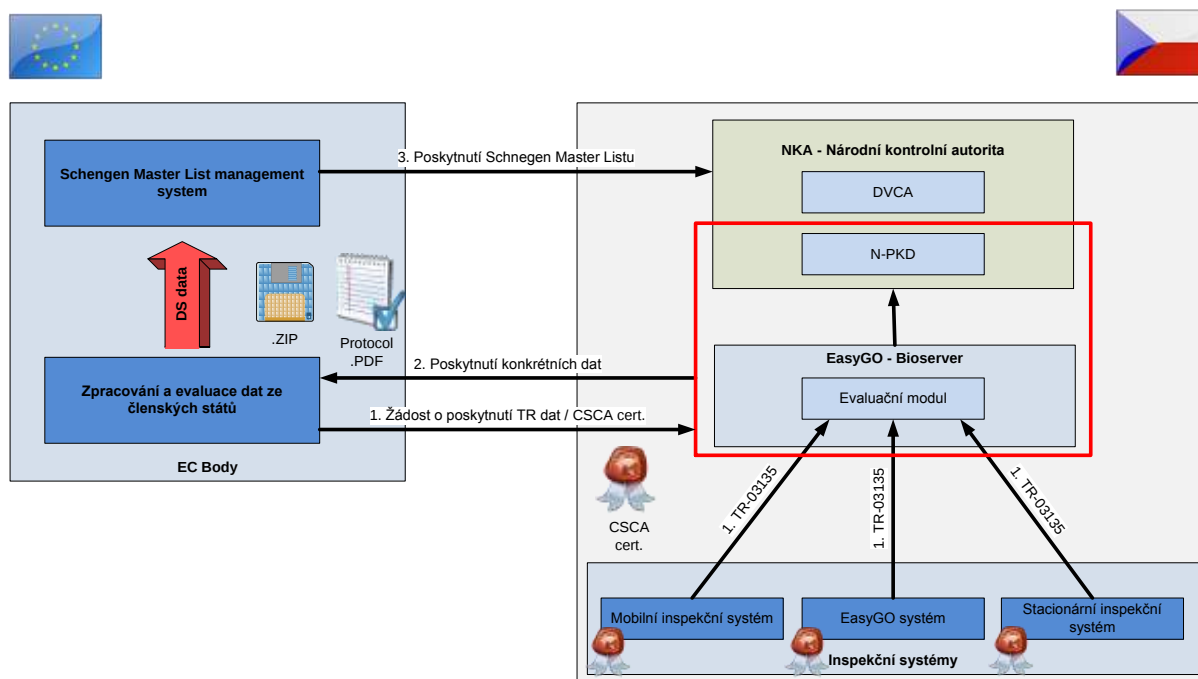
Uvedené transakční záznamy budou poskytovány prostřednictvím dedikované URL adresy do úložiště evaluačního modulu systému EasyGO, která následně provede distribuci potřebných dat pro systém N-PKD, který je součástí systému NKA.

3 Technické zadání

Níže popsané požadované rozšiřující funkcionality realizované zadavatelem provozovanými systémy musí zabezpečit následující proces:

- 1) Evropská komise (DG Home) zašle emailem pracovišti Národní kontrolní autority vybraný CSCA certifikát konkrétní země.
- 2) Pracoviště Národní kontrolní autority (dále také jako NKA) vyžádá v evaluačním subsystému systému EasyGO .PDF report a .ZIP soubor s korespondujícími Document Signer certifikáty, které jsou získány z TR Logů, a zašle je zpět Evropské komisi (DG Home).
- 3) Na základě zaslaného reportu pracovištěm Národní kontrolní autority provede Evropská komise validaci důvěryhodnosti zaslaného certifikátu.
- 4) V případě, že všechna kritéria byla naplněna, je předmětný CSCA certifikát vystaven v nově vydaném Schengen Mater Listu.
- 5) V případě, že je SML vydán, je tento naimportován do úložiště N-PKD (NKA) jako sub-modulu systému N-PKD (NKA), který je následně poskytne registrovaným inspekčním systémům prostřednictvím komponenty DVCA.

Mimo tento proces vyžádaný pracovištěm Evropské komise, bude systém EasyGO aktivně přenášet data související s provedením Pasivní autentizace modulu N-PKD (funkční součást NKA) pro možné rozšíření obsahu zadavatelem vydávaného Master Listu na základě zadavatelem získaného CSCA certifikátu a provedené vlastní evaluace.



Obrázek 2: Přehled procesů požadovaného řešení

Počet terminálů, ze kterých budou přenášena transakční data, bude až 5 000. Z tohoto důvodu zadavatel požaduje, aby dodané řešení bylo kapacitně schopné obsloužit alespoň 7 000 terminálů, kde počet transakcí celkem za hodinu bude 20 000.

3.1 Doplnění funkcí evaluačního modulu EasyGO aplikačního serveru

Zadavatel požaduje doplnění funkcionalit evaluačního modulu systému EasyGO o funkcionalitu statistického zpracování transakčních logů inspekčních systémů provozovaných zadavatelem, které jsou ve formátu BSI TR-03135.

Všechny registrované inspekční systémy budou poskytovat transakční záznamy ve formátu .XML jak je definován BSI TR-03135. Tento formát obsahuje veškeré nutné informace, které jsou nezbytné pro sdílení dat pro sestavení Schengen Master listu na úrovni Evropské komise.

Evaluační modul systému EasyGO – Bioserver bude podle požadavku zadavatele rozšířen o následující funkcionalitu:

1. Uložení transakčního logu do datového úložiště ze jmenovaných inspekčních systémů. Vlastní úložiště bude dostupné prostřednictvím URL,
2. Identifikace typu .XML souboru podle TR-03135:
 - a. Basic,
 - b. Minimal extended,
 - c. Extended.
3. Náhled v grafické a tabulkové podobě nad reporty sestavených z transakčních logů, kde bude možné filtrovat na základě:
 - a. Četnosti výskytu podle typu dokladu,
 - b. Četnosti výskytu podle vydávací autority – reference na Document Signer certifikát a kořenový certifikát,
 - c. Výsledku kontroly doklady s rozdělením na:
 - i. Elektronické kontroly,
 - ii. Optické kontroly.
 - d. Doba inspekce kontrolovaných částí dokladu – bude-li na úrovni .XML informací k dispozici.
 - e. Statistika vůči konkrétnímu terminálu, na kterém byla transakce provedena.
4. Konverze všech transakčních logů .XML do formátu basic, v případě, že je zpracován transakční soubor ve formátu „*Minimal extended/Extended*“ a jejich průběžná distribuce systému NKA, který následně provede zpracování pro potřebu procesu vytvoření Schengen Master Listu na úrovni modulu N-PKD.
Jedná se o případy, kdy Evropská komise poskytne CSCA certifikát země, který není zaveden na úrovni modulu N-PKD a jakkoliv kvalifikován.

V takovém případě na základě předem nastaveného počtu výskytu Document Signer certifikátů z realizovaných inspekcí bude možné rozhodnout o jeho posunutí do primárního úložiště N-PKD (modul NKA) pro jeho následné zavedení řízeným procesem do Master Listu nebo Defect Listu, který vydává pracoviště NKA pro potřeby kontroly e-cestovních dokladů.

Pro naplnění všech požadavků Evropské komise zodpovědné za vydávání Schengen Master Listu je nezbytné připravit report ve formátu .PDF a .ZIP soubor se všemi korespondujícími DS certifikáty, pro které byl zaslán CSCA certifikát konkrétní země.

Součástí požadované funkcionality je správa reportů a jejich vytváření, které musí být realizováno v konkrétním dialogu.

Zpracování reportu bude ve formátu .PDF, podle následujícího níže uvedeného vzoru. Povinné položky reportu jsou (v anglickém jazyce):

1. CSCA Certificate Issuing Country:
2. CSCA Certificate Details:
3. Period of log-data acquisition:
4. First occurrence of a DS Certificate referencing this CSCA Certificate
5. Amount of days with occurrence of DS Certificates referencing this CSCA Certificate
6. Amount of different DS Certificates referencing this CSCA Certificate
7. SHA-1 Fingerprints of DS Certificates referencing this CSCA Certificate
8. Amount of border checks involving different eMRTDs that contain one of the above DS Certificates:
9. Anomalies of the CSCA Certificate
10. Anomalies of DS Certificates referencing this CSCA Certificate
11. Additional information / remarks
12. Rapporteur's Authority
 - a. Member State
 - b. Organisation / Authority
 - c. Contact
 - d. Date Form was completed



CSCA Certificate Validation Form

1. CSCA Certificate Issuing Country:

AUSTRIA

2. CSCA Certificate Details:

Subject

C=AT, O=GV, OU=BMI, CN=CSCA-AUSTRIA

Serial Number

fd39007ae82f585 (HEX)

SubjectKey Identifier

041604141fe1572e9b35121363a50fee3e2ce2c1d187a8dd

Validity

Sun Jul 19 10:50:44 CEST 2026 - Sun Jul 19 10:50:44 CEST 2026

SHA-1 Fingerprint

dee16e09666b5693809a1d13c2fec401d1bb438c

3. Period of log-data acquisition:

2015-03-27 00:00:00.0 - 2016-01-26 11:40:31.367

4. First occurrence of a DS Certificate referencing this CSCA Certificate:

2015-07-17

5. Amount of days with occurrence of DS Certificates referencing this CSCA Certificate:

71

6. Amount of different DS Certificates referencing this CSCA Certificate:

15

7. SHA-1 Fingerprints of DS Certificates referencing this CSCA Certificate:

59f4369b8876e2b76ee097667431890ddd51f9d7
0db9d43e86d0aac9b59cbdc6dc11b8496e0244e2
0deab377dd4c81269d604bb9e33b1e6795e8e4a7
32a413f0a2322a25a307132a06e1693e1d1790b3
0fede7e253a1affefelaaf72ff6ed9ca66464ea2c
5695b52f25407868f5246d71fbc23a7662a8d54b
67852aa81e5174708384ffb524cc7110682585c4
6d322b40303252d3611f74c59d84417b944a2922
a2e0426049ab46d25c97023d824276c1ac64fb27
d9c89623ddf82d09ae8d720e73736da048a964b1
f13d60a87fcfb990cebf6a7a5a34802b5040aef1
a5b94cbac1bf2acd1ccef2e3ca0743f224d2ab3c
17c88bccb9f00eaeaa3294fe4a4a20f5a64324af
1d61b6109fb0f6f06e58cbe2e8d6987481b30110
23a35d8eaa6c5354190d43fd662ae20ec2870d6

8. Amount of border checks involving different eMRTDs that contain one of the above DS Certificates:

132

9. Anomalies of the CSCA Certificate:



CSCA Certificate Validation Form

--

10. Anomalies of DS Certificates referencing this CSCA Certificate:

--

11. Additional information / remarks:

CSCA certificate is used for the issuance of the following document types: P

--

12. Rapporteur's Authority:

Member State <table border="1"><tr><td></td></tr></table>		Organisation / Authority <table border="1"><tr><td></td></tr></table>	
Contact <table border="1"><tr><td></td></tr></table>		Date Form was completed <table border="1"><tr><td></td></tr></table>	

13. Please send the completed validation form to:

3.2 Realizace interface mezi systémem EasyGO a sub-modulem NKA – N-PKD

Mezi evaluačním modulem systému EasyGO bude vybudován komunikační interface, který bude zpracovávat data nezbytná pro poskytnutí informací k semi-automatickému vytvoření Schengen Master Listu vydávaným NKA.

Zabezpečení komunikace bude realizováno prostřednictvím TLS certifikátu, který vydá Technická certifikační autorita NKA (Tech CA NKA).

EasyGO aplikační server jak již bylo uvedeno, bude v tomto případě centrální komponentou, která bude přijímat transakční data z následujících inspekčních systémů:

1. EasyGO automatické brány,
2. Systém stacionární kontroly cestovního dokladu,
3. Mobilní inspekční systémy.

V modulu N-PKD jako sub-modulu systému NKA budou nastaveny automatické procesy, které zabezpečí automatické pracovní postupy (zákaznická definice pracovních postupů), která zajistí distribuci CSCA certifikátů do jednotlivých kvalifikovaných úložišť.

3.3 Doplnění serveru do infrastruktury automatizovaného biometrického systému

Jak bylo uvedeno výše, je požadováno oddělení výkonu aplikační a evaluační části. Z tohoto důvodu bude dodán 1 nový server, na které budou migrovány funkce statistického zpracování dat a komunikace mezi oběma systémy NKA – EasyGO.

Požadavek na server, který bude umístěn v blade :

- Procesor Intel® Xeon® E5-2600 product family; Intel® Xeon® E5-2600 v2 product family nebo kvalitativně a cenově obdobný. Server musí být osazený dvěma CPU s minimálně 4 jádry na CPU a musí dosahovat minimálně 380 bodů v benchmarku SPEC CFP2006 rates Result Published by SPEC ve sloupci Result Base.
- Server musí být osazen minimálně 8x fyzickými pamětmi typu RAM „low voltage“ kompatibilní se sběrnici procesoru o minimální velikosti 32 GB o rychlosti 1600MHz,
- Součástí požadovaného serveru jsou dva SAS disky o rychlosti 15000 RPM o minimální velikosti min. 500GB per HDD, přičemž disky musí být zapojeny v raid 0, 1, a určeny pro běh serveru v režimu 24x7.
- RAID řadič musí být z důvodu kompatibility se stávajícím prostředím podporován ze strany VMware. Nabízený server musí být kompatibilní s OS MS Windows 2012 R2 Server, Linux, VMware.
- Každý server by měl mít možnost osazení dvěma rozšiřujícími kartami, přičemž server pro EasyGO ISY musí navíc umožňovat osazení standardní PCI/PCI-X kartou, full size, full length, do které bude umístěn HSM modul.
- Požadovaná konektivita 2x10Gb ethernet,
- Prediktivní analýza poruch pro pevné disky, procesory, paměť.

Server bude dodán s OS Windows Server. Podpora dálkové správy pomocí redundantních management modulu chassis. Možnost vzdáleného zjištění sériového čísla komponentů. Prohlášení o shodě. Podmínkou umožnění dodávky je, že veškerý dodávaný hardware bude nový, nepoužitý a bude dodán včetně dokumentace. V nabídce požadujeme uvést typ, název a počet veškerého zařízení a software.

Server navržený uchazečem musí být plně kompatibilní se stávajícím blade chassis, kterým je HP BladeSystem c7000 provozovaný v následující konfiguraci v datovém centru na Letišti Václava Havla v Praze Ruzyni:

- 1-fázová rackmount (10U) blade police; kapacita: 16x half-height nebo 8x full-height blade, 8x blade interconnect;
- 1x Onboard Administrator with KVM – management modul
- Power Discovery Services, Intelligent Power Module
- 4x hot-plug Active Cool 200 ventilátor
- Onboard Administrator with KVM – management modul s konzolovým přepínačem (redundantní)

- 1-fázový napájecí modul pro HP BladeSystem c7000
- HP BladeSystem PCI Expansion Blade – I/O blade; 2x PCI-X nebo 2x PCIe I/O slot
- 2x Passtrought gigabit ethernet module
- 5x 2400 W Gold hot-plug zdroj napájení
- 5x 2 m napájecí kabel (IEC320-C20/IEC320-C19)

Blade chassis je vybaveno dvěma passtrough moduly 1 Gbit, které jsou připojeny k dodávaným TOR switchům.

3.4 Výčet dodávek uchazeče

V této části zadávací dokumentace je uveden výčet dodávek uchazeče:

Dodávka	Počet
Analýza a návrh řešení	1 sada
Dodávka a implementace automatických procesů – NKA pro modul N-PKD	1 sada
Rekonfigurace systémového prostředí NKA a EasyGO	1 sada
Dodávka a implementace evaluačního a reportovacího modulu NKA s integrací registrovaných inspekčních systémů	1 sada
Dodávka serveru včetně instalace a migrace dat	1 sada
Testování a finální akceptace díla	1 sada
Podpora provozu do 30.4.2017 v rozsahu alespoň 2 MD / měsíc	1 sada
Úprava systémové dokumentace	1 sada