PŘÍLOHA Č. 1 - DEFINICE POJMŮ A ZKRATEK

Pojem / Zkratka	Plný text	Vysvětlení
AIS EOP	Agendový informační systém Evidence občanských průkazů	V současnosti je evidence zabezpečována IS EOP (Informační systém Evidence občanských průkazů)
AKO	Akceptační komise	Projektový orgán, který provádí akceptaci plnění smlouvy
Aplet		Programový kód zaveditelný a spustitelný v systému Java Card. Každý applet může obsahovat jednu nebo více aplikací s vlastním zabezpečením přístupu
Asymetrická kryptografie	-----	Asymetrická kryptografie neboli kryptografie veřejných klíčů využívá dvojici klíčů (soukromý klíč a veřejný klíč) pro algoritmy šifrování a digitálního podepisování (např. algoritmy RSA, DSA atd.)
autenticita	-----	Garance, že konkrétní zpráva pochází z konkrétního zdroje. Autenticity je dosaženo např. elektronickým podepsáním výsledku hash funkce z obsahu zprávy.
autentizace	-----	Proces ověření proklamované identity subjektu. Rozlišujeme autentizaci entity (osoby, programu) a autentizaci zprávy.
bezkontaktní čip	-----	Pro účely smlouvy se jím rozumí nosič dat s biometrickými údaji
biometrický údaj	-----	Pro účely smlouvy se jím rozumí údaj o zobrazení obličeje a údaj o otiscích prstů rukou (§ 5 odst. 2 zákona o cestovních dokladech)
BSI	Bundesamt für Sicherheit in der Informationstechnik	Německý spolkový úřad pro bezpečnost IT
CA	Certifikační autorita	Souhrn technických a organizačně-administrativních prostředků, které umožňují vystupovat jako poskytovatel certifikačních služeb
Certifikát	-----	Datová zpráva vydaná CA, která spojuje data pro ověřování podpisů (veřejný klíč) s identitou subjektu vlastnícího tato data
Certifikát pravosti	-----	Certifikát, jímž se ověřuje pravost a neporušenost biometrických údajů. Je vydán NCA na žádost DS. Dále je certifikát pravosti poskytován tuzemským DV a zahraničním NCA. Pojem je zaveden (připravovaným) Zákonem o certifikaci veřejných dokladů s biometrickými údaji
CIS	Cizinecký informační systém	Informační systém, obsahující mj. údaje o cizincích s povoleným pobytem na území ČR, o jejich cestovních dokladech a povoleních k pobytu
Citlivý údaj	-----	Osobní údaj vypovídající o národnostním, rasovém, etnickém původu apod.; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů,
cizinecký e-pas	cizinecký elektronický pas	Personalizovaný strojově čitelný cizinecký pas České republiky vydávaný podle § 108 odst. 1 písm. d) zákona č.326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů ve znění pozdějších předpisů, s přihlédnutím k implementaci Nařízení Rady (ES) č. 2252/2004 ze dne 13. prosince 2004 o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy (dále jen „Nařízení“) a v souladu s Rozhodnutím Komise ze dne 28. února 2005 a Rozhodnutím Komise ze dne 28.června 2006, kterým se stanoví technické specifikace norem pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy (dále jen „Rozhodnutí“)
CRL	Certificate revocation list	Seznam zneplatněných certifikátů
CS-M	-----	Centrální aplikace pro monitorování a správu

Pojem / Zkratka	Plný text	Vysvětlení
CS-MZV		Externí systém Ministerstva zahraničních věcí (vývěska), sloužící pro výměnu dat žádostí o e-pas nabraných na zastupitelských úřadech s centrálním systémem CDBP
CVS	Centrální výpočetní středisko MV	-----
DB	Databáze	-----
e-Blesk	elektronický pas typu e-Blesk	Personalizovaný strojově čitelný cestovní pas s biometrickými údaji uloženými v nosiči dat s biometrickými údaji, vyráběný ve zrychleném režimu.
e-cestovní doklad	elektronický cestovní doklad	Personalizovaný strojově čitelný cestovní doklad s biometrickými údaji uloženými v nosiči dat s biometrickými údaji; též souhrnné označení pro: e-pas, cizinecký e-pas, uprchlický e-pas
e-pas	elektronický pas	Personalizovaný strojově čitelný cestovní pas České republiky vydávaný státním občanům České republiky podle § 5 odst. 1 písm. a) zákona č. 329/1999 Sb., o cestovních dokladech a o změně zákona č. 283/1991 Sb., o Policii České republiky ve znění pozdějších předpisů (zákon o cestovních dokladech), ve znění zákona č. 217/2002 Sb., zákona 320/2002 Sb., zákona č. 539/2004 Sb., zákona 559/2004 Sb. a zákona č. 136/2006 Sb., s přihlédnutím k implementaci Nařízení a v souladu s Rozhodnutími
EAC	Extended Access Control	(dodatečná kontrola přístupu); Podle ICAO se jedná o kombinaci prokázání pravosti čipu (CA) a terminálu (TA) / EAC Extended Access Control being according to ICAO the combination of chip authentication and terminal authentication
EAL	Evaluation Assurance Level	Úroveň záruk bezpečnosti IS definovaná v ISO/IEC 15408
EF.SOD	A RFC3369 CMS Signed Data Structure, signed by the Dokument Signer (DS). Carries the hashed LDS Data Groups.	CMS struktura typu signed data, která obsahuje jednotlivé haše LDS datových skupin.
eOP	elektronický občanský průkaz	personalizovaný občanský průkaz se strojově čitelnými údaji podle § 2 odst. 2 písm. b) zákona č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů a personalizovaný občanský průkaz se strojově čitelnými údaji a s kontaktním elektronickým čipem (dále jen „eOP s čipem“) podle § 2 odst. 2 písm. a) zákona č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů
ePKP	elektronické PKP	Personalizovaný strojově čitelný průkaz o povolení k pobytu, s biometrickými údaji, vydávaný státním příslušníkům třetích zemí v souladu se zákonem č. 326/1999 Sb.
garant		Koordinuje činnost týmu na straně zadavatele MV a odpovídá za poskytnutí součinnosti zadavatele MV v rámci daného týmu a schvaluje výstupy poskytovatele.
HSM	Hardware Security Module	Hardwarový modul pro bezpečné uložení klíčů a provádění kryptografických operací
I.CA	První certifikační autorita, a.s.	Akreditovaný poskytovatel certifikačních služeb
ICAO	International Civil Aviation Organization	Mezinárodní organizace pro civilní letectví
ICAO PKD	ICAO Public Key Directory	Orgán ICAO pro mezinárodní koordinaci a výměnu certifikátů, spojených s vydáváním e-cestovních dokladů.
Infrastruktura Projektu CDBP	-----	HW a SW vybavení systému CDBP, respektive systému pro zpracování žádostí, pořizování a zpracování dat pro výrobu a dodávání e-cestovního dokladu, eOP a zpracování protokolů, pořizování a zpracování dat pro výrobu a dodávání ePKP, včetně jeho provozování.
IS	Informační systém	-----

Pojem / Zkratka	Plný text	Vysvětlení
Is	Inspekční systém	Místo pro ověřování pravosti e-cestovního dokladu a autentizace jeho držitele s využitím biometrických údajů (otisk prstu)
IS ECD	Informační systém evidence cestovních dokladů	§ 29 zákona o cestovních dokladech
IS EO	Informační systém evidence obyvatel	§ 3 zákona o evidenci obyvatel
IS EOP	Informační systém evidence občanských průkazů	§ 17 zákona o občanských průkazech
ISZR	Informační Systém Základních Registrů	Rozhraní pro komunikaci se systémem Základních registrů
Kořenový certifikát	-----	Certifikát, vystavený CA pro svůj veřejný klíč, podepsaný odpovídajícím soukromým klíčem ("self-signed" certifkát)
KRP	Komise pro realizaci Projektu CDBP	Společný vrcholný řídící orgán Projektu CDBP mezi smluvními stranami, jehož členy jsou určení zástupci MV a STC; odpovídá za realizaci Projektu CDBP
KS-E	Klientský systém - specimeny	Klientská část systému pro pořizování žádostí o specimen e-cestovního dokladu
KS-E2	Klientský systém - specimeny	Klientská část systému pro pořizování žádostí o specimen ePKP
KS-M	Klientský systém - mobilní	Mobilní verze klientské části systému
KS-O	Klientský systém - obce	Klientská část systému pro obecní úřady
KS-P	Klientský systém - OAMP	Klientská část systému pro cizinecké a uprchlické e-pasy
KS-PKP	Klientský systém - OAMP	Klientská část systému pro ePKP
KS-PRVD	Klientský systém - pro příjem a výdej dat výrobci dokladů	Klientská část centrálního systému – zajišťuje řízený přenos úspěšně zpracovaných žádostí o e-pasy a eOP uložených v PDB (provozní databáze CS) k VD (výrobce dokladů) a příjem zpracovaných dat od VD
KS-PRVD2	Klientský systém - pro příjem a výdej dat výrobci dokladů	Klientská část centrálního systému – zajišťuje řízený přenos úspěšně zpracovaných protokolů o pořízení biometrických údajů pro ePKP a žádostí o cizinecké a uprchlické e-pasy, uložených v PDB (provozní databáze CS) k VD (výrobce dokladů) a příjem zpracovaných dat od VD
KS-R	Klientský systém - reklamace	Klientská část systému určeného pro možnost kontroly reklamovaných e-pasů, ePKP a eOP
KS-SP	Klientský systém pro zvláštní doklady	klientská část systému pro systém podléhající utajení
KS-T	Kontrolní aplikace	Aplikace pro speciální kontrolní stanice
KS-x	-----	Souhrnný pojem pro KS-O a KS-P
LINK certifikát	-----	Speciální typ certifikátu certifikační autority, který slouží k přenesení důvěr ze starého klíče na nový klíč; link certifikát certifikuje nový klíč pomocí starého a tak v systému, kde je důvěryhodný starý klíč, je po aplikaci LINK certifikátu důvěryhodný i klíč nový
milník	-----	Klíčový termín v Projektu CDBP, ve kterém je na sebe bezprostředně vázáno více událostí; zkráceně označovaný písmenem „M“ a pořadovým číslem
MRA	Mobilní registrační autorita	Mobilní registrační autorita akreditovaného poskytovatele certifikačních služeb
MZSLA	Měsíční zpráva SLA	Zkratka pro pravidelný dokument/report "Měsíční zpráva o rozsahu a kvalitě poskytovaných služeb za období: …"
nepopiratelnost	-----	Nemožnost odmítnout autorství zprávy. Nepopiratelnosti je dosaženo elektronickým podepsáním zprávy soukromým klíčem, který má právě jednoho vlastníka (např. držitel karty s kvalifikovaným certifikátem)
MZV	Ministerstvo zahraničních věcí	
neslučitelnost rolí	-----	Nepřípustná kombinace dvou rolí, vykonávaná jednou osobou

Pojem / Zkratka	Plný text	Vysvětlení
netHSM	-----	Kryptografické moduly – zařízení pro bezpečné uložení citlivého klíčového materiálu
OAMP MV	Odbor azylové a migrační politiky	-----
oblast systémové integrace	-----	Oblast Projektu CDBP v souladu s Organizačním schématem Projektu CDBP
OCIS		Odbor centrálních informačních systémů
Osobní údaj	-----	Jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.
OÚ	Obecní úřad	Obecní úřad obce s rozšířenou působností a úřady městských částí Praha 1 až Praha 22, stanovené statutem hl.m.Prahy
PIN	Personal identification number	Osobní identifikační číslo
PIN Pad	-----	Bezpečný hardware, který umožní vkládání PIN kódů
PK MV	Projektová kancelář MV	Projektová kancelář MV, která zajišťuje řízení součinnosti a koordinaci Projektu CDBP na straně MV
PK STC	Projektová kancelář STC	Projektová kancelář STC, která zajišťuje řízení a koordinaci Projektu CDBP - výkonný orgán řízení Projektu CDBP
Plán akceptací	----	Dokument definuje předávané a akceptované výstupy a jejich akceptační kritéria
Pracoviště OAMP	-----	Pracoviště, na kterém probíhají procesy spojené s cizineckými e-pasy, uprchlickými e-pasy a doklady ePKP
Projekt CDBP	Projekt cestovních dokladů s biometrickými údaji	Projekt na dodávání osobních dokladů vydávaných v působnosti Ministerstva vnitra, včetně systému zpracování žádostí, pořizování a zpracování dat
Protokol o pořízení	Protokol o pořízení biometrických údajů pro ePKP	Formalizovaný dokument, který je výstupem procesu pořízení údajů pro výrobu dokladu ePKP. Z technického hlediska je pak protokol o pořízení souhrnem pořízených dat.
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.
PSeP	Personalizační SW elektronických pasů	Systém pro personalizaci osobních dokladů vydávaných v působnosti Ministerstva vnitra
PUK	Personal Unblocking Number	Kód sloužící pro odblokování PIN
PZKS	Plán zvládání krizových situací	Dokument popisující nestandardní situace nebo havárie velkého rozsahu na KS-X stanicích; viz Krizový štáb
RFC	Request For Comments	Internetový standard
ROB	Registr obyvatel	Součást Informačního systému Základních registrů, jednotné místo pro vedení referenčních údajů o fyzických osobách
SKO	Sponzorská komise	Řídící orgán Státní tiskárny cenin v Projektu CDBP
Specimen	-----	Vzor e-cestovního dokladu, ePKP a nebo eOP
STC	STÁTNÍ TISKÁRNA CENIN, státní podnik	Poskytovatel služby („Dodávání osobních dokladů vydávaných v působnosti Ministerstva vnitra, včetně systému zpracování žádostí, pořizování a zpracování dat“).
symetrická kryptografie	-----	Používá k šifrování i dešifrování jediný klíč
Systém CDBP		Systém pro zajištění dodávání osobních dokladů v působnosti Ministerstva vnitra se strojově čitelnými údaji a s nosičem dat s biometrickými údaji, včetně systému zpracování žádostí a pořizování a zpracování dat.
TA	Terminal Authentication	Protokol pro prokázání pravosti terminálu a jeho oprávnění číst e-cestovní doklad

Pojem / Zkratka	Plný text	Vysvětlení
TAR	Tým pro analýzu rizik a bezpečnostní dokumentaci	Realizační tým, který zodpovídá za provedení analýzy rizik a tvorbu/aktualizaci bezpečnostní dokumentace v oblasti SI II
TCS	Tým pro centrální systém a certifikační autoritu MV	Realizační tým, který zodpovídá za přípravu technické infrastruktury (vyjma HW klientských pracovišť), dohledový systém včetně jeho implementace a za přípravu provozu infrastruktury. Dále zodpovídá za přípravu a realizaci služeb certifikační autority pro výdej a management certifikátů pro uživatele/operátory klientských stanic a pro systémové certifikáty
TK	Token TK	Klíč zajišťující korektní nahrávání apletů na kontaktní čip.
TKX	Tým pro klientská pracoviště	Realizační tým, který zodpovídá za přípravu a podporu technické infrastruktury klientských pracovišť; komunikuje s OÚ a MV. Zajišťuje podklady pro stavební připravenost, kontroluje ji a koordinuje instalace. Dále je zodpovědný za přípravu a realizaci školení.
TNN	Tým PKI	Realizační tým, který zodpovídá za kompletní dodávky komponent PKI, včetně odpovídající bezpečnostní dokumentace v oblasti SI I
Token		Kryptograficky zabezpečená datová struktura obsahující identifikátory aplikace a jeho otisk určená pro vzdálenou správu aplikací realizovaných přes dodatečné bezpečnostní domény (SSD)
TOP	Tým organizace provozu	Realizační tým, který zodpovídá za provoz systému CDBP.
TPS	Tým pro personalizační SW	Realizační tým, který zodpovídá za realizaci systému pro personalizaci e-cestovních dokladů
TPV	Tým pro personalizaci a výrobu	Realizační tým, který zodpovídá za realizaci výroby a personalizace dokladů
TRK	Tým řízení rizik a kvality	Pracovní tým pro řízení rizik a kvality Projektu CDBP
TSP	Tým smluvní připravenosti	Realizační tým, který zodpovídá za přípravu dodatků smlouvy o umístění technického zařízení na OÚ a MV
TSW	Tým pro softwarové aplikace a procesy	Realizační tým, který zodpovídá za vývoj kompletního programového vybavení pro oblast CS a KS-x
TTC	Tým testování a compliance	Realizační tým, který zajišťuje provedení nezávislého testování systému jako celku a testování shody dokumentace
účastníci Projektu CDBP	-----	Všechny subjekty, které se podílejí na Projektu CDBP
Uchovávání osobních údajů	-----	Udržování údajů v takové podobě, která je umožňuje dále zpracovávat.
UNO	-----	Pracoviště nebo komponenty pořízené OÚ na vlastní náklady
uprchlický e-pas	-----	Personalizovaný strojově čitelný uprchlický pas České republiky vydávaný podle § 61zákona č.325/1999 Sb., o azylu a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů (zákon o azylu), ve znění pozdějších předpisů s přihlédnutím k implementaci Nařízení a v souladu s Rozhodnutími
VBP	Výbor pro bezpečnost projektu CDBP	Výbor pro bezpečnost projektu CDBP zajišťuje řízení a koordinaci bezpečnosti informací v systému CDBP
VP	Vedoucí projektu	Určený zástupce jednotlivých účastníků Projektu CDBP
Změnové řízení (změnový požadavek)		Požadavek na změnu předmětu smlouvy. Standardní proceduru Řízení změn popisuje Plán kvality Projektu CDBP.
Zneplatněný certifikát	-----	Certifikát, u nějž byla ukončena platnost bez možnosti obnovy této platnosti a který je uveden v seznamu CRL.
Zpracovatel	-----	Ve smyslu zákona na ochranu osobních údajů (zákon č. 101/2000 Sb.) je to každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.
ZR	Základní registry veřejné zprávy	Centrální registry veřejné správy, vzniklé na základě zákona č. 111/2009 Sb. ve znění pozdějších předpisů, o základních registrech: ROB – Registr obyvatel

Pojem / Zkratka	Plný text	Vysvětlení
		RPP – Registr práv a povinností ROS – Registr osob RUIAN – registr územní identifikace
ZÚ	Zastupitelský úřad	Zastupitelský úřad České republiky
ZVS	Záložní výpočetní středisko	-----
ZVZ	Zákon o veřejných zakázkách	Zákon č.137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů

Verze 1.00