Certifikační politika

Certifiakční politika CA ve správě Kooperativa pojišťovna a.s. Vienna Insurance Group

Verze dokumentu	
Verze	1.1
Autor	SEFIRA spol. s r.o., Tomáš Vaněk, Petr Nižnanský
Datum	17.3. 2017
Počet stran	37

Historie změn

Datum	Popis	Verze
18. 4. 2016	Základní verze.	1.0
17.3.2017	Aktualizace dokumentu po nasazení HSM	1.1

Obsah

1. Úvod

1.1. Přehled

Tento dokument reprezentuje certifikační politiku, kterou se řídí provoz certifikačních autorit VIG CZ ve správě Kooperativa, pojišťovna, a.s. Vienna Insurance Group. Dokument vymezuje podmínky, práva a povinnosti subjektů, základní parametry a vlastnosti poskytovaných služeb, certifikátů a revokačních seznamů. Definuje procesy, které řídí poskytování těchto služeb. Těmi se rozumí zejména proces registrace, vydání certifikátu a jejich správa, zneplatnění vydaných certifikátů a další související činnosti.

Dokument je vystavěn na podkladě všeobecně uznávaných norem:

- RFC3647 – Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework
- RFC3280 – Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL)

Struktura této certifikační politiky vychází z platné legislativy pro APCS (Akreditovaní poskytovatelé certifikačních služeb).

1.2. Název a jednoznačné určení dokumentu

Tato certifikační politika je publikována pod názvem Certifikační politika CA VIG CZ.pdf.

Certifikační politika nemá přiřazeno žádné identifikační OID. V certifikátech vydávaných certifikačními autoritami není na tuto politiku uvedena reference.

1.3. Participující subjekty

1.3.1. Certifikační autority (dále „CA“)

Infrastruktura veřejných klíčů VIG CZ je reprezentována kořenovou autoritou a dvěma podřízenými, které jsou určeny pro externí a interní pracovníky VIG CZ.

Kořenová autorita („VIG Czech Republic - Root CA“ dále jen RootCA) podepisuje certifikáty podřízených certifikačních autorit. Tato autorita nevydává certifikáty zařízením ani fyzickým osobám.

Podřízená autorita pro interní uživatele („VIG Czech Republic - Internal users CA“ dále jen InternalCA) vydává certifikáty pouze pro zaměstnance skupiny VIG.

Podřízená autorita pro externí uživatele („VIG Czech Republic - External users CA“ dále jen ExternalCA) vydává certifikáty pouze pro externí uživatele.

1.3.2. Registrační autority (dále „RA“)

RootCA neprovozuje žádnou registrační autoritu pro fyzické osoby a vydávání certifikátů se řídí interními procesy skupiny VIG.

InternalCA i ExternalCA vydávají své certifikáty prostřednictvím CzechIdMng, CzechIdMng je webová aplikace, do které přistupují uživatelé pomocí jména a hesla.

1.3.3. Držitelé certifikátů

Držitelem certifikátu od RootCA se rozumí další certifikační autority.

Držitelem certifikátu od InternalCA a ExternalCA se rozumí fyzické osoby, které požádaly o vydání certifikátu a měly na tento úkon patřičné právo.

O certifikáty z InternalCA smí žádat pracovníci (dále je budeme označovat jako interní uživatelé) s pracovně-právním vztahem s některou z následujících společnosti:

- Kooperativa, pojišťovna, a. s. Vienna Insurance Group

- **Česká podnikatelská pojišťovna, a.s., Vienna Insurance Group** Dalších majetkově propojených subjektů

O certifikáty z ExternalCA smí žádat uživatelé bez pracovně-právního vztahu s některou z výše uvedených společností.

1.3.4. Spoléhající se strany

Spoléhající se stranou je jakýkoli subjekt, který využívá certifikáty. Spoléhající se strana je před použitím certifikátu povinna provést ověření jeho platnosti nejméně provedením těchto kroků:

- ověří platnost certifikátu podle atributů `notBefore` a `notAfter`
- ověří, že certifikát vydala příslušná certifikační autorita

Je doporučeno provést kontrolu dle seznamu zneplatněných certifikátů, ověřit rozšíření `basicConstraints` (základní omezení) a ověřit správnost použití klíče (`keyUsage` a `extendedKeyUsage`).

1.3.5. Jiné participující subjekty

Nejsou definovány.

1.4. Použití certifikátu

Všechny certifikáty vydané dle této certifikační politiky je povoleno používat pouze k účelu, který je v certifikátu vyznačen.

1.4.1. Přípustné použití certifikátu

Certifikáty RootCA jsou vydávány pro další certifikační autority. Z této povahy vyplývá i jejich použití pro vydávání dalších certifikátů a dalších činností spojených s provozem CA.

Certifikáty InternalCA a ExternalCA jsou vydávány pro autentizaci do portálů provozovaných VIG a pro vytváření elektronického podpisu.

1.4.2. Omezení použití certifikátu

Certifikáty nesmí být používány v rozporu s jejich určením specifikovaným atributem `keyUsage`, případně `extendedKeyUsage`.

1.5. Správa politiky

1.5.1. Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Za správu této certifikační politiky je odpovědný úsek informačních technologií Kooperativa, pojišťovna, a.s. Vienna Insurance Group

1.5.2. Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Kontaktní osobou pro věci týkající se této certifikační politiky je operátor certifikační autority. Kontaktní e-mail ca@vig.cz.

1.5.3. Subjekt odpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů certifikačních služeb

Rozhodnutí o shodě a je plně v kompetenci úseku informačních technologií Kooperativa, pojišťovna, a.s. Vienna Insurance Group

1.5.4. Postupy pro schvalování certifikační politiky

Úseku informačních technologií Kooperativa, pojišťovna, a.s. Vienna Insurance Group stanovuje všechny postupy pro schvalování certifikační politiky v souladu s interní legislativou společnosti.

1.6. Přehled použitých pojmů a zkratek

Zkratka	Význam
CA	Certifikační autorita
CP	Certifikační politika
CRL	Seznam zneplatněných certifikátů
CzechIdMng	Webový portál pro uživatele určený k vydávání a revokování certifikátů
DN	Distinguished Name – rozlišovací jméno objektu dle norem rodiny X.500
Garant	Osoba odpovědná za správnost informací o přiřazených uživatelích v IDM, navíc s možností udělovat oprávnění pro vydávání certifikátů.
ExternalCA	Podřízená certifikační autorita pro interní uživatele (VIG Czech Republic - External CA)
Externí uživatelé	Viz. 1.3.3
IDM	Identity Management systém
InternalCA	Podřízená certifikační autorita pro externí uživatele (VIG Czech Republic - Internal CA)
Interní uživatelé	Viz. 1.3.3
OID	Object Identifier – číselný identifikátor objektu, nebo atributu dle ISO/ITU, IANA atd.
PKI	Public Key Infrastructure – infrastruktura veřejných klíčů
RA	Registrační autorita
RFC	Request For Comment – dokument normativního, doporučujícího, či informativního charakteru v konkrétní oblasti informačních technologií (protokoly, aplikace, mechanismy, dokumentace atd.) obecně uznávaný odbornou veřejností.
RootCA	Kořenová certifikační autorita (VIG Czech Republic - Root CA)

2. Odpovědnost za zveřejňování a úložiště informací a dokumentace

2.1. Úložiště informací a dokumentace

Autoritativním úložištěm pro informace a dokumentaci týkající se PKI VIG, tedy zejména certifikační politiky je úsek informačních technologií Kooperativa, pojišťovna, a.s. Vienna Insurance Group Autoritativním úložištěm pro publikování certifikátů certifikačních autorit, certifikátů uživatelů PKI a seznamů zneplatněných certifikátů je samotná certifikační autorita. Seznamy zneplatněných certifikátů jsou navíc publikovány také na webovém serveru.

2.2. Zveřejňování informací a dokumentace

Certifikáty certifikačních autorit jsou publikovány na adrese pki.vig.cz.

2.3. Periodicita zveřejňování informací

Seznamy zneplatněných certifikátů RootCA jsou publikovány v pravidelných časových intervalech (1 rok) a v případě zneplatnění kteréhokoli certifikátu CA.

Seznamy zneplatnění certifikátů InternalCA a ExternalCA jsou publikovány v pravidelných intervalech nejdéle však jednou za 3 dny.

2.4. Řízení přístupu k jednotlivým typům úložišť

Informace publikované certifikačními autoritami jsou přístupné všem správcům PKI. Těmito informacemi se rozumí certifikáty CA, seznamy zneplatněných certifikátů. Seznamy zneplatněných certifikátů jsou publikovány také na webovém serveru, kde jsou volně dostupné.

Změny a zápis těchto informací je omezen a řízen.

Přístup k bezpečnostní dokumentaci uložené a spravované úsek informačních technologií Kooperativa, pojišťovna, a.s. Vienna Insurance Groupje řízen interními procesy a platnou firemní legislativou.

3. Identifikace a autentizace

3.1. Pojmenování

3.1.1. Typy jmen

Všechny certifikáty vydávané PKI VIG obsahují jméno/název subjektu a název certifikační autority, která certifikát vydala. Pro tento účel jsou v certifikátu pole:

- `Subject` – vlastník certifikátu
- `Issuer` – certifikační autorita

3.1.1.1. Kořenová certifikační autorita

Pole `Issuer` i `Subject` v certifikátu RootCA jsou naplněny těmito atributy:

Atribut	Význam	Hodnota
`cn`	CommonName – rozlišovací jméno certifikační autority	VIG Czech Republic - Root CA
`dc`	DomainComponent	koop
`dc`	DomainComponent	int

3.1.1.2. Pořízená certifikační autorita pro interní uživatele

Pole `Issuer` v certifikátu InternalCA je naplněno těmito atributy:

Atribut	Význam	Hodnota
`cn`	CommonName – rozlišovací jméno certifikační autority	VIG Czech Republic - Root CA
`dc`	DomainComponent	koop
`dc`	DomainComponent	int

Pole `Subject` v certifikátu InternalCA je naplněno těmito atributy:

Atribut	Význam	Hodnota
`cn`	CommonName – rozlišovací jméno certifikační autority	VIG Czech Republic - Internal CA
`dc`	DomainComponent	koop
`dc`	DomainComponent	int

3.1.1.3. Pořízená certifikační autorita pro externí uživatele

Pole `Issuer` v certifikátu ExternalCA je naplněno těmito atributy:

Atribut	Význam	Hodnota
`cn`	CommonName – rozlišovací jméno certifikační autority	VIG Czech Republic - Root CA
`dc`	DomainComponent	koop
`dc`	DomainComponent	int

Pole `Subject` v certifikátu ExternalCA je naplněno těmito atributy:

Atribut	Význam	Hodnota
cn	CommonName – rozlišovací jméno certifikační autority	VIG Czech Republic - External CA
dc	DomainComponent	koop
dc	DomainComponent	int

3.1.1.4. Certifikáty koncových uživatelů

Pole `Issuer` je v certifikátu naplněno vždy údaji z InternalCA nebo ExternalCA.

Pole `Subject` je minimálně naplněno těmito údaji:

Atribut	Význam	Hodnota
cn	CommonName – rozlišovací jméno certifikační autority	Jméno a příjmení daného uživatele (případně s tituly)
o	Organization	Organizace uživatele
un	UnstructureName (oid 1.2.840.113549.1.9.2)	Číslo zaměstnance (u externistů jiné jednoznačné id)
c	Country	Země

Dále může `Subject` obsahovat tyto údaje:

Atribut	Význam	Hodnota
ou	OrganizationUnit	Organizační jednotka
t	Title	Pracovní titul (např. Manažer IT, Java developer, Účetní atd.)

Pro email uživatele se může volitelně vyskytnout v rozšíření `SubjectAltName`.

3.1.2. Požadavek na významovost jmen

Všechna jména a názvy uvedené v DN certifikátu musí být smysluplné a doložitelné.

3.1.3. Anonymita a používání pseudonymu

Používání pseudonymů v DN certifikátů není dovoleno. Všechny certifikáty vydávané certifikačními autoritami musí být přiřaditelné konkrétní certifikační autoritě. Vydávání anonymních certifikátů není dovoleno.

3.1.4. Pravidla pro interpretaci různých forem jmen

Z důvodu kompatibility s jinými subjekty v mezinárodním prostředí nejsou v certifikátech používány národní znakové sady. Všechna jména a názvy jsou uvedeny bez diakritických znamének.

3.1.5. Jedinečnost jmen

Jednoznačnost jmen je zajištěna prostřednictvím atributu `serialNumber`, který je vkládán do rozlišovacího jména (DN – distinguished name) a je plněn unikáním identifikátorem držitelem certifikátu.

3.1.6. Obchodní značky

Ve vydávaných certifikátech není povoleno používat názvy, které by mohly být obchodními značkami třetích stran. Všechny údaje v atributech `CN` (Common Name) a `subjectAltName` uvedené v certifikátu musí být vztažitelné k jeho držiteli.

3.2. Počáteční ověření identity

3.2.1. Metody dokazování vlastnictví soukromého klíče

RootCA - žádost o vydání a samotný akt vydání certifikátu probíhá vygenerováním žádosti u nově vznikající CA a ručním nahrání této žádosti na vydávající CA. Vlastnictví soukromého klíče je prokázáno podepsání dat žádosti soukromým klíčem.

InternalCA a ExternalCA – žádosti se generují na straně autorit.

3.2.2. Ověřování identity právnické osoby nebo organizační složky státu

Certifikáty nejsou vydávány organizačním složkám.

3.2.3. Ověřování identity fyzické osoby

Ověřování fyzických osob probíhá ve webovém portálu určeném k vydávání certifikátů na základě znalosti jména a hesla.

3.2.4. Neověřené informace vztahující se k držiteli certifikátu

Všechny informace v certifikátech vydávaných certifikačními autoritami PKI VIG jsou ověřené.

3.2.5. Ověřování specifických práv

Není aplikováno.

3.2.6. Kritéria pro interoperabilitu

Kořenová certifikační autorita (RootCA) smí navazovat vztahy důvěry s PKI jiných subjektů pouze na základě potvrzených vzájemných dohod.

3.3. Identifikace a autentizace při zpracovávání požadavků na výměnu párových dat

3.3.1. Identifikace a autentizace při rutinní výměně párových dat

RootCA - rutinní výměna klíčů probíhá procesem, který není automatizován, před koncem doby platnosti certifikátů CA. Výměna a autentizace je realizována stejně jako v případě vydání nového certifikátu.

InternalCA a ExternalCA - výměna a autentizace je realizována stejně jako v případě vydání nového certifikátu. Tedy ve webové aplikaci, kam se uživatelé autentizují jménem a heslem.

3.3.2. Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

Výměna klíčů po zneplatnění probíhá stejným procesem jako vydání nového certifikátu.

3.4. Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

RootCA – žádosti o zneplatnění certifikátu provádí bezpečnostní manažer dané podřízené CA.

InternalCA a ExternalCA - zneplatnit certifikát může každý uživatel ve webovém portálu (CzechIdMng), kam se autentizuje pomocí jména a hesla.

4. Požadavky na životní cyklus certifikátu

4.1. Žádost o vydání certifikátu

4.1.1. Subjekty oprávněné podat žádost o vydání certifikátu

RootCA - o vydání certifikátu smí žádat provozovatelé certifikačních autorit PKI VIG.

InternalCA - o vydání certifikátu smí požádat interní uživatel, který má patřičné oprávnění od svého garanta.

ExternalCA - o vydání certifikátu smí požádat externí uživatel, který má patřičné oprávnění od svého garanta.

4.1.2. Registrační proces a odpovědnosti poskytovatele a žadatele

Žádosti o certifikát jsou zpracovávány podle platného registračního procesu. Správnost údajů je zajištěna automatizovaným transferem informací z IDM na InternalCA nebo ExternalCA.

4.2. Zpracování žádosti o certifikát

4.2.1. Identifikace a autentizace

Informace o uživatelích jsou získávány z IDM.

4.2.2. Přijetí nebo zamítnutí žádosti o certifikát

Všechny žádosti z IDM jsou automaticky zpracovány. Schvalovací proces probíhá v IDM (konkrétně v CzechIdMng), kde uživatel může požádat svého garanta o právo k vydání certifikátu.

4.2.3. Doba zpracování žádosti o certifikát

Maximální doba zpracování žádosti není stanovena.

4.3. Vydání certifikátu

4.3.1. Úkony CA v průběhu vydávání certifikátu

Certifikáty jsou vydány automaticky.

4.3.2. Oznámení o vydání certifikátu držiteli certifikátu

Uživatelům je zaslán email s informací o vydání certifikátu.

4.4. Převzetí vydaného certifikátu

4.4.1. Úkony spojené s převzetím certifikátu

Převzetí vydaného certifikátu probíhá stažením certifikátu (s klíčem ve formátu pfx) z IDM.

4.4.2. Zveřejňování vydaných certifikátů poskytovatelem

Služba není poskytována.

4.4.3. Oznámení o vydání certifikátu jiným subjektům

Služba není poskytována.

4.5. Použití párových dat a certifikátu

4.5.1. Použití párových dat a certifikátu držitelem certifikátu

Podpisový pár klíčů uživatelů je používán k autentizaci k interním portálům a vytváření elektronického podpisu.

4.5.2. Použití párových dat a certifikátu spoléhající se stranou

Všechny vydané certifikáty obsahují rozšíření `keyUsage`, případně rozšíření `extendedKeyUsage`, která vymezuje použití klíče. Certifikáty musí být využívány pouze v souladu s nastavenými rozšířeními.

4.6. Obnova certifikátu

Službou obnovení certifikátu je v kontextu tohoto dokumentu myšleno obnovení již zneplatněného certifikátu a/nebo vydání následného certifikátu se stejnými daty pro ověřování elektronických podpisů a novou dobou platnosti.

4.6.1. Podmínky pro obnovení certifikátu

Služba obnovení certifikátu není poskytována.

4.6.2. Subjekty oprávněné požadovat obnovení certifikátu

Služba obnovení certifikátu není poskytována.

4.6.3. Zpracování požadavku na obnovení certifikátu

Služba obnovení certifikátu není poskytována.

4.6.4. Oznámení o vydání obnoveného certifikátu držiteli certifikátu

Služba obnovení certifikátu není poskytována.

4.6.5. Úkony spojené s převzetím obnoveného certifikátu

Služba obnovení certifikátu není poskytována.

4.6.6. Zveřejňování vydaných obnovených certifikátů poskytovatelem

Služba obnovení certifikátu není poskytována.

4.6.7. Oznámení o vydání obnoveného certifikátu jiným subjektům

Služba obnovení certifikátu není poskytována.

4.7. Výměna klíče v certifikátu

Služba není poskytována.

4.7.1. Podmínky pro výměnu klíče

Není aplikováno.

4.7.2. Subjekty oprávněné požadovat výměnu klíče v certifikátu

Není aplikováno.

4.7.3. Zpracování požadavku na výměnu klíče v certifikátech

Není aplikováno.

4.7.4. Oznámení o vydání certifikátu s vyměněným klíčem držiteli

Není aplikováno.

4.7.5. Úkony spojené s převzetím certifikátu s vyměněným klíčem

Není aplikováno.

4.7.6. Zveřejňování vydaných certifikátů s vyměněným klíčem

Není aplikováno.

4.7.7. Oznámení o vydání certifikátu s vyměněným klíčem jiným subjektům

Není aplikováno.

4.8. Změna údajů v certifikátu

Údaje jsou čerpány z IDM, kde probíhá i jejich změna. Samotná změna údajů v certifikátu není podporována.

4.8.1. Podmínky pro změnu údajů v certifikátu

Není aplikováno.

4.8.2. Subjekty oprávněné požadovat změnu údajů v certifikátu

Není aplikováno.

4.8.3. Zpracování požadavku na změnu údajů v certifikátu

Není aplikováno.

4.8.4. Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Není aplikováno.

4.8.5. Úkony spojené s převzetím certifikátu se změněnými údaji

Není aplikováno.

4.8.6. Zveřejňování vydaných certifikátů se změněnými údaji

Není aplikováno.

4.8.7. Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Není aplikováno.

4.9. Zneplatnění a pozastavení platnosti certifikátu

4.9.1. Podmínky pro zneplatnění certifikátu

Certifikáty jsou zneplatněny v případě, kdy hrozí, nebo došlo ke kompromitaci nebo ztrátě jejich soukromého podpisového klíče.

4.9.2. Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu smí požádat sám uživatel prostřednictvím CzechIdMng, nebo jeho Garant v IDM.

4.9.3. Požadavek na zneplatnění certifikátu

Požadavek je řízen revokačním procesem CA.

4.9.4. Doba odkladu požadavku na zneplatnění certifikátu

Tato doba není specifikována. Certifikáty jsou zneplatňovány neprodleně v souladu s revokačním procesem.

4.9.5. Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu

Žádost o zneplatnění certifikátu musí být zpracována bez prodlení.

4.9.6. Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn

Spoléhající se strana je povinna kontrolovat platnost všech certifikátů v certifikačním řetězci.

4.9.7. Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je vydáván jednou ročně pro RootCA.

InternalCA a ExternalCA vydávají seznamy nejdéle jednou za tři dny.

4.9.8. Maximální zpoždění při vydání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů jsou vydávány nejdéle jednou za tři dny.

4.9.9. Možnost ověření statutu certifikátu on-line (dále „OCSP“)

Služba není poskytována.

4.9.10. Požadavky při ověřování statutu certifikátu on-line

Služba není poskytována.

4.9.11. Jiné způsoby oznamování zneplatnění certifikátů

Služba není poskytována.

4.9.12. Případné odlišnosti postupu zneplatnění v případě kompromitace dat

V tomto případě nejsou žádné odlišnosti od standardních postupů.

4.9.13. Podmínky pro pozastavení platnosti certifikátu

Služba není poskytována.

4.9.14. Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Není aplikováno.

4.9.15. Zpracování požadavku na pozastavení platnosti certifikátu

Není aplikováno.

4.9.16. Omezení doby pozastavení platnosti certifikátu

Není aplikováno.

4.10. Služby související s ověřováním statutu certifikátu

4.10.1. Funkční charakteristiky

Tato služba je poskytována prostřednictvím vystavení CRL na webu.

4.10.2. Dostupnost služeb

Není definováno.

4.10.3. Další charakteristiky služeb statutu certifikátu

Nejsou definovány.

4.11. Ukončení poskytování služeb pro držitele certifikátu

Služba je ukončena doručením žádosti o ukončení, kterou podává Garant ? organizačního celku CA. Je-li důvodem ukončení služby zároveň důvod k revokaci, jsou certifikáty CA zneplatněny. O této skutečnosti jsou držitelé certifikátů informováni pomocí emailu.

4.12. Úschova privátního klíče u důvěryhodné třetí strany a jejich obnova

Služba úschovy soukromého podpisového klíče u třetí osoby není poskytována.

4.12.1. Politika a postupy při úschově a obnovování privátního klíče a certifikátu

Není aplikováno.

4.12.2. Politika a postupy při zapouzdřování a obnovování šifrovacího klíče pro relaci

Tato služba není poskytována.

5. Management, provozní a fyzická bezpečnost

5.1. Fyzická bezpečnost

5.1.1. Umístění a konstrukce

5.1.2. Fyzický přístup

Lokalita, kde jsou umístěny certifikační autority, je chráněna strážní službou. Vstup do objektu je povolen pouze na základě identifikačního průkazu.

Přístup do prostoru, kde jsou umístěny certifikační autority je řízený. Vstup do chráněné oblasti je omezen pouze na oprávněné osoby. K autorizaci je využívána identifikační karta.

Návštěva a pohyb návštěv v objektu je povolen pouze v doprovodu oprávněné osoby po ověření totožnosti

Infrastruktura certifikační autority je náležitě fyzicky zabezpečena. Konkrétní požadavky na fyzickou bezpečnost prostor, kde jsou umístěny technické prvky certifikační autority jsou specifikovány v interní legislativě společnosti.

5.2. Procesní bezpečnost

5.2.1. Důvěryhodné role

Pracovní náplně v rámci infrastruktury veřejných klíčů certifikačních autorit jsou přiděleny několika odděleným rolím. Rozdělení funkcí mezi role vychází z požadavku oddělení jednotlivých oblastí činnosti, s omezením možnosti zneužití systému. Jednotlivé funkce mohou být rozděleny mezi více pracovníků.

Všechny role v tomto výčtu jsou označovány jako důvěryhodné. Vlastník aplikace (PKI) je zodpovědný za dostupnost takového počtu pracovníků v konkrétní roli, aby byl zajištěn bezproblémový provoz a odpovídající kvalita poskytovaných služeb.

CA Administrator - úkolem této role je správa certifikační autority na „systémové úrovni" (definice a změny hesel systémových a aplikačních účtů, bezpečný start služeb, zálohování, obnova a validace databází, …).

Certificate Manager (CA Officer) - role Certificate Manager je zodpovědná za vydávání a revokaci certifikátů. Dále je zodpovědná za správu bezpečnostních parametrů a politik prostředí PKI. Jejím úkolem je udržovat soulad prostředí s platnou certifikační politikou.

Auditor - tato role dohlíží na provoz infrastruktury. Nemá žádnou výkonnou pravomoc.

5.2.2. Počet osob požadovaných na zajištění jednotlivých činností

K provedení operací, které jsou označeny jako bezpečnostně senzitivní, je podle povahy operace nutná přítomnost dvou až tří osob.

5.2.3. Identifikace a autentizace pro každou roli

Role jsou identifikováni uživatelským jménem a heslem.

5.2.4. Role vyžadující rozdělení povinností

Modely rolí pro obě certifikační autority PKI VIG jsou nastaveny tak, aby nedocházelo ke kumulaci pravomocí.

Každá z certifikačních autorit obsazuje vlastní model rolí.

5.3. Personální bezpečnost

5.3.1. Požadavky na kvalifikaci, zkušenosti a bezúhonnost

U každého pracovníka, který bude zařazen do role správy nebo dohledu PKI VIG musí být zkoumána jeho způsobilost pro vykonávání povinností vyplývajících z této role.

5.3.2. Posouzení způsobilosti osob

Před obsazením pracovníka do klíčové role správy PKI VIG musí být posouzena jeho způsobilost.

V rámci posuzování vhodnosti pracovníka pro konkrétní roli může být i požadavek na prokázání bezúhonnosti. Ta je posuzována podle výpisu z rejstříku trestů.

V souladu se zavedenými postupy pro nábor zaměstnanců každý pracovník poskytuje informace v průběhu vstupního osobního pohovoru. Pro doplnění informací, jejich ověření a aktualizaci mohou být prováděny další pohovory s odpovědnými pracovníky.

5.3.3. Požadavky na přípravu pro výkon role, vstupní školení

Všichni pracovníci, podílející se na provozu, správě, údržbě a rozvoji systémů PKI VIG, jsou vyškoleni. Součástí školení je i školení o bezpečnosti systému a o chování v havarijních situacích.

5.3.4. Požadavky a periodicita školení

S implementací nových vlastností PKI musí pracovníci v rolích správy projít školením, kde jsou seznámeni s těmito vlastnostmi. Dále jsou povinni v rámci přidělené role udržovat a zvyšovat svoji kvalifikaci.

5.3.5. Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Výměny osob mezi jednotlivými rolemi (přestupy z role do role) nejsou prováděny.

5.3.6. Postihy za neoprávněné činnosti zaměstnanců

Všechny neautorizované operace provedené pracovníky v rolích správy jsou považovány za bezpečnostní incident. Jsou řešeny odpovídajícím způsobem.

5.3.7. Požadavky na nezávislé zhotovitele (dodavatele)

Na smluvní (externí) pracovníky, jejichž činnost souvisí s PKI VIG, jsou uplatňována obdobná kritéria jako na zaměstnance VIG.

5.3.8. Dokumentace poskytovaná zaměstnancům

Zaměstnancům je poskytována pouze dokumentace, která je nezbytná pro vykonávání činností vyplývajících z pracovní náplně.

5.4. Auditní záznamy (logy)

5.4.1. Typy zaznamenávaných událostí

Všechny certifikační autority zaznamenávají informace o všech operacích provedených správci, informace o stavu a provozu systému a služeb a o periodicky prováděných automatických operacích.

5.4.2. Periodicita zpracování záznamů

Auditní logy jsou zpracovávány při podezření, nebo po bezpečnostním incidentu.

Auditní záznamy jsou kontrolovány osobami v odpovídající roli pověřené tímto úkolem.

5.4.3. Doba uchování auditních záznamů

Auditní záznamy jsou uchovávány po minimální dobu 3 let.

5.4.4. Ochrana auditních záznamů

Přístup k auditním logům certifikačních autorit je řízen. Log je mechanismy certifikační autority chráněn proti modifikaci.

5.4.5. Postupy pro zálohování auditních záznamů

Auditní logy jsou součástí záloh dat certifikačních autorit.

5.4.6. Systém shromažďování auditních záznamů (interní nebo externí)

V rámci implementace není řešen.

5.4.7. Postup při oznamování události subjektu, který ji způsobil

Není poskytováno.

5.4.8. Hodnocení zranitelnosti

Všechna závažná porušení bezpečnosti jsou okamžitě eskalována odpovědné osobě, nebo organizační složce.

5.5. Uchovávání informací a dokumentace

5.5.1. Typy informací a dokumentace, které se uchovávají

V rámci provozu certifikační autority jsou archivovány informace pro účely auditu, výsledky provedených auditů a dokumentace registračního procesu.

5.5.2. Doba uchování uchovávaných informací a dokumentace

Všechna data jsou v archivu uchovávána po dobu nejméně 3 let.

5.5.3. Ochrana úložiště uchovávaných informací a dokumentace

Data a dokumenty v archivu jsou chráněny způsobem odpovídajícím jejich bezpečnostní citlivosti a významu. Mechanismy a procesní opatření jsou předmětem interních předpisů upravujících problematiku archivů.

5.5.4. Postupy při zálohování uchovávaných informací a dokumentace

Uchovávané informace jsou zálohovány pro potřeby obnovy v případě havárie v souladu s interními postupy.

5.5.5. Požadavky na používání časových razítek při uchovávání informací a dokumentace

Celá infrastruktura je synchronizována dle přesného času založeného na UTC. Všechny auditní záznamy v sobě nesou informaci o čase, ve kterém byly pořízeny. Pro označování není využíváno služby časových razítek.

5.5.6. Systém shromažďování uchovávaných informací a dokumentace (interní nebo externí)

Archivní kopie jsou ukládány v souladu s jejich bezpečnostní úrovní.

5.5.7. Postupy pro získání a ověření uchovávaných informací a dokumentace

Archivní záznamy zpřístupňuje vedoucí CA spolu s auditorem.

5.6. Výměna veřejného klíče v nadřízeném systémovém certifikátu poskytovatele

Výměna veřejného klíče v certifikátu CA je v případě standardních situací (uplynutí platnosti certifikátu) s dostatečným časovým předstihem (minimálně jeden rok před uplynutím doby platnosti tohoto certifikátu) prováděna formou vydání nového certifikátu. V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, že by mohla být ohrožena bezpečnost procesu tvorby elektronických podpisů, resp. značek, tzn. změny kryptografických algoritmů, délky klíčů, atd.) je tato činnost prováděna v adekvátním časovém období.

5.7. Obnova po havárii nebo kompromitaci

5.7.1. Postup v případě incidentu a kompromitace

Postupy a chování v případě bezpečnostního incidentu nebo havárie jsou upraveny v havarijním plánu obnovy.

5.7.2. Poškození výpočetních prostředků, softwaru nebo dat

V případě poškození kterékoli z komponent, na kterých je poskytována služba PKI, se postupuje dle scénářů uvedených havarijním plánu obnovy.

5.7.3. Postup při kompromitaci privátního klíče CA

Dojde-li k prozrazení soukromého klíče certifikační autority, je tento klíč bez prodlení zneplatněn a informace o zneplatnění je publikována v CRL. V tomto okamžiku přestávají platit všechny certifikáty vydané touto CA.

Po zneplatnění jsou informováni správci všech podřízených certifikačních autorit (v případě RootCA).

5.7.4. Schopnost obnovit činnost po havárii

Postupy pro zotavení po havárii jsou uvedeny v dokumentu plán obnovy.

5.8. Ukončení činnosti CA nebo RA

Infrastruktura veřejných klíčů slouží jako technologická platforma zejména pro ochranu citlivých informací. K ukončení provozu PKI tedy může dojít z důvodu změny v technologii služeb, které ochranu zajišťují, nebo v důsledku přechodu PKI na jinou platformu.

Provoz může být ukončen také z důvodu převzetí závazků této certifikační autority jinou autoritou.

Uživatelé a subjekty, s nimiž má certifikační autorita nastaven vztah důvěry, jsou informováni 3 měsíce před ukončením činnosti. Toto ustanovení je platné pro všechny certifikační autority (RootCA, InternalCA a ExternalCA).

6. Technická bezpečnost

6.1. Generování a instalace párových dat

Podpisový pár klíčů certifikačních autorit jsou generovány v bezpečném hardwarovém modulu. Klíče uživatelských certifikátů jsou generovány na straně InternalCA a ExternalCA.

6.1.1. Generování párových dat

Klíčové páry certifikačních autorit v hierarchii CA VIG CZ jsou generovány a uloženy v hardwarovém kryptografickém modulu splňujícím požadavky FIPS 140-2. Generování těchto klíčových párů probíhá kontrolovaným procesem, na jehož průběh dohlíží Certificate Manager a CA Auditor.

Klíčové páry jednotlivých komponent nebo systémů CA VIG CZ (infrastrukturní klíče) jsou generovány v kontrolovaném prostředí systémů VIG CZ. Tyto klíčové páry jsou uloženy v kryptografickém modulu; pro přístup k těmto klíčovým párům je nutné vložit čipovou kartu obsluhy a zadat PIN.

Klíčové páry operátorů VIG CA CZ jsou generovány ve vyhrazených čipových kartách, které svou konstrukcí neumožňují export soukromých klíčů. Pro použití soukromých klíčů je vždy nutné zadat PIN. Čipové karty jsou následně předány operátorům.

6.1.2. Předání privátního klíče vlastníkovi

Certifikáty (s privátními klíči ve formě pfx) jsou předány uživatelům přes CzechIdMng.

6.1.3. Předání veřejného klíče certifikační autoritě

Veřejné klíče jsou vytvářeny na straně CA a není potřeba je předávat.

6.1.4. Poskytování veřejného klíče spoléhajícím se stranám

Služba není poskytována.

6.1.5. Délky párových dat

Délky klíčů jsou nastaveny s ohledem na doporučení mezinárodních organizací a s ohledem na aktuální metody útoků na klíčový materiál kryptoanalytickými metodami.

Všechny klíče certifikačních autorit mají délku 4096b (RSA algoritmus) a všechny veřejné klíče uživatelů mají délku 2048b (RSA algoritmus).

6.1.6. Generování veřejných klíčů a kontrola jejich kvality

Parametry veřejného klíče jsou nastaveny přímo na CA.

6.1.7. Omezení pro použití párových dat

Použití párových dat v uživatelských certifikátech je omezeno na digitální podpis a verifikaci digitálně podepsaných dat v případě, kdy je digitální podpis použit jako důkaz pravosti dat. Párová data nelze použít k podpisu certifikátů a CRL.

6.2. Ochrana privátních klíčů a bezpečnost kryptografických modulů

6.2.1. Standardy a podmínky používání kryptografických modulů

Kryptografický modul použitý pro generování a úschovu soukromého klíče certifikačních autorit (nástroj pro vytváření elektronického podpisu) působících v hierarchii VIG CA CZ splňuje požadavky standardu FIPS 140-2 Level 3.

6.2.2. Sdílení tajemství

Soukromý klíč certifikační autority je během provozu uložen v aktivovaném a konfigurovaném kryptografickém modulu (nástroji pro vytváření elektronického podpisu), k jehož zapnutí a vypnutí postačuje jedna osoba.

K aktivování kryptografického modulu (nástroje pro vytváření elektronického podpisu) a k obnově soukromého klíče po havárii (případně v jiném kryptografickém modulu) je zapotřebí součinnosti několika, minimálně však dvou osob.

6.2.3. Úschova privátních klíčů

Není aplikováno.

6.2.4. Zálohování privátních klíčů

Soukromý klíč certifikační autority je zálohován v zašifrované formě; k šifrování je použit symetrický algoritmus AES. Zašifrované klíče jsou uložené na pevném disku zařízení obsahujícího příslušný kryptografický modul. Zálohovat tyto klíče může jedna osoba; obnovit do aktivovaného modulu, ze kterého zálohy pocházejí, také.

Při obnově zálohovaných klíčů do nového nebo inicializovaného modulu je zapotřebí součinnosti minimálně dvou osob.

6.2.5. Uchovávání privátních klíčů

Není aplikováno.

6.2.6. Transfer privátních klíčů do kryptografického modulu nebo z kryptografického modulu

Soukromý klíč certifikační autority je generován v kryptografickém modulu (bezpečném kryptografickém modulu) a veškeré operace s nezašifrovaným klíčem se provádějí pouze v tomto modulu. Klíč opouští kryptografický modul pouze na zálohách v zašifrované podobě.

Klíč je do původního kryptografického modulu vkládán se záloh po autentizaci jednoho pracovníka s přístupem k zálohám klíčů a ke kryptografickému modulu.

Klíč je do nového nebo inicializovaného kryptografického modulu vkládán se záloh po autentizaci dvou pracovníků, kteří nemají přístup k záloze soukromého klíče a kteří nemají právo na aktivaci soukromého klíče (spuštění procesu certifikační autority).

6.2.7. Uložení privátních klíčů v kryptografickém modulu

Soukromý klíč certifikační autority je během provozu uložen v nezašifrovaném tvaru v aktivovaném a konfigurovaném kryptografickém modulu (bezpečném kryptografickém modulu), k jehož zapnutí a vypnutí postačuje jedna osoba.

K aktivování kryptografického modulu (bezpečného kryptografického modulu) a k obnově soukromého klíče po havárii (případně v jiném kryptografickém modulu) je zapotřebí součinnosti několika, minimálně však dvou osob.

6.2.8. Postup při aktivaci privátních klíčů

Soukromý podepisovací klíč certifikační autority je aktivován autorizovanou obsluhou v souladu se provozními a bezpečnostními procedurami. Postup při deaktivaci privátních klíčů

6.2.9.

Soukromý podepisovací klíč certifikační autority je deaktivován automaticky příslušnou certifikační autoritou.

6.2.10. Postup při zničení privátních klíčů

Soukromý klíč certifikační autority uložený v HSM modulu je zničen prostředky poskytovanými HSM modulem v případě ukončení činnosti certifikační autority, jejíž klíče jsou v HSM modulu uloženy. Toto zničení soukromého klíče se provádí autorizovanou obsluhou na základě požadavku role Certificate Manager.

Zničení soukromého klíče je provedeno uvedením HSM do inicializovaného stavu, kdy je pomocí mechanismů HSM bezpečně vymazán veškerý kryptografický materiál (včetně soukromého klíče CA). Zničení soukromého klíče zahrnuje i smazání zálohovaných kopií klíčů a deaktivaci karet použitých pro přístup ke klíčům.

6.2.11. Hodnocení kryptografického modulu

Vzhledem ke skutečnosti, že kryptografický modul užívaný k úschově soukromého klíče certifikační autority úspěšně prošel hodnocením podle standardu FIPS 140–2 na úroveň 3, nepředpokládá se, že by obsahoval závažné chyby na úrovni designu zařízení. Přesto se průběžně sleduje, zda nebyl objeven útok na toto zařízení, aby bylo možné včas na takové ohrožení reagovat.

6.3. Další aspekty správy párových dat

6.3.1. Uchovávání veřejného klíče

Archivace veřejných klíčů je prováděna prostředky certifikační autority.

6.3.2. Maximální doba platnosti vydávaného certifikátu

Platnost certifikátu RootCA je 20 let. Platnost certifikátů InternalCA a ExternalCA je 10 let. Platnost uživatelských certifikátů je 18 měsíců.

6.4. Aktivační data

6.4.1. Generování a instalace aktivačních dat

Není aplikováno.

6.4.2. Ochrana aktivačních dat

Není aplikováno.

6.4.3. Ostatní aspekty aktivačních dat

Není aplikováno.

6.5. Počítačová bezpečnost

6.5.1. Specifické technické požadavky na počítačovou bezpečnost

Všechny změny v prostředí poskytování služby musí být prověřeny mimo produkční prostředí. Před nasazením jsou přezkoumány všechny dopady na stávající službu vydávání a správy certifikátů.

Systémy a síťové prvky, z nichž je infrastruktura složena (serverová část služby), jsou předmětem bezpečnostních kontrol. Na operační systémy jsou v případě výskytu bezpečnostní nebo jiné chyby potenciálně ohrožující provoz a důvěrnost služby aplikovány opravy.

Aplikace opravných balíků se řídí standardními mechanismy. Tedy před aplikací musí být vyhodnoceny dopady na provoz a balík prověřen v testovacím prostředí.

6.5.2. Hodnocení počítačové bezpečnosti

Prostředí slouží pro interní potřebu VIG a nepracuje s informacemi ve smyslu zák. č. 412/2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti.

6.6. Bezpečnost životního cyklu

6.6.1. Řízení vývoje systému

Vývoj systému služeb PKI probíhal v souladu se standardními metodikami pro zajištění vývoje a řízení kvality.

6.6.2. Kontroly řízení bezpečnosti

PKI VIG je vybudováno na komponentách, jež umožňují řízení a kontroly řízení bezpečnosti jednotlivých činností prováděných systémem a správci.

6.6.3. Řízení bezpečnosti životního cyklu

Celý životní cyklus systému služby PKI VIG je řízen tak, aby byl v souladu s požadavky relevantní legislativy České republiky. Všechny činnosti probíhají v souladu s touto certifikační politikou, bezpečnostními politikami a provozní dokumentací služby.

6.7. Síťová bezpečnost

Infrastruktura je rozdělena do segmentů podle senzitivity jednotlivých komponent. Mezi segmenty je provoz omezen a řízen bezpečnostní bránou. Konkrétní implementovaná opatření jsou předmětem provozní a konfigurační dokumentace.

6.8. Časová razítka

Všechny auditní informace produkované certifikační autoritou, vydané certifikáty, seznamy zneplatněných certifikátů, ale také informace v bezpečnostní databázi CA jsou opatřeny časovým údajem, ale samotná časová razítka nejsou využívána.

7. Profily certifikátů, seznamu zneplatněných certifikátů a OCSP

7.1. Profil certifikátu

Všechny certifikační autority vydávají certifikáty pro certifikační autority v souladu s normou ISO/IEC 9594-8 (X.509) a RFC 3280.

Délka klíče certifikačních autorit je 4096 bitů.

Délka klíče uživatelských certifikátů je 2048 bitů.

Certifikáty vydávané certifikační autoritami obsahují tyto základní atributy:

Atribut	Hodnota	Význam
Version	3	Verze certifikátu dle X.509
Serial Number	Unikátní číslo	Číslo certifikátu
Signature Algorithm	Podpisový algoritmus	Algoritmus, který je použit pro podpis certifikátu
Issuer	Viz kap. 3.1.1 Typy jmen	DN certifikační autority
Validity – Not Before	Datum a čas dle RFC3280	Začátek platnosti certifikátu
Validity – Not After	Datum a čas dle RFC3280	Konec platnosti certifikátu
Subject	DN dle X.501	jméno/název držitele certifikátu
Signature	Podpis CA	Podpis certifikační autority, která certifikát vydala.

A informace o veřejném klíči

Atribut	Hodnota	Význam
Public Key Algorithm	rsaEncryption	Algoritmus veřejného klíče
RSA Public Key	Hodnota veřejného klíče	Veřejný klíč

7.1.1. Číslo verze

Certifikáty jsou vydávány v souladu s normou ve formátu X.509 verze 3.

7.1.2. Rozšiřující položky v certifikátu

V certifikátech vydávaných uživatelů a zařízením obsahují tato povolená rozšíření:

Extenze	Význam	Povinné
X509v3 Key Usage	Povolené použití certifikátu, viz dále.	Ano
X509v3 CRL Distribution Points	URI distribučního místa seznamů zneplatněných certifikátů (CRL) v notaci X.500	Ano
X509v3 Authority Key Identifier	Otisk klíče CA, která certifikát podepsala	Ano

Extenze	Význam	Povinné
X509v3 Subject Key Identifier	Otisk veřejného klíče	Ano

Nastavení kritičnosti a hodnoty rozšíření odpovídají RFC3280.

7.1.2.1. KeyUsage

Certifikáty certifikačních autorit obsahují minimálně tyto atributy:

5	keyCertSign	Klíče jsou využívány pro podepisování certifikátů.
6	cRLSign	Klíče jsou využívány pro podepisování seznamů zneplatněných certifikátů.

Certifikáty uživatelů obsahují minimálně tyto atributy:

0	digitalSignature	Klíče jsou využívány pro digitální podpis (nevztahuje se na podpis certifikátů a CRL).
1	nonrepudiation	Klíče jsou využívány pro verifikaci digitálně podepsaných dat v případě, kdy je digitální podpis použit jako důkaz pravosti dat (nevztahuje se na podpis certifikátů a CRL).

7.1.2.2. Basic Constraints

Certifikační autority mají nastavenu extenzi basicConstraints hodnotou CA: TRUE.

Uživatelské certifikáty mají nastavenou extenzi basicConstraints hodnotou CA: FALSE.

7.1.3. Objektové identifikátory (dále „OID“) algoritmů

Certifikáty jsou vydávány s algoritmy s OID odpovídajícími RFC 3370.

7.1.4. Způsoby zápisu jmen a názvů

Problematika zápisu jmen a názvů je upravena v kap. 3.1.

7.1.5. Omezení jmen a názvů

V certifikátech je povoleno použití pouze smysluplných jmen. Není dovolenou používání vulgarismů, pseudonymů a názvů, které mohou být v rozporu se zákony nebo mohou být registrovanou ochrannou známkou.

7.1.6. OID certifikační politiky

Identifikátor certifikační politiky není definován a využíván. V certifikátu není uveden.

7.1.7. Rozšiřující položka „Policy Constraints“

Tato extenze není využívána.

7.1.8. Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „Policy Qualifiers“

Identifikátor certifikační politiky není definován a využíván. V certifikátu není uveden.

7.1.9. Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Identifikátor certifikační politiky není definován a využíván. V certifikátu není uveden.

7.2. Profil seznamu zneplatněných certifikátů

Seznamy zneplatněných certifikátů publikované certifikačními autoritami obsahují následující informace:

Atribut	hodnota	význam
Version	2	Verze CRL
Signature Algorithm	Podpisový algoritmus	Algoritmus, který je použit pro podpis CRL
Issuer	Název CA	DN certifikační autority
Last Update	Časový údaj v GMT	Okamžik vydání CRL
Next Update	Časový údaj v GMT	Okamžik vydání další aktualizace CRL
CRL extensions	Viz kap 7.2.2	Rozšíření obsažená v CRL
Revoked Certificates	Viz kap 7.2.2	Záznamy zneplatněných certifikátů

Seznamy zneplatněných certifikátů obsahují následující rozšíření (CRL Extension):

Rozšíření	hodnota	význam
X509v3 CRL Number	číslo	Pořadové číslo CRL
X509v3 Authority Key Identifier	Otisk klíče	Otisk klíče certifikační autority, která vydala CRL

7.2.1. Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány v souladu s normami ve verzi 2.

7.2.2. Rozšiřující položky CRL a záznamů v CRL

Záznam o zneplatnění v CRL obsahuje následující atributy a rozšíření:

Atribut	hodnota	význam
Serial Number	číslo	sériové číslo certifikátu
Revocation Date	Datum a časový údaj v GMT	okamžik kdy byl certifikát zneplatněn
CRL entry extensions	Viz následující tabulka	Rozšíření záznamu

Každý záznam o zneplatnění obsahuje následující rozšíření:

Rozšíření	hodnota	význam
X509v3 CRL Reason Code	Řetězec	Důvod proč byl certifikát zneplatněn
Invalidity Date	Datum a časový údaj v GMT	Pokud je důvodem kompromitace klíčů, pak je obsaženo v rozšíření specifikující poslední známou dobu kdy byl certifikát ještě validní.

7.3. Profil OCSP

Služba online ověřování stavu certifikátu není poskytována.

7.3.1. Číslo verze

Služba online ověřování stavu certifikátu není poskytována.

7.3.2. Rozšiřující položky OCSP

Služba online ověřování stavu certifikátu není poskytována.

8. Hodnocení shody a jiná hodnocení

8.1. Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Pro zajištění definované úrovně bezpečnosti infrastruktury a tím i vysoké kvality poskytovaných služeb, je prováděna pravidelná kontrola shody.

Při každé změně HW a SW vybavení, na kterém jsou služby poskytovány, musí být zkoumán dopad změn na bezpečnost a kvalitu služeb.

Všechny tyto pravidelné audity a kontroly mohou být podle potřeby doplněny další kontrolou.

ti.

8.2. Vztah hodnotitele k hodnocenému subjektu

Pravidelná kontrola provozu je prováděna interními pracovníky VIG.

8.3. Postup v případě zjištění nedostatků

Všechny zjištěné nedostatky jsou komunikovány. Podle charakteru nedostatku jsou naplánovány a provedeny činnosti technologického (konfigurační změny, implementace dalších technologických opatření atd.) charakteru a/nebo doplněna a aktualizována relevantní dokumentace tak, aby byl nedostatek odstraněn.

9. Ostatní obchodní a právní záležitosti

9.1. Poplatky

Poplatky za služby nejsou uplatňovány.

9.1.1. Poplatky za vydání nebo obnovení certifikátu

Není aplikováno.

9.1.2. Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

Není aplikováno.

9.1.3. Poplatky za informaci o statutu certifikátu nebo o zneplatnění certifikátu

Není aplikováno.

9.1.4. Poplatky za další služby

Není aplikováno.

9.1.5. Jiná ustanovení týkající se poplatků (vč. refundací)

Není aplikováno.

9.2. Finanční odpovědnost

Není aplikováno.

9.2.1. Krytí pojištěním

Není aplikováno.

9.2.2. Další aktiva a záruky

Není aplikováno.

9.2.3. Pojištění nebo krytí zárukou pro koncové uživatele

Není aplikováno.

9.3. Citlivost obchodních informací

9.3.1. Výčet citlivých informací

Za důvěrné jsou považovány následující informace:

- privátní podpisový klíč certifikační autority – je zpřístupněn definovaným postupem a způsobem pouze certifikační autoritě prostřednictvím přístupových funkcí rozhraní
- auditní záznamy certifikační autority – nejsou určeny pro zveřejnění mimo organizaci, pokud to nevyžadují zákonné normy nebo jiné předpisy
- výsledky auditů infrastruktury – jsou považované za informace důvěrného charakteru obecně. Přístup je umožněn pouze definované skupině osob.
- bezpečnostní dokumentace, procesní dokumentace pro správu infrastruktury, plán pro zvládání krizových situací a plán obnovy – jsou zpřístupněny pouze konkrétní skupině osob obsazené v rolích správy

Nakládání s těmito informacemi je limitováno. Smějí být zveřejněny pouze v souladu s touto politikou, nebo zákonnými normami České republiky. Důvěrné informace jsou chráněny technickými a administrativními prostředky a jejich zveřejnění mimo povolenou mez je považováno za hrubé porušení této politiky, případně dalších souvisejících předpisů.

9.3.2. Informace mimo rámec citlivých informací

Informace v certifikátech, seznamy zneplatněných certifikátů, důvod zneplatnění a další informace, které nejsou označeny jako důvěrné, obecně nejsou za důvěrné považovány a smějí být sděleny nebo zveřejněny.

9.3.3. Odpovědnost za ochranu citlivých informací

Zaměstnanec, který nakládá s údaji a informacemi uvedenými v kap. 9.3.1 Výčet citlivých informací je zodpovědný za jejich ochranu. Tyto informace nesmí být poskytnuty třetí straně bez souhlasu vlastníka PKI VIG.

9.4. Ochrana osobních údajů

9.4.1. Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je řešena v souladu s požadavky příslušných zákonných norem.

9.4.2. Osobní údaje

Osobními informacemi jsou veškeré osobní údaje uživatelů či pracovníků podléhající ochraně ve smyslu příslušných zákonných norem.

9.4.3. Údaje, které nejsou považovány za citlivé

Osobní informace nepovažované za citlivé jsou zejména informace pracovního charakteru jako čísla služebních telefonů, názvy funkcí, služební e-mailové adresy apod., pokud nejsou jiným platným interním předpisem explicitně považována za citlivé.

9.4.4. Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů odpovídají pracovníci, kteří s těmito údaji přímo pracují a dále správci certifikačních autorit.

9.4.5. Oznámení o používání důvěrných informací a souhlas s používáním citlivých informací

Problematiky oznamování o používání důvěrných informací a souhlasu s používáním citlivých informací je řešena v souladu s požadavky příslušných zákonných norem.

9.4.6. Jiné okolnosti zpřístupňování osobních údajů

V případě zpřístupňování osobních údajů je postupováno dle požadavků příslušných zákonných norem.

9.5. Práva duševního vlastnictví

Soukromé a veřejné klíče jsou vlastnictvím subjektu, který je vytvořil. Takové vlastnictví vzniká a je platné pouze na základě platných předpisu a vztahů popsaných v předpisové základně společnosti, pracovní smlouvě či jejich dodatcích apod.

9.6. Zastupování a záruky

9.6.1. Zastupování a záruky CA

Podepsáním a vydáním certifikátu uživateli certifikační autorita zaručuje, že byly dodrženy všechny postupy a procesy související s tímto aktem. Certifikační autorita zaručuje, že byla dodržena všechna související ustanovení certifikační politiky a prováděcí směrnice a že vydaný certifikát, je spojen s certifikační autoritou, které byl vydán.

9.6.2. Zastupování a záruky RA

Není aplikováno.

9.6.3. Zastupování a záruky držitele certifikátu, podepisující nebo označující osoby

Vlastník certifikátu zaručuje, že jeho identifikační údaje uvedené v certifikátu jsou pravdivé. Rovněž musí zajistit svou bezvýhradnou kontrolu nad použitím privátního klíče příslušného k danému certifikátu určenému k digitálnímu podepisování a autentizaci.

9.6.4. Zastupování a záruky spoléhajících se stran

Není aplikováno.

9.6.5. Zastupování a záruky ostatních zúčastněných subjektů

Není aplikováno.

9.7. Zřeknutí se záruk

Není aplikováno.

9.8. Omezení odpovědnosti

Za provoz a bezpečnost certifikačních autorit odpovídají jejich správci a bezpečnostní manažer VIG.

9.9. Odpovědnost za škodu, náhrada škody

V případě, že vznikne škoda nebo podezření na škodu, je VIG oprávněn uvedenou skutečnost vyšetřit v souladu s příslušnou interní předpisovou základnou.

9.10. Doba platnosti, ukončení platnosti

9.10.1. Doba platnosti

Certifikační politika zůstává v platnosti do doby, než vyprší poslední certifikát, který byl na jejím základě vydán. Aktualizace ustanovení certifikační politiky nahrazují ustanovení neplatná.

9.11. Komunikace mezi zúčastněnými subjekty

Komunikace mezi certifikačními autoritami se řídí interními směrnicemi.

9.12. Změny

9.12.1. Postup při oznamování změn

Změny v této certifikační politice jsou oznamovány formou aktualizace dokumentu v úložišti, případně zveřejněním na intranetovém portále.

9.12.2. Okolnosti, při kterých musí být změněn OID

Není aplikováno.