S M 0 0 0 7 7 3

Certifikační politika a prováděcí směrnice pro oblast PKI a služeb Certifikační autority CETIN

Účel:

Dokument definuje požadavky společnosti CETIN na výdej a správu certifikátů pro systémy podporující PKI.

Působnost:

Směrnice je závazná pro všechny zaměstnance společnosti CETIN, osoby činné pro společnost na základě dohod o pracích konaných mimo pracovní poměr a pro všechny další subjekty, které jsou smluvně zavázány směrnici respektovat.

Proces:

Řízení a zajišťování bezpečnosti

Garant dokumentu		Vlastník procesu		Schvalovatel	
Vondruška Pavel		Rivola Pavel		Šedivý Juraj	
Datum	*Podpis*	*Datum*	*Podpis*	*Datum*	*Podpis*

OBSAH:

1 ÚVODNÍ USTANOVENÍ

1.1 Účel

Dokument "Certifikační politika a prováděcí směrnice pro oblast PKI a služeb Certifikační autority CETIN" (dále jen Certifikační politika nebo zkráceně CP) definuje požadavky společnosti CETIN na výdej a správu certifikátů pro systémy podporující PKI.

Stanovuje soubor požadavků a popis jejich implementace vztahující se k činnostem, povinnostem a závazkům všech subjektů, které přímo či nepřímo přicházejí do styku s certifikačními službami, nebo jsou na nich závislé.

Cílem je nastavení procesní důvěry v certifikáty vydávané v rámci budovaného systému PKI ve společnosti.

1.2 Působnost

Směrnice je v celém rozsahu závazná pro všechny zaměstnance společnosti CETIN, osoby činné pro společnost na základě dohod o pracích konaných mimo pracovní poměr a pro všechny další subjekty, které jsou smluvně zavázány směrnici respektovat (dále jen zaměstnanci).

1.3 Zkratky a pojmy

Audit – je podle této CP činnost, kterou auditor (pověřená osoba) provádí kontrolu bezpečnostní shody postupů v předpisové základně certifikační autority s prováděnými činnostmi.

Adresářová služba – specializovaná aplikace pro ukládání dat, upravující dále přístup k těmto datům a obsahující pravidla organizace těchto dat, k těmto datům se přistupuje zpravidla pomocí protokolu LDAP.

Certifikát – je datová zpráva, která spojuje soukromý klíč a veřejný klíč s osobou vlastníka a stvrzuje ověření identity této osoby. Jedná se o datovou zprávu, která je vydána poskytovatelem certifikačních služeb a která umožňuje s dostatečnou spolehlivostí a věrohodností ověřit, které fyzické osobě nebo pro jaké zařízení byl tento certifikát vydán.

Seznam certifikátů, které byly zneplatněny (CRL, Certificate revocation list). Seznam certifikátů, které byly předčasně zneplatněny. Obsahuje přesný časový údaj, kdy byl vydán a identifikuje certifikáty, které byly zneplatněny. CRL je podepsán zaručeným elektronickým podpisem poskytovatele a je veřejně přístupný.

Data pro dešifrování jsou jedinečná data, která se používají pro dešifrování datové zprávy, dále jen soukromý klíč.

Data pro ověřování elektronického podpisu jsou jedinečná data, která se používají pro ověření elektronického podpisu, dále jen veřejný klíč.

Data pro šifrování jsou jedinečná data, která se používají pro vytváření šifrování datové zprávy, dále jen veřejný klíč.

Data pro vytváření elektronického podpisu jsou jedinečná data, která podepisující osoba používá pro vytváření elektronického podpisu, dále jen soukromý klíč.

Datová zpráva jsou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích používaných při zpracování a přenosu dat elektronickou formou.

DN (Distinguish Name) – struktura, která umožňuje v certifikátu zajistit jednoznačnou identifikaci jména.

Elektronický podpis jsou 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.

Informační systém certifikačních služeb (ISCS) je systém, jehož prostřednictvím realizuje poskytovatel certifikačních služeb vydávající certifikáty své kritické služby, mezi něž patří generování a správa párových dat poskytovatele, podepisování certifikátů a seznamů certifikátů, které byly zneplatněny, vytváření auditních záznamů apod.

Ověření platnosti certifikátu – Ověřuje se, zda
- Integrita certifikátu nebyla porušena
- Certifikát poskytovatele byl platný v okamžiku podpisu.
- Certifikát nebyl v okamžiku ověření uveden na tehdy platném seznamu certifikátů, které byly zneplatněny (CRL).

Ověření platnosti podpisu – proces ověření platnosti podpisu spočívá zejména v:
- Prověření integrity podepsané zprávy.
- Prověření platnosti certifikátu podepisující se entity.
- Prověření platnosti certifikátu poskytovatele certifikačních služeb.

Párová data tvoří data pro vytváření elektronického podpisu a jim odpovídající data pro ověřování elektronického podpisu nebo data pro šifrování a jim odpovídající data pro dešifrování.

Podepisující osoba je fyzická osoba, která má prostředek pro vytváření podpisu a podepisuje svým jménem.

Prostředkem pro ověřování elektronických podpisů nebo značek rozumíme technické zařízení a/nebo programové vybavení, které se používá k ověřování elektronických podpisů.

Registrační autorita (RA) je součástí CA, je zřizována k provádění úkonů sloužících k převzetí a zpracování žádosti o certifikát a jeho další správou, zajišťuje důvěryhodnou komunikaci žadatele s CA a podporu procesů spojených s výdejem a obnovou certifikátu. Zajišťuje přijímání žádostí o předčasné ukončení platnosti certifikátu a poskytování informací o platnosti vystavených certifikátů.

Uživatel je subjekt, který se spoléhá na správnost (jak věcnou, tak formální) propojení veřejného klíče se jménem a příjmením vlastníka certifikátu.

Zaručený elektronický podpis je elektronický podpis, který splňuje následující požadavky:
1. je jednoznačně spojen s podepisující osobou,
2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Zneplatněný certifikát je certifikát, který je nebo byl uveden na seznamu certifikátů, kterým byla ukončena platnost (CRL). Tento seznam periodicky uveřejňuje poskytovatel certifikačních služeb.

Žadatel je fyzická osoba, která podává na Registrační autoritu žádost o službu spojenou se založením účtu pro výdej a následnou správu libovolného typu certifikátů. Správa spočívá zejména v obnově a případném zneplatnění.

2 ODPOVĚDNOSTI A PRAVOMOCI

2.1 Povinnosti

Jednotlivé subjekty v rámci poskytovatele certifikačních služeb musí splnit záruky, které jsou určeny v dokumentech, které specifikují činnost těchto subjektů.)

2.1.1 Povinnosti certifikační autority

CA CETIN je povinna vydávat certifikáty v souladu s touto směrnicí, jakožto i s dalšími dokumenty, které specifikují činnosti certifikační autority a registrační autority. CA CETIN je výslovně povinna:

- zajistit přístup ke kořenovému certifikátu poskytovatele,
- v souladu s touto politikou vydávat seznam certifikátů, které byly zneplatněny (CRL),

- zajistit přístup k informacím o certifikátech, které byly zneplatněny,
- zajistit podmínky pro korektní chování subjektů, jejichž činnost slouží k zajištění správné činnosti CA CETIN (správa CA, RA).

Všechny zúčastněné strany jsou povinny dodržovat platný právní řád ČR a předpisovou základnu společnosti.

2.1.2 Povinnosti registrační autority

RA CA CETIN je povinna zajišťovat výdej a správu certifikátů v souladu s touto směrnicí, jakožto i s dalšími dokumenty, které specifikují činnosti registrační autority. RA CA CETIN je výslovně povinna:

- zakládat a deaktivovat účty držitelů certifikátů pouze na základě přijatého příkazu,
- zneplatňovat certifikáty osobám na základě hodnověrné žádosti,
- potvrzovat na vyžádání platnost konkrétního certifikátu jiným osobám,
- provádět procesní podporu koncového uživatele (poskytnout informace o CA, typech certifikátů, zajistit opakovaná vydání aktivačních kódů, obnovu certifikátů, výdej následných certifikátů, poskytnout odkazy na návody a postupy,…)

2.1.3 Povinnosti vlastníků certifikátů

Vlastníci certifikátů jsou zejména povinni:

- používat certifikáty a odpovídající soukromé klíče výhradně pro účel, pro který byl vydán a v souladu s touto směrnicí,
- správně a korektně vystupovat v procesech definovaných v předpisové základně zejména ve vztahu k RA,
- chránit a držet v utajení senzitivní informace, které by mohly vést ke kompromitaci využívaných PKI metod, a to zejména soukromé klíče, aktivační kódy a přístupová hesla,
- zacházet s prostředky, jakož i s párovými daty s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
- bez prodlení vyrozumět RA o jakémkoli důvodném podezření o možné kompromitaci svého soukromého klíče a zároveň požádat o ukončení platnosti odpovídajícího certifikátu. Toto vyrozumění musí být učiněno způsobem, který je definován v CP,
- dodržovat veškerá ustanovení, podmínky a omezení uložená poskytovatelem v souvislosti s užíváním soukromého klíče a příslušných certifikátů. Tato omezení jsou definována zejména v CP, v certifikátu samotném a v předpisové základně společnosti a dodržovat další omezení definovaná v českém právním řádu,
- u exportovatelných certifikátů provádět jejich zálohu včetně soukromého klíče a to tak, aby nemohlo dojít k jejich kompromitaci a bylo možné je použít v případě potřeby obnovit certifikát a nedocházelo tak ke zbytečným ztrátám licencí nebo zátěže subjektů CA CETIN,
- podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu k datům v certifikátu.

Za škodu způsobenou porušením předchozích povinností odpovídá vlastník certifikátu. Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil platnost použitých certifikátů resp. zaručeného elektronického podpisu nebo nepostupoval v souladu s povinnostmi této CP.

2.1.4 Povinnosti spoléhající se strany

Spoléhající se strana je povinna provést veškeré úkony potřebné k tomu, aby ověřila, že odpovídající certifikát je platný a v případě ověření zaručeného elektronického podpisu, ověřila jeho platnost.

2.1.5 Povinnost zveřejňování seznamu certifikátů, které byly zneplatněny (CRL) a certifikátu poskytovatele

Poskytovatel certifikačních služeb je povinen zveřejňovat dvěma nezávislými způsoby seznam certifikátů, které byly zneplatněny. Seznam certifikátů, které byly zneplatněny, je vydáván a zveřejňován periodicky, 1x za 24 hodin a dále vždy při přijetí žádosti o zneplatnění certifikátu z důvodu kompromitace soukromého klíče. Certifikát, který byl zneplatněn, musí být uveden v nejbližším vydaném seznamu zneplatněných certifikátů.
CRL je dostupný dvěma nezávislými způsoby tak, aby informace o certifikátech, které byly zneplatněny, byla dostupná nepřetržitě, tj. (24 × 7). Tato dostupnost je zajišťována provozováním tří na sobě nezávislých distribučních míst (adresářové služby, dvou publikačních serverů).

Totéž obdobně platí pro kořenový certifikát poskytovatele.

2.2 Odpovědnost

2.2.1 Odpovědnost certifikační autority

CA poskytuje záruky na jedinečnost sériového čísla jí vydaných certifikátů a certifikátu.

CA poskytuje záruku na zneplatnění certifikátu, pokud byla žádost o zneplatnění podána v souladu s požadavky definovanými v CP.

2.2.2 Odpovědnost registrační autority

RA vykonává služby spojené s registrací uživatele, založením a vedením účtu u certifikační autority, vydáním aktivačních kódů a životním cyklem certifikátů. Veškeré uvedené odpovědnosti přecházejí na jednotlivé zaměstnance zařazené k výkonu pracovní činnosti na RA nebo jsou smluvně upraveny v outsourcingové smlouvě.

2.2.3 Odpovědnost vlastníka certifikátu

V případě nedodržení povinností definovaných v CP, odpovídá vlastník certifikátu (fyzická osoba) za zneužití senzitivních informací, zejména soukromých klíčů, aktivačních kódů a přístupových hesel, resp. procesů spojených se správou certifikátů a za škody, které tím společnosti vznikly.

2.2.4 Odpovědnost podepisujících se osob

Odpovědnost podepisující se osoby při komunikaci mimo prostředí CETIN je dána platným právním řádem ČR.

2.2.5 Kontaktní adresa

CETIN a.s.
Certifikační autorita CETIN
Pavel Vondruška
Českomoravská 2510/19,
Libeň, 190 00 Praha 9.
e-mail: pavel.vondruska@cetin.cz
tel.: +420 23846 8183

Aktuální kontaktní údaje jsou zveřejněny na kontaktních stránkách CA CETIN.
Kontaktní stránky jsou dostupné na adrese http://ca.cetin.cz a http://ca2.cetin.cz .
Změny těchto údajů nejsou důvodem k zahájení změnového řízení tohoto dokumentu.

2.2.6 Organizace pověřená správou

Řízením, správou a provozem CA CETIN registrační autority je pověřena organizační jednotka Bezpečnost a IMS.

2.3 Zveřejňování a uchovávání informací

2.3.1 Informace zveřejňované certifikační autoritou

CA CETIN zveřejňuje:

- Certifikační politiku (odkaz uveden v certifikátu),
- kořenový certifikát poskytovatele,
- seznam certifikátů, které byly zneplatněny,
- kontaktní údaje CA CETIN a RA,
- seznam vydaných certifikátů pro šifrování.

2.3.2 Způsob a periodicita zveřejňování

CP je zveřejněna po celou dobu platnosti a dále minimálně 2 roky po ukončení platnosti posledního z certifikátů, který byl podle této směrnice vydán. CP je přístupná na kontaktních stránkách CA CETIN.

Certifikát poskytovatele je zveřejněn po celou dobu jeho platnosti a minimálně 2 roky po ukončení platnosti. Certifikát poskytovatele je přístupný na kontaktních stránkách poskytovatele a v místě RA.

Seznam certifikátů, které byly zneplatněny, je vydáván a zveřejňován periodicky, 1x za 24 hodin a při přijetí žádosti o zneplatnění certifikátu z důvodu kompromitace soukromého klíče. CRL je přístupné na kontaktních stránkách CA CETIN, v adresářové službě a informace o platnosti certifikátu je možné dále získat telefonickým dotazem na RA.
Vydané certifikáty pro šifrování jsou zveřejňovány do 20 min po jejich vydání. Seznam vydaných certifikátů pro šifrování je přístupný v rámci adresářových služeb CETIN.

2.4 Podřízené certifikační autority CA CETIN

2.4.1 Kontaktní osoba

Marek Anýž, os. číslo 066123
Windows administrátor
Oddělení Provoz / 44121
Českomoravská 2510/19,
Libeň, 190 00 Praha 9.

2.4.2 Identifikace podřízených certifikačních autorit

Zřízeny jsou dvě podřízené certifikační autority.

CA1 -> CA CETIN G2 01 -> cewcap401.ad.cetin
cn=CA CETIN G2 01, dc=ad, dc=cetin
certifikát vydán 12.4.2018, platnost 10 let

CA2 -> CA CETIN G2 02 -> cewcap402.ad.cetin
cn=CA CETIN G2 02, dc=ad, dc=cetin
certifikát vydán 12.4.2018, platnost 10 let

2.4.3 Politika podřízených certifikačních autorit

CA slouží automatickému přidělování certifikátů pro doménové stroje a doménové kontroléry. Vydané certifikáty slouží k ověření daného stroje (Client Authentication) a pro podepsání a šifrování komunikace RDP (Remote Desktop). Automatické vydání certifikátů těmto strojům je řízeno doménovou politikou.

Pro výdej certifikátů se používají následující šablony:
SCCM Client Certificate pro automatizované vydávání certifikátů (Client Authentication),
SCCM Client Certificate Outside pro manuální vydávání certifikátů (Client Authentication) pro stroje mimo doménu AD.CETIN,
Domain Controller pro automatizované vydávání certifikátů (Client Authentication, Server Authentication) pro doménové kontroléry,
Domain Controller Authentication pro automatizované vydávání certifikátů (Client Authentication, Server Authentication, Smart Card Logon) pro doménové kontroléry,
Computer RDP (Server Authentication, Remote Desktop Authentication).

Tato autorita vydává certifikáty pro aplikaci Bitlocker a to jak pro serverovou část, tak klientskou část, vydává i certifikát pro odemknutí účtu (tento musí být vydán manuálně).

Manuální proces zajišťuje administrátor domény AD.CETIN.

CA vydává CLR a publikuje jej na k tomu určeném webu.
CLR je dále dostupné přes ldap (adresa je uvedena ve vydaných certifikátech).

2.4.4 Parametry vydaných certifikátů

Platnost 1 rok
RSA 2048
Otisk pro podpis SHA512
Automatická obnova certifikátu 6 týdnů před vypršením platnosti certifikátu.

Syntaxe: CN=název stroje v AD (nazev.ad.cetin)

Komponenta	Cert. purpose	CA Template	Enhanced Key Usage
Site server	Server authentication	Web Server	Server Authentication (1.3.6.1.5.5.7.3.1)
Management, distribution point, Boot images	Client authentication	Workstation Authentication	Client Authentication (1.3.6.1.5.5.7.3.2).
Windows client computers	Client authentication	Workstation Authentication	Client Authentication (1.3.6.1.5.5.7.3.2).
Network Unlock Certificate	Encryption	User	Network Unlock 1.3.6.1.4.1.311.67.1.1

3 POPIS ČINNOSTÍ

3.1 Vstupní registrace

Každý žadatel o certifikát, musí podstoupit proces vstupní registrace. O zavedení účtu u certifikační autority a tedy práva na vydání a údržbu certifikátu se žádá v k tomu určené aplikaci IDM. Žádost je schvalována dle zde nastaveného workflow.
Výsledkem úspěšné vstupní registrace je založení účtu v CA CETIN a u netechnických účtů zaslání aktivačních kódů pro vytvoření certifikátu.

3.1.1 Typy vydávaných certifikátů

- Certifikát k autentizaci zaměstnance (ou=AUTH)
- Certifikát k autentizaci externisty (ou=EXT)
- Certifikát k autentizaci externích obchodních partnerů, kteří potřebují přistupovat do NOP (ou=SPEC)
- Certifikát pro šifrování a vytváření podpisu (určeno pro aplikaci Entrust Security Provider) (ou=EMPL)
- Certifikáty pro SSL komunikaci, weby, zařízení a specifické účely (ou=WEB, ou=DEVICES, ou=SPEC)
- Certifikáty pro LTE - eNB systémové moduly (ou=LTE)
- Autentizace operátorů CA CETIN (ou=office)
- Testovací certifikáty (ou=TEST)

3.1.2 Syntaxe podporovaných jmen

Certifikační autorita CETIN ve vydávaných certifikátech podporuje následující typy jmen (CN, DN):

- Certifikát k autentizaci zaměstnance (ou=AUTH), syntaxe
  cn=Jmeno Prijmeni + serialNumber=AA012356, ou=AUTH, o=cetin, c=cz
  AA012356 = AA + osobní číslo zaměstnance, doplněno nulami na 6 číslic

- Certifikát k autentizaci externisty (ou=EXT), syntaxe
  cn=Jmeno Prijmeni + serialNumber=x0012356, ou=EXT, o=cetin, c=cz
  x0012356 = login externisty

- Aplikace Entrust Security Provider / určeno pro šifrování, podpis (ou=EMPL)
  cn=Jmeno Prijmeni + serialNumber=1234, ou=EMPL, o=cetin, c=cz
  1234 = osobní číslo zaměstnance

- Certifikáty pro externí obchodní partnery, kteří potřebují přistupovat do NOP
  cn=Jmeno Prijmeni Společnost, ou=SPEC, o=cetin, c=cz

- Certifikáty pro SSL komunikaci, weby, zařízení a specifické účely (ou=WEB, ou=DEVICES, ou=SPEC)
  cn=DNS jmeno, ou=WEB, o=cetin, c=cz
  cn=DNS jmeno, ou=DEVICE, o=cetin, c=cz

cn=DNS jmeno, ou=SPEC, o=cetin, c=cz

- Certifikáty pro LTE - eNB systémové moduly (ou=LTE), syntaxe
  cn=SN.nokiasiemensnetworks.com,ou=LTE,o=cetin,c=CZ
  cn=SN.huawei.com, ou=LTE, o=cetin, c=CZ
  cn=723280100046.zte.com.cn, ou=LTE, o=cetin, c=CZ
  SN= sériové číslo systémového modulu

Díky použití jedinečných číselných identifikátorů v atributu serialNumber je zajištěna jednoznačnost DN jména v rámci adresářového stromu CETIN a.s.

3.2 Vydání následného certifikátu v době platnosti certifikátu

Certifikáty spravované klientskou aplikací Entrust Security Provider jsou obnovovány automaticky v časových termínech, které jsou uvedeny v odstavci „Doba platnosti certifikátů“. To znamená, že osobní certifikáty pro podepisování a šifrování jsou automaticky distribuovány na stranu klienta.
Platnost certifikátů k autentizaci zaměstnanců je hlídána na straně RA. Před vypršení platnosti certifikátu jsou uživateli automaticky zaslány aktivační kódy obnově certifikátu. Obnovu provádí uživatel sám prostřednictvím webového rozhraní Entrust Authority™ Digital Identity Management.
V případě certifikátů pro SSL a jiné specifické účely je evidovaný žadatel o tento certifikát (zaměstnanec) informován, že se blíží expirace certifikátu. Obnova je provedena na základě jeho žádosti.
U ostatních typů certifikátů nejsou kódy k obnově automaticky zasílány (týká se i certifikátů pro autentizaci externistů). Vydání následného certifikátu k těmto typům se děje na základě žádosti.

3.3 Vydání následného certifikátu při neplatnosti dříve vydaného certifikátu

Jestliže se vlastník certifikátu dostane do situace, kdy platnost jeho certifikátu vypršela, protože nevyužil možnosti automatického vydání následného certifikátu nebo nechal propadnout zaslané kódy k jeho obnově, pak musí postupovat následujícím způsobem:

- Z vlastníka certifikátu se stává opět žadatel (nevlastní žádný platný certifikát). Žadatel musí zažádat RA o nové vydání aktivačních kódů (může zažádat zavoláním na HelpDesk, zažádat vyplněním formuláře v aplikaci Clooney nebo zavolat na podporu RA)
- Pokud má žadatel v IDM příslušný přístup schválen, pak na základě této žádosti jsou žadateli vydány nové aktivační kódy pro vytvoření následného certifikátu.

3.4 Podání žádosti o ukončení platnosti certifikátu

Žádosti o ukončení platnosti certifikátu lze podat následujícími způsoby:

- automaticky vygenerovaná žádost při zrušení role v IDM,
- telefonicky z MT na RA, podmínkou je, že MT žadatele je uveden v X.500,
- pomocí formuláře v aplikaci Clooney,
- osobně v místě RA.

Samotné ukončení platnosti certifikátu se děje v systému CA CETIN a provádí je operátor RA. Pokud z oprávněného důvodu nebude žádost o ukončení platnosti certifikátu akceptována, operátor RA o tom neprodleně vyrozumí žadatele o zneplatnění certifikátu. V případě akceptace žádosti se může žadatel o kladném výsledku přesvědčit při vydání nejbližšího CRL.

Při podání žádosti o ukončení platnosti osobního certifikátu je v rámci interního systému CA CETIN ukončena platnost všem vystaveným certifikátům, pokud žadatel nezažádá výslovně jinak.

3.4.1 Oprávněné osoby

O ukončení platnosti svého může podat žádost jeho vlastník.

Majitel nákladového střediska je oprávněn žádat o ukončení platnosti certifikátu osoby spadající do kompetence jeho nákladového střediska. Přímý nadřízený nebo garant smlouvy mohou požádat o zneplatnění certifikátu pro jim podřízené osoby.

Specialista CA je oprávněn žádat o ukončení platnosti certifikátu libovolného vlastníka certifikátu v místě RA nebo formou žádosti v elektronické podobě podepsanou zaručeným elektronickým podpisem. Operátor RA je v tomto případě povinen o ukončení platnosti certifikátu bezodkladně informovat vlastníka certifikátu (e-mailem, SMS, telefonicky). Výjimku z této povinnosti tvoří externisté.

RA je oprávněna ukončit platnost certifikátu v případě přijetí požadavku o jeho zneplatnění a to prostřednictvím servisního požadavku nebo od oprávněné osoby. Dále RA je oprávněna ukončit platnost v případě, kdy byl certifikát vydán, ale vlastník certifikátu oznámil hodnověrným způsobem zjištěné nedostatky v průběhu tzv. akceptace certifikátu vlastníkem nebo pokud dojde k nesouladu s údaji uvedenými v X. 500. RA operátor je oprávněn ukončit platnost certifikátu také v případě, že byly použity aktivační kódy, ale selháním hardwaru nebo výpadkem sítě nebyly certifikáty u uživatele vytvořeny a operátor RA byl o této skutečnosti hodnověrným způsobem informován. Operátor RA je oprávněn ukončit platnost certifikátu také v případě, že byly vydány žadateli nové aktivační kódy. Operátor RA provádí zneplatnění certifikátů vlastníkům certifikátu, kterým byl ukončen zaměstnanecký poměr a tyto osoby samy včas nepožádaly o zneplatnění, a stejně tak i bývalým externistům, u nichž o zneplatnění včas nepožádal garant smlouvy. V takovém případě je na základě synchronizace s adresářovými službami vytvořena žádost o zablokování účtu a zneplatnění certifikátu tuto žádost vyřizuje operátor RA.

4 POPIS ČINNOSTÍ - Provozní požadavky

Tato kapitola definuje požadavky kladené na provádění jednotlivých činností v rámci poskytování certifikačních služeb.

4.1 Žádost o vydání certifikátu

- Certifikát k autentizaci zaměstnance - žádá se v IDM , PKI Production_AUTENTIZACE
- Certifikát k autentizaci externisty - žádá se v IDM, PKI Production_AUTENTIZACE
- Aplikace Entrust Security Provider (šifrování) - žádá se v IDM, přístup PKI Production_ENTRUST-SIFROVANI
- Certifikáty pro SSL komunikaci, weby, zařízení a specifické účely (ou=WEB, ou=DEVICES, ou=SPEC) - žádá se v IDM, PKI-SSL Production_CERTIFIKAT. Jde o technický účet
- SSL certifikáty pro externí obchodní partnery, kteří potřebují přistupovat do NOP, žádá se v IDM , PKI-SSL Production_NOP_CERTIFIKAT , jde o technický účet
- Certifikáty pro LTE - eNB systémové moduly (ou=LTE) - žádost mohou podat jen osoby uvedené v postupu PP006972 a to v souladu se zde uvedeným procesem
- Testovací certifikáty - žádá se osobně nebo elektronicky u osoby odpovědné za provoz CA

4.2 Vydání certifikátu

Předpokladem vydání certifikátu je schválení požadavku dle 4.1.

- Operátor RA založí účet v certifikační autoritě (pokud dosud nebyl zřízen) a v případě netechnických účtů a certifikátů pro NOP vygeneruje aktivační kódy.
- Předá aktivační kódy žadateli takovým způsobem, aby nevzniklo žádné podezření na kompromitaci aktivačních kódů; při kompromitaci či podezření na kompromitaci aktivačních kódů provede RA jejich nové vygenerování a předání (upřednostňuje se odeslání aktivačních kódů rozděleně pomocí e-mailu+SMS).
- Operátor RA zapíše provedený úkon do pracovního výkazu.
- Operátor RA uzavře pracovní příkaz v nástroji Clooney.

4.3 Akceptace certifikátu vlastníkem

Od vydání certifikátu má nový vlastník 5 pracovních dnů na kontrolu úplnosti, správnosti a přesnosti údajů, které jsou v certifikátu uvedeny. Vlastník certifikátu porovnává shodu a správnost jednotlivých položek se skutečností. V případě, že zjistí nesoulad, je povinen toto oznámit hodnověrným způsobem operátorovi RA. Za hodnověrný způsob se považuje zejména: přidělení servisního požadavku, použití mobilního telefonu nebo e-mailu uvedeného v tel. seznamu.
Pokud se potvrdí, že se jedná o skutečné nedostatky, musí být certifikát zneplatněn a provedena opatření vedoucí k nápravě.

4.4 Ukončení platnosti certifikátu

Procesy vedoucí k ukončení platnosti certifikátu mohou mít dva stavy:

- Ukončení platnosti certifikátu se zachováním uživatelského účtu v systému CA CETIN. Certifikátům je ukončena platnost, právo uživatele na používání služeb PKI však zůstává nezměněné a žadatel může požádat o vydání nových následných certifikátů. Tato varianta je nejčastěji využívána v případě ukončení platnosti certifikátu na základě žádosti vlastníka certifikátu.
- Ukončení platnosti certifikátů se zrušením uživatelského účtu v systému CA CERTIN (deaktivace). Certifikátům je ukončena platnost a současně je zrušeno právo vlastníka certifikátu na využívání služeb PKI. Varianta se používá například při rozhodnutí vlastníka nákladového střediska o ukončení poskytování služeb PKI dané osobě nebo odchodu vlastníka certifikátu ze společnosti.

4.4.1 Důvody k ukončení platnosti certifikátu

Certifikátům může být ukončena platnost zejména na základě některého z následujících důvodů:

- Vlastník certifikátu přestal být zaměstnancem společnosti nebo ukončil smluvní vztah s CETIN.
- Vlastník certifikátu požádá o ukončení platnosti certifikátu, například z důvodu pozbytí platnosti některého z údajů uvedených v certifikátu.
- Vlastník nákladového střediska, přímý nadřízený nebo garant smlouvy požádá o ukončení platnosti certifikátu pro osoby v jeho podřízenosti.
- Dojde ke kompromitaci soukromého klíče osoby nebo je zde důvodná obava z možnosti zneužití párových klíčů. V tomto případě podává žádost o ukončení platnosti certifikátu vlastník certifikátu nebo majitel nákladového střediska, přímý nadřízený či garant smlouvy.
- Vlastník certifikátu oznámí nedostatky v obsahu nebo v procesu vytvoření certifikátu, a to v průběhu akceptace certifikátu.
- Poskytovatel certifikačních služeb musí rovněž ukončit platnost osobního certifikátu, dozví-li se prokazatelně, že podepisující osoba zemřela, nebo ji soud způsobilosti k právním úkonům zbavil nebo omezil, nebo pokud údaje, na základě kterých byl certifikát vydán, přestaly platit.
- Poskytovatel certifikačních služeb ukončí platnost vydaných certifikátů z důvodu ukončení platnosti certifikátu poskytovatele. V tomto případě je vlastník certifikátu o této skutečnosti vyrozuměn zasláním e-mailu.

Při podání žádosti o ukončení platnosti certifikátu může oprávněná osoba uvést jeden z následujících důvodů, který je operátorem RA zaznamenán do systému CA CETIN a odtud převzat do CRL:

- Superseded – certifikát byl nahrazen novějším certifikátem (např. bylo třeba změnit některé hodnoty nebo rozšíření certifikátu, které se však netýkají změny DN, patří sem např. vydání následného certifikátu, změna e-mailu).
- Key Compromise - soukromý klíč vlastníka certifikátu byl nebo mohl být zcizen nebo není pod kontrolou vlastníka (např. byl ukraden celý notebook/ počítač, byla zcizena záloha certifikátu se soukromým klíčem, došlo k výměně disku bez toho, že by byl certifikát odebrán, v profilu uživatele pracoval jiný zaměstnanec a certifikát byl exportovatelný i se soukromým klíčem …)
- Affilation Changed - identifikační údaje držitele certifikátu se změnily. Např. přestal být pravdivý obsah atributu Organization (O) neboť zaměstnanec rozvázal pracovní poměr. Používá se tedy při odchodu zaměstnance.
- Cessation of Operation – předmět certifikátu byl vyřazen z provozu. Patří sem např. rychlý odchod, přechod do mimoevidenčního stavu apod. Pro SSL certifikáty to znamená, že např. webový server byl nahrazen jiným serverem s novým jménem.
- Unspecified – všechny ostatní případy, kdy bylo potřeba certifikát zneplatnit (bez možnosti jeho obnovy), ale nejedná se o některou z předchozích možností

4.4.2 Frekvence vydání seznamu certifikátů, které byly zneplatněny

Seznam certifikátů, které byly zneplatněny, je vydáván nejméně 1x za 24 hodin a navíc vždy při přijetí žádosti o zneplatnění certifikátu z důvodu kompromitace soukromého klíče.

V případě mimořádných situací je možné vydat CRL s delší dobou platnosti. K vydání takovéhoto CRL vydává příkaz specialista CA. Specialista CA může vydat mimořádné CRL podle potřeby tj. mimo periodické pořadí.

4.4.3 Požadavky na ověření přítomnosti certifikátu na CRL

Strana, která se spoléhá na certifikáty CA CETIN, je povinna ověřit certifikát způsobem, který odpovídá danému použití.

4.4.4 On-line dostupnost seznamu certifikátu, které byly zneplatněny

Seznam certifikátů, které byly zneplatněny, je veřejně přístupným seznamem on-line dostupným následujícím způsobem:

- pomocí http protokolu na kontaktních stránkách CA (intranet, Internet, 24 × 7),
- pomocí ldap protokolu v systému provozovaném CA CETIN. (24 × 7).

4.4.5 Požadavky na on-line ověření

Spoléhající se subjekt musí zajistit konfiguraci použitého řešení tak, aby bylo schopné kontrolovat aktuální CRL pomocí protokolu http nebo LDAP.

4.4.6 Jiné formy zpřístupnění CRL

Informace, zda je certifikát platný, je dále dostupná (pro spoléhající se subjekty) dotazem na RA.

4.4.7 Zvláštní požadavky při kompromitaci klíče

Při zjištění kompromitace klíče je požadováno neprodlené podání žádosti o ukončení platnosti certifikátu na RA.

4.5 Procedury bezpečnostního dohledu

Monitoring systémů CA CETIN zajišťuje dohledový systém společnosti ISIDAS (Information System Incident Detection and Analysis System). Bezpečnostně významné události provozu CA CETIN jsou zaznamenávány v databázi bezpečnostních událostí.

4.5.1 Typy zaznamenávaných událostí

K zaznamenávání událostí se využívá log systému CA CETIN a dále systém bezpečnostního dohledu, který v reálném čase (dle použitého způsobu sběru událostí) sbírá a vyhodnocuje bezpečnostně relevantní události z jednotlivých dohledovaných systémů a vytváří z nich souhrnná hlášení. Systém ISIDAS zaznamenává informace i o vybraných operacích, které jsou podkladem pro kontroly bezpečnosti a zpětné dohledávání realizovaných operací a dále vyhodnocuje události detekující mimořádné události.

Hlášení bezpečnostního dohledu jsou eskalována podle definovaných scénářů zodpovědným pracovníkům, kteří zajistí nápravu.

Události zaznamenávané v rámci bezpečnostního dohledu CA CETIN:

- vydání certifikátu,
- ukončení platnosti certifikátu,
- nakládání s párovými daty poskytovatele během celého jejich životního cyklu,
- požadavek na ukončení platnosti certifikátu včetně údajů o žádající osobě a výsledku operace,
- neoprávněný požadavek na ukončení platnosti certifikátu včetně údajů o žádající osobě a výsledku,
- přístup oprávněných uživatelů do jednotlivých subsystémů ISCS,
- pokusy o neoprávněný přístup do systému,
- zveřejnění vydaných certifikátů včetně informace o výsledku operace,
- akceptace žádosti o ukončení platnosti certifikátu,
- zveřejnění CRL,
- změna údajů o vlastnících certifikátů,
- akce oprávněných uživatelů systému.

4.6 Archivace záznamů

4.6.1 Typy uchovávaných záznamů

Informační systém certifikačních služeb uchovává následující informace:

- data shromážděná systémem bezpečnostního dohledu,
- auditní záznamy (logy) systému Entrust CA a systému centrální adresářové služby,
- seznam vydaných certifikátů,
- záloha databáze databázového systému, který je využívána systémem Entrust CA,
- vydaná CRL,
- oznámení o zjištěných nedostatcích v průběhu akceptace vydaných certifikátů.

V tištěné formě jsou archivovány zejména následující záznamy:

- zprávy z prováděných auditů.

4.6.2 Období archivace a kontroly čitelnosti archivovaných záznamů

Archivace záznamů je prováděna nejméně po dobu 2 let. Archivaci je nutno provádět na média, která mají výrobcem zaručovanou životnost záznamu minimálně po dobu archivace.

4.6.3 Zabezpečení archivních záznamů

Přístup k archivním záznamům má pouze specialista CA a jeho nadřízený.

4.7 Výměna párových dat

4.7.1 Výměna párových dat koncového uživatele

Tato výměna je odlišná podle typu certifikátu a použité aplikace.

- Po přihlášení do aplikace Entrust Security Provider se automaticky vygeneruje nový klíčový pár. Toto nastane v případě, že se uživatel přihlásí on-line ke svému osobnímu profilu v době 100 dní před vypršením platnosti příslušného soukromého klíče.
- Certifikát k autentizaci (zaměstnanec). Před vypršením doby platnosti klíče pro autentizaci jsou vlastníku zaslány aktivační kódy pro vygenerování následného certifikátu. Certifikát si uživatel generuje sám.
- Certifikát k autentizaci (externista, NOP). Výměna není nijak podporována. Externista, garant NOP musí o zaslání nových aktivačních kódů pro vygenerování následného certifikátu požádat. Certifikát si uživatel generuje sám.
- U certifikátů pro weby a zařízení není automatická výměna podporována. Vlastník je pouze informován, že se blíží konec platnosti daného certifikátu a zda jej chce obnovit.
- U certifikátů určených pro LTE je výměna plně automatizována a děje se při exiraci certifikátu pomocí protokolu CMPV2

4.7.2 Výměna párových dat poskytovatele

Nejpozději 3 roky před vypršením platnosti certifikátu poskytovatele vygeneruje poskytovatel svá nová párová data. K veřejné části klíče nově vytvořených párových dat je vytvořen nový certifikát poskytovatele, který je zveřejněn na stejných místech jako původní certifikát poskytovatele. Nově vydávané certifikáty jsou od té chvíle podepisovány novými párovými daty poskytovatele. Doba 3 roky je stanovena s ohledem na maximální dobu platnosti vystavovaných certifikátů.

4.8 Obnovení činnosti po kompromitaci párových dat poskytovatele

4.8.1 Poškození výpočetních zdrojů, software a/nebo dat

Poškození hardware, software nebo dat, která generují záznam do logu CA a sběrného kanálu ISIDAS, jsou detekována jako mimořádné události systémem bezpečnostního dohledu.

4.8.2 Postup při ukončení platnosti certifikátu poskytovatele

V případě ukončení platnosti certifikátu poskytovatele, které není vynuceno kompromitací soukromého klíče, se neprovádí žádná mimořádná procesní a jiná opatření.

4.8.3 Ukončení platnosti certifikátu poskytovatele z důvodů kompromitace párových dat poskytovatele

V případě ukončení platnosti certifikátu poskytovatele certifikačních služeb z důvodu kompromitace párových dat poskytovatele nebo v případě důvodné obavy ze zneužití párových dat poskytovatele postupuje následovně:
Poskytovatel
- ukončí platnost všech vystavených certifikátů vydaných touto certifikační autoritou a uvede je na seznamu certifikátů, které byly zneplatněny (CRL),
- ukončí platnost certifikátu poskytovatele a uvede ho na seznamu certifikátů, které byly zneplatněny (CRL),
- přeruší poskytování certifikačních služeb,
- uvede informaci o ukončení platnosti certifikátu poskytovatele na svých kontaktních stránkách a vydá ji formou sdělení pro všechny zaměstnance CETIN,
- protokolárně zničí párová data poskytovatele.

Specialista CA požádá o mimořádný audit. Cílem mimořádného auditu je zjistit příčiny kompromitace párových dat poskytovatele a přijmout následná opatření. Po té může poskytovatel vygenerovat nová párová data poskytovatele a pokračovat v poskytování certifikačních služeb.

4.9 Ukončení činnosti poskytovatele certifikačních služeb

Provozovatel certifikační autority zajistí následující skutečnosti:

- zpřístupní informaci o ukončení činnosti poskytovatele certifikačních služeb na svých kontaktních stránkách nejméně dva měsíce před plánovaným ukončením činnosti,
- zašle informaci o ukončení činnosti poskytovatele certifikačních služeb e-mailem všem osobám, kteří mají v tomto okamžiku platný certifikát, a to nejméně dva měsíce před plánovaným ukončením činnosti,
- ukončí platnost vystavených certifikátů ke dni ukončení činnosti,
- ukončí platnost certifikátu poskytovatele ke dni ukončení činnosti,
- ukončí poskytování certifikačních služeb,
- prokazatelně zničí párová data poskytovatele.

5 Mechanizmy fyzické, procedurální a personální bezpečnosti

5.1 Fyzická bezpečnost

Servery CA se nacházejí v zabezpečeném sále v datovém centru JZM, Praha 5. Pro zajištění objektové bezpečnosti těchto serverů se využívá nastavení fyzické bezpečnosti příslušného sálu a nad rámec těchto opatření se využívají samostatné uzamykatelné klece. Publikační servery CA CETIN jsou umístěny v zabezpečeném sále v budově Chodov, Praha.

5.2 Procedurální bezpečnost

5.2.1 Důvěryhodné role

Důvěryhodná role je taková role, jejíž činnost, ke které je oprávněna, může vést k bezpečnostním problémům, pokud není prováděna správně, ať již záměrně, či neúmyslně.

CA CETIN pro svoji činnost využívá tyto role
- Specialista CA (Specialista pro certifikační služby
- RA Operátor (RO)
- RevA Operátor (RevO)
Role RA a RevA mohou být vykonávány současně.

5.2.2 Bezpečnostní komise - CA

Trojice osob složená ze zástupců rolí SM, RA a manažera pro bezpečnost tvoří bezpečnostní komisi CA, která může vykonávat všechny pravomoci v systému Entrust a řešit tak libovolné krizové situace.

5.3 Personální bezpečnost

5.3.1 Požadavky na osobnostní profil, kvalifikaci a praxi v oboru osob v důvěryhodných rolích

Osoby, které budou zodpovědné za poskytování certifikačních služeb, musí být pečlivě vybrány na základě posouzení loajality a důvěryhodnosti. Zaměstnanci musí být občany České republiky nebo mít trvalý pobyt na území České republiky, avšak nejméně po dobu pěti let. Musí mít čistý trestní rejstřík.

5.3.2 Požadavky na školení a další vzdělávání pro každou roli

Veškerý personál, zapojený do poskytování certifikačních služeb musí být dostatečně vyškolen. Témata jednotlivých školení zahrnují práci s programovým i hardwarovým vybavením poskytovatele certifikačních služeb, operační a bezpečnostní postupy a praktické uplatňování bezpečnostních a certifikačních politik a dalších předpisů.

5.3.3 Proškolování a jeho frekvence

Osoby pracující v rámci poskytovatele certifikačních služeb musí být neustále seznamovány s aktuálními předpisy týkajícími se jejich činnosti.
Významná změna příslušných předpisů je důvodem k provedení školení, jehož náplní jsou vzniklé změny. Program a průběh školení musí být zaznamenán písemnou formou.
Významnými změnami v tomto smyslu jsou například změny programového nebo hardwarového vybavení, změny v požadavcích na bezpečnost, případně další změny, které mají dostatečný vliv na bezpečnost provádění certifikačních služeb.
Školení osob v důvěryhodných rolích musí proběhnout minimálně jedenkrát do roka.

5.3.4 Požadavky na smluvní pracovníky

Osoby, jež vykonávají pro poskytovatele certifikačních služeb činnosti na základě smluvního vztahu, musí splňovat tyto podmínky:

- bezúhonnost,
- odborná způsobilost.

5.3.5 Poskytování dokumentace

Dokumentace potřebná k provádění činností v rámci poskytovatele certifikačních služeb je poskytnuta všem osobám, kterých se týká a jejichž činnost definuje, nebo jiným způsobem ovlivňuje. Změny v těchto dokumentech jsou zveřejněny neprodleně. Neaktuální dokumentace je stažena a dle interních směrnic skartována.

6 Technická bezpečnost

6.1 Generování párových dat a jejich instalace

6.1.1 Generování párových dat

6.1.1.1 Párová data koncových uživatelů

Párová data koncových uživatelů si žadatelé generují sami ve webové aplikaci Entrust Authority™ Digital Identity Management na adrese https://ca.cetin.cz/p12 nebo na záložní adrese: https://ca2.cetin.cz/p12 .
Soukromý klíč je určen pro asymetrický algoritmus RSA a velikost příslušného modulu musí být roven nebo větší než 1 024 bitů. Hashovací algoritmus v podpisovém schématu je SHA-2 (pokud je to z hlediska kompatibility nutné lze vydat speciální typ certifikátu a použít SHA1).

6.1.1.2 Párová data pro SSL certifikáty (weby, servery, spec. zařízení LTE)

Soukromý klíč určený k SSL, LTE je vždy generován v technickém zařízení.
Certifikát pro LTE je generován pomocí protokolu CMPV2 a ostatní SSL certifikáty vložením požadavku na certifikát (CSR) ve formátu PKCS10 (CSR) do publikovaného rozhraní CA CETIN (web connector). Detaily v 6.1.3.

6.1.1.3 Párová data poskytovatele

Párová data poskytovatele byla generována na serveru CA v aplikaci Entrust 8.1. Soukromý klíč je určen pro asymetrický algoritmus RSA a velikost příslušného modulu je 2 048 bitů. Hashovací algoritmus v podpisovém schématu je SHA-2.

6.1.2 Doručení soukromého klíče jeho vlastníku

Soukromý klíč určený k SSL, NOP, podepisování a autentizaci, je vždy generován pod výhradní kontrolou žadatele. Certifikační autorita CETIN nenabízí službu generování klíčového páru určeného k podpisu a autentizaci, a proto neexistuje situace, kdy by bylo třeba předávat soukromý klíč podepisující osobě.
Soukromý klíč žadatele o certifikát určený k šifrování je uchováván v zašifrované podobě v databázi Entrust/CA a je určen pro obnovu klíče v případě potřeby. Je předán bezpečným kanálem vytvořeným aplikací Entrust Security Provider.

6.1.3 Doručení veřejného klíče žadatelem o certifikát

Veřejný klíč žadatele o certifikát, určený pro ověření podpisu a pro certifikát určený pro šifrování, je CA doručen prostřednictvím bezpečného komunikačního kanálu mezi žadatelem a CA CETIN. Nastavení a zabezpečení tohoto kanálu zajišťuje na straně uživatele aplikace Entrust Security Provider. V případě doručení veřejného klíče pro certifikát k autentizaci a NOP se na straně žadatele používá web aplikace Entrust Authority™ Digital Identity Management na adrese https://ca.cetin.cz/p12 nebo na záložní adrese: https://ca2.cetin.cz/p12 .
Pro doručení veřejného klíče se v případě využití CSR žádosti o SSL certifikát využívá webová aplikace Entrust Authority™ CSR Enrollment na adrese https://ca.cetin.cz/p10 nebo na záložní adrese: https://ca2.cetin.cz/p10 .

6.1.4 Distribuce veřejného klíče poskytovatele certifikačních služeb

Veřejný klíč je obsažen v kořenovém certifikátu CA. Certifikát poskytovatele lze stáhnout z kontaktních stránek CA CETIN http://ca.cetin.cz nebo na záložní adresa http://ca2.cetin.cz .

6.1.5 Délka veřejného klíče

Certifikační autorita kontroluje, zda příchozí žádosti o certifikát obsahují veřejný klíč s délkou modulu 2048 bitů. Pokud žadatel potřebuje z důvodu kompatibility velikost modulu nižší (1024 bitů) je potřeba toto uvést v žádosti o certifikát a operátor RA připraví potřebnou šablonu pro příslušný typ certifikátu.
Velikost modulu veřejného klíče u certifikátu CA CETIN je 2 048 bitů.

6.2 Požadavky na správu párových dat

6.2.1 Archivace veřejného klíče

Veřejný klíč poskytovatele je archivován po dobu 2 let od chvíle jeho vypršení nebo ukončení platnosti. Po celou dobu musí být k dispozici i dálkovým přístupem prostřednictvím webových stránek Certifikační autority.
Ostatní veřejné klíče nejsou archivovány.

6.2.2 Doba platnosti certifikátu

6.2.2.1 Certifikáty certifikační autority

Certifikát certifikační autority je vydán s platností 20 let. Jeho platnost je od 9. 11. 2015 do 9.11.2035.

6.2.2.2 Certifikáty podřízené certifikační autority

Certifikáty podřízené certifikační autority se vydávají s platností 10 let. Platnost však nesmí být delší, něž je platnost kořenového certifikátu certifikační autority - tj. max. do 9.11.2035.

6.2.2.3 Certifikáty pro spravované v aplikaci Entrust Security Provider (šifrování a podepisování)

Certifikační autorita vydává osobní uživatelské certifikáty spravované v aplikaci Entrust Security provider s následujícími parametry životního cyklu osobních certifikátů:

Doba platnosti vydávaných certifikátů.....	24 měsíců (2 roky)
Doba platnosti klíče určeného k šifrování…….....	90%

6.2.2.4 Certifikáty pro autentizaci

Doba platnosti certifikátů a odpovídajících klíčů určených pro autentizaci je 2 roky.

6.2.2.5 Certifikáty pro eNB / LTE

Doba platnosti certifikátů a odpovídajících klíčů vdávaných pro autentizaci eNB / LTE je 3 roky.

6.2.2.6 Certifikáty pro weby, zařízení a specifické účely

Doba platnosti certifikátů pro web, zařízení a specifické účely je 3 roky, pokud není v žádosti uveden požadavek na kratší období platnosti.

6.2.2.7 Certifikáty určené pro testování

Testovací certifikáty se vydávají na dobu maximálně 6 měsíců. Výjimku může stanovit specialista CA.

6.3 Řízení bezpečnosti

Výrobce systému Entrust deklaruje, že postupy při vývoji aplikace Entrust Authority Security Manager 8.1 jsou v souladu s požadavky na zabezpečení pro úroveň EAL4 podle normy ISO/IEC 15408. Z hlediska nároků na bezpečnost (v průběhu životního cyklu vyvíjené aplikace) se jedná zejména o soulad s následujícími třídami: „ACM – configuration management“, „ADO – Delivery and operation“, „ALC Life cycle support“ a „ATE – Tests“.

7 SOUVISEJÍCÍ DOKUMENTACE

7.1 Řídící dokumenty

- PP006972 Postup operátora RA CETIN
- Nařízení č. 910/2014 Evropského parlamentu a Rady o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES

7.2 Záznamy

Záznamy vedené operátory RA zachycují dosažené výsledky a poskytují důkaz o provedených činnostech.
Jejich přehled a uložení je uvedeno v PP006972.

8 ZÁVĚREČNÁ A PŘECHODNÁ USTANOVENÍ

Certifikační autorita CA CETIN není součástí kritické informační infrastruktury společnosti, systém je zařazen mezi kritické systémy společnosti (systémy nutné pro podporu a funkčnost interních významných systémů).
Přezkoumávání obsahu tohoto dokumentu se provádí vždy při změně právních předpisů upravujících problematiku PKI (eIDAS), nebo v pravidelných ročních intervalech.
Za provedení kontroly aktuálnosti (revize) obsahu dokumentu odpovídá garant dokumentu. Kontrolou dodržování této směrnice je pověřen manažer pro bezpečnost.

9 PŘÍLOHY

Bez příloh.