Kvalifikovaný poskytovatel certifikačních služeb eIdentity a.s.

ACAeID 21 Certifikační prováděcí směrnice/CPS – QS

eIdentity a.s.
Vinohradská 4,130 00 Praha 3
Tel: 222 866 150-1
fax: 222 866 190
Email: info@eidentity.cz

Verze:	1.5
Odpovídá:	Milan Berka
Datum:	20.04.2021
Utajení:	Veřejný dokument

Schváleno:

Verze	Schválil	
1.5	Ing. Ladislav Šedivý	

Historie dokumentu:

Verze	Datum	Autor	Poznámka
1.0	20.02.2005	Ing. Jiří Hejl	
1.1	20.05.2005	Ing. Jiří Hejl	Konsolidace pojmů, rejstřík
1.2	10.12.2008	Ing. Jiří Hejl	Aktualizace na základě novely zákona č. 455/1991 Sb., přidání rodného listu jako další uznaný osobní doklad, změna kontaktních údajů. Změna OID této certifikační politiky.
1.2	02.11.2009	Ing. Jiří Hejl	Revize dokumentu
1.3	15.5.2014	Doc. RNDr. Milan Berka, CSc.	Upřesnění doby platnosti certifikátů a požadavků na HASH a délku klíče
1.3	05. 03. 2017	Ludmila Daňková Doc. RNDr. Milan Berka, CSc.	Revize dokumentu
1.4	08.02.2019	Doc. RNDr. Milan Berka, CSc.	Úprava povinnosti uchovávat identifikační údaje
1.4	18.08.2019	Milan Berka	Změna Zákona o ochraně osobních údajů
1.5	20.04.2021	Milan Berka	Úprava vzhledem k auditu eIDAS, veřejný dokument

OBSAH

1 ÚVOD

Certifikační prováděcí směrnice se zabývá oblastmi, které již byly podrobněji rozpracovány v jiných dokumentech, především v Certifikačních politikách, vytvořených v rámci tohoto projektu. Protože by nebylo účelné kopírovat stávající dokumenty do certifikační prováděcí směrnice, ve směrnici jsou na několika místech uvedeny pouze odkazy na existující dokumenty. Tyto dokumenty budou k dispozici každému, kdo bude provádět audit tak, aby se mohl seznámit s procedurami podrobněji. Takové rozdělení dokumentů bude snáze udržovatelné, musí se však dbát na aktuálnost verzí dokumentů v odkazech.
Dokument se také odkazuje na platné Certifikační politiky pro poskytované služby. Tyto dokumenty jsou veřejné a jsou přístupné všem.

Certifikační prováděcí směrnice – QS podporuje Certifikační politiky pro kvalifikované služby (Qualified Services – QS).

Struktura předkládaného dokumentu vychází ze dvou dokumentů: RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework a Doporučené struktury CP a CPS vydané Ministerstvem vnitra ČR pro poskytovatele certifikačních služeb vydávajících kvalifikované certifikáty.

Systém je budován a provozován ve shodě s právním prostředím České republiky a EU.

Dokument je určen projektovému týmu projektu a osobám zodpovědným za provoz ACAeID.

Dokument nebude veřejně publikován, ale bude přístupný pro audit ACAeID a pro další definované aktivity, pro které je přístup k Certifikační prováděcí směrnici nezbytný. Veřejná publikace dokumentu představuje bezpečnostní riziko.

Za údržbu tohoto dokumentu odpovídá předseda Výboru pro politiky.

1.1 Přehled

Tato Certifikační prováděcí směrnice (CPS) vznikla proto, aby bylo možné vydávat, používat a zneplatňovat certifikáty vydané ACAeID v souladu s Certifikačními politikami (CP). Postupy, pravidla, technologie a ostatní skutečnosti popsané v této CPS dokladují důvěryhodnost a integritu řešení ACAeID při poskytování certifikačních služeb, a to po celou dobu životního cyklu certifikátů či jiných produktů poskytovaných provozovatelem.

Ve veřejné části webového prostoru budou umístěny informace, které umožní zájemci či žadateli kvalifikovaně se rozhodnout o poskytovaných službách, svých povinnostech a právech. K dispozici mu bude také Certifikační politika a další dokumenty k poskytované službě.

Tato CPS pokrývá oblast kvalifikovaných certifikačních služeb. Zajištění ostatních certifikačních služeb je popsáno v jiných Certifikačních prováděcích směrnicích.

1.2 Název a identifikace dokumentu

Tento dokument má tyto identifikační znaky:

Identifikační znak	Význam identifikačního znaku	Hodnota
Název dokumentu	Název dokumentu v čitelné podobě	Certifikační prováděcí směrnice ACAeID
OID	Identifikace dokumentu v rámci prostoru OID eIdentity a.s.	1.2.203.27112489.1.21.1.4

1.3 Subjekty participující na PKI

1.3.1 Certifikační autority (CA)

Akreditovanou certifikační autoritu eIdentity a.s. tvoří kořenová autorita a autorita vydávající kvalifikované certifikáty (QCA). Kořenová autorita RCA vydává certifikáty pouze podřízeným certifikačním autoritám a vydala tedy i kvalifikovaný systémový certifikát pro kvalifikovanou certifikační autoritu QCA.

Tato komerční autorita QCA nevydává certifikáty pro žádné podřízené certifikační autority, ale jen jednotlivým žadatelům.

Společnost eIdentity a.s. provozuje i další certifikační autority, které se řídí svými Certifikačními politikami a provozními předpisy.

Pro zajištění potřebné úrovně bezpečnosti provozu se využívá služeb neveřejné interní Operátorské autority, která vydává certifikáty pouze pro technologické komponenty a operátory systému ACAeID.

1.3.2 Registrační autority (RA)

Jako Registrační autority pracují důvěryhodní Operátoři registračního místa, kteří provádějí proces ověření skutečností nutných pro vydání certifikátu. S každým Operátorem registračního místa je uzavřen smluvní vztah, operátoři jsou pravidelně školeni a kontrolováni. Operátorem se může stát pouze osoba, která splní kvalifikační předpoklady.

1.3.3 Držitelé kvalifikovaných certifikátů – podepisující/pečetící osoby

Podepisující osobou se stává každá fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby a je držitelem kvalifikovaného certifikátu vydaného ACAeID podle Zákona 297/2016 Sb..

Označující/pečetící osobou je každá fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek/pečetí a je držitelem kvalifikovaného certifikátu, vydaného ACAeID podle Zákona 297/2016 Sb...

1.3.4 Spoléhající se strany

Spoléhající se stranou je každý jedinec nebo skupina, která využívá certifikátů vydaných ACAeID a/nebo elektronických podpisů a pečetí nebo značek s nimi souvisejících.

1.3.5 Jiní účastníci

Další účastníci jsou kontrolní a regulační orgány státu podle Zákona a orgány činné v trestním řízení, případně další orgány, kterým to ze zákona přísluší.

1.4 Použití certifikátu

Certifikáty vydané podle této směrnice se mohou použít jen k účelům, které předpokládá Zákona, který specifikují Certifikační politiky.

1.4.1 Přípustné použití certifikátu

Typickými aplikacemi, které je možné použít v souvislosti s certifikáty vydávanými podle této politiky, jsou aplikace umožňující vytvářet a ověřovat elektronické podpisy jako například systémy elektronické pošty, podepisovací a ověřovací aplikace pro podepisování dokumentů a jiných typů souborů obecně, pokud jsou v souladu s požadavky Zákona.

1.4.2 Nepřípustné použití certifikátu

Certifikáty se nesmí používat v rozporu s účelem, ke kterému byly vydány, a to jak z technického hlediska (např. podle omezení KeyUsage), tak i z právního hlediska (např. v rozporu se Zákonem).

1.5 Správa politiky

Za údržbu tohoto dokumentu odpovídá předseda Výboru pro politiky.

1.5.1 Organizace spravující dokument

eIdentity a.s.
Vinohradská 184
130 00 Praha 3
Česká republika

1.5.2 Kontaktní osoba

Předseda Výboru pro politiky
eIdentity a.s.
Vinohradská 184
130 00 Praha 3
Česká republika

Tel: +420 222 866 150
Fax: +420 222 866 159
Email: PAA-manager@eidentity.cz

1.5.3 Subjekt odpovědný za rozhodování o souladu dokumentace

Soulad těchto politik schvaluje Výbor pro politiky na základě schůze Výboru a v souladu s jednacím řádem tohoto orgánu. Před tím jsou politiky projednány na Poradě vedení a jsou poskytnuty k připomínkování členům vedení společnosti. Jednotlivé směrnice jsou projednány na Poradě vedení společnosti.

1.5.4 Postupy schvalování

Postupy jsou určeny jednacím řádem Výboru pro politiky. Směrnice schvaluje Porada vedení společnosti.

1.6 Přehled použitých pojmů a zkratek

Zákon	Zákon 297/2016 Sb. o elektronickém podpisu
ACAeID, ACA	akreditovaná certifikační autorita eIdentity a.s. poskytující kvalifikované certifikační služby
RCA	Kořenová certifikační autorita
CCA	Komerční certifikační autorita
RM	Registrační místo
ORM	Operátor registračního místa
CP	Certifikační politika
CPS	Certifikační prováděcí směrnice
CC	Komerční certifikát
CSC	Komerční serverový certifikát
RQSC	Kořenový kvalifikovaný systémový certifikát
CRL	Seznam zneplatněných certifikátů
poskytovatel, PCS	Poskytovatel certifikačních služeb
EVI	Evidenční část informačního systému PCS
revokace	zneplatnění certifikátu
DN	Distiguished Name – Jednoznačná identifikace držitele certifikátu

2 ODPOVĚDNOST ZA PUBLIKOVÁNÍ A ÚLOŽIŠTĚ

ACAeID zveřejňuje seznam vydaných kvalifikovaných certifikátů a seznam zneplatněných certifikátů.

2.1 Úložiště

V informačním systému ACAeID jsou zpracovávány a uchovávány informace v souladu se Zákonem tak, aby záznamy nebo jejich změny mohly provádět pouze pověřené osoby, aby bylo možno kontrolovat správnost záznamů, a aby jakékoliv technické nebo programové změny porušující tyto bezpečnostní požadavky byly zjevné. Zveřejňované informace jsou určeny zejména spoléhajícím se třetím stranám, aby bylo možné rozhodnout o platnosti kvalifikovaného certifikátu s požadovaným stupněm důvěry.

2.2 Zveřejňování informací

K veřejným informacím je možné přistupovat pomocí webových služeb.

Vydané certifikáty jsou zveřejněny v Seznamu vydaných certifikátů, který bude publikován na adresách, které jsou uvedeny v jednotlivých certifikačních politikách.

Veřejně dostupné jsou tyto položky certifikátu:

- Sériové číslo certifikátu
- Platnost od – do

U certifikátů, k jejichž zveřejnění dal držitel souhlas, budou veřejně dostupné ještě tyto položky:

- Držitel (Subjekt)
- Vlastní certifikát ve formátu DER, PEM a TXT

Certifikáty, které byly zneplatněny, budou zveřejněny v Seznamu zneplatněných certifikátů. Tento seznam bude dostupný (vždy nejméně na jednom místě) v elektronické formě ve formátu CRL na adresách, které jsou uvedeny v certifikačních politikách:

V osobním účtu Žadatele může žádající osoba získat další podrobnější informace o stavu své žádosti či o odebíraných službách. Tyto informace jsou však neveřejné a jsou dostupné jen příslušné osobě Žadatele. Údaje v osobním účtu jsou chráněny v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, dobu jejich uchovávání a strukturu stanovuje Zákon.

Součástí veřejně dostupných informací jsou také dokumenty jednotlivých Certifikačních politik, které jsou zveřejněny na WWW stránkách společnosti.

Zveřejněny jsou také certifikáty všech vydávajících autorit.

Dále jsou zveřejněny i procesní, obchodní a další pomocné informace, které se vztahují k poskytovaným službám.

2.3 Periodicita zveřejňování

Publikování CP a CPS schvaluje a odpovědnou osobu určuje Výbor pro politiky v souladu s jednacím řádem tohoto Výboru.

Certifikační politika je schválena dříve, než je podle ní možné vydat první certifikát. Periodicita zveřejňování dalších informací není určena a závisí na nutnosti udržovat informace v aktuálním stavu. Periodicita zveřejňování CRL je popsána dále v dokumentu a v certifikačních politikách. Řídí se požadavky Zákona a Nařízení.

2.4 Řízení přístupu k úložišti

Publikování CP schvaluje a odpovědnou osobu určuje Výbor pro politiky v souladu s jednacím řádem tohoto výboru.

Zveřejnění a aktualizaci Seznamu vydaných certifikátů a Seznamu zneplatněných certifikátů provádí Operátor CA.

Frekvence zveřejňování informací probíhá v souladu s tímto dokumentem.

3 IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

Certifikáty CA eIdentity a.s. obsahují v polích Subject a Issuer jména ve formátu X.501. Aktuální stav je vždy popsán v platné certifikační politice.
Certifikát uživatele musí obsahovat alespoň jeden z atributů CN nebo Pseudonym.

3.1.2 Požadavek na sémantický význam jmen

Všechna pojmenování uvedená v DN certifikátu musí být smysluplná a doložitelná.

3.1.3 Anonymita a používání pseudonymu

CA eIdentity nevydává anonymní certifikáty. Certifikát lze vystavit na pseudonym. Tato skutečnost je v certifikátu jednoznačně určena atributem Pseudonym.

3.1.4 Pravidla pro interpretaci různých forem pojmenování

Tam, kde to RFC3280 dovoluje, lze použít národní znakové sady UTF8.

3.1.5 Jednoznačnost jmen

CA eIdentity zaručuje automatickou kontrolou unikátnost vazby DN v poli Subject certifikátu na jednoho konkrétního uživatele. Uživatel však může mít více certifikátů se stejným DN v poli Subject.

3.1.6 Rozpoznávání, autentizace a význam obchodních značek

Všechny údaje uvedené v certifikátu uživatele se musí prokazatelně vztahovat k jeho osobě. CA eIdentity tuto skutečnost ověřuje. To vylučuje možnost zneužití obchodní značky třetí osoby.

3.2 Počáteční ověření identity

3.2.1 Metody důkazu vlastnictví (POP – proof of possession) soukromého klíče

Žadatel o certifikát musí prokázat vlastnictví soukromého klíče odpovídající veřejnému klíči, který má být uveden v certifikátu. Za prokazatelnou se považuje žádost ve formátu PKCS#10 nebo ekvivalentní metoda (SPKAC). Principem je předání veřejného klíče spolu s případnými dalšími daty certifikační autoritě tak, aby tento balík byl podepsán odpovídajícím soukromým klíčem. V případě vygenerování párových dat certifikační autoritou není důkaz vlastnictví nutný.

3.2.2 Prokázání identity právnické osoby

Identitu prokazuje organizace předložením originálu nebo ověřeného opisu výpisu

z obchodního rejstříku, výpisu ze živnostenského rejstříku či jiné listiny, na základě, které byla organizace zřízena. Z dokladu musí být patrno úplné obchodní jméno organizace, přidělené identifikační číslo, sídlo a statutární orgán. Pro účely komunikace s eIdentity a.s. může statutární orgán zplnomocnit další osobu. Podpisy na dokumentech musí být ověřitelné.

3.2.3 Prokázání identity fyzické osoby

Fyzická osoba prokazuje svoji identitu platným, nepoškozeným osobním dokladem a pro účely vydání kvalifikovaného certifikátu dokládá svoje identifikační údaje dvěma platnými, nepoškozenými osobními doklady. Osobní doklady jsou přijímány za předpokladu, že jsou platné a že z nich lze zjistit identitu žadatele.

Občan ČR předkládá jako primární osobní doklad platný občanský průkaz.

Cizinec předkládá jako primární osobní doklad platný cestovní, služební, cizinecký, diplomatický nebo jinak nazvaný pas vydaný cizím státem; nebo průkaz o povolení k pobytu vydaný příslušným orgánem ČR. Občan členského státu Evropské unie, občan Islandu, Lichtenštejnska, Norska a Švýcarska může předložit jako osobní doklad také doklad, který mu byl vydán jako doklad k prokazování totožnosti na území příslušného státu. Typ dokladu a údaje v něm obsažené musí být psány latinkou. Doklad musí obsahovat anglický překlad údajů v něm uvedených.

Jako druhý osobní doklad, za předpokladu, že nebyl předložen jako primární, se přijímá u občana ČR platný cestovní pas, řidičský průkaz nebo rodný list.

Jako druhý osobní doklad, za předpokladu, že nebyl předložen jako primární, se přijímá u cizince platný řidičský průkaz, cestovní, služební, cizinecký, diplomatický nebo jinak nazvaný pas vydaný cizím státem; nebo průkaz o povolení k pobytu vydaný příslušným orgánem ČR. Občan členského státu Evropské unie, občan Islandu, Lichtenštejnska, Norska a Švýcarska může předložit Jako druhý osobní doklad, za předpokladu, že nebyl předložen jako primární, se přijímá jako osobní doklad také doklad, který mu byl vydán jako doklad k prokazování totožnosti na území příslušného státu. Typ dokladu a údaje v něm obsažené musí být psány latinkou. Doklad musí obsahovat anglický překlad údajů v něm uvedených.

Dojde-li v době platnosti certifikátu ke změně údajů, je držitel povinen oznámit poskytovateli změnu údajů. V případě, že se jedná o změnu údajů uvedených v certifikátu, dojde ke zneplatnění certifikátu. **Při vydání dalšího certifikátu je nutné každý změněný údaj ověřit.**

3.2.4 Neověřované informace

Všechny informace uvedené v certifikátu od ACAeID jsou ověřené.

3.2.5 Ověřování specifických práv

V případě, že žadatel požaduje umístit do certifikátu informaci o jeho pracovní pozici v organizaci (viz Titul či pracovní role v DN), dokládá tuto skutečnost souhlasem organizace, který je v písemné podobě a je podepsán statutárním orgánem nebo osobou, která má zmocnění ke komunikaci s eIdentity a.s. Podpis musí být ověřitelný. (Např. telefonicky, notářem apod.) O ověření je třeba provést záznam.

3.2.6 Kritéria pro interoperaci (spolupráci)

CA eIdentity může spolupracovat s CA třetích stran pouze při splnění následujících podmínek

- Spolupracující CA uzavře s CA eIdentity smlouvu o spolupráci.
- CPS spolupracující CA splňuje požadavky CPS eIdentity.
- Je prokázána shoda CPS se skutečnou praxí spolupracující CA. Tuto shodu je nutno prokazovat každoročně.

3.3 Identifikace a autentizace pro požadavky na výměnu klíče (Re-key)

3.3.1 Identifikace a autentizace pro rutinní výměnu klíče

Tato služba se neposkytuje.

3.3.2 Identifikace a autentizace pro výměnu klíče po zneplatnění

Tato služba se neposkytuje.

3.4 Identifikace a autentizace pro požadavek na zneplatnění

O zneplatnění certifikátu může požádat držitel, podepisující osoba nebo označující osoba.

Certifikát zneplatňuje poskytovatel

- na základě přijaté žádosti o zneplatnění
- pokud žadatel kvalifikovaný certifikát nepřevezme
- pokud žadatel požádá o ukončení zpracování osobních údajů
- na základě uvědomění držitele nebo podepisující osoby, že hrozí nebezpečí zneužití jejich dat pro vytváření elektronických podpisů
- v případě, že byl kvalifikovaný certifikát vydán na základě nepravdivých nebo chybných údajů
- dozví-li se prokazatelně, že podepisující osoba zemřela nebo zanikla nebo ji soud způsobilosti k právním úkonům zbavil nebo omezil
- dozví-li se prokazatelně, že údaje, na jejichž základě byl kvalifikovaný certifikát vydán, pozbyly pravdivosti
- pokud mu Ministerstvo nařídí zneplatnění kvalifikovaného certifikátu jako předběžné opatření, pokud existuje důvodné podezření, že kvalifikovaný certifikát byl padělán nebo pokud byl vydán na základě nepravdivých údajů nebo v případě, kdy bylo zjištěno, že podepisující osoba používá prostředek pro vytváření podpisu, který vykazuje bezpečnostní nedostatky, které umožňují padělání zaručených elektronických podpisů nebo změnu podepisovaných údajů.

Pokyn pro zneplatnění může podat držitel nebo podepisující osoba pro své certifikáty nebo odpovědná osoba eIdentity a.s. pro ostatní případy.

Žádost o zneplatnění nebo uvědomění držitele nebo podepisující osoby musí být v písemné formě a musí obsahovat

- Sériové číslo certifikátu
- Označení držitele, kterému byl certifikát vydán
- Heslo pro zneplatnění certifikátu

Pokud si žadatel heslo nepamatuje nebo ho nezná, musí žádost o zneplatnění podat osobně na registračním místě, kde musí také prokázat svou totožnost. V případě, že žádost o zneplatnění podává držitel, jímž je organizace, musí být žádost podepsána statutárním orgánem nebo osobou, která má oprávnění jednat za společnost. Podpis musí být ověřitelný.

Žádost o zneplatnění nebo uvědomění držitele nebo podepisující osoby lze podat (nejméně jedna možnost je vždy dostupná)

- Elektronicky v účtu žadatele
- Osobně na RM
- Faxem na číslo dle kapitoly Certifikačních politik.

Žádost podaná faxem je zpracována následující pracovní den po doručení žádosti poskytovateli.

Pokyn pro zneplatnění může podat žadatel pro své certifikáty nebo Security Officer pro ostatní případy. Pokyn poté vykoná Operátor CA.

4 FUNKČNÍ POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Kdo může podat žádost o vydání certifikátu

O kvalifikovaný certifikát může žádat každá fyzická osoba, která je povinna uvádět pouze pravdivé informace a tyto také odpovídajícím způsobem doložit. Žádat může pouze ten, koho soud způsobilosti k právním úkonům nezbavil nebo neomezil.

4.1.2 Registrační proces a odpovědnosti

Vlastní registrace žádosti je rozdělena do dvou oblastí. První oblastí je evidence žadatelů a výběr služby. Druhou oblast tvoří prokázání skutečností uvedených ve fázi evidence, a pokud je prokázání dostatečné, dojde k vydání certifikátu.

Evidence údajů je plně v zodpovědnosti žadatele. Žadatel je zodpovědný za to, že uváděné údaje jsou správné, úplné a pravdivé. Evidované údaje pak prokazuje v procesu ověření na registračním místě.

Za ověření údajů zodpovídá Operátor registračního místa, který je také plně zodpovědný za schválení těchto údajů a za vystavení certifikátu. Operátor registračního místa pracuje podle seznamu úkonů procesu registračního místa, který je připraven na základě struktury uváděných údajů. O průběhu procesu registračního místa je pořízen Protokol o průběhu procesu registračního místa.

Operátor registračního místa je oprávněn žádost zrušit a certifikát nevydat, pokud není přesvědčen, že uváděné údaje jsou odpovídajícím způsobem doloženy. Žadatel může reklamovat práci Operátora registračního místa u vedení eIdentity a.s. s uvedením podrobností případu.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

4.2.1.1 Zájem o službu

Předpokládá se webový formulář, který je přístupný přes SSL/TLS a jehož obsahem je vysvětlení pravidel, účelu a použití kvalifikovaného certifikátu, včetně podmínek pro jeho užívání (doporučený HW, SW apod.) na straně žadatele a požadavky na držitele vyplývající ze zákona 297/2016 Sb.

Zájemce vyplní:

- Jméno (včetně dalšího jména apod.)
- Příjmení
- V systému unikátní email adresa s výhradním právem přístupu zájemce
- V systému unikátní přihlašovací jméno

Na uvedenou emailovou adresu následně odejde email s URL a heslem, na základě, kterého zájemce pokračuje v procesu žádosti. Tím se ověří platnost emailové adresy. Heslo má omezenou platnost 5 dní. Přihlašovací jméno se emailem nepřenáší, zájemce si ho musí pamatovat nebo si stránku vytisknout.

Pokud uvedená emailová adresa již je evidována u jiného žadatele, dojde zde k jejímu odmítnutí. Systém nedovolí také duplicitu přihlašovacích jmen. Na stránce bude také specifikován povolený formát vstupních dat s uvedením příkladu vyplnění.

Pokud nedojde k přihlášení zájemce do systému do konce omezené platnosti hesla nebo na příkaz Operátora EVI se záznam o zájemci ze systému odstraní. Na takto pořízené údaje se hledí tak, jako by nebyly použity. Nevztahuje se na ně povinnost je uchovávat po Zákonem definovanou dobu.

4.2.1.2 Vyplnění identifikačních údajů žadatele

Webový formulář je dostupný v účtu klienta. Přístup je přes SSL/TLS, autentizace přihlašovacím jménem a zaslaným heslem. Autentizace může být také certifikátem od jiné určené certifikační autority eIdentity a.s.

Žadatel vyplní:

- Jméno – pevně vyplněno z minulého kroku
- Příjmení – pevně vyplněno z minulého kroku
- Email spojení – pevně vyplněno z minulého kroku
- Celé jméno – vznikne ze Jména a Příjmení, nelze měnit
- Adresa bydliště
- Číslo primárního osobního dokladu
- Typ a znaky dalšího dokladu, který bude předložen při osobní návštěvě na registračním místě
- Registrované další emailové adresy (po zadání nové emailové adresy na ni bude zaslán email s URL pro potvrzení adresy).

Takto je popsán subjekt žadatele pro účely zákona. Tomuto subjektu – žadateli se vytvoří účet v informačním systému EVI, ve kterém jsou vedeny informace o historii jeho žádostí o certifikáty a o jeho vydaných certifikátech. Bude zde i možnost měnit identifikační údaje (je vedena i jejich historie) s následným posouzením Operátorem EVI, zda tato změna má či nemá vliv na již vydané certifikáty (zda dojde k administrativnímu zneplatnění apod.) a zda je případně nutná opětovná osobní návštěva na registračním místě.

Zde je možné také měnit přístupové heslo k účtu žadatele.

4.2.1.3 Účet žadatele

Účet žadatele obsahuje informace o evidovaných osobních údajích, nabídku dostupných služeb, přehled rozpracovaných žádostí a vydaných certifikátů.

Vydání následného certifikátu je možné vyřídit elektronicky. Žadatel bude upozorněn zprávou

na primární emailovou adresu o blížícím se termínu vypršení platnosti kvalifikovaného certifikátu. Pokud se nezměnily skutečnosti, které uvedl při žádosti o kvalifikovaný certifikát, bude mu na jeho žádost, kterou tímto ještě platným certifikátem podepíše, vydán následný certifikát se stejnými údaji. Takový certifikát bude mít však odlišné některé položky obsahu, například dobu platnosti, jiné sériové číslo certifikátu, bude vytvořen pro nový veřejný klíč žadatele a mohou být změněny i informace o akreditované vystavující (QCA), komerční (CCA) či kořenové (RCA) certifikační autoritě.

V osobním účtu žadatele bude také možné požádat o zneplatnění certifikátu či zrušit probíhající žádost o vydání.

Účet žadatele může být doplněn o další nabízené služby.

4.2.1.4 Žádost o vydání kvalifikovaného certifikátu

Na tento webový formulář se přejde z odkazu Žádosti o další certifikát z tabulky seznamu kvalifikovaných certifikátů žadatele. Žadatel může mít k dispozici jeden či více kuponů, které budou označovat nestandardní platební či procesní podmínky.

Předvyplněno bude:

- Označení, že je certifikát vydán jako kvalifikovaný certifikát podle zákona 297/2016 Sb.
- Název obchodní firmy kvalifikovaného poskytovatele a stát, ve kterém je poskytovatel usazen
- Elektronická značka kvalifikovaného poskytovatele založená na kvalifikovaném certifikátu poskytovatele
- CDP – odkaz, kde lze přistoupit k CRL
- Politika, podle které došlo k vydání
- Celé jméno
- Jméno
- Příjmení

Poskytovatel doplní dodatečně v okamžiku vydání kvalifikovaného certifikátu:

- Správný datum a čas počátku a konce platnosti kvalifikovaného certifikátu
- Unikátní číslo vydávaného kvalifikovaného certifikátu
- Data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby
- Zda se jedná o pseudonym

Žadatel vyplní:

- DN subjektu včetně jména či pseudonymu či pracovního zařazení
- Emailová adresa – výběr ze seznamu registrovaných emailových adres nebo žádná
- Omezení kvalifikovaného certifikátu podle povahy a rozsahu jen pro určité použití (Key Usage)
- Unikátní identifikace žadatele u eIdentity a.s. – doplní pevně systém (ACA-SerialNumber) nebo údaj spravovaný ústředním orgánem státní správy, na základě,

kterého je možné osobu jednoznačně identifikovat (BIO) nebo pověří poskytovatele, aby takový údaj u ústředního orgánu státní správy zajistil
- Volitelně označení kuponu na speciální cenu či akci
- Vyjádření souhlasu se zveřejněním certifikátu
- Heslo pro zneplatnění certifikátu.

Pokud pravidla ústředního orgánu státní správy pro přidělení údaje BIO vyžadují uvedení dalších osobních údajů, pak tyto osobní údaje budou zpracovány se souhlasem subjektu údajů v nezbytné míře pouze pro účely vystavení údaje BIO a poté budou zničeny.

Po vyplnění bude žádost odeslána k formální kontrole Operátorem EVI. Formální kontrola prozkoumá jednak obsah připravovaného komerčního certifikátu a také platnost kuponu na speciální cenu či akci ve vztahu k poskytované službě. Formální kontrola může také určit, jaké skutečnosti musí žadatel doložit (a také jak) při vydávání komerčního certifikátu.

4.2.1.5 Žádost o vydání kvalifikovaného certifikátu pro pečeť

Na tento webový formulář se přejde z odkazu Žádosti o další certifikát z tabulky seznamu kvalifikovaných certifikátů žadatele.

Předvyplněno bude:

- Označení, že je certifikát vydán jako kvalifikovaný certifikát podle zákona 297/2016 Sb.
- Název obchodní firmy kvalifikovaného poskytovatele a stát, ve kterém je poskytovatel usazen
- Elektronická značka kvalifikovaného poskytovatele založená na kvalifikovaném certifikátu poskytovatele
- CDP – odkaz, kde lze přistoupit k CRL
- Politika, podle které došlo k vydání kvalifikovaného certifikátu / pečeti

Poskytovatel doplní dodatečně v okamžiku vydání kvalifikovaného certifikátu:

- Správný datum a čas počátku a konce platnosti kvalifikovaného certifikátu
- Unikátní číslo vydávaného kvalifikovaného certifikátu
- Data pro ověřování elektronických značek, která odpovídají datům pro vytváření elektronických značek, jež jsou pod kontrolou označující osoby

Žadatel vyplní:

- Jednoznačnou identifikaci držitele
- Jednoznačnou identifikaci označující osoby, případně také prostředku pro vytváření elektronických značek
- Emailová adresa – výběr ze seznamu registrovaných emailových adres nebo žádná
- Omezení kvalifikovaného certifikátu podle povahy a rozsahu jen pro určité použití (KeyUsage)
- Označení kuponu (bonu) na speciální cenu či akci
- Vyjádření souhlasu se zveřejněním certifikátu

- Heslo pro zneplatnění.

Po vyplnění bude žádost odeslána k formální kontrole. Formální kontrola prozkoumá jednak obsah připravovaného kvalifikovaného certifikátu a také platnost kuponu na speciální cenu či akci ve vztahu k vydávanému kvalifikovanému systémovému certifikátu. Formální kontrola také určí, jaké skutečnosti bude muset žadatel doložit (a také jak) při vydávání kvalifikovaného certifikátu.

4.2.1.6 Smlouva a platba

Po úspěšné formální kontrole (a případných opravách žádosti) bude připraven návrh smlouvy na vydání odpovídajícího kvalifikovaného certifikátu, bude generována výzva k zálohové platbě za službu a oba dokumenty budou elektronicky zaslány žadateli. Po obdržení platby na účet, zajištění požadovaných údajů BIO a odsouhlasení smlouvy o poskytnutí služby žadatelem bude uvolněno generování klíčů a zaslání žádosti o certifikát dle PKCS#10 nebo obdobným způsobem. Teprve nyní, po doplnění evidenčních údajů do formátu podle PKCS#10 (nebo obdobného) se na tyto údaje pohlíží jako na úplnou Žádost o poskytnutí služby. Žádost se přenáší do systému CA, kde dochází k registračnímu procesu a k vlastnímu vydání certifikátu.

Ve smlouvě žadatel stvrdí mimo jiné, že:

- poskytl přesné a kompletní informace podle požadavku CP
- používá výhradně klíčového páru v souladu s ostatním omezením
- učinil účelná opatření k zabránění neautorizovaného použití soukromého klíče
- generoval klíče
    - algoritmem určeným pro účely kvalifikované služby
    - délka klíče vyhovuje pro účely kvalifikovaného služby
    - tak, že zůstal výhradním držitelem soukromého klíče dle požadavků dané služby
- upozorní bez zbytečného odkladu v době platnosti certifikátu
    - že soukromý klíč byl ztracen, zcizen či existuje možnost zneužití
    - že se soukromý klíč nenachází pod výhradní kontrolou držitele z důvodu možného zneužití aktivačních dat (PIN) nebo z jiných důvodů
    - na nepřesnosti nebo změny údajů, na základě, kterých byl certifikát vydán
- v případě kompromitace soukromého klíče ho přestane okamžitě a napořád používat
- zda souhlasí se zveřejněním vydaného certifikátu

Daňový doklad za poskytnuté služby je zaslán poštou.

4.2.1.7 Registrační místo

Operátor registračního místa postupuje podle schváleného postupu a provede kontrolu

vyplněných informací oproti předloženým dokumentům. Pokud bude vše v pořádku, pořídí opisy dokladů a dokumentů, na jejichž základě došlo k ověření údajů a doplní je o prohlášení žadatele, že ten souhlasí s jejich archivací po dobu, kterou stanovuje Zákon.

Operátor uzavře smlouvu s žadatelem o poskytnutí služby, zadá pokyn k vystavení certifikátu a ten po jeho vystavení protokolárně předá žadateli.

Žadatel obdrží Smlouvu o poskytování služby, Protokol o průběhu procesu registračního místa a Protokol o převzetí certifikátu.

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Pokyn k vystavení certifikátu může vydat Operátor registračního místa na základě uzavřené písemné Smlouvy o poskytování služeb, a to pouze v případě, že si je jist správným doložením údajů ze strany Žadatele a splněním jeho dalších povinností (zejména uhrazení ceny za poskytovanou službu na základě Výzvy k platbě apod.).

Při nedostatečnosti při prokazování údajů či při jiném porušení registračního procesu musí Operátor zamítnout žádost a neposkytnout objednávanou službu. Případné následující kroky (např. forma vrácení zálohové platby apod.) bude řešena se Žadatelem či plátcem individuálně.

4.2.3 Doba zpracování žádosti o certifikát

Časový limit, ve kterém dojde ke zpracování žádosti o certifikát, není pevně stanoven. Jedná se o interaktivní proces, jehož délku určuje převážně žadatel. Společnost eIdentity a.s. poskytuje certifikační služby bez zbytečného odkladu.

Po provedené platbě na základě zaslané výzvy je žádost považována za závaznou objednávku. Žadatel má možnost navrhnout termín schůzky pro vydání certifikátu. Pokud se žadatel pro vyzvednutí certifikátu nedostaví do 30 dnů od zaplacení nebo si nedomluví jiný postup, žádost je zrušena. Provedená platba je žadateli vrácena snížena o prokazatelné náklady spojené s marným poskytnutím plnění objednaných služeb ve výši 40% účtované částky.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

Vydáním pokynu k vystavení certifikátu pro interní systém CA se sestaví obsah certifikátu, spočte z něj otisk podle schváleného schématu elektronického podpisu (SHA2) a předá ho k podepsání na Podepisovací pracoviště. Zde dojde k podepsání otisku a získaný podpis odešle zpět do CA ke konečnému vytvoření certifikátu ve formátech DER, PEM a TXT.

4.3.2 Oznamování vydání certifikátu podepisující osobě

Certifikát ve výše zmíněných formátech je od tohoto okamžiku k dispozici trvale v osobním účtu žadatele a jeho obsah je součástí Protokolu o převzetí certifikátu.

4.4 Převzetí certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Součástí předání certifikátu je i Protokol o převzetí certifikátu, ve kterém žadatel stvrzuje převzetí certifikátu. Certifikát, který byl vydán v souladu s touto CPS a CP nelze odmítnout. Žadatel může požádat však ihned o zneplatnění.

Protokol o převzetí certifikátu obsahuje výpis certifikátu v textové formě, ze které je zřejmý obsah certifikátu, okamžik převzetí a podpis žadatele a ORM. Jednu kopii si odnáší žadatel a druhá kopie zůstává součástí dokumentace žádosti.

Pokud protokol obsahuje chybné údaje a žadatel jej přesto převezme a potvrdí, nese díl odpovědnosti za případné následky. Např. privátní klíč není v QSCD i když je to v certifikátu uvedeno.

4.4.2 Zveřejňování vydaných certifikátů certifikační autoritou

Vydaný kvalifikovaný certifikát je po převzetí umístěn do seznamu vydaných kvalifikovaných certifikátů. Zveřejněny jsou pouze tyto údaje:

- Sériové číslo certifikátu
- Doba platnosti od-do

V případě, že žadatel souhlasil se zveřejněním certifikátu, jsou ještě navíc zobrazeny údaje:

- Držitel (subject)
- Certifikát ve formátu DER
- Certifikát ve formátu PEM
- Certifikát v textové formě

4.4.3 Oznámení vydání certifikátu jiným subjektům

CA informuje o vydání certifikátu odpovídajícího ORM vyhotovením Protokolu o převzetí certifikátu.

4.4.4 Uchovávání údajů o žadateli

Po vydání a převzetí certifikátu se uchovávají údaje, umožňující jednoznačnou identifikaci fyzické osoby – vztahuje se na totožnost žadatele o vydání všech kvalifikovaných certifikátů dle nařízení eIDAS (i totožnost fyzické osoby oprávněné jednat za právnickou osobu žádající o vydání kvalifikovaného certifikátu pro elektronickou pečeť) po zákonem stanovenou dobu (10 let). Do vydání certifikátu je možné na žádost žadatele údaje odstranit.

4.5 Použití párových klíčů a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem/podepisující osobou

Soukromý klíč, který se vztahuje k vydanému kvalifikovanému certifikátu, může být použit pouze v souladu se Zákonem a se Smlouvou a toto použití je povoleno až po předchozím převzetí odpovídajícího kvalifikovaného certifikátu a musí být ukončeno po uplynutí doby platnosti či při zneplatnění tohoto kvalifikovaného certifikátu.

Podepisující osoba je povinna zacházet s daty pro vytváření elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití a uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný certifikát o tom, že hrozí nebezpečí zneužití jejich dat pro vytváření zaručeného elektronického podpisu.

4.5.2 Používání veřejného klíče a certifikátu spoléhající se stranou

Spoléhající strana může spoléhat pouze na certifikáty a veřejné klíče, které byly vydány a používány v souladu s odpovídající certifikační politikou, použity v souladu s údaji v certifikátu, a které nemají označen za neplatný žádný certifikát ve svém certifikačním řetězci. Spoléhající se strana je plně zodpovědná za veškeré úkony, které je musí vykonat před tím, než získá důvěru v platnost certifikátu a veřejného klíče. Doporučený postup je uveden např. v Nařízení vlády č. 495/2004 Sb. a Vyhlášce 496/2004 Sb. k elektronickým podatelnám.

4.6 Obnovení certifikátu

Tato možnost se neposkytuje. Je možné požádat o vydání následného certifikátu.

4.6.1 Okolnosti pro obnovení certifikátu

Tato možnost se neposkytuje.

4.6.2 Kdo může požadovat obnovení

Tato možnost se neposkytuje.

4.6.3 Zpracování požadavku na obnovu certifikátu

Tato možnost se neposkytuje.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli/podepisující osobě

Tato možnost se neposkytuje.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Tato možnost se neposkytuje.

4.6.6 Zveřejňování vydaných obnovených certifikátů certifikační autoritou

Tato možnost se neposkytuje.

4.6.7 Oznamování vydání certifikátu jiným subjektům

Tato možnost se neposkytuje.

4.7 Výměna klíče (re-key) v certifikátu

Tato možnost se neposkytuje.

4.7.1 Okolnosti pro výměnu klíče v certifikátu

Tato možnost se neposkytuje.

4.7.2 Kdo může požadovat výměnu klíče v certifikátu

Tato možnost se neposkytuje.

4.7.3 Provedení požadavku na výměnu klíče

Tato možnost se neposkytuje.

4.7.4 Oznámení o vydání certifikátu s vyměněným klíčem podepisující osobě

Tato možnost se neposkytuje.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným klíčem podepisující osobou

Tato možnost se neposkytuje.

4.7.6 Zveřejňování vydaných certifikátů s vyměněným klíčem

Tato možnost se neposkytuje.

4.7.7 Oznámení o vydání certifikátu s vyměněným klíčem jiným subjektům

Tato možnost se neposkytuje.

4.8 Změna certifikátu (modification)

Tato možnost se neposkytuje.

4.8.1 Okolnosti pro změnu certifikátu

Tato možnost se neposkytuje.

4.8.2 Subjekty oprávněné požadovat změnu certifikátu

Tato možnost se neposkytuje.

4.8.3 Zpracování požadavku na změnu certifikátu

Tato možnost se neposkytuje.

4.8.4 Oznámení o vydání změněného certifikátu podepisující osobě

Tato možnost se neposkytuje.

4.8.5 Úkony spojené s převzetím změněného certifikátu

Tato možnost se neposkytuje.

4.8.6 Zveřejňování vydaných změněných certifikátů

Tato možnost se neposkytuje.

4.8.7 Oznámení o vydání změněného certifikátu jiným subjektům

Tato možnost se neposkytuje.

4.9 Zneplatnění a pozastavení platnosti certifikátu

4.9.1 Okolnosti pro zneplatnění certifikátu

Podepisující osoba musí neprodleně požádat o zneplatnění certifikátu v případě, kdy hrozí nebezpečí zneužití dat pro vytváření zaručeného elektronického podpisu.

Zneplatnit certifikát může i vydavatel v souladu s bodem 3.4. této CPS.

Zneplatněný certifikát nemůže být obnoven.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění může požádat pouze držitel certifikátu nebo na základě skutečností dle bodu 3.4 této CPS.

Zneplatnění certifikátu CA musí být schváleno dvěma osobami najednou.

4.9.3 Provedení požadavku na zneplatnění certifikátu

Musí být provedeno v souladu s bodem 3.4 této CPS.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

Tato doba není specifikována

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

Certifikát je zneplatněn neprodleně. Informace o zneplatnění certifikátu se musí objevit v prvním zveřejněném CRL do uplynutí 12 hodin od přijetí žádosti o zneplatnění.

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

Spoléhající se strany musí kontrolovat platnost všech certifikátů v certifikačním řetězci – viz kapitola 4.5.2 této CPS.

4.9.7 Periodicita vydávání CRL

CRL se vydává denně s periodicitou 12 hodin.

4.9.8 Maximální zpoždění CRL

CRL se zveřejňuje neprodleně.

4.9.9 Možnost ověřování zneplatnění/statusu certifikátu on-line

Tato služba se neposkytuje.

4.9.10 Požadavky při on-line ověřování zneplatnění/statusu certifikátu

Tato služba se neposkytuje.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Tato služba se neposkytuje.

4.9.12 Speciální podmínky při kompromitaci soukromého klíče

Tato služba se neposkytuje.

4.9.13 Okolnosti pro pozastavení platnosti certifikátu

Tato služba se neposkytuje.

4.9.14 Kdo může požadovat pozastavení platnosti certifikátu

Tato služba se neposkytuje.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

Tato služba se neposkytuje.

4.9.16 Omezení doby pozastavení platnosti certifikátu

Tato služba se neposkytuje.

4.10 Služby statutu certifikátu

4.10.1 Funkční charakteristiky

Tato služba se poskytuje zveřejněním CRL na webových stránkách eIdentity a.s.

4.10.2 Dostupnost služeb

Tato služba se poskytuje nepřetržitě.

4.10.3 Další charakteristiky služeb statutu certifikátu

Tato služba se neposkytuje.

4.11 Ukončení poskytování služeb pro podepisující osobu

S ukončením platnosti kvalifikovaného certifikátu v případě, že žadatel nepožádal o vystavení následného kvalifikovaného certifikátu, končí obchodní vztah se žadatelem. Osobní konto žadatele a jeho osobní údaje zůstávají nadále aktivní a žadatel může kdykoliv opět požádat o navázání obchodního vztahu objednáním nabízené služby.

Pokud požádá držitel/podepisující osoba o ukončení zpracování osobních údajů, dojde ke zneplatnění jeho certifikátů, jeho osobní údaje se přesunou do archivu a přestanou se zpracovávat.

4.12 Úschova klíče u důvěryhodné třetí strany a jeho obnova

Tato služba se neposkytuje.

4.12.1 Politika a postupy při úschově a obnovování klíče

Tato služba se neposkytuje.

4.12.2 Politika a postup při zapouzdřování (encapsulation) a obnovování relačního klíče (session key)

Tato služba se neposkytuje.

5 BUDOVY, MANAGEMENT A PROVOZNÍ ŘÍZENÍ

5.1.1 Umístění objektu

Hostingové Centrum je provozováno v prostorech typu D, které se nachází v Kongresovém Centru Praha na adrese Kongresové centrum Praha, 5. května 65, Praha 4.

5.1.2 Fyzický přístup do objektu HC

Vlastní Housingové centrum společnosti T-Mobile CZ a.s.se nachází v prvním podzemním patře komplexu Kongresového centra Praha, mimo jiné s dalšími prostory skladového využití a třemi podzemními patry pro parkování automobilů. Komplex je ucelený, v areálu jsou přítomny firmy s různým výrobním zaměřením – komunikační společnosti a společnosti s obchodním zaměřením. Celý komplex je ve vlastnictví akciové společnosti Kongresové centrum Praha, a.s. založené hlavním městem Prahou, která uzavřela nájemní smlouvu s T-Mobile CZ a.s.

Budova Kongresového Paláce je umístěna na okraji plošiny (geomorfologicky) v severovýchodní části Pankráce, nad stanicí podzemní dráhy „Vyšehrad“, okolí tvoří dominanty budova hotelu Corinthia Towers, Nuselský most, a vícepodlažní činžovní městská zástavba s komerčním využitím v přízemních podlažích.

Kongresové Centrum Praha tvoří hlavní budova (Kongresový Palác) a vedlejší budova sloužící pro administrativní účely s částí o velikosti 1/3, ve které sídlí hotel Holiday Inn. Budovy jsou vzájemně propojeny jedním vzdušným mostem, který ale není standardně zpřístupněn. Nicméně celý komplex sdílí společné podzemí prostory (celkem 3 podzemní patra). Tyto prostory jsou využívány jako skladovací a parkovací prostory. Společným znakem obou budov je dostatečný počet osobních i nákladních výtahů pro dopravu osob a technologií. Vstup do obou budov je standardně možný přes personální vchody (rozměr min. 3600 x 2500 mm), které jsou střeženy 24hodin denně strážní službou.

Nosný systém budov je skeletový železobetonový s podélnými trámy, mezi nimiž jsou provedeny příčné průvlaky. Strop je železobetonový trámový, podlahy betonové. Stěny budov jsou kryty omítkou. Vnitřní příčky jsou vyzděny. Okna budov jsou ocelová či hliníková, zasklená bezpečnostním sklem. Místnosti v podzemních prostorech okna nemají.

Parkovací a odstavné plochy – parkování je řešeno systémem podzemních parkovišť pod oběma budovami Kongresového Centra. Parkovací stání jsou k dispozici ve všech třech podzemních úrovních stejně tak jako na vyhrazených nadzemních parkovištích v areálu kolem budovy. Vjezd vozidel je řízen ostrahou majitele nemovitosti nebo automaticky systémem čipových karet.

5.1.3 Vlastní objekt Housingového Centra

Hranici objektu Housingového Centra tvoří vnitřní železobetonová zeď stavebně výše specifikovaná, masivní ocelové vstupní dveře a rovněž ocelové dveře větších rozměrů spolu s nájezdovou rampou pro navážení větších kusů technologií.

Provozní řád Housing Centra upravuje všechny skutečnosti týkající se provozu, bezpečnosti a pohybu osob v HC.

Vstup do prostor HC je možný pro zaměstnance a Oprávněné osoby (zejména zákazníky housingových služeb) při prokázání se identifikačním průkazem strážní službě v suterénu Kongresového paláce a dále použitím čipové karty pro otvírání zabezpečených prostor HC (elektronická čipová karta / potvrzení heslem PIN).

Přítomnost návštěv v objektu HC je možná pouze v doprovodu zaměstnance T-Systems nebo Oprávněné osoby, po ověření totožnosti. Pohyb návštěv v HC upravuje provozní řád HC.
Pohyb osob v prostorech HC je dále monitorován systémem CCTV.

Bezpečnost je dále v celém prostoru HC posílena o systém EZS a EPS s vyvedeným výstupem hlášení na dispečink společnosti T-Mobile CZ(NCC) a stanoviště strážní služby KCP. V objektu rovněž sídlí vlastní jednotka Hasičského sboru.
V prostorech HC je instalováno samostatné zařízení EPS/SHZ. Jeho stavy a hlášení jsou monitorovány na dispečinku T-Mobile CZa dispečinku hasičského sboru KCP.

5.1.4 Typ objektu HC

Objekt lze určit jako typu 3, neboť poskytuje určitý stupeň odolnosti proti násilnému průniku. Objekt je pevné stavební konstrukce, nemá okna, dveře mají ocelové rámy a jsou mechanicky zabezpečeny tak, že poskytují stejný stupeň odolnosti jako ostatní části hranice objektu. Housingové Centrum T-Mobile CZbylo navrženo a vystavěno s požární odolností 90min.

5.1.5 Popis bezpečnostních prvků

Prostory HC jsou zajišťovány systémem certifikovaným pro stupeň „T“ CONCEPT 3000.
Přístup do zabezpečených prostor je pouze na základě IPK a PIN (současně).
Dále jsou pro zabezpečení vstupů používány zámky ABLOY a bezpečnostní vložky WEBER.
Pro zajištění technologických stojanů s vyšší bezpečností jsou používány vložky ABLOY.

5.1.6 Typ zabezpečené oblasti

Vzhledem ke stavební konstrukci oblasti a zabezpečení dveří se bude jednat o zabezpečenou oblast typu 3, neboť poskytuje vysoký stupeň odolnosti proti narušiteli, který je vybaven přenosnými nástroji. Hranice zabezpečené oblasti vykazuje vysoký stupeň odolnosti proti skrytému vniknutí.

5.1.7 Tabulka bodového ohodnocení bezpečnostních opatření v zabezpečené oblasti

BEZPEČNOSTNÍ OPATŘENÍ	TYP	BODOVÉ OHODNOCENÍ
Hodnocení úschovného objektu a jeho zámku	T. 3 – 3 body T. 2 – 2 body S1 = SS1 x SS2	S1=6
Zabezpečená oblast	T. 3 – 3 body	SS3=3
Uzamykací systém zabezpečené oblasti	T. 2 – 2 body	SS4=2
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	S2 = SS3 x SS4	S2=6
Objekt	T. 3 – 3 body	S3=3
Kontrola vstupu	T. 2 – 2 body	SS6=3
Režim návštěv v objektu Návštěvy s doprovodem	3 body	SS7=3
Celkové hodnocení kontroly vstupu	S4 = SS6 + SS7	S4=6
Strážní služba	T. 3 – 3 body	SS8=3
Úroveň technických prostředků EZS	T. – body	SS91=3
Instalace technických prostředků EZS	T. 2 – 2 body	SS92=3
Mezivýsledek (SS 9)		SS9=3
Celkové hodnocení strážní služby a systému EZS	S5 = SS8 + SS9	S5=6

5.1.7.1 Tabulka zabezpečené oblasti v souvislosti s mírou rizika

ZABEZPEČENÁ OBLAST KATEGORIE „D“	Míra rizika	
	Současný stav	standard pro střední riziko
Povinné : (S1) + (S2) + (S3)	15	8
Povinné : (S4) + (S5)	12	3
Nepovinné : (S6)	0	3
Celkový výsledek	27	14

5.1.8 Vyhodnocení fyzické bezpečnosti

Na základě vyhodnocení rizik je stav bezpečnostních opatření v oblasti fyzické bezpečnosti takový, že odpovídají vyhlášce NBÚ č. 339/1999 Sb. a bezpečnostním standardům, respektive

při realizaci ochrany perimetru by bodové ohodnocení odpovídalo dokonce i ochraně „PT“ oblasti při velké míře rizika.

5.1.9 Dokumentace fyzické bezpečnosti

Dokumentace fyzické bezpečnosti HC je důvěrného charakteru a není tudíž k dispozici třetím osobám.

5.1.10 Kontrolní opatření

Ve smyslu ČSN se provádí testování funkčnosti a revize EZS, EPS/SHZ.

5.1.11 Pravidla pro pohyb osob

Vstup do objektu a zabezpečené oblasti je povolen samostatně pouze Oprávněným osobám ve smyslu provozního řádu HC T-Systems T-Mobile CZ. Pracovníci strážní služby nejsou ke vstupu do HC oprávněni. Při odchodu všech oprávněných osob z HC EZS vyhodnotí prostory jako prázdné a aktivuje bezpečností čidla.

5.1.12 Návštěvy

Návštěvy jsou možné jen v doprovodu zaměstnance T-Mobile CZ s oprávněním pro vstup do HC nebo s Oprávněnými osobami (zejména zákazníci). Režim návštěv se řídí podmínkami Provozního řádu T-Mobile CZ.

5.1.13 Pravidla pro používání systémů EZS, EPS

Pro každou oprávněnou osobu je stanoven originální IPK a PIN. Při nakládání s přístupovými kódy je nutné dbát na jejich důvěrnost. V případě odcizení karty IPK a současném prozrazení kódu PIN je možné tuto kartu okamžitě deaktivovat.

5.1.14 Pravidla pro manipulace s klíči od stojanů v HC

Klíče od stojanů jsou vydány oprávněným osobám zákazníka a jejich duplikáty jsou uloženy na dispečinku T-Mobile CZ. V případě žádosti zákazníka nejsou duplikáty klíčů umístěny na dispečinku. Ztrátu klíče hlásí Oprávněná osoba neprodleně na dispečink T-Mobile CZ.

5.1.15 Pravidla pro výkon fyzické ostrahy

Nepřetržitou ostrahu všech prostor KCP zabezpečují pracovníci bezpečnostní služby KCP.

5.2 Fyzická kontrola

5.2.1 Pravidla pro pohyb osob

Vstup do objektu a zabezpečené oblasti je povolen samostatně pouze Oprávněným osobám. Pracovníci strážní služby nejsou ke vstupu oprávněni.

5.2.2 Návštěvy

Viz výše.

5.2.3 Umístění a konstrukce

Viz výše.

5.2.4 Fyzický přístup

Základní bezpečnostní opatření pro kontrolu vstupu obsahuje:

- Přístup do HC přes bezpečnostní “komoru“
- dvojitý systém identifikace IPK/PIN
- uzamykatelné stojany, CCTV kamery
- nepřetržitý autonomní přístup (režim 24 x 7 x 365)

Systém autorizace vstupu je řešen kombinací IPK a PIN. Pro držitele karet je standardní režim přístupu nepřetržitý, tj. 24 hodin denně, 7 dní v týdnu. Karty jsou nepřenosné, tedy vždy na jméno Oprávněné osoby (proškolené). Platnost určitých karet lze časově omezit nebo nastavit pouze na určitou část dne. V ceně standardní služby Housing zařízení jsou již dvě karty, lze zajistit vydání dalších.

Objekt Kongresového Centra je nepřetržitě monitorován kamerovým systémem ochranné služby objektu, vnitřní prostory DC pak kamerami dohledového centra společnosti T-Systems T-Mobile CZ. Nedílnou součástí je také elektronická zabezpečovací signalizace. Je použit modulární systém CONCEPT s homologací pro vyšší rizika, ČTÚ, NBÚ, EZÚ (v souladu s ČSN 33 4590). Oba systémy jsou napojené na pult centrální ochrany dohledového centra společnosti a také dispečinku objektu.

Stojany pro zařízení poskytované společnosti T-Mobile CZ jsou uzamykatelné. Volitelně lze navíc zvýšit zabezpečení ohrazením prostoru od okolních stojanů bezpečnostní klecí.

Speciální postup je aplikován v případě potřeby přístupu k objektu Housingového Centra nákladní dopravou. Ten je umožněn od 5,00 do 23,00 hod. a výhradně za spolupráce zaměstnanců Dohledového centra T-Systems T-Mobile CZ.

5.2.5 Elektřina a klimatizace

Zabezpečení napájení obsahuje:

- střídavé napájení 230 V i stejnosměrné 48 V pro každý stojan dvojící nezávislých přívodů a se samostatným jištěním
- příkon na jeden stojan je standardně až do 2,5 kW; vyšší příkony nutno řešit individuálně zejména s ohledem na možnosti odvodu tepla ze stojanu

- kapacita baterií dimenzována na 4hodinový provoz, generátorový výkon v objektu KCP je 3,6 MW

Dodávka elektrické energie do objektu je realizována ze dvou různých rozvoden trojicí 22kV přívodů. Tyto přívody jsou dále jištěny čtveřicí dieselových generátorů v kaskádě o výkonu 4x900kW s garantovaným náběhem do 5 minut od případného (současného) výpadku obou přívodních větví.

Napájení všech stojanů a zařízení je nepřímé, přes baterie. Nemůže tudíž dojít ani ke krátkodobému výpadku při přepínání nouzových zdrojů (lze přirovnat k online UPS). Každé zařízení (stojan) má dvě nezávislé připojení k zdroji napájení. Baterie zálohují jak střídavé, tak stejnosměrné rozvody. Rozvody k jednotlivým zařízením jsou vedeny výhradně mezi podlahami, nedochází tak k rušení datových kabelů vedených stropem.

Klimatizace poskytuje prostředí:

- zálohované klimatizační jednotky udržují teplotu prostředí na 22 °C (± 3 °C)
- relativní vlhkost 45 % - 70 %
- podmínky vyhovují ETS 300 019-1-3.

Prostory Datového Centra jsou plně vybaveny bezprašnými nátěry. Zálohování vnitřních klimatizačních jednotek je systémem N+1.

5.2.6 Vlivy vody

Místnosti jsou vybaveny pod stávající stropní deskou ochranným podhledem z pozinkovaného plechu pro zvýšení odolnosti proti pronikající vodě.

5.2.7 Protipožární opatření a ochrana

Prostory jsou vybaveny protipožární ochranou, která obsahuje:

- detektory kouře a teploty v Datovém Centru i objektu vlastního Kongresového centra
- stabilní samo zhášecí protipožární systém v Datovém Centru
- dvojité protipožární dveře
- hasičský sbor se dvěma jednotkami přímo v objektu

Prostory DC jsou umístěny v železobetonovém skeletovém objektu, prostory jsou vystavěny a zkolaudovány s požární odolností 90 min. Požární odolnost konstrukcí je stanovena dle čl. 7.1.1 ČSN 73 0802.

Dveře Datového Centra jsou protipožární EW 90D1 (odolnost 90 min) a jsou osazeny v dělených zárubních, požární uzávěry – protipožární klapky, PPK jsou PKM –90 (odolnost 90 min).

Systém celkového protipožárního zajištění je zajišťován pomocí EPS (Elektronický Protipožární Systém) - signalizační zařízení a SHZ (Stabilní Hasicí Zařízení), které se řadí mezi aktivní prvky požární ochrany budov a zařízení.

Stabilní hasicí zařízení je pevně instalovaným systémem k ochraně drahých zařízení. Na systém EPS/SHZ vydává dovozce "Prohlášení o shodě" podle § 13 Zákona č. 22/1997 Sb. a § 11 nařízení vlády č. 178/1997 Sb., na základě schvalovacích listů (MV Ředitelství HZS ČR), certifikátů (Technický ústav požární ochrany MV) a dalších dokumentů.

Systém je konstruován k vypuštění specifického množství hasiva FM-200 (halogenový alkan - 1, 1, 1, 2, 3, 3, 3 - heptafluorpropan (CF3CHFCF3). Tento elektricky nevodivý plyn hasí požár narušováním vazeb reakce spalování. FM-200 rychle potlačuje plameny, zabraňuje znovuvznícení, nezanechává zbytkové materiály a nevyžaduje úklid po vypuštění – vyvětrá se odvětrávacím zařízením. Systém je konstruován k velmi rychlému zásahu (10 sekund a méně), aby se minimalizovali škody na zařízení a snížilo nebezpečí ohrožení života. Potřebné množství FM-200 bylo profesionálně kalkulováno tak, aby splňovalo přísné požadavky Factory Mutual Research Corporation a National Fire Protection Association. Na systému jsou prováděny revize v předepsaných lhůtách podle ČSN a vyhlášky MV ČR 21/1996 Sb.
Kongresové centrum disponuje vlastním profesionálním hasičským záchranným sborem. Jedná se o trvalou profesionální službu dispečinku s pultem centrální ochrany a dvou hasičských skupin pro nezávislý okamžitý zásah.

5.2.8 Ukládání médií

Uskladnění zálohovacích médií není nijak řešeno poskytovatelem. Zákazník si může své média uložit v zamykatelném stojanu, nebo odnést mimo prostor HC.

5.2.9 Nakládání s odpady

V prostorech HC nevznikají žádné specifické odpady. Odpad při manipulaci a instalaci technologie musí zákazník po ukončení prací odnést z prostor HC.

5.2.10 Zálohy mimo budovu

Pro úschovu aktiv ACAeID se využívá bezpečnostní schránka v Růžové ulici, Praha 1 s 24hodinovým režimem vstupu. Ukládají se zde kopie záloh informačního systému a archivní kopie dat v elektronické podobě.

5.3 Kontrola procedurální bezpečnosti

5.3.1 Důvěryhodné role

Důvěryhodné role jsou:

- statutární zástupce
- ředitel společnosti
- ředitel bezpečnosti
- Technický ředitel

5.3.2 Počet osob požadovaných na zajištění jednotlivých činností

Pro bezpečnostní operace je vyžadována přítomnost nejméně dvou důvěryhodných osob najednou.

5.3.3 Identifikace a autentizace pro každou roli

Jednotliví uživatelé se do aplikace hlásí pomocí čipových karet nebo USB tokenů.

5.3.4 Role vyžadující rozdělení povinností

Role, které vyžadují rozdělení, jsou:

- ředitel provozu
- ředitel bezpečnosti

5.4 Kontroly personální bezpečnosti

5.4.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Společnost eIdentity a.s. při práci s lidskými zdroji buduje systém, který zabezpečuje, že budou najímáni pouze důvěryhodní zaměstnanci a je dbáno o to, aby jejich loajalita ke společnosti byla podporována a udržována. Personální práce eIdentity a.s. vede k tomu, že lidé si uvědomují zájem společnosti o ně samé, že cítí sounáležitost se svou společností, identifikují se s ní a cítí jasnou přímou úměrnost mezi úspěchem společnosti a svým prospěchem. Pro společnost je základním východiskem důvěra ve vlastní zaměstnance, která má pozitivní vliv na míru akceptování některých omezení. Personální bezpečnost je součástí aktivit spadajících pod řízení lidských zdrojů, je tedy neoddělitelnou součástí práce všech vedoucích pracovníků eIdentity a.s. Personální bezpečnost eIdentity a.s. vnímá jako součást řádné správy společnosti, neboť je vyjádřením péče o svěřená aktiva.

Personální bezpečnost v oblasti ochrany citlivých aktiv tedy eIdentity a.s. vnímá jako zintenzivnění výše uvedeného systému u osob, které jsou určeny k práci s citlivými aktivy. Organicky navazuje na současný systém řízení lidských zdrojů.

Termínem personální bezpečnost eIdentity a.s. označuje souhrn všech postupů, které vedou k ověření důvěryhodnosti zaměstnanců a k jejich vzdělávání vedoucímu k bezpečnostnímu povědomí o možných bezpečnostních hrozbách a rizicích a k jednání, která toto povědomí odráží.

Důvěryhodnost zaměstnanců je jedním ze základních kvalifikačních předpokladů pro výkon pracovní činnosti v rámci eIdentity a.s. Je zárukou toho, že pracovník, který disponuje svěřenými hodnotami, svého postavení nezneužije a nezpůsobí tak poskytovateli ztrátu.
Ověření důvěryhodnosti zaměstnance je proces zahrnující shromažďování, ověřování a vyhodnocování informací. Výstupem je rozhodnutí, zda může být daný jmenovaný pracovník (pracovník usilující o jmenování) považován za důvěryhodnou osobu.

Zdrojem informací jsou pracovník sám a osoby, které zaměstnance znají. Dalším zdrojem jsou

veřejně přístupné informační zdroje.

Bezúhonnost se posuzuje podle výpisu z rejstříku trestů.

Pracovník poskytuje informace v průběhu vstupního osobního pohovoru a dále při periodických pohovorech s vedoucími pracovníky společnosti.

Další osoby poskytují informace v situacích (bezpečnostní incident), které vyvolají potřebu ověřit získané informace.

Postup posuzování spočívá v pečlivém zvažování řady proměnných údajů, které sestavují „celkový profil osobnosti“ (whole person concept). V procesu rozhodování jsou zvažovány dostupné, spolehlivé informace o pracovníkovi, příznivé i nepříznivé, ze současné doby i z minulosti.

Posuzovatel bere v úvahu při hodnocení závažnosti chování pracovníka následující faktory:

- povahu, rozsah a závažnost chování
- okolnosti, za jakých ke zkoumanému chování došlo, aby bylo možné posoudit vědomou účast
- četnost a časový odstup od zkoumaného chování
- dobrovolnost při účasti na zkoumaném chování
- příznaky nebo nedostatek příznaků nápravy
- motivaci ke zkoumanému chování
- potenciální možnost nátlaku, donucování, využívání nebo vydírání
- pravděpodobnost pokračování nebo opakovaného výskytu zkoumaného negativního chování

Každý případ je posuzován odděleně ve své podstatě. Pochybnosti o důvěryhodnosti posuzovaného pracovníka jsou podnětem ke zvažování bezpečnostních rizik, která by vyplynula z realizace hrozeb definovaných v celkové bezpečnostní politice.

Konečné rozhodnutí o tom, zda považovat pracovníka za důvěryhodného a spolehlivého musí být jednoznačně v souladu se zájmy společnosti a musí být rozhodnutím všeobsáhlé zralé úvahy.

Zvažována v kontextu profilu celé osobnosti je:

- loajalita k organizaci
- konkurenční vlivy
- sexuální chování
- osobní chování
- posouzení finančních poměrů
- alkohol
- užívání drog
- citové, mentální problémy a poruchy osobnosti
- kriminální chování

- porušování bezpečnosti
- nebezpečné aktivity
- zneužití systémů informační techniky

Loajalita k organizaci
Posuzovaný pracovník musí být beze všech pochybností loajální vůči společnosti. Jestliže existuje jakýkoli důvod k podezření o loajalitě ke společnosti, je zpochybněna i ochota pracovníka střežit svěřené citlivé informace.

Konkurenční vlivy
Posuzovaný pracovník může představovat bezpečnostní riziko, jestliže se u něho vyskytují přímé vazby na konkurenci a mohl by mít sklony k jednání, které by bylo v rozporu s cíli společnosti.

Sexuální chování
Sexuální chování se stává možným ohrožením bezpečnosti, jestliže zahrnuje kriminální jednání, poukazuje na emociální poruchy, na narušenou osobnost a může tak vystavit posuzovaného pracovníka donucování, využívání nebo vydírání, popřípadě když toto chování odráží nedostatek úsudku nebo diskrétnosti. Sexuální orientace nebo preference nejsou v souvislosti s posuzováním bezpečnostní spolehlivosti v žádném případě samy o sobě předmětem zkoumání ani zvažování.

Osobní chování
Chování posuzovaného pracovníka, které se vyznačuje nedostatkem úsudku, nespolehlivostí, nedostatkem upřímnosti, nečestností nebo neochotou podřídit se pravidlům a předpisům může být ukazatelem, že pracovník nemusí být schopen řádně chránit svěřené informace.

Posouzení finančních poměrů
Posuzovaná osoba, která se nachází ve finančně napjaté situaci, představuje bezpečnostní riziko možností, že se zúčastní nezákonné činnosti pro získání peněz. Nevysvětlitelný vysoký příjem je důvodem pro zvýšenou pozornost věnovanou posuzovanému zaměstnanci.

Alkohol
Nadměrná spotřeba alkoholu často vede k uplatňování pochybného úsudku, k nespolehlivosti, neschopnosti ovládnout impulzivní chování a zvyšuje riziko úniku informací v důsledku nedbalosti.

Užívání drog
Užívání drog nastoluje otázky, jak dalece je posuzovaná osoba ochotná nebo schopná ochraňovat svěřené informace. Zneužívání drog nebo drogová závislost mohou zhoršit sociální nebo profesionální jednání a zvýšit rizika neautorizovaného sdělení citlivých informací.
Užíváním drog je rozuměno zneužívání drog jako nezákonné užívání drog nebo užívání zákonem povolených drog způsobem, který se rozchází se schváleným lékařským doporučením.

Emocionální a mentální poruchy
Emocionální a mentální poruchy nebo narušení osobnosti mohou být příčinou významných nedostatků v psychologických, sociálních a profesionálních činnostech posuzované osoby. Tyto

nedostatky představují možné ohrožení bezpečnosti, protože mohou znamenat i poruchy soudnosti, spolehlivosti a stability. V takovémto případě musí být pro úplné a řádné zhodnocení případných diskvalifikujících nebo polehčujících informací využit pověřený profesionál.

Kriminální chování
Minulá nebo opakovaná kriminální činnost vytváří pochybnosti o soudnosti posuzované osoby, její spolehlivosti a důvěryhodnosti.

Porušování bezpečnosti
Nedodržování bezpečnostních předpisů vyvolává pochybnosti o důvěryhodnosti posuzované osoby, její ochotě a schopnosti střežit citlivé informace.

Zneužití systémů informační techniky
Nedodržování pravidel, postupů, směrnic nebo předpisů závazných pro systémy informační techniky může způsobit ohrožení bezpečnosti a vyvolat otázky o důvěryhodnosti posuzované osoby, její ochotě a schopnosti řádně střežit utajované systémy, sítě a informace. Systémy informačních technologií zahrnují všechna zařízení užívaná pro komunikace, přenosy, zpracování, manipulaci a ukládání informací.

Dále popsané způsoby chování by za normálních okolností měly vést k nepříznivému posudku nebo k ukončení dalšího postupu zjišťování spolehlivosti a důvěryhodnosti:
odmítnutí podrobit se vyžadovanému postupu pro stanovení spolehlivosti a důvěryhodnosti nebo odmítnutí spolupráce při tomto postupu odmítnutí sdělit nebo poskytnout úplné, upřímné a pravdivé odpovědi na oprávněné otázky oprávněných osob v souvislosti s postupem zjišťování možného ohrožení bezpečnosti pracovníkem nebo při zjišťování jeho spolehlivosti a důvěryhodnosti v průběhu posuzování vyjdou najevo spolehlivé, významné a diskvalifikující nepříznivé informace.

Vejdou-li ve známost informace týkající se možnosti ohrožení bezpečnosti a vztahují se k osobě, která je v současné době jmenovaným pracovníkem eIdentity a.s., pak posuzovatel zvažuje, zda tato osoba:

- dobrovolně oznámila tyto informace
- pravdivě a úplně odpověděla na otázky odpovědných pracovníků
- vyhledala pomoc a řídila se pokyny profesionálů tam, kde to bylo vhodné
- vyřešila nebo se zdá pravděpodobné, že vyřeší možné ohrožení bezpečnosti
- vykázala se kladnými změnami chování a postoji v zaměstnání

Pokud posuzovatel po zhodnocení informací o možném ohrožení bezpečnosti rozhodne, že informace nejsou natolik závažné, aby vedly k doporučení odvolání pracovníka, může doporučit podmíněný souhlas s varováním, že pracovník bude odvolán, pokud se budou incidenty podobné povahy v budoucnosti opakovat.

Vůči stávajícím zaměstnancům se opatření personální bezpečnosti aplikují v přiměřeném rozsahu.

S každým zaměstnancem eIdentity je podepisována doložka smlouvy o bezpečnostní odpovědnosti. U smluv se zaměstnanci třetí strany je podepsána smlouva zachování důvěrnosti.

5.4.2 Požadavky na přípravu

Zaměstnanci a ostatní pracovníci ACAeID musí absolvovat průběžný cyklus bezpečnostního a aplikačního vzdělávání.

5.4.3 Požadavky a frekvence dalšího školení

Školení se organizují tak, aby každý pracovník byl školen alespoň jednou měsíčně.

5.4.4 Periodicita a posloupnost „job rotation“ mezi různými rolemi

Nepředpokládá se, že by probíhala pravidelná změna pracovních pozic zaměstnanců. Pakliže to bude pro zajištění provozu nezbytně nutné, může zaměstnanec dočasně vykonávat jinou roli. Musí však před tím absolvovat patřičné proškolení.

5.4.5 Postihy za neautorizované činnosti zaměstnanců

Vykonávání neautorizované činnosti se považuje za hrubé porušení pracovní kázně a sankce se řídí zákoníkem práce.

5.4.6 Požadavky na nezávislé zhotovitele (dodavatele)

Doporučuje se certifikát NBÚ na stupeň důvěrné.

5.4.7 Dokumentace poskytovaná zaměstnancům

Dokumentace, která se předává zaměstnanci, se týká specifikace jeho pracovní náplně a popisu systémů, se kterými pracuje na úrovni příručky uživatele.

5.5 Auditní záznamy (logy)

5.5.1 Typy zaznamenávaných událostí

Auditní záznamy obsahují informace především o následujících událostech:

- spuštění a vypnutí systému
- vytvoření žádosti o certifikát, její schválení či zamítnutí
- vytvoření či revokace certifikátu
- vytvoření CRL
- vytvoření či zničení podepisovacích klíčů CA, infrastruktury a operátorů
- spuštění či vypnutí auditních funkcí
- změny auditních parametrů
- přechod na záložní auditní medium z důvodu chyby hlavního média
- všechna úspěšná i neúspěšná přihlášení do systému

.

5.5.2 Periodicita zpracování záznamů

Auditní záznamy jsou zpracovávány nejméně 1x týdně, jinak bezprostředně po bezpečnostním incidentu.

5.5.3 Doba uchování auditních záznamů

Auditní záznamy se uchovávají po dobu 10 let.

5.5.4 Ochrana auditních záznamů

Auditní záznamy jsou kontrolovány a schvalovány Security Officerem. Přístup k auditním záznamům má pouze Security Auditor. Využívá funkcí systému dostupných pouze po přihlášení osoby v této roli. Auditní události jsou zobrazeny v přehledné tabulce.

Je umožněn výběr událostí z logu dle kritérií:

- současné dění – obsahuje nejaktuálnější události, stránka se automaticky obnovuje
- pokročilý výběr – je možné zadat časový interval, požadovaný typ, uživatele či vyhledávaný řetězec

.

5.5.5 Postupy pro zálohování auditních záznamů

Auditní logy jsou ukládány v databázi a jsou zálohovány stejně jako ostatní databázové informace tak, aby bylo možné jejich plné obnovení po případné poruše.

5.5.6 Systém shromažďování auditních záznamů

Auditní záznamy jsou uchovávány v databázi. V případě selhání databáze nebo zjištění nedostatečné úložné kapacity je tato skutečnost ihned oznámena administrátorovi systému e-mailovou zprávou a auditní záznamy dále jsou generovány na náhradní medium. Po odstranění problému jsou dočasné záznamy přesunuty administrátorem systému zpět do primárního úložiště. Po dobu záznamu na dočasné medium ani během přesunu nejsou administrátorovi systému zpřístupněny funkce pro prohlížení auditních záznamů.
Aby se minimalizovala nutnost využití náhradního media, je systémový administrátor upozorněn na možnost nedostatku úložného prostoru již při využití kapacity na 80%. Celková kapacita je koncipována tak, aby zbývajících 20% vystačilo na minimálně 3 dny běžného provozu systému, což poskytuje administrátorovi dostatečný prostor pro nápravu. Nikdy nedochází k automatickému přepisování záznamů.
Audit je koncipován jako interní, kdy každá entita si audituje svoje vnitřní informace.

5.5.7 Oznamování subjektu, který způsobil událost

Neposkytuje se.

5.5.8 Hodnocení zranitelnosti

Události s vyšším stupněm závažnosti jsou oznamovány Security Officerovi automaticky emailem nebo prostřednictvím SMS.

5.6 Archivace záznamů

5.6.1 Typy záznamů, které se archivují

Archivace dat CA eIdentity je pravidelně provedena jednou měsíčně. Na DVD medium jsou vypáleny soubory obsahující všechny certifikáty, všechna CRL/ARL a auditní logy za dané období. Otisky souborů a času jejich pořízení jsou uvedeny v přiloženém souboru podepsaném systémovým operátorem. DVD medium je následně uzavřeno, což znemožní jeho další přepis. DVD media jsou uložena v trezoru v sídle společnosti eIdentity a.s.

5.6.2 Doba uchování archivovaných záznamů

Pro archivaci jsou vybírána media, u kterých výrobce zaručuje minimální dobu čitelnosti 3 roky. Po dvou letech jsou média přepalována. Celková doba archivace dat je 10 let.

5.6.3 Ochrana úložiště archivovaných záznamů

Práva k prohlížení archivu závisí na sledovaných položkách. Certifikáty a CRL může prohlížet každá osoba, která má oprávněný přístup k archivním informacím. Auditní archivní informace jsou přístupné pouze oprávněným osobám prostřednictvím prohlížecí aplikace. Osoby, které mají oprávnění k přístupu, musí být poučeny, že v archivu se vyskytují osobní údaje. Archivované údaje jsou šifrovány.

5.6.4 Postupy při zálohování archivovaných záznamů

Postupy odpovídají bodu 5.6.1 této CPS.

5.6.5 Požadavky na používání časových razítek u archivovaných záznamů

Postupy odpovídají bodu 5.6.1 této CPS.

5.6.6 Systém shromažďování archivovaných záznamů

Archivní kopie se ukládají interně.

5.6.7 Postupy pro získání a ověření archivních údajů

Součástí archivu je seznam otisků archivovaných souborů včetně záznamu času pořízení, který je elektronicky podepsán Operátorem EVI/CA v okamžiku pořízení.

5.7 Výměna klíče CA

Výměna klíčů CA nebude prováděna.

5.8 Obnova po havárii nebo kompromitaci

5.8.1 Postup v případě incidentu a kompromitace

V případě bezpečnostního incidentu odpovídajícího rozsahu se postupuje v souladu s Plánem zvládání krizové situace a Plánem obnovy.

5.8.2 Poškození výpočetních prostředků, software a/nebo data

Systém je navržen tak, že je možné vyměnit jakoukoliv část poškozené výpočetní techniky, software a dat tak, aby mohl být provoz zachován.

5.8.3 Postup při kompromitaci soukromého klíče entity

V případě kompromitace privátního klíče ACAeID dojde k jeho okamžitému zneplatnění a umístění na seznam zneplatněných certifikátů.

Dojde k zneplatnění všech certifikátů, které byly vydány za pomoci kompromitovaného klíče ACAeID.

O skutečnosti je informována veřejnost tak, že je situace popsána na stránkách eIdentity a.s., které jsou nepřetržitě dostupné. Každý žadatel je dále na tuto situaci upozorněn doporučeným dopisem případně navíc ještě elektronickým dopisem. Žadatelé mají v tomto případě nárok na vydání nového certifikátu zdarma.

5.8.4 Schopnost pokračovat v činnosti po havárii

Činnost po nehodě se řídí Plánem zvládání krizové situace a plánem obnovy.

5.9 Ukončení činnosti CA nebo RA

Provozovatel informuje Ministerstvo vnitra nejméně 3 měsíce před předpokládaným ukončením činnosti. Vynaloží veškeré možné úsilí k tomu, aby vedená evidence byla převzata jiným kvalifikovaným poskytovatelem certifikačních služeb.

Provozovatel dále informuje doporučeným dopisem každého Žadatele o svém záměru ukončit činnost nejméně 2 měsíce předem.

Provozovatel nejméně 30 dní před ukončením činnosti informuje Ministerstvo vnitra v případě, že se nepodařilo zajistit převzetí evidence jiným kvalifikovaným poskytovatelem.

Obdobná ustanovení platí i v případě jiných způsobů ukončení činnosti.

6 KONTROLY TECHNICKÉ BEZPEČNOSTI

6.1 Generování a instalace párových klíčů

6.1.1 Generování párových klíčů

Pár klíčů CA eIdentity je vygenerován během procesu instalace třemi vyškolenými pracovníky CA. Ke generování je využit nově nainstalovaný software a hardware. Klíč je generován v kryptografickém modulu, který splňuje normu FIPS 140-2 Level 3 a je uveden na stánkách ministerstva, jako nástroj, u kterého byla vyslovena shoda.

Klíče jsou generovány dle předem připraveného procesu popsaného v instalační příručce podepisovacího pracoviště CA eIdentity.

Klíče ACAeID se mohou použít pouze k podepisování kvalifikovaných certifikátů a seznamu zneplatněných certifikátů.

Páry klíčů operátorské CA, operátorů CA a operátorů RA eIdentity jsou generovány v kryptografických modulech splňujících normu FIPS 140-2 Level 2.

Generování klíčů koncových uživatelů je obecně řešeno přímo uživateli. Pro kvalifikované certifikáty je možno použít generování klíčů za pomoci některého internetového prohlížeče. V případě systémových kvalifikovaných certifikátů uživatel převážně použije nástroje systému, pro který chce certifikát použít.

6.1.2 Předání soukromého klíče podepisující osobě

Žadatelé generují soukromé klíče vlastními prostředky ve svém prostředí. Případně ve vlastním QSCD u operátora RM na RM.

6.1.3 Předání veřejného klíče certifikační autoritě

Veřejný klíč uživatele je dodán CA eIdentity v podobě PKCS#10 nebo jiného elektronicky podepsaného balíku dat v rámci SSL spojení.

6.1.4 Předání veřejného klíče CA potenciálním spoléhajícím se stranám

Certifikáty CA eIdentity jsou zveřejněny na webových stránkách CA eIdentity, společně s otisky certifikátu pořízenými alespoň dvěma různými algoritmy. Tytéž informace jsou k dispozici na webu MVČR a v tištěné podobě v centru ACA eIdentity.

6.1.5 Délky klíče

Délky klíčů musí být dostatečné vzhledem k současným metodám pro odhalení soukromého klíče kryptografickou analýzou používání klíčů. Současný standard pro velikost klíčů je 2048 bitů a více. CA eIdentity odmítne vydat certifikát generovaný s párem klíčů velikosti menší než 2048 bitů. Požadovaná délka klíče se bude v čase zvyšovat.

6.1.6 Parametry pro generování veřejného klíče a ověřování kvality

Přijaty budou pouze unikátní veřejné klíče. Bohužel, není možné ověřit, že stejný veřejný klíč se nenachází u jiné CA.

6.1.7 Účel pro použití klíče (pole použití klíče pro X.509 v3)

Kvalifikované certifikáty vydané CA eIdentity slouží výhradně k vytváření elektronického podpisu a jsou takto i označeny.

6.2 Ochrana soukromého klíče a kontroly kryptografického modulu

6.2.1 Standardy a kontroly kryptografických modulů

Klíče CA eIdentity jsou generovány hardwarovým modulem splňujícím požadavky normy FIPS 140-2 Level 3. Klíče operátorské CA a operátorů jsou generovaný hardwarovými moduly.

6.2.2 Sdílení tajemství (m z n)

Veškeré citlivé operace CA eIdentity vyžadují přítomnost dvou operátorů. Každý z těchto operátorů zná část kódu, který umožní tyto operace provést. Jedná se o sdílení tajemství dvou ze dvou osob.

6.2.3 Úschova soukromých klíčů

Soukromé klíče CA eIdentity a jejich operátorů jsou uloženy výhradně v úložištích odpovídajících hardwarových tokenů. Žádné jiné úložiště soukromých klíčů neexistuje.

6.2.4 Zálohování soukromých klíčů

Soukromý klíč CA eIdentity je zálohován během procesu jeho vytvoření. Klíč je vyexportován v zakryptované podobě za použití asymetrické šifry pomocí klíče, který je rozdělen na několik částí uložených v různých hardwarových tokenech. Tyto části jsou pak rozděleny mezi operátory CA eIdentity. Obnova klíče je možná pouze za účasti všech částí šifrovacího klíče. Šifrovaný pár klíčů CA eIdentity je uložen v zabezpečeném prostoru, do kterého smí přistupovat pouze zodpovědní zástupci společnosti.

Soukromé klíče operátorů a částí systému nejsou zálohovány.

6.2.5 Archivace soukromých klíčů

CA eIdentity nearchivuje soukromé klíče.

6.2.6 Transfer soukromých klíčů do/z kryptografického modulu

Všechny páry klíčů CA eIdentity, operátorské CA či operátorů jsou generovány uvnitř kryptografických modulů a jsou označeny jako neexportovatelné.

Jedinou výjimkou uvedeného pravidla jsou klíče systémové, jež jsou generovány nástroji v závislosti na systému, ve kterém budou použity.

6.2.7 Uložení soukromých klíčů v kryptografickém modulu

Soukromé klíče jsou uloženy v kryptografických modulech v šifrované formě.

6.2.8 Postup aktivování soukromého klíče

K aktivaci soukromého klíče CA je zapotřebí dvou operátorů, kteří ve správném pořadí vloží do podepisovacího pracoviště své části PINu.

Soukromé klíče operátorů jsou aktivovány po vložení hardwarového tokenu na základě PINu. Pro využití systému CA eIdentity je kromě PINu nutné zadat i přihlašovací údaje.

6.2.9 Postup při deaktivaci soukromého klíče

Soukromý klíč CA eIdentity je deaktivován vypnutím podepisovacího pracoviště.

Soukromé klíče operátorů jsou deaktivovány vyjmutím hardwarového tokenu z pracoviště.

6.2.10 Postup při zničení soukromého klíče

Rozhodnutí o zničení soukromého klíče CA eIdentity mohou provést pouze majitelé firmy na základě závažných důvodů, např. jeho kompromitace. Ke zničení klíče musí být přítomni dva operátoři a zástupce vedení společnosti. O zničení klíče je sepsán protokol podepsaný všemi zúčastněnými.

Pro ničení soukromých klíčů jsou použity nulovací funkce kryptografických modulů.

6.2.11 Hodnocení kryptografických modulů

Použité kryptografické zařízení HSM Eracom C8000 má prohlášení o shodě v souladu s požadavky Zákona.

6.3 Další aspekty klíčového hospodářství

6.3.1 Archivace veřejného klíče

Veřejný klíč CA eIdentity, veřejné klíče jednotlivých komponent i veřejné klíče operátorů jsou zálohovány a archivovány v rámci standardních procedur zálohování serverů CA eIdentity. Data jsou archivována na DVD disky a ukládána do trezoru.

6.3.2 Maximální doba platnosti certifikátu vydaného podepisující osobě a párových klíčů

Podepisovací certifikát CA je vydáván dle odpovídající certifikační politiky. Certifikáty vydané

CA eIdentity mají dobu platnosti zpravidla 1 rok, maximálně 3 roky. Při delší době platnosti certifikátu než jeden rok, musí být použita dvojnásobná délka HASH a/nebo dvojnásobná délka klíče. Před skončením platnosti podepisovacího certifikátu přestane být tento užíván k vydávání dalších certifikátů, aby žádný z vydaných certifikátů neměl dobu platnosti přesahující dobu platnosti certifikátu, kterým byl podepsán. Po ukončení platnosti klíče bude privátní klíč protokolárně zničen a certifikát (jako neplatný) bude archivován.

Období použití klíčů odpovídá době platnosti certifikátu.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data k podepisovacím klíčům CA eIdentity jsou vytvořena během procesu instalace podepisovacího pracoviště, kdy dochází mimo jiné i ke generování těchto párových dat. Aktivačními daty podepisovacích klíčů je PIN rozdělený mezi dva operátory tak, že každý z nich zná pouze svou část.

Jakožto aktivační data ke klíčům operátorů slouží také PIN. Vytváření PINů se řídí těmito pravidly:

- PIN má alespoň 8 znaků
- PIN musí obsahovat nejméně jeden abecední a jeden numerický znak
- PIN není slovníkové slovo.

6.4.2 Ochrana aktivačních dat

Operátoři CA a RA jsou smluvně vázáni chránit svá aktivační data a nesou za jejich případné zneužití zodpovědnost. Kromě znalosti aktivačních dat vyžaduje pokus o zneužití soukromého klíče i získání hardwarového tokenu, na kterém jsou tato data uložena. V případě operátorů CA je navíc možnost použití soukromého klíče v rámci systému CA omezena na konkrétní pracoviště.

6.4.3 Ostatní aspekty aktivačních dat

Aktivační data slouží výhradně k aktivaci soukromého klíče a nesmí být užita k jinému účelu, ani vkládána do jakéhokoli systému nesouvisejícího s tímto použitím. Aktivační data nikdy nesmí být přenášena po síti v nezašifrované podobě.

V případě podezření na prozrazení aktivačních dat jsou tato bezodkladně znehodnocena jakýmkoli možným způsobem, včetně případného zničení párových dat.

6.5 Řízení počítačové bezpečnosti

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Veřejná část systému CA eIdentity je přístupná pomocí HTTP a HTTPS protokolu. Všechny komponenty veřejné části kromě registrace nových uživatelů jsou určeny pouze ke čtení a neumožňují vzdálenému uživateli změnu údajů. Registrace uživatelů vyžaduje vstup ze strany zájemce a je vedena striktně pomocí HTTPS protokolu.

Klientská část systému CA je zpřístupněna uživatelům šifrovaným kanálem HTTPS, kterým jsou předávána veškerá citlivá data. Přístup k údajům uživatele je umožněn až po zadání uživatelského jména hesla. Toto rozhraní je jediným bodem komunikace s veřejností, všechny ostatní systémy CA eIdentity jsou mimo vnitřní síť CA eIdentity nepřístupné.

Operátoři přistupují ke své části systému CA pomocí VPN autentizované svým certifikátem. V rámci systému se pak kromě certifikátu prokazují i svým uživatelským jménem a heslem. Každý operátor má přiřazeny autorizační informace příslušné své roli. Všechny aktivity operátorů jsou zaznamenávány do auditního logu. Operátoři, pokud to jejich role nevyžaduje, nemají přístup ke složkám systému na nižších úrovních, jako např. přístup k operačnímu systému.

Systémy CA jsou fyzicky umístěny v chráněném objektu typu D a přístup k nim mají pouze vyjmenované osoby.

6.5.2 Hodnocení počítačové bezpečnosti

Hodnocení vychází z ČSN ISO 27 000, CWA 14167-1 a TS 101456 a soulad s těmito normami je ověřen auditem. Audity jsou prováděny na shodu s Nařízením eIDAS a normami:

•General Policy Requirements for TSPs (EN 319 401)
•Conformity Assessment, Requirements for CAB accreditation (EN 319 403)
•Policy Requirements for TSPs issuing Q and non-Q certificates (EN 319 411, 2 parts)
•Certificate profiles (EN 319 412, 5 parts)
•Policy requirements for TSAs (EN 319 421)
•Time stamping profile (EN 319 422)
•AdES Signature formats: CAdES, PAdES (EN 319 122 / 142)

6.6 Technické kontroly životního cyklu

6.6.1 Řízení vývoje systému

Vývoj systému probíhal podle pravidel Zabezpečení vývoje.

6.6.2 Kontroly řízení bezpečnosti

Systém CA eIdentity obsahuje nástroje pro kontrolu integrity aplikace, které jsou pravidelně spouštěny a jejich výstup vyhodnocován. Integrita aplikace je ověřována otisky souborů aplikace na provozních serverech oproti jejich otiskům pořízených vývojáři před jejich uvedením do provozu.

6.7 Řízení síťové bezpečnosti

Pro zajištění síťové bezpečnosti jsou v rámci systému CA eIdentity použity firewally několika úrovní.

Všechny servery CA eIdentity mají IP adresy z neveřejného rozsahu, což zaručuje nemožnost jejich adresace sítí Internet. Jediným bodem spojení s internetem je veřejné rozhraní na portech HTTP a HTTPS, které je chráněno firewallem na 7. vrstvě OSI modelu.

Vnitřní část systému od vnější je oddělena firewallem na 5. vrstvě OSI modelu, který umožňuje

přístup k vnitřní části pouze autorizovaným VPN klientům.

Na každém ze serverů je navíc ještě nakonfigurován lokální firewall znemožňující přístup k nepublikovaným portům i v rámci vnitřní sítě.

6.8 Časová razítka

Auditní logy a databázové záznamy žádostí o certifikát, žádostí o revokaci certifikátu, CRL a certifikátů obsahují informace o čase. Čas je v rámci vnitřní sítě synchronizován oproti CA APP serveru protokolem NTP.

7 CERTIFIKÁT, CRL A OCSP PROFILY

7.1 Profil certifikátu

Profily jednotlivých certifikátů jsou uvedeny v jednotlivých certifikačních politikách k jednotlivým službám.

7.2 Profil CRL

Profily jednotlivých CRL jsou uvedeny v jednotlivých certifikačních politikách k jednotlivým službám

7.3 Profil OCSP

Profily OCSP jsou uvedeny v jednotlivých certifikačních politikách k jednotlivým službám

8 AUDIT SHODY A OSTATNÍ HODNOCENÍ

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Audit se provádí nejméně jednou ročně nebo při každé změně konfigurace.

8.2 Identita a kvalifikace hodnotitele

Hodnotitel musí vlastnit certifikát, který ho opravňuje k vykonávání takové činnosti.

8.3 Vztah hodnotitele k hodnocené entitě

Hodnotitel nesmí být v žádném obchodním vztahu s hodnoceným.

8.4 Hodnocené oblasti

Seznam témat a způsob jejich hodnocení je dán použitou metodologií hodnocení.

8.5 Postup v případě zjištění nedostatků

Při zjištění nedostatků dojde k úpravě bezpečnostní dokumentace a následně popisu systému, případně implementačních či konfiguračních nastavení tak, aby došlo k odstranění nedostatků.

8.6 Sdělování výsledků hodnocení

Výsledky auditů jsou dostupné statutárnímu zástupci organizace a pracovníkovi zodpovědnému za bezpečnost provozu (Manager IT, Security Officer apod.).

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání, příp. obnovení certifikátu

Výše poplatků za vydání certifikátu podřízeným certifikačním autoritám je určována individuálně v nabídce služeb. Služba obnovení certifikátu se neposkytuje. Lze však vydat následný certifikát.

9.1.2 Poplatky za přístup k certifikátu

Přístup k seznamu vydaných certifikátů (CRL) je zdarma.

9.1.3 Poplatky za informace o stavu certifikátu a o zneplatnění

Přístup k CRL je zdarma.

9.1.4 Poplatky za další služby

Ceny dalších poskytovaných služeb jsou uvedeny v Ceníku služeb.

9.1.5 Jiná ustanovení týkající se poplatků

S ohledem na výše cen účtovaných služeb se nepředpokládá žádné rozložení plateb za odebrané služby.

9.2 Finanční zodpovědnost

9.2.1 Krytí pojištěním

Společnost eIdentity a.s. má uzavřenu pojistku podnikatelských rizik v dostatečné výši, aby byly pokryty případné finanční škody.

9.2.2 Další aktiva

Společnost eIdentity a.s. má připraveny i další kapitálové zdroje, které zajistí poskytování kvalitních certifikačních služeb na požadované úrovni kvality.

9.2.3 Pojištění nebo krytí zárukou pro koncové entity/uživatele

Služba se neposkytuje.

9.3 Důvěrnost obchodních informací

9.3.1 Stupnice (klasifikace) důvěrnosti informací

Za neveřejné obchodní informace se považují zejména informace o odebíraných službách, jejich ceny a obchodní smlouvy s nimi svázané. Za další takové informace se považují i smlouvy s třetími stranami, které se podílejí na provozu či jeho zajištění ACAeID, žádosti o poskytnutí služby, auditní a transakční záznamy, havarijní plány a plány obnovy, certifikační prováděcí směrnice, způsoby ochrany osobních údajů, zabezpečení obsluhy systému ACAeID, bezpečnostní opatření a jejich realizace.

9.3.2 Informace mimo rámec stupnice důvěrnosti informací

Za takové jsou považovány informace, které jsou zveřejněné pomocí webových služeb.

9.3.3 Odpovědnost za ochranu důvěrných informací

Každý pracovník, který přijde s informacemi podle kapitoly 9.3.1 do styku, je nesmí poskytnout třetí straně bez souhlasu odpovědného pracovníka eIdentity a.s.

9.4 Důvěrnost osobních informací

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. a je podrobně popsána v neveřejném dokumentu ACAeID20 Ochrana osobních údajů.

9.4.1 Plán důvěrnosti

Tato oblast je zpracována v dokumentu ACAeID20 Ochrana osobních údajů.

9.4.2 Osobní údaje

Tato oblast je zpracována v dokumentu ACAeID20 Ochrana osobních údajů.

9.4.3 Informace, které nejsou osobními údaji

Tato oblast je zpracována v dokumentu ACAeID20 Ochrana osobních údajů.

9.4.4 Odpovědnost za ochranu osobních údajů

Tato oblast je zpracována v dokumentu ACAeID20 Ochrana osobních údajů.

9.4.5 Oznámení a souhlas s používáním osobních údajů

Tato oblast je zpracována v dokumentu ACAeID20 Ochrana osobních údajů.

9.4.6 Zpřístupňování osobních údajů

Tato oblast je zpracována v dokumentu ACAeID20 Ochrana osobních údajů.

9.4.7 Jiné náležitosti zpřístupňování osobních údajů

Tato oblast je zpracována v dokumentu ACAeID20 Ochrana osobních údajů.

9.5 Práva duševního vlastnictví

ACAeID zachovává veškerá práva na intelektuální vlastnictví týkající se obsahu certifikátu a revokačních dat, obsahu politik, podle kterých se řídí poskytování certifikačních služeb a obsahu jmen, která mohou obsahovat ochranné známky, obchodní či jiné chráněné informace.

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

ACAeID zaručuje, že:

- Veškeré údaje v certifikátu jsou uvedeny po jejich úspěšném prokázání hodnověrnými dokumenty
- Jsou uvedeny pouze správné a pravdivé údaje
- Certifikáty jsou vydány plně v souladu s touto CP
- Služba zneplatnění je poskytována plně v souladu s CP

Další záruky mohou být specifikovány ve smlouvě o poskytnutí služby.

9.6.2 Zastupování a záruky RA

ACAeID zaručuje, že průběh procesu na registračním místě bude plně v souladu s touto CP.

9.6.3 Zastupování a záruky podepisující osoby

Podepisující osoby budou ručit za informace podle smlouvy o poskytnutí služby.

9.6.4 Zastupování a záruky spoléhajících se stran

Předpokládá se, že spoléhající se strany postupují v souladu se zákonem 297/2016 Sb. a jeho prováděcími předpisy.

9.6.5 Zastupování a záruky ostatních účastníků

Neposkytuje se.

9.7 Zřeknutí se záruk

Poskytování služeb se řídí zejména zákonem 297/2016 Sb. a nelze se zříci záruk v něm určených.

9.8 Hranice (meze) odpovědnosti

Hranice odpovědnosti jsou dány zákonem 297/2016 Sb. a jsou závazné pro všechny prvky PKI.

9.9 Náhrada škody

V případě vydání certifikátu, jehož obsah neodpovídá skutečnostem ověřeným v průběhu zdárného procesu na registračním místě, nebo v případě neoprávněného zneplatnění certifikátu, bude poskytnut nový certifikát zdarma.

Další možné náhrady škody vycházejí z ustanovení příslušných zákonů a o jejich výši může rozhodnout soud.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Certifikační politika zůstává v platnosti do konce doby platnosti posledního kvalifikovaného certifikátu, který byl podle této politiky vydán. Novou verzi schvaluje a vyhlašuje Výbor pro politiky na základě svého jednacího řádu.

9.10.2 Ukončení

Úpravy CP včetně zajištění souladu politik schvaluje Výbor pro politiky.

9.10.3 Důsledky ukončení a přetrvání závazků

CP bude platit nejméně po dobu platnosti posledního podle ní vydaného certifikátu.

9.11 Komunikace mezi účastníky

Pro účely individuální komunikace s jednotlivými subjekty se může využít prostředí jejich osobních účtů nebo emailových adres, telefonických rozhovorů či osobního jednání.

9.12 Změny

9.12.1 Postup při změnách

Řeší jednací řád Výboru pro politiky.

9.12.2 Postup při oznamování změn

Řeší jednací řád Výboru pro politiky.

9.12.3 Okolnosti, při kterých musí být změněn OID

Řeší jednací řád Výboru pro politiky.

9.13 Opatření pro řešení sporů

V případě nesouhlasu s postupem pracovníků eIdentity a.s. je možné se obrátit přímo na statutární orgán společnosti, případně se obrátit na soud místně příslušný sídlu poskytovatele.

9.14 Relevantní právní úprava

Činnost eIdentity a.s. se řídí právním řádem České republiky.

9.15 Shoda s právními předpisy

Systém je provozován ve shodě s požadavky zákona 297/2016 Sb., 110/2019 Sb., dalšími požadavky a je provozován jako akreditovaný k poskytování kvalifikovaných certifikačních služeb.

9.16 Další ustanovení

Není použito.

9.16.1 Celková dohoda

Není použito.

9.16.2 Postoupení práv

Není použito.

9.16.3 Oddělitelnost

Není použito.

9.16.4 Platby obhájcům a zřeknutí se práv

Není použito.

9.16.5 Vyšší moc

Smlouva o poskytnutí služby může obsahovat ustanovení o působení vyšší moci.

9.17 Další opatření

Není použito.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato CPS – QS byla projednána na jednání Výboru pro politiky a podle zápisu byla přijata a vyhlášena.