ACAeID 10.9 Politika služby vzdáleného podpisu dle eIDAS - BankID

Kvalifikovaný poskytovatel služeb vytvářejících důvěru eIdentity a.s.

Jan Stelibský

25.03.2024

Obsah

Copyright © 2024 eIdentity a.s.

Žádná část tohoto dokumentu nesmí být kopírována žádným způsobem bez písemného souhlasu majitelů autorských práv.

Některé názvy produktů a společností citované v tomto díle mohou být ochranné známky příslušných vlastníků.

Schváleno:

Verze	Schválil
1.0	Ing. Ladislav Šedivý

Historie dokumentu:

Verze	Datum	Autor	Poznámka
1.0	25.03.2024	Jan Stelibský	Počáteční verze

1 Úvod

1.1 Přehled

Tento dokument popisuje politiku služby vzdáleného podpisu dle eIDAS poskytovanou společnosti eIdentity a.s.

1.2 Název a identifikace dokumentu

Český normalizační institut přidělil společnosti eIdentity a.s. OID ve tvaru 1.2.203.27112489.

Podtřída 1.2.203.27112489.1. je interně určena pro dokumentaci ACAeID, její další členění je určeno číslem dokumentu a jeho verzí, tedy např. 10.1.1.1 značí dokument ACAeID10.1 ve verzi 1.1.

Identifikační znak	Význam identifikačního znaku	Hodnota
Název dokumentu	Název dokumentu v čitelné podobě	ACAeID 10.9 Politika služby vzdáleného podpisu dle eIDAS - BankID
OID	Identifikace dokumentu v rámci prostoru OID eIdentity a.s.	1.2.203.27112489.1.10.9.1.0

Podporovaná podpisová OID dle této politiky:

- 0.4.0.19431.2.1.2 (eu-advanced-x509, AdES založený na X.509 certifikátech)
- 0.4.0.19431.1.1.3 (EU SSASC policy) - podpisové klíče jsou uloženy v QSCD.

1.3 Participující subjekty

1.3.1 Poskytovatel služeb

Službu vzdáleného podepisování poskytuje společnost eIdentity a.s..

Údaje pro kontaktování společnosti:

eIdentity a.s.

Vinohradská 184

130 00 Praha 3

Česká republika

mail: info@eidentity.cz

DS: vhcdupm

1.3.2 Podepisující osoba

Uživatel, který využívá službu k vytvoření kvalifikovaného elektronického podpisu dokumentu.

1.3.3 Spoléhající se strany

Spoléhající se stranou je subjekt, který se spoléhá na elektronický podpis vytvořený v rámci Služby.

1.3.4 Jiné participující subjekty

Bankovní instituce, které zprostředkovávají svým uživatelům službu BankID, participují v roli poskytovatelů ztotožnění pomocí prostředku elektronické identifikace a z toho vyplývajících údajů pro vydání certifikátu. Bankovní identita a.s. vyvíjí a provozuje službu vzdáleného podepisování pro poskytovatele služeb.

1.4 Použití Služby

1.4.1 Přípustné použití Služby

Službu lze využívat pouze v procesech vytváření elektronického podpisu pro klienta ve prospěch konkrétní třetí strany v souladu s platnou právní úpravou.

1.4.2 Omezení použití služby

Služba podle této Politiky nesmí sloužit k jakémukoli nelegálnímu účelu a její použití je omezeno na přípustné způsoby popsané v kapitole 1.4.1.

1.5 Správa politiky

Za údržbu a schválení tohoto dokumentu odpovídá Výbor pro politiky.

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

eIdentity a.s.

Vinohradská 184

130 00 Praha 3

Česká republika

1.5.2 Kontaktní osoba organizace spravující politiku nebo prováděcí směrnici

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 postupů poskytovatele a postupy jiných poskytovatelů služeb vytvářejících důvěru

Soulad politiky s jí odpovídající prováděcí směrnicí schvaluje Výbor pro politiky na základě schůze Výboru a v souladu s jednacím řádem tohoto orgánu.

1.5.4 Postupy při schvalování prováděcí směrnice

Postupy jsou určeny jednacím řádem Výboru pro politiky.

1.6 Pojmy a zkratky

eIDAS Nařízení Evropského parlamentu a Rady (EU) č. 910/2014

ACAeID, ACA Informační systém eIdentity a.s., poskytující služby vytvářející důvěru

CP Certifikační politika

CPS Certifikační prováděcí směrnice

QC Kvalifikovaný certifikát pro elektronický podpis

QSC Kvalifikovaný certifikát pro elektronickou pečeť

RQSC Kořenový kvalifikovaný certifikát pro elektronickou pečeť

CRL Seznam zneplatněných certifikátů

poskytovatel, PSVD Poskytovatel služeb vytvářejících důvěru

EVI Evidenční část informačního systému PCS

soukromý klíč Data pro vytváření elektronických podpisů nebo pečetí

veřejný klíč Data pro ověřování elektronických podpisů nebo pečetí

revokace zneplatnění certifikátu

DN Distinguished Name Jednoznačná identifikace subjektu certifikátu

Bank iD Bankami poskytovaná metoda digitálního ověření totožnosti

ZR Základní registry

DIA Digitální a informační agentura

2 Odpovědnost za zveřejňování a úložiště informací a dokumentace

2.1 Úložiště informací a dokumentace

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 a dokumentace

eIdentity zveřejňuje informace na svých webových stránkách www.eidentity.cz. Součástí zveřejňovaných informací je zejména tato politika a související certifikační politiky.

Informace lze získat také pomocí následujících kontaktních údajů:

eIdentity a.s.

Vinohradská 184

130 00 Praha 3

Česká republika

mail: info@eidentity.cz

DS: vhcdupm

2.3 Periodicita zveřejňování informací

eIdentity zveřejňuje informace bez zbytečného odkladu po schválení změn Výborem.

2.4 Řízení přístupu k jednotlivým typům úložišť

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

3 Identifikace a autentizace ke službě

3.1 Počáteční ověření identity

3.1.1 Ověřování identity fyzické osoby

Pro ověření identity pro vydání certifikátu a využití služby Remote Signu se postupuje dle eIDAS čl. 21 1)b a d. Využívají se prostředky úrovně značná, které jsou registrovany v NIA a jsou používány v schématu Bankovní identity, které jsou poskytovány Bankami. Tyto prostředky zaručují podmínku ekvivalence fyzické prezence. Vydání certifikátu a použití služby je možné pouze pokud

- osoba má elektronickou identitu vydanou Bankou
- fyzickou osobu lze identifikovat v Základních registrech a banka má aktuální data o fyzické osobě získané buď online dotazem nebo zpracováním notifikací z ISZR.

3.2 Ověření identity při prodloužení služby

Prodloužení Služby se neposkytuje.

3.3 Změna údajů

Změna údajů se neprovádí.

4 Požadavky na životní cyklus služby

4.1 Uzavření smlouvy

Na základě požadavku spoléhající se strany je uživatel přesměrován na stránky rozhraní Služby, kde jednorázově souhlasí s vytvořením kvalifikovaného podpisu. Před vytvořením podpisu se získává jednorázový souhlas klienta s podpisem dokumentu a uzavírá rámcová smlouva mezi fyzickou osobou a eIdentity a.s na 2 roky, pokud již nebyla uzavřena.

4.2 Zřízení Služby

Služba se zřizuje automaticky při každém použití služby. Před zřízením služby musí existovat platná smlouva mezi osobou a eIdentity.

4.2.1 Registrační proces a odpovědnosti

Proces popisuje politika vydávání certifkátů ACAeID 10.8, dostupná na stránkách eIdentity a.s.

4.2.2 Převzetí vydaného Certifikátu

Certifikát zůstavá ve správě eIdentity na kvalifikovaném prostředku. Nepředává se konečnému uživateli.

4.3 Konec platnosti Smlouvy

Smlouva má platnost 2 roky nebo lze zneplatit žádostí na kontaktních místech eIdentity, a.s.

4.4 Používání Služby

Služba se využivá k vydání jednorázového certifikátu a podpisu dokumentů v jedné transakci. Použití služby iniciuje spoléhající se strana, která ve svém procesu požaduje po uživateli služby podpis dokumentu pomocí kvalifikovaného certifikátu. Spoléhající strana zakládá v rozhraní Služby požadavek na podpis dokumentu. Dokumenty jsou uploadovány do rozhraní Služby. Uživatel je pak spoléhající se stranou přesměrován na uživatelské rozhraní Služby pro vytvoření elektronického podpisu.

Uživateli je zobrazena stránka se souhlasem k podpisu, kde si může zobrazit podepisované dokumenty a kde může vyjádřit svůj souhlas s vytvořením podpisu.

Po vyjádření souhlasu si uživatel v rozhraní služby zvolí banku a je přesměrován na rozhraní banky pro ztotožnění elektronickou identifikací. V bance je autentizován pomocí prostředku elektronické identifikace a je mu zobrazena stránka se souhlasem pro vytvoření podpisu, vydání certifikátu a předání údajů potřebných k vydání certifikátu.

Po dvoufaktorové autentizaci souhlasu je uživatel navrácen do uživatelského rozhraní Služby a potvrdí uzavření rámcové smlouvy, pokud již nebyla uzařena, a potvrdí souhlas s vydáním kvalifikovaného certifikátu.

Následně Služba vytvoří pár klíčů na QSCD, vydá kvalifikovaný certifikát a vytvoří pomocí QSCD kvalifikovaný podpis dokumentů. Po dokončení podpisu je uživatel přesměrován do rozhraní spoléhající se strany a spoléhající se strana si může stáhnout z rozhraní Služby podepsané dokumenty. Zároveň je uživatel z bezpečnostních důvodů informován o podpisu dokumentu zprávou na e-mail uvedený v žádosti o certifikát a formou SMS na telefonní číslo získané cestou BankID. Klíče a certifikát jsou po provedení podpisu z QSCD odstraněny bez možnosti obnovy.

5 Postupy správy, řízení a provozu

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

Technologie jsou umístěny v datovém centrum splňujícím požadavky Tier III. Technologie je umístěna geograficky odděleně od jiných provozních prostor eIdentity a Bankovní identita, a.s.

5.1.2 Fyzický přístup

Požadavky na fyzický přistup jsou řešeny interními normami dotčených společností. Ochrana objektu je řešena zabezpečovacím systémem a systémem pro sledování pohybu osob a dopravních prostředků.

5.1.3 Elektřina a klimatizace

Provozní sál s technologiemi splňuje požadavky Tier III, má aktivní chlazení, 2 nezávislé-větvě napájení, jistěné UPS a dieselagregátem.

5.1.4 Vlivy vody

Datacentrum je umístěno mimo povodňovou zónu a jsou nainstalována čidla průniku vody.

5.1.5 Protipožární opatření a ochrana

Datacentrum je vybaveno systémem protipožární ochrany včetně automatického systému hašení.

5.1.6 Ukládání médií

Paměťová média, obsahující provozní zálohy a záznamy v elektronické podobě, jsou ukládána v kovových skříních, popř. trezorech. Kopie jsou ukládány v jiné geografické lokalitě, než kde je umístěno provozní pracoviště, na kterém záznamy vznikly.

5.1.7 Nakládání s odpady

Kancelářský odpad obsahující neveřejné informace je likvidován skartováním.

5.1.8 Zálohy mimo budovu

Kopie provozních záloh jsou zpracovávány v souladu s příslušnými směrnicemi.

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

Důvěryhodné role jsou:

statutární zástupce

ředitel společnosti

ředitel bezpečnosti (Security Officer)

Provozní manager ICT

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

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

5.2.3 Identifikace a autentizace pro každou roli

Jednotliví uživatelé se do aplikace hlásí pomocí osobních certifikátů v kryptografických zařízeních.

5.2.4 Role vyžadující rozdělení povinností

Role, které vyžadují rozdělení, jsou:

ředitel provozu

ředitel bezpečnosti

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Společnost eIdentity a.s. při práci s lidskými zdroji vybudovala 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.

5.3.2 Posouzení spolehlivosti osob

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.

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.

5.3.3 Požadavky na školení

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

5.3.4 Požadavky a periodicita doškolování

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

5.3.5 Periodicita a posloupnost rotace pracovníků 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.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

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

5.3.7 Požadavky na nezávislé dodavatele

Doporučuje se osvědčení podnikatele pro přístup k utajovaným informacím do stupně utajení VYHRAZENÉ vydané NBÚ nebo Prohlášení podnikatele o vytvoření podmínek pro ochranu utajované informace stupně utajení Vyhrazené.

5.3.8 Dokumentace poskytovaná zaměstnancům

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

5.4 Postupy zpracování auditních záznamů

5.4.1 Typy zaznamenávaných událostí

Auditní záznamy obsahují informace o všech důležitých událostech provozu systému.

5.4.2 Periodicita zpracování záznamů

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

5.4.3 Doba uchování auditních záznamů

Auditní záznamy se uchovávají po dobu nejméně 10 let.

5.4.4 Ochrana auditních záznamů

Přístup k auditním logům je řízen a logy jsou chráněny proti pozměnění.

5.4.5 Postupy pro zálohování auditních záznamů

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

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

O shromažďování auditních záznamů se vede evidence.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Neposkytuje se.

5.4.8 Hodnocení zranitelnosti

Události s vyšším stupněm závažnosti jsou eskalovány automaticky emailem odpovědné osobě.

5.5 Uchovávání záznamů

5.5.1 Typy uchovávaných záznamů

Archivace dat QCA 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 čas jejich archivace jsou uvedeny v přiloženém souboru, který je elektronicky podepsán.

5.5.2 Doba uchování 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 15 let.

5.5.3 Ochrana úložiště 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, jsou poučeny, že v archivu se vyskytují osobní údaje.

5.5.4 Postupy při zálohování záznamů

Postupy odpovídají bodu 5.5.1 této CP.

5.5.5 Požadavky na používání časových razítek při uchovávání záznamů

Záznamy v sobě nesou informaci o čase, ve kterém byly pořízeny. Nevyužívá se časových razítek, systémový čas je však navázán na UTC.

5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí) .

Archivní kopie se ukládají do bankovní schránky.

5.5.7 Postupy pro získání a ověření uchovávaných informací

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

5.5.8 Obnova po havárii nebo kompromitaci

5.5.9 Postup ošetření incidentu nebo kompromitace

V případě bezpečnostního incidentu odpovídajícího rozsahu se postupuje v souladu s dokumentem Plán pro zvládání krizových situací a plán obnovy.

5.5.10 Poškození výpočetních prostředků, softwaru nebo dat

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

5.5.11 Schopnost obnovit činnost po havárii

V případě bezpečnostního incidentu odpovídajícího rozsahu se postupuje v souladu s dokumentem Plán pro zvládání krizových situací a plán obnovy.

5.6 Ukončení činnosti poskytovatele služeb

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

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

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

Obdobná ustanovení platí i v případě jiných způsobů ukončení činnosti.

6 Řízení technické bezpečnosti

6.1 Počítačová bezpečnost

6.1.1 Specifické technické požadavky na počítačovou bezpečnost

Veřejná část systému ACA 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. Přístupové servery jsou pravidelně testovány na známé zranitelnosti.

Komunikace mezi ACAeID a Bank iD je zabezpečena šifrovaným kanálem HTTPS a je garantována smlouvou mezi eIdentity a.s. a Bankovní identitou a.s.

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

Systémy ACAeID jsou od internetového provozu odděleny vhodným bezpečnostním zařízením (např. firewall) a prostupný provoz je řízen a kontrolován.

Systémy ACAeID jsou fyzicky umístěny v chráněném objektu typu „D” a přístup k nim mají pouze určené osoby.

6.1.2 Hodnocení počítačové bezpečnosti

Hodnocení vychází z níže uvedených norem a soulad s těmito normami je ověřen auditem:

CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements/Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty pro elektronický podpis – část 1: Požadavky na bezpečnost systémů.

ČSN ETSI TS 101 456 - Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty

ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky

ČSN ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

ČSN ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací.

ČSN EN ISO 19011 - Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu.

6.2 Technické řízení životního cyklu

6.2.1 Řízení vývoje systému pro poskytování služby

Vývoj systému probíhal podle pravidel zabezpečení vývoje.

6.2.2 Řízení správy bezpečnosti

Systém ACA 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.

6.2.3 Řízení životního cyklu bezpečnosti

Řízení bezpečnosti probíhá v uzavřeném cyklu:

Analýza požadavků a definice systému

Návrh a řešení systému

Integrace

Implementace

Provoz (užívání)

Nepřetržité hodnocení provozu

Nepřetržité školení uživatelů

6.3 Řízení bezpečnosti sítě

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

6.4 Ochrana proti padělání a odcizení dat

Ochrana před padělaním a odcizením dat je zárukou bezpečnosti všech systémů eIdentity. Všechni zaměstnanci společnosti byli informováni o bezpečnostních postupech a mají příslušná oprávnění k provádění těchto opatření. Ochrana je tedy součástí celého systému řízení bezpečnosti informací a spolupodílí se na všech úrovních společnosti.

7 Hodnocení shody a jiná hodnocení

7.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Audit souladu systému s jeho dokumentací a požadavky se provádí nejméně jednou ročně nebo při každé změně konfigurace.

7.2 Identita a kvalifikace hodnotitele

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

7.3 Vztah hodnotitele k hodnocenému subjektu

Hodnotitel se nesmí podílet na budování či provozování hodnoceného systému.

7.4 Hodnocené oblasti

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

7.5 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.

7.6 Sdělování výsledků hodnocení

Výsledky auditů jsou dostupné statutárnímu zástupci organizace a pracovníkovi zodpovědnému za bezpečnost provozu.

8 Ostatní obchodní a právní záležitosti

8.1 Poplatky

8.1.1 Poplatky za využívání služby

Účtování poplatků je dáno smlouvou s konkrétní třetí stranou (formou může být paušální poplatek za určité časové období, placení za každé úspěšné vytvoření podpisu apod.).

8.1.2 Poplatky za další služby

Není relevantní pro tento dokument.

8.1.3 Postup při refundování

Není relevantní pro tento dokument.

8.2 Finanční odpovědnost

8.2.1 Krytí pojištěním

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

8.2.2 Další aktiva

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

8.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Služba se neposkytuje.

8.3 Důvěrnost obchodních informací

8.3.1 Rozsah důvěrných 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.

8.3.2 Informace mimo rámec důvěrných informací

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

8.3.3 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.

8.4 Ochrana osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. A rovněž s nařízením Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

8.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění. Za ochranu osobních údajů ve společnosti eIdentity a.s. odpovídá DPO.

8.4.2 Informace považované za osobní údaje

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění.

8.4.3 Informace nepovažované za osobní údaje

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění.

8.4.4 Odpovědnost za ochranu osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění.

8.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění.

8.4.6 Poskytování osobních údajů pro soudní či správní účely

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění.

8.4.7 Jiné okolnosti zpřístupňování osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění.

8.4.8 Práva duševního vlastnictví

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

8.5 Zastupování a záruky

8.5.1 Zastupování a záruky eIdentity

Společnost eIdentity a.s. zaručuje, že:

- podpis odpovídá dokumentu předloženému uživateli
- data pro vytváření elektronického podpisu jsou použita pouze v souladu se Službou a nebyla použita pro žádný jiný účel

Další záruky mohou být specifikovány ve smlouvě o poskytnutí služby.

8.5.2 Zastupování a záruky kontaktního místa

Společnost eIdentity a.s. zaručuje, že průběh procesů v Aplikaci bude plně v souladu s touto politikou.

8.5.3 Zastupování a záruky ostatních zúčastněných subjektů

Neposkytuje se.

8.6 Zřeknutí se záruk

Poskytování služeb se řídí zejména Nařízením Evropského parlamentu a Rady (EU) č. 910/2014.

8.7 Omezení odpovědnosti

Hranice odpovědnosti jsou dány Nařízením Evropského parlamentu a Rady (EU) č. 910/2014.

8.8 Záruky a odškodnění

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

8.8.1 Doba platnosti, ukončení platnosti

8.8.2 Doba platnosti

Politika zůstává v platnosti do konce poskytování služeb kvalifikovaného podpisu. Novou verzi schvaluje a vyhlašuje Výbor pro politiky na základě svého jednacího řádu.

8.8.3 Ukončení platnosti

Úpravy politiky včetně zajištění souladu politik schvaluje Výbor pro politiky.

8.8.4 Důsledky ukončení a přetrvání závazků

Politika bude platit nejméně po dobu provozu Služby.

8.9 Individuální upozorňování a komunikace se zúčastněnými subjekty

8.9.1 Novelizace

8.9.2 Postup při novelizaci

Postup probíhá řízeným procesem.

8.9.3 Postup a periodicita oznamování

Postup probíhá řízeným procesem.

8.9.4 Okolnosti, při kterých musí být změněn OID

Postup probíhá řízeným procesem.

8.10 Ustanovení o 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.

8.11 Rozhodné právo

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

8.12 Shoda s právními předpisy

Systém je provozován ve shodě s požadavky zákonů a předpisů, zároveň je provozován jako akreditovaný k poskytování kvalifikovaných služeb vytvářejících důvěru.

8.12.1 Další ustanovení

Není použito.

8.12.2 Rámcová dohoda

Není použito.

8.12.3 Postoupení práv

Není použito.

8.12.4 Oddělitelnost ustanovení

Není použito.

8.12.5 Vymáhání (poplatky za právní zastoupení a zřeknutí se práv)

Není použito.

8.12.6 Vyšší moc

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

8.13 Další opatření

Není použito.

9 Závěrečná ustanovení

Tato politika byla projednána na jednání Výboru pro politiky a podle zápisu byla přijata a vyhlášena.