ACAeID 10.9 Politika služby vzdáleného podpisu dle eIDAS – BankID

Kvalifikovaný poskytovatel služeb vytvářejících důvěru

Klasifikace dokumentu: TLP:CLEAR

Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze: 1.0.1
Datum: 07.05.2026
Vlastník dokumentu: LŠiroký (eIdentity, a.s.)
Schválil: Ing. Ladislav Šedivý

---

1 Úvod

1.1 Přehled

Tento dokument stanovuje politiku služby vzdáleného vytváření kvalifikovaných elektronických podpisů podle nařízení eIDAS, poskytovanou společností eIdentity a.s. ve vazbě na službu BankID / vzdálené podepisování.

Politika vymezuje účel a použití služby, participující subjekty, požadavky na ověření identity, životní cyklus služby, provozní a bezpečnostní opatření, hodnocení shody a vybrané obchodní a právní podmínky služby.

Služba je poskytována jako kvalifikovaná služba vytvářející důvěru v rozsahu vytváření kvalifikovaných elektronických podpisů na dálku s využitím kvalifikovaného prostředku pro vytváření elektronických podpisů (QSCD).

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, například 10.1.1.1 označuje dokument ACAeID 10.1 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 OID podpisových politik a politik služby vzdáleného podepisování dle této politiky:

- 0.4.0.19431.2.1.2 – **eu-advanced-x509**; politika pro AdES podpis založený na X.509 certifikátu.
- 0.4.0.19431.1.1.3 – **EU SSASC policy**; politika pro serverové vzdálené podepisování v režimu, kdy jsou data pro vytváření elektronického podpisu uložena a používána v QSCD.

1.3 Participující subjekty

1.3.1 Poskytovatel služeb

Službu vzdáleného podepisování poskytuje společnost eIdentity a.s.

Kontaktní údaje:

eIdentity a.s.
Hvožďanská 2053/3
148 00 Praha 4
Česká republika

E-mail: info@eidentity.cz

Datová schránka: vhcdupm

1.3.2 Podepisující osoba

Podepisující osobou je fyzická osoba, která 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 Bank iD, vystupují v roli poskytovatelů ztotožnění pomocí prostředku elektronické identifikace a poskytují údaje potřebné pro vydání kvalifikovaného certifikátu.

Bankovní identita a.s. zajišťuje provoz a rozvoj integračního prostředí Bank iD a podílí se na technické a procesní integraci služby vzdáleného podepisování s bankovní identitou.

1.4 Použití Služby

1.4.1 Přípustné použití Služby

Službu lze využívat pouze v podporovaných procesech vytváření kvalifikovaného elektronického podpisu pro podepisující osobu ve prospěch konkrétní spoléhající se strany a v souladu s platnou právní úpravou.

Služba je určena zejména pro podepisování dokumentů připravených bankou nebo jinou oprávněnou spoléhající se stranou v rámci podporovaného procesu.

1.4.2 Omezení použití Služby

Služba podle této politiky nesmí být použita k nelegálnímu účelu nebo způsobem, který je v rozporu s touto politikou, příslušnou certifikační politikou, smluvními podmínkami nebo právními předpisy.

Použití Služby je omezeno na přípustné způsoby popsané v kapitole 1.4.1.

1.5 Správa politiky

Za údržbu, přezkum a schválení tohoto dokumentu odpovídá Výbor pro politiky eIdentity a.s.

1.5.1 Organizace spravující politiku nebo prováděcí směrnici

eIdentity a.s.
Hvožďanská 2053/3
148 00 Praha 4
Česká republika

1.5.2 Kontaktní osoba organizace spravující politiku nebo prováděcí směrnici

Předseda Výboru pro politiky eIdentity a.s.

E-mail: 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 jednání Výboru a v souladu s jeho jednacím řádem.

1.5.4 Postupy při schvalování prováděcí směrnice

Postupy při schvalování prováděcí směrnice a souvisejících změn jsou určeny jednacím řádem Výboru pro politiky.

1.6 Pojmy a zkratky

Pojem / zkratka	Význam
ACAeID	Informační systém eIdentity a.s. poskytující služby vytvářející důvěru
AdES	Advanced Electronic Signature; pokročilý elektronický podpis
Bank iD	Bankami poskytovaná metoda digitálního ověření totožnosti
CAB	Conformity Assessment Body; subjekt posuzování shody
CP	Certifikační politika
CPS	Certifikační prováděcí směrnice
CRL	Certificate Revocation List; seznam zneplatněných certifikátů
DIA	Digitální a informační agentura
eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014
ETSI	European Telecommunications Standards Institute

GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679
HTTPS	Hypertext Transfer Protocol Secure; zabezpečený protokol pro komunikaci přes síť
ISZR	Informační systém základních registrů
OID	Object Identifier; objektový identifikátor
OVR	Označení požadavku podle ETSI TS 119 431-1
PSVD / TSP	Poskytovatel služeb vytvářejících důvěru / Trust Service Provider
QTSP	Qualified Trust Service Provider; kvalifikovaný poskytovatel služeb vytvářejících důvěru
QC	Kvalifikovaný certifikát pro elektronický podpis
QSCD	Qualified Signature Creation Device; kvalifikovaný prostředek pro vytváření elektronických podpisů
SAD	Signature Activation Data; data pro aktivaci podpisu vázaná na konkrétní podpisovou transakci
SCDev	Signature Creation Device; prostředek pro vytváření elektronických podpisů
SSASC	Server Signing Application Service Component; komponenta služby serverového podepisování
UTC	Coordinated Universal Time; koordinovaný světový čas
ZR	Základní registry
Data pro vytváření elektronických podpisů	Jedinečná data používaná podepisující osobou k vytváření elektronických podpisů
Data pro ověřování elektronických podpisů	Data používaná k ověření elektronického podpisu
Revokace	Zneplatnění certifikátu

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 s právními a regulatorními požadavky tak, aby záznamy nebo jejich změny mohly provádět

pouze pověřené osoby, aby bylo možné kontrolovat správnost záznamů a aby jakékoliv technické nebo programové změny porušující bezpečnostní požadavky byly zjistitelné.

Zveřejňované informace jsou určeny zejména spoléhajícím se stranám, aby mohly posoudit platnost a důvěryhodnost kvalifikovaného certifikátu a elektronického podpisu 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 prostřednictvím kontaktních údajů uvedených v kapitole 1.3.1.

2.3 Periodicita zveřejňování informací

eIdentity zveřejňuje schválené informace bez zbytečného odkladu po jejich schválení Výborem pro politiky.

2.4 Řízení přístupu k jednotlivým typům úložišť

Publikování politiky schvaluje Výbor pro politiky. Odpovědnou osobu za zveřejnění a správu publikovaných dokumentů určuje Výbor pro politiky v souladu se svým jednacím řádem.

Přístup k neveřejným nebo interním dokumentům a úložištím je řízen podle jejich klasifikace, účelu a oprávnění konkrétní osoby.

---

3 Identifikace a autentizace ke službě

3.1 Počáteční ověření identity

3.1.1 Ověřování identity fyzické osoby

Pro ověření identity fyzické osoby za účelem vydání kvalifikovaného certifikátu a využití služby vzdáleného podpisu se postupuje podle čl. 24 odst. 1a písm. c) nařízení eIDAS.

Ověření identity je založeno na použití prostředku pro elektronickou identifikaci podle § 38ab odst. 1 zákona č. 21/1992 Sb., o bankách, tj. bankovní identity, s úrovní záruky **značná** , v kombinaci s dalšími kontrolami a ověřovacími mechanismy zajišťujícími spolehlivé určení totožnosti podepisující osoby.

Vydání bankovní identity bankou je podmíněno předchozím ověřením totožnosti klienta, zejména ověřením totožnosti za fyzické přítomnosti, ověřením totožnosti prostřednictvím prostředku pro elektronickou identifikaci s úrovní záruky vysoká, ověřením prostřednictvím Národního bodu pro identifikaci a autentizaci nebo ověřením v informačním systému veřejné správy.

Vydání kvalifikovaného certifikátu a použití služby vzdáleného podpisu je možné pouze tehdy, pokud jsou splněny následující podmínky:

- podepisující osoba má elektronickou identitu vydanou bankou zapojenou do schématu Bank iD;
- fyzickou osobu lze jednoznačně identifikovat v základních registrech;
- banka disponuje aktuálními údaji o fyzické osobě, získanými buď on-line dotazem do základních registrů, nebo zpracováním notifikací z informačního systému základních registrů;
- údaje předané prostřednictvím Bank iD jsou dostatečné pro vydání jednorázového kvalifikovaného certifikátu podle certifikační politiky ACAeID 10.8.

3.2 Ověření identity při prodloužení služby

Prodloužení Služby se neposkytuje. Služba je poskytována pro konkrétní podpisovou transakci a její použití je spojeno s vydáním krátkodobého kvalifikovaného certifikátu.

3.3 Změna údajů

Změna údajů v rámci již zahájené nebo dokončené podpisové transakce se neprovádí. Pokud údaje potřebné pro vydání kvalifikovaného certifikátu neodpovídají požadavkům příslušné certifikační politiky, certifikát není vydán a podpisová transakce není dokončena.

---

4 Požadavky na životní cyklus služby

4.1 Uzavření smlouvy

Na základě požadavku spoléhající se strany je podepisující osoba přesměrována do uživatelského rozhraní Služby, kde se před vytvořením kvalifikovaného elektronického podpisu získává její souhlas s podpisem dokumentu.

Pokud dosud nebyla uzavřena rámcová smlouva mezi podepisující osobou a eIdentity a.s., je její uzavření potvrzeno před dokončením podpisové transakce. Rámcová smlouva je uzavírána na dobu 2 let, pokud není stanoveno jinak.

4.2 Zřízení Služby

Služba je zřízena automaticky při použití služby pro konkrétní podpisovou transakci. Před zřízením služby musí být splněny podmínky této politiky, příslušné certifikační politiky a smluvních podmínek.

4.2.1 Registrační proces a odpovědnosti

Registrační proces pro vydání krátkodobého kvalifikovaného certifikátu je popsán v certifikační politice ACAeID 10.8, která je dostupná na webových stránkách eIdentity a.s.

4.2.2 Převzetí vydaného certifikátu

Krátkodobý kvalifikovaný certifikát je vydán a použit v rámci Služby pro konkrétní podpisovou transakci. Certifikát ani data pro vytváření elektronického podpisu nejsou předávána podepisující osobě jako samostatný prostředek.

Data pro vytváření elektronického podpisu jsou vytvářena a používána v QSCD.

4.3 Konec platnosti smlouvy

Smlouva má platnost 2 roky, pokud není stanoveno jinak. Smlouvu lze ukončit nebo zneplatnit způsobem uvedeným ve smluvních podmínkách nebo na kontaktních místech eIdentity a.s.

4.4 Používání Služby

Služba se používá k vydání krátkodobého kvalifikovaného certifikátu pro elektronický podpis a k vytvoření kvalifikovaného elektronického podpisu dokumentu v rámci jedné podpisové transakce.

Použití Služby iniciuje spoléhající se strana, která ve svém procesu požaduje po podepisující osobě podepsání dokumentu pomocí kvalifikovaného elektronického podpisu. Spoléhající se strana založí v rozhraní Služby požadavek na podpis dokumentu a nahraje dokumenty určené k podpisu. Podepisující osoba je následně ze systému spoléhající se strany přesměrována do uživatelského rozhraní Služby.

V uživatelském rozhraní Služby je podepisující osobě zobrazena stránka se souhlasem k podpisu, na které má možnost zobrazit si podepisované dokumenty a vyjádřit souhlas s vytvořením kvalifikovaného elektronického podpisu.

Po vyjádření souhlasu si podepisující osoba v rozhraní Služby zvolí banku a je přesměrována do rozhraní banky za účelem ověření identity a autentizace prostřednictvím Bank iD. V rozhraní banky je podepisující osoba autentizována pomocí prostředku elektronické identifikace a je jí zobrazena informace o souhlasu s vytvořením podpisu, vydáním kvalifikovaného certifikátu a předáním údajů potřebných pro vydání certifikátu.

Po provedení dvoufaktorové autentizace a potvrzení souhlasu je podepisující osoba navrácena do uživatelského rozhraní Služby. Pokud dosud nebyla uzavřena rámcová smlouva mezi podepisující osobou a eIdentity a.s., podepisující osoba potvrdí její uzavření. Současně potvrdí souhlas s vydáním krátkodobého kvalifikovaného certifikátu pro elektronický podpis.

Následně Služba v rámci QSCD vygeneruje podpisový pár klíčů, vydá krátkodobý kvalifikovaný certifikát pro elektronický podpis a pomocí QSCD vytvoří kvalifikovaný elektronický podpis dokumentu. Po dokončení podpisové transakce je podepisující osoba přesměrována zpět do rozhraní spoléhající se strany a spoléhající se strana si může z rozhraní Služby stáhnout podepsané dokumenty.

Z bezpečnostních důvodů je podepisující osoba informována o provedeném podpisu zprávou zaslanou na e-mailovou adresu uvedenou v žádosti o certifikát a SMS zprávou na telefonní číslo získané prostřednictvím Bank iD. V případě, že podepisující osoba popře žádost o podpis nebo vytvoření podpisu, postupuje eIdentity podle interních pravidel pro řešení takové události; zejména zajistí zneplatnění příslušného certifikátu, pokud je to s ohledem na stav transakce relevantní, a informuje banku nebo jiný subjekt, který proces inicioval.

Data pro vytváření elektronického podpisu, resp. podpisový soukromý klíč, jsou po provedení podpisové transakce z QSCD odstraněny bez možnosti obnovy. Životní cyklus krátkodobého kvalifikovaného certifikátu je řízen podle příslušné certifikační politiky ACAeID 10.8.

Služba je určena pouze pro podepisování dokumentů připravených bankou nebo jinou oprávněnou spoléhající se stranou v rámci podporovaných procesů, například hypoteční nebo jiné smluvní dokumentace.

---

5 Postupy správy, řízení a provozu

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

Technologie podporující Službu jsou umístěny v chráněném datovém centru splňujícím požadavky na vysokou dostupnost, fyzickou ochranu a řízený přístup. Technologie jsou umístěny geograficky odděleně od jiných provozních prostor eIdentity a relevantních partnerů.

5.1.2 Fyzický přístup

Fyzický přístup k technologiím je řízen interními bezpečnostními pravidly eIdentity a provozovatele datového centra. Ochrana objektu je zajištěna technickými a organizačními opatřeními, zejména systémem kontroly vstupu, zabezpečovacím systémem, monitoringem pohybu osob a evidencí vstupů.

Přístup k technologiím mají pouze oprávněné osoby.

5.1.3 Elektřina a klimatizace

Provozní prostory s technologiemi jsou vybaveny odpovídajícím napájením, klimatizací a záložními zdroji. Napájení je zajištěno redundantně a chráněno záložními zdroji, zejména UPS a náhradním zdrojem elektrické energie.

5.1.4 Vlivy vody

Datové centrum je chráněno proti rizikům způsobeným vodou. Jsou přijata opatření pro snížení rizika průniku vody, včetně odpovídajícího umístění a detekčních prvků.

5.1.5 Protipožární opatření a ochrana

Datové centrum je vybaveno systémem protipožární ochrany, detekce požáru a odpovídajícími prostředky hašení.

5.1.6 Ukládání médií

Paměťová média obsahující provozní zálohy, archivní záznamy nebo neveřejné informace jsou ukládána v chráněných úložištích s řízeným přístupem. Kopie důležitých záznamů mohou být ukládány v jiné geografické lokalitě, než kde je umístěno provozní pracoviště.

5.1.7 Nakládání s odpady

Odpad obsahující neveřejné informace je likvidován bezpečným způsobem, zejména skartací nebo jiným způsobem odpovídajícím klasifikaci informací a interním pravidlům eIdentity.

5.1.8 Zálohy mimo budovu

Kopie provozních záloh a vybraných archivních záznamů jsou zpracovávány a ukládány v souladu s interními pravidly pro zálohování, archivaci, obnovu a ochranu informací.

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

Důvěryhodné role jsou zejména:

- statutární zástupce;
- ředitel společnosti;
- bezpečnostní ředitel;
- provozní ředitel;
- další role určené interní dokumentací eIdentity podle povahy provozu a bezpečnostních činností.

Důvěryhodné role, jejich odpovědnosti, pravomoci a případné neslučitelnosti jsou dále vymezeny v interní dokumentaci bezpečnostních a provozních rolí.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Pro bezpečnostně významné operace může být vyžadována účast nejméně dvou důvěryhodných osob. Rozsah činností, u nichž se tento požadavek uplatní, je stanoven interní bezpečnostní a provozní dokumentací.

5.2.3 Identifikace a autentizace pro každou roli

Osoby v důvěryhodných a provozních rolích se k systémům přihlašují individuálně, s využitím přidělených autentizačních prostředků. Sdílení identit nebo autentizačních prostředků není přípustné.

Přístupy jsou přidělovány podle role, odpovědnosti a principu nezbytné potřeby.

5.2.4 Role vyžadující rozdělení povinností

Rozdělení povinností se uplatňuje zejména mezi rolemi, jejichž souběh by mohl vést ke střetu zájmů, neoprávněné změně systému, obcházení kontrol nebo snížení nezávislosti bezpečnostního dohledu.

Role vyžadující oddělení jsou zejména:

- bezpečnostní ředitel;
- provozní ředitel;
- administrátorské a auditní role;
- další role uvedené v interní matici bezpečnostních a provozních rolí.

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

eIdentity zajišťuje, aby osoby podílející se na poskytování, správě nebo bezpečnosti Služby měly odpovídající kvalifikaci, zkušenosti, důvěryhodnost a znalosti nezbytné pro výkon svěřené role.

Důvěryhodnost zaměstnanců a dalších pracovníků je jedním ze základních předpokladů pro výkon činností, při nichž dochází k přístupu k citlivým aktivům, systémům nebo informacím.

5.3.2 Posouzení spolehlivosti osob

Spolehlivost osob je posuzována přiměřeně povaze jejich role, oprávnění a přístupu k citlivým aktivům. Zdrojem informací může být zejména pracovník sám, veřejně dostupné informace, reference, interní záznamy a další podklady v souladu s právními předpisy.

Bezúhonnost může být ověřována výpisem z rejstříku trestů, pokud je to přiměřené a v souladu s právními předpisy.

5.3.3 Požadavky na školení

Zaměstnanci a další pracovníci podílející se na poskytování Služby musí absolvovat vstupní bezpečnostní a aplikační školení v rozsahu odpovídajícím jejich roli.

5.3.4 Požadavky a periodicita doškolování

Zaměstnanci a další pracovníci musí absolvovat pravidelné doškolování v oblasti bezpečnosti, provozních pravidel, ochrany informací a relevantních změn v dokumentaci nebo systémech.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Pravidelná rotace pracovníků mezi rolemi se obecně nepředpokládá. Pokud je pro zajištění provozu nezbytné, aby pracovník dočasně vykonával jinou roli, musí být předem proškolen a musí mu být přidělena pouze oprávnění nezbytná pro výkon dané role.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

Neoprávněná činnost nebo porušení bezpečnostních pravidel se posuzuje podle závažnosti a může být řešeno jako porušení pracovních povinností, smluvních povinností nebo jako bezpečnostní incident. Sankce se řídí pracovněprávními předpisy, smluvními podmínkami a interními pravidly eIdentity.

5.3.7 Požadavky na nezávislé dodavatele

Dodavatelé, kteří se podílejí na poskytování, správě nebo bezpečnosti Služby, musí splňovat bezpečnostní, smluvní a organizační požadavky stanovené eIdentity. Přístup dodavatelů k systémům, informacím nebo prostorám je řízen, evidován a omezen na nezbytný rozsah.

Podle povahy činnosti mohou být po dodavateli požadována dodatečná bezpečnostní opatření, prohlášení, smluvní závazky, bezpečnostní prověrky nebo jiné důkazy způsobilosti.

5.3.8 Dokumentace poskytovaná zaměstnancům

Zaměstnancům a dalším pracovníkům je poskytována dokumentace potřebná pro výkon jejich role, zejména popis pracovní náplně, provozní postupy, bezpečnostní pravidla a uživatelská nebo administrátorská dokumentace systémů, se kterými pracují.

5.4 Postupy zpracování auditních záznamů

5.4.1 Typy zaznamenávaných událostí

Auditní záznamy obsahují informace o důležitých událostech provozu Služby, zejména o událostech souvisejících s vydáním certifikátu, vytvořením podpisu, autentizací, změnami konfigurace, administrátorskými zásahy, bezpečnostními událostmi a přístupy k relevantním systémům.

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou pravidelně zpracovávány a vyhodnocovány. Události s vyšší závažností jsou vyhodnocovány bez zbytečného odkladu, zejména v případě bezpečnostního incidentu nebo podezření na kompromitaci.

5.4.3 Doba uchování auditních záznamů

Auditní záznamy se uchovávají po dobu stanovenou právními a regulatorními požadavky, příslušnými politikami a interní dokumentací. Není-li stanovena delší doba, auditní záznamy se uchovávají nejméně 10 let.

5.4.4 Ochrana auditních záznamů

Přístup k auditním logům je řízen a omezen pouze na oprávněné osoby. Auditní záznamy jsou chráněny proti neoprávněné změně, smazání, zničení nebo neoprávněnému zpřístupnění.

5.4.5 Postupy pro zálohování auditních záznamů

Auditní logy jsou ukládány a zálohovány tak, aby bylo možné jejich obnovení po poruše, incidentu nebo jiné mimořádné události. Zálohy jsou chráněny obdobně jako primární auditní záznamy.

5.4.6 Systém shromažďování auditních záznamů

O shromažďování auditních záznamů se vede evidence. Auditní záznamy mohou být shromažďovány v interních systémech eIdentity nebo v určených systémech pro log management a bezpečnostní monitoring.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Oznamování události subjektu, který ji způsobil, se standardně neposkytuje, pokud právní předpis, smluvní závazek nebo interní postup nestanoví jinak. Události s dopadem na bezpečnost, důvěryhodnost nebo dostupnost Služby jsou řešeny podle pravidel řízení incidentů.

5.4.8 Hodnocení zranitelnosti

Události s vyšším stupněm závažnosti a zjištění související se zranitelnostmi jsou eskalovány odpovědným osobám. Identifikované zranitelnosti jsou evidovány, vyhodnocovány a řešeny v souladu s interním procesem řízení zranitelností a změnového řízení.

5.5 Uchovávání záznamů

5.5.1 Typy uchovávaných záznamů

eIdentity uchovává záznamy vztahující se k poskytování Služby tak, aby bylo možné zpětně prokázat řádné provedení jednotlivých úkonů, splnění požadavků této politiky, souvisejících certifikačních politik a právních a regulatorních požadavků vztahujících se ke kvalifikovaným službám vytvářejícím důvěru.

Uchovávány jsou zejména:

- údaje a záznamy související s žádostí o vydání kvalifikovaného certifikátu;
- záznamy o ověření identity a autentizaci podepisující osoby;
- záznamy o souhlasu podepisující osoby s vytvořením podpisu;
- záznamy o vydání kvalifikovaného certifikátu;
- vydané kvalifikované certifikáty;
- záznamy o vytvoření kvalifikovaného elektronického podpisu;
- záznamy o ukončení životního cyklu podpisového klíče a krátkodobého certifikátu;
- seznamy zneplatněných certifikátů a související revokační informace;
- auditní a provozní logy;
- bezpečnostní záznamy, záznamy o administrátorských zásazích a záznamy o relevantních bezpečnostních událostech;
- záznamy potřebné pro řešení reklamací, sporů, incidentů a prokázání souladu při auditu.

Archivované záznamy jsou opatřeny takovými technickými a organizačními opatřeními, aby byla zajištěna jejich integrita, důvěrnost, dostupnost a ověřitelnost po celou dobu uchování.

5.5.2 Doba uchování záznamů

Záznamy vztahující se k poskytování Služby jsou uchovávány po dobu stanovenou právními předpisy, regulatorními požadavky, příslušnými ETSI normami, certifikačními politikami a interní dokumentací eIdentity.

Není-li pro konkrétní typ záznamu stanovena delší doba uchování, jsou záznamy uchovávány po dobu nejméně 15 let od jejich vzniku nebo od ukončení poskytování příslušné služby, podle toho, která skutečnost nastane později.

Doba uchování auditních záznamů je stanovena tak, aby umožňovala zpětné prokázání činností souvisejících s poskytováním kvalifikované služby, řešení incidentů, reklamací, sporů a provádění auditů.

5.5.3 Ochrana úložiště záznamů

Uchovávané záznamy jsou chráněny proti neoprávněnému přístupu, změně, zničení, ztrátě nebo neoprávněnému zpřístupnění. Přístup k archivním záznamům je řízen podle typu záznamu, jeho klasifikace a oprávnění konkrétní osoby.

Veřejně dostupné informace, zejména vydané certifikáty a revokační informace, mohou být zpřístupněny v rozsahu stanoveném příslušnou certifikační politikou. Auditní, provozní, bezpečnostní a transakční záznamy jsou dostupné pouze oprávněným osobám prostřednictvím řízených přístupových mechanismů.

Osoby s oprávněním k přístupu k archivním záznamům jsou poučeny o povinnosti zachovávat důvěrnost informací a o tom, že archivní záznamy mohou obsahovat osobní údaje, důvěrné informace, provozní informace a bezpečnostně citlivé informace.

5.5.4 Postupy při zálohování záznamů

Záznamy jsou pravidelně zálohovány v souladu s interními pravidly zálohování, archivace a obnovy. Zálohování je prováděno tak, aby bylo možné obnovit záznamy v případě technické poruchy, poškození dat, bezpečnostního incidentu nebo jiné mimořádné události.

Záložní kopie jsou ukládány odděleně od produkčních systémů a chráněny proti neoprávněnému přístupu, změně, ztrátě a zničení. Integrita archivovaných dat je ověřována prostřednictvím kontrolních mechanismů, zejména pomocí kryptografických otisků, elektronického podpisu nebo jiných odpovídajících prostředků.

5.5.5 Požadavky na používání časových údajů při uchovávání záznamů

Záznamy obsahují údaj o čase, ve kterém byly pořízeny nebo zpracovány. Systémový čas relevantních systémů je synchronizován s důvěryhodným zdrojem času navázaným na UTC.

U vybraných archivních záznamů mohou být pro posílení prokazatelnosti, integrity a časového určení použity elektronické podpisy, elektronické pečetě, elektronická časová razítka nebo jiné odpovídající technické prostředky.

5.5.6 Systém shromažďování uchovávaných záznamů

Záznamy jsou shromažďovány a uchovávány v systémech eIdentity určených pro provozní evidenci, auditní záznamy, bezpečnostní monitoring a archivaci. Ukládání a správa archivních kopií probíhá podle interních pravidel eIdentity pro archivaci, zálohování a ochranu záznamů.

Archivní kopie mohou být uchovávány v elektronické podobě na zabezpečených úložištích, případně na oddělených archivních médiích nebo v jiném řízeném úložišti, pokud takový způsob uchování splňuje požadavky na integritu, dostupnost, důvěrnost a obnovitelnost záznamů.

5.5.7 Postupy pro získání a ověření uchovávaných informací

Uchovávané informace lze získat pouze řízeným postupem a pouze osobami, které k tomu mají oprávnění. Každý přístup k auditním, provozním nebo bezpečnostně citlivým archivním záznamům je prováděn v souladu s interními pravidly řízení přístupu a je přiměřeně evidován.

Ověření integrity archivovaných informací se provádí zejména porovnáním kryptografických otisků, ověřením elektronického podpisu, elektronické pečeti, časového údaje nebo jiného mechanismu použitého při archivaci.

5.5.8 Obnova po havárii nebo kompromitaci

V případě bezpečnostního incidentu, havárie, kompromitace, poškození systému, softwaru nebo dat se postupuje podle interní dokumentace pro zvládání incidentů, krizových situací, obnovu služeb a kontinuitu činností.

Cílem obnovy je zajistit obnovení dostupnosti, integrity a důvěrnosti systémů a záznamů potřebných pro poskytování Služby a pro prokázání řádného poskytování kvalifikované služby.

5.5.9 Postup ošetření incidentu nebo kompromitace

V případě bezpečnostního incidentu nebo podezření na kompromitaci se postupuje podle interní politiky řízení incidentů, plánu pro zvládání krizových situací a plánu obnovy. Incident je evidován, klasifikován, analyzován, řešen a vyhodnocen v souladu s interními pravidly eIdentity a použitelnými právními a regulatorními požadavky.

Pokud incident může mít dopad na důvěrnost, integritu nebo dostupnost Služby, na data pro vytváření elektronických podpisů, na vydané certifikáty nebo na důvěryhodnost poskytované služby, jsou přijata přiměřená nápravná a ochranná opatření včetně případné eskalace, oznámení příslušným orgánům a informování dotčených subjektů.

5.5.10 Poškození výpočetních prostředků, softwaru nebo dat

Systém je navržen a provozován tak, aby bylo možné v případě poškození výpočetních prostředků, softwaru nebo dat obnovit provoz Služby v požadovaném rozsahu a čase. Obnova může zahrnovat výměnu poškozených technických prostředků, obnovu softwaru, obnovu konfigurací, obnovu dat ze záloh nebo aktivaci náhradních provozních postupů.

5.5.11 Schopnost obnovit činnost po havárii

eIdentity udržuje postupy a opatření pro obnovu činnosti po havárii nebo jiné mimořádné události. Tyto postupy jsou stanoveny v interní dokumentaci pro kontinuitu činností, zvládání krizových situací a obnovu služeb.

Postupy obnovy jsou pravidelně přezkoumávány a podle potřeby testovány tak, aby byla zajištěna schopnost obnovit poskytování Služby v požadovaném čase a rozsahu.

5.6 Ukončení činnosti poskytovatele služeb

eIdentity v případě plánovaného ukončení poskytování Služby postupuje řízeným způsobem tak, aby byla zachována dostupnost potřebných záznamů, ochrana uživatelů, informování příslušných orgánů a minimalizace dopadů na spoléhající se strany.

eIdentity informuje DIA nejméně 3 měsíce před předpokládaným ukončením činnosti. Současně vynaloží veškeré možné úsilí k tomu, aby vedená evidence byla převzata jiným kvalifikovaným poskytovatelem služeb vytvářejících důvěru, pokud je to relevantní a proveditelné.

eIdentity dále informuje dotčené uživatele nebo smluvní partnery o záměru ukončit činnost v přiměřené lhůtě a způsobem odpovídajícím povaze poskytované Služby a smluvním podmínkám.

Pokud se nepodaří zajistit převzetí evidence jiným kvalifikovaným poskytovatelem služeb vytvářejících důvěru, eIdentity informuje DIA nejméně 30 dní před ukončením činnosti. Obdobná ustanovení platí i v případě jiných způsobů ukončení poskytování Služby.

---

6 Řízení technické bezpečnosti

6.1 Soulad s ETSI TS 119 431-1

Služba vzdáleného vytváření kvalifikovaných elektronických podpisů podle této politiky je z hlediska technických, provozních a bezpečnostních požadavků posuzována také ve vazbě na ETSI TS 119 431-1 V1.3.1, zejména v rozsahu požadavků vztahujících se k poskytování služby provozující vzdálený QSCD / SCDev a k serverovému vytváření kvalifikovaných elektronických podpisů.

Pro účely této politiky jsou relevantní zejména následující požadavky ETSI TS 119 431-1:

- **OVR-6.4.3-01A** – požadavky na procedurální kontroly, zejména na důvěryhodné role, rozdělení odpovědností, oddělení neslučitelných činností, řízení privilegovaných oprávnění, schvalování citlivých operací a kontrolu provozních postupů;
- **OVR-6.5.3-01A** – požadavky na počítačovou bezpečnost, zejména na bezpečnou konfiguraci systémů, řízení privilegovaných přístupů, logování, monitoring, řízení zranitelností, ochranu systémových komponent a ochranu proti neoprávněným zásahům;
- **OVR-6.5.4-01** – požadavky na technické řízení životního cyklu, zejména na bezpečný vývoj, řízení změn, testování, schvalování změn, nasazování, správu verzí, ukončování komponent a řízení bezpečnosti v průběhu životního cyklu služby.

Požadavky podle ETSI TS 119 431-1 jsou v prostředí eIdentity naplňovány kombinací této politiky, certifikační politiky ACAeID 10.8, Zprávy pro uživatele, certifikační prováděcí směrnice, interních bezpečnostních politik, pravidel pro bezpečnostní a provozní role, řízení přístupů, řízení změn, incident managementu, politiky bezpečnosti vývoje, systémové bezpečnostní dokumentace, auditní a archivační dokumentace a související provozní dokumentace.

Detailní mapování požadavků ETSI TS 119 431-1 na konkrétní dokumenty, postupy a auditní důkazy je vedeno v samostatné auditní matici a předkládá se auditorovi jako součást důkazní dokumentace.

6.2 Počítačová bezpečnost

6.2.1 Specifické technické požadavky na počítačovou bezpečnost

Veřejně dostupné části systému ACAeID a služby vzdáleného podpisu jsou zpřístupněny prostřednictvím zabezpečeného komunikačního kanálu HTTPS. Případný provoz prostřednictvím protokolu HTTP je omezen pouze na veřejné informace nebo je přesměrován na HTTPS tak, aby nedocházelo k přenosu citlivých údajů nezabezpečeným kanálem.

Komponenty veřejné části systému, které slouží pouze k poskytování veřejných informací, jsou určeny pouze ke čtení a neumožňují vzdálenému uživateli provádět změny údajů v systému. Veškeré úkony, při nichž dochází ke zpracování osobních údajů, údajů pro vydání certifikátu, údajů souvisejících s autentizací uživatele nebo údajů souvisejících s vytvořením elektronického podpisu, jsou prováděny výhradně prostřednictvím zabezpečených komunikačních kanálů.

Komunikace mezi systémem ACAeID / službou vzdáleného podpisu a Bank iD je zabezpečena šifrovaným komunikačním kanálem HTTPS. Podmínky integrace, bezpečnosti komunikace, odpovědností a předávání údajů jsou upraveny smluvním vztahem mezi eIdentity a.s. a Bankovní identitou a.s.

Autentizace podepisující osoby a potvrzení souhlasu s vytvořením kvalifikovaného elektronického podpisu probíhá prostřednictvím Bank iD a prostředků elektronické identifikace zapojených do schématu bankovní identity. Citlivé údaje jsou v rámci Služby předávány výhradně zabezpečenými kanály a pouze v rozsahu nezbytném pro vydání krátkodobého kvalifikovaného certifikátu a vytvoření kvalifikovaného elektronického podpisu.

Systémy ACAeID a související komponenty služby vzdáleného podpisu jsou odděleny od veřejného internetového provozu pomocí bezpečnostních síťových prvků, zejména firewallů a dalších mechanismů řízení a kontroly síťového provozu. Přístup z veřejné sítě je omezen pouze na nezbytná rozhraní Služby. Ostatní systémy a interní komponenty jsou dostupné pouze z vyhrazených interních nebo správcovských sítí.

Přístupové servery, veřejná rozhraní a další relevantní komponenty Služby jsou pravidelně testovány na známé zranitelnosti. Zjištěné zranitelnosti jsou vyhodnocovány a řešeny v souladu s interním procesem řízení zranitelností a změnového řízení.

Systémy ACAeID a související technologické komponenty jsou provozovány v chráněném datovém centru s řízeným fyzickým přístupem. Přístup k technologiím mají pouze určené a oprávněné osoby v souladu s pravidly fyzické bezpečnosti, řízení přístupů a bezpečnostních a provozních rolí.

6.2.2 Hodnocení počítačové bezpečnosti

Hodnocení počítačové bezpečnosti systému pro poskytování Služby vychází z požadavků právních předpisů, technických norem a veřejně dostupných specifikací vztahujících se k poskytování kvalifikovaných služeb vytvářejících důvěru, vzdálenému vytváření kvalifikovaných elektronických podpisů, správě kvalifikovaných prostředků na dálku a řízení bezpečnosti informací.

Soulad s těmito požadavky je ověřován v rámci interních přezkumů, bezpečnostních kontrol a auditů, včetně posouzení shody prováděného subjektem posuzování shody.

Pro hodnocení počítačové bezpečnosti jsou relevantní zejména následující normy, specifikace a předpisy:

- **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 27002** – Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací;
- **ČSN ISO/IEC 27005** – Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací;
- **ČSN EN ISO 19011** – Směrnice pro auditování systémů managementu;
- **ETSI EN 319 401 V3.1.1** – *Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers*;

- **ETSI TS 119 431-1 V1.3.1** – *Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev*;
- **ETSI TS 119 461** – *Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects*;
- **Prováděcí nařízení Komise (EU) 2025/1567**, kterým se stanoví prováděcí pravidla k nařízení (EU) č. 910/2014, pokud jde o správu kvalifikovaných prostředků pro vytváření elektronických podpisů na dálku a kvalifikovaných prostředků pro vytváření elektronických pečetí na dálku jako služeb vytvářejících důvěru.

Požadavky uvedených norem a předpisů jsou naplňovány prostřednictvím technických, organizačních a provozních opatření popsaných v této politice, v souvisejících certifikačních politikách, certifikační prováděcí směrnici, interních bezpečnostních politikách a provozní dokumentaci eIdentity.

6.3 Technické řízení životního cyklu

6.3.1 Řízení vývoje systému pro poskytování služby

Vývoj, úpravy a údržba systému pro poskytování Služby probíhají podle interních pravidel zabezpečeného vývoje, řízení změn a provozního nasazování. Tato pravidla stanovují požadavky na návrh, implementaci, testování, schvalování a nasazování změn do produkčního prostředí.

Změny systému, které mohou mít dopad na bezpečnost, dostupnost, integritu nebo důvěryhodnost Služby, podléhají řízenému procesu posouzení, schválení, testování a dokumentace. Před nasazením do produkčního prostředí se ověřuje zejména funkčnost změny, její bezpečnostní dopad, dopad na poskytování Služby a soulad s touto politikou, souvisejícími certifikačními politikami a interní bezpečnostní dokumentací eIdentity.

Produkční prostředí Služby je odděleno od vývojového a testovacího prostředí. Nasazení změn do produkčního prostředí provádějí pouze oprávněné osoby v souladu s pravidly pro bezpečnostní a provozní role, řízení přístupů a změnové řízení.

6.3.2 Řízení správy bezpečnosti

Systém ACAeID a komponenty služby vzdáleného podpisu obsahují technické a organizační mechanismy pro ověřování integrity, řízení konfigurací, sledování bezpečnostních událostí a kontrolu provozního stavu Služby.

Integrita aplikací a vybraných systémových komponent je ověřována pomocí kontrolních mechanismů, zejména kryptografických otisků, kontrol konfigurací nebo jiných prostředků umožňujících zjistit neoprávněnou změnu. Výstupy kontrol integrity jsou pravidelně vyhodnocovány oprávněnými osobami.

Konfigurace systémů a bezpečnostních prvků je spravována řízeným způsobem. Změny konfigurací jsou evidovány a prováděny pouze oprávněnými osobami. V případě zjištění neočekávané změny, odchylky nebo podezření na neoprávněný zásah je událost posouzena a řešena podle interních pravidel pro řízení bezpečnostních událostí a incidentů.

Systémová a aplikační bezpečnost je dále podporována logováním, monitoringem, řízením zranitelností, řízením privilegovaných přístupů a pravidelným přezkumem relevantních bezpečnostních opatření.

6.3.3 Řízení životního cyklu bezpečnosti

Řízení bezpečnosti Služby probíhá v uzavřeném a opakovaném cyklu, který zahrnuje zejména:

- analýzu požadavků a bezpečnostních potřeb Služby;
- návrh a posouzení bezpečnostní architektury;
- implementaci technických a organizačních opatření;
- testování a ověření funkčnosti a bezpečnosti;
- schválení změn před jejich nasazením;
- provoz a průběžné sledování bezpečnostního stavu;
- vyhodnocování provozních a bezpečnostních událostí;
- řízení zranitelností a nápravných opatření;
- pravidelné přezkumy, audity a aktualizace bezpečnostní dokumentace;
- školení osob podílejících se na provozu a správě Služby.

Bezpečnostní opatření jsou v průběhu životního cyklu Služby pravidelně přezkoumávána s ohledem na změny právních a regulatorních požadavků, změny technologií, výsledky auditů, zjištěné zranitelnosti, bezpečnostní incidenty a změny v architektuře nebo provozu Služby.

V případě ukončení, nahrazení nebo významné změny komponenty Služby se postupuje řízeným způsobem tak, aby bylo zajištěno bezpečné ukončení jejího používání, ochrana uchovávaných záznamů, zachování auditní stopy a minimalizace dopadů na důvěrnost, integritu, dostupnost a důvěryhodnost Služby.

6.4 Řízení bezpečnosti sítě

Síťová bezpečnost systémů ACAeID a souvisejících komponent Služby je zajišťována vícevrstvým modelem ochrany, který zahrnuje zejména oddělení veřejně dostupných rozhraní od interních systémů, řízení síťového provozu, filtrování komunikace a omezení přístupů pouze na nezbytná komunikační rozhraní.

Systémy ACAeID a komponenty Služby jsou od veřejného internetového provozu odděleny bezpečnostními síťovými prvky, zejména firewally a dalšími mechanismy pro řízení, kontrolu a monitorování síťové komunikace. Prostupný provoz je povolen pouze v rozsahu nezbytném pro poskytování Služby, její správu a bezpečný provoz.

Přístup k interním systémům, administrátorským rozhraním a provozním komponentám Služby je omezen na oprávněné osoby a vyhrazené komunikační cesty. Administrátorské a provozní přístupy jsou řízeny v souladu s pravidly řízení přístupů, bezpečnostních a provozních rolí a interní bezpečnostní dokumentací eIdentity.

Komunikace se spoléhajícími se stranami, Bank iD a dalšími relevantními systémy probíhá prostřednictvím zabezpečených komunikačních kanálů. Bezpečnost síťové komunikace je podporována monitorováním, logováním, pravidelným vyhodnocováním bezpečnostních událostí a řízením zranitelností.

Změny síťové konfigurace, bezpečnostních pravidel a komunikačních rozhraní jsou prováděny řízeným způsobem v souladu s procesem změnového řízení. Změny, které mohou mít dopad na bezpečnost nebo dostupnost Služby, podléhají posouzení dopadu a schválení oprávněnými osobami.

6.5 Ochrana proti padělání a odcizení dat

Ochrana proti padělání, neoprávněné změně, odcizení nebo neoprávněnému zpřístupnění dat je zajišťována kombinací technických, organizačních a provozních opatření. Cílem těchto opatření je chránit zejména údaje potřebné pro vydání kvalifikovaného certifikátu,

údaje související s autentizací a souhlasem podepisující osoby, data pro vytváření elektronického podpisu, podepisované dokumenty, vytvořené podpisy, auditní záznamy a další informace zpracovávané v rámci Služby.

Data jsou chráněna zejména prostřednictvím řízení přístupových oprávnění, oddělení rolí, šifrované komunikace, logování bezpečnostně relevantních činností, monitorování provozu, kontroly integrity, zálohování a archivace záznamů. Přístup k datům je umožněn pouze oprávněným osobám a systémovým komponentám v rozsahu nezbytném pro poskytování Služby a plnění jejich rolí.

Data pro vytváření elektronických podpisů jsou vytvářena a používána v prostředí QSCD. Jejich použití je vázáno na konkrétní podpisovou transakci a souhlas podepisující osoby. Po dokončení podpisové transakce je životní cyklus podpisového klíče ukončen v souladu s touto politikou, příslušnou certifikační politikou a provozní dokumentací.

Integrita aplikací, konfigurací, auditních záznamů a vybraných archivovaných dat je chráněna kontrolními mechanismy, zejména kryptografickými otisky, elektronickými podpisy, elektronickými pečetěmi, časovými údaji nebo jinými odpovídajícími prostředky. Zjištěné odchylky nebo podezření na neoprávněnou změnu dat jsou posuzovány jako bezpečnostní událost nebo incident a řešeny podle interních pravidel řízení incidentů.

Zaměstnanci a další osoby podílející se na poskytování, správě nebo bezpečnosti Služby jsou seznámeni s bezpečnostními postupy, povinnostmi ochrany informací a pravidly pro nakládání s daty. Oprávnění k provádění bezpečnostně významných činností jsou přidělována pouze určeným osobám v souladu s jejich rolí, odpovědností a principem nezbytné potřeby.

---

7 Hodnocení shody a jiná hodnocení

7.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Soulad Služby s touto politikou, souvisejícími certifikačními politikami, certifikační prováděcí směrnicí, interní bezpečnostní dokumentací a použitelnými právními, regulatorními a normativními požadavky je pravidelně ověřován.

Hodnocení se provádí zejména:

- nejméně jednou ročně v rámci interního přezkumu nebo interního auditu;

- v rámci pravidelného posouzení shody kvalifikované služby prováděného subjektem posuzování shody;
- při významné změně architektury, konfigurace, provozního modelu nebo bezpečnostních opatření Služby;
- po významném bezpečnostním incidentu nebo události, která může mít dopad na důvěryhodnost Služby;
- při změně právních, regulatorních nebo normativních požadavků, pokud taková změna může mít dopad na poskytování Služby.

Konfigurační změny běžného provozního charakteru jsou posuzovány v rámci změnového řízení. Změny, které mohou mít dopad na bezpečnost, důvěryhodnost nebo soulad Služby, podléhají přiměřenému bezpečnostnímu posouzení a podle povahy změny také mimořádnému hodnocení.

7.2 Identita a kvalifikace hodnotitele

Hodnocení shody kvalifikované služby provádí způsobilý subjekt posuzování shody, který splňuje požadavky právních předpisů a příslušných akreditačních pravidel pro posuzování služeb vytvářejících důvěru.

Interní audity a interní bezpečnostní hodnocení provádějí osoby s odpovídající kvalifikací, znalostí systému řízení bezpečnosti informací, požadavků eIDAS, příslušných ETSI norem a interní bezpečnostní dokumentace eIdentity.

Hodnotitel musí mít odpovídající odbornou způsobilost, znalost použitelných požadavků a oprávnění k provedení hodnocení v rozsahu daného typu hodnocení.

7.3 Vztah hodnotitele k hodnocenému subjektu

Hodnotitel musí být nezávislý na činnostech, které jsou předmětem hodnocení, a nesmí být v postavení, které by mohlo ohrozit objektivitu nebo nestrannost hodnocení.

Osoba provádějící interní audit nebo interní bezpečnostní hodnocení nesmí hodnotit činnost, za jejíž návrh, implementaci nebo provoz je přímo odpovědná. V případě externího posouzení shody musí být zachována nezávislost a nestrannost subjektu posuzování shody podle příslušných akreditačních pravidel.

7.4 Hodnocené oblasti

Rozsah hodnocení je určen povahou Služby, použitou metodikou hodnocení, požadavky právních předpisů, ETSI norem, certifikačních politik a interní dokumentace eIdentity.

Hodnocení se zaměřuje zejména na:

- soulad Služby s touto politikou a souvisejícími politikami;
- ověření identity a autentizaci podepisující osoby;
- proces vydání krátkodobého kvalifikovaného certifikátu;
- proces vytvoření kvalifikovaného elektronického podpisu;
- řízení podpisových klíčů a jejich životního cyklu v QSCD;
- ochranu dat pro vytváření elektronických podpisů;
- bezpečnost technických komponent služby;
- řízení přístupů a důvěryhodných rolí;
- auditní záznamy, logování a uchovávání záznamů;
- řízení změn a technický životní cyklus služby;
- řízení zranitelností a bezpečnostních incidentů;
- fyzickou, provozní a síťovou bezpečnost;
- smluvní a právní požadavky vztahující se ke Službě;
- plnění relevantních požadavků ETSI TS 119 431-1, ETSI EN 319 401 a dalších použitelných norem.

7.5 Postup v případě zjištění nedostatků

Zjištěné nedostatky, neshody nebo doporučení jsou evidovány, klasifikovány podle závažnosti a předány odpovědným osobám k řešení. Pro každý relevantní nedostatek se stanoví nápravné opatření, odpovědná osoba a termín splnění.

Nápravná opatření mohou zahrnovat zejména:

- úpravu bezpečnostní nebo provozní dokumentace;
- změnu technického, konfiguračního nebo procesního nastavení;
- doplnění nebo úpravu bezpečnostních opatření;
- doplnění auditních nebo provozních důkazů;
- proškolení odpovědných osob;
- opakované ověření účinnosti přijatého opatření.

Realizace nápravných opatření je sledována do jejich vypořádání. Účinnost přijatých opatření je ověřována přiměřeně povaze a závažnosti zjištění.

7.6 Sdělování výsledků hodnocení

Výsledky hodnocení jsou zpřístupněny osobám odpovědným za řízení a bezpečnost Služby, zejména statutárnímu zástupci, bezpečnostnímu řediteli, provoznímu řediteli a dalším určeným osobám podle povahy zjištění.

Výsledky posouzení shody jsou uchovávány jako součást řízené dokumentace eIdentity a jsou poskytovány příslušným orgánům, auditorům nebo subjektu posuzování shody v rozsahu stanoveném právními předpisy, smluvními závazky nebo pravidly posuzování shody.

Informace o zjištěních, která mohou mít dopad na důvěryhodnost, bezpečnost nebo kontinuitu Služby, jsou eskalovány odpovědným osobám bez zbytečného odkladu.

---

8 Ostatní obchodní a právní záležitosti

8.1 Poplatky

8.1.1 Poplatky za využívání služby

Účtování poplatků je stanoveno smlouvou s konkrétní spoléhající se stranou nebo smluvním partnerem. Forma účtování může zahrnovat zejména paušální poplatek za určité časové období nebo poplatek za úspěšně vytvořený podpis.

8.1.2 Poplatky za další služby

Není relevantní pro tento dokument, pokud není ve smluvních podmínkách stanoveno jinak.

8.1.3 Postup při refundování

Není relevantní pro tento dokument, pokud není ve smluvních podmínkách stanoveno jinak.

8.2 Finanční odpovědnost

8.2.1 Krytí pojištěním

eIdentity má sjednáno pojištění podnikatelských rizik v rozsahu přiměřeném povaze poskytovaných služeb vytvářejících důvěru.

8.2.2 Další aktiva

eIdentity zajišťuje zdroje potřebné pro poskytování služeb vytvářejících důvěru na požadované úrovni kvality, bezpečnosti a dostupnosti.

8.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Samostatné pojištění nebo krytí zárukou pro koncové uživatele se v rámci této politiky neposkytuje, pokud není ve smluvních podmínkách stanoveno jinak.

8.3 Důvěrnost obchodních informací

8.3.1 Rozsah důvěrných informací

Za neveřejné obchodní informace se považují zejména informace o odebíraných službách, jejich cenách, obchodních smlouvách, smlouvách s třetími stranami podílejícími se na provozu nebo zajištění Služby, žádostech o poskytnutí služby, auditních a transakčních záznamech, havarijních plánech a plánech obnovy, certifikační prováděcí směrnici, způsobech ochrany osobních údajů, zabezpečení obsluhy systému ACAeID, bezpečnostních opatřeních a jejich realizaci.

8.3.2 Informace mimo rámec důvěrných informací

Za informace mimo rámec důvěrných informací se považují informace, které byly eIdentity zveřejněny prostřednictvím webových stránek nebo jiným určeným způsobem.

8.3.3 Odpovědnost za ochranu důvěrných informací

Každá osoba, která přijde do styku s důvěrnými informacemi, je povinna chránit je před neoprávněným zpřístupněním, změnou, ztrátou nebo zneužitím. Poskytnutí důvěrných informací třetí straně je možné pouze na základě oprávnění, právního požadavku, smluvního ujednání nebo souhlasu odpovědné osoby eIdentity.

8.4 Ochrana osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 (GDPR), zákonem č. 110/2019 Sb., o zpracování osobních údajů, a souvisejícími právními předpisy.

8.4.1 Politika ochrany osobních údajů

Za řízení ochrany osobních údajů ve společnosti eIdentity odpovídá určená odpovědná osoba nebo pověřenec pro ochranu osobních údajů, pokud je jmenován. Podrobnosti jsou stanoveny v interní dokumentaci ochrany osobních údajů a ve veřejně dostupných informacích o zpracování osobních údajů.

8.4.2 Informace považované za osobní údaje

Za osobní údaje se považují veškeré informace o identifikované nebo identifikovatelné fyzické osobě, zejména identifikační údaje, kontaktní údaje, údaje získané prostřednictvím Bank iD, údaje potřebné pro vydání certifikátu, údaje o podpisové transakci a další údaje zpracovávané v rámci poskytování Služby.

8.4.3 Informace nepovažované za osobní údaje

Za osobní údaje se nepovažují údaje, které se nevztahují k identifikované nebo identifikovatelné fyzické osobě, nebo údaje, které byly anonymizovány tak, že již nelze identifikovat konkrétní fyzickou osobu.

8.4.4 Odpovědnost za ochranu osobních údajů

eIdentity zajišťuje ochranu osobních údajů prostřednictvím technických a organizačních opatření odpovídajících povaze, rozsahu, kontextu a účelům zpracování a rizikům pro práva a svobody fyzických osob.

8.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Podepisující osoba je informována o zpracování osobních údajů v rozsahu stanoveném právními předpisy. Pokud je pro konkrétní zpracování vyžadován souhlas, je získáván před zahájením takového zpracování. V ostatních případech je zpracování založeno na jiném odpovídajícím právním titulu.

8.4.6 Poskytování osobních údajů pro soudní či správní účely

Osobní údaje mohou být zpřístupněny orgánům veřejné moci, soudům, správním orgánům nebo jiným oprávněným subjektům pouze v rozsahu a za podmínek stanovených právními předpisy.

8.4.7 Jiné okolnosti zpřístupňování osobních údajů

Osobní údaje mohou být zpřístupněny také v dalších případech stanovených právními předpisy, smluvními závazky nebo v rozsahu nezbytném pro poskytování Služby, ochranu práv eIdentity, řešení incidentů, reklamací nebo sporů.

8.4.8 Práva duševního vlastnictví

eIdentity zachovává veškerá práva k duševnímu vlastnictví týkající se obsahu certifikátů, revokačních dat, politik, dokumentace, interních postupů a dalších chráněných prvků souvisejících s poskytováním služeb vytvářejících důvěru.

8.5 Zastupování a záruky

8.5.1 Zastupování a záruky eIdentity

eIdentity zaručuje, že:

- kvalifikovaný elektronický podpis odpovídá dokumentu předloženému podepisující osobě v rámci Služby;
- data pro vytváření elektronického podpisu jsou použita pouze v souladu se Službou a nebyla použita pro jiný účel;
- Služba je provozována v souladu s touto politikou, příslušnou certifikační politikou a použitelnými právními a regulatorními požadavky.

Další záruky mohou být specifikovány ve smlouvě o poskytnutí služby nebo ve smluvních podmínkách.

8.5.2 Zastupování a záruky kontaktního místa

eIdentity zajišťuje, že průběh procesů v rámci Služby bude v souladu s touto politikou a související dokumentací. Pokud se na procesu podílí kontaktní místo nebo jiný partner, jeho odpovědnosti jsou vymezeny smluvně nebo v příslušné provozní dokumentaci.

8.5.3 Zastupování a záruky ostatních zúčastněných subjektů

Záruky ostatních zúčastněných subjektů se řídí příslušnými smlouvami, provozní dokumentací a právními předpisy.

8.6 Zřeknutí se záruk

Poskytování Služby se řídí zejména nařízením eIDAS, touto politikou, příslušnou certifikační politikou a smluvními podmínkami. eIdentity neposkytuje jiné záruky nad rámec stanovený právními předpisy nebo smluvními ujednáními.

8.7 Omezení odpovědnosti

Odpovědnost eIdentity je stanovena právními předpisy, zejména nařízením eIDAS, a příslušnými smluvními podmínkami. Omezení odpovědnosti nesmí být v rozporu s kogentními ustanoveními právních předpisů.

8.8 Záruky a odškodnění

Náhrada škody a případné odškodnění se řídí příslušnými právními předpisy a smluvními podmínkami. O výši náhrady škody může rozhodnout příslušný soud, pokud není věc vyřešena jiným právně přípustným způsobem.

8.8.1 Doba platnosti, ukončení platnosti

Tato politika zůstává v platnosti do jejího nahrazení novější verzí, zrušení nebo ukončení poskytování Služby.

8.8.2 Doba platnosti

Novou verzi politiky schvaluje a vyhlašuje Výbor pro politiky na základě svého jednacího řádu.

8.8.3 Ukončení platnosti

Ukončení platnosti této politiky nebo její nahrazení novou verzí se provádí řízeným procesem. Změny politiky včetně zajištění souladu s navazující dokumentací schvaluje Výbor pro politiky.

8.8.4 Důsledky ukončení a přetrvání závazků

Ukončením platnosti této politiky nejsou dotčeny povinnosti uchovávat záznamy, chránit důvěrné informace, chránit osobní údaje a plnit povinnosti vyplývající z právních předpisů, smluvních podmínek a auditních požadavků.

8.9 Individuální upozorňování a komunikace se zúčastněnými subjekty

8.9.1 Novelizace

Novelizace této politiky probíhá řízeným procesem. Změny jsou posuzovány z hlediska dopadu na Službu, soulad s právními a regulatorními požadavky a návaznost na související dokumentaci.

8.9.2 Postup při novelizaci

Návrh změny politiky je předložen k přezkumu a schválení Výboru pro politiky. Po schválení je nová verze politiky zveřejněna způsobem stanoveným touto politikou.

8.9.3 Postup a periodicita oznamování

Oznámení o změnách politiky se provádí přiměřeným způsobem podle povahy změny. Změny, které mají významný dopad na uživatele, spoléhající se strany nebo způsob poskytování Služby, jsou komunikovány bez zbytečného odkladu po jejich schválení.

8.9.4 Okolnosti, při kterých musí být změněn OID

OID politiky se mění v případě takové změny politiky, která má zásadní dopad na její účel, rozsah, pravidla poskytování Služby nebo na posuzování souladu. O změně OID rozhoduje Výbor pro politiky.

8.10 Ustanovení o řešení sporů

V případě nesouhlasu s postupem pracovníků eIdentity nebo s poskytováním Služby se může dotčená osoba obrátit na eIdentity prostřednictvím určených kontaktních údajů. Není-li spor vyřešen smírně, může být předložen příslušnému soudu podle právních předpisů České republiky.

8.11 Rozhodné právo

Činnost eIdentity a poskytování Služby se řídí právním řádem České republiky a přímo použitelnými právními předpisy Evropské unie.

8.12 Shoda s právními předpisy

Služba je provozována ve shodě s použitelnými právními a regulatorními požadavky vztahujícími se ke kvalifikovaným službám vytvářejícím důvěru, zejména s nařízením eIDAS a navazujícími předpisy, a je předmětem posuzování shody v rozsahu stanoveném právními předpisy.

8.12.1 Další ustanovení

Není použito.

8.12.2 Rámcová dohoda

Není použito, není-li ve smluvních podmínkách stanoveno jinak.

8.12.3 Postoupení práv

Postoupení práv se řídí smluvními podmínkami a právními předpisy.

8.12.4 Oddělitelnost ustanovení

Pokud se některé ustanovení této politiky stane neplatným nebo neúčinným, nemá tato skutečnost vliv na platnost a účinnost ostatních ustanovení, pokud z povahy věci nevyplývá jinak.

8.12.5 Vymáhání

Vymáhání práv a povinností se řídí příslušnými právními předpisy a smluvními podmínkami.

8.12.6 Vyšší moc

Smlouva o poskytnutí Služby může obsahovat ustanovení o působení vyšší moci. Události vyšší moci nemají vliv na povinnosti eIdentity přijmout přiměřená opatření k ochraně záznamů, bezpečnosti a kontinuity Služby v rozsahu, ve kterém je to možné.

8.13 Další opatření

Další opatření mohou být stanovena v souvisejících certifikačních politikách, certifikační prováděcí směrnici, interní bezpečnostní dokumentaci, smluvních podmínkách nebo auditní dokumentaci.

---

9 Závěrečná ustanovení

Tato politika byla projednána Výborem pro politiky a podle zápisu byla přijata a vyhlášena.

Politika nabývá účinnosti dnem stanoveným při jejím schválení a zůstává platná do jejího nahrazení novou verzí nebo do ukončení poskytování Služby.

Historie dokumentu

Verze 1.0

Datum: 25. 03. 2024
Autor: Jan Stelibský

Počáteční verze.

Verze 1.0.1

Datum: 07. 05. 2026
Autor: Libor Široký

Doplněna kapitola 6.1 Soulad s ETSI TS 119 431-1, celková revize textu.