**Příloha č. 1** – Systémová bezpečnostní politika

Kvalifikovaná certifikační autorita eIdentity

# ACAeID 17.1 Systémová bezpečnostní politika správy zařízení zákazníka

eIdentity a.s.

Vinohradská 184,130 00 Praha 3

Tel: 222 866 150-1

fax: 222 866 190

Email: info@eidentity.cz

Verze: 1.4

Odpovídá: XXXXXXXXXXX

Datum: 11. 7. 2023

Utajení: Pro interní potřebu eIdentity a.s. a pro zákazníka

Copyright 19 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 |  |
| 1.4 | Ing. Ladislav Šedivý |  |

Historie dokumentu:

|  |  |  |  |
| --- | --- | --- | --- |
| Verze | Datum | Autor | Poznámka |
| 1.0 | 26.06.2019 | XXXXXXXXXXXXXXXXX | Nový dokument |
| 1.1 | 18.10.2019 | XXXXXXXXXXXXXXXXX | Upřesnění práv a povinností |
| 1.2 | 05.11.2019  17.11.2019 | XXXXXXXXXXXXXXXXX | Doplnění dokumentace výrobce a norem |
| 1.2 | 20.11.2019 | XXXXXXXXXXXXXXXXX | Úprava použitého systému |
| 1.2 | 09.07.2020 | XXXXXXXXXXXXXXXXX | Vynesení HW do Přílohy č.1 |
| 1.3 | 30.11.2021 | XXXXXXXXXXXX | Zobecnění dokumentu |
| 1.4 | 11.7.2023 | XXXXXXXXXXXX | Rozšíření pro další zákazníky |

Obsah

[ACAeID 17.1 Systémová bezpečnostní politika správy zařízení zákazníka - 1 -](#_Toc89153570)

[1. Úvod - 4 -](#_Toc89153571)

[2. Cíle systémové bezpečnostní politiky - 4 -](#_Toc89153572)

[3. Platnost dokumentu - 4 -](#_Toc89153573)

[4. Bezpečnostní systémová politika - 5 -](#_Toc89153574)

[A. Přehled použitých pojmů a zkratek - 5 -](#_Toc89153575)

[B. Správa uživatelů - 5 -](#_Toc89153576)

[C. Podepisování - 5 -](#_Toc89153577)

[D. Použité technologie - 6 -](#_Toc89153578)

[E. Požadavky na auditní záznamy - 6 -](#_Toc89153579)

[F. Smluvní požadavky - 7 -](#_Toc89153580)

[G. Splnění požadavků výrobce HSM a relevantních norem - 7 -](#_Toc89153581)

[5. Represe - 8 -](#_Toc89153582)

[Literatura - 8 -](#_Toc89153583)

[Příloha č. 1 – Seznam podporovaného HW u zákazníka - 9 -](#_Toc89153584)

# Úvod

Společnost eIdentity a.s. poskytuje službu správy zařízení zákazníka pro elektronické pečetě a elektronické podpisy. Tato služba umožňuje uchování privátních klíčů v bezpečném HW a ověření oprávněného přístupu uživatelů k těmto klíčům a to tak, aby oprávněný uživatel měl pod výhradní kontrolou svůj privátní klíč.

# Cíle systémové bezpečnostní politiky

Cílem této systémové bezpečnostní politiky je definovat standardy pro instalaci a správu zařízení zákazníka tak, aby bylo zaručeno podepisování a pečetění u zákazníka jeho zaměstnanci v souladu s Nařízením Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Systémová bezpečnostní politika je podřízena Celkové bezpečnostní politice ACAeID 23 a odpovídající Certifikační politice CP 10.1 až CP 10.6, řeší pouze ty aspekty, které ve výše uvedených politikách nejsou uvedeny.

# Platnost dokumentu

Tento dokument se týká všech osob, které odpovídají nějakým způsobem za smluvní vztahy mezi zákazníkem a eIdentity a.s., dále všech osob, které se podílejí na správě daných zařízení, a to jak ze strany dodavatele (eIdentity a.s.), tak zákazníka.

# Bezpečnostní systémová politika

## Přehled použitých pojmů a zkratek

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

ACAeID, ACA Informační systém eIdentity a.s., poskytující kvalifikované certifikační služby

HSM Hardware Security Module – Hardwarový bezpečnostní modul

OTP One Time Password – jednorázový klíč

Time Stamp Časové razítko

QSCD Kvalifikovaný prostředek pro vytváření elektronických podpisů/pečetí

SIEM Správa bezpečnostních informací a událostí

## Správa uživatelů

* + Aplikační server pod správou eIdentity a.s. přebírá uživatele ze správy uživatelů zákazníka, drží vztah uživatel – klíčové hospodářství HSM
  + Právo uživatele používat řešení HSM je založeno na členství ve skupině v správě uživatelů zákazníka
  + Rozhraní pro uživatele
    - Prvotní zavedení (nastavení OTP nebo certifikátu uživatele, vytvoření přístupu ke klíčovému hospodářství HSM)
    - Změna hesla ke klíčovému hospodářství HSM
    - Generování klíčů a vytváření žádosti o certifikát
    - Import certifikátu a spárování s klíčem
    - Smazání klíče a souvisejícího certifikátu
  + Rozhraní pro správce
    - Mazání klíčů
    - Mazání uživatelů
    - Zrušení OTP nebo certifikátu uživatele
  + Kontrola oprávněnosti přístupu uživatelů
  + Správa privilegovaných uživatelů (správců)

## Podepisování/pečetění

* + Ověření identity na základě vzájemné autentizace mezi serverem a uživatelem
  + Vrácení seznamu klíčů pro uživatele zastoupeného identitou ze správy uživatelů zákazníka (pro libovolnou autentizovanou komponentu)
  + Zobrazení rozhraní pro zadání OTP nebo certifikátu uživatele a přístupové fráze
  + Ověření zadaného OTP nebo certifikátu uživatele
  + Komunikace s HSM (podpis)
  + Komunikace s API (informace o potřebě připojení TimeStamp, vrácení výsledků)

Dále mimo vlastní strukturu HSM stojí komponenta, která přijímá požadavky na vytváření podpisů/pečetí od aplikací, komunikuje s vlastním API a HSM a předává podepsané dokumenty zpět uživatelům.

Všechny komponenty HSM odesílají logy na syslog server, jsou zapojeny do systému dohledu a zálohování (vše součástí řešení komponenty HSM). Sběr logů organizuje, dohled a vyhodnocování logů provádí eIdentity a.s.

## Použité technologie

Servery běží pod aktuální verzí systému, který je specifikován v dokumentaci výrobce. Aktualizace a nastavení serverů, které mají vztah k práci HSM serveru, provádí eIdentity a.s. podle požadavků ČSN ISO/IEC 27 001, případně zákonu o kybernetické bezpečnosti a odpovídajícím Vyhláškám (především vyhlášce č.82/2018 Sb.), pokud systémy spadají do oblasti KII nebo VIS.

Autentizace uživatele je řešena pomocí certifikátů nebo více faktorové autentizace s podporou standardu RFC 6238.

HSM server bude obsahovat QSCD zařízení v podobě karty, která bude zajišťovat správu klíčů pro kvalifikovaný elektronický podpis a nástroje pro kvalifikovanou elektronickou pečeť.

Součástí komponenty HSM bude vlastní syslog server, který bude zpřístupňovat data správě eIdentity a.s.

## Požadavky na auditní záznamy

V oblasti vytváření auditních záznamů jsou (při zohlednění specifických vlastností konkrétních modulů a komponent) implementovaná následující bezpečnostní opatření:

* Systém vytváří bezpečnostně relevantní auditní záznamy o prováděných aktivitách.
* Systém vytváří záznamy o následujících událostech:
* změny bezpečnostně relevantního nastavení (nastavení bezpečnostní funkcionality včetně nastavení vytváření auditních záznamů),
* přístupy k dokumentům,
* operace s jednotlivými dokumenty včetně metadat,
* předávání dokumentů mezi úložišti,
* přihlášení a odhlášení uživatelů a administrátorů,
* použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení,
* činnosti provedené administrátory,
* činnosti vedoucí ke změně přístupových oprávnění,
* neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů (neúspěšné pokusy o přístup),
* zahájení a ukončení činností technických aktiv (HW, SW, síťová infrastruktura,
* automatická varovná nebo chybová hlášení technických aktiv,
* přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech,
* operace provádějící operace transakce s daty, a to zejména citlivými, hromadnými, a to jak na základě interakce uživatele, tak na základě systémových událostí (např. nastalý čas).
* Vytvářené záznamy obsahují:
* informace o čase vzniku události,
* identitu koncového uživatele a
* informace o události (změně).
* Bezpečnostně relevantní auditní záznamy systém:
* ukládá v systému po dobu 30 dní a
* předává protokolem syslog, resp. ve formátu textových logů, do centrálního úložiště logů, resp. SIEM nebo přímo eIdentity a.s

Kromě vytváření a předávání bezpečnostně relevantních auditních záznamů vytváří každá komponenta lokální transakční log, který je předáván do centrálního zpracování.

## Smluvní požadavky

Tato systémová bezpečnostní politika je přílohou smlouvy mezi eIdentity a.s. a zákazníkem.

## Splnění požadavků výrobce HSM a relevantních norem

Všechny systémy užité v infrastruktuře zákazníka musí splňovat požadavky výrobce, které jsou uvedeny v dokumentaci k HW uvedenému v příloze č. 1. Podporovaný HW je uveden v příloze č. 1.

Řízení informační bezpečnosti při správě HSM eIdentity a.s. odpovídá ČSN ISO/IEC 27 001 [2].

**Organizační bezpečnost**

V rámci řešení projektu a provozu musí být sestavena pracovní Bezpečnostní skupina ze zástupců eIdentity a.s. a zákazníka. Tato skupina musí pokrývat všechny bezpečnostní požadavky a funkce vyžadované odpovídajícími ISO normami a dokumentací dodavatele HSM modulu. Struktura skupiny musí být součástí smlouvy včetně náplně jednotlivých funkcí.

**Bezpečnost lidských zdrojů**

Pracovníci eIdentity a.s. a zákazníka, kteří se podílejí na provozu systému, musí být prověřeni a vybráni dle požadavků Bezpečnostní skupiny. Pracovníci zákazníka odpovídají za provoz klientských systémů, AD, interní sítě zákazníka. Pracovníci eIdentity a.s. pak za provoz podpisového/pečetícího serveru.

**Fyzická bezpečnost a bezpečnost prostředí**

Umístění podpisového/pečetícího serveru, sítě a stanic zákazníka musí odpovídat požadavkům odpovídajících norem, včetně ochrany proti malware a včasného řešení zranitelností. Mimo jiné musí být řešena otázka přístupu správců k jednotlivým zařízením v infrastruktuře zákazníka.

Aktualizace OS a SW podpisového/pečetícího serveru zajišťuje eIdentity a.s.

**Bezpečnost komunikace a provozu**

Komunikace mezi stanicemi zákazníka a podpisovým/pečetícím serverem musí probíhat bezpečnými protokoly. Za autentizaci uživatelů odpovídá zákazník, který spravuje své systémy AD, co se týká autentizace a autorizace. Neoprávněný přístup nějakého uživatele s parametry jiného uživatele je odpovědnost zákazníka.

eIdentity a.s. je povinna doložit protokol o přístupu jednotlivých uživatelů k podpisovému/pečetícímu serveru ve formě LOGu s parametry KDO, KDY, ODKUD.

**Řízení přístupu**

Za řízení přístupu odpovídá zákazník a všechny bezpečnostní incidenty v tomto směru řeší on.

**Aspekty řízení kontinuity, Havarijní plánování a plánování obnovy po havárii**

Za řízení kontinuity podpisového/pečetícího serveru odpovídá eIdentity a.s. Řízení kontinuity z hlediska stanic a dokumentů je záležitost zákazníka.

Každá strana musí mít vypracovanou dokumentaci k jednotlivým oblastem a musí ji na vyžádání poskytnout smluvní straně.Zpracování chybějící dokumentace řídí pracovní Bezpečnostní skupina. Je také žádoucí poskytovat výsledky auditů, které se týkají společného projektu.

Všechny tyto požadavky je možné ověřit buď certifikačním auditem zákazníka nebo auditem, kontrolujícím jednotlivé požadavky. eIdentity a.s. tyto podmínky splňuje, což je možné doložit certifikáty jak ISO norem, tak souladu s nařízením eIDAS.

# Represe

Porušení této bezpečnostní politiky zaměstnancem se považuje za hrubé porušení pracovní kázně a má za následek disciplinární řízení, jehož výsledkem může být až rozvázání pracovního poměru se zaměstnancem z důvodu hrubého porušení pracovní kázně. Porušení politiky smluvním partnerem je ošetřeno smlouvou.

# Literatura

[1] ČSN ISO/IEC 15 408 Common Criteria

[2] ČSN ISO/IEC 27 001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací

# Příloha č. 1 – Seznam podporovaného HW u zákazníka

nShield HSM family Public Security Target.

Thales Luna K7 Cryptographic module