VOJENSKÝ ÚTVAR 9066
TRENČÍN
Č. p.: 6.spojp-EL 7/11-1-87/2025

Trenčín, 13. marec 2025
Výtlačok jediný.
Počet listov: 9

Schvaľujem:

Vyhlásenie o zverejnení PKI (PKI Disclosure Statement)

Spracovateľ: Centrum IB / Úsek PKIaCA

Verzia: 1.0

Dátum platnosti: 17. APR. 2025

Verejné údaje – IS CAMOSR

Olbrachtova 5, 911 01 TRENČÍN
tel.: +421 960 40 79 89
e-mail: pki@mil.sk
web: http://pki.mil.sk

Ochranné známky

Mená produktov uvádzané v tomto dokumente môžu byť registrované ochranné známky príslušných firiem.

História zmien

Verzia	Dátum	Opis revízie
1.0.	13.03.2025	Prvá verzia dokumentu

Obsah

ZOZNAM OBRÁZKOV A TABULIEK

Obrázky

Tento dokument neobsahuje obrázky

Tabuľky

SKRATKY A POJMY

Skratky

CA	–	Certifikačná autorita (Certification Authority)
MOSR	–	Ministerstvo obrany Slovenskej republiky
CP	–	Certifikačný poriadok (Certificate Policy)
CPS	–	Pravidlá na výkon certifikačných činností (Certificate Practice Statement)
CRL	–	Zoznam zrušených certifikátov (Certificate Revocation List)
HSM	–	Bezpečné zariadenie na vyhotovenie elektronického podpisu; kryptografický modul, hardvérový bezpečnostný modul (Hardware Security Modul)
PMA	–	Autorita pre správu CP (Policy Management Authority)
NBÚ	–	Národný bezpečnostný úrad
KC	–	Kvalifikovaný certifikát pre elektronický podpis
KCPe	-	Kvalifikovaný certifikát pre elektronickú pečať
RA	–	Registračná autorita (Registration Authority)
LRA	–	Lokálna RA – je RA konajúca v mene CAMOSR, pôsobiaca v teritóriu Regionálneho centra KIS, v ktorého pôsobnosti je zriadená.
PKI	–	Infraštruktúra verejných kľúčov (Public Key Infrastructure)
CAMOSR	–	Certifikačná autorita, poskytovateľ dôveryhodných služieb Ministerstva obrany Slovenskej republiky
TSA	–	Time Stamp Authority (autorita časovej pečiatky)
QSCD	–	Kvalifikované zariadenie na vyhotovenie elektronického podpisu

Pojmy

Dôveryhodná služba - elektronická služba, ktorá sa spravidla poskytuje za odplatu a spočíva:

a) vo vyhotovovaní, overovaní a validácii elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, alebo

b) vo vyhotovovaní, overovaní a validácii certifikátov pre autentifikáciu webových sídel, alebo

c) v uchovávaní elektronických podpisov, pečatí alebo certifikátov, ktoré s týmito službami súvisia.

Kvalifikovaný poskytovateľ dôveryhodných služieb - poskytovateľ dôveryhodných služieb, ktorý poskytuje kvalifikované dôveryhodné služby podľa zákona č. 272/2016 Z. z. o dôveryhodných službách, a ktorá má na poskytovanie týchto služieb kvalifikáciu Národného bezpečnostného úradu (ďalej len NBÚ).

Certifikát pre elektronický podpis – je elektronické osvedčenie, ktoré spája údaje na validáciu elektronického podpisu s fyzickou osobou a potvrdzuje aspoň jej meno alebo pseudonym.

Certifikát pre elektronickú pečať - je elektronické osvedčenie, ktoré spája údaje na validáciu elektronického podpisu s právnickou osobou a potvrdzuje jej názov.

Poskytovateľ dôveryhodných služieb – poskytovateľ dôveryhodných služieb, ktorý vykonáva dôveryhodné služby spojené s vydávaním, archivovaním, rušením platnosti certifikátov, overovaním ich platnosti a pod.

Držiteľ – entita identifikovaná v certifikáte ako držiteľ súkromného kľúča prislúchajúceho k verejnému kľúču obsiahnutému v certifikáte.

Elektronická pečať - sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme s cieľom zabezpečiť pôvod a integritu týchto pridružených údajov.

Elektronický podpis – informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá obsahuje údaj umožňujúci identifikáciu podpisovateľa.

Hashovacia funkcia (hash, message digest, fingerprint) – rýchlo spočítateľná funkcia, ktorá dostane na vstupe dokument ľubovoľnej dĺžky a zostrojí z neho pomerne krátku (napr. 160 bitov) charakteristiku, nazývanú hashovacia hodnota (tiež hašovacia hodnota, hash).

Kvalifikovaný certifikát pre elektronickú pečať - je certifikát pre elektronickú pečať:
a) ktorý vydal kvalifikovaný poskytovateľ dôveryhodných služieb pre elektronický podpis,
b) ktorý spĺňa požiadavky Prílohy číslo III Nariadenia (EÚ) 910/2014

Kvalifikovaný certifikát pre elektronický podpis - je certifikát elektronický podpis:
a) ktorý vydal kvalifikovaný poskytovateľ dôveryhodných služieb pre elektronický podpis,
b) ktorý spĺňa požiadavky Prílohy číslo I Nariadenia (EÚ) 910/2014.

Kvalifikovaný elektronický podpis – je zdokonalený elektronický podpis vyhotovený s použitím zariadenia na vyhotovenie kvalifikovaného elektronického podpisu a založený na kvalifikovanom certifikáte pre elektronické podpisy.

Mandátny certifikát - je kvalifikovaný certifikát vydaný fyzickej osobe, oprávnenej zo zákona alebo na základe zákona konať za inú osobu alebo orgán verejnej moci alebo v ich mene, alebo osobe, ktorá vykonáva činnosť podľa osobitného predpisu alebo vykonáva funkciu podľa osobitného predpisu a obsahuje údaje uvedené v § 8 písm. a) až c) zákona č. 272/2016 Z. z.

Podpisová politika – je súbor pravidiel, ktoré vyjadrujú použiteľnosť certifikátu a/alebo triedy aplikácií so spoločnými bezpečnostnými požiadavkami.

Používateľ certifikátu – entita, ktorá koná na báze dôvery v daný certifikát a/alebo na základe elektronického podpisu overeného daným certifikátom. Synonymom pojmu používateľ certifikátu je pojem strana spoliehajúca sa na certifikát.

Pravidlá na výkon certifikačných činností – postupy, ktoré certifikačná autorita uplatňuje pri vydávaní certifikátov.

Kvalifikované zariadenie na vyhotovenie elektronického podpisu (QSCD) - zariadenie na vyhotovenie elektronického podpisu, ktoré spĺňa požiadavky stanovené v prílohe II Nariadenia eIDAS.

Subjekt – entita identifikovaná v certifikáte ako držiteľ súkromného kľúča prislúchajúceho k verejnému kľúču obsiahnutému v certifikáte.

Vlastná CA – časť infraštruktúry poskytovateľa dôveryhodných služieb (obsahujúca napr. HSM modul), ktorá spolu s poskytovateľom vydáva certifikáty.

Zdokonalený elektronický podpis – je elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26 Nariadenia (EÚ) 910/2014.

Žiadateľ o certifikát – entita, ktorá certifikačnej autorite predkladá žiadosť v mene jedného alebo viacerých subjektov.

X.509 - medzinárodný štandard, ktorý okrem iného definuje aj formát certifikátu verejného kľúča.

1 ÚVOD

Vyhlásenie o zverejnení PKI (Public Key Infrastructure Disclosure Statement) slúži na informovanie používateľov o politike a postupoch poskytovateľa dôveryhodných služieb pri správe infraštruktúry verejných kľúčov (PKI). Tento dokument, vytvorený v súlade s normou ETSI EN 319 411-1, poskytuje prehľad o zásadách bezpečnosti, zodpovednostiach strán a súlade s právnymi požiadavkami.

Cieľom vyhlásenia je zabezpečiť transparentnosť procesov PKI, čím sa posilňuje dôvera používateľov v elektronické transakcie a komunikáciu. Umožňuje lepšie pochopiť, ako poskytovateľ certifikačných služieb chráni integritu a dôvernosť digitálnych certifikátov, ktoré sú kľúčové pre ochranu citlivých informácií v digitálnom prostredí.

2 KONTAKTNÉ ÚDAJE

Zriaďovateľom a prevádzkovateľom CAMOSR je Ministerstvo obrany Slovenskej republiky.

1. Kontaktné údaje Certifikačnej autority MOSR

   Adresa: **VÚ 9066 Trenčín**
   Certifikačná autorita MOSR (CAMOSR)
   Olbrachtova 5
   911 01 Trenčín

2. Kontaktné údaje LRA Trenčín

   Adresa: **VÚ 9066 Centrum KIS ZÁPAD**
   Lokálna registračná autorita MOSR (LRAMOSR)
   Legionárska 5
   911 01 Trenčín

3. Kontaktné údaje LRA Bratislava

   Adresa: **VÚ 9066 Centrum KIS JUH**
   Lokálna registračná autorita MOSR (LRAMOSR)
   Za kasárňou 3
   Bratislava

4. Kontaktné údaje LRA Zvolen

Adresa:	**VÚ 9066 Centrum KIS STRED**
	Lokálna registračná autorita MOSR (LRAMOSR)
	Borovianska cesta 1
	960 01 Zvolen

5. Kontaktné údaje LRA Prešov

Adresa:	**VÚ 9066 Centrum KIS VÝCHOD**
	Lokálna registračná autorita MOSR (LRAMOSR)
	Námestie Legionárov 4
	080 01 Prešov

6. Telefón, fax, email a web

e-mail:	**pki@mil.sk**
www:	**http://pki.mil.sk**
Pracovný čas	
telefón:	**+421 (0)960 401 111 (Kontaktné centrum)**
fax:	**+421 (0)960 407 470**
Mimopracovný čas	
telefón:	**+421 (0)960 406 400, 40 22 00 (DRKIS)**
fax:	**+421 (0)960 406 420 (DRKIS)**

3 TYPY CERTIFIKÁTOV, POSTUPY OVERENIA A POUŽITIE

3.1 Typy certifikátov

Typ	Popis	Účel
QCP-n-qscd	Kvalifikovaný certifikát pre fyzickú osobu vydaný na kvalifikované zariadenie na vyhotovenie elektronického podpisu	Kvalifikovaný elektronický podpis
QCP-l-qscd	Kvalifikovaný certifikát pre právnickú osobu vydaný na kvalifikované zariadenie na vyhotovenie elektronického podpisu	Kvalifikovaná elektronická pečať

Tabuľka 1: Typy certifikátov

Podrobné profily certifikátov sú zverejnené v Certifikačnom poriadku.

Okrem kvalifikovaných certifikátov koncových používateľov je CAMOSR vydávajúcou certifikačnou autoritou pre certifikáty využívané pri poskytovaní vlastných kvalifikovaných dôveryhodných služieb:

- **OCSP Signer**: OCSP služba pre overovanie kvalifikovaných certifikátov pre elektronický podpis a pečať

- **TSA**: služba poskytovania časovej pečiatky

Všetky certifikáty služieb pre poskytovanie kvalifikovaných dôveryhodných služieb sú dostupné na stránke https://pki.mil.

3.2 Postupy overenia

Overenie identity fyzickej osoby:

Fyzickou osobou je osoba organizačne spadajúca pod Ministerstvo obrany SR alebo Generálny štáb ozbrojených síl SR.

Fyzická osoba musí preukázať svoju totožnosť dvomi z týchto osobných dokladov, pričom minimálne jeden musí obsahovať fotografiu fyzickej osoby, jej rodné číslo a adresu trvalého bydliska:

- občiansky preukaz,
- služobný preukaz profesionálneho vojaka,
- cestovný pas,
- vodičský preukaz,
- rodný list,

- zbrojný preukaz,
- kartičku poistenca.

Všetky doklady, predkladané žiadateľmi o certifikát, musia byť buď originály, alebo úradne overené kópie originálov. Nesmie v nich byť žiaden údaj doplňovaný, pozmeňovaný, prečiarknutý a podobne.

Ak fyzická osoba zastupuje na LRA inú fyzickú osobu, musí sa navyše preukázať úradne overeným (notárom alebo matrikou) plnomocenstvom, z textu ktorého jednoznačne vyplýva, že zastupujúca fyzická osoba bola splnomocnená splnomocňujúcou fyzickou osobou konať v danej veci v jej mene.

Subjekt (fyzická alebo právnická osoba), ktorý zastupuje fyzickú osobu, sa vo veci fyzickej osoby, ktorú zastupuje, v žiadnom prípade nemôže nechať zastupovať iným subjektom.

CAMOSR bude zaznamenávať tento proces pre každý certifikát. Dokumentácia o identifikácii musí minimálne obsahovať:

- identita osoby, ktorá vykonáva identifikáciu,
- vyhlásenie podpísané touto osobou, že overila identitu subjektu resp. žiadateľa o certifikát tak, ako to vyžaduje tento certifikačný poriadok,
- jednoznačné identifikačné čísla z predložených osobných dokladov dokladujúcich identitu autentizovanej osoby,
- dátum a čas vykonania identifikácie.

Súčasťou dokumentácie o identifikácii musí byť vyplnený formulár obsahujúci zozbierané identifikačné údaje, ktorý bude vlastnoručne podpísaný identifikovanou osobou v prítomnosti osoby vykonávajúcej autentizáciu identity.

Kontrola údajov na predložených dokladoch

V prípade ľubovoľných odôvodnených pochybností o totožnosti žiadateľa môže LRA jeho registráciu odmietnuť. Pracovník LRA kontroluje na predložených dokladoch najmä nasledovné:

Osobné doklady fyzickej osoby:

a) platnosť predloženého dokladu

Upozornenie: V prípade neplatného osobného dokladu sa postupuje ako pri chýbajúcom osobnom doklade - RA registráciu odmietne

b) plnoletosť fyzickej osoby (t.j. vek 18 rokov)

c) či nie je zjavný nesúlad medzi fotografiou v osobnom doklade a vzhľadom majiteľa osobného dokladu

Upozornenie: Ak áno, RA môže odmietnuť registráciu.

d) zhodnosť predložených dokladov, t.j. či údaje na jednom doklade neodporujú údajom na inom doklade

Výpisy z obchodného registra: - len ak sa to bude týkať VOP, úradov a zariadení zriadených MOSR

e) či výpis nie je starší ako 3 mesiace

f) či majú fyzické osoby (stačí jedna fyzická osoba, ak na výpise nie je uvedené inak), ktoré predložili daný výpis, právo konať (podpisovať) za danú právnickú osobu (t.j. či sú jej štatutárnymi zástupcami)

g) či je výpis úradne overený (notárom alebo matrikou), ak sa nejedná o originál

Poznámka. Výpis z obchodného registra získaný z Internetu je pri konaní na RA nepoužiteľný.

Plnomocenstvo:

h) či je plnomocenstvo úradne overené (notárom alebo matrikou)

i) či sa údaje, uvedené v plnomocenstve, ktoré definujú zastupujúcu fyzickú resp. právnickú osobu, zhodujú s údajmi uvedenými na osobných dokladoch zastupujúcej fyzickej osoby resp. s údajmi uvedenými na výpise z obchodného registra zastupujúcej právnickej osoby

j) rozsah plnomocenstva - t.j. či plnomocenstvo oprávňuje splnomocnenú fyzickú alebo právnickú osobu k požadovanému úkonu na RA v mene splnomocňujúcej fyzickej alebo právnickej osoby

k) či plnomocenstvo nie je časovo obmedzené alebo ak obsahuje inú podmienku, či je táto splnená

Druh predložených dokladov (napr. občiansky preukaz, pas) a príslušné údaje z nich zaznamená pracovník RA na príslušný formulár, ktorý zostáva na RA.

Pri mandátnych certifikátoch sa oprávnenie konať preukazuje podľa zoznamu dokladov, ktoré sú pre dané oprávnenie uvedené v zozname oprávnení podľa § 9 zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov.

Overenie identity právnickej osoby:

Identita právnickej osoby sa bude autentizovať na základe názvu právnickej osoby, iného identifikačného údaja, ak taký existuje (spravidla je to napr. IČO), adresy a dôkazu existencie danej právnickej osoby (spravidla výpisom z obchodného registra).

LRA bude overovať tieto údaje a okrem autentickosti žiadajúcej osoby sa bude overovať, že daná osoba má právo jednať v mene danej právnickej osoby v danej veci.

Právnická osoba musí byť registrovaná na území Slovenskej republiky a musí preukázať svoju totožnosť výpisom z obchodného registra nie starším ako tri mesiace.

Právnická osoba musí spadať do organizačnej štruktúry Ministerstva obrany SR alebo Generálneho štábu ozbrojených síl SR.

Fyzické osoby (jedna alebo viac, podľa predloženého výpisu z obchodného registra), ktoré na základe predloženého výpisu z obchodného registra konajú na LRA za danú právnickú osobu, musia preukázať svoju totožnosť.

V mene právnickej osoby môže na LRA konať len osoba, ktorá je jej štatutárom (alebo viac takýchto osôb súčasne, ak to vyžaduje predložený výpis z obchodného registra), prípadne sa právnická osoba môže nechať zastupovať fyzickou alebo inou právnickou osobou, ktorá na LRA predloží oprávnenie na konanie v mene zastupovanej osoby nasledovne:

- poverením, ak je daná fyzická osoba zamestnancom právnickej osoby, v mene ktorej koná a pracovno-právny vzťah má podložený pracovnou zmluvou,
- úradne overenej plnej moci, ak daná fyzická osoba nemá pracovno-právny vzťah podložený pracovnou zmluvou k právnickej osobe, v mene ktorej koná.

Subjekt (fyzická alebo právnická osoba), ktorý zastupuje právnickú osobu, sa vo veci právnickej osoby, ktorú zastupuje, v žiadnom prípade nemôže nechať zastupovať iným subjektom.

V prípade, že právnická osoba nemôže preukázať svoju totožnosť výpisom z obchodného registra, musí takáto právnická osoba písomne preukázať okrem svojej totožnosti aj legálnosť (resp. „dôvod“) svojej existencie (s využitím a poukázaním na zákon alebo iný predpis, ktorý o subjekte daného typu pojednáva).

3.3 Použitie certifikátu

Kvalifikované certifikáty je možné používať iba v súlade s platnými právnymi predpismi a za podmienok, ktoré sú definované v Certifikačnej politike (CP) a Pravidlách na výkon certifikačných činnosti (CPS). Akékoľvek iné použitie je zakázané.

4 SPOĽAHLIVOSŤ

Kvalifikovaný certifikát smie byť použitý iba na podpis alebo pečať.

Doba, počas ktorej sú uchovávané registračné informácie a záznamy udalostí je min. 10 rokov.

5 POVINNOSTI ŽIADATEĽA O CERTIFIKÁT

Povinnosťou žiadateľa o certifikát je:

- predložiť RA presné, pravdivé a úplné informácie v súlade s požiadavkami CP,
- predložiť RA všetky požadované dokumenty,
- zabezpečiť, aby pri generovaní kľúčov bola použitá vhodná dĺžka kľúča a vhodné algoritmy, ktoré sú v súlade s predpísanou podpisovou politikou, ak si ich generuje sám,
- predložiť RA vygenerovanú žiadosť o certifikát, na základe ktorej sa má vydať certifikát, táto žiadosť o certifikát musí obsahovať údaje, ktoré sú v súlade s údajmi

na predkladaných dokumentoch a formulároch, kľúče musia byť vygenerované v QSCD,

- prevziať certifikát vydaný na základe jeho žiadosti.

Povinnosťou držiteľa certifikátu (subjektu) je:

- neustále chrániť svoje privátne kľúče a QSCD, v ktorých sú uložené, a heslá na prístup k privátnym kľúčom v súlade s touto CPS a tiež ako je stanovené v jeho zmluve o vydaní a používaní certifikátu,
- používať len kvalitné, silné heslá na prístup k privátnym kľúčom,
- v prípade straty QSCD, straty, zneužitia alebo kompromitácie privátneho kľúča, zabudnutia hesla na prístup k privátnemu kľúču alebo ak nastali zmeny alebo sa vyskytli nepresnosti v údajoch uvedených v danom certifikáte bezodkladne požiadať o zrušenie daného certifikátu. Toto musí byť urobené prostredníctvom mechanizmu, ktorý je v súlade s CP,
- po kompromitácii okamžite a natrvalo zastaviť používanie daného privátneho kľúča,
- dodržovať všetky lehoty, podmienky a obmedzenia uložené na používanie svojich privátnych kľúčov, certifikátov a QSCD,
- precízne sa identifikovať a vyjadrovať pri ľubovoľnej komunikácii s RA resp. CAMOSR,
- používať poskytnuté certifikáty len s aplikáciami, ktoré boli certifikované ako produkty pre kvalifikovaný elektronický podpis/pečať,
- získať a do používaných aplikácií nainštalovať certifikát CAMOSR (ktorá vydala jeho certifikát) a tiež koreňový certifikát CA NBÚ (ktorá vydala certifikát CAMOSR), aby bola zabezpečená správna činnosť používaných aplikácií.

Držiteľ certifikátu, ktorý nedodržiava resp. nedodržiaval svoje povinnosti, nemá nárok na náhradu prípadnej škody.

6 KONTROLA STAVU CERTIFIKÁTU SPOLIAHAJUCIMI SA STRANAMI

Strany spoliehajúce sa na certifikát sú povinné:

- získať a do používaných aplikácií nainštalovať certifikát CA (ktorá vydala jeho kvalifikovaný certifikát) a tiež koreňový certifikát CA NBÚ (ktorá vydala certifikát pre CAMOSR), aby bola zabezpečená správna činnosť používaných aplikácií (aby aplikácia mohla verifikovať celú certifikačnú cestu v súlade so štandardom X.509 verzie 3),
- používať certifikát len na účel, pre ktorý bol vydaný, ako je to dané informáciami v certifikáte,
- predtým, ako sa na daný kvalifikovaný elektronický podpis spoľahnú, overiť certifikát patriaci k danému KEPu na jeho platnosť (tzn. overovať, že certifikát bol v danom čase platný a že sa nenachádzal na aktuálnom zozname zrušených certifikát vydanom CAMOSR),

Za účelom overenia platnosti certifikátu obsahuje každý certifikát adresu zoznamu zrušených certifikátov (CRL) a adresu služby Online Certificate Status Protocol (OCSP).

7 OBMEDZENIE ZÁRUK A ZODPOVEDNOSTI

CAMOSR sa riadi platnými zákonmi Slovenskej republiky, najmä Nariadením eIDAS a zákonom č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách).

CAMOSR sa zaväzuje, že pri výkone svojich činností bude dodržiavať ustanovenia platnej legislatívy SR, bezpečnostnej dokumentácie CAMOSR, „Certifikačného poriadku CAMOSR“ a postupy stanovené „Pravidlami na výkon certifikačných činností CAMOSR“ a „Pravidlami na výkon služby poskytovania časovej pečiatky“.

CAMOSR garantuje jednoznačnosť čísla (`Serial Number`) každého ňou vydaného certifikátu, tzn. garantuje, že neexistujú a nikdy nebudú existovať žiadne dva certifikát, ktoré by mali rovnaké číslo.

CAMOSR zaručuje výkon kvalifikovaných dôveryhodných služieb v súlade so svojím CP a CPS.

CAMOSR ručí za to, že pri podpisovaní ňou vydávaných certifikátov a CRL použije vlastný privátny kľúč uložený v HSM module patriaci k jej vlastnému certifikátu.

CAMOSR poskytuje záruku, že ňou vydaný certifikát bude vyhovovať štandardu X.509 verzie 3.

8 APLIKOVATEĽNÉ DOHODY, CPS A CP

Vzťah medzi Žiadateľom o certifikát a CAMOSR sa okrem ustanovení príslušných právnych predpisov riadi zmluvou a ustanoveniami platného CP a CPS.

Vzťah medzi Spoliehajúcou stranou a CAMOSR nie je upravený zmluvou a riadi sa príslušnými ustanoveniami platného CP a CPS.

Všetky verejné informácie možno získať na adrese https://pki.mil.sk.

9 ZÁSADY OCHRANY OSOBNÝCH ÚDAJOV

Ochrana osobných údajov je riešená v súlade s platnou legislatívou týkajúcou sa osobných údajov t.j. zákonom Slovenskej republiky č. 18/2018 Z. z. o ochrane osobných údajov a Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

10 NÁHRADA ŠKODY

CAMOSR je zodpovedná výlučne za škody spôsobené spoliehaním sa na informácie, ktoré obsahujú certifikáty ňou vydané. CAMOSR si vyhradzuje právo každý takýto prípad najskôr prešetriť a posúdiť. V prípade, keď CAMOSR nespôsobila chybu v informáciách uvedených v certifikátoch, za prípadné vzniknuté škody CAMOSR nezodpovedá.

CAMOSR v žiadnom prípade nezodpovedá za škody spôsobené neoprávneným alebo neopatrným použitím certifikátu, použitím certifikátu mimo rámca definovaného certifikátom a certifikačným poriadkom, neoprávneným alebo neopatrným použitím CRL, použitím neplatného certifikátu (exspirovaného alebo zrušeného), zneužitím súkromného kľúča subjektu, treťou osobou, vyššou mocou (živelná pohroma, vojna prípadne iné nekontrolovateľné udalosti alebo sily).

CAMOSR ani jej LRA nie sú zodpovedné za nesprávne údaje predložené žiadateľom o certifikát, ktoré sa pri registrácii nedajú overiť.

CAMOSR nie je zodpovedná za nepriame, následné alebo náhodné škody, stratu zisku, stratu dát alebo iné škody vzniknuté v súvislosti s používaním alebo nefunkčnosťou certifikátu, kvalifikovaného elektronického podpisu alebo aplikácií, ktoré certifikát používajú.

CAMOSR nevykonáva funkciu prostredníka medzi držiteľmi certifikátov a používateľmi certifikátov.

CAMOSR nie je zodpovedná za škody vzniknuté v čase od podania žiadosti o zrušenie certifikátu do okamihu zverejnenia daného certifikátu v novom CRL, ak bol daný certifikát zverejnený v novom CRL v stanovenej lehote, spresnenej v tomto dokumente.

Rozsah právnych záruk CAMOSR, ako poskytovateľa kvalifikovaných dôveryhodných služieb, je definovaný v Zmluve o vydaní a používaní certifikátu.

CAMOSR poskytuje záruku na použitie ňou vydaných certifikátov podľa platnej legislatívy. Predpokladom je, že boli dodržané príslušné ustanovenia tohto CP. Organizácia disponuje dostatočnými prostriedkami na plnenie prípadných záväzkov vyplývajúcich z poskytovanej záruky.

Záruku a z nej vyplývajúce plnenie, je možné uznať len za predpokladu, že subjekt neporušil svoje povinnosti (hlavne ochranu svojho privátneho kľúča), a že každý, kto sa v danom prípade spoliehal na certifikát vydaný CAMOSR, urobil všetko, aby prípadnej škode zabránil, hlavne že si overil aktuálny stav predmetného certifikátu (t.j. či daný certifikát nebol v rozhodujúcom čase, keď sa na neho spoliehalo, na zozname zrušených certifikátov).

Neoverenie stavu certifikátu pomocou zoznamu zrušených certifikátov sa kvalifikuje ako hrubé porušenie povinností vyplývajúcich z CP, dôsledkom čoho zanikajú akékoľvek nároky na prípadné uplatňovanie si záruky voči CAMOSR.

CAMOSR a ani zriaďovateľ CAMOSR nemajú žiadnu finančnú zodpovednosť za prípadné škody, ktoré by vznikli držiteľovi certifikátu alebo strane spoliehajúcej sa na

certifikát v súvislosti s používaním certifikátu s nejakou konkrétnou aplikáciou resp. hardvérom alebo v súvislosti s tým, že certifikát nie je možné používať s nejakou konkrétnou aplikáciou resp. hardvérom.

Akákoľvek žiadosť o náhradu škody musí byť podaná písomne.

11 ROZHODNÉ PRÁVO, SŤAŽNOSTI A RIEŠENIE SPOROV

CAMOSR si vyhradzuje právo každý sporný prípad najprv preskúmať.

Pre potreby interpretácie ustanovení CP alebo riešenia sporov sa možno obrátiť na LRA a v prípade nesúhlasu s jej rozhodnutím na najbližšiu vyššiu inštanciu. Inštancie sú usporiadané vzostupne v poradí:

- LRA
- CAMOSR (vybavuje len písomne podané žiadosti a podnety)
- NBÚ SR

Prednostne bude snahou riešiť spory dohodou.

Povinnosťou každej inštancie je prípad zaprotokolovať a dať žiadateľovi o certifikát resp. sťažovateľovi vysvetlenie resp. návrh na riešenie sporu a v prípade jeho nesúhlasu prípad postúpiť na vyššiu inštanciu.

Žiadnym rozhodnutím niektorej z tu definovaných inštancií nie je dotknuté právo sťažovateľa postúpiť sťažnosť nezávislému súdu.

12 POSKYTOVATEĽ DVÔVERYHODNÝCH SLUŽIEB A ÚLOŽISKO, LICENCIE, ZNAČKY DVÔVERYHODNOSTI A AUDIT

CAMOSR je akreditovaná ako kvalifikovaný poskytovateľ dôveryhodných služieb podľa nariadenia eIDAS a zapísaná do Zoznamu kvalifikovaných poskytovateľov dôveryhodných služieb: https://eidas.ec.europa.eu/efda/tl-browser.

Poskytovanie týchto služieb je minimálne raz za 24 mesiacov podrobené posúdeniu zhody s príslušnými právnymi predpismi a technickými štandardami nezávislým Orgánom posudzovania zhody.

Certifikácia CAMOSR:

Certifikát pre kvalifikovanú dôveryhodnú službu vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis,
Certifikát pre kvalifikovanú dôveryhodnú službu vyhotovovania a overovania kvalifikovaných certifikátov pre elektronickú pečať,
Certifikát pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických pečiatok.