Akreditovaná certifikační autorita eIdentity

ACAeID 35 Zpráva pro uživatele

Verze:	1.2
Odpovídá:	Ing. Jiří Hejl
Datum:	21. 12. 2012
Utajení:	Veřejný dokument

Copyright © 2006 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.

ACAeID 35 Zpráva pro uživatele					Počet stran: 19
Verze	**Datum**	**Autor**	**Schválil**	**Přílohy**	**Poznámka**
0.9	20.02 2007	Ing. Jiří Hejl	Ing. Ladislav Šedivý		Komplexní verze
1.0	10. 05.2007	Ing. Jiří Hejl	Ing. Ladislav Šedivý		Jazyková revize
1.0	07. 11. 2008	Ing. Jiří Hejl	Ing. Ladislav Šedivý		Revize dokumentu
1.1	02. 11.2009	Ing. Jiří Hejl	Ing. Ladislav Šedivý		Úprava dokumentu
1.2	21. 12. 2012	Ing. Jiří Hejl	Ing. Ladislav Šedivý		Úprava dokumentu

OBSAH

1 ÚVOD

Tento dokument poskytuje základní přehled o hierarchii certifikačních autorit eIdentity a.s., právech a povinnostech držitelů certifikátů a časových razítek.

Tento dokument má informační charakter, nenahrazuje certifikační politiky a není součástí smlouvy o poskytování certifikačních služeb mezi zákazníkem a eIdentity a.s..

Organizace spravující dokument:

eIdentity a.s.
Vinohradská 184
130 00 Praha 3, Česká republika, IČO: 27112489
Společnost je zapsaná u Městského soudu v Praze oddíl B, vložka 9080

1.1 Kontroly bezpečnostní shody, audity a jiné kontroly

Datum	Typ auditu/kontroly	Výrok kontrolora/auditora
20. 9. 2007	Kontrola bezpečnostní shody	ACA eIdentity splňuje požadavky prokázání bezpečnostní shody podle vyhl. č. 378/2007 Sb.
20. 9. 2007	Audit ISMS	ACA eIdentity splňuje požadavky auditu systému řízení bezpečnosti informací (ISMS) podle vyhl. č. 378/2007 Sb.
19. 12. 2008	Částečná kontrola bezpečnostní shody	1. poskytovatel provozuje důvěryhodné systémy v souladu se Zákonem a Vyhláškou, což doložil věrohodnými důkazy 2. poskytovatel provádí změny v důvěryhodných systémech v souladu s bezpečnostní dokumentací, což bylo doloženo jak výše uvedeno a odvozeno ze stavu dokumentace a reálného stavu systému z r. 2005 až 2008 3. částečná kontrola bezpečnostní shody proběhla v termínech, uvedenými ve Vyhlášce 4. částečná kontrola bezpečnostní shody proběhla v souladu s Vyhláškou
27. 3. 2010	Částečná kontrola bezpečnostní shody	ACA eIdentity splňuje požadavky prokázání bezpečnostní shody podle vyhl. č. 378/2007 Sb.
27. 3. 2010	Audit ISMS	ACA eIdentity splňuje požadavky auditu systému řízení bezpečnosti informací (ISMS) podle vyhl. č. 378/2007 Sb.
12. 4. 2010	Částečná kontrola bezpečnostní shody	ACA eIdentity splňuje požadavky prokázání bezpečnostní shody podle vyhl. č.378/2007 Sb. a to i po doplnění o službu časových razítek

12. 4. 2010	Audit ISMS	ACA eIdentity splňuje požadavky auditu systému řízení bezpečnosti informací (ISMS) podle vyhl. č. 378/2007 Sb. a to i po doplnění o službu časových razítek
3. 3. 2011	Částečná kontrola bezpečnostní shody	1. poskytovatel provozuje důvěryhodné systémy v souladu se Zákonem a Vyhláškou, což doložil věrohodnými důkazy 2. poskytovatel provádí změny v důvěryhodných systémech v souladu s bezpečnostní dokumentací, což bylo doloženo jak výše uvedeno a odvozeno ze stavu dokumentace a reálného stavu systému z r. 2005 až 2009 3. částečná kontrola bezpečnostní shody proběhla v termínech, stanovených Vyhláškou 4. částečná kontrola bezpečnostní shody proběhla v souladu s Vyhláškou
28. 3. 2012	Audit ISMS	Hodnocený systém jako celek splňuje kombinovaná kritéria ISO/IEC 27001, CWA 14167-1, ETSI TS 101 456 102 023.

2 KONTAKTNÍ INFORMACE

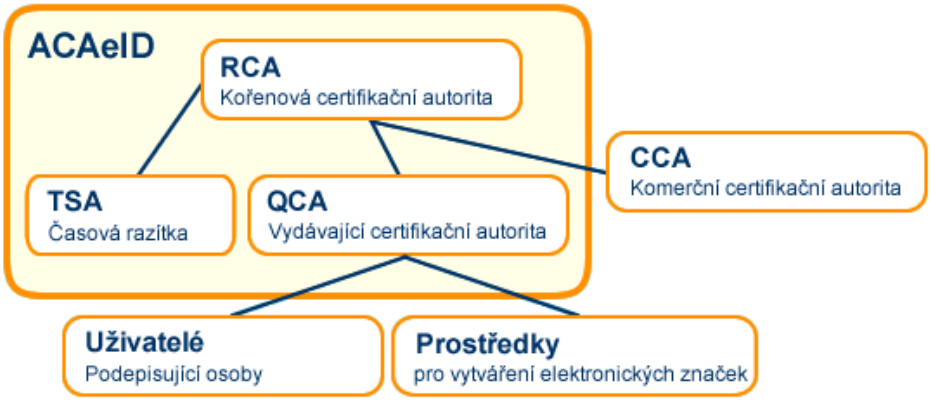
eIdentity a.s.
Vinohradská 184
130 00 Praha 3, Česká republika

Tel: +420 222 866 150 Fax: +420 222 866 159
E-mail: info@eidentity.cz
Web: http://www.eidentity.cz

Informace o vydaných či zneplatněných certifikátech a certifikační politiky naleznete také na:
http://pub1.acaeid.cz
http://pub2.acaeid.cz
http://www.acaeid.cz

3 TYPY SLUŽEB, OVĚŘOVACÍ PROCEDURY

3.1 Akreditované služby



Akreditovaná certifikační autorita eIdentity a.s. (ACAeID) je tvořena kořenovou certifikační autoritou (RCA) a autoritou vydávající kvalifikované a kvalifikované systémové certifikáty pro podepisující a označující osoby (QCA). RCA vydává kvalifikované systémové certifikáty pouze podřízeným certifikačním autoritám (tedy i QCA a CCA). QCA vydává kvalifikované certifikáty a kvalifikované systémové certifikáty jednotlivým žadatelům. Kořenová certifikační autorita (RCA) vydala kvalifikovaný systémový certifikát pro autoritu vydávající kvalifikovaná časová razítka (TSA).

QCA poskytuje tyto služby:

- Vydání kvalifikovaného certifikátu
- Vydání kvalifikovaného certifikátu s vyznačením identifikátoru ministerstva práce a sociálních věcí (MPSV)
- Vydání kvalifikovaného certifikátu s vyznačením pracovní pozice v organizaci
- Vydání kvalifikovaného systémového certifikátu
- Vydání kvalifikovaného časového razítka

Mezi další služby ACAeID patří pravidelné vydávání seznamu zneplatněných certifikátů (CRL) či seznamu vydaných certifikátů.

Během procesu vydávání certifikátu je vždy ověřována totožnost žadatele o certifikát prostřednictvím jeho osobních dokladů a v případě certifikátu pro právnickou nebo podnikající fyzickou osobu i vazba žadatele o certifikát na tuto osobu.

Podrobný popis registračních postupů je uveden v příslušných certifikačních politikách

3.2 Komerční služby

Pro účely šifrování, identifikace, ale také pro vytváření a ověřování elektronických podpisů v oblasti běžné komerční komunikace lze využít elektronických certifikátů, vydaných Komerční certifikační autoritou (CCA).

Tato certifikační autorita vydává také elektronické certifikáty pro technologické komponenty informačních systémů (např. pro webové servery či servery elektronické pošty, zabezpečeně komunikující pomocí SSL/TLS).

CCA poskytuje tyto služby:

- Vydání komerčního certifikátu pro elektronický podpis
- Vydání komerčního certifikátu pro šifrování zpráv
- Vydání komerčního certifikátu pro identifikaci
- Vydání komerčního serverového certifikátu pro SSL/TLS

3.3 Počáteční ověření identity žadatele o certifikát

3.3.1 Ověření souladu dat, tj. postup při ověřování, zda má osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů nebo data pro vytváření elektronických značek odpovídající datům pro ověřování elektronických značek

Žadatel o kvalifikovaný certifikát, nebo kvalifikovaný systémový certifikát musí prokázat vlastnictví soukromého klíče odpovídající veřejnému klíči, který má být uveden v kvalifikovaném certifikátu. Principem je předání veřejného klíče spolu s případnými dalšími daty certifikační autoritě tak, aby tento balík nebo jeho otisk byl podepsán odpovídajícím soukromým klíčem. Většinou se taková zpráva vytváří prostředky prostředí, ve kterém se klíče a kvalifikovaný certifikát, nebo kvalifikovaný systémový certifikát budou používat.

3.3.2 Ověřování identity právnické osoby nebo organizační složky státu

Identitu prokazuje právnická osoba předložením originálu nebo ověřené kopie výpisu z obchodního rejstříku, výpisu ze živnostenského rejstříku či jiné listiny, na základě které byla organizace zřízena. Z dokladu musí být patrno úplné obchodní jméno organizace, přidělené identifikační číslo, sídlo a statutární orgán. Pro účely jednání s eIdentity a.s. může statutární orgán zmocnit další osobu.

3.3.3 Ověřování identity fyzické osoby

Fyzická osoba prokazuje svoji identitu platným, nepoškozeným osobním dokladem a pro účely vydání kvalifikovaného certifikátu dokládá svoje identifikační údaje dvěma platnými, nepoškozenými osobními doklady.

Občan České republiky předkládá jako primární osobní doklad občanský průkaz. Jako druhý osobní doklad se přijímá platný cestovní pas, řidičský průkaz nebo rodný list.

Primárním dokladem pro ověření totožnosti žadatele, jenž není občanem České republiky, je platný pas – cestovní, diplomatický, nebo průkaz o povolení k pobytu vydaný příslušným orgánem ČR. Občan EU, občan Islandu, Lichtenštejnska, Norska a Švýcarska může předložit jako osobní doklad také doklad, který mu byl vydán k prokázání totožnosti na území příslušného státu. Typ dokladu a údaje v

něm obsažené musí být psány latinkou. Doklad musí obsahovat anglický překlad údajů v něm uvedených. Druhým dokladem totožnosti může být řidičský průkaz nebo pas - cestovní, diplomatický, nebo průkaz o povolení k pobytu vydaný příslušným orgánem ČR. Občan EU, občan Islandu, Lichtenštejnska, Norska a Švýcarska může předložit jako osobní doklad také doklad, který mu byl vydán k prokázání totožnosti na území příslušného státu. Druhý doklad totožnosti nesmí být shodný s předloženým primárním dokladem totožnosti, musí být psán latinkou a údaje v něm uvedené musí obsahovat anglický překlad.

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

O zneplatnění certifikátu může požádat držitel nebo podepisující osoba. Zneplatnění certifikátu je prováděno v souladu s příslušnou certifikační politikou.

Žádost o zneplatnění musí být v písemné formě a musí obsahovat:

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

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

Žádost o zneplatnění lze podat:

- Elektronicky v účtu žadatele
- Osobně na RM
- Faxem

3.5 Identifikace a autentizace žadatele o časové razítko

Pro využívání služby kvalifikovaných časových razítek je nutné nejdříve uzavřít Smlouvu.

Mimo obchodních podmínek poskytování služby kvalifikovaného časového razítka je obsahem smlouvy i určení způsobu identifikace a autentizace žádající eIdentity a případně je ve smlouvě uvedena i osoba pověřená a zodpovědná ve věcech souvisejících s plněním této smlouvy.

Pro identifikaci a autentizaci lze použít komerční nebo komerční serverový certifikát vydaný některou certifikační autoritou společnosti eIdentity a.s. nebo je možné smluvně sjednat jiný způsob identifikace a autentizace.

V případě úspěšné identifikace a autentizace získá žadatel jemu odpovídající autorizaci k poskytované službě.

4 OMEZENÍ POUŽITÍ

4.1 Kvalifikované certifikáty

Kvalifikované certifikáty se mohou použít jen k účelům, které stanovuje zákon 227/2000 Sb.

4.1.1 Přípustné použití kvalifikovaného certifikátu

Typickými aplikacemi, které je možné použít v souvislosti s kvalifikovanými certifikáty, jsou aplikace umožňující vytvářet a ověřovat elektronické podpisy či elektronické značky jako například systémy elektronické pošty, podepisovací a ověřovací aplikace pro podepisování dokumentů a jiných typů souborů obecně, pokud jsou v souladu s požadavky zákona 227/2000 Sb.

4.1.2 Nepřípustné použití kvalifikovaného certifikátu

Certifikáty se nesmí používat v rozporu s účelem, ke kterému byly vydány a to jak z technického hlediska (např. podle omezení KeyUsage) tak i z právního hlediska (např. v rozporu se zákonem 227/2000 Sb.).

Takovým nepřípustným použitím kvalifikovaného certifikátu může být například jeho použití pro šifrování či identifikaci účastníka šifrované komunikace v prostředí protokolu SSL/TLS.

4.2 Komerční certifikáty

Komerční certifikáty vydané podle Certifikační politiky se mohou použít jen k účelům, které jsou v certifikátu vyznačeny.

4.2.1 Přípustné použití komerčního certifikátu

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

4.2.2 Nepřípustné použití komerčního certifikátu

Certifikáty se nesmí používat v rozporu s účelem, ke kterému byly vydány (např. podle omezení KeyUsage).

4.3 Kvalifikovaná časová razítka

Kvalifikovaná časová razítka se mohou použít jen k účelům, které stanovuje zákon 227/2000 Sb.

4.3.1 Přípustné použití kvalifikovaného časového razítka

Kvalifikované časové razítko je datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

4.3.1 Nepřípustné použití kvalifikovaného časového razítka

Kvalifikovaná časová razítka nesmí uživatel využít v rozporu s vydávaným účelem nebo s platnou legislativou.

5 POVINNOSTI KLIENTŮ (ŽADATELŮ)

Klient certifikační autority eIdentity a.s. je právnická nebo fyzická osoba, která je v příslušném smluvním vztahu s eIdentity a.s.

Klient (žadatel) musí zejména:

- Seznámit se s certifikační politikou, podle které má být vydán certifikát, časové razítko.
- Poskytovat pravdivé a úplné informace poskytovateli certifikačních služeb.
- Neprodleně informovat poskytovatele certifikačních služeb o změnách údajů, které jsou uvedeny ve smlouvě o poskytování certifikačních služeb nebo ve vystaveném certifikátu.
- Nakládat se soukromým klíčem, který odpovídá veřejnému klíči v certifikátu vydaném podle libovolné certifikační politiky, s náležitou péčí, tak, aby nemohlo dojít k jeho neoprávněnému použití, a užívat soukromý klíč pouze pro účely stanovené v certifikační politice, podle které byl vystaven odpovídající certifikát.
- Neprodleně uvědomit poskytovatele certifikačních služeb o skutečnostech, které vedou ke zneplatnění certifikátu, zejména o podezření, že soukromý klíč byl zneužit, a požádat o zneplatnění certifikátu.
- Žadatel o kvalifikované časové razítko je vždy po obdržení odpovědi na žádost o kvalifikované časové razítko povinen zjistit informaci o stavu zpracování této žádosti. V případě, že kvalifikované razítko bylo vydáno, provede dále tyto činnosti:
  a) ověří platnost elektronické značky pomocí kvalifikovaného systémového certifikátu vydávající TSU
  b) ověří platnost elektronických značek celého příslušného certifikačního řetězce
  c) ověří, zda OID politiky pro vydávání kvalifikovaných časových razítek, které je uvedeno v odpovědi, odpovídá správnému OID
  d) v případě, že žádost obsahovala položku „nonce“ nebo/a položku „reqPolicy“, ověří, že její hodnota v odpovědi je shodná.

6 POVINNOSTI SPOLÉHAJÍCÍCH SE STRAN

6.1 Povinnosti spoléhajících se stran - certifikáty

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

6.2 Povinnosti spoléhajících se stran – kvalifikovaná časová razítka

Spoléhající se strana je povinna ověřit obsah časového razítka:

- otisk (hash) ověřovaných dat
- platnost elektronické značky pomocí certifikátu TSU

Získat bezpečným způsobem aktuální příslušná CRL a ověřit platnost:

- elektronické značky pomocí kvalifikovaného systémového certifikátu vydávající TSU
- elektronických značek celého příslušného certifikačního řetězce

Zvážit, zda časové razítko vydané podle této politiky, je vhodné pro účel, ke kterému bylo použito.
Ověřit, zda jsou kryptografické funkce použité v časovém razítku stále platné a bezpečné, jedná se zejména o:

- kryptografickou funkci pro tvorbu hashe
- kryptografický algoritmus použitý při označování razítka
- délku klíče u kryptografického algoritmu použitého pro označení razítka

7 OMEZENÍ ZÁRUKY A ODPOVĚDNOSTI

Hranice odpovědnosti jsou dány zákonem 227/2000 Sb.

Odpovědnost za škodu je specifikována ve smlouvě o poskytování služby.

Společnost eIdentity a.s. neodpovídá za škodu vzniklou žadateli nebo třetím stranám v důsledku porušení závazků žadatele nebo v souvislosti s tímto porušením anebo uvedením jakkoliv nesprávných údajů žadatelem.

8 SMLOUVY, CERTIFIKAČNÍ POLITIKY

Vztah mezi klientem a eIdentity a.s., je (kromě příslušných ustanovení povinných právních předpisů) upraven smlouvou. S jejím návrhem je klient seznámen předem.

Platné certifikační politiky jsou dostupné na webových stránkách společnosti eIdentity a.s.

9 OCHRANA OSOBNÍCH ÚDAJŮ

Zásady ochrany osobních údajů jsou obsaženy v certifikační politice a všeobecných obchodních podmínkách. Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 101/2000 Sb.

10 POLITIKA NÁHRAD A REKLAMACE

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

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

11 PRÁVNÍ PROSTŘEDÍ

Společnost eIdentity a.s. se při své činnosti řídí příslušnými ustanoveními právního řádu České republiky, zejména:

- vyhláškou České republiky č. 378/2006 Sb. o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb)
- zákonem České republiky č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů
- zákonem České republiky č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších
- zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb. a zákonem č. 440/2004 Sb.
- nařízením vlády České republiky č. 495/2004 Sb., kterým se provádí zákon č. 227/200 Sb.
- zákonem České republiky č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

12 AKREDITACE, AUDITY A KONTROLY

Společnosti eIdentity a.s. byla udělena Ministerstvem informatiky České republiky akreditace k výkonu činnosti akreditovaného poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty pod č. j. MI1471/31-2005 50 ze dne 12. 9. 2005, která nabyla právní moci dne 28. 9. 2005. V srpnu 2010 byla akreditace rozšířena i o oblast vydávání kvalifikovaných časových razítek.

Bezpečnost informací ve společnosti eIdentity a.s. je řízena. Společnost má zpracovánu odpovídající bezpečností dokumentaci a shoda s ní je ověřována pravidelnými audity v souladu s požadavky zákona č. 227/2000 Sb.