# CAcert – Přehled postupů certifikace (CPS) a Zásady certifikátů (CP)

Název: CPS [COD6](https://svn.cacert.org/CAcert/Policies/ControlledDocumentList.html)

Vytvořeno: 20060726, koncept od 20091108

Editor: NN

Stav: POLICY (ZÁSADY) [p20140731](https://wiki.cacert.org/PolicyDecisions#p20140731)

Licence: [CC-by-sa+DRP](https://wiki.cacert.org/Policy#Licence)

Český překlad: alkas

#### POZOR!Tento překlad slouží k pochopení popisovaného tématu.Právní platnost má POUZE anglický originál!

Obsah

1. Úvod 5

1.1 Přehled 5

1.2 Název a identifikace dokumentu 5

1.3 Kdo se podílí na infrastruktuře veřejných klíčů (PKI) 6

1.3.1 Certifikační autority 6

1.3.2 Registrační autority 6

1.3.3 Odběratelé 6

1.3.4 Spoléhající strany 6

1.3.5 Ostatní účastníci 6

1.4 Použití certifikátů 7

1.4.1 Správná použití certifikátů 7

1.4.2 Zakázaná použití certifikátů 8

1.4.3 Nespolehlivé aplikace 8

1.4.4 Omezené použití certifikátů 8

1.4.5 Kořenové certifikáty a jména (názvy) 9

1.5 Správa zásad 10

1.5.1 Organizace spravující dokument 10

1.5.2 Kontaktní osoba 11

1.5.3 Osoba určující vhodnost dokumentu CPS jako zásad 11

1.5.4 Schvalovací procedury CPS 11

1.5.5 Aktualizace CPS 11

1.6 Definice a zkratky 11

2. Odpovědnost za zveřejnění a úložiště 12

2.1 Úložiště 12

2.2 Zveřejňování certifikačních údajů 13

2.3 Doba nebo četnost publikace 13

2.4 Řízení přístupu k úložištím 13

3. Identifikace a ověření pravosti 13

3.1 Pojmenování 13

3.1.1 Typy jmen / názvů 13

3.1.2 Je nutné, aby jména (názvy) měly význam 14

3.1.3 Anonymita nebo pseudonymita odběratelů 14

3.1.4 Pravidla pro interpretaci různých tvarů jmen 14

3.1.5 Jedinečnost jmen 14

3.1.6 Uznání, ověření a úloha obchodních známek (trademarks) 15

3.1.7 Mezinárodní názvy domén 15

3.2 Počáteční ověření totožnosti 16

3.2.1 Metoda ověření vlastnictví privátního klíče 16

3.2.2 Určení totožnosti jednotlivce 16

3.2.3 Ověření totožnosti organizace 17

3.2.4 Neověřené údaje odběratele 17

3.2.5 Ověření autority 17

3.2.6 Kritérium pro součinnost 17

3.3 Žádosti o obnovení klíčů 17

3.4 Žádosti o odvolání certifikátů 18

4. Provozní požadavky životního cyklu certifikátu 18

4.1 Požadavky na vystavení certifikátů 18

4.1.1 Kdo může požádat o certifikát 18

4.1.2 Přidání adres 18

4.1.3 Příprava žádosti o certifikát (CSR) 18

4.2 Zpracování požadavku na certifikát 18

4.2.1 Identifikace (věření) 19

4.2.2 Ověření vlastnictví/oprávnění/správy 19

4.2.3 Dostupné možnosti 19

4.2.4 Procedury pro klientské certifikáty 20

4.2.5 Procedury pro serverové certifikáty 20

4.2.6 Procedury pro certifikáty pro podepisování kódu 20

4.2.7 Ověření domény organizace 20

4.3 Vystavení certifikátu 20

4.3.1 Akce CA během vydání certifikátu 20

4.3.2 Upozornění CA odběrateli o vystavení certifikátu 21

4.4 Přijetí certifikátu 21

4.4.1 Ustanovení o příjmu certifikátu 21

4.4.2 Zveřejnění certifikátu certifikační autoritou 21

4.4.3 Upozornění na vydání certifikátu certifikační autoritou jiným entitám 21

4.5 Klíčový pár a použití certifikátu 21

4.5.1 Použití klíčů odběratelem a jeho odpovědnost 22

4.5.2 Použití spoléhající stranou a její odpovědnost 22

4.6 Obnova certifikátu 24

4.7 Změna klíče certifikátu 24

4.8 Modifikace certifikátu 24

4.9 Odvolání a suspendování certifikátů 25

4.9.1 Podmínky odvolání 25

4.9.2 Kdo může odvolání vyžádat 25

4.9.3 Procedura žádosti o odvolání 25

4.9.4 Prodleva žádosti o odvolání 25

4.9.5 Doba, v níž musí CAcert zpracovat žádost o odvolání 25

4.9.6 Požadavek kontroly odvolání pro spoléhající strany 25

4.9.7 Frekvence vydávání CRL (dá-li se použít) 25

4.9.8 Nejdelší latence CRL (dá-li se použít) 25

4.9.9 Dostupnost kontroly odvolání / stavu certifikátu on-line 25

4.9.10 Požadavky na on-line kontrolu odvolání 25

4.9.11 Jiné dostupné formy inzerence odvolání 25

4.9.12 Zvláštní požadavky ohledně prozrazení klíče 26

4.9.13 Podmínky pro suspendování certifikátů 26

4.9.14 Kdo může požadovat suspendování 26

4.9.15 Procedura pro žádost o suspendování 26

4.9.16 Omezení doby suspendování 26

4.10 Služby stavu certifikátů 26

4.10.1 Provozní charakteristiky 26

4.10.2 Dostupnost služby 26

4.10.3 Volitelné vlastnosti 26

4.11 Ukončení odběru 26

4.12 Zabezpečené úložiště klíčů a jejich obnova 26

4.12.1 Zabezpečené úložiště klíčů, zásady obnovy a postupy 26

4.12.2 Zapouzdření klíče sezení, zásady obnovy a postupy 26

5. Zařízení, správa a řízení provozu 26

5.1 Fyzické ovládání 26

5.1.1 Napájení a klimatizace 26

5.1.2 Vystavení vodě 27

5.1.3 Prevence a ochrana před požárem 27

5.1.4 Uložení médií 27

5.1.5 Likvidace odpadů 27

5.1.6 Záloha mimo lokalitu 27

5.2 Procedurální řízení 27

5.2.1 Důvěryhodné role 27

5.2.2 Počet osob potřebných pro úkol 27

5.2.3 Identifikace a ověření pro každou roli 27

5.2.4 Role vyžadující oddělení povinností 28

5.3 Řídicí personál 28

5.3.1 Požadavky na kvalifikaci, zkušenost a vyklizení (?) 28

5.3.2 Procedury testů pozadí 28

5.3.3 Požadavky na vyškolení 28

5.3.4 Opakování školení - četnost a požadavky 28

5.3.5 Střídání úkolů – četnost a pořadí 28

5.3.6 Sankce za neoprávněné akce 28

5.3.7 Požadavky nezávislého dodavatele 28

5.3.8 Dokumentace dodávaná personálu 28

5.4 Procedury záznamu auditu 28

5.5 Archivace záznamů 28

5.6 Střídání klíčů 29

5.7 Náprava prozrazení a obnova po havárii 29

5.8 Ukončení CA nebo RA 29

5.8.1 Ukončení CA 29

5.8.2 Ukončení RA 29

6. Řízení technické bezpečnosti 29

6.1 Generování a instalace páru klíčů 29

6.1.1 Generování páru klíčů 29

6.1.2 Zabezpečení privátního klíče odběratele 29

6.1.3 Dodání veřejného klíče vydavateli certifikátu 30

6.1.4 Dodání veřejného klíče z CA spoléhajícím stranám 30

6.1.5 Velikosti klíčů 30

6.1.6 Generování parametrů veřejného klíče a kontrola kvality 30

6.1.7 Účely použití klíčů 30

6.2 Ochrana privátního klíče a řízení techniky kryptografického modulu 30

6.2.1 Standardy a ovládání kryptografického modulu 30

6.3 Další hlediska správy páru klíčů 31

6.3.1 Archivace veřejných klíčů 31

6.3.2 Doba funkčnosti certifikátu a doba použití páru klíčů 31

6.4 Aktivační data 31

6.5 Řízení počítačové bezpečnosti 31

6.6 Řízení technického životního cyklu 31

6.7 Řízení bezpečnosti sítě 31

6.8 Použití časových razítek 31

7. Profily certifikátů, CRL a OSCP 31

7.1 Profil certifikátu 32

7.1.1 Číslo verze / čísla verzí 32

7.1.2 Rozšiřující údaje certifikátu 32

7.1.3 Algoritmus identifikátorů objektu 33

7.1.4 Tvary jmen / názvů 33

7.1.5 Omezení jmen / názvů 33

7.1.6 Identifikátor objektu zásad certifikátu 33

7.1.7 Použití rozšíření omezení zásad. 33

7.1.8 Syntaxe a sémantika kvalifikátorů zásad 33

7.2 Profil CRL 33

7.2.1 Čísla verzí 33

7.2.2 CRL a jeho rozšířené položky 33

7.3 Profil OCSP 33

7.3.1 Čísla verzí 33

7.3.2 Rozšíření OCSP 33

8. Audit dodržování a další hodnocení 33

8.1 Četnost nebo podmínky hodnocení 34

8.2 Totožnost a kvalifikace poradce 34

8.3 Vztah poradce k hodnocené entitě 34

8.4 Hodnocená témata 34

8.5 Akce k nápravě zjištěných nedostatků 35

8.6 Sdělování výsledků 35

9. Ostatní provozní a právní záležitosti 35

9.1 Poplatky 35

9.2 Finanční odpovědnost 35

9.2.1 Krytí pojištěním 35

9.2.2 Ostatní aktiva 35

9.2.3 Pojištění nebo záruční krytí pro koncové entity 35

9.3 Důvěrnost obchodních informací 36

9.3.1 Rozsah důvěrných imformací 36

9.4 Ochrana osobních údajů 36

9.4.1 Plán ochrany soukromí 36

9.4.2 Údaje považované za soukromé 36

9.4.3 Údaje nepovažované za soukromé 36

9.4.4 Odpovědnost za ochranu soukromých údajů 36

9.4.5 Upozornění a souhlas k použití soukromých údajů 36

9.4.6 Zveřejnění podle justičních nebo správních procesů 36

9.4.7 Ostatní podmínky uvolnění informací 36

9.5 Práva intelektuálního vlastnictví 36

9.5.1 Vlastnictví a licence 37

9.5.2 Značka 37

9.5.3 Dokumenty 37

9.5.4 Kód 37

9.5.5 Certifikáty, kořenové certifikáty 37

9.6 Reprezentace a garance 37

9.7 Dementi garancí 37

9.8 Omezení odpovědnosti 38

9.9 Nezapojené osoby 38

9.10 Odpovědnost mezi Členy 38

9.11 Odškodnění 38

9.12 Lhůta a ukončení 38

9.12.1 Lhůta 38

9.12.2 Ukončení 38

9.12.3 Účinek ukončení a přežití 38

9.13 Individuální oznámení a komunikace s účastníky 38

9.14 Změny 38

9.15 Opatření k řešení sporů 39

9.16 Nadřazený zákon 39

9.17 Shoda s aplikovatelným právem 39

9.18 Zákon o digitálním podpisu 39

9.19 Zákon o ochraně soukromí 39

9.20 Právní proces pro vnější fóra 39

9.21 Různá ustanovení 39

9.21.1 Celková dohoda 39

9.21.2 Přiřazení 40

9.21.3 Oddělitelnost 40

9.21.4 Vynucení (poplatky právnímu zástupci a zřeknutí se práv) 40

9.21.5 Force majeure [vyšší moc] 40

## 1. Úvod

### 1.1 Přehled

Tento dokument je Přehled postupů certifikace (Certification Practise Statement, CPS) CAcertu, komunitní certifikační autority (CA). Popisuje pravidla a procedury, které používá CAcert pro provoz své CA a platí pro všechny účastnící se PKI, včetně zaručovatelů, členů a samotné CAcert.

### 1.2 Název a identifikace dokumentu

Tento dokument je Přehled postupů certifikace (CPS) CAcert. CPS zároveň plní roli Zásad certifikátů (Certificate Policy, CP)

* Tento dokument je COD6 podle číslovacího schématu oficiálních dokumentů CAcert (CAcert Official Documents, COD).
* Dokument je strukturován podle Chokhani a kol., [RFC3647](http://www.ietf.org/rfc/rfc3647.txt), [kapitola 4](http://tools.ietf.org/html/rfc3647#section-4). Všechna záhlaví jsou odvozena odtamtud.
* Byl upraven a revidován (nebo bude revidován), aby vyhověl nebo i překročil kritéria *Certificate Authority Review Checklist* od *Davida E, Rosse* („DRC“) a zásad CA patřící Nadaci Mozilla.
* Číslo OID (ID objektu) přiřazené tomuto dokumentu: 1.3.6.1.4.1.18506.4.4.x (x = schválená verze) ([iana.org](http://www.iana.org/assignments/enterprise-numbers))
* © CAcert Inc. 2006-2009.
* Starší poznámky napsal Christian Barmala v dokumentu umístěném pod licenci GNU pro volné dokumenty a pod copyright FSF. Avšak to koliduje s řídicími ustanoveními Konfigurace-řídicí specifikace (Configuration-Control Specification, CCS [COD2]) ohledně kritérií auditu.

CPS je autoritativní dokument, který řídí jiné dokumenty kromě těch, kde je to výslovně zamítnuto. Viz též 1.5.1 Organizace spravující dokument.

### 1.3 Kdo se podílí na infrastruktuře veřejných klíčů (PKI)

Certifikační autorita je legálně provozována sdružením CAcert Incorporated, registrovaným roku 2002 v Novém Jižním Walesu v Austrálii, v zastoupení širší Komunity členů CAcert. Podrobnosti o sdružení jsou na [CAcert wiki](http://wiki.cacert.org/wiki/CAcertIncorporated).

CAcert je Komunita tvořená Členy, kteří souhlasí s Dohodou komunity CAcert ([CAcert Community Agreement](http://www.cacert.org/policy/CAcertCommunityAgreement.php), CCA). Po technické stránce je CA provozována Komunitou pod řízením Výboru CAcert Incorporated. (Členové Komunity: nezaměňovat se *Členy sdružení*, o kterých se tento dokument nikde dále nezmiňuje.)

#### 1.3.1 Certifikační autority

Podle současného (tohoto) CPS nevydává CAcert certifikáty vnějším zprostředkujícím CA.

#### 1.3.2 Registrační autority

Registrační autority (RA) se řídí Zásadami zaručování (Assurance Policy, AP [[COD13](http://www.cacert.org/policy/AssurancePolicy.php)]).

#### 1.3.3 Odběratelé

CAcert vydává certifikáty pouze Členům. Tito Členové se pak stávají odběrateli.

#### 1.3.4 Spoléhající strany

Spoléhající strana je Člen, který souhlasil s Dohodou komunity CAcert (CCA [[COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php)]), a který používáním certifikátu CAcert činí rozhodnutí na základě toho certifikátu.

#### 1.3.5 Ostatní účastníci

**Členové.** Členství v Komunitě je definováno v Dohodě komunity CAcert (CCA, [[COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php)]).Pouze Členové se mohou SPOLEHNOUT nebo se stát odběrateli. Členství je bezplatné.

**Arbitr.** Starší a zkušený Člen komunity CAcert, který řeší spory mezi Členy, včetně sporů o spolehlivost certifikátů, podle Zásad řešení sporů (Dispute Resolution Policy, DRP, [[COD7](http://www.cacert.org/policy/DisputeResolutionPolicy.php)]).

**Prodejce.** Dodavatel softwaru, který integruje certifikáty CAcert do svého softwaru, mají „proxy“ roli Spoléhajících stran; jsou předmětem jiné licence.

**Nezapojené osoby** (NRP). Jsou to uživatelé webových prohlížečů a podobného softwaru, kteří nejsou seznámeni s certifikáty CAcert, které mohou použít, ani s variantami použití. Jejich vztah k Cacertu je popsán dokumentem „Nezapojené osoby – zřeknutí a licence (Non-Related Persons – Disclaimer and License, NRP-DaL [COD4]). Žádná jiná práva ani vztahy nejsou předpokládána ani nabízena.

### 1.4 Použití certifikátů

CAcert slouží jako vydavatel certifikátů pro jednotlivce, podniky, vlády, veřejně prospěšné společnosti, sdružení, církve, školy, nevládní organizace a jiné skupiny. Certifikáty CAcert jsou zamýšleny pro nízkonákladové komunitní aplikace, zvláště tam, kde se mohou dobrovolníci stát zaručovateli a pomáhat CAcertu s pomocí komunitě.

Typy certifikátů a jejich příslušné a odpovídající aplikace jsou definovány v §1.4.1. Zakázané aplikace jsou definovány v §1.4.2. Použití pro odborníky může být dohodnuto smlouvou nebo je umístěno do zvláštního prostředí, jak je popsáno v §1.4.4. Nespolehlivé aplikace jsou předmětem §1.4.3 a rizika, odpovědnosti a závazky řeší §9.

| *Typ* | *Správná použití certifikátů* |
| --- | --- |
| **Obecný** | **Protokol** | **Popis** | **Poznámky** |
| Server | TLS | šifrování webového serveru | Umožňuje zašifrování |
| vestavěný | vestavěná identifikace serveru | E-mailové servery,IM servery |
| Klient | S/MIME | šifrování e-mailů | „Digitální podpisy“ používané v S/MIME nejsou právně platné podpisy osob, ale zato umožňují šifrovací režim S/MIME |
| TLS | identifikace klienta | Uzly musí být bezpečné |
| TLS | webové aplikaces podpisem | Pouze identifikace certifikátem, viz §1.4.3. |
| „Digitální podepisování“ | dokumenty podepsané člověkem | Pouze uvnitř větší aplikace a s pravidly jako jsou zvláštní zásady, dohodnuto ve smlouvě, atd.- viz §1.4.4. |
| Kód | Authenticode, ElfSign, Java | podepisování kódu | Podpisy na balíčcích jsou důkazem jejich členství a oznámením totožnosti |
| PGP | OpenPGP | podepisování klíče | Podpisy na klíčích Členů jsou důkazem jejich členství a oznámením totožnosti |
| Speciální | 30.9.509 | OCSP, časové razítkování | Dostupné pouze správcům systémů CAcert, jak je stanoveno v Zásadách bezpečnosti |

Tabulka 1.4. Typy certifikátů

#### 1.4.1 Správná použití certifikátů

Všeobecná použití.

* Serverové certifikáty CAcert lze použít na webových serverech k zapnutí ochrany šifrováním. Vhodné aplikace mohou být webmail a diskusní (chat) fóra.
* Serverové certifikáty CAcert lze použít k zapnutí šifrování SSL/TLS ve vestavěných protokolech, například mailových serverech nebo IM-serverech. [IM = Instant Messaging, okamžité posílání zpráv – bez zpoždění e-mailů.]
* Klientské certifikáty CAcert lze použít k zapnutí ochrany e-mailů šifrováním. (Viz §1.4.3 – varování ohledně podpisů.)
* Klientské certifikáty CAcert lze použít na webových serverech k náhradě identifikace/přihlášení heslem za přihlášení certifikátem.
* Klíče OpenPGP s podpisy CAcert lze použít k šifrování a podepisování souborů a e-mailů, pokud se používá software kompatibilní s OpenPGP.
* Klientské certifikáty CAcert lze použít pro identifikaci ve webových aplikacích.
* Certifikáty CAcert pro podepisování kódu lze použít k podpisu kódu pro distribuci jiným osobám.
* Časová razítka lze použít pro přidání záznamu o čase k digitálním dokumentům.

#### 1.4.2 Zakázaná použití certifikátů

Certifikáty CAcert nejsou navrženy, zamýšleny ani schváleny pro tyto aplikace:

* Použití nebo další prodej pro řídicí zařízení pracující za nebezpečných okolností, nebo pro použití vyžadující samoopravnou činnost (překonání chyb), například v provozu jaderných zařízení, letecké navigaci nebo leteckých komunikačních systémech, řízení vzdušného provozu, řízení zbraňových systémů, tam, kde selhání může přímo způsobit smrt, zranění osob nebo závažné poškození prostředí [ekologickou katastrofu].

#### 1.4.3 Nespolehlivé aplikace

Certifikáty CAcert nejsou navrženy ani zamýšleny k použití v následujících aplikacích a nemohou pro ně být dostatečně spolehlivé:

* **Podepisování uvnitř protokolů.** Digitální podpisy vytvořené certifikáty CAcert nenesou ŽÁDNÝ právní nebo lidský význam. Viz §9.15.1. Zvláště protokoly jako S/MIME běžně automaticky aplikují digitální podpisy jako část potřebnou pro protokol. Účel kryptografického podpisu v S/MIME a podobných protokolech je (standardně) přísně omezen na účely zabezpečení protokolu:
	+ poskytnout určité potvrzení, že se používá známý certifikát,
	+ umožnění šifrování,
	+ zajištění celistvosti e-mailové zprávy během přenosu.
* **Nepopiratelné** (non-repudiation) **aplikace.** Z používání certifikátů CAcert nemá být vyvozována nepopiratelnost. Namísto toho mohou certifikáty poskytnout podporu nebo důkaz o akcích, avšak takový důkaz lze testovat v jakémkoli sporu.
[*Nepopiratelnost je schopnost prokázat zpětně jednání či událost tak, aby dané jednání či událost nemohly být následně popřeny.*]
* **Aplikace elektronického obchodování (E-komerce).** Finanční transakce nebo platby, nebo e-komerce vysokých cen.
* Používání anonymních certifikátů (kořenových třídy 1 nebo členských zprostředkujících) v jakékoli aplikaci vyžadující nebo očekávající prokázání totožnosti.

#### 1.4.4 Omezené použití certifikátů

Podle smlouvy nebo ve specifickém prostředí (například uvnitř společnosti/podniku) mají Členové CAcert povoleno používat certifikáty pro vyšší bezpečnost, přizpůsobené nebo experimentální aplikace. Avšak takové použití je omezeno na zmíněné entity a tyto entity přebírají plnou odpovědnost za jakoukoli škodu nebo hmotnou odpovědnost způsobenou takovým použitím.

**Digitálně podepisující aplikace.** Klientské certifikáty CAcert mohou používat zaručení Členové v aplikacích, které poskytují nebo podporují podpis dokumentů člověkem (zde: „digitální podpis“). Ten musí být částí širšího rámce a sady pravidel. Použití a důvěra (spolehnutí) musí být dokumentována buď zvláštními zásadami CAcert pro digitální podepisování, nebo jiným vnějším režimem dohodnutým stranami.

#### 1.4.5 Kořenové certifikáty a jména (názvy)

**Pojmenované certifikáty.** Členům, kteří jsou zaručeni, lze vydávat certifikáty obsahující jejich ověřená jména. V této roli CAcert řídí a podporuje síť zaručovatelů, kteří ověřují totožnost Členů. Všechna jména jsou ověřena, ať zaručením nebo jinou metodou definovanou zásadami (srovnej Organizace).

**Anonymní certifikáty.** Členové mohou obdržet certifikáty, které jsou anonymní, což je definováno jako certifikáty bez jména, nebo se společným názvem například „Community Member“ (Člen komunity), „WoT user“ (uživatel webu důvěry) atd. Jejich místo je někde mezi certifikáty se jménem a certifikáty podepsanými samy sebou. Obsahují pořadová čísla, která jsou zaručeně vysledovatelná cestou sporu Člena, avšak jejich spolehlivost není definována. CAcert v této roli poskytuje infrastrukturu, chrání Člena před zvládnutím pracného a zmateného procesu, který by musel podstoupit, aby získal vyrobené certifikáty.

**Pseudonymní certifikáty.** CAcert v současné době nevydává pseudonymní certifikáty, kde by jméno zvolil Člen a nebylo by ověřitelné podle žádných dokumentů.

**„Pokročilé“ certifikáty.** Dosud nezaručení Členové nemají dovoleno vytvářet pokročilé druhy certifikátů, jako skupinové (wildcard) nebo obsahující alternativní názvy (SAN).

**Kořenové certifikáty.** Jejich přehled následuje. Tyto certifikáty jsou v procesu auditu a budou dodány prodejcům prostřednictvím (nejvyšší úrovně) kořenového certifikátu.

* **Kořenový certifikát (nejvyšší úrovně).** Používá se jen k on-line podpisům zprostředkujících certifikátů CAcert. Tento kořenový certifikát je uložen offline (není přístupný z Internetu).
* **Členský zprostředkující certifikát (SubRoot).** Určen novým, dosud nezaručeným Členům (mají určitá omezení). Není definována spolehlivost. (Nahrazují kořenový certifikát třídy 1, odpovídají typu „Ověření domény“ - DV.)
* **Zaručené zprostředkující.** Dostupné pouze zaručeným Členům – jednotlivcům, určené k podpisu certifikátů se jmény. Vhodné pro Spolehnutí dle těchto i jiných zásad. Ověření je přibližně typu „Ověření jednotlivce“ (IV).
* **Organizační zprostředkující.** Dostupné pouze Členům – zaručeným organizacím. Vhodné pro Spolehnutí dle těchto i jiných zásad. Ověření je přibližně typu „Ověření organizace“ (OV).

|  | *Úroveň zaručení* |  |
| --- | --- | --- |
|  | Členové +) | Zaručení členové | Zaručovatelé |  |
| *Třída kořenu* | Anonymní | Jméno | Anonymní | Jméno | Jméno+anonymní | *Poznámky* |
| Kořenový nejvyšší úrovně |  |  |  |  |  | Podepisuje pouze ostatní zprostředkující certifikáty CAcert |
| Členský zprostředku-jící |  |  |  |  |  | +) Pro členy pouze se základní kontrolou v § 4.2.2 (spolehlivost není definována) |
| Zaručený zprostředku-jící |  |  |  |  |  | Jen pro zaručené Členy. Plná spolehlivost. |
| Organizační zprostředku-jící |  |  |  |  |  | Zaručené organizace – Členové. Plná spolehlivost. |
| Doba platnosti certifikátů | 6 měsíců | 24 měsíců |  |
| Typy | Klient, server | Skupinový (wildcard), SAN | Podepisování kódu | (Včetně typů vlevo.) |

Tabulka 1.4.5b Certifikáty pod auditovanými kořeny

|  |  |  |
| --- | --- | --- |
|  | ***Úroveň zaručení*** |  |
|  | **Členové** | **Zaručení Členové** |  |
| ***Třída kořenového certifikátu*** | **Anonymní** | Jméno | Anonymní | **Jméno** | *Poznámky* |
| Třída **1** |  |  |  |  | Pro všechny Členy, spolehlivost nedefinována. |
| Třída **3** |  |  |  |  | Jen pro zaručené Členy, plná spolehlivost. |
| **Doba platnosti certifikátů** | 6 měsíců | 24 měsíců |  |
| Dostupné typy | Pouze jednoduchý | Skupinový (wildcard), SAN |

Tabulka 1.4.5 Certifikáty pod starým kořenovým – audit neprošel

**Staré kořenové certifikáty.** Jejich rozložení je v tabulce 1.4.5 a popis dále. Tyto kořenové certifikáty nesplňují audit a budou používány, jen tam, kde nové kořenové certifikáty neslouží:

* (staré) **Kořenové certifikáty třídy 1.** Používají se především pro certifikáty bez jména a u dosud nezaručených Členů. Pro kompatibilitu je mohou používat i zaručení Členové.
* (staré) **Kořenové certifikáty třídy 3 (zprostředkující).** Používají se především pro certifikáty obsahující jména zaručených členů. Podepsány kořenovým certifikátem třídy 1. Členové se mohou rozhodnout, zda budou spoléhat na tyto certifikáty pro zaručené Členy, výběrem zprostředkujícího certifikátu třídy 3 jako kotvy důvěry pro zaručené Členy.

### 1.5 Správa zásad

Viz 1.2 Název a identifikace dokumentu, kde je uveden všeobecný rozsah platnosti tohoto dokumentu.

#### 1.5.1 Organizace spravující dokument

Tento dokument spravuje skupina pro zásady v komunitě CAcert podle Zásad ohledně zásad (Policy on Policy, [COD1](http://www.cacert.org/policy/PolicyOnPolicy.php)).

#### 1.5.2 Kontaktní osoba

Pro dotazy k tomuto dokumentu:

* Připojte se ke skupině pro zásady v diskusním fóru na [lists.cacert.org](http://lists.cacert.org/mailman/listinfo).
* Pošlete e-mail na support(zavináč)cacert.org
* IRC: irc.cacert.org #CAcert (ssl port 7000, non-ssl port 6667)

#### 1.5.3 Osoba určující vhodnost dokumentu CPS jako zásad

Tento dokument (CPS) a ostatní dokumenty zásad jsou spravovány skupinou pro zásady (policy group), což je skupina Členů Komunity na fóru zásad. Viz výše – diskusní fóra.

#### 1.5.4 Schvalovací procedury CPS

Dokument CPS je řízen a aktualizován podle Zásad ohledně zásad (Policy on Policy, [COD1](http://www.cacert.org/policy/PolicyOnPolicy.php)), které jsou částí Konfigurace-řídicí specifikace (Configuration-Control Specification, COD2).

Ve stručnosti: fórum pro zásady připravuje a diskutuje. Po poslední výzvě dostává dokument status KONCEPT (DRAFT) na stanovenou dobu. Nepřijde-li po tuto dobu žádná připomínka / doplněk / návrh, získává dokument status ZÁSADY (POLICY). Proces je modelován podle některých vlastností procesu RFC (Request For Comment, výzva k připomínkám), používaného v IETF (Internet Engineering Task Force, komando pro výstavbu Internetu).

#### 1.5.5 Aktualizace CPS

Probíhá stejně, jak uvedeno výše.

### 1.6 Definice a zkratky

**Certifikát (Certificate)**Certifikát je část kryptografických údajů používaných k ověření určitých prohlášení, zejména ohledně totožnosti a členství.

**CAcert (CAcert)**CAcert je komunitní certifikační autorita, jak je definována pod §1.2 Identifikace.

**Člen (Member)**Každý, kdo souhlasí s Dohodou kmunity CAcert (CAcert Community Agreement, CCA - [COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php)). To si obecně vyžaduje mít účet registrovaný u CAcert a používat data, programy a služby CAcert. Člen může být jednotlivec („fyzická osoba“), nebo organizace (také „právnická osoba“).

**Komunita (Community)**Skupina Členů, kteří souhlasí s CCA ([COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php)) nebo s rovnocennými dohodami.

**Nezaručený Člen (Unassured Member)**Člen, který dosud nebyl zaručen.

**Odběratel** (abonent) **(Subscriber)**
Člen, který si vyžádá a obdrží certifikát.

**Zaručený Člen (Assured Member)**Člen, jehož totožnost byla úspěšně ověřena zaručovateli nebo jinou metodou schválenou podle Zásad zaručování (Assurance Policy).

**Zaručovatel (Assurer)**Zaručený Člen, který je oprávněn ověřovat totožnost jiných Členů podle Zásad zaručování (AP, COD13)

**Jméno / Název (Name)**Definováno v Zásadách zaručování (AP, [COD13](http://www.cacert.org/policy/AssurancePolicy.php)). Popisuje jméno [jednotlivce] nebo název [organizace] Člena ověřeného procesem zaručení.

**Správce organizace (Organisation Administrator)** („O-admin“)
Zaručovatel, který je oprávněn jednat jménem organizace. Správce organizace je organizací oprávněn zaručit totožnost jiných uživatelů v organizaci.

**Zaručovatel organizace (Organisation Assurer)**Zaručovatel, který je oprávněn provádět zaručování v organizacích.

**Nezapojené osoby (Non-Related Persons, „NRP“)**Jsou to obvykle uživatelé webových prohlížečů nebo podobného softwaru. NRP nejsou obecně seznámeny s CAcert nebo s certifikáty, které mohou používat, ani s možnostmi jejich použití. Nemají dovoleno SPOLÉHAT, ale mohou POUŽÍVAT podle licence pro nezapojené osoby (NRP-DaL [NRP-Dementi a Licence], [COD4](http://www.cacert.org/policy/NRPDisclaimerAndLicence.php)).

**Spolehlivost (Reliance)**Průmyslový termín označující akt rozhodnutí, včetně převzetí rizika. Takové rozhodnutí zčásti nebo úplně závisí na obsahu certifikátu.

**Spoléhající strana (Relying Party)**Průmyslový termín označující toho, kdo spoléhá (rozhoduje nebo nese rizika) zčásti nebo úplně na certifikát.

**Pojmenování odbětatele (Subscriber Naming)**Termín používaný tímto CPS k popisu všech pojmenovaných dat v certifikátu. Přibližně odpovídá průmyslovým termínům jako „Pojmenování předmětu“ nebo „Rozlišující název“, které zde nejsou použity.

**Ověření (Verification)**Průmyslový termín označující akt kontroly a řízení přesnosti a užitečnosti(?) jednotlivého prohlášení.

**Vyhodnocení (Validation)**Průmyslový termín označující proces inspekce a ověření údajů a vedlejších prohlášení na pozadí prohlášení.

**Použití (Usage)**Událost povolení certifikátu účastnit se protokolu, jak rozhodne nebo použije uživatelský software.

**Spoléhající strana CAcert (CAcert Relying Party)**Členové CAcert, kteří rozhodují částečně nebo plně spoléhajíce na certifikát vydaný CAcert. Pouze Členové CAcert smí Spoléhat na certifikáty CAcert, podle Dohody komunity CAcert (CCA).

**Prodejci (Vendors)**Nečlenové, kteří distribuují kořenový a/nebo zprostředkující certifikát CAcert jakýmkoli způsobem, včetně (ale nejen) dodáváním těchto certifikátů se svými produkty, jako prohlížeči, e-mailovými klienty nebo servery. Prodejci podléhají zvláštní licenci.

**Konfigurace-řídicí specifikace (Configuration-Control Specification)** („CCS“)Kritéria auditu, která řídí toto CPS (Certification Practise Statement, Přehled postupu specifikace). CCS je dokumentována v COD2. CCS je také dokumentem řízeným CCS, tedy sám sebou.

## 2. Odpovědnost za zveřejnění a úložiště

### 2.1 Úložiště

CAcert neprovozuje žádná úložiště ve smyslu vyhledávání údajů jiných než týkajících se certifikátů pro širokou veřejnost.

Podle Zásad zaručování (Assurance Policy, [COD13](http://www.cacert.org/policy/AssurancePolicy.php)) existují pro Členy prostředky k hledání, získávání a ověřování určitých údajů o nich samých a ostatních.

### 2.2 Zveřejňování certifikačních údajů

CAcert publikuje:

* Úložiště CRL (Certificate Revocation List, seznam odvolaných certifikátů). V provozu je odpovídač OCSP.
* Kořenový certifikát a zprostředkující certifikáty.

CAcert nezveřejňuje výslovně informace o vydaných certifikátech. Avšak kvůli účelům certifikátů a povaze jmen / názvů a e-mailových adres, která je v podstatě veřejná, předpokládá, že všechny údaje z certifikátů jsou veřejné a mohou být zveřejněny po vydání certifikátu a jeho doručení Členovi.

### 2.3 Doba nebo četnost publikace

Kořenový certifikát, zprostředkující certifikát a seznam odvolaných certifikátů (CRL) jsou po svém vydání veřejně přístupné.

### 2.4 Řízení přístupu k úložištím

Žádné podmínky.

## 3. Identifikace a ověření pravosti

### 3.1 Pojmenování

#### 3.1.1 Typy jmen / názvů

**Klientské certifikáty.** Jméno/název odběratele sestává z:

* subjectAltName=
Jedné či více ověřených e-mailových adres odběratele ve formátu rfc822Name.
* EmailAddress=
Jedné či více ověřených e-mailových adres odběratele. To je podle RFC5280 [4.2.1.6](http://tools.ietf.org/html/rfc5280#section-4.2.1.6) zastaralé a má být vyřazeno. Obsahuje také SHA1 haš náhodného čísla, jestliže člen zvolil SSO (Single Sign-On, jednotné přihlášení) během podání žádosti o podpis certifikátu (CSR).
* CN=
Obecného jména / obecného názvu – hodnotu tvoří:
	+ Text „CAcert WoT Member“ pro anonymní certifikáty.
	+ Jméno odběratele – člena jednotlivce, je-li zaručen podle AP (Zásad zaručování, [v současnosti 50 a více body zaručení].
	+ Název zvolený organizací – u členů - organizací zaručených podle OAP (Zásad zaručování organizací).

**Individuální serverové certifikáty.** Název odběratele se skládá z údajů:

* CN=
Obecné jméno / obecný název – hodnotu tvoří doménový název serveru v doméně, kde je Člen majitelem/správcem.
* subjectAltName=
Další názvy serveru, pro nějž je Člen majitelem/správcem domény, lze přidat, aby umožnily certifikátu sloužit pro několik domén provozovaných na téže IP-adrese.
* Všechna ostatní pole jsou nepovinná, buď musí mít hodnotu CN, nebo jsou prázdná.

**Certifikáty pro organizace.** Totéž, co výše, a tyto další údaje:

* OU=
název organizační jednotky (organizationalUnitName, nastaven správcem organizace [O-admin], musí ověřit O-admin).
* O=
název organizace (organizationName) je pevně daný název organizace.
* L=
umístění (localityName) – [sídlo organizace / pobočky].
* ST=
jméno státu nebo provincie [správní územní jednotky, např. kraj] (stateOrProvinceName).
* C=
jméno státu/země (countryName).
* contact=
e-mailová adresa kontaktní osoby.

Kromě OU a CN jsou pole vybírána z účtu Člena a jsou taková, jak byla ověřena procesem Zaručení organizace. Další údaje o odběrateli, i když jsou zjištěny a/nebo se uchovávají, nejsou v certifikátu zapsány.

#### 3.1.2 Je nutné, aby jména (názvy) měly význam

Každé jméno/název Člena (pole CN=) je zaručen(o) podle Zásad zaručování ([COD13](http://www.cacert.org/policy/AssurancePolicy.php)) nebo podzásad (např. Zásady zaručování organizací). Význam a varianty viz tyto dokumenty.

Anonymní certifikáty mají všechny tentýž obecný název v poli subject. Viz §1.4.5.

E-mailové adresy se ověřují podle §4.2.2.

#### 3.1.3 Anonymita nebo pseudonymita odběratelů

Viz §1.4.5.

#### 3.1.4 Pravidla pro interpretaci různých tvarů jmen

Interpretace jmen se řídí Zásadami zaručování, je spravována pomocí účtu uživatele a je předmětem změn, které může provést arbitr. Změny interpretace arbitráží podezřelé jako podvod (například „phishing“) se mohou rychleji než zásady dostat do plně dokumentovaných pravidel.

#### 3.1.5 Jedinečnost jmen

Jedinečnost jmen/názvů v certifikátech není zaručena. Každý certifikát má jedinečné pořadové číslo (serial number), které ukazuje na jediný účet a tedy patří jednomu určitému Členovi. Viz Prohlášení o zaručení v Zásadách zaručování ([COD13](http://www.cacert.org/policy/AssurancePolicy.php)).

Doména s určitým názvem a konkrétní e-mailová adresa mohou být registrovány pouze jednomu Členovi.

#### 3.1.6 Uznání, ověření a úloha obchodních známek (trademarks)

Zásady zaručování organizací (Organization Assurance Policy, [COD11](http://www.cacert.org/policy/OrganisationAssurancePolicy.php)) řídí záležitosti jako obchodní známky všude, kde je to na místě. Ohledně obchodní známky může vzniknout spor. Viz §9.13.

#### 3.1.7 Mezinárodní názvy domén

Certifikáty obsahující mezinárodní názvy domén (International Domain Names, IDN), obsahující prefix ACE (ASCII Compatible Encoding [kódování do ASCII], [RFC3490 sekce 5](http://www.ietf.org/rfc/rfc3490#section-5)), budou použity pouze pro domény vyhovující aspoň jedné z těchto podmínek:

* Registrátor domén nejvyšší úrovně (Top Level Domains, TLD) určený pro doménu má zásady, které obsahují přijatelné prostředky k zabránění stavu, kdy by byly dvě stejně psané domény registrovány různým entitám.
* Názvy domén obsahují jen kódové kombinace z jedné znakové sady unicode, vyjma sady „Common“, dále jsou v nich povolené ASCII číslice ['0'-'9', hex. kód 0030-0039] a pomlčka '-' [hex. kód 002D].

E-mailové adresy, obsahující v doménové části (za '@') názvy IDN, musí také vyhovovat jedné z výše uvedených podmínek.

Následuje seznam přípustných TLD registrátorů:

|  |  |  |
| --- | --- | --- |
| .ac | [Rejstřík](http://www.nic.ac/) | [Zásady](http://www.nic.ac/pdf/AC-IDN-Policy.pdf)  |
| .ar | [Rejstřík](http://www.nic.ar/) | [Zásady](http://www.nic.ar/616.html) |
| .at | [Rejstřík](http://www.nic.at/) | [Zásady](http://www.nic.at/en/service/legal_information/registration_guidelines/) ([seznam znaků](http://www.nic.at/en/service/technical_information/idn/charset_converter/)) |
| .biz | [Rejstřík](http://www.neustarregistry.biz/) | [Zásady](http://www.neustarregistry.biz/products/idns) |
| .br | [Rejstřík](http://registro.br/) | [Zásady](http://registro.br/faq/faq6.html) |
| .cat | [Rejstřík](http://www.domini.cat/) | [Zásady](http://www.domini.cat/normativa/en_normativa_registre.html) |
| .ch | [Rejstřík](http://www.switch.ch/id/) | [Zásady](http://www.switch.ch/id/terms/agb.html#anhang1) |
| .cl | [Rejstřík](http://www.nic.cl/) | [Zásady](http://www.nic.cl/CL-IDN-policy.html) |
| .cn | [Rejstřík](http://www.cnnic.net.cn/) | [Zásady](http://www.faqs.org/rfcs/rfc3743.html) (Směrnice JET) |
| .de | [Rejstřík](http://www.denic.de/) | [Zásady](http://www.denic.de/en/richtlinien.html) |
| .dk | [Rejstřík](http://www.dk-hostmaster.dk/) | [Zásady](http://www.dk-hostmaster.dk/index.php?id=151) |
| .es | [Rejstřík](https://www.nic.es/) | [Zásady](https://www.nic.es/media/2008-12/1228818323935.pdf) |
| .fi | [Rejstřík](http://www.ficora.fi/) | [Zásady](http://www.ficora.fi/en/index/palvelut/fiverkkotunnukset/aakkostenkaytto.html) |
| .gr | [Rejstřík](https://grweb.ics.forth.gr/english/index.html) | [Zásady](https://grweb.ics.forth.gr/english/ENCharacterTable1.jsp) |
| .hu | [Rejstřík](http://www.domain.hu/domain/) | [Zásady](http://www.domain.hu/domain/English/szabalyzat.html) (sekce 2.1.2) |
| .info | [Rejstřík](http://www.afilias.info/) | [Zásady](http://www.afilias.info/register/idn/) |
| .io | [Rejstřík](http://www.nic.io/) | [Zásady](http://www.nic.io/IO-IDN-Policy.pdf) |
| .ir | [Rejstřík](https://www.nic.ir/) | [Zásady](https://www.nic.ir/IDN) |
| .is | [Rejstřík](http://www.isnic.is/) | [Zásady](http://www.isnic.is/english/domain/rules.php) |
| .jp | [Rejstřík](http://jprs.co.jp/) | [Zásady](http://www.iana.org/assignments/idn/jp-japanese.html) |
| .kr | [Rejstřík](http://domain.nic.or.kr/) | [Zásady](http://www.faqs.org/rfcs/rfc3743.html) (Směrnice JET) |
| .li | [Rejstřík](http://www.switch.ch/id/) | [Zásady](http://www.switch.ch/id/terms/agb.html#anhang1) (spravováno rejstříkem .ch) |
| .lt | [Rejstřík](http://www.domreg.lt/public?pg=&sp=&loc=en) | [Zásady](http://www.domreg.lt/public?pg=8A7FB6&sp=idn&loc=en) ([seznam znaků](http://www.domreg.lt/static/doc/public/idn_symbols-en.pdf)) |
| .museum | [Rejstřík](http://about.museum/) | [Zásady](http://about.museum/idn/idnpolicy.html) |
| .no | [Rejstřík](http://www.norid.no/) | [Zásady](http://www.norid.no/domeneregistrering/veiviser.en.html) (sekce 4) |
| .org | [Rejstřík](http://www.pir.org/) | [Zásady](http://pir.org/PDFs/ORG-Extended-Characters-22-Jan-07.pdf) |
| .pl | [Rejstřík](http://www.nask.pl/) | [Zásady](http://www.dns.pl/IDN/idn-registration-policy.txt) |
| .pr | [Rejstřík](https://www.nic.pr/) | [Zásady](https://www.nic.pr/idn_rules.asp) |
| .se | [Rejstřík](http://www.nic-se.se/) | [Zásady](http://www.iis.se/en/domaner/internationaliserad-doman-idn/) ([seznam znaků](http://www.iis.se/docs/teckentabell-03.pdf)) |
| .sh | [Rejstřík](http://www.nic.sh/) | [Zásady](http://www.nic.sh/SH-IDN-Policy.pdf) |
| .th | [Rejstřík](http://www.thnic.or.th/) | [Zásady](http://www.iana.org/assignments/idn/th-thai.html) |
| .tm | [Rejstřík](http://www.nic.tm/) | [Zásady](http://www.nic.tm/TM-IDN-Policy.pdf) |
| .tw | [Rejstřík](http://www.twnic.net.tw/) | [Zásady](http://www.faqs.org/rfcs/rfc3743.html) (Směrnice JET) |
| .vn | [Rejstřík](http://www.vnnic.net.vn/) | [Zásady](http://www.vnnic.vn/english/5-6-300-2-2-04-20071115.htm) ([seznam znaků](http://vietunicode.sourceforge.net/tcvn6909.pdf)) |

Toto kritérium bude uplatněno na e-mailové adresy a názvy serverů pro všechny typy certifikátů.

Výbor CAcert Inc. je oprávněn v tomto seznamu přidat nebo odebrat přípustné registrátory TLD.

### 3.2 Počáteční ověření totožnosti

Ověření totožnosti se řídí Zásadami zaručování (Assurance Policy, COD13), na něž čtenáře odkazujeme. Následující text je jen stručný přehled (výtah).

#### 3.2.1 Metoda ověření vlastnictví privátního klíče

CAcert používá standardní průmyslové techniky důkazu vlastnictví privátního klíče.

U serverových certifikátů X.509 je ověřen starý digitální podpis žádosti o certifikát (CSR). U klientských certifikátů X.509 pro prohlížeče „Netscape“ používá SPKAC (Signed Public Key And Challenge) protokol výzva-odpověď (challenge-response) ke kontrole privátního klíče dynamicky. U klientských certifikátů X.509 pro prohlížeče „Explorer“ používá ActiveX protokol výzva-odpověď ke kontrole privátního klíče dynamicky.

#### 3.2.2 Určení totožnosti jednotlivce

**Dohoda.** Uživatel Internetu se stane Členem, když souhlasí s Dohodou komunity CAcert ([COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php)) a registruje si účet na webu, který je on-line. Během registračního procesu se Členové žádají, aby o sobě poskytli údaje:

* Platný a funkční e-mail.
* Celé jméno a datum narození tak, jak je uvedeno na dokladech totožnosti.
* Osobní údaje potřebné pouze k obnově hesla.

On-line účet zřizuje metodu identifikace pro všechny žádosti o službu, jako například o certifikáty.

**Zaručování.** Každý Člen je zaručován podle Zásad zaručování (Assurance Policy, AP, [COD13](http://www.cacert.org/policy/AssurancePolicy.php)).

**Certifikáty,** Člen může získat certifikáty různé úrovně v závislosti na celkovém počtu bodů zaručení, které obdržel. Viz §1.4.5. Viz tabulka 3.2b. Má-li člen už 50 a více bodů, stává se *zaručeným členem* a může si pak vyžadovat certifikáty se svým (zaručeným) jménem nebo jmény.

Tabulka 3.2.b – jak se body zaručení odrážejí v certifikátech

| **Bodů zaručení** | **Úroveň** | **Služba** | **Poznámky** |
| --- | --- | --- | --- |
| 0 | Nezaručený Člen | Anonymní | Certifikáty beze jmen, pod kořenem třídy 1. Omezená expirace 6 měsíců. |
| 1 - 49 | Nezaručený Člen | Anonymní | Certifikáty beze jmen, pod zprostředkujícím třídy 3. Omezená expirace 6 měsíců. |
| 50 - 99 | Zaručený Člen | Ověřený | Certifikáty s ověřeným jménem pro S/MIME, weby, digitální podpis e-mailů. Expirace 24 měsíců. |
| 100++ | Zaručovatel | Podepisování kódu | Vše co výše, navíc může vytvářet certifikáty pro podpis kódu. |

#### 3.2.3 Ověření totožnosti organizace

Ověřování organizací je převedeno ze Zásad zaručování do Zásad zaručování organizací ([COD11](http://www.cacert.org/policy/OrganisationAssurancePolicy.php)), na které čtenáře odkazujeme. Následující text je jen stručný přehled (výtah).

Organizace představují speciální výzvy. Cílem procesu zaručení organizace je umožnit, aby se název organizace mohl objevit v certifikátech. Proces silně závisí na procesech pro jednotlivce, popsaných výše.

Zaručování organizací dosahuje standardu uvedeného v Zásadách zaručování organizací (Organization Assurance Policy, OAP), stručně popsaných zde:

1. organizace existuje,
2. název organizace je správný a konzistentní,
3. podpisová práva: žadatel může podepisovat v zastoupení organizace, a
4. organizace souhlasila s články Dohody komunity CAcert ([COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php)) a je tedy předmětem arbitráže.

#### 3.2.4 Neověřené údaje odběratele

Všechny údaje v certifikátu jsou ověřené, viz Prohlášení spoléhající strany (Relying Party Statement), §4.5.2.

#### 3.2.5 Ověření autority

Oprávnění obdržet certifikát je založeno na následujícím:

**Adresy.**  Člen prohlašuje, že má oprávnění pro doménu nebo e-mailovou adresu, když přidává adresu, §4.1.2. (Ovládání [suverenita] je testována prostředky popsanými v §4.2.2.)

**Jednotlivci.** Oprávnění podílet se jako Člen je založeno na Dohodě komunity CAcert (CCA, [COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php)). Je vyžadováno zaručování pomocí podepsaných formulářů CAP.

**Organizace.** Oprávnění pro zaručení organizace se zakládá na formuláři COAP, podepsaném oprávněným zástupcem organizace. Oprávnění Správce organizace (O-admin) se také zakládá na formuláři COAP. Viz Zásady zaručování organizací.

#### 3.2.6 Kritérium pro součinnost

CAcert v současnosti nevydává certifikáty pro podřízené CA nebo pro jiné PKI. Jiné CA se mohou stát Členy a jsou pak předmětem týchž ustanovení spolehlivosti jako všichni Členové.

### 3.3 Žádosti o obnovení klíčů

Probíhají prostřednictvím účtu Člena.

### 3.4 Žádosti o odvolání certifikátů

Probíhají prostřednictvím účtu Člena. Ztratí-li Člen heslo, nebo v podobném případě, musí Člen napsat e-mail týmu podpory, který buď využije proces kladení otázek uložených pro případ ztráty hesla, nebo založí spor.

## 4. Provozní požadavky životního cyklu certifikátu

Všeobecný životní cyklus nového certifikátu pro člena jednotlivce (fyzickou osobu):

1. Člen dodá prohlášení ke své adrese (doména/e-mail)-
2. Systém otestuje adresu, zda skutečně patří Členovi.
3. Člen vytvoří pár klíčů – privátní a veřejný.
4. Člen předloží žádost o certifikát (CSR) s možnostmi, které si přeje (anonymní certifikát, jednotný podpis [SSO], kořenový certifikát).
5. Systém vyhodnotí a přijme CSR podle známých údajů: prohlášení, zaručení, řízení (co bude ovládat), formální podrobnosti.
6. Systém podepíše žádost – vznikne certifikát.
7. Systém zpřístupní (vystaví) certifikát Členovi.
8. Člen přijme certifikát.

(Některé kroky se někdy vynechávají, například u anonymních certifikátů.)

### 4.1 Požadavky na vystavení certifikátů

[V původním textu se rozlišuje přihláška (postup uživatele) a žádost (soubor CSR). Přihlášku budeme raději překládat jako požadavek.]

#### 4.1.1 Kdo může požádat o certifikát

Požadavek na certifikát mohou předložit Členové. Od vystavení certifikátů se Členové stávají odběrateli.

#### 4.1.2 Přidání adres

Člen může vyhlásit vlastnictví nebo oprávnění pro doménu nebo e-mailovou adresu na on-line systému. Je to nezbytný krok pro vydání certifikátu. Existují tyto podmínky ovládání:

* Vyhlášení vlastnictví nebo oprávnění má právní význam a může hrát roli v řešení sporů.
* Každá jednotlivá adresa může patřit pouze jednomu účtu.
* Když Člen učiní prohlášení, certifikátový aplikační systém automaticky zahájí test, zda Člen skutečně doménu/adresu vlastní/ovládá/spravuje, viz dále.

#### 4.1.3 Příprava žádosti o certifikát (CSR)

Členové si generují své vlastní páry klíčů. Dohoda komunity CAcert (CAcert Community Agreement, [COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php)) zavazuje Člena, aby odpovídal za bezpečnost. Viz Dohodu komunity CAcert (CCA) 2.5, §9.6.

Žádost o certifikát (CSR) k předložení automatizovanému systému připraví Člen.

### 4.2 Zpracování požadavku na certifikát

Proces požadavku na vystavení certifikátu je plně automatizován. Žádosti, schválení i zamítnutí jsou zpracovány webovým systémem. Každý požadavek by měl být zpracován za méně než minutu.

Když jsou vyžadovány certifikáty mající sloužit více účelům, musí být vyplněny požadavky pro každý účel.

#### 4.2.1 Identifikace (ověření)

Člen(ka) se přihlásí ke svému účtu na webu CAcert a tím se ověří jeho/její totožnost, protože zadá jméno a heslo, nebo se přihlásí svým klientským certifikátem od CAcert.

#### 4.2.2 Ověření vlastnictví/oprávnění/správy

V principu jsou pro každou adresu provedena alespoň dvě ověření.

**E-mailový „ping“.** E-mailová adresa je ověřena testem *ping*:

* Systém vygeneruje cookie (obsah je náhodný, těžko k uhodnutí) ve tvaru řetězce.
* Systém pošle cookie Členovi e-mailem.
* Přijme-li Člen(ka) tento e-mail, zadá cookie na web.
* Zadáním kódu ověří, že tuto e-mailovou adresu vlastní nebo ovládá.

**E-mail – ovládání.** E-mailové adresy pro klientské certifikáty se ověřují těmito testy:

1. Na e-mailové adrese úspěšně proběhl ping-test.
2. Člen(ka) musí podepsat formulář CAP nebo jeho ekvivalent a musí být oceněn(a) aspoň jedním bodem zaručení.

**Ovládání domény.** Adresy domén pro serverové certifikáty jsou ověřeny provedením dvou z následujících testů:

1. Test „e-mail ping“ je proveden na e-mailové adrese zvolené z adres poskytnutých *whois* nebo odvozených z názvu domény.
2. Systém vygeneruje cookie, kterou pak Člen umístí do DNS.
3. Systém vygeneruje cookie, kterou pak Člen umístí do hlaviček HTTP nebo do textového souboru.
4. Alespoň dva zaručovatelé vydají prohlášení, že Člen vlastní/ovládá doménu dotyčného názvu.
5. Systém vygeneruje cookie, kterou pak Člen umístí do registračních údajů *whois*.

Poznámky:

* Občas může CAcert přidat jiné metody.
* Statické cookies jsou uchovány během života certifikátu pro příležitostné otestování.
* Dynamické testy lze opakovat později podle volby CAcert.
* Kontroly ovládání domény mohou být v budoucnu rozšířeny, aby se vztahovaly také na ovládání e-mailových adres.

#### 4.2.3 Dostupné možnosti

[Pro vydávané certifikáty existují alespoň dva „podkořeny“ (subroots), které se dále označují jako „členský“ (nezaručených Členů) a „zaručený členský“ (zaručených Členů). Úprava předložených žádostí CSR před jejich podpisem probíhá podle dvou různých procedur.]

Člen má tyto dostupné možnosti:

* Každá ověřená e-mailová adresa je dostupná pro klientské certifikáty.
* Každá ověřená doménová adresa je dostupná pro serverové certifikáty.
* Není-li člen zaručen, pak má dostupný pouze členský zprostředkující (podkořenový, subroot) certifikát.
* Je-li Člen zaručen, pak má dostupný certifikát jak pro Členy, tak pro zaručené Členy.
* Je-li zaručeno jméno, může být vloženo do klientského certifikátu nebo signatury OpenPGP.

#### 4.2.4 Procedury pro klientské certifikáty

Pro klientský certifikát jednotlivce se vyžaduje:

* E-mailová adresa je ohlášena a přidána.
* E-mailová adresa je otestována ping-testem.
* Pro subroot Členů musí mít Člen aspoň jeden bod zaručení a mít podepsaný formulář CAP.
* Pro subroot zaručených Členů musí mít Člen aspoň padesát bodů zaručení.

#### 4.2.5 Procedury pro serverové certifikáty

Pro serverový certifikát se vyžaduje:

* Doména je ohlášena a přidána.
* Doména je testována dvakrát, viz výše.
* Pro subroot Členů musí mít Člen aspoň jeden bod zaručení a mít podepsaný formulář CAP.
* Pro subroot zaručených Členů musí mít Člen aspoň padesát bodů zaručení.

#### 4.2.6 Procedury pro certifikáty pro podepisování kódu

Certifikáty pro podpis kódu jsou dostupné pouze zaručovatelům. Jsou zpracovávány podobně jako klientské certifikáty.

#### 4.2.7 Ověření domény organizace

Domény organizací jsou zpracovávány podle Zásad zaručování organizací a Příručky organizací.

### 4.3 Vystavení certifikátu

#### 4.3.1 Akce CA během vydání certifikátu

**Velikosti klíčů.** Členové mohou požadovat klíče jakékoli velikosti, kterou umožňuje algoritmus klíčů. Mnohá starší hardwarová zařízení vyžadují krátké klíče.

**Algoritmy.** CAcert v současnosti podporuje pouze algoritmus RSA pro klíče X.509; podepisování X.509 používá algoritmus SHA-1 „message digest“ [přibližně: „výtah ze zprávy“ - nemyslí se však zdviž]. Podepisování OpenPGP používá podepisování RSA klíčů RSA a DSA [„Digital Signing Algorithm“ (algoritmus digitálního podpisu) Spojených států amerických].

**Proces pro certifikáty:** Webový systém vydávání certifikátů ověřuje všechny detaily každého certifikátu. Vystavování je založeno na systému „šablon“, který vybírá profily pro dobu platnosti, velikost a algoritmus certifikátu.

1. Je ověřena žádost o certifikát (CSR).
2. Ze souboru žádosti (CSR) jsou extrahovány a ověřeny údaje:
* Jméno/název - §3.1,
* e-mailová adresa - §4.2.2,
* adresa domény - §4.2.2.
1. Certifikát je vygenerován ze šablony.
2. Údaje jsou okopírovány ze žádosti (CSR).
3. Certifikát je podepsán.
4. Certifikát je uložen a odběrateli je odeslána e-mailová zpráva.

**Proces pro podpisy klíčů OpenPGP:** Webový systém vydávání certifikátů ověřuje všechny detaily každého Sub-ID (pod-identifikátoru). Vystavování je založeno na konfiguraci, která vybírá profily pro dobu platnosti, velikost a algoritmus podpisu tímto procesem:

1. Je ověřen veřejný klíč.
2. Z klíče jsou extrahovány a ověřeny údaje (jméno/název, e-mailové adresy). Jsou povoleny jen kombinace údajů podle tabulky 4.3.1.
3. Je vygenerován podpis klíče OpenPGP.
4. Podpis klíče je aplikován na klíč.
5. Podepsaný klíč je uložen a odběrateli je odeslána e-mailová zpráva.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Ověřené jméno/název | Neověřené jméno | Prázdné jméno |
| Ověřený e-mail |  |  |  |
| Neověřený e-mail |  |  |  |
| Prázdný e-mail |  |  |  |

Tabulka 4.3.1 Povolené údaje v podepsaných klíčích OpenPGP

#### 4.3.2 Upozornění CA odběrateli o vystavení certifikátu

Jakmile je certifikát podepsán, je zpřístupněn Členovu účtu a (odkaz) odeslán Členovi. Je také interně archivován.

### 4.4 Přijetí certifikátu

#### 4.4.1 Ustanovení o příjmu certifikátu

Není třeba, aby Člen výslovně potvrdil přijetí certifikátu. V případě, kdy Člen certifikát výslovně *nepřijme*, musí být certifikát odvolán a vytvořen znovu.

#### 4.4.2 Zveřejnění certifikátu certifikační autoritou

CAcert v současnosti nepublikuje vydané certifikáty do žádného úložiště. Pokud bude CAcert provozovat úložiště, bude zveřejnění certifikátů a podpisů záviset na rozhodnutí Člena. Avšak předpokládá se, že vydané a Členovi doručené certifikáty budou zveřejněny. Viz §2.2.

#### 4.4.3 Upozornění na vydání certifikátu certifikační autoritou jiným entitám

Nejsou žádné vnější entity, kterým by mělo být oznamováno vydání certifikátů.

### 4.5 Klíčový pár a použití certifikátu

Všichni Členové (odběratelé a spoléhající strany) jsou vázáni Dohodou komunity Cacert (CCA, [COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php)). Viz zvláště odstavce CCA 2.3 až 2.5.

#### 4.5.1 Použití klíčů odběratelem a jeho odpovědnost

Odběratel by měl používat klíče jen k jejich správnému účelu indikovanému v certifikátu, nebo podle širší dohody s ostatními.

#### 4.5.2 Použití spoléhající stranou a její odpovědnost

Spoléhající strana (Členové) mohou spoléhat na toto prohlášení:

|  |
| --- |
| Relying Party StatementCertificates are issued to Members only.All information in a certificate is verified. |

Český překlad:

|  |
| --- |
| Prohlášení spoléhající straněCertifikáty jsou vydávány pouze Členům.Všechny údaje v certifikátu jsou ověřeny. |

Následující poznámky jsou dodatkem Prohlášení a lze je považovat za jeho omezení.

**4.5.2.a Metody ověření**

Termín „ověření“, jak je použit v Prohlášení, znamená jednu z možností:

|  |  |  |  |
| --- | --- | --- | --- |
| **Typ** | **Jak** | **Autorita** | **Poznámky** |
| **Zaručení** | Podle Zaručovacího programu CAcert (CAP) | Zásady zaručování | Do certifikátu jdou jen údaje zaručené 50 body dle CAP |
| **Vyhodnocení** | Automatizované kontroly domény a e-mailové adresy | Tento dokument | Viz §4.2.2 |
| **Řízeno** | Programy nebo „profily“, které kontrolují údaje v žádosti o podpis certifikátu (CSR) | Tento dokument | Viz §7.1 |

**4.5.2.b Kdo může spoléhat**

**Členové mohou spoléhat.** Spoléhající strany jsou Členové, takže jsou vázáni tímto dokumentem (Přehled postupů certifikace, CPS) a Dohodou komunity CAcert (CCA, [COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php)). Licence a povolení se spolehnout nejsou přiřaditelné.

**Dodavatelé softwaru.** Kořenové certifikáty CAcert mohou být distribuovány v softwaru, dodavatelé mohou sjednat smlouvu s CAcert podle dokumentu Prodejce třetí strany – dementi a licence - ROZPRACOVÁNO (Third Party Vendor - Disclaimer and Licence [WIP]). Tato licence začleňuje dodavatele do komunity v tom, že dodavatel souhlasí s řešením sporů uvnitř fóra CAcert.

**Nezapojené osoby (NRP) se nemohou spolehnout.** Osoba, která není ve vztahu k CAcert smlouvou zavazující strany k řešení sporů na fóru CAcert, je nezapojená osoba (NRP). Nezapojená osoba nemá povoleno spoléhat, a není tedy spoléhající stranou, Další podrobnosti viz Nezapojené osoby – dementi a licence (NRP – Disclaimer and License, [COD4](http://www.cacert.org/policy/NRPDisclaimerAndLicence.php)).

**4.5.2.c Akt spolehnutí**

**Rozhodnutí.** Spolehnutí znamená provést rozhodnutí, které částečně nebo plně závisí na údajích certifikátu. Spoléhající strana může začlenit údaje certifikátu, a vyplývající údaje jako členství, do svého rozhodování. Při rozhodování by spoléhající strana měla také:

* uvážit svou vlastní rovnici rizika,
* uvážit všeobecná omezení zaručovacího procesu, certifikátů a širších záležitostí zabezpečení,
* provést další kontroly pro získání více informací,
* zvážit širší dohodu s jinými Členy, a
* použít správný protokol nebo úzus spolehnutí (dále).

**Prozkoumání certifikátu.** Spoléhající strana musí o každém certifikátu rozhodnout, zda ho použije. Musí certifikát prozkoumat procesem zvaným *vyhodnocení (validation)*. Údaje certifikátu obsahují kromě jiných:

* jméno/název,
* dobu platnosti certifikátu,
* aktuální seznam odvolaných certifikátů (CRL),
* řetěz certifikátů a kontrolu platnosti certifikátů v řetězu,
* vydavatele certifikátu (CAcert),
* pro spolehnutí se vyžaduje zprostředkující kořenový certifikát (zaručení Členové, organizace a třída 3),
* účel certifikátu.

**Udržování záznamů.** Záznamy - podklady rozhodnutí - mají být udržovány. Certifikáty mají být uchovávány. Tím by měly vzniknout dostatečné důkazy ke stanovení, kdo jsou strany (zvláště certifikáty, na něž se spoléhá), ke stanovení sporných transakcí a ke stanovení širší dohody, která definuje akt.

**Širší protokol.** Spolehnutí bude v principu částí širšího protokolu (obvyklá metoda dosažení a dodržení dohody), který představuje a uchovává dostatečný důkaz pro řešení sporů podle Arbitrážního fóra CAcert. Protokol by si měly dohodnout všechny strany a přizpůsobit ho potřebám. Tento dokument (CPS) nedefinuje žádný takový protokol. Při absenci takového protokolu bude spolehnutí oslabeno; spor bez dostatečných důkazů může arbitr odmítnout.

**Porovnání s použitím.** Spolehnutí přesahuje použití. Použití je omezeno tím, že ponechává akt softwaru jako totální, jedině platnou autoritu. Spolehnutím Člen také posiluje algoritmickou činnost softwaru svou vlastní kontrolou z provozního, technického a certifikátového hlediska.

**4.5.2.d Rizika a omezení spolehnutí**

**Kořenové certifikáty a použití jmen/názvů.** Tam, kde je použit kořenový certifikát třídy 1, může být tento odběratel novým Členem, včetně členů s počtem bodů zaručení nula. Není-li poskytnuto jméno, znamená to, že je nedostupné. Za těchto podmínek není spolehnutí definováno a spoléhající strany by měly být obezřetné. Viz tabulka 4.5.2.

|  |  |
| --- | --- |
| *Třída kořenového certifikátu* | *Prohlášení spolehlivosti pro Členy* |
| **Anonymní**(všichni Členové) | **Pojmenované**(pouze zaručení Členové) |
| Třída**1** | **Nespoléhat.**Spoléhající strana musí použít jiné metody kontroly. | Nespoléhat. Ačkoli jmenovaný Člen byl CAcertem zaručen, není spolehnutí pro kořenový certifikát třídy 1 definováno (vydán jen pro kompatibilitu). |
| Podkořen**Člen** |
| Třída**3** | Nespoléhat na jméno (je-li dostupné). Člen byl CAcertem zaručen, ale spolehnutí není definováno. | Člen jmenovaný v certifikátu byl zaručen CAcertem. |
| Podkořen**Zaručený** |

Tabulka 4.5.2 Prohlášení o spolehnutí

**Softwarový agent.** Při spoléhání na certifikát by měly spoléhající strany vědět, že váš software odpovídá za způsob, jakým zobrazuje údaje z certifikátu. Skrývá-li váš softwarový agent některé údaje, může pro ně být jedinou nápravou volba jiného softwarového agenta.

**Škodlivé programy (malware).** Při spoléhání na certifikát by měly spoléhající strany vědět, že platformy zranitelné viry nebo trójskými koni, nebo mající jinou slabinu, nemusí zpracovávat certifikáty správně a mohou dávat klamné nebo podvodné výsledky. Je vaší odpovědností zajistit, abyste používali platformu, která je zabezpečena vzhledem k potřebám aplikace.

**4.5.2.e Když je něco špatně**

V případě, že vyvstane problém mimo spolehnutí Člena, je jeho jedinou cestou **založit spor podle Zásad řešení sporů (DRP).** Viz §9.13. Za tím účelem musí být uchováván certifikát (a další důkazy).

**Jaká osoba?** Členové mohou instalovat certifikáty jiným jednotlivcům, nebo na servery, ale Člen, jemuž je certifikát vydán, zůstává odpovědnou osobou. Například u zaručení organizace je jí vydán certifikát pro použití jednotlivci nebo servery uvnitř organizace, ale přitom organizace zůstává odpovědnou osobou.

**Softwarový agent.** Spoléhá-li Člen na kořenový certifikát CAcert včleněný do softwaru dodaného prodejcem, pak se rizika, odpovědnost ani závazky Člena nepřenášejí automaticky na prodejce.

### 4.6 Obnova certifikátu

Certifikát může být kdykoli obnoven. Procedura obnovy certifikátu je stejná, jako při jeho počátečním vystavení.

### 4.7 Změna klíče certifikátu

[Tato funkce umožňuje změnit klíče (například po ztrátě privátního klíče) a zachovat ostatní údaje certifikátu. Bezpečnostně není zcela korektní.]

Změna klíčů certifikátu není nabízena ani podporována. Novou žádostí (CSR) musí být vyžádán a vystaven nový certifikát s novým veřejným klíčem [přitom vznikne i privátní klíč].

### 4.8 Modifikace certifikátu

„Modifikace“ certifikátů nejsou nabízeny ani podporovány. Místo toho musí být standardním způsobem vyžádán a vystaven nový certifikát.

### 4.9 Odvolání a suspendování certifikátů

#### 4.9.1 Podmínky odvolání

Certifikáty lze odvolávat při splnění těchto podmínek:

1. Odběratel odvolá certifikát pomocí svého on-line účtu.
2. Certifikát je odvolán členem týmu podpory při nouzové akci. Taková akce musí být neprodleně hlášena k řešení sporu pro ratifikaci.
3. Pod dohledem arbitra ve včas objednaném nařízení z podaného sporu.

Toto jsou jediné tři podmínky, za nichž může k odvolání dojít.

#### 4.9.2 Kdo může odvolání vyžádat

Viz výše.

#### 4.9.3 Procedura žádosti o odvolání

Odběratel se přihlásí ke svému on-line účtu na webu <http://www.cacert.org/>.

V jakémkoli jiném případě, jako je ztráta hesla nebo podvod, musí být založen spor, a to e-mailem na support(zavináč)cacert.org.

#### 4.9.4 Prodleva žádosti o odvolání

Žádné podmínky.

#### 4.9.5 Doba, v níž musí CAcert zpracovat žádost o odvolání

Odvolání pomocí webováého rozhraní pro odběratele obecně trvá nejvýše jednu minutu.

Spor podaný za účelem odvolání bude zpracován během několika pracovních dnů, avšak záleží také na uvážení arbitra.

#### 4.9.6 Požadavek kontroly odvolání pro spoléhající strany

Každý odvolaný certifikát je zapsán do seznamu odvolaných certifikátů (CRL). Spoléhající strany musí kontrolovat, je-li pořadové číslo certifikátu zapsáno v nejnovější verzi tohoto seznamu a tím ověřit, zda spolehnutí na certifikát stále platí.

#### 4.9.7 Frekvence vydávání CRL (dá-li se použít)

Po každém odvolání certifikátu je vydán nový CRL.

#### 4.9.8 Nejdelší latence CRL (dá-li se použít)

Doba latence mezi odvoláním certifikátu a vydáním nového CRL je 1 hodina.

#### 4.9.9 Dostupnost kontroly odvolání / stavu certifikátu on-line

Je dostupný odpovídač OCSP na webové adrese <http://ocsp.cacert.org/>.

#### 4.9.10 Požadavky na on-line kontrolu odvolání

Spoléhající strany musí před spolehnutím zkontrolovat aktuální status.

#### 4.9.11 Jiné dostupné formy inzerce odvolání

Žádné.

#### 4.9.12 Zvláštní požadavky ohledně prozrazení klíče

Odběratelé jsou povinni při nejbližší příležitosti prozrazené certifikáty odvolat.

#### 4.9.13 Podmínky pro suspendování certifikátů

Suspendování certifikátů není dostupné [neprovádí se].

#### 4.9.14 Kdo může požadovat suspendování

Nepřipadá v úvahu.

#### 4.9.15 Procedura pro žádost o suspendování

Nepřipadá v úvahu.

#### 4.9.16 Omezení doby suspendování

Nepřipadá v úvahu.

### 4.10 Služby stavu certifikátů

#### 4.10.1 Provozní charakteristiky

Je dostupný odpovídač OCSP na webové adrese <http://ocsp.cacert.org/>.

#### 4.10.2 Dostupnost služby

OCSP je zpřístupněn na experimentálním základě.

#### 4.10.3 Volitelné vlastnosti

Žádné podmínky.

### 4.11 Ukončení odběru

Certifikáty obsahují datum konce platnosti.

### 4.12 Zabezpečené úložiště klíčů a jejich obnova

#### 4.12.1 Zabezpečené úložiště klíčů, zásady obnovy a postupy

CAcert negeneruje ani zabezpečeně neukládá klíče odběratelů.

#### 4.12.2 Zapouzdření klíče sezení, zásady obnovy a postupy

Žádné podmínky.

## 5. Zařízení, správa a řízení provozu

### 5.1 Fyzické ovládání

Odkazujeme na Zásady bezpečnosti (Security Policy [SP], [COD8](http://www.cacert.org/policy/SecurityPolicy.html)).

* Umístění a konstrukce sídla – SP2.1
* Fyzický přístup – SP2.3

#### 5.1.1 Napájení a klimatizace

Viz Zásady bezpečnosti (Security Policy[SP], [COD8](http://www.cacert.org/policy/SecurityPolicy.html)) - 2.1.2.

#### 5.1.2 Vystavení vodě

Viz SP 2.1.4 ([COD8](http://www.cacert.org/policy/SecurityPolicy.html)).

#### 5.1.3 Prevence a ochrana před požárem

Viz SP 2.1.4 ([COD8](http://www.cacert.org/policy/SecurityPolicy.html)).

#### 5.1.4 Uložení médií

Viz SP 4.3 ([COD8](http://www.cacert.org/policy/SecurityPolicy.html)).

#### 5.1.5 Likvidace odpadů

Žádné podmínky.

#### 5.1.6 Záloha mimo lokalitu

Viz SP 4.3 ([COD8](http://www.cacert.org/policy/SecurityPolicy.html)).

### 5.2 Procedurální řízení

#### 5.2.1 Důvěryhodné role

* **Technické týmy:**
	+ podpora uživatelů
	+ správci systémů – kritických i ne-kritických
	+ vývojáři softwaru
	+ řadiči klíčů

Viz SP 9.1 ([COD8](http://www.cacert.org/policy/SecurityPolicy.html)).

* **Zaručování:**
	+ Zaručovatelé
	+ Ostatní osoby oprávněné podle [COD13](http://www.cacert.org/policy/AssurancePolicy.php)

Viz Zásady zaručování ([COD13](http://www.cacert.org/policy/AssurancePolicy.php)).

* **Správa:**
	+ Ředitelé (členové výboru CAcert Inc., čili „Výboru“
	+ Interní auditor
	+ Arbitr [rozhodčí sporů]

#### 5.2.2 Počet osob potřebných pro úkol

CAcert pracuje na principech *čtyři oči* a *dvojí řízení*. Všechny důležité role vyžadují alespoň dvě osoby. Člověk může plnit úkol a další ho pozorovat (*čtyři oči*), nebo dvě osoby spolupracují (*dvojí řízení*).

#### 5.2.3 Identifikace a ověření pro každou roli

Osoby ve všech důležitých rolích musí být zásadně zaručeny alespoň na úroveň zaručovatele podle Zásad zaručování (AP). Viz Zásady zaručování (Assurance Policy, [COD13](http://www.cacert.org/policy/AssurancePolicy.php)).

**Technické.** Viz SP 9.1 ([COD8](http://www.cacert.org/policy/SecurityPolicy.html)).

#### 5.2.4 Role vyžadující oddělení povinností

Role všeobecně usilují o oddělení povinností [funkcí]; jak role používající princip *čtyř očí*, tak role používající princip *dvojího řízení*.

### 5.3 Řídicí personál

#### 5.3.1 Požadavky na kvalifikaci, zkušenost a vyklizení (?)

|  |  |  |
| --- | --- | --- |
| **Role** | **Zásady** | **Poznámky** |
| Zaručovatel | [COD13](http://www.cacert.org/policy/AssurancePolicy.php) | Složil test Výzva zaručovatele a je zaručen 100+ body |
| Zaručovatel organizací | [COD11](http://www.cacert.org/policy/OrganisationAssurancePolicy.php) | Vyškolen a zkoušen dvěma dohlížejícími zaručovateli organizací. |
| Technici | SM=>COD08 | Týmy odpovídající za testování |
| Arbitr | [COD7](http://www.cacert.org/policy/DisputeResolutionPolicy.php) | Zkušení zaručovatelé |

Tabulka 5.3.1 Role řízení

#### 5.3.2 Procedury testů pozadí

Viz Zásady bezpečnosti (Security Policy, SP) 9.1.3 ([COD8](http://www.cacert.org/policy/SecurityPolicy.html)).

#### 5.3.3 Požadavky na vyškolení

Žádné podmínky.

#### 5.3.4 Opakování školení - četnost a požadavky

Žádné podmínky.

#### 5.3.5 Střídání úkolů – četnost a pořadí

Žádné podmínky.

#### 5.3.6 Sankce za neoprávněné akce

Jakékoli sporné akce – ať nejisté nebo hrubě nedbalé – mohou být podány jako spor. Arbitr má široké možnosti zvážení sankcí: ztráta bodů, doškolení, ukončení přístupu, ukončení funkce. Viz Zásady řešení sporů (Dispute Resolution Policy, DRP).

#### 5.3.7 Požadavky nezávislého dodavatele

Žádné podmínky.

#### 5.3.8 Dokumentace dodávaná personálu

Žádné podmínky.

### 5.4 Procedury záznamu auditu

Viz Zásady bezpečnosti (Security Policy, SP) 4.2, 5 ([COD8](http://www.cacert.org/policy/SecurityPolicy.html)).

### 5.5 Archivace záznamů

Standardní doba uchovávání je 7 let. Jednou archivované záznamy lze získat a ověřovat pouze cestou podání sporu. Archivují se tyto záznamy:

|  |  |  |  |
| --- | --- | --- | --- |
| **Záznam** | **Povaha** | **Výjimky** | **Dokumentace** |
| Člen | Jméno uživatele, primární a další e-mailové adresy, bezpečnostní otázky, datum narození | Zrušení členi, kteří se nikdy nestali odběrateli: 0 roků | Zásady bezpečnosti (SP) a Zásady ochrany soukromí (PP) |
| Zaručení | Formuláře CAP | „aspoň 7 let“ dle pomocných zásad | Zásady zaručování (AP) 4.5 |
| Zaručení organizace | Formuláře COAP | Dle pomocných zásad | Zásady zaručování organizací (OAP) |
| Certifikáty a odvolání | Pro spolehnutí | 7 let po ukončení | Tento dokument (CPS) |
| Kritické role | Pracovní záznamy kontroly pozadí | Pod přímým řízením arbitra | Zásady bezpečnosti (SP) 9.1.3 |

Tabulka 5.5 Dokumenty a jejich uchovávání

### 5.6 Střídání klíčů

Viz Zásady bezpečnosti (Security Policy, SP) 9.2 ([COD8](http://www.cacert.org/policy/SecurityPolicy.html)).

### 5.7 Náprava prozrazení a obnova po havárii

Viz Zásady bezpečnosti (Security Policy, SP) 5, 6 ([COD8](http://www.cacert.org/policy/SecurityPolicy.html)). (Omezení služby viz §1.4.)

### 5.8 Ukončení CA nebo RA

[CA – certifikační autorita. RA – registrační autorita.]

#### 5.8.1 Ukončení CA

V případě ukončení provozu budou zajištěny kořenové a pod-kořenové certifikáty a veškeré soukromé údaje o Členech. Certifikáty budou předány odpovědné straně za jediným účelem: vydat odvolání. Údaje o Členech budou bezpečným způsobem zničeny.

#### 5.8.2 Ukončení RA

Když se zaručovatel rozhodne ukončit své odpovědnosti, provede to založením sporu a pak jedná podle pokynů arbitra.

Jde-li o neúmyslné ukončení [úmrtí], je proces stejný, ale spor musí založit jiná strana.

## 6. Řízení technické bezpečnosti

### 6.1 Generování a instalace páru klíčů

#### 6.1.1 Generování páru klíčů

Odběratelé si vygenerují svůj vlastní pár klíčů.

#### 6.1.2 Zabezpečení privátního klíče odběratele

Neexistují technické podmínky určující, jak má odběratel vygenerovat a bezpečně ukládat své privátní klíče, avšak Dohoda komunity CAcert (CCA) 2.5 ukládá odběrateli závazek zabezpečení. Viz §9.6.

#### 6.1.3 Dodání veřejného klíče vydavateli certifikátu

Členové se přihlašují ke svým on-line účtům. Veřejné klíče jsou doručeny zkopírováním a vložením do příslušného okna [textového pole pro CSR]. Veřejné klíče jsou u X.509 dodávány ve tvaru podepsané žádosti o certifikát (CSR) nebo u OpenPGP ve tvaru sám sebou podepsaném.

#### 6.1.4 Dodání veřejného klíče z CA spoléhajícím stranám

Kořenové certifikáty CA jsou distribuovány takto:

* publikací na webu CAcert při přístupu jak v HTTP, tak v HTTPS,
* jako vložené v software třetích stran – webových prohlížečích, e-mailových klientech. Jejich dodavatelé jsou předmětem smlouvy pro prodejce třetích stran (Third Party Vendor Agreement).

#### 6.1.5 Velikosti klíčů

Velikost (délka) klíčů odběratele není omezena.

Kořenové a zprostředkující klíče CAcert X.509 mají v současnosti 4096 bitů. Kořenové klíče X.509 používají RSA a podepisují algoritmem výtahu zprávy SHA-1. Viz §4.3.1.

Podepisování OpenPGP používá jak RSA, tak DSA (1024 bitů).

CAcert přidává delší klíče a haše v souladu s obecnými kryptografickými trendy, jak je podporují hlavní dodavatelé softwaru.

#### 6.1.6 Generování parametrů veřejného klíče a kontrola kvality

Žádné podmínky.

#### 6.1.7 Účely použití klíčů

Kořenové klíče CAcert mají všeobecné použití. Každý kořenový klíč může podepsat všechny všeobecné účely: klient, server, kód.

Web ovládá účely použití, které lze podepsat. Toho se dosahuje systémem „šablon“.

### 6.2 Ochrana privátního klíče a řízení techniky kryptografického modulu

#### 6.2.1 Standardy a ovládání kryptografického modulu

Pod-kořenové klíče jsou uloženy na jediném stroji, který pracuje jako kryptografický modul, neboli *podepisující server*. Pracuje jako jediný démon [služba] pouze pro podepisování. Podepisující server má tyto bezpečnostní vlastnosti:

* Je připojen pouze k jedinému spoji (sériovému USB) určenému pouze k tomu účelu. Ten ho spojuje se serverem on-line účtů. Sám podepisující server není přímo připojen k síti, ani k vnitřní LAN (ethernetu), ani ke konzolovému přepínači [tzv. KVM – klávesnice, video, myš].
* Protokol používaný na zmíněném USB spoji je speciální, s jednou výzvou, obsluhující pouze žádosti o podepisování certifikátů.
* Démon je navržen tak, že nezobrazuje klíče.
* Démon obsahuje „aktivku“, která monitoruje webový server vyžadující přístup.
* Démon ukončí svou činnost, když detekuje chybný požadavek.
* Démon sídlí v zašifrovaném oddílu.
* Podepisující server může být (re)startován jedině z přímého přístupu systémového správce.
* Fyzický přístup k podepisujícímu serveru podléhá *dvojímu řízení*.

Viz §5 a Zásady bezpečnosti (Security Policy, SP) 9.3.1 ([COD8](http://www.cacert.org/policy/SecurityPolicy.html)).

(Kryptografické moduly založené na hardwaru, komerci a standardech byly vyzkoušeny a testovány, i podobné, ale bylo zjištěno, že nevyhovují, například pracují jen s malými délkami klíčů a jsou výkonově omezeny.)

### 6.3 Další hlediska správy páru klíčů

#### 6.3.1 Archivace veřejných klíčů

Odběratelské certifikáty, včetně veřejných klíčů, jsou ukládány do databáze podporující on-line systém. Nejsou zpřístupněny v archivu dostupném veřejností ani odběrateli, viz §2. Jsou zálohovány normální zálohovací procedurou CAcert, ale jejich dostupnost je na odpovědnosti odběratele.

#### 6.3.2 Doba funkčnosti certifikátu a doba použití páru klíčů

Doba funkčnosti [délka platnosti] certifikátu a jeho páru klíčů závisí na stavu zaručení Člena [odběratele], viz §1.4.5 a Zásady zaručování (AP, [COD13](http://www.cacert.org/policy/AssurancePolicy.php)).

Kořenový certifikát CAcert (nejvyšší úrovně) má expirační dobu 30 let. Pod-kořenové certifikáty mají 10 let a budou měněny rychleji. Délka klíče kořenových certifikátů je zvolena za účelem zajistit Členům CAcert optimální bezpečnost založenou na současných doporučeních [kryptografické komunity](http://www.keylength.com/) a maximálních limitech obecně dostupného softwaru. V době vzniku tohoto dokumentu to bylo 4096 bitů.

### 6.4 Aktivační data

Žádné podmínky.

### 6.5 Řízení počítačové bezpečnosti

Viz Zásady bezpečnosti (Security Policy, SP).

### 6.6 Řízení technického životního cyklu

Viz Příručka zabezpečení (Security Manual, SM) 7 „Vývoj software“.

### 6.7 Řízení bezpečnosti sítě

Viz Příručka zabezpečení (Security Manual, SM) 3.1 „Logické zabezpečení – síť“.

### 6.8 Použití časových razítek

Každý server je časově synchronizován pomocí NTP (Network Time Protocol, protokol času sítě). V současnosti není nabízena žádná služba „časového razítkování“.

## 7. Profily certifikátů, CRL a OSCP

CAcert definuje ve svých zásadách, příručkách a jiných dokumentech všechny významy, sémantiky a profily vztahující se k vydávání certifikátů a podpisů. Významy, které mohou být zapsány ve vnějších normách nebo dokumentech, nebo se nacházejí v širších [obecnějších?] konvencích, nejsou zahrnuty, nejsou CAcertem používány a nesmí být vyvozovány Členem ani nezapojenou osobou.

[CRL: Certificate Revocation List (seznam odvolaných certifikátů); OCSP: Online Certificate Status Protocol (on-line protokol o stavu certifikátu)]

### 7.1 Profil certifikátu

#### 7.1.1 Číslo verze / čísla verzí

Vydané certifikáty X.509 jsou ve tvaru verze v3. Tvar podpisů PGP závisí na několika faktorech, a proto zde nejsou žádné podmínky.

#### 7.1.2 Rozšiřující údaje certifikátu

Klientské certifikáty obsahojí tato rozšíření:

* basicConstraints=CA:FALSE (critical) [základní omezení: nejde o certifikační autoritu (kritická vlastnost)]
* keyUsage=digitalSignature,keyEncipherment,keyAgreement (critical) [použití klíče: digitální podpis, šifrování klíčem, dohoda klíče (kritická)]
* extendedKeyUsage=emailProtection,clientAuth,msEFS,msSGC,nsSGC [rozšířené použití klíče: ochrana e-mailu, prokázání identity klienta, šifrování systému souborů EFS, zastaralé Server-Gated Cryptography]
* authorityInfoAccess=OCSP;URI:[http://ocsp.cacert.org](http://ocsp.cacert.org/) [přístup k informacím autority (AIA) – OCSP je na uvedeném odkazu URI]
* crlDistributionPoints=URI:<crlUri> - nahradit URI, kde se nachází CRL příslušný k certifikátu [distribuční místo CRL – pro představu: CAcert podepsané kořenovým c. třídy 1: <http://crl.cacert.org/revoke.crl>, podepsané zprostředkujícím certifikátem třídy 3: <http://crl.cacert.org/class3-revoke.crl>]
* subjectAltName=(dle §3.1.1) [alternativní název subjektu (SAN)]

Certifikáty pro podpis kódu obsahují tato rozšíření:

* basicConstraints=CA:FALSE (critical) [základní omezení: nejde o certifikační autoritu (kritická vlastnost)]
* keyUsage=digitalSignature,keyEncipherment,keyAgreement (critical) [použití klíče: digitální podpis, šifrování klíčem, dohoda klíče (kritická)]
* extendedKeyUsage=emailProtection,clientAuth,codeSigning,msCodeInd,msCodeCom, msEFS,msSGC,nsSGC [rozšířené použití klíče: ochrana e-mailu, prokázání identity klienta, podepisování kódu,...]
* authorityInfoAccess=OCSP;URI:[http://ocsp.cacert.org](http://ocsp.cacert.org/) [přístup k informacím autority (AIA) – OCSP je na uvedeném odkazu URI]
* crlDistributionPoints=URI:<crlUri> - nahradit URI, kde se nachází CRL příslušný k certifikátu [distribuční místo CRL – pro představu: CAcert podepsané kořenovým certif. třídy 1: <http://crl.cacert.org/revoke.crl>, podepsané zprostředkujícím certif. třídy 3: <http://crl.cacert.org/class3-revoke.crl>]
* subjectAltName=(dle §3.1.1) [alternativní název subjektu (SAN)]

Podpisy klíče OpenPGP v současnosti nemají rozšířené údaje. V budoucnu sem může být doplněno pořadové číslo ve formě rozšíření.

#### 7.1.3 Algoritmus identifikátorů objektu

Žádné podmínky.

#### 7.1.4 Tvary jmen / názvů

Viz §3.1.1.

#### 7.1.5 Omezení jmen / názvů

Viz §3.1.1.

#### 7.1.6 Identifikátor objektu zásad certifikátu

Do certifikátů jsou vkládány tyto definované OID (Object ID, identifikátor objektu):

|  |  |  |
| --- | --- | --- |
| **OID** | **Typ/význam** | **Poznámka** |
| 1.3.6.1.4.1.18506.4.4 | Přehled postupů certifikace (CPS) | (tento dokument) |

Verze jsou definovány připojenými čísly, například .1 (1.3.6.1.4.1.18506.4.4.1)

#### 7.1.7 Použití rozšíření omezení zásad.

Žádné podmínky.

#### 7.1.8 Syntaxe a sémantika kvalifikátorů zásad

Žádné podmínky.

### 7.2 Profil CRL

#### 7.2.1 Čísla verzí

CRL jsou vytvářeny ve formátu X.509.

#### 7.2.2 CRL a jeho rozšířené položky

Nejsou zde žádná rozšíření.

### 7.3 Profil OCSP

#### 7.3.1 Čísla verzí

Odpovídač OCSP pracuje ve verzi 1.

#### 7.3.2 Rozšíření OCSP

Žádné podmínky.

## 8. Audit dodržování a další hodnocení

Jsou dvě hlavní linie hodnocení:

* **Audit systémů.** Analyzuje CA z hlediska bezpečnosti činnosti a provozu. Je prováděn ve dvou fázích: shoda dokumentů s kritérii a shoda provozu s dokumentací.
* **Audit kódu.** Analyzuje zdrojový kód. Je prováděn na dvou úrovních: Bezpečnostní koncepce na úrovni webových aplikací a bezpečnost zdrojového kódu s přehledem chyb.

Více informací viz stránka auditu na <http://wiki.cacert.org/wiki/Audit/>.

### 8.1 Četnost nebo podmínky hodnocení

První audity se konaly koncem roku 2005 a od té doby pokračují. I když jsou dokončeny, očekává se, že budou trvalé.

* **Audit systémů.**
* **Audit kódu.**

### 8.2 Totožnost a kvalifikace poradce

**Auditoři systémů.** CAcert využívá auditory pracovních systémů se širokými zkušenostmi o plném rozsahu: podnikání, informačních systémů a oblasti zabezpečení. Při výběru auditora pracovních systémů hledá CAcert zkušenosti obsahující mj. PKI, kryptografii, správu, auditování, udržovací a regulační prostředí, obchodní/podnikatelskou strategii, softwarové inženýrství, sítě, právo (včetně více-jurisdikčních záležitostí), systémy totožnosti, podvody, správu informačních technologií.

**Auditoři kódu.** Viz Zásady bezpečnosti (Security Policy, SP), sekce 7, 9.1.

### 8.3 Vztah poradce k hodnocené entitě

Zvláštní vnitřní vymezení osoby auditora:

* Musí být zaručen zaručovateli CAcert a musí být zkontrolováno jeho zázemí.
* Nesmí být aktivní v jakékoli (jiné) roli v CAcert. Zejména to nesmí být zaručovatel, člen sdružení, nebo mít jakoukoli jinou roli nebo funkci.
* Ačkoli se od auditora očekává, aby se během procesu auditu zabýval různými aktivitami (zaručování, školení), jejich výsledky jsou pozastaveny, dokud neukončí roli auditora.
* Auditor musí ohlásit CAcertu všechny potenciální konflikty zájmů, které by mohly v budoucnu nastat.

Zvláštní vnější vymezení osoby auditora:

* Má mít ověřitelnou delší zkušenost s ochranou soukromí a zabezpečením uživatelů.
* Nesmí pracovat pro konkurenční organizaci.
* Nesmí pracovat pro národní bezpečnost, zpravodajskou službu, LEO („Logistics and Engineering Operations“?) nebo podobné agentury.

Auditor musí být sladěn s auditorským týmem. Stejná omezení platí obecně pro všechny členy týmu, ale mohou se různit. Jakékoli odchylky musí být dokumentovány a schváleny výborem CAcert, Inc.

### 8.4 Hodnocená témata

Audity systémů jsou všeobecně prováděny podle kritérií. CAcert vyžaduje, aby kritéria byla otevřená:

* Publikovaná. Kritéria musí být dostupná všem zainteresovaným stranám.
* Srozumitelná. Musí být srozumitelná v tom, že podávají dostatečné informace v čitelné formě pro zainteresované strany zaměřené na podstatná a důležitá témata. (Záhadná bezpečnostní kritéria mohou tento požadavek ovlivnit.)
* Úplná. Musí existovat dostatečné údaje o pozadí celé záležitosti. Zejména je nutno vyhnout se nezdokumentovaným praktikám nebo konvencím úmyslně drženým v utajení.
* Aplikovatelná. Kritéria se musí přímo a jednoznačně týkat potřeb identifikovaných zainteresovaných stran (Členů, spoléhajících stran, odběratelů, zaručovatelů).

Současná kritéria viz [DRC](http://rossde.com/CA_review/) (David Ross Criteria, krítéria Davida Rosse). Pokud auditor zjistí, že kritéria nesplňují výše uvedené požadavky, pak je nutno kritéria přepracovat, aby požadavkům vyhověla, nebo kritéria zcela opustit (v obou případech s vysvětlením).

### 8.5 Akce k nápravě zjištěných nedostatků

Viz aktuální [seznam dokončených auditů](http://wiki.cacert.org/wiki/Audit/Done) – ukončené práce; [seznam „co ještě“](http://wiki.cacert.org/wiki/AuditToDo) - rozpracováno.

Auditor může vydat směrnice k provedení změn, ať jsou podstatné pro úspěch auditu nebo pro jiné extrémní situace. Směrnice by měly být založeny na kritériích, na odhadnutém minimu bezpečných praktik, nebo na přehledně popsané logice. Nejdříve má proběhnout adekvátní diskuse s komunitou (například s výborem CAcert Inc. a se skupinou pro zásady), pak lze vydat směrnice. Ty se mají řídit stejnými standardy, jako kritéria uvedená výše.

Dokumenty (vydané směrnice a akce): [wiki.cacert.org/wiki/AuditDirectives](http://wiki.cacert.org/wiki/AuditDirectives).

### 8.6 Sdělování výsledků

Aktuální i minulé údaje auditu jsou dostupné na [wiki.cacert.org/wiki/Audit](http://wiki.cacert.org/wiki/Audit/). CAcert zastává zásady otevřenosti, a audit není výjimkou.

Tento dokument (CPS) a jiné dokumenty jsou předmětem Zásad ohledně zásad (Policy on Policy, PoP, COD1). Audity pokrývají celkové procesy více než kterýkoli dokument, a dokumenty se mohou lišit od dodaných hlášení auditu.

## 9. Ostatní provozní a právní záležitosti

### 9.1 Poplatky

Struktura současných poplatků je uložena na [wiki.cacert.org/wiki/Price](http://wiki.cacert.org/wiki/Price). Změny struktury poplatků budou občas oznámeny na [blogu](http://blog.cacert.org/). CAcert si vyhrazuje právo stanovit ceny poplatků za služby. Všechny poplatky jsou nerefundovatelné.

### 9.2 Finanční odpovědnost

Finančním rizikem se primárně zabývají Zásady řešení sporů (Dispute Resolution Policy, DRP, [COD7](http://www.cacert.org/policy/DisputeResolutionPolicy.php)).

#### 9.2.1 Krytí pojištěním

Žádné podmínky.

#### 9.2.2 Ostatní aktiva

Žádné podmínky.

#### 9.2.3 Pojištění nebo záruční krytí pro koncové entity

Žádné podmínky.

### 9.3 Důvěrnost obchodních informací

#### 9.3.1 Rozsah důvěrných informací

CAcert má zásadu transparence a otevřenosti. Výchozí stav je takový, že údaje jsou veřejné v maximálním rozsahu, pokud nejsou řízeny ustanoveními specifické zásady (například hesla) nebo nařízeními arbitra.

### 9.4 Ochrana osobních údajů

Ochrana soukromí je pokryta Dohodou komunity CAcert (CCA, COD9) a Zásadami ochrany soukromí (Privacy Policy, [COD5](https://www.cacert.org/policy/PrivacyPolicy.html)).

#### 9.4.1 Plán ochrany soukromí

Žádné podmínky.

#### 9.4.2 Údaje považované za soukromé

Datum narození uživatele a otázky pro případ ztráty hesla jsou považovány za plně soukromé.

#### 9.4.3 Údaje nepovažované za soukromé

Údaje které lze vkládat do certifikátu, nejsou považovány za soukromé, neboť se očekává, že je bude Člen publikovat v rámci rutinního používání certifikátu. Tyto údaje jsou většinou jména a názvy, domény, e-mailové adresy, pořadová čísla certifikátů.

Podle Zásad zaručování (Assurance Policy, AP, [COD13](http://www.cacert.org/policy/AssurancePolicy.php)) je stav Člena (tj. zaručen, zaručovatel atd.) přístupný jiným Členům.

Údaje umístěné na fóra mimo on-line systém (wiki, blogy, zásady atd.) nejsou považovány za soukromé – jsou považovány za publikované jako příspěvky Členů. Viz Dohoda (CCA) 1.3 (COD9).

#### 9.4.4 Odpovědnost za ochranu soukromých údajů

CAcert je soukromá organizace a bere soukromí velmi vážně. Jakékoli záležitosti soukromí mohou být převedeny na řešení sporu.

#### 9.4.5 Upozornění a souhlas k použití soukromých údajů

Členům je dovoleno spoléhat na certifikáty jiných Členů. V přímém důsledku všeobecného práva spoléhat mohou Členové číst a ukládat certifikáty a/nebo údaje v nich obsažené tam, kde jsou správně přítomny ve vztahu a v rozsahu potřebném pro dohodnutý vztah.

#### 9.4.6 Zveřejnění podle justičních nebo správních procesů

Jakékoli zveřejnění podle procesu zahraničních soudů (nebo podobného) je řízeno arbitrem.

#### 9.4.7 Ostatní podmínky uvolnění informací

Žádné.

### 9.5 Práva intelektuálního vlastnictví

CAcert se angažuje ve filosofii otevřeného a svobodného Internetu, povšechně zapouzdřeného otevřeným a svobodným zdrojem. Avšak vlivem přísných regulačních ustanovení uložených kritérii auditu (Konfigurace-řídicí specifikace, CCS), všeobecného prostředí a role CA, a závazku bezpečnosti Členů jsou některé odchylky nezbytné.

#### 9.5.1 Vlastnictví a licence

Aktiva spadající pod řízení CCS musí být přenesena na CAcert. Viz Zásady ohledně zásad (PoP) 6.2 ([COD1](http://www.cacert.org/policy/PolicyOnPolicy.php#6.2)), Dohoda komunity CAcert (CCA) 1.3 ([COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php#1.3)). To jest: CAcert může svobodně použít, modifikovat, distribuovat a jiným způsobem vést činnost CA, když považuje přínos za vhodný.

#### 9.5.2 Značka

Značka (v širším smyslu) CAcert se skládá z loga, názvu, obchodní známky, služebních značek atd. Použití značky je přísně omezeno výborem a je k němu potřebné povolení. Viz [m20070917.5](http://wiki.cacert.org/wiki/TopMinutes-20070917).

#### 9.5.3 Dokumenty

CAcert vlastní nebo vyžaduje plné ovládání svých dokumentů, zvláště těch, které jsou pokryty CCS. Viz PoP 6.2 ([COD1](http://www.cacert.org/policy/PolicyOnPolicy.php#6.2)). Odběratelé přenášejí práva, viz Dohoda komunity CAcert (CCA) 1.3 (COD9). Odběratelé zaručují, že mají právo přenášet.

Dokumenty jsou obecně licencovány svobodnou, otevřenou licencí. Viz [wiki.cacert.org/wiki/PolicyDrafts/DocumentLicence](http://wiki.cacert.org/wiki/PolicyDrafts/DocumentLicence). Kromě případů, kde je to výslovně sjednáno, rozšiřuje CAcert zpětně na odběratele nevýlučnou, neomezenou trvalou licenci dovolující jim znovu svobodně užívat svou původní práci. Viz PoP 6.4 ([COD1](http://www.cacert.org/policy/PolicyOnPolicy.php#6.4)), CCA 1.3 ([COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php#1.3)).

#### 9.5.4 Kód

CAcert vlastní svůj kód nebo vyžaduje plné ovládání svého používaného kódu prostřednictvím svobodné a otevřené licence. Viz Konfigurace-řídicí specifikace (CCS).

CAcert licencuje svůj kód pod GPL (General Public License, všeobecná veřejná licence). CAcert rozšiřuje zpětně na odběratele nevýlučnou, neomezenou trvalou licenci dovolující jim znovu svobodně užívat svou původní práci.

#### 9.5.5 Certifikáty, kořenové certifikáty

CAcert uplatňuje práva na své intelektuální vlastnictví na certifikáty vydávané Členům a na kořenové certifikáty. Viz Dohoda komunity CAcert (CCA) 4.4 ([COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php#4.4)) a Konfigurace-řídicí specifikace (CCS). Certifikáty mohou používat pouze Členové podle COD9; ostatní podle nabízených licencí, například Nezapojené osoby – dementi a licence (Non-Related Persons – Disclaimer and License) ([COD4](http://www.cacert.org/policy/NRPDisclaimerAndLicence.php)).

### 9.6 Reprezentace a garance

**Členové.** Všichni Členové komunity souhlasí s Dohodou komunity CAcert (CCA, [COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php)), primárním dokumentem pro representace a garance. Členové jsou: odběratelé, spoléhající strany, registrační agenti a samotný CAcert.

**RA.** Registrační agenti jsou navíc vázáni Zásadami zaručování (Assurance Policy, AP), zvláště odstavci 3.1, 4.1 ([COD13](http://www.cacert.org/policy/AssurancePolicy.php)).

**CA.** Certifikační autorita je dále vázána dokumentem CCS (Konfigurace-řídicí specifikace).

**Prodejci třetích stran.** Distributoři kořenových certifikátů dostávají nabídku „Prodejci třetích stran – dementi a licence“ (3PV-DaL => CODx) a je jim nabídnuta táž pozice jako Členům, jestliže souhlasí stát se Členy komunity.

### 9.7 Dementi garancí

Osobám, které neakceptují uvedené dohody, je nabízena dohoda „Nezapojené osoby – dementi a licence“ (NRP-DaL, [COD4](http://www.cacert.org/policy/NRPDisclaimerAndLicence.php)). Jakékoli reprezentace a záruky jsou přísně omezeny na nominální použití. V podstatě: nezapojené osoby (NRP) mohou POUŽÍVAT, ale nesmí SPOLÉHAT.

V dnešním prostředí agresivních podvodů a v kontextu CAcert jako komunitní certifikační autority (CA)by měly všechny strany chápat, že CAcert a jeho odběratelé, zaručovatelé a další role poskytují služby na základě nejlepšího úsilí (Best Effort). Viz §1.4. CAcert se snaží dosáhnout přiměřené minimální úrovně kvality služeb svým Členům bez nadměrných rizik u nezapojených osob (NRP). Viz [Principy](http://svn.cacert.org/CAcert/principles.html).

CAcert v zastoupení komunity a sebe sama nevytváří garance, záruky ani přísliby, že služba nebo certifikáty jsou přiměřené potřebám a okolnostem.

### 9.8 Omezení odpovědnosti

??? [9.9 = 9.8.1; 9.10 = 9.8.2; 9.11 = 9.8.3]

### 9.9 Nezapojené osoby

CAcert v zastoupení souvisejících stran (RA[zaručovatelů], odběratelů atd.) a sebe sama odmítá veškerou odpovědnost za NRP při jejich používání certifikátů CAcert. Viz NRP-DaL ([COD4](http://www.cacert.org/policy/NRPDisclaimerAndLicence.php)).

### 9.10 Odpovědnost mezi Členy

Odpovědnosti mezi Členy se zabývá řešení vnitřních sporů, které řídí odpovědnost a jakékoli hranice. Viz §9.13.

### 9.11 Odškodnění

Žádné podmínky.

### 9.12 Lhůta a ukončení

#### 9.12.1 Lhůta

Žádné podmínky.

#### 9.12.2 Ukončení

Pro ukončení dohody založí Členové spor. Viz § 9.13 a Dohodu komunity CAcert (CCA) 3.3 ([COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php#3.3)).

Různé dokumenty (včetně ukončení) jsou pod [COD1](http://www.cacert.org/policy/PolicyOnPolicy.php).

Ukončení CA viz §5.8.1.

#### 9.12.3 Účinek ukončení a přežití

Žádné podmínky.

### 9.13 Individuální oznámení a komunikace s účastníky

Všichni účastníci jsou povinni udržovat svoje primární e-mailové adresy, uvedené v seznamu, v dobrém funkčním stavu. Viz Dohoda komunity CAcert (CCA) 3.5 ([COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php#3.5)).

### 9.14 Změny

Změny tohoto dokumentu (CPS) jsou řízeny [COD1](http://www.cacert.org/policy/PolicyOnPolicy.php). Jakékoli změny členských dohod jsou zaznamenány podle Dohody komunity CAcert (CCA) 3.4 ([COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php#3.4)).

### 9.15 Opatření k řešení sporů

CAcert poskytuje každému Členovi nebo jiné zúčastněné straně fórum a prostředek k založení sporu.

* Pravidla řešení sporů jsou v Zásadách řešení sporů (CAcert COD7).
* Založení (podání) sporu se provádí e-mailovou zprávou na support(zavináč)cacert.org.

Členové souhlasí, že předloží veškeré spory fóru CAcert k řešení. Pravidla obsahují speciální opatření pro pomoc nečlenům a dalším založit spor na tomto fóru.

### 9.16 Nadřazený zákon

Nadřazený zákon je zákon Nového Jižního Walesu v Austrálii. Obecně jsou podle tohoto zákona spory vyslechnuty arbitrem. Výjimečně si může arbitr zvolit, že aplikuje obecný zákon stran a událostí, to však není pravděpodobné, protože výsledky mohou být v rozporu s komunitou.

### 9.17 Shoda s aplikovatelným právem

??? [9.18 = 9.17.1; 9.19 = 9.17.2]

### 9.18 Zákon o digitálním podpisu

V Commonwealthu a australských státech prošly různé zákony o elektronických transakcích, které se zabývají digitálními podpisy. Souhrnně tyto zákony hovoří o „technologicky neutrálním“ modelu a povolují, ale neregulují, použití digitálních podpisů.

To znamená zvláště, že podpisy vytvořené certifikáty vydanými CAcert nejsou samy o sobě právně závaznými podpisy lidí, alespoň podle australských zákonů. Viz §1.4.3. Avšak certifikáty mohou hrát svou roli ve větších podepisujících aplikacích. Viz §1.4.1, „digitálně podepisující“ certifikáty. Tyto aplikace mohou ukládat stranám významné závazky, rizika a odpovědnosti.

### 9.19 Zákon o ochraně soukromí

Viz Zásady ochrany soukromí (Privacy Policy, [COD5](https://www.cacert.org/policy/PrivacyPolicy.html)).

### 9.20 Právní proces pro vnější fóra

CAcert bude poskytovat informace o svých Členech pouze po legální soudní obsílce nebo ekvivalentním procesu soudu kompetentní justice. Všechny žádosti z legálních obsílek se posuzují podle Zásad řešení sporů (Dispute Resolution Policy, DRP), viz §9.13 a [COD7](http://www.cacert.org/policy/DisputeResolutionPolicy.php). Tedy všechny žádosti se považují za spory, k jejichž řešení je oprávněn a má autoritu jen řádně jmenovaný arbitr, který má také autoritu vydat nařízení v případech takových žádostí.

Soudní obsílka by měla obsahovat dostatečnou právní základnu k podpoře arbitra v plnomocném rozhodnutí, že budou uvolněny informace vztahující se k podání [založení sporu], včetně jmen / názvů strany reklamující v občanskoprávní věci a indikace, zda jsou tyto strany Členy nebo nejsou (a tedy jsou předmětem Zásad řešení sporů [Dispute Resolution Policy, DRP]).

### 9.21 Různá ustanovení

#### 9.21.1 Celková dohoda

Všichni Členové komunity souhlasí s Dohodou komunity CAcert (Cacert Community Agreement, CCA, [COD9](http://www.cacert.org/policy/CAcertCommunityAgreement.php)). Tato dohoda včleňuje také jiné klíčové dokumenty, jako tento dokument Přehled postupů certifikace (Certification Practice Statement, CPS), Zásady řešení sporů (Dispute Resolution Policy, DRP) a Zásady ochrany soukromí (Privacy Policy, PP). Viz Dohoda komunity CAcert (CAcert Community Agreement, CCA) 4.2.

Dokument Konfigurace-řídicí specifikace (Configuration-Control Specification, CCS) je sada zásad, kterými se komunita řídí, a jejíž částí jsou výše uvedené dokumenty. Viz COD2. Dokumenty, které dosáhly konečného stavu ZÁSADY (POLICY), jsou uloženy na [www.cacert.org/policy/](http://www.cacert.org/policy/)[.](http://www.cacert.org/policy/.A%C4%8Dkoli) Ačkoli podrobné praktiky lze najít i na jiných místech na webu a na [wiki](http://wiki.cacert.org/), dokumenty CCS, které dosáhly stavu KONCEPT a ZÁSADY, jsou řídicí dokumenty.

#### 9.21.2 Přiřazení

Práva uvedená v Dohodě komunity CAcert (CCA) nemohou být přiřazena obvyklým způsobem.

#### 9.21.3 Oddělitelnost

Žádné podmínky.

#### 9.21.4 Vynucení (poplatky právnímu zástupci a zřeknutí se práv)

Výši poplatků stanoví arbitr. Pokud existují náhrady, stanoví jejich výši rovněž arbitr.

#### 9.21.5 Force majeure [vyšší moc]

Žádné podmínky.

# --- Zde končí tyto zásady ---