# Konfigurace-Řídicí Specifikace

|  |  |
| --- | --- |
| Název: CCS [COD2](https://svn.cacert.org/CAcert/Policies/ControlledDocumentList.html)  Datum vytvoření: 20091214  Editor: Iang  Stav: POLICY [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! |  |
|

### Úvod

Konfigurace-Řídicí Specifikace (Configuration-Control Specification, CCS COD2) řídí a sleduje ty dokumenty, procesy a aktiva, která jsou kritická pro činnost, bezpečnost a dohled nad působením CAcert.

Tento dokument je procedura pro CCS. Tento dokument samotný je komponentou CCS, viz §2. Všechna ostatní dokumentace a proces specifikovaný uvnitř je odvozený a je řízen CCS.

CCS je formátován, inspirován a navržen, aby vyhověl potřebám kritéria Davida Rosse (David Ross Criterium - [Certificate Authority Review Checklist](http://rossde.com/CA_review/)) - sekce A.1 (DRC-A.1) CCS lze chápat jako index do systémového auditu podle DRC.

### Dokumenty

#### Seznam řízených dokumentů

Tento dokument (CCS) tvoří Seznam řízených dokumentů (Controlled Document List, CDL) primárních neboli "kořenových" dokumentů zvaných též Zásady (Policies). Primární dokumenty mohou autorizovat jiné, sekundární dokumenty pro připojení k CDL, neboli "působit" mimo seznam.

Seznam řízených dokumentů obsahuje čísla, umístění a stav všech řízených dokumentů. Seznam je součástí tohoto CCS.

#### Změny

Změny do dokumentů probíhají podle specifikace v Zásadách ohledně zásad (Policy on Policy, PoP). [CDL](https://svn.cacert.org/CAcert/Policies/ControlledDocumentList.html) spravuje Důstojník zásad.

#### Řízení

Zásady CAcert musí být vlastněny / přeneseny do CAcert. Viz Zásady ohledně zásad (PoP) 6.2.

### Hardware

#### Seznam řízeného hardware

Kritické systémy [tj. nezbytné pro činnost CAcert; pozn. překl.] jsou definovány Zásadami bezpečnosti (Security Policy).

#### Změny

Viz Zásady bezpečnosti (Security Policy).

#### Řízení

Zásady bezpečnosti (Security Policy) dávají exekutivní odpovědnost za hardware Výboru (Board of) CAcert Inc. Přístup je delegován Inženýrům přístupu (Access Engineers, SP 2) a Správcům systémů (Systems Administrators, SP 3). Právní vlastnictví může být smluvně delegováno na jiné organizace (SP 9.4).

### Software

#### Seznam řízeného software

Kritický software je definován Zásadami bezpečnosti.

#### Změny

Viz Zásady bezpečnosti.

#### Řízení

CAcert vlastní svůj kód, nebo požaduje plné oprávnění k používanému kódu „s otevřeným zdrojem (open source)“ pomocí ověřené, bezplatné a otevřené licence. Takový kód musí být identifikován a spravován hodnotitelem softwaru.

Vývojáři přenášejí plná práva na CAcert (podobným způsobem jako dokumenty), nebo organizují své příspěvky podle správného bezplatného a otevřeného režimu zdrojového kódu, režimu schváleného Výborem. Tam, kde je kód publikován (mimo rozsah tohoto dokumentu), je nutno předejít porušení licenčních podmínek - například záležitosti prolínání s GPL [GNU Public License – pozn. překl.].

Vedoucí týmu hodnotitelů softwaru udržuje registr přidělování titulů (názvů) nebo plnou licenci a registr software podle schválených licencí pro otevřené zdroje (open source).

### Certifikáty

Tato sekce se vztahuje na kořenové a zprostředkující (Sub-root) certifikáty, ne na certifikáty pro koncovou entitu (odběratele, člena).

#### Seznam certifikátů

Certifikáty (kořenové a zprostředkující) mají v CPS svůj seznam.

#### Změny

Tvorba a použití certifikátů je řízena Zásadami bezpečnosti. Používání certifikátů je řízeno Vyhláškou o použití certifikátů (Certification Practice Statement).

#### Archiv

Viz Zásady bezpečnosti.

### Deníky (Logs)

#### Seznam řízených deníků

Deníky jsou definovány Zásadami bezpečnosti.

#### Změny

Změny hardware, software a kořenových certifikátů jsou zapisovány do deníků v souladu se Zásadami bezpečnosti.

#### Archiv

Viz Zásady bezpečnosti.

### Data

#### Typy dat

Typy citlivých údajů o členech definují Zásady zaručování (Assurance Policy).

#### Změny

Změny a přístup k citlivým údajům o členech jsou definovány podle Zásad zaručování, Dohody komunity CAcert (CAcert Community Agreement) a Zásad řešení sporů (Dispute Resolution Policy). Implementace kolekce a paměť pro citlivé údaje o členech (programy uživatelského rozhraní a databáze) je definována Zásadami bezpečnosti (Security Policy).

#### Archiv

Uchovávání dat je řízeno Zásadami bezpečnosti (Security Policy) a Dohodou komunity CAcert (CAcert Community Agreement).