|  |  |
| --- | --- |
| Název: SP [COD8](https://svn.cacert.org/CAcert/Policies/ControlledDocumentList.html)  Datum vytvoření: 20090216  Editor: iang  Stav: POLICY [p20140731](#p20140731)  Licence: [CC-by-sa+DRP](#Licence)  Český překlad: alkas POZOR! Tento překlad slouží k pochopení popisovaného tématu. Právní platnost má POUZE anglický originál! |  |
|  |

# Zásady bezpečnosti systémů CAcert

## 1. Úvod

### 1.1. Motivace a rozsah platnosti

Tyto Zásady bezpečnosti (Security Policy) určují zásady pro bezpečnou činnost kritických počítačových systémů CAcert. Tyto systémy jsou:

1. Fyzický hardware, základ pro logické služby
2. Webový server + databáze (centrální server(y))
3. Podepisovací služba (podepisovací server)
4. Zdrojový kód (změny a opravy)

Výbor CAcert, Inc. (dále "výbor") může do Příručky bezpečnosti (Security Manual) přidat další komponenty.

#### 1.1.1. Role obsluhy

Jsou obsazeny kritické [stěžejní, nejdůležitější pro činnost] role. Jsou definovány takto:

* Inženýr přístupu (Access Engineer)
* Správce systémů (Systems Administrator)
* Inženýr podpory (Support Engineer)
* Poradce ve věcech softwaru (Software Assessor)

#### 1.1.2. Mimo rozsah platnosti

Nekritické systémy nejsou popsány touto příručkou, ale mohou být podle ní zavedeny a ovlivněny, pokud se nacházejí v bezpečnostním kontextu. Architektura je také mimo rozsah, viz Certification Practise Statement (??? CAcert Policy Statement? V orig. pouze CPS!) [CPS]#6.2.

### 1.2. Principy

Důležité principy těchto Zásad bezpečnosti (Security Policy) jsou:

* *Dvojité řízení* – řídit úkol musí aspoň dva lidé
* *Čtyři oči* – na úkolu se musí podílet aspoň dva lidé: vykonavatel a pozorovatel.
* *Nadbytečnost (redundance)* – žádná osoba není jediná oprávněná provést jakýkoli úkol.
* *Zabezpečené úložiště (escrow)* – kde jsou uloženy citlivé údaje (zálohy, hesla) s jinými součástmi (partiemi).
* *Žurnál* – události jsou zapisovány do souboru.
* *Rozdělení účasti (separation of concerns)* – když je stěžejní úkol rozdělen mezi dvě osoby z různých oblastí.
* *Audit* – když pověřený externista kontroluje praktiky a zásady.
* *Autorita* – každá akce je oprávněna buď zásadami, nebo arbitrem.

Každý úkol nebo akce je zajištěn/a různými ochranami odvozenými z výše uvedených principů.

### 1.3. Definice termínů

*Inženýr přístupu (Access Engineer*)

Člen, který obsluhuje kritický hardware, včetně údržby, řízení přístupu a fyzické bezpečnosti. Viz §1.1.

*Poradce ohledně softwaru (Software Assessor*)

Člen, který reviduje opravy („záplaty“, patches) co do bezpečnosti a funkčnosti, signs-off na nich, a začleňuje je do úložiště (repozitáře, repository). Viz §7.2.

*Inženýr podpory (Support Engineer*)

Člen, který spravuje seznam podpory a má přístup k citlivým údajům pomocí online rozhraní. Viz §8.

*Správce systémů (Systems Administrator*)

Člen, který obsluhuje klíčové systémy a má přístup k bezpečnostně citlivým funkcím nebo údajům.

### 1.4. Dokumenty a řízení verzí

#### 1.4.1. Dokument Zásady bezpečnosti (Security Policy)

Tyto Zásady bezpečnosti jsou částí Konfigurace-řídicí specifikace pro účely auditu (DRC-A.1). Je řízen Zásadami ohledně zásad (Policy on Policy) pro účely řízení verzí.

Tento dokument zásad popisuje, co je už provedeno, namísto „jak to provést“. **Některé sekce jsou prázdné, což znamená "odkaz do Příručky".**

#### 1.4.2. Dokument Příručka bezpečnosti (Praktiky) - Security Manual (Practices)

Tyto zásady výslovně přesouvají podrobné bezpečnostní praktiky do Příručky bezpečnosti ([Security Manual](http://wiki.cacert.org/SecurityManual), "SM"). Příručka bezpečnosti popisuje, jak je vše provedeno. Protože praktiky se občas mění, také mezi každou událostí praktik, je Příručka bezpečnosti pod přímým řízením příslušných vedoucích týmů. Je umístěna na CAcert wiki a podléhá řízení verzí.

Sekce Záhlaví (Headings) je v obou dokumentech stejná. Pokud jsou sekce v jednom dokumentu prázdné, očekává se, že budou dokumentovány v druhém. "Dokument dále v Příručce bezpečnosti (Document further in Security Manual)" lze vyvodit z jakékoli sekce záhlaví v Zásadách.

#### 1.4.3. Bezpečnostní procedury

Týmoví vedoucí mohou občas výslovně přesunout jednoduché, soudržné komponenty bezpečnostních praktik do samostatných dokumentovaných procedur. Každá procedura bude ovládána na stránce wiki a bude pod její kontrolou, pravděpodobně na [SystemAdministration/Procedures](http://wiki.cacert.org/SystemAdministration/Procedures). Každá procedura musí mít výslovný odkaz v Příručce bezpečnosti (Security Manual).

## 2. FYZICKÁ BEZPEČNOST

### 2.1. Zařízení

CAcert hostuje klíčové servery ve vysoce bezpečném zařízení. Platí zde nezávislé ověřování fyzické a přístupové bezpečnosti.

### 2.2. Fyzická aktiva

#### 2.2.1. Počítače

Počítač budou před uvedením do provozu inventarizovány. Seznam inventáře musí být přístupný všem Inženýrům přístupu (Access Engineers) a všem Správcům systémů (Systems Administrators). Seznam musí podléhat změnovému řízení.

Každá jednotka bude jednoznačně a odlišně identifikována na všech viditelných stranách. Stroje budou uzavřeny v zabezpečeném zařízení (klece a/nebo uzamčené rošty [racks]).

#### 2.2.1.1 Akvizice

Vybavení pro klíčové účely bude získáno způsobem, který minimalizuje předakvizi

ní bezpečnostní riziko.

#### 2.2.2. Služba

Vybavení, které je předmětem bezpečnostně rizikové služby, musí být ukryto/utajeno, je-li služba požadována. See also §2.2.3.3.

#### 2.2.3. Média

#### 2.2.3.1 Bezpečnostní opatření

Paměťová média (diskové jednotky, pásky, vyměnitelná média) je při akvizici inventarizováno a je sledováno jeho použití.

Nové paměťové médium (disk nebo vyměnitelné) bude před použitím bezpečně vymazáno a přeformátováno.

#### 2.2.3.2 Paměť

Vyměnitelné médium bude vždy bezpečně uloženo, i když se nepoužívá. Jednotky uchovávané pro opětné použití jsou před uložením bezpečně vymazány. Opětné použití smí být pouze v kritických systémech.

Nastane-li změna stavu média, zapíše se do deníku hlášení udávající nový stav.

#### 2.2.3.3 Konec používání

Paměťová média, která obsahují kritická data a mají být ze služby odebrána, budou zničena nebo jinak zajištěna. Provést tyto kroky:

1. Médium je bezpečně zničeno, **nebo**
2. Médium je bezpečně vymazáno a bezpečně uloženo.

Záznamy o bezpečném vymazání a metoda konečné likvidace bude sledována v inventáři aktiv. Když jde o kritická data, musí ukončení každého kroku označit dva systémoví správci.

### 2.3. Fyzický přístup

V souladu s principem dvojího řízení musí být na místě alespoň dvě osoby s oprávněním přístupu zároveň, aby mohl být fyzický přístup povolen.

#### 2.3.1. Oprávnění přístupu

Přístup k fyzickému zařízení musí být autorizován.

#### 2.3.2. Profily přístupu

Příručka bezpečnosti musí uvádět různé profily přístupu. Alespoň jeden Inženýr přístupu musí ve všech případech řídit přístup. Při logickém přístupu musí být přítomen aspoň jeden Správce systémů. Za přítomnosti Správce systémů je možný pouze nejzákladnější a nejbezpečnější přístup.

Neexistují žádná vlastní oprávnění k přístupu k datům. Správci systémů jsou oprávněni přistupovat k „syrovým“ datům podle těchto zásad. Nikdo další nesmí k „syrovým“ datům přistupovat. Všichni odpovídají za ochranu dat před přístupem neoprávněných osob.

#### 2.3.3. Zaznamenávání přístupu

Všechny fyzické přístupy jsou zaznamenány a hlášeny všem.

#### 2.3.4. Nouzový přístup

Pro nouzový přístup nesmí existovat žádná procedura. Pokud podle úsudku Správce systémů je nezbytné získat nouzový přístup za účelem vyhnout se vážnému poškození, je nutno co nejdříve vyhledat nezávislé oprávnění vydané arbitrem. Viz Zásady řešení sporů (DRP).

#### 2.3.5. Kódy a zařízení fyzické bezpečnosti

Všichni pracovníci, kteří vlastní kódy fyzické bezpečnosti a zařízení (klíče), musí být oprávněni a dokumentováni.

## 3. LOGICKÁ BEZPEČNOST

### 3.1. Síť

#### 3.1.1. Infrastruktura

Současné a úplné diagramy fyzické a logické infrastruktury sítě CAcert jsou udržovány vedoucím týmu Správců systémů. Tyto diagramy obsahují popis kabeláže, podrobnosti konfigurace fyzických portů, očekávané / povolené směry toku dat a všechny další stálé informace podle potřeby. Diagramy jsou revidovány a musí být při každé změně aktualizovány.

##### 3.1.1.1. Vnější konektivita

Zvenku jsou viditelné pouze takové služby, které jsou potřebné pro normální provoz; systémy a servery, které nevyžadují přístup k Internetu pro svou normální činnost, nesmí takový přístup dostat. Stane-li se takový přístup dočasně potřebným pro nějaký oprávněný úkol správy, může být takový přístup udělen podle procedur správy systémů a musí být ohlášen a zaznamenán.

##### 3.1.1.2. Vnitřní konektivita

Vnitřní spojení systémů a serverů do infrastruktury CAcert jsou udržována na minimu nutnému pro rutinní operace. Každá nově požadovaná konektivita musí být vyžádána a schválena vedoucí týmu správců systému a pak se musí objevit v příslušném diagramu (diagramech) infrastruktury.

#### 3.1.2. Operační konfigurace

##### 3.1.2.1. „Přítok“

Všechny porty, na nichž se očekává příchozí provoz, musí být dokumentovány; provoz do ostatních portů musí být blokován. Neočekávaný provoz musí být zaznamenán jako výjimka.

##### 3.1.2.2. „Výtok“

Veškerý zahájený odchozí provoz musí být dokumentován; provoz na jiná místa určení musí být blokován. Neočekávaný provoz musí být zaznamenán jako výjimka.

#### 3.1.3. Detekce narušení

Záznamy jsou (manuálně nebo automaticky) pravidelně zkoumán na neobvyklé vzorky a/nebo provoz; anomálie jsou zkoumány, jakmile se vyskytnou a jsou hlášeny odpovědným osobám téměř v reálném čase (například textová hlášení, e-mail) a co nejdříve prozkoumány. Podezřelé aktivity, které mohou indikovat skutečné narušení systému nebo vniknutí do něj, spustí protokol odpovědi na incident, popsaný v sekci 5.1.

### 3.2. Operační systém

Jakýkoli operační systém použitý na strojích - kritických serverech musí být dostupný pod softwarovou licencí open-source schválenou OSI.

#### 3.2.1. Šifrování disku

Jakýkoli operační systém použitý na kritických serverových strojích musí podporovat softwarové šifrování celého disku nebo diskového oddílu, a tato možnost šifrování musí být zapnuta pro všechny relevantní disky nebo oddíly při první instalaci operačního systému na daném stroji.

#### 3.2.2. Operační konfigurace

Servery musí zapnout pouze ty funkce operačního systému, které jsou nutné k podpoře potřebných služeb. Možnosti a „balíčky“ vybrané při instalaci operačního systému jsou dokumentovány. Nově instalované systémy musí prozkoumány k zajištění, že jsou aktivní pouze požadované služby a jejich funkčnost je omezena konfiguračními volbami. Veškerý požadovaný aplikační software musí používat podobné techniky k zajištění minimální vystavené stopy [tj. aby o sobě navenek prozradil co nejméně].

Dokumentaci pro instalaci a konfiguraci serverů s příslušnými softwarovými balíčky a konfiguracemi udržují Správci systémů.

#### 3.2.3. Opravy-záplaty (patching)

Software použitý na provozních serverech musí být udržován aktuální vzhledem k opravám ovlivňujícím softwarovou bezpečnost. Aplikace oprav musí být schválena vedoucím týmu Správců systémů, plně dokumentována v denících a ohlášena e-mailem seznamu Správců systémů při svém dokončení (viz §4.2).

##### 3.2.3.1. Nouzové „záplatování” (opravy)

Aplikace opravy je považována za *nouzovou,* když vejde ve známost, že lze zneužít slabinu určité části softwaru (na serverech umožňujících přímý přístup místních uživatelů; nouzové místní zneužití může být také považováno za stav nouze). Aplikace oprav má v tomto případě nastat co nejdříve a obejít normální postup změn konfigurace. Vedoucí týmu Správců systémů musí buď schválit opravu, nebo nařídit nápravnou akci a oznámit případ založením sporu.

**Deklarace nouzové opravné situace nemá nastávat pravidelně.** Vedoucí týmu musí nouzové opravy dokumentovat v pravidelných přehledech pro Výbor, nezávisle na založených sporech.

### 3.3. Aplikace

Žádosti na ad hoc dotazy do databáze aplikací pro pracovní nebo podobné účely musí být schváleny arbitrem.

### 3.4. Řízení přístupu

Veškerý přístup ke kritickým údajům a službám je řízen a protokolován.

#### 3.4.1. Přístup k aplikacím

Obecný přístup Členů je poskytován aplikací sloužící jen k tomu účelu. Obecně jsou funkce zpřístupněny podle bodů zaručení a podobnými metodami řízenými softwarovým systémem.

#### 3.4.2. Zvláštní oprávnění

Přídavný nebo zvláštní přístup se uděluje podle oprávnění uvedených v těchto řídicích seznamech přístupu (viz §1.1.1):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Název seznamu** | **Kdo** | **Účel přístupu** | **Vztah** | **Manažer** |
| Seznam fyzického řízení | Inženýři přístupu | Řízení přístupu personálu k hardwaru | bez jiných rolí | Vedoucí týmu přístupu |
| Seznam fyzického přístupu | Správci systémů | Úroveň hardwaru pro instalaci a obnovu ze zálohy | Výhradně s Inženýry přístupu a Poradci ohledně softwaru | Vedoucí týmu Správců systémů |
| Seznam přístupu SSL | Správci systémů | Úroveň Unix shellu / účtu / | Standardně všichni na Seznamu fyzického přístupu | Vedoucí týmu Správců systémů |
| Seznam přístupu k úložišti | Poradci ohledně softwaru | Změna úložiště zdrojového kódu | Výhradně s Inženýry přístupu a Správci systémů | Vedoucí týmu Poradců ohledně Softwaru |
| Seznam přístupu podpory | Inženýr podpory | Funkce podpory ve webové aplikaci | Výhradně s Inženýry přístupu a Správci systémů | Vedoucí týmu podpory |

Všechny změny personálu uvedených seznamů musí schválit Výbor.

#### 3.4.3. Ověření totožnosti (identifikace, authentication)

Kde je to možné, použijí se silné metody identifikace. Všechna schémata identifikace musí být dokumentována.

#### 3.4.4. Odebrání přístupu

Akce vedoující k ukončení musí být dokumentovány. Viz §9.1.7.

## 4. PROVOZNÍ BEZPEČNOST

### 4.1. Správa systému

Primární úkoly Správy systémů se provádějí podle principu „čtyř očí“. Tyto úkoly jsou: ověření výkonnosti záloh, aplikace oprav softwaru, vytvoření a smazání účtu a údržba hardwaru.

#### 4.1.1. Privilegvané účty a hesla

Přístup k privilegovaným účtům (účet správce „root“ a uživatelský účet pomocí SSH nebo konsoly) musí být přísně řízen. Hesla a privátní klíče SSH použité pro vstup do systémů musí být ve všech případech utajena před správci systémů CAcert.

##### 4.1.1.1. Oprávnění uživatelé

Pro přístup k účtům jsou oprávněni pouze Správci systémů uvedení na seznamech přístupů v §3.4.2. Vedoucí týmu Správců systémů může dočasně povolit Poradcům softwaru přístup k aplikaci pomocí SSH za účelem hloubkového ladění, nebo na zvláštní příkaz arbitra.

##### 4.1.1.2. Přístup k systémům

Všechny přístupy jsou zabezpečené, žurnálované a monitorované.

##### 4.1.1.3. Změny

Procerura pro změnu hesel a klíčů SSH je dokumentována.

#### 4.1.2. Požadovaná doba odezvy týmu

Doby odpovědi jsou dokumentovány pro plánování obnovy z havárie (Disaster Recovery). Viz §6.

#### 4.1.3. Změna procedur správy

Všechny změny systémové konfigurace musí být zaznamenány a hlášeny v pravidelných přehledech Výboru CAcertu.

#### 4.1.4. Outsourcing (vnější správa a dohled)

### 4.2. Vedení žurnálu

#### 4.2.1. Pokrytí

Všechny citlivé události musí být spolehlivě zaznamenány. Záznamy budou zrušeny po uplynutí doby dokumentované v Příručce bezpečnosti.

#### 4.2.2. Přístup a zabezpečení

Přístup k žurnálům musí být omezen. Bezpečnost záznamů bude dokumentována. Také doba uchovávání žurnálů musí být dokumentována.

#### 4.2.3. Automatizované žurnály

Záznam žurnálů bude automatizován a k zálohám se použijí příslušné automatizované systémem poskytnuté nástroje. Automatizované záznamy budou periodicky prohlíženy; podezřelé události budou označeny a včas prozkoumány.

#### 4.2.4. Provozní (ruční) záznamy

Změny konfigurace, ať jakkoli malé, musí být zapsány.

Všechny fyzické návštěvy musí být zapsány; návštěvník a Inženýr přístupu podají hlášení.

### 4.3. Záloha

Procedury pro všechny zálohy musí být dokumentovány podle následujících pod-odstavců.

#### 4.3.1. Typ

Je třeba pořizovat provozní zálohy a zálohy pro obnovu po havárii (disaster recovery). Provozní zálohy mohou být on-line a místní. Zálohy pro případ havárie musí být off-line a vzdálené.

#### 4.3.2. Četnost

#### 4.3.3. Paměť

Zálohy musí být chráněny na téže úrovni jako samotné kritické systémy. Zálohy pro případ havárie mohou být distribuovány.

#### 4.3.4. Doba použití a opětovné použití

Viz §2.2.3.

#### 4.3.5. Šifrování

Zálohy musí být zašifrovány a musí být přenášeny pouze zabezpečenými kanály. Zálohy uložené mimo sídlo musí být dvojitě zašifrovány s použitím různých metod.

#### 4.3.6. Ověřování záloh

K ověření zálohy je třeba dvou Správců systému CAcert. Pokud jsou klíč a záloha pohromadě, musí být dodržen princip čtyř očí. Další účely kromě ověření úspěšné zálohy viz dále.

#### 4.3.7. Správa klíčů

Zašifrované klíče musí bezpečně uložit Správci systémů CAcert. S příručkami zálohování musí být uložena i papírová dokumentace.

#### 4.3.8. Čtení záloh

Podmínky a procedury pro zkoumání záloh musí být dokumentovány a být pod dohledem arbitra, jsou-li použity pro jiné účely než ověření a obnova.

### 4.4. Doba uložení dat

#### 4.4.1. Uživatelská data

Ukončení dat uživatele je pod řízením arbitra. Viz CCA.

#### 4.4.2. Systémové žurnály (logs)

Viz §4.2.1.

#### 4.4.3. Hlášení incidentů

Viz §5.6.

## 5. ODEZVA NA INCIDENT

### 5.1. Incidenty

### 5.2. Detekce

Standard pro monitorování, výstrahy a hlášení musí být dokumentován.

### 5.3. Okamžitá akce

#### 5.3.1. Závažnost a priorita

Při zjištění incidentu se musí provést počáteční odhad závažnosti a priority.

#### 5.3.2. Komunikace

Počáteční hlášení musí jít jako oběžník.

Pro přímou podporu při vysoké prioritě nebo vysoké závažnosti incidentu bude založeno komunikační fórum.

#### 5.3.3. Eskalace

Bude založen proces eskalace pro účely přehledu a správy, úměrně k závažnosti a prioritě. Přehled začíná „čtyřma očima“ a končí u arbitra. Správa začíná vedoucím týmu a končí u Výboru.

### 5.4. Vyšetřování

Incidenty musí být vyšetřeny. Vyšetřování musí být dokumentováno. Je-li závažnost incidentu vysoká, musí být důkaz zabezpečen a eskalován arbitrovi.

### 5.5. Odezva

### 5.6. Hlášení

Hlášení o incidentu musí být publikováno. Hlášení incidentu se píše v závěru vyšetřování. K dokumentaci vyšetřování bude připojena jeho úplná kopie. Citlivé údaje mohou být vytaženy may be do přílohy hlášení, do níž bude omezen přístup. Vedoucí týmu Správců systémů odpovídá za publikaci a údržbu.

Incidenty nejsou obvykle utajené ani důvěrné a informace o postupu jsou publikovány co nejdříve. Existence události, způsob ani metody jejího zpracování nemusí být utajeny. Viz §9.5.

## 6. OBNOVA PO HAVÁRII

Za obnovu po havárii odpovídá Výbor CAcert, Inc.

### 6.1. Provozní procesy

Výbor musí vytvořit a udržovat dokumentaci provozních procesů. Na tomto seznamu musí být určeny jádrové procesy pro účely kontinuity procesu / obnovy po havárii.

### 6.2. Časy obnovy

Výbor identifikuje standardní časy pro všechny procesy a musí stanovit maximální přípustné výpadky a cílové doby obnovy jádrových procesů.

### 6.3. Plán

Výbor musí mít základní plán obnovy.

### 6.4. Seznam klíčových osob

Výbor musí udržovat seznam klíčových osob s veškerými potřebnými informacemi. Viz §10.1. Seznam musí být dostupný, i když infrastruktura CAcertu není přístupná.

## 7. POSOUZENÍ SOFTWARU

Tým posuzování softwaru odpovídá za bezpečnost a údržbu kódu.

### 7.1. Autorita

Zdrojový kód je podle Konfigurace – řídicí specifikace (CCS). Přídavky k týmu jsou předmětem schválení Výborem. Viz §3.4.2.

### 7.2. Úkoly

Primární úkoly posuzovatelů softwaru jsou:

1. Keep the code secure in its operation,
2. Fix security bugs, including incidents,
3. Audit, Verify and sign-off proposed patches,
4. Provide guidance for architecture,

Software assessment is not primarily tasked to write the code. In principle, anyone can submit code changes for approval.

### 7.3. Repository

### 7.4. Prohlídka

Vedoucí týmu nebo jeho stanovený zástupce odhlašuje opravy. Každá změna softwaru musí být posouzena jinou osobou než autorem. Autor a odepisující osoby musí být zaznamenány do deníku. Čím riskantnější je zdroj, tím více prohlídek je nutno dělat.

### 7.5. Test a chyby

Tým softwarových poradců udržuje testovací systém. Každá oprava bude vytvořena a testována. Stav testu každé opravy musí být zaznamenán.

Tým posouzení softwaru udržuje systém registrace chyb. Primární komunikace prochází tímto systémem. Přístup správce je třeba udělit všem Poradcům softwaru, vývojářům softwaru a Správcům systému. Přístup pro předložení chyby bude poskytnut každému Členu, který o něj požádá.

### 7.6. Výroba

## 8. PODPORA

### 8.1. Autorita

Softwarové rozhraní obsahuje funkce pro Inženýra podpory. Přístup ke zvláštním funkcím podléhá přísné kontrole. Přidávaní členové týmu podléhají schválení Výborem a funkce softwaru podléhají Konfiguraci – řídicí specifikaci (CCS). Viz §3.4.2.

Inženýři podpory nemají žádnou vlastní autoritu provést jakoukoli akci, musí získat autoritu případ od případu. Autorita vyžadovaná každým případem musí být vedena těmito zásadami nebo Příručkou bezpečnosti nebo jiným zjevně aplikovatelným dokumentem. Není-li Členova autorita zpochybněna, může Člen tuto autoritu poskytnout. Pokud ne, je třeba vyžádat si arbitrovu autoritu.

Inženýři podpory odpovídají za dodržování zásad a praktik.

### 8.2. Odpovědnosti

Inženýři podpory mají tyto odpovědnosti:

* Obnovit účet člena podle dokumentace v Příručce bezpečnosti.
* Odpověď na všeobecné žádosti Čenů o informace nebo vysvětlení. Inženýři podpory nemohou vytvořit závazné prohlášení. Odpovědi musí být založeny na zásadách a praktikách.
* Další úkoly a odpovědnosti specifikované jinými zásadami, například Zásadami řešení sporů (DRP).

### 8.3. Kanály

Podporu lze vždy vyžádat e-mailem u support(zavináč)cacert(tečka)org. Jiné kanály lze zpřístupnit a dokumentovat v Příručce bezpečnosti.

### 8.4. Záznamy a deníky (žurnály, logs)

* Použití rozhraní s omezeným přístupem musí být zapsáno do deníku.
* Všechny kanály podpory budou zaneseny do deníku.
* Soukromé žádosti o podporu je nutno ohlašovat v příslušných kanálech a také tam zaznamenávány (například CC [Carbon Copy v e-mailu]).

### 8.5. Arbitráž

Inženýři podpory předávají dotazy vyžadující autoritu arbitrovi a mohou také být být povoláni působit jako výchozí správci/manažeři případů. Viz Zásady řešení sporů (DRP) a [Příručka manažera případu.](https://svn.cacert.org/CAcert/Arbitration/arbitration_case_manager.html) Inženýři podpory musí znát tato témata, i když nejsou v seznamu arbitrů nebo manažerů případů.

### 8.6. Odkazy

## 9. ADMINISTRATIVA

### 9.1. Personální

#### 9.1.1. Role a odpovědnosti

* Inženýr přístupu: odpovídá za řízení přístupu k hardwaru a za údržbu hardwaru.
* Správce systému: odpovídá za údržbu jádrových služeb a za integritu.
* Poradce ve věcech softwaru: udržuje základ kódu a potvrzuje zabezpečení ("sign-off") oprav a vydaných verzí.
* Inženýr podpory: „lidské“ rozhraní uživatelů.
* Vedoucí týmů: koordinace týmů, hlášení Výboru.
* Všichni: odezvy na arbitrova nařízení změn. Odezva na kritické záležitosti zabezpečení. Pozorování.
* Výbor: opravňuje nové osoby a přístupy. Koordinuje všechny.
* Arbitr: vede ABC [arbitrovanou kontrolu pozadí]. Opravňuje výjimky zásad.

#### 9.1.2. Personální úrovně

Každý tým má nejméně dva členy dostupné kdykoli. Jednotlivci nikdy nejsou aktivní ve více než jednom týmu současně, ale měli by sledovat činnost ostatních týmů. Výlučnosti viz §3.4.2.

Jedna osoba v každém týmu, určená vedoucím týmu, podává hlášení Výboru.

#### 9.1.3. Práce s novými členy týmů

Noví členové týmů potřebují:

* Doporučení vedoucího týmu
* Arbitrovanou kontrolu „pozadí“ (Arbitrated Background Check, ABC)
* Oprávnění Výborem

Tým podporuje proces zařazování nových členů.

#### 9.1.4. Arbitrovaná kontrola „pozadí“ - procedury

Arbitrovaná kontrola „pozadí“ (ABC) musí být provedena podle směrnic arbitra s další osobou, manažerem případu, aby byly zajištěny „čtyři oči“. „ABC“ jsou prováděny s plnou vážností.

#### 9.1.4.1. Rozsah

Vyšetřování v rámci ABC obsahuje zkoumání:

* znalosti ve specifické oblasti
* porozumění dobré bezpečnostní praxe specifické oblasti
* historie aktivity v komunitě
* reputace a postavení uvnitř komunity
* poskytnuté reference
* konflikty zájmů

#### 9.1.4.2. Pokrytí

ABC je třeba vykonat pro každé osoby v kritické roli. Viz §1.1.1.

#### 9.1.4.3. Dokumentace

Proces ABC bude dokumentován jako procedura.

Dokumentace kontroly každé osoby je třeba uchovat s možností nahlédnutí při každé další arbitráži. Musí obsahovat:

* Souhlas s příslušnými zásadami, atd.
* Kontaktní údaje. Viz §10.1.

#### 9.1.4.4. Ochrana soukromí u kritických rolí

Okolnosti ochrany soukromí:

* procedura a směrnice (doporučení) jsou veřejné
* rozhovory, dokumenty nejsou veřejné,
* souhrn důkazů musí být v nařízení,
* arbitr může nařídit ukrýt otázky důkazů,
* kontaktní údaje budou uloženy do kontaktního adresáře.

Důvěryhodné role CAcert dávají určité soukromí pro ochranu soukromí ostatních.

#### 9.1.5. Oprávnění

Jak osoby, tak přístupy musí být oprávněny Výborem. Pouze Výbor může schválit nové osoby nebo jakékoli přístupy k systémům. Každá osoba bude navržena Výboru s platnou podpůrnou informací, viz výše.

Výbor by měl rokovat přímo a celý. Členové Výboru, kteří jsou aktivní v příslušné oblasti, se zdrží voleb, ale podpoří rokování. Úvahy a rozhodnutí budou dokumentovány. Všechny konflikty zájmů budou prozkoumány.

#### 9.1.6. Bezpečnost

Všechny osoby odpovídají za sledování a hlášení bezpečnostních záležitostí. Celý CAcert pozoruje vše, kdykoli je to možné. Každá osoba odpovídá za úspěšné řešení záležitostí, nebo zajistí, že budou úplně popsány v hlášení.

Viz §9.5.

#### 9.1.7. Ukončení role personálu

Důvodem ukončení přístupu může být odstoupení (výpověď), nařízení arbitra, nebo rozhodnutí Výboru či vedoucího týmu. Při ukončení (z kteréhokoli důvodu) musí být zabezpečen přístup a údaje. Viz §3.4.4.

Ustanovení o arbitráži přesahuje každé ukončení osob s kritickou rolí. To znamená, že i když osoba odstoupí z kritické role, je stále vázána Zásadami řešení sporů (DRP - COD7) a arbitr může obnovit jakékoli ustanovení této dohody nebo zavázat osobu nařízeními.

#### 9.1.8. HR [Human Resources, lidské zdroje] a školení

Odpovědností vedoucího týmu je koordinovat technické testování a školení, zvláště u nových členů týmu.

### 9.2. Správa kořenového klíče

#### 9.2.1. Generování kořenového klíče

Kořenové klíče se generují pouze na pokyn Výboru. Musí být generovány úplně dokumentovanou a prohlédnutou procedurou. Procedura musí obsahovat:

* Použití hardwaru vybudovaného bezpečně jen k danému účelu a ihned poté vyčistěného/smazaného/zničeného.
* Dvojitý dohled nad všemi fázemi, včetně Výboru.
* Silná sbírka primární entropie, oddělené od použití entropie.
* Denní testovací cykly procesu.
* Dokumentace každého provedeného kroku s postupem procedury.
* Každý účastník potvrdí provedený proces a jeho výsledky.

#### 9.2.2. Záloha a úschova

Kořenové klíče musí být uloženy na spolehlivé výměnné médium použité pouze k tomu účelu. Privátní klíče musí být zašifrovány a to dvakrát. Heslo musí být silné a musí být uschováno odděleně od média s klíči. Dvojí dohled je třeba dodržet.

Kořen nejvyšší úrovně musí být uschován pod řízením Výboru. Pod-kořeny mohou být uschovány jak Výborem, tak týmem Správců systému.

#### 9.2.3. Obnova

Obnova musí být provedena pouze pod autoritou arbitra.

#### 9.2.4. Odvolání

### 9.3. Zákon (právní aspekty)

#### 9.3.1. Odpovědnost

Výbor se zodpovídá Komunitě za správu certifikační autority (CA) na výkonné úrovni.

#### 9.3.2. Odpověď na vnější (právní) dotaz

Všechny vnější dotazy na import zabezpečení jsou založeny jako spory a předloženy arbitrovi podle Zásad řešení sporů (DRP). Musí být uvědoměn Výbor a vedoucí příslušných týmů.

Pouze arbitr má oprávnění zabývat se vnějšími dotazy a/nebo vytvořit proceduru. Inženýři přístupu, Správci systémů, inženýři podpory, členové Výboru a další klíčové role nemají oprávnění odpovídat na právní dotazy. Arbitrovo nařízení může instruovat jednotlivce a poskytne vám oprávnění jednat.

### 9.4. Outsourcing (vnější správa a dohled)

Komponenty mohou být spravovány zevně (outsourcovány). Jakákoli uspořádání outsourcingu musí být dokumentována. Všechna uspořádání musí být:

* se Členy CAcert, kteří jsou
  + zaručovatelé, jako jednotlivci, nebo
  + zaručené organizace, kde všechen zúčastněný personál jsou zaručovatelé,
* se Členy, kteří mají potřebné znalosti a v dobrém kontaktu s vedoucím(i) týmu (týmů),
* předmětem auditu,
* transparentní a nebránící zabezpečení,
* podle těchto zásad a Příručky bezpečnosti,
* zcela podle arbitráže a Zásad řešení sporů (DRP) pro účely zabezpečení, a
* podle ducha komunity a v mezích principů CAcert.

Smlouvy musí být psány s předchozími body na mysli. Outsourcing kritických komponent musí být schválen Výborem.

### 9.5 Důvěrnost, zabezpečení

CAcert je otevřená organizace a zachovává princip otevřeného přístupu tam, kde je to možné. Viz [Principy](https://svn.cacert.org/CAcert/principles.html). Toto není prohlášení zásad, ale prohlášení bezpečnosti; pokud mohou být bezpečnostní záležitosti udržovány pouze s určitou mírou důvěrnosti nebo utajení, najít jiný způsob.

Konkrétně: důvěrnost nebo utajení může být udrženo pouze podle definované metody v zásadách, nebo pod dohledem arbitra (on sám se řídí Zásadami řešení sporů [DRP]). Výjimka sama nesmí být tajná ani důvěrná. Všechny utajené a důvěrné údaje jsou přehlédnuty podle arbitráže a mohou být zrušeny. Všichni by měli usilovat o redkci nebo odstranění podobných omezení.

## 10. ODKAZY

### 10.1 Kontakty

Kontaktní údaje všech klíčových osob a týmů musí být dokumentovány.

### 10.2 Dokumenty

Všechny připojené dokumenty musí samy být dokumentovány.

### 10.3 Související dokumenty

Pro pohodlnou dostupnost mají být relevantní a pomocné dokumenty odkazovány[, například pomocí URL].