



KATEDRA INFORMATIKY  
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY  
UNIVERZITA KOMENSKÉHO, BRATISLAVA

---

ARCHÍV ELEKTRONICKÝCH  
DOKUMENTOV  
(diplomová práca)

MICHAL FORIŠEK

---

Vedúci: doc. RNDr. Daniel Olejár, PhD.

Bratislava  
29. apríla 2004



Čestne prehlasujem, že som túto diplomovú prácu vypracoval samostatne s použitím citovaných zdrojov.

.....



## Podakovanie

Chcel by som poďakovať vedúcemu mojej diplomovej práce doc. RNDr. Danielovi Olejárovi, PhD. za všetky konzultácie, ktoré mi dali veľa nielen k tejto práci, ale aj do života.

Okrem toho chcem poďakovať všetkým mojim priateľom za to, že robia môj svet krajším. A samozrejme mojim skvelým rodičom za úplne všetko.



## License information

This work is licensed under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/1.0/> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA. If you are interested in commercial use of this work or its derivatives, please contact the author at <misof@ksp.sk>.

## Informácie o licencií

Na túto prácu sa vzťahuje Creative Commons Attribution-NonCommercial License. Jej znenie nájdete na <http://creativecommons.org/licenses/by-nc/1.0/>, prípadne dostanete poštou, ak napíšete na adresu Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA. Ak máte záujem využiť túto prácu (alebo práce od nej odvodené) na komerčné účely, kontaktujte prosím autora e-mailom na adresu <misof@ksp.sk>.



# Obsah

<b>1</b>	<b>Úvod</b>	<b>1</b>
<b>2</b>	<b>Formulácia problému</b>	<b>3</b>
2.1	Životný cyklus dokumentu . . . . .	4
2.2	Procedúry archívu . . . . .	5
<b>3</b>	<b>Nástroje pre riešenie problému</b>	<b>7</b>
3.1	Kryptografické prostriedky . . . . .	7
3.2	Informačná bezpečnosť . . . . .	16
3.2.1	Klasifikácia informácií . . . . .	16
3.2.2	Common Criteria . . . . .	16
3.2.3	Ostatné stránky bezpečnosti systému . . . . .	17
3.2.4	Základné pojmy z informačnej bezpečnosti . . . . .	17
<b>4</b>	<b>Profil ochrany</b>	<b>21</b>
4.1	Úvod . . . . .	21
4.1.1	Identifikácia PP . . . . .	22
4.1.2	Prehľad . . . . .	23
4.1.3	Organizácia dokumentu . . . . .	24
4.1.4	Konvencie . . . . .	25
4.2	Popis systému . . . . .	25
4.2.1	Interakcia systému s okolím . . . . .	26
4.2.2	Target of Evaluation . . . . .	28
4.2.3	Úrovne bezpečnosti . . . . .	29
4.3	Bezpečnostné prostredie . . . . .	32
4.3.1	Aktíva . . . . .	32
4.3.2	Legislatívne požiadavky . . . . .	32
4.3.3	Predpoklady bezpečnej prevádzky . . . . .	34

4.3.4	Identifikácia hrozieb . . . . .	35
4.3.5	Organizačná bezpečnostná politika . . . . .	39
4.4	Bezpečnostné ciele . . . . .	39
4.4.1	Bezpečnostné ciele pre TOE . . . . .	40
4.4.2	Bezpečnostné ciele pre prostredie . . . . .	40
4.4.3	Bezpečnostné ciele pre TOE spolu s prostredím . . . . .	43
4.5	Bezpečnostné požiadavky . . . . .	45
4.5.1	Funkčné požiadavky na prostredie . . . . .	45
4.5.2	Funkčné požiadavky na TOE . . . . .	59
4.5.3	Požiadavky na záruky . . . . .	73
4.5.4	Sila kryptografických funkcií . . . . .	77
4.6	Zdôvodnenie . . . . .	77
4.6.1	Pokrytie bezpečnostných cieľov . . . . .	78
4.6.2	Dostatočnosť bezpečnostných cieľov . . . . .	82
4.6.3	Pokrytie požiadaviek na funkcie a záruky . . . . .	89
4.6.4	Dostatočnosť požiadaviek na funkcie a záruky . . . . .	94
4.6.5	Závislosti medzi požiadavkami . . . . .	100
4.6.6	Zdôvodnenie požiadaviek na záruky . . . . .	108
4.7	Použité skratky . . . . .	110
<b>5</b>	<b>Ostatné hľadiská bezpečnosti</b>	<b>113</b>
5.1	Organizačná bezpečnosť . . . . .	113
5.2	Klasifikácia a zabezpečenie aktív . . . . .	114
5.3	Personálna bezpečnosť . . . . .	115
5.4	Fyzická bezpečnosť . . . . .	115
5.5	Kontrola prístupu . . . . .	117
<b>6</b>	<b>Záver</b>	<b>119</b>
<b>A</b>	<b>Slovníček pojmov z inf. bezpečnosti</b>	<b>121</b>
<b>B</b>	<b>Obsah priloženého CD</b>	<b>127</b>
	<b>Literatúra</b>	<b>129</b>

# Kapitola 1

## Úvod

Ľudská spoločnosť potrebuje v súčasnosti na svoje fungovanie denne spracúvať obrovské množstvo informácií. Dôsledkom toho je stále častejšie používanie digitálnej výpočtovej technológie a informačno-komunikačných technológií (IKT). Na druhej strane, práve používanie IKT vedie často k ďalšiemu zvyšovaniu objemu spracúvaných informácií a potrebe nových technológií. Vývoj spoločnosti pod vplyvom IKT sa zvykne označovať pojmom informatizácia spoločnosti.

Nesmieme však zabúdať na to, že informatizácia spoločnosti nemá len technologický aspekt. Jej asi najdôležitejšou súčasťou je prepracovanie súčasných procesov tak, aby mohli prebiehať v elektronickej podobe. Pri tom ale treba brať ohľad na zodpovedajúce právne aspekty a zanedbateľná nie je ani „výchova“ obyvateľstva, ktoré musí novým technológiám dôverovať, aby ich začalo používať.

Klasické komunikačné technológie sa vyvíjali dlhé roky a odrážajú obmedzenia, ktoré kladú tradičné spôsoby ukladania a spracúvania informácií. Mnohé postupy sa však dajú výrazne zjednodušiť pri prechode od tradičných foriem ukladania informácií k informáciám v digitálnej podobe. Avšak pri spracúvaní informácií v digitálnej podobe vznikajú nové problémy, ktoré doteraz buď vôbec neexistovali, alebo boli omnoho jednoduchšie riešiteľné. Za všetky spomeňme napríklad problém, ako podpísať elektronický dokument.

Na Slovensku začala výraznejšia informatizácia spoločnosti iba v deväťdesiatych rokoch minulého storočia. Rýchlo bolo treba riešiť viacero akútnych problémov spojených s informatizáciou spoločnosti, preto sa ešte nebolo kedy zaoberať koncepčnými problémami dlhodobejšieho charakteru. Táto diplomová práca si kladie za cieľ aspoň sčasti zaplniť túto medzeru – preskúmať

problémy súvisiace s archiváciou elektronických dokumentov a navrhnúť konštru systému ich archivácie.

Veľké množstvá informácií bude po spracovaní treba na dlhšiu dobu uschovať. Klasickým riešením sú archívy obsahujúce tieto informácie na materiálnych nosičoch (papier, magnetická páska, mikrofilm, atď.). Toto riešenie sa ponúka aj pre informáciu v digitálnej podobe. Bude sa tu samozrejme treba zaoberať problémami klasických archívov (napr. trvácnosť a obnovovanie záznamu, ochrana utajovaných informácií). Pravdepodobne vzniknú aj nové problémy, jedným môže byť objem dát, ktoré bude potrebné archivovať. Na druhej strane vznikajú aj nové možnosti, ako napríklad nepretržitá dostupnosť archivovaných dokumentov prostredníctvom počítačovej siete. Archivovanie informácií v digitálnej podobe nám navyše dáva možnosť napr. kryptografickými prostriedkami zabezpečiť dáta pred nepovolaným prístupom, zabezpečiť ich integritu a pod.

V tejto diplomovej práci sa na návrh archívu elektronických dokumentov dívame ako na bezpečnostný projekt. Prvým krokom k vytvoreniu bezpečného systému je vytvorenie jeho profilu ochrany – množiny požiadaviek, ktoré sú nutné a postačujúce pre dostatočné zaistenie informačnej bezpečnosti takéhoto systému. Naším hlavným cieľom bude práve vytvorenie profilu ochrany pre archív elektronických dokumentov.

## Štruktúra diplomovej práce

V kapitole 2 uvedieme základnú terminológiu: čo je to dokument, aké sú rozdiely medzi klasickým a elektronickým dokumentom a aké služby poskytuje archív.

Kapitola 3 obsahuje popis jednotlivých nástrojov, ktoré budeme pri návrhu archívu elektronických dokumentov používať. V časti 3.1 sú uvedené potrebné základy kryptografie, v časti 3.2 oboznámime čitateľa so základnými pojmami a normami z oblasti informačnej bezpečnosti.

Hlavným výsledkom tejto diplomovej práce je kapitola 4, ktorá obsahuje súbor štyroch profilov ochrany pre archív elektronických dokumentov.

V kapitole 5 stručne rozoberieme tie hľadiská bezpečnosti systému, ktorých sa profil ochrany explicitne nedotýka.

V závere (kapitola 6) zhrnieme dosiahnuté výsledky a uvedieme niektoré ďalšie ciele, ktoré sa na ich základe dajú stanoviť.

# Kapitola 2

## Formulácia problému

V tejto kapitole sa pokúsime čo najpresnejšie formulovať problematiku archívu elektronických dokumentov. Stručne zhrnieme, čo rozumieme pod pojmom dokument. Uvedieme typický životný cyklus dokumentu a porovnáme, čo sa v jednotlivých fázach zmení pri prechode k elektronickým dokumentom. Rozdiskutujeme, aké služby má archív používateľom poskytovať a aké legislatívne požiadavky sú naň kladené. V závere kapitoly stručne načrtujeme samotný návrh archívu elektronických dokumentov.

### Čo je to dokument?

Na dokument sa v tejto práci budeme pozerieť ako na objekt určený na uchovávanie a prenos informácií. Pod pojmom *klasický dokument* budeme rozumieť dokument viazaný na pevné médium (ako papier, mikrofilm a pod.), na ktorom sú informácie zaznamenané analógovo. Protikladom bude *elektronický dokument*, u ktorého sú informácie na médiu zaznamenané v digitálnej podobe. Pokiaľ bude z kontextu vyplývať, o akom type dokumentu hovoríme, budeme niekedy slovo *klasický*, resp. *elektronický* vynechávať.

### Formálna definícia dokumentu.

**Dokument** je ľubovoľný objekt, pomocou ktorého možno prenášať informácie. Pri popise dokumentu musíme zobrať do úvahy jeho nosič, formát a obsah.

**Nosič dokumentu** predstavuje fyzické médium, obsahujúce informácie, ktoré dotýčny dokument prenáša a spôsob, akým je informácia na tomto

médiu zaznamenaná. Podľa nosiča rozlišujeme dokumenty *elektronické* (informácia je zaznamenaná v digitálnej podobe) a *klasické* (informácia je zaznamenaná v analógovej podobe).

**Formát dokumentu** je formálny popis, ako interpretovať údaje, uložené na tomto nosiči a naopak, ako danú informáciu na daný nosič uložiť. (Príkladom formátu elektronického dokumentu je Adobe Portable Document Format (PDF, viď [Ado03]). Príkladom formátu klasického dokumentu je šablóna na vyplnenie daňového priznania.)

**Obsah dokumentu** je samotná informácia, ktorá je uložená na danom nosiči v danom formáte.

## 2.1 Životný cyklus dokumentu

Z pohľadu archívu môžeme životný cyklus klasického dokumentu rozdeliť do niekoľkých fáz. Stručne popíšeme, ako vyzerajú a čo sa počas nich s dokumentom deje.

**Vznik a použitie.** V tejto fáze je dokument vytvorený a prípadne aj používaný. So samotným archívom táto fáza nesúvisí, uvádzame ju len kvôli kompletnosti popisu životného cyklu dokumentu.

**Vloženie do archívu.** Dokument je vložený do archívu. Pri vkladaní je o ňom známych viacero jeho atribútov (doba, počas ktorej má byť archivovaný, stupeň utajenia a pod.). Archív si môže vytvoriť a uložiť interné informácie o archivovanom dokumente. V prípade potreby môže byť súčasťou procesu vkladania dokumentu do archívu jeho transformácia (napr. zmena formátu), tá však nesmie zmeniť obsah dokumentu.

Archív môže pri vložení dokumentu vydať potvrdenie o jeho archivácii. Toto potvrdenie by malo slúžiť ako doklad, že v danom čase bol tento dokument naozaj vložený do archívu.

**Archivácia.** Základným cieľom, ktorý musí archív plniť počas archivácie dokumentu, je zabezpečiť jeho *integritu*, *dostupnosť* (availability) a prípadne aj *utajenie* (confidentiality).

*Integrita dokumentu* znamená, že počas doby archivácie by mal obsah dokumentu zostať nezmenený. Zabezpečenie integrity zahŕňa nielen starostlivosť o materiál, na ktorom je dokument vyhotovený, ale aj ochranu

dokumentu pred neoprávnenými zásahmi, ktoré by mohli viesť k jeho poškodeniu, prípadne zničeniu.

*Zabezpečenie dostupnosti* znamená, že daný dokument by mal byť kedykoľvek k dispozícii entitám, ktoré sú na to oprávnené. Archív môže prípadne vydávať kópie archivovaných dokumentov.

V prípade, že archivované dokumenty podliehajú rôznym stupňom utajenia, musí archív zabezpečiť adekvátne obmedzenie prístupu k nim.

**Výber a zničenie.** V tejto fáze svojho životného cyklu je dokument z archívu odstránený a väčšinou aj fyzicky zničený.

Už pri tomto hrubom náčrte životného cyklu klasického dokumentu vidíme, že životný cyklus elektronického dokumentu sa od neho bude vo viacerých ohľadoch odlišovať. Základným dôvodom bude samotná jeho odlišná podstata. V niektorých situáciách nám bude elektronická podoba dokumentu ponúkať nové možnosti, prípadne uľahčí manipuláciu s ním, avšak vzniknú aj nové problémy, ktoré sme pri klasických dokumentoch nepoznali.

Na rozdiel od klasického dokumentu, ktorý je od okamihu svojho vzniku v podstate nemenný, elektronický dokument sa dá ľahko zmeniť počas ľubovoľnej fázy svojej existencie. Preto je napríklad ťažšie zabezpečiť jeho integritu počas archivácie. K elektronickému dokumentu je ľahké zhotoviť takmer ľubovoľne veľké množstvo kópií, tie sú (na rozdiel od kópií klasických dokumentov) nerozoznateľné od originálu. Tieto skutočnosti sa musia odraziť pri návrhu realizácie jednotlivých procedúr ľubovoľného archívu elektronických dokumentov.

## 2.2 Procedúry archívu

V tejto časti stručne popíšeme jednotlivé operácie s elektronickými dokumentami, ktoré by mal poskytovať archív elektronických dokumentov. Nebudeme sa zatiaľ zaoberať konkrétnymi problémami pri realizácii týchto operácií, avšak uvedieme niekoľko výhod, ktoré nám poskytujú elektronické dokumenty oproti klasickým.

**Príjem a uloženie dokumentu.** Klient doručí (či už fyzicky alebo poštou na pevnom médiu, alebo prostredníctvom počítačovej siete) dokumenty určené na archivovanie. S každým dokumentom sú asociované údaje,

ktoré hovoria o jeho vlastníkovi a predpokladanej dobe archivácie. (V závislosti od služieb poskytovaných konkrétnym archívom môžu tieto údaje byť doplnené ďalšími, napríklad stupňom utajenia dokumentu, či požiadavkami upresňujúcimi spôsob archivácie, napr. nutnosť okamžitej dostupnosti počas celej doby archivácie.)

Dokument je spracovaný a zaradený do archívu. Vykonajú sa funkcie na zabezpečenie jeho integrity. (Do auditných záznamov zapíše jeho hašovacia hodnota, vytvorí sa jeho záložná kópia, z ktorej ho v prípade ľubovoľnej chyby vieme obnoviť a pod.)

V prípade požiadavky klienta mu môže byť vydané (archívom elektronicky podpísané) potvrdenie o vložení dokumentu do archívu.

**Vyhľadávanie.** Archívy verejne prístupných elektronických dokumentov môžu ako jednu zo služieb poskytovať vyhľadávanie konkrétnych dokumentov podľa názvu, autora alebo iných charakteristík. Pri elektronických dokumentoch je aj možnosť tzv. fulltextového vyhľadávania (vyhľadávanie kľúčových slov nielen v názve dokumentu, ale v celom jeho texte).

**Vytváranie kópií.** Archív môže byť schopný vydať autorizovanému žiadateľovi kópiu archivovaného dokumentu. Pomocou elektronického podpisu mu navyše vie vydať potvrdenie o tom, že ide naozaj o kópiu dotyčného archivovaného dokumentu.

**Odstránenie dokumentu z archívu.** Po uplynutí požadovanej doby archivácie je dokument vyradený z archivácie a buď vrátený vlastníkovi, alebo zničený. Často je žiadané, aby dokument, ktorý prestáva byť archivovaný, bol z archívu bezpečne odstránený, t.j. aby ho neskôr nebolo možné použitím softvérových ani hardvérových prostriedkov obnoviť.

Nesmieme zabúdať, že popri uvedených operáciách, ktoré vznikajú na vonkajší podnet, sú tu aj ďalšie interné operácie, ktoré sú potrebné na zabezpečenie integrity a prípadne aj utajenia archivovaných dokumentov počas dlhšieho časového intervalu. Ako príklad uveďme starnutie nosičov elektronických dokumentov, proti ktorému sa dá brániť pravidelnou kontrolou čitateľnosti médií a pravidelným presunom archivovaných dokumentov na nové médiá. Podrobnejšie sa týmito operáciami budeme zaoberať pri návrhu profilu ochrany (kapitola 4), kde nám automaticky vyplynú z identifikovaných hrozieb a stanovených bezpečnostných cieľov.

# Kapitola 3

## Nástroje pre riešenie problému

### 3.1 Kryptografické prostriedky

Bezpečnostné funkcie archívu elektronických dokumentov sa realizujú pomocou kryptografických prostriedkov. V tejto časti uvedieme základné pojmy z kryptografie, ktoré budeme ďalej využívať pri návrhu archívu. Podrobnejší popis tu spomenutých kryptografických prostriedkov nájde čitateľ napr. v [Sti95] alebo [MvOV97].

#### Kryptosystémy

*Kryptografia* je veda o návrhu kryptosystémov. Jej základnou úlohou je umožniť dvom subjektom (väčšinou označovaným Alica a Bob) komunikáciu po nezabezpečenom komunikačnom kanáli tak, aby ich útočník nemohol odpočúvať ani zmeniť prenášanú informáciu bez toho, aby si to všimli. Pasívny útočník sa zvykne označovať Eva (eavesdropper), aktívny Oskar (opponent). Základným nástrojom pri návrhu kryptosystémov je šifrovanie.

Nech Alica má informáciu, ktorú chce odoslať Bobovi. Túto informáciu budeme nazývať *otvorený text* (plaintext,  $p$ ). Pomocou *klúča* (key,  $k$ ) ju Alica zašifruje, čím vznikne *šifrový text* (ciphertext,  $c$ ). Zašifrovanú informáciu pošle Bobovi. Oskar s ňou nedokáže nič spraviť, ale Bob z nej dokáže pomocou svojho klúča získať pôvodný otvorený text.

Formálne je *kryptosystém* definovaný ako 7-ica  $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}, f_{\mathcal{E}}, f_{\mathcal{D}})$ , kde:  $\mathcal{P}$  a  $\mathcal{C}$  sú konečné množiny, predstavujúce možné otvorené a šifrované texty.  $\mathcal{K}$  je konečná množina prípustných klúčov.  $\mathcal{E}$  je množina (šifrovacích) funkcií z  $\mathcal{P}$

do  $\mathcal{C}$  a  $\mathcal{D}$  je množina (dešifrovacích) funkcií<sup>1</sup> z  $\mathcal{C}$  do  $\mathcal{P}$ . Každému kľúču  $k \in \mathcal{K}$  sú priradené (funkciami  $f_{\mathcal{E}}, f_{\mathcal{D}}$ ) šifrovacia funkcia  $e_k$  a dešifrovacia funkcia  $d_k$ , pričom platí, že pre ľubovoľný otvorený text  $p \in \mathcal{P}$  je  $d_k(e_k(x)) = x$ .

Posledná podmienka hovorí, že dešifrovacia funkcia  $d_k$  musí správne dešifrovať ľubovoľný otvorený text, zašifrovaný funkciou  $e_k$ . Aby to mohlo platiť, každá funkcia  $e_k$  musí zjavne byť injektívna. Príkladmi jednoduchých kryptosystémov sú napr. substitučná, permutačná a Vigenèrova šifra.

Existuje viacero delení kryptosystémov, najčastejšie sa používa hľadisko *symetrickosti* použitej šifry. Podľa tohto hľadiska rozlišujeme *symetrické*, *asymetrické* a *hybridné* kryptosystémy.

Pri *symetrickom kryptosystéme* používajú Alica a Bob ten istý kľúč na šifrovanie aj dešifrovanie. V tomto prípade sa ale na ňom musia dohodnúť – či už sa vopred stretnú alebo na prenos kľúča použijú bezpečný komunikačný kanál. Šifrovacie funkcie použité v symetrických kryptosystémoch rozdeľujeme na *prúdové* (šifrované údaje sa spracúvajú ako prúd znakov) a *blokové* (šifrované údaje sa spracúvajú po blokoch pevnej veľkosti).

Príkladom jednoduchej prúdovej šifry je Vernamova šifra [Ver26] (známa tiež ako one-time pad). Väčšina v praxi používaných prúdových šifier je založená na princípe, že z kľúča pomocou generátora pseudonáhodných čísel vygeneruje dostatočne dlhú postupnosť bitov, ktorou otvorený text prexoruje.

Príkladmi jednoduchej blokovej šifry sú substitučná šifra a permutačná šifra. Špeciálnou skupinou blokových šifier sú tzv. *Feistelovské šifry* [Fei73] – iterované šifry, pri ktorých je vďaka ich návrhu proces šifrovania a dešifrovania takmer identický.

Od 26. mája 2002 je podľa NIST (National Institute for Standards and Technology, USA) štandardným symetrickým kryptosystémom známym ako AES (Advanced Encryption Standard) bloková šifra Rijndael. Špecifikáciu kryptosystému AES udáva dokument FIPS 197 [NIST01a], na internete je dostupná aj pôvodná špecifikácia šifry Rijndael [DR01].

Pri *asymetrickom kryptosystéme* Alica používa iný kľúč na šifrovanie ako Bob na dešifrovanie. Zjavne pri takýchto kryptosystémoch musí Bob vopred

---

<sup>1</sup>Z matematického hľadiska šifrovaciu a dešifrovaciu funkciu môže predstavovať dokonca ľubovoľná relácia na  $P \times C$ , v ktorej každému šifrovému textu prislúcha najviac jeden otvorený text. Inými slovami pre niektoré otvorené texty nám šifrovacia funkcia môže vrátiť viacero rôznych šifrových textov.

zverejniť nejaké informácie, z ktorých si Alica zostrojí taký kľúč, aby zašifrovanú správu prečítal len Bob. Preto sa takémuto kryptosystému niekedy hovorí *kryptosystém s verejným kľúčom* (public-key kryptosystems). Väčšinou Bob zverejňuje priamo kľúč, ktorým treba šifrovať jemu posielané správy. Tomuto kľúču hovoríme *verejný kľúč*. Jedine Bob má k dispozícii *súkromný kľúč*, ktorým sa dajú dešifrovať správy šifrované verejným kľúčom. Asymetrické kryptosystémy sú založené na predpoklade, že útočník nevie z Bobovho verejného kľúča efektívne zostrojiť Bobov súkromný kľúč. (Bob vie svoj súkromný kľúč, pretože ho vygeneroval naraz so svojim verejným kľúčom, t.j. nemusel ho zostrojovať zo svojho verejného kľúča.)

Neexistujú kryptosystémy s verejným kľúčom, ktoré by boli absolútne bezpečné – totiž útočník, ktorý chce rozšifrovať daný šifrový text  $c$  má vždy možnosť postupne skúšať všetky možné otvorené texty  $p$  a každý z nich zašifrovať verejnou šifrovacou funkciou až kým nenájde (jediný) otvorený text, z ktorého zašifrovaním dostane  $c$ . Preto sa zvykne požadovať, aby public-key kryptosystém bol aspoň výpočtovo bezpečný – ľubovoľný útok musí mať také veľké časové nároky, aby ho útočník na súčasných počítačoch nemal šancu úspešne použiť.

Medzi klasické asymetrické kryptosystémy patria RSA [RSA78, schéma 3.1] a ElGamal [ElG85]. RSA je založený na probléme faktorizácie, ElGamal na probléme diskretného logaritmu. K týmto problémom zatiaľ nie je známy efektívny algoritmus. Keby sa nejaký našiel, útočník by vedel efektívne zostrojiť k verejnému kľúču súkromný, čím by narušil bezpečnosť kryptosystému.

## Podpisové schémy

Pri klasických dokumentoch vlastnoručný podpis slúžil okrem iného aj ako potvrdenie, že dokument je autentický a pochádza od podpisujúceho. Z toho vyplývajú dve vlastnosti, ktoré musí každý (aj elektronický) podpis mať: Na jednej strane za danú osobu sa nesmie byť schopný podpísať nikto iný, na druhej strane každý musí mať možnosť overiť si pravosť podpisu. Podotkneme, že pri elektronických podpisoch je toto overenie jednoznačné, a tak znemožňuje útočníkovi napodobenie podpisu. Tento problém klasických podpisov teda pri elektronických podpisoch odpadá.

Vznikajú tu však nové problémy. Kópia elektronického podpisu je nerozoznateľná od originálu, preto v prípade potreby musíme explicitne zabezpečiť, aby podpísaný dokument nemohol byť použitý viackrát. Napr. keď

1. Bob si vygeneruje 2 veľké prvočísla  $p$  a  $q$ .
2. Spočíta hodnoty  $n = pq$  a  $\Phi(n) = (p - 1)(q - 1)$ .
3. Zvolí si náhodné  $b \in \{1, 2, \dots, \Phi(n) - 1\}$  nesúdeliteľné s  $\Phi(n)$ .
4. Spočíta  $a = b^{-1} \bmod \Phi(n)$  (napr. Euklidovym algoritmom [Wei, search: Euclidean Algorithm] alebo ako  $a = b^{\Phi(n)-2}$ ).
5. Zverejní hodnoty  $n$  a  $b$  ako svoj verejný kľúč. Hodnota  $a$  predstavuje jeho súkromný kľúč. Šifrovacia funkcia bude  $e_{n,b}(x) = x^b \bmod n$ , dešifrovacia funkcia  $d_a(y) = y^a \bmod n$ .

*Funkcia  $\Phi(k)$  je Eulerova funkcia, udávajúca počet prirodzených čísel menších ako  $x$  a nesúdeliteľných s ním. Všimnite si, že na vypočítanie hodnoty  $a$  Bob použil hodnotu  $\Phi(n)$ , ktorú nezverejnil.*

Tabuľka 3.1: RSA kryptosystém – generovanie kľúčov.

podpíšeme útočníkovi príkaz na prevod 1 000 Sk na jeho účet, boli by sme neradi, keby ho mohol použiť stokrát. Tento problém sa dá riešiť tak, že podpísaná správa bude obsahovať okrem samotného dokumentu nejaké dáta navyše, ktoré zabránia jej viacnásobnému použitiu. V našom príklade by takéto dáta mohol predstavovať napr. náhodný reťazec bitov vygenerovaný serverom banky.

Bezpečnostným problémom je aj to, že v prípade, ak útočník získa tajné údaje, pomocou ktorých obeť podpisuje dokumenty (napr. súkromný kľúč obete), je schopný vytvoriť podpis obete bez jej fyzickej prítomnosti. Klasický podpis nedokáže vytvoriť nik iný ako jeho autor. Podobný bezpečnostný problém však existuje v niektorých ázijských krajinách, kde majú občania svoje „pečiatky“, ktoré môžu používať namiesto podpisu. Pri elektronickom podpise je riešenie týchto problémov úlohou infraštruktúry verejných kľúčov (public-key infrastructure, PKI), ktorú rozoberieme v neskoršej časti tejto kapitoly.

Formálne *podpisová schéma* je 7-ica  $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{S}, \mathcal{V}, f_S, f_V)$ , kde:  $\mathcal{P}$  a  $\mathcal{C}$  sú konečné množiny, predstavujúce možné dokumenty a podpisy.  $\mathcal{K}$  je konečná

množina prípustných kľúčov.  $\mathcal{S}$  je množina (podpisovacích) funkcií z  $\mathcal{P}$  do  $\mathcal{C}$  a  $\mathcal{V}$  je množina (overovacích) funkcií z  $\mathcal{P} \times \mathcal{C}$  do  $\{0, 1\}$ . Každému kľúču  $k \in \mathcal{K}$  sú priradené (funkciami  $f_{\mathcal{S}}, f_{\mathcal{V}}$ ) podpisovacia funkcia  $s_k$  a overovacia funkcia  $v_k$ , pričom platí, že pre ľubovoľný dokument  $p \in \mathcal{P}$  je  $v_k(x, y) = 1$  práve vtedy, ak  $y = s_k(x)$ .

Posledná podmienka hovorí, že overovacia funkcia  $v_k(p, s)$  vráti 1 práve vtedy, ak  $s$  je podpis dokumentu  $k$  pri použití kľúča  $k$ . Funkcia  $v_k$  je verejná,  $s_k$  je súkromná. Podobne ako kryptosystémy s verejným kľúčom ani podpisové schémy nemôžu byť absolútne bezpečné – totiž útočník má vždy možnosť vyskúšať všetky možné podpisy k danému dokumentu a pomocou verejnej funkcie  $v_k$  nájsť ten správny. Preto aj od dobrej podpisovej schémy budeme požadovať len jej výpočtovú bezpečnosť – aby útočník nebol schopný k danému dokumentu podpis zostrojiť efektívne.

Na podpisovú schému sa dá ľahko prerobiť ľubovoľný kryptosystém s verejným kľúčom, ktorého šifrovacie funkcie sú bijekcie. Schéma 3.2 ukazuje podpisovú schému založenú na RSA. Existuje aj ElGamalova podpisová schéma, jej modifikáciou je algoritmus Digital Signature Standard [NIST01c].

1. Bob zostrojí hodnoty  $p, q, n, \Phi(n), a, b$  rovnako ako pri RSA kryptosystéme – viď schému 3.1.
2. Bobova podpisovacia funkcia bude  $s_a(x) = x^a \bmod n$ , overovacia funkcia  $v_{n,b}(x, y) = 1 \iff y^b \equiv x \pmod{n}$ .

*Bob teda podpíše správu tak, že ju dešifruje, čo vie spraviť jedine on. Hocikto iný vie pomocou jeho verejného kľúča šifrovať, a teda overiť pravosť podpisu.*

Tabuľka 3.2: RSA podpisová schéma.

Špeciálnym prípadom podpisových schém sú tzv. nepopierateľné podpisy (undeniable signatures). Ich myšlienka je nasledujúca: Aby podpísaný dokument nemohol byť použitý bez vedomia autora podpisu, musí ten byť zahrnutý do procesu overovania. Navyše súčasťou takej schémy musí byť aj protokol, ktorým vie ktokoľvek dokázať, že konkrétny podpis nie je jeho – inak by mohol autor podpisu poprieť jeho pravosť, ak sa mu to hodí. Nepop-

riteľné podpisy sa dajú realizovať napr. pomocou Chaum-van Antwerpovej schémy, navrhnutej v [CvA90].

## Hašovacie funkcie

Pri samotnej realizácii elektronického podpisu však narážame na niekoľko nezanedbateľných problémov. Známe algoritmy sú pre veľké dokumenty často až neúnosne pomalé. Veľkosť výsledného podpisu je porovnateľná s veľkosťou dokumentu – teda podpísaním sa značne zväčší objem prenášaných dát. A navyše je tu aj bezpečnostné riziko. Totiž väčšina schém realizujúcich elektronický podpis priamo predpokladá, že podpisovaná správa je krátka (stovky až tisíce bitov). Rozdeliť správu na úseky požadovanej dĺžky a podpísať samostatne každý z nich nemusí byť najšťastnejšie riešenie – umožníme totiž útočníkovi ľubovoľne zmeniť poradie týchto úsekov, prípadne niektoré z nich vynechať. Potrebujeme vedieť zabezpečiť integritu podpísanej správy.

Riešením všetkých spomenutých problémov sú *hašovacie funkcie*. Hašovacia funkcia je rýchlo spočítateľná funkcia, ktorá dostane na vstupe dokument ľubovoľnej dĺžky a zostrojí z neho pomerne krátku (napr. 160 bitov) charakteristiku, nazývanú *hašovacia hodnota* (hash, message digest, fingerprint). Túto hašovaciu hodnotu potom podpíšeme použitím nejakej podpisovej schémy.

Samozrejme, použitie nevhodnej hašovacej funkcie môže výrazne oslabiť bezpečnosť použitej podpisovej schémy. Napríklad keby sme ako charakteristiku dokumentu brali jej posledných 160 bitov a podpísali nejaký dokument, útočník by vedel podpísať našim podpisom ľubovoľný iný dokument, ktorý sa s našim zhoduje na posledných 160 bitoch – jednoducho by k nemu pripojil ten istý podpis.

Je rozumné požadovať, aby k danému podpísanému dokumentu útočník nedokázal zostrojiť iný s rovnakým podpisom. Odhliadnuc od bezpečnosti použitej podpisovej schémy to znamená, že k danému dokumentu nesmie byť útočník schopný efektívne zostrojiť iný dokument s tou istou hašovacou hodnotou.

Iný možný útok vyzerá nasledovne: Útočník si vytvorí dva dokumenty s rovnakou hašovacou hodnotou a presvedčí obeť, aby podpísala jeden z nich. Tým ale získa podpis aj na druhý dokument, o ktorom podpisujúci nevie. Preto budeme požadovať silnejšiu vlastnosť hašovacej funkcie – aby útočník nebol schopný efektívne zostrojiť žiadne dve správy s rovnakou hašovacou hodnotou.

Ešte je tu tretí, nie až taký zjavný útok. Pri mnohých podpisových schémach sa nedá zabrániť tomu, aby útočník získal podpis náhodného reťazca bitov. Naša hašovacia funkcia by mala útočníkovi zabrániť, aby zostrojil k tomuto reťazcu bitov, teda danej hašovacej hodnote, príslušný dokument. K dobrej hašovacej funkcii by teda nemala existovať efektívne spočítateľná „inverzná“ funkcia. (Úvodzovky preto, že nejde o inverznú funkciu v matematickom zmysle. Hašovacia funkcia priamo zo svojej podstaty nie je injektívna, a teda nemá inverznú funkciu.)

Formálne definície: Hašovacia funkcia  $h$  je *jednosmerná* (one-way, trap-door), ak sa k danému  $y$  nedá efektívne nájsť  $x$  také, že  $h(x) = y$ . Dvojicu dokumentov s rovnakou hašovacou hodnotou voláme *kolízia*. Hašovacia funkcia  $h$  je *slabo odolná voči kolíziám*, ak sa k dokumentu  $x$  nedá efektívne nájsť dokument  $x'$  také, že  $h(x) = h(x')$ . Funkcia  $h$  je *silne odolná voči kolíziám*, ak sa nedajú efektívne nájsť dva dokumenty  $x, x'$  také, že  $h(x) = h(x')$ .

Hašovacia funkcia, ktorá je silno odolná voči kolíziám, je zjavne aj slabo odolná voči kolíziám. Dá sa ukázať, že za rozumných podmienok (viď [Sti95], kap. 7) je aj jednosmerná, preto stačí od hašovacej funkcie požadovať silnú odolnosť voči kolíziám.

Medzi v kryptografii najpoužívanejšie hašovacie funkcie v súčasnosti patria SHA1 [Eas01, NIST02] a MD5 [Riv92]. Mimo oblasť kryptografie treba ešte spomenúť hašovaciu funkciu CRC32 (32-bit cyclic redundancy check-sum), ktorá sa používa takmer výlučne ako kontrolný súčet pri prenose údajov, napr. v archívoch formátu ZIP.

## Časové pečiatky

Často potrebujeme vedieť dokázať nielen to, že sme dokument podpísali, ale aj to, kedy sme ho podpísali. Takýchto príkladov je veľa, napr. rôzne zmluvy, ktoré nadobúdajú či končia platnosť okamihom podpisania. Uvedme si ešte niekoľko komplikovanejších príkladov, ktoré názornejšie ukážu potrebu časových pečiatok.

Predstavme si situáciu, kedy útočník nejakým spôsobom získa súkromný kľúč jedného z účastníkov schémy. V tomto okamihu nielenže vie podpisovať namiesto neho, ale (z pohľadu ostatných užívateľov) je ohrozená aj autenticita dokumentov, ktoré dotyčný účastník podpísal pred prezradením jeho súkromného kľúča. (Rovnako dobre ako on mohol aj tieto správy podpísať útočník.)

Iný príklad: Bob si prečítal predchádzajúci odsek a prišiel na skvelý spôsob, ako si zarobiť. Elektronicky podpísal zmluvu a v okamihu, keď dostal tovar a mal zaplatiť, zverejnil svoj súkromný kľúč a začal tvrdiť, že jeho podpis na zmluve je falošný.

Tieto problémy vznikajú z vyššie uvedeného dôvodu – zo samotného podpisu nemáme ako zistiť, kedy bol vytvorený. Potrebovali by sme akúsi *časovú pečiatku* (timestamp), ktorou by sme označili správu a ktorá by označovala, kedy bola správa podpísaná. Potom by sme napr. problém s Bobom vedeli riešiť rovnako ako napr. problém pri strate kreditnej karty – jeho podpis by platil do okamihu, kým neupozorní príslušný orgán na to, že jeho súkromný kľúč bol kompromitovaný (ekvivalent oznámenia straty kreditnej karty banke). A keďže časová pečiatka na zmluve je staršia, zmluva stále platí.

Existuje viacero spôsobov realizácie časových pečiatok. Dve najjednoduchšie uvádzame v schémach 3.3 a 3.4. Pri zahrnutí tretej strany (služby časových pečiatok, timestamp service, TSS) vzniká samozrejme riziko, že jej súkromný kľúč bude prezradený. Schéma 3.4 dáva TSS možnosť datovať podpisy do minulosti, t.j. vydať časovú pečiatku so skorším časom ako je v čase jej vydania. Túto možnosť jej podstatne obmedzíme, ak bude „pečiatkovaná“ a zverejňovaná informácia zahŕňať nielen samotný podpísaný dokument, ale aj nejaké dáta závisiace od predchádzajúcich opečiatkovaných dokumentov. Takto bude môcť nezávislý pozorovateľ kedykoľvek overiť, že dokumenty podpísané danou TSS boli naozaj podpísané v poradí podľa ich časových pečiatok. Podrobnejšie detaily tohto postupu sa dajú nájsť napr. v [Sti95].

Problematika časových pečiatok je podrobnejšie rozobraná v [HS91] a [BHS93].

Existuje viacero verejne dostupných služieb časových pečiatok, ako príklad spomenieme PGP Digital Timestamping Service [Sta], prevádzkovaný I.T. Consultancy Limited, Jersey, Channel Islands.

## Public Key Infrastructure (PKI)

Systémy, ktoré využívajú kryptografické funkcie, potrebujú postupy napr. na tvorbu nových kľúčov, ich bezpečnú distribúciu, zrušenie platnosti kľúča v prípade jeho kompromitácie, či bezpečné zničenie kľúča. Súhrn týchto postupov voláme PKI (infraštruktúra verejných kľúčov). PKI teda okrem iného popisuje protokoly na tvorbu, distribúciu, používanie, obnovovanie a zničenie kryptografických kľúčov.

1. Bob získa nejakú aktuálnu informáciu, napr. kurzy valút.
2. Podpíše pôvodný dokument zreťazený s touto informáciou.
3. Výsledný podpis zverejní, napr. v novinách, na webe a pod.

*Podpísaním správy Bob dokáže, že podpis nemohol vzniknúť skôr – podpísané aktuálne informácie skôr neexistovali. Vďaka zverejneniu podpisu bude neskôr vedieť dokázať, že v danej chvíli už tento podpis existoval.*

Tabuľka 3.3: Jednoduché časové pečiatky bez účasti tretej strany.

1. Bob podpíše dokument, podpísaný dokument pošle dôveryhodnému zdroju časových pečiatok.
2. TSS podpíše trojicu (dokument, Bobov podpis, aktuálny čas).

Tabuľka 3.4: Časové pečiatky s dôveryhodnou treťou stranou.

Podrobnejší popis fungovania PKI presahuje rámec tejto práce, v prípade potreby ho čitateľ nájde napr. v knihách [Sti95] a [MvOV97]. Praktickú príručku k PKI a open-source implementáciám predstavuje [Xen00].

## 3.2 Informačná bezpečnosť

### 3.2.1 Klasifikácia informácií

Pokiaľ budeme pracovať s dokumentmi, ktoré majú rôzny stupeň utajenia, u ktorých je rôzne dôležitou požiadavkou zachovanie dostupnosti počas archivácie a pod., potrebujeme systematický prístup klasifikácie týchto dokumentov. Jednu možnosť ponúka FIPS 199 [NIST03b]. Podľa neho je každému dokumentu priradený vektor informácií, ktoré udávajú stupne požiadavok na zachovanie jeho dôvernosti, integrity a dostupnosti. Stupeň požiadavky môže byť N/A (nedá sa aplikovať), nízky, stredný a vysoký.

Napr. elektronicky podpísaná zmluva bude mať nízky stupeň požiadavky na dostupnosť, stredný na dôvernosť a vysoký na zachovanie integrity.

### 3.2.2 Common Criteria

Na návrh archívu elektronických dokumentov sa v tejto práci budeme dívať v prvom rade ako na bezpečnostný projekt – návrh systému, využívajúceho informačno-komunikačné technológie (IKT systému). Totiž vzhľadom na charakter činností, ktoré bude archív elektronických dokumentov vykonávať, je pre zabezpečenie jeho funkčnosti nutné zabezpečiť jeho informačnú bezpečnosť.

Prvým krokom návrhu IKT systému z hľadiska zabezpečenia jeho informačnej bezpečnosti je vypracovanie tzv. *profilu ochrany*. Základným nástrojom pri jeho tvorbe nám budú Common Criteria [CC99].

Common Criteria (CC, celým názvom Common Criteria for Information Technology Security Evaluation) sú štandardom (ISO/IEC 15408), ktorý má byť použitý ako pri návrhu, tak aj pri vyhodnocovaní bezpečnostných vlastností IKT systémov. Význam takejto bázy spoločných kritérií je v tom, že dosiahnuté hodnotenie systému bude pochopiteľné pre širší okruh adresátov.

Aktuálna verzia CC (verzia 2.1, vydaná roku 1999) je rozčlenená do troch častí. Prvá časť (Introduction and General Model, [CCa99]) definuje, ktorých častí návrhu IKT systému sa CC týkajú a ako sa majú používať. Druhá časť

(Security Functional Requirements, [CCb99]) predstavuje katalóg funkčných požiadaviek, ktoré môžu byť kladené na IKT systém. Každá funkčná požiadavka implikuje bezpečnostné funkcie, ktoré musí implementácia IKT systému spĺňať. Tretia časť (Security Assurance Requirements, [CCc99]) predstavuje katalóg požiadaviek, ktoré musí IKT systém spĺňať, aby bola jeho bezpečnosť overiteľná.

Pre podrobnejšie pochopenie filozofie Common Criteria odporúčame pozrieť si oficiálnu prezentáciu [CCo], obsahujúcu prehľad Common Criteria, prípadne aj oficiálnu prezentáciu [CCP] o používaní profilov ochrany (PP).

Publikácia [NIST99] obsahuje možný postup pri návrhu profilu ochrany pre krátkodobé komerčné produkty. Nebudeme sa ňou pri našom návrhu priamo riadiť, keďže oblasť jej zamerania je jemne odlišná, ale sčasti z nej budeme čerpať inšpiráciu.

### 3.2.3 Ostatné stránky bezpečnosti systému

Common Criteria sa zaoberajú výlučne technickou stránkou informačnej bezpečnosti systému. Pri návrhu zabezpečenia ostatných stránok bezpečnosti (napr. fyzickej či personálnej bezpečnosti) sa budeme opierať o Praktickú príručku zabezpečenia informačnej bezpečnosti (Information Technology – Code of practice for information security management, [BS00], štandard ISO/IEC 17799).

Iným zaujímavým zdrojom je Príručka ošetrovania incidentov v počítačovej bezpečnosti [NIST04]. Ide o súhrn rôznych praktických odporúčaní, vypracovaný skupinou expertov. V prvých častiach sa hovorí o zriadení tímu schopného odstraňovať následky incidentov a potláčať príčiny ich vzniku. Ďalšie časti sa postupne zaoberajú ošetrovaním rôznych druhov incidentov, ako sú napr. zabránenie vykonávaniu funkcie (denial of service attack), nepriateľský kód alebo neautorizovaný prístup k dátam. Každý typ incidentu je definovaný, sú uvedené metódy jeho prevencie, odhalenia, analýzy, odstránenia a obnovenia bezpečného stavu systému.

### 3.2.4 Základné pojmy z informačnej bezpečnosti

Keďže jazykom Common Criteria je angličtina, budeme sčasti nútení aj v našom návrhu používať angličtinu. Názvy jednotlivých častí budeme uvádzať v angličtine aj slovenčine, samotné funkčné a záručné požiadavky uvedieme v

originálnom anglickom znení, zvyšok textu vrátane všetkých vysvetľujúcich poznámok bude v slovenčine, aby sme zbytočne neznižovali čitateľnosť textu.

V Dodatku A nájdete podrobný slovníček použitých pojmov z oblasti informačnej bezpečnosti. Tento slovníček obsahuje pri každom pojme aj jeho stručnú definíciu. Odporúčame použiť ho v prípade, že si čitateľ nie je istý prekladom či významom niektorého nami použitého pojmu.

Na tomto mieste uvedieme definície niekoľkých základných pojmov. V nasledujúcej kapitole budeme tieto pojmy pravidelne používať, preto je nutné, aby ich čitateľ ovládal.

**Profil ochrany (Protection Profile, PP).** Implementačne nezávislá špecifikácia bezpečnostných požiadaviek, ktoré má spĺňať množina možných produktov alebo systémov. Je to vysokoúrovňová abstrakcia bezpečnostného zámeru a obsahuje zdôvodnenia, funkcionálne požiadavky a požiadavky na záruky. Príklady PP: [NIST01b], [SCSUG01].

**Bezpečnostný zámer (Security Target, ST).** Implementačne závislá špecifikácia bezpečnostných požiadaviek na daný IKT systém. Spresňuje daný profil ochrany, navyše od neho obsahuje popis, ako sú pri implementácii systému zabezpečené jednotlivé bezpečnostné ciele. Súčasťou bezpečnostného zámeru je zdôvodnenie, že je úplnou inštanciou použitého profilu ochrany. Príklady ST: [RSA02], [LC04].

**Manažment rizík.** Celkový proces identifikácie, riadenia, eliminácie alebo minimalizácie neurčitých udalostí, ktoré môžu mať vplyv na zdroje systému. Zahŕňa analýzu rizík, analýzu cost-benefit, výber, implementáciu a testovanie, evaluáciu bezpečnosti opatrení a celkové posúdenie bezpečnosti.

**Fyzická bezpečnosť.** Oblasť bezpečnosti IKT systémov, zahŕňajúca kontrolu fyzického prístupu k aktívam a ich fyzickú ochranu pred poškodením, zničením či odcudzením.

**Organizačná bezpečnosť.** Oblasť bezpečnosti IKT systémov, jej cieľom je udržanie úrovne informačnej bezpečnosti v rámci organizácie. Zahŕňa interné postupy vedúce k dosiahnutiu tohto cieľa, ako aj postupy slúžiace k ochrane aktív pri spolupráci s tretími stranami.

**Personálna bezpečnosť.** Oblasť bezpečnosti IKT systémov, ktorej cieľom je pomocou vhodných opatrení minimalizovať riziká vyplývajúce z ľudských chýb, zneužitia právomocí, podvodu a pod.

**Audit.** Nezávislé skúmanie a vyhodnotenie záznamov a aktivít za účelom určenia súladu s definovanými pravidlami a zistenia prípadných nedostatkov v bezpečnostnej politike IKT systému alebo jej uplatňovaní. Možnosť auditu systému je vo väčšine prípadov nutnou súčasťou jeho zabezpečenia.



# Kapitola 4

## Profil ochrany (Protection Profile)

Táto kapitola obsahuje profil ochrany archívu elektronických dokumentov, vytvorený na základe Common Criteria, v2.1 (viď [CC99]).

Podľa filozofie Common Criteria samotný profil ochrany nie je implementačne špecifický – t.j. v tejto kapitole zhrnieme funkčné požiadavky, ktoré by mala každá implementácia archívu elektronických dokumentov spĺňať. Uvedieme popis bezpečnostného prostredia, v ktorom budeme náš návrh robiť – predpoklady kladené na toto prostredie, obmedzenia a hrozby z neho vyplývajúce.

Z nich ďalej stanovíme bezpečnostné ciele, ktoré chce nami navrhovaný systém dosiahnuť. Z tých budú vyplývať funkčné požiadavky, požiadavky na záruky a požiadavky kladené na bezpečnostné prostredie.

### 4.1 Úvod (Introduction)

Tento dokument definuje požiadavky na systémy, ktoré realizujú dlhodobé archivovanie elektronických dokumentov. Keďže potreba archivovania elektronických dokumentov vzniká v mnohých, častokrát diametrálne odlišných prostrediach, môžu byť na bezpečnosť archívu elektronických dokumentov kladené rôzne nároky. Preto tento dokument špecifikuje štyri profily ochrany s rastúcou úrovňou zabezpečenia. Tieto profily ochrany postupne zvyšujú funkčné požiadavky aj požiadavky kladené na záruky, ktoré má navrhovaný systém poskytovať.

Profily ochrany uvedené v tomto dokumente budeme označovať *úrovne bezpečnosti*. Jednotlivé profily ochrany (a teda úrovne bezpečnosti) sú hierarchické. Teda napr. PP úrovne bezpečnosti 3 obsahuje všetky funkčné požiadavky aj požiadavky na záruky, ktoré obsahujú PP úrovne bezpečnosti 1 a 2. Pokiaľ nie je povedané inak, všetky predpoklady, hrozby, organizačné bezpečnostné politiky, požiadavky a zdôvodnenia uvedené v tomto dokumente sa dotýkajú všetkých štyroch úrovní bezpečnosti.

Používatelia tohto dokumentu si sami zvolia, ktorý profil ochrany/ktorá úroveň bezpečnosti je pre nich primeraná, prihliadnuc k prostrediu, v ktorom bude konkrétny archív operovať.

Tento profil ochrany abstrahuje od povahy archivovaných dokumentov. Pokiaľ sa na archivované dokumenty vzťahuje špeciálna legislatíva (ako napríklad zákon o ochrane osobných údajov, prípadne zákon o ochrane utajovaných skutočností), je na autorovi ST, aby zvolil primerane vysokú úroveň bezpečnosti, prípadne inak zohľadnil legislatívne požiadavky na zabezpečenie archivovaných dokumentov.

#### 4.1.1 Identifikácia PP

**Názov:** Profil ochrany archívu elektronických dokumentov, úroveň bezpečnosti 1.

**Registrácia:** *Tento profil ochrany zatiaľ nebol nikde oficiálne registrovaný.*

**Verzia PP:** 1.0 z apríla 2004

**CC:** Part 2 extended, part 3 conformant, EAL 1 augmented

**Názov:** Profil ochrany archívu elektronických dokumentov, úroveň bezpečnosti 2.

**Registrácia:** *Tento profil ochrany zatiaľ nebol nikde oficiálne registrovaný.*

**Verzia PP:** 1.0 z apríla 2004

**CC:** Part 2 extended, part 3 conformant, EAL 2 augmented

**Názov:** Profil ochrany archívu elektronických dokumentov, úroveň bezpečnosti 3.

**Registrácia:** *Tento profil ochrany zatiaľ nebol nikde oficiálne registrovaný.*

**Verzia PP:** 1.0 z apríla 2004

**CC:** Part 2 extended, part 3 conformant, EAL 3 augmented

**Názov:** Profil ochrany archívu elektronických dokumentov,  
úroveň bezpečnosti 4.

**Registrácia:** *Tento profil ochrany zatiaľ nebol nikde oficiálne registrovaný.*

**Verzia PP:** 1.0 z apríla 2004

**CC:** Part 2 extended, part 3 conformant, EAL 4 augmented

**Autor:** Michal Forišek, FMFI UK Bratislava

**Verzia CC:** Common Criteria version 2.1

**Kľúčové slová:** archív, elektronické dokumenty

## 4.1.2 Prehľad

Profily ochrany uvedené v tomto dokumente špecifikujú minimálne bezpečnostné požiadavky kladené na archív elektronických dokumentov v rôznych bezpečnostných prostrediach. Tieto prostredia sú v tejto časti stručne zhrnuté. Ich podrobnejší popis nájdete v časti 4.2.

### PP úrovne bezpečnosti 1

Funkčné požiadavky aj požiadavky na záruky kladené na archív pri tejto úrovni bezpečnosti zodpovedajú prostrediu, v ktorom je nízka hrozba nepriateľských aktivít. Bezpečnostné požiadavky zahŕňajú separáciu rolí, ktorá poskytuje ochranu proti chybám autorizovaných používateľov. Neautorizovaným používateľom je obmedzený prístup k systému.

### PP úrovne bezpečnosti 2

Funkčné požiadavky aj požiadavky na záruky kladené na archív pri tejto úrovni bezpečnosti zodpovedajú prostrediu, kde síce je hrozba nepriateľských aktivít, ale nie od autorizovaných používateľov. Dopad prípadného úniku dát zo systému alebo straty archivovaných dát by mal byť nízky. Táto úroveň bezpečnosti pridáva zabezpečenie proti útoku nepriateľského používateľa pomocou dôslednejšej autentifikácie a procedúr v prípade neúspešnej autentifikácie.

### PP úrovne bezpečnosti 3

Funkčné požiadavky aj požiadavky na záruky kladené na archív pri tejto úrovni bezpečnosti zodpovedajú prostrediu, kde je dopad prípadného úniku či straty dát zo systému stredne závažný. Táto úroveň bezpečnosti navyše požaduje kontrolu integrity dát, pribúdajú mechanizmy na ich ochranu pred používateľmi s fyzickým prístupom. Takisto sú pridané nové požiadavky na záruky, ktoré umožnia kontrolovať bezpečné fungovanie systému.

### PP úrovne bezpečnosti 4

Funkčné požiadavky aj požiadavky na záruky kladené na archív pri tejto úrovni bezpečnosti zodpovedajú prostrediu, kde je dopad prípadného úniku či straty dát zo systému závažný. Na tejto úrovni bezpečnosti už považujeme za nepriateľských prostredie aj používateľov. Táto úroveň bezpečnosti by mala chrániť systém aj proti nepriateľským autorizovaným používateľom. Vyžaduje dostatočné záruky, že bezpečnostné funkcie systému naozaj fungujú bez chýb.

## 4.1.3 Organizácia dokumentu

Spomínané štyri profily ochrany sú prezentované ako jeden dokument. Keďže sú hierarchické, väčšina tohto dokumentu sa dotýka všetkých štyroch profilov ochrany. Všetky informácie, ktoré sa dotýkajú len konkrétnych profilov ochrany, budú jasne označené. Tento dokument je rozdelený do nasledujúcich častí:

- Časť 4.1 (Úvod) obsahuje úvodný popis našich profilov ochrany.
- Časť 4.2 (Popis systému) obsahuje podrobnejší popis realizácie a operácií archívu elektronických dokumentov. Tiež obsahuje podrobnejší popis jednotlivých úrovní bezpečnosti.
- Časť 4.3 (Bezpečnostné prostredie) obsahuje diskusiu o prostredí, v ktorom TOE realizujeme. Tu je uvedený zoznam hrozieb, ktorým musí čeliť TOE v kooperácii s prostredím.
- V časti 4.4 (Bezpečnostné ciele) definujeme bezpečnostné ciele pre TOE a jeho prostredie, ktoré sa budeme snažiť dosiahnuť.

- V časti 4.5 (Bezpečnostné požiadavky) uvedieme funkčné požiadavky a požiadavky na záruky, ktoré kladieme na TOE a jeho okolie. Tieto nám umožnia dosiahnuť vytýčené bezpečnostné ciele.
- V časti 4.6 (Zdôvodnenie) uvedieme podrobné zdôvodnenie rozhodnutí, ktoré boli spravené pri návrhu tohto profilu ochrany. Ukážeme, že naše bezpečnostné ciele pokrývajú všetky identifikované hrozby a predpoklady. Takisto ukážeme, že pomocou uvedených funkčných požiadaviek a požiadaviek na záruky vieme tieto bezpečnostné ciele dosiahnuť.
- V časti 4.7 (Použité skratky) sú stručne zhrnuté významy skratiek použitých v texte PP.

#### 4.1.4 Konvencie

Až na niekoľko výnimiek sú značenie, formátovanie a ostatné konvencie použité v tomto dokumente sú konzistentné s CC, verziou 2.1. Samotné znenia funkčných požiadaviek a požiadaviek na záruky sú uvádzané v angličtine v doslovnom znení z použitej verzie CC, zvyšný text vrátane vysvetľujúcich poznámok je v slovenčine. Navyše oproti konvenciám z CC boli kvôli uľahčeniu čítania zavedené nasledujúce pravidlá:

- Každá aplikácia operácie priradenia, výberu alebo upresnenia na funkčnú požiadavku je vysádzaná tučným písmom a podčiarknutá.
- Dokument obsahuje funkčné požiadavky, v ktorých boli niektoré operácie ponechané na upresnenie v bezpečnostnom zámere (ST). Tieto operácie sú označené [ST assignment: ...], resp. [ST selection: ...] a vysádzané kurzívou. V prípade operácie výberu sú uvedené možnosti, z ktorých si autor ST môže vybrať. V prípade operácie priradenia je uvedená špecifikácia priraditeľných subjektov, resp. objektov.
- Ak funkčná požiadavka obsahuje operácie, ktorých upresnenie je ponechané na autora ST, je za ňou spravidla uvedená poznámka, ktorá upresňuje význam potrebných upresnení.

## 4.2 Popis systému (TOE Description)

V mnohých navzájom rôznych situáciách sa stretávame s potrebou archivovať elektronické dokumenty. Pod pojmom „archív elektronických dokumentov“

rozumieme v tomto profile ochrany systém, ktorého základnou úlohou je zabezpečiť archivovanie elektronických dokumentov, ochranu ich integrity, prípadne aj dostupnosť a/lebo dôvernosť.

V závislosti od prostredia, v akom sú použité, od nárokov na zabezpečenie archivovaných dokumentov a od dodatočných požadovaných funkcií sa budú líšiť aj samotné implementácie archívu. V ďalšom texte popíšeme úplnú implementáciu archívu elektronických dokumentov, ku ktorej je písaný tento profil ochrany. Konkrétne implementácie v prostrediach, kde je kladený nižší dôraz na zabezpečenie systému, dostaneme z úplnej vynechaním a zlúčením častí, ktoré v konkrétnom bezpečnostnom prostredí nie sú relevantné. Ako sme už načrtli v 4.1.2 a podrobne rozoberieme v 4.2.3, problematiku rôznych nárokov na bezpečnosť bude tento profil ochrany riešiť definovaním štyroch *úrovní bezpečnosti*, z ktorých budú vyplývať rôzne funkčné požiadavky a požiadavky kladené na záruky, ktoré má systém poskytovať.

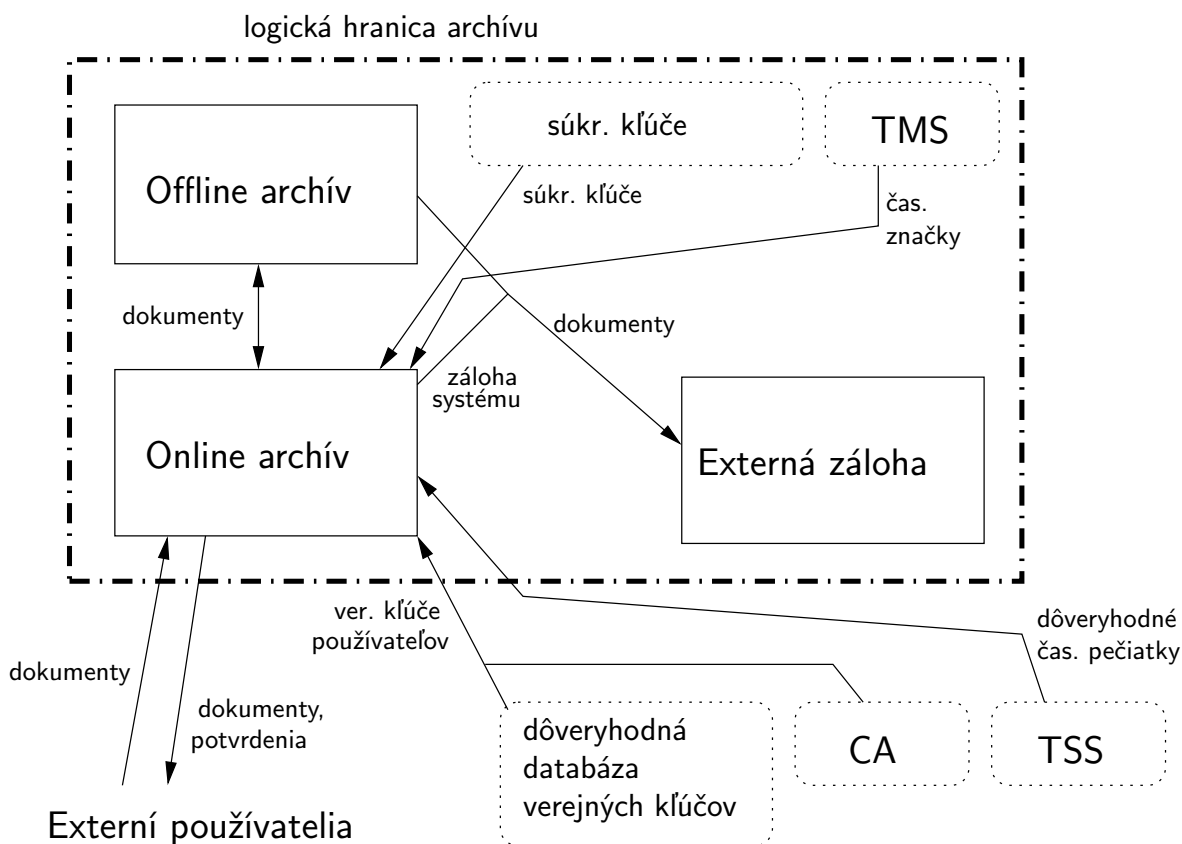
### 4.2.1 Interakcia systému s okolím

Obrázok 4.1 ukazuje možné logické rozdelenie archívu elektronických dokumentov, interakciu jednotlivých častí medzi sebou a jeho interakciu s IT prostredím, v ktorom sa nachádza. Archív elektronických dokumentov a jeho klienti tvoria uzavretý systém, fungujúci na základe ich dohody. Popíšeme teraz význam jednotlivých častí obrázku.

Samotný archív môže byť rozčlenený na dve časti, online a offline časť. K dokumentom uloženým v online archíve môžu autorizovaní používatelia pristupovať prostredníctvom počítačovej siete bez zásahu tretej strany. V praxi väčšinou online archív predstavuje diskové pole, offline archív dokumenty uložené na externých médiách.

Motivácií k takejto separácii je viacero. Spomeňme napríklad, že offline skladovanie dokumentov je v súčasnosti finančne neporovnateľne výhodnejšie. Navyše použitím vhodných nosičov (napr. neprepísateľné médiá ako CD-R, DVD-R) vieme ľahšie zabezpečiť integritu offline archivovaných dokumentov. Cenou za túto záruku je samozrejme zníženie ich dostupnosti. (Archív môže napr. ponúkať službu, kedy na požiadanie oprávnený zamestnanec dočasne presunie žiadané dokumenty z offline do online archívu.)

V prípade veľkého dopadu potenciálnej straty archivovaných dokumentov je potrebné zriadiť externý záložný archív. Tento archív by sa mal nachádzať na fyzicky odlišnom mieste, aby zvýšil pravdepodobnosť prežitia archivovaných materiálov aj v prípade prírodnej katastrofy (požiar, povodeň a pod.)



Obr. 4.1: Interakcia archívu a IT okolia

Väčšinou pôjde o offline archív s identickými záložnými kópiami archivovaných dokumentov. Okrem toho je potrebné na mieste mimo samotného online archívu pravidelne ukladať zálohy jeho software a údajov súvisiacich s bezpečnosťou.

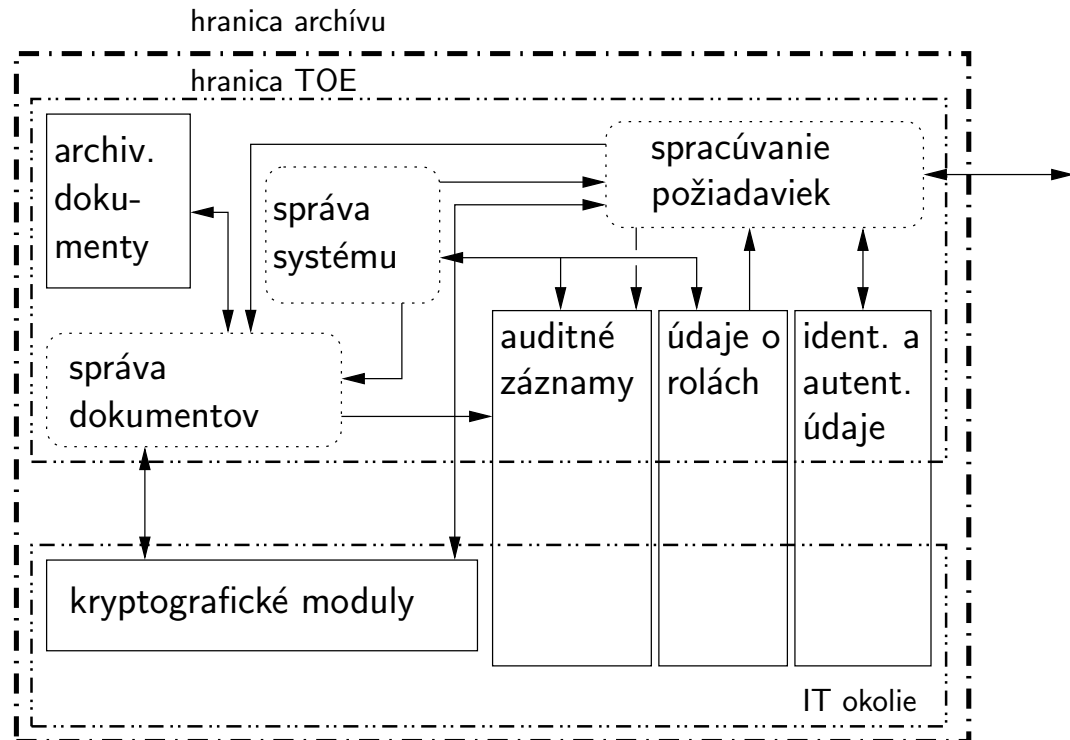
TMS (Time-Marking Service) je služba časových značiek, TSS (Time-Stamping Service) je služba časových pečiatok. Kvôli vedeniu auditných záznamov môže archív implementovať vlastnú službu časových značiek, prípadne (v prípade požadovaných vyšších záruk) využiť služby externej TSS. Časová značka je ekvivalent časovej pečiatky s nižšou presnosťou (napr. na sekundy) a úrovňou bezpečnosti. Podrobnejšie je problematika časových značiek rozpracovaná v [Vaš04].

CA (certifikačná autorita) poskytuje archívu kryptografické kľúče, ktoré je archív následne schopný použiť pri komunikácii s klientmi. Príkladom ta-

kejšto komunikácie môže byť prijatie zašifrovaného dokumentu určeného na uloženie do archívu, prípadne elektronické podpísanie vydávanej kópie archivovaného dokumentu. Tieto kľúče budú pravdepodobne uložené distribuovane v rámci systému (napr. každý používateľ má svoj súkromný kľúč, niektoré kľúče sú viazané na kryptografické tokeny a pod.) a musia byť príslušne chránené.

Archív môže využiť služby CA aj pri overovaní verejného kľúča klienta, prípadne môže verejné kľúče klientov získavať z nejakého dôveryhodného zdroja verejných kľúčov.

#### 4.2.2 Target of Evaluation



Obr. 4.2: Logické rozčlenenie archívu na TOE a okolie

Obrázok 4.2 ukazuje možné logické rozčlenenie archívu elektronických dokumentov. Významom tohto obrázku *nie je* vynútiť si zobrazenú architektúru systému, ide skôr o ukážku jednej možnosti, ako splniť požiadavky kladené

týmto profilom ochrany. *TOE (Target of Evaluation)* pre náš profil ochrany bude samotný systém realizujúci archivovanie dokumentov. Prípadné zvyšné časti archívu, ktoré navrhovaný systém využíva, budeme nazývať *(IT) okolím, resp. prostredím TOE*.

Funkcie, ktoré má archív plniť, môžeme rozdeliť na:

1. funkcie plnené TOE
2. kryptografické funkcie plnené kryptografickými modulmi
3. ostatné funkcie, ktoré môže zabezpečiť buď TOE alebo prostredie

Funkčné požiadavky na funkcie z prvej skupiny uvádzame v časti 4.5.2. Tieto funkcie musí realizovať priamo TOE a priamo sa dotýkajú jeho úlohy. Funkčné požiadavky na funkcie z druhej a tretej skupiny uvádzame v časti 4.5.1. Viaceré funkcie z tretej skupiny môžu byť zabezpečené operačným systémom (napr. identifikácia a autentifikácia) alebo podporným softvérom.

Ako znázorňuje obrázok, niektoré funkcie (napr. audit) môžu byť realizované v spolupráci TOE a prostredia. Navrhovaný systém môže byť napríklad realizovaný ako softvérový produkt bežiaci pod konkrétnym operačným systémom. V takomto prípade môže operačný systém (časť prostredia) spravovať prístup k auditným záznamom, zatiaľ čo TOE je zodpovedný za korektné generovanie ich obsahu.

### 4.2.3 Úrovne bezpečnosti

Ako sme už viackrát uviedli, archív elektronických dokumentov môže byť implementovaný v rôznych prostrediach a môžu byť kladené rôzne nároky na jeho bezpečnosť. Jeden extrém predstavuje napríklad systém určený na archivovanie interných firemných údajov, ku ktorému majú prístup len zamestnanci firmy. Opačný extrém predstavuje použitie v štátnej správe, kde je potrebné archivovať údaje o občanoch, niektoré z nich majú byť verejne dostupné prostredníctvom internetu, na iné sa vzťahuje zákon o ochrane osobných údajov, prípadne zákon o ochrane utajovaných skutočností. Ďalším príkladom je komerčný systém na archivovanie elektronických dokumentov, ktorý ponúka klientom možnosť archivovať dokumenty za cenu úmernú dobe archivácie a požiadavkám.

Rôzne nároky týchto implementácií na úroveň bezpečnosti systému riešime v tomto profile ochrany definovaním hierarchie štyroch *úrovní bezpečnosti*. Úlohou používateľov je analyzovať prostredie, v ktorom chcú konkrétny

archív implementovať, vyhodnotiť úroveň rizika, aké sú ochotní akceptovať, vyhodnotiť možné hrozby a podľa výsledkov si zvoliť príslušnú úroveň bezpečnosti, ktorú bude musieť ich implementácia splňať.

Množina predpokladov, identifikovaných hrozieb, bezpečnostných cieľov, funkčných požiadaviek a požiadaviek na záruky pre každú úroveň bezpečnosti tvorí samostatný profil ochrany.

### Úroveň bezpečnosti 1

*Úroveň bezpečnosti 1* predstavuje najnižšiu úroveň zabezpečenia. Systém implementovaný podľa tejto úrovne bezpečnosti je vhodné použiť v prostredí, kde je zanedbateľná, prípadne nízka pravdepodobnosť nepriateľských aktivít. Na dosiahnutie zabezpečenia systému pred chybami používateľov je zavedená separácia rolí. Systém by mal implementovať aspoň dve roly. Jedna z nich (administrátor) je bude zodpovedná okrem iného za správu bezpečnostných funkcií a používateľských kont, druhá (úradník) za operácie s archivovanými dokumentami. Je obmedzený prístup neautorizovaných používateľov do systému.

Všetky použité kryptografické algoritmy by mali zodpovedať medzinárodným štandardom. Všetky kryptografické funkcie by mali byť buď implementované priamo systémom a príslušne zabezpečené, alebo vykonávané kryptografickými modulmi, ktoré boli overené proti FIPS 140-2 na úroveň bezpečnosti 1 (alebo na zodpovedajúcu úroveň podľa iného podobného štandardu).

Profil ochrany na úrovni bezpečnosti 1 zodpovedá úrovni záruk *EAL 1 augmented* podľa Common Criteria.

### Úroveň bezpečnosti 2

*Úroveň bezpečnosti 2* je primeraná v prostredí, kde síce hrozia nepriateľské aktivity, ale nie od autorizovaných používateľov a kde je dopad prípadného prezradenia či poškodenia archivovaných dokumentov nízky. Úroveň zabezpečenia je zvýšená dôslednejšou ochranou proti útokom neautorizovaných používateľov prostredníctvom počítačovej siete. Podobne ako pri úrovni bezpečnosti 1 je potrebné implementovať aspoň dve navzájom nezlúčiteľné roly. Zvyšuje sa počet udalostí ukladaných do auditných záznamov. Pribúda kryptografická ochrana auditných záznamov aj zálohovaných údajov. Nároky na zabezpečenie prípadných kryptografických modulov stúpajú na úroveň 2.

Profil ochrany na úrovni bezpečnosti 2 zodpovedá úrovni záruk *EAL 2 augmented* podľa Common Criteria.

### Úroveň bezpečnosti 3

Systém navrhovaný s cieľom dosiahnuť *úroveň bezpečnosti 3* je primerané použiť v potenciálne nepriateľskom prostredí, kde je stredný dopad prípadného prezradenia či poškodenia archivovaných dokumentov. Táto úroveň bezpečnosti vyžaduje dodatočnú kontrolu integrity všetkých údajov v systéme, vrátane samotných archivovaných dokumentov. Zvyšuje sa ochrana proti používateľom s fyzickým prístupom k systému. Pribúdajú ďalšie požiadavky na záruky, ktorých cieľom je dodať dôveru, že systém funguje správne a bezpečne.

Táto úroveň bezpečnosti pridáva ochranu proti nepriateľským autorizovaným používateľom. Je vyžadovaná implementácia troch bezpečnostných rolí. Treťou rolou je auditor, ktorý je zodpovedný za správu a kontrolu auditných záznamov (a tým aj ostatných autorizovaných používateľov). Kryptografické moduly realizujúce dôležité kryptografické funkcie musia byť overené proti FIPS 140-2 na úroveň bezpečnosti 3.

Profil ochrany na úrovni bezpečnosti 3 zodpovedá úrovni záruk *EAL 3 augmented* podľa Common Criteria.

### Úroveň bezpečnosti 4

Systém navrhovaný s cieľom dosiahnuť *úroveň bezpečnosti 4* je primerané použiť v potenciálne nepriateľskom prostredí s potenciálne nepriateľskými autorizovanými používateľmi, kde by dopad prípadného prezradenia či poškodenia archivovaných dokumentov bol vysoký. Kvôli ochrane proti nepriateľským autorizovaným používateľom je vyžadovaná implementácia štyroch bezpečnostných rolí. Štvrtou rolou je operátor, zodpovedný za zálohovanie systému. Sú vyžadované dostatočné záruky, že bezpečnostné funkcie systému fungujú správne.

Kryptografické moduly realizujúce dôležité kryptografické funkcie musia byť overené proti FIPS 140-2 na úroveň bezpečnosti 4. (Toto je v súčasnej dobe ešte stále veľmi silná požiadavka. Napriek tomu ak sa autor ST rozhodne nesplniť ju, prípadne ju nahradíť inou, mal by v zdôvodnení uviesť motiváciu k takémuto kroku.)

Profil ochrany na úrovni bezpečnosti 4 zodpovedá úrovni záruk *EAL 4 augmented* podľa Common Criteria.

## 4.3 Bezpečnostné prostredie (Security Environment)

### 4.3.1 Aktíva

Primárnym aktívom, ktoré treba ochraňovať, sú samotné archivované dokumenty. Je nutné ochraňovať ich dôvernosť, autentickosť, integritu a dostupnosť.

Takisto je nutné ochraňovať dôvernosť a integritu interných údajov, ktoré zabezpečujú bezpečnosť systému (ako sú napríklad hašovacie hodnoty hesiel, súkromné kryptografické kľúče a pod.)

### 4.3.2 Legislatívne požiadavky

V tejto časti uvedieme tie časti slovenskej legislatívy (platné k 1. 1. 2004), ktoré sa priamo dotýkajú fungovania archívu elektronických dokumentov v podobe, v akej ho navrhujeme. Ku každej z nich uvedieme stručný komentár, ktoré časti zákona súvisia s našou problematikou. V tomto prehľade nie je zahrnutá legislatíva platná v krajinách Európskej únie, ale vzhľadom na požiadavky kladené na legislatívu SR pri integrácii do európskych štruktúr predpokladáme, že naša súčasná legislatíva s ňou už je kompatibilná. Úplné znenia všetkých tu uvedených zákonov (okrem starého zákona o archívniectve) nájdete napríklad v [Zbi].

#### **Zákon o účtovníctve (zákon č. 431/2002 Z.z.)**

- § 31 hovorí o účtovných záznamoch, umožňuje používať účtovné záznamy v elektronickej podobe, ak ich je možné previesť do písomnej formy.
- § 35 hovorí o uchovávaní účtovnej dokumentácie. Zákon určuje minimálnu dobu archivácie pre účtovné záznamy. Táto sa pohybuje od 5 do 10 rokov. Na nakladanie s účtovnou dokumentáciou sa vzťahujú všeobecné predpisy o archívniectve.

**Zákon o archívnictve (zákon č. 149/1975 Zbierky)**

Celý tento zákon sa dotýka archívnictva, definuje archívne dokumenty, podmienky na ich ochranu a využívanie. (Ďalej ešte hovorí o štátnych archívoch.) Vzhľadom na rok, z ktorého pochádza, neobsahuje nič špecificky sa dotýkajúce archivovania elektronických dokumentov. Z pohľadu tohto zákona je teda rovnako dobre možné archivovať dokumenty v elektronickej aj v klasickej podobe.

**Zákon o ochrane utajovaných skutočností (zákon č. 241/2001 Z.z.)**

Plný názov zákona: Zákon o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.

- § 3 hovorí o klasifikácii utajovaných skutočností podľa stupňa utajenia.
- § 6 hovorí o koncepcii ochrany utajovaných skutočností, okrem iného sa v ňom spomína personálna bezpečnosť, administratívna bezpečnosť, šifrová ochrana informácií, fyzická a objektová bezpečnosť, atď.
- Druhá hlava (§ 9,10) hovorí o zodpovednosti za ochranu utajovaných skutočností.
- Piata hlava (§ 49,50) podrobnejšie špecifikuje fyzickú a objektovú bezpečnosť.
- § 52,53 hovoria o certifikácii technických a systémových prostriedkov, ktoré sú použité pri ochrane utajovaných skutočností. Podmienkou certifikácie technického prostriedku je posúdenie jeho bezpečnostného projektu. Ten bližšie špecifikuje § 54.
- Tretia časť (§ 61-65) hovorí o šifrovej ochrane informácií.

**Zákon o elektronickom podpise (zákon č. 215/2002 Z.z.)**

Tento zákon okrem iného definuje elektronický podpis, zaručený elektronický podpis, časovú pečiatku, podmienky ich používania a platnosti.

**Ostatné**

V okrajových prípadoch sa ešte uvažovanej problematiky môže dotýkať Občiansky zákonník a Obchodný zákonník.

### 4.3.3 Predpoklady bezpečnej prevádzky (Secure Usage Assumptions)

V tejto časti vymenujeme predpoklady, na základe ktorých je postavený celý ďalší návrh a analýza systému.

#### **Predpoklady platné pre všetky úrovne bezpečnosti**

*A.Auditori kontrolujú auditné záznamy.* Je nutné mať auditné záznamy o relevantných udalostiach. Tieto záznamy musia byť kontrolované auditorom.

*A.Bezpečný operačný systém.* Operačný systém použitý pri realizácii TOE poskytuje bezpečnostné funkcie, ktoré efektívne potláčajú hrozby, týkajúce sa zvolenej úrovne bezpečnosti.

Tento PP sa špecificky nevenuje vlastnostiam použitého operačného systému. Je však potrebné uvedomiť si, že operačný systém väčšinou funguje ako prostredník medzi niektorými časťami TOE. Použitý operačný systém nesmie mať zraniteľnosti, ktoré by ohrozili bezpečné fungovanie TOE. V prípade, že niektoré bezpečnostné funkcie budú ponechané na operačný systém, je nutné použiť dostatočne bezpečný operačný systém.

*A.Certifikačná autorita a PKI.* Predpokladáme, že existuje akreditovaná certifikačná autorita a public-key infraštruktúra potrebná na to, aby archív mohol bezpečnou cestou získať a obnovovať svoje verejné a súkromné kľúče, ktoré bude môcť používať pri komunikácii so svetom (na šifrovanie aj podpisovanie dokumentov) a na overovanie pravosti verejných kľúčov klientov.

*A.Čitateľnosť médií.* Médiá použité na ukladanie offline archivovaných dokumentov sú čitateľné. Prípadné starnutie médií je riešené pravidelnou kontrolou a kopírovaním údajov na nové médiá. S každým typom použitých médií sa spravuje aj dostatočný počet funkčných čítacích zariadení.

*A.Fyzická ochrana.* Všetky dôležité komponenty TOE (hardvér, softvér, prípadne aj firmvér) sú dostatočne chránené proti fyzickému útoku, ktorý by mohol narušiť ich funkčnosť alebo bezpečnosť údajov v nich obsiahnutých.

*A.Kompetentní administrátori, operátori, úradníci a auditori.* Všetci administrátori, operátori, úradníci aj auditori, ktorí zabezpečujú fungovanie TOE, sú kompetentní vykonávať svoje funkcie.

*A.Manažment autentifikačných údajov.* Je zabezpečené, aby si všetci používatelia boli nútení pravidelne meniť svoje autentifikačné údaje (heslá a pod.). Autentifikačné údaje musia nadobúdať primerané hodnoty (napr. mať primeranú dĺžku, zložitosť, odlišnosť od predchádzajúcich).

*A.Upozornenie zodpovedných na bezpečnostné problémy.* Všetci používatelia bezodkladne informujú zodpovedných o prípadných bezpečnostných problémoch, čím sa minimalizuje dopad týchto problémov a potenciálna možnosť poškodenia systému.

*A.Výuka proti sociálnemu inžinierstvu.* Všetci používatelia sú informovaní o technikách sociálneho inžinierstva a metódach boja proti nim.

*A.Zničenie autentifikačných údajov.* V prípade zmeny prístupových práv používateľa (napr. rozviazanie pracovného pomeru, zmena úrovne jeho zodpovednosti) sú príslušné autentifikačné údaje a s nimi súvisiace privilégia odstránené.

### **Predpoklady platné len pre niektoré úrovne bezpečnosti**

*A.Administrátori, operátori, úradníci a auditori nezneužívajú právomoci.* (Úroveň bezpečnosti 1-2.) Administrátorom, operátorom, úradníkom a auditorom sa verí, že nezneužijú svoje právomoci.

*A.Kooperatívni používatelia.* (Úroveň bezpečnosti 1-3.) Používatelia na vykonávanie svojich činností potrebujú prístup k niektorým informáciám obsiahnutým v TOE. Predpokladá sa, že sa budú správať kooperatívne, t.j. výhradne spôsobom zamýšľaným pri návrhu TOE.

*A.Časové pečiatky.* (Úroveň bezpečnosti 4.) Predpokladáme, že existuje externá služba časových pečiatok, ktorej služby bude môcť archív v prípade potreby využívať.

### **4.3.4 Identifikácia hrozieb**

Na tomto mieste identifikujeme a rozoberieme hrozby, ktoré sa týkajú nami navrhovaného TOE. V ďalších častiach na základe identifikovaných hrozieb

navrhujeme bezpečnostné ciele a operácie, ktoré povedú k dosiahnutiu stanovených bezpečnostných cieľov a eliminácií identifikovaných hrozieb.

Hrozby, ktorými sa budeme zaoberať, môžeme rozdeliť do niekoľkých skupín:

- Hrozby súvisiace s kryptografiou.
- Hrozby spojené s právomocami používateľov.
- Hrozby spojené s externým útokom.
- Hrozby spojené s poškodením dokumentov.
- Hrozby spojené s funkčnosťou systému.

---

### Hrozby, dotýkajúce sa všetkých úrovní bezpečnosti

#### Hrozby spojené s kryptografiou

*T.Kompromitácia súkromných kľúčov.* Môže dôjsť k prezradeniu, prípadne aj k úmyselnej zmene používaných súkromných kryptografických kľúčov.

*T.Útok na kryptografické funkcie.* Na miestach, kde procedúry archívu využívajú kryptografické funkcie, sa môže útočník pokúsiť tieto funkcie prelomiť a tak kompromitovať bezpečnosť aktív. Tento útok sa môže týkať ľubovoľných kryptografických funkcií vrátane kódovania, dekódovania, podpisovania a rátania hašovacej hodnoty. Metódou útoku je buď využiť zraniteľnosť v dotyčnom algoritme (resp. jeho implementácii), alebo využiť hrubú silu pri hľadaní vhodných kľúčov a vstupov. Cieľom útočníka je získať prístup k utajovaným údajom.

#### Hrozby spojené s právomocami používateľov

*T.Poškodenie údajov chybou používateľa.* Používateľ omylom zmaže údaje, čím ohrozí funkčnosť systému, prípadne znemožní dostupnosť zmazaných dát.

*T.Vynechanie dôležitej administratívnej činnosti.* Administrátor, operátor, úradník alebo auditor zabudne vykonať nejakú činnosť, ktorá je dôležitá pre zabezpečenie systému.

*T.Zneužitie privilégií na získanie údajov.* Používateľ zneužije svoje privilégiá s cieľom získať prístup k citlivým údajom (napr. archivovaným dokumentom, údajom súvisiacim s bezpečnosťou TOE a pod.)

### **Hrozby spojené s externým útokom**

*T.Neoprávnené získanie prístupu.* Hacker sa môže pokúsiť využiť zraniteľnosti v jemu prístupnej časti archívu, aby takto získal neoprávnené privilégiá a následný prístup k archivovaným údajom.

*T.Neoprávnený fyzický prístup.* Útočník sa môže pokúsiť získať fyzický prístup k chráneným aktívam, a to najčastejšie obídením alebo oklamaním bezpečnostnej kontroly pri vstupe do fyzicky chránenej časti systému. Tým je okamžite ohrozená dostupnosť archivovaných dokumentov a zvyšuje sa útočníkov potenciál ohroziť aj ich autentickosť.

*T.Odpočúvanie komunikácie.* Útočník môže monitorovať komunikáciu, ktorá prebieha elektronickou cestou medzi archívom a zvyškom sveta. Takto získané údaje môže použiť na ďalšie napadnutie systému, prípadne môže touto cestou získať neoprávnený prístup k dokumentom ukladaným do archívu.

*T.Sociálne inžinierstvo.* Útočník sa môže pokúsiť použitím techník sociálneho inžinierstva získať informácie o prístupe do systému, jeho použití a fungovaní a prípadne ich využiť na neoprávnený prístup do systému a jeho poškodenie.

*T.Zabránenie vykonávaniu funkcie.* Cieľom tohto útoku<sup>1</sup> je zabrániť cieľovému systému vykonávať jeho funkciu. Použité metódy zahŕňajú využitie zraniteľnosti systému na jeho poškodenie a zahltenie systému väčším množstvom požiadaviek ako je schopný spracúvať.

### **Hrozby spojené s poškodením dokumentov**

*T.Starnutie čítacích zariadení.* Zároveň so vznikom nových typov médií sa zariadenia, slúžiace na čítanie starých typov médií, postupne prestávajú používať. Toto môže byť problémom v prípade, ak v archíve zostanú archivované dokumenty na médiách, ku ktorým už nebudú čítacie zariadenia existovať.

---

<sup>1</sup>Známeho pod anglickým názvom *denial of service attack*.

*T.Starnutie médií.* Je možné, že počas archivácie dokumentu na dlhšiu dobu jeho médium natolko zostarne, že dokument nebude čitateľný.

### **Hrozby spojené s funkčnosťou systému**

*T.Nepriateľský kód.* Do systému sa (napr. prostredníctvom autorizovaného používateľa, hackera, vďaka zraniteľnosti a pod.) dostane a následne je spustený nepriateľský kód. Ten môže narušiť integritu, dostupnosť a j utajenie aktív systému.

Môže ísť napr. o počítačový vírus, *trójskeho koňa* (program, ktorý pod zámienkou presvedčí používateľa, aby ho spustil a ktorého jedinou úlohou je napadnutie a poškodenie systému, na ktorom je spustený) alebo o *rootkit* (program, ktorý je zameraný na vyhľadávanie a využitie zraniteľností v systéme).

*T.Zlyhanie hardvéru alebo softvéru.* Chyba v používanom hardvéri alebo softvéri môže obmedziť, prípadne úplne znemožniť archívu vykonávanie jeho funkcií.

Hrozby, dotýkajúce sa len niektorých úrovní bezpečnosti

### **Hrozby spojené s právomocami používateľov**

*T.Chyby administrátorov, operátorov, úradníkov a auditorov.* (Úrovne bezpečnosti 1-2.) Administrátor, operátor, úradník alebo auditor môže neúmyselne zapríčiniť chybu, ktorá povedie k narušeniu bezpečnosti systému.

*T.Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov.* (Úrovne bezpečnosti 3-4.) Administrátor, operátor, úradník alebo auditor môže neúmyselne zapríčiniť chybu, ktorá povedie k narušeniu bezpečnosti systému, prípadne úmyselne upraviť konfiguráciu systému tak, aby tým narušil jeho bezpečnosť.

### **Hrozby spojené s poškodením dokumentov**

*T.Prírodná katastrofa.* (Úrovne bezpečnosti 3-4.) V prípade prírodnej katastrofy (požiar, povodeň, zemetrasenie a pod.), ktorá zasiahne samotný

archív, môže dôjsť k vážnemu poškodeniu aj zničeniu všetkých aktív, vrátane archivovaných dokumentov.

### Hrozby spojené s funkčnosťou systému

*T.Chyby v softvéri archívu* (Úrovne bezpečnosti 2-4.) V samotnej softvérovej implementácii archívu môžu byť chyby, ktoré môžu viesť ako k narušeniu bezpečnostných funkcií archívu, tak aj k poškodeniu samotných archivovaných dokumentov. Tieto chyby mohli vzniknúť neúmyselne (výsledok zlého návrhu, resp. zlej implementácie), ale aj úmyselne (programátorom nechané zadné dvierka, umožňujúce mu prístup do systému).

### 4.3.5 Organizačná bezpečnostná politika

*P.Kryptografické štandardy.* Všetky použité kryptografické prostriedky (šifrovacie, hašovacie funkcie, atď.) musia byť v súlade so štandardmi ISO, legislatívou, prípadne aj inými podmienkami, vyplývajúcimi z povahy archivovaných dokumentov.

(Za medzinárodné štandardy sa považujú napr. šifrovacie algoritmy triple-DES, AES, RSA, podpisové schémy RSA, ElGamal a hašovacie funkcie MD5 a SHA-1. Dobrou možnosťou je používať výhradne funkcie, ktoré NIST odporúčal, prípadne schválil ako FIPS.)

*P.Používanie informácií na autorizované účely.* Ľubovoľné informácie obsiahnuté v TOE by mali byť použité výhradne na autorizované účely.

## 4.4 Bezpečnostné ciele (Objectives)

V tejto časti definujeme bezpečnostné ciele nášho systému. Tieto ciele odrážajú náš zámer zabrániť uskutočneniu identifikovaných hrozieb a splňať uvedenú bezpečnostnú politiku.

Bezpečnostné ciele rozdelíme kvôli prehľadnosti na ciele, ktoré má splniť TOE, ciele, ktoré má splniť prostredie, v ktorom bude TOE prevádzkovaný a ciele, ktoré plní TOE v kooperácii s prostredím. V rámci každej časti sú samostatne uvedené ciele, ktoré sa dotýkajú len niektorých úrovní bezpečnosti, pri názve každého z nich sú uvedené úrovne bezpečnosti, ktorých sa dotýka. V rámci skupiny sú bezpečnostné ciele zoradené abecedne podľa názvov.

#### 4.4.1 Bezpečnostné ciele pre TOE

Bezpečnostné ciele pre všetky úrovne bezpečnosti

*O.Archivované dokumenty.* TOE musí zabezpečiť zachovanie integrity, dôvernosti a prípadne aj dostupnosti archivovaných dokumentov.

*O.Zálohovanie a obnova systémových dát.* Systémové dáta musia byť pravidelne zálohované. Priestor na ukladanie týchto záloh musí byť dostatočne veľký. Musí existovať možnosť efektívne obnoviť systém pomocou zálohovaných dát.

#### 4.4.2 Bezpečnostné ciele pre prostredie

Bezpečnostné ciele pre všetky úrovne bezpečnosti

##### Ciele nedotýkajúce sa IT

*O.Auditori kontrolujú auditné záznamy.* Je potrebné sledovať všetky udalosti súvisiace s bezpečnosťou systému. Kvôli tomuto účelu musia auditori kontrolovať auditné záznamy s frekvenciou zodpovedajúcou úrovni možného rizika.

*O.Čitateľnosť médií.* Je potrebné zabezpečiť čitateľnosť médií použitých na ukladanie offline archivovaných dokumentov. Prípadné starnutie médií je potrebné riešiť pravidelnou kontrolou a kopírovaním údajov na nové média. S každým typom použitých médií je potrebné spravovať aj dostatočný počet funkčných čítacích zariadení.

*O.Dokumentácia pre administrátorov, operátorov, úradníkov a auditorov.* Administrátori, operátori, úradníci aj auditori majú mať k dispozícii dostačujúcu dokumentáciu o konfigurácii a prevádzke systému.

*O.Fyzická ochrana.* Zodpovední za fungovanie TOE musia zabezpečiť, že všetky dôležité komponenty TOE sú dostatočne chránené proti fyzickému útoku, ktorý by mohol narušiť ich funkčnosť alebo bezpečnosť údajov v nich obsiahnutých.

*O.Inštalácia systému.* Zodpovední za fungovanie TOE musia zabezpečiť, že bude na svoje miesto doručený, nainštalovaný a následne spravovaný tak, aby nebola narušená jeho informačná bezpečnosť.

- O.Kompetentní administrátori, operátori, úradníci a auditori.* Administrátori, operátori, úradníci aj auditori majú byť kompetentní vykonávať svoje úlohy a zabezpečiť fungovanie systému a jeho bezpečnosť.
- O.Manažment autentifikačných údajov.* Treba zabezpečiť, aby používatelia boli nútení pravidelne meniť svoje autentifikačné údaje (heslá a pod.). Autentifikačné údaje musia nadobúdať primerané hodnoty (napr. mať primeranú dĺžku, zložitosť, odlišnosť od predchádzajúcich).
- O.Upozornenie zodpovedných na bezpečnostné problémy.* O ľubovoľnom bezpečnostnom probléme je potrebné čo najskôr informovať zodpovedných, čím sa minimalizuje dopad týchto problémov a potenciálna možnosť poškodenia systému.
- O.Výuka proti sociálnemu inžinierstvu.* Užívatelia musia byť poučení o technikách sociálneho inžinierstva a metódach potláčania takýchto útokov.
- O.Zničenie autentifikačných údajov.* Treba umožniť vhodné zničenie autentifikačných údajov a odstránenie s nimi súvisiacich privilégií v prípade zmeny prístupových práv používateľa (napr. rozviazanie pracovného pomeru, zmena úrovne jeho zodpovednosti).

### **Ciele dotýkajúce sa IT**

- O.Bezpečnostné roly.* Treba udržiavať bezpečnostné roly a ich priradenie používateľom.
- O.Certifikačná autorita a PKI.* Archív získava, spravuje a obnovuje vlastné kryptografické kľúče, ktoré môže používať pri komunikácií so svetom. Vie si overiť pravosť a platnosť ľubovoľného korektného verejného kľúča klienta.
- O.Kryptografické funkcie.* Všetky implementované kryptografické algoritmy (používané na šifrovanie/dešifrovanie, autentifikáciu, podpisovanie, atď.) musia byť v súlade s príslušnými štandardmi. Všetky použité kryptografické moduly musia mať dostatočnú overenú úroveň zabezpečenia (napr. podľa FIPS 140-2).
- O.Operačný systém.* Použitý operačný systém by mal poskytovať dostatočnú úroveň bezpečnosti, teda napr. separáciu domén (napr. archivovaných

dát od dát potrebných pre fungovanie TOE) a neobíditeľnosť bezpečnostných mechanizmov. Vhodné je dodržiavať bezpečnostné požiadavky odporúčané NISTom v [NIST03a].

*O.Overenie bezpečnostných funkcií.* Je potrebné overiť, či správne fungujú všetky funkcie poskytované softvérom a hardvérom súvisiacim s bezpečnosťou systému.

*O.Pravidelná kontrola integrity.* Je potrebné pravidelne kontrolovať integritu hardvéru aj softvéru použitého v systéme.

### Bezpečnostné ciele len pre niektoré úrovne bezpečnosti

#### Ciele nedotýkajúce sa IT

*O.Administrátori, operátori, úradníci a auditori nezneužívajú právomoci.* (Úroveň bezpečnosti 1-2.) Treba dôveryhodných administrátorov, operátorov, úradníkov a auditorov.

*O.Bezpečnosť počas životného cyklu.* (Úroveň bezpečnosti 2-4.) Počas fázy vývoja systému je potrebné mať k dispozícii vhodné nástroje a postupy, umožňujúce vytvoriť bezpečný systém. Počas operačnej fázy je potrebné efektívne odhaľovať a odstraňovať chyby.

*O.Hľadanie chýb v zdrojovom kóde.* (Úroveň bezpečnosti 4.) Vykoná sa inšpekcia zdrojového kódu systému s cieľom odhaliť neúmyselne aj úmyselne spravené chyby v ňom, vrátane prípadných zadných dvierok ponechaných programátorom.

*O.Kooperatívni používatelia.* (Úroveň bezpečnosti 1-3.) Je potrebné zabezpečiť, aby sa používatelia pri vykonávaní svojich činností správali kooperatívne, t.j. výhradne spôsobom zamýšľaným pri návrhu TOE.

*O.Oprava identifikovaných bezpečnostných chýb.* (Úroveň bezpečnosti 2-4.) Dodávateľ systému opravuje bezpečnostné chyby odhalené používateľmi.

### Ciele dotýkajúce sa IT

*O.Trusted path.* (Úroveň bezpečnosti 3-4.) Je potrebné vytvoriť medzi používateľom a systémom dôveryhodný komunikačný kanál. Takisto je potrebné vytvoriť dôveryhodný kanál slúžiaci na prístup k údajom súvisiacim s bezpečnosťou systému. Tieto kanály by mali zaručovať identity komunikujúcich strán (a teda vylúčiť možnosť odpočúvania treťou stranou a zásahu tretej strany do komunikácie).

(Trusted path prvého typu môže byť realizovaná napríklad pomocou PKI, trusted path druhého typu ako lokálna administrátorská konzola.)

#### 4.4.3 Bezpečnostné ciele pre TOE spolu s prostredím

##### Bezpečnostné ciele pre všetky úrovne bezpečnosti

*O.Časové značky.* Archív generuje časové značky za účelom overenia následnosti zaznamenaných udalostí.

*O.Import a export údajov.* Pri importe a exporte údajov cez nedôveryhodné prostredie je potrebné ich chrániť pred neautorizovaným prístupom a modifikáciou.

*O.Individuálna zodpovednosť a auditné záznamy.* Za každú zo zaznamenaných udalostí je zodpovedný používateľ, ktorý je jej pôvodcom. V auditných záznamoch musí byť pri každej udalosti okrem jej pôvodcu uvedený aj presný čas a dátum tejto udalosti.

*O.Manažment autorizácie používateľov.* Je potrebné spravovať údaje o autentifikáciách a právomociach používateľov tak, aby boli konzistentné s organizačnou bezpečnosťou a personálnou politikou.

*O.Manažment konfigurácie.* Je potrebné implementovať manažment konfigurácie systému – zmien hardvéru, softvéru, firmvéru, dokumentácie, testov a ich dokumentácie v priebehu vývoja a životného cyklu systému.

*O.Manažment konfigurácie bezpečnostných funkcií.* Je potrebné implementovať manažment údajov súvisiacich s bezpečnostnou politikou a funkciami vynucujúcimi bezpečné fungovanie systému.

*O.Obmedzenie administratívneho prístupu.* Administrátori by nemali mať automaticky prístup k dátam iných používateľov. V prípade, že je to

potrebné pri odstraňovaní chýb v systéme, resp. bezpečnostných problémov, je nutné ich prístup k dátam používateľov kontrolovať a zaznamenať.

- O. Obmedzenie možností pred autentifikáciou.* Kým si TOE neoverí identitu používateľa, mal by tento mať príslušne obmedzenú množinu povolených operácií so systémom.
- O. Odstránenie nepriateľského kódu obnovou.* Po prípadnom napadnutí a poškodení systému nepriateľským kódom musí byť možné obnoviť ho do funkčného stavu, v ktorom už systém nebude obsahovať dotýčny nepriateľský kód.
- O. Ochrana pred nepriateľským kódom.* Treba implementovať postupy a mechanizmy, brániace nepriateľskému kódu napadnúť systém. (Např. antivírová ochrana, zákaz inštalovať programy stiahnuté z internetu.)
- O. Ochrana uložených auditných záznamov.* Všetky auditné záznamy musia byť chránené proti neautorizovanému prístupu, zmene, prípadne zmažaniu. Tým sa zabezpečí individuálna zodpovednosť používateľov.
- O. Ochrana údajov pri internom prenose.* Počas interných presunov údajov (či už ide o dáta používateľov, alebo údaje súvisiace z bezpečnostnými funkciami) je potrebné zabezpečiť ich integritu a dôvernosť.
- O. Reakcia na možnú stratu auditných záznamov.* V prípade, že ukladací priestor určený pre auditné záznamy je plný, resp. skoro plný, je potrebné zabrániť strate nových auditných záznamov. Je potrebné informovať zodpovedných o vzniknutej situácii, situáciu riešiť a prípadne dočasne obmedziť rozsah povolených akcií.
- O. Udržiavanie bezpečnostných atribútov pre používateľov.* S každým používateľom je okrem jeho identity potrebné asociovať aj množinu jeho bezpečnostných atribútov (ako sú např. príslušnosť k rolám v rámci systému, prístupové práva, atď.).
- O. Zistenie modifikácie softvéru a záložných údajov.* Každé porušenie integrity použitého softvéru vrátane záložných údajov musí byť odhaliteľné. Preto je potrebné zaviesť spôsob kontroly ich integrity.

## Bezpečnostné ciele len pre niektoré úrovne bezpečnosti

*O.Časové pečiatky.* (Úroveň bezpečnosti 4.) Archív v pravidelných intervaloch získa dôveryhodnú časovú pečiatku od tretej strany, túto pečiatku použije na zaručenie následnosti zaznamenaných udalostí.

*O.Reakcia na odhalené útoky.* (Úrovne bezpečnosti 2-4.) Je potrebné implementovať automatickú notifikáciu (prípadne iné spôsoby reakcie) v prípade, že bezpečnostné funkcie systému odhalia pokus o útok. Nasledovať by mala snaha podrobne identifikovať útok a zabrániť mu.

## 4.5 Bezpečnostné požiadavky (Security Requirements)

### 4.5.1 Funkčné požiadavky na prostredie

V tejto časti špecifikujeme funkčné požiadavky, ktoré sa vzťahujú na IT okolie nášho systému. ST, ktoré chcú byť konformné s našim profilom ochrany, môžu tieto požiadavky špecifikovať ako požiadavky na TOE, na jeho okolie alebo na oboje. (Pri vhodnej implementácii môže niektoré z týchto funkčných požiadaviek realizovať priamo TOE, ale nie je to vyžadované.)

Ak je funkčná požiadavka v texte uvedená bez špecifikovania úrovne bezpečnosti, znamená to, že sa vzťahuje na všetky úrovne. V opačnom prípade je jasne vyznačené, na ktoré úrovne bezpečnosti sa jej text vzťahuje.

Tabuľka 4.1 obsahuje funkčné požiadavky uvedené v tejto časti. Kvôli ľahšej orientácii sú utriedené v abecednom poradí. Pri každej požiadavke je uvedený, kde je zaradená a ktorých úrovni bezpečnosti sa dotýka.

Tabuľka 4.1: Funkčné požiadavky na prostredie.

Funkčná požiadavka	Časť textu	úrovne bezp.
FAU_GEN.1 Audit data generation	4.5.1.2 Bezpečnostný audit	1-4
FAU_GEN.2 User identity association	4.5.1.2 Bezpečnostný audit	1-4
FAU_SAR.1 Audit review	4.5.1.2 Bezpečnostný audit	1-2,3-4
FAU_SAR.3 Selectable audit review	4.5.1.2 Bezpečnostný audit	1-4
FAU_STG.1 Protected audit trail storage	4.5.1.2 Bezpečnostný audit	1-4
FAU_STG.3 Action in case of possible audit data loss	4.5.1.2 Bezpečnostný audit	1-4

Tabuľka 4.1: (pokračovanie)

Funkčná požiadavka	Časť textu	úrovne bezp.
FAU_STG.4 Prevention of audit data loss	4.5.1.2 Bezpečnostný audit	1-2,3-4
FCS_CKM.4 Cryptographic key destruction	4.5.1.6 Správa kryptografických kľúčov	1-4
FCS_COP.1 Cryptographic operation	4.5.1.8 Kryptografické moduly	1-4
FDP_ACC.1 Subset access control	4.5.1.3 Kontrola prístupu	1-4
FDP_ACF.1 Security attribute based access control	4.5.1.3 Kontrola prístupu	1-4
FDP_ITT.1 Basic internal transfer protection	4.5.1.5 Interné presuny dát	1-4
FDP_UCT.1 Basic data exchange confidentiality	4.5.1.5 Interné presuny dát	1-4
FIA_AFL.1 Authentication failure handling	4.5.1.4 Ident. a autentifikácia	2-4
FIA_ATD.1 User attribute definition	4.5.1.4 Ident. a autentifikácia	1-4
FIA_UAU.1 Timing of authentication	4.5.1.4 Ident. a autentifikácia	1-4
FIA_UID.1 Timing of identification	4.5.1.4 Ident. a autentifikácia	1-4
FIA_USB.1 User-subject binding	4.5.1.4 Ident. a autentifikácia	1-4
FMT_MOF.1 Management of security functions behaviour	4.5.1.1 Bezpečnostné roly	1-4
FMT_MSA.1 Management of security attributes	4.5.1.1 Bezpečnostné roly	1-4
FMT_MSA.2 Secure security attributes	4.5.1.1 Bezpečnostné roly	2-4
FMT_MSA.3 Static attribute initialisation	4.5.1.1 Bezpečnostné roly	1-4
FMT_MTD.1 Management of TSF data	4.5.1.1 Bezpečnostné roly	1-2,3-4
FMT_SMR.2 Restrictions on security roles	4.5.1.1 Bezpečnostné roly	1-2,3,4
FPT_AMT.1 Abstract machine testing	4.5.1.7 Testovanie systému	1-4
FPT_ITT.1 Basic internal TSF data transfer protection	4.5.1.5 Interné presuny dát	1-4
FPT_RVM.1 Non-bypassability of the TSP	4.5.1.3 Kontrola prístupu	1-4
FPT_SEP.1 TSF domain separation	4.5.1.3 Kontrola prístupu	1-4
FPT_STM.1 Reliable time stamps	4.5.1.2 Bezpečnostný audit	1-4
FTP_TRP.1 Trusted path	4.5.1.4 Identifikácia a autentifikácia	3-4

#### 4.5.1.1 Bezpečnostné roly

Právomoc vykonávať mnohé z funkcií špecifikovaných v tomto profile ochrany bude priradená jednej z bezpečnostných rolí, definovaných v rámci systému. Rozdelenie právomocí prispeje k bezpečnosti systému tým, že sťaží používateľom zneužitie ich právomocí. V ideálnom prípade by mal každý používateľ

mať práve právomoci potrebné na vykonávanie jeho úlohy v systéme.

V tejto časti definujeme bezpečnostné roly, ktorým budeme v ďalšom texte pridelať práva a povinnosti. Každéj role môže byť priradených viacero jednotlivcov. Pokiaľ to text tohto profilu ochrany explicitne nezakazuje, môže jednotlivec zastávať aj viacero bezpečnostných rolí.

Nie je nutné, aby TOE implementoval všetky uvedené bezpečnostné roly. Zo zvolenej úrovne bezpečnosti však vyplývajú požiadavky na separáciu rolí (t.j. niektoré dvojice rolí nemôže zastávať jeden používateľ). V prípade, že TOE neimplementuje všetky uvedené roly, právomoci pôvodne pridelené neimplementovanej role musia byť prerozdelené medzi implementované roly.

Definujeme nasledujúce bezpečnostné roly:

**Administrátor** – rola autorizovaná inštalovať, konfigurovať a spravovať systém, tvoriť a rušiť používateľské kontá a pod.

**Operátor** – rola autorizovaná vykonávať zálohy systémových aj archivovaných dát a prípadnú obnovu systému zo zálohy.

**Úradník** – rola autorizovaná prijímať dokumenty, určené na archiváciu, vkladať ich do archívu, vydávať potvrdenia a kópie a pod.

**Auditor** – rola autorizovaná kontrolovať a spravovať auditné záznamy.

Funkčné požiadavky dotýkajúce sa tejto oblasti:

#### **FMT\_SMR.2 Restrictions on security roles**

Hierarchical to: FMT\_SMR.1

Upozornenie: FMT\_SMR.1 má rôzne znenie pre rôzne úrovne bezpečnosti.

ZNENIE PRE ÚROVNE BEZPEČNOSTI 1-2

**FMT\_SMR.2.1** The IT environment shall maintain the roles: **Administrátor**, **Úradník**.

ZNENIE PRE ÚROVEŇ BEZPEČNOSTI 3

**FMT\_SMR.2.1** The IT environment shall maintain the roles: **Administrátor**, **Úradník**, **Auditor**.

ZNENIE PRE ÚROVEŇ BEZPEČNOSTI 4

**FMT\_SMR.2.1** The IT environment shall maintain the roles: **Administrátor**, **Operátor**, **Úradník**, **Auditor**.

ZNENIE PRE VŠETKY ÚROVNE BEZPEČNOSTI

**FMT\_SMR.2.2** The **IT environment** shall be able to associate users with roles.

**FMT\_SMR.2.3** The **IT environment** shall ensure that **no identity is authorised to assume more than one of the implemented roles.**

Dependencies: FIA\_UID.1 Timing of identification

### **FMT\_MOF.1 Management of security functions behaviour**

Hierarchical to: No other components.

**FMT\_MOF.1.1** The **IT environment** shall restrict the ability to **modify the behavior of** the functions **listed in table 4.2** to **the authorised roles specified in the table.**

Dependencies: FMT\_SMR.1 Security roles

Tabuľka 4.2: Autorizované roly pre FMT\_MOF.1.

<b>Funkcia</b>	<b>Autorizovaná rola</b>
Identifikácia a autentifikácia	Iba administrátori by mali mať právomoc špecifikovať, prípadne zmeniť maximálny povolený počet neúspešných pokusov o autentifikáciu.
Správa kont	Iba administrátori by mali mať právomoc vytvárať nové používateľské kontá v systéme, priraďovať im práva a bezpečnostné roly.

### **FMT\_MSA.1 Management of security attributes**

Hierarchical to: No other components.

**FMT\_MSA.1.1** The **IT environment** shall enforce the **Politika kontroly prístupu pre prostredie listed in 4.5.1.9** to restrict the ability to **modify** the security attributes [*ST assignment: list of security attributes*] to **Administrátors.**

Poznámka: V ST musia byť explicitne uvedené prístupové práva a iné bezpečnostné atribúty, ktoré má administrátor povolené meniť.

Dependencies: (FDP\_ACC.1 Subset access control  
or  
FDP\_IFC.1 Subset information flow control)  
FMT\_SMR.1 Security roles

### **FMT\_MSA.3 Static attribute initialisation**

Hierarchical to: No other components.

**FMT\_MSA.3.1** The **IT environment** shall enforce the **Politika kontroly prístupu pre prostredie listed in 4.5.1.9** to provide *[ST selection: restrictive, permissive, other property]* default values for security attributes that are used to enforce the SFP.

**FMT\_MSA.3.2** The **IT environment** shall allow the **Administrátor** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT\_MSA.1 Management of security attributes  
FMT\_SMR.1 Security roles

### **FMT\_MTD.1 Management of TSF data**

Hierarchical to: No other components.

Upozornenie: FMT\_MTD.1 má rôzne znenie pre rôzne úrovne bezpečnosti.

ZNENIE PRE ÚROVNE BEZPEČNOSTI 1-2

**FMT\_MTD.1.1** The **IT environment** shall restrict the ability to **view and delete** the **audit logs** to the role *[ST assignment: authorised role(s)]*.

Poznámka: Autor ST by mal priradiť možnosť prístupu k auditným záznamom jednej z rolí definovaných v príslušnom ST. Pravdepodobne pôjde o tú istú rolu ako pri FAU\_SAR.1.

ZNENIE PRE ÚROVNE BEZPEČNOSTI 3-4

**FMT\_MTD.1.1** The **IT environment** shall restrict the ability to **view and delete** the **audit logs** to the role **Auditor**.

Dependencies: FMT\_SMR.1 Security roles

### **FMT\_MSA.2 Secure security attributes**

Hierarchical to: No other components.

Upozornenie: FMT\_MSA.1 sa dotýka len úrovní bezpečnosti 2-4.

ZNENIE PRE ÚROVNE BEZPEČNOSTI 2-4

**FMT\_MSA.2.1** The **IT environment** shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV\_SPM.1 Informal TOE security policy model  
(FDP\_ACC.1 Subset access control  
**or**  
FDP\_IFC.1 Subset information flow control)  
FMT\_MSA.1 Management of security attributes  
FMT\_SMR.1 Security roles

### 4.5.1.2 Bezpečnostný audit

*Bezpečnostný audit* zahŕňa operácie, dotýkajúce sa generovania, ukladania a kontroly auditných záznamov. Kontrola auditných záznamov je dôležitá pri odhaľovaní chýb a nepriateľských akcií používateľov.

#### FAU\_GEN.1 Audit data generation

Hierarchical to: No other components.

**FAU\_GEN.1.1** The **IT environment** shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the **minimum** level of audit; and
- c) **The events listed in the table 4.3**

**FAU\_GEN.1.2** The **IT environment** shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *[ST assignment: other audit relevant information]*

Dependencies: FPT\_STM.1 Reliable time stamps

Tabuľka 4.3: Auditovateľné udalosti.

Funkcia	Komponent z CC	Udalosť
Bezpečnostný audit	FAU_GEN.1 Audit data generation	Zmena množiny auditovaných udalostí. Pokus zmazať staré auditné záznamy.
Bezpečnostný audit	FIA_ATD.1 User attribute definition	Úspešné aj neúspešné pokusy zaujať bezpečnostnú rolu.
Bezpečnostný audit	FIA_AFL.1 Authentication failure handling (úrovne bezpečnosti 2-4)	Zmena počtu povolených neúspešných pokusov o autentifikáciu.  Výskyt maximálneho počtu neúspešných pokusov o autentifikáciu. Odblokovanie zablokovaného konta administrátorom.

Tabuľka 4.3: (pokračovanie)

Funkcia	Komponent z CC	Udalosť
Správa kont		Pridanie roly alebo používateľa. Zmena prístupových práv pre rolu alebo používateľa.

**FAU\_GEN.2 User identity association**

Hierarchical to: No other components.

**FAU\_GEN.2.1** The **IT environment** shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU\_GEN.1 Audit data generation  
FIA\_UID.1 Timing of identification

**FAU\_SAR.1 Audit review**

Hierarchical to: No other components.

Upozornenie: FAU\_SAR.1 má rôzne znenie pre rôzne úrovne bezpečnosti.

**ZNENIE PRE ÚROVNE BEZPEČNOSTI 1-2**

**FAU\_SAR.1.1** The **IT environment** shall provide [*ST assignment: authorised users*] with the capability to read **all audit information** from the audit records.

**FAU\_SAR.1.2** The **IT environment** shall provide the audit records in a manner suitable for the user to interpret the information.

Poznámka: Autor ST by mal priradiť možnosť prístupu k auditným záznamom jednej z rolí definovaných v príslušnom ST (napr. administrátorom).

**ZNENIE PRE ÚROVNE BEZPEČNOSTI 3-4**

**FAU\_SAR.1.1** The **IT environment** shall provide **Auditors** with the capability to read **all audit information** from the audit records.

**FAU\_SAR.1.2** The **IT environment** shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU\_GEN.1 Audit data generation

**FAU\_SAR.3 Selectable audit review**

Hierarchical to: No other components.

**FAU\_SAR.3.1** The **IT environment** shall provide the ability to perform searches of audit data based on **the type of the event** and **the user responsible for causing the event.**

Dependencies: FAU\_SAR.1 Audit review

### **FAU\_STG.1 Protected audit trail storage**

Hierarchical to: No other components.

**FAU\_STG.1.1** The **IT environment** shall protect the stored audit records from unauthorised deletion.

**FAU\_STG.1.2** The **IT environment** shall be able to **detect** modifications to the audit records.

Dependencies: FAU\_GEN.1 Audit data generation

### **FAU\_STG.3 Action in case of possible audit data loss**

Hierarchical to: No other components.

**FAU\_STG.3.1** The **IT environment** shall **notify the administrator** if the audit trail exceeds **90% of the allocated space**.

Dependencies: FAU\_STG.1 Protected audit trail storage

### **FAU\_STG.4 Prevention of audit data loss**

Hierarchical to: FAU\_STG.3

Upozornenie: FAU\_STG.4 má rôzne znenie pre rôzne úrovne bezpečnosti.

#### **ZNENIE PRE ÚROVNE BEZPEČNOSTI 1-2**

**FAU\_STG.4.1** The **IT environment** shall **prevent auditable events**, except those taken by the *[ST assignment: authorised user]* if the audit trail is full.

Poznámka: Autor ST by mal zvoliť jednu z rolí definovaných v príslušnom ST (napr. administrátorov). Pravdepodobne pôjde o tú istú rolu ako pri FAU\_SAR.1.

Dependencies: FAU\_STG.1 Protected audit trail storage

### **FPT\_STM.1 Reliable time stamps**

Hierarchical to: No other components.

**FPT\_STM.1.1** The **IT environment** shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

### 4.5.1.3 Kontrola prístupu

*Kontrola prístupu* zahŕňa opatrenia, zabraňujúce neautorizovanému prístupu k informáciám.

#### FDP\_ACC.1 Subset access control

Hierarchical to: No other components.

**FDP\_ACC.1.1** The **IT environment** shall enforce the **Politika kontroly prístupu pre prostredie listed in 4.5.1.9** on *[ST assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]*.

Poznámka: V ST je potrebné explicitne definovať objekty a subjekty, ktorých sa má spomínaná politika dotýkať, ako aj uviesť operácie, na ktoré sa má táto politika vzťahovať.

Dependencies: FDP\_ACF.1 Security attribute based access control

#### FDP\_ACF.1 Security attribute based access control

Hierarchical to: No other components.

**FDP\_ACF.1.1** The **IT environment** shall enforce the **Politika kontroly prístupu pre prostredie listed in 4.5.1.9** to objects based on **the identity of the subject and the set of roles that the subject is authorized to assume**.

**FDP\_ACF.1.2** The **IT environment** shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *[ST assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*.

**FDP\_ACF.1.3** The **IT environment** shall explicitly authorise access of subjects to objects based on the following additional rules: *[ST assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]*.

**FDP\_ACF.1.4** The **IT environment** shall explicitly deny access of subjects to objects based on the *[ST assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]*.

Poznámka: ST musí explicitne uviesť atribúty, podľa ktorých sa rozhoduje o udelení prístupu. (Môže ísť napr. o vlastníctvo objektu, zoznamy povoľujúce/zakazujúce prístup, nastavenie prístupových práv a pod.) Vo FDP\_ACF.1.3 by mal autor ST uviesť pravidlá, vyhodnotením ktorých môže byť explicitne **povolený** prístup. Vo FDP\_ACF.1.4 by mal autor ST uviesť pravidlá, vyhodnotením ktorých môže byť explicitne **zamietnutý** prístup. Úmyslom je, aby tieto doplnené pravidlá pokrývali výnimky zo všeobecných pravidiel vyplývajúcich z FDP\_ACF.1.1.

Dependencies: FDP\_ACC.1 Subset access control  
 FMT\_MSA.3 Static attribute initialisation

#### **FPT\_SEP.1 TSF domain separation**

Hierarchical to: No other components.

**FPT\_SEP.1.1** **Each operating system in the IT environment** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

**FPT\_SEP.1.2** **Each operating system in the IT environment** shall enforce separation between the security domains of subjects in its scope of control.

Dependencies: No dependencies

#### **FPT\_RVM.1 Non-bypassability of the TSP**

Hierarchical to: No other components.

**FPT\_RVM.1.1** **Each operating system in the IT environment** shall ensure that its policy enforcement functions are invoked and succeed before each function within its scope of control is allowed to proceed.

Dependencies: No dependencies

#### **4.5.1.4 Identifikácia a autentifikácia**

*Identifikácia a autentifikácia* zahŕňa rozpoznanie entity (napríklad používateľa, iného IT systému, zariadenia) a overenie jej identity.

#### **FIA\_ATD.1 User attribute definition**

Hierarchical to: No other components.

**FIA\_ATD.1.1** The **IT environment** shall maintain the following list of security attributes belonging to individual users: the set of roles that the user is authorized to assume, *[ST assignment: other security attributes]*.

Poznámka: Je potrebné udržiavať všetky bezpečnostné atribúty, ktoré sú potrebné na vynútenie Politiky kontroly prístupu pre prostredie (uvedenej v 4.5.1.9), generovanie dostatočných auditných záznamov a správnu identifikáciu a autentifikáciu používateľov.

Dependencies: No dependencies

#### **FIA\_UAU.1 Timing of authentication**

Hierarchical to: No other components.

**FIA\_UAU.1.1** The **IT environment** shall allow [*ST assignment: list of **IT environment**-mediated actions*] on behalf of the user to be performed before the user is authenticated.

**FIA\_UAU.1.2** The **IT environment** shall require each user to be successfully authenticated before allowing any other **IT environment**-mediated actions on behalf of that user.

Dependencies: FIA\_UID.1 Timing of identification

#### **FIA\_UID.1 Timing of identification**

Hierarchical to: No other components.

**FIA\_UID.1.1** The **IT environment** shall allow [*ST assignment: list of **IT environment**-mediated actions*] on behalf of the user to be performed before the user is identified.

**FIA\_UID.1.2** The **IT environment** shall require each user to be successfully identified before allowing any other **IT environment**-mediated actions on behalf of that user.

Dependencies: No dependencies

Poznámka: FIA\_UAU.1 a FIA\_UID.1 umožňujú autorovi ST špecifikovať akcie, ktoré môžu byť vykonané na podnet používateľa, ktorý nie je identifikovaný a/lebo autentifikovaný. Nesmie však ísť o akcie dotýkajúce sa bezpečnosti TOE. Autor ST by okrem doplnenia akcií, ktoré nie sú relevantné z hľadiska bezpečnosti mal navyše o každej uviesť zdôvodnenie, prečo je tomu tak. Príkladom takejto akcie môže byť požiadavka o kópiu verejne prístupných archivovaných údajov.

#### **FIA\_USB.1 User-subject binding**

Hierarchical to: No other components.

**FIA\_USB.1.1** The **IT environment** shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Dependencies: No dependencies

#### **FIA\_AFL.1 Authentication failure handling**

Hierarchical to: No other components.

Upozornenie: FIA\_AFL.1 sa dotýka len úrovni bezpečnosti 2-4.

ZNENIE PRE ÚROVNE BEZPEČNOSTI 2-4

**FIA\_AFL.1.1** If authentication is not performed in a cryptographic module that has been FIPS 140-2 validated to a level corresponding to úroveň bezpečnosti, the **IT environment** shall detect when an **Administrator configurable number of** unsuccessful authentication attempts have occurred since the last successful authentication for the indicated user identity.

**FIA\_AFL.1.2** When the defined number of unsuccessful authentication attempts has been met or surpassed, the **IT environment** shall [*ST assignment: list of actions to take*].

Poznámka: Akcie v prípade prekročenia limitu na počet neúspešných pokusov o autentifikáciu môžu zahŕňať napr. zablokovanie konta (na určitý čas, prípadne do odblokovania administrátorom), informovanie administrátora a pod. Aby nemohlo dôjsť k útoku spôsobiacemu zabránenie vykonávania funkcie, konto administrátora sa nesmie dať takýmto spôsobom zablokovať.

Dependencies: FIA\_UAU.1 Timing of authentication

### **FTP\_TRP.1 Trusted path**

Hierarchical to: No other components.

Upozornenie: FTP\_TRP.1 sa dotýka len úrovni bezpečnosti 3-4.

#### ZNENIE PRE ÚROVNE BEZPEČNOSTI 3-4

**FTP\_TRP.1.1** The **IT environment** shall provide a communication path between itself and [*ST selection: remote, local, both remote and local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

**FTP\_TRP.1.2** The **IT environment** shall permit [*ST selection: the IT environment, the TSF, local users, remote users*] to initiate communication via the trusted path.

**FTP\_TRP.1.3** The **IT environment** shall require the use of the trusted path for **initial user authentication**, [*ST assignment: other services for which trusted path is required*].

Poznámka: Trusted path môže byť potrebná pri ľubovoľnej interakcii dotýkajúcej sa bezpečnosti TOE. ST by mal identifikovať všetky situácie, kedy je trusted path vyžadovaná.

Dependencies: No dependencies

#### 4.5.1.5 Interné presuny dát

##### FDP\_ITT.1 Basic internal transfer protection (iteration 1)

Hierarchical to: No other components.

**FDP\_ITT.1.1** The IT environment shall enforce the Politika kontroly prístupu pre prostredie listed in 4.5.1.9 to prevent the modification of user data when it is transmitted between physically-separated parts of the IT environment.

Dependencies: (FDP\_ACC.1 Subset access control  
or  
FDP\_IFC.1 Subset information flow control)

##### FDP\_ITT.1 Basic internal transfer protection (iteration 2)

Hierarchical to: No other components.

**FDP\_ITT.1.1** The IT environment shall enforce the Politika kontroly prístupu pre prostredie listed in 4.5.1.9 to prevent the disclosure of confidential user data when it is transmitted between physically-separated parts of the IT environment.

Dependencies: (FDP\_ACC.1 Subset access control  
or  
FDP\_IFC.1 Subset information flow control)

##### FDP\_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

**FDP\_UCT.1.1** The IT environment shall enforce the Politika kontroly prístupu pre prostredie listed in 4.5.1.9 to be able to transmit and receive objects in a manner protected from unauthorised disclosure.

Dependencies: (FDP\_ACC.1 Subset access control  
or  
FDP\_IFC.1 Subset information flow control)  
(FDP\_ITC.1 Inter-TSF trusted channel  
or  
FTP\_TRP.1 Trusted path)

##### FPT\_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

**FPT\_ITT.1.1** The IT environment shall protect security-relevant IT environment data from modification and confidential IT environment data from disclosure when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

#### 4.5.1.6 Správa kryptografických kľúčov

##### FCS\_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

**FCS\_CKM.4.1** The **IT environment** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*ST assignment: cryptographic key destruction method*] that meets the following: [*ST assignment: list of standards*].

Poznámka: Autor ST by mal špecifikovať metódu používanú na bezpečné zničenie kryptografických kľúčov, ktorým vypršala platnosť, ako aj štandardy, ktoré táto metóda spĺňa.

Dependencies: (FDP\_ITC.1 Import of user data without security attributes  
or  
FCS\_CKM.1 Cryptographic key generation)  
FMT\_MSA.2 Secure security attributes

#### 4.5.1.7 Testovanie systému

##### FPT\_AMT.1 Abstract machine testing

Hierarchical to: No other components.

**FPT\_AMT.1.1** The **IT environment** shall run a suite of tests [*ST selection: during initial start-up, periodically during normal operation, at the request of an authorised user, under other conditions*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the **IT environment**.

Poznámka: Autor ST musí špecifikovať, kedy a ako často majú byť vykonávané testy „abstraktného stroja“ (či už ide čisto o hardvérovú platformu systému alebo o kombináciu hardvéru a softvéru, ktorá vytvára prostredie, v ktorom beží samotný systém). Častejšie vykonávanie týchto testov síce dáva väčšiu dôveru vo funkčnosť systému, na druhej strane však môže negatívne ovplyvniť jeho dostupnosť používateľom.

Dependencies: No dependencies

#### 4.5.1.8 Kryptografické moduly

Kryptografické funkcie môže TOE prenechať kryptografickým modulom. Je samozrejme možné použiť jeden kryptografický modul, overený voči FIPS 140-2 na príslušnú úroveň, ktorý bude vykonávať všetky požadované funkcie.

Na druhej strane niekedy môže byť vhodnejšie použiť viacero rôznych kryptografických modulov na vykonávanie rôznych funkcií. V takomto prípade môžu byť moduly vykonávajúce menej dôležité funkcie aj primerane menej zabezpečené (a teda lacnejšie).

#### **FCS\_COP.1 Cryptographic operation**

Hierarchical to: No other components.

**FCS\_COP.1.1** The **FIPS 140-2 validated cryptographic module** shall perform *[ST assignment: list of cryptographic operations]* in accordance with a specified cryptographic algorithm *[ST assignment: cryptographic algorithm]* and cryptographic key sizes *[ST assignment: cryptographic key sizes]* that meet the following: *[ST assignment: list of standards]*.

Poznámka: Autor ST by mal špecifikovať všetky kryptografické operácie, ktoré budú realizované kryptografickými modulmi (napr. šifrovanie, počítanie hašovacích hodnôt, overovanie elektronického podpisu). Pre každú z nich by mal uviesť použitý algoritmus a štandardy, ktoré tento algoritmus spĺňa.

Dependencies: (FDP\_ITC.1 Import of user data without security attributes  
**or**  
 FCS\_CKM.1 Cryptographic key generation)  
 FCS\_CKM.4 Cryptographic key destruction  
 FMT\_MSA.2 Secure security attributes

#### **4.5.1.9 Politika kontroly prístupu pre prostredie**

IT prostredie by malo dodržiavať politiku kontroly prístupu, ktorá by vynucovala nasledujúce skutočnosti:

Subjektom (používateľom) bude povolený prístup k objektom (dátam) na základe nasledujúcich údajov:

- a) Identita subjektu.
- b) Rola alebo roly, ktoré môže zastávať.
- c) Typ požadovaného prístupu.
- d) V prípade potreby vlastníctvo príslušného súkromného kľúča.

Každý objekt má explicitne určený subjekt (resp. rolu), ktorý je jeho vlastníkom. Spravovanie prístupových práv pre objekt je súčasťou zodpovednosti jeho vlastníka. Prístupové práva zahŕňajú právo na čítanie, zápis, prípadne na spustenie.

Musí byť možné priradiť konkrétne prístupové práva jednotlivcovi aj role a takisto priradiť každému jednotlivcovi jednu alebo viac rolí s rôznymi prístupovými právami.

### **4.5.2 Funkčné požiadavky na TOE**

V tejto časti špecifikujeme funkčné požiadavky, ktoré sa vzťahujú priamo na funkcionality TOE. Ak je funkčná požiadavka v texte uvedená bez špecifikovania úrovne bezpečnosti,

znamená to, že sa vzťahuje na všetky úrovne. V opačnom prípade je jasne vyznačené, na ktorej úrovni bezpečnosti sa jej text vzťahuje.

Tabuľka 4.4 obsahuje funkčné požiadavky uvedené v tejto časti. Kvôli ľahšej orientácii sú utriedené v abecednom poradí. Pri každej požiadavke je uvedené, kde je zaradená a ktorých úrovni bezpečnosti sa dotýka.

Tabuľka 4.4: Funkčné požiadavky na prostredie.

Funkčná požiadavka	Časť textu	úrovne bezp.
FAU_GEN.1 Audit data generation	4.5.2.2 Bezpečnostný audit	1-4
FAU_GEN.2 User identity association	4.5.2.2 Bezpečnostný audit	1-4
FAU_SAR.1 Audit review	4.5.2.2 Bezpečnostný audit	1-2,3-4
FAU_SAR.3 Selectable audit review	4.5.2.2 Bezpečnostný audit	1-4
FAU_STG.1 Protected audit trail storage	4.5.2.2 Bezpečnostný audit	1-4
FAU_STG.3 Action in case of possible audit data loss	4.5.2.2 Bezpečnostný audit	1-4
FAU_STG.4 Prevention of audit data loss	4.5.2.2 Bezpečnostný audit	1-2,3-4
FDP_ACC.1 Subset access control	4.5.2.3 Kontrola prístupu	1-4
FDP_ACF.1 Security attribute based access control	4.5.2.3 Kontrola prístupu	1-4
FDP_ARC_BKP.1 Zálohovanie systému	4.5.2.7 Zálohovanie, kontrola a obnova	1-4
FDP_ARC_BKP.2 Dôveryhodné zálohovanie systému	4.5.2.7 Zálohovanie, kontrola a obnova	2-4
FDP_ETC.2 Export of user data with security attributes	4.5.2.5 Import a export údajov	1-4
FDP_ITC.2 Import of user data with security attributes	4.5.2.5 Import a export údajov	1-4
FDP_ITT.1 Basic internal transfer protection (iteration 1)	4.5.2.5 Import a export údajov	1-4
FDP_ITT.1 Basic internal transfer protection (iteration 2)	4.5.2.5 Import a export údajov	1-4
FDP_RIP.1 Subset residual information protection	4.5.2.7 Zálohovanie, kontrola a obnova	1-4
FDP_SDI.1 Stored data integrity monitoring	4.5.2.7 Zálohovanie, kontrola a obnova	1-4
FDP_UCT.1 Basic data exchange confidentiality	4.5.2.5 Import a export údajov	1-4
FIA_UAU.1 Timing of authentication	4.5.2.4 Ident. a autentifikácia	1-4
FIA_UID.1 Timing of identification	4.5.2.4 Ident. a autentifikácia	1-4
FIA_USB.1 User-subject binding	4.5.2.4 Ident. a autentifikácia	1-4
FMT_MOF.1 Management of security functions behaviour	4.5.2.1 Bezpečnostné roly	1-4

Tabuľka 4.4: (pokračovanie)

Funkčná požiadavka	Časť textu	úrovne bezp.
FPT_ARC_ASE.1 Podpisovanie auditných záznamov	4.5.2.2 Bezpečnostný audit	2-4
FPT_ARC_ATE.1 Pečiatkovanie auditných záznamov	4.5.2.2 Bezpečnostný audit	4
FPT_ITT.1 Basic internal TSF data transfer protection	4.5.2.5 Import a export údajov	1-4
FPT_RVM.1 Non-bypassability of the TSP	4.5.2.3 Kontrola prístupu	1-4
FPT_STM.1 Reliable time stamps	4.5.2.2 Bezpečnostný audit	1-4
FPT_TST.1 TSF testing	4.5.2.7 Zálohovanie, kontrola a obnova	1-4
FRU_RSA.1 Maximum quotas	4.5.2.6 Využívanie zdrojov	1-4

#### 4.5.2.1 Bezpečnostné roly

##### FMT\_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

**FMT\_MOF.1.1** The **IT environment** shall restrict the ability to **modify the behavior of** the functions **listed in table 4.5** to **the authorised roles specified in the table**.

Dependencies: FMT\_SMR.1 Security roles

Tabuľka 4.5: Autorizované roly pre FMT\_MOF.1.

Funkcia	Autorizovaná rola
Bezpečnostný audit	Iba administrátori by mali mať právomoc konfigurovať parametre uchovávania auditných záznamov. (Úrovne bezpečnosti 2-4.) Iba administrátori by mali mať právomoc konfigurovať frekvenciu podpisovania auditných záznamov. (Úroveň bezpečnosti 4.) Iba administrátori by mali mať právomoc konfigurovať frekvenciu pečiatkovania auditných záznamov.
Zálohovanie	Iba administrátori by mali mať právomoc konfigurovať parametre zálohovania.

Tabuľka 4.5: (pokračovanie)

Funkcia	Autorizovaná rola
	(Úrovne bezpečnosti 1-3.) Iba [ST assignment: autorizovaná rola] by mali mať právomoc spustiť proces zálohovania. (Úroveň bezpečnosti 4.) Iba operátori by mali mať právomoc spustiť proces zálohovania.
Konfigurácia	Iba administrátori by mali mať právomoc konfigurovať parametre TSF.
Archivované dokumenty	Iba úradníci by mali mať právomoc spracovať požiadavku na uloženie dokumentu do archívu. Iba úradníci by mali mať právomoc spracovať požiadavku na vystavenie overenej kópie archivovaného dokumentu autorizovanému klientovi. Iba úradníci by mali mať právomoc odstrániť z archívu dokumenty, ktoré už nemajú byť ďalej archivované.

#### 4.5.2.2 Bezpečnostný audit

##### FAU\_GEN.1 Audit data generation

Hierarchical to: No other components.

**FAU\_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the **minimum** level of audit; and
- c) **The events listed in the table 4.6.**

**FAU\_GEN.1.2** The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **the information specified in the table 4.6 in the column Dodatočné údaje, [ST assignment: other audit relevant information]**

Dependencies: FPT\_STM.1 Reliable time stamps

Tabuľka 4.6: Auditovateľné udalosti.

Funkcia	Komponent	Udalosť	Dodatočné údaje
Bezpečnostný audit	FAU_GEN.1 Audit data generation	Zmena množiny auditovateľných udalostí.  Pokus zmazať staré auditné záznamy.	
Bezpečnostný audit	FPT_ARC_ASE.1 Podpisovanie auditných záznamov (úroveň bezpečnosti 2-4)	Podpis auditného záznamu.	Vypočítaný podpis.
Bezpečnostný audit	FPT_ARC_ATE.1 Pečiatkovanie auditných záznamov (úroveň bezpečnosti 4)	Pečiatkovanie auditného záznamu.	Získaná dôveryhodná časová pečiatka
Konfigurácia		Ľubovoľná zmena konfigurácie TSF.	
Kryptografické kľúče		Vloženie nového súkromného a verejného kľúča archívu Zničenie súkromného a verejného kľúča archívu	Verejný kľúč.  Verejný kľúč.
Archivované dokumenty		Vloženie dokumentu do archívu  Vystavenie potvrdenej kópie Odstránenie dokumentu z archívu	Identifikačné údaje o dokumente a jeho vlastníčkovi. Bezpečnostné požiadavky. Identifikačné údaje o dokumente. Identifikačné údaje o dokumente.

### FAU\_GEN.2 User identity association

Hierarchical to: No other components.

**FAU\_GEN.2.1** The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU\_GEN.1 Audit data generation  
FIA\_UID.1 Timing of identification

**FAU\_SAR.1 Audit review**

Hierarchical to: No other components.

Upozornenie: FAU\_SAR.1 má rôzne znenie pre rôzne úrovne bezpečnosti.

**ZNENIE PRE ÚROVNE BEZPEČNOSTI 1-2**

**FAU\_SAR.1.1** The TSF shall provide [*ST assignment: authorised users*] with the capability to read **all audit information** from the audit records.

**FAU\_SAR.1.2** The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Poznámka: Autor ST by mal priradiť možnosť prístupu k auditným záznamom jednej z rolí definovaných v príslušnom ST (napr. administrátorom).

**ZNENIE PRE ÚROVNE BEZPEČNOSTI 3-4**

**FAU\_SAR.1.1** The TSF shall provide **Auditors** with the capability to read **all audit information** from the audit records.

**FAU\_SAR.1.2** The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU\_GEN.1 Audit data generation

**FAU\_SAR.3 Selectable audit review**

Hierarchical to: No other components.

**FAU\_SAR.3.1** The TSF shall provide the ability to perform searches of audit data based on **the type of the event** and **the user responsible for causing the event.**

Dependencies: FAU\_SAR.1 Audit review

**FAU\_STG.1 Protected audit trail storage**

Hierarchical to: No other components.

**FAU\_STG.1.1** The TSF shall protect the stored audit records from unauthorised deletion.

**FAU\_STG.1.2** The TSF shall be able to **detect** modifications to the audit records.

Dependencies: FAU\_GEN.1 Audit data generation

**FAU\_STG.3 Action in case of possible audit data loss**

Hierarchical to: No other components.

**FAU\_STG.3.1** The TSF shall **notify the administrator** if the audit trail exceeds **90% of the allocated space.**

Dependencies: FAU\_STG.1 Protected audit trail storage

#### **FAU\_STG.4 Prevention of audit data loss**

Hierarchical to: FAU\_STG.3

Upozornenie: FAU\_STG.4 má rôzne znenie pre rôzne úrovne bezpečnosti.

##### ZNENIE PRE ÚROVNE BEZPEČNOSTI 1-2

**FAU\_STG.4.1** The TSF shall **prevent auditable events**, except those taken by the *[ST assignment: authorised user]* if the audit trail is full.

Poznámka: Autor ST by mal zvoliť jednu z rolí definovaných v príslušnom ST (napr. administrátorov). Pravdepodobne pôjde o tú istú rolu ako pri FAU\_SAR.1.

Dependencies: FAU\_STG.1 Protected audit trail storage

#### **FPT\_STM.1 Reliable time stamps**

Hierarchical to: No other components.

**FPT\_STM.1.1** The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

#### **FPT\_ARC\_ASE.1 Podpisovanie auditných záznamov**

Hierarchical to: No other components.

Upozornenie: FPT\_ARC\_ASE.1 sa dotýka len úrovni bezpečnosti 2-4.

##### ZNENIE PRE ÚROVNE BEZPEČNOSTI 2-4

**FPT\_ARC\_ASE.1.1** TSF by mali pravidelne spočítať elektronický podpis, prípadne hašovaciu hodnotu pomocou kľúča, pre položky v auditnom zázname. Spočítaný podpis, resp. hašovacia hodnota, je následne zapísaný do auditného záznamu. Túto udalosť budeme nazývať podpis auditného záznamu.

**FPT\_ARC\_ASE.1.2** Do podpisovaných, resp. hašovaných dát musia byť zahrnuté minimálne nasledujúce dáta: všetky položky, pridané do auditného záznamu od posledného podpisu auditného záznamu a podpis, resp. hašovacia hodnota spočítaná pri predchádzajúcom podpise auditného záznamu.

**FPT\_ARC\_ASE.1.3** Administrátor by mal mať možnosť nastaviť frekvenciu, s akou sú auditné záznamy podpisované.

Dependencies: FAU\_GEN.1 Audit data generation  
FMT\_MOF.1 Management of security functions behavior

Zdôvodnenie: Ide o implementačne nenáročnú požiadavku, ktorá však nie je zahrnutá v CC. Pomôže plniť bezpečnostný cieľ **O.Ochrana uložených auditných záznamov**.

#### **FPT\_ARC\_ATE.1 Pečiatkovanie auditných záznamov**

Hierarchical to: No other components.

Upozornenie: FPT\_ARC\_ATE.1 sa dotýka len úrovne bezpečnosti 4.

#### ZNENIE PRE ÚROVEŇ BEZPEČNOSTI 4

**FPT\_ARC\_ATE.1.1** TSF by mali pravidelne získať elektronicky podpísanú časovú pečiatku od dôveryhodnej tretej strany. Táto časová pečiatka je následne zapísaná do auditného záznamu. Túto udalosť budeme nazývať pečiatkovanie auditného záznamu.

**FPT\_ARC\_ATE.1.2** Do podpisovaných a pečiatkovaných dát musia byť zahrnuté minimálne nasledujúce dáta: všetky položky, pridané do auditného záznamu od posledného pečiatkovania auditného záznamu a podpísaná časová pečiatka spočítaná pri predchádzajúcom pečiatkovaní auditného záznamu.

**FPT\_ARC\_ATE.1.3** Administrátor by mal mať možnosť nastaviť frekvenciu, s akou sú auditné záznamy pečiatkované.

Dependencies: FAU\_GEN.1 Audit data generation  
FMT\_MOF.1 Management of security functions behavior  
FTP\_TRP.1 Trusted path

Zdôvodnenie: Táto požiadavka zvyšuje úroveň zabezpečenia auditných záznamov prostredníctvom dôveryhodnej tretej strany. V Common Criteria ekvivalentná požiadavka nie je zahrnutá, preto uvádzame vlastné znenie. Táto požiadavka pomôže plniť bezpečnostný cieľ **O.Ochrana uložených auditných záznamov**, ktorý môže byť na tejto úrovni bezpečnosti ohrozený akciami autorizovaných používateľov.

### 4.5.2.3 Kontrola prístupu

*Kontrola prístupu* zahŕňa opatrenia, zabráňujúce neautorizovanému prístupu k informáciám.

#### **FDP\_ACC.1 Subset access control**

Hierarchical to: No other components.

**FDP\_ACC.1.1** The TSF shall enforce the **Politika kontroly prístupu pre TOE listed in 4.5.2.8** on *[ST assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]*.

Poznámka: V ST je potrebné explicitne definovať objekty a subjekty, ktorých sa má spomínaná politika dotýkať, ako aj uviesť operácie, na ktoré sa má táto politika vzťahovať.

Dependencies: FDP\_ACF.1 Security attribute based access control

### **FDP\_ACF.1 Security attribute based access control**

Hierarchical to: No other components.

**FDP\_ACF.1.1** The TSF shall enforce the **Politika kontroly prístupu pre TOE listed in 4.5.2.8** to objects **based on the identity of the subject and the set of roles that the subject is authorized to assume.**

**FDP\_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *[ST assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*.

**FDP\_ACF.1.3** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *[ST assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]*.

**FDP\_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the *[ST assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]*.

Poznámka: ST musí explicitne uviesť atribúty, podľa ktorých sa rozhoduje o udelení prístupu. (Môže ísť napr. o vlastníctvo objektu, zoznamy povoľujúce/zakazujúce prístup, nastavenie prístupových práv a pod.) Vo FDP\_ACF.1.3 by mal autor ST uviesť pravidlá, vyhodnotením ktorých môže byť explicitne **povolený** prístup. Vo FDP\_ACF.1.4 by mal autor ST uviesť pravidlá, vyhodnotením ktorých môže byť explicitne **zamietnutý** prístup. Úmyslom je, aby tieto doplnené pravidlá pokrývali výnimky zo všeobecných pravidiel vyplývajúcich z FDP\_ACF.1.1.

Dependencies: FDP\_ACC.1 Subset access control  
FMT\_MSA.3 Static attribute initialisation

### **FPT\_RVM.1 Non-bypassability of the TSP**

Hierarchical to: No other components.

**FPT\_RVM.1.1** The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

#### **4.5.2.4 Identifikácia a autentifikácia**

*Identifikácia a autentifikácia* zahŕňa rozpoznanie entity (napríklad používateľa, iného IT systému, zariadenia) a overenie jej identity.

**FIA\_UAU.1 Timing of authentication**

Hierarchical to: No other components.

**FIA\_UAU.1.1** The TSF shall allow [*ST assignment: list of TSF-mediated actions*] on behalf of the user to be performed before the user is authenticated.

**FIA\_UAU.1.2** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA\_UID.1 Timing of identification

**FIA\_UID.1 Timing of identification**

Hierarchical to: No other components.

**FIA\_UID.1.1** The TSF shall allow [*ST assignment: list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

**FIA\_UID.1.2** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

Poznámka: FIA\_UAU.1 a FIA\_UID.1 umožňujú autorovi ST špecifikovať akcie, ktoré môžu byť vykonané na podnet používateľa, ktorý nie je identifikovaný a/lebo autentifikovaný. Nesmie však ísť o akcie dotýkajúce sa bezpečnosti TOE. Autor ST by okrem doplnenia akcií, ktoré nie sú relevantné z hľadiska bezpečnosti mal navyše o každej uviesť zdôvodnenie, prečo je tomu tak. Príkladom takejto akcie môže byť požiadavka o kópiu verejne prístupných archivovaných údajov.

**FIA\_USB.1 User-subject binding**

Hierarchical to: No other components.

**FIA\_USB.1.1** The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Dependencies: No dependencies

Dependencies: No dependencies

### 4.5.2.5 Import a export údajov

*Import údajov* sa dotýka situácií, kedy zvonka prichádzajú do TOE údaje, pričom vieme overiť identitu ich zdroja (napr. pri šifrovanej komunikácii, podpísané autorom a pod.).

*Export údajov* je presun údajov do iného zariadenia, nachádzajúceho sa mimo TOE.

Za import a export údajov explicitne považujeme aj presun údajov medzi fyzicky oddelenými časťami TOE cez nedôveryhodné prostredie.

#### FDP\_ETC.2 Export of user data with security attributes

Hierarchical to: No other components.

**FDP\_ETC.2.1** The TSF shall enforce the **Politika kontroly prístupu pre TOE listed in 4.5.2.8** when exporting user data, controlled under the SFP(s), outside of the TSC.

**FDP\_ETC.2.2** The TSF shall export the user data with the user data's associated security attributes.

**FDP\_ETC.2.3** The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

**FDP\_ETC.2.4** The TSF shall enforce the following rules when user data is exported from the TSC: *[ST assignment: additional exportation control rules]*.

Dependencies: (FDP\_ACC.1 Subset access control  
or  
FDP\_IFC.1 Subset information flow control)

#### FDP\_ITC.2 Import of user data with security attributes

Hierarchical to: No other components.

**FDP\_ITC.2.1** The TSF shall enforce the **Politika kontroly prístupu pre TOE listed in 4.5.2.8** when importing user data, controlled under the SFP, from outside of the TSC.

**FDP\_ITC.2.2** The TSF shall use the security attributes associated with the imported user data.

**FDP\_ITC.2.3** The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

**FDP\_ITC.2.4** The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

**FDP\_ITC.2.5** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: *[ST assignment: additional importation control rules]*.

Dependencies: (FDP\_ACC.1 Subset access control  
**or**  
 FDP\_IFC.1 Subset information flow control)  
 (FDP\_ITC.1 Inter-TSF trusted channel  
**or**  
 FTP\_TRP.1 Trusted path)  
 FPT\_TDC.1 Inter-TSF basic TSF data consistency

### **FDP\_ITT.1 Basic internal transfer protection (iteration 1)**

Hierarchical to: No other components.

**FDP\_ITT.1.1** The TSF shall enforce the **Politika kontroly prístupu pre TOE listed in 4.5.2.8** to prevent the **modification** of user data when it is transmitted between physically-separated parts of the TOE.

Dependencies: (FDP\_ACC.1 Subset access control  
**or**  
 FDP\_IFC.1 Subset information flow control)

### **FDP\_ITT.1 Basic internal transfer protection (iteration 2)**

Hierarchical to: No other components.

**FDP\_ITT.1.1** The TSF shall enforce the **Politika kontroly prístupu pre TOE listed in 4.5.2.8** to prevent the **disclosure of confidential** user data when it is transmitted between physically-separated parts of the TOE.

### **FDP\_UCT.1 Basic data exchange confidentiality**

Hierarchical to: No other components.

**FDP\_UCT.1.1** The TSF shall enforce the **Politika kontroly prístupu pre TOE listed in 4.5.2.8** to be able to **transmit and receive** objects in a manner protected from unauthorised disclosure.

Dependencies: (FDP\_ACC.1 Subset access control  
**or**  
 FDP\_IFC.1 Subset information flow control)  
 (FDP\_ITC.1 Inter-TSF trusted channel  
**or**  
 FTP\_TRP.1 Trusted path)

### **FPT\_ITT.1 Basic internal TSF data transfer protection**

Hierarchical to: No other components.

**FPT\_ITT.1.1** The TSF shall protect TSF data from **disclosure and modification** when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

#### 4.5.2.6 Využívanie zdrojov

##### FRU\_RSA.1 Maximum quotas

Hierarchical to: No other components.

**FRU\_RSA.1.1** The TSF shall enforce maximum quotas of the following resources: *[ST assignment: controlled resources]* that *[ST selection: individual user, defined group of users, subjects]* can use *[ST selection: simultaneously, over a specified period of time]*.

Poznámka: Môže byť potrebné limitovať objem dát, ktoré môžu jednotliví klienti archivovať. Ak je táto požiadavka pre konkrétny ST relevantná, jeho autor doplní popis zdrojov, na ktoré sa majú kvóty vzťahovať.

Dependencies: No dependencies

#### 4.5.2.7 Zálohovanie, kontrola a obnova

*Zálohovanie a obnova* systému je proces ukladania pomocných dát, z ktorých je v prípade kritickej chyby možné systém obnoviť do pôvodného stavu. Archivované údaje je takisto potrebné zálohovať a kontrolovať ich integritu. Po skončení archivácie je potrebné tieto údaje zaručene zmazať.

##### FDP\_SDI.1 Stored data integrity monitoring

Hierarchical to: No other components.

**FDP\_SDI.1.1** The TSF shall monitor user data stored within the TSC for **all integrity errors** on all objects, based on the following attributes: *[ST assignment: user data attributes]*.

Dependencies: No dependencies

##### FDP\_RIP.1 Subset residual information protection

Hierarchical to: No other components.

**FDP\_RIP.1.1** The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: *[ST assignment: list of objects]*.

Poznámka: Po odstránení dokumentu z online archívu je potrebné zaručiť, že obsah dokumentu bude dostatočným spôsobom zmazaný. Je na autorovi ST, aby doplnil detaily realizácie.

Dependencies: No dependencies

### **FDP\_ARC\_BKP.1 Zálohovanie systému**

Hierarchical to: No other components.

- FDP\_ARC\_BKP.1.1** Systém by mal poskytovať [ST selection: pravidelnú, v prípade požiadavky] možnosť zálohovania systémových aj používateľských údajov.
- FDP\_ARC\_BKP.1.2** Zálohované údaje by mali byť dostatočné na to, aby sa dalo len pomocou nich systém zrekonštruovať na identickom hardvéri.
- FDP\_ARC\_BKP.1.3** Systém by mal poskytovať možnosť obnovy, pri ktorej sa obnoví stav systému v okamihu zvolenej zálohy. Bez ohľadu na stav

Dependencies: FMT\_MOF.1 Management of security functions behavior

Zdôvodnenie: Zálohovanie je nutné pre zabezpečenie funkčnosti systému v prípade zlyhania jeho hardvéru a softvéru.

### **FDP\_ARC\_BKP.2 Dôveryhodné zálohovanie systému**

Hierarchical to: FDP\_ARC\_BKP.1 Zálohovanie systému

Upozornenie: FDP\_ARC\_BKP.2 sa dotýka len úrovni bezpečnosti 2-4.

#### **ZNENIE PRE ÚROVNE BEZPEČNOSTI 2-4**

- FDP\_ARC\_BKP.2.1** Zálohované údaje by mali byť chránené proti modifikáciám pomocou elektronického podpisu alebo hašovacej hodnoty s kľúčom. Všetky zálohované údaje súvisiace s bezpečnosťou systému musia byť ukladané zašifrované. Všetky používateľské údaje, u ktorých je potrebné chrániť dôvernosc, musia byť ukladané zašifrované.
- FDP\_ARC\_BKP.2.2** Zálohované údaje by mali byť dostatočné na to, aby sa dalo len pomocou nich a použitých kryptografických kľúčov systém zrekonštruovať na identickom hardvéri.

Dependencies: FDP\_ARC\_BKP.1 Zálohovanie systému

Zdôvodnenie: Zálohovanie je nutné pre zabezpečenie funkčnosti systému v prípade zlyhania jeho hardvéru a softvéru. Na vyšších úrovniach bezpečnosti je potrebné aj zálohy účinne chrániť pred úmyselným poškodením a neautorizovaným prístupom.

### **FPT\_TST.1 TSF testing**

Hierarchical to: No other components.

- FPT\_TST.1.1** The TSF shall run a suite of self tests [*ST selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [ST assignment: conditions under which self test should occur]*] to demonstrate the correct operation of the TSF.
- FPT\_TST.1.2** The TSF shall provide authorised users with the capability to verify the integrity of TSF data.
- FPT\_TST.1.3** The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Dependencies:     FPT\_AMT.1 Abstract machine testing

#### 4.5.2.8 Politika kontroly prístupu pre TOE

TOE by mal dodržiavať politiku kontroly prístupu, ktorá by vynucovala nasledujúce skutočnosti:

Subjektom (používateľom) bude povolený prístup k objektom (dátam) na základe nasledujúcich údajov:

- a) Identita subjektu.
- b) Rola alebo roly, ktoré môže zastávať.
- c) Typ požadovaného prístupu.
- d) V prípade potreby vlastníctvo príslušného súkromného kľúča.

Každý objekt má explicitne určený subjekt (resp. rolu), ktorý je jeho vlastníkom. Spravovanie prístupových práv pre objekt je súčasťou zodpovednosti jeho vlastníka. Prístupové práva zahŕňajú právo na čítanie, zápis, prípadne na spustenie.

Musí byť možné priradiť konkrétne prístupové práva jednotlivcovi aj role a takisto priradiť každému jednotlivcovi jednu alebo viac rolí s rôznymi prístupovými právami.

#### 4.5.3 Požiadavky na záruky

V tejto časti uvedieme požiadavky na záruky, ktoré musí TOE na zvolenej úrovni bezpečnosti poskytovať. Vzhľadom na to, že znenie týchto požiadaviek nemeníme a neupravujeme, nebudeme ho tu uvádzať. Čitateľ ho nájde v tretej časti Common Criteria [CCc99].

### 4.5.3.1 Úroveň bezpečnosti 1

Požiadavky na záruky na tejto úrovni bezpečnosti sú požiadavky kladené EAL 1, doplnené o **ATE\_FUN.1 Functional testing**. Táto požiadavka zvyšuje dôveru v správne plnenie funkcií archívu. Požiadavky sú zhrnuté v tabuľke 4.7.

Tabuľka 4.7: Požiadavky na záruky – úroveň bezpečnosti 1.

Trieda záruk	Požiadavka	EAL
Configuration Management	ACM_CAP.1 Version numbers	EAL 1
Delivery and Operation	ADO_IGS.1 Installation, generation, and start-up procedures	EAL 1-7
Development	ADV_FSP.1 Informal functional specification	EAL 1-3
	ADV_RCR.1 Informal correspondence demonstration	EAL 1-4
Guidance Documents	AGD_ADM.1 Administrator guidance	EAL 1-7
	AGD_USR.1 User guidance	EAL 1-7
Tests	ATE_FUN.1 Functional testing	EAL 2-5
	ATE_IND.1 Independent testing – conformance	EAL 1

### 4.5.3.2 Úroveň bezpečnosti 2

Požiadavky na záruky na tejto úrovni bezpečnosti sú požiadavky, ktoré kladie CSPP – Guidance for COTS Security Protection Profiles [NIST99]. Ide o požiadavky, kladené na EAL 2, doplnené o viaceré požiadavky z vyšších úrovní EAL a o požiadavku ALC\_FLR.2, ktorá nie je zahrnutá v žiadnom EAL. Súbor týchto požiadaviek sa zvykne označovať EAL-CSPP, jeho úlohou je poskytnúť dostatočnú úroveň záruk prostredníctvom dodatočných požiadaviek na dodávateľa systému. Do EAL 3 chýba požiadavka ADV\_HLD.2.

Tabuľka 4.8: Požiadavky na záruky – úroveň bezpečnosti 2.

Trieda záruk	Požiadavka	EAL
Configuration Management	ACM_CAP.3 Authorization controls	EAL 3
	ACM_SCP.2 Problem tracking CM coverage	EAL 4
Delivery and Operation	ADO_DEL.1 Delivery procedures	EAL 2-3
	ADO_IGS.1 Installation, generation, and start-up procedures	EAL 1-7
Development	ADV_FSP.1 Informal functional specification	EAL 1-3
	ADV_HLD.1 Descriptive high-level design	EAL 2

Tabuľka 4.8: (pokračovanie)

<b>Trieda záruk</b>	<b>Požiadavka</b>	<b>EAL</b>
	ADV_RCR.1 Informal correspondence demonstration	EAL 1-4
	ADV_SPM.1 Informal TOE security policy model	EAL 4
Guidance Documents	AGD_ADM.1 Administrator guidance	EAL 1-7
	AGD_USR.1 User guidance	EAL 1-7
Life Cycle Support	ALC_DVS.1 Identification of security measures	EAL 3-5
	ALC_FLR.2 Flaw reporting procedures	None
Tests	ATE_COV.2 Analysis of coverage	EAL 3-5
	ATE_DPT.1 Testing: high-level design	EAL 3-4
	ATE_FUN.1 Functional testing	EAL 2-5
	ATE_IND.2 Independent testing – sample	EAL 2-6
Vulnerability Assessment	AVA_MSU.2 Validation of analysis	EAL 4-5
	AVA_SOF.1 Strength of TOE security function evaluation	EAL 2-7
	AVA_VLA.1 Developer vulnerability analysis	EAL 2-3

### 4.5.3.3 Úroveň bezpečnosti 3

Požiadavky na záruky na tejto úrovni bezpečnosti sú vybrané z EAL 3, EAL 4 a navyše je pridaná požiadavka ALC\_FLR.2.

Tabuľka 4.9: Požiadavky na záruky – úroveň bezpečnosti 3.

<b>Trieda záruk</b>	<b>Požiadavka</b>	<b>EAL</b>
Configuration Management	ACM_CAP.3 Authorization controls	EAL 3
	ACM_SCP.2 Problem tracking CM coverage	EAL 4
Delivery and Operation	ADO_DEL.1 Delivery procedures	EAL 2-3
	ADO_IGS.1 Installation, generation, and start-up procedures	EAL 1-7
Development	ADV_FSP.2 Fully defined external interfaces	EAL 4
	ADV_HLD.2 Security enforcing high-level design	EAL 3-4
	ADV_IMP.1 Subset of the implementation of the TSF	EAL 4
	ADV_LLD.1 Descriptive low-level design	EAL 4-5
	ADV_RCR.1 Informal correspondence demonstration	EAL 1-4
	ADV_SPM.1 Informal TOE security policy model	EAL 4
Guidance Documents	AGD_ADM.1 Administrator guidance	EAL 1-7
	AGD_USR.1 User guidance	EAL 1-7
Life Cycle Support	ALC_DVS.1 Identification of security measures	EAL 3-5
	ALC_FLR.2 Flaw reporting procedures	None

Tabuľka 4.9: (pokračovanie)

Trieda záruk	Požiadavka	EAL
	ALC_TAT.1 Well-defined development tools	EAL 4
Tests	ATE_COV.2 Analysis of coverage	EAL 3-5
	ATE_DPT.1 Testing: high-level design	EAL 3-4
	ATE_FUN.1 Functional testing	EAL 2-5
	ATE_IND.2 Independent testing – sample	EAL 2-6
Vulnerability Assessment	AVA_MSU.2 Validation of analysis	EAL 4-5
	AVA_SOF.1 Strength of TOE security function evaluation	EAL 2-7
	AVA_VLA.2 Independent vulnerability analysis	EAL 4

#### 4.5.3.4 Úroveň bezpečnosti 4

Požiadavky na záruky na tejto úrovni bezpečnosti sú požiadavky kladené v EAL 4, doplnené z EAL 5 požiadavkami **ATE\_DPT.2 Testing: low-level design** a **AVA\_VLA.3 Moderately resistant** a navyše požiadavkou **ALC\_FLR.3 Systematic flaw remediation**, ktorá nie je v žiadnom EAL.

Tabuľka 4.10: Požiadavky na záruky – úroveň bezpečnosti 4.

Trieda záruk	Požiadavka	EAL
Configuration Management	ACM_AUT.1 Partial CM automation	EAL 4-5
	ACM_CAP.4 Generation support and acceptance procedures	EAL 4-5
	ACM_SCP.2 Problem tracking CM coverage	EAL 4
Delivery and Operation	ADO_DEL.2 Detection of modification	EAL 4-6
	ADO_IGS.1 Installation, generation, and start-up procedures	EAL 1-7
Development	ADV_FSP.2 Fully defined external interfaces	EAL 4
	ADV_HLD.2 Security enforcing high-level design	EAL 3-4
	ADV_IMP.1 Subset of the implementation of the TSF	EAL 4
	ADV_LLD.1 Descriptive low-level design	EAL 4-5
	ADV_RCR.1 Informal correspondence demonstration	EAL 1-4
	ADV_SPM.1 Informal TOE security policy model	EAL 4
Guidance Documents	AGD_ADM.1 Administrator guidance	EAL 1-7
	AGD_USR.1 User guidance	EAL 1-7
Life Cycle Support	ALC_DVS.1 Identification of security measures	EAL 3-5
	ALC_FLR.3 Systematic flaw remediation	None
	ALC_LCD.1 Developer defined life-cycle model	EAL 4

Tabuľka 4.10: (pokračovanie)

Trieda záruk	Požiadavka	EAL
	ALC_TAT.1 Well-defined development tools	EAL 4
Tests	ATE_COV.2 Analysis of coverage	EAL 3-5
	ATE_DPT.2 Testing: low-level design	EAL 5-6
	ATE_FUN.1 Functional testing	EAL 2-5
	ATE_IND.2 Independent testing – sample	EAL 2-6
Vulnerability Assessment	AVA_MSU.2 Validation of analysis	EAL 4-5
	AVA_SOF.1 Strength of TOE security function evaluation	EAL 2-7
	AVA_VLA.3 Moderately resistant	EAL 5

#### 4.5.4 Sila kryptografických funkcií (Strength of Function)

Minimálna úroveň sily kryptografických funkcií (SOF, strength of function level) pre TOE a jeho IT prostredie je SOF-basic pre všetky úrovne bezpečnosti. Použitá má byť vždy, ak nie je explicitne uvedené inak.

Autentifikačné mechanizmy špecifikované v **FIA\_UAU.1 Timing of authentication** by mali spĺňať nasledovnú požiadavku: Pravdepodobnosť, že sa počas minúty náhodných pokusov podarí útočníkovi uspieť musí byť menšia ako  $10^{-6}$ .

Všetky použité kryptografické moduly musia byť overené proti FIPS 140-2 na rovnakú úroveň, ako je úroveň bezpečnosti zvoleného profilu ochrany. Od úrovne bezpečnosti 3 je nutné používať takéto kryptografické moduly na vykonávanie všetkých kryptografických funkcií a ukladanie nezašifrovaných verejných a súkromných kľúčov.

V prípade vydania novej verzie FIPS 140 sa tieto požiadavky automaticky vzťahujú na ňu namiesto FIPS 140-2.

## 4.6 Zdôvodnenie (Rationale)

Táto časť obsahuje zdôvodnenie volieb, ktoré sme spravili pri písaní predchádzajúcich častí. Zdôvodníme, že nami navrhovaný profil ochrany je korektný a vnútorne konzistentný. Ukážeme, že všetky nami zvolené bezpečnostné ciele, funkčné požiadavky a požiadavky na záruky sú dostatočné a opodstatnené.

### 4.6.1 Pokrytie bezpečnostných cieľov

V nasledujúcich tabuľkách ukážeme súvis medzi jednotlivými bezpečnostnými cieľmi a prostredím (definovaným hrozbami, predpokladmi a bezpečnostnými politikami). Údaje v tabuľkách sú zoradené abecedne podľa prvého stĺpca.

Tabuľka 4.11: Vzťah bezpečnostných cieľov pre TOE a hrozieb.

Bezpečnostný cieľ	Adresované hrozby
O.Archivované dokumenty	T.Zneužitie privilégii na získanie údajov.
O.Zálohovanie a obnova systémových dát.	T.Zlyhanie hardvéru alebo softvéru.  T.Poškodenie údajov chybou používateľa.

Tabuľka 4.12: Vzťah bezpečnostných cieľov pre prostredie a hrozieb.

Bezpečnostný cieľ	Adresované hrozby
O.Bezpečnostné roly.	T.Chyby administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 1-2.) T.Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.)
O.Bezpečnosť počas životného cyklu. (Úrovne bezpečnosti 2-4.)	T.Nepriateľský kód.  T.Zlyhanie hardvéru alebo softvéru.
O.Čitateľnosť médií.	T.Starnutie čítacích zariadení. T.Starnutie médií.
O.Dokumentácia pre administrátorov, operátorov, úradníkov a auditorov.	T.Chyby administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 1-2.) T.Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.) T.Kompromitácia súkromných kľúčov. T.Sociálne inžinierstvo.
O.Fyzická ochrana.	T.Neoprávnený fyzický prístup.
O.Hľadanie chýb v zdrojovom kóde. (Úroveň bezpečnosti 4.)	T.Chyby v softvéri archívu (Úrovne bezpečnosti 2-4.)
O.Inštalácia systému.	T.Zlyhanie hardvéru alebo softvéru.
O.Kompetentní administrátori, operátori, úradníci a auditori.	T.Chyby administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 1-2.)

Tabuľka 4.12: (pokračovanie)

Bezpečnostný cieľ	Adresované hrozby
	T.Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.)
O.Kryptografické funkcie.	T.Kompromitácia súkromných kľúčov. T.Útok na kryptografické funkcie.
O.Oprava identifikovaných bezpečnostných chýb. (Úrovne bezpečnosti 2-4.)	T.Chyby v softvéri archívu (Úrovne bezpečnosti 2-4.)
O.Overenie bezpečnostných funkcií.	T.Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.) T.Nepriateľský kód.
O.Pravidelná kontrola integrity.	T.Nepriateľský kód.
O.Trusted path. (Úrovne bezpečnosti 3-4.)	T.Neoprávnené získanie prístupu.  T.Odpočúvanie komunikácie.
O.Upozornenie zodpovedných na bezpečnostné problémy.	T.Neoprávnené získanie prístupu.  T.Nepriateľský kód. T.Zabránenie vykonávaniu funkcie.
O.Výuka proti sociálnemu inžinierstvu.	T.Sociálne inžinierstvo.
O.Overenie bezpečnostných funkcií.	T.Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.) T.Nepriateľský kód.

Tabuľka 4.13: Vzťah bezpeč. cieľov pre TOE s prostredím a hroziab.

Bezpečnostný cieľ	Adresované hrozby
O.Časové pečiatky. (Úroveň bezpečnosti 4.)	T.Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.) T.Vynechanie dôležitej administratívnej činnosti.
O.Časové značky.	T.Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.) T.Vynechanie dôležitej administratívnej činnosti.
O.Import a export údajov.	T.Neoprávnené získanie prístupu. T.Odpočúvanie komunikácie.

Tabuľka 4.13: (pokračovanie)

Bezpečnostný cieľ	Adresované hrozby
O. Individuálna zodpovednosť a auditné záznamy.	T. Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.) T. Neoprávnené získanie prístupu. T. Vynechanie dôležitej administratívnej činnosti. T. Zneužitie privilégií na získanie údajov.
O. Manažment konfigurácie.	T. Zlyhanie hardvéru alebo softvéru. T. Nepriateľský kód.
O. Manažment konfigurácie bezpečnostných funkcií.	T. Vynechanie dôležitej administratívnej činnosti.
O. Obmedzenie administratívneho prístupu.	T. Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.) T. Kompromitácia súkromných kľúčov.
O. Obmedzenie možností pred autentifikáciou.	T. Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.) T. Neoprávnené získanie prístupu.
O. Odstránenie nepriateľského kódu obnovou.	T. Nepriateľský kód.
O. Ochrana pred nepriateľským kódom.	T. Sociálne inžinierstvo. T. Nepriateľský kód.
O. Ochrana uložených auditných záznamov.	T. Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.)
O. Ochrana údajov pri internom prenose.	T. Kompromitácia súkromných kľúčov. T. Zneužitie privilégií na získanie údajov. T. Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.)
O. Reakcia na možnú stratu auditných záznamov.	T. Chyby administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 1-2.) T. Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.)
O. Reakcia na odhalené útoky. (Úrovne bezpečnosti 2-4.)	T. Neoprávnené získanie prístupu.
O. Udržiavanie bezpečnostných atribútov pre používateľov.	T. Chyby administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 1-2.)

Tabuľka 4.13: (pokračovanie)

Bezpečnostný cieľ	Adresované hrozby
	T.Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.)
O.Zistenie modifikácie softvéru a záložných údajov.	T.Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov. (Úrovne bezpečnosti 3-4.) T.Poškodenie údajov chybou používateľa.

Tabuľka 4.14: Vzťah organizačných bezpečnostných politík a bezpečnostných cieľov.

Org. bezp. politika	Bezpečnostné ciele
P.Kryptografické štandardy.	O.Kryptografické funkcie.
P.Používanie informácií na autorizované účely.	O.Auditori kontrolujú auditné záznamy.  O.Bezpečnostné roly. O.Manažment autorizácie používateľov. O.Obmedzenie možností pred autentifikáciou. O.Udržiavanie bezpečnostných atribútov pre používateľov.

Tabuľka 4.15: Vzťah predpokladov a bezpečnostných cieľov.

Predpoklad	Bezpečnostné ciele
A.Administrátori, operátori, úradníci a auditori nezneužívajú právomoci. (Úrovne bezpečnosti 1-2.)	O.Administrátori, operátori, úradníci a auditori nezneužívajú právomoci. (Úrovne bezpečnosti 1-2.)
A.Auditori kontrolujú auditné záznamy.	O.Auditori kontrolujú auditné záznamy.
A.Bezpečný operačný systém.	O.Operačný systém.
A.Certifikačná autorita a PKI.	O.Certifikačná autorita a PKI.
A.Časové pečiatky. (Úroveň bezpečnosti 4.)	O.Časové pečiatky. (Úroveň bezpečnosti 4.)
A.Čitateľnosť médií.	O.Čitateľnosť médií.
A.Fyzická ochrana.	O.Fyzická ochrana.
A.Kompetentní administrátori, operátori, úradníci a auditori.	O.Kompetentní administrátori, operátori, úradníci a auditori.
A.Kooperujúci používatelia. (Úrovne bezpečnosti 1-3.)	O.Kooperujúci používatelia. (Úrovne bezpečnosti 1-3.)

Tabuľka 4.15: (pokračovanie)

Predpoklad	Bezpečnostné ciele
A.Manažment autentifikačných údajov.	O.Manažment autentifikačných údajov.
A.Upozornenie zodpovedných na bezpečnostné problémy.	O.Upozornenie zodpovedných na bezpečnostné problémy.
A.Výuka proti sociálnemu inžinierstvu.	O.Výuka proti sociálnemu inžinierstvu.
A.Zničenie autentifikačných údajov.	O.Zničenie autentifikačných údajov.

## 4.6.2 Dostatočnosť bezpečnostných cieľov

V tejto časti rozdiskutujeme, že nami stanovené bezpečnostné ciele sú dostatočné, teda že poskytujú efektívne protiopatrenia proti identifikovaným hrozbám, dostatočne pokrývajú všetky organizačné bezpečnostné politiky a zodpovedajú predpokladom.

### Hrozby spojené s kryptografiou

**T.Kompromitácia súkromných kľúčov** adresuje situáciu, kedy sú súkromné kryptografické kľúče, uložené v systéme, prezradené, prípadne úmyselne zmenené.

Protiopatrenia:

**O.Dokumentácia pre administrátorov, operátorov, úradníkov a auditorov** zabezpečí dostatočnú dokumentáciu bezpečnej konfigurácie TOE. Táto dokumentácia minimalizuje možnosť chyby spravej týmto používateľmi.

**O.Kryptografické funkcie** zabezpečí, že všetky kryptografické funkcie implementované v TOE sú overené. Prípadné použitie overených kryptografických modulov zabezpečí ochranu kryptografických kľúčov počas ich uloženia v module.

**O.Obmedzenie administratívneho prístupu.** Administrátori nemajú automaticky prístup k súkromným kľúčom ostatných používateľov. Redukciou počtu používateľov s právom na prístup k danému súkromnému kľúču znížime pravdepodobnosť jeho kompromitácie.

**O.Ochrana údajov pri internom prenose.** Pri prenose kryptografických kľúčov v rámci systému je znížené riziko ich prezradenia neautorizovaným používateľom.

**T.Útok na kryptografické funkcie** adresuje situáciu, kedy útočník prelomí použitú kryptografickú funkciu a tak kompromituje bezpečnosť aktív.

Protiopatrenia:

**O.Kryptografické funkcie** zabezpečí, že všetky kryptografické funkcie implementované v TOE sú overené, neobsahujú známe chyby a sú použité dostatočné dĺžky kľúčov.

## Hrozby spojené s právomocami používateľov

**T.Chyby administrátorov, operátorov, úradníkov a auditorov.** (Úrovne bezpečnosti 1-2.) Táto hrozba adresuje chyby, ktoré neúmyselne spraví administrátor, operátor, úradník alebo auditor a naruší tak bezpečnosť systému.

Protiopatrenia:

**O.Bezpečnostné roly.** zabezpečuje, že každý používateľ má v každom okamihu priradenú bezpečnostnú rolu. Toto zabráni používateľom spraviť chybné úkony, ktoré nie sú v danom okamihu autorizovaní spraviť.

**O.Dokumentácia pre administrátorov, operátorov, úradníkov a auditorov** zabráni chybám prameniácim z nedorozumenia prostredníctvom dostatočnej dokumentácie systému.

**O.Kompetentní administrátori, operátori, úradníci a auditori** poskytuje používateľov schopných dodržiavať potrebné bezpečnostné postupy. Tým sa znižuje pravdepodobnosť, že spravia chybu.

**O.Reakcia na možnú stratu auditných záznamov** zabezpečí, že všetky závažné chyby spravené používateľmi rôznymi od auditora sú zaznamenané v auditných záznamoch, a teda môžu byť odhalené.

**O.Udržiavanie bezpečnostných atribútov pre používateľov** zabráni používateľom spraviť chybné úkony, ktoré nie sú autorizovaní spraviť.

**T.Chyby a nepriateľské akcie administrátorov, operátorov, úradníkov a auditorov.** (Úrovne bezpečnosti 3-4.) Táto hrozba adresuje chyby, ktoré neúmyselne spraví administrátor, operátor, úradník alebo auditor a naruší tak bezpečnosť systému. Tiež adresuje úmyselné upravenie konfigurácie systému používateľom s cieľom narušiť jeho bezpečnosť.

Protiopatrenia:

**O.Bezpečnostné roly** zabezpečuje, že každý používateľ má v každom okamihu priradenú bezpečnostnú rolu. Toto zabráni používateľom spraviť chybné úkony, ktoré nie sú v danom okamihu autorizovaní spraviť.

**O.Časové značky** zabezpečia jednoznačné zistenie časovej následnosti akcií z auditných záznamov.

**O.Dokumentácia pre administrátorov, operátorov, úradníkov a auditorov** zabráni chybám prameniácim z nedorozumenia prostredníctvom dostatočnej dokumentácie systému.

**O.Individuálna zodpovednosť a auditné záznamy** zabezpečuje individuálnu zodpovednosť za auditovateľné udalosti. Každý používateľ je v auditných záznamoch jednoznačne identifikovaný, takže každá akcia môže byť priradená konkrétnemu používateľovi. Kontrola auditných záznamov odhalí používateľov zneužívajúcich právomoci a je možné vyvodiť proti nim dôsledky.

**O.Kompetentní administrátori, operátori, úradníci a auditori** poskytuje používateľov schopných dodržiavať potrebné bezpečnostné postupy. Tým sa znižuje pravdepodobnosť, že spravia chybu.

**O.Obmedzenie administratívneho prístupu.** Administrátori nemajú automaticky prístup k citlivým údajom ostatných používateľov. Limitovanie možných operácií u používateľov vedie k zníženiu možného dopadu nepriateľských, resp. chybných akcií používateľov.

**O.Obmedzenie možností pred autentifikáciou** redukuje množinu akcií, ktoré môže používateľ vykonať pred riadnou autentifikáciou.

**O.Ochrana uložených auditných záznamov** zabezpečí, že auditné záznamy sú chránené proti neautorizovanému prístupu, úprave, resp. zmazaniu.

**O.Overenie bezpečnostných funkcií** zabezpečí, že hardvér a softvér zaisťujúci bezpečnosť systému funguje správne.

**O.Reakcia na možnú stratu auditných záznamov** zabezpečí, že všetky závažné chyby spravené používateľmi rôznymi od auditora sú zaznamenané v auditných záznamoch, a teda môžu byť odhalené.

**O.Udržiavanie bezpečnostných atribútov pre používateľov** zabráni používateľom spraviť chybné úkony, ktoré nie sú autorizovaní spraviť.

**O.Zistenie modifikácie softvéru a záložných údajov** umožní odhaliť každú modifikáciu softvéru alebo záložných údajov, z ktorých môže byť softvér obnovený.

Protiopatrenia na úrovni(ach) bezpečnosti 4:

**O.Časové pečiatky** zabezpečia dôveryhodné a jednoznačné zistenie časovej následnosti akcií z auditných záznamov.

**T.Poškodenie údajov chybou používateľa** zahŕňa situácie, kedy používateľ omylom zmaže alebo inak poškodí niektoré dôležité systémové dáta. Príkladom môže byť nepochopenie príkazu, stlačenie nesprávnej klávesy, výber nesprávnej možnosti a pod.

Protiopatrenia:

**O.Zálohovanie a obnova systémových dát** poskytuje možnosť takúto chybu napraviť obnovením poškodených dát pomocou zálohy.

**O.Zistenie modifikácie softvéru a záložných údajov** umožňuje odhaliť, že takáto chyba nastala.

**T.Vynechanie dôležitej administratívnej činnosti** adresuje situácie, kedy je bezpečnosť systému ohrozená tým, že nie je vykonaná potrebná administratívna činnosť.

Protiopatrenia:

**O.Časové značky** zabezpečia jednoznačné zistenie časovej následnosti akcií používateľov z auditných záznamov.

**O. Individuálna zodpovednosť a auditné záznamy** zabezpečuje individuálnu zodpovednosť za auditovateľné udalosti. Každý používateľ je v auditných záznamoch jednoznačne identifikovaný, takže každá akcia môže byť priradená konkrétnemu používateľovi. Kontrola auditných záznamov odhalí používateľov zanedbávajúcich povinnosti a je možné vyvodiť proti nim dôsledky.

**O. Manažment konfigurácie bezpečnostných funkcií** zabezpečí, že všetky konfiguračné údaje súvisiace s bezpečnosťou systému sú korektné spravované, a teda konzistentné s organizačnými bezpečnostnými politikami.

Protiopatrenia na úrovni(ach) bezpečnosti 4:

**O. Časové pečiatky** zabezpečia dôveryhodné a jednoznačné zistenie časovej následnosti akcií používateľov z auditných záznamov.

**T. Zneužitie privilégií na získanie údajov** adresuje situácie, kedy používateľ zneužije svoje privilégiá s cieľom získať prístup k citlivým údajom, prípadne sa pokúsi dostať tieto údaje mimo TOE.

Protiopatrenia:

**O. Archivované dokumenty** zabezpečí ochranu integrity a dôveryhodnosti archivovaných dokumentov.

**O. Individuálna zodpovednosť a auditné záznamy** zabezpečuje individuálnu zodpovednosť za auditovateľné udalosti. Každý používateľ je v auditných záznamoch jednoznačne identifikovaný, takže každá akcia môže byť priradená konkrétnemu používateľovi. Kontrola auditných záznamov odhalí používateľov, ktorí zneužívajú svoje právomoci s cieľom získať prístup k údajom.

**O. Ochrana údajov pri internom prenose.** zabezpečí citlivé údaje pri ich presúvaní v rámci TOE.

## Hrozby spojené s externým útokom

**T. Neoprávnené získanie prístupu** adresuje situácie, kedy útočník zvonka získa (napr. vďaka zraniteľnosti v autentifikačnom kóde, nedostatočným metódam autentifikácie a pod.) prístup k interným dátam TOE.

Protiopatrenia:

**O. Individuálna zodpovednosť a auditné záznamy** zabezpečuje individuálnu zodpovednosť za auditovateľné udalosti. Každý používateľ je v auditných záznamoch jednoznačne identifikovaný, takže každá akcia môže byť priradená konkrétnemu používateľovi. Kontrola auditných záznamov umožní odhaliť neautorizované aktivity a následne ich výsledky odstrániť.

**O. Obmedzenie možností pred autentifikáciou** redukuje množinu akcií, ktoré môže používateľ vykonať pred riadnou autentifikáciou.

**O.Upozornenie zodpovedných na bezpečnostné problémy** zabezpečí, že o odhalenom útoku sú informovaní kompetentní používatelia, čím sa zníži možný dopad útoku.

Protiopatrenia na úrovni(ach) bezpečnosti 2-4:

**O.Reakcia na odhalené útoky** poskytuje automatickú notifikáciu o útokoch odhalených bezpečnostnými funkciami, prípadne aj ďalšie reakcie s cieľom potlačiť tieto útoky.

Protiopatrenia na úrovni(ach) bezpečnosti 3-4:

**O.Trusted path** poskytne záruky o identite subjektu, s ktorým TOE komunikuje.

**T.Neoprávnený fyzický prístup** zahŕňa situácie, kedy útočník využije zraniteľnosť na získanie fyzického prístupu k systému.

Protiopatrenia:

**O.Fyzická ochrana** poskytuje dostatočnú úroveň fyzickej ochrany systému na zabránenie takýmto útokom.

**T.Odpočúvanie komunikácie.** Útočník môže monitorovať komunikáciu, ktorá prebieha elektronickou cestou medzi archívom a zvyškom sveta. Takto získané údaje môže použiť na ďalšie napadnutie systému, prípadne môže touto cestou získať neoprávnený prístup k dokumentom ukladaným do archívu.

Protiopatrenia:

**O.Import a export údajov** zabezpečí, že všetky dôverné údaje importované do a exportované z TOE sú pred útočníkom dostatočne chránené.

Protiopatrenia na úrovni(ach) bezpečnosti 3-4:

**O.Trusted path** dáva záruky, že sa posielané údaje bezpečne dostanú k TOE, resp. k určenému príjemcovi.

**T.Sociálne inžinierstvo** adresuje situácie, kedy sa útočník pokúsi použitím techník sociálneho inžinierstva získať informácie o prístupe do systému, jeho použití a fungovaní a prípadne ich využiť na neoprávnený prístup do systému a jeho poškodenie.

Protiopatrenia:

**O.Dokumentácia pre administrátorov, operátorov, úradníkov a auditorov** poskytuje používateľom jednoznačné personálne inštrukcie, ktoré je potrebné dodržiavať.

**O.Ochrana pred nepriateľským kódom** poskytuje súbor postupov, ktorých úlohou je neumožniť nepriateľskému kódu prístup do systému. Cieľom útoku sociálnym inžinierstvom môže byť práve vloženie takéhoto kódu do systému.

**O.Výuka proti sociálnemu inžinierstvu** zabezpečuje, že používatelia sú dostatočne informovaní o metódach boja proti technikám sociálneho inžinierstva.

**T.Zabránenie vykonávaniu funkcie.** Cieľom tohto útoku<sup>2</sup> je zabrániť cieľovému systému vykonávať jeho funkciu. Použité metódy zahŕňajú využitie zraniteľnosti systému na jeho poškodenie a zahltenie systému väčším množstvom požiadaviek ako je schopný spracúvať.

Protiopatrenia:

**O.Upozornenie zodpovedných na bezpečnostné problémy** zabezpečí, že kompetentné subjekty sú v prípade takéhoto útoku upozornené a môžu ho riešiť.

### Hrozby spojené s poškodením dokumentov

**T.Prírodná katastrofa.** (Úroveň bezpečnosti 3-4.) V prípade prírodnej katastrofy (požiar, povodeň, zemetrasenie a pod.), ktorá zasiahne samotný archív, môže dôjsť k vážnemu poškodeniu aj zničeniu všetkých aktív, vrátane archivovaných dokumentov.

Protiopatrenia:

**O.Archivované dokumenty** zabezpečí vhodné zálohovanie dôležitých archivovaných dokumentov.

**T.Starnutie čítacích zariadení.** Zároveň so vznikom nových typov médií sa zariadenia, slúžiace na čítanie starých typov médií, postupne prestávajú používať. Toto môže byť problémom v prípade, ak v archíve zostanú archivované dokumenty na médiách, ku ktorým už nebudú čítacie zariadenia existovať.

Protiopatrenia:

**O.Čitateľnosť médií** zabezpečí účinné protiopatrenia.

**T.Starnutie médií.** Je možné, že počas archivácie dokumentu na dlhšiu dobu jeho médium natolko zostarne, že dokument nebude čitateľný.

Protiopatrenia:

**O.Čitateľnosť médií** zabezpečí účinné protiopatrenia.

### Hrozby spojené s funkčnosťou systému

**T.Chyby v softvéri archívu.** (Úroveň bezpečnosti 2-4.) Táto hrozba adresuje neúmyselné aj úmyselné chyby v softvéri archívu, či už sú výsledkom zlého návrhu, zlej implementácie alebo ide o zadné dvierka do systému.

Protiopatrenia na úrovni(ach) bezpečnosti 2-4:

**O.Oprava identifikovaných bezpečnostných chýb** zabezpečuje opravu nájdených chýb.

Protiopatrenia na úrovni(ach) bezpečnosti 4:

---

<sup>2</sup>Známeho pod anglickým názvom *denial of service attack*.

**O.Hľadanie chýb v zdrojovom kóde** zabezpečuje, že zdrojový kód je počas evaluácie TOE preskúmaný, čím sa zníži pravdepodobnosť, že obsahuje chyby.

**T.Nepriateľský kód** adresuje situácie, kedy napr. autorizovaný používateľ alebo hacker spustí v rámci systému nepriateľský kód, ktorý môže narušiť integritu, dostupnosť aj utajenie aktív systému.

Protiopatrenia:

**O.Manažment konfigurácie** zabezpečí, že nepriateľský kód nemôže byť do systému vložený počas jeho konfigurácie.

**O.Odstránenie nepriateľského kódu obnovou** umožňuje po zistení prítomnosti nepriateľského kódu obnoviť systém do bezpečného stavu a v rámci tohto procesu nepriateľský kód (napr. vírus) odstrániť.

**O.Ochrana pred nepriateľským kódom** poskytuje súbor postupov, ktorých úlohou je neumožniť nepriateľskému kódu prístup do systému.

**O.Overenie bezpečnostných funkcií** zabezpečí, že hardvér a softvér zaisťujúci bezpečnosť systému funguje správne.

**O.Pravidelná kontrola integrity** umožňuje v rozumnom čase odhaliť prítomnosť nepriateľského kódu v systéme.

Protiopatrenia na úrovni(ach) bezpečnosti 2-4:

**O.Bezpečnosť životného cyklu** poskytuje prostriedky, ktoré zaisťujú, že počas fázy vývoja nebude do systému vložený nepriateľský kód. Počas operačnej fázy znižuje pravdepodobnosť vloženia nepriateľského kódu prostredníctvom identifikácie a nápravy chýb.

**T.Zlyhanie hardvéru alebo softvéru** adresuje zlyhanie komponentu, následkom ktorého systém stratí schopnosť vykonávať niektorú zo svojich funkcií.

Protiopatrenia:

**O.Manažment konfigurácie** zabezpečuje, že sa realizuje systematická správa konfigurácie systému. V dôsledku toho je zabezpečené, že príčinou zlyhania kritického systémového komponentu nie je jeho nesprávna konfigurácia.

**O.Inštalácia systému** zabezpečí, že TOE je dodaný, nainštalovaný a spravovaný spôsobom, ktorý má za cieľ zaisťiť jeho bezpečnosť. Prípadné zlyhanie kritického komponentu systému teda nebude následkom nesprávnej inštalácie systému.

**O.Zálohovanie a obnova systémových dát** poskytuje možnosť obnoviť systémové dáta v prípade ich poškodenia pri zlyhaní niektorého komponentu (napr. pevného disku).

Protiopatrenia na úrovni(ach) bezpečnosti 2-4:

**O.Bezpečnosť životného cyklu** poskytuje prostriedky, ktoré znížia vo fáze vývoja pravdepodobnosť nedokonalostí v hardvéri a softvéri systému. Počas operačnej fázy sa snaží nachádzať a opravovať chyby škôr, ako spôsobia zlyhanie kritického komponentu systému.

**O.Oprava identifikovaných bezpečnostných chýb** zabezpečuje, že dodávateľ opraví chyby nájdené v jeho kóde. Ich ignorovanie by mohlo viesť k zlyhaniu kritického komponentu.

### 4.6.3 Pokrytie funkčných požiadaviek a požiadaviek na záruky

V tabuľke 4.16 ukazujeme, že každá funkčná požiadavka (kladená na TOE alebo jeho prostredie) sa vzťahuje na aspoň jeden bezpečnostný cieľ. V tabuľke 4.17 ukazujeme to isté o požiadavkách na záruky.

Tabuľka 4.16: Vzťah funkčných požiadaviek a bezpečnostných cieľov.

Funkčná požiadavka	Bezpečnostné ciele
FAU_GEN.1 Audit data generation	O.Individuálna zodpovednosť a auditné záznamy
FAU_GEN.2 User identity association	O.Individuálna zodpovednosť a auditné záznamy
FAU_SAR.1 Audit review	O.Individuálna zodpovednosť a auditné záznamy
FAU_SAR.3 Selectable audit review	O.Individuálna zodpovednosť a auditné záznamy
FAU_STG.1 Protected audit trail storage	O.Ochrana uložených auditných záznamov
FAU_STG.3 Action in case of possible audit data loss	O.Reakcia na možnú stratu auditných záznamov
FAU_STG.4 Prevention of audit data loss	O.Reakcia na možnú stratu auditných záznamov
FCS_CKM.4 Cryptographic key destruction	O.Ochrana pred nepriateľským kódom O.Reakcia na odhalené útoky (úrovne bezpečnosti 2-4)
FCS_COP.1 Cryptographic operation	O.Archivované dokumenty O.Kryptografické funkcie
FDP_ACC.1 Subset access control	O.Archivované dokumenty O.Obmedzenie administratívneho prístupu
FDP_ACF.1 Security attribute based access control	O.Archivované dokumenty O.Obmedzenie administratívneho prístupu
FDP_ARC_BKP.1 Zálohovanie systému	O.Archivované dokumenty O.Odstránenie nepriateľského kódu obnovou O.Zálohovanie a obnova systémových dát

Tabuľka 4.16: (pokračovanie)

<b>Funkčná požiadavka</b>	<b>Bezpečnostné ciele</b>
FDP_ARC_BKP.2 Dôveryhodné zálohovanie systému (úrovne bezpečnosti 2-4)	O.Archivované dokumenty  O.Odstránenie nepriateľského kódu obnovou O.Zálohovanie a obnova systémových dát O.Zistenie modifikácie softvéru a záložných údajov
FDP_ETC.2 Export of user data with security attributes	O.Archivované dokumenty  O.Import a export údajov
FDP_ITC.2 Import of user data with security attributes	O.Archivované dokumenty  O.Import a export údajov
FDP_ITT.1 Basic internal transfer protection	O.Ochrana údajov pri internom prenose
FDP_RIP.1 Subset residual information protection	O.Archivované dokumenty
FDP_SDI.1 Stored data integrity monitoring	O.Archivované dokumenty
FDP_UCT.1 Basic data exchange confidentiality	O.Import a export údajov
FIA_AFL.1 Authentication failure handling (úrovne bezpečnosti 2-4)	O.Reakcia na odhalené útoky (úrovne bezpečnosti 2-4)
FIA_ATD.1 User attribute definition	O.Udržiavanie bezpečnostných atribútov pre používateľov
FIA_UAU.1 Timing of authentication	O.Obmedzenie administratívneho prístupu O.Obmedzenie možností pred autentifikáciou
FIA_UID.1 Timing of identification	O.Individuálna zodpovednosť a auditné záznamy O.Obmedzenie administratívneho prístupu
FIA_USB.1 User-subject binding	O.Udržiavanie bezpečnostných atribútov pre používateľov
FMT_MOF.1 Management of security functions behaviour	O.Manažment konfigurácie  O.Manažment konfigurácie bezpečnostných funkcií
FMT_MSA.1 Management of security attributes	O.Manažment autorizácie používateľov  O.Udržiavanie bezpečnostných atribútov pre používateľov
FMT_MSA.2 Secure security attributes (úrovne bezpečnosti 2-4)	O.Manažment konfigurácie bezpečnostných funkcií
FMT_MSA.3 Static attribute initialisation	O.Manažment konfigurácie bezpečnostných funkcií

Tabuľka 4.16: (pokračovanie)

<b>Funkčná požiadavka</b>	<b>Bezpečnostné ciele</b>
FMT_MTD.1 Management of TSF data	O.Individuálna zodpovednosť a auditné záznamy O.Ochrana uložených auditných záznamov
FMT_SMR.2 Restrictions on security roles	O.Bezpečnostné roly
FPT_ARC_ASE.1 Podpisovanie auditných záznamov (úrovne bezpečnosti 2-4)	O.Ochrana uložených auditných záznamov
FPT_ARC_ATE.1 Pečiatkovanie auditných záznamov (úroveň bezpečnosti 4)	O.Ochrana uložených auditných záznamov
FPT_AMT.1 Abstract machine testing	O.Overenie bezpečnostných funkcií O.Pravidelná kontrola integrity
FPT_ITT.1 Basic internal TSF data transfer protection	O.Ochrana údajov pri internom prenose  O.Zálohovanie a obnova systémových dát
FPT_RVM.1 Non-bypassability of the TSP	O.Operačný systém O.Obmedzenie administratívneho prístupu
FPT_SEP.1 TSF domain separation	O.Operačný systém
FPT_STM.1 Reliable time stamps	O.Časové značky O.Individuálna zodpovednosť a auditné záznamy
FPT_TST.1 TSF testing	O.Ochrana pred nepriateľským kódom O.Overenie bezpečnostných funkcií O.Pravidelná kontrola integrity O.Zistenie modifikácie softvéru a záložných údajov
FRU_RSA.1 Maximum quotas	O.Archivované dokumenty
FTP_TRP.1 Trusted path (úrovne bezpečnosti 3-4)	O.Trusted path (úrovne bezpečnosti 3-4)

Tabuľka 4.17: Vzťah požiadaviek na záruky a bezpečnostných cieľov.

<b>Požiadavka</b>	<b>Úr. bezp.</b>	<b>Bezpečnostné ciele</b>
ACM_AUT.1 Partial CM automation	4	EAL 4-5 O.Manažment konfigurácie
ACM_CAP.1 Version numbers	1	EAL 1 O.Manažment konfigurácie
ACM_CAP.3 Authorization controls	2-3	EAL 3 O.Manažment konfigurácie
ACM_CAP.4 Generation support and acceptance procedures	4	EAL 4-5  O.Manažment konfigurácie

Tabuľka 4.17: (pokračovanie)

Požiadavka	Úr. bezp.	Bezpečnostné ciele
ACM_SCP.2 Problem tracking CM coverage	2-4	EAL 4 O.Manažment konfigurácie
ADO_DEL.1 Delivery procedures	2-3	EAL 2-3
ADO_DEL.2 Detection of modification	4	EAL 4-6
ADO_IGS.1 Installation, generation, and start-up procedures	1-4	EAL 1-7  O.Inštalácia systému
ADV_FSP.1 Informal functional specification	1-2	EAL 1-3 O.Bezpečnosť počas životného cyklu (úrovne bezpečnosti 2-4)
ADV_FSP.2 Fully defined external interfaces	3-4	EAL 4 O.Bezpečnosť počas životného cyklu (úrovne bezpečnosti 2-4)
ADV_HLD.1 Descriptive high-level design	2	EAL 2 O.Bezpečnosť počas životného cyklu (úrovne bezpečnosti 2-4)
ADV_HLD.2 Security enforcing high-level design	3-4	EAL 3-4  O.Bezpečnosť počas životného cyklu (úrovne bezpečnosti 2-4)
ADV_IMP.1 Subset of the implementation of the TSF	3-4	EAL 4  O.Hľadanie chýb v zdrojovom kóde (úroveň bezpečnosti 4)
ADV_LLD.1 Descriptive low-level design	3-4	EAL 4-5 O.Bezpečnosť počas životného cyklu (úrovne bezpečnosti 2-4)
ADV_RCR.1 Informal correspondence demonstration	1-4	EAL 1-4  O.Bezpečnosť počas životného cyklu (úrovne bezpečnosti 2-4)
ADV_SPM.1 Informal TOE security policy model	2-4	EAL 4  O.Bezpečnosť počas životného cyklu (úrovne bezpečnosti 2-4)
AGD_ADM.1 Administrator guidance	1-4	EAL 1-7 O.Auditori kontrolujú auditné záznamy O.Dokumentácia pre administrátorov, operátorov, úradníkov a auditorov

Tabuľka 4.17: (pokračovanie)

Požiadavka	Úr. bezp.	Bezpečnostné ciele
		O.Inštalácia systému O.Kompetentní administrátori, operátori, úradníci a auditori O.Manažment autorizácie používateľov O.Manažment konfigurácie O.Manažment konfigurácie bezpečnostných funkcií O.Ochrana pred nepriateľským kódom
AGD_USR.1 User guidance	1-4	EAL 1-7 O.Dokumentácia pre administrátorov, operátorov, úradníkov a auditorov O.Ochrana pred nepriateľským kódom
ALC_DVS.1 Identification of security measures	2-4	EAL 3-5
ALC_FLR.2 Flaw reporting procedures	2-3	O.Bezpečnosť počas životného cyklu (úrovne bezpečnosti 2-4) O.Oprava identifikovaných bezpečnostných chýb (úrovne bezpečnosti 2-4)
ALC_FLR.3 Systematic flaw remediation	4	O.Bezpečnosť počas životného cyklu (úrovne bezpečnosti 2-4) O.Oprava identifikovaných bezpečnostných chýb (úrovne bezpečnosti 2-4)
ALC_LCD.1 Developer defined life-cycle model	4	EAL 4
ALC_TAT.1 Well-defined development tools	3-4	EAL 4
ATE_COV.2 Analysis of coverage	2-4	EAL 3-5
ATE_DPT.1 Testing: high-level design	2-3	EAL 3-4
ATE_DPT.2 Testing: low-level design	4	EAL 5-6
ATE_FUN.1 Functional testing	2-4	EAL 2-5
ATE_IND.1 Independent testing – conformance	1	EAL 1
ATE_IND.2 Independent testing – sample	2-4	EAL 2-6
AVA_MSU.2 Validation of analysis	2-4	EAL 4-5

Tabuľka 4.17: (pokračovanie)

Požiadavka	Úr. bezp.	Bezpečnostné ciele
AVA_SOF.1 Strength of TOE security function evaluation	2-4	EAL 2-7
AVA_VLA.1 Developer vulnerability analysis	2	EAL 2-3
AVA_VLA.2 Independent vulnerability analysis	3	EAL 4
AVA_VLA.3 Moderately resistant	4	EAL 5

#### 4.6.4 Dostatočnosť funkčných požiadaviek a požiadaviek na záruky

*Nasledujúce bezpečnostné ciele sa dotýkajú všetkých úrovní bezpečnosti.*

**O.Administrátori, operátori, úradníci a auditori nezneužívajú právomoci** (úrovne bezpečnosti 1-2) je zabezpečený predpokladom **A.Administrátori, operátori, úradníci a auditori nezneužívajú právomoci** (úrovne bezpečnosti 1-2), ktorí hovoria, že fungovanie TOE zabezpečujú dôveryhodní pracovníci.

**O.Archivované dokumenty** je zabezpečený zahrnutím viacerých požiadaviek. **FDP\_ETC.2 Export of user data with security attributes** a **FDP\_ITC.2 Import of user data with security attributes** zabezpečujú korektnú manipuláciu s archivovanými dokumentami pri ich vkladaní do archívu a výbere z neho. **FDP\_RIP.1 Subset residual information protection** zabezpečí, že po vybratí dokumentu z archívu je tento zaručene zmazaný. Počas doby archivovania dokumentov **FDP\_ACC.1 Subset access control** a **FDP\_ACF.1 Security attribute based access control** zabezpečia obmedzenie prístupu k archivovaným dokumentom, **FCS\_COP.1 Cryptographic operation** zabezpečí používanie vhodných kryptografických funkcií na zabezpečenie dôvernosti dokumentov, **FDP\_SDI.1 Stored data integrity monitoring** zabezpečí pravidelnú kontrolu ich integrity. Pravidelné zálohovanie (a prípadnú obnovu, ak z dôvodu chyby dôjde k narušeniu ich integrity) zabezpečia **FDP\_ARC\_BKP.1 Zálohovanie systému** a na úrovniach bezpečnosti 2-4 aj **FDP\_ARC\_BKP.2 Dôveryhodné zálohovanie systému**. Dostupnosť archivovaných dokumentov zaručí **FRU\_RSA.1 Maximum quotas**.

**O.Auditori kontrolujú auditné záznamy** je zabezpečený predpokladom **A.Auditori kontrolujú auditné záznamy**, ktorý stanovuje, že auditori pravidelne kontrolujú auditné záznamy. Tiež je podporovaný požiadavkou **AGD\_ADM.1 Administrator Guidance**, ktorá administrátorom poskytuje potrebné informácie.

**O.Bezpečnostné roly** je zabezpečený zahrnutím **FMT\_SMR.2 Restrictions on security roles**, čím je pokrytá požiadavka mať množinu bezpečnostných rolí a asociovať s nimi používateľov.

**O.Bezpečnosť počas životného cyklu** (úrovne bezpečnosti 2-4) je zabezpečená viacerými požiadavkami na záruky: Požiadavky **ADV\_FSP.1 Informal functional specification** (úrovne bezpečnosti 1-2), **ADV\_FSP.2 Fully defined external interfaces** (úrovne bezpečnosti 3-4), **ADV\_HLD.1 Descriptive high-level design** (úroveň bezpečnosti 2), **ADV\_HLD.2 Security enforcing high-level design** (úrovne bezpečnosti 3-4), **ADV\_IMP.1 Subset of the implementation of the TSF** (úroveň bezpečnosti 4), **ADV\_LLD.1 Descriptive low-level design** (úrovne bezpečnosti 3-4), **ADV\_RCR.1 Informal correspondence demonstration** a **ADV\_SPM.1 Information TOE security policy model** spoločne zabezpečujú, že už pôvodný design systému je robený s ohľadom na dostatočnú úroveň bezpečnosti. Požiadavky **ALC\_FLR.2 Flaw reporting procedures** (úrovne bezpečnosti 2-3) a **ALC\_FLR.3 Systematic flaw remediation** (úroveň bezpečnosti 4) pokrývajú požiadavku nachádzania a opravovania chýb počas operácie systému.

**O.Certifikačná autorita a PKI** je zabezpečený predpokladom **A.Certifikačná autorita a PKI**, ktorý stanovuje, že archív vie bezpečnou cestou získať a obnovovať svoje verejné a súkromné kľúče a takisto si vie overiť pravosť verejných kľúčov klientov.

**O.Časové pečiatky** (úroveň bezpečnosti 4) je zabezpečený predpokladom **A.Časové pečiatky** (úroveň bezpečnosti 4), ktorý hovorí, že archív môže využiť služby externej TSS.

**O.Časové značky** je zabezpečený zahrnutím **FPT\_STM.1 Reliable time stamps**, ktorý stanovuje, že archív si generuje časové značky pre potrebu vyznačenia následnosti udalostí v auditných záznamoch.

**O.Čitateľnosť médií** je zabezpečený predpokladom **A.Čitateľnosť médií**, ktorý zabezpečuje, že médiá použité na archiváciu dokumentov budú v každom okamihu čitateľné.

**O.Dokumentácia pre administrátorov, operátorov, úradníkov a auditorov** je poskytnutá požiadavkami **AGD\_ADM.1 Administrator Guidance** a **AGD\_USR.1 User Guidance**, ktoré poskytujú administrátorom a používateľom dostatočné informácie o správnom používaní systému.

**O.Fyzická ochrana** je zabezpečený predpokladom **A.Fyzická ochrana**, ktorý hovorí, že všetky dôležité komponenty TOE (hardvér, softvér, prípadne aj firmvér) sú dostatočne chránené proti fyzickému útoku, ktorý by mohol narušiť ich funkčnosť alebo bezpečnosť údajov v nich obsiahnutých.

**O.Hľadanie chýb v zdrojovom kóde** (úroveň bezpečnosti 4) je zabezpečený požiadavkou **ADV\_IMP.1 Subset of the implementation of the TSF** (úroveň bezpečnosti 4), súčasťou ktorej je kontrola zdrojového kódu.

**O.Import a export údajov** je zabezpečený kombináciou viacerých požiadaviek: **FDP\_UCT.1 Basic data exchange confidentiality** zabezpečí ochranu údajov počas

prenosu, **FDP\_ETC.2 Export of user data with security attributes** a **FDP\_ITC.2 Import of user data with security attributes** ich správne zaradenie do systému a správne odoslanie z neho.

**O.Individuálna zodpovednosť a auditné záznamy** je zabezpečený kombináciou viacerých požiadaviek. **FIA\_UID.1 Timing of identification** pokrýva požiadavku, že používatelia sa musia identifikovať pred vykonávaním operácií súvisiacich s bezpečnosťou TOE. **FAU\_GEN.1 Audit data generation** zabezpečuje, že všetky potrebné údaje o operáciách dotýkajúcich sa bezpečnosti TOE budú auditované, **FAU\_GEN.2 User identity association** a **FPT\_STM.1 Reliable time stamps** zabezpečujú, že v auditných záznamoch je pri každej operácii uvedený jej presný čas vykonania a identity zodpovedných používateľov. Vďaka **FMT\_MTD.1 Management of TSF data** nemajú iní používatelia ako auditori právo zmazať auditné záznamy. **FAU\_SAR.1 Audit review** umožní dostupnosť auditných záznamov na kontrolu, takže môže byť vyvodená osobná zodpovednosť.

**O.Inštalácia systému** je zabezpečený kombináciou viacerých požiadaviek: **ADO\_IGS.1 Installation, generation, and start-up procedures** a **AGD\_ADM.1 Administrator guidance** pokrývajú požiadavku poskytnúť administrátorom dostatočné informácie potrebné na správnu inštaláciu systému. Tiež je podporovaný predpokladom **A.Kompetentní administrátori, operátori, úradníci a auditori**.

**O.Kompetentní administrátori, operátori, úradníci a auditori** je zabezpečený predpokladom **A.Kompetentní administrátori, operátori, úradníci a auditori**. Tiež je podporovaný požiadavkou **AGD\_ADM.1 Administrator Guidance**, ktorá administrátorom poskytuje potrebné informácie.

**O.Kooperatívni používatelia** (úrovne bezpečnosti 1-3) je zabezpečený predpokladom **A.Kooperatívni používatelia** (úrovne bezpečnosti 1-3), ktorý stanovuje, že autorizovaní používatelia sa správajú podľa určených pravidiel.

**O.Kryptografické funkcie** je zabezpečený zahrnutím **FCS\_COP.1 Cryptographic operation**, čím je pokrytá požiadavka, aby vždy boli používané bezpečné kryptografické funkcie zodpovedajúce štandardom.

**O.Manažment autentifikačných údajov** je zabezpečený predpokladom **A.Manažment autentifikačných údajov**, ktorý vynucuje vhodnú politiku spravovania autentifikačných údajov.

**O.Manažment autorizácie používateľov** je zabezpečený zahrnutím **FMT\_MSA.1 Management of security attributes**, ktorý pokrýva požiadavku, aby administrátori spravovali bezpečnostné atribúty používateľov. Je tiež podporovaný predpokladom **A.Kompetentní administrátori, operátori, úradníci a auditori**, ktorý poskytuje administrátorov kompetentných vykonávať tieto činnosti a požiadavkou **AGD\_ADM.1 Administrator Guidance**, ktorá administrátorom poskytuje potrebné informácie.

**O. Manažment konfigurácie** je zabezpečený zahrnutím **FMT\_MOF.1 Management of security functions behaviour**, ktorý pokrýva požiadavku, že konfiguráciu systému môžu vykonávať iba autorizovaní používatelia. Je podporovaný predpokladom **A. Kompetentní administrátori, operátori, úradníci a auditori**, ktorý poskytuje používateľov kompetentných vykonávať tieto činnosti. Tiež je podporovaný viacerými požiadavkami na záruky: **AGD\_ADM.1 Administrator Guidance** poskytuje administrátorom potrebné informácie, **ACM\_CAP.1 Version numbers**, od úrovne bezpečnosti 2 **ACM\_CAP.3 Authorisation controls**, **ACM\_SCP.2 Problem tracking CM coverage** a na úrovni bezpečnosti 4 aj **ACM\_AUT.1 Partial CM automation** a **ACM\_CAP.4 Generation support and acceptance procedures** zabezpečujú, že manažment konfigurácie je implementovaný a používaný.

**O. Manažment konfigurácie bezpečnostných funkcií** je zabezpečený zahrnutím nasledujúcich predpokladov: **FMT\_MSA.2 Secure security attributes** (úroveň bezpečnosti 2-4) a **FMT\_MSA.3 Static attribute initialisation** zabezpečia, že parametre bezpečnostných funkcií majú vhodné hodnoty, **FMT\_MOF.1 Management of security functions behaviour** zabezpečí, že tieto parametre môžu meniť len autorizovaní používatelia. Tiež je podporovaný požiadavkou **AGD\_ADM.1 Administrator Guidance** a predpokladom **A. Kompetentní administrátori, operátori, úradníci a auditori**, ktoré poskytnú autorizovaných používateľov kompetentných a schopných konfigurovať bezpečnostné funkcie.

**O. Obmedzenie administratívneho prístupu** je zabezpečený zahrnutím **FDP\_ACC.1 Subset access control**, **FDP\_ACF.1 Security attribute based access control**, **FIA\_UAU.1 Timing of authentication** a **FIA\_UID.1 Timing of identification**. Prítomnosť **FIA\_UAU.1 Timing of authentication** a **FIA\_UID.1 Timing of identification** zabezpečujú, že administrátori, operátori, úradníci ani auditori nemôžu vykonávať operácie súvisiace s bezpečnosťou TOE, kým neprešli príslušnou identifikáciou a autentifikáciou. **FDP\_ACC.1 Subset access control** a **FDP\_ACF.1 Security attribute based access control** zabezpečujú, že administrátori, operátori, úradníci a auditori majú možnosť vykonávať len operácie súvisiace s náplňou ich práce. **FPT\_RVM.1 Non-bypassability of the TSP** zabezpečuje, že administrátori, operátori, úradníci ani auditori nemôžu vykonať operácie, ktoré nie sú autorizovaní vykonávať, pomocou obídenia funkcií vynucujúcich bezpečnostnú politiku.

**O. Obmedzenie možností pred autentifikáciou** je zabezpečený zahrnutím **FIA\_UAU.1 Timing of authentication**, kde je určené, že používateľ nemôže vykonať žiadne akcie dotýkajúce sa bezpečnosti systému, kým nebol autentifikovaný.

**O. Odstránenie nepriateľského kódu obnovou** je zabezpečený zahrnutím **FDP\_ARC\_BKP.1 Zálohovanie systému** a od úrovne bezpečnosti 2 aj zahrnutím **FDP\_ARC\_BKP.2 Dôveryhodné zálohovanie systému**, ktoré zabezpečia korektné a bezpečné zálohovanie a prípadnú obnovu systémových dát.

**O.Ochrana pred nepriateľským kódom** je zabezpečený zahrnutím požiadaviek **AGD\_ADM.1 Administrator Guidance** a **AGD\_USR.1 User Guidance**, ktoré zabránia, aby používatelia zaviedli takýto kód do systému omylom. Takisto je podporovaný zahrnutím požiadavky **FPT\_TST.1 TSF testing**, ktorá zabezpečí pravidelné testovanie funkčnosti bezpečnostných funkcií, a teda okrem iného aj ľubovoľné zásahy nepriateľského kódu do ich fungovania (ako napr. nakazenie programu vykonávajúceho bezpečnostnú funkciu počítačovým vírusom).

**O.Ochrana uložených auditných záznamov** je zabezpečený zahrnutím viacerých požiadaviek. **FAU\_STG.1 Protected audit trail storage** pokrýva požiadavku, aby auditné záznamy boli chránené proti zmene a zmazaniu. **FMT\_MTD.1 Management of TSF data** ich chráni proti neautorizovanému prístupu. Od úrovne bezpečnosti 2 je zabezpečený aj zahrnutím **FPT\_ARC\_ASE.1 Podpisovanie auditných záznamov** a od úrovne bezpečnosti 4 zahrnutím **FPT\_ARC\_ATE.1 Pečiatkovanie auditných záznamov**, ktoré poskytujú dodatočné záruky, že auditné záznamy neboli modifikované neautorizovaným spôsobom.

**O.Ochrana údajov pri internom prenose** je zabezpečený zahrnutím dvoch požiadaviek: **FPT\_ITT.1 Basic internal TSF data transfer protection** zabezpečí integritu a dôvernú presúvaných údajov súvisiacich s bezpečnosťou TOE, **FDP\_ITT.1 Basic internal transfer protection**. zabezpečí integritu používateľských dát (vrátane samotných archivovaných dokumentoch) pri presunoch v rámci TOE. Príkladom takéhoto interného presunu je vytváranie záloh.

**O.Operačný systém** je zabezpečený predpokladom **A.Operačný systém**, ktorý hovorí, že operačný systém poskytuje bezpečnostné funkcie požadované pre fungovanie TOE. Je tiež podporovaný **FPT\_SEP.1 TSF domain separation**, zabezpečujúcim separáciu domén v rámci TOE a **FPT\_RVM.1 Non-bypassability of the TSP**, zabezpečujúcim neobíditeľnosť bezpečnostných funkcií operačného systému.

**O.Oprava identifikovaných bezpečnostných chýb** (úrovne bezpečnosti 2-4) je zabezpečený zahrnutím **ALC\_FLR.2 Flaw reporting procedures** (úrovne bezpečnosti 2-3), resp. **ALC\_FLR.3 Systematic Flaw remediation** (úroveň bezpečnosti 4). Tie pokrývajú požiadavku, aby dodávateľ opravil používateľmi identifikované bezpečnostné chyby.

**O.Overenie bezpečnostných funkcií** je zabezpečený zahrnutím požiadavky **FPT\_TST.1 TSF testing**, ktorá zabezpečí pravidelné testovanie funkčnosti bezpečnostných funkcií a podporovaný zahrnutím **FPT\_AMT.1 Abstract machine testing**, vďaka ktorému je overené, že hardvér a firmvér potrebný na zabezpečenie bezpečnostných funkcií správne funguje,

**O.Pravidelná kontrola integrity** je zabezpečený zahrnutím **FPT\_AMT.1 Abstract machine testing**, vďaka ktorému je overené, že hardvér a firmvér potrebný na zabezpečenie bezpečnostných funkcií správne funguje a podporovaný zahrnutím **FPT\_TST.1**

**TSF testing**, ktorá zabezpečí pravidelné testovanie funkčnosti bezpečnostných funkcií.

**O.Reakcia na možnú stratu auditných záznamov** je zabezpečený zahrnutím **FAU\_STG.3 Action in case of possible audit data loss** a **FAU\_STG.4 Prevention of audit data loss**. Tie definujú akcie v prípade blížiaceho sa zaplnenia priestoru určeného na auditné záznamy a akcie v prípade, že sa tento priestor zaplní. Napriek tomu, že podľa CC je **FAU\_STG.4** hierarchicky nadradený **FAU\_STG.3**, rozhodli sme sa začleniť oba. Toto je opodstatnené, lebo akcie uvedené v **FAU\_STG.4** nie sú nadmnožinou akcií z **FAU\_STG.3**.

**O.Reakcia na odhalené útoky** (úrovne bezpečnosti 2-4) je zabezpečený zahrnutím **FIA\_AFL.1 Authentication failure handling** (úrovne bezpečnosti 2-4), vďaka ktorému je odhalenému útočníkovi zablokovaná možnosť autentifikácie. Korektné zmazanie potenciálne kompromitovaných kryptografických kľúčov v prípade odhaleného úspešného útoku zabezpečí **FCS\_CKM.4 Cryptographic key destruction**.

**O.Trusted path** (úrovne bezpečnosti 3-4) je zabezpečený zahrnutím **FTP\_TRP.1 Trusted path** (úrovne bezpečnosti 3-4), ktorý požadovanú trusted path k používateľovi poskytne.

**O.Udržiavanie bezpečnostných atribútov pre používateľov** je zabezpečený zahrnutím viacerých požiadaviek. **FIA\_ATD.1 User attribute definition** a **FIA\_USB.1 User-subject binding** pokrývajú požiadavku, že s každým používateľom (resp. subjektom konajúcim v jeho mene) je potrebné mať asociovanú množinu jeho bezpečnostných atribútov. **FMT\_MSA.1 Management of security attributes** zabezpečuje, že tieto atribúty môžu meniť len autorizovaní používatelia.

**O.Upozornenie zodpovedných na bezpečnostné problémy** je zabezpečený predpokladom **A.Upozornenie zodpovedných na bezpečnostné problémy** ktorý hovorí, že všetci používatelia bezodkladne informujú zodpovedných o prípadných bezpečnostných problémoch, čím sa minimalizuje dopad týchto problémov a potenciálna možnosť poškodenia systému.

**O.Výuka proti sociálnemu inžinierstvu** je zabezpečený predpokladom **A.Výuka proti sociálnemu inžinierstvu**, ktorý hovorí, že všetci používatelia sú informovaní o technikách sociálneho inžinierstva a metódach boja proti nim.

**O.Zistenie modifikácie softvéru a záložných údajov** je zabezpečený požiadavkou **FPT\_TST.1 TSF testing**, ktorá zabezpečí pravidelné testovanie funkčnosti bezpečnostných funkcií a od úrovne bezpečnosti 2 aj zahrnutím **FDP\_ARC\_BKP.2 Dôveryhodné zálohovanie systému**, ktorá zabezpečí korektné a bezpečné zálohovanie systémových dát.

**O.Zničenie autentifikačných údajov** je zabezpečený predpokladom **A.Zničenie autentifikačných údajov**, ktorý hovorí, že autentifikačné údaje, ktorým skončila plat-

nosť, sú zo systému odstránené.

**O.Zálohovanie a obnova systémových dát** je zabezpečený zahrnutím **FDP\_ARC\_BKP.1 Zálohovanie systému** a od úrovne bezpečnosti 2 aj zahrnutím **FDP\_ARC\_BKP.2 Dôveryhodné zálohovanie systému**, ktoré zabezpečia korektné a bezpečné zálohovanie a prípadnú obnovu systémových dát. **FPT\_ITT.1 Basic internal TSF data transfer protection** zabezpečí integritu záloh počas ich prenosu v rámci TOE.

## 4.6.5 Závislosti medzi požiadavkami

### Funkčné požiadavky na úrovni bezpečnosti 1

V tabuľke 4.18 ukážeme splnenie závislostí medzi jednotlivými funkčnými požiadavkami na úrovni bezpečnosti 1.

Tabuľka 4.18: Závislosti pre funkčné požiadavky  
– úroveň bezpečnosti 1.

Funkčná požiadavka	Závisí na	Stav
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	zahrnuté
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation	zahrnuté
	FIA_UID.1 Timing of identification	zahrnuté
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation	zahrnuté
FAU_SAR.3 Selectable audit review	FAU_SAR.1 Audit review	zahrnuté
FAU_STG.1 Protected audit trail storage	FAU_GEN.1 Audit data generation	zahrnuté
FAU_STG.3 Action in case of possible audit data loss	FAU_STG.1 Protected audit trail storage	zahrnuté
FAU_STG.4 Prevention of audit data loss	FAU_STG.1 Protected audit trail storage	zahrnuté
FCS_CKM.4 Cryptographic key destruction	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	zahrnuté FDP_ITC.2
	FMT_MSA.2 Secure security attributes	<b>nezahrnuté</b>
FCS_COP.1 Cryptographic operation	FCS_CKM.4 Cryptographic key destruction	zahrnuté
	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	zahrnuté FDP_ITC.2

Tabuľka 4.18: (pokračovanie)

Funkčná požiadavka	Závisí na	Stav
	FMT_MSA.2 Secure security attributes	<b>nezahrnuté</b>
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	zahrnuté
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	zahrnuté zahrnuté
FDP_ARC_BKP.1 Zálohovanie systému	<i>žiadne závislosti</i>	
FDP_ETC.2 Export of user data with security attributes	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	zahrnuté FDP_ACC.1
FDP_ITC.2 Import of user data with security attributes	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path FPT_TDC.1 Inter-TSF basic TSF data consistency	zahrnuté FDP_ACC.1 <b>nezahrnuté</b> <b>nezahrnuté</b>
FDP_ITT.1 Basic internal transfer protection	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	zahrnuté FDP_ACC.1
FDP_UCT.1 Basic data exchange confidentiality	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path	zahrnuté FDP_ACC.1 <b>nezahrnuté</b>
FIA_ATD.1 User attribute definition	<i>žiadne závislosti</i>	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	zahrnuté
FIA_UID.1 Timing of identification	<i>žiadne závislosti</i>	
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition	zahrnuté
FMT_MOF.1 Management of security functions behaviour	FMT_SMR.1 Security roles	zahrnuté FMT_SMR.2
FMT_MSA.1 Management of security attributes	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control FMT_SMR.1 Security roles	zahrnuté FDP_ACC.1 zahrnuté FMT_SMR.2

Tabuľka 4.18: (pokračovanie)

Funkčná požiadavka	Závisí na	Stav
FMT_MSA.3 Static attribute initialisation	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	zahrnuté zahrnuté FMT_SMR.2
FMT_MTD.1 Management of TSF data	FMT_SMR.1 Security roles	zahrnuté FMT_SMR.2
FMT_SMR.2 Restrictions on security roles	FIA_UID.1 Timing of identification	zahrnuté
FPT_AMT.1 Abstract machine testing	<i>žiadne závislosti</i>	
FPT_ITT.1 Basic internal TSF data transfer protection	<i>žiadne závislosti</i>	
FPT_RVM.1 Non-bypassability of the TSP	<i>žiadne závislosti</i>	
FPT_SEP.1 TSF domain separation	<i>žiadne závislosti</i>	
FPT_STM.1 Reliable time stamps	<i>žiadne závislosti</i>	

### Funkčné požiadavky na vyšších úrovni bezpečnosti

V tabuľke 4.19 uvedieme funkčné požiadavky, ktoré pribúdajú na vyšších úrovniach bezpečnosti a ukážeme, ako sú splnené ich závislosti.

Tabuľka 4.19: Závislosti pre funkčné požiadavky  
– úrovne bezpečnosti 2-4.

Funkčná požiadavka	Závisí na	Stav
FDP_ARC_BKP.2 Dôveryhodné zálohovanie systému (úrovne bezpečnosti 2-4)	FDP_ARC_BKP.1 Zálohovanie systému	zahrnuté
FIA_AFL.1 Authentication failure handling (úrovne bezpečnosti 2-4)	FIA_UAU.1 Timing of authentication	zahrnuté
FMT_MSA.2 Secure security attributes (úrovne bezpečnosti 2-4)	ADV_SPM.1 Informal TOE security policy model FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	zahrnuté zahrnuté FDP_ACC.1 zahrnuté zahrnuté FMT_SMR.2

Tabuľka 4.19: (pokračovanie)

Funkčná požiadavka	Závisí na	Stav
FPT_ARC_ASE.1 Podpisovanie auditných záznamov (úrovne bezpečnosti 2-4)	FAU_GEN.1 Audit data generation  FMT_MOF.1 Management of security functions behaviour	zahrnuté  zahrnuté
FPT_ARC_ATE.1 Pečiatkovanie auditných záznamov (úroveň bezpečnosti 4)	FAU_GEN.1 Audit data generation  FMT_MOF.1 Management of security functions behaviour FTP_TRP.1 Trusted path	zahrnuté  zahrnuté zahrnuté
FTP_TRP.1 Trusted path (úrovne bezpečnosti 3-4)	<i>žiadne závislosti</i>	

#### Zdôvodnenie nezahrnutia FMT\_MSA.2 na úrovni bezpečnosti 1

Viaceré komponenty majú závislosť na komponente **FMT\_MSA.2 Secure security attributes**. Podľa predpokladov pre túto úroveň bezpečnosti je potreba tohto komponentu zanedbateľná, navyše ak sa na vykonávanie kryptografických funkcií používa kryptografický modul overený proti FIPS 140-2, ten spĺňa požiadavky kladené komponentmi závisiacimi na **FMT\_MSA.2 Secure security attributes**.

#### Zdôvodnenie nezahrnutia FTP\_ITC.1 a FTP\_TRP.1 na úrovniach bezpečnosti 1-2

Na týchto úrovniach bezpečnosti ide o zbytočne silnú požiadavku, dostatočnú úroveň zabezpečenia vieme dosiahnuť napr. pomocou jednoduchého šifrovania komunikácie.

#### Zdôvodnenie nezahrnutia FPT\_TDC.1

Jediná zvolená funkčná požiadavka, ktorá na FPT\_TDC.1 podľa CC závisí je **FDP\_ITC.2 Import of user data with security attributes**. Túto funkčnú požiadavku sme zvolili kvôli možnosti používateľov ukladať do archívu dokumenty so stanovanými požiadavkami na utajenie a pod. – teda nie kvôli importovaniu dát od iných trusted IT produktov, preto táto požiadavka v našom prípade nemá zmysel.

### Požiadavky na záruky na úrovni bezpečnosti 1

Tabuľky 4.20, 4.21, 4.22, 4.23 ukazujú splnenie závislostí medzi požiadavkami na záruky pre jednotlivé úrovne bezpečnosti. Obsahujú len priame závislosti, keďže nepriame z nich implicitne vyplývajú a všetky sú splnené.

Tabuľka 4.20: Závislosti medzi požiadavkami na záruky – úroveň bezpečnosti 1.

Požiadavka na záruky	Závisí na	Stav
ACM_CAP.1 Version numbers	<i>žiadne závislosti</i>	
ADO_IGS.1 Installation, generation, and start-up procedures	AGD_ADM.1	zahrnuté
ADV_FSP.1 Informal functional specification	ADV_RCR.1	zahrnuté
ADV_RCR.1 Informal correspondence demonstration	<i>žiadne závislosti</i>	
AGD_ADM.1 Administrator guidance	ADV_FSP.1	zahrnuté
AGD_USR.1 User guidance	ADV_FSP.1	zahrnuté
ATE_FUN.1 Functional testing	<i>žiadne závislosti</i>	
ATE_IND.1 Independent testing – conformance	ADV_FSP.1	zahrnuté
	AGD_ADM.1	zahrnuté
	AGD_USR.1	zahrnuté

Tabuľka 4.21: Závislosti medzi požiadavkami na záruky – úroveň bezpečnosti 2.

Požiadavka na záruky	Závisí na	Stav
ACM_CAP.3 Authorization controls	ACM_SCP.1	zahrnuté ACM_SCP.2
	ALC_DVS.1	zahrnuté
ACM_SCP.2 Problem tracking CM coverage	ACM_CAP.3	zahrnuté
ADO_DEL.1 Delivery procedures	<i>žiadne závislosti</i>	
ADO_IGS.1 Installation, generation, and start-up procedures	AGD_ADM.1	zahrnuté
ADV_FSP.1 Informal functional specification	ADV_RCR.1	zahrnuté
ADV_HLD.1 Descriptive high-level design	ADV_FSP.1	zahrnuté
ADV_RCR.1 Informal correspondence demonstration	<i>žiadne závislosti</i>	
ADV_SPM.1 Informal TOE security policy model	ADV_FSP.1	zahrnuté
AGD_ADM.1 Administrator guidance	ADV_FSP.1	zahrnuté
AGD_USR.1 User guidance	ADV_FSP.1	zahrnuté
ALC_DVS.1 Identification of security measures	<i>žiadne závislosti</i>	

Tabuľka 4.21: (pokračovanie)

Požiadavka na záruky	Závisí na	Stav
ALC_FLR.2 Flaw reporting procedures	žiadne závislosti	
ATE_COV.2 Analysis of coverage	ADV_FSP.1 ATE_FUN.1	zahrnuté zahrnuté
ATE_DPT.1 Testing – high-level design	ADV_HLD.1 ATE_FUN.1	zahrnuté zahrnuté
ATE_FUN.1 Functional testing	žiadne závislosti	
ATE_IND.2 Independent testing – sample	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1	zahrnuté zahrnuté zahrnuté zahrnuté
AVA_MSU.2 Validation of analysis	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	zahrnuté zahrnuté zahrnuté zahrnuté
AVA_SOF.1 Strength of TOE security function evaluation	ADV_FSP.1  ADV_HLD.1	zahrnuté  zahrnuté
AVA_VLA.1 Developer vulnerability analysis	ADV_FSP.1 ADV_HLD.1 AGD_ADM.1 AGD_USR.1	zahrnuté zahrnuté zahrnuté zahrnuté

Tabuľka 4.22: Závislosti medzi požiadavkami na záruky  
– úroveň bezpečnosti 3.

Požiadavka na záruky	Závisí na	Stav
ACM_CAP.3 Authorization controls	ACM_SCP.1 ALC_DVS.1	zahrnuté ACM_SCP.2 zahrnuté
ACM_SCP.2 Problem tracking CM coverage	ACM_CAP.3	zahrnuté
ADO_DEL.1 Delivery procedures	žiadne závislosti	
ADO_IGS.1 Installation, generation, and start-up procedures	AGD_ADM.1	zahrnuté
ADV_FSP.2 Fully defined external interfaces	ADV_RCR.1	zahrnuté
ADV_HLD.2 Security enforcing high-level design	ADV_FSP.1  ADV_RCR.1	zahrnuté ADV_FSP.2  zahrnuté
ADV_IMP.1 Subset of the implementation of the TSF	ADV_LLD.1  ADV_RCR.1 ALC_TAT.1	zahrnuté  zahrnuté zahrnuté
ADV_LLD.1 Descriptive low-level design	ADV_HLD.2	zahrnuté

Tabuľka 4.22: (pokračovanie)

Požiadavka na záruky	Závisí na	Stav
	ADV_RCR.1	zahrnuté
ADV_RCR.1 Informal correspondence demonstration	<i>žiadne závislosti</i>	
ADV_SPM.1 Informal TOE security policy model	ADV_FSP.1	zahrnuté ADV_FSP.2
AGD_ADM.1 Administrator guidance	ADV_FSP.1	zahrnuté ADV_FSP.2
AGD_USR.1 User guidance	ADV_FSP.1	zahrnuté ADV_FSP.2
ALC_DVS.1 Identification of security measures	<i>žiadne závislosti</i>	
ALC_FLR.2 Flaw reporting procedures	<i>žiadne závislosti</i>	
ALC_TAT.1 Well-defined development tools	ADV_IMP.1	zahrnuté
ATE_COV.2 Analysis of coverage	ADV_FSP.1 ATE_FUN.1	zahrnuté ADV_FSP.2 zahrnuté
ATE_DPT.1 Testing – high-level design	ADV_HLD.1 ATE_FUN.1	zahrnuté ADV_HLD.2 zahrnuté
ATE_FUN.1 Functional testing	<i>žiadne závislosti</i>	
ATE_IND.2 Independent testing – sample	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1	zahrnuté ADV_FSP.2 zahrnuté zahrnuté zahrnuté
AVA_MSU.2 Validation of analysis	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	zahrnuté zahrnuté ADV_FSP.2 zahrnuté zahrnuté
AVA_SOF.1 Strength of TOE security function evaluation	ADV_FSP.1  ADV_HLD.1	zahrnuté ADV_FSP.2  zahrnuté ADV_HLD.2
AVA_VLA.2 Independent vulnerability analysis	ADV_FSP.1  ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 AGD_ADM.1 AGD_USR.1	zahrnuté ADV_FSP.2  zahrnuté zahrnuté zahrnuté zahrnuté zahrnuté

Tabuľka 4.23: Závislosti medzi požiadavkami na záruky – úroveň bezpečnosti 4.

Požiadavka na záruky	Závisí na	Stav
ACM_AUT.1 Partial CM automation	ACM_CAP.3	zahrnuté ACM_CAP.4
ACM_CAP.4 Generation support and acceptance procedures	ACM_SCP.1	zahrnuté ACM_SCP.2

Tabuľka 4.23: (pokračovanie)

Požiadavka na záruky	Závisí na	Stav
	ALC_DVS.1	zahrnuté
ACM_SCP.2 Problem tracking CM coverage	ACM_CAP.3	zahrnuté ACM_CAP.4
ADO_DEL.2 Detection of modification	ACM_CAP.3	zahrnuté ACM_CAP.4
ADO_IGS.1 Installation, generation, and start-up procedures	AGD_ADM.1	zahrnuté
ADV_FSP.2 Fully defined external interfaces	ADV_RCR.1	zahrnuté
ADV_HLD.2 Security enforcing high-level design	ADV_FSP.1	zahrnuté ADV_FSP.2
	ADV_RCR.1	zahrnuté
ADV_IMP.1 Subset of the implementation of the TSF	ADV_LLD.1	zahrnuté
	ADV_RCR.1	zahrnuté
	ALC_TAT.1	zahrnuté
ADV_LLD.1 Descriptive low-level design	ADV_HLD.2	zahrnuté
	ADV_RCR.1	zahrnuté
ADV_RCR.1 Informal correspondence demonstration	<i>žiadne závislosti</i>	
ADV_SPM.1 Informal TOE security policy model	ADV_FSP.1	zahrnuté ADV_FSP.2
AGD_ADM.1 Administrator guidance	ADV_FSP.1	zahrnuté ADV_FSP.2
AGD_USR.1 User guidance	ADV_FSP.1	zahrnuté ADV_FSP.2
ALC_DVS.1 Identification of security measures	<i>žiadne závislosti</i>	
ALC_FLR.3 Systematic flaw remediation	<i>žiadne závislosti</i>	
ALC_LCD.1 Developer defined life-cycle model	<i>žiadne závislosti</i>	
ALC_TAT.1 Well-defined development tools	ADV_IMP.1	zahrnuté
ATE_COV.2 Analysis of coverage	ADV_FSP.1	zahrnuté ADV_FSP.2
	ATE_FUN.1	zahrnuté
ATE_DPT.2 Testing: low-level design	ADV_HLD.2	zahrnuté
	ADV_LLD.1	zahrnuté
	ATE_FUN.1	zahrnuté
ATE_FUN.1 Functional testing	<i>žiadne závislosti</i>	
ATE_IND.2 Independent testing – sample	ADV_FSP.1	zahrnuté ADV_FSP.2
	AGD_ADM.1	zahrnuté
	AGD_USR.1	zahrnuté
	ATE_FUN.1	zahrnuté
AVA_MSU.2 Validation of analysis	ADO_IGS.1	zahrnuté
	ADV_FSP.1	zahrnuté ADV_FSP.2
	AGD_ADM.1	zahrnuté
	AGD_USR.1	zahrnuté

Tabuľka 4.23: (pokračovanie)

Požiadavka na záruky	Závisí na	Stav
AVA_SOF.1 Strength of TOE security function evaluation	ADV_FSP.1	zahrnuté ADV_FSP.2
	ADV_HLD.1	zahrnuté ADV_HLD.2
AVA_VLA.3 Moderately resistant	ADV_FSP.1	zahrnuté ADV_FSP.2
	ADV_HLD.2	zahrnuté
	ADV_IMP.1	zahrnuté
	ADV_LLD.1	zahrnuté
	AGD_ADM.1	zahrnuté
	AGD_USR.1	zahrnuté

#### 4.6.6 Zdôvodnenie požiadaviek na záruky

##### Úroveň bezpečnosti 1

EAL pre túto úroveň je EAL 1 augmented. Augmentáciu predstavuje požiadavka **ATE\_FUN.1 Functional testing**. V Common Criteria je ATE\_FUN.1 zaradený až do EAL 2. Zníženie pravdepodobnosti neodhalených chýb v TSF je však natoľko dôležité, že túto požiadavku kladieme aj na tejto úrovni bezpečnosti.

##### Úroveň bezpečnosti 2

EAL pre túto úroveň je EAL 2 augmented (EAL-CSPP). Dôvody augmentácie EAL-CSPP oproti EAL 2 sú uvedené v [NIST99], explicitne uvedieme argumentáciu pre požiadavky prekračujúce EAL 3.

**ACM\_SCP.2 Problem tracking configuration management coverage**. Keďže hlavnou úlohou navrhovaného systému je práve zaistiť bezpečnosť interných dát, sledovanie bezpečnostných chýb je rozumná požiadavka.

**ADV\_SPM.1 Informal TOE security policy model** predstavuje jednorázovú činnosť, ktorá inak nezasahuje do procesu vývoja systému. Zaradená je aj kvôli splneniu závislosti **FMT\_MSA.2 Secure security attributes**.

**ALC\_FLR.2 Flaw Report Procedures** nie je zaradená v žiadnom EAL. V praxi býva dobrým zvykom poskytnúť používateľom jasne definovaný postup oznamovania nájdených chýb, ktorý následne vedie k ich opraveniu a

upozorneniu používateľov na opravu. Táto požiadavka nedefinuje konkrétne postupy, preto by jej dopad na dodávateľov, ktorí už majú spravený postup oznamovania chýb, mal byť minimálny. ALC\_FLR.2 plní bezpečnostný cieľ **O.Oprava identifikovaných bezpečnostných chýb**.

**AVA\_MSU.2 Validation of analysis** Táto požiadavka by v praxi nemala mať prílišný dopad. Vyžaduje, aby dodávateľ spravil dokumentáciu pre používateľov a administrátorov na úrovni adekvátnej na pochopenie fungovania TOE a externých kontrol potrebných na jeho bezpečnú prevádzku. Túto dokumentáciu je následne povinný analyzovať s účelom odhaliť a odstrániť všetky nepresné a zavádzajúce informácie.

### Úroveň bezpečnosti 3

EAL pre túto úroveň je EAL 3 augmented. Obsahuje všetky požiadavky na záruky z EAL-CSPP (EAL pre úroveň bezpečnosti 2), zdôvodnenie pre komponenty prekračujúce EAL 3 zostáva nezmenené. Pridáva sa niekoľko nových požiadaviek, ktoré CC zaraďuje až do EAL 4. Zdôvodnenie tejto augmentácie:

**ADV\_FSP.2 Fully defined external interfaces.** Nejde o náročnú požiadavku, plná definícia externých rozhraní je aj tak nutná pri korektnom vývoji produktu. Jej prínosom bude pomoc pri testovaní TOE a pri hľadaní zraniteľností.

**AVA\_VLA.2 Independent vulnerability analysis.** Na tejto úrovni bezpečnosti sa už zaoberáme útokmi s cieľom preniknúť do prostredia. Dopad z prípadného úspechu takéhoto útoku už nie je zanedbateľný. Kvôli tomu je nutné vykonať aspoň nejaké testy a analýzu odolnosti voči takýmto útokom.

**ADV\_IMP.1 Subset of the implementation of the TSF** je začlenená kvôli splneniu závislosti **AVA\_VLA.2 Independent vulnerability analysis**. Táto požiadavka poskytne podrobnejšiu dokumentáciu o realizácii časti TSF, ktorá pomôže pri vyššie spomínanej analýze odolnosti voči útokom.

**ADV\_LLD.1 Descriptive low-level design** je začlenená kvôli splneniu závislosti predchádzajúcich požiadaviek. Táto požiadavka poskytne podrobnejšiu dokumentáciu o dizajne systému, ktorá pomôže pri vyššie spomínanej analýze odolnosti voči útokom.

**ALC\_TAT.1 Well-defined development tools** už vďaka začleneniu predchádzajúcich požiadaviek má splnené všetky závislosti. Keďže bezpečnosť navrhovaného systému je prvoradou požiadavkou, je rozumné vyžadovať už na tejto úrovni bezpečnosti, aby bol význam implementácie jednoznačný.

#### Úroveň bezpečnosti 4

EAL pre túto úroveň je EAL 4 augmented. Augmentácia pochádza zo začlenenia troch komponentov z EAL 5 a komponentu ALC\_FLR.3, ktorý nie je začlenený v žiadnom EAL. Zdôvodnenie tejto augmentácie:

**ALC\_FLR.3 Systematic Flaw Remediation** vyžaduje po dodávateľovi riešiť problémy nahlásené používateľmi, identifikovať a opravovať chyby, automaticky distribuovať správy o bezpečnostných chybách a ich oprave a realizovať kontroly, ktoré znížia potenciál vzniku nových chýb, ALC\_FLR.3 plní bezpečnostný cieľ **O.Oprava identifikovaných bezpečnostných chýb**.

**AVA\_VLA.3 Moderately resistant.** Na tejto úrovni bezpečnosti sa zaoberáme vážnymi hrozbami a dopad z prípadného poškodenia integrity a/lebo dôvernosti dát je vysoký. Nepriateľské môže byť nielen prostredie, ale aj autorizovaní používatelia. Kvôli tomu musí TOE byť odolný voči útokom s cieľom preniknúť do systému. Oproti AVA\_VLA.2 (ktorý je vyžadovaný na EAL 4) vyžaduje AVA\_VLA.3 navyše aby bolo vykonávané a prezentované systematické vyhľadávanie zraniteľností systému. Toto predstavuje značné zvýšenie záruk oproti AVA\_VLA.2.

**ATE\_DPT.2 Testing: low-level design.** Podobné dôvody nás vedú aj k začleneniu tejto požiadavky. Je potrebné otestovať bezpečnostné funkcie na low-level úrovni. ATE\_DPT.2 zvyšuje oproti ATE\_DPT.1 úroveň podrobnosti, s akou musia byť tieto testy spravené. Okrem zníženia pravdepodobnosti výskytu neodhalených chýb sa zvyšuje aj pravdepodobnosť odhalenia vloženého nepriateľského kódu. Testovanie na úrovni subsystémov dodá záruky, že každý subsystém funguje správne.

## 4.7 Použité skratky

**AES:** Advanced Encryption Standard (šifrovací algoritmus), [NIST01a].

**CA:** certifikačná autorita

**CC:** Common Criteria, [CC99].

**DES:** Data Encryption Standard (šifrovací algoritmus).

**EAL:** Evaluation Assurance Level, úroveň poskytovaných záruk

**FIPS:** Federal Information Processing Standard, štandard spracúvania informácií v USA.

**FMFI UK:** Fakulta matematiky, fyziky a informatiky Univerzity Komenského

**IKT:** informačno-komunikačné technológie

**IT:** informačné technológie

**ISO:** International Organization for Standardization, Medzinárodná organizácia pre štandardizáciu

**NIST:** National Institute for Standards and Technology, Národný inštitút pre štandardy a technológie v USA.

**PP:** Protection Profile – profil ochrany (tento dokument)

**RSA:** Rivest-Shamir-Adleman cipher (šifrovací algoritmus), [RSA78]

**ST:** Security Target, bezpečnostný zámer

**TMS:** Time-Marking Service – služba časových značiek

**TOE:** Target of Evaluation – navrhovaný IKT systém

**TSC:** TOE Scope of Control – oblasť spadajúca pod kontrolu systému

**TSS:** Time-Stamping Service – služba časových pečiatok

**TSF:** TOE Security Functions – funkcie zaisťujúce bezpečnosť systému

**TSP:** TOE Security Policy – bezpečnostná politika systému

**Z.z.:** Zbierka zákonov



# Kapitola 5

## Ostatné hľadiská bezpečnosti

Common Criteria sa sústreďujú len na špecifikáciu bezpečnostných požiadaviek kladených na samotný IT systém a jeho IT okolie. Nezaoberajú sa inými hľadiskami bezpečnosti, ako je napríklad personálna politika, legislatíva a pod. V tejto kapitole sa budeme stručne zaoberať ostatnými hľadiskami, na ktoré treba myslieť pri zabezpečení funkčnosti a bezpečnosti nášho IT systému. Väčšina uvedených tém je podrobnejšie rozpracovaná v [BS00].

### 5.1 Organizačná bezpečnosť

#### Infraštruktúra zaisťujúca bezpečnosť

V rámci organizácie je potrebné vytvoriť vhodnú infraštruktúru, ktorej cieľom bude kontrolovať implementáciu informačnej bezpečnosti v organizácii. Vhodný orgán v rámci organizácie by mal rozhodovať o bezpečnostnej politike, prideliť zamestnancom bezpečnostné roly a koordinovať ďalšiu implementáciu informačnej bezpečnosti. Môže byť potrebné, aby organizácia nadviazala kontakt s externými špecialistami kvôli udržaniu kroku s rozvojom vedy. Takisto môže byť vhodné nadviazať kontakt s externými expertmi na bezpečnosť kvôli nezávislej kontrole bezpečnosti (napríklad penetračnému testovaniu), bezpečnostnému auditu, prípadne riešeniu bezpečnostných problémov.

Pre každé z aktív organizácie by mali byť jasne a jednoznačne určení zamestnanci zodpovední za jeho ochranu a vykonávanie s tým spojených bezpečnostných procesov. Bezpečnostná politika organizácie by mala obsa-

hovať všeobecné pokyny určujúce právomoci a zodpovednosti jednotlivých zamestnancov.

## Prístup tretej strany a outsourcing

V prípade, že k interným údajom organizácie má (fyzický alebo logický) prístup tretia strana, je potrebné zaistiť ich bezpečnosť proti nej. Prístup tretej strany k interným údajom musí byť kontrolovaný. Je potrebné vykonať analýzu rizík vyplývajúcich z umožnenia prístupu k údajom a z nej vyvodíť príslušné bezpečnostné opatrenia. Tieto by mali byť odsúhlasené a zmluvne schválené uvedenou treťou stranou.

V niektorých situáciách môže byť dokonca nutný outsourcing – prenechanie spracúvania údajov tretej strane. Tieto údaje pritom opúšťajú organizáciu. V takomto prípade je nutné zmluvne zabezpečiť dôvernosc spracúvaných údajov. Zmluva o outsourcingu má z hľadiska outsourcingujúcej organizácie za úlohu minimalizovať riziko z prípadných chýb a/lebo nepriateľských akcií tretej strany spracúvajúcej údaje. Mala by obsahovať okrem iného nasledujúce údaje: Zabezpečenia údajov počas doby, kedy sú mimo organizácie, postihy pre spracúvajúcu stranu v prípade porušenia dôvernosti údajov, právo auditu pre outsourcingujúcu organizáciu.

## 5.2 Klasifikácia a zabezpečenie aktív

Úlohou klasifikácie informácií je zabezpečiť, aby každé z informačných aktív bolo chránené primerane k jeho obsahu. Informácie môžu vyžadovať rôznu stupeň utajenia, mať rôzne požiadavky na dostupnosť, môže byť nutné zachovať ich integritu a pod. Niektoré informácie môžu vyžadovať špeciálne zaobchádzanie. Preto by mal byť v rámci organizácie vyvinutý systém klasifikácie informácií, ktorý každú informáciu stručne ale jednoznačne označí požiadavkami na manipuláciu s ňou.

Ako sme už spomínali v kapitole 3, jednu možnosť ponúka FIPS 199 [NIST03b]. Podľa neho je každému dokumentu priradený vektor informácií, ktoré udávajú stupne požiadavok na zachovanie jeho dôvernosti, integrity a dostupnosti. Stupeň požiadavky môže byť N/A (nedá sa aplikovať), nízky, stredný a vysoký.

Logicky súvisiacim krokom s klasifikáciou informácií je samotná implementácia rôznych úrovní ochrany informačných aktív, kde úrovne ochrany

zodpovedajú rastúcim požiadavkám na bezpečnosť, špecifikovaným pri klasifikácii informácií. Obzvlášť pre vyššie úrovne bezpečnosti môže byť potrebné jednoznačne definovať postupy na ukladanie, kopírovanie, prenos (elektronickou aj klasickou cestou) a zničenie takýchto informácií.

## 5.3 Personálna bezpečnosť

Jednou z úloh personálnej bezpečnosti je znížiť riziko ľudskej chyby, krádeže, podvodu, zneužitia a pod. V prípade organizácie realizujúcej IT systém to v prvom rade znamená zahrnúť zodpovednosť za ochranu informačných aktív do popisu zamestnania. Následne aj v pracovnej zmluve musia byť tieto zodpovednosti zahrnuté spolu s postihmi v prípade ich nedodržania.

Pri prijímaní zamestnanca je potrebné vykonať dostatočnú kontrolu jeho odbornej spôsobilosti a prípadnej praxe v danej oblasti. V prípade práce s dôvernými údajmi je potrebné, aby pracovník po prijatí podpísal zmluvu o utajovaní pracovných dokumentov.

Riziko ľudskej chyby vieme najlepšie znížiť prostredníctvom dostatočného školenia zamestnancov. Témou takéhoto školenia môžu byť napríklad samotné bezpečnostné procedúry pri spracúvaní informácií, obsluha jednotlivých nástrojov na ich spracúvanie (napr. konkrétneho počítačového programu) a pod. Zamestnanci by mali vedieť, ako reagovať pri neželaných situáciách, ako sú odhalenie zraniteľnosti systému, prípadne jeho napadnutia, odhalenie chyby v používanom softvéri a podobne.

## 5.4 Fyzická bezpečnosť

Ak organizácia realizuje IT systém spracúvajúci informácie, u ktorých je dôležité zachovanie integrity a/lebo dôvernosti, je potrebné tento IT systém chrániť pred fyzickým prístupom nepovolaných osôb. Základným krokom je definovanie bezpečnostných okruhov okolo miest, kde sú uložené citlivé informácie. Bezpečnostný okruh je tvorený fyzickou prekážkou, zabraňujúcou nekontrolovaný prístup dovnútra (napr. steny miestnosti alebo budovy) a oprávneným človekom a/lebo mechanizmom kontrolovaným vstupom. Je potrebné jasne definovať a správne kontrolovať prístupové práva pre každý bezpečnostný okruh.

Fyzickú časť IT systému je potrebné chrániť nielen pred neoprávneným

prístupom, ale aj pred poškodením. Už sme spomínali školenia zamestnancov, ktoré znížia riziko poškodenia nesprávnym zaobchádzaním. Sú potrebné opatrenia napríklad proti poškodeniu ohňom, prachom a pod. Môže byť vhodné používať záložné zdroje a minimalizovať tak riziko straty informácií pri výpadku elektrického prúdu.

Zaujímavý detail, na ktorý netreba zabúdať, je fyzické zničenie uložených informácií. Často je žiadané, aby dáta, ktoré prestali byť aktuálne (napr. dokument, ktorému skončila doba archivácie, identifikačné údaje prepusteného pracovníka a pod.), boli fyzicky odstránené. Niektoré operačné systémy však ponúkajú možnosť obnovenia zmazaných súborov – tie sú ešte dlhšiu dobu po „zmazaní“ fyzicky zaznamenané na príslušnom pamäťovom médiu. U magnetických pamätí dochádza dokonca k tzv. pamäťovému efektu, kedy sa môžu dať pôvodné dáta obnoviť aj po tom, ako boli prepísané novými. Je preto potrebné zaručiť, že v prípade potreby budú dôverné dáta naozaj zmazané. Podrobnejšie sa touto problematikou zaoberá napr. [Gut96].

Takisto v prípade vyradovanie hardvéru je potrebné prekontrolovať, či neobsahuje žiadne dôverné informácie a prípadne ich pred vyradením bezpečne odstrániť.

V rámci organizácie spracúvajúcej dôverné informácie je potrebné dodržiavať tzv. politiku čistého stola. Zamestnanec je povinný zabezpečiť, aby pri jeho odchode z priestorov organizácie boli všetky informačné aktíva uložené na určených zabezpečených miestach. Na žiadnom z počítačov, resp. terminálov nesmie zostať prihlásený.

Do fyzickej bezpečnosti patrí aj oblasť, ktorá je veľmi zaujímavá práve pre archívy elektronických dokumentov, kde sa digitálna informácia uložená na pevných médiách skladuje počas dlhej doby. Životnosť niektorých médií používaných v dnešnej dobe sa meria len na desiatky rokov. Existujú postupy, ako ich životnosť predĺžiť, resp. správnym skladovaním neznížiť. V prípade končiacej životnosti média je potrebné údaje z neho bezpečne presunúť na nové médium.

Podrobnejšie sa vyhodnotením životnosti médií a možných postupov na jej predĺženie zaoberá napríklad práve prebiehajúci Data Preservation Program v NISTe (<http://www.itl.nist.gov/div895/isis/datastorage.html>). Už boli vypracované viaceré štúdie životnosti médií (napr. [LoCb]) a postupov starostlivosti o ne (napr. [LoCa]).

## 5.5 Kontrola prístupu

Prístup k informáciám by mal byť kontrolovaný podľa požiadaviek na ich bezpečnosť a iných požiadaviek vyplývajúcich z obchodných vzťahov. Pravidlá prístupu by mali byť formulované v pozitívnom zmysle, t.j. vo všeobecnosti je prístup k danej informácii zamietnutý a jednotlivé pravidlá ho môžu niektorým subjektom povoliť. (Opačná formulácia, t.j. „všetko, čo nie je zakázané, je povolené“, často vedie k bezpečnostným problémom.)

Môže byť potrebné spraviť formálne procesy registrácie a rušenia registrácie používateľov. V rámci procesu registrácie sa napr. overí a zaznamená identita používateľa (a prípadne jeho právo využívať služby systému), v rámci systému sa mu prideli jednoduše identifikátor (UID), vygeneruje sa mu používateľské konto a pod. Súčasťou procesu registrácie by mal byť krok, kedy je používateľ oboznámený so zmluvou, obsahujúcou práva a povinnosti vyplývajúce z registrácie a následne túto zmluvu potvrdí.

Jedným z najbežnejších spôsobov identifikácie používateľa sú heslá. Zamestnanci by mali byť zodpovední za utajenie svojich hesiel a ich dostatočnú bezpečnostnú úroveň. Utajenie zahŕňa okamžitú zmenu v prípade možnej kompromitácie, neuchovávanie papierovej kópie hesla, nezahŕňanie hesla do automatických prihlasovacích procesov a podobne. V prípade vytvorenia nového konta, prípadne zabudnutého hesla dostane používateľ nové dočasné heslo – toto by však malo mať obmedzenú dĺžku platnosti a musí mu byť doručené bezpečným spôsobom.

Pri pripojeniach prostredníctvom počítačovej siete zvonka (t.j. nie z priestorov organizácie) môže byť potrebná autentifikácia používateľa napr. prostredníctvom vhodného kryptografického tokenu.

Je potrebné v pravidelných intervaloch robiť kontrolu prístupových práv používateľov s cieľom odhaliť prípadné chyby administrátorov a/lebo neoprávnené získania prístupových práv využitím zraniteľnosti systému.

Prístup k zariadeniam prostredníctvom počítačovej siete je potrebné vo všeobecnosti zakázať a povoliť ho len používateľom, ktorí na to majú dôvod a oprávnenie.



# Kapitola 6

## Záver

Hlavným výsledkom tejto práce je vytvorenie štyroch profilov ochrany pre archív elektronických dokumentov. Tieto profily ochrany sú odstupňované podľa úrovne bezpečnosti, ktorú ponúkajú. Vyššia úroveň bezpečnosti samozrejme predstavuje viac požiadaviek na funkcie, ktoré musí systém vykonávať a na záruky, ktoré musí poskytovať. Z praktického hľadiska je dôležité, že zvýšenie bezpečnostných požiadaviek sa prejaví aj na cene realizácie takéhoto systému.

Nami navrhovaná škála štyroch odstupňovaných profilov ochrany by mala byť dostatočná na to, aby si konzument, ktorý potrebuje realizovať archív elektronických dokumentov, mohol na základe svojich potrieb, prostredia, v ktorom archív bude fungovať a svojich finančných možností zvoliť vhodný profil ochrany. Je samozrejme možné v prípade potreby vytvoriť aj kompromis medzi nami vypracovanými možnosťami, a to zvolením niektorého profilu ochrany a pridaním opodstatnených požiadaviek z vyšších úrovní bezpečnosti doň.

Logicky ďalším krokom pri realizácii konkrétneho archívu elektronických dokumentov bude doplnenie nami vypracovaného profilu ochrany na bezpečnostný zámer. Na to je potrebné navrhnúť konkrétnu hardvérovú a softvérovú realizáciu jednotlivých operácií a ukázať, že spĺňa požiadavky kladené vo zvolenom profile ochrany. Podľa tohto bezpečnostného zámeru sa následne zostrojí konkrétny archív elektronických dokumentov.

Témy rozpracované v kapitole 5 sme rozpracovali len orientačne, pre prevádzkovateľa archívu elektronických dokumentov by bolo potrebné zaoberať sa týmito témami podrobnejšie, keďže sú pre bezpečné fungovanie archívu elektronických dokumentov rovnako dôležité ako samotná informačná bez-

pečnosť.

Pri našom návrhu sme viaceré témy uviedli ako predpoklady. Pri realizácii archívu elektronických dokumentov v praxi sa môže ukázať, že niektorý z týchto predpokladov nebude splnený. V takomto prípade bude pravdepodobne potrebné príslušný profil ochrany doplniť o ďalšie funkčné požiadavky a požiadavky na záruky, ktoré zabezpečia platnosť nášho predpokladu.

# Dodatok A

## Slovníček pojmov z informačnej bezpečnosti

**Access (prístup)** (1) Špecifický typ interakcie medzi subjektom a objektom, ktorého výsledkom je tok informácií od jedného k druhému. (2) Schopnosť a prostriedky potrebné na dosiahnutie, uloženie alebo získanie údajov; na komunikáciu s alebo použitie nejakého zdroja IKT systému.

**Access control (riadenie prístupu)** (1) Ohraničenie práv alebo možností subjektu komunikovať s inými subjektmi alebo používať funkcie alebo služby IKT systému. (2) Obmedzenia riadiace prístup subjektu k objektu.

**Access right (prístupové právo)** Povolenie uskutočňovať nejaký typ prístupu (access type) udelené subjektu alebo objektu

**Access type (typ prístupu)** Špecifický typ interakcie ktorý možno uplatniť na nejakom objekte.

**Accountability (zodpovednosť)** Vlastnosť alebo stav IKT systému umožňujúca priradiť činnosti uskutočňované v systéme jednotlivcom, ktorých potom možno za ne brať na zodpovednosť. Činnosti zahŕňajú porušenia a pokusy o porušenia bezpečnostnej politiky ako aj povolené činnosti.

**Administrator (administrátor)** Osoba, ktorá je v kontakte s IKT systémom a je zodpovedná za udržiavanie jeho operačných schopností.

**Assets (aktíva)** Údaje, ktoré majú pre danú organizáciu hodnotu. Úlohou informačnej bezpečnosti je identifikovať hrozby proti nim a realizovať opatrenia na ich ochranu.

**Assurance (záruka)** Stupeň dôvery v to, že IKT systém adekvátne splna bezpečnostné požiadavky. Dva hlavné aspekty záruk sú efektívnosť a korektnosť.

**Assurance level (úroveň záruk)** Preddefinovaná množina komponentov záruk, ktorá priraduje mieru vlastnej bezpečnostnej kvality IKT systému. Ak IKT systém dosahuje nejakú úroveň záruk, znamená to že sa na IKT systém použili všetky prostriedky záruk (assurance measures) prislúchajúce danej úrovni.

- Attack (útok)** Pokus o obídenie bezpečnostných mechanizmov IKT systému. Môže byť aktívny (narušenie údajov) alebo pasívny (získanie údajov).
- Audit (audit)** Nezávislé skúmanie a vyhodnotenie záznamov a aktivít za účelom určenia súladu s definovanými pravidlami a zistenia prípadných nedostatkov v bezpečnostnej politike IKT systému alebo jej uplatňovaní.
- Authentication (autentifikácia)** (1) Overenie identity používateľa, zariadenia alebo inej entity. (2) Overenie integrity uložených, prenášaných údajov, alebo údajov iným spôsobom vystavených možnosti neoprávnenej modifikácie v IKT systéme.
- Autorization (autorizácia)** Udelenie prístupových práv pre používateľa, program alebo proces.
- Availability (dostupnosť)** Požiadavka, aby informácia a iné zdroje systému boli prístupné oprávneným používateľom bez zbytočného zdržania vtedy, keď to je potrebné.
- Certification (certifikácia)** Vyčerpávajúca evaluácia technických a netechnických bezpečnostných rysov systému, ktorá sa robí ako časť, alebo na podporu procesu schvaľovania/akreditácie. Stanovuje rozsah, v ktorom sa konkrétny návrh a implementácia zhoduje so zadanou množinou bezpečnostných požiadaviek.
- Channel (kanál)** Cesta v systéme, slúžiaca na prenos údajov. Môže tiež predstavovať mechanizmus, prostredníctvom ktorého sa cesta realizuje.
- Compromise (kompromitácia)** Narušenie bezpečnosti systému, ktoré môže viesť k odhaleniu citlivej informácie.
- Confidentiality (dôvernosť)** Bezpečnostný atribút vyjadrujúci to, že obsah správy, údajov nie je odhalený nepovolanej osobe, procesu, entite alebo organizácii.
- Configuration (konfigurácia)** Výber jednej z možných kombinácií parametrov systému.
- Configuration control (riadenie konfigurácie)** Manažment zmien hardvéru, softvéru, firmvéru a dokumentácie systému v priebehu jeho vývoja a celého životného cyklu.
- Configuration management (manažment konfigurácie)** Manažment bezpečnostných charakteristík a záruk systému prostredníctvom zmien hardvéru, softvéru, firmvéru, dokumentácie, testov a ich dokumentácie v priebehu vývoja a životného cyklu systému.
- Contingency plan (plán na zachovanie kontinuity činnosti)** Plán reakcií na mimoriadne situácie, operácie zálohovania a obnovy systému po havárii, ktorý je súčasťou bezpečnostného programu organizácie. Jeho cieľom je zaistiť dostupnosť kritických zdrojov a umožniť kontinuitu operácií systému v núdzových situáciách.
- Cost-risk analysis (analýza rizík a nákladov)** Odhad nákladov na ochranu údajov v systéme v porovnaní s ujmou spôsobenou stratou alebo kompromitáciou údajov.
- Countermeasure (protiopatrenie)** Činnosť, zariadenie, procedúra, technika alebo iný prostriedok, ktorý redukuje zraniteľnosť systému nejakou hrozbou.

- Covert Channel (skrytý kanál)** Komunikačný kanál, ktorý umožňuje nejakému procesu prenášať informácie spôsobom, ktorá je v rozpore s bezpečnostnou politikou systému.
- Data (údaje)** Informácia v špecifickej fyzickej reprezentácii.
- Data confidentiality (dôvernosť údajov)** Bezpečnostný atribút údajov, ktorý vyjadruje, že údaje sú chránené pred neoprávneným odhalením.
- Data integrity (integrita údajov)** Bezpečnostný atribút údajov, ktorý vyjadruje, že údaje sú chránené pred neoprávnenou modifikáciou alebo zničením.
- Data security (bezpečnosť údajov)** Ochrana údajov pred neoprávnenou (neúmyselnou alebo zámernou) modifikáciou, zničením alebo odhalením.
- Denial of service (odmietnutie služby)** Zabránenie autorizovanému prístupu k nejakej položke alebo službe systému, alebo oneskorenie časovo kritickej operácie.
- Environment (prostredie)** Všetko (používatelia, procedúry, objekty, podmienky, iné systémy), čo má vplyv na systém.
- Evaluation (evaluácia)** Odborné technické posúdenie vlastností skúmaného systému, ktorého cieľom je určiť, či skúmaný systém vyhovuje stanoveným požiadavkám.
- Formal (formálny)** Založený na jednoznačnej syntaxi a sémantike.
- Formal proof (formálny dôkaz)** Matematický dôkaz.
- Formal Security Policy Model (formálny model bezpečnostnej politiky)** Matematicky presná formulácia bezpečnostnej politiky. Aby bol dostatočne presný, takýto model musí reprezentovať počiatočný stav systému, spôsob, akým systém prechádza z jedného stavu do druhého a definíciu „bezpečného“ stavu systému. Musí sa dať formálne dokázať, že ak počiatočný stav systému vyhovuje definícii bezpečného stavu a ak sú všetky požiadavky, ktoré model vyžaduje, splnené, tak potom budú aj všetky nasledujúce stavy systému bezpečné.
- Formal specification (formálna špecifikácia)** Popis systému používajúci obmedzenú syntax a gramatiku formálneho logického systému a množinu termínov, ktoré boli presne definované alebo špecifikované.
- Formal verification (formálna verifikácia)** Proces používajúci formálne dôkazy na demonštráciu konzistencie (verifikácia návrhu) medzi formálnou špecifikáciou systému a formálnym modelom bezpečnostnej politiky alebo medzi formálnou špecifikáciou a implementáciou systému (verifikácia implementácie).
- Functional testing (funkcionálne testovanie)** Časť bezpečnostného testovania, pri ktorom sa deklarované rysy systému testujú na korektnosť operácií.
- Functionality (funkcionalita)** Množina funkcionálnych bezpečnostných požiadaviek, ktorá sa má implementovať v IKT systéme.
- Granularity (granularita)** Rozlišovacia úroveň, na ktorú možno nejaký mechanizmus nastaviť.

**Identification (identifikácia)** Proces, ktorý umožňuje IKT systému rozpoznať nejakú entitu.

**Implementation (implementácia)** Fáza vývojového procesu systému, v ktorej sa detailná špecifikácia systému realizuje pomocou hardvéru a softvéru.

**Individual accountability (individuálna zodpovednosť)** Schopnosť systému spojiť identitu používateľa s časom, metódou a stupňom prístupu k systému.

**Informal (neformálny)** Vyjadrený v prirodzenom jazyku.

**Informal specification (neformálna špecifikácia)** Popis/špecifikácia systému v prirodzenom jazyku.

**Least privilege (najmenšie privilégium)** Princíp, ktorý vyžaduje, aby každý subjekt dostal najmenšie možné oprávnenia, ktoré postačujú pre výkon jeho úloh.

**Need-to-know principle** Princíp, ktorého uplatňovanie znamená, že subjekt má prístup, pozná alebo vlastní iba špecifické informácie, potrebné pre výkon jeho oficiálnych povinností.

**Object (objekt)** Pasívna entita, ktorá obsahuje alebo dostáva informáciu. Z prístupu k objektu vyplýva aj prístup k informácii, ktorú objekt obsahuje.

**Object reuse (opätovné použitie objektu)** Priradenie a opätovné použitie pamäťového média (napr. rámca stránky, sektora disku, magnetickej pásky) ktoré už obsahovalo nejaké objekty. Aby sa pamäťové médiá dali bezpečne znova použiť, nesmú obsahovať zvyšky údajov predchádzajúcich objektov, ktoré boli na nich uložené.

**Organizational Security Policy (Organizačná bezpečnostná politika)** Súbor právnych noriem, pravidiel a praktík, ktoré upravujú spôsob, ako organizácia manažuje, ochraňuje a distribuuje citlivú informáciu.

**Password (heslo)** Chránený/súkromný reťazec znakov, ktorý slúži na overenie identity alebo na autorizovanie prístupu k údajom.

**Penetration (prienik)** Úspešné obídenie bezpečnostných mechanizmov systému.

**Penetration testing (penetračné testovanie)** Časť bezpečnostného testovania, pri ktorej sa hodnotiaci pokúša obísť bezpečnostné mechanizmy systému. Predpokladá sa, že hodnotiaci môže používať kompletnú dokumentáciu systém, ale ináč pracuje v tých istých podmienkach ako obyčajný používateľ.

**Permissions (povolenia)** Popis typov oprávnených interakcií subjektu s objektom. Príklady: čítanie, zápis, vykonávanie, pridávanie, modifikácia a odstraňovanie.

**Personnel security (personálna bezpečnosť)** Procedúry prijaté na zabezpečenie toho, že personál, ktorý má prístup k citlivým informáciám, má na to aj príslušné oprávnenia.

**Physical security (fyzická bezpečnosť)** Použitie fyzických prekážok a kontrolných procedúr ako preventívnych opatrení a protiopatrení proti hrozbám.

- Privacy (súkromie)** (1) Schopnosť jednotlivca alebo organizácie kontrolovať zbieranie, uchovávanie, zdieľanie a šírenie informácie o svojej osobe alebo organizácii. (2) Právo jednotlivca na ochranu informácie osobného charakteru a na definovanie oprávnených používateľov tejto informácie a spôsobu jej použitia.
- Privilege (privilégium)** Špeciálne oprávnenie, pridelené konkrétnemu používateľovi na vykonávanie bezpečnostne relevantných operácií.
- Profile (profil)** Podrobný bezpečnostný popis fyzickej štruktúry, komponentov, umiestnenia, vzťahov, a všeobecného operačného prostredia systému.
- Protection profile (profil ochrany, PP)** Implementačne nezávislá špecifikácia bezpečnostných požiadaviek, ktoré má spĺňať množina možných produktov alebo systémov. Je to vysokoúrovňová abstrakcia bezpečnostného zámeru a obsahuje zdôvodnenia, funkcionálne požiadavky a požiadavky na záruky.
- Recovery procedures (procedúry obnovy)** Činnosti potrebné na obnovu výpočtových kapacít systému a dátových súborov po zlyhaní systému.
- Reliability (spoľahlivosť)** Rozsah, v ktorom sa dá očakávať, že systém plní svoje funkcie s požadovanou presnosťou.
- Resource (zdroj)** Čokoľvek, čo sa používa alebo spotrebováva pri plnení funkcie.
- Risk (riziko)** Očakávaná strata následkom uskutočnenia hrozby, zohľadňujúca slabé miesta systému a útočný potenciál nositeľa hrozby.
- Risk management (manažment rizík)** Celkový proces identifikácie, riadenia, eliminácie alebo minimalizácie neurčitých udalostí, ktoré môžu mať vplyv na zdroje systému. Zahŕňa analýzu rizík, analýzu cost-benefit, výber, implementáciu a testovanie, evaluáciu bezpečnosti opatrení a celkové posúdenie bezpečnosti.
- Role (rola)** Definovaný súbor funkcionálne príbuzných operácií a oprávnení potrebných na vykonávanie týchto operácií, ktoré môžu byť priradené používateľovi.
- Secure state (bezpečný stav)** Podmienka, za ktorej žiaden subjekt nemôže pristúpiť k nejakému objektu neoprávneným spôsobom.
- Security target (bezpečnostný zámer)** Produktovo špecifický popis, rozpracúvajúci všeobecnejšie požiadavky z protection profile, zahŕňajúci informácie/svedectvá výrobcov o tom, ako systém/produkt spĺňa požiadavky protection profile.
- Security testing (testovanie bezpečnosti)** Proces, ktorý sa používa na overenie toho, že bezpečnostné rysy systému sú implementované v súlade s návrhom a že sú adekvátne pre predpokladané aplikačné prostredie. Proces zahŕňa ručné testovanie, penetračné testovanie a verifikáciu.
- Sensitive information (citlivá informácia)** Informácia, ktorú určila oprávnená autorita a ktorá má byť chránená pred neoprávneným zverejnením, zmenou, stratou alebo zničením, ktoré by prinajmenšom spôsobili znateľnú škodu niekomu alebo niečomu.

**Subject (subjekt)** Aktívna entita (osoba, proces alebo zariadenie) ktorá spôsobuje tok informácie medzi objektmi alebo zmeny stavu systému.

**Threat (hrozba)** Činnosť alebo udalosť, ktorá môže ohroziť bezpečnosť systému.

**Validation (ohodnocovanie)** Proces ohodnocovania užitočnosti systému vzhľadom na jeho účel alebo zamýšľané použitie.

**Verification (overovanie)** Proces porovnávania dvoch špecifikácií systému rozličnej úrovne za účelom zistenia, či navzájom správne korešpondujú.

**Virus (vírus)** Samoreprodukujúci sa zlomyseľný segment programu, ktorý sa sám pripája k aplikácii, alebo inému vykonateľnému komponentu systému a nezanecháva vonkajšie stopy svojej prítomnosti.

**Vulnerability (zraniteľné miesto, zraniteľnosť)** Bezpečnostná slabina systému, ktorá sa dá použiť na narušenie bezpečnosti systému.

# Dodatok B

## Obsah priloženého CD

Na priloženom CD je uložená táto diplomová práca v elektronickej podobe. Okrem toho je na ňom uložená všetka citovaná literatúra, ktorá bola dostupná v elektronickej podobe. Uvedieme niekoľko prehľadných tabuliek, v ktorých ku každému súboru na CD uvedieme odkaz na literatúru, ktorú obsahuje.

Tabuľka B.1: Adresár /bezpecnost – citovaná literatúra z oblasti informačnej bezpečnosti.

Názov súboru	Odkaz
Certificate Issuing and Management Components PPs.pdf	[NIST01b]
Common Criteria Familiarization.ps	[CCo]
Common Criteria v2.1 part 1.pdf	[CCa99]
Common Criteria v2.1 part 2.pdf	[CCb99]
Common Criteria v2.1 part 3.pdf	[CCc99]
Cryptographic Communications System Protection Profile.pdf	[CCS00]
FIPS 140-2 Security Requirements for Cryptographic Modules.pdf	[NIST01d]
FIPS 199 - Standard for information classification (draft).pdf	[NIST03b]
NIST SP800-61 Computer Security Incident Handling Guide.pdf	[NIST04]
NISTIR-6462 Guidance for COTS Security Protection Profiles.pdf	[NIST99]
NISTIR-6985 COTS Security PP - Operating Systems.pdf	[NIST03a]
RSA Keon CA Security Target.pdf	[RSA02]
RedHat Enterprise Linux 3 Security Target.pdf	[LC04]
Smart Card Protection Profile.pdf	[SCSUG01]
Using Common Criteria Protection Profiles.ps	[CCP]

Tabuľka B.2: Adresár /kryptografia – citovaná literatúra z oblasti kryptografie.

Názov súboru	Odkaz
AES Proposal - Rijndael (ammended).pdf	[DR01]
FIPS 180-2 - Secure Hash Standard.pdf	[NIST02]
FIPS 186-2 Digital Signature Standard.pdf	[NIST01c]
FIPS 197 - Advanced Encryption Standard.pdf	[NIST01a]
RFC 1321 - The MD5 Message-Digest Algorithm.html	[Riv92]
RFC 3174 - US Secure Hash Algorithm 1 (SHA1).html	[Eas01]

Tabuľka B.3: Adresár /legislativa – zákony a vyhlášky.

Názov súboru	Odkaz
Vyhlaska 455-2001 o administratívnej bezpečnosti.html	[Zbi]
Vyhlaska 62-1976 o podnikových archívoch.html	[Zbi]
Vyhlaska 628-2002 o archívoch a registratúrach.pdf	[Zbi]
Zakon 149-1975 o archívniectve.html	[Zbi]
Zakon 215-2002 o elektronickom podpise.pdf	[Zbi]
Zakon 241-2001 o ochrane utajovaných skutočností.html	[Zbi]
Zakon 395-2002 o archívoch a registratúrach.pdf	[Zbi]
Zakon 428-2002 o ochrane osobných údajov.pdf	[Zbi]
Zakon 431-2002 o účtovníctve.pdf	[Zbi]
Zakon 433-2003 zákonník práce.pdf	[Zbi]

Tabuľka B.4: Adresár /ostatne – nezaraďené dokumenty.

Názov súboru	Odkaz
Adobe Portable Document Format Reference.pdf	[Ado03]
Cylinder Disc and Tape Care in a Nutshell.html	[LoCa]
Study of CD longevity.pdf	[LoCb]
Gutmann - Secure Deletion of Data.html	[Gut96]

# Literatúra

- [Ado03] Adobe Systems Inc. Adobe Portable Document Format, version 1.5. 2003. [http://partners.adobe.com/asn/acrobat/sdk/public/docs/PDFReference15\\_v5.pdf](http://partners.adobe.com/asn/acrobat/sdk/public/docs/PDFReference15_v5.pdf).
- [BHS93] D. Bayer, S. Haberand, and S. Stornetta. Improving the efficiency and reliability of digital time-stamping. In *Sequences II, Methods in Communication, Security, and Computer Science*. Springer-Verlag, 1993.
- [BS00] *Information Technology – Code of practice for information security management*. 2000. Štandard ISO/IEC 17799, BS 7799.
- [CC99] *Common Criteria for Information Technology Security Evaluation*. 1999. Verzia 2.1, pozostáva z troch častí, štandard ISO/IEC 15408.
- [CCa99] *Common Criteria Part 1: Introduction and General Model*. 1999. Verzia 2.1, <http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF>.
- [CCb99] *Common Criteria Part 2: Security Functional Requirements*. 1999. Verzia 2.1, <http://www.commoncriteria.org/docs/PDF/CCPART2V21.PDF>.
- [CCc99] *Common Criteria Part 3: Security Assurance Requirements*. 1999. Verzia 2.1, <http://www.commoncriteria.org/docs/PDF/CCPART3V21.PDF>.
- [CCo] Common Criteria Familiarization. [http://csrc.nist.gov/cc/Documents/Guidance/CC\\_Overview.ppt](http://csrc.nist.gov/cc/Documents/Guidance/CC_Overview.ppt).
- [CCP] Using Common Criteria Protection Profiles. [http://csrc.nist.gov/cc/Documents/Guidance/Using\\_PPs.ppt](http://csrc.nist.gov/cc/Documents/Guidance/Using_PPs.ppt).

- [CCS00] Cryptographic Communications System Protection Profile. 2000. Draft.
- [CLR89] Thomas Cormen, Charles Leiserson, and Ronald Rivest. *Introduction to Algorithms*. MIT Press, 1989.
- [CvA90] J. Chaum and H. van Antwerpen. Undeniable signatures. *Advances in Cryptology—CRYPTO’89 (LNCS 435)*, pages 212–216, 1990.
- [DR01] Joan Daemen and Vincent Rijmen. AES Proposal: Rijndael. 2001. <http://csrc.nist.gov/encryption/aes/rijndael/Rijndael-ammended.pdf>.
- [Eas01] D. Eastlake. US Secure Hash Algorithm 1 (RFC 3174). 2001. <http://www.faqs.org/rfcs/rfc3174/>.
- [ElG85] T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 1985.
- [Fei73] H. Feistel. Cryptography and Computer Privacy. *Scientific American*, 1973.
- [Gut96] Peter Gutmann. Secure Deletion of Data from Magnetic and Solid-State Memory. *Sixth USENIX Security Symposium Proceedings*, 1996. [http://www.cs.auckland.ac.nz/~pgut001/pubs/secure\\_del.html](http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html).
- [HS91] S. Haberand and S. Stornetta. How to timestamp a digital document. *Journal of Cryptology*, (3), 1991.
- [LC04] Syntegra Limited and Oracle Corporation. Red Hat Enterprise Linux 3 Security Target. 2004. [http://www.cesg.gov.uk/site/iacs/itsec/media/sectarg/Linux\\_v1.7.pdf](http://www.cesg.gov.uk/site/iacs/itsec/media/sectarg/Linux_v1.7.pdf).
- [LoCa] Library of Congress. Cylinder Disc and Tape Care in a Nutshell. <http://www.loc.gov/preserv/care/record.html>.
- [LoCb] Library of Congress. Study of CD longevity. <http://www.loc.gov/preserv/study%20of%20CD%20longevity.pdf>.

- [MvOV97] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997. <http://www.cacr.math.uwaterloo.ca/hac/>.
- [NIST] National Institute of Standards and Technology. Data Preservation Program. <http://www.itl.nist.gov/div895/isis/datastorage.html>.
- [NIST99] National Institute of Standards and Technology. CSPP – Guidance for COTS Security Protection Profiles (NISTIR 6462). 1999. <http://csrc.nist.gov/publications/nistir/ir6462.pdf>.
- [NIST01a] National Institute of Standards and Technology. Advanced Encryption Standard (FIPS 197). 2001. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
- [NIST01b] National Institute of Standards and Technology. Certificate Issuing and Management Components Family of Protection Profiles. 2001. [http://csrc.nist.gov/pki/documents/CIMC\\_PP\\_final-corrections\\_20010126.pdf](http://csrc.nist.gov/pki/documents/CIMC_PP_final-corrections_20010126.pdf).
- [NIST01c] National Institute of Standards and Technology. Digital Signature Standard (FIPS 186-2). 2001. <http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf>.
- [NIST01d] National Institute of Standards and Technology. Security Requirements for Cryptographic Modules (FIPS 140-2). 2001. <http://csrc.nist.gov/publications/fips/fips140-2/fips-1402.pdf>.
- [NIST02] National Institute of Standards and Technology. Secure Hash Standard (FIPS 180-2). 2002. <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>.
- [NIST03a] National Institute of Standards and Technology. COTS Security Protection Profile – Operating Systems (NISTIR 6985). 2003. <http://www.csrc.nist.gov/publications/nistir/nistir-6985.pdf>.
- [NIST03b] National Institute of Standards and Technology. Standards for Security Categorization of Federal Information and Information

- Systems (DRAFT FIPS 199). 2003. <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>.
- [NIST04] National Institute of Standards and Technology. Computer Security Incident Handling Guide (NIST SP 800-61). 2004. <http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>.
- [Riv92] R. L. Rivest. The MD5 Message-Digest Algorithm (RFC 1321). 1992. <http://www.faqs.org/rfcs/rfc1321/>.
- [RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, (21), 1978.
- [RSA02] RSA Security Inc. RSA Keon CA System v6.5 Security Target. 2002. [http://niap.nist.gov/cc-scheme/ST\\_VID4007-ST.pdf](http://niap.nist.gov/cc-scheme/ST_VID4007-ST.pdf).
- [SCSUG01] Smart Card Security User Group. Smart Card Protection Profile. 2001. <http://www.bsi.bund.de/cc/pplist/scsugpp.pdf>.
- [Sta] PGP Digital Timestamping Service. <http://www.itconsult.co.uk/stamper.htm>.
- [Sti95] Douglas R. Stinson. *Cryptography: Theory and Practice*. CRC Press, 1995.
- [Vaš04] Juraj Vaško. Časové značky v prostredí Slovenska. Master's thesis, Faculty of Mathematics, Physics and Informatics, Comenius University, Bratislava, 2004.
- [Ver26] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Amer. Inst. Elec. Eng.* 45, pages 109–115, 1926.
- [Wei] Eric Weisstein. Eric Weisstein's World of Mathematics. <http://mathworld.wolfram.com/>.
- [Xen00] Symeon (Simos) Xenitellis. *The Open-source PKI Book*. 2000. <http://ospkibook.sourceforge.net/>.
- [Zbi] Elektronická zbierka zákonov. <http://www.zbierka.sk/>.