**Záznam**
**z 8. stretnutia Pracovnej skupiny pre bezpečnostné štandardy (PS10)**
**uskutočneného 27. júna 2013 na MF SR**

---

**Zúčastnení:**
Peter Bíro (MF SR, predseda), Anna Levčíková (MF SR, člen), František Tomajko (NASES, člen), František Boda (ITAS, člen), Ľubor Illek (SOIT, člen), Lukáš Hlavička (CSIRT.SK, zástupca), Peter Kišša (ITAS, prizvaný), Rastislav Karbas (ITAS, prizvaný), Rastislav Bocko (Anext, prizvaný)

**Ospravedlnení:**
Tibor Kárász (MH SR, zástupca), Jaroslav Janáček (SISp, člen), Erika Slivová (ITAS, člen)

**Neospravedlnení:**
Martin Horňák (MŠVVŠ SR, člen), Ondrej Zimen (ÚOOÚ, člen), Štefan Porubčan (ITAS, člen), Lucia Menkeová (Rowan Legal, člen), Rastislav Machel (nezávislý expert, člen)

---

**Program zasadnutia**

1. Diskusia k návrhu štandardu pre architektúru cloud computingu.
2. Diskusia k návrhu bezpečnostných štandardov pre cloud computing.
3. Návrh NASES k štandardu SAML.
4. Návrh štandardu pre úrovne autentifikácie.
5. Ostatné

**Priebeh zasadnutia:**

Zasadnutie Pracovnej skupiny pre bezpečnostné štandardy (ďalej len „PS10“) viedol jej predseda P. Bíro. Záznam zapisoval P. Bíro (MF SR).

**Úvodné informácie**

P. Bíro úvodom informoval, že toto stretnutie je posledné pred stretnutím Komisie pre štandardizáciu IS VS (ďalej len „Komisia“) a ďalšie substantívne návrhy k elektronickým formulárom už nebudú po tomto stretnutí prijímané. Ďalej zhrnul témy, ktoré sa majú v novele objaviť

**1. Diskusia k návrhu štandardu pre architektúru cloud computingu**

P. Hlavička uviedol, že mu v návrhu absentuje kategorizácia ohľadom kritickosti informačných systémov. Uvedené bolo diskutované v ďalšej časti.

P. Kišša predstavil aktuálny návrh štandardu pre referenčnú architektúru cloudu, ktorého cieľom je zadefinovať referenčný architektúrny rámec. Architektúra sa skladá z logických vrstiev, z ktorých každá zabezpečuje určitú funkciu.

P. Bíro sa opýtal, čo sa vzhľadom na sémantiku rozumie pod „referenčnou“ a aká požiadavka má z návrhu vyplývať – pravdepodobne „ak sa buduje cloud, tak takto“, s čím

navrhovateľ súhlasil. Prívlastok „referenčná“ bude z návrhu vypustený. Doplňujúco uviedol, že to, že za správu cloud computingu zodpovedá jeho poskytovateľ, je dané predchádzajúcim štandardom. Na otázku či má byť navrhovaná architektúra jediná, p. Kišša odvetil, že áno, p. Hlavička následne upozornil na súlad s pripravovanou stratégiou pre cloud computing a p. Bíro na dostatočnú flexibilitu návrhu. P. Kišša odvetil, že tvorcovia návrhu štandardu v určitej časti tvorili aj návrh stratégie, takže by mal byť súlad zabezpečený. Bolo zhodnotené, že stav príslušného OPIS projektu členom PS10 nie je známy.

P. Levčíkovej chýbal kontext záväzných prvkov architektúry verejnej správy ako centrálny metainformačný systém. P. Kišša v tom nevidel problém, pretože architektúrou navrhovaný systém je opäť len informačný systém verejnej správy (ďalej len „IS VS“), s čím súhlasil aj p. Bíro. P. Bíro ďalej navrhol nahradiť „komponenty“ pojmom „moduly“ v súlade s delením Ústredného portálu verejnej správy, voči čomu neboli výhrady. Vlastný systém sa považoval za systém na správu cloudu, podrobnosti ako sa prepája tento systém s inými sa v návrhu nerieši, to by malo byť vyriešené generický pre IS VS. V dôvodovej správe by to však mohlo byť doplnené, kde to nadväzuje na ostatnú centrálnu architektúru.

P. Bíro upozornil aj, že uvedený návrh sa týka akéhokoľvek cloudu povinných osôb, nezávisle od toho, či to bude centrálny cloud štátnej správy alebo cloud napr. materských škôl. Rozvoj tzv. „eGovernment cloudov“ patrí na strategicko-politickú úroveň, nie do štandardov.

V krátkosti prebehla aj diskusia ohľadom propagovaného argumentu „30-50% percentného ušetrenia vo verejnej správe pri nasadení cloudu“, čo viacerí členovia PS10 spochybnili, nakoľko pôvodný zdroj vychádza z iných téz (v súčasnosti je omnoho vyššia virtualizácia) a pre iné prostredie (nie verejnej správy).

PS10 však vo všeobecnosti nemala výhrady určiť štandard, ktorý stanoví architektúru cloudu.

P. Bíro uviedol, že návrh pravdepodobne nie je kompletný, keďže mu absentuje napr. vlastná záloha, p. Kišša odvetil, že to je technologický, nie logický pohľad. Podľa p. Illeka by mala byť úplná, záverom bolo, že každá funkcionalita by teda mala byť nájditeľná v konkrétnych moduloch, čo predkladateľ dopracuje. Uvedené bude popísané v dôvodovej správe resp. metodike.

Na otázku p. Levčíkovej p. Kišša uviedol, že povinné funkcionality z návrhu vypadli. P. Levčíková spochybnila súvis 4 prierezových blokov v schéme, nakoľko sa v architektúre nevyskytujú, čo p. Kišša potvrdil. Uvedené bloky budú vypustené. Podľa p. Bíra bude celá architektúra v prílohe, pričom obrázok schémy bude pravdepodobne v dôvodovej správe resp. metodike.

P. Illek sa opýtal, či by nemali byť bezpečnostné požiadavky štandardu pre správu cloud computing párované na konkrétne vrstvy. Podľa p. Kiššu by sa každá vrstva mala zaoberať vlastnou bezpečnosťou, pričom úplné napárovanie by bolo veľmi komplikované. Tento názor zdieľal aj p. Bíro, pričom vzhľadom na časovú obtiažnosť takéhoto párovania to bolo podľa neho na zapracovanie nereálne. Takýto dokument však považoval za

zaujímavý, aj keď jeho rozsah by mohol byť aj niekoľko strán, možno by to však mohlo byť v metodike. P. Bíro považoval za súvisiaci problém aj prípadnú kontrolu správnosti.

P. Hlavička položil otázku, čo sa stane, keď niekto realizuje viaceré komponenty v jednom komponente. P. Kišša povedal, že to nie je možné, lebo na to nebude mať oprávnenia. P. Bíro sa opýtal, či to teda má byť porušením štandardu. P. Kišša odpovedal, že áno.

***K vrstve dopytu:***

P. Bíro mal pripomienku k zneniu definície vrstvy, pretože vrstva nemanažuje iba katalóg, ale podľa schémy aj rôzne iné moduly. Vhodné podľa neho bude použitie predvetia „sa skladá z“.

P. Bíro uviedol, že počet modulov nesedí so schémou. P. Kišša odvetil, že z nej neboli vypustené voliteľné komponenty (z vrstvy dopytu manažment ponuky služieb, modelovanie dopytu, reporting využívania, dodržiavanie dohody o poskytovanej úrovni cloudových služieb (ďalej len „SLA“), fakturácia a vyhodnocovanie a kvalita využívaných služieb („quality of experience“), vrstvy poskytovania služieb kvalita služieb („quality of service“) a modelovanie kapacít), aby sa nezvyšovala bariéra, čo bude opravené. P. Kišša prisľúbil doplniť krátke vysvetlenia aj k voliteľným komponentom. Na otázku rozšíriteľnosti uviedol, že možné sú aj ďalšie.

P. Hlavička považoval moduly pre dodržiavanie SLA a reporting využitia za zásadné pre používanie cloud computingu. P. Bíro upozornil, že po ich vypustení nesedí definícia vrstvy, ktorá má principiálne spravuje SLA. Ak to má robiť, minimálne modul dodržiavania SLA tam musí byť a za kritický ho používal aj z pohľadu bezpečnosti a prípadných súdnych sporov. Podľa p. Kiššu k tomuto nebol v ITAS jednotný názor. PS10 jednohlasne odhlasovala doplnenie tohto modulu ako povinného. Nadväzne musela byť pozmenená na povinnú aj kvalita služieb. P. Bíro zhodnotil, že na základe nešťastného prekladu sa komponenty kvalita využívaných služieb a kvalita služieb vecne podobajú.

PS10 sa nezaoberala presnými formuláciami odrážok jednotlivých komponentov.

<u>Ku komponentu portálu a prístupu k službám</u>

P. Bírovi sa nezdal názov „komponent portálu“, pretože nebolo jasné, čo to portál je a ponechal by iba „prístup k službám“, čo je všeobecnejšie. Ďalej nepovažoval „prístup“ v zmysle prístupu k službám za súladný s obsahom, lebo daný modul slúži iba na objednávanie (vybavovanie prístupu k službám), ale nie na poskytovanie služieb, t.j. pristupovanie k nim. Do tohto modulu sa prezentačne publikuje katalóg služieb, čo je možné prirovnať ku košíku e-shopu.

<u>Ku komponentu manažmentu používateľov a prístupových práv</u>

Do modulu sa k pojmu „autorizácie“ doplní aj „identifikácie a autentizácie“. Pojem „životného cyklu používateľa“ bude pravdepodobne nahradený.

Keďže používateľ bol premenovaný na odberateľa (osoba, ktorá má zmluvný vzťah s poskytovateľom cloudu), pri právnickej osobe sú používateľmi jej zamestnanci.

<u>Ku komponentu manažmentu objednávok</u>

P. Bíro mal otázku, aký je rozdiel tohto komponentu od komponentu portálu a prístupu k službám P. Kišša odvetil, že tento komponent poskytuje biznis logiku, t.j. je to obslužný modul, ktorý vygeneruje „objednávku“.

***K vrstve poskytovania služieb***

Uvedená vrstva je výkonná.

Ku komponentu spracovania požiadavky a aktivácie a deaktívácie služby

V názve bude doplnená aj deaktivácia.

Ku komponentu repozitára modelu služieb

Komponent obsahuje štandardizované šablóny.

Ku komponentu modelovania a návrhu služieb

Komponent slúži na vkladanie cloudových služieb.

Ku komponentu konfigurácie služieb

P. Bíro mal nejasnosť v zaradení tohto komponentu. Podľa p. Kiššu je toto výkonný modul. P. Bíro navrhol zmeniť názov na „realizáciu“, keďže konfiguráciou sa sémanticky rozumie nastavovanie.

Ku komponentu monitorovania služby

Komponent slúži na realizáciu monitorovania.

Ku komponentu manažmentu stavu služby

Komponent slúži na správu monitorovania a prezentáciu.

Ku komponentu manažmentu stavu služby

Komponent slúži na správu monitorovania a prezentáciu.

Ku komponentu využívania služby

Komponent slúži najmä na štatistické účely.

***K vrstve poskytovania služieb***

P. Bíro uviedol, že definičná veta „vrstva izoluje vrstvu „poskytovania služieb“ od potencionálne heterogénnych prostriedkov pomocou abstrakcie.“ je z väčšej časti nezrozumiteľná. Podľa p. Hlavičku pravdepodobne poskytuje jednotné rozhranie pre všetky hardvérové prostriedky, čo p. Kišša potvrdil.

Ku komponentu katalóg prostriedkov a repozitára

Na otázku p. Bíra ohľadom prostriedkov a zdrojov p. Kišša odvetil, že je to to isté. V celom dokumente preto bude použitý jednotný pojem „zdroje“. P. Bíro mal otázku, ktorá sa týkala rozdielu katalógu a repozitára, bolo uzavreté, že sa bude používať iba katalóg.

Ku komponentu konfigurácie prostriedkov

Komponent zabezpečuje realizáciu prideľovania zdrojov.

Ku komponentu meranie využívania

Meranie a monitorovanie bude zjednotené, bude použité iba monitorovanie. Komponent vykonáva monitorovanie. P. Bíro skonštatoval, že pre služby bolo monitorovanie a realizácia (konfigurácia) v jednom module, pre zdroje je to rozdelené. Podľa p. Kiššu je tento model vo vzťahu ku konkrétnym službám (ako využíva zdroje), komponent stavu prostriedkov sa zaoberá tým, aký je reálny stav konkrétnych zdrojov. P. Hlavička mal otázku k pojmu „fond“, p. Bíro odvetil, že takéto technické podrobnosti nie sú pre štandard potrebné, bude sa preto používať iba pojem „zdroje“.

P. Bíro záverom zhodnotil, že celý koncept slúži iba na zaradenie funkcií do konkrétnych logických častí, ale nijako ich funkčne neobmedzujeme požiadavkami, čo p. Kišša potvrdil.

## 2. Diskusia k návrhu bezpečnostných štandardov pre cloud computing

P. Bíro úvodom reprodukoval pripomienky zaslané zástupcom Úradu na ochranu osobných údajov.

***K definíciám***

Prvá časť sa týkala pojmov „cloud computing“ a „cloudová služba“.

P. Bíro mal otázku k tomu, či cloudovú službu nemôžeme mať pre úroveň elektronickej služby 3 a nižšie. P. Kišša odvetil, že sa to myslelo tak, že to má byť bez osobného kontaktu. P. Bíro odvetil, že „bez interakcie“ je povedané už v definícii cloud computingu. P. Illek doplnil, že v definovaní pojmov nie je vhodné stanovovať na ne požiadavky. P. Bíro navrhol nahradiť pojem „bez interakcie“ pojmom „bez osobného kontaktu“.

P. Kišša uviedol, že sa mu vzhľadom na vágnosť nezdá vhodné použitie pojmu „s minimálnym časovým obmedzením“. P. Bíro odvetil, že toto nahradilo pôvodné „rýchlo“, ale lepší pojem zatiaľ nenašiel, ani ho nikto iný nenavrhol.

P. Bíro si nebol istý, či je pri definícii cloud computingu zahrnutý aj „diverzifikovaný prístup k sieti“ (=„nezávisle od lokality“ atď.) a „elasticita“ (=„na základe voliteľného škálovania“ atď.). P. Kišša uviedol, že ITAS k tomuto nevzniesol pripomienky, takže je to pravdepodobne v poriadku.

Po diskusii bolo nahradené znenie „podľa potreby“, čo môže byť aj automatizované, pojmom „na vyžiadanie“.

K dohode o poskytovanej úrovni cloudových služieb bolo zodpovedané, že môže byť uzavretá aj medzi sprostredkovateľom a odberateľom. P. Bíro sa opýtal, kto rozhoduje o tom, s kým to je uzavreté – podľa p. Kiššu o tom rozhoduje samotný odberateľ. P. Levčíková mala pripomienku, že zmluvne sa nastavujú pravidlá, nie očakávania. P. Bíro uviedol pripomienku Úradu na ochranu osobných údajov, ktorá znela, že dohoda môže povinne obsahovať aj požiadavky podľa ich legislatívy. Keďže však môžu byť aj iné takéto predpisy (napr. mlčanlivosť), navrhol doplniť „v súlade s osobitnými predpismi“, avšak iba do metodiky, aby nepríslušná legislatíva nepredpisovala do zmluvných vzťahov povinný súlad – na to sú tu súdne konania a obchodné právo.

P. Kišša upozornil, aby boli v pojme „odberateľ cloudových služieb“ všade cloudové služby a nie iba služby.

P. Bíro uviedol, že Úrad na ochranu osobných údajov mal požiadavku na zadefinovanie pojmu „tretia strana“, podľa p. Bíra je tento pojem používaný v množstve predpisov a už zadefinovaný v inej časti výnosu, takže to nie je potrebné.

P. Levčíková sa opýtala, či by nebolo potrebné zadefinovať aj používateľa, p. Bíro však uviedol, že pravdepodobne tento pojem nie je nikde potrebné použiť, takže je takáto definícia zbytočná.

P. Bíro mal otázku, či má audítor preskúmavať aj zmluvné vzťahy, t.j. ako to bolo uvedené v pôvodnom návrhu predkladateľa alebo iba dodržiavanie podmienok pre cloud. Odpoveďou bolo, že sa malo jednať o dodržiavanie podmienok pre cloud.

***K bezpečnostným požiadavkám na cloud computing***

Ku kategorizácii cloudových služieb p. Illek uviedol, že sa nikde ďalej nepoužívajú. P. Bíro uviedol, že sú zavedené kvôli referencovaniu, a to aj z iných dokumentov.

P. Illek navrhol presunúť celú časť ohľadom cloudu do samostatnej prílohy, čím sa zároveň môže vytvoriť priestor pre voľnejšie texty. P. Bíro povedal, že možné to je, ale v tejto chvíli v tom nevidí žiadny prínos, keďže to už je naformulované ako znenie hlavnej časti výnosu. Čiastočným problémom by mohla byť následná výrazne vnorená hierarchia nadpisov. PS10 odhlasovala ponechanie v hlavnom texte (6 za ponechanie, 2 za presunutie do prílohy, 0 sa zdržalo).

K modelu SaaS bolo uzavreté, že aj keď je aplikácia softvérom, bude kvôli lepšej pochopiteľnosti explicitne uvedená prostredníctvom „vrátane“.

P. Bíro mal otázku, či sa v privátnom cloude a ďalej malo jednať iba o „prevádzkovateľa“ alebo aj o ostatné funkcie. Odpoveďou bolo, že to môže byť prevádzkovateľ, poskytovateľ aj sprostredkovateľ. P. Bíro vyjadril pochybnosti o „zdieľaní záujmov“ v definícii, ale skonštatoval, že lepšie vyjadrenie pre odlíšenie od verejnosti asi nie je.

P. Bíro mal otázku k verejnému cloudu, a to či odberateľ nie je (nesmie byť) alebo nemusí byť prevádzkovateľom cloudových služieb, t.j. či povinná osoba nemôže byť odberateľom vlastného cloudu. Záverom diskusie bolo zosúladiť znenie s ostatnými typmi cloudu.

Na otázku, či je „cloud computing“ ekvivalentom „IS VS“ v bezpečnostných štandardoch bol vyslovený súhlasný záver. Uvedené bude vhodne napárované na bezpečnostné štandardy, pričom bude potrebné zosúladiť napárovanie s bezpečnostnými štandardmi, podľa toho, či sa má použiť cloud computing alebo cloudová služba.

P. Hlavička podotkol, že v požiadavkách by malo byť všetko, čo je špecifické pre cloud, absentovali mu napr. závislosti. P. Bíro uviedol, že je potrebné navrhnúť konkrétne doplnenia. P. Hlavička prisľúbil naformulovať znenie, ktoré by sa malo objaviť najmä v bezpečnostnej politike.

P. Bíro mal otázku, čo sa rozumie „sieťovou konektivitou“ vo vzťahu k tomu, že to má byť aktívom. P. Karbas odpovedal, že cloud má byť dostupný, t.j. aby sa riziková analýza zaoberala aj napr. tým, že cloud má iba jedného poskytovateľa siete a podobne.

Pôvodne explicitne uvádzané normy budú uvedené v dôvodovej správe resp. metodike.

P. Hlavička navrhol zaoberať sa aj kompatibilitou s bezpečnostnou politikou odberateľa. P. Bíro uviedol, že to závisí od konceptu, záverom PS10 bolo, že poskytovateľ by mal osobitnou politikou popísať, ako sa k tomu bude stavať.

P. Illekovi aj p. Hlavičkovi chýbali úrovne bezpečnosti informačných systémov, aby bolo možné presnejšie stanovovať súlad bezpečnostných požiadaviek. P. Bíro uviedol, že takáto klasifikácia pravdepodobne vznikne až v pripravovanom zákone o informačnej bezpečnosti. Zároveň upozornil, že aj v súčasnosti mnohé organizácie verejnej správy outsourcujú svoje informačné systémy bez ohľadu na klasifikáciu citlivosti svojich údajov, čo nie je samozrejme správne. Podľa p. Bíra aj na európskej úrovni zatiaľ nie je známa takáto klasifikácia, existujú však minimálne požiadavky na bezpečnosť.

P. Illek navrhol zaoberať sa kritickými aktívami, p. Bíro však položil otázku, či je známe, čo by malo byť takto označené.

P. Illek ďalej uviedol, že v návrhu podľa neho úplne absentuje bezpečnosť z pohľadu odberateľa – čo povinne majú spraviť správcovia IS VS, aby mohli používať cloud resp. cloudovú službu, napríklad presnejší popis SLA. P. Bíro povedal, že vzhľadom na časovú tieseň asi nie je možné túto tému zapracovať, pričom zatiaľ k nej neexistujú žiadne podklady.

P. Bíro mal otázku, či nie je „neoprávnený prístup“ v bode 6 k manažmentu rizík to isté ako „nedostatočná izolácia“ v bode 4. PS10 sa zhodla, že aj keď je to podobné, je možné to explicitne ponechať oddelené. Pred slovami „izolované prostrediu“ bude odstránené „virtuálne“.

V diskusii ku kompromitácii a zlyhaniu správy šifrovacích kľúčov bol záver, že budú ponechané oba, pričom sa bude hovoriť o „kompromitácii šifrovacích kľúčov“ a „zlyhaní správy šifrovacích kľúčov“.

P. Hlavička navrhol zaoberať sa aj správou záplat, pretože to vzhľadom na dopad považoval za kritické a takisto zneužitie a kompromitácia privilegovaných účtov. PS10 zhodnotila, že hrozieb je ďaleko viac, ako je možné tu vymenovať, takže je vhodné ponechať najmä tie, ktoré sa týkajú špecificky cloud computingu alebo sú pre ne kritické.

K auditom v písm. d) mal p. Illek otázku, aký audit si môže používateľ vyžiadať – aj platformy resp. v akom rozsahu ? P. Bíro uviedol, že je to možné ponechať aj na dohodu, ale to môže skončiť aj žiadnym auditom. Vhodnejšie by bolo zaoberať sa auditom na všetkých zdrojoch, ktoré sa týkajú cloudových služieb, poskytovaných odberateľovi – napr. či nemá niekto neoprávnený prístup k jeho údajom. P. Karbas uviedol, že v praxi je to možné premietať aj do finančných úhrad takýchto auditov, aj keď nie je zrejmé, ako by to vyzeralo pri verejnej správe. Doplnkovo navrhol bod 2 úplne vypustiť. P. Illek zhodnotil, že ak by sa bod 2 vypustil, obdobne by to malo byť obdobné aj pre bod 3. P. Hlavička s p. Illekom k bodu 3 navrhli preformulovať, „ktorý je pripravený tak, aby neovplyvnil...“ PS10 odhlasovala (7 za, 0 proti, 1 sa zdržal), aby audit aj penetračné testy odberateľa v návrhu zostali.

P. Hlavička navrhoval pri § 32 tzv. „multi-vendor“ princíp, t.j. viacnásobné overenie ochranným softvérom, napr. antivírom. P. Bíro mal výhradu vzhľadom na to, že existuje veľmi veľké množstvo typov škodlivého kódu, pričom veľa ochranných softvérov sa

navzájom „neznáša“. Podľa p. Illeka tento návrh nepatril k § 32, ani sa mu celkový návrh nezdal, najmä z dôvodu., že to nie je minimálnou požiadavkou, ktorú týmito štandardmi určujeme. PS10 odhlasovala, že tento návrh nebude vložený (0 za povinnú podobu, 0 za odporúčanú podobu, 6 proti akejkoľvek podobe, 1 sa zdržal).

P. Bíro mal otázku k doplnku k § 33, písm. f), bodu 1 - čo sa rozumie „multi-tenant prostredím“. Podľa p. Karbasa je to „schopnosť a spôsob prevádzky softvéru, kde viac nezávislých inštancií dokáže nezávisle pracovať v zdieľanom prostredí, pričom inštancie sú logicky oddelené, ale fyzicky spojené“. P. Illek uviedol odlišnú definíciu, podľa ktorej je to ak „jedna inštancia poskytuje služby viacerým subjektom.“ PS10 sa zhodla, že v tejto časti bude daný pojem vypustený.

K písm. f), bodu 2, PS10 diskutovala o povinnosti segmentácie siete v zmysle oddelenia vrstiev podľa prílohy č. 7 resp. oddelenia manažmentovej platformy na úrovni siete od ostatných modulov, avšak nebol uzavretý žiadny konkrétny návrh. P. Bíro uviedol, že ak bude k tomuto doplnkovo zaslaný relevantný návrh, bude ho ešte možné akceptovať.

P. Hlavička k písm. h) navrhol doplniť „testovanie aktualizácie virtualizačného prostredia a softvéru pre správu cloudu v testovacom prostredí“, voči čomu nemala PS10 žiadne výhrady.

K písm. i), bodu 3 – funkcii ochrany proti DDoS p. Illek povedal, že uvedené je podľa neho predmetom SLA a navrhol doplniť znenie v tomto zmysle. PS10 hlasovaním uzavrela ponechanie tohto bodu (6 za ponechanie, 1 proti, 0 sa zdržalo).

P. Hlavička k písm. i) navrhol doplniť dva nové body „zabezpečiť podporu monitoringu prostredníctvom SIEM“ a „zabezpečiť podporu integrácie bezpečnostných monitorovacích prvkov a sond“. Z diskusie vyplynulo, že sa pravdepodobne jedná o „synchronizáciu monitorovania“, ale PS10 nebola vzhľadom na predčasné opustenie stretnutia predkladateľom jednoznačne presvedčená o jednoznačnom porozumení zneniu ani jedného z navrhovaných bodov, preto sa PS10 zhodla, že pred vyjadrením počká na doplňujúci návrh p. Hlavičku.

P. Illek navrhol požiadavky ohľadom zaznamenávania § 40, písm. i). P. Bíro uviedol, že takéto štrukturálne zmeny zhodnotí po stretnutí.

P. Bíro položil otázku, ktorých typov záloh sa má týkať zálohovanie v geograficky vzdialenej lokalite. Diskusiou PS10 prišla k záveru, že navrhované je už v podstate obsiahnuté v aktuálnom znení písm. b) § 39.

P. Bíro mal otázku k slovu „podporovať“ v písm. m) bode 2 a navrhol túto požiadavku zaviesť ako povinnú pre správu platformy, čo PS10 po diskusii akceptovala.

P. Bíro sa spýtal, čo sa rozumelo návrhom písm. m), bodom 5. Záverom PS10 bolo vztiahnuť celé písm. m) voči správe platformy.

P. Illek navrhol k odseku 2, písm. a) doplniť to vo vzťahu k SLA alebo ho vypustiť. PS10 hlasovaním vypustenie zamietla (1 za vypustenie, 6 proti, 0 sa zdržalo), pričom doplnenie nepovažovala za potrebné.

PS10 upravila odsek 2, písm. c) nahradením prvej skratky VM pojmom „virtuálne komponenty“ a vypustením príkladu v závere ustanovenia.

P. Illek mal otázku, či sa všetko, čo spĺňa definíciu cloud computingu podľa úvodných ustanovení automaticky rozumie cloudom alebo sa má brať na účely tohto návrhu iba taký cloud, ktorý spĺňa definíciu resp. príslušné parametre. P. Bíro uviedol, že podľa neho je to tá druhá verzia, ale bude to potrebné overiť z právneho pohľadu. P. Illek požiadal uvedené vysvetlenie doplniť do dôvodovej správy.

P. Kišša prisľúbil do konca týždňa preposlať úpravy k architektúre cloud computingu.

## 3. Návrh NASES k štandardu SAML

P. Bocko úvodom k tejto téme zhrnul zmeny oproti predchádzajúcej verzii, pričom jednou z najvýznamnejších bola zmena názvu zo „SAML token“ na „SAML Assertion“, pričom vecne sa jedná o dátovú štruktúru, využívanú v SAML.

P. Bíro mal otázku, čo by malo odznieť vo výnose. Odpoveďou bol návrh na použitie znenia kapitoly 5 ku návrhu štandardu pre federáciu identít. Z uvedeného nebolo zrejmé, čo sa rozumie federačným scenárom identity, preto bolo PS10 uzavreté, že federačným scenárom je ak viaceré IS VS používajú práve jedného poskytovateľa identít.

Podrobnými atribútmi sú tie, ktoré sú vymenované v návrhu, pričom p. Bíro ďalej požiadal predkladateľa rozpísať anglické skratky a vysvetliť významy. Všetky návrhy sú iba alternatívami. Pojem „binding“ má predstavovať API. P. Bíro mal otázku k verzii SOAP, záverom bolo jeho použitie podľa príslušnej časti výnosu. Návrh sa mal týkať iba situácie, ak je poskytovateľom identít ÚP VS. P. Bíro namietol, že sa nemá jednať o „ÚP VS“, ale o „správcu ÚP VS“. V tejto súvislosti prebiehala diskusia ohľadom toho, či sa v pojmoch SAML Assertion jednalo o informačné systémy alebo organizácie.

NASES sa k otázke, či sa má SAML 2.0 používať všeobecne alebo iba pri integrácii s ÚP VS nevyjadril

Atribúty SAML Assertion majú byť podľa predkladateľa rozšíriteľné. P. Bíro sa opýtal, ako je to zosúladené s dátovými prvkami. Podľa p. Bocka môže identita po prihlásení zastupovať iba jednu ďalšiu identitu. V súvislosti s číselníkom pre DelegationType padla otázka, čo je to za číselník. Zástupca SOIT navrhol používať štandardizovaný centrálny číselník. Pre p. Bíra boli nejasné obsahy navrhovaných identifikátorov a ďalej uviedol, že uvedené by malo byť v tvare resp. hĺbke popisu dátových prvkov, pretože podľa súčasného návrhu sú nevytvoriteľné, keďže absentuje obsah a účel. Predkladateľ bol požiadaný o doplnenie a úpravu v zmysle uvedených pripomienok, nakoľko PS10 to v uvedenom tvare nemohla schváliť.

## 4. Návrh štandardu pre úrovne autentifikácie

Nakoľko podľa p. Illeka bol návrh iba podmnožinou požiadaviek podľa STORK, mal zásadný návrh, aby sa prebrali QAA úrovne podľa STORK, pričom je možné pridať piatu úroveň 0 – v tvare „štandardom pre úrovne autentifikácie je úroveň,“ resp. „požiadavky na úroveň X vzhľadom na registráciu, pridelenie autentifikačných nástrojov, kvalitu registračného procesu atď. zodpovedajú úrovni X podľa metodiky STORK...“.

P. Bíro upozornil, že ak to má byť použité ako štandard, je tým pádom potrebné STORK preložiť, pretože existuje veľké množstvo osôb, ktorých sa to dotkne a nebudú vedieť to

použiť a ďalej mal pochybnosť o legislatívnej použiteľnosti príslušnej metodiky bez ďalších úprav vzhľadom na jej pomerne voľnú textáciu. Ďalším problémom môže byť pravdepodobná nemožnosť priameho legislatívneho odkazovania na zahraničné dokumenty. Po diskusii sa PS10 zhodla, že QAA úrovne budú prebraté úplne, a ak to bude časovo možné stihnúť, budú preložené ako samostatná príloha výnosu, inak budú iba relevantne odkazované. Napárovanie konkrétnych mechanizmov a autentizačných prostriedkov patria do metodického pokynu.

## 5. Ostatné

P. Bíro záverom uviedol, že sa nebudú otvárať nové vecné témy. Predpokladaná účinnosť výnosu je 1.1.2014.

## 6. Závery

1/ Zaslať úpravy v zmysle diskusie ku bodu 2 stretnutia.

Zabezpečí: L. Hlavička Termín: 29.6.2013

2/ Zaslať úpravy v zmysle diskusie ku bodu 4 stretnutia.

Zabezpečí: F. Tomajko Termín: 29.6.2013

3/ Zapracovanie pripomienok zo stretnutia.
Zabezpečí: P. Bíro Termín: stretnutie Komisie