

Workshop

Zníženie vyžadovanej úrovne zabezpečenia pri zasielaní podaní cez ÚPVS na QAA Level 3

Štefan Szilva (NASES) - QAA Level 3 a technické náležitosti MobileID na ÚPVS
Lukáš Hupka (MIRRI) - MobileID – produktový manažment

9. a 14. decembra 2021

Workshop k zníženiu vyžadovanej úrovne zabezpečenia na QAA Level 3

Program workshopu:

1. téma: QAA Level 3

- dôvody zníženia úrovne zabezpečenia a nevhodnosti vynucovania úrovne QAA Level 4 (minimálne pre služby dostupné cez integračné rozhrania),
- rozsah služieb, ktorých sa zmena dotkne,
- možnosti technického riešenia pri kontrole vyžadovanej úrovne zabezpečenia.

2. téma: MobileID

- rozšírenie číselníkov typov autentifikačných prostriedkov v ÚPVS IAM o "MobileID" a jeho zaradenie do úrovne QAA Level 3,
- pripravované pridanie možnosti prihlasovania cez MobileID na prihlasovacej obrazovke ÚPVS IAM.

Workshop k zníženiu vyžadovanej úrovne zabezpečenia na QAA Level 3

Zdôvodnenie zmeny:

- Všetky služby dostupné cez integračné rozhrania ÚPVS sú výlučne na úrovni QAA Level 3
 - Elektronické podania zasielané z integrovaných systémov (napríklad z registratúrnych systémov) sú zasielané na úrovni QAA Level 3
- Povinnosť v zmysle Nariadenia eIDAS je akceptovať všetky notifikované prostriedky elektronickej identifikácie na rovnakej alebo vyššej úrovni ako je vyžadovaná úroveň pre prístup k službe „online“
- Rovnocennosť prístupu cez GUI a API
- Informácie o QAA Level 3 uvedené v [Release pláne nasadzovaných zmien ÚPVS](#) od roku 2018
- Podrobné zdôvodnenie bolo [zverejnené v ozname v júni 2021 na ÚPVS](#).
- Strategická priorita Multikanálový prístup NKIVS z roku 2017
- § 25 ods. 7 zákona o e-Governmente – povinnosť sprístupniť služby prostredníctvom aplikačných rozhraní

Workshop k zníženiu vyžadovanej úrovne zabezpečenia na QAA Level 3

Dopady na existujúce integrované systémy:

1. Služby sprístupnené prostredníctvom konštruktora správy ÚPVS

- **Bez dopadov** na samotnú službu a jej prijímanie do elektronickej schránky
- Čiastočný dopad výlučne v prípade, ak OVM nevyhnutne potrebuje vynucovať QAA Level 4 (v takom prípade prosíme kontaktovať NASES)

2. Služby poskytované na špecializovaných portáloch

- Je potrebné preveriť, či váš informačný systém kontroluje zo SAML tokenu:
 - úroveň zabezpečenia v položke „QAALevel“ a v prípade vynucovania QAA Level 4 prehodnotiť a po prehodnotení akceptovať QAA Level 3
 - prostriedky elektronickej identifikácie v položke „AuthResourceType“ a rozšíriť povolené prostriedky

Workshop k zníženiu vyžadovanej úrovne zabezpečenia na QAA Level 3

Potrebné kroky na strane OVM:

1. Meta IS

- Vyhľadanie služieb daného OVM v Meta IS a kontrola vyžadovanej úrovne zabezpečenia autentifikácie
- V prípade QAA Level 4 prehodnotenie oprávnenosti tejto požiadavky
 - podkladov [zverejnené na slovensko.sk](https://www.zverejnené-na-slovensko.sk)
- Zmena informácie o úrovni zabezpečenia v Meta IS

2. Preverenie prípadných obmedzení na špecializovaných portáloch

- V prípade vykonávania kontroly QAA Level zo SAML tokenu povoliť úroveň 3
- V prípade vykonávania kontroly AuthResourceType zo SAML tokenu povoliť hodnotu 12 (MobileID)

Workshop k zníženiu vyžadovanej úrovne zabezpečenia na QAA Level 3

Vyžadovaný KEP nesúvisí s úrovňou QAA Level

- V minulosti sa rozšírila nesprávna informácia, že v prípade vyžadovania KEP v elektronickom podaní je potrebné v MetaIS uvádzať úroveň „4“.
- Úroveň zabezpečenia autentifikácie nesúvisí s vyžadovaním autorizácie na elektronickom podaní.
 - Autorizácia v zmysle zákona je **súhlas s vykonaním konkrétneho právneho úkonu** – typicky elektronického podania alebo elektronického úradného dokumentu
 - Autentifikácia je **overenie deklarovanej identity**
- Kvalifikovaný elektronický podpis je možné vyžadovať pri ľubovoľnom QAA Level, napríklad aj pri službách nevyžadujúcich autentifikáciu

Workshop k zníženiu vyžadovanej úrovne zabezpečenia na QAA Level 3

Možnosti vynucovania QAA Level, ktoré však neodporúčame

- V prijímaných Sk-Talk správach kontrola zahrnutého technického SAML tokenu (element QAALevel)
 - Následne je potrebné zo strany gestora služby zaslanie informácie o nedostatočnosti použitého prostriedku používateľovi, čo pre používateľa môže byť máťúce keďže obvykle už predtým obvykle dostane doručenku
- Na špecializovaných portáloch z WebSSO SAML tokenu (element QAALevel)
 - V prípade nesplnenia podmienok je potrebné používateľa informovať, že daný prostriedok nie je podporovaný aj so zdôvodnením a odporúčaním ďalšieho postupu

Workshop k zníženiu vyžadovanej úrovne zabezpečenia na QAA Level 3

Možnosti testovania rôznych úrovní QAA Level

- V testovacom prostredí ÚPVS je možné sa prihlásiť zahraničnými testovacími identitami cez eIDAS uzol
 - Informácie vo FAQ na strane 13: https://www.slovensko.sk/img/CMS4/eIDAS/FAQ_eIDAS.pdf
- Testovanie MobileID s QAA Level 3 bude možné v ďalších mesiacoch

Workshop k zníženiu vyžadovanej úrovne zabezpečenia na QAA Level 3

MobileID

- Integračný manuál IAM ÚPVS bol 9. 12. 2021 doplnený o AuthResourceType 12 – MobileID
- Bude dosahovať úroveň zabezpečenia autentifikácie QAA Level 3
- V 1. polroku 2022 pribudne na prihlasovacej obrazovke tlačidlo (dlaždica) pre prihlasovanie s MobileID (predpoklad marec/apríl)
- Prihlasovanie na ÚPVS cez MobileID je určené **pre „desktopový“ scenár** – t.j. MobileID len nahrádza občiansky preukaz s čítačkou a používateľ po prihlásení pokračuje na desktope
- Mobilný scenár (plnohodnotný) bude podporovaný až v neskorších fázach
 - spôsoby blokovania alebo umožnenia autentifikovaného prístupu z mobilného zariadenia k službe budú oznámené v krátkom čase
- Prihlasovanie na špecializované portály cez MobileID
 - Predpokladá sa hromadné pridanie možnosti prihlasovania cez MobileID na prihlasovaciu stránku všetkých Service providerov integrovaných na ÚPVS IAM WebSSO.
 - Integrované subjekty budú môcť požiadať NASES, aby na prihlasovacej stránke otvárajanej z ich portálu nebola možnosť MobileID, pokiaľ budú vynucovať QAA Level 4.
 - Prihlásenie už autentifikovaného používateľa cez WebSSO z iných portálov bude funkčné – v prípade potreby blokovat takého prihlásenie je možné riešiť len kontrolou QAA Level a AuthResourceType v SAML tokene.

Workshop k zníženiu vyžadovanej úrovne zabezpečenia na QAA Level 3

Slovensko v mobile (Lukáš Hupka)

- Prezentácia základnej plánovanej funkčnosti
- Časový harmonogram
- Služby sprístupňované priamo cez aplikáciu Slovensko v mobile (prispôsobené služby)

Workshop k zníženiu vyžadovanej úrovne zabezpečenia na QAA Level 3

Ďakujeme

stefan.szilva@nases.gov.sk

lukas.hupka@mirri.gov.sk