„Autentifikácia pre prístup k službám ÚPVS prostredníctvom CAMP“

Opis predmetu zákazky

Obsah

Popis požiadavky

Jednou s najvyšších priorít projektu CAMP je sprístupnenie služieb ÚPVS na CAMP pre systémy, ktoré zastupujú OVM (v režime integrácie stroj- stroj).

Pre prístup k existujúcim SOAP službám ÚPVS a súvisiacu úspešnú autorizáciu sa vyžaduje priloženie platného STS SAML2 IAM tokenu. Pre tento účel STS SAML2 token poskytuje všetky potrebné informácie a to najmä:

- ID zastupujúcej identity evidovanej v IAM a jej typ,
- ID zastupovanej identity evidovanej v IAM a jej typ,
- údaje o zastupovaní,
- údaje o vyplývajúcich oprávneniach,
- QAA level,
- typ použitého prostriedku pre autentifikáciu.

Pre naplnenie tohto predpokladu sa v projekte CAMP uvažovalo s využitím možnosti získania STS SAML2 tokenu IAM v zastúpení akéhokoľvek subjektu - vo vyššie uvedenom prípade by CAMP získaval token v mene integrujúcich sa OVM svojim vlastným technickým účtom ako univerzálne zastupujúcou identitou. Jedná sa o využitie tzv. IOM prístupu / role k STS službe IAM, pričom táto možnosť bola v IAM implementovaná výhradne pre potreby IOM v intenciách toho času platnej legislatívy. Táto možnosť je však z prevádzkového a bezpečnostného hľadiska krajne nevhodná.

Preto je potrebné navrhnúť taký spôsob autentifikácie, ktorý by:

- použili systémy priamo zastupujúce OVM pri prístupe k rozhraniam zverejneným v CAMP a zároveň,
- umožnil sprístupniť ÚPVS služby bez použitia IOM prístupu.

Návrh tohto spôsobu je popísaný v nižšie uvedenej kapitole.

Návrh riešenia

Stručný biznis popis

IAM ÚPVS poskytne autentifikačnú metódu, určenú pre systémy (aplikácie) priamo zastupujúce OVM, prípadne PO. Metóda bude sprístupnená v CAMP ako REST API. Metóda bude založená na autentifikácii osoby certifikátom, jej výstupom bude základný oAuth2 JWT token IAM, pričom sa jedná o autentifikačný prostriedok s úrovňou „pokročilá“. V zmysle legislatívy sa pre túto úroveň vyžaduje autentifikácia dvoma rôznymi faktormi:

- vyššie uvedený certifikát bude jedným z nich,
- druhým faktorom bude autentifikácia menom a heslom. Túto autentifikáciu zastreší CAMP: pre prístup aplikácie k autentifikačnej metóde IAM ÚPVS vystavenej na CAMP sa bude vyžadovať

„basic“ autentifikácia (menom a heslom). V prípade úspešnej „basic“ autentifikácie CAMP zašle v hlavičke do IAM identifikátor organizácie (GUID identity v IAM), ktorej aplikácia sa autentifikovala. IAM pred vydaním tokenu overí, či táto identita je tou istou identitou, ktorá sa autentifikovala certifikátom: t. j. dôjde k overeniu že oboma faktormi sa autentifikovala tá istá osoba.

S IAM ÚPVS JWT tokenom budú systémy priamo pristupovať na REST rozhrania zverejnené na CAMP. Základný OAuth2 JWT token bude obsahovať minimálnu sadu údajov (dôraz je kladený čo čo najmenšiu veľkosť tokenu): napríklad tie údaje, ktoré sú nevyhnutné pre vykonanie konverzie do IAM SAML2.0 tokenu.

V prípade, ak je koncovou službou sprístupňovanou v CAMP SOAP služba (vyžadujúca SAML2 token), tak IAM ÚPVS poskytne službu pre konverziu IAM tokenu: z oAuth2 JWT tokenu na STS SAML2 token. Túto službu využije CAMP v kontexte konverzie z REST do SOAP.

Okrem toho môže IAM poskytnúť konverznú tokenovú službu pre získanie rozšíreného JWT IAM tokenu (vstupom je základný IAM JWT token). Tento by mal obsahovať rozšírenú sadu údajov, aby sa bolo možné autorizovať voči koncovým REST službám ÚPVS až raz budú implementované. Momentálne ÚPVS poskytuje iba SOAP služby. Preto je poskytnutie tejto konverznej služby témou budúceho rozvoja.

Detailný biznis popis

Autentifikačná metóda

Jedná sa o metódu založenú na autentifikácii na základe x509 self-signed certifikátu. Defacto sa jedná o implementáciu metódy, ktorá sa spomína v prílohe č.3 k DNR CAMP v tabuľke č.2 na strane 6 ako "**Predloženie podpísaného JWT s identifikátorom aplikácie"** s poznámkou: "**OUT-OF-SCOPE** súčasnej implementácie (technicky možné riešenie, ktoré bude detailizované po potvrdení MIRRI)".

Vstup metódy:

- Autentifikačná požiadavka podpísaná privátnym kľúčom - certifikátom systému (technického účtu), ktorý žiada o autentifikáciu,
- Identifikátor organizácie (GUID identity v IAM). Údaj zasiela CAMP v hlavičke ako výsledok „basic“ autentifikácie aplikácie pri prístupe k autentifikačnej metóde – viď kap. Stručný biznis popis.

Výstup metódy:

- Základný IAM JWT (podpísaný IAMom ÚPVS). JWT obsahuje minimálnu sadu údajov. Konečný rozsah údajov uvádzaný v tokene bude špecifikovaný počas analýzy. Jedná sa najmä o:
    - ID zastupujúcej identity evidovanej v IAM a jej typ (pri integrácii stroj – stroj sa jedná o technický účet. Technický účet je špeciálny typ identity v IAM, ktorá reprezentuje systém/aplikáciu),
    - ID zastupovanej identity evidovanej v IAM a jej typ (typicky OVM),

- QAA level 3 (na úrovni 3, nakoľko certifikát a registračný proces ktorým sa certifikát zaeviduje do IAM zodpovedá úrovni autentifikácie pokročilá),
- typ použitého prostriedku (certifikát).

Predpoklady a ich naplnenie:

Pre úspešnú autentifikáciu touto metódou sa musia v evidencii IAM nachádzať údaje o:

- technickom účte – identita v IAM, ktorá je biznis interpretáciou aplikácie a je nosičom certifikátu (verejného kľúča),
- zastupovanej identite. Identifikátor tejto identity je zhodný s identifikátorom organizácie, ktorá bola uvedená na vstupe metódy (toto overenie realizuje IAM),
- zastupovaní medzi zastupovanou identitou a technickým účtom,
- certifikáte. Certifikát je naviazaný na technický účet - viď druhá odrážka vyššie.

Pre naplnenie týchto predpokladov sa využije:

- technický účet: pre založenie a zmenu technického účtu, certifikátu a zastupovania a oprávnení na zastupovanú identitu sa využijú existujúce procesy IAM nasadené v produkčnom prostredí (tzv. žiadosti a procesy CRAC),
- zastupovaná identita: využije sa existujúca evidencia OVM v IAM,
- zastupovanie medzi zastupovanou identitou a technickým účtom: viď vyššie,
- certifikát: viď vyššie.

Registračné procesy

Pre registráciu aplikácie sa využije existujúci registračný proces v CAMP.

Autentifikačné flow na strane CAMP pri prístupe k REST API na CAMP

Aplikácia organizácie bude na REST rozhrania zverejnené na CAMP môcť pristupovať aj priamo s oAuth2 JWT tokenom, ktorý vydal IAM v zmysle vyššie uvedenej autentifikačnej metódy, t. j. bez potreby autentifikácie jednou z existujúcich CAMP autentifikačných metód. Od CAMP sa bude vyžadovať aby:

1. overil platnosť IAM oAuth JWT tokenu, ktorý pre aplikáciu vydal IAM ÚPVS. Za týmto účelom musí mať CAMP uložené metaúdaje IAM ÚPVS (verená časť kľúča pre overenie podpísaného JWT). V rámci tohto kroku CAMP overí aj časovú platnosť tokenu,
2. získal z tokenu identifikátor zastupovanej identity a použil ho nasledovne: CAMP overí, či pod týmto identifikátorom existuje v CAMP zaregistrovaná organizácia a či táto organizácia má zaregistrovanú aplikáciu, ktorej identifikátor je uvedený v hlavičke volania daného REST API,
3. volanie služby presmeroval na cieľové rozhranie - koncovú službu. Ak je cieľovým rozhraním SOAP služba tak CAMP realizuje:
    1. konverziu REST na SOAP,
    2. konverziu JWT tokenu vydaného IAM ÚPVS na STS SAML2 token. Na tento účel využije službu pre konverziu IAM tokenov, ktorú poskytne IAM ÚPVS. Jedná sa o STS službu, na ktorú už CAMP podľa špecifikácie má byť integrovaný, na vstupe je však potrebné uviesť,

navyše JWT token vydaný IAM ÚPVS. CAMP zabezpečí aj cacheovania STS SAML2 tokenov za účelom zníženia záťaže na IAM ÚPVS.

Výhody navrhovaného riešenia

- riešenie vyžaduje minimálny vývoj na strane ÚPVS IAM,
- riešenie podporuje plnohodnotnú autorizáciu prístupu k službám na základe tokenu, ktorý bol priamo vydaný pristupujúcemu systému (eliminuje sa potreba využitia IOM prístupu / role),
- riešenie nevyžaduje úpravu registračného procesu na strane CAMP. Pre prvú fázu sa nevyžaduje väzba medzi identifikátorom aplikácie a identifikátorom technického účtu,
- riešenie vyžaduje malé úpravy na strane CAMP,
- riešenie je použiteľné aj pre integrované PO (režime stroj-stroj),
- riešenie je jednoducho rozšíriteľné aj pre integráciu systémov, ktoré autentifikujú koncového používateľa a v jeho mene volajú služby: typicky špecializované portály, ktoré majú autentifikovaného používateľa cez WEBSSO.

Rekapitulácia dopadov na IAM ÚPVS

- otestovanie a nasadenie služieb oAuth2 servera IAM:
    - oAuth2 autentifikačná metóda - autentifikácia na základe certifikátu,
    - služba pre konverziu z IAM JWT do IAM STS SAML2.

Rekapitulácia dopadov na CAMP

V zmysle vyššie uvedeného návrhu sa jedná o:

- úprava autentifikačného flow:
    - overenie a akceptovanie JWT vydaného IAM,
    - volanie služby pre konverziu IAM tokenov: z oAuth2 na SAML2 v kontexte konverzie protokolu REST na SOAP a cacheovania SAML2 tokenov získaných konverziou.

Harmonogram realizačných prác na strane ÚPVS

Nasadenie navrhovaného riešenia na testovacie prostredie za účelom akceptačného testovania a integrácie s CAMP:

- do 2 mesiacov odo dňa nadobudnutia účinnosti Zmluvy.