Bezpečnosť gridových systémov

Dynamické prostredia, akým je aj grid, zaoberajúce sa riešením rozsiahlych projektov, ktoré spájajú množstvo rôznych inštitúcií a často presahujúce územia jednotlivých štátov, či celých kontinentov, prinášajú nové bezpečnostné problémy, pre ktoré je nutné nájsť spoľahlivé riešenia.

Bezpečnostné otázky autentifikácie a autorizácie nie sú špecifické len pre gridové prostredie. Gridová komunita sa snaží aplikovať, využívať a rozvíjať už existujúce technológie v rámci gridového kontextu. V tejto časti sa budeme zaoberať niektorými pre grid typickými technológiami a infraštruktúrami, ktoré úspešne riešia problémy autentifikácie a autorizácie, ako aj spôsobmi ich rozšírenia.

Autentifikácia

Autentifikácia je proces overenia identity používateľa alebo služby. Najčastejšie používanou metódou autentifikácie v dnešných počítačových systémoch je kombinácia používateľského mena a hesla, ktoré sa overuje v príslušnej databáze. Vzhľadom k organizačným a geografickým vzdialenostiam gridového počítania, uvedená metóda nie je vhodná. Preto bolo potrebné v gride nájsť iné metódy autentifikácie jednotlivých entít, ktoré sú dostatočne jednoduché na používanie a administráciu, ale pritom sú ľahko škálovateľné a umožňujú funkčnú spoluprácu.

V gride sa pre uvedené ciele využívajú technológie založené na PKI (Public Key Infrastructure) a certifikátoch identity, kde každý používateľ a služba vlastní certifikát verejného kľúča podpísaný niektorou dôveryhodnou certifikačnou autoritou (CA). Tento certifikát, obvykle certifikát formátu X.509, spolu so zodpovedajúcim súkromným kľúčom používa vlastník certifikátu pre svoju autentifikáciu [Kou05]. Zvyčajne platí, že CA je dôveryhodná pre všetkých používateľov a vzťahy medzi entitami sú vopred stanovené a centrálne sledované. Všetky interakcie sú monitorované a manažované administrátormi, ktorí môžu reagovať, ak správanie nejakého subjektu nie je v súlade s politikou využitia daného distribuovaného systému a ukončiť tak dôveryhodnosť porušujúcej entity.

V súčasnej dobe je zväčša pre entity v gride prístupná nejaká certifikačná autorita zodpovedná za spoľahlivé vydávanie certifikátov. Napr. pre Českú republiku je takouto certifikačnou autoritou CESNET CA (https://pki.cesnet.cz/), ktorá umožňuje všetkým členom akademickej obce získať certifikát uznávaný všetkými významnými gridovými

projektmi v Európe a tak využívať PKI služby v gridovom prostredí.[45] Koreňové certifikáty akademických certifikačných autorít z Európy je možné nájsť na bezpečnom úložisku *Trusted Academic Certification Authority Repository*[46]. Medzi minimálne požiadavky kladené na CA patrí najmä nutnosť predloženia osobných dokladov žiadateľa pri podávaní žiadosti o certifikát; ďalej sa vyžaduje, aby počítač, na ktorom sa vykonávajú operácie s podpisovacím kľúčom CA, nebol pripojený k žiadnej počítačovej sieti, vyžaduje sa, aby všetky operácie s týmto kľúčom boli zaznamenávané, kladie sa dôraz na včasné vydávanie zoznamov predčasne zrušených certifikátov (CRL), apod.

Proxy X.509 certifikáty

Používateľ sa pri autentifikácii vlastnej osoby musí preukázať digitálnym X.509 certifikátom vydaným niektorou dôveryhodnou certifikačnou autoritou. Súkromný kľúč používateľa, ktorý je chránený heslom, je uložený na strane používateľa. Aby používateľ nemusel zadávať toto heslo pri každom prístupe ku gridovým službám, čo je pre používateľa otravná a zdržujúca činnosť, ponúka gridové infraštruktúra rozšírenie klasickej podoby PKI formou tzv. *proxy certifikátov*. Proxy certifikát, ktorý má limitovanú životnosť (spravidla dvanásť hodín) a ktorému je odovzdaná časť práv z certifikátu používateľa, sa využíva pri autentifikácii bez nutnosti zadávania hesla. Proxy certifikátom sa prezentuje určitá aplikácia, na ktorú používateľ delegoval časť svojich práv a ktorá teda môže po dobu platnosti proxy certifikátu konať v mene používateľa, tzn. riešiť v jeho mene určitú úlohu, čo používateľa odľahčí od neustáleho zadávania hesla počas behu aplikácie, tzv. princíp *Single Sign-On* (SSO).

Súkromný kľúč používateľa, ktorý je chránený heslom, slúži práve na delegovanie práv a na vygenerovanie a podpísanie dočasného proxy certifikátu, t. j. vydavateľom proxy certifikátu nie je CA, ale používateľ, pričom používateľov certifikát je k proxy certifikátu pripojený. Súkromný kľúč proxy certifikátu je uložený na disku, resp. zaslaný príslušnej aplikácii v nezašifrovanej forme. Používateľ tak nemusí zadávať heslo k svojmu privátnemu kľúču pri každom využívaní gridovej služby. Krátka doba platnosti proxy certifikátu znižuje riziko plynúce z prípadnej kompromitácie kľúča. Proxy certifikáty výrazne uľahčujú použitie gridu a zvyšujú aj bezpečnosť používateľovho certifikátu, pretože sa takmer po celú dobu pracuje iba s krátkodobým proxy certifikátom [Kou05, HS09b].

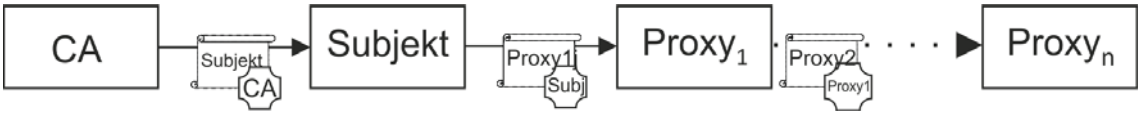
Po zaslaní úlohy do gridu je proxy certifikát, súkromný kľúč pre proxy certifikát a normálny certifikát (avšak nie dlhodobý súkromný kľúč používateľa) poslaný danej službe spolu s úlohou. Ak chce delegovaná služba pri riešení úlohy preukázať svoju delegovanú identitu inej službe, odošle podpísanú žiadosť spolu s proxy certifikátom a štandardným certifikátom, nie však proxy súkromný kľúč. Tieto informácie sú dostatočné na preukázanie, že vzdialená služba má právo používať delegovanú identitu.

[45] V Slovenskej republike je v súčasnosti certifikačná autorita SlovakGrid na Ústave informatiky Slovenskej akadémie vied v rekonštrukcii http://ups.savba.sk/ca/ca.html

[46] https://www.tacar.org/cert/list

Navyše, ak vzdialená služba musí ďalej delegovať práva na iné služby, môže sa vytvoriť nový proxy certifikát odkazujúci na predošlý, ktorý využíva nová služba; v tomto prípade dochádza k predĺženiu overovaného reťazca certifikátov, Obrázok 0-1.

Slabou stránkou tohto modelu je možná kompromitácia proxy privátneho kľúča, čo je kompenzované jeho krátkou životnosťou. Rovnako v prípade ďalšieho delegovania iným službám, o ktorých počiatočný používateľ nemusí mať žiadnu vedomosť a ktoré vystupujú v jeho mene, je možné zneužitie identity používateľa nedôveryhodnou službou, čo však môže byť kompenzované uložením celých delegovacích reťazcov pri zaznamenávaní vykonaných aktivít.



Obrázok 0-1 Proxy delegácia

Služba MyProxy

MyProxy je služba pre bezpečné ukladanie prístupových poverení (certifikáty, privátne kľúče) rovnako ako proxy certifikát. Služba MyProxy používa protokol proxy delegácie umožňujúci klientom získať krátkodobý proxy certifikát bez exportu dlhodobých kľúčov zo servera MyProxy. Pre tento účel určený MyProxy server poskytuje oveľa bezpečnejšie úložisko pre používateľské kľúče ako bežná pracovná stanica alebo súborový server a navyše môže v sebe integrovať kryptografický hardvér na jeho ochranu. Na získanie prístupových poverení z MyProxy úložiska musí najskôr prebehnúť autentifikácia klienta. Súčasné verzie MyProxy podporujú autentifikáciu cez heslo, certifikát, Kerberos, alebo PAM (Pluggable Authentication Modules). Uvedené umožňuje používateľom, príp. úlohám bežiacim v mene používateľa, získať prístupové poverenia z MyProxy servera kedykoľvek a kdekoľvek je to potrebné. Oproti štandardnej dvanásť hodinovej životnosti proxy certifikátu je životnosť prístupových poverení na MyProxy zvyčajne až sedem dní. Navyše môže byť služba MyProxy použitá na obnovu delegovacích certifikátov, čo umožní pre dôveryhodné dlhodobé služby ich vykonávanie bez toho, aby boli zrušené kvôli časovému obmedzeniu [MBH05].

Autorizácia

Ako už bolo spomenuté skôr, autorizácia je proces, pri ktorom sa overuje či autentifikovaný klient má oprávnenie použiť danú službu. Rozvoj a špecifické vlastnosti gridových technológií si vyžiadali zavedenie nových autorizačných mechanizmov, keďže žiadna z dovtedy dostupných autorizačných metód neposkytovala úplne funkcionalitu, ktorá je pre gridy požadovaná. Preto vznikli a stále vznikajú a vyvíjajú sa v danej oblasti sofistikované gridové autorizačné služby, ktoré poskytujú efektívnejšie nástroje na riešenie autorizačnej problematiky. Ďalej sú uvedené najvýznamnejšie existujúce autorizačné mechanizmy používané v gridovom prostredí.

Súbor grid map file

Jedným z prvých autorizačných mechanizmov pre gridové prostredie implementovaný pomocou nástroja Globus Toolkit [Glob] bol jednoduchý mechanizmus tzv. *grid map file*, kde vlastník zdroja robí rozhodnutia na základe informácií obsiahnutých v súbore s rovnakým názvom. *Grid map file* je zoznam všetkých autorizovaných gridových používateľov s ich DN menami, pričom jednotliví používatelia sú mapovaní na účty lokálnych používateľov. Súbor *grid map file* môže tiež slúžiť ako zoznam pre riadenie prístupu (access control list, ACL). Administrátor môže upravovať obsah súboru a tak kontrolovať aké certifikované entity majú prístup k daným službám, Obrázok 0-2. Rovnako môže konfigurovať cez premenné prostredia, ktorý *grid map file* súbor bude daná služba využívať v závislosti od lokálnej politiky riadenia prístupu.

# Distinguished Name	*local User ID*
"/C=SK/O=SlovakGrid/O=UCM/CN=Ladislav Huraj"	.voce
"/DC=es/DC=irisgrid/O=ugr/CN=gines.rubio"	augersgm001

Obrázok 0-2 Autorizačné údaje v súbore grid map file (zjednodušený príklad)

Pri uvedenom mechanizme je možné využívať aj tzv. *spoločný účet* (Pool Account). Spoločný účet predstavuje skupinu používateľov, ktorí majú rovnaké lokálne práva a preto môžu na zdroji vystupovať pod jedným účtom, Obrázok 0-3. Hoci je na jednej strane administrácia spoločného účtu jednoduchšia, oveľa ťažšia alebo dokonca nemožná je spätná kontrola vykonaných operácií pre konkrétneho používateľa. Navyše každá entita patriaca do spoločného účtu môže pristupovať k dátam a programom iných používateľov patriacich do daného účtu, čo môže viesť nielen k neoprávnenému prístupu k dátam, ale používatelia nepriamo preberajú zodpovednosť za programy spustené inými entitami v rámci spoločného účtu a nesú dôsledky za akékoľvek porušenia, ktoré vykonal iný používateľ.

# Distinguished Name	*local User ID*
"/C=SK/O=SlovakGrid/O=UCM/CN=Ladislav Huraj"	.voce
"/DC=cz/DC=cesnet-ca/O=Masaryk University/CN=Vlasta Zakova"	.voce
"/C=SK/O=SlovakGrid/O=UMB/CN=Vladimir Siladi"	.voce

Obrázok 0-3 Príklad mapovania viac entít na jeden spoločný lokálny účet

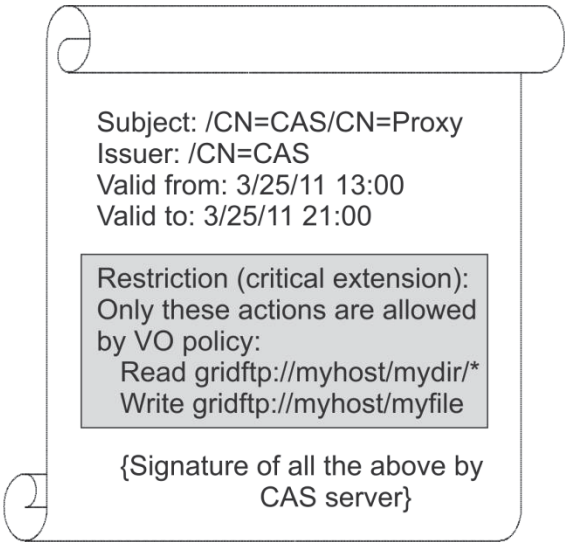
Nevýhodou mechanizmu *grid map file* je, že autorizačné povolenie je typu boolean, t. j. prístup je buď povolený, alebo zamietnutý, a neexistuje žiadny spôsob na vykonanie jemnozrnného povolenia umožňujúceho používateľom určité oprávnenia iné ako je len jednoduché členstvo vo VO. Preto je diferenciácia medzi používateľmi manažovateľná iba na lokálnej úrovni a môže odrážať len lokálne politiky a nie napr. politiku v rámci celej virtuálnej skupiny. Navyše, využívanie rôznych *grid map file* súborov pre rôzne oprávnenia používateľov pri prostrediach s veľkým počtom používateľov alebo

komplikovanou štruktúrou organizácie by znamenalo veľké a časté zmeny všetkých *grid map file* súborov pre všetky lokálne nastavenia [ACC+05].

Community Authorization Service (CAS)

Služba *Community Authorization Service (CAS)* umožňuje oddelenie bezpečnostnej politiky zdroja a VO politík, čím zlepšuje autorizačný proces používateľov. CAS predstavuje push model autorizačnej služby [L+03]. Hlavnou charakteristikou CAS je, že vlastník zdroja deleguje časť autorizačných práv správcom určitého spoločenstva (napr. VO administrátorom) a tak umožní správcom spoločenstva určiť, ktorí členovia daného spoločenstva môžu využívať tieto práva. Rovnako ako pri VOMS službe uvedenej nižšie, je dosiahnutie tohto cieľa realizované pomocou centrálneho CAS serveru, ktorý pôsobí ako dôveryhodná tretia strana medzi používateľmi VO a vlastníkom zdrojov. CAS server rozhodne, či má daný používateľ dostatočné oprávnenie a pridelí používateľovi práva na vykonanie požadovanej činnosti na základe roly, ktorú používateľa v spoločnosti zastáva, t. j. presadzuje sa *riadenie prístupu na základe rolí*.

CAS poskytuje škálovateľnosť čo do počtu používateľov a počtu virtuálnych organizácii. Každý používateľov musí byť známy a musí byť dôveryhodný pre CAS server, avšak to neplatí medzi používateľom a vlastníkom zdrojov. Obdobne, každý vlastník zdrojov musí byť pre CAS server takisto známy a dôveryhodný, ale nie pre každého používateľa. Ak sa však do úvahy berie veľký dopyt na zdroj, použitie jediného CAS servera nie je z pohľadu škálovateľnosti moc vhodné. Ak sa pokúsi príliš veľký počet používateľov o prístup na zdroj v rovnakom čase, môže sa jediný CAS server zahltiť, a tak sa stáva potenciálnym bodom zlyhania systému [JAE10].



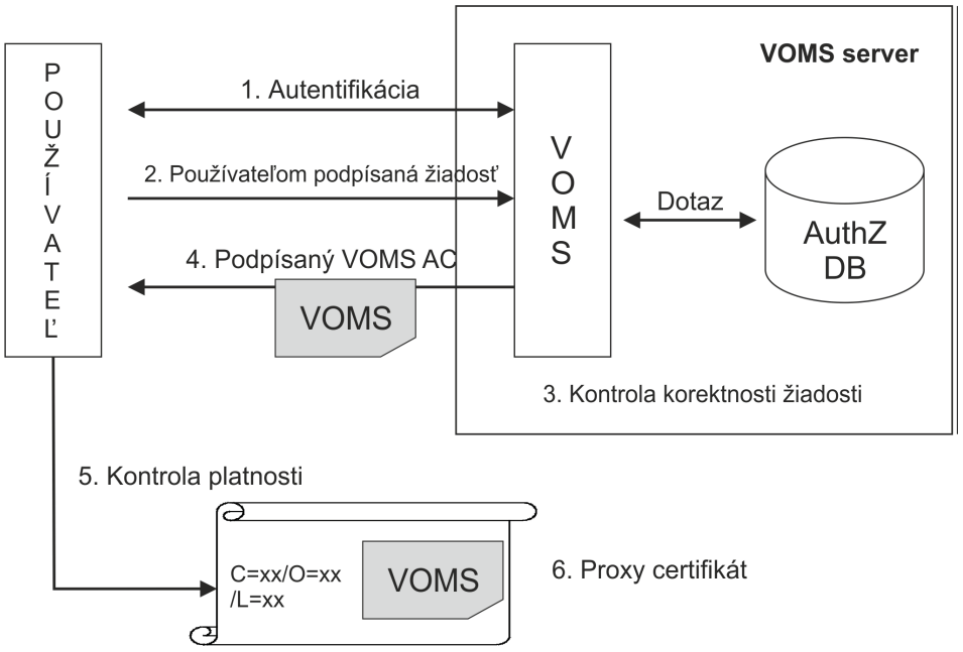
Obrázok 0-4 Príklad zjednodušeného proxy certifikátu vydaného CAS. Certifikát identifikuje používateľa ako člena VO a zoznam používateľských práv v rámci VO. [PKW+03].

Pri CAS mechanizme stačí, ak súbor *grid map file* obsahuje iba mená CAS serverov a nie všetkých VO používateľov.

Rozdiel medzi ďalej opísanou službou VOMS a CAS službou je predovšetkým vo vydaných potvrdeniach. CAS nevydáva atribútové certifikáty, ale celý nový proxy certifikát s označením CAS servera (CAS Server Distinguish Name) ako subjektom; autorizačná informácia je uložená ako položka rozšírenia v certifikáte, Obrázok 0-4. Druhý rozdiel je v jemnosti uvádzaných práv, kde CAS nezaznamenáva skupiny či roly, ale iba oprávnenia.

Služba VOMS

Služba *Virtual Organization Membership Service (VOMS)* bola vytvorená v spolupráci dvoch európskych projektov DataGrid a DataTAG na manažovanie autorizačných informácií o virtuálnych organizáciách. Každá virtuálna organizácia má svoj vlastný VOMS server a samostatnú databázu. VOMS sa používa na vytvorenie atribútových certifikátov umožňujúcich používateľovi prístup ku gridovým zdrojom a obsahujúcich informácie o VO používateľoch. VOMS môže byť tiež použitý pre generovanie súborov *grid map file* [ACC03].



Obrázok 0-5 VOMS.

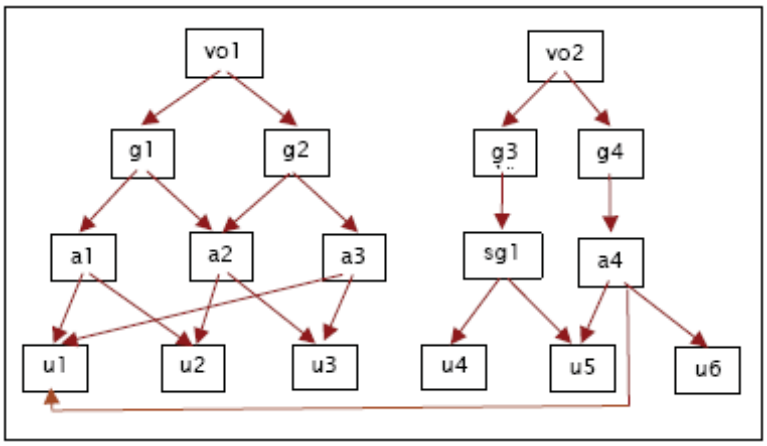
Informácie o roliach a oprávneniach používateľa v rámci virtuálnej organizácie sú v tomto mechanizme gridovým službám prezentované prostredníctvom rozšírenia proxy certifikátu, takže nie sú potrebné žiadne zmeny na úrovni komunikačného protokolu. V čase, keď je vytváraný proxy certifikát, je kontaktovaný jeden alebo viacero VOMS serverov. Každý VOMS server vráti atribútový certifikát (AC), ktorý je podpísaný za príslušnú virtuálnu organizáciu jej VOMS serverom a obsahuje informácie o členstve

používateľa v skupinách a jeho roly v rámci danej VO. Takýto systém umožňuje flexibilnú správu používateľských oprávnení, používateľ si môže vybrať aké skupiny alebo roly z priradených práv potrebuje pre svoju prácu. Napr. používateľ s administrátorskými právami tak môže pracovať so svojou bežnou identitou a oprávnením a len pre operácie súvisiace so správou použiť administrátorský certifikát. V tomto prípade sa jedná o autorizačný push model, Obrázok 0-5.

Ako už bolo spomenuté, VOMS proxy certifikát môže obsahovať informácie o členstve používateľa vo virtuálnej organizácii, vrátane informácií o tom, do ktorej *skupiny* (group) používateľ patrí a aké *roly* (role) má právo zastávať. Vo VOMS terminológii, skupina je podmnožina členov VO, ktorí zdieľajú rovnaké povinnosti a práva v rámci projektu. Skupiny sú usporiadané hierarchicky, začínajúce od koreňovej skupiny danej VO, a tvoria acyklický graf, kde uzly vytvárajú skupiny a podskupiny prepojené hranami, Obrázok 0-6.

Používateľ môže byť členom ľubovoľného počtu skupín a VOMS proxy certifikát obsahuje zoznam všetkých skupín, do ktorých používateľ patrí. Členstvo v skupine znamená aj členstvo vo všetkých nadskupinách, ktoré sú hierarchicky vyššie. Keď je vytvorený VOMS proxy certifikát, používateľ si môže vybrať jednu z týchto skupín ako primárnu skupinu.

Rola je atribút, ktorý obvykle umožňuje používateľovi získať špeciálne privilégiá na plnenie špecifických úloh. V rámci skupiny môže používateľ zastávať rôzne roly. Obrátené tvrdenie nie je vo všeobecnosti platné. V zásade sú skupiny spojené s oprávneniami, ktoré používateľ má, kým roly sú spojené s oprávneniami, ktoré používateľ zastáva len čas od času. Poznamenajme, že roly sú pripojené ku skupinám, t. j. roly v rôznych skupinách s rovnakým názvom sú rozdielne.



Obrázok 0-6 Hierarchické usporiadanie skupín do acyklického grafu; vo predstavujú VO, g sú skupiny, a atribúty v skupine a u sú používatelia s príslušnými priradeniami.

Navyše pre zvýšenie flexibility je tiež možné popísať špecifické vlastnosti a všeobecné informácie o používateľovi pomocou tzv. *spôsobilosti* (capability). Pomocou tejto

charakteristiky je možné pre používateľov zvýšiť na strane vlastníka zdrojov jemnozrnnosť oprávnení.

Skupiny, roly a spôsobilosti sú definované jednotlivými VO; môžu byť priradené k používateľovi pri inicializácii alebo pridané dodatočne. Skupiny, roly a spôsobilosti sú používateľovi určené *plným kvalifikovaným atribútovým menom* (Fully Qualified Attribute Name, FQAN). Formát je nasledovný:

`/VO[/group[/subgroup(s)]][/Role=role][Capability=cap].`

Príklad FQAN je uvedený na obrázku Obrázok 0-7.

```
/ voce
/ voce / production
/ voce / Role=VO-Admin
/ voce / production / Role=Admin
/ voce / production / Capability=long-jobs
/ voce / Capability=large-space
```

Obrázok 0-7 Príklad FQAN

```
subject   : /C=SK/O=SlovakGrid/O=UCM/CN=Ladislav Huraj/CN=proxy
issuer    : /C=SK/O=SlovakGrid/O=UCM/CN=Ladislav Huraj
identity  : /C=SK/O=SlovakGrid/O=UCM/CN=Ladislav Huraj
type      : proxy
strength  : 1024 bits
path      : /tmp/x509up_u797
timeleft  : 11:59:53
=== VO voce extension information ===
VO        : voce
subject   : /C=SK/O=SlovakGrid/O=UCM/CN=Ladislav Huraj
issuer    : /DC=cz/DC=cesnet-ca/O=CESNET/CN=voms1.egee.cesnet.cz
attribute : /voce/Role=NULL/Capability=NULL
timeleft  : 11:59:53
uri       : voms1.egee.cesnet.cz:7001
```

Obrázok 0-8 Príklad výpisu VOMS proxy certifikátu pomocou príkazu voms-proxy-info –all, kde vrchná časť zodpovedá proxy certifikátu a spodná VOMS rozšíreniu.

V tabuľke Tabuľka 0-1 je uvedená štruktúra VOMS atribútového certifikátu. Dátový typ *n* označuje číslo, *s* reťazec a *t* označuje ASN.1 reprezentáciu času. Certifikát môže obsahovať atribút s niekoľkými stavebnými blokmi. To umožňuje používateľovi rôznych VOMS serverov kontaktovať a zhromažďovať všetky údaje zhrnuté v proxy certifikáte.

Tabuľka 0-1: VOMS rozšírenie pre proxy certifikát [FC04].

ATRIBÚT	DÁTOVÝ TYP	VYSVETLENIE
Name:	Voms	Reason: Return Voms information
OID:	1.3.6.1.4.1.8005 .100.100.1	ID objekt pre VOMS
ŠTRUKTÚRA		
SIGLEN	n	dĺžka VOMS podpisu v bytoch
SIGNATURE	s	VOMS podpis
USER	s	DN používateľovho certifikátu
UCA	s	DN certifikačnej autority, ktorá vydala používateľov certifikát
SERVER	s	DN serverového certifikátu
SCA	s	DN pre CA, ktorá vydala certifikát servera
VO	s	meno VO, ku ktorej server patrí
TIME1	t	začiatok doby platnosti VOMS atribútu
TIME1	t	koniec doby platnosti VOMS atribútu
DATALEN	n	dĺžka dát
DATA		atribútové dáta vo forme <meno atribútu>: <hodnota atribútu >, napr. GROUP: s ROLE: s CAP: s

VOMS zlepšuje a prekonáva obmedzenia CAS systému opísaného v predchádzajúcej časti. CAS nevydá atribútové certifikáty, VOMS vydáva samostatné atribútové certifikáty, ktoré sú pridané ako rozšírenie k proxy certifikátu. Následkom toho je, že služba VOMS je viac zameraná na používateľa a na manažment oprávnení a umožňuje vlastníkom zdrojov robiť konečné autorizačné rozhodnutie na základe vlastnej interpretácii atribútových certifikátov vydaných VOMS serverom. VOMS navyše umožňuje hlavnému správcovi VO delegovať administráciu členstva používateľov na ďalších správcov a tak uľahčiť prácu a znížiť záťaž hlavného správcu VO [JAE10].

Štandard PERMIS

PERMIS (PrivilEge and Role Management Infrastructure Standard) je ďalšou z existujúcich autorizačných infraštruktúr, ktorá je založená na atribútoch zahrňujúca nasledujúce komponenty [L+03]:

i) autorizačnú politiku napísanú v XML, digitálne podpísanú a zabezpečenú ako X.509 atribútový certifikát,
ii) používateľské autorizačné tokeny, ktoré sú atribútovými certifikátmi zodpovedajúcimi štandardu X.509,
iii) jeden alebo viacero adresárových LDAP serverov, ktoré sa používajú na ukladanie atribútových certifikátov (politiky a autorizačných tokenov),
iv) Access Control Decision Function (ADF),
v) API funkciu k ADF, ktorá je volaná funkciou AEF,
vi) rôzne nástroje pre tvorbu atribútových certifikátov a politík.

Systém PERMIS pracuje v autorizačnom pull modeli. Používateľ kontaktuje zdroj (alebo presnejšie AEF zdroja), ktorý potom kontaktuje PERMIS ADF. PERMIS ADF robí rozhodnutia, na základe používateľských atribútov (získaných z používateľských atribútových certifikátov) a politiky zdroja, a vracia to AEF. AEF potom vynucuje toto rozhodnutie v mene zdroja. Rozhodovanie systému PERMIS sa deje v dvoch etapách. V prvej fáze, ktorá spravidla prebieha prihlásením používateľa, prebieha hodnotenie používateľových atribútových certifikátov podľa politiky a odmietnutie nedôvery-hodných používateľov. Platné atribúty sú ponechané a vrátené AEF. Druhá etapa, ktorá zvyčajne nastáva keď sa používateľ pokúsi vykonať nejakú akciu, je udelenie alebo odopretie na základe overených používateľových atribútov a politiky [CO02, L+03, JAE10].

Systém Shibboleth

Súčasné gridové riešenia sa v maximálnej miere snažia podporovať interoperabilitu medzi rôznymi organizáciami. V oblasti autorizácie sa preto skúmajú prístupy, ktoré sú schopné využívať a kombinovať autorizačné mechanizmy rôznych organizácií, pokiaľ možno bez zásahu používateľa tak, aby používateľ mohol voľne využívať rôzne služby ponúkané rôznymi organizáciami a pritom zostalo zachované požadované zabezpečenie a princíp Single Sign-on.

Uvedený prístup je veľmi dobre využiteľný aj mimo gridového prostredia. Príkladom je projekt Shibboleth[47], ktorý vznikol pre podporu digitálnych knižníc a má množstvo faktorov spoločných s gridovú problematikou. Shibboleth je orientovaný na prostredie webu a umožňuje, aby používateľ, ktorý pristupuje k webovému serveru, bol autorizovaný pomocou informácií, ktoré sú spravované jeho domovskou inštitúciou. Umožňuje tak, aby používateľ pristupoval k elektronickým zdrojom odkiaľkoľvek bez potreby dodatočného hesla. Organizácie tak napríklad nemusia nútiť používateľov, aby

[47] https://www.shibboleth.net/

používali proxy servery pre prístup k digitálnym knižniciam, ale používateľ môže priamo pristupovať k serveru knižnice, ktorý v mene používateľa kontaktuje domovský autorizačný server používateľa a je schopný prevziať a spracovať výsledok autorizačného procesu. Z pohľadu používateľa je dôležité, že celý proces je maximálne transparentný [Kou05].

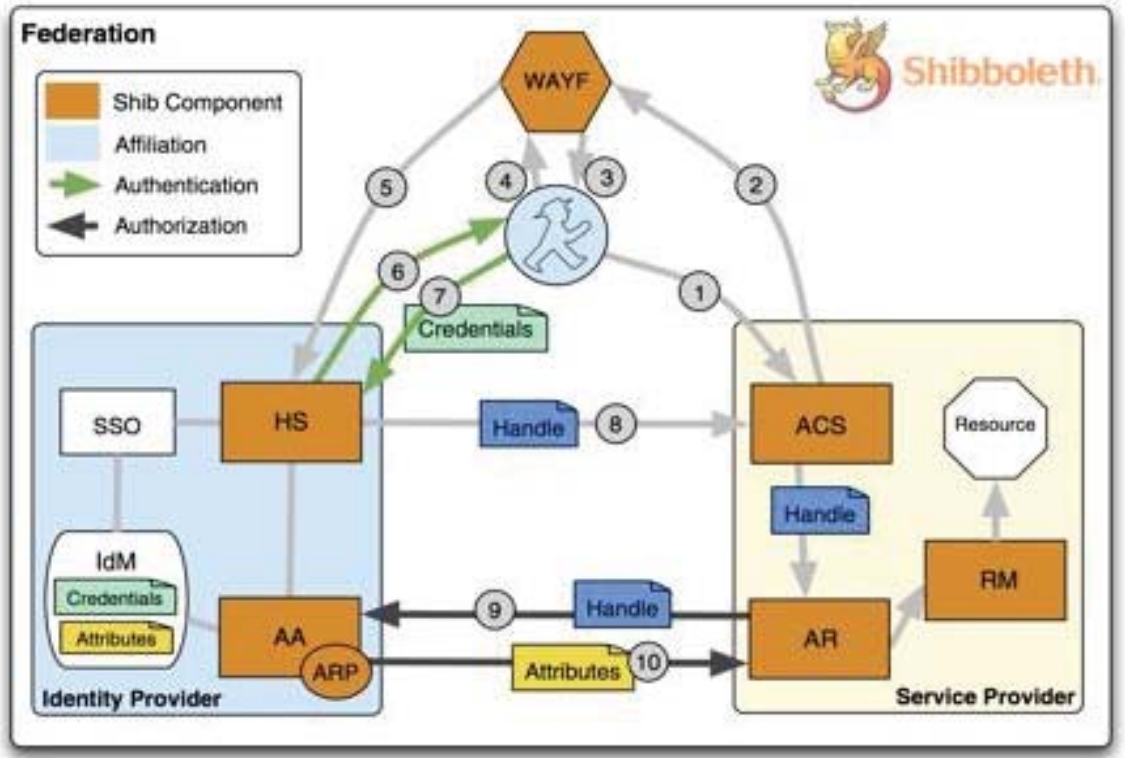
Shibboleth je teda autentifikačná a autorizačná federalizujúca architektúru. Z hľadiska autentifikácie, Shibboleth podporuje myšlienku budovania federácií spolupracujúcich organizácií, ktoré si vzájomne dôverujú pri autentifikácií používateľov. Takýmto spôsobom sa rozširujú možnosti lokálnych autentifikačných a autorizačných mechanizmov a systém umožňuje účastníkom federácie vzájomne využívať miestne bezpečnostné procedúry, pomocou čoho používateľ môže používať pre prístup k viacerým vzdialeným prostriedkom rovnaké prihlasovacie údaje ako pre svoj domáci lokálny prístup. Z hľadiska autorizácie, Shibboleth je mechanizmus založený na atribútoch a podporuje federatívne zdieľanie a prístup k zdrojom na základe používateľských atribútov. Presnejšie povedané, Shibboleth implementuje *SAML protokol* (Security Assertion Markup Language) pre bezpečný prenos informácií o identite používateľov medzi používateľskými organizáciami a poskytovateľmi zdrojov.

Ako je znázornené na Obrázok 0-9, medzi hlavné súčasti Shibboleth architektúry patrí poskytovateľ identity (Identity Provider, IdP), poskytovateľ služieb (Service Provider, SP) a služba *Where Are You From* (WAYF). Obvykle je poskytovateľ identity nainštalovaný na strane používateľskej domovskej organizácie, zatiaľ čo poskytovateľ služieb je nainštalovaný na strane vlastníka zdroja. Obrázok 0-9 tiež ilustruje proces prístupu používateľa k zdrojom, ktorý je realizovaný prostredníctvom interakcie komponentov systému Shibboleth. Charakteristickým rysom architektúry Shibboleth je, že sa spolieha na domáce inštitúcie používateľa pri vykonávaní autentifikácie používateľa a pre vykonávanie autorizácie sa spolieha na vlastníkov zdrojov a ich určenie prístupových práv pre daného používateľa. V dôsledku toho Shibboleth oddeľuje autentifikáciu používateľa vykonanú používateľovou domovskou inštitúciou a autorizáciu používateľa vykonanú vlastníkom zdrojov na základe získaných používateľských atribútov. Idea systému Shibboleth našla uplatnenie aj v gridovom prostredí [JAE10].

Zjednodušený postup autentifikácie a autorizácie, znázornený na obrázku Obrázok 0-9, prebieha nasledovne:

1. Používateľ sa snaží pristupovať ku zdroju, ktorý je lokalizovaný na strane poskytovateľa služieb SP.
2. Poskytovateľ služieb SP potrebuje identifikovať domovskú organizáciu, v ktorej je používateľ známy. Preto poskytovateľ služieb SP presmeruje používateľa na službu WAYF.
3. Služba WAYF zobrazí zoznam poskytovateľov identity.
4. Používateľ vyselektuje svojho poskytovateľa identity IdP, t. j. domovskú organizáciu.

5. WAYF service presmeruje používateľa na jeho poskytovateľa identity IdP.
6. Jeho domovská organizácia skontroluje, či je používateľ legitímny alebo nie. Ak nie, požiada používateľa o jeho prihlasovacie poverenia.
7. Používateľ poskytne svoje poverenia domovskej organizácii.
8. Následne po úspešnom autentifikovaní poskytovateľ identity IdP vytvorí správu Handle a pošle ju poskytovateľovi služieb SP.
9. Poskytovateľ služieb SP pošle atribútovú požiadavku o používateľovi poskytovateľovi identity IdP zaslaním prijatej správy Handle.
10. Atribútová autorita (AA) verifikuje správu Handle. Po úspešnej verifikácií AA podľa pravidiel Attribute Release Policy rozhodne či pošle atribúty poskytovateľovi služieb SP. Následne Resource Manager na strane poskytovateľa služieb vykoná autorizáciu používateľa podľa zaslaných atribútov.



Obrázok 0-9 Architektúra Shibboleth a interakcia jej komponentov [MSZ07].

V gridovom prostredí býva samotným problém zapísanie prístupovej politiky, pretože faktorov, ktoré ju ovplyvňujú, môže byť veľmi veľa a sú veľmi rôznorodé. Často nepostačuje iba jednoduchý statický zoznamom používateľov, príp. skupín, ktorý je zapísaný v konfigurácii služby, ale výsledná prístupová politika je tvorená ako výsledok vyhodnotenia množstva čiastkových pravidiel. Napríklad vedúci gridového projektu môže definovať skupinu používateľov, ktorí môžu používať výpočtové prostriedky priradené tomuto projektu, ale lokálne správcovia týchto prostriedkov môžu definovať vlastnú prístupovú politiku, ktorá musí byť tiež vyhodnotená. Príkladom môže byť situácia, kedy lokálny správca chce preferovať používateľa pochádzajúceho z lokálnej

inštitúcie pred ostatnými, ktorým je prístup povolený iba v okamihu, kedy výpočtové prostriedky nie sú zaťažené. Takýchto pravidiel môže byť množstvo, môžu byť definované na viacerých miestach a vyhodnocovanie prístupovej politiky je potom veľmi zložitý proces. Tieto problémy vyústili v definovaní jazykov založených na XML, ktoré umožňujú štandardizovaným spôsobom zapísať aj zložité prístupové politiky a tiež ponúkajú nástroje pre efektívne spracovanie týchto pravidiel.

V oblasti autorizácie sa gridové prostredia snažia priblížiť a využiť výsledky, ktoré sú dostupné v oblasti webových služieb. Najmä spomínané spracovanie pravidiel pre riadenie prístupu je založené na výsledkoch z oblasti webových služieb a štandardov. Novým smerovaním v tejto oblasti je práve jazyk SAML, značkovací jazyk pre presadzovanie zabezpečovacích postupov, ktorý je založený na jazyku XML (eXtensible Markup Language) a slúži k výmene atribútov a informácií pre autentifikáciu a autorizáciu.

Pomocou SAML potvrdení môže byť presadzované, že sa jedná o daného používateľa a ten má navyše určité privilégiá. SAML dokument môže byť digitálne podpísaný pomocou XML podpisu a/alebo zašifrovaný pomocou XML šifrovania. SAML systém poskytuje distribúciu informácií medzi určitou platformou a organizáciou. Napr. nejaký portál autentifikuje Alicu a vie, že Alice má vymedzenú rolu, t. j. určité privilégiá. Portálová aplikácia to pomocou štandardu SAML pripojí k požiadavke zaslanej ďalšej webovej službe. Webová služba sa pozrie na portálovú identitu, overí digitálny podpis portálu a povolí alebo zakáže prístup používateľa vzhľadom k jeho roli. SAML štandard nahrádza, resp. rozširuje mechanizmy používané pri všetkých typoch certifikátov. Shibboleth je pomocou SAML štandardu schopný vyriešiť problém vzájomného prepojenia bezpečnostných politík disjunktných organizácií bez nutnosti využívať tretiu dôveryhodnú stranu, ako tomu bolo pri štandarde X.509 [Kou05, HS09b].

GridShib

Vzhľadom k podobným cieľom, ktoré Shibboleth a gridy majú, vznikol nový projekt GridShib, ktorý sa snaží o väčšie prepojenie gridov a princípov, na ktorých je Shibboleth založený. GridShib je softvérový produkt, ktorý umožňuje prevádzkyschopnosť medzi Globus Toolkit a Shibboleth. Kompletný softvérový balík pozostáva z dvoch modulov: jeden pre Globus Toolkit (GT) a ďalšie pre Shibboleth. S oboma nainštalovanými a nakonfigurovanými modulmi môže gridová služba *GT Grid Service Provider* bezpečne žiadať používateľské atribúty od služby *Shibboleth Identity Provider* [BBF+06].

Zhrnutie

Gridové prostredie si vyžaduje osobité autentifikačné aj autorizačné procesy. Tabuľka 0-2 ukazuje stručný súhrn jednotlivých gridových autentifikačných a autorizačných infraštruktúr, ktoré boli detailnejšie opísané v predchádzajúcich častiach. Okrem toho, že je každé z tý0063hto riešení zamerané na konkrétny bezpečnostný mechanizmus autentifikácie alebo autorizácie, má každý z nich isté výhody, ale aj nevýhody. A preto

iba jedna jediná z uvedených infraštruktúr nemusí spĺňať všetky potrebné bezpečnostné požiadavky vznesené rôznymi aplikačnými doménami.

Tabuľka 0-2: Zhrnutie hlavných gridových autorizačných infraštruktúr [JAE10].

	Funkcionalita	**Použiteľnosť**	**Riadenie prístupu**	**Škálovateľ-nosť**	**Administratívna záťaž**
Grid map file a proxy certifikáty	Autentifikácia a obmedzená autorizácia	Ťažkopádny autentifikačný aj autorizačný proces	Hrubozrnné riadenie prístupu z hľadiska autorizácie	Nie je škálovateľné pre rozsiahle gridové VO	Veľká záťaž pre poskytovateľov zdrojov
Shibboleth	Autentifikácia aj autorizácia	Dobrá použiteľnosť pri autentifikácii	Jemnozrnné riadenie prístupu z hľadiska autorizácie	Dobre škálovateľné pre rozsiahle gridové VO	Malá záťaž pre poskytovateľov zdrojov
CAS	VO systém riadenia ako základ pre autorizáciu založenú na roliach používateľov	Jednoduché rozhranie pre používateľský manažment	Jemnozrnné riadenie prístupu z hľadiska autorizácie	Nie je dobre škálovateľné v prípadoch veľkého počtu prístupov	Veľká záťaž pre VO administrátorov
VOMS	VO systém riadenia ako základ pre autorizáciu založenú na atribútoch	Jednoduché rozhranie a nástroje pre VO manažment	Jemnozrnné riadenie prístupu z hľadiska autorizácie	Poskytuje lepšiu škálovateľ-nosť ako CAS	Malá záťaž pre VO administrátorov