

Autentifikácia v Grid

Adrian Bagala
FIIT STU Bratislava

GCCP2005

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Bezpečnosť

- Utajenosť
- Integrita
- Autenticita
- GSI (Grid Security Infrastructure)

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Autentifikácia

- overenie identity entity
- entita:
 - používateľ
 - aplikácia, proces
- X.509 certifikát
- proxy certifikát

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

X.509 certifikát

- ID a meno subjektu
- verejný kľúč subjektu
- identifikátor certifikačnej authority, ktorá podpisuje daný certifikát
- digitálny podpis certifikačnej authority

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

X.509 certifikát

- **Súkromný kľúč**
 - šifrovaný
 - zabezpečený dodatočnou autentifikáciou - heslom
 - práva čítania vlastníka
- **Jednosmerná autentifikácia**
- **Vzájomná autentifikácia**
- **Dôveryhodnosť - CA**

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Proxy certifikát

- **Nový certifikát**
 - odvodený od X.509 cert.
 - identita vlastníka, ktorá je mierne pozmenená
 - verejný kľúč
 - podpísaný jeho vlastníkom
 - krátkodobá platnosť (12h)

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Proxy certifikát

- **Súkromný kľúč**
 - nešifrovaný
 - práva čítania vlastníka
 - chránený samotným súborovým systémom

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Single sign-on

- X.509 certifikát - manuálna autentifikácia
 - pri každom použití je nutnosť dodatočnej autentifikácie
 - potreba neustálej prítomnosti používateľa
 - obmedzujúce

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Single sign-on

- Proxy certifikát – opakovaná autentifikácia
 - dodatočná autentifikácia len pri vytváraní
 - single sign-on
 - možnosť opakovaného použitia s krátkou dobou platnosti
 - ochrana spriazneného X.509 cert.

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Delegovanie

- Používateľ Grid systému
 - prístupuje k Grid prostriedkom a službám
 - pri každom prístupe sa autentifikuje X.509 cert. alebo proxy cert.
 - spúšťa rôzne procesy a aplikácie

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Delegovanie

- **Procesy a aplikácie**
 - prístupujú a využívajú Grid služby a prostriedky
 - vykonávajú úlohy v mene používateľa
 - nutnosť autentifikácie

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Delegovanie

- Proxy certifikáty
 - delegovanie oprávnení na spustené procesy a aplikácie
 - možnosť vykonávania úloh v mene používateľa
 - možnosť autentifikácie bez potreby zadania autorizačnej frázy (single sign-on)

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Globus Toolkit 4.0

- open source nástroj na tvorbu grid systémov
- autentifikácia certifikátmi
 - X.509 cert.
 - proxy cert. (single sign-on, delegovanie)
- nutnosť dôvery
 - vhodná konfigurácia
 - import certifikátov dôveryhodných CA
 - súbor podpisových politík

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Globus Toolkit 4.0

Generovanie X.509 cert.

- `grid-cert-request`
 - súkromný kľúč
 - šifrovaný
 - autorizačná fráza (heslo)
 - právo na čítanie len pre vlastníka
 - certifikačná žiadosť
 - podpis CA = certifikát (právo na čítanie pre všetkých používateľov)

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Globus Toolkit 4.0

Generovanie proxy cert.

- `grid-proxy-init`
 - nový súkromný kľúč
 - proxy certifikát
 - verejný kľúč
 - podpísaný súkromným kľúčom používateľa
 - rozšírený názov subjektu
 - krátka doba platnosti (12h)

Bezpečnosť

Autentifikácia

X.509 certifikát

Proxy certifikát

Single sign-on

Delegovanie

Globus Toolkit

Globus Toolkit 4.0

- proxy súbor
 - proxy verejný kľúč
 - proxy súkromný kľúč
 - X.509 verejný kľúč
 - /tmp adresár
 - práva na čítanie a zápis len pre vlastníka

Ďakujem za pozornosť!