

MediGrid a bezpečnost

Michal Procházka, Daniel Kouřil
{michalp,kouril}@ics.muni.cz

Masarykova Universita

Horní Cerekev 10. 5. 2007

Oblasti zájmu

- TPM - Trusted Platform Module
- Federace

TPM - Bezpečnostní zařízení

- Pevně svázáno se základní deskou
- Poskytuje kryptografické operace
- Kontrola stavu systému (BIOS, operační systém, soubory, ...)
- Využívá PKI

TPM a MediGrid

- Běh webové služby v kontrolovaném prostředí
- Ověření "pravosti" webové služby
- Bezpečné uložení privátního klíče od certifikátu webové služby
- Nemožnost vytvářet falešné webové služby

Federace

- Decentralizovaná správa uživatelů
- Vybudované vztahy důvěry
- Bezpečná autentizace
- Podpora autorizace

Federace a MediGrid

- Identity Management omezen pouze na data nutná pro MediGrid
- Aktuálnost a pravost informací o uživateli
- Podpora autorizace

- Funkční server s TPM a podporou PKCS#11
- Spuštění kontrolovaného prostředí
- Migrace klíčů

- Middleware pro federace - Shibboleth
- Zprovoznění IDP

Děkuji za pozornost.