



**Důvěřujte
JEN PROVĚŘENÝM...**

Personal Identity Verification

Pavel Dobiš, ICT Security Architect

Personal Identity Verification

Agenda

Aplikace PIV v MO USA

Architektura PIV

Fyzická bezpečnost a PIV

Informační bezpečnost a PIV

Co je to PIV

Personal Identity Verification není Pivo :o)

- Soubor lidí, procesů a technologií poskytující jednotnou identifikační kartu prostřednictvím nichž lze provádět bezpečnou identifikaci respektive autentizaci
- Standardizován a popsán v mnoha standardech



Fyzický přístup



Logický přístup



Vzdálený přístup



El. podepisování

PIV Standardy

Standards	FIPS 201	Personal Identity Verification (PIV) of Federal Employees and Contractors.
	FIPS 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors (chng1)
Implementation Guide	SP 800-73	Interfaces for Personal Identity Verification (4 parts): 1- End-Point PIV Card Application Namespace, Data Model and Representation 2- End-Point PIV Card Application Interface 3- End-Point PIV Client Application Programming Interface 4- The PIV Transitional Data Model and Interfaces
	SP 800-76	Biometric Data Specification for Personal Identity Verification
	SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
	SP 800-79	Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)
	SP 800-87	Codes for Identification of Federal and Federally-Assisted Organizations
Test Guidelines	SP 800-85	
	SP 800-85A	PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance)
	SP 800-85B	PIV Data Model Test Guidelines

PIV není o jednom výrobci





APLIKACE PIV V USA MO

12.11.2013

Personal Identity Verification

Ministerstvo obrany USA



Standardizovaná karta

■ Centralizovaná bezpečnost

- Access Control Rule & Global PIN management

■ Obecný kontejner (on-card buffers)

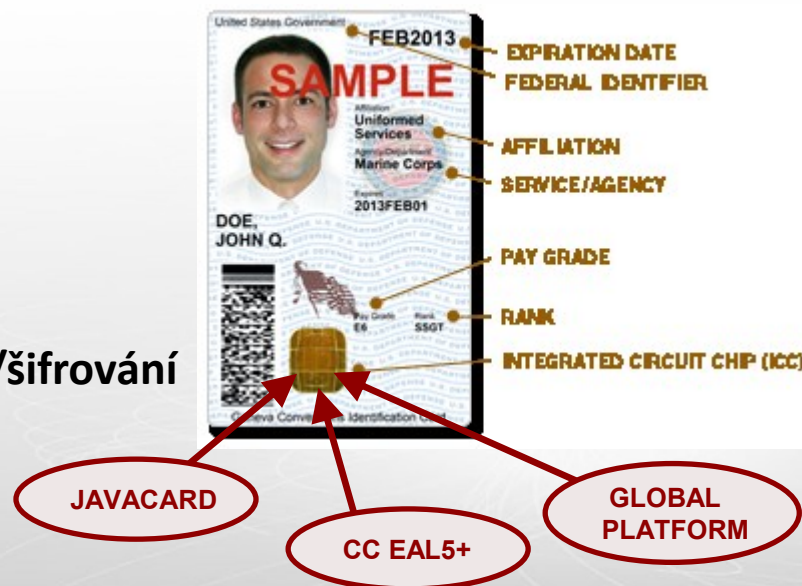
- Zaměstnacké ID
- Zdravotnické informace
- PIV Identita (id, obličej, otisk prstu)

■ PKI pro autentizaci (login), el. podpis/šifrování

- RSA Key Pairs/ X.509 Certifikáty

■ Další oblasti

- Vícenásobné Global Platform domény
- Plug-in podpora



Souhrn

- Centrální místo využíváno pro MO USA (Army, Air Force, Navy, Marines) a 25+ agentur
- 30M+ karet nasazeno v rámci PIVu
- 3.8M aktivních karet denně k přístupu k PC, ochraně emailu a digitálně podepsaných dokumentů
- 2.8M vydaných karet za rok
- Přes 11,000 vydaných karet denně
- Přes 2600 operátorských stanic v 1000 lokalitách ve 27 zemích
- Užívané v neklasifikovaných, ale i ve velmi citlivých prostředích
- Snížení počtu útoků o 46%

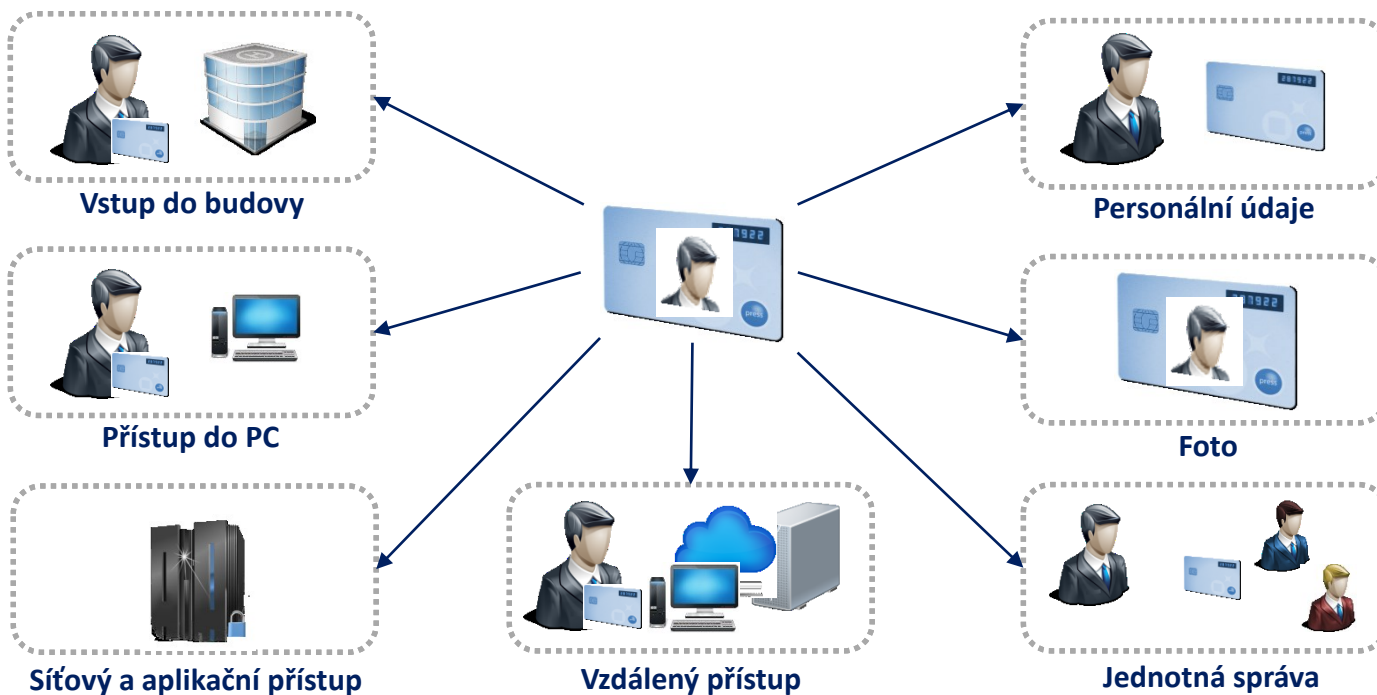


ARCHITEKTURA PIV

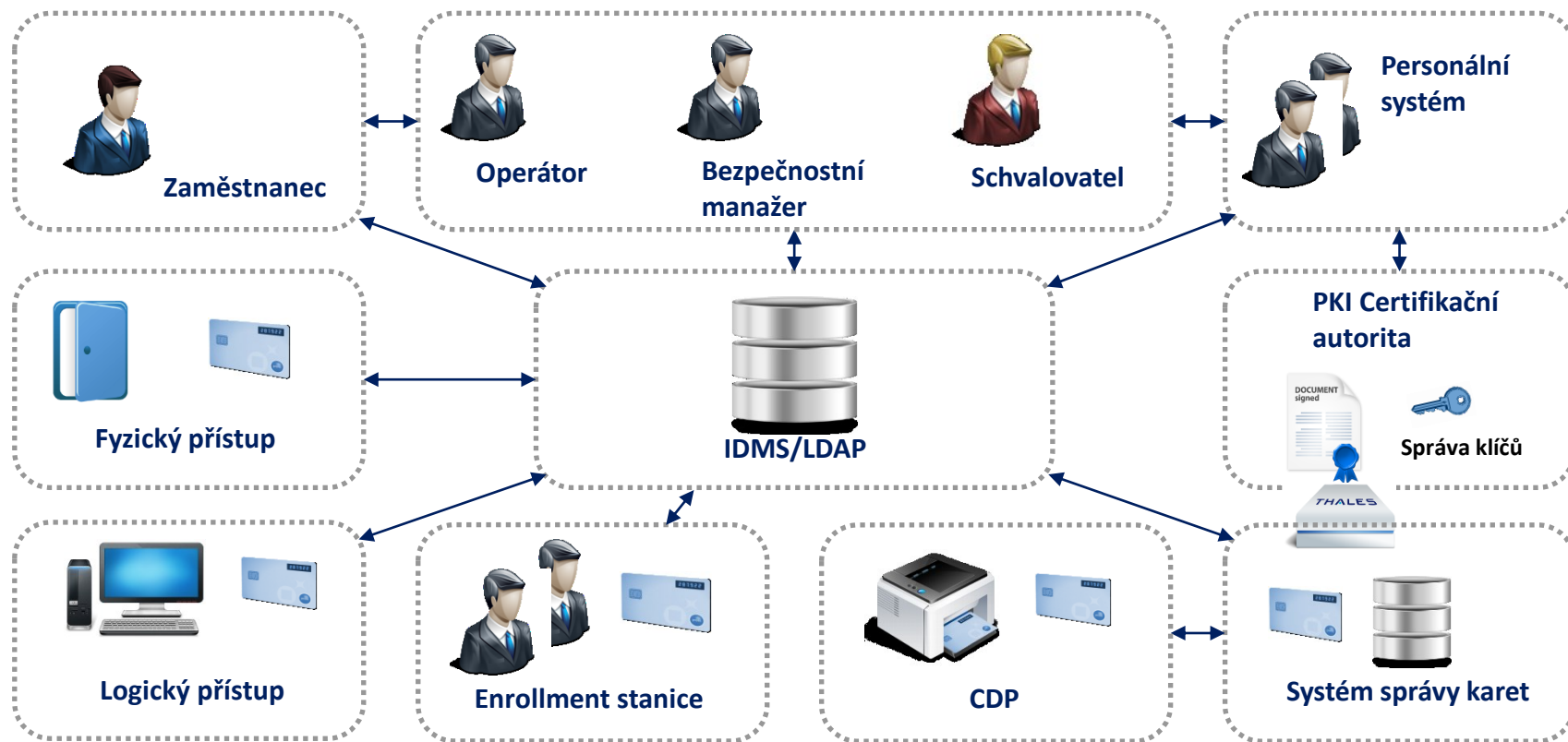
12.11.2013 Personal Identity Verification

Jak vidí PIV uživatel?

Uživatelský pohled



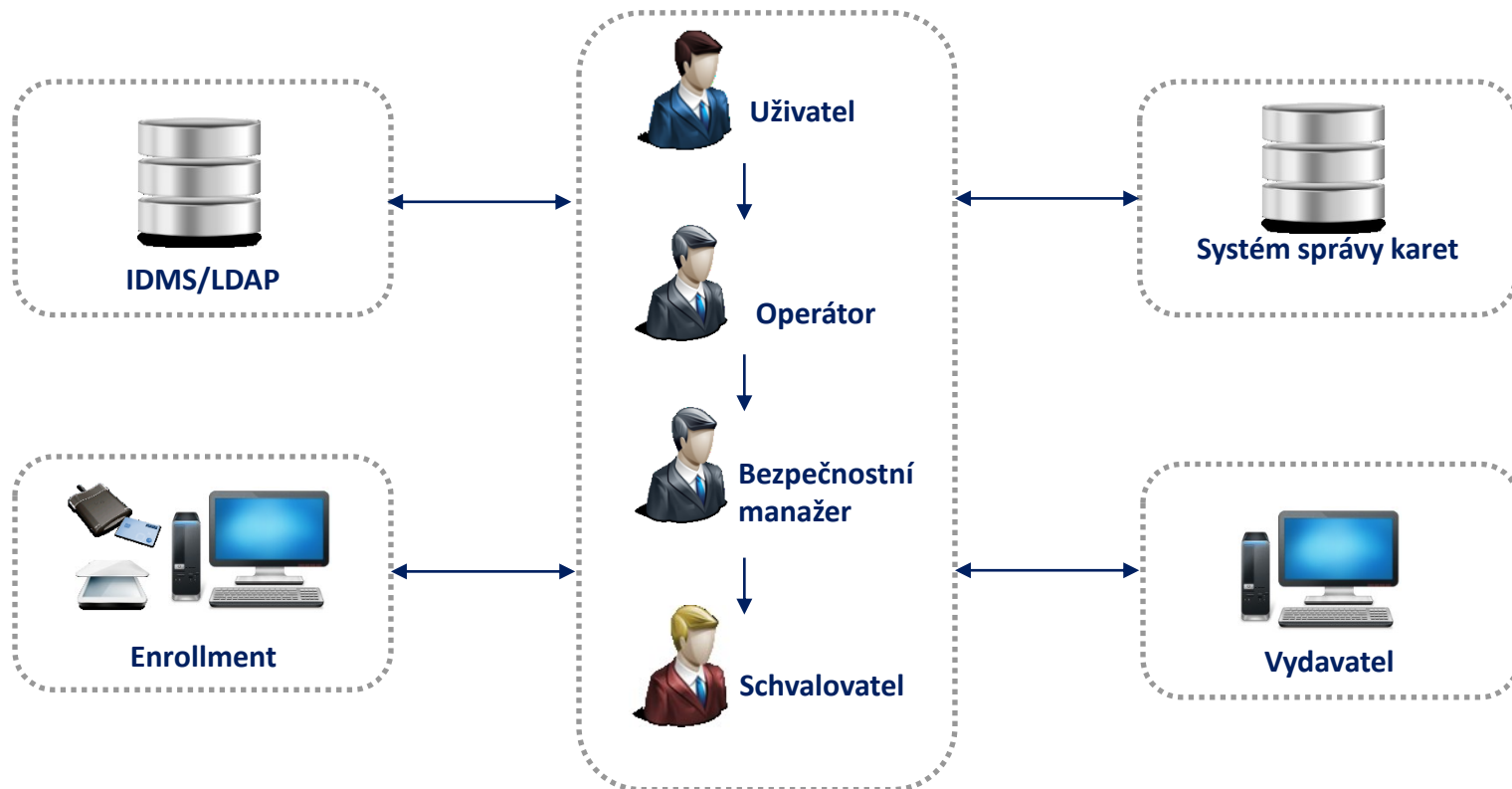
Architektura standardu PIV



Typické role standardu PIV

Role	Odpovědnost
Zaměstnanec	předat doklady potvrzující prokazovanou totožnost
Bezpečnostní manažer	zodpovídá za bezpečnostní otázky
Schvalovatel	zdůvodňuje potřeby zavedení identity a provádí její autorizaci
Operátor	služby podporující prokázání identity
Vydavatel	na základě schváleného požadavku provádí vydání karty s příslušnými oprávněními

Ověření identity a vydání karty





FYZICKÁ BEZPEČNOST A PIV

12.11.2013 Personal Identity Verification

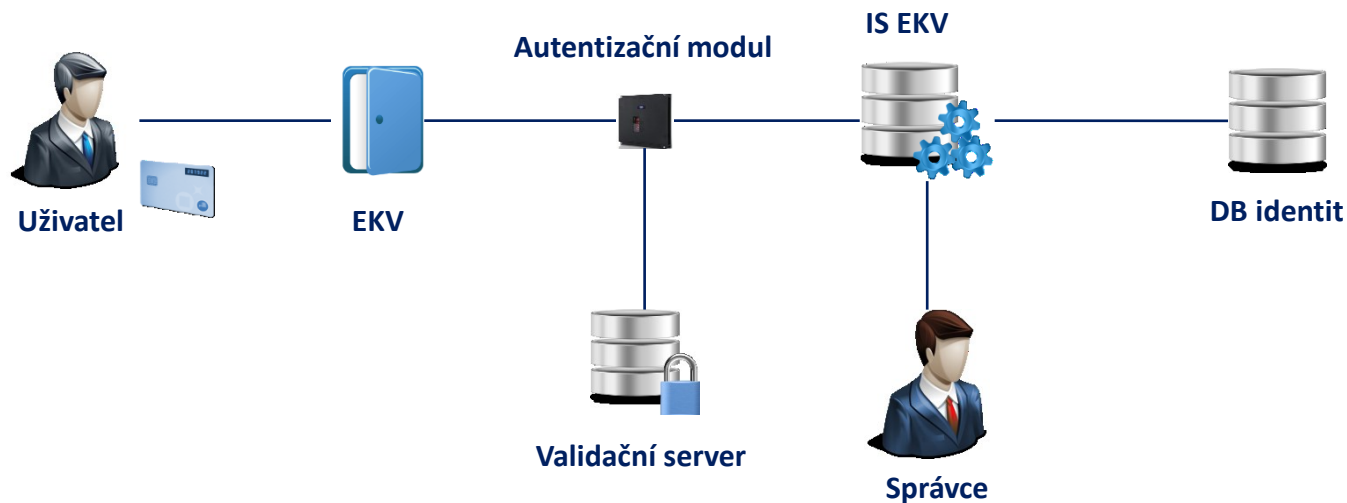
Autentizační metody

Odolnost metody oproti hrozbám

autentizační metody	zablokování		padělání		klonování		ztráta		sdílení	
FASC-N										
CHUID+VIS										
CAK										
PIV+PIN										
PIV+PIN+BIO										

Architektura fyzické autentizace

srovnání s PIV



PIV Autentizační modul

- **Podporované protokoly:**
 - PIV (RS 485)
 - Wiegand
- **Podpora až 2 čteček**
- **Certifikováno dle FIPS 140-2 Level 1**
- **Certifikován dle PIV standardu**

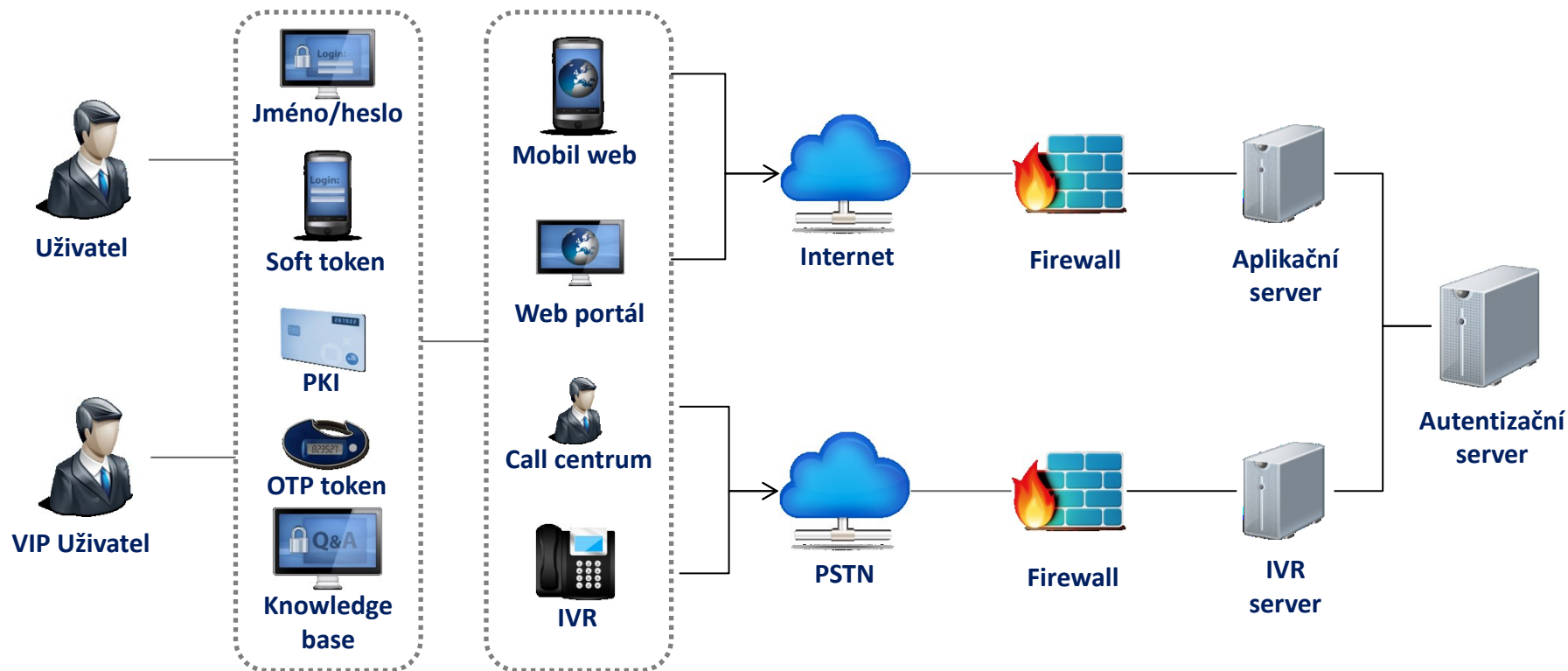




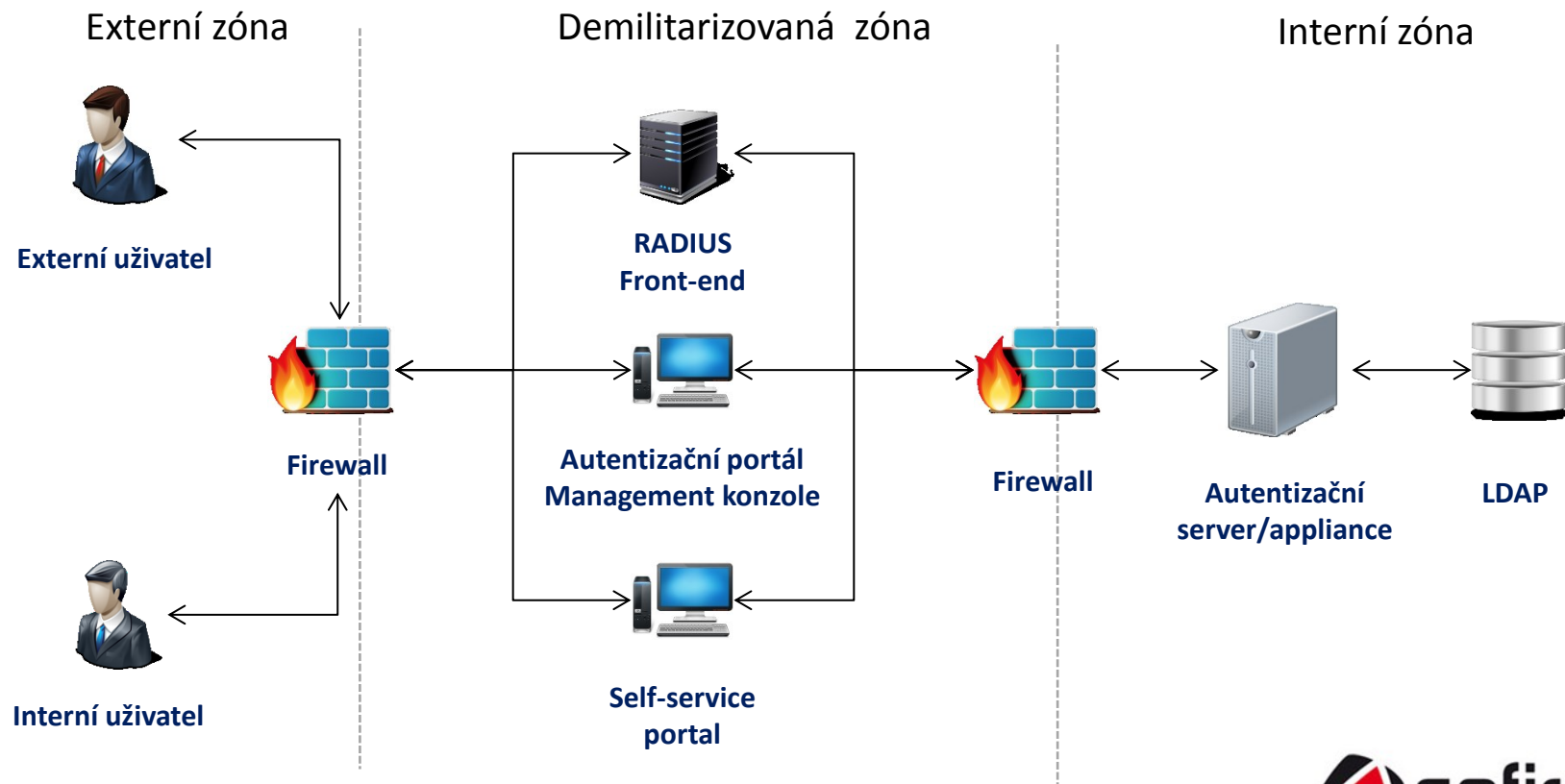
INFORMAČNÍ BEZPEČNOST A PIV

12.11.2013 Personal Identity Verification

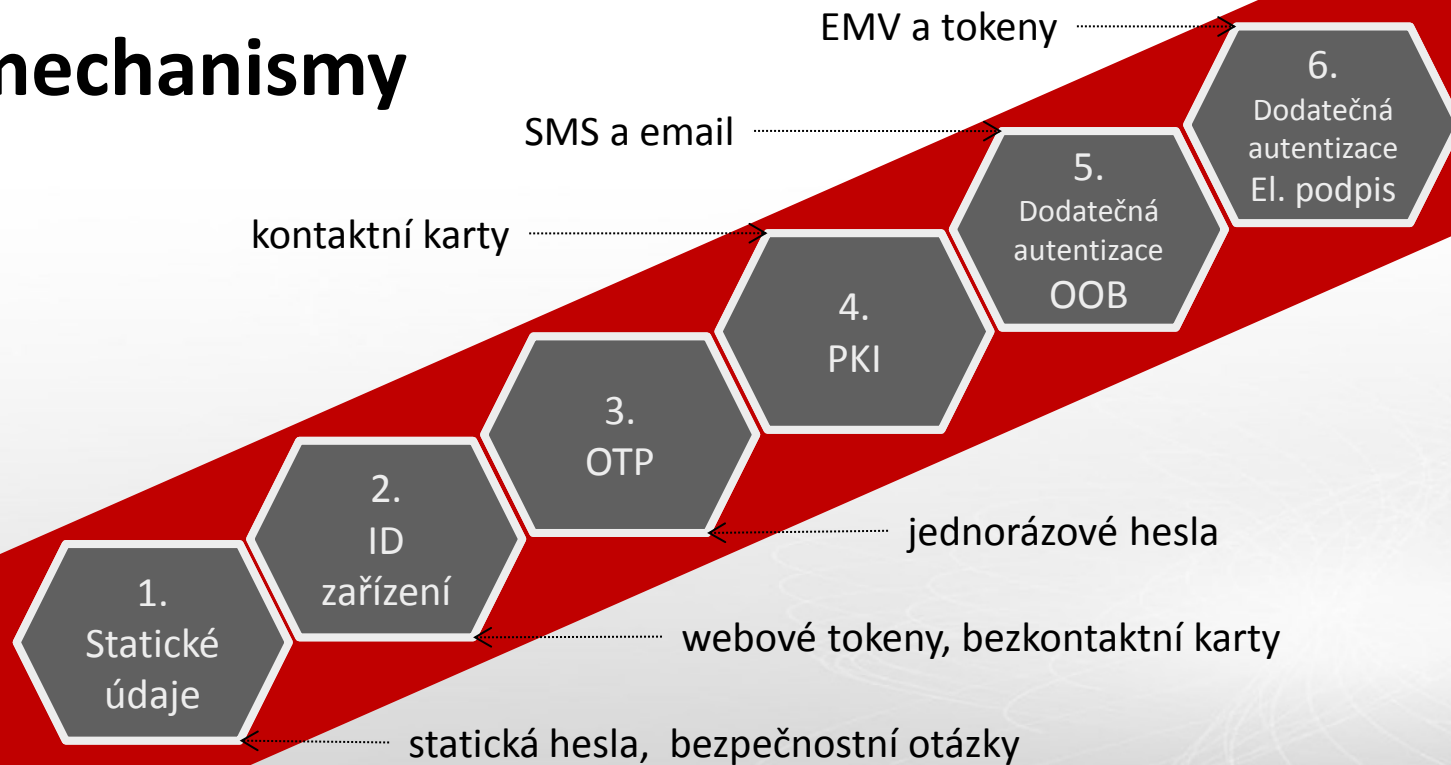
Architektura logické autentizace



Architektura v kontextu infrastruktury



Autentizační mechanismy



Přínosy PIVu

Efektivní kombinace autentizačních metod a nástrojů

Maximalizace uživatelského komfortu při zachování vysoké bezpečnosti

Využití stávajících autentizačních nástrojů

Sjednocení fyzického a logického přístupu

Podpora pro Self-Enrollment

Jak zavádět PIV

- **Procesně je PIV prakticky ve většině organizací již zaveden**
- **Fyzická bezpečnost**
 - Technologicky je nutné PIV zavádět po etapách
- **Informační bezpečnost**
 - Nezávisle na fyzické bezpečnosti lze využívat i karty pro autentizaci

Děkuji za pozornost

Pavel Dobiš

dobis@sefira.cz

