ZIFO, AIFO a bezpečnost osobních údajů v systému ZR

Ing. Eva Vrbová

ředitelka Odboru základních identifikátorů

Hradec Králové
2.–3. 4. 2012

úřad pro ochranu osobních údajů
the office for personal data protection

INTEGROVANÝ OPERAČNÍ PROGRAM

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ

isss
Internet ve státní správě a samosprávě
LOCAL AND REGIONAL INFORMATION SOCIETY
Vsegrádská konference, Y4DIS

Agenda

- Postavení informačního systému ORG
- Aktuální problematika zavedení AIFO do praxe
- Principy odvození ZIFO a AIFO
- Bezpečnost na prvním místě
- Řešitel IS ORG
- ORG je připraven na ověřovací provoz

Informační systém ORG

- je specifický informační systém ZR
- generuje a přiděluje identifikátory ZIFO, AIFO a vede jejich evidenci
- je jediným místem, které umí provázat AIFO jedné a téže fyzické osoby v různých agendách
- komunikuje s okolím výhradně a pouze jen prostřednictvím ISZR
- oprávnění pro přístup ke službám ORG je řešeno centrálně na úrovni ISZR a RPP

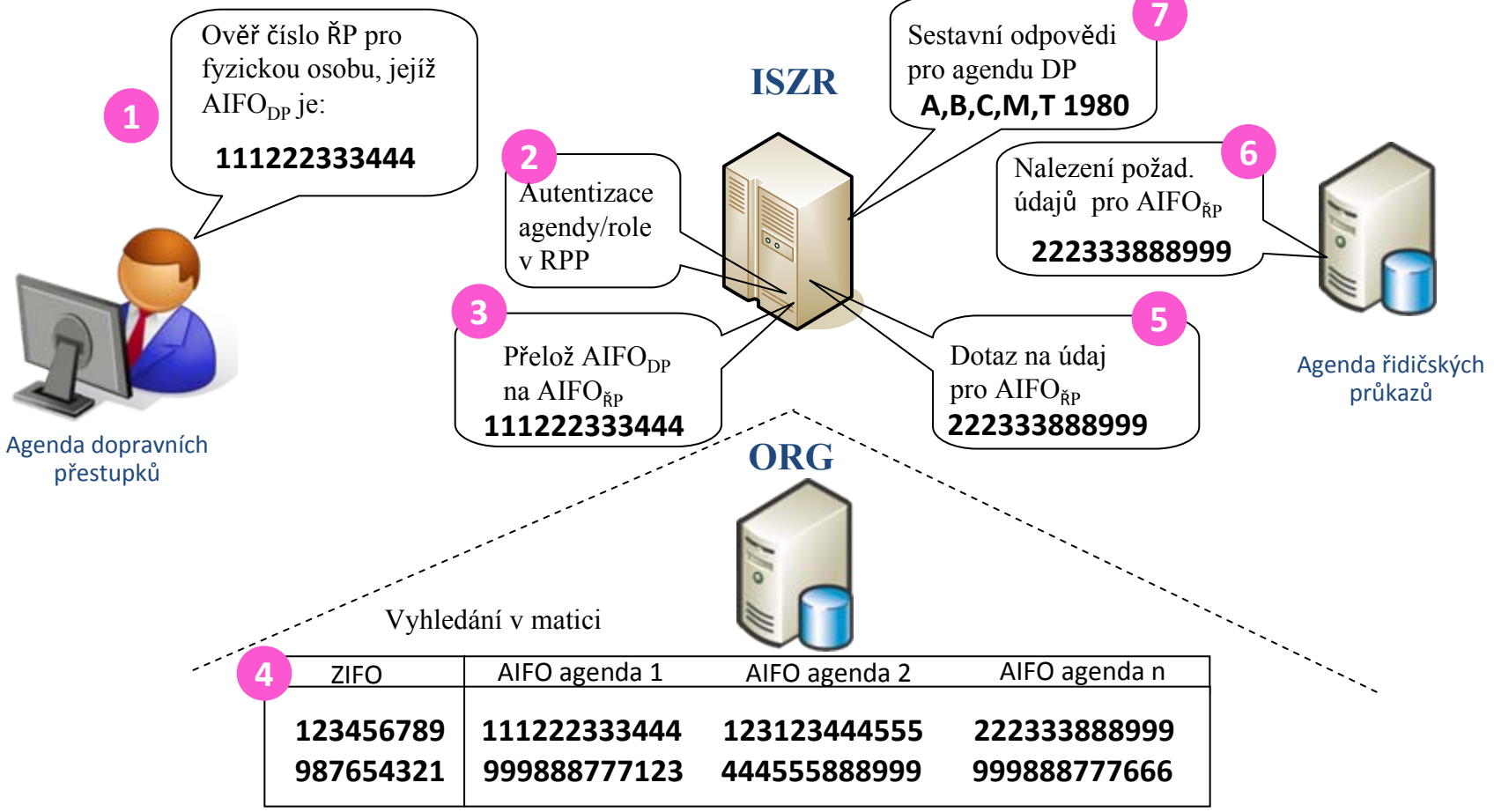
K čemu vlastně AIFO slouží?

- AIFO je bezvýznamový identifikátor fyzické osoby v agendě
- AIFO je v podstatě „klíčem“ pro sdílení dat mezi ZR a AIS v prostředí eGovernmentu
- Předávaná data není možní bez znalosti vazeb mezi AIFO jedné osoby propojovat
- AIFO chrání před neoprávněným sdružováním dat charakteru osobních údajů

K čemu vlastně AIFO slouží?

- Zavedení AIFO neovlivní užití stávajících identifikátorů: RČ, číslo pojištěnce…
- AIFO se může za života fyzické osoby v odůvodněných případech měnit
- AIFO = vícenásobná digitální identita občana

Jak je matice AIFO používána?



Matice AIFO v praxi

- 1 agenda v jednom AIS = ideální stav
- 1 agenda provozována více AIS = realita
- „n“ agend v jednom AIS
  - pozor na zákon č. 101/2000 Sb. o ochraně osobních údajů, §5 odst. 1 písm. h):

„nesdružovat osobní údaje, které byly získány k rozdílným účelům“

Jak AIS takové AIFO obdrží?

1. AIS iniciuje vyhledání osoby v ROB

2. Nalezené $AIFO_{ROB}$ je převedeno prostřednictvím ORG na $AIFO_{AIS}$

3. Dále komunikuje AIS se systémem ZR již jen prostřednictvím přiděleného AIFO

Speciální případy AIFO

- V důsledku zjištěných chyb v evidenci fyzických osob v agendě primárního editora může dojít k:
  - SLOUČENÍ OSOBY
  - ROZDĚLENÍ OSOBY
  - ZRUŠENÍ OSOBY
- Stávající ZIFO a příslušná AIFO jsou zneplatněna (nelze je dále používat)
- Jsou vygenerována nová ZIFO & AIFO
- O změnách je AIS informován notifikačními službami

Jak bude AIS aktualizovat data?

1. Aktualizace prostřednictvím notifikací
2. AIS musí přihlásit v ORG AIFO k odběru notifikací
3. AIS volá notifikační služby „*robCtiZmeny*“ nebo „*orgCtiZmenyAIFO*“
4. AIS obdrží selektivní seznam AIFO,u kterých došlo ke změně
5. AIS pomocí služby ROB „*robCtiAIFO*“ získá aktuální referenční údaj, který použije pro aktualizaci své evidence

Principy odvození ZIFO

- ZIFO je generováno jako náhodný řetězec požadované délky pomocí generátoru náhodných čísel v HSM, který pracuje na principu fyzikálních jevů
- ZIFO je navrženo v dostatečné délce, aby nebyla možná jeho zpětná rekonstrukce z AIFO

Principy odvození ZIFO

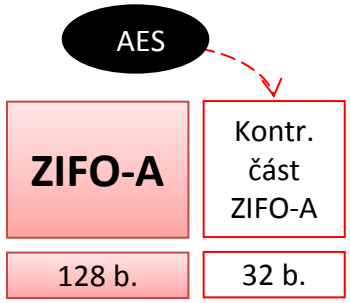
- ZIFO je složeno ze 2 samostatných, avšak vzájemně a nezaměnitelně propojených částí
  - ZIFO-A
  - ZIFO-B

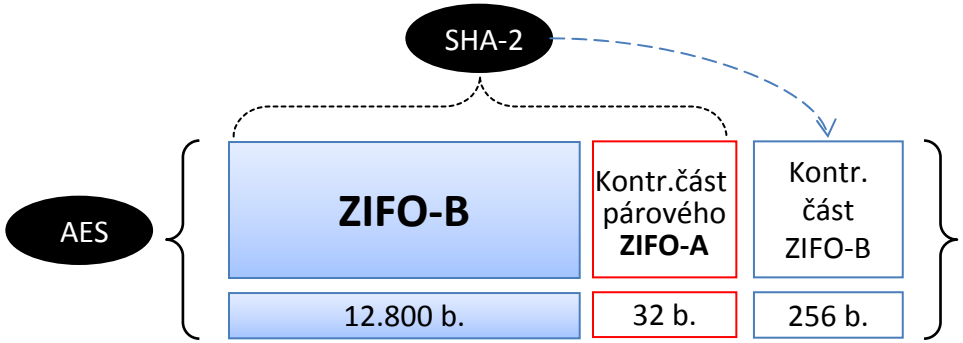
ZIFO bez kontrolních mechanismů:

ZIFO = (ZIFO-A ‖ ZIFO-B) = 12 928 b.

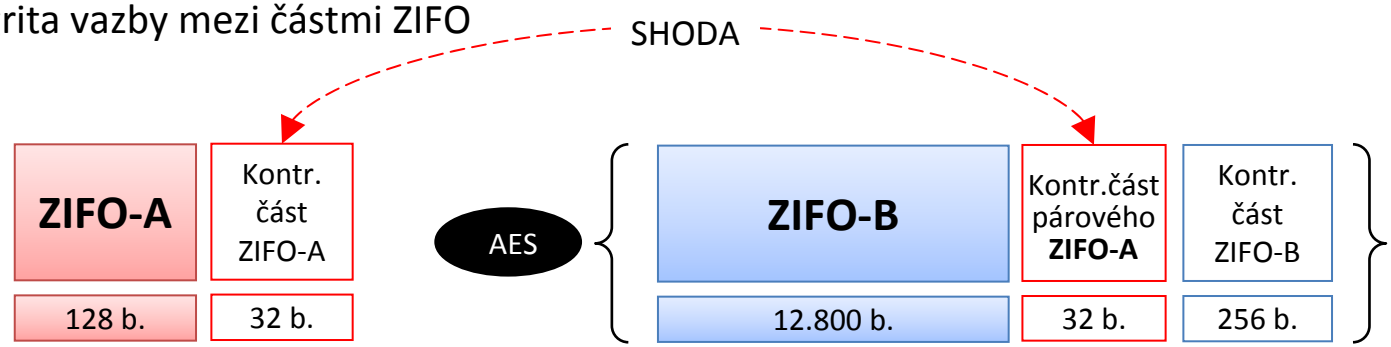
Principy odvození ZIFO

- Prvky pro zajištění integrity ZIFO





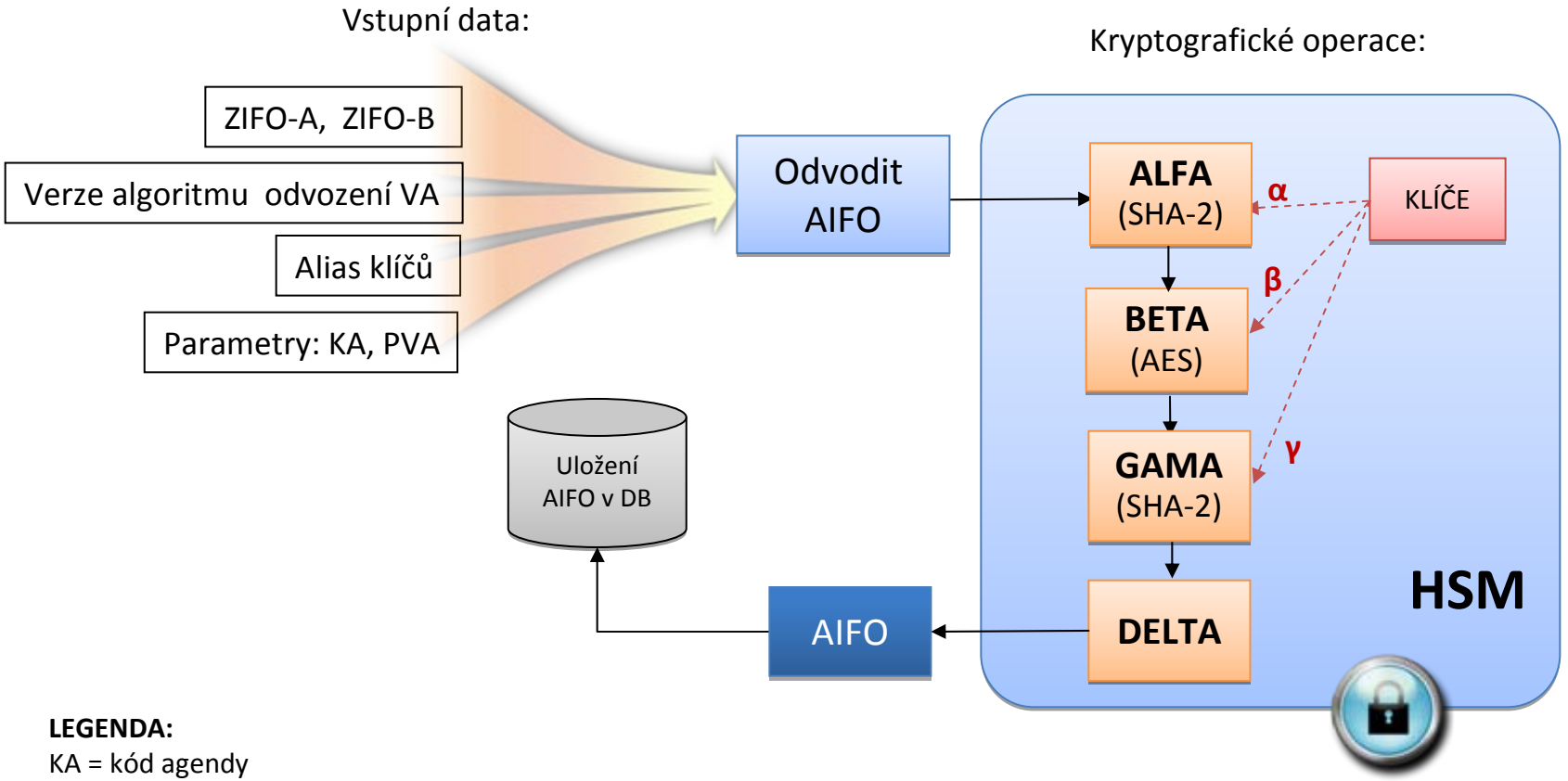
Integrita vazby mezi částmi ZIFO



Principy odvození AIFO

- Odvození AIFO probíhá v HSM
- Algoritmus odvození AIFO vyžívá posloupnosti 3 standardních kryptografických funkcí
- Ztráta certifikace (všeobecné věrohodnosti) jedné z funkcí bezprostředně neohrožuje věrohodnost AIFO
- Úprava algoritmu odvození AIFO při ztrátě certifikace některé z kryptografických funkcí a výměna AIFO v agendách je potřebná, nikoliv bezprostředně nutná
- Implementaci úprav lze provádět postupně a plánovitě (v horizontu např. 1 až 2 let)

Principy odvození AIFO



LEGENDA:
KA = kód agendy
PVA = pořadí varianty AIFO
Alias klíčů = jednoznačný identifikátor použitých šifrovacích klíčů

Bezpečnost AIFO, nástroje

- Kryptografické odvození AIFO zajišťuje věrohodnost v dlouhodobém horizontu
- ORG umožňuje AIFO z iniciativy AIS změnit
- Existence nástrojů pro výměnu AIFO
  - Kompromitace AIFO (nahrazení 1 AIFO)
  - Kompromitace AIS (nahrazení všech AIFO v agendě)
- Kompromitace AIS má dopad na všechny ostatní AIS v rámci agendy

Řešitel IS ORG

- Společnost se zaměřením na vývoj, výrobu a implementaci software a poskytování komplexních služeb v oblasti IT
- Certifikace „Integrovaného systému řízení“ dle norem ISO 9001, ISO 10006, ISO 14001, ISO 20000 a ISO 27001.
- NBÚ osvědčení podnikatele na stupeň „Důvěrné“

Závěr

- ORG je připraven na ověřovací provoz ZR
- Koncepce ZIFO a AIFO výrazně ovlivní aplikace e-Governmentu v několika příštích desetiletích
- Stávající zavedené identifikátory na úrovni AIS ve smyslu klíče k datům nejsou prozatím omezeny
- Zavedení ZR znamenají pro ÚOOÚ nové kompetence
- e-Government není a ani nemůže být cílem, nýbrž jen cestou ke zlepšení služeb občanům

Dovětek…

Motto: 1 … 2 … 3 … začínáme!

Děkuji za pozornost