



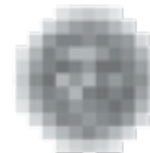
Informační systém ORG

Eva Vrbová

ředitelka Odboru základních identifikátorů



EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ



úřad pro ochranu
osobních údajů
the office for personal
data protection

Identifikátory fyzických osob

Rodné číslo

Občané ČR

Cizinci s trvalým pobytem v ČR

Číslo zdravotního pojištěnce

Strukturou kopíruje RČ, pro většinu občanů ČR se shoduje s RČ

Rozdíl je v individuálním vyřešení duplicit v RČ
Vlastní vytváření identifikátorů pro zaměstnance (cizince) bez trvalého pobytu

Identifikátor MPSV

Vlastní struktura dle metodiky MPSV

Rodné číslo

V roce 2054 dojde k přetečení číselné řady „roku“ a očekává se změna struktury RČ nebo náhrada jiným

Životnost stávajících identifikátorů

Číslo zdravotního pojištěnce

S ukončením stávající struktury RČ nutno řešit změnu
Není důvod, proč nezachovat individuální identifikátor
nadále

Identifikátor MPSV

Nemá přímou vazbu na RČ

Není důvod proč nezachovat individuální identifikátor



Cílem je zavedení bezvýznamových identifikátorů ZIFO a AIFO pro účely bezpečného sdílení dat

Identifikátory pro eGovernment

Identifikátory AIFO svými vlastnostmi řeší především ochranu osobních dat v prostředí internetu

Stávající zavedené identifikátory na úrovni agend ve smyslu klíče k datům nejsou a nebudou nijak omezeny

4

IS ORG – jak to začalo...



IS ORG – jak to začalo...



5

IS ORG – co to znamená?

- V období přípravy zákona č.111/2000 Sb. nebylo vůbec jasné, která organizace bude plnit úkoly, spojené s generováním ZIFO a AIFO
- Byla proto vytvořena zkratka ORG jako obecné označení organizace, která bude v budoucnu tyto úkoly plnit
- Bylo rozhodnuto, že platí: ORG = ÚOOÚ

Z toho vyplývá, že budovaný systém =

Působnost ÚOOÚ

- kontrolní činnost podle zákona 101/2000 Sb.
- nevyžádaná obchodní sdělení (spam) – zákon č. 480/2004 Sb., O některých službách informační společnosti
- přidělování ZIFO a přidělování AIFO – informační systém ORG (viz zákon č. 111/2009 Sb.)

Potenciál vybraného řešení IS ORG

- Preference unikátního řešení s vysokou mírou stability matematického aparátu v dlouhodobém horizontu, použitelnost SHA-2 je podle NISTu odhadována na období 2011–2030
- Matematický aparát umožňuje průběžnou změnu algoritmu s ohledem na jeho zastarávání
- Otevřenost řešení s využitím standardních kryptografických metod a bezpečných HW komponentů
- Bezpečnost AIFO ve vztahu k reverznímu inženýrství
- Ochrana osobních údajů v komunikačním prostředí ve vztahu k matici AIFO

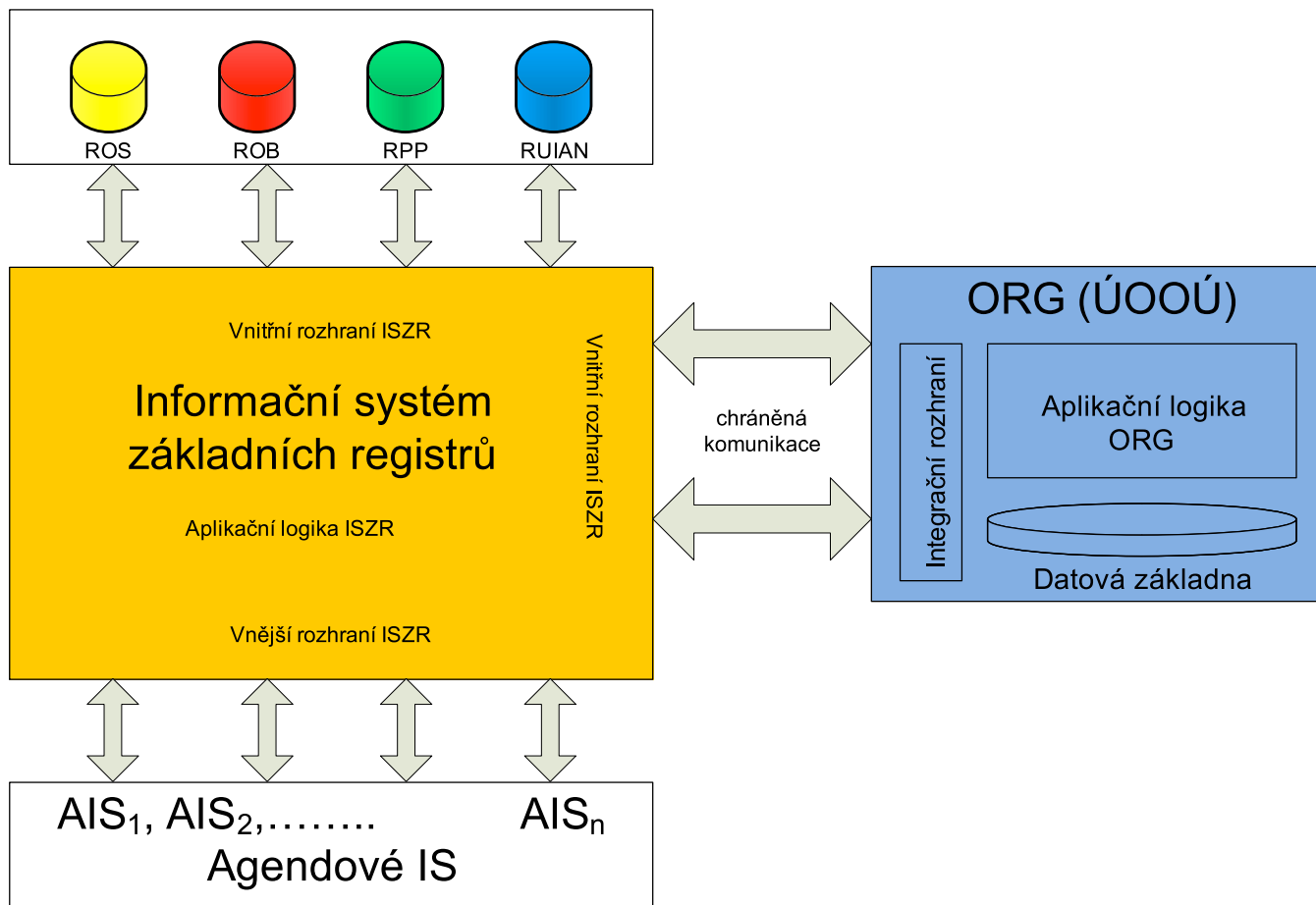
IS ORG (1)

- ORG je specifický informační systém ZR
- ORG neobsahuje žádná osobní data
- generuje a přiděluje identifikátory ZIFO a AIFO, vede jejich evidenci
- zajišťuje převody AIFO v systému základních registrů – převádí AIFO jedné agendy na AIFO druhé agendy
- AIFO = vícenásobná digitální identita
- Po přechodnou dobu RČ zůstává v platnosti ⁹

IS ORG (2)

- komunikuje výhradně a pouze jen s informač-ním systémem základních registrů (ISZR)
- při každé komunikaci AIS s ISZR (a základními registry) dochází k ověřování oprávnění úředníka/uživatele na požadovanou operaci
- správcem a současně editorem údajů ORG je ÚOOÚ

IS ORG (3)



Podmínky pro přidělení AIFO

- zákon č.111/2009 Sb. v § 2 jen obecně uvádí:
 - orgánem veřejné moci je státní orgán, územní samosprávný celek a fyzická nebo právnická osoba, byla-li jí svěřena působnost v oblasti veřejné správy
 - agendou je souhrn činností spočívajících ve výkonu vzájemně souvisejících činností v rámci působnosti orgánu veřejné moci
 - agendovým informačním systémem je informační systém veřejné správy, který slouží k výkonu agendy

Princip tvorby ZIFO a AIFO

- Filosofie identifikátorů



Alice Bílá

ZIFO_{AR}

AIFO_{AR}, agenda: AIFO_{AR}, agenda 2 AIFO_{AR}, agenda n



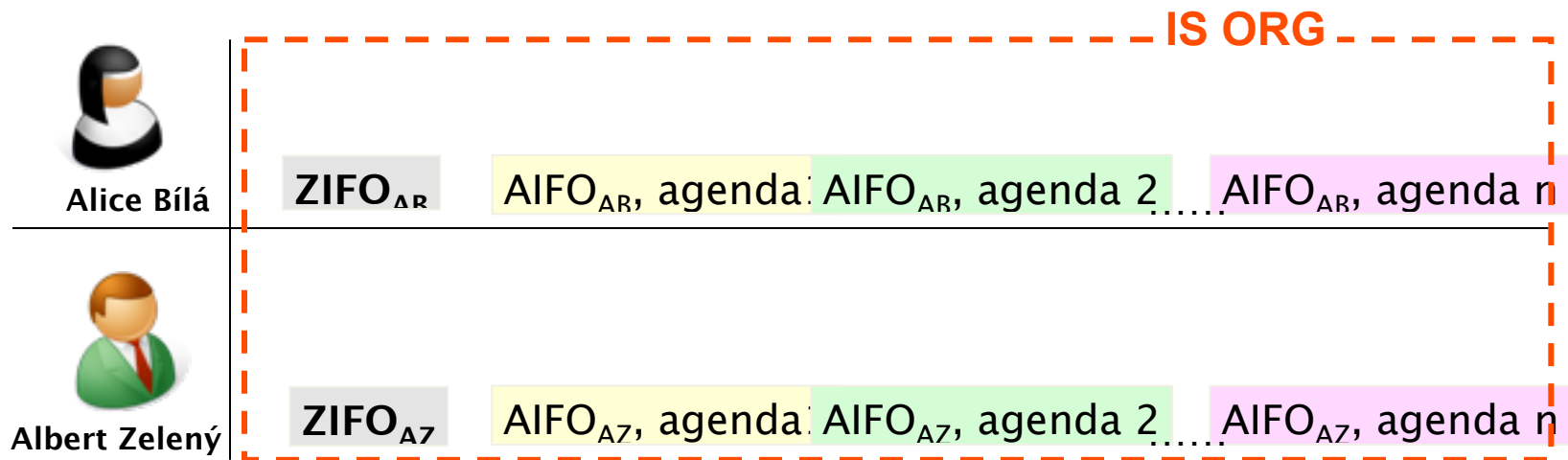
Albert Zelený

ZIFO_{AZ}

AIFO_{AZ}, agenda: AIFO_{AZ}, agenda 2 AIFO_{AZ}, agenda n

Princip tvorby ZIFO a AIFO

- Filosofie identifikátorů



Etapy projektu ORG

ORG Base <ul style="list-style-type: none">• základní funkcionality (generování ZIFO, AIFO, transformace AIFO x AIFO) → zahájit napojení ostatních komponent ZR• omezený výkon• provoz pouze v jedné lokalitě	02-09/2011
ORG Advanced <ul style="list-style-type: none">• další funkcionality → odladění v návaznosti na požadavky ostatních komponent ZR, doplnění chybějící funkcionality• navýšení výkonu v souladu s náběhem celého ISZR• provoz stále v jedné lokalitě	10-12/2011
ORG Full <ul style="list-style-type: none">• plná funkcionality• 100% výkon• redundantní provoz v primární a záložní	Ostrý provoz: od 1.7.2012

Aktuální stav realizace IS ORG

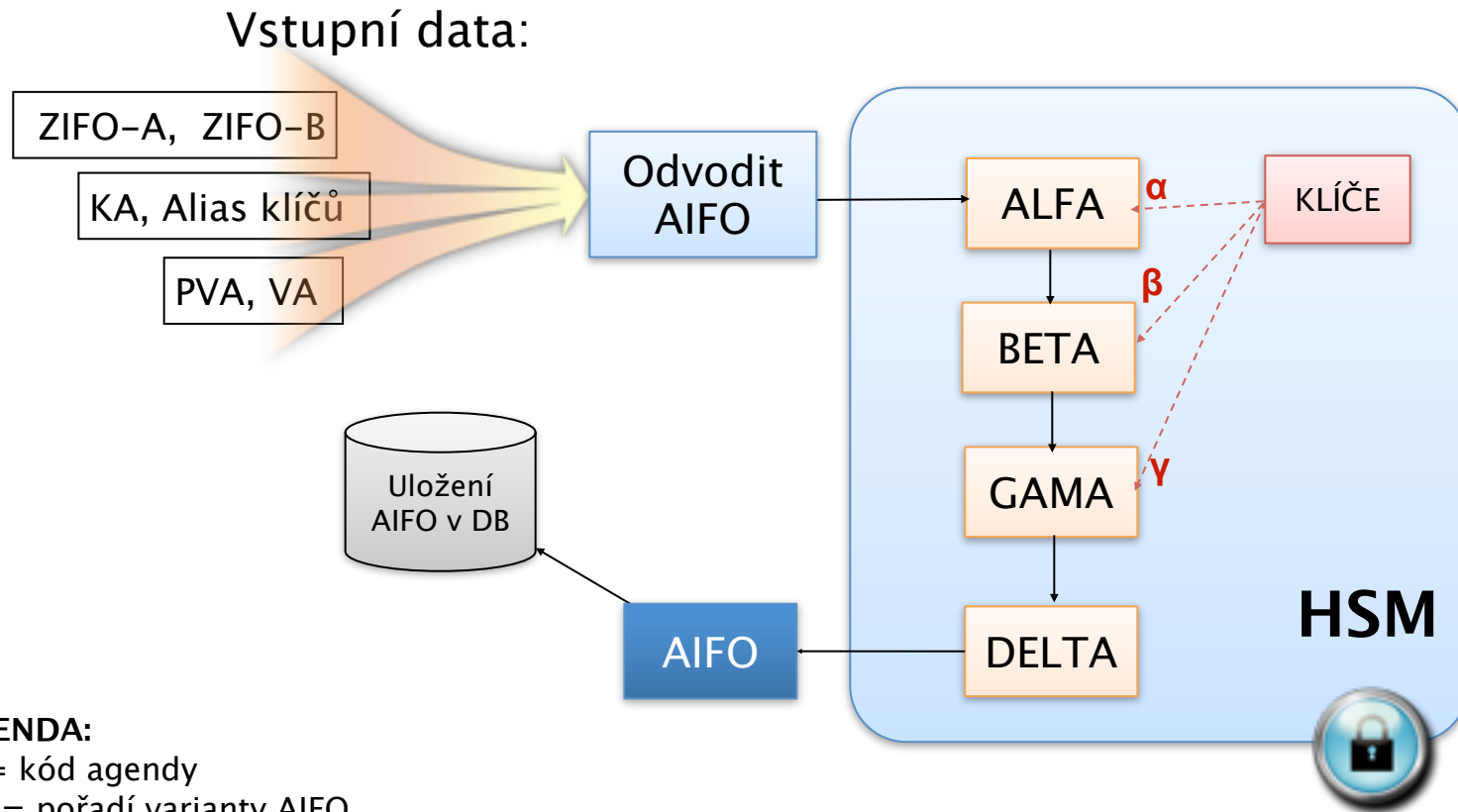
- Dokončeny vývojové práce MA
- Dokončeny vývojové práce IR
- Dokončeny vývojové práce DB
- Dokončeny vývojové práce AL
- Probíhají implementační práce na řídicím pracovišti
- Probíhají implementační práce na DC první lokality
- Probíhá integrace pro připojení k ISZR
- Připravují se integrační a výkonové testy

Řešitelé SW části IS ORG

- Tesco SW, a.s. – generální dodavatel
- Telematix Services, a.s. – řešitel matematického aparátu pro generování ZIFO, AIFO



Odvození AIFO



LEGENDA:

KA = kód agendy

PVA = pořadí varianty AIFO

VA = verze algoritmu

Alias klíčů = jednoznačný identifikátor použitých šifrovacích klíčů

Základní parametry řešení IS ORG (1)

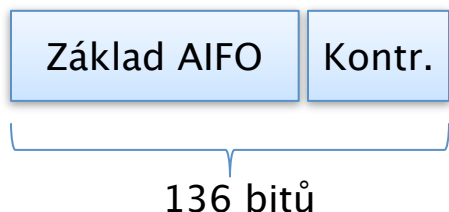
- Odvození AIFO probíhá v bezpečných zařízeních HSM
- Algoritmus odvození AIFO vyžívá posloupnosti 3 standardních kryptografických funkcí
- Ztráta certifikace (věrohodnosti) jedné z funkcí neohrožuje věrohodnost AIFO
- Úprava algoritmu odvození AIFO při ztrátě certifikace některé z kryptografických funkcí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

Základní parametry řešení IS ORG (2)

- AIFO lze v případě kompromitace opakovaně nahradit
 - náhrada jednotlivého AIFO (metoda kompromitace AIFO)
 - hromadná náhrada všech AIFO v agendě (metoda kompromitace AIS)
- AIFO lze odvodit kdykoliv znovu, např. ke kontrolním účelům

Základní parametry řešení IS ORG (3)

- **Struktura AIFO**



Délka 128 bitů představuje 2^{128} možností variant AIFO
pro každou jednotlivou agendu, což je $3,4 \times 10^{38}$ AIFO
včetně provozních duplicit a zrušených.

- **AIFO má primárně binární formát**

```
11111010 11110100 01110101 01000000 10101000 00000000  
01100111 10110100 01001100 11100100 00100011 11111000  
11010001 00010101 00100101 01110010 01100000
```

- **AIFO lze v agendách interpretovat v libovolném formátu (IS ORG formáty blíže nespecifikuje)**

20

Základní parametry řešení IS ORG (4)

- Pro komunikaci s ostatními systémy bude převážně používán formát BASE-64

```
+vR1QKgAZ7RM5CP40RUlcm
```

- Příklad interpretace AIFO v hexadecimálním formátu:

```
FAF47540A80067B44CE423F8D115257  
260
```

Ještě jednou bezpečnost...

- při řešení matematického aparátu pro generování ZIFO, AIFO byl kladen maximální důraz na zabezpečení IS ORG
- Jsou použity tři klíče α, β, γ
- Pro prolomení jednoho klíče o délce 128 bitů je nutno provést $3,4 \times 10^{38}$ testů, což by při počtu 256×10^6 testů/sec trvalo 42149543×10^{15} roků

Závěr

- **stávající zavedené identifikátory** na úrovni agend ve smyslu klíče k datům **nejsou a nebudou nijak omezeny**
- koncepce řešení ZIFO a AIFO výrazně ovlivní budoucí aplikace e-Governmentu v několika příštích desetiletích
- nové kompetence ÚOOÚ
- e-Government není a ani nemůže být cílem, nýbrž jen cestou ke zlepšení služeb občanům
- na této cestě bude mít zásadní význam kvalita řešení matematického aparátu ORG a jeho bezpečnost

Dovětek ...



Ochrana dat v době moderní a globální informační společnosti bude nabývat stále většího významu ...

24

Děkuji za pozornost

**DISKUS
E?**



25