Zabezpečení citlivých dat informačních systémů státní správy

Ing. Michal Vackář
Mgr. Boleslav Bobčík

T · · Systems

Citlivá data?

- Co to je?
- Kde to je?
- Kdo to za to odpovídá?
- Jak je ochránit?
- Jak se z toho nezbláznit
- Jak se v džungli neztratit

T · · Systems

Virtuální identita osoby
Citlivé informace

- Osoba-jednotlivec v elektronickém prostředí
  - **Aspekty identity**: množiny atributů popisující osobu v určitém kontextu
  - **Identita**: souhrn všech aspektů
- Nežádoucí stav
  - Nekontrolované propojení všech aspektů do jednoho celku
  - Zneužitelnost
  - **„Velký bratr“**

Trestní rejstřík Řidičský průkaz Zbrojní průkaz	Zdravotní stav Krevní skupina DNA	Vzdělání Jazykové znalosti
Zaměstnání Pracovní pozice Výdělek	Jméno Pohlaví Věk	Bankovní spojení Historie transakcí Platební karty
Členství v organizacích	Adresa Telefon E-mail	Bankovní spojení Historie transakcí Platební karty

„Velký bratr“

- Centralizované databáze identit
  - Velké množství zahrnutých jednotlivců
  - Velké množství atributů
  - **Zneužitelnost**

- Decentralizované databáze
  - Obsahují jen vybrané aspekty identit
  - Záznamy musí obsahovat identifikátor osoby
    - Identifikátory jsou obvykle dlouhodobě neměnné
  - **Propojitelnost databází**
    - ... pomocí známých identifikátorů

Příklady identifikátorů:

- Číslo občanského průkazu
- Číslo cestovního pasu
- Číslo řidičského průkazu
- Rodné číslo
- E-mail
- **... a mnoho dalších...**

T · · Systems

Propojitelnost informací

Jméno	Bydliště	Rodné číslo
Jan Novák	Praha, Milevská	540518/1232
Pankrác Malý	Břeclav, Polní	570204/4568
Milada Trojanová	Brno, Cejl	[illegible]
Servác Zelený	Sokolov, Údolní	680310/2460
Věra Pohlová	Praha, Chodovská	655411/8428
Bonifác Jedlička	Ústí nad Labem, Brandova	790627/1010
Jarmila Ostrá	Pelhřimov, Pařížská	715902/8063
Ondřej Novotný	Ostrava, Horská	741225/9921

Číslo účtu	Rodné číslo	Zůstatek
1024701	680310/2460	65536,00
1024702	591[illegible]/7546	29810,50
1024703	645[illegible]/1880	4548,00
1024704	7[illegible]5902/8063	209457,30

Řešení problému vazeb mezi informacemi (daty)

- Aspekty identity mají různé identifikátory
  - Identifikátory přiděluje centrální autorita
  - Každý identifikátor platí jen ve vymezené oblasti
  - Mezi všemi identifikátory jedné identity existuje vazba
    - ... ale tuto vazbu zná pouze centrální autorita

- Propojení záznamů identity
  - Centrální autorita sdělí identifikátory platné pro vybrané oblasti
  - Podléhá řízení přístupových práv, auditu apod.

- Příklady
  - Rakousko: Bereichsabgrenzungsverordnung (sourcePIN, ssPIN)
  - ČR: základní registry veřejné správy (ZIFO, AIFO)

T · · Systems

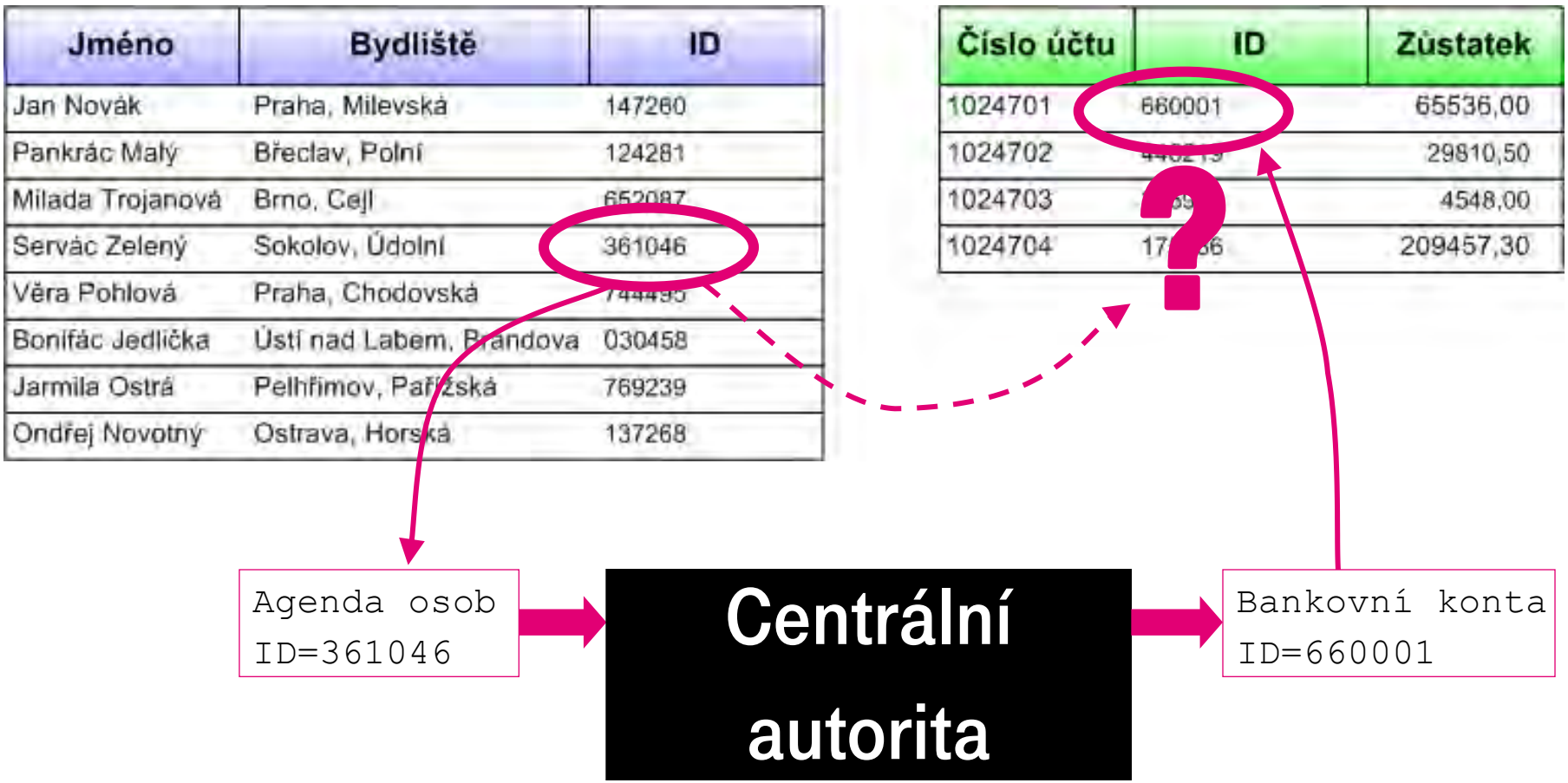
Vazba pomocí bezpečných identifikátorů

Agenda osob

Jméno	Bydliště	ID
Jan Novák	Praha, Milevská	147260
Pankrác Malý	Břeclav, Polní	124281
Milada Trojanová	Brno, Cejl	652087
Servác Zelený	Sokolov, Údolní	361046
Věra Pohlová	Praha, Chodovská	744495
Bonifác Jedlička	Ústí nad Labem, Brandova	030458
Jarmila Ostrá	Pelhřimov, Pařížská	769239
Ondřej Novotný	Ostrava, Horská	137268

Bankovní konta

Číslo účtu	ID	Zůstatek
1024701	660001	65536,00
1024702	4402[illegible]	29810,50
1024703	[illegible]	4548,00
1024704	17[illegible]6	209457,30

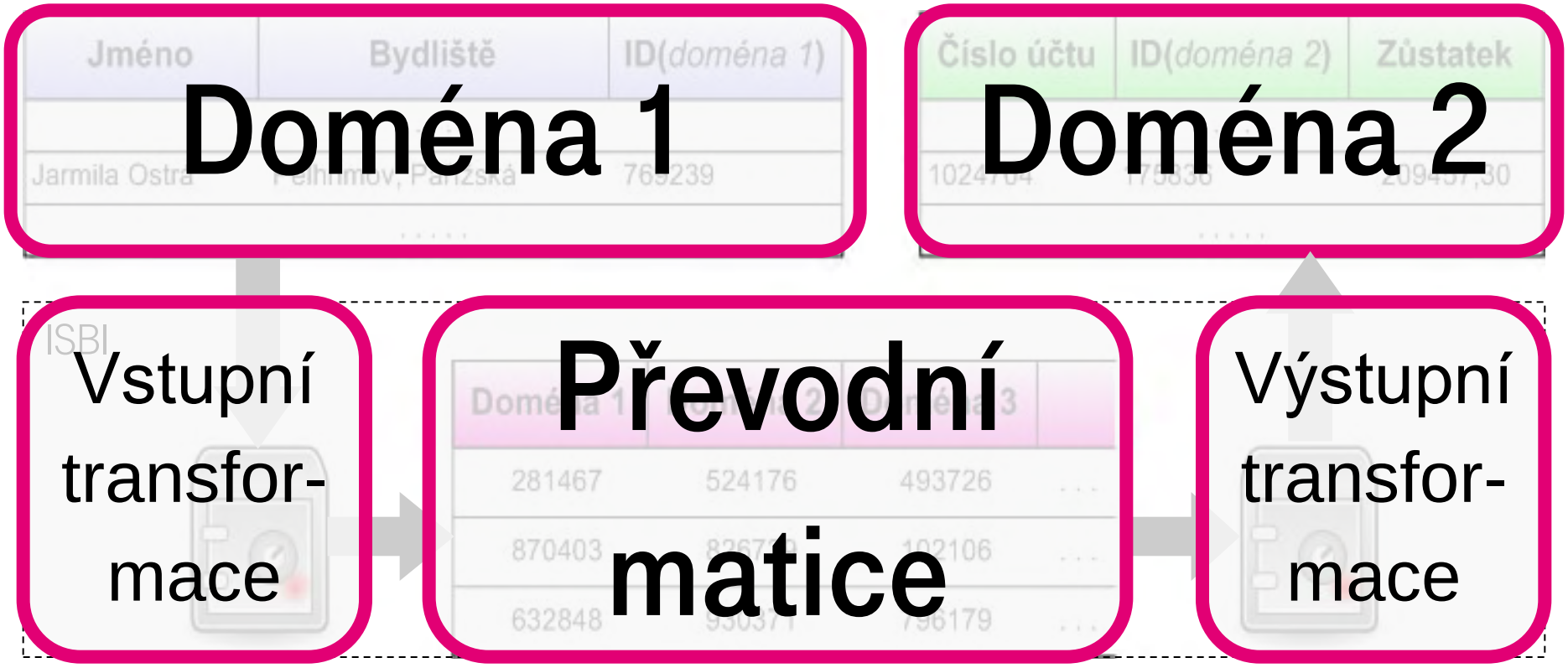


Řešení T-Systems
Informační systém bezpečných identifikátorů ISBI

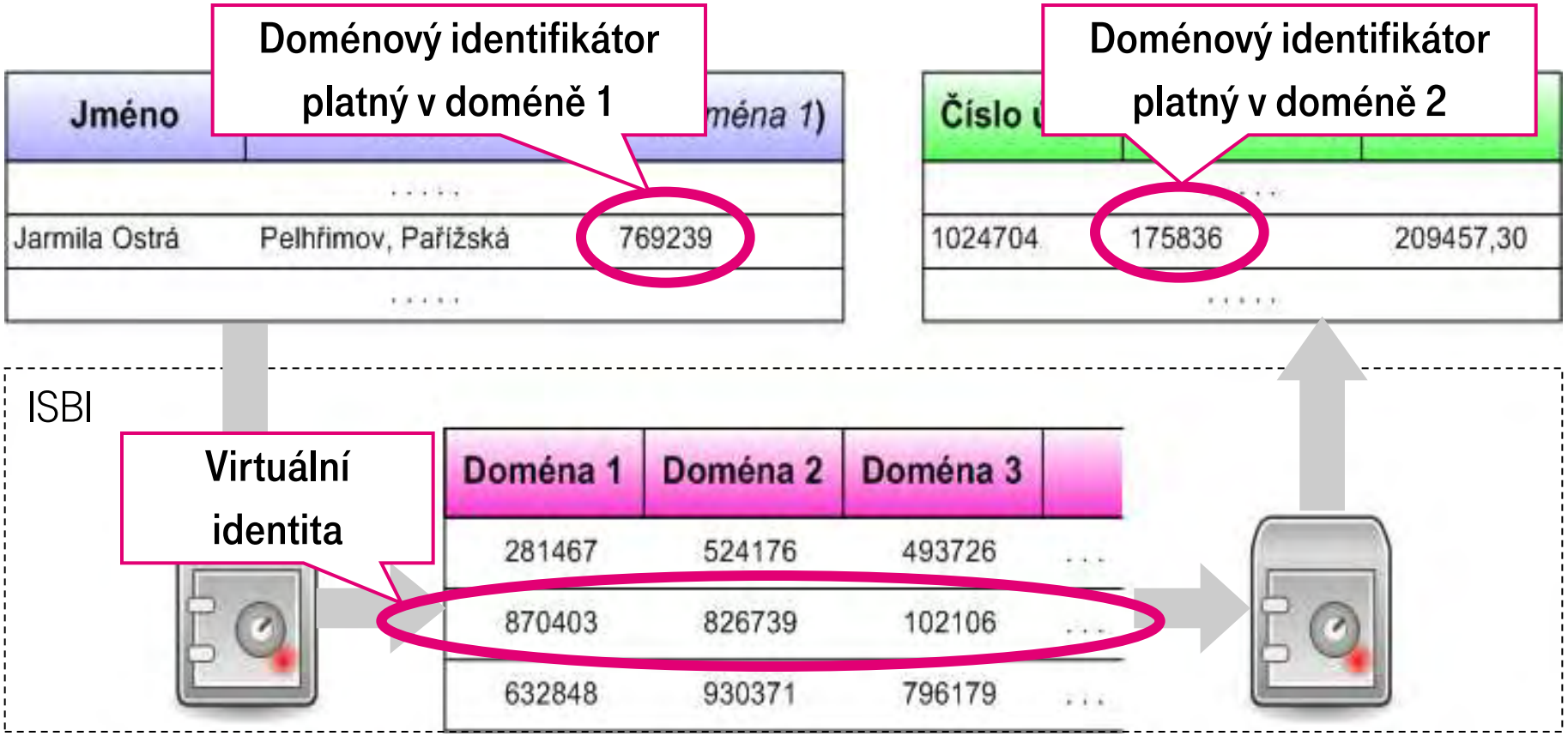
- Principy
  - **Doména**: oblast, ve které je potřeba aspekt identity opatřit identifikátorem
  - **Doménový identifikátor**: identifikátor vztahující se k osobě, platný v jedné doméně
  - **Virtuální identita**: souhrn všech doménových identifikátorů, které pro osobu existují

- Informační systém bezpečných identifikátorů (ISBI)
  - **Identifikátorová autorita**: vydává doménové identifikátory a řídí jejich životní cyklus
  - **Bezkoliznost**: garance, že se doménové identifikátory různých osob v jedné doméně liší
  - **Anonymita**: ISBI neobsahuje žádné osobní údaje (propojení virtuální identity s konkrétní osobou pouze na základě údajů v některé z domén)
  - **Bezpečnost**: odolnost vůči vnějším útočníkům i privilegovaným insiderům
  - **Robustnost**: schopnost zotavení po rozsáhlé havárii nebo masivním útoku

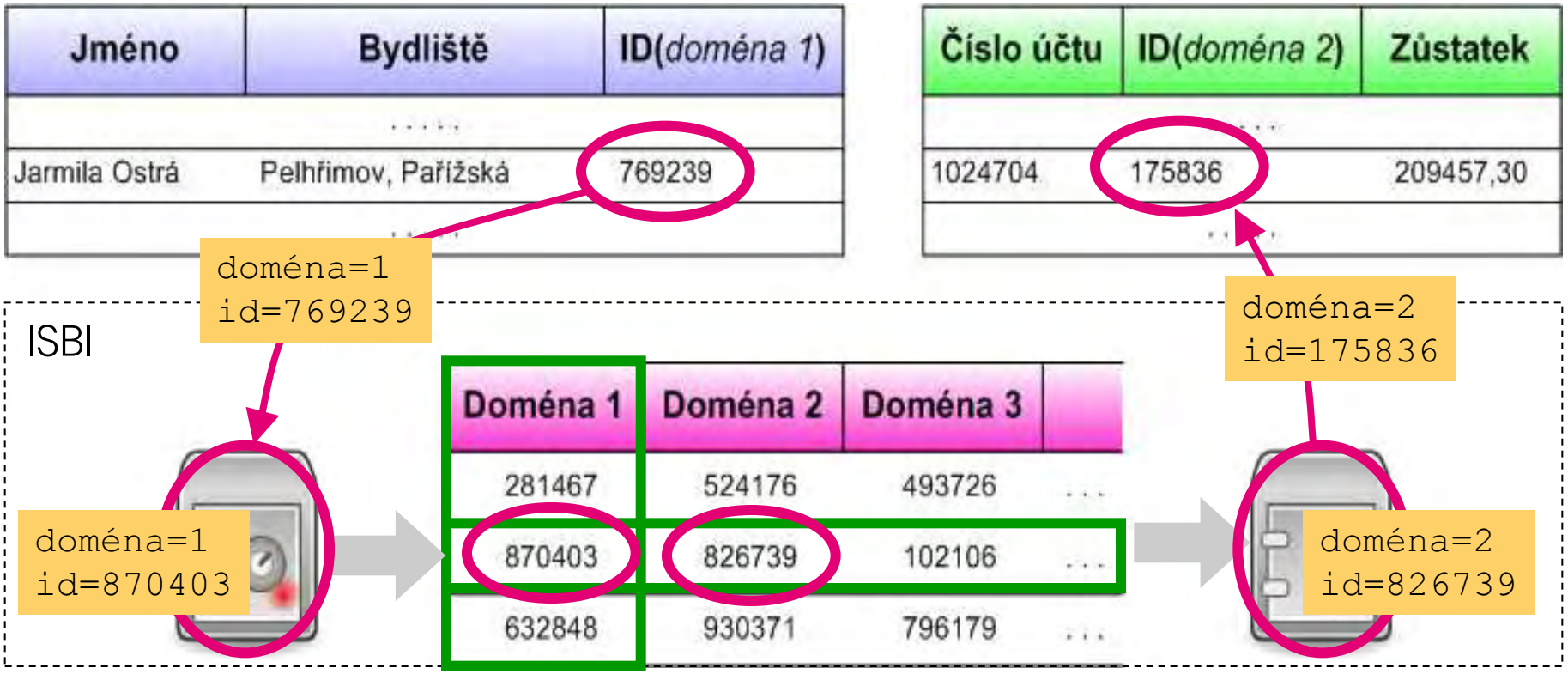
Ilustrace principů ISBI – domény



Ilustrace principů ISBI – doménové identifikátory



Ilustrace principů ISBI – princip činnosti



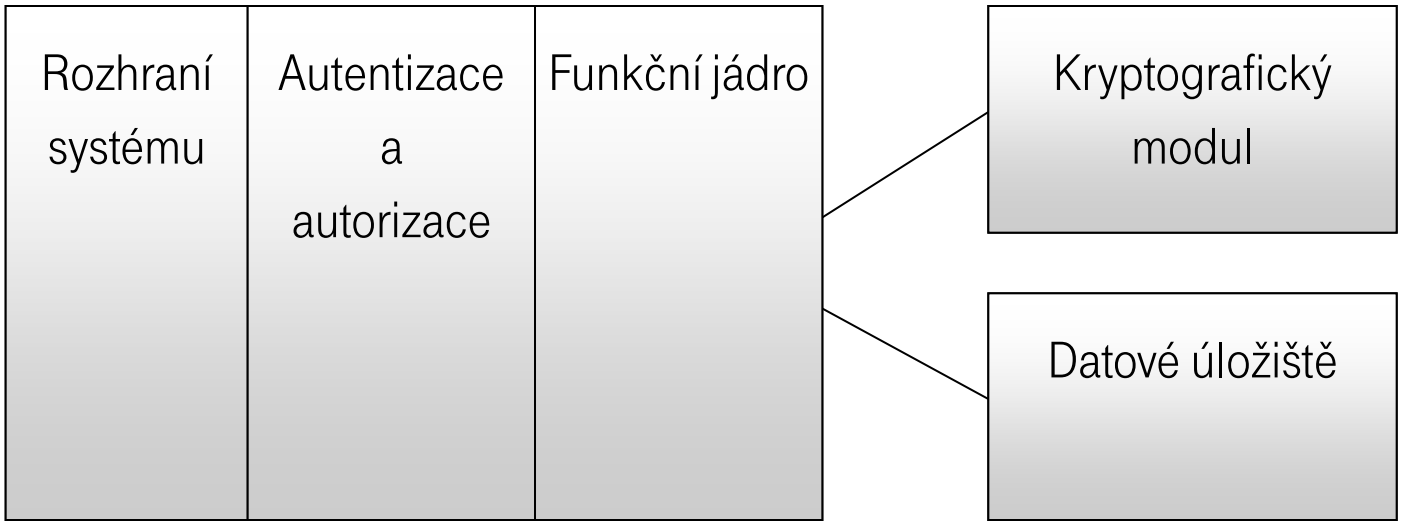
Doménové identifikátory

- Doménový identifikátor
  - 128-bitové číslo náhodného charakteru
  - Mimo ISBI nelze:
    - určit, zda dva identifikátory patří stejné osobě
    - určit, zda dva identifikátory patří do téže domény
    - převést identifikátor mezi dvěma doménami
  - Kolize (stejný identifikátor) v jedné doméně jsou z principu vyloučené

- Kódování
  - `8123456-ABCDEFG-ZYXWVUT-579KMNP`
  - Posloupnost 28 alfanumerických symbolů (bez rozlišení velikosti písmen)
  - Zabudovaný kontrolní mechanismus (CRC)
  - Robustní přenos pomocí analogových komunikačních prostředků (hlas, tisk...)

T · · Systems

Architektura ISBI



Datové úložiště

- uchovává převodní matici v **zakódované** podobě
- neobsahuje žádná osobní data
- vybudováno na standardech vysoce škálovatelných technologií

Vlastnosti systému bezpečných identifikátorů

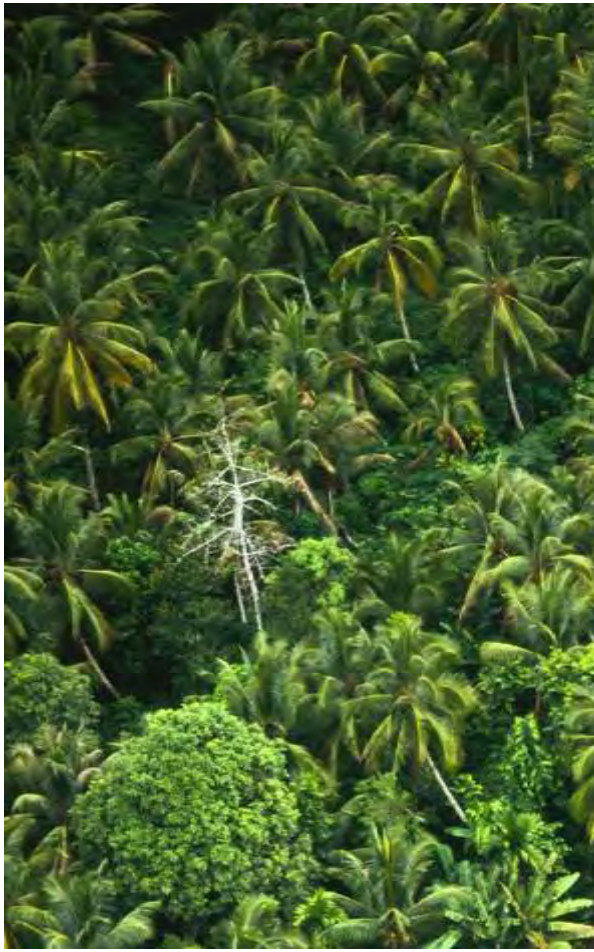
- Teoretické hranice
  - Limit počtu domén: více než **1 milion**
  - Limit počtu virtuálních identit: více než **4 miliardy**
  - Maximální počet doménových identifikátorů: více než **18 trilionů**

- Způsob zabezpečení
  - Moderní kryptografické algoritmy
    - Certifikace pro šifrování i přísně tajných informací
    - Odolnost i vůči kvantové kryptoanalýze
  - Kryptografické klíče (velikost 512 bitů)
    - Využití bezpečnostních HW zařízení pro uložení a správu klíčů
    - Ani správce systému nemá možnost získat klíče

T · · Systems

Citlivá data a ISBI
Rekapitulace

- Proč ISBI
  - Abychom pomohli v zamezení zneužití citlivých dat
- Jak nám ISBI pomůže
  - Rozdělí data do oddělených domén
  - Databáze bez ISBI nemá potřebnou vypovídající hodnotu
  - Bez ISBI nelze data provázat a vytěžit potřebné informace
- Proti čemu ISBI chrání
  - Proti přístupu neautorizovaných uživatelů
  - Proti zcizení datové základny
  - Proti zneužití dat administrátory databází
- Čemu ISBI nezabrání
  - Zneužití dat oprávněným uživatelem - umožní ale dohledání potřebných informací v auditu



T · · Systems


Pomůžeme Vám v ICT džungli.
T Systems

Děkuji za pozornost

T · · Systems