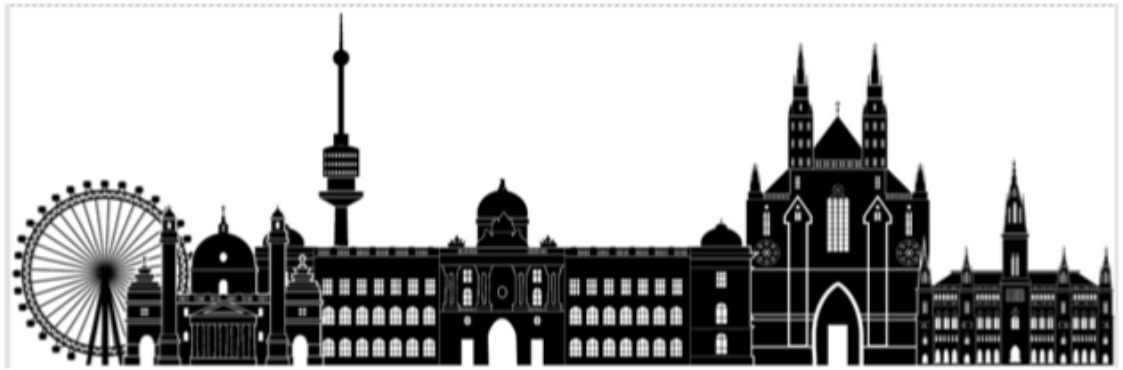
BBFA



MAPPING
Managing Alternatives for Privacy, Property and Internet Governance

Business Cases for Trust & Identity Federation

Trust & Internet Identity Meeting Europe

7 Feb 18 @Vienna

Do trust schemes have a problem?

How schemes see themselves?

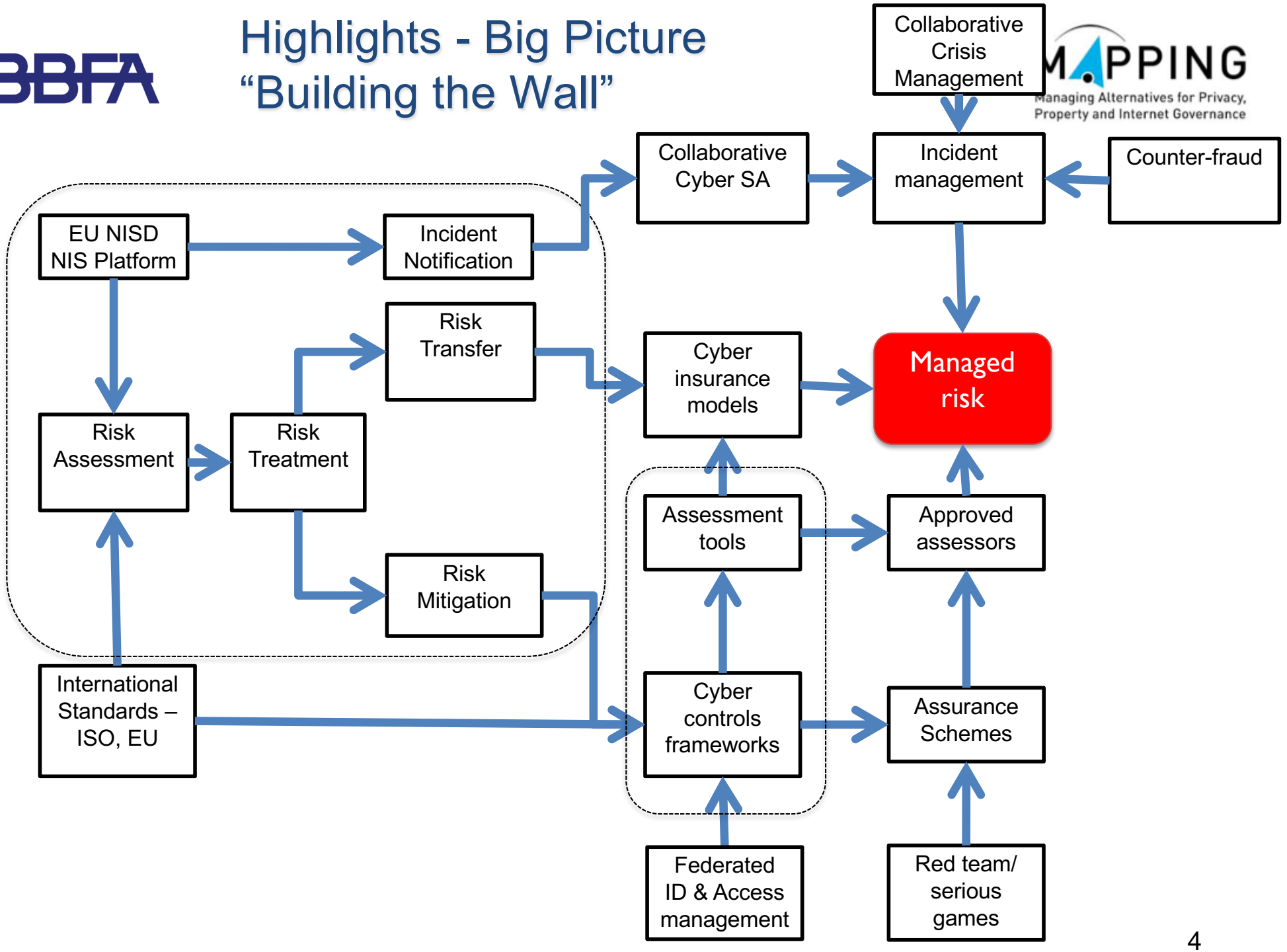
How others see trust schemes

Identity Misconceptions

- All about person
- All about me and my privacy
- All about government
- People must be in control of their own data
- Police shouldn’t be involved

- NO!! - It’s all about risk:
  - Regulatory compliance
  - Opportunity
  - Branding
  - IT
  - Cybercrime & fraud
  - Insider
  - Partner/customer/supplier

Highlights - Big Picture
"Building the Wall"



CCSA & Incident Management

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Info centric
Intel led

Layered proactive defence
Rumsfeld-based

Collaborative Crisis Management

Collaborative Cyber SA Hubs & Nodes

Incident management

Counter-fraud

Federated ID & access management

Red team/ serious games

ROLO OrgID registers

Cyber controls frameworks

PANCRAS Defeat fake docs and products

Taxonomies & Automation

Others

Triage & Analysis Processes

Priority Info Requirements

Why Federation?

1. Business is becoming more collaborative and international
2. Increasing legal, regulatory and commercial requirements for accountability and information protection in regulated industries
3. Information protection requires access control
4. Access control requires identity, authentication and authorisation, which are the basis of trust
5. Trust across multiple organisations requires federation
   - Organisations have to be considered **trustworthy** to trust each other
   - Organisations need a common language of business to understand each other
6. **Federation** requires **collaborative governance** and agreed **Common Policy**
7. US, European and Asian federation bodies are pressing ahead and setting federation standards, leveraging national ID activities
8. Each nation needs an industry-led collaborative governance body for federated trust for industry

Increasing Attack Surface

- More users
- More devices – internet of things/everything…
- More mobile
- More cloud(s?)
- More BYO Disaster
- More sensitivity – my info, health
- More critical systems – smart metering, big data
- Weak cyber borders >> internet governance under strain
- Increasing expectations and temptations → unwise decisions

Just **Surface Web**
….add
Deep web
Dark Web

- UK – 50M smart meters by 2020 in 30M buildings (UK Gov)
- 76% of financially active organisations in UK are not registered in UK or at all (& can't tell the difference). (UK Gov)
- 65% of IP theft is by insiders (SANS)

Identity Failure at Its Worst
The Context for HSPD-12/FIPS 201

- Sept. 11th, 2001, 19 terrorists boarded aircraft at two airports
  - The 20th had been denied access to the US by a suspicious immigration official in Orlando the previous month
  - 18 of 19 had been issued US identification documents
- Credential interoperability was non-existent
  - NYC buildings were locked-down to only local credentials
    - External aid providers were turned away
  - Pentagon was locked down
    - Arlington County Fire was turned away after photographer incident
    - Pentagon police chief was detained
      - No rapid electronic authentication mechanism was available

International Levels of Assurance

Level of Assurance	Identity Proofing	Credential	Authentication
4 – High Assurance	Government documents and ID. Independent verification & gov checks. Biometric	Hard PKI cryptographic token. FIPS 140/2 Level 2 crypto and Level 3 physical	Multifactor remote authN Biometric (PIV-I)
3 – Medium Assurance	Government documents and ID. Independent verification. Biometric	OTP or cryptographic token	Multifactor remote authN
2 – Low Assurance	Government documents and ID	Tokens, passwords & PINs	Single factor remote authN
1 - Pseudo-Anonymous	Negligible/nil	Tokens, passwords & PINs	Challenge - response

Internal Gov

Regulated Industry

Citizen

Biometrics	On Card	At Back end
Use	Multi-factor AuthN without infrastructure (but risky and costly)	De-duplication Higher security and trust Rapid revocation
Enrolment	Bind ID to Card Late bind for issuance Prove card works correctly	De-duplication


EUROPOL
The Internet Organised Crime Threat Assessment (iOCTA)
2014
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL
MAKING EUROPE SAFER

EC3 iOCTA 2014

"Meanwhile cybercrime itself is a growing problem. Trends suggest considerable increases in the scope, sophistication, number and types of attacks, number of victims and economic damage. There are two important factors worth highlighting in this context:

- *Crime-as-a Service (CaaS)*
- *Anonymisation"*

ID Fraud = a top EU crime enabler

Cybercrime 2011
McAfee - US: $1 trl/year
Overall - rising $2 trl
UK fraud > £56 bn
EU fraud > €500bn

If we are not winning, we must be losing

Red Dragon Rising
Cybercrime 2015
Overall $7.4 trl

©Getty

Willy Selten, who has appealed his two-and-a-half-year sentence for selling 300 tonnes of horsemeat as beef

©Alamy

Shift workers in Qingdao, China, descale, debone and repackage fish products for export

©Daniel Stier

Using a laser knife to test the identity of a fish fillet

Joint Strike Fighter
F-35 – Lightning II

Partners - Australia, Canada, Denmark, Italy, Netherlands, Norway, Turkey, UK, US
Buyers- Israel, Japan, Korea and maybe Belgium
1,300 suppliers - 40,000 parts - $US 500bn

Banks
Impact of Various Regulations in the Pipeline

MAPPING
Managing Alternatives for Privacy, Property and Internet Governance

Source Dr Anthony Kirby 2016

	Timing	Buy-side impact	Sell-side impact	Custodian impact	FMI impact	Gov / LE Impact	Risk Impact	Business impact	Systems impact	Data impact
AIFMD Reporting	Jul 2014	LOW-HIGH	LOW-MED	MEDIUM	LOW	LOW	LOW-HIGH	LOW-HIGH	LOW-HIGH	LOW-HIGH
TD 2	Jul 2015	LOW	LOW	LOW	LOW	MEDIUM	LOW	LOW	LOW	LOW
UCITS V	Mar 2016	LOW	LOW	LOW	LOW	LOW	LOW	LOW	MEDIUM	MEDIUM
EMIR	June 2016	LOW-HIGH	HIGH	MEDIUM	MED-HIGH	MEDIUM	MED-HIGH	LOW-HIGH	LOW-HIGH	HIGH
MAR	Jul 2016	MEDIUM	HIGH	MED-HIGH	HIGH	MEDIUM	MEDIUM	MEDIUM	MED-HIGH	HIGH
SFTR	>Jan 2017	MED-HIGH	HIGH	LOW	MEDIUM	MEDIUM	MEDIUM	MED-HIGH	MED-HIGH	HIGH
PRIIPs	>Mar 2017	HIGH	LOW	MED-HIGH	LOW	MEDIUM	MEDIUM	HIGH	HIGH	HIGH
MLD 4	Jun 2017	HIGH	HIGH	HIGH	LOW	MEDIUM	HIGH	MEDIUM	HIGH	HIGH
CRS	Sep 2017	MED-HIGH	HIGH	HIGH	LOW	MEDIUM	MEDIUM	MEDIUM	MEDIUM	HIGH
Benchmarks	Dec 2017	LOW-HIGH	HIGH	MEDIUM	HIGH	MEDIUM	HIGH	HIGH	MEDIUM	HIGH
ELTIF/MMR	Dec 2017?	LOW-HIGH	LOW	MEDIUM	LOW	LOW	LOW	MEDIUM	MEDIUM	MEDIUM
MIFID 2	Jan 2018	HIGH	HIGH	MEDIUM	HIGH	LOW	MEDIUM	HIGH	HIGH	HIGH
IDD	Jan 2018	LOW-HIGH	LOW	MEDIUM	LOW	LOW	MEDIUM	MEDIUM	MEDIUM	HIGH
PSD 2	Jan 2018	LOW	LOW	MEDIUM	LOW	HIGH	LOW	LOW	LOW	MEDIUM
GDPR	May 2018	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH
FRTB	Q1 2019?	LOW	HIGH	MEDIUM	LOW	MEDIUM	HIGH	MED-HIGH	HIGH	HIGH
CSDR settlement	Q1 2019?	MEDIUM	HIGH	HIGH	MED-HIGH	LOW	MEDIUM	MED-HIGH	MED-HIGH	HIGH

So what? #1

- Bank's top issue – EU General Data Protection Regulation (GDPR) – fine up to 4% of global turnover with significant reputational damage
- Highest impact - data (quality)

- How much and for whom?
  - Anti Money Laundering Directive 4
    MLD 4 covers payments €10k+ and is extended to virtual currencies. Requires identification, strong authentication, beneficiary traceability & persons of significant control (PSC)
  - Payment Services Directive
    PSD2 requires requirement for Secure Customer Authentication, except for contactless card payments under €50, card not present transaction under €10, and payments to a payee that the payer has explicitly whitelisted

General Data Protection Regulation

- Privacy as a fundamental human right, must be considered with other human rights. Policy collisions: privacy vs public safety (surveillance)
- Based on Pseudonymity:
  - Personal data exists somewhere in the system
  - The Relying Party does not know the identity of the person but knows that someone else does. A legal means exists to discover the identity of a person if required
- Anonymity. No personal data exists in the system
- Veronymity. Explicit declaration of identity (usually for legal reasons)
- Right to be Forgotten is not absolute.

- Other regulations: NIS Directive, eIDAS, Services Framework Directive ++
- Many Questions
  - What is personal data and what can & cannot be written to a block chain?
  - Safe Harbor >> Privacy Shield? Microsoft in Dublin

Lessons learned

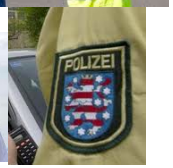
- Blockchains support communities and connect them
- Compliant permissioned blockchains require:
  - Strong authentication & access control
  - Data attributes from authoritative sources
- Collaborative authentication requires PKI federation, which can replace Proof of work
- All entities bind to trusted Organisation IDs. Need new organisational registers of accurate attributes (<24 hours).
  - **Current banking re-validation costs $100bn/year**
- Implement collaborative enablers:
  - Block chains
  - PKI federation
  - ROLO

So what? #2

- 17 technologies; block chain (BC) is the most discussed for DLT, not for crypto currencies.
- 50+ traded crypto currencies
- Block chain could support fiat or crypto currencies, or equity/assets – anything of value
- DLT/BC gives speed, scale and immutability. Financial and non-financial.
  - Xi Exchange and SETL - $2trl/day → <2 mins
  - Estonian patient records and privacy records
  - Diamonds

- Any regulated/compliant BC depends on:
  - Strong access control for access to the chain and data in the chain
  - Attributes from authoritative sources.





Employee - Gov




Employee - Industry

4 Contexts of Identity

Plus:
- Device ID
- Organisation ID
- Software Authentication
- Data Authentication

Citizen

Consumer

Level 3+ Identity Federations (PKI) - a UK perspective

Any nation could put itself at the centre…

Potential **Gov & Ind** CSPs
EADS/Cassidian, Citi, Entrust, SAFE/BioPharma, Symantec, Trustis

Early Adopters
Cross Certified Orgs:
MOD
NHS
NPIA/Police
DWP+

Other Potential National Bridges or CAs:
USA, Australia, Canada, NZ, NL, BE, FR, DE, IT+, NO, SWE, ESP
Interpol, EU, NATO

UK PKI Bridge

LoA 2+ Brokers

CertiPath Aero/Def

Participants
Cross Certified:
Boeing
Lockheed Martin Northrop Grumman
Raytheon
EADS/Airbus
BAE Systems

Credential Svc Providers:
Exostar, SITA, ARINC, CitiBank

Pending:
MoDUK
Rolls Royce
Finmechannica

(Emerging Bridge)

SAFE-BioPharma

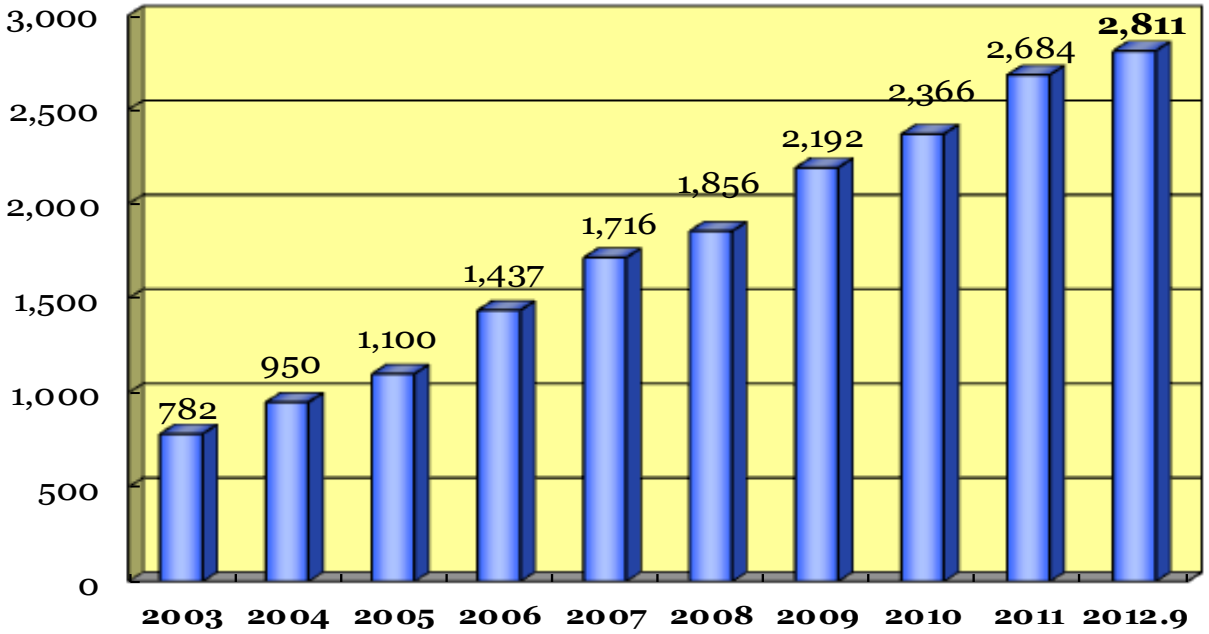
Participants:
AstraZeneca
Bristol-Myers-Squibb
Genzyme
GlaxoSmithKline
Johnson & Johnson
Merck
Nektar
Organon
Pfizer
Procter & Gamble
Roche
Sanofi-Aventis

Potential UK CSPs:
Citi, EADS, Entrust, Symantec,

Potential UK CSPs:
Citi, EADS, Entrust, Symantec,
Verizon Business+

Number of Digital Certificates

- 5 Accredited CAs issued accredited certificates to subscriber around 28 million in total.
- Major PKI Applications
  - Internet Banking, Online Stock, Internet Shopping, Procurement, e-Government Services



Numbers of annual issuance of certificates (2012.09, published by KISA)

Copyright © 2011 KICA. All Rights Reserved

Some EU National e-ID initiatives

Nation	Name	Purpose	Population	LoA	Biometrics	Features	Remarks
Estonia	ID	E-gov, Societal	1.3 M +	4	Face	Auth, Sign, Encrypt	
Estonia	E-residency	E-gov & business	8M target	3	Nil	Auth, Sign, Encrypt	10 k today
Belgium	.beID	Societal	12 M	3	Face	Auth, Sign, Encrypt	
Germany	Personal ausweis	E-gov	80 M +	3/4	Face	Auth, Sign, Encrypt	Low adoption of eID
France	France Connect	E-gov	Starting	2/3?	?	?	
UK	Verify	Limited E-gov	50 M	2	Nil	Auth	333 k 1.5 uses/year
Austria	Personal ausweis	E-gov	10 M	3/4	Face	Auth, Sign, Encrypt	
NL	DigID	E-gov	12 M	3	Face	Auth, Sign	Tax only
Malta	E-ID	E-gov	400 k	3	Face	Auth	Voting
Ireland	ID card	Travel	5M	3	Face	Auth	Requires passport

Other National e-ID initiatives

Nation	Name	Purpose	Population	LoA	Biometrics	Features	Remarks
Malaysia	My Kad	E-Gov, societal, bank, email	30 M	4	Face, finger	Auth, sign, encrypt	1st e-ID
NZ	RealMe	E-Gov, online services	5 M	3	Face, (video)	Auth	
Japan	My Number	E-Gov	130 M	3/4	Face, ?	Auth, ?	Disaster services
Korea	(New project)	E-Gov	40 M	3/4	Face, ?	Auth, sign, encrypt	Resident Registration Number fraud
Singapore	E-IC	e-Gov, societal, bank	5 M	3/4	Face, ?	Auth, sign, encrypt	Design stage
Nigeria	e-ID	E-gov, societal	180 M	4	Face, finger	Auth, sign, encrypt	Agricultural subsidy fraud
Kenya	(new project)	E-Gov	44 M	?	Face, finger		
India	Aadhar	Societal	1 bn +	3/4	Face, Iris, retina	Auth, Sign, Encrypt	Largest deployment
US	NSTIC	Industry-led societal	?	2/3	?	Auth	Online only. Pilots
US	18F	E-gov	300 M	3/4	Face, finger, ?	Auth, Sign, Encrypt	Design stage
China	Starts 2017	E-Gov or societal	1.4 bn	4	Multiple	Auth, ??	Counter fraud

The Identity Space

People – are they the people they claim to be?

Devices – are they what they claim to be?

Can I bind them together to enable trust?

Software – is it what it claims to be?

Organisations – are they who they claim to be?

Mac OS

Microsoft Windows

SAP

intelEct SCADA SYSTEMS

ORACLE

symantec.

POST OFFICE

BARCLAYS

NHS

e·on

AIRBUS

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

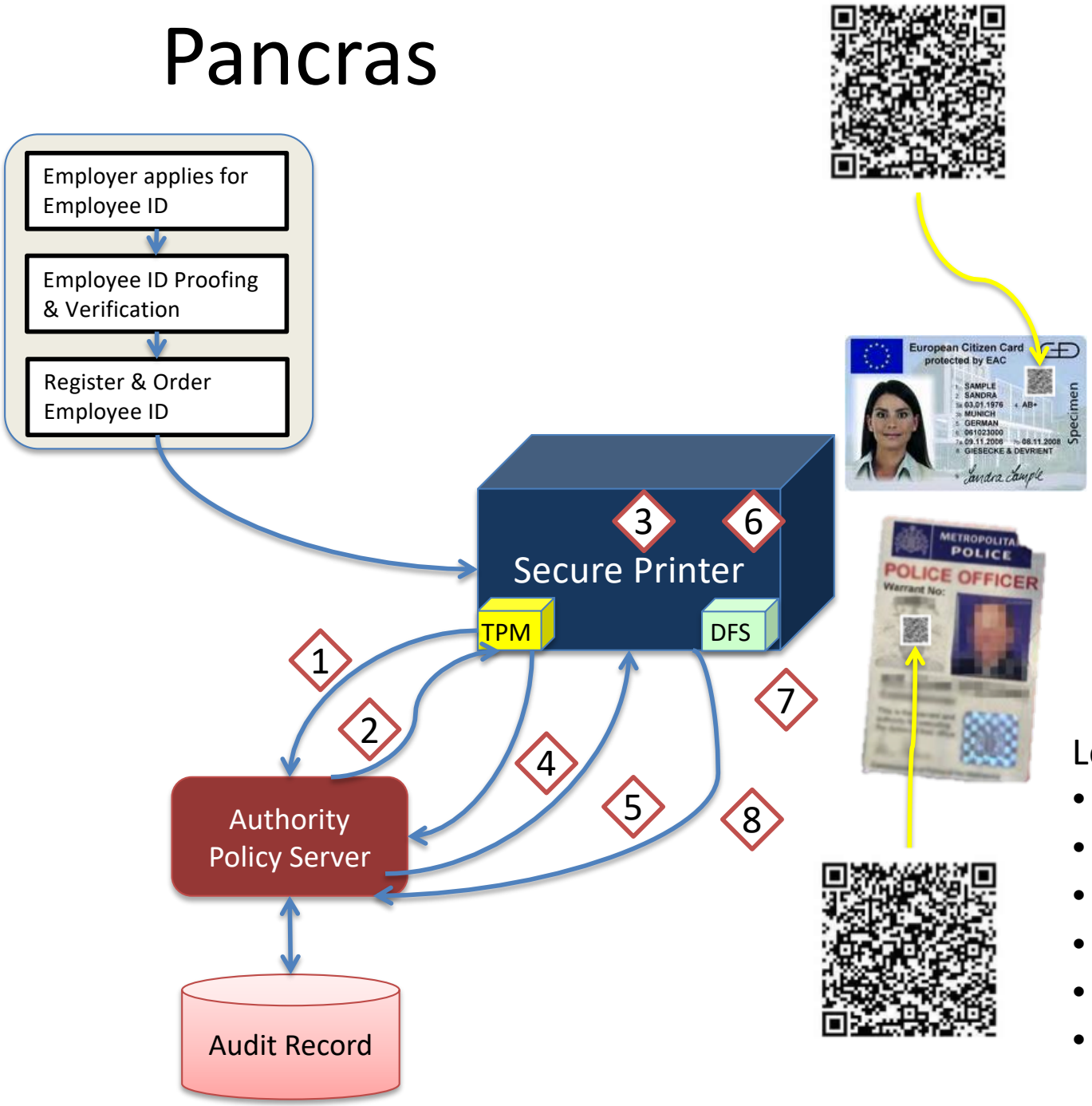
BRITISH AIRWAYS

sky

Boots

CabinetOffice

Pancras



1. Printer sends Trusted Platform Model (TPM) Authentication request
2. Server issues TPM authorisation
3. Printer prints document less barcode
4. Printer sends TPM signed document fingerprint to policy server
5. Server returns signed fingerprint and policy authorisation code
6. Printer prints encrypted barcode including signed fingerprint and policy authorisation code
7. Document printed
8. Printer sends signed confirmation of valid print to policy server

Long Term Impact:

- All banks
- All governments
- All regulated industries
- ASINP
- ++
- = All level 3+

TPM = Trusted Platform Module
DFS = Document Fingerprint Scanner

Fake organisations

- Every entity in cyberspace binds to an organisation
- ID systems are based on revocation times:
  - LoA 3 – 24 hours
  - LoA 4 – 4 hours
- Yet:
  - Over 70% of financially active organisations in a country are not registered in that country or at all
  - Attributes are few, inaccurate and inadequately checked
- Action is needed for authoritative data

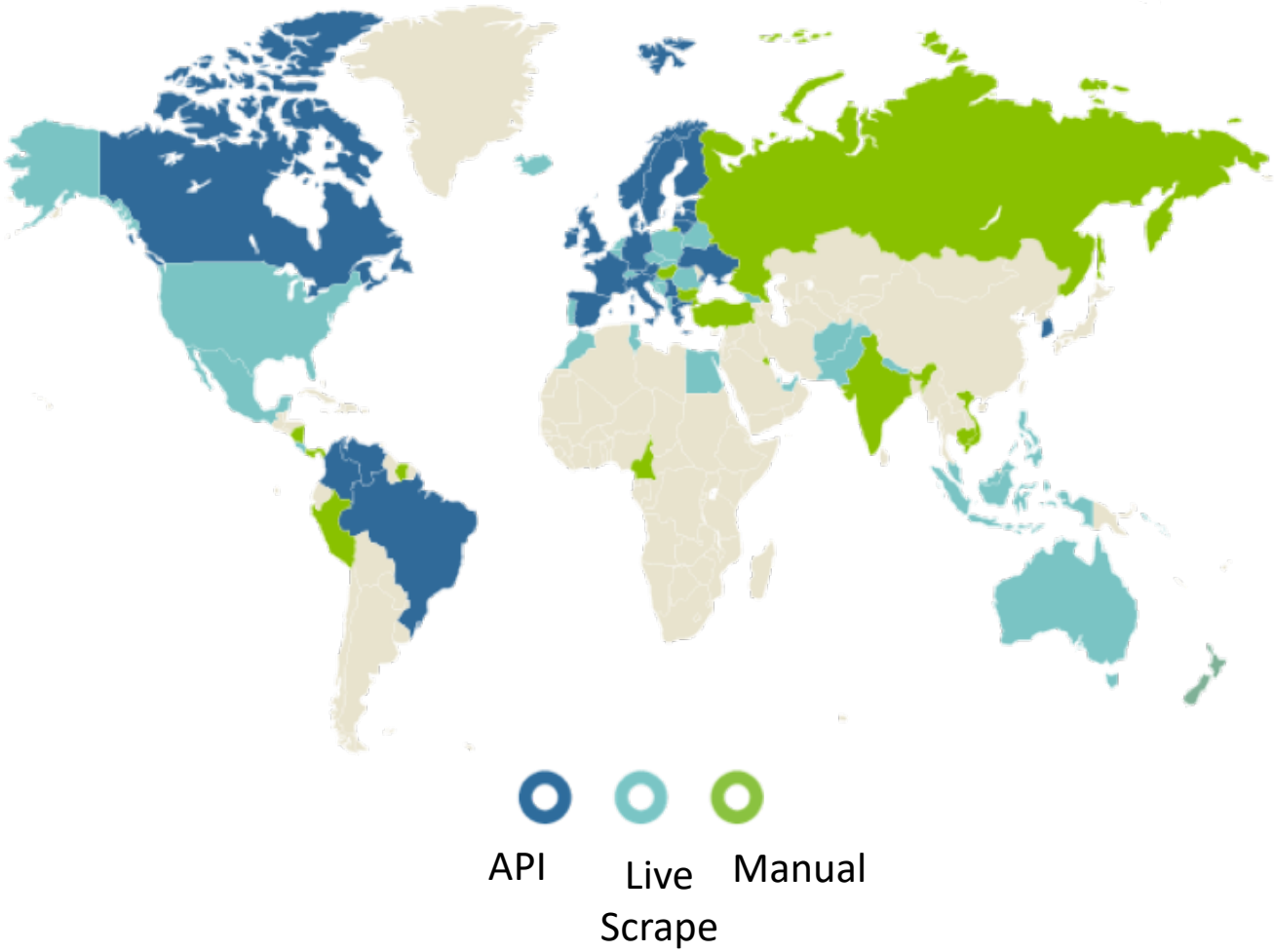
ROLO

- Register of Legal Organisations
- For any digital economy and society
- Every entity in cyberspace binds to an organisation
- Authoritative data pulled from authoritative sources
- ROLO Specification - 6 categories of attributes
  - Identification and cybersecurity status
  - Authority to act
  - Licensing
  - Government procurement
  - White list
  - Asset traceability
- Several nations adapting the ROLO specification
- Supports automation

Who are Kyckr?

We provide a **single point of access** to authoritative business information from 200+ National Business Registers across the planet

We've **extended our offering** from simple provision of this information to providing **KYC solutions** for our customers



- **On-boarding**
- **Data Cleansing**
- **Remediation**
- **Monitoring**

Why Blockchain?

- Once data is written to a blockchain it becomes **immutable**
- It is **highly distributed**
- This can be used **as proof** that a party acted based on the knowledge it had at the time of a transaction
- We can use the '**block generation time'** on most networks
- Data can be written to specific node addresses
- Could potentially be used to **monitor the history** of a company
- Provide an assured basis to improve data quality and to increase interoperability & re-use

Digital – Good Decisions depend on Quality Information

75%

Amount of defence mission critical information held in industry

Good decisions require
- Authoritative data
- Traceability

96%

Company-company interactions
vs 4% Government contracts

ISO Tech Committee 307

Themes:

1. Terminology (UK)
2. Reference Architecture (US)
3. Security (RU)
4. **Identity (KR)**
5. Smart contracts (DE)
6. Use cases (JP)
7. *Governance*
8. *Interoperability*

Blockchain and Distributed Ledger Technology scenarios

MAPPING
Managing Alternatives for Privacy, Property and Internet Governance

Financial

Redesign costly legacy workflows, improve liquidity and free up capital. Help reduce infrastructure costs, increase transparency, reduce fraud and improve execution and settlement times.

Retail & Manufacturing

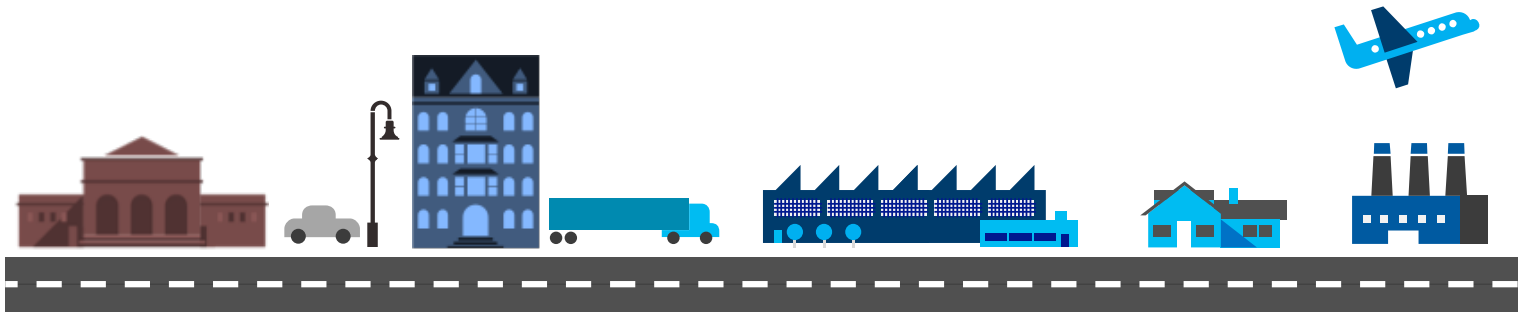
Better supply chain management, smart contract platforms, digital currencies, and tighter cybersecurity.

Healthcare

Removes third-party verifiers such as health information exchanges by directly linking patient records to clinical and financial stakeholders. Provides fast, secure, authenticated access to personal medical records across healthcare organizations and geographies.

Government

Increase transparency and traceability of how money is spent. Track asset registration, such as vehicles. Reduce fraud and operational costs.



Popular scenarios where blockchains add value

Financial
Trading
Deal origination
POs for new securities
Equities
Fixed income
Derivatives trading
Total Return Swaps (TRS)
2nd generation derivatives
The race to a zero middle office
Collateral management
Settlements
Payments
Transferring of value
Know your client (KYC)
Anti money laundering
Crowd Funding
Peer-to-peer lending
Compliance reporting
Trade reporting & risk visualizations
Betting & prediction markets

Insurance
Claim filings
MBS/Property payments
Claims processing & admin
Fraud detection/prediction
Telematics & ratings
Digital authentication
Asset management
Automated underwriting
Self-administered insurance

Media
Digital rights management
Game monetization
Art authentication
Purchase & usage monitoring
Ticket purchases
Fan tracking
Ad click fraud reduction
Resell of authentic assets
Real time auction & ad placements

Software Development
Micronization of work (pay for algorithms, tweets, ad clicks, etc.)
Expanse of marketplace
Disbursement of work
Direct to developer payments
API platform plays
Notarization & certification
P2P storage & compute sharing
DNS

Medical
Records sharing
Prescription sharing
Compliance
Personalized medicine
DNA sequencing

Asset Titles
Diamonds
Designer brands
Car leasing & sales
Home Mortgages & payments
Land title ownership
Digital asset records

Government
Voting
Vehicle registration
WIC, Vet, SS, benefits, distribution
Licensing & identification
Copyrights

Identity
Personal
Objects
Families of objects
Digital assets
Multifactor Authentication
Refugee tracking
Education & badging
Purchase & review tracking
Employer & Employee reviews

IoT
Device to Device payments
Device directories
Operations (e.g. water flow)
Grid monitoring
Smart home & office management
Cross-company maintenance markets

Payments
Micropayments (apps, 402)
B2B international remittance
Tax filing & collection
Rethinking wallets & banks

Consumer
Digital rewards
Uber, AirBNB, Apple Pay
P2P selling, craigslist
Cross company, brand, loyalty tracking

Supply Chain
Dynamic ag commodities pricing
Real time auction for supply delivery
Pharmaceutical tracking & purity
Agricultural food authentication
Shipping & logistics management

MAPPING
Managing Alternatives for Privacy, Property and Internet Governance

HMG Office of Government Science report for UK Prime Minister

Published 19 Jan 2016

Change in HMG

Industry collaboration

NL, EE, KR, JP participation starting

Identity & Access Management essential

Where is the equivalent for your country?

BBFA

MAPPING
Managing Alternatives for Privacy, Property and Internet Governance

Distributed Ledger Technologies for Public Good: leadership, collaboration and innovation

UK Blockchain Showcase

- 2-3 July 18 at The Guildhall in London
- 670 people
- 15+ demonstrators
  - Proof of concept
  - Pilot
  - Operational
- Many sectors – health, food, aviation, police, ICOs, maritime, gambling, charities, finance, insurance….

- UK plus international partner(s)

- www.dltshowcase.uk (next week)

Developments

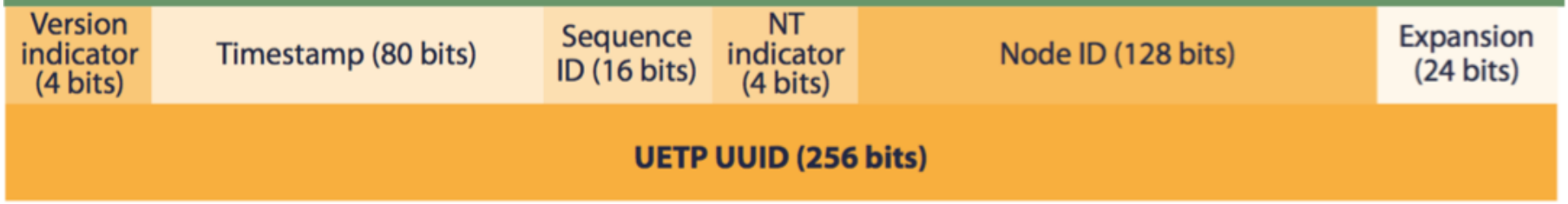
- Cryptocurrencies:
  - Anonymised, speculative, avoid regulation, criminal
  - (Pseudonymised) moving to regulatory compliance and fiat currency replacement
- DLT
  - Accountability
  - Traceability
  - Identifier management
  - NOT personal data

W3C standard

First requirement for the economic internet

Universal Unique Identification is a first requirement for the Economic Internet.

UETP provides the UETP Universal Unique Identifier (UUUID), also allowing current ecosystems to interconnect.



Please note that the NT indicator is an ecosystem indicator.

Examples of UETP IDs / certificates

ID type	Practical example
Personal ID	A personal electronic identity of Thomas Bauer, issued by a German bank, under the policies of a competent German policy authority governed by the laws and principles of the European Union
Organisation ID	An organisation electronic ID along the lines of the Global Legal Entity Identifier Framework
Asset ID	An electronic asset ID representing a vehicle with its unique manufacturing and local registration number and legitimate owner
Machine ID	An electronic ID of the traffic light around the corner
Money ID	An electronic wallet ID representing digital money
Message ID	A message ID referencing to a delivery confirmation in a transaction
Information ID	An ID with product description details and translations.
Rule set (legal)	In the legal jurisdiction of the Netherlands, no alcohol can be sold in transactions to people younger than 18 years.
Rule set (fiscal)	In the fiscal jurisdiction of Mongolia the transaction tax for sales / purchase transaction of milk is 15% and can be paid automatically.
Transaction ID	Representing a container and reference ID for all IDs that together make up for a specific transaction.

From "separate service communication" To one "group chat"

Traditional transactions

Several separated two, three and four party communication models

UETP transactions

The n-party "group chat"

Sedicii ZKP – How it works

Identity Attributes can be matched without being shared

"ThisismyPassword"

aC7$FgO;Kjx#

Emily's Device

Password

Password Hash

X

Random pattern

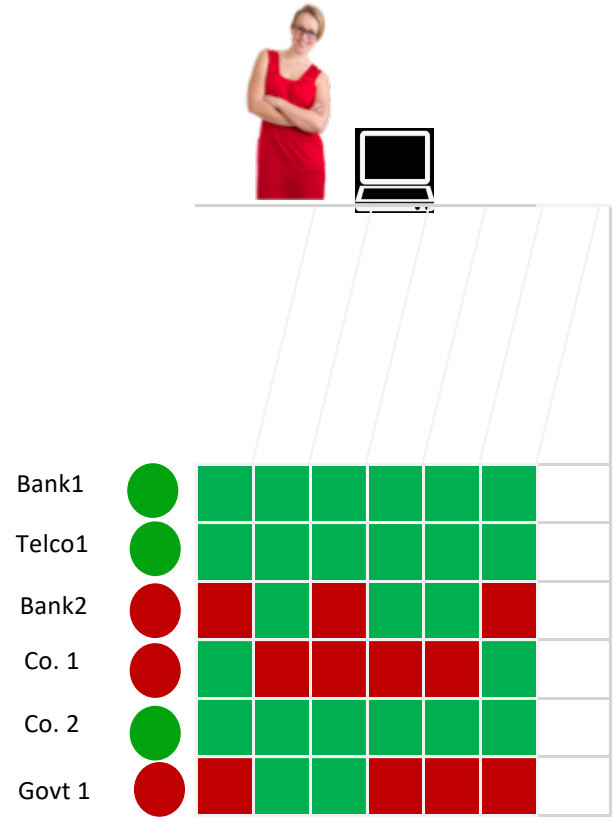
=

Match patterns by testing permutations

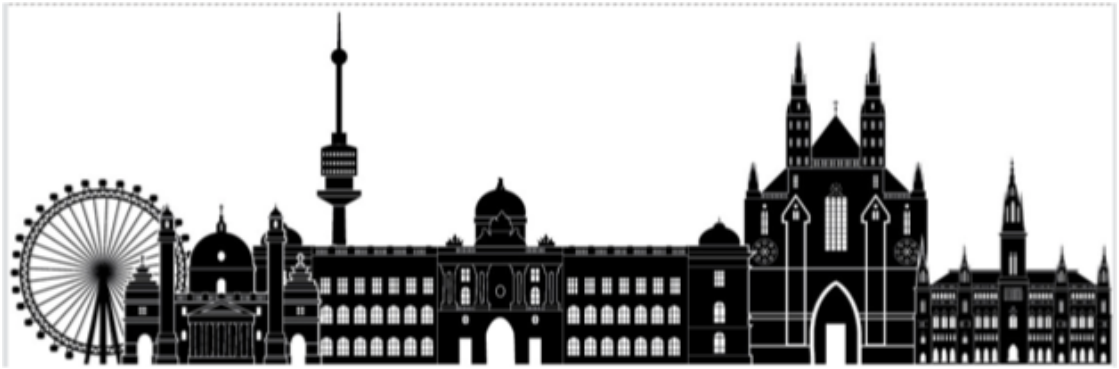
Auth Server

Zero Knowledge Proof

Interconnected Organisations and Hubs



BBFA



MAPPING
Managing Alternatives for Privacy, Property and Internet Governance

Business Cases for Trust & Identity Federation

patrick.curry@bbfa.info

Whew!!
Any Questions?