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”

- Risk Assessment
- Risk Treatment
- Risk Mitigation
- EU NISD NIS Platform
- Incident Notification
- Risk Transfer
- Collaborative Cyber SA
- Cyber insurance models
- Assessment tools
- Cyber controls frameworks
- Federated ID & Access management
- Managed risk
- Approved assessors
- Assurance Schemes
- Red team/serious games

International Standards – ISO, EU

Collaborative Crisis Management

Counter-fraud

Federated ID & Access management

Assurance Schemes
CCSA & Incident Management

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

Collaborative Cyber SA Hubs & Nodes

- Federated ID & access management
- Cyber controls frameworks
- Taxonomies & Automation
- Triage & Analysis Processes
- Priority Info Requirements

Collaborative Crisis Management

- Red team/serious games

Incident management

Counter-fraud

- ROLO OrgID registers
- PANCRAS Defeat fake docs and products
- Others

Info centric
Intel led
Layered proactive defence
Rumsfeld-based

Highlights - Big Picture "Building the Wall"
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

- 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. 11\textsuperscript{th}, 2001, 19 terrorists boarded aircraft at two airports
  – The 20\textsuperscript{th} 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

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

### Biometrics

<table>
<thead>
<tr>
<th>Biometrics</th>
<th>On Card</th>
<th>At Back end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use</td>
<td>Multi-factor AuthN without infrastructure (but risky and costly)</td>
<td>De-duplication Higher security and trust Rapid revocation</td>
</tr>
<tr>
<td>Enrolment</td>
<td>Bind ID to Card Late bind for issuance Prove card works correctly</td>
<td>De-duplication</td>
</tr>
</tbody>
</table>
“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
Willy Selten, who has appealed his two-and-a-half-year sentence for selling 300 tonnes of horsemeat as beef.

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

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
## Impact of Various Regulations in the Pipeline

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AIFMD</td>
<td>Jul 2014</td>
<td>LOW-HIGH</td>
<td>LOW-MED</td>
<td>MEDIUM</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW-HIGH</td>
<td>LOW-HIGH</td>
<td>LOW-HIGH</td>
</tr>
<tr>
<td>TD 2</td>
<td>Jul 2015</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
</tr>
<tr>
<td>UCITS V</td>
<td>Mar 2016</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>EMIR</td>
<td>June 2016</td>
<td>LOW-HIGH</td>
<td>HIGH</td>
<td>MEDIUM</td>
<td>MED-HIGH</td>
<td>MED-HIGH</td>
<td>LOW-HIGH</td>
<td>LOW-HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>MAR</td>
<td>Jul 2016</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>MED-HIGH</td>
<td>HIGH</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
<tr>
<td>SFTR</td>
<td>&gt;Jan 2017</td>
<td>MED-HIGH</td>
<td>HIGH</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>MED-HIGH</td>
<td>MED-HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>PRIIPs</td>
<td>&gt;Mar 2017</td>
<td>HIGH</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>MLD 4</td>
<td>Jun 2017</td>
<td>HIGH</td>
<td>LOW</td>
<td>MED-HIGH</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
<tr>
<td>CRS</td>
<td>Sep 2017</td>
<td>MED-HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
<tr>
<td>Benchmark</td>
<td>Dec 2017</td>
<td>LOW-HIGH</td>
<td>HIGH</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>MEDIUM</td>
<td>HIGH-HIGH</td>
<td>MEDIUM</td>
<td>HIGH-HIGH</td>
</tr>
<tr>
<td>ELTIF/MMR</td>
<td>Dec 2017?</td>
<td>LOW-HIGH</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>MIFID 2</td>
<td>Jan 2018</td>
<td>HIGH</td>
<td>HIGH</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>IDD</td>
<td>Jan 2018</td>
<td>LOW-HIGH</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
<tr>
<td>PSD 2</td>
<td>Jan 2018</td>
<td>LOW</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>LOW</td>
<td>HIGH</td>
<td>LOW</td>
<td>LOW</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>GDPR</td>
<td>May 2018</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>FRTB</td>
<td>Q1 2019?</td>
<td>LOW</td>
<td>HIGH</td>
<td>MEDIUM</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
<tr>
<td>CSDR settlement</td>
<td>Q1 2019?</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td>MED-HIGH</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>MED-HIGH</td>
<td>MED-HIGH</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

Source: Dr Anthony Kirby 2016
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
• 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
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.
4 Contexts of Identity

- Citizen
- Consumer
- Employee - Gov
- Employee - Industry

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

Potential UK CSPs
- Citi, EADS, Entrust, Symantec

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

Credential Svc Providers:
- Exostar, SITA, ARINC, CitiBank

Pending:
- MoDUK
- Rolls Royce
- Finmeccanica

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

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

UK PKI Bridge

LoA 2+ Brokers

CertiPath Aero/Def

(Emerging Bridge)

SAFE-BioPharma

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

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

Interpol, EU, NATO
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)
<table>
<thead>
<tr>
<th>Nation</th>
<th>Name</th>
<th>Purpose</th>
<th>Population</th>
<th>LoA</th>
<th>Biometrics</th>
<th>Features</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estonia</td>
<td>ID</td>
<td>E-gov, Societal</td>
<td>1.3 M +</td>
<td>4</td>
<td>Face</td>
<td>Auth, Sign, Encrypt</td>
<td></td>
</tr>
<tr>
<td>Estonia</td>
<td>E-residency</td>
<td>E-gov &amp; business</td>
<td>8M target</td>
<td>3</td>
<td>Nil</td>
<td>Auth, Sign, Encrypt</td>
<td>10 k today</td>
</tr>
<tr>
<td>Belgium</td>
<td>.belID</td>
<td>Societal</td>
<td>12 M</td>
<td>3</td>
<td>Face</td>
<td>Auth, Sign, Encrypt</td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>Personal ausweis</td>
<td>E-gov</td>
<td>80 M +</td>
<td>3/4</td>
<td>Face</td>
<td>Auth, Sign, Encrypt</td>
<td>Low adoption of eID</td>
</tr>
<tr>
<td>France</td>
<td>France Connect</td>
<td>E-gov</td>
<td>Starting</td>
<td>2/3?</td>
<td>?</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>UK</td>
<td>Verify</td>
<td>Limited E-gov</td>
<td>50 M</td>
<td>2</td>
<td>Nil</td>
<td>Auth</td>
<td>333 k 1.5 uses/year</td>
</tr>
<tr>
<td>Austria</td>
<td>Personal ausweis</td>
<td>E-gov</td>
<td>10 M</td>
<td>3/4</td>
<td>Face</td>
<td>Auth, Sign, Encrypt</td>
<td></td>
</tr>
<tr>
<td>NL</td>
<td>DigID</td>
<td>E-gov</td>
<td>12 M</td>
<td>3</td>
<td>Face</td>
<td>Auth, Sign</td>
<td>Tax only</td>
</tr>
<tr>
<td>Malta</td>
<td>E-ID</td>
<td>E-gov</td>
<td>400 k</td>
<td>3</td>
<td>Face</td>
<td>Auth</td>
<td>Voting</td>
</tr>
<tr>
<td>Ireland</td>
<td>ID card</td>
<td>Travel</td>
<td>5M</td>
<td>3</td>
<td>Face</td>
<td>Auth</td>
<td>Requires passport</td>
</tr>
</tbody>
</table>
### Other National e-ID initiatives

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

**People** – are they the people they claim to be?

**Devices** – are they what they claim to be?

**Software** – is it what it claims to be?

**Organisations** – are they who they claim to be?

Can I bind them together to enable trust?
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

British Business Federation Authority - office@federatedbusiness.org
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
• 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

96% Good decisions require
  • Authoritative data
  • Traceability

Company-company interactions vs 4% Government contracts

info@bbfa.info
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

ISO/TC 307
Blockchain and electronic distributed ledger technologies
Blockchain and Distributed Ledger Technology scenarios

**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

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

#### 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

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

#### Media
- 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
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?
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
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.

<table>
<thead>
<tr>
<th>Version indicator (4 bits)</th>
<th>Timestamp (80 bits)</th>
<th>Sequence ID (16 bits)</th>
<th>NT indicator (4 bits)</th>
<th>Node ID (128 bits)</th>
<th>Expansion (24 bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**UETP UUID (256 bits)**

Please note that the NT indicator is an ecosystem indicator.
## Examples of UETP IDs / certificates

<table>
<thead>
<tr>
<th>ID type</th>
<th>Practical example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal ID</td>
<td>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</td>
</tr>
<tr>
<td>Organisation ID</td>
<td>An organisation electronic ID along the lines of the Global Legal Entity Identifier Framework</td>
</tr>
<tr>
<td>Asset ID</td>
<td>An electronic asset ID representing a vehicle with its unique manufacturing and local registration number and legitimate owner</td>
</tr>
<tr>
<td>Machine ID</td>
<td>An electronic ID of the traffic light around the corner</td>
</tr>
<tr>
<td>Money ID</td>
<td>An electronic wallet ID representing digital money</td>
</tr>
<tr>
<td>Message ID</td>
<td>A message ID referencing to a delivery confirmation in a transaction</td>
</tr>
<tr>
<td>Information ID</td>
<td>An ID with product description details and translations.</td>
</tr>
<tr>
<td>Rule set (legal)</td>
<td>In the legal jurisdiction of the Netherlands, no alcohol can be sold in transactions to people younger than 18 years.</td>
</tr>
<tr>
<td>Rule set (fiscal)</td>
<td>In the fiscal jurisdiction of Mongolia the transaction tax for sales / purchase transaction of milk is 15% and can be paid automatically.</td>
</tr>
<tr>
<td>Transaction ID</td>
<td>Representing a container and reference ID for all IDs that together make up for a specific transaction.</td>
</tr>
</tbody>
</table>
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

“This is my Password”
Emily’s Device

Password

aC7$FgO;Kjx#

Password Hash

X

Random pattern

= Match patterns by testing permutations

Zero Knowledge Proof

Identity Attributes can be matched without being shared
Interconnected Organisations and Hubs

Companies

Emily's Golden Record

Govt.

Banks

Telco’s

Utilities

Bank1
Telco1
Bank2
Co. 1
Co. 2
Govt 1
Business Cases for Trust & Identity Federation

patrick.curry@bbfa.info

Whew!!
Any Questions?