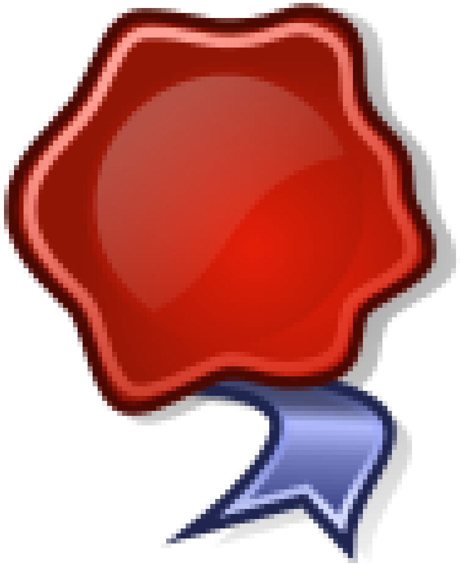
The many applications of digital certificates



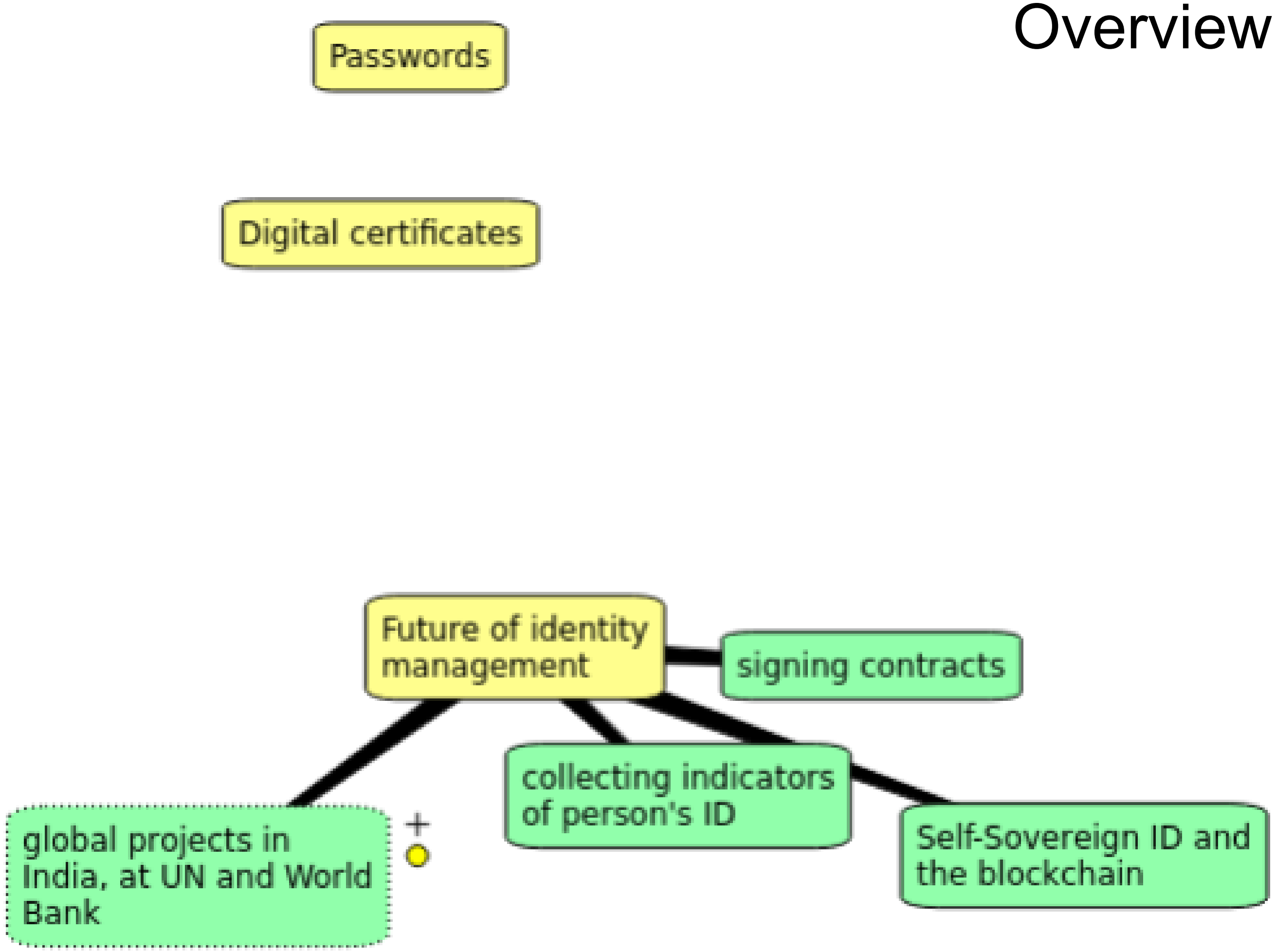
Digital certificates appear in many unexpected places. This session discovers them, and explains their various functions in terms accessible to ordinary users. Added-value of encryption over mere log-ins, the future of passwords.

Disclaimer

This presentation will be about technology from a socio-economic persepective. For mathematical details of cryptography, please see the recent German presentation of my colleague Guenter Waller, **http://www.pc-treff-bb.de/Vortraege/Zertifikate.pdf**

You will find clickable links to the current presentation on my **www.thomasruddy.eu**

Overview



Passwords

Digital certificates

Future of identity management

signing contracts

collecting indicators of person's ID

Self-Sovereign ID and the blockchain

global projects in India, at UN and World Bank

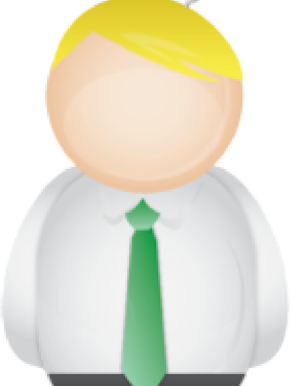
Theses

- Cryptography developed through *military* applications like Enigma encryption.
  - Encryption needs authentication.
- We live in states based on law and order.
- The integrity of society relies on ID management.
- ID mgmt can make contracts non-repudiable.
- Blockchain may make contracts self- executable.
- We are under threat from corporations taking over ID mgmt for a society that is valuing convenience over data security.

Identity is an assertion presented by a person.

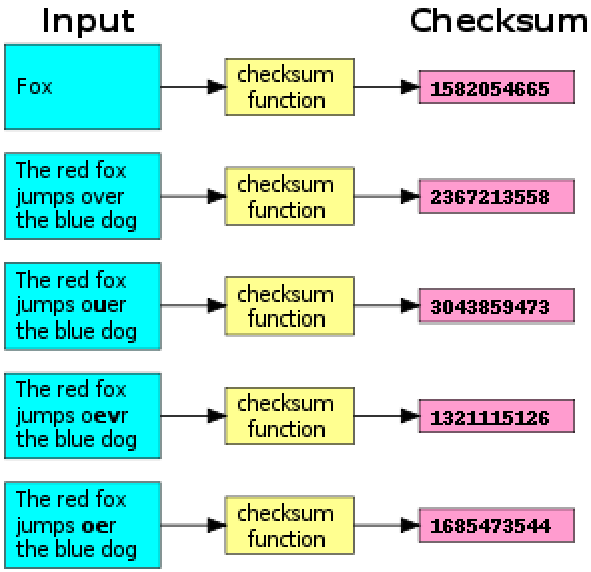
Authentication is a statement (from a trust provider, typically working for a “rent”). TP signs person’s public key.

Person “signs” document with her private key.



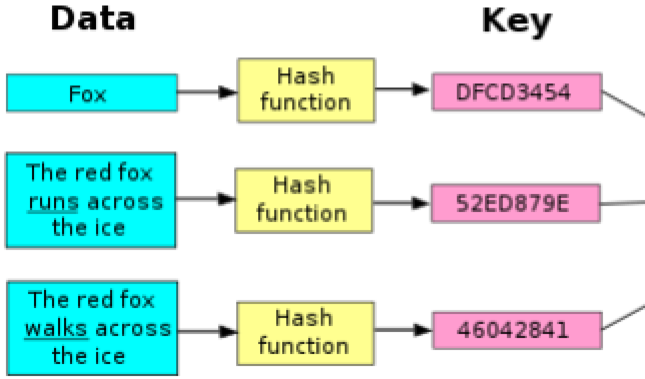
Relying party verifies doc. with sender’s public key.

Authentication



Verifying authenticity of downloaded software

Creating a CHF, source: https://en.wikipedia.org/wiki/Cryptographic_hash_function

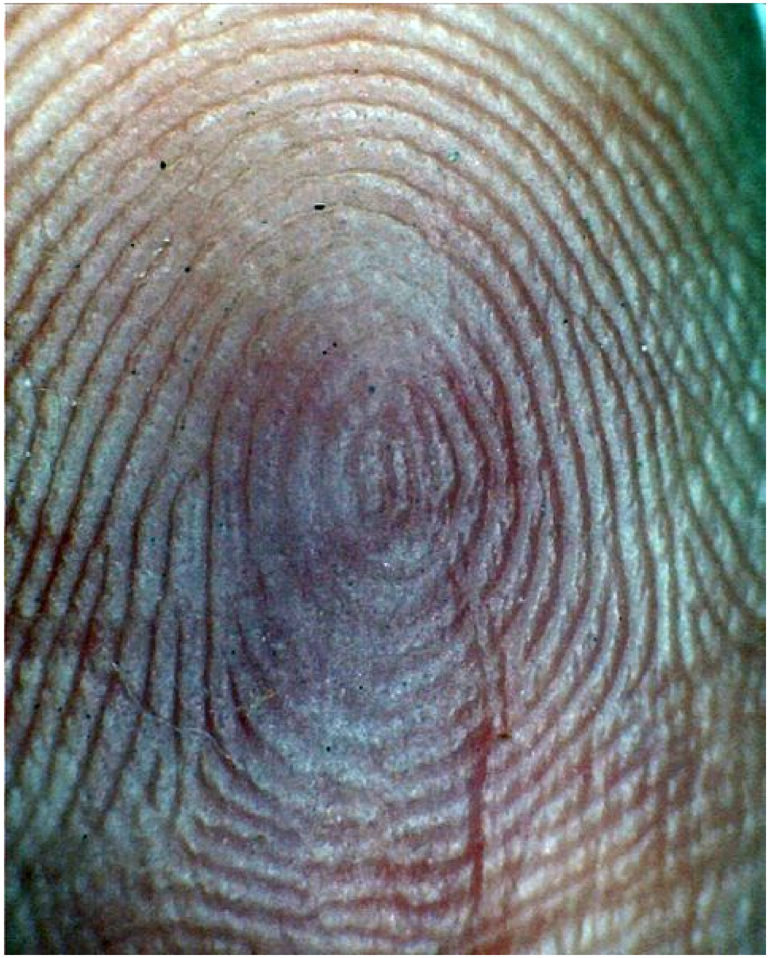


Digital fingerprint

“Fingerprints are created by applying a cryptographic hash function to a public key. ”

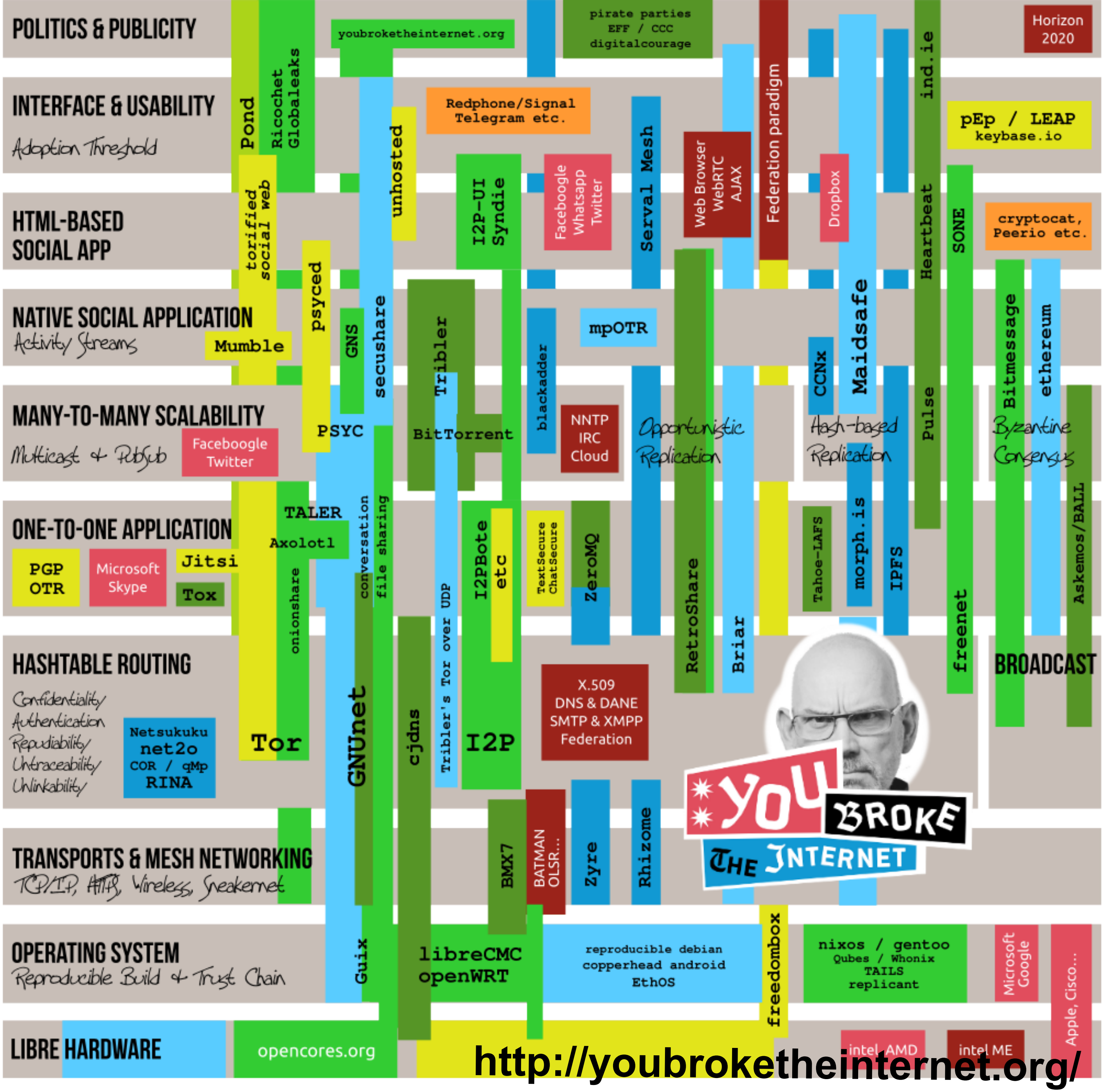
https://en.wikipedia.org/wiki/Public_key_fingerprint

Photo credit: Author Saurabh R. Patilon Wikimedia



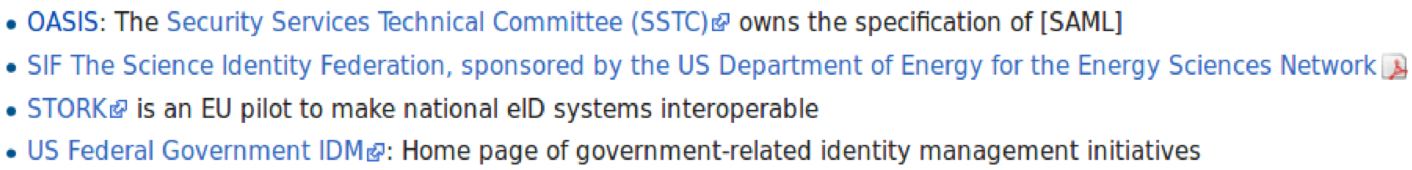
Basic uses of certificates

1. Logging-in to Websites
2. Securing one’s own Websites
3. Downloading software
4. Sending email
5. Signing documents
6. Using certificates instead of passwords
7. Long-term document preservation (PDF/A, **https://www.pdfa.org/topics/**)

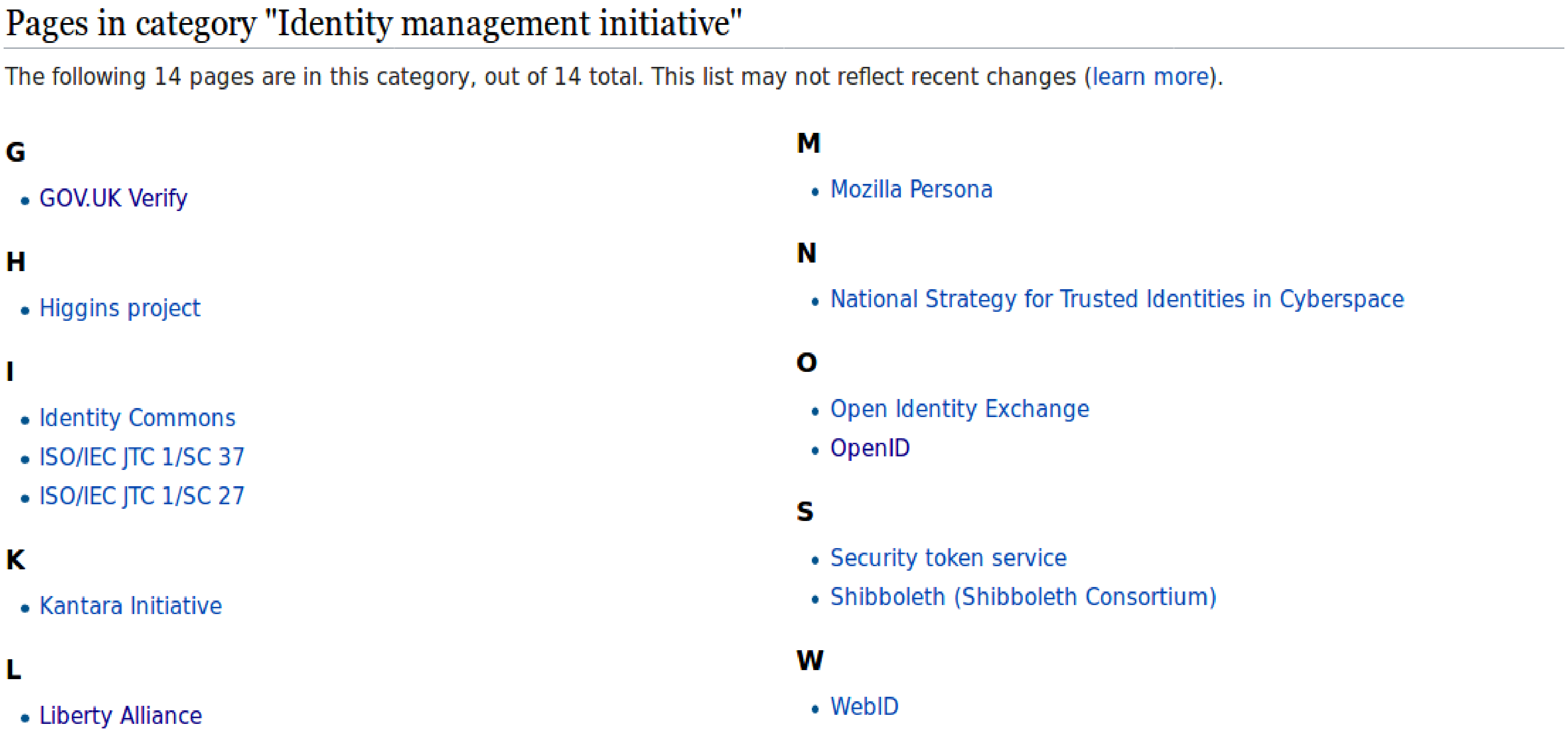


http://youbroketheinternet.org/

Samples of id. management initiatives listed in Wikipedia



- OASIS: The Security Services Technical Committee (SSTC) owns the specification of [SAML]
- SIF The Science Identity Federation, sponsored by the US Department of Energy for the Energy Sciences Network
- STORK is an EU pilot to make national eID systems interoperable
- US Federal Government IDM: Home page of government-related identity management initiatives



Pages in category "Identity management initiative"

The following 14 pages are in this category, out of 14 total. This list may not reflect recent changes (learn more).

G

- GOV.UK Verify

H

- Higgins project

I

- Identity Commons
- ISO/IEC JTC 1/SC 37
- ISO/IEC JTC 1/SC 27

K

- Kantara Initiative

L

- Liberty Alliance

M

- Mozilla Persona

N

- National Strategy for Trusted Identities in Cyberspace

O

- Open Identity Exchange
- OpenID

S

- Security token service
- Shibboleth (Shibboleth Consortium)

W

- WebID

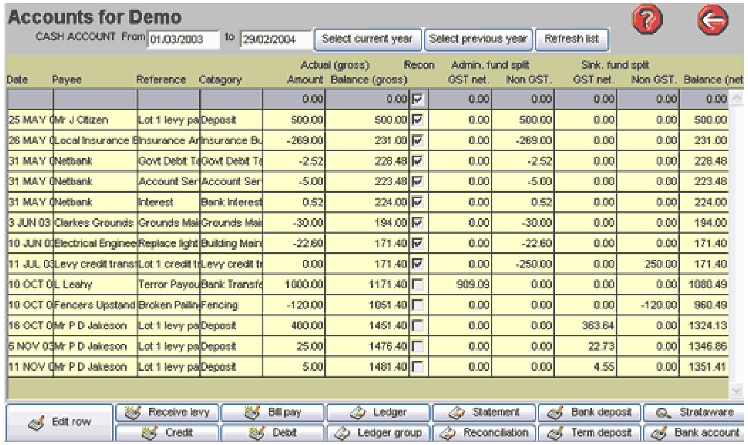
The Future of Digital Identity

- Getting beyond Google/Facebook passwords

- The MyData Global Network organized by Finns **mydata.org**

- **Mydex.org** and Qiy / Sovrin / blockchain ledger (recommend Vigna/Casey *Age of Cryptocurency*)

- Kupplinger-Cole



Accounts for Demo

CASH ACCOUNT From 01/03/2003 to 29/02/2004

				Actual (gross)		Recon	Admin. fund split		Sink. fund split		
Date	Payee	Reference	Catagory	Amount	Balance (gross)		GST net.	Non GST.	GST net.	Non GST.	Balance (net
				0.00	0.00	☑	0.00	0.00	0.00	0.00	0.00
25 MAY 0	Mr J Citizen	Lot 1 levy pa	Deposit	500.00	500.00	☑	0.00	500.00	0.00	0.00	500.00
26 MAY 0	Local Insurance B	Insurance Ar	Insurance Bu	-269.00	231.00	☑	0.00	-269.00	0.00	0.00	231.00
31 MAY 0	Netbank	Govt Debit Ta	Govt Debit Ta	-2.52	228.48	☑	0.00	-2.52	0.00	0.00	228.48
31 MAY 0	Netbank	Account Ser	Account Ser	-5.00	223.48	☑	0.00	-5.00	0.00	0.00	223.48
31 MAY 0	Netbank	Interest	Bank Interest	0.52	224.00	☑	0.00	0.52	0.00	0.00	224.00
3 JUN 03	Clarkes Grounds	Grounds Mai	Grounds Mai	-30.00	194.00	☑	0.00	-30.00	0.00	0.00	194.00
10 JUN 0	Electrical Enginee	Replace light	Building Main	-22.60	171.40	☑	0.00	-22.60	0.00	0.00	171.40
11 JUL 03	Levy credit transf	Lot 1 credit tr	Levy credit tr	0.00	171.40	☑	0.00	-250.00	0.00	250.00	171.40
10 OCT 0	L Leahy	Terror Payou	Bank Transfe	1000.00	1171.40	□	909.09	0.00	0.00	0.00	1080.49
10 OCT 0	Fencers Upstand	Broken Palin	Fencing	-120.00	1051.40	□	0.00	0.00	0.00	-120.00	960.49
16 OCT 0	Mr P D Jakeson	Lot 1 levy pa	Deposit	400.00	1451.40	□	0.00	0.00	363.64	0.00	1324.13
6 NOV 03	Mr P D Jakeson	Lot 1 levy pa	Deposit	25.00	1476.40	□	0.00	0.00	22.73	0.00	1346.86
11 NOV 0	Mr P D Jakeson	Lot 1 levy pa	Deposit	5.00	1481.40	□	0.00	0.00	4.55	0.00	1351.41

Document signing made convenient

- **www.signinghub.com** claim: “Expert in high-trust, Advanced & Qualified Electronic Signatures, Turnkey solution providing both local and remote signing plus a built-in complete PKI system”
- **docusign.com** is competitor offering fewer features
- Some solutions collect user profiles (via surveillance techniques) to secure IDs.
- Keybase.io is little project also centralizing indicators of one’s ID, but less invasively.

SaaS in the Cloud

- Currently 81 entries for identity-access-mgmt, **https://azuremarketplace.microsoft.com**

- Salesforce, SAP, Citrix
- Axciom -- recent breach!
- Adobe Document Cloud, Adobe Sign, **https://acrobat.adobe.com/us/en/sign.html**

Trust frameworks in law

Identity systems have their own rules, which fit into their respective trust frameworks. The later fall under general ID mgmt law, which in turn comprises part of general commercial law.

Source: Makaay, Esther / Tom Smedinghoff / Don Thibeau (2017): "Trust Frameworks: Their Critical Role in Critical Role in Governing Identity Systems", **http://www.openidentityexchange.org/wp-content/uploads/2017/06/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf**

Historical development of ID paradigms

- Phase One: **Centralized** Identity (administrative control by a single authority or hierarchy)
- Phase Two: **Federated** Identity (administrative control by multiple, federated authorities)
- Phase Three: **User-Centric** Identity (individual or administrative control across multiple authorities without requiring a federation, vs. *server*-centric)
- Phase Four: **Self-Sovereign** Identity (individual control across any number of authorities) - **the Blockchain**, e.g.

World’s largest ID program

- India is registering one billion citizens
  - Supreme court has ruled in favour of citizen privacy
- World Bank has a program, **www.worldbank.org/en/programs/id4d**

- **Understanding digital certificates is useful, and applying them manually is possible. However, big companies are offering mainstream signing solutions with greater convenience for a larger public.**