SK Conference: Identification physically and digitaly

Joseph Leibenguth, Technical Advisor
Nov 2015

Agenda

- Market trends: Travel Segment
- Travel Key Needs: Travel Identification Program
- Combining strengths for secure identity solutions
- A Digital Future
- When digital / machine readable features reinforce the physical document
- Megatrends
- Virtual DNA

Market Trends: Travel Segment

770 Mu

Over 770 million ePassports now

667 Mu in October 2014 – source ICAO

53%

53% of passports will have a smart chip by 2017

$15bn

The global border control and biometric market will grow from $5bn to $15bn from 2012 to 2021 source Frost & Sullivan February 2013

Travel Key Needs

- Migrate to new travel documents to actively combat fraud and increase trust at both national and international levels
  ePassport, eResident permit
- Make border crossing faster, more secure and more convenient
  Border and Visa management
- Bring new services to passengers
  New ePassport generation,on-line services

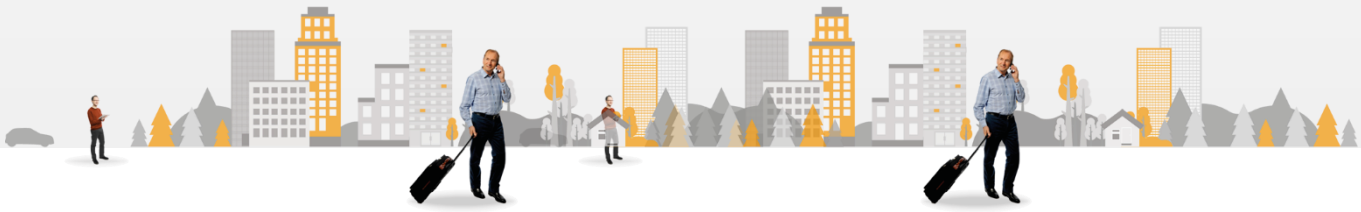
The right time for the Traveler Identification Program

As experts of both documents and related solutions, Gemalto strongly supports this initiative and shares the vision that there must be a global fight against fraud by securing all the links in the security chain.

The TRIP (Traveler identification Program) initiative is a framework for security and facilitation, representing an evolution of ICAO's requirements on secure documents to focus more on identification management.

gemalto

Combining strengths for secure identity solutions



gemalto

TRUB by Gemalto

gemalto

Quality, precision, security and innovation

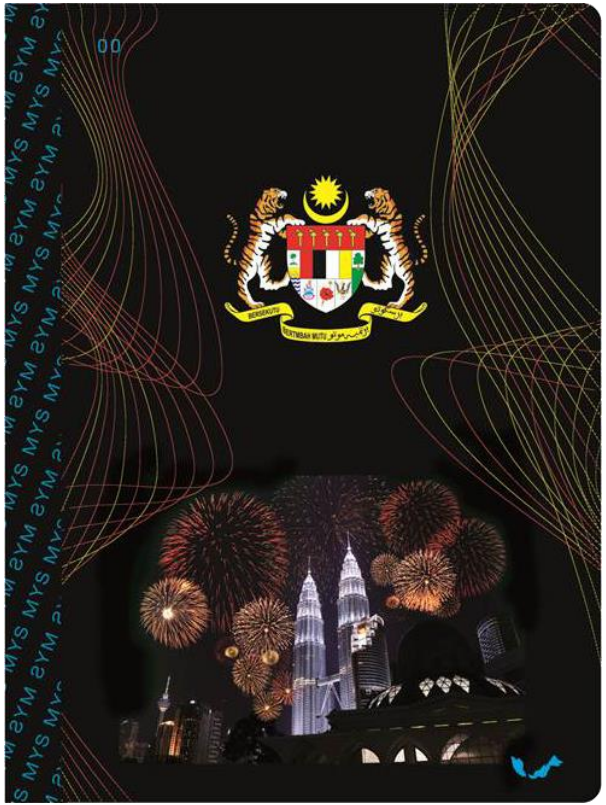
Sealys Color in PC - Indisputable proof of identity now in high-definition color for cards and passports

Quality, precision, security and innovation

Sealys 3D surface - Authenticity you can see and feel

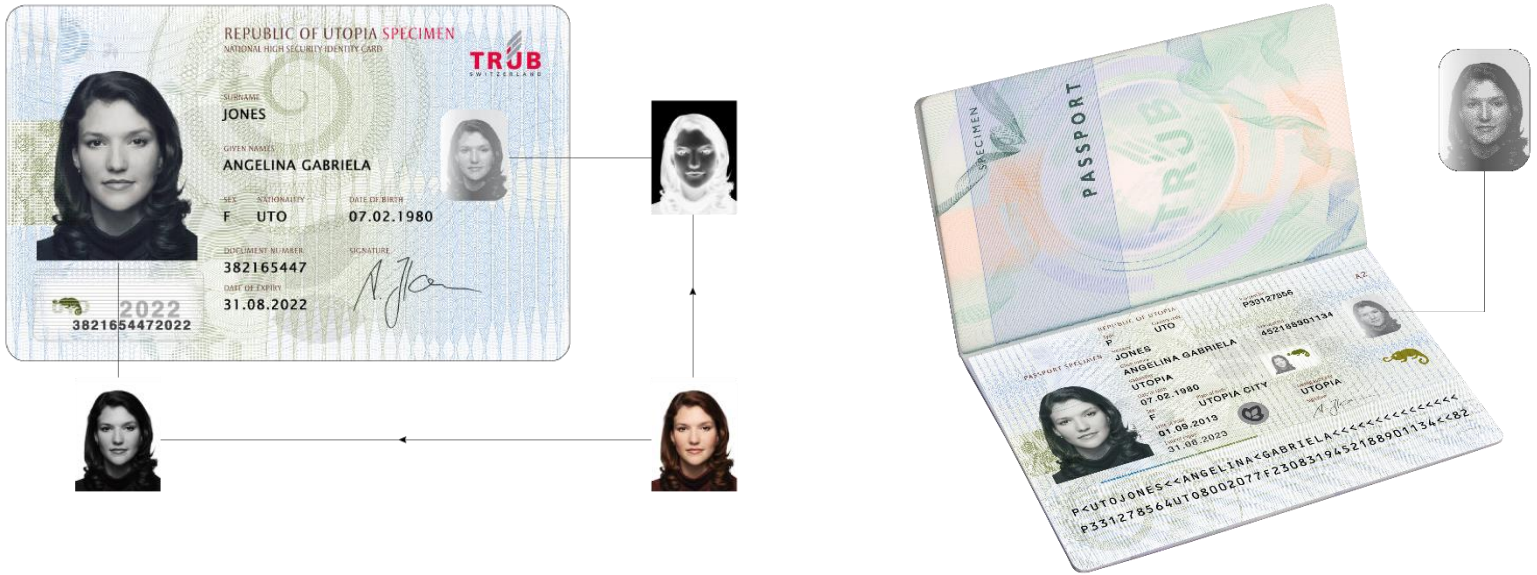
Quality, precision, security and innovation

Sealys True Vision – Now you can see



Quality, precision, security and innovation

Sealys Window Lock - A new dimension in photo protection



gemalto

Quality, precision, security and innovation

Sealys Edge Sealer - At the cutting edge of document security

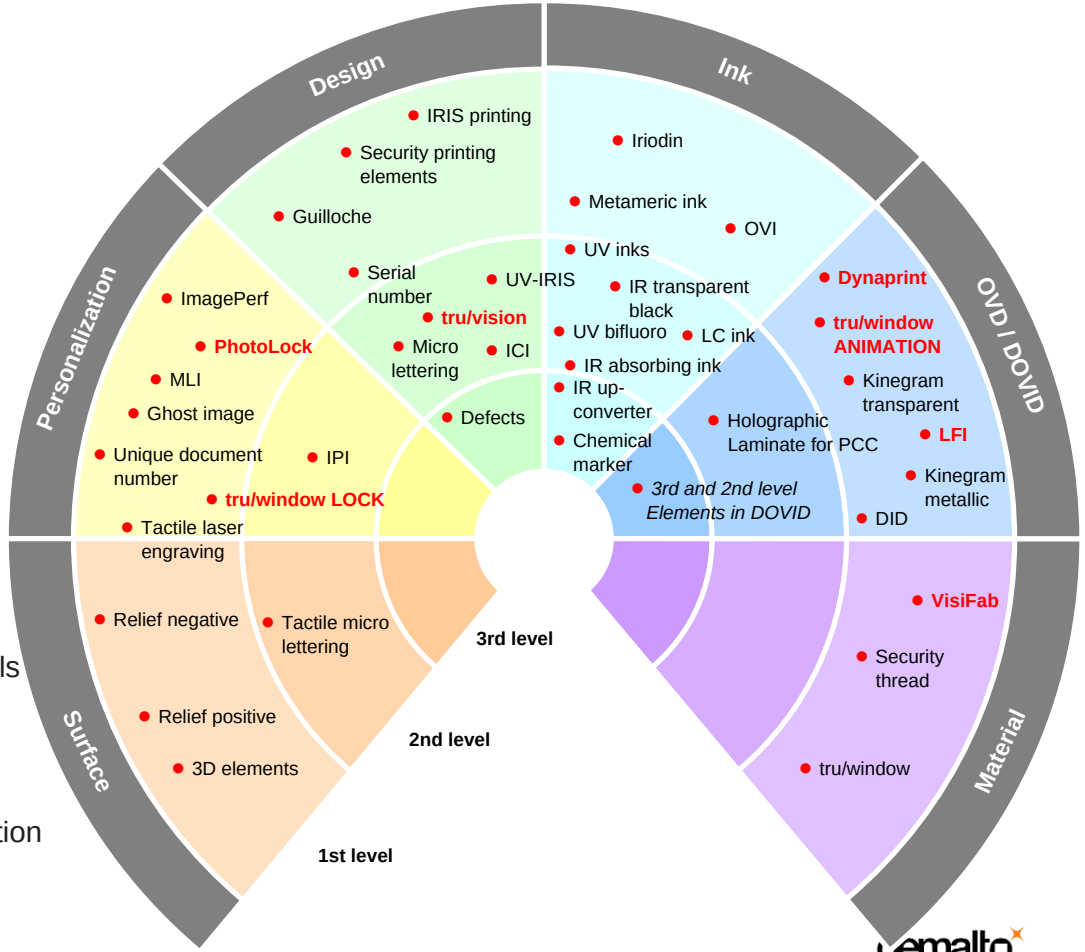
Quality, precision, security and innovation

Sealys Datapage 600e - The world’s thinnest datapage with a chip

gemalto

Security features for polycarbonate documents

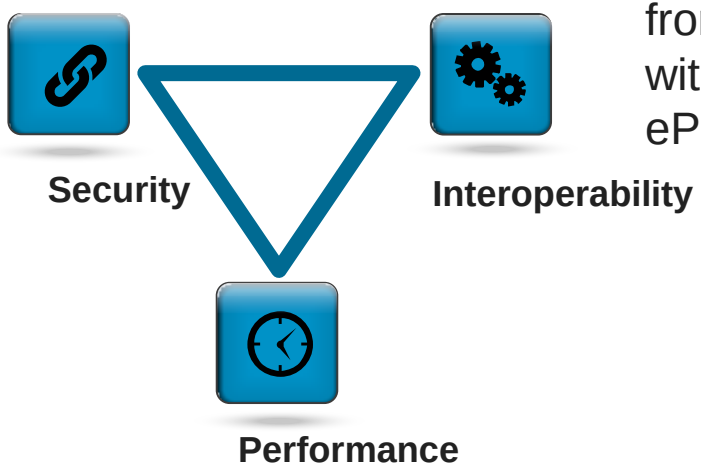
- Security concept
  - Photo, text and document protection
  - Multi-layer approach
  - Multiple personalized holder data (CoreMark, tru/window™ LOCK, MLI, ImagePerf)
  - Electronic data storage
- Security measures
  - Balanced set of security features and techniques implemented into the document providing multiple integrated layers of security to defeat fraudulent attack
- Offering/Portfolio
  - Comprehensive portfolio of optical and physical security features for polycarbonate documents
  - Classification in different categories and security levels
- Innovation
  - Continuous development of new security features for photo, text and document protection
  - Cooperation with partners and Universities



OS: Perfect Equilibrium for Optimal Results

Strong Common Criteria Evaluation

Wide range of algorithms and long key lengths



Gemalto OS have been tested during all major interoperability test events since 2004. Our products are field proven, with citizens from 30 countries traveling with their Gemalto ePassports

Gemalto eTravel is one of the fastest products of the market, according to ICAO international tests sessions

End to End Security for Higher Citizen Privacy

- Full security on the entire value chain, from the OS to the Issuance and Verification solution
- Our leading security team deliver the latest counter measure against various attacks
- Our Products achieve stringent security certificates

Common Criteria

Bundesamt für Sicherheit in der Informationstechnik

ANSSI Agence nationale de la sécurité des systèmes d'information

- Support of the latest Enhanced security mechanisms
  - Extensive set of key lengths supported
  - AES and Elliptic Curves cryptography

gemalto

A Digital Future

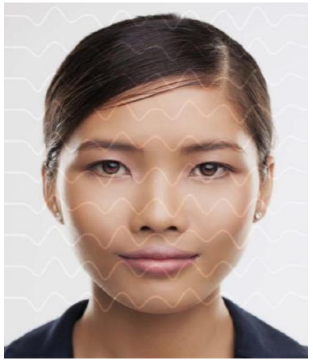
- Physical identity documents
  - ePassport
  - Driving License
  - Permanent Resident
  - etc

- Virtual & Mobile identity
  - Digital credentials for various personas
  - Derived Government issued credentials in cyberspace
  - Presentation local or online. Usages to be defined

- Its not 2030 – its much closer. Convenience with rapid adoption
- Privacy & Security issues will be overcome quickly
- 9303 will need more parts for digital & virtual travel credentials

Security on top of Photo

- Surface embossing on top of photo
- Black & white Laser Sealer
  - Enhanced security on personalization phase
  - Reveals any attempts to modify photo
  - Cost effective security feature
- Color or luminance Guillochés
  - Adapted to color photo
  - The guillochés pattern can be personalized and diversified for each card
- Encoded information in Guillochés
  - To the original picture is added the personalized guilloche
  - High quality color photo for insertion of robust watermarking



Digital Seal: example for Visas

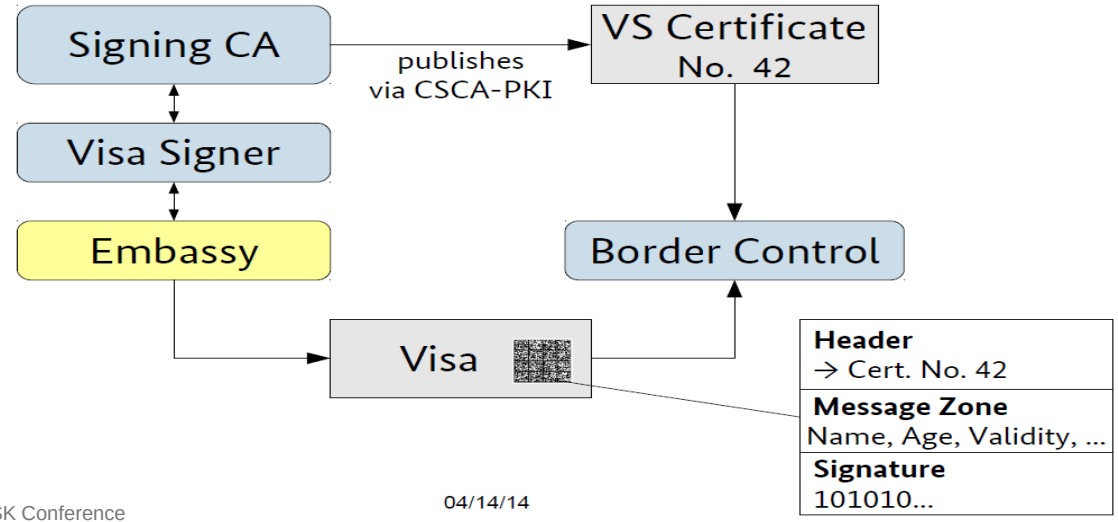
- EU currently developing new visa sticker
  - Joint proposal from France (ANTS) and Germany (BSI)
- “if we have a sticker, then let's make it secure”
- Typical Threats
  - stolen blanks
  - Transfer to another passport
  - Alter data fields (name, age, validity date, ...)
  - Faking from scratch
- *This document specifies a digital seal to ensure the authenticity and integrity of visa documents in a comparatively cheap, but highly secure manner using asymmetric cryptography*

Digital Seal: example for Visas

- Personalization: Each seal verifies the information printed on the visa document, and is thus tied to the visa applicant
- Easy verification: Even untrained personal is able to verify a visa document protected with a dig-ital seal by using low cost equipment, such as an application (“app”) on a smart phone.

Visible Digital Seal:

cryptographic signature of visa data stored as 2D Barcode



Coesys Document Verification Solution

Enabling sophisticated document security feature verification. Authorities select and control zones and features of interest for each document type.

Know Your Customer – Drivers and Use case

Drivers for the private sector

MNO

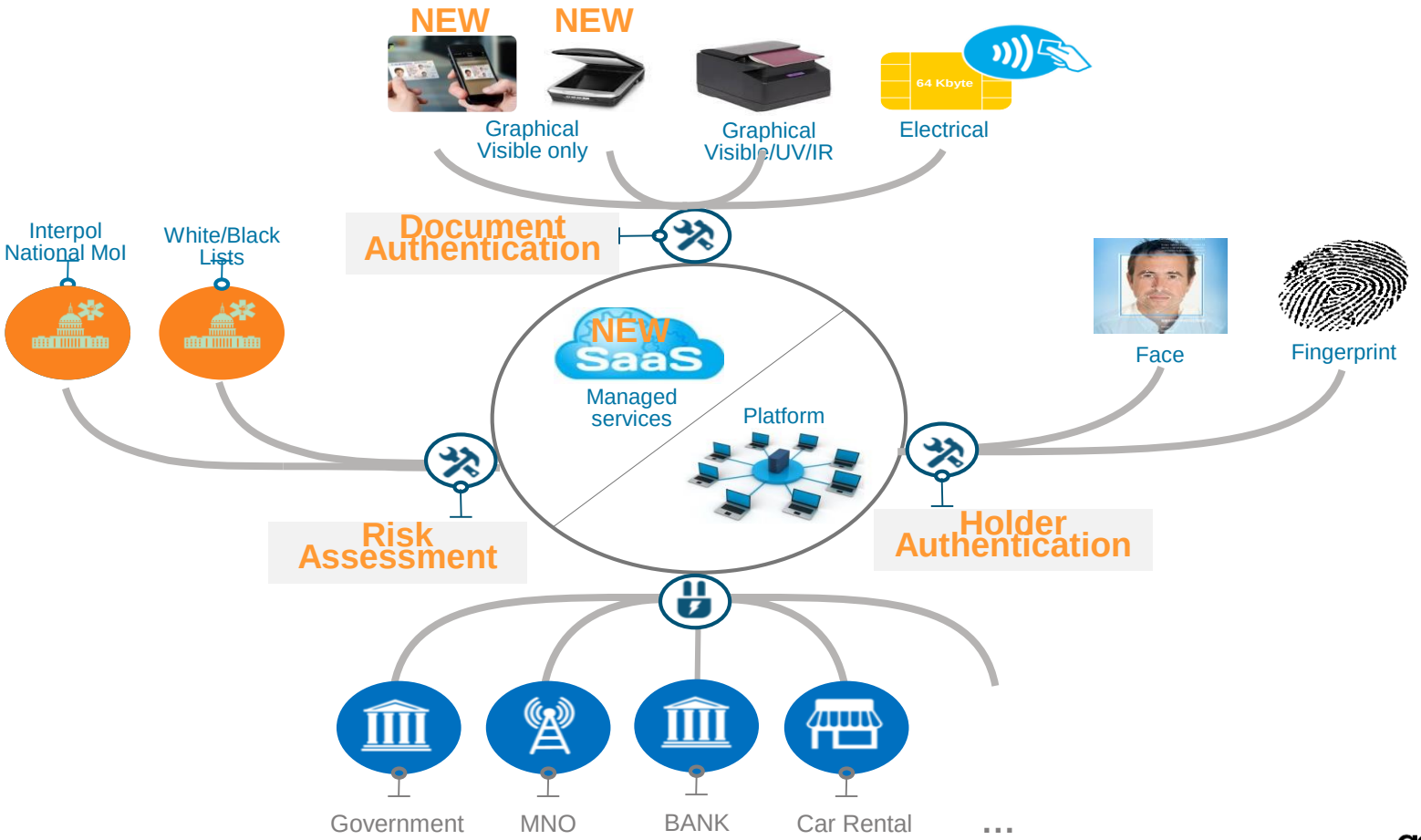
- MNOs experiment a high level of Identity **fraud**, involving phone robbery
- National **regulations** often impose inquiries prior to the subscription of a new line

BANK

- Banks experiment a high level of Identity **fraud**, involving financial losses on credit cards and loans
- Anti Money Laundering (AML) and Anti Terrorism financing **regulations** impose KYC prior to the opening of a bank account

Use case

KYC – Offer

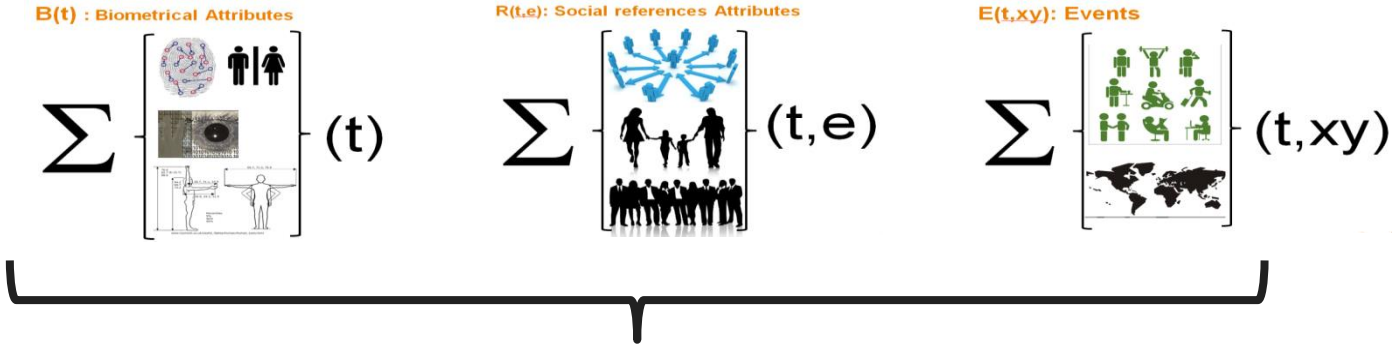

NEW
NEW
Graphical
Visible only
Graphical
Visible/UV/IR
64 Kbyte
Electrical
Interpol
National MoI
White/Black
Lists
Document
Authentication
NEW
SaaS
Managed
services
Platform
Face
Fingerprint
Risk
Assessment
Holder
Authentication
Government
MNO
BANK
Car Rental
...

Megatrends

- Digitalization of the world
  - Ubiquitous computing
    - Any services, anywhere and anytime within a secure and user friendly context.
  - Federation/aggregation of services…leading to ambiance intelligence concepts
- Needs of Privacy enforcement
  - No free meals: if you do not pay for a product then you are the product.
- More and more virtualization
  - Faster and simpler development
  - Easy access for any size of companies
  - Shorter life cycles

IDENTITY: What is it?

- Collection of Attributes(*)

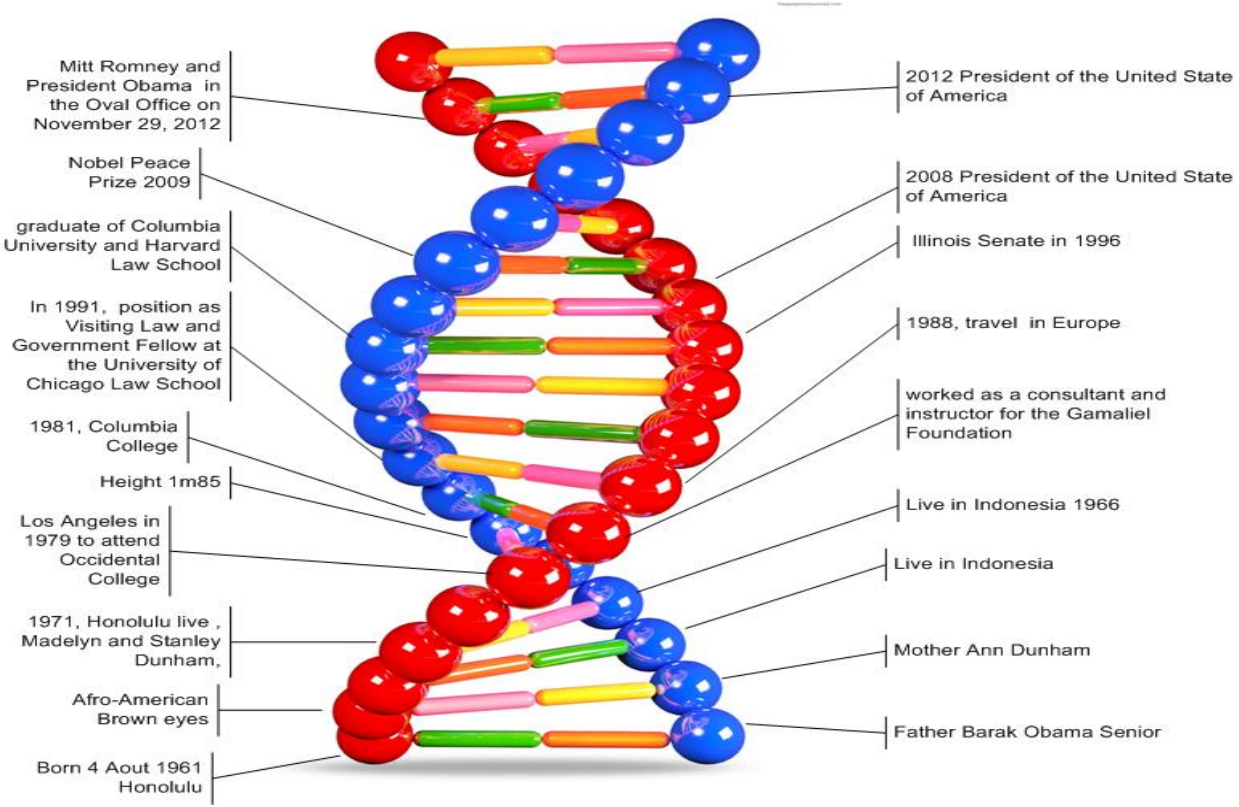


=

Identity Signature footprint (a virtual DNA)

* Most of them are referenced to the time (and the space)

Identity: a virtual DNA



- Redundant
- Traceable
- Cross-checkable
- Recordable
  - Partially
- Authentic
  - Cannot be faked globally

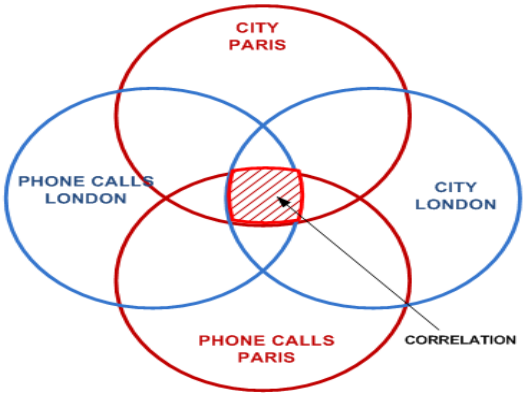
$$DNA(t) = \begin{pmatrix} B(t) \\ R(t,e) \\ E(t,xy) \end{pmatrix}$$

The Privacy by Design : 7 Principles

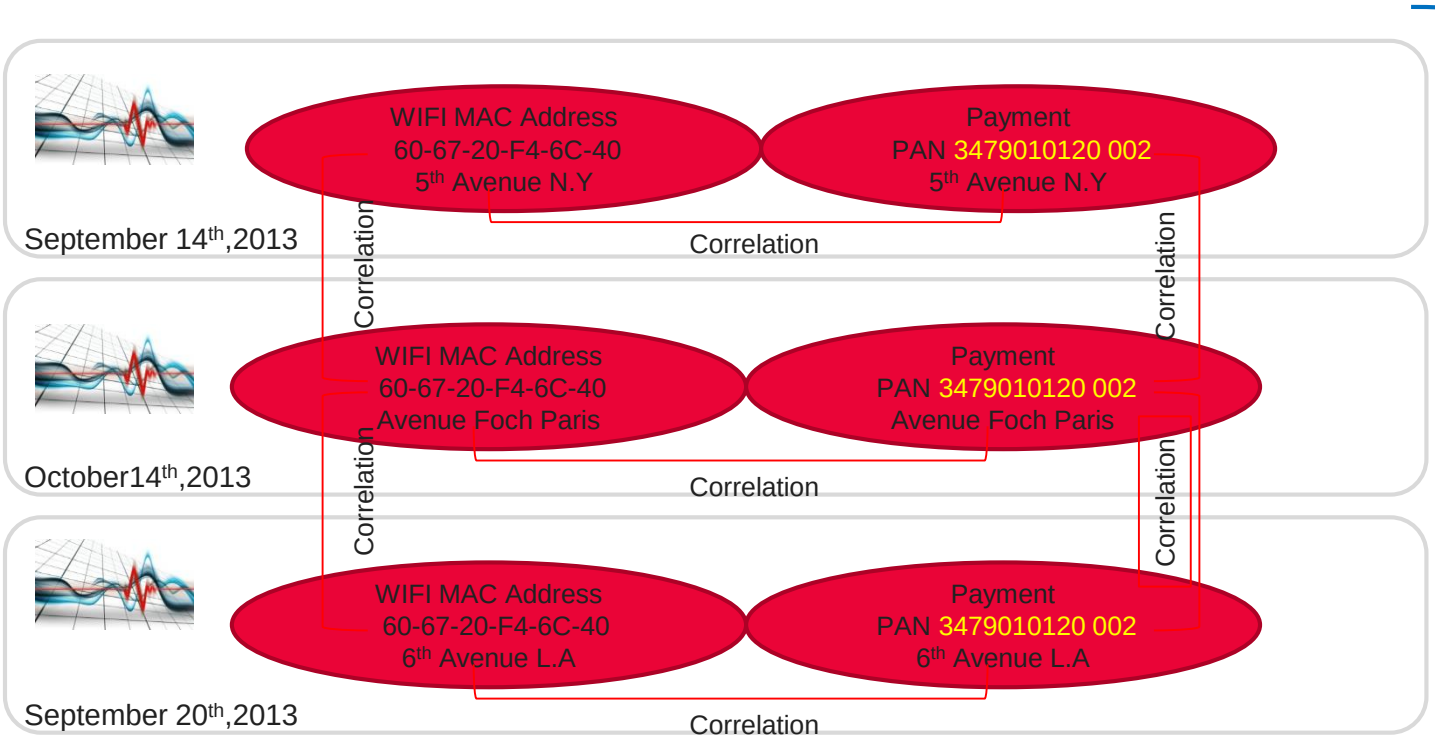
- 1. Proactive not Reactive; Preventative not Remedial
- 2. Privacy as the Default Setting
- 3. Privacy Embedded into Design
- 4. Full Functionality — Positive-Sum, not Zero-Sum
- 5. End-to-End Security — Full Lifecycle Protection
- 6. Visibility and Transparency — Keep it Open
- 7. Respect for User Privacy — Keep it User-Centric

Design impacts about Data Correlation

- The No Traceability property: The hardest property to support for data exchanges with:
  - No large constant data
  - No large identifier
  - No diversified Public key
  - No UUID
  - No static combination of small constants (fingerprinting)



Data Correlation & scoring example



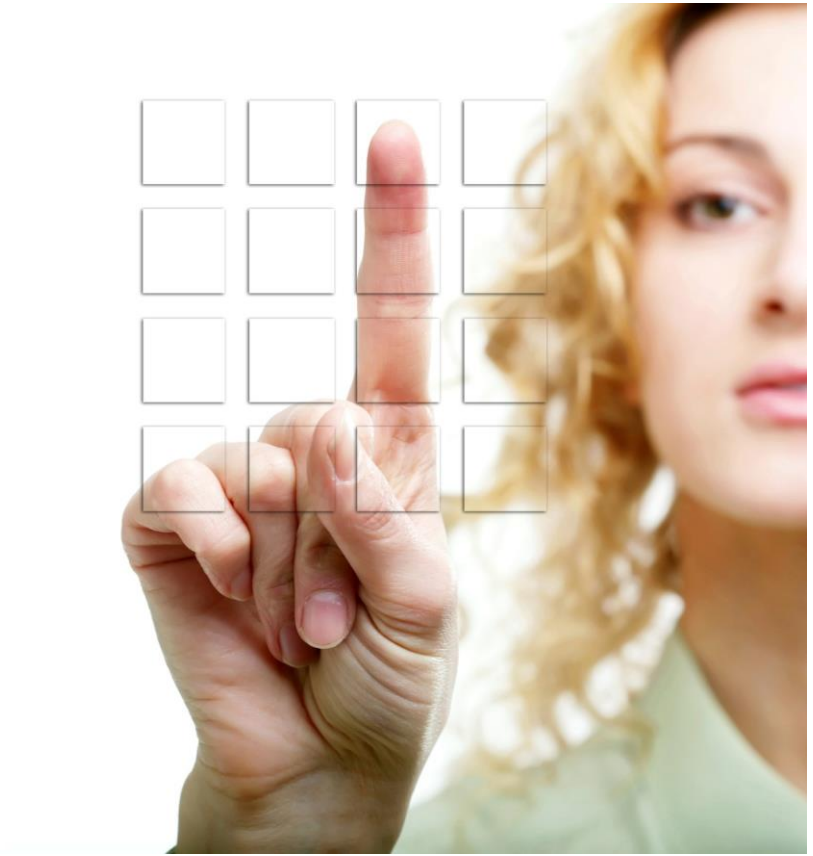
Scoring

60-67-20-F4-6C-40 = 3479010120 002 = John Does

What did we?

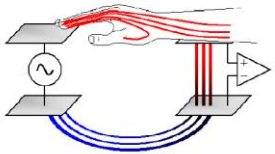
eGo

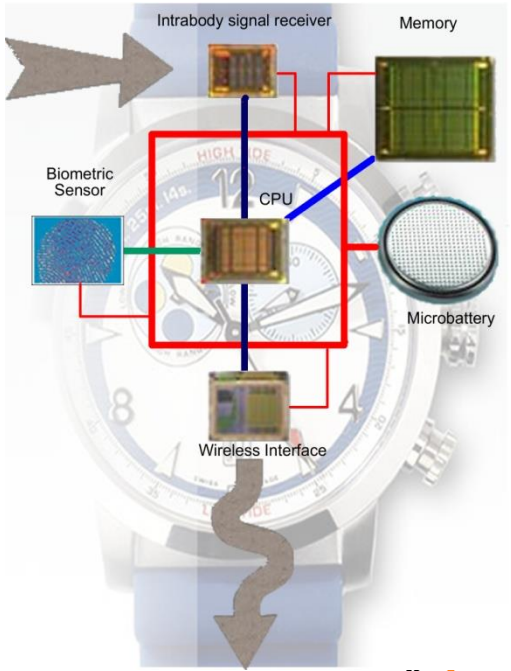
What you touch is yours



The eGo project

- Started in 2004
  - eGo Catrene program in 2010 to 2014 (www.ego-project.eu)
  - H20 Catrene program in 2015 to 2018
- Minimal technology for a wearable device and the user's credentials support
  - Easy pairing (BCC) of any eGo compliant devices touched by the user
  - Long autonomy on several weeks
  - Harsh Environment support
  - Credentials recovery
  - Multi-tenants and multi-TSM
- Privacy by Design
  - authenticity, anonymity, non traceability.
  - Non relay attack possibility (UWB), Lost detection
  - Common criteria capable
- User's interface Friendly
  - Education/age independence (natural user's interface)
  - Single sign-on and strong authentication (2FA)
  - Automatic and programmed application termination (UWB)
  - On the go transaction and long transaction support
  - Fast (<200 ms) application setup
  - Implicit (pre-agreement) and explicit (post-agreement) eGo pairing
- Side effect capability
  - Accurate RTLS





eGo™; concept

- **What is it?**
  - A new way to establish a bidirectional secure, high-speed wireless channel between “objects”
  - Implemented in a secure portable device hosting all usual applications/credentials of a smart card
- **What is the form factor?**
  - Any form factor as a watch, a key ring, a jewel capable to host the eGo electronic
- **How it works?**
  - A unidirectional intra-body communication wakes up the eGo device and bootstrap a high speed wireless and bidirectional communication between eGo and an eGo compliant device
- **What do we get?**
  - A logical channel between eGo and an eGo compliant device which has been previously touched.
- **Market drivers**
  - Natural, no education needed, user friendly

Thank you!


gemalto
security to be free
Securing the identity
of billions of citizens
> Securing identity and protecting privacy
> Enabling trusted eServices
> Facilitating travel experience while enhancing security