BUNDES DRUCKEREI

# Identidades digitales: desafíos, tecnologías y soluciones

Digital Identities: Challenges, Technologies & Solutions

Walter Fumy, Chairman ISO/IEC JTC 1/SC 27
Chief Scientist
Bundesdruckerei GmbH

# Agenda

## I. Introduction & Motivation

- Major trends & digital identities
- Entropy & identification

## II. Simplicity & the Human Factor

- Passwords must die
- Biometrics as a (limited) alternative

## III. Standards, Solutions & Documents

- ISO/IEC initiatives
- Example areas of application
- System on Document
- Intrinsic object IDs

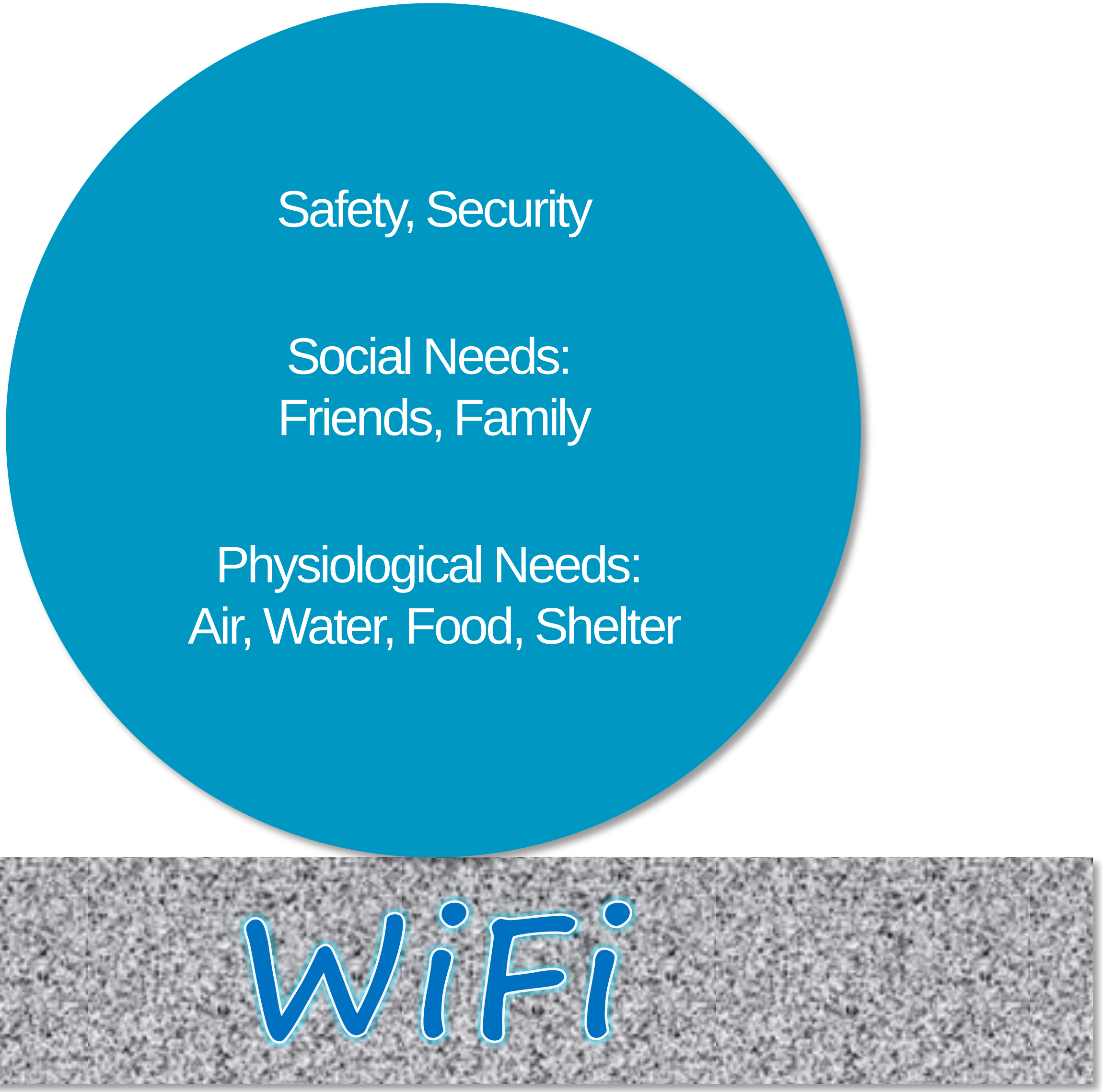
## IV. Futures of ID

## V. Conclusion

I

# Introduction & Motivation

# Basic Human Needs

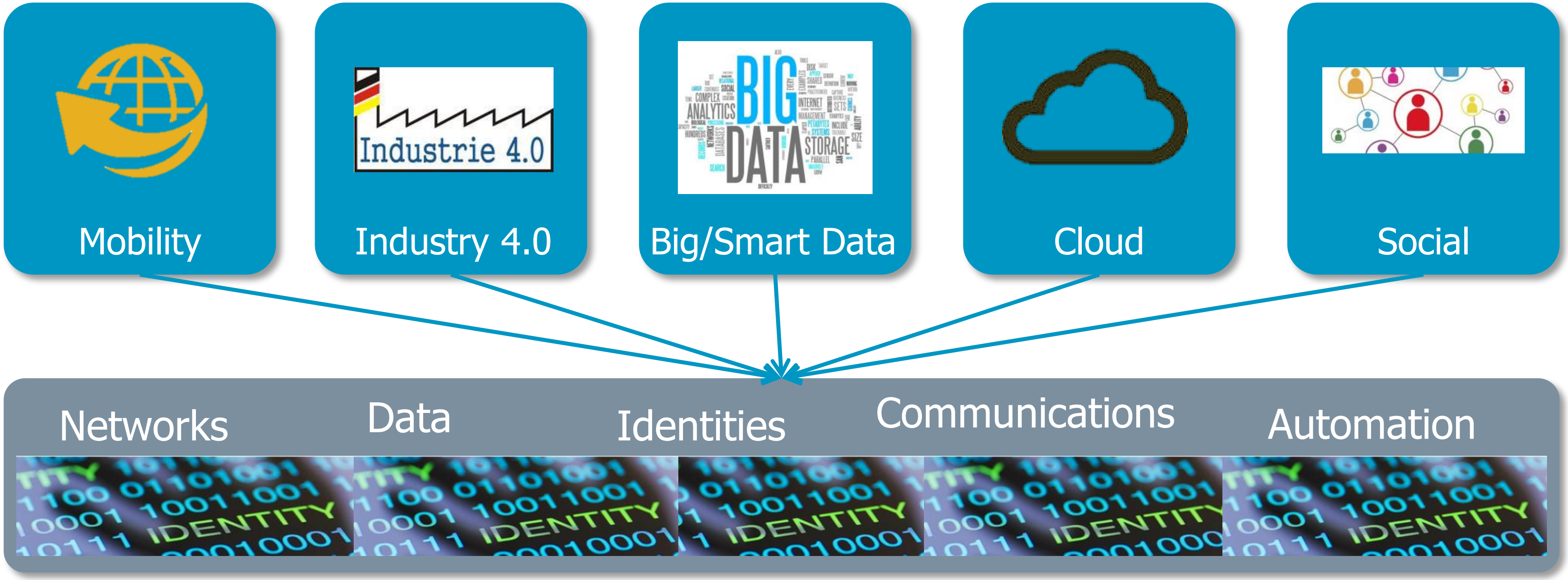


Safety, Security

Social Needs:
Friends, Family

Physiological Needs:
Air, Water, Food, Shelter

# Major Trends and Digital Identities



Mobility

Industry 4.0

Big/Smart Data

Cloud

Social

Networks

Data

Identities

Communications

Automation

**Need for technologies to uniquely authenticate persons, objects and processes**

**Identity management for individuals, objects & processes**

# Orders of Magnitude – *We are not that many*

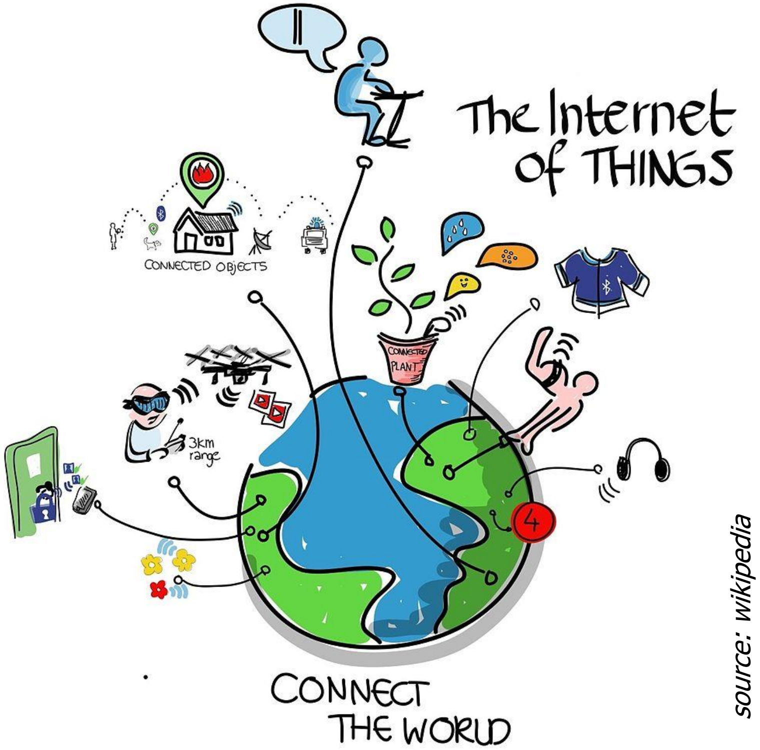
*grain of rice* →

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Alice & Bob | | | | | | |
| | | | | | | | |
| | | | | | | | 23 |
| | | | 27 | | | *giga* | |
| IPv4 | | | | | | | |
| *tera* | | | | | | | |
| | | *peta* | | | | | |
| DES | | | | *exa* | | | 63 |

# Internet of Things (IoT)

IoT is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure, where "things" can refer to a wide variety of objects and devices.

- „26 billion devices on the IoT by 2020" (Gartner)
- „more than 30 billion devices on the IoT by 2020" (ABI Research)
- „1 trillion devices by 2025"
- „individuals in urban environments each surrounded by 1.000 to 5.000 trackable objects"
- „largest IT market ever"



source: wikipedia

Standardization efforts

- ISO/IEC JTC 1/SWG 5, ITU-T JCA-IoT, IEEE-P2413, … and many more

# Names of large numbers

Q:
How much
is a trillion?

$10^6$ = million

$10^9$ ?=? billion ?=? $10^{12}$

$10^{12}$ ?=? trillion ?=? $10^{18}$

$10^{15}$ ?=? quadrillion ?=? $10^{24}$

$10^{18}$ ?=? quintillion ?=? $10^{30}$

A:
It depends*

*) *short scale vs. long scale*

# Orders of Magnitude (II)

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Alice<br>& Bob | | | | | | | | | | | | | | | |
| | | | | *million* | | | 23 | | | | 27 | | | *billion* | | |
| IPv4 | | | | | | | | *trillion* | | | | | | | | |
| | | *peta* | | | | | | DES | | | | *Trillion* | | | | |
| | | | | | | *zetta* | | | | | | | | | | |
| *yotta* | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | 127 | |
| AES<br>-128 | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| AES<br>-196 | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | 255 | | IPv6 |

# Entropy & Identification

In information theory, **entropy** quantifies the expected value of information contained in a ‘message’, usually in bits

- toss of a fair coin has an entropy of 1 bit
- identification of a random, unknown person has < 33 bits of entropy

Learning a new fact about a person reduces the entropy of their identity by

$$\Delta S = - \log2 \Pr(X=x)$$

where Pr(X=x) is the probability that the fact would be true of a random person

$$-\log2 \Pr(\text{date of birth} = \text{Aug } 05) = -\log2\ (1/365) = 8{,}51 \text{ bits}$$

Web browsers are subject to “device fingerprinting” via version and configuration information they transmit

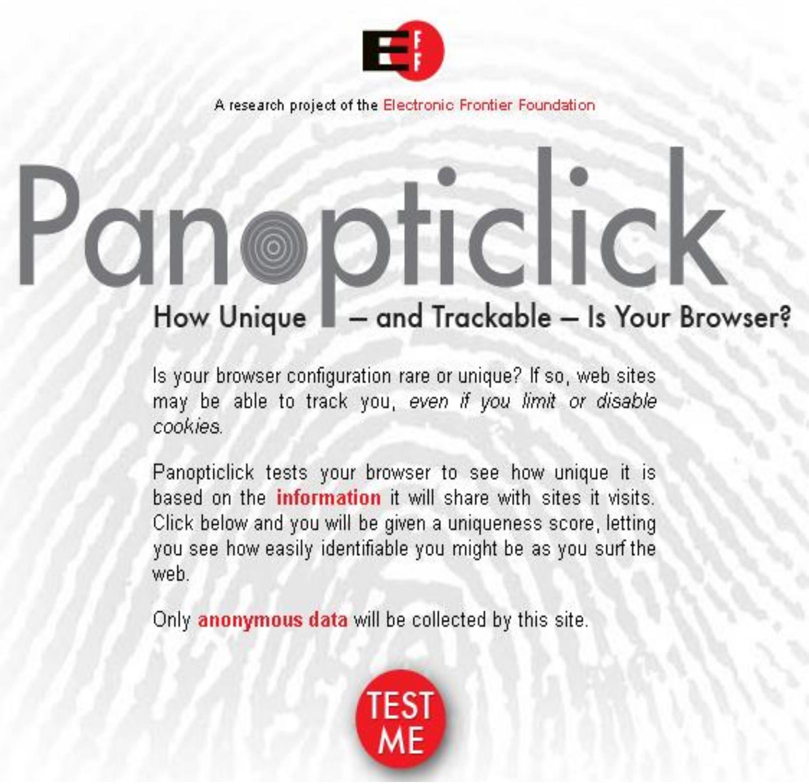
- E.g., ‘User-Agent’ string containing name, operating system and version number of the browser typically reveals ~15 bits of entropy*

**) source: Peter Eckersley: „How Unique Is Your Web Browser?”, 2010*

# Entropy Harvesting – *Your Browser's Intrinsic ID*

Panopticlick investigates the real-world effectiveness of browser identification algorithms

- 83.6% of browsers* show unique fingerprint
- 94.2% when Adobe Flash or Java VM is enabled
- ~ 5% with anonymity set of size 2
- browser fingerprints change quite rapidly, however, correctly guessing and following these fingerprint changes is not too hard
- potential global identifier – similar to a cookie that can hardly be deleted
- for some defenses against browser fingerprinting see https://panopticlick.eff.org/



A research project of the Electronic Frontier Foundation

Panopticlick

How Unique – and Trackable – Is Your Browser?

Is your browser configuration rare or unique? If so, web sites may be able to track you, *even if you limit or disable cookies*.

Panopticlick tests your browser to see how unique it is based on the **information** it will share with sites it visits. Click below and you will be given a uniqueness score, letting you see how easily identifiable you might be as you surf the web.

Only **anonymous data** will be collected by this site.

TEST ME

**) source: Peter Eckersley:*
*„How Unique Is Your Web Browser?", 2010*

II

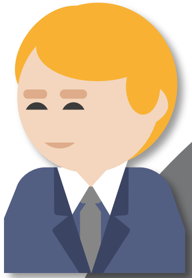
# Simplicity & the human factor

# Law of Nature ?

Security

Simplicity

# Challenge –
# *The Human Factor*



i love you

???

let me in

# j%7K&yPx$ can be difficult to remember – *the 15 most used passwords in 2014 vs. 2013*

| 2014 | 2013 |
|---|---|
| 123456 | 123456 |
| password | password |
| 12345 | 12345678 |
| 12345678 | qwerty |
| qwerty | abc123 |
| 1234567890 | 123456789 |
| 1234 | 111111 |
| baseball | 1234567 |
| dragon | **iloveyou** |
| football | adobe123 |
| 1234567 | 123123 |
| monkey | admin |
| **letmein** | 1234567890 |
| abc123 | **letmein** |
| 111111 | photoshop |

*source: splashdata.com*

**„To keep your customers, keep it simple“**

*Harvard Business Review, 2012*

# Design Principles for Secure Systems
## *Selected History*

1883 – Six principles of Kerckhoff, including

- Secure even if everything about the system, except the key, is public knowledge
- Easy to use and should not require its users to know and comply with a long list of rules

1975 – Eight principles of Saltzer & Schröder, including

- Economy of Mechanism: Keep the design as simple and small as possible
- Least Privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job
- Psychological Acceptability

1999 – Whitten & Tygar: Why Johnny can't encrypt – A case study (PGP 5.0)

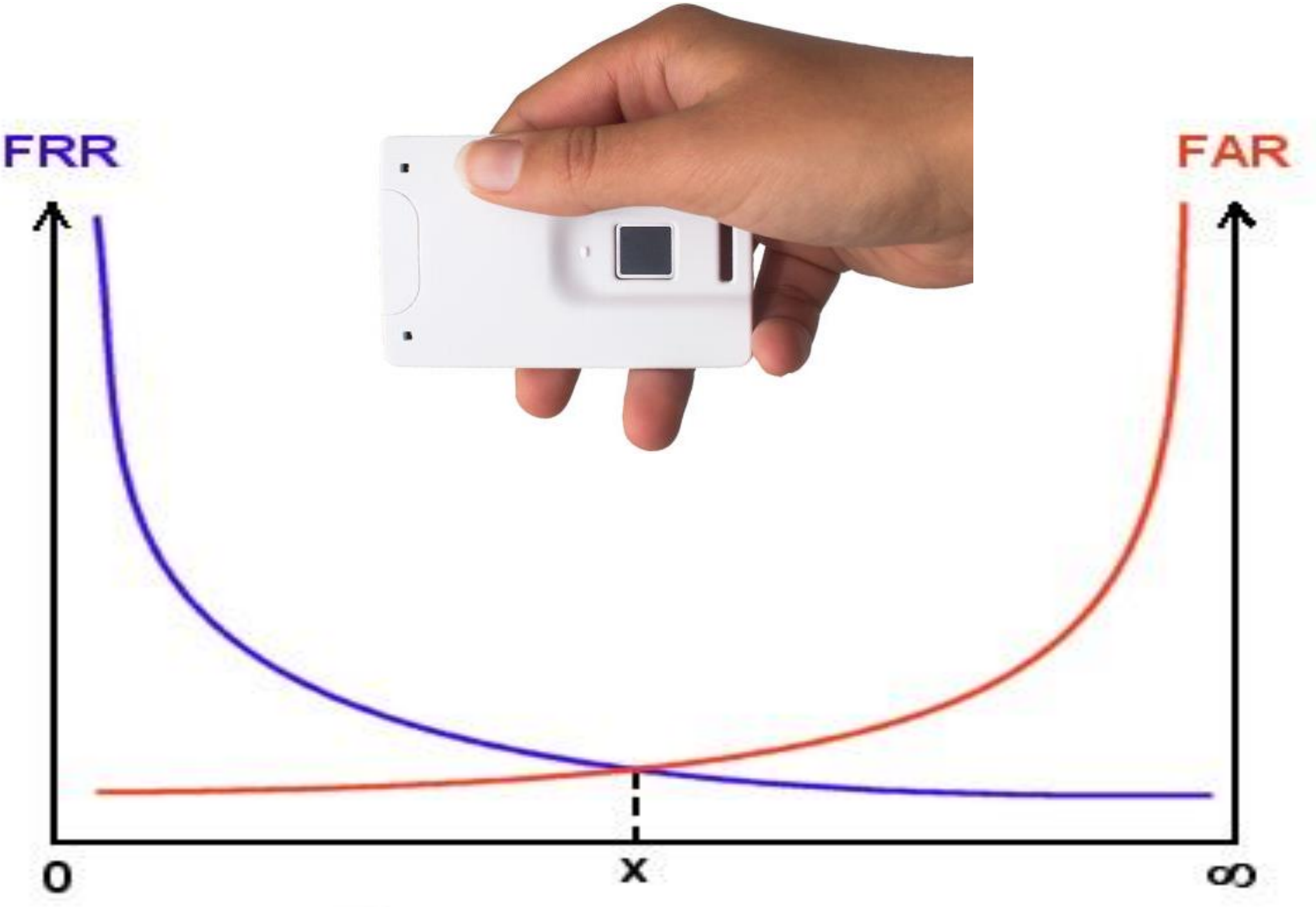
2005 – M.E. Zurko: User-Centered Security

# Password Practice*

- 30% of adult users maintain 10 or more unique passwords
  - 8% maintain 21 or more
- 81% of users do not use a unique password for each website
  - 33% use the same password for each website
  - 48% use a few different passwords
- 51% dislike the prospect of remembering another username or password
- 37% have to ask for assistance on their username or password for at least one website per month

*) source: passwordresearch.com

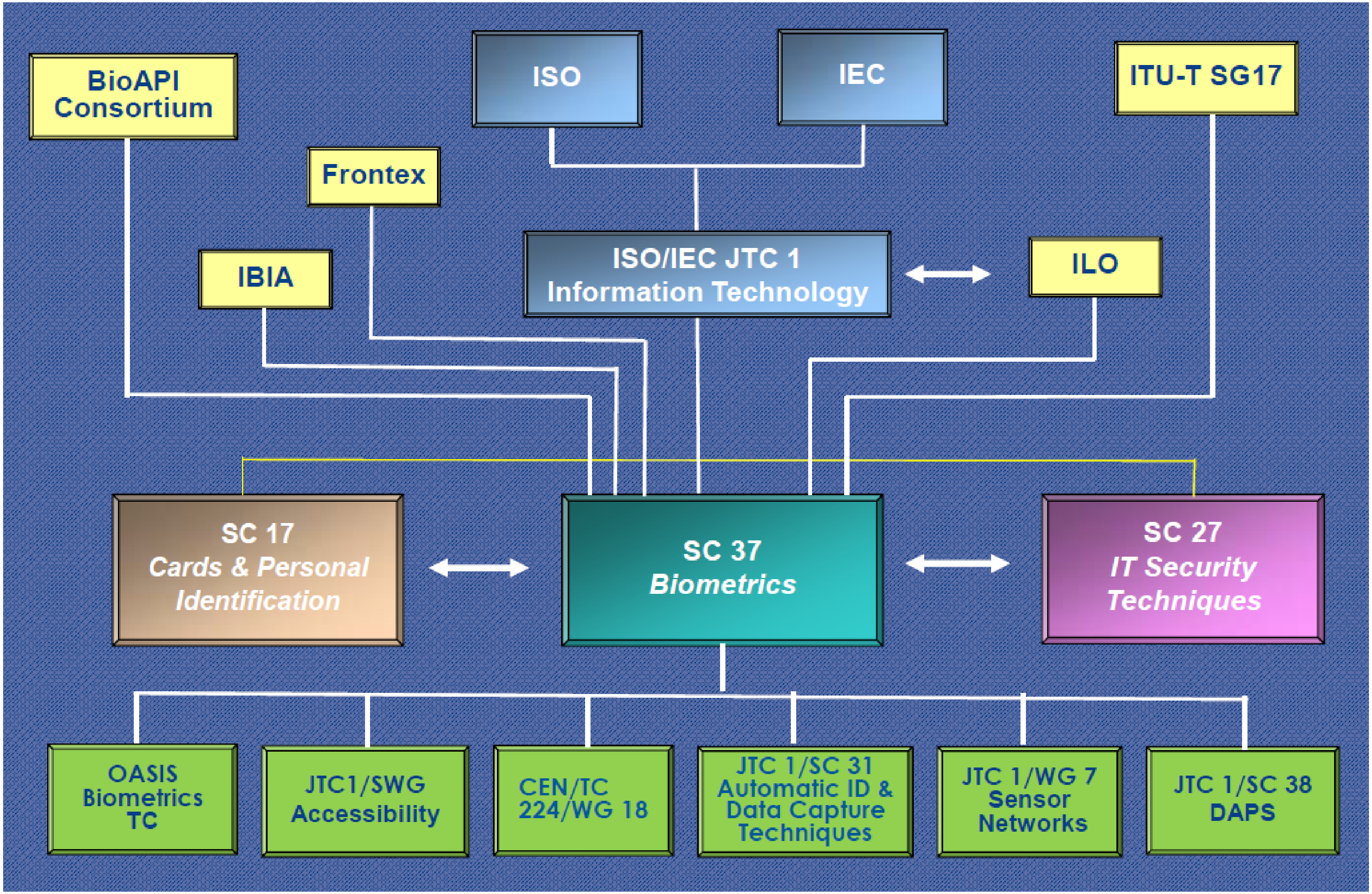
# Biometrics to replace Passwords?



# Mobility & Financial Services are Reshaping the Biometrics Marketplace

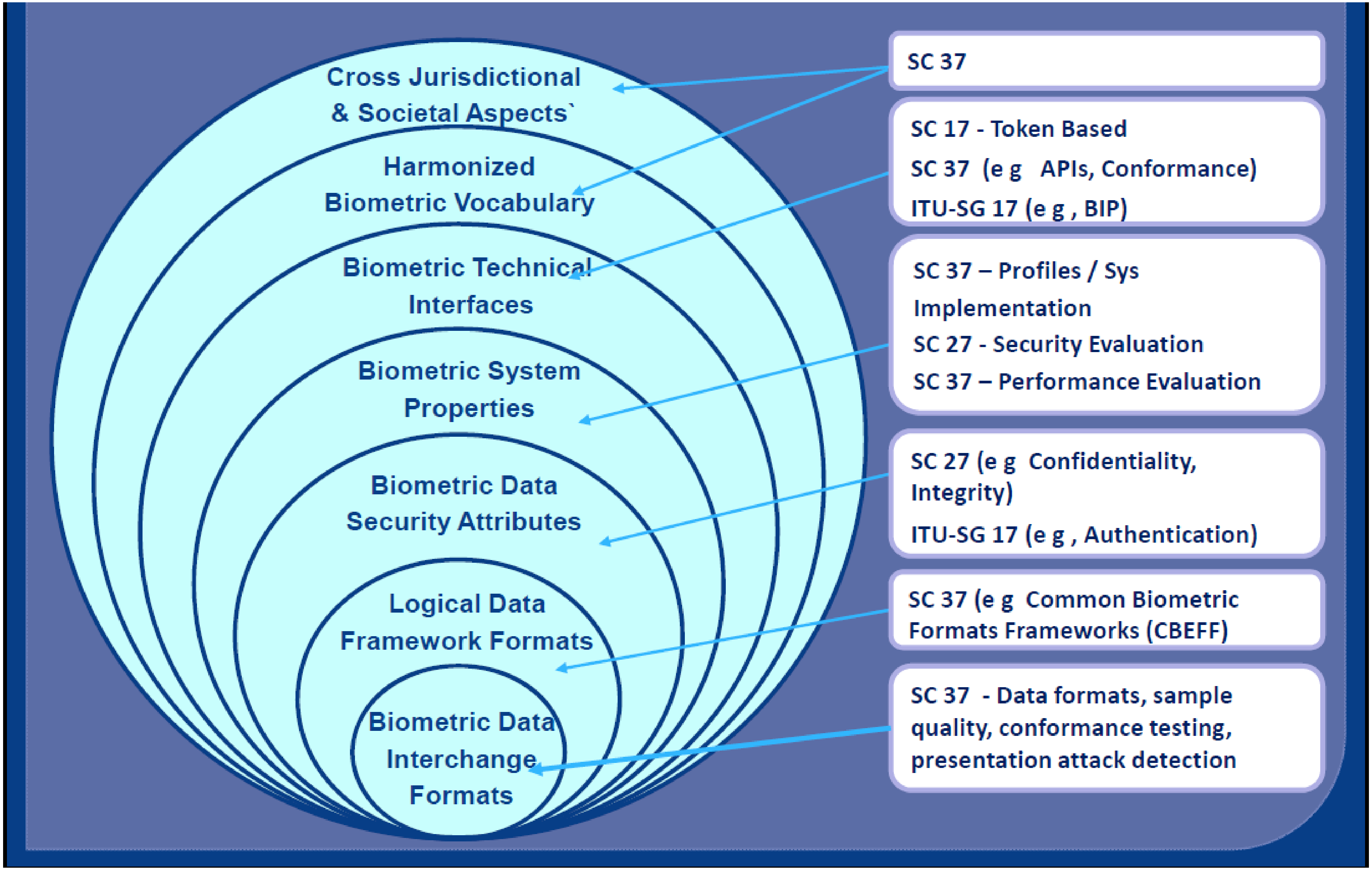
- Biometric authentication such as fingerprint, face and voice recognition integrated in mobile devices
  - Biometric authentication in smartphones have transitioned from “early adopter phase” to “early maturity phase”
- Some Japanese banks are adopting vein pattern recognition for customer authentication
- Barclays plans to adopt finger vein recognition
- MasterCard and Zwipe have announced a contactless payment card featuring an integrated fingerprint sensor without the need for a battery

# Biometrics Standardization


BioAPI Consortium
ISO
IEC
ITU-T SG17
Frontex
IBIA
ISO/IEC JTC 1 Information Technology
ILO
SC 17 Cards & Personal Identification
SC 37 Biometrics
SC 27 IT Security Techniques
OASIS Biometrics TC
JTC1/SWG Accessibility
CEN/TC 224/WG 18
JTC 1/SC 31 Automatic ID & Data Capture Techniques
JTC 1/WG 7 Sensor Networks
JTC 1/SC 38 DAPS

*source: Fernando Podio, SC 37 Chairman*

# Biometrics Standardization
*within ISO/IEC JTC 1*



Cross Jurisdictional & Societal Aspects`

Harmonized Biometric Vocabulary

Biometric Technical Interfaces

Biometric System Properties

Biometric Data Security Attributes

Logical Data Framework Formats

Biometric Data Interchange Formats

SC 37

SC 17 - Token Based
SC 37 (e g APIs, Conformance)
ITU-SG 17 (e g , BIP)

SC 37 – Profiles / Sys Implementation
SC 27 - Security Evaluation
SC 37 – Performance Evaluation

SC 27 (e g Confidentiality, Integrity)
ITU-SG 17 (e g , Authentication)

SC 37 (e g Common Biometric Formats Frameworks (CBEFF)

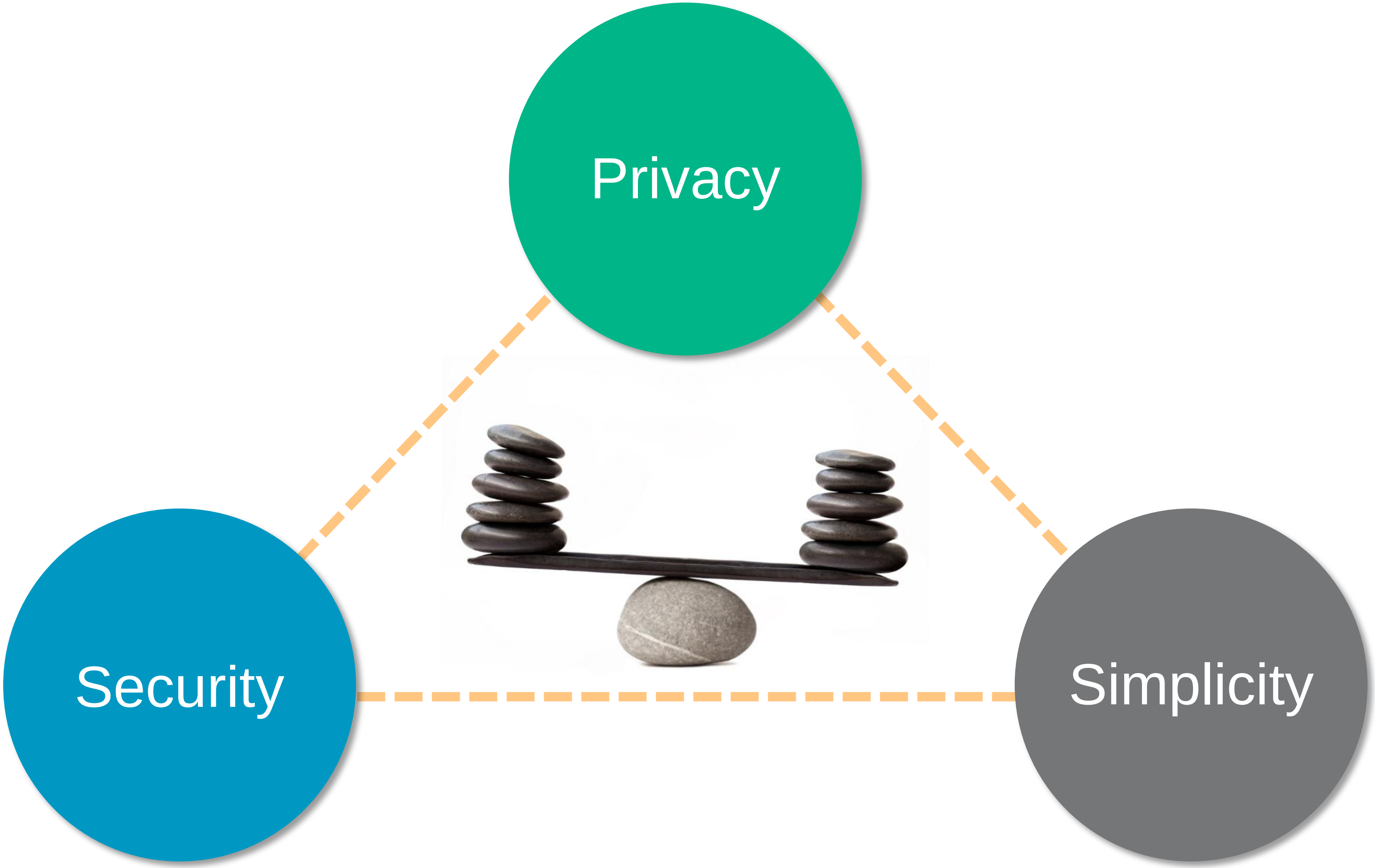
SC 37 - Data formats, sample quality, conformance testing, presentation attack detection

*source: Fernando Podio, SC 37 Chairman*

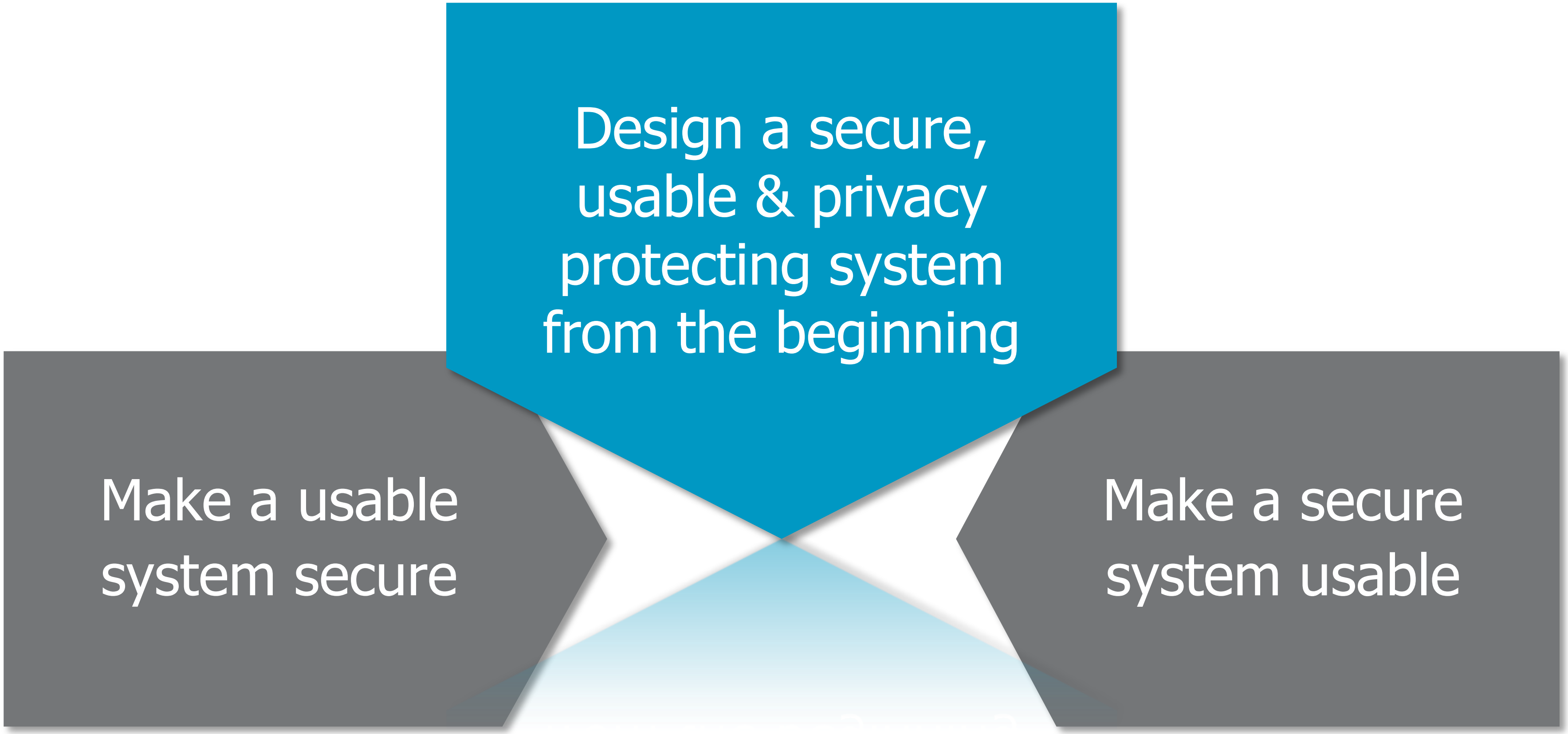
# Biometrics Challenges include

- Evolving sensor technology (sensitivity, ergonomics, size)
- Confidence in the performance (faster and more robust matches)
  - Multimodal biometrics
  - Robust liveness detection
- Cancelable biometrics

# The Challenge – Revisited



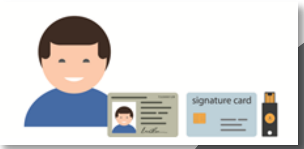
# Approaches



Design a secure, usable & privacy protecting system from the beginning

Make a usable system secure

Make a secure system usable



III

# Digital Identities

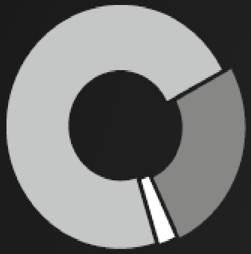
## Standards, Solutions & Documents

# ISO in figures (2014)

## MEMBERS

**NATIONAL STANDARDS BODIES**

**165**



**119**
MEMBER BODIES

**42**
CORRESPONDENT MEMBERS

**4**
SUBSCRIBER MEMBERS

## ISO/TC

**TECHNICAL BODIES**

**3 511** comprising

| TECHNICAL COMMITTEES | WORKING GROUPS |
|---|---|
| 238 | 2 592 |
| **SUBCOMMITTEES** | **AD HOC STUDY GROUPS** |
| 521 | 160 |

## MEETINGS

**TECHNICAL MEETINGS**
in progress – on average, each working day of the year somewhere in the world

**19**

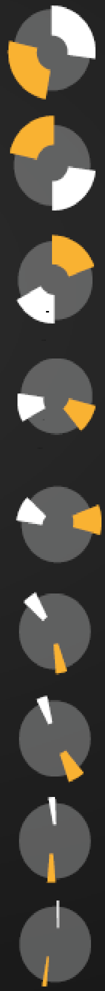
| TECHNICAL MEETINGS IN 2014 | NUMBER OF COUNTRIES HOSTING TECHNICAL MEETINGS |
|---|---|
| 1995 | 46 |

## DEVELOPMENT OF INTERNATIONAL STANDARDS

**PORTFOLIO OF ISO STANDARDS**
by sector at the end of 2014

**20 493**

% of International Standards
% of DIS and FDIS



27.4 % 26 %
Engineering technologies

22.7 % 21.5 %
Materials technologies

17.1 % 19 %
Electronics, information technology and telecommunications

10.6 % 9.7 %
Transport and distribution of goods

9.3 % 10 %
Generalities, infrastructures, sciences and services

5.6 % 3.8 %
Agriculture and food technology

4 % 6.1 %
Health, safety and environment

2.5 % 2.7 %
Construction

0.8 % 1.3 %
Special technologies

**INTERNATIONAL STANDARDS AND STANDARDS-TYPE DOCUMENTS**
published in 2014

**1468**

**NEW PROJECTS REGISTERED**

**1852**

**WORK ITEMS**
listed on the work programmes of technical committees

**4 696**

WORK ITEMS AT PREPARATORY STAGE
**1429**

COMMITTEE DRAFTS
**1067**

DRAFT INTERNATIONAL STANDARDS (DIS) AND FINAL DRAFT INTERNATIONAL STANDARDS (FDIS)
**2 200**

Source: www.iso.org

# ISO/IEC JTC 1 – Information Technology

## *Security Related Sub-committees*

| | |
|---|---|
| SC 6 | Telecommunications and information exchange between systems |
| SC 7 | Software and systems engineering |
| SC 17 | Cards and personal identification |
| SC 25 | Interconnection of information technology equipment |
| SC 27 | IT Security techniques |
| SC 29 | Coding of audio, picture, multimedia and hypermedia information |
| SC 31 | Automatic identification and data capture techniques |
| SC 32 | Data management and interchange |
| SC 36 | Information technology for learning, education and training |
| SC 37 | Biometrics |
| SC 38 | Distributed application platforms and services (DAPS) |
| SC 40 | IT Service Management and IT Governance |

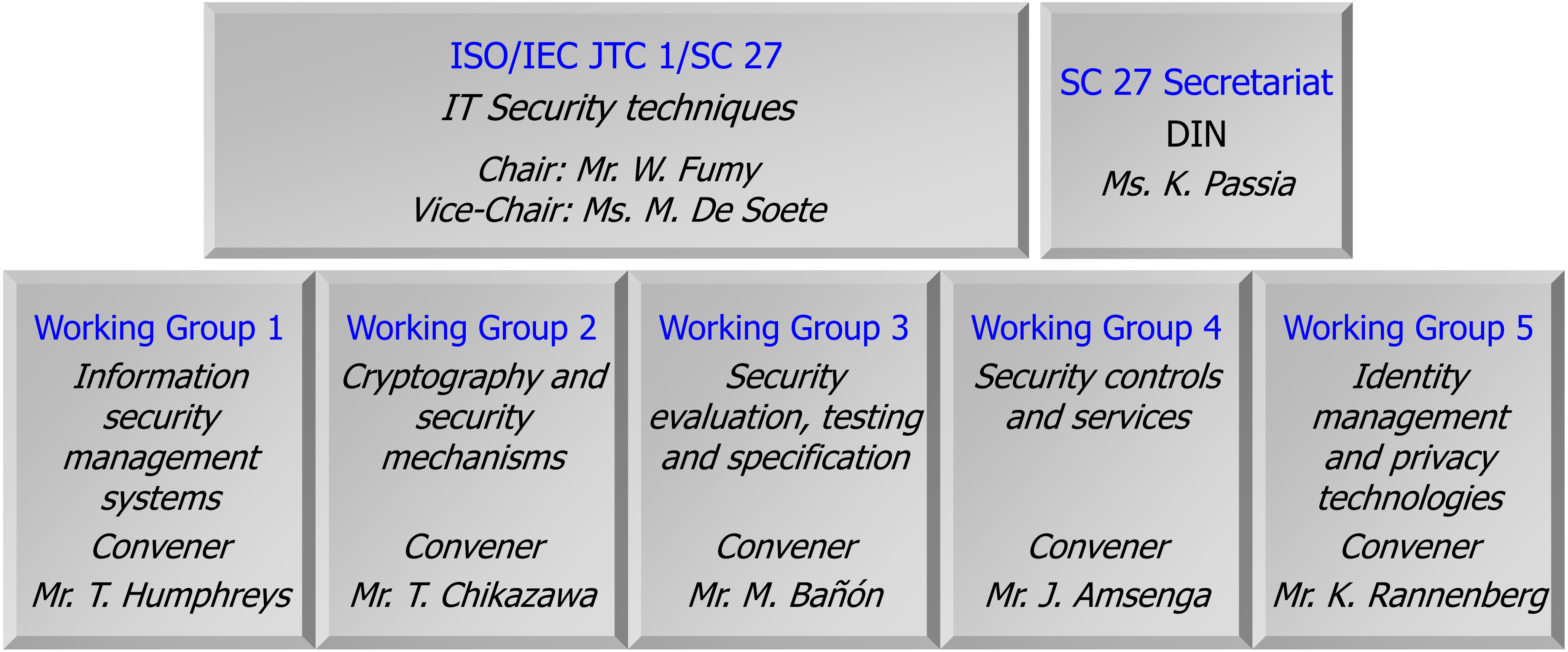
# Machine Readable Travel Documents
## *Major Contributions from JTC 1 Subcommittees*

**ICAO TAG-TRIP***

- **ISO/IEC JTC 1/SC 37**
  **Biometrics**
  - ISO/IEC 19785
  - ISO/IEC 19794
- **ISO/IEC JTC 1/SC 17**
  **Cards and Personal Identification**
  - ISO/IEC 7816
  - ISO/IEC 10373
  - ISO/IEC 14443
- **ISO/IEC JTC 1/SC 27**
  **IT Security Techniques**
  - ISO/IEC 9796-2
  - ISO/IEC 9797
  - ISO/IEC 11770-2

*) Technical Advisory Group on Traveler Identification Programs

# SC 27 – IT Security Techniques
## *Organization*



ISO/IEC JTC 1/SC 27

*IT Security techniques*

*Chair: Mr. W. Fumy*
*Vice-Chair: Ms. M. De Soete*

SC 27 Secretariat

DIN

*Ms. K. Passia*

Working Group 1

*Information security management systems*

*Convener*

*Mr. T. Humphreys*

Working Group 2

*Cryptography and security mechanisms*

*Convener*

*Mr. T. Chikazawa*

Working Group 3

*Security evaluation, testing and specification*

*Convener*

*Mr. M. Bañón*

Working Group 4

*Security controls and services*

*Convener*

*Mr. J. Amsenga*

Working Group 5

*Identity management and privacy technologies*

*Convener*

*Mr. K. Rannenberg*

**http://www.jtc1sc27.din.de/en**

# SC 27 Members

## P-members (voting)

Algeria, Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Côte-d'Ivoire, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, India, Italy, Ireland, Israel, Jamaica, Japan, Kazakhstan, Kenya, Rep. of Korea, Luxembourg, Rep. of Macedonia, Malaysia, Mauritius, Mexico, Morocco, The Netherlands, New Zealand, Norway, Peru, Poland, Romania, Russian Federation, Singapore, Slovakia, Slovenia, South Africa, Spain, Sri Lanka, Sweden, Switzerland, Thailand, Ukraine, United Arab Emirates, United Kingdom, United States of America, Uruguay (Total: 52)

## O-members (observing)

Belarus, Bosnia and Herzegovina, Costa Rica, El Salvador , Ghana, Hong Kong, Hungary, Iceland, Indonesia, Islamic Rep. of Iran, Lithuania, Portugal, Saudi Arabia, Serbia, State of Palestine, Swaziland, Turkey (Total: 18)

# ID Management @ ISO/IEC

ISO/IEC 24760: A framework for identity management

- Part 1: Terminology and concepts
- Part 2: Reference architecture and requirements
- Part 3: Practice

ISO/IEC 24760 provides foundations for other identity management related international standards including:

- ISO/IEC 29003: Identity proofing
- ISO/IEC 29100: Privacy framework
- ISO/IEC 29101: Privacy reference architecture
- ISO/IEC 29115: Entity authentication assurance framework
- ISO/IEC 29146: A framework for access management

*source: ISO/IEC JTC 1/SC 27/WG 5*

# The ISO/IEC ID Management Framework

According to ISO/IEC 24760-1, Identity Management covers the lifecycle of identity information from initial enrolment to archiving or deletion, and  includes the governance, policies, processes, data, technology, and standards, which may include:

- Application(s) implementing an identity register;
- Authenticating* the identity;
- Establishing provenance of identity information;
- Establishing the link between identity information and an entity;
- Maintaining the identity information;
- Ensuring the integrity of the identity information;
- Providing credentials and services to facilitate authentication of an entity as a known identity;
- Mitigating the risk of identity information theft or misuse.

**) ISO/IEC 24760 defines authentication as „the formalized process of verification that, if successful, results in an authenticated identity for an entity."*

# The ISO/IEC ID Management Framework – *Privacy Requirements*

An identity management system conforming to ISO/IEC 24760 should provide privacy-related capabilities to:

- Implement mechanisms, including policies, processes, and technology, for minimal disclosure;
- Authenticate entities that use identity information;
- Minimize the ability to link identities;
- Record and audit the use of identity information;
- Protect against inadvertently generating risks to privacy, e,g. those posed by inadequately protecting identity information in logs and audit trails;
- Implement policies for selective disclosure;
- Support the use of pseudonyms;
- Implement policies to engage a human entity for explicit direction or consent, for activities related to their sensitive identity information.

# ISO/IEC 29115:2013
Entity Authentication Assurance

ISO/IEC 29115 provides a framework for managing entity authentication assurance in a given context. In particular, it specifies

- four levels of entity authentication assurance (LoA 1 to 4)
- criteria and guidelines for achieving each of the four levels

| Level | Description | Objective | Control |
|---|---|---|---|
| LoA 1 – low | Little or no confidence in asserted ID | ID is unique within a context | Self-asserted |
| LoA 2 – medium | Some confidence in asserted ID | ID is unique within context and entity exists objectively | Proof of ID through use of ID information from authoritative source |
| LoA 3 – high | High confidence in asserted ID | ID is unique within context, entity exists objectively, and ID is verified | Proof of ID through use of ID information from authoritative source + verification |
| LoA 4 – very high | Very high confidence in asserted ID | ID is unique within context, entity exists objectively, and ID is verified | Proof of ID through use of ID information from multiple authoritative sources + verification + entity witnessed in-person* |

**) applies to human entities only*

# The eIDAS Token Specification

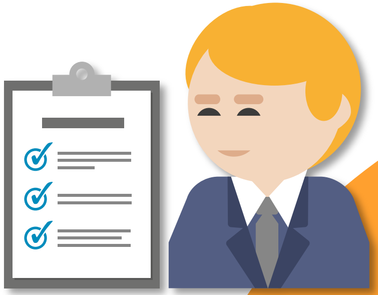
## TR-03110 Advanced Security Mechanisms for MRTDs and eIDAS token

- Part 2: Protocols for electronic identification, authentication and trust services (eIDAS)*

- Contribution from the German and French IT security agencies BSI and ANSSI, supported by European industry partners
- Provides a modular Secure element API to protect the data stored on tokens for electronic identification, 2-factor authentication and signatures (eIDAS token)

- Protocols specified
  - PACE
  - Extended Access Control (EAC) based on Terminal Authentication (Version 2) and Chip Authentication (Version 2 & 3)
  - Restricted Identification (RI)
  - Pseudonymous Signatures (PS)
  - Enhanced Role Authentication (ERA)

*) available from http://www.bsi.bund.de/literat/tr/index.htm



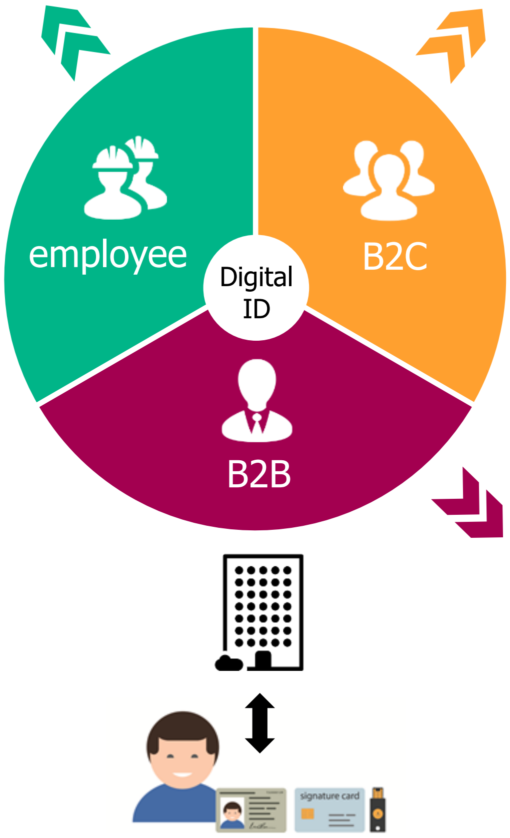
# Compliance management

7 of the 10 most frequent compliance violations are directly related to identity management

ISACA (Information Systems Audit & Control Association)

# Corporate IDs & their applications

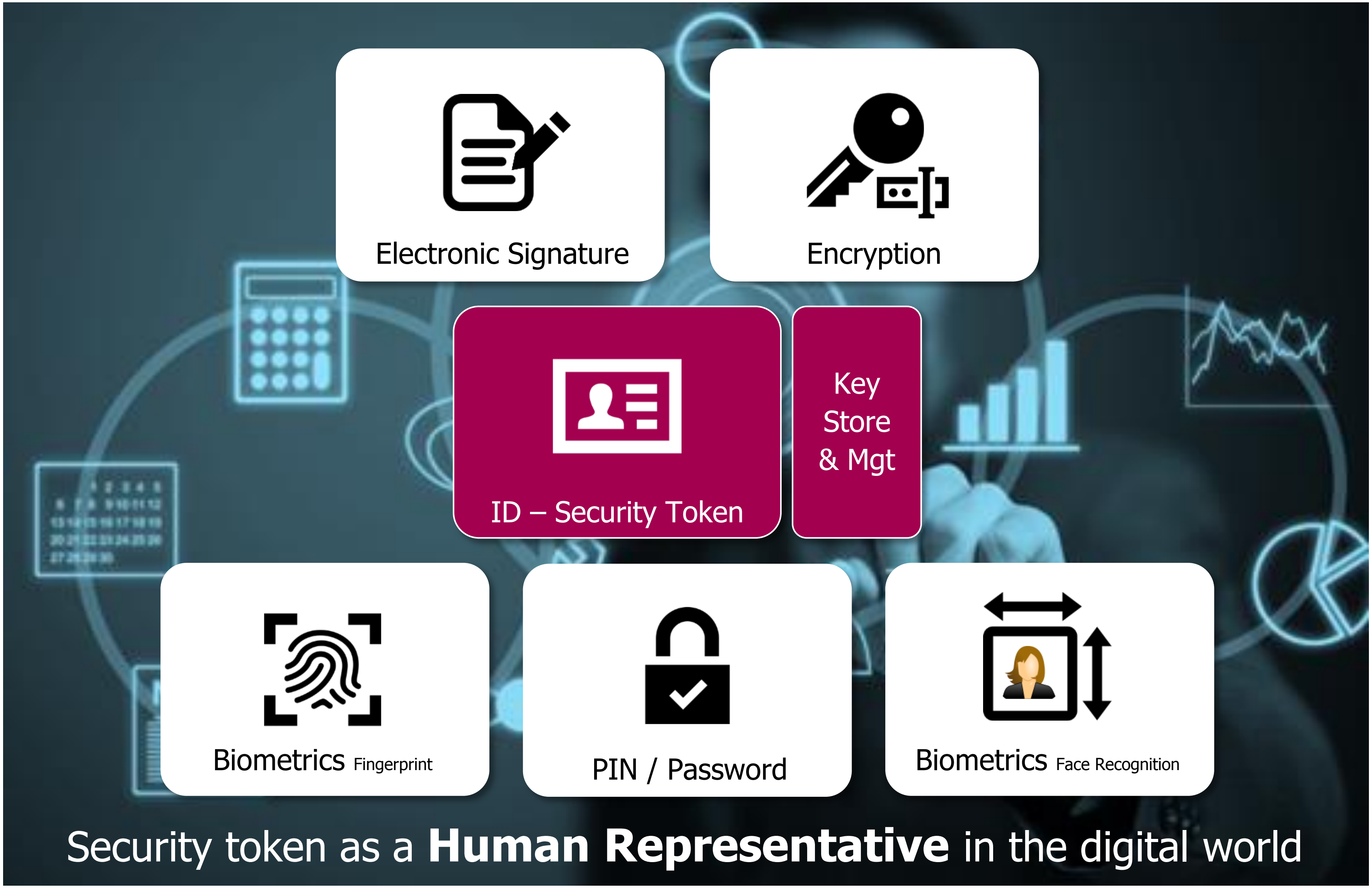
- secure access
- Single-Sign-On / data encryption
- machine login
- process approval
- Virtual Private Network



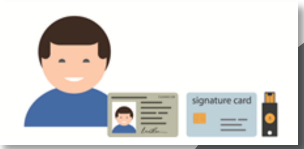
- secure transactions
- secure & simple registration
- electronic signature
- document verification

- online visitor registration
- secure access to cross company applications (cloud)

# The digital world requires new mechanisms



Security token as a **Human Representative** in the digital world

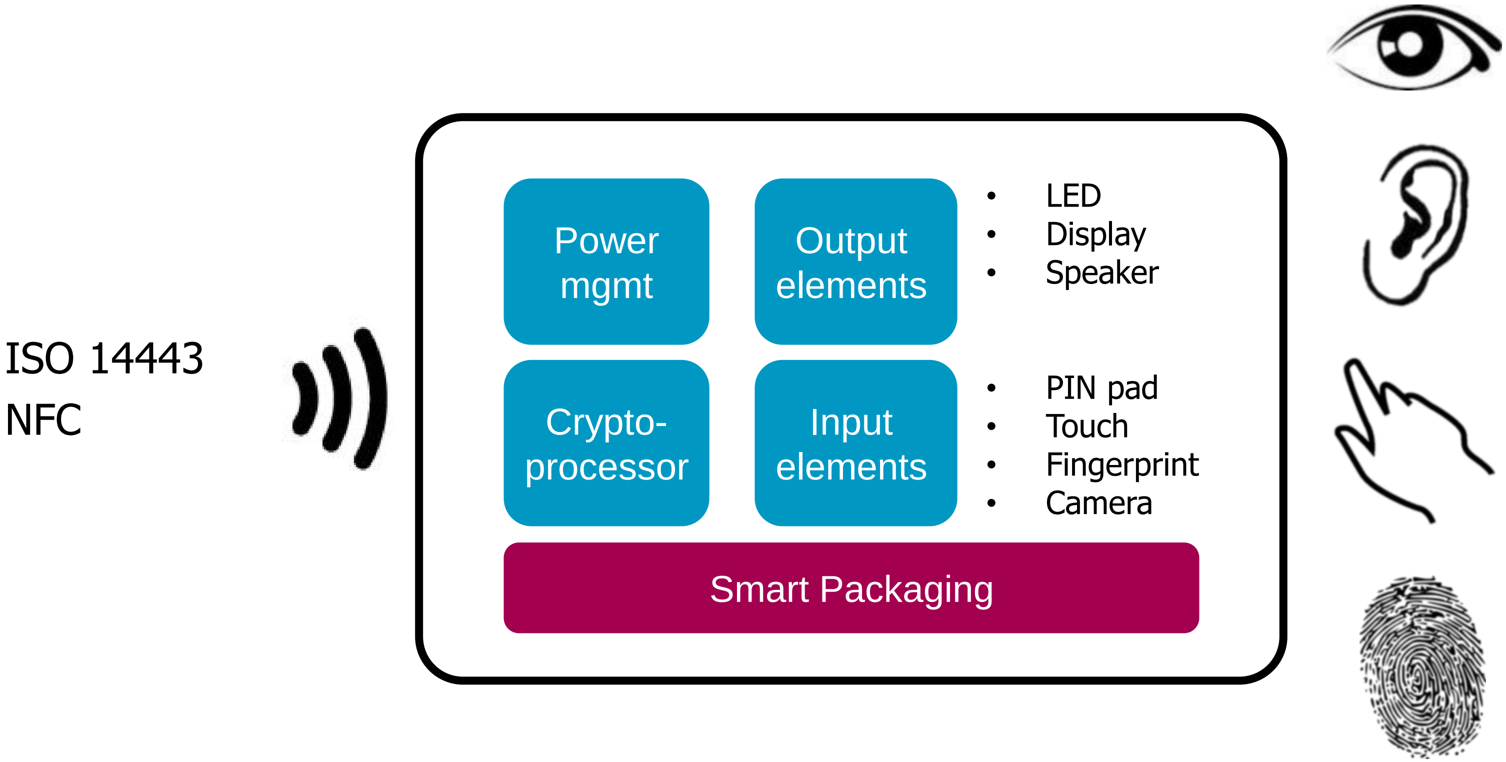


III.2

# System on Document

# System on Document –
# *Your Digital Representative*

- ID document adopts new functions with multifunctional components
- Interactive and easy to use with a maximum degree of privacy protection
- Highly integrated system solution
- Major challenges for hardware and software



ISO 14443
NFC

Power mgmt

Output elements

- LED
- Display
- Speaker

Crypto-processor

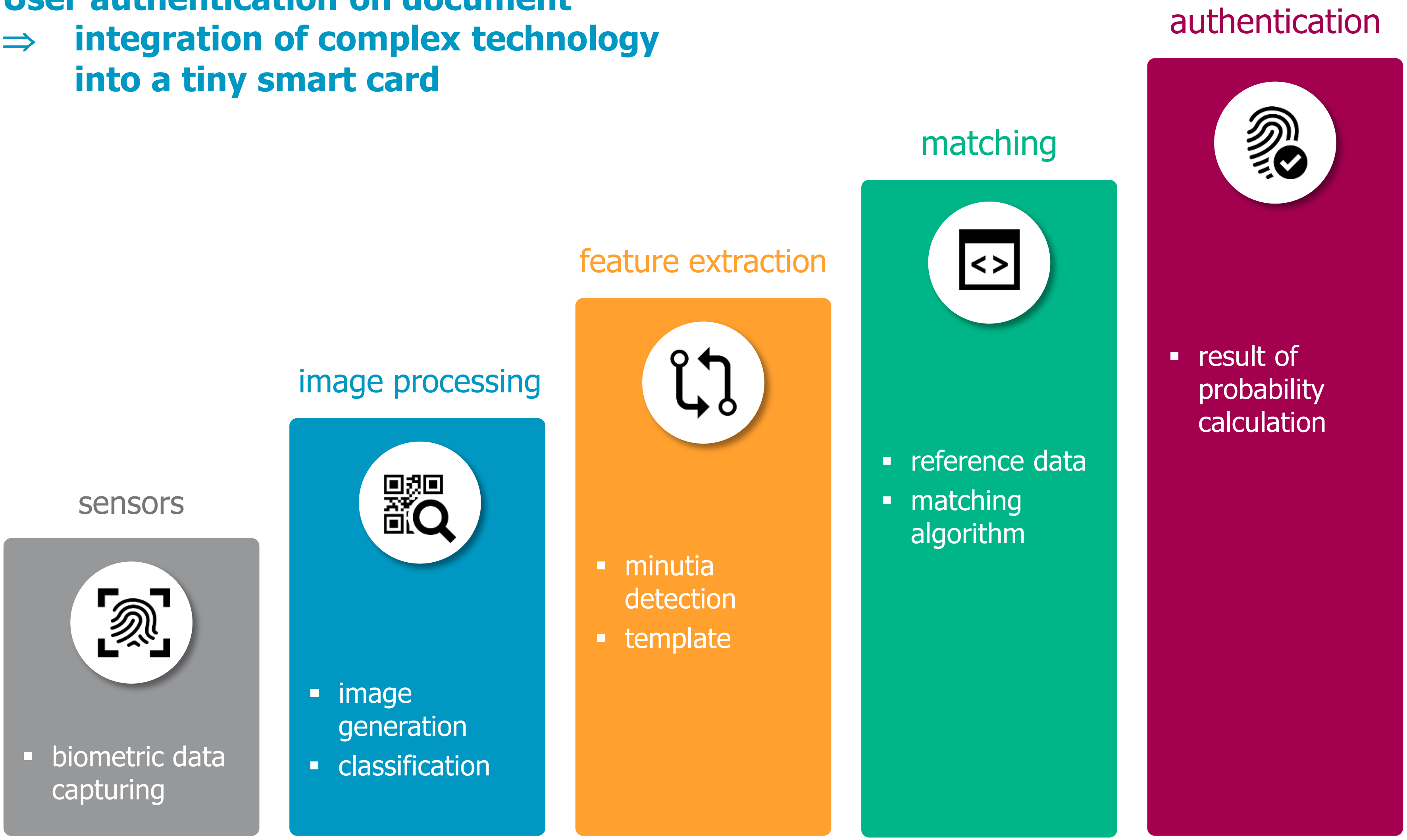
Input elements

- PIN pad
- Touch
- Fingerprint
- Camera

Smart Packaging

# System on Document – *Challenges*

## User authentication on document
## ⇒ integration of complex technology into a tiny smart card



sensors

- biometric data capturing

image processing

- image generation
- classification

feature extraction

- minutia detection
- template

matching

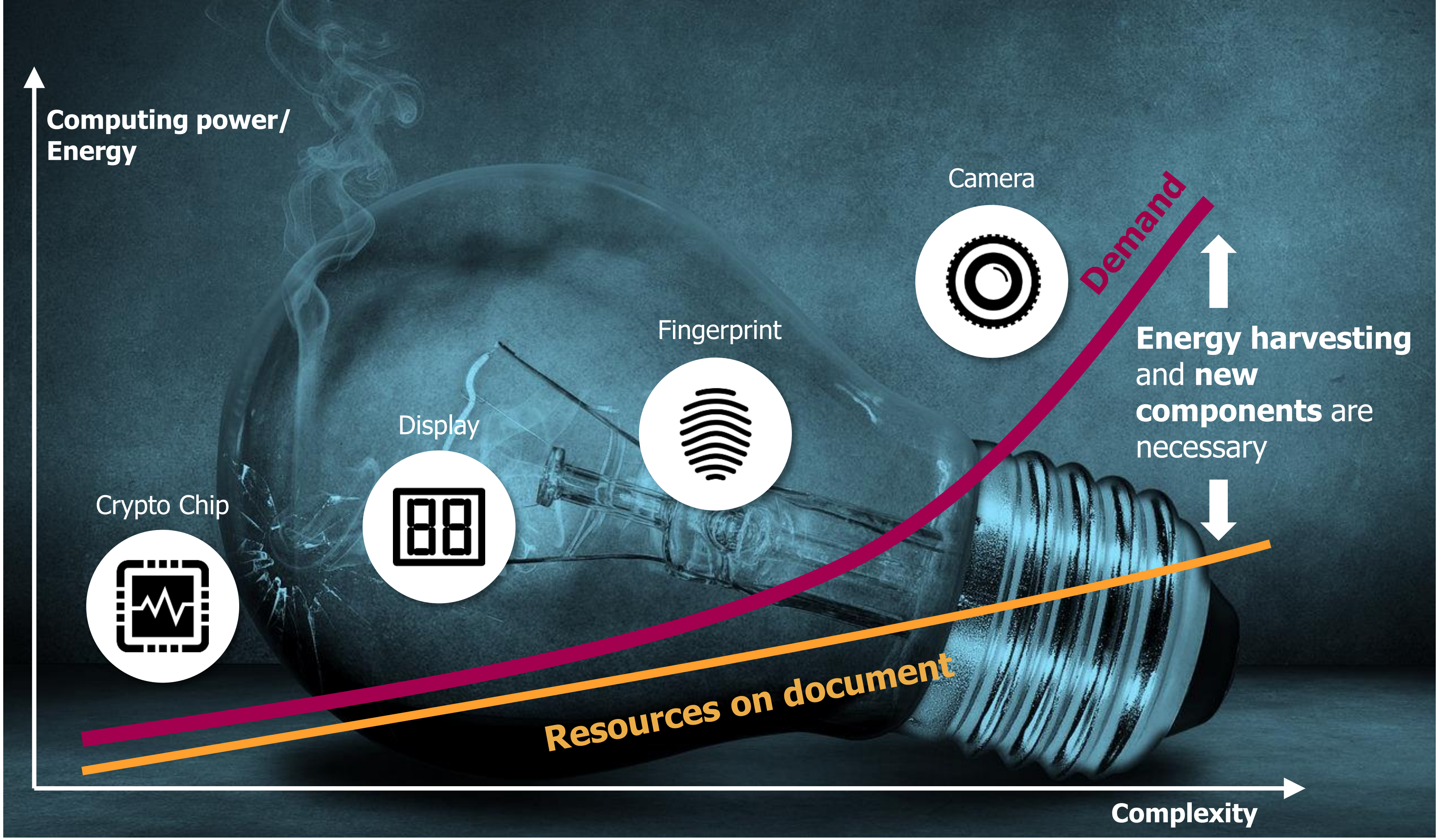
- reference data
- matching algorithm

authentication

- result of probability calculation

# System on Document – *Challenges (cont.)*

Additional electronic components require more computing power and energy



**Energy harvesting** and **new components** are necessary

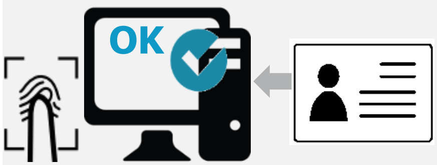
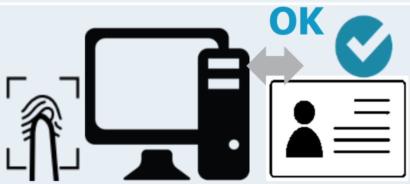
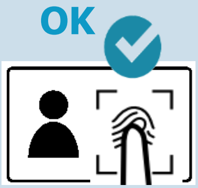
# System on Document – *Hardware and software challenges*

## Reliable and secure operation with limited resources

- New concepts for energy harvesting using power from reader terminals
- High performance and low power components required
- Lightweight software algorithms and user friendly interfaces

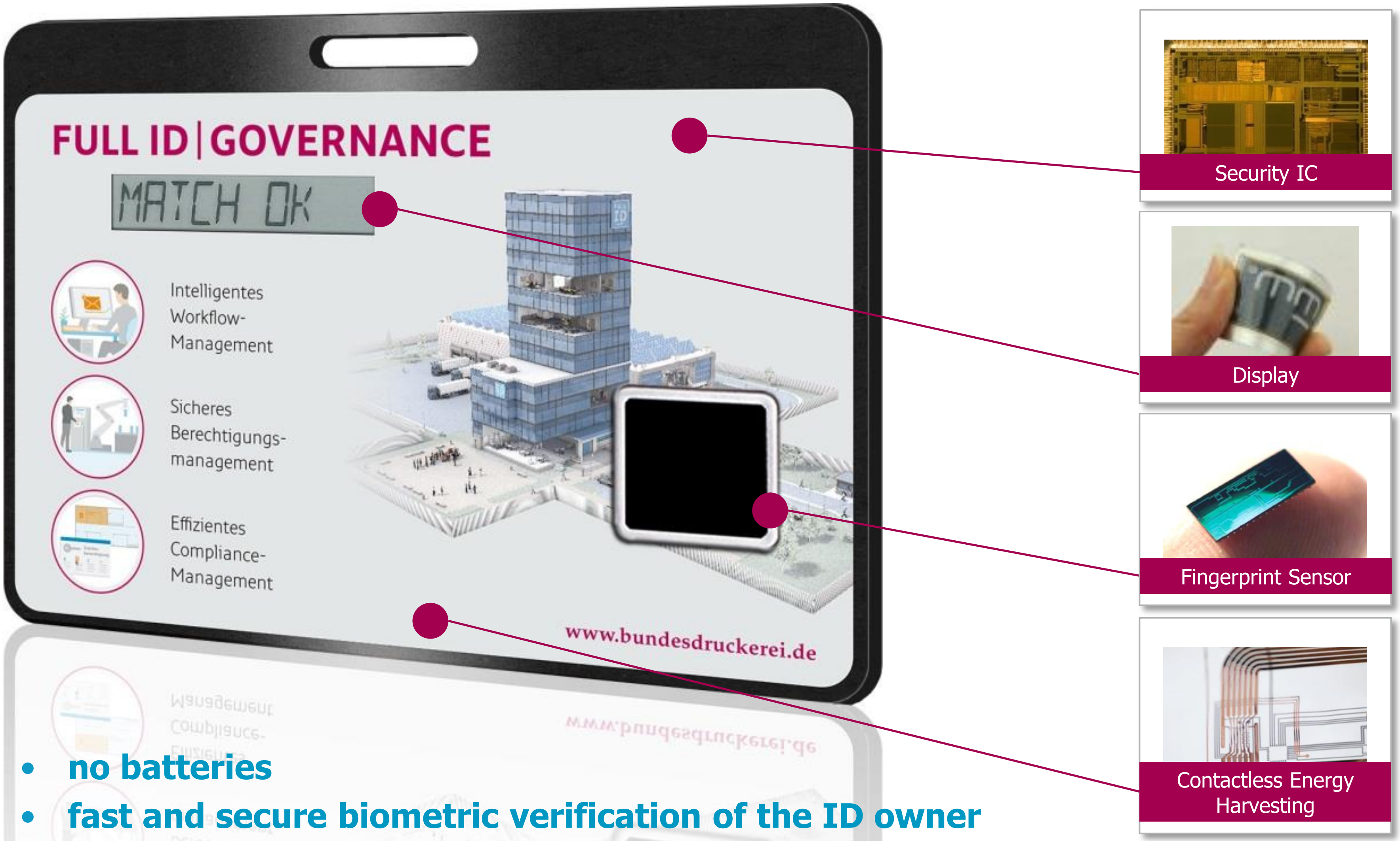
| | PC | Smartphone | Contactless Card |
|---|---|---|---|
| Energy | 1 kW | 10 W | 25 mW |
| Computing power | | | |
| Frequency | 4 GHz | 2 GHz | 150 MHz |
| CPU cores | 16 | 4 | 1 |
| Bit | 64 | 32 | 16 |
| Memory (RAM) | 4 GB | 2 GB | 8 kB |
| Time for 1:1 Match | 10µs | 10ms | 100ms |

# System on Document –
## *Evolution of fingerprint authentication*

| | **Template on Document** | | **Match on Document** | | **System on Document** | |
|---|---|---|---|---|---|---|
| | external | internal | external | internal | external | internal |
| **Sensor and data capturing** | ✓ | | ✓ | | | ✓ |
| **Matching algorithm** | ✓ | | | ✓ | | ✓ |
| **Storage of reference data** | | ✓ | | ✓ | | ✓ |
| **Key Properties** | - Strong requirements for interoperability<br>- e.g. ePassport | | - Reference data never leave the document<br>- Better protection of privacy | | - Reference data and captured data never leave the document<br>- Maximum protection of privacy | |
| **Schematic** |  | |  | |  | |

**increasing complexity of the document & increasing security**

# ID Document with On-card Fingerprint Sensor and Display


FULL ID | GOVERNANCE
MATCH OK
Intelligentes Workflow-Management
Sicheres Berechtigungs-management
Effizientes Compliance-Management
www.bundesdruckerei.de
Security IC
Display
Fingerprint Sensor
Contactless Energy Harvesting

- **no batteries**
- **fast and secure biometric verification of the ID owner**

# ID Document with On-card Fingerprint Sensor and Display

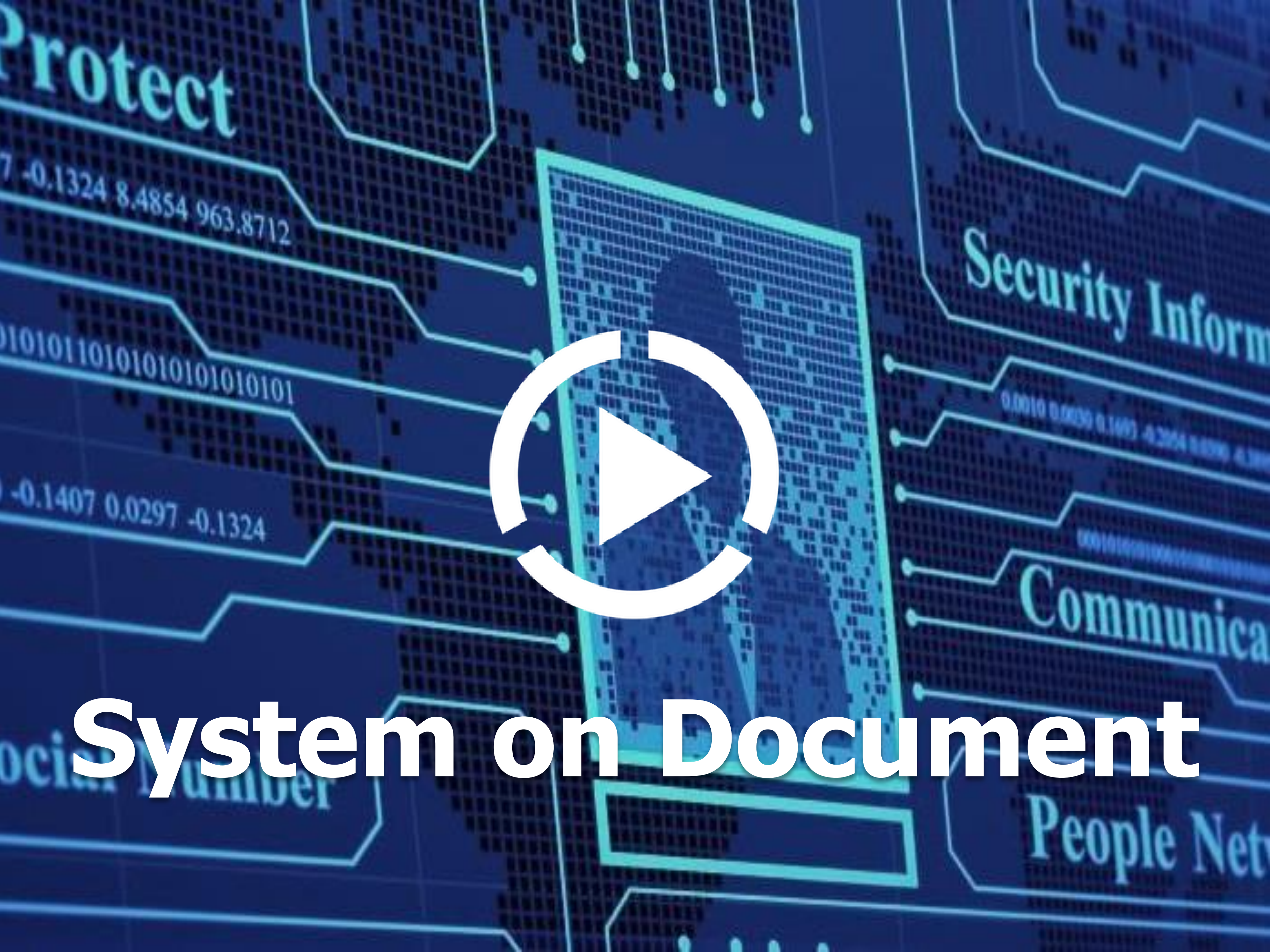
FULL ID | GOVERNANCE
MATCH OK
Intelligentes Workflow-Management
Sicheres Berechtigungs-management
Effizientes Compliance-Management
www.bundesdruckerei.de

| **Specifications** | |
|---|---|
| Dimensions | 53.98 mm x 85.6 mm x 2.5 mm, ID-T format |
| Power | Contactless / energy harvesting / no battery |
| Interface | ISO 14443 / 13.56 MHz |
| Security IC | SMX |
| Card body | High quality monocoque architecture |
| Fingerprint sensor | Capacitive area sensor |
| Display | ePaper display / LED |
| Design | Full colour design / personalization |

Informational self-determination ensured at all times

## High degree of data protection

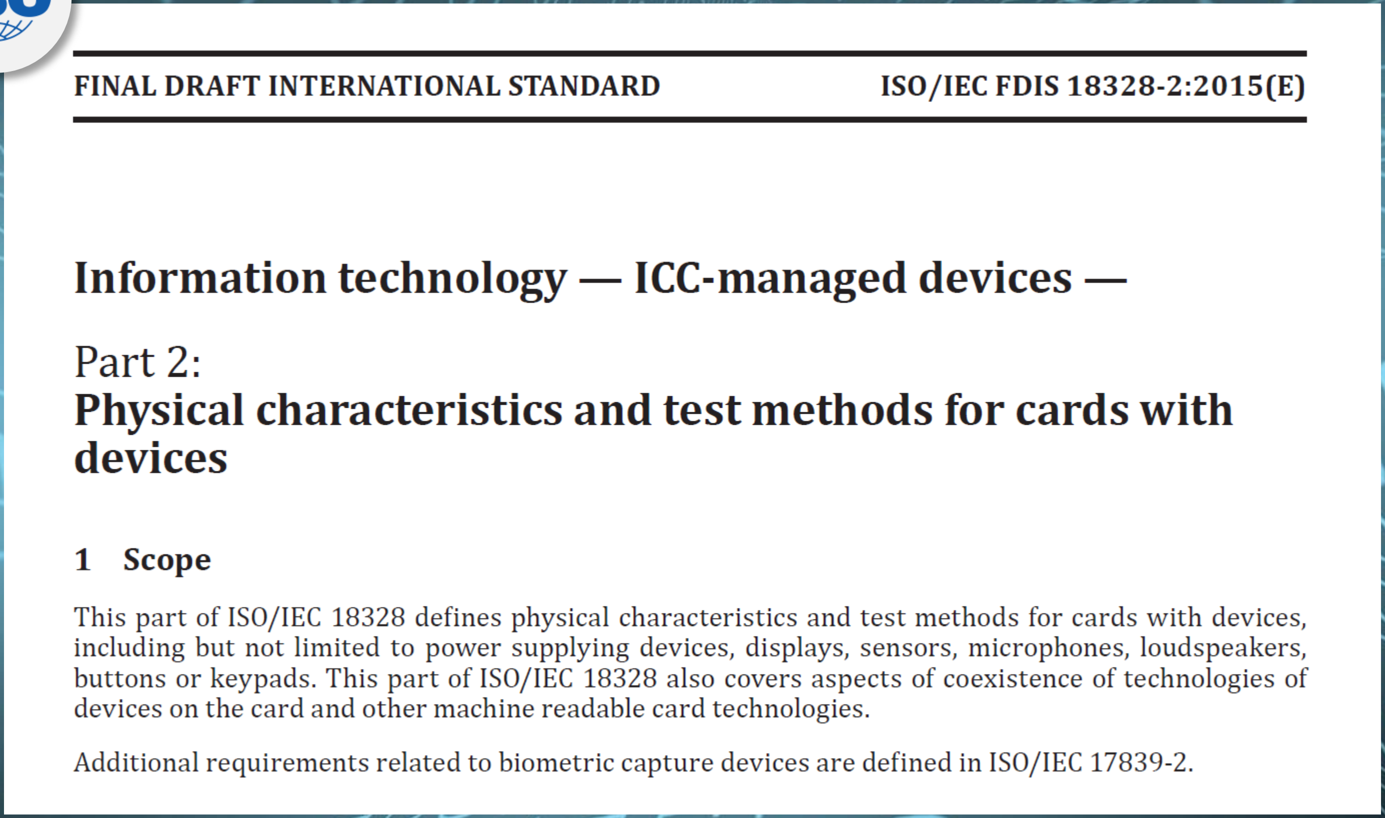
- The sensitive biometric data never leaves the ID document. The document captures, safely stores and verifies on card.
- “Verification on document" offers a high degree of data protection and ensures the user's informational self-determination at all times
- No personal biometric data is sent to a background system



# System on Document

# ISO/IEC 18328
*New Multipart Standard for Multifunctional Smartcards*

## New International Standard for multifunctional smartcards to be published soon, including ID-T format



**FINAL DRAFT INTERNATIONAL STANDARD** **ISO/IEC FDIS 18328-2:2015(E)**

### Information technology — ICC-managed devices —

Part 2:
**Physical characteristics and test methods for cards with devices**

### 1 Scope

This part of ISO/IEC 18328 defines physical characteristics and test methods for cards with devices, including but not limited to power supplying devices, displays, sensors, microphones, loudspeakers, buttons or keypads. This part of ISO/IEC 18328 also covers aspects of coexistence of technologies of devices on the card and other machine readable card technologies.

Additional requirements related to biometric capture devices are defined in ISO/IEC 17839-2.

# Topics addressed in ISO/IEC 18328-2

Definition of physical characteristics

Definition of test methods

Valid for devices on card

Coexistence with other existing technologies

- Cards with devices, including but not limited to power supplying devices, displays, sensors, microphones, loudspeakers, buttons or keypads
- Additional requirements related to biometric capture devices are also defined in ISO/IEC 17839-2
- Annex: ID-T size card
  - Same length and width as normal ID-1 size card, but thicker
  - 85.60 mm (3.370 in) wide by 53.98 mm (2.125 in) high by 2.50 mm (0.098 in) thick

# Intrinsic Object IDs

III.3

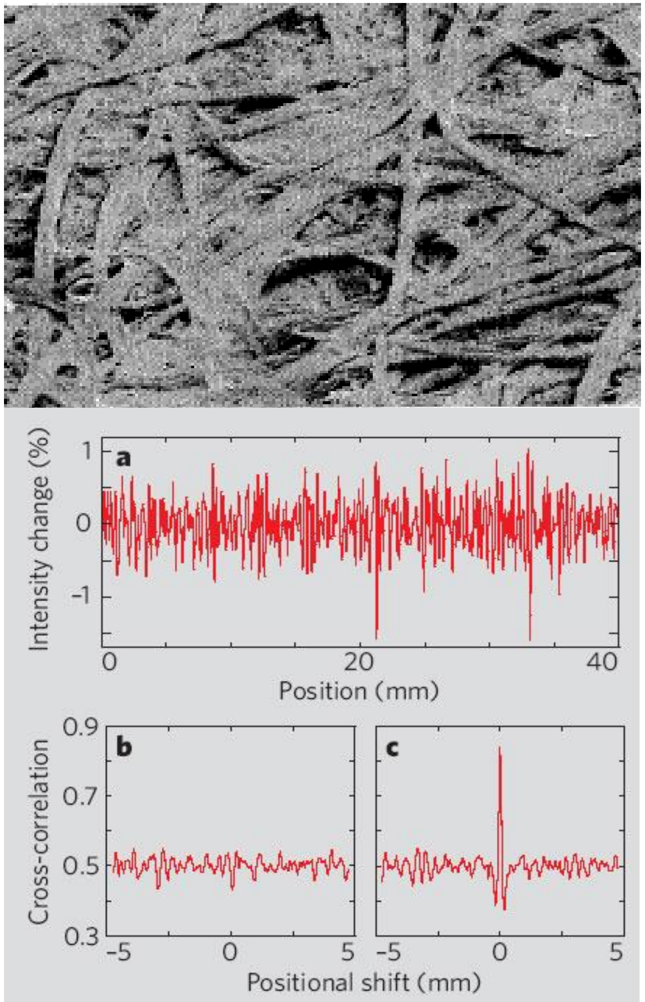
# ‚Fingerprint' of Documents – *Many objects carry intrinsic ID*

R. Cowburn et al, Nature vol 436-28: 2005

- "[…] almost all paper documents, plastic cards and product packaging contain a unique physical identity code formed from microscopic imperfections in the surface. This covert ‚fingerprint' is intrinsic and virtually impossible to modify controllably."
- Laser Speckle Effect

William Clarkson et al, IEEE Security & Privacy, 2009

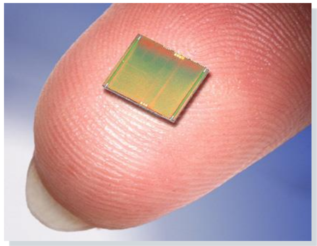
- "[…] measuring the three-dimensional surface of a page using only a commodity scanner […] we generate a concise fingerprint that uniquely identifies the document. Our technique is secure against counterfeiting and robust to harsh handling."

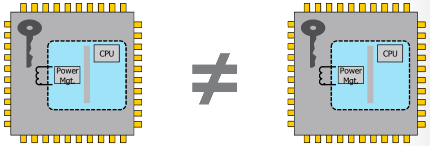


*Source: Nature vol 436-28, 2005*

# Intrinsic Object IDs & Physical Unclonable Functions

## Silicon based PUFs

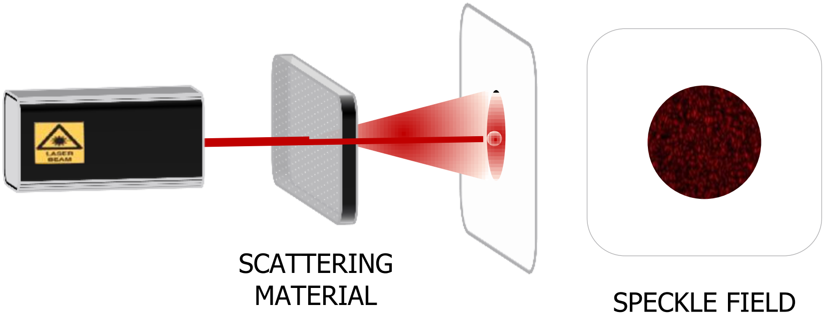




**Unavoidable and uncontrollable variations at a molecular scale - well below the tolerances of manufacturing process - make each silicon chip unique**

**Localized on the chip**

## Optical PUFs



**Randomness of material (intrinsic or explicitly introduced) makes each scattering object unique**

**Beyond the chip, material-based**

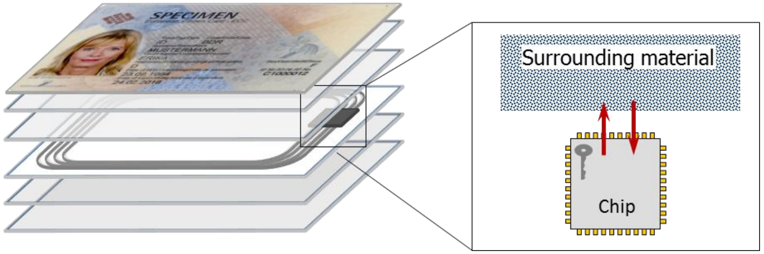
# Optical PUFs for Security Documents ?

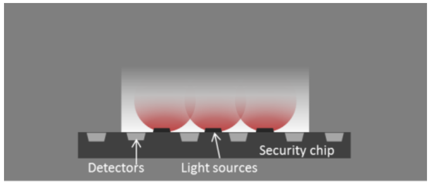
Although optical PUFs have been considered first among the various PUF architectures discusses today, the adoption of optical PUFs for security documents with embedded chips is still a research topic.

Challenges include

- to equip a security chip with sufficient measuring means,
- to design appropriate material structures and to integrate them into the document.

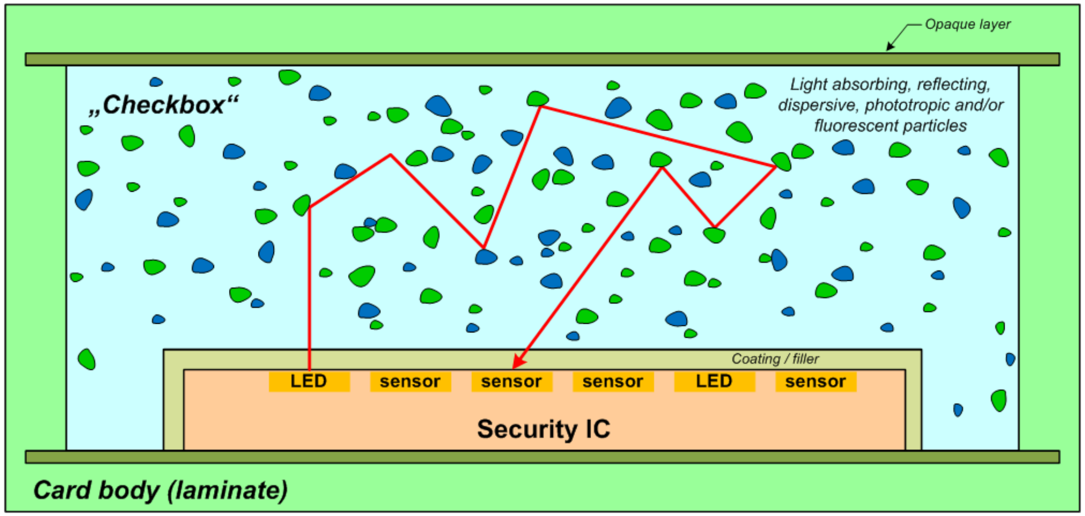
An integration into security documents imposes several restrictions on the light sources and sensors, as well as on the available light propagation distance.



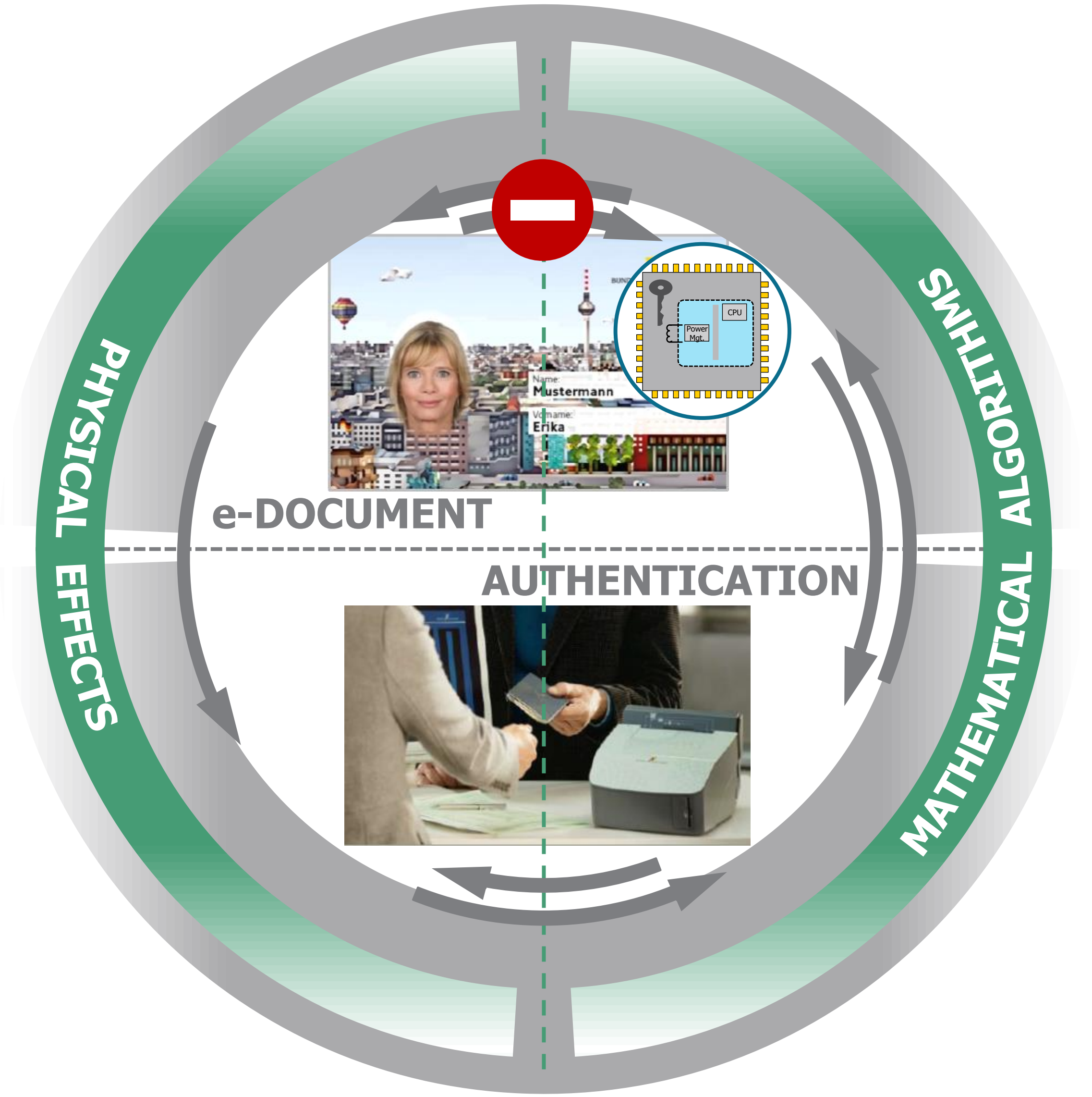


# Optical PUFs for Security Documents

- Document integrated optical PUFs allow extending the cryptographic security architecture beyond the boundaries of the security chip and to involve its physical surroundings.
  - The security chip can authenticate its physical surroundings – the two become one logical entity.
  - Keying material can be stored chip externally in the PUF.



# Closing the Authentication Circle



# International Standardization of PUFs

- Considered at ICAO RFI meeting, Montreal, July 2014

- ISO/IEC JTC 1/SC 27/WG 3 Study Period on Physically Unclonable Functions for Non-Stored Security Parameter Generation

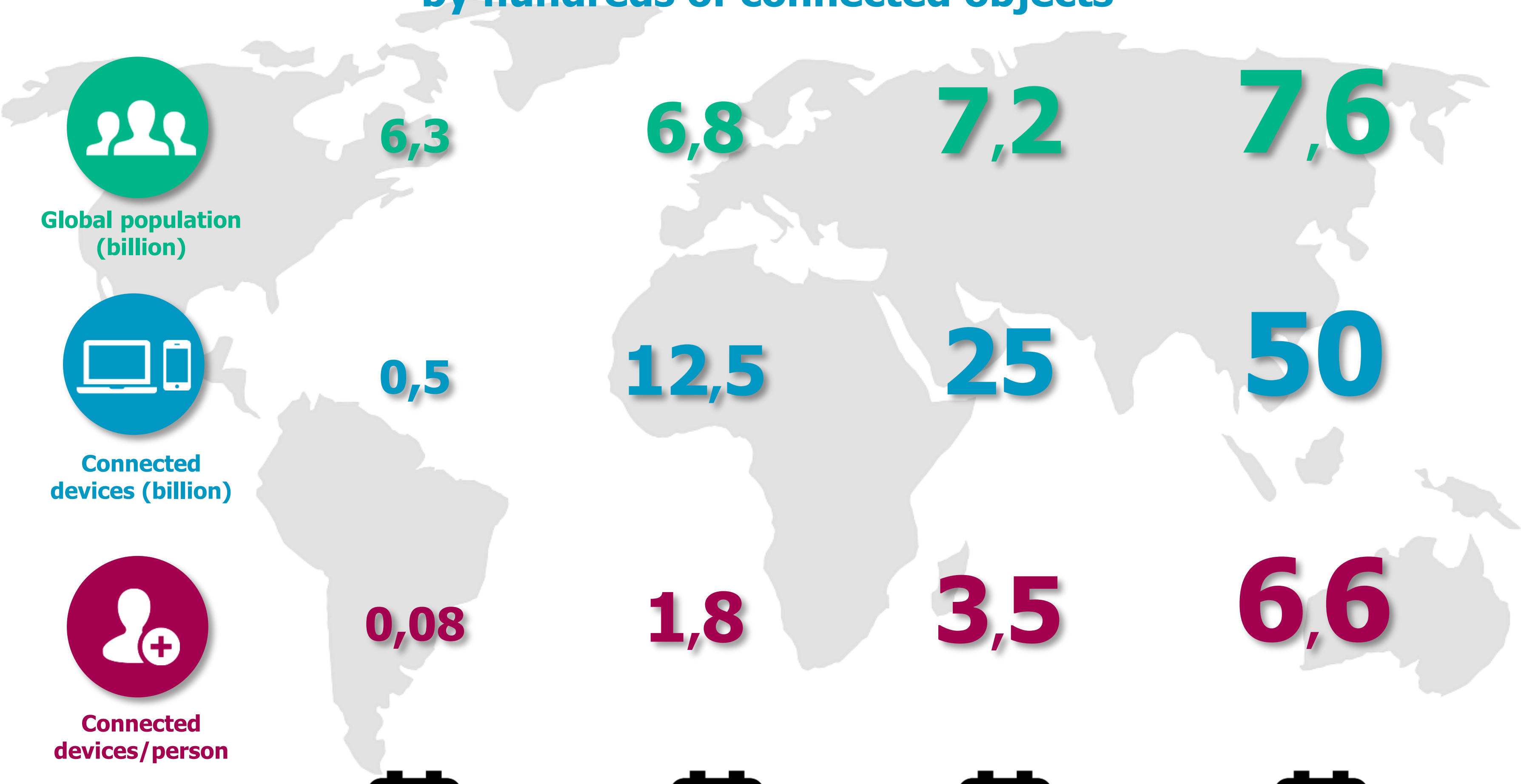
  - NWIP: Security requirements, test and evaluation methods for physically unclonable functions for generating non-stored security parameters
  - *Scope: This International Standard specifies security requirements and test and evaluation methods for Physically Unclonable Functions (PUFs).*
    *Specified security requirements include uniqueness of outputs for a batch of PUFs, reliability of outputs for a given PUF with a given input, and diffuseness (or unpredictability) of outputs for a given PUF under random inputs, and related evidence. The test and evaluation methods consist of analysis of design aspects of the PUF against the security requirements, and comparison between statistical analyses of the responses from a batch of PUFs or a unique PUF versus specified thresholds.*

# Futures of Identity

IV

# Trend: Increased Connectedness

## Every person will almost always be surrounded by hundreds of connected objects



| | 2003 | 2010 | 2015 | 2020 |
|---|---|---|---|---|
| Global population (billion) | 6,3 | 6,8 | 7,2 | 7,6 |
| Connected devices (billion) | 0,5 | 12,5 | 25 | 50 |
| Connected devices/person | 0,08 | 1,8 | 3,5 | 6,6 |

Source: CISCO IBSG

# Futures of Identity – *Smart Home*

BUNDES DRUCKEREI

The **Smart Home** „knows“ residents and guests and automatically assigns rights.

## ID Management Requirements

- User friendliness via mostly implicit authentication based on multi-modal biometric and behavioral patterns
- Pseudonyms („Guest A“)

## Use cases for smartcards

- Expression of intent (e.g., pay for multimedia stream)
- Applications with high security needs (e.g., physical access)

# Futures of Identity – *Corporate Environment*

Traditional ID cards might become **almost redundant** in the not too distant future

- Doors or gates will be able to recognize authorized persons automatically, without the need for explicit authentication
- Augmented reality screens or glasses will support security personnel to identify roles & rights of persons

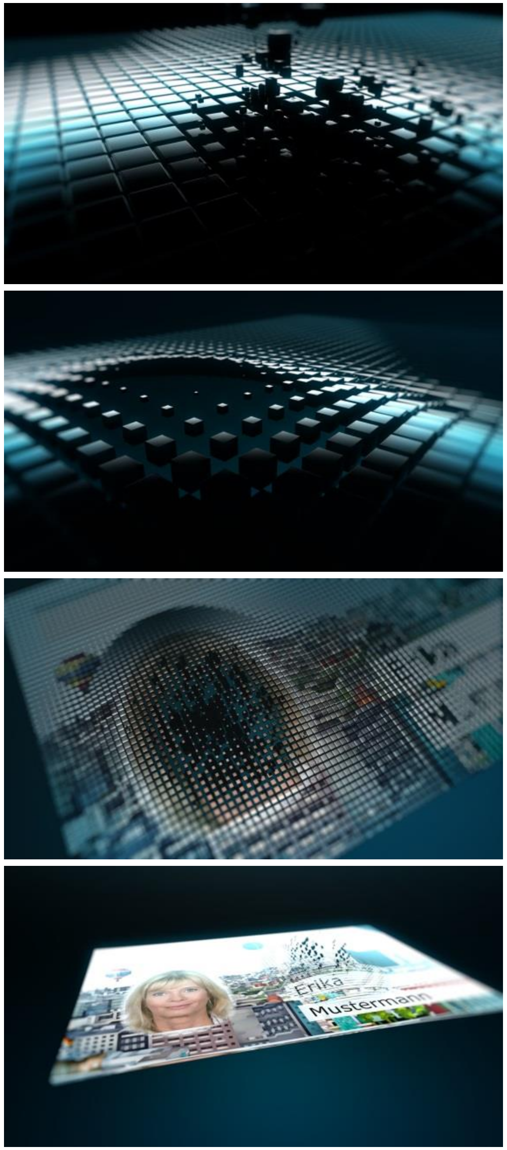
## ID Management Requirements

- Multi-modale Biometrics, Augmented Reality, Big Data

## Benefits of smartcards include

- Crypto-Toolbox, e.g., digital signatures
- Easy to check manually
- Corporate Identity

# Futures of Identity –
# *Claytronics (‘programmable matter’)*



- **Catoms** (‚claytronic atoms‘) are nanoscale computers designed to form much larger 3D objects
- Catoms will eventually have the ability to move around, communicate with others, change color, and physically connect to other catoms to form different shapes
- futuretimeline.net forecasts first mass market claytronic products for **2040**

ID documents may loose their traditional form factor

- think of ID tokens made from eID catoms certified to meet special security requirements
- users may morph their ID token according to personal taste or functional needs (e.g., from ID card to brouch or ring and back to ID card)

# Claytronics – Der Film

Claytronics

BUNDES DRUCKEREI

# Conclusions

BUNDESDRUCKEREI

1 Personal authentication transactions are predicted to increase from millions to billions … and perhaps trillions*
⇒ Secure digital IDs and their efficient management are essential

2 Users need to become more security-aware
⇔ Security needs to become more user-friendly

3 System on Document combines high security, usability & privacy protection

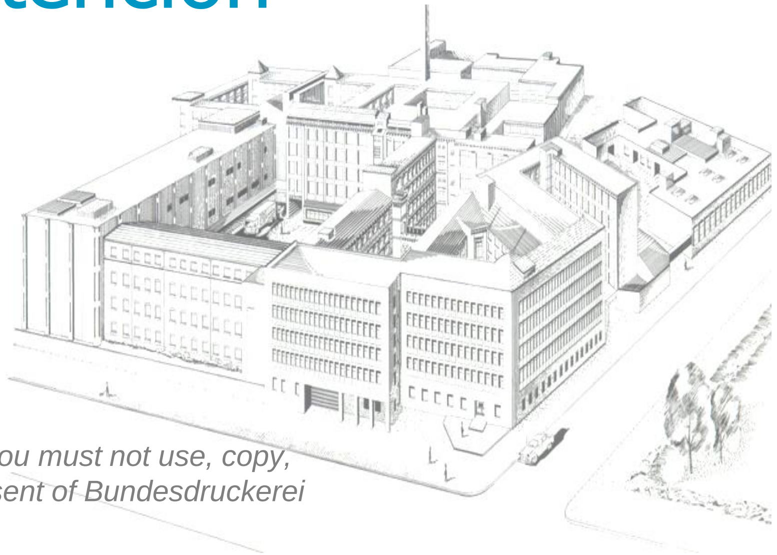
4 System on Document drives technology due to the strong demands regarding electronics, materials & systems

5 ID documents made from catoms are a powerful vision for the day after tomorrow

***) Source: Acuity Market Research, Nov 2013**

# Muchos gracias por su atención

walter.fumy@bdr.de



**Disclaimer:** *This presentation is owned by Bundesdruckerei GmbH. You must not use, copy, distribute or publish its content or parts thereof without the written consent of Bundesdruckerei GmbH. Copyright 2015 by Bundesdruckerei GmbH.*