secunet

# Conformity and Interoperability – Key Prerequisites for Security of eID documents

Holger Funke, 27th April 2017, ID4Africa Windhoek

# Agenda

1. **About secunet Security Networks AG**
2. Timeline of interoperability for eID documents
3. Requirements and technical guidelines
4. Interoperability as a result of conformity
5. Conclusion

# Facts & figures

## secunet Security Networks AG

- Customer-orientated corporate culture
- More than 430 employees at ten sites in Germany
- Founded in 1997
- Listed as prime standard on the German Stock Exchange
- Largest shareholder (79%): Giesecke & Devrient GmbH
- 2016 turnover: € 115.7m, 2016 EBIT: € 13.7m.*
  (*preliminary results)

# secunet stands for

## Trust

- IT security partner of the Federal Republic of Germany
- In-depth customer understanding
- Protection of confidential customer data and infrastructures
- Partner of the Alliance for Cyber Security

## Experience

- Almost 20 years in the market
- Outstanding expert knowledge and understanding of cryptographic processes
- Long-term customer relationships
- National and international project references

**Premium IT Security Made in Germany**

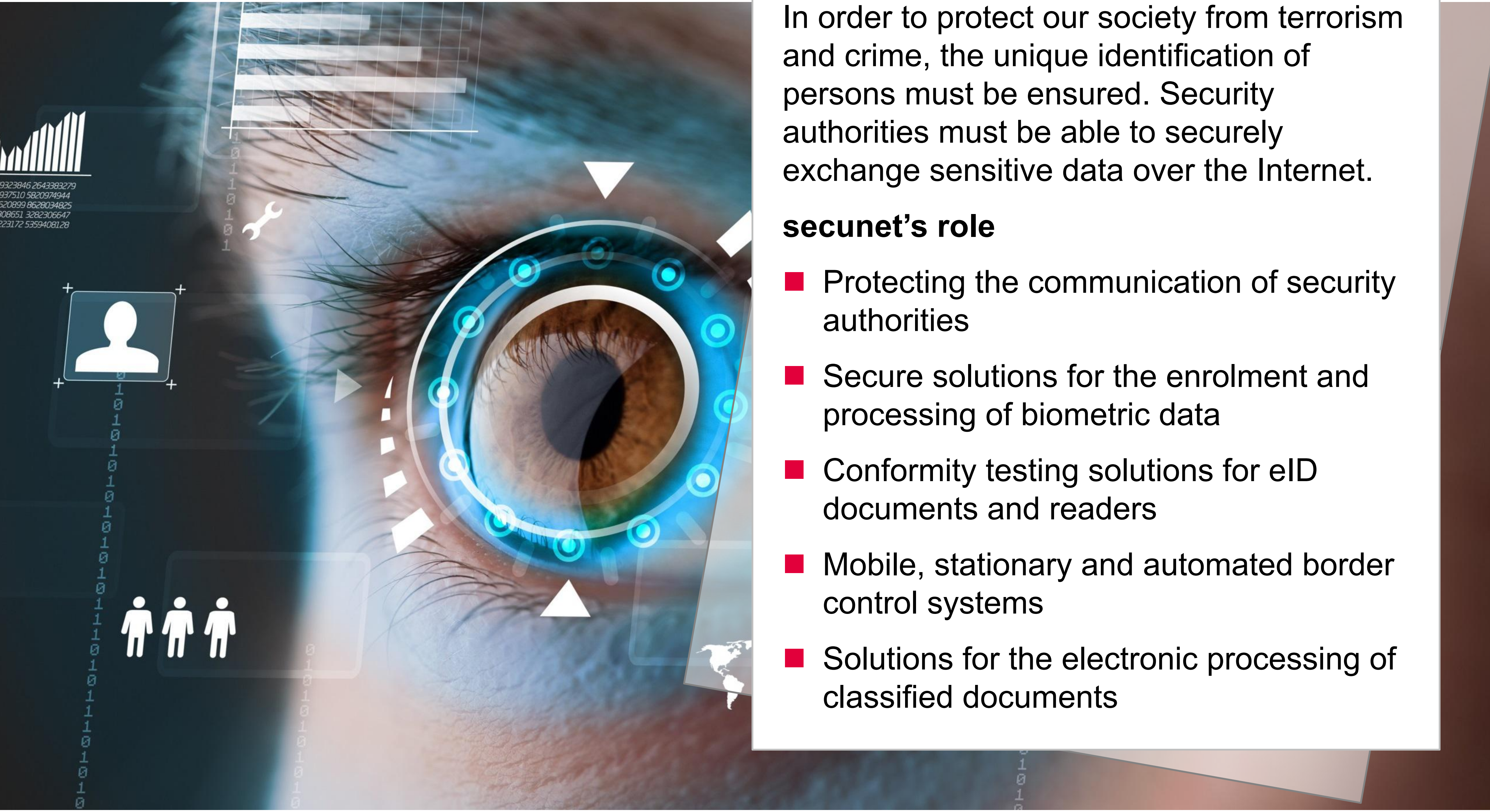
## Internationalism

- Highest EU and NATO approvals
- Collaboration in international committees
- International project awards

## Innovation

- Forward-looking, wide-ranging developments for complex tasks
- Tailored security through customised solutions
- Broad product and consultation portfolio

# Business Unit Homeland Security



## Facts

In order to protect our society from terrorism and crime, the unique identification of persons must be ensured. Security authorities must be able to securely exchange sensitive data over the Internet.

## secunet’s role

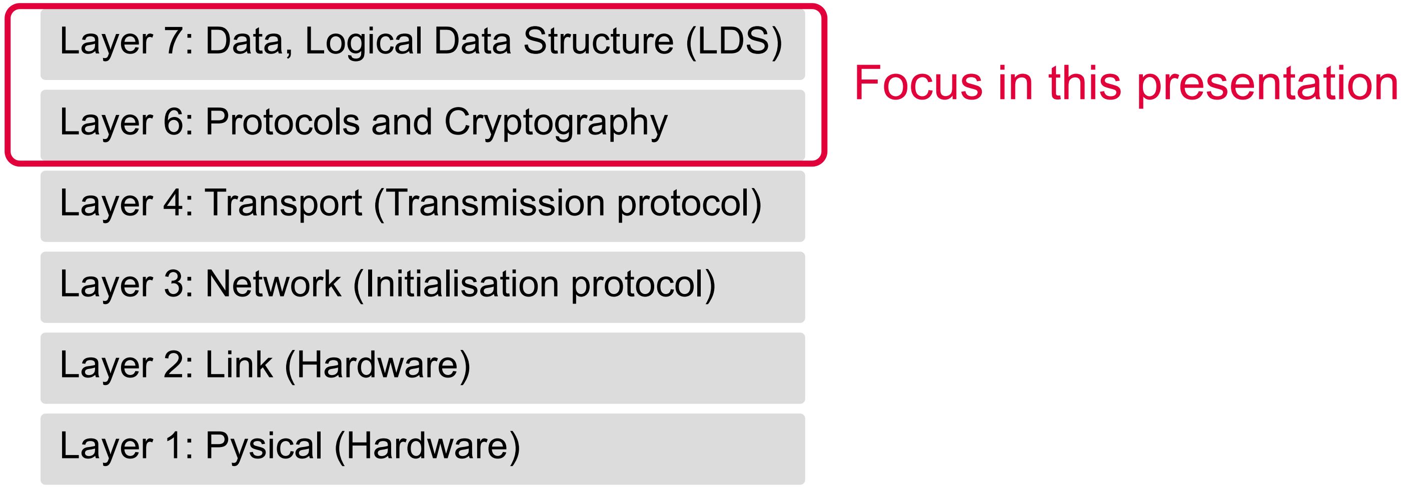
- Protecting the communication of security authorities
- Secure solutions for the enrolment and processing of biometric data
- Conformity testing solutions for eID documents and readers
- Mobile, stationary and automated border control systems
- Solutions for the electronic processing of classified documents

# Agenda

1. About secunet Security Networks AG
2. **Timeline of interoperability for eID documents**
3. Requirements and technical guidelines
4. Interoperability as a result of conformity
5. Conclusion

# Some basics regarding ePassports

- An electronic passport contains a chip with encrypted biographic and biometric data of the holder and also cryptographic information
- An integrated chip increases the security of the document
- The “International Civil Aviation Organization” (ICAO) sets and manages the framework for issuing and managing passports (e.g. Doc 9303)
- Additional specifications for datapage, physical security features, background systems…
- Chip can be separated in several layers according to ISO / OSI layer model:



Layer 7: Data, Logical Data Structure (LDS)

Layer 6: Protocols and Cryptography

Layer 4: Transport (Transmission protocol)

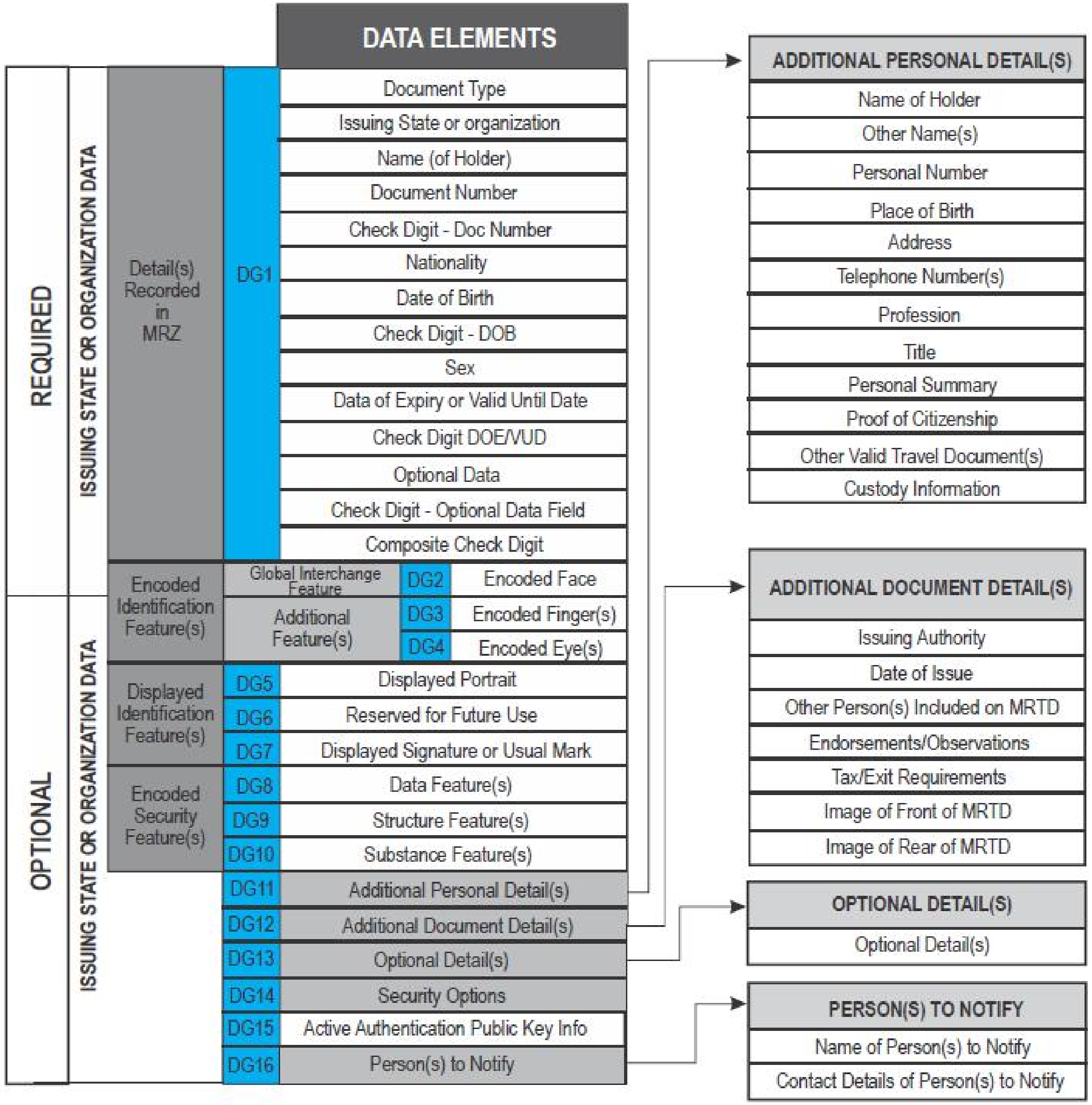
Layer 3: Network (Initialisation protocol)

Layer 2: Link (Hardware)

Layer 1: Pysical (Hardware)

Focus in this presentation

# Which information can be stored in an ePassport?



| | | | | | DATA ELEMENTS |
|---|---|---|---|---|---|
| REQUIRED | ISSUING STATE OR ORGANIZATION DATA | Detail(s) Recorded in MRZ | | DG1 | Document Type |
| | | | | | Issuing State or organization |
| | | | | | Name (of Holder) |
| | | | | | Document Number |
| | | | | | Check Digit - Doc Number |
| | | | | | Nationality |
| | | | | | Date of Birth |
| | | | | | Check Digit - DOB |
| | | | | | Sex |
| | | | | | Data of Expiry or Valid Until Date |
| | | | | | Check Digit DOE/VUD |
| | | | | | Optional Data |
| | | | | | Check Digit - Optional Data Field |
| | | | | | Composite Check Digit |
| | | Encoded Identification Feature(s) | Global Interchange Feature | DG2 | Encoded Face |
| OPTIONAL | ISSUING STATE OR ORGANIZATION DATA | | Additional Feature(s) | DG3 | Encoded Finger(s) |
| | | | | DG4 | Encoded Eye(s) |
| | | Displayed Identification Feature(s) | | DG5 | Displayed Portrait |
| | | | | DG6 | Reserved for Future Use |
| | | | | DG7 | Displayed Signature or Usual Mark |
| | | Encoded Security Feature(s) | | DG8 | Data Feature(s) |
| | | | | DG9 | Structure Feature(s) |
| | | | | DG10 | Substance Feature(s) |
| | | | | DG11 | Additional Personal Detail(s) |
| | | | | DG12 | Additional Document Detail(s) |
| | | | | DG13 | Optional Detail(s) |
| | | | | DG14 | Security Options |
| | | | | DG15 | Active Authentication Public Key Info |
| | | | | DG16 | Person(s) to Notify |

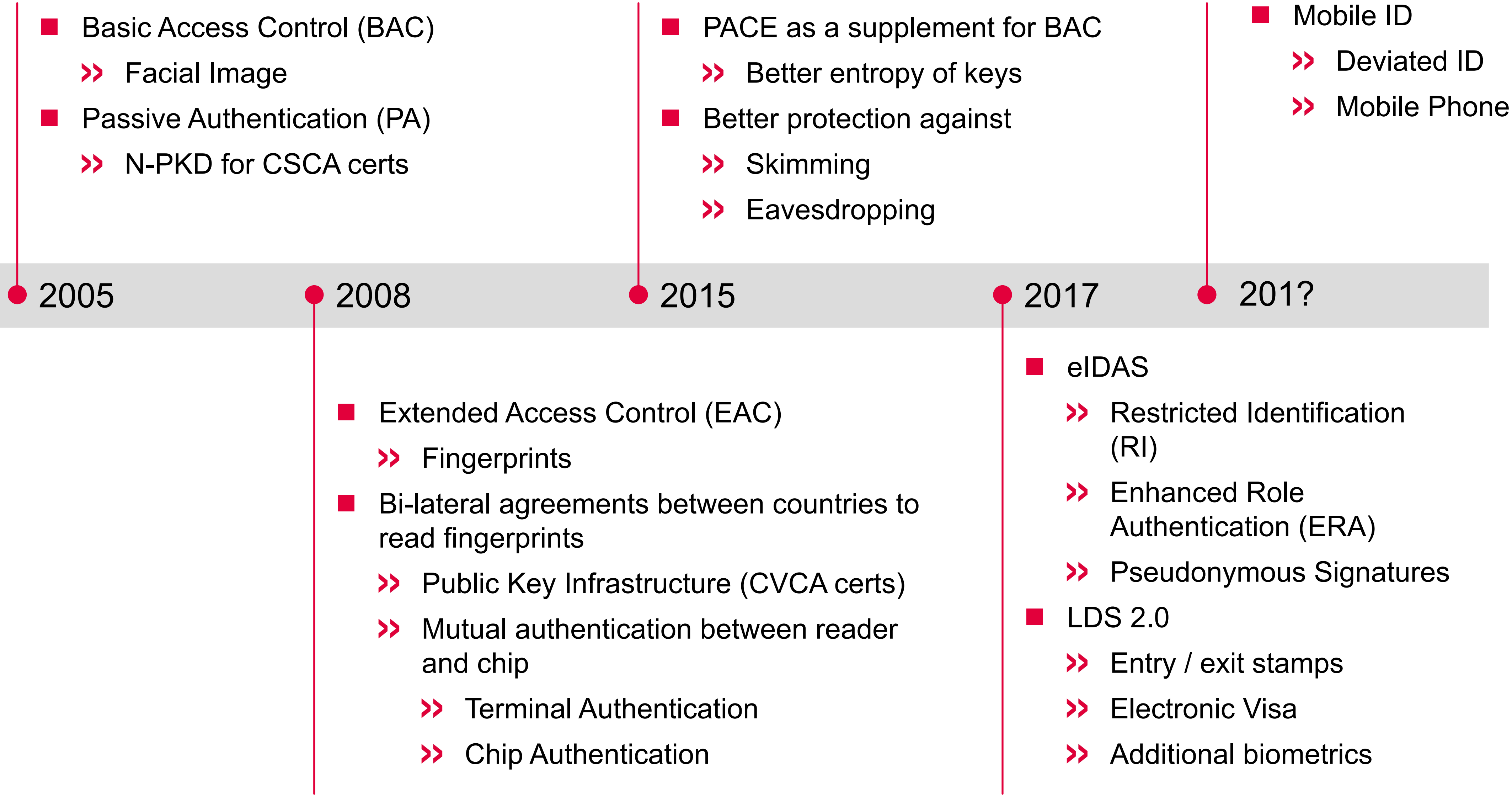
| ADDITIONAL PERSONAL DETAIL(S) |
|---|
| Name of Holder |
| Other Name(s) |
| Personal Number |
| Place of Birth |
| Address |
| Telephone Number(s) |
| Profession |
| Title |
| Personal Summary |
| Proof of Citizenship |
| Other Valid Travel Document(s) |
| Custody Information |

| ADDITIONAL DOCUMENT DETAIL(S) |
|---|
| Issuing Authority |
| Date of Issue |
| Other Person(s) Included on MRTD |
| Endorsements/Observations |
| Tax/Exit Requirements |
| Image of Front of MRTD |
| Image of Rear of MRTD |

| OPTIONAL DETAIL(S) |
|---|
| Optional Detail(s) |

| PERSON(S) TO NOTIFY |
|---|
| Name of Person(s) to Notify |
| Contact Details of Person(s) to Notify |

# Milestones of eID documents (chip)



2005

- Basic Access Control (BAC)
  - Facial Image
- Passive Authentication (PA)
  - N-PKD for CSCA certs

2008

- Extended Access Control (EAC)
  - Fingerprints
- Bi-lateral agreements between countries to read fingerprints
  - Public Key Infrastructure (CVCA certs)
  - Mutual authentication between reader and chip
    - Terminal Authentication
    - Chip Authentication

2015

- PACE as a supplement for BAC
  - Better entropy of keys
- Better protection against
  - Skimming
  - Eavesdropping

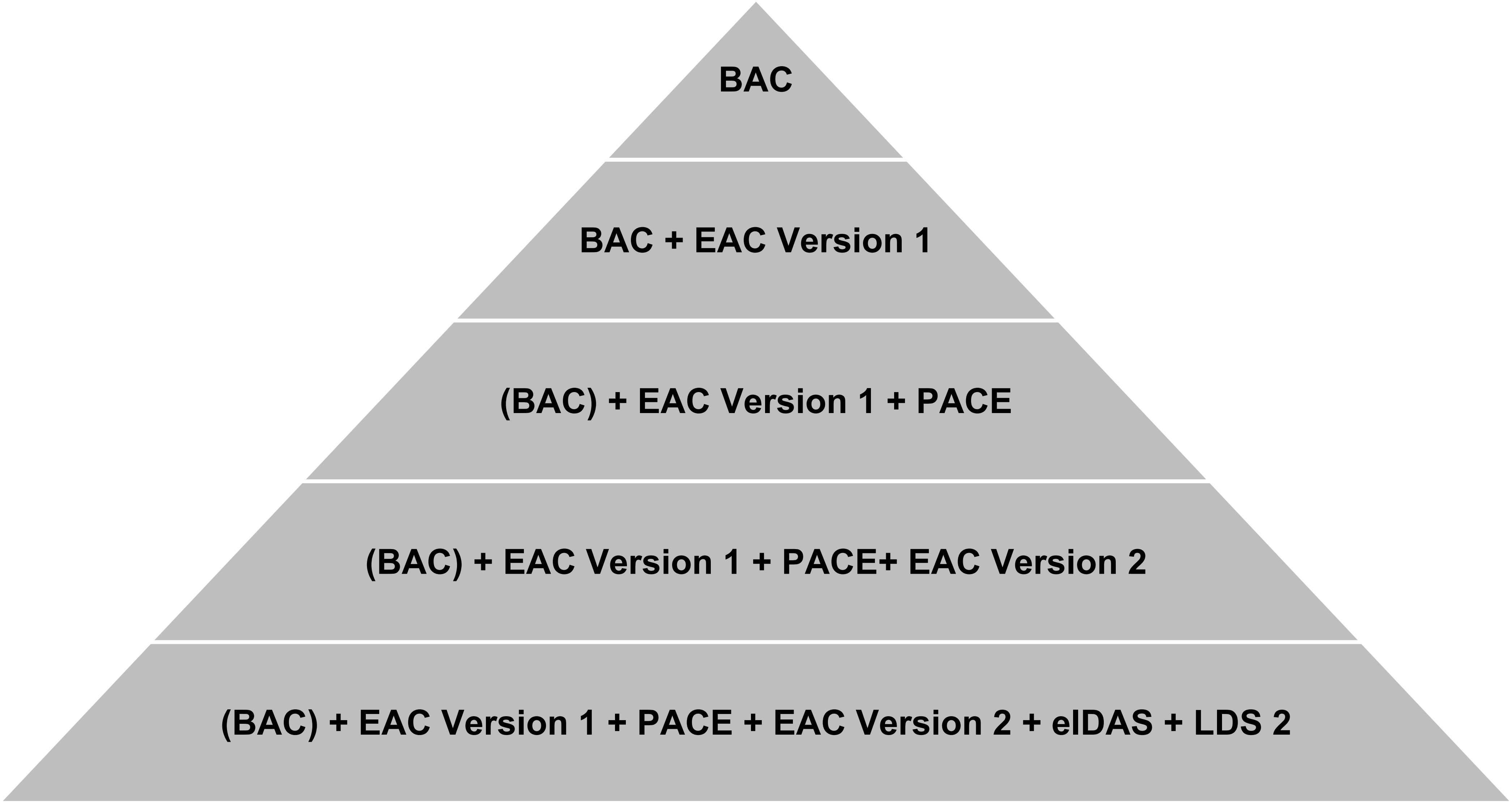
2017

- eIDAS
  - Restricted Identification (RI)
  - Enhanced Role Authentication (ERA)
  - Pseudonymous Signatures
- LDS 2.0
  - Entry / exit stamps
  - Electronic Visa
  - Additional biometrics

201?

- Mobile ID
  - Deviated ID
  - Mobile Phone

# Complexity of eID protocols



BAC

BAC + EAC Version 1

(BAC) + EAC Version 1 + PACE

(BAC) + EAC Version 1 + PACE+ EAC Version 2

(BAC) + EAC Version 1 + PACE + EAC Version 2 + eIDAS + LDS 2

# Agenda

1. About secunet Security Networks AG
2. Timeline of interoperability for eID documents
3. **Requirements and technical guidelines**
4. Interoperability as a result of conformity
5. Conclusion

# Test Specifications to assure Interoperability

ePassports and inspection systems must be conform to the following test specifications:

- BSI TR-03105
  - Part 3.2 eMRTD with EACv1
  - Part 3.3 eMRTD with EACv2
  - (Part 3.4 eSign for ID card)
- BSI TR-03105
  - Part 5.1 Inspection systems with EACv1
  - Part 5.2 Reader with EACv2
  - (Part 5.3 Terminal software for ID card reader)
- ICAO Technical Guidelines
  - Part 3: eMRTD with EACv1 and PACE
  - Part 4: Inspection systems with EACv1 and PACE

Federal Office
for Information Security

# Structure of Test Specifications

## Components of Test Specification

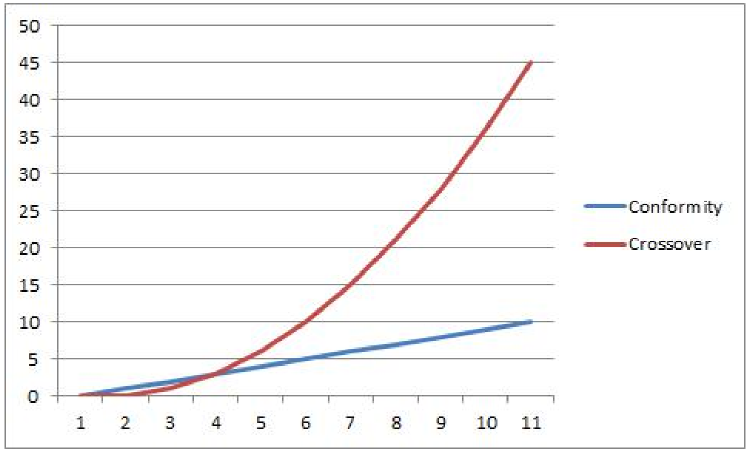
- Description of general test requirements
- Test setup / Testing environment
- Definition of suitable test profiles / implementation profiles
- Implementation Conformance Statement (ICS)
- Definition of testing or configuration data
- Definition of test cases according to a unified data structure
- Each test case should concentrate on a single feature to be tested!

## Structure of Test Case

- **Test case ID**: unique identifier for each test case
- **Purpose**: objective of the test case
- **Version**: current version of this test case independent from the test specification
- **Reference**: where is this feature / behaviour specified
- **Preconditions**: setup of test case
- **Test scenario**: description of test case, step by step and corresponding expected result
- **Postconditions**: setdown of test case

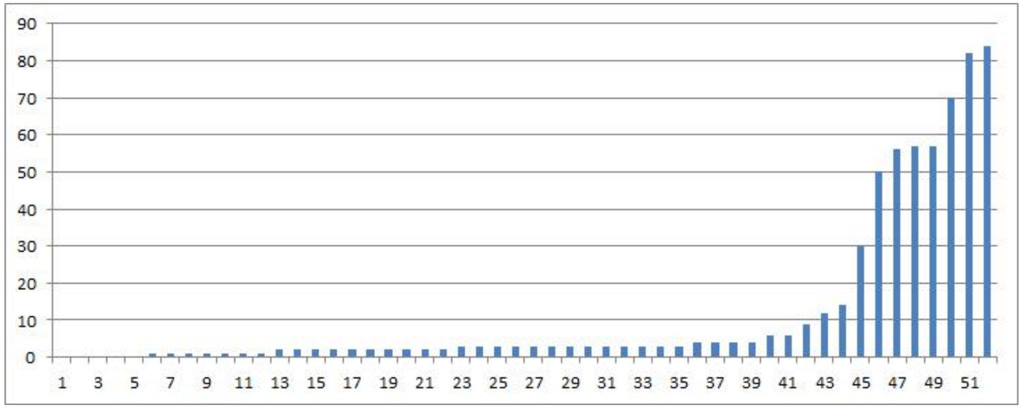
# Official Interoperability Tests

- Since 2003 interoperability tests for ePassports were performed to assure international interoperability
- Crossover tests in combination with conformity tests
- Crossover tests:
  - Every ePassport is tested with every inspection system
- Conformity tests:
  - Every ePassport is tested against the test specification



- Benefits of conformity testing:
  - Less efforts (crossover test can only be handled with a low number of devices to test)
  - Every feature of an ePassport or inspection system can be tested separately
  - Detailed failure analysis allows to improve the stability of the whole eMRTD eco system
  - Results help not only to improve the stability of ePassports and inspection systems but also to improve the quality of (test) specifications and test tools

# Results and Experience of last Interoperability Tests



- Madrid 2014 (ICAO)
  - Focus on PACE
  - Companies and countries took part in the test
  - 10 inspection systems, 3 test labs
  - 52 completely different ePassports were tested
  - Detailed results:

    http://blog.protocolbench.org/2014/07/results-sac-interoperability-test-madrid-2014/

- London 2016 (Security Document World)
  - Focus on PACE and PACE-CAM
  - 17 document provides, 27 ePassports, 12 inspection systems, 2 test labs
  - Inspection system were tested in crossover tests
  - ePassports were additionally tested against subset of ICAO test specification
    - 8502 test cases were performed, 98% passed
  - Detailed results:

    http://blog.protocolbench.org/2016/05/results-emrtd-interoperability-test-2016/

SDW INTEROP

- **Next InteropTest: End of September at Joint Research Center (JRC) in Italy organised by the European Commission and performed by JRC with focus on PACE!**

# Check Interoperability with tools automatically

## Golden Reader Tool (GRT)

- Reference implementation for ePassports with biometric data
- Reads the data stored on the ICAO compliant chip and displays them

secunet (GRT platinum edition

## GlobalTester (GT)

- For conformity tests of eID documents and inspection systems
- Support of all relevant protocols in context of eID documents (PACE, TA, CA etc.)
- Used at several interoperability tests worldwide since 2006
- Customers: chip vendors, application vendors, national security printers, test labs…
- Detailed test report -> certification

secunet (GlobalTester

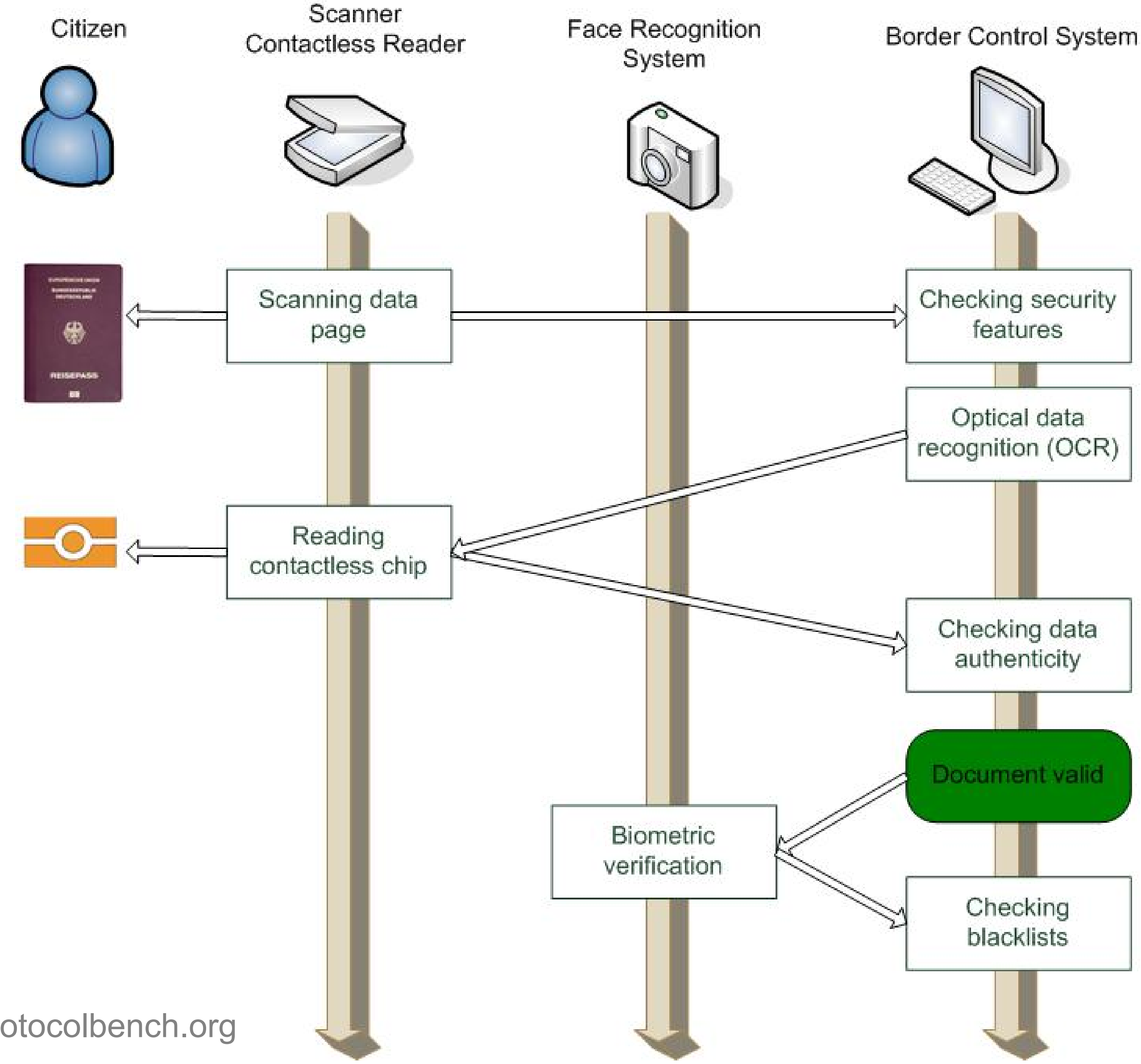
# Agenda

1. About secunet Security Networks AG
2. Timeline of interoperability for eID documents
3. Requirements and technical guidelines
4. **Interoperability as a result of conformity**
5. Conclusion

# One Result of Interoperability: Automated Border Control

## eGates:

- Automated border control increases security:
  - Spend less time for standard tasks
  - More time for analysing critical ePassports



Source: blog.protocolbench.org

# Example for Automated Border Control: EasyPASS

| Travellers | 2015* | 2016* |
|---|---|---|
| Overall Entry (Germany) | 39.9 | 40.9 |
| Overall Exit (Germany) | 39.4 | 40.4 |
| EasyPass Users | 9.1 | 12.1 |
| Frankfurt Airport (overall) | 25.5 | 24.9 |
| Part of EasyPASS (Frankfurt) | **18.0%** | **25.0%** |

* In million users, Source: Federal Police

# Agenda

1. About secunet Security Networks AG
2. Timeline of interoperability for eID documents
3. Requirements and technical guidelines
4. Interoperability as a result of conformity
5. **Conclusion**

# Conclusion

- Interoperability of eID documents is
  - the result of conformity testing
  - easily and automatically testable by using internationally established tools
  - key functionality for world-wide travelling
  - the key element for automatic border control

Security of eID documents is achieved by interoperability.

secunet

**Holger Funke**

Principal - Division Homeland Security

**secunet Security Networks AG**

Hauptstr. 35
33178 Borchen
Germany
Phone +49 201 5454-3865
Fax +49 201 5454-1324
holger.funke@secunet.com