Towards electronic identification and trusted services for biometric authenticated transactions in the Single Euro Payments Area

CASED

21.05.14 | **Nicolas Buchmann**, Christian Rathgeb, Harald Baier and Christoph Busch

TECHNISCHE UNIVERSITÄT DARMSTADT

Fraunhofer SIT

h_da

LOEWE – Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz

da/sec
BIOMETRICS AND INTERNET-SECURITY RESEARCH GROUP

Outline

- **Introduction / Motivation**
- **System components**
  - eIDAS
  - Incorporation of biometrics
  - BioPACE V2
- **System Overview**
- **Conclusion**

Outline

- **Introduction / Motivation**
- **System components**
  - eIDAS
  - Incorporation of biometrics
  - BioPACE V2
- **System Overview**
- **Conclusion**

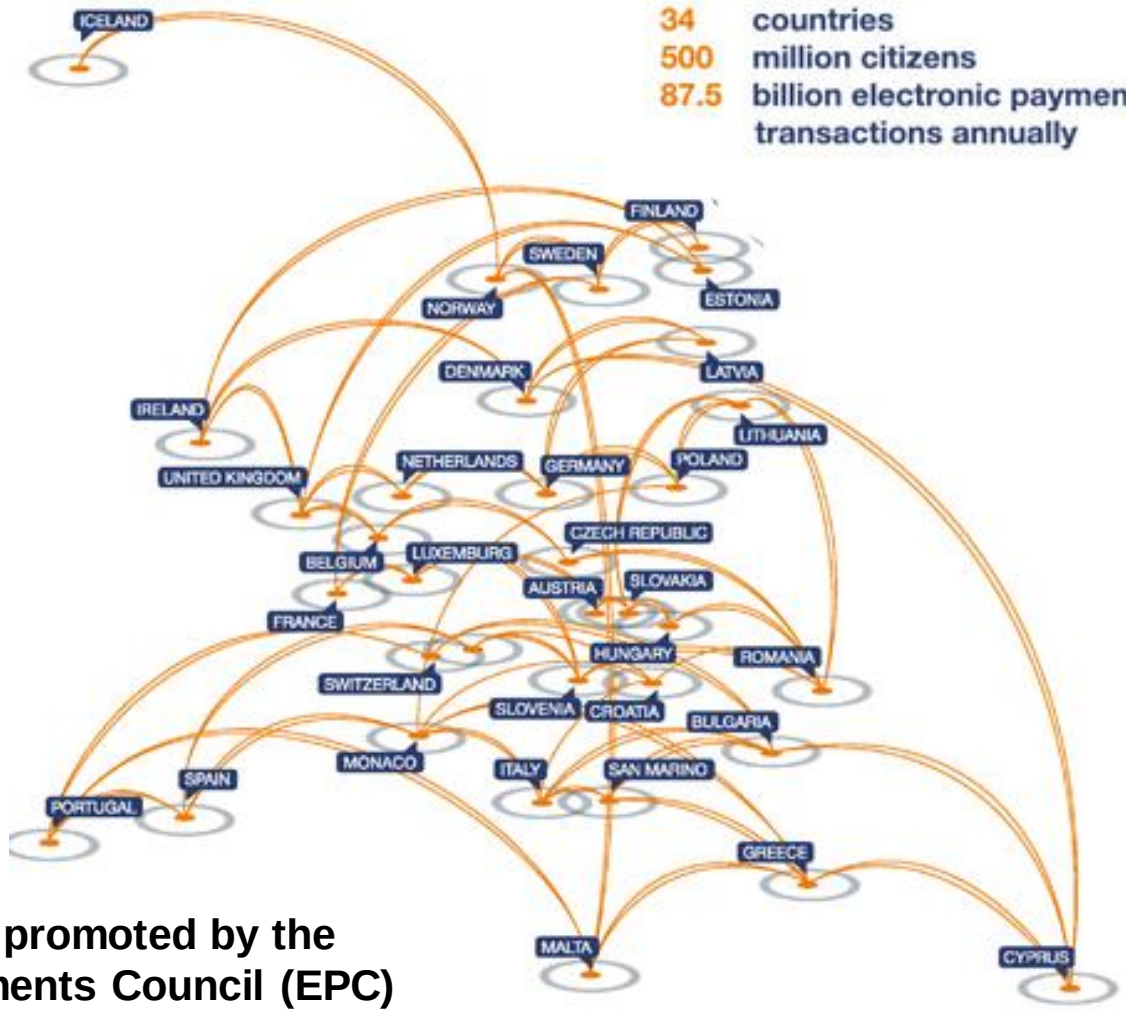
Introduction

- **Oct, 2013: European Parliament Committee on Industry, Research and Energy (ITRE) initiated the regulation and harmonisation for electronic identification, authentication and trust services (eIDAS) between EU member states**

- **The upcoming EU regulation will ensure mutual recognition and acceptance of electronic identification across borders**

- **Opportunity for trusted electronic transactions in the Single Euro Payments Area (SEPA).**

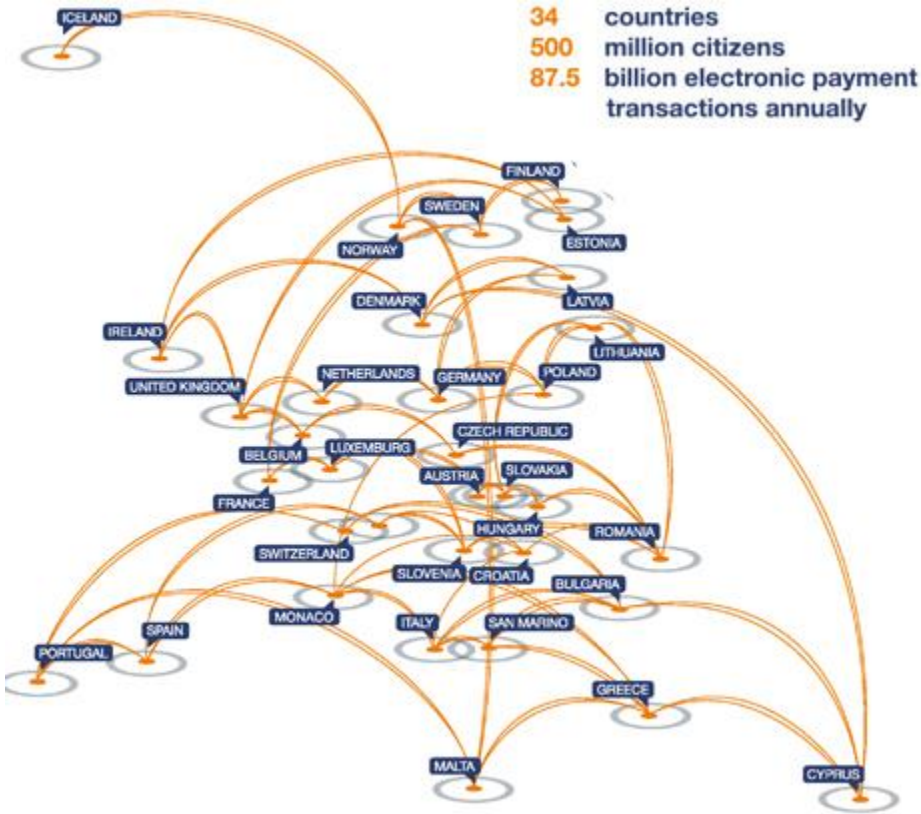
Introduction - Single Euro Payments Area (SEPA)



Supported and promoted by the European Payments Council (EPC)

Introduction – SEPA requirements

- **Security protocol based on a standard which has been proven secure and functional in practice**
- **Pre-conditions apply to the upcoming eIDAS standard**
- **Building a bridge between the upcoming eIDAS standard and SEPA transactions provides a mutual gain for both sectors**
- **Ongoing process of the eIDAS regulation is strengthened by new use cases targeted at millions of users (e.g. secure home eBanking and skimming prevention at ATMs).**



- **SEPA transactions could rely on standards which have been proven secure in another high-security domain.**

Introduction – Contribution of proposed System

- **Adaption of the upcoming eIDAS standard towards trusted banking transactions resulting in security and privacy enhancements**
- **Extension of the eIDAS standard regarding privacy compliant biometric authenticated transactions to enhances user convenience, trust and confidence towards eBanking and eBusiness**
- **Very limited amount of existing proposals on the integration of biometrics into trusted banking transactions**
- **Proposed system fully relies on standardised and provable secure protocols, infrastructure, and technologies, vital for any kind of banking transaction application**

Introduction – Motivation

- **A study in 2010 by Deutsche Bank Research identified the harmonisation of the diverse regulatory regimes across Europe as one of the main obstacles for cross-border financial service profit**

- **Despite the fact, that eIDAS is an upcoming standard, which will eliminate the aforementioned obstruction, it will rely on existing infrastructure**

Outline

- **Introduction / Motivation**
- **System components**
  - eIDAS
  - Incorporation of biometrics
  - BioPACE V2
- **Conclusion**

electronic identification, authentication and trust services (eIDAS) – Status of eID

CASED

- **Operational eID systems: Belgium, Estonia, Germany, Italy, Latvia, the Netherlands, Portugal, Romania, and Spain**
- **Planned for near future: France, Hungary and Slovakia**
- **regulation aims at the harmonisation for electronic identification, authentication and trust services (eIDAS) between EU member states**

electronic identification, authentication and trust services (eIDAS) – Security goals

CASED

- Between two entities (e.g. a user and a bank with an eID enabled service) eIDAS provides mutual authentication and key agreement to establish a secure channel

- The user can be certain that he is communicating with his bank and the bank can be assured to communicate with a user in possession of a valid eIDAS token

- During the eIDAS procedure, user and bank agree on an ephemeral common secret to create a secure channel between the two parties which provides authenticity, integrity and confidentiality for further communication

Incorporation of biometrics

- **Strong link between the holder and the eIDAS token**
- **Higher entropy for keying material**

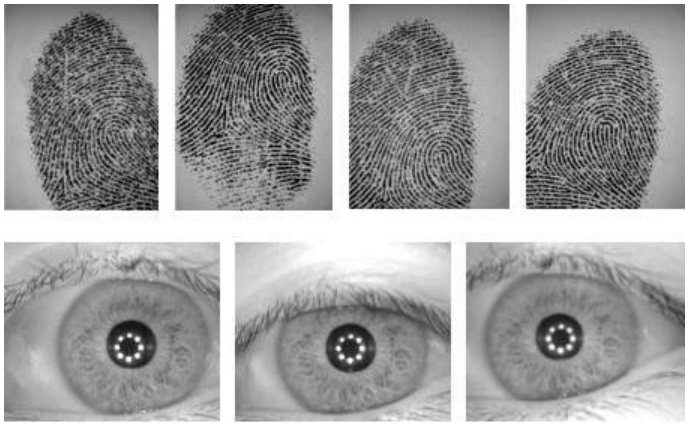
Entropy reported in literature for different biometric characteristics

Biometric characteristic	Entropy
Fingerprint	84 bits
Iris	249 bits
Face	56 bits

  - 6 digit numeric PIN ~20bit entropy

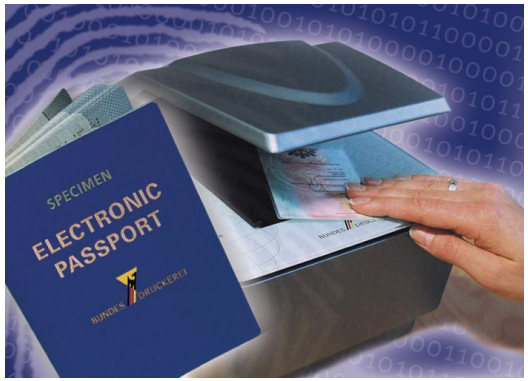
- **Cannot be forgotten, lost, stolen, shared or duplicated by the user**

- **Biometric authenticated transactions**



Password Authenticated Connection Establishment (PACE)

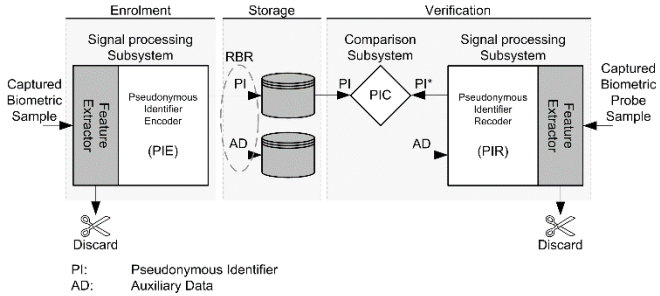
- **Prevents unauthorised access to eIDAS token**
- **Token reader needs optical access to the data page**
- **Session key agreement**
- **Establishes a secure channel (authenticity, integrity, and confidentiality)**



- **Input:**
  - Machine Readable Zone (MRZ)
  - Card Access Number (CAN)
  - PIN “123456”

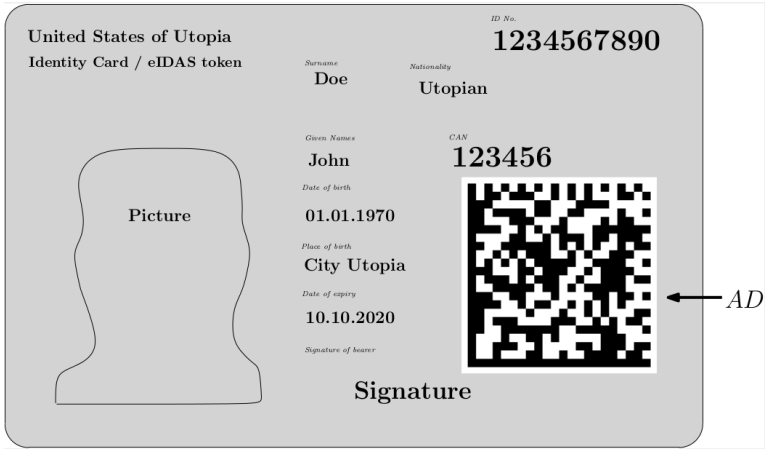
BioPACE V2 - initialisation phase

- **biometric enrolment is conducted (PI + AD)**

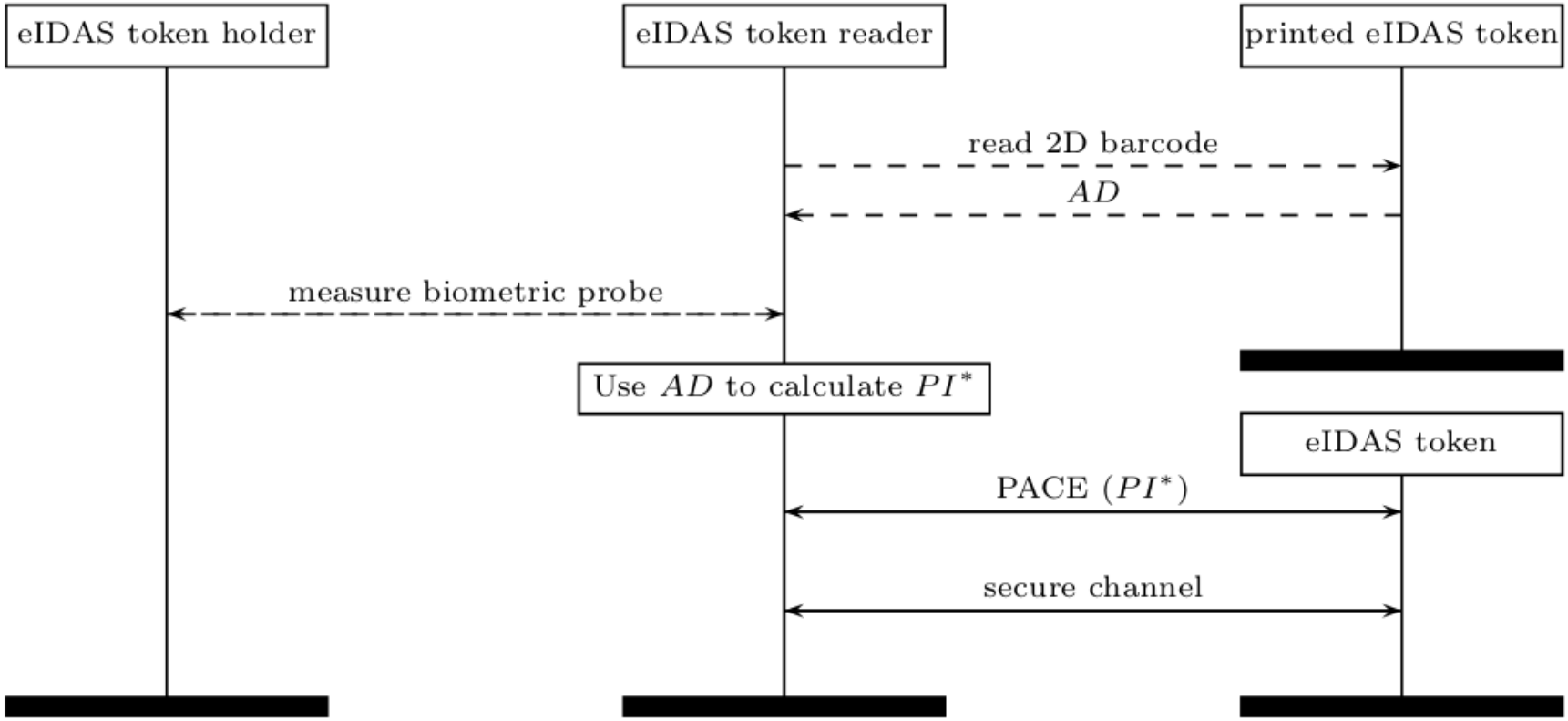


- ***PI* is stored in the secure memory of the token** ISO/IEC 24745 standard

- ***AD* printed on the token as 2D barcode**



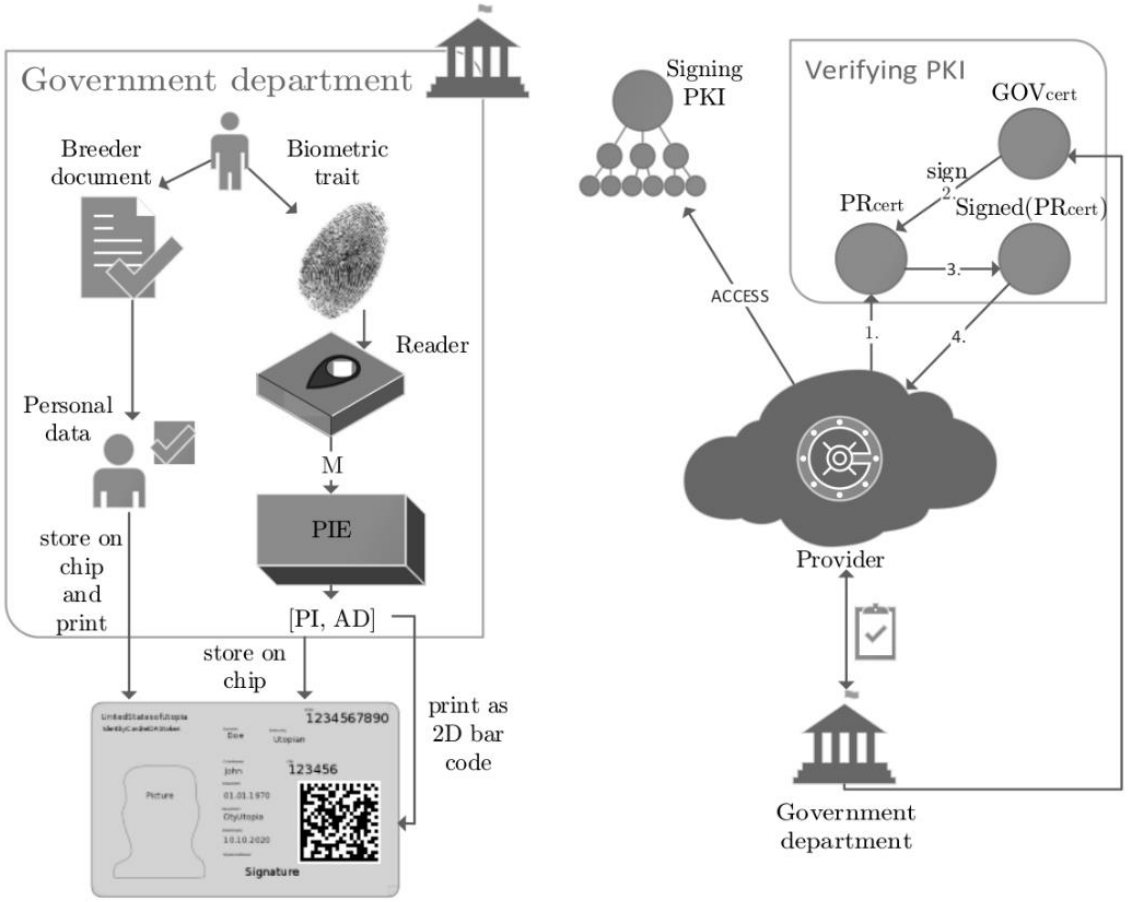
BioPACE V2 - regular use phase



Outline

- **Introduction / Motivation**
- **System components**
  - eIDAS
  - Incorporation of biometrics
  - BioPACE V2
- **System Overview**
- **Conclusion**

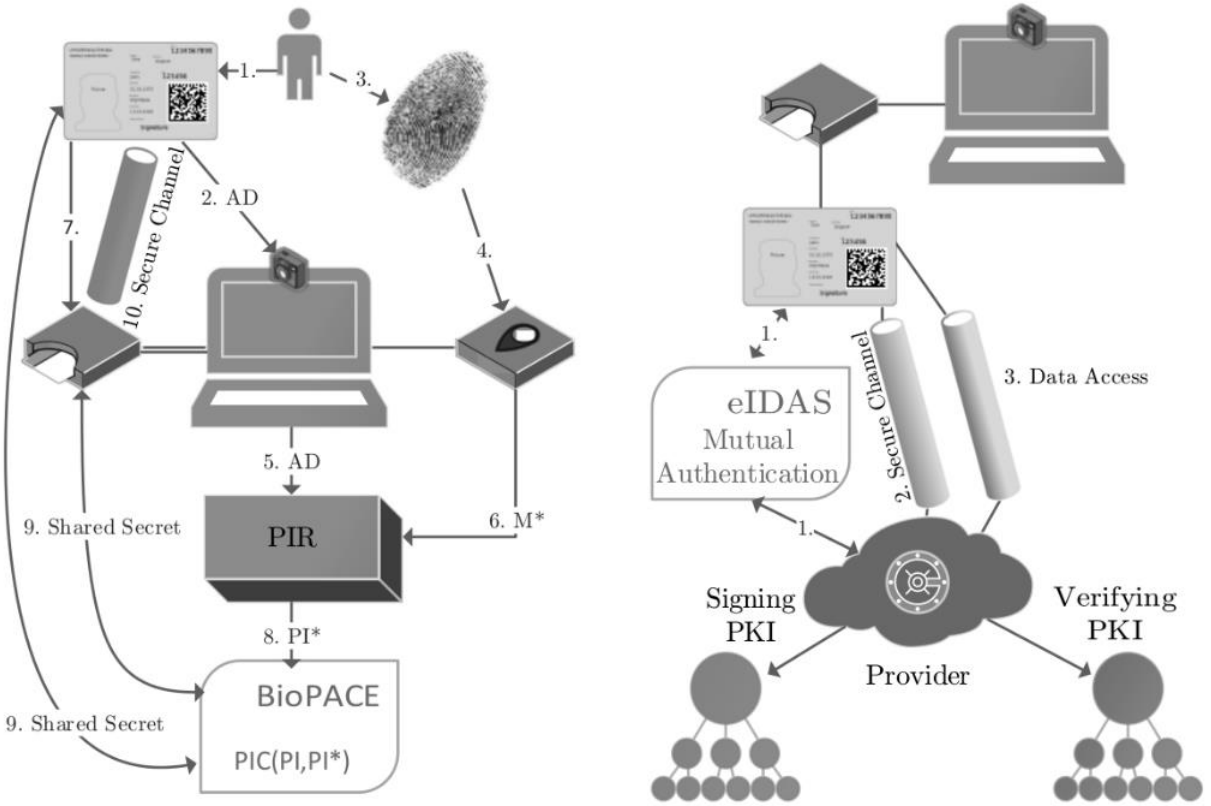
System Overview 1/2



(a) eIDAS token issuing and enrolment. (b) eIDAS provider activation.

Figure 1: Wrap-up of (a) token issuing, enrolment, and (b) provider activation.

System Overview 2/2



(a) Entity auth.: Token – Reader (b) Entity auth.: Token – Provider

Figure 2: Wrap-up of authentication of token and (a) reader, and (b) provider.

Outline

- **Introduction / Motivation**
- **System components**
  - eIDAS
  - Incorporation of biometrics
  - BioPACE V2
- **System Overview**
- **Conclusion**

Conclusion

- eIDAS adapted towards trusted eBanking and eBusiness
- Extended eIDAS with respect to privacy compliant biometric authenticated transactions
- Fully relies on standardised and provable secure protocols, infrastructure, and technologies
- Significant improvement of user convenience, trust, and confidence towards eBanking and eBusiness
- Costs are considered negligible for both parties since users can rely on hardware, which is for the most part, already available
- Service providers can employ an already established infrastructure and, delegate expensive hardware support to government departments
- We identify eIDAS as an appropriate key driver in future eBanking services

Further questions:

CASED