Overview of Technical Developments

Emerging technologies
relevant for e-voting
in the next 5 years

Herbert.Leitold@a-sit.at

Introducing myself …

- Secure Information Technology Center Austria, A-SIT
  - Public funded non-profit association
  - Advises public sector on IT security

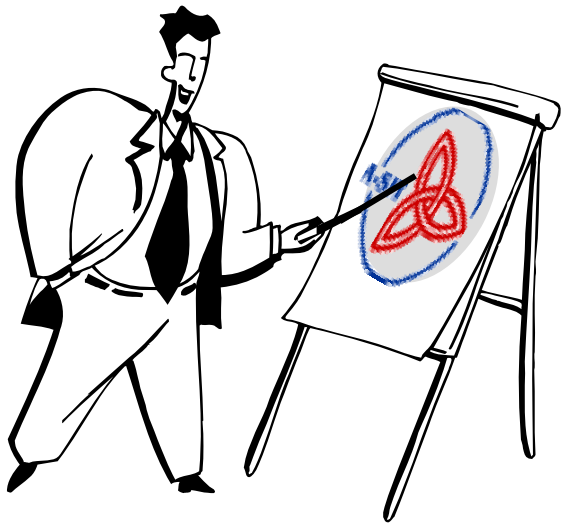
- A few words on myself
  - Managing A-SIT Graz branch "Technology Assessment"
  - Head of E-Government Innovation Center EGIZ

EGIZ

BUNDESKANZLERAMT ÖSTERREICH

IAIK TU Graz

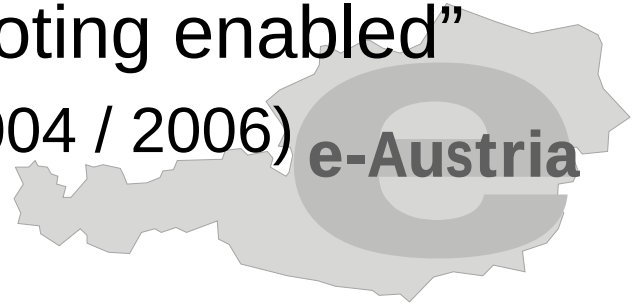
Table of Contents



- Introduction
  - E-Voting in Austria
- eID - Electronic Identification
  - EU Initiatives
  - Situation in Austria
  - eID Large Scale Pilots
- Trusted Computing
  - a candidate to improve e-voting security

E-Voting in Austria

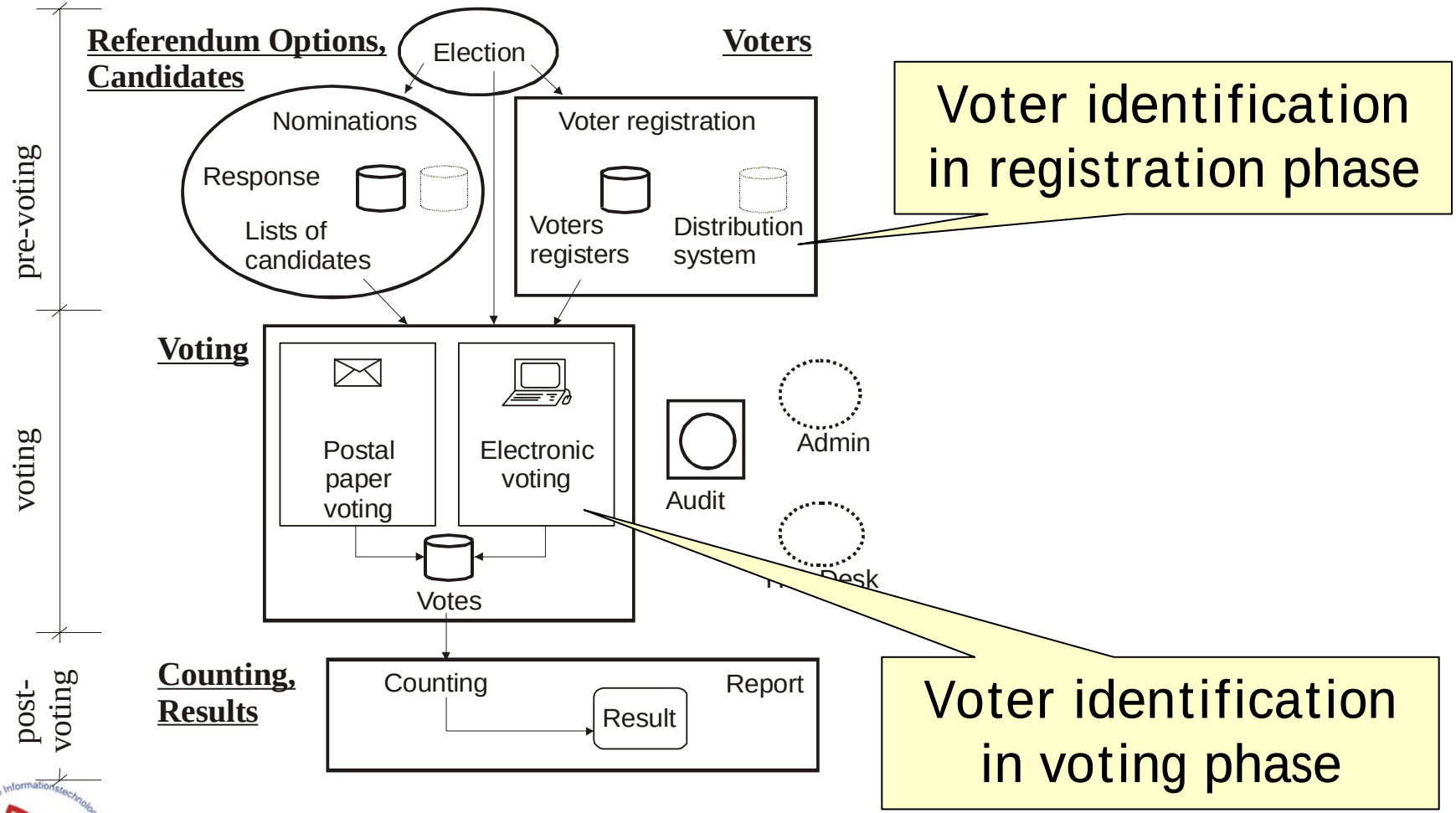
- Since CoE Recommendation 2004
  - Nov. 2004: Working Group on Legal, Technical and International Aspects
    - Report to the Federal Minister of Interior
  - Nov. 2006: Working Group on E-Participation
    - established by BLSG (federal-regional-local ICT coordination)
- No legal basis for casting a vote electronically
- Student unions or chambers “e-voting enabled”
  - So far, limited to academic tests (2004 / 2006)



PART I: eID – Electronic Identification

- Role of eID in E-Voting
  - Pre-voting phase
  - Voting phase
- EU Initiatives
  - i2010
  - Large Scale Pilots 2007+
- Status in Austria
  - Citizen Card projects

Voter identification



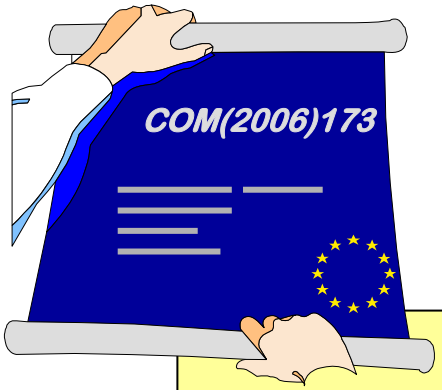
Identification in CoE Recommendations

D. Security, General requirements

80. The e-voting system shall restrict access to its services, **depending on the user identity** or the user role, to those services explicitly assigned to this user or role. **User authentication** shall be effective before any action can be carried out.

82. **Identification of voters** and candidates in a way that they can unmistakably be distinguished from other persons **(unique identification)** shall be ensured.

eID in the European Union



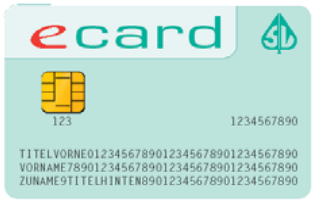
i2010 eGovernment Action Plan

... for ensuring that **by 2010 European citizens and businesses will be able to benefit from secure and convenient electronic means, issued at local, regional or national levels and complying with data protection regulations, to identify themselves to public services in their own or in any other Member State.**

cf. Ministerial Declaration "Manchester Declaration" 11/2005,
Council Conclusions "eGovernment for all Europeans" 06/2006

Status in Austria: Citizen Cards

Bank cards (ATM cards)
Each bank card issued since March 2005 is also an SSCD (as of Signature Directive 1999/93/EC)



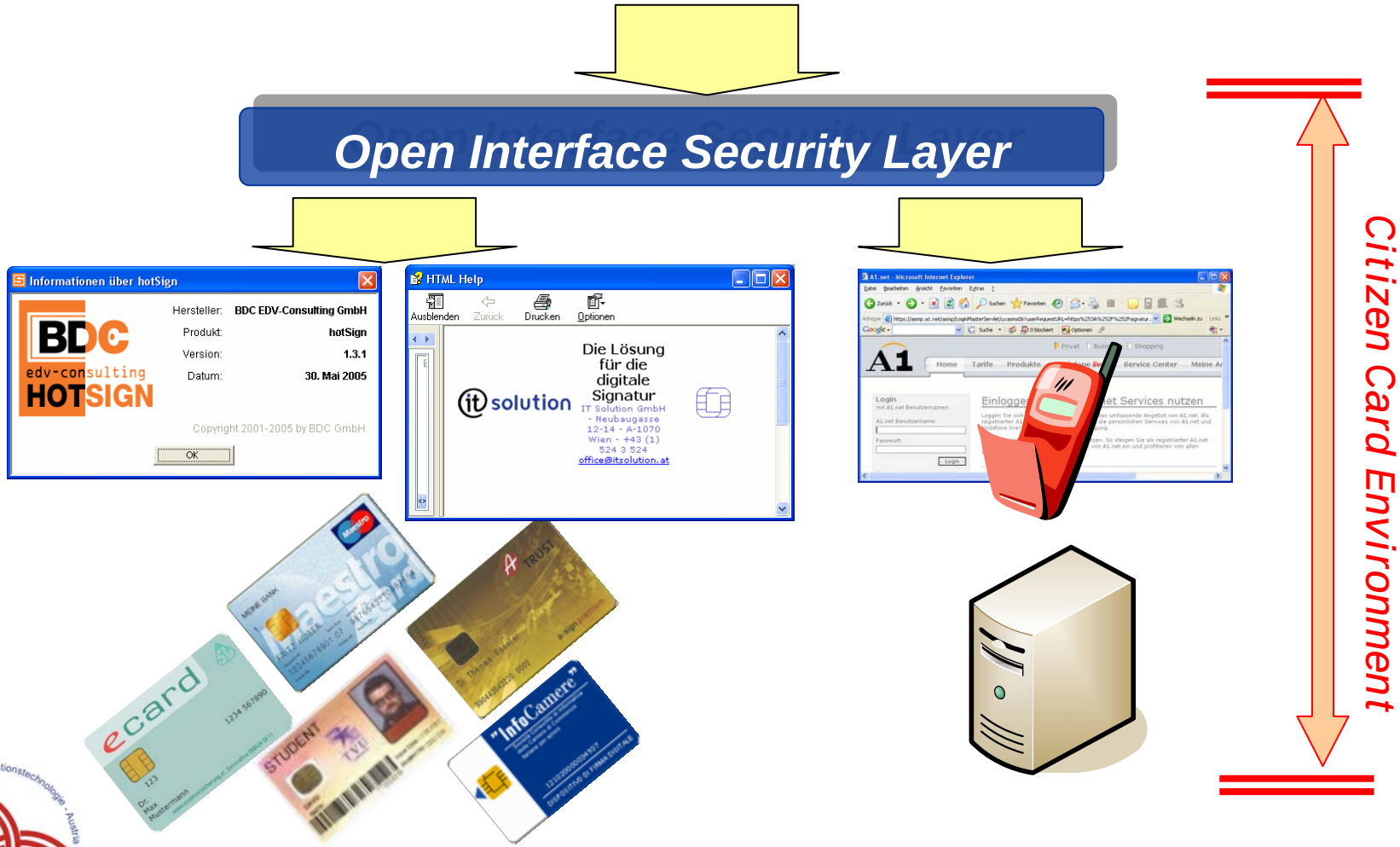
Health insurance cards:
SSCD, Rollout Mai-Nov. 2005
100 % coverage (8 Mio.) reached end of Nov. 2005

Mobile phones:
each mobile phone
(since March 2004)

Further initiatives:
- CSP signature cards
- Public servant service card
- Student service cards, etc.

ID Cards?

Status in Austria: Integration of Technologies



EU Large Scale Pilots

EU AT

STATE OF THE PLAY: The Austrian EU presidency together with the Commission and the MS has worked out the frame for a call. The commission now prepares the call until 4/2007. AT, BE, NL, PT look for further app. seven in total MS to competently answer the call.

Objective 1.2 Towards pan-European recognition of electronic IDs (eIDs)

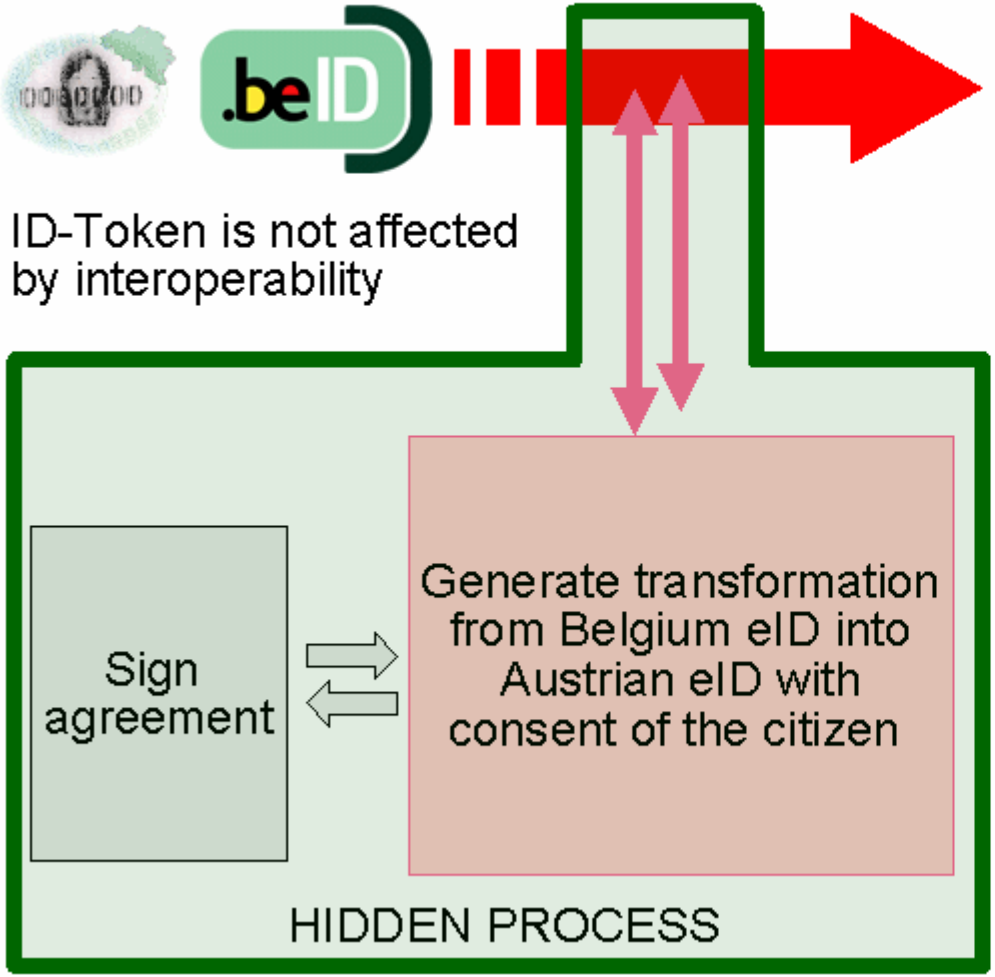
Objective

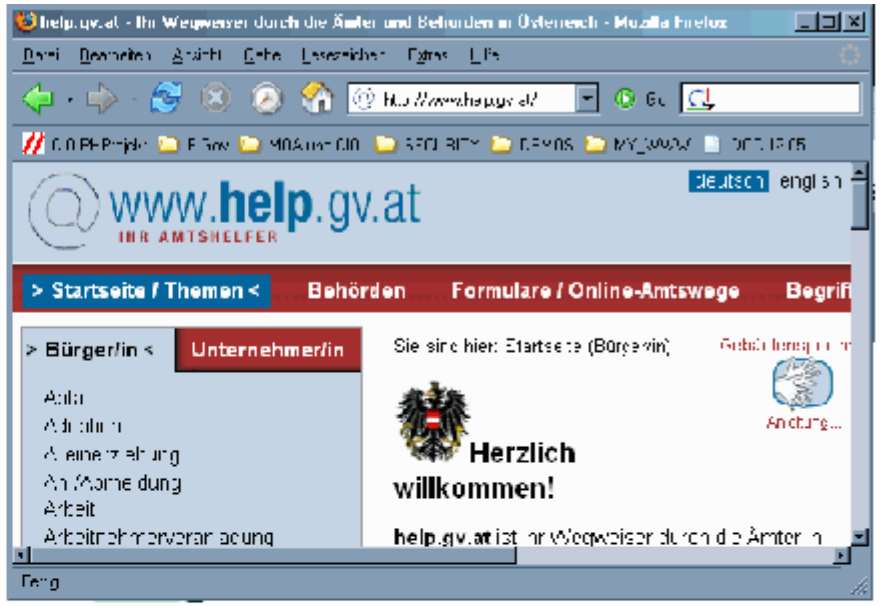
The objective is the implementation of an EU wide interoperable system for recognition of eID and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State. This will facilitate for instance, company registration or procurement, mobile working, social security, taxation or health reimbursement. It will open the door to new business opportunities, advance the internal market and facilitate the free movement of citizens.

Support will be provided to one pilot action that should

– Contribute to accelerate the deployment of eID for public services, while ensuring co-ordination between national and EC initiatives in the field and support federated eID management schemes across Europe based on open standard definitions where

Good Practice – Large Scale Piloting

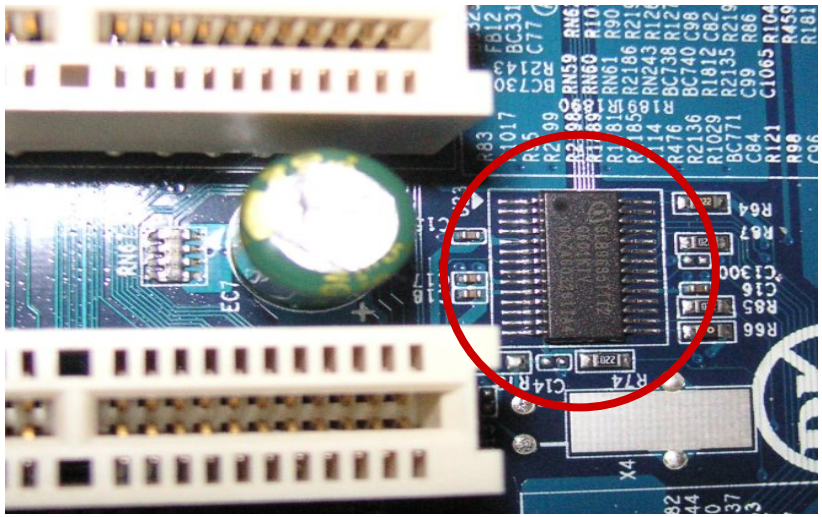




Application is not affected by interoperability

LEGAL AGREEMENTS?
TECHNICAL INTEROPERABILTY?
……

PART II: Trusted Computing



- Problem Statement
- TCG Basics
- Secure Boot
- Key Management

Problem Statement

- IT security requires certain credentials
  - encryption/signature keys, passwords, PINs, …
- Protection solely based on software mechanisms is vulnerable to attacks
  - Worms, viruses, spyware, hackers …
- Hardware modules are a solution
  - Smartcards and readers are still a cost factor
  - Integration into platform (PC, laptop, mobile phone …) desirable

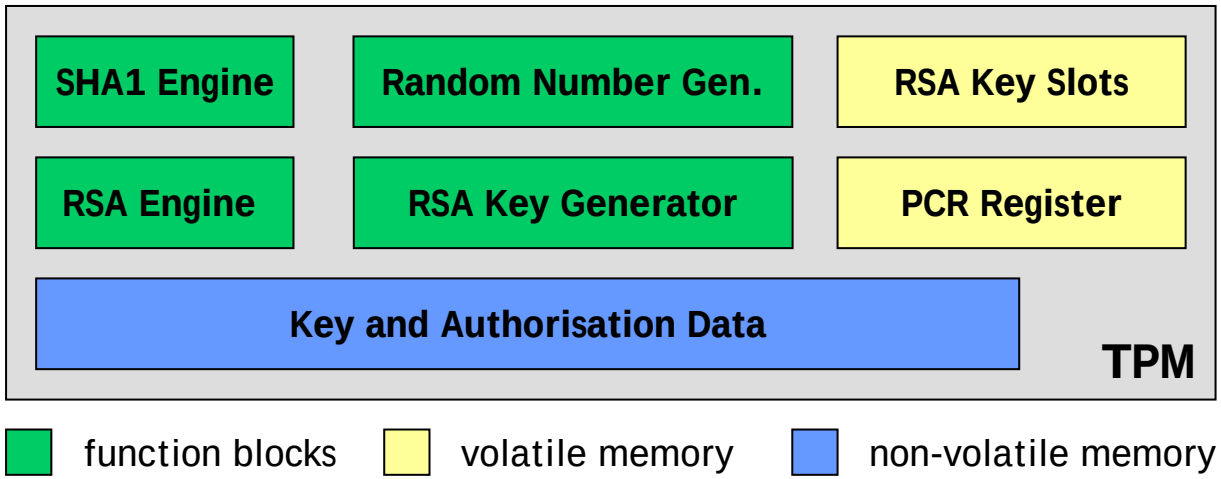
Trusted Computing - Organisation

- Until 1999 known as TCPA – Trusted Computing Platform Alliance
  - Compaq, HP, IBM, Microsoft (others followed)
- 2003+: TCG – Trusted Computing Group
  - Promotors: AMD, HP, IBM, Infineon, Intel, Lenovo, Microsoft, Sun
  - Various membership levels down to academic observes

TPM Chip – Basic Component

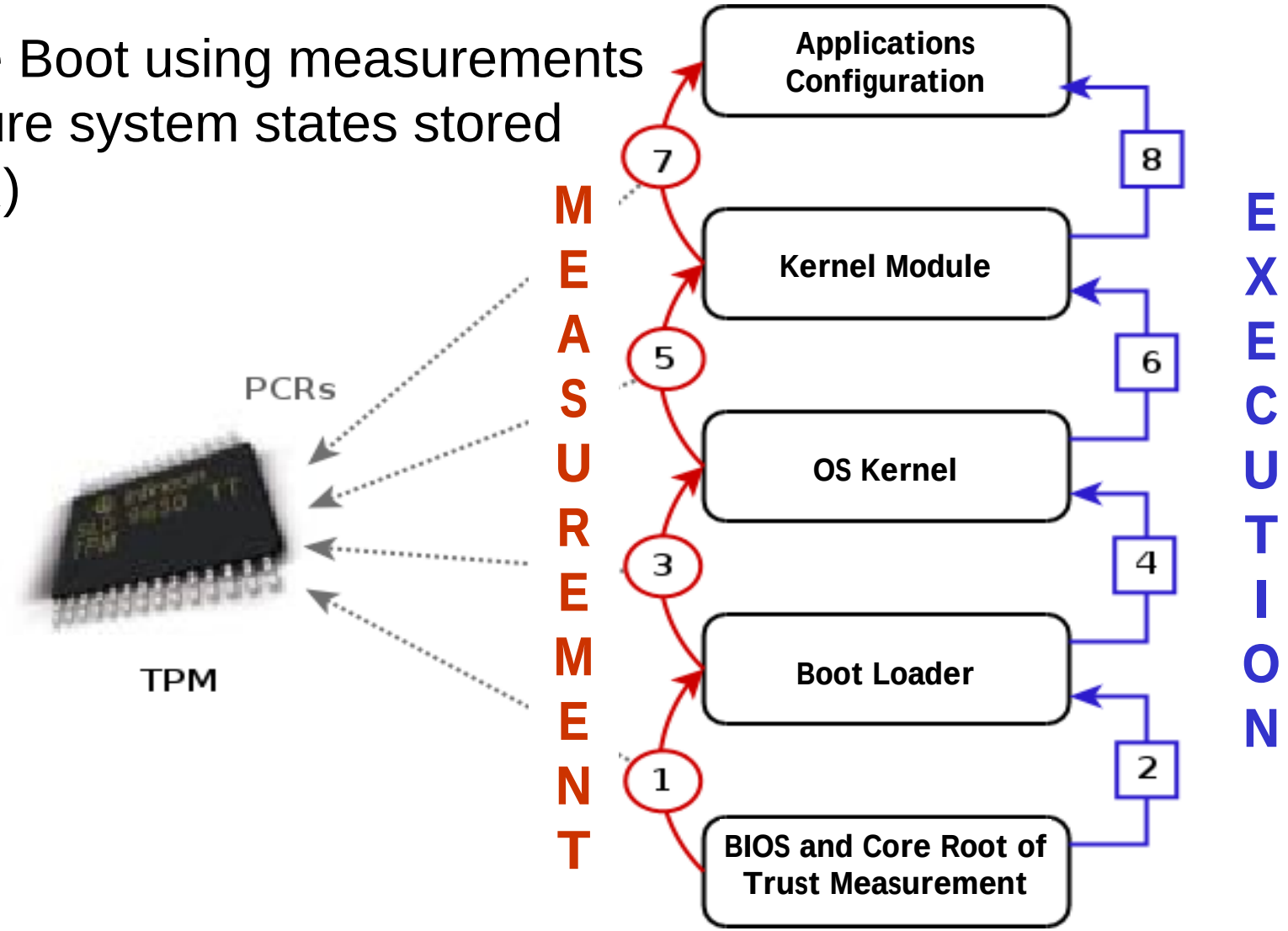
© Infineon

- TPM – Trusted Platform Module
  - Integrated into new motherboards – cannot be removed
  - Nowadays, already millions of PCs shipped with TPMs
- Major functions
  - Trusted Boot – Chain of Trust
  - Crypto: Encryption, Digital Signatures

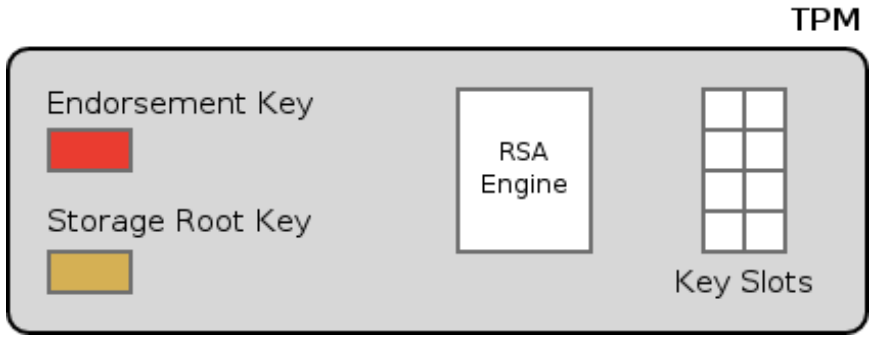


Chain of Trust and Trusted Boot

Secure Boot using measurements of secure system states stored in PCR)

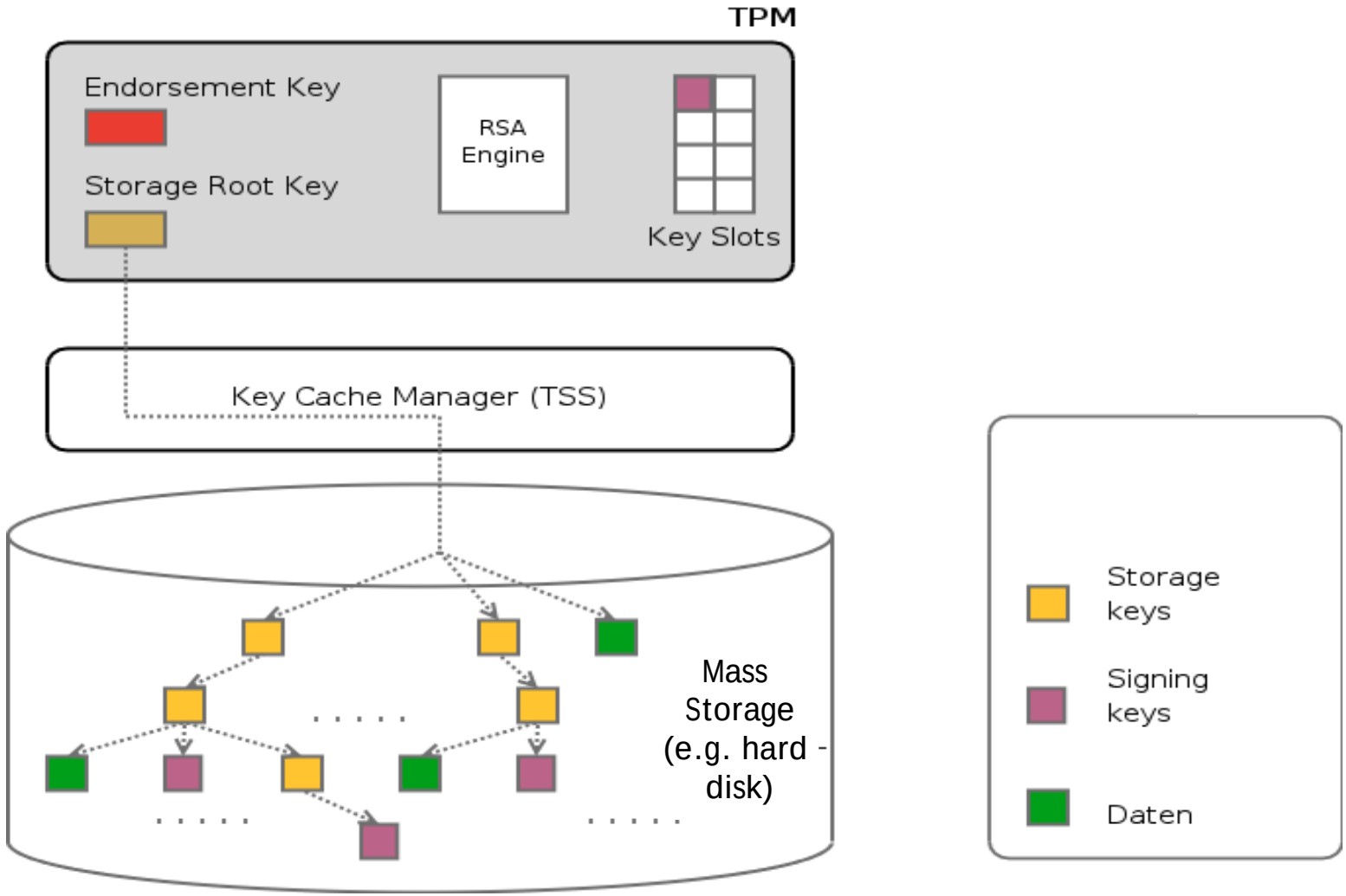


Key Management (1/3)

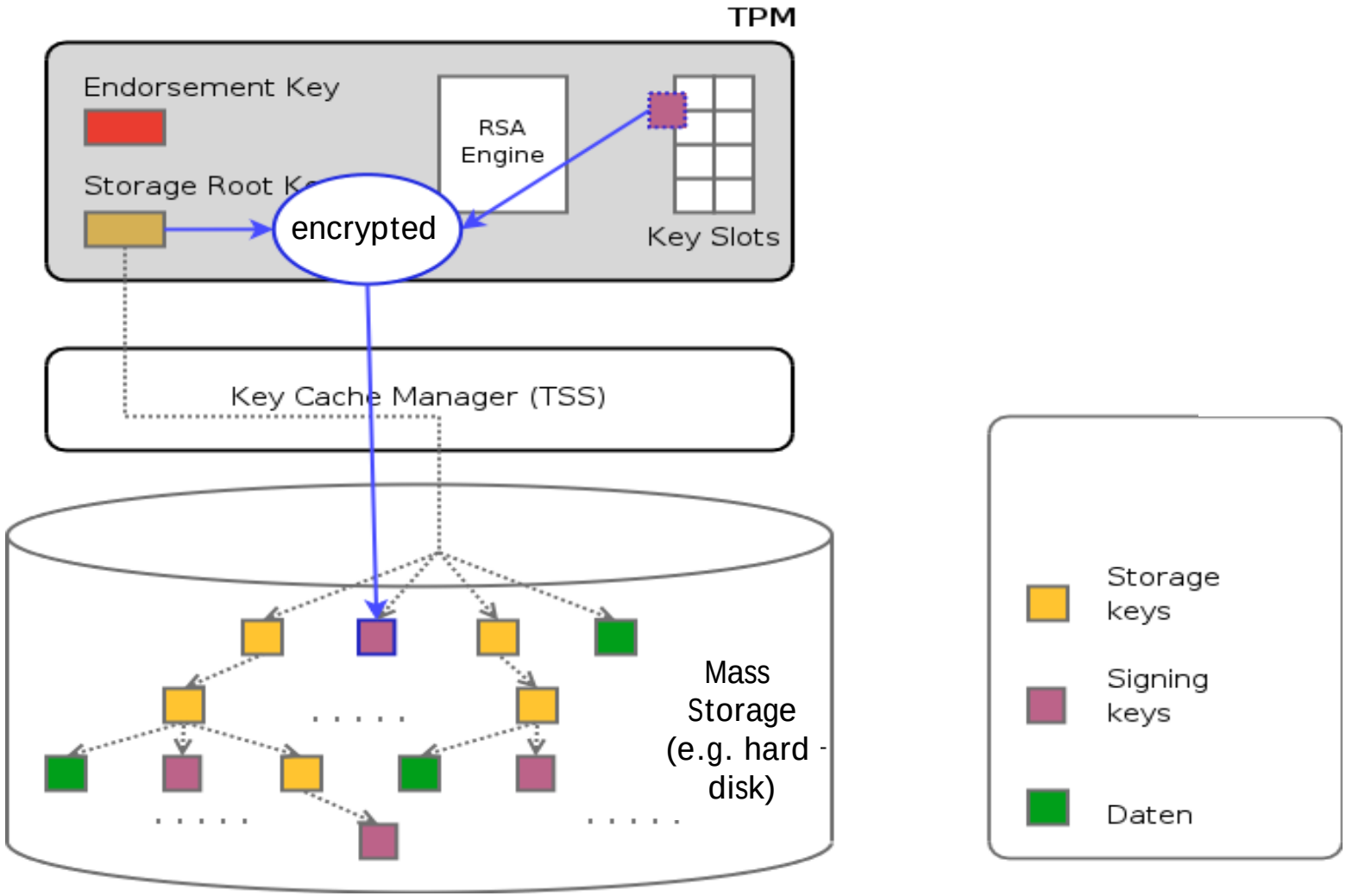


- Endorsement Key and Storage Root Key are the only keys that are stored in the TPM
- Arbitrary further keys (e.g. for encryption or digital signatures) can be loaded to the TPM
  - Secured by the TPM's SRK

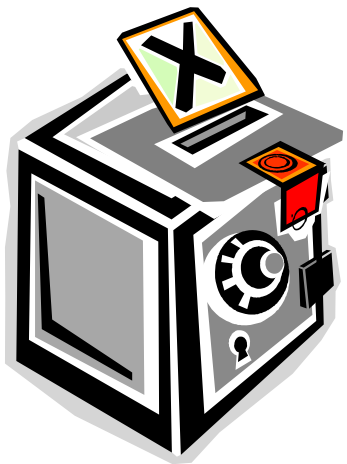
Key Management (2/3)



Key Management (3/3)



Conclusions



Two enabling technologies will be broadly available in the next 5-8 years

- Electronic Identities
  - Backed by high-quality national identity bases
- Trusted Computing
  - Shipment of PCs with TPMs started
  - Operating Systems will increasingly support Trusted Computing

both expected to influence the e-voting security landscape

Thank you for Your attention!

http://www.a-sit.at
http://www.buergerkarte.at

Herbert.Leitold@a-sit.at