# Can eID card make life easier and more secure?

Michal Ševčík
Industry Solution Consultant
Hewlett-Packard, Slovakia
ITAPA, November 9th, 2010

# Content

- eID Primary Functions
- eID Privacy Features and Security Threats
- Identification / Authentication using eID
- Conclusions and Outlook

# New German eID


**Standard:**

- All non-biometric data electronically stored

- Digital photograph (only for entitled authorities, e.g. police and border control)

**Upon request (no extra charge):**

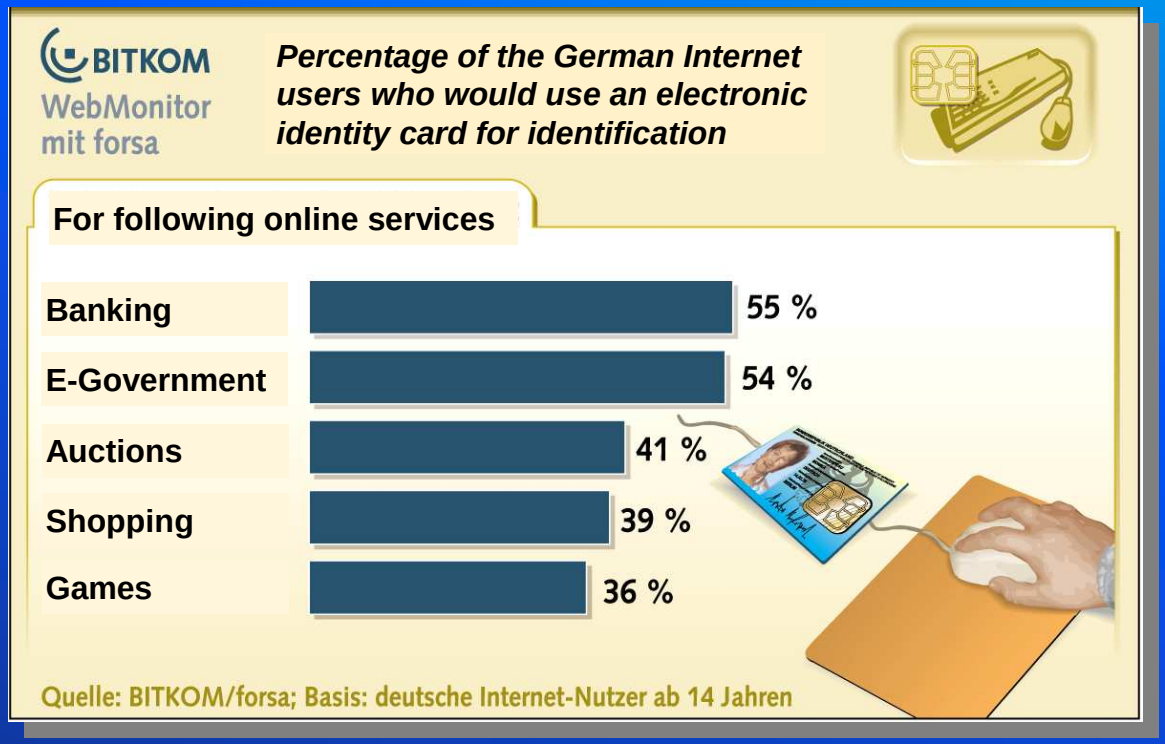
- electronic ID function (access only to certain non-biometric data fields)

- Two fingerprints
  (only for entitled authorities, e.g. police and border control)

**Upon request (extra costs):**

- Qualified electronic signature

# Demand for a Secure Identification Online



# Basic Terminology

- **Identification** is a process to recognize an entity from the real world and to establish its identity.
- **Identification of the person** is submitting information related to that person (eg name), which are necessary for its unambiguous designations in relation to the system (eg hospital IS)

# Basic Terminology cont.

- **Authentication of the person** is a process of verifying the authenticity of the declared identity of the person. Authentication approaches could be based on:
  - **what the person knows** - knowledge of passwords, access codes, PINs etc. - password authentication
  - **what the person has** - an identity card, passport, magnetic card, etc. – token authentication
  - **what the person is** - authentication using biometric parameters (fingerprint, face or palms biometrics,…) - biometric authentication

# eID Primary and Extra Functions


- Primary functions
  - Identification (in real as well as electronic world)
  - Authentication (in real as well as electronic world)
  - Qualified Digital Signature (QC)
  - Encryption

# eID Primary and Extra Functions


- Extra functions / Other applications
  - Restricted Identity / Pseudonyms / Sector Identifiers
  - Data comparison (e.g. age verification, document expiry)
  - Data & Application modification (e.g. holder's permanent address, health insurance, certificates)
  - Emergency data set provisioning
  - Special data provisioning (health insurance membership)

# Compliance with Legislation and Standards

- **EU Directive** 95/46/EC (data protection)
- No enforced standard yet (ECC)
- Different initiatives:
  - **BSI TR-03110**, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)Version 2.05
  - **CEN/TS 15480-1**, Identification card systems – European Citizen Card – Part 1: Physical, electrical and transport protocol characteristics
  - **CEN/TS 15480-2**, Identification card systems – European Citizen Card – Part 2: Logical data structures and card services
  - **prEN 14890** Application interface for smart cards used as secured signature creation devices (part 1 basic requirements, part 2 additional services)
- **ENISA** recommendations/reports

# eID Card Practical Use

**Age verification** - to verify whether a person is older or younger than a given age to get access to age-restricted services or products

**Address verification** - to verify whether a person lives in a certain area or not to gain access to locally restricted services


**Registration** - to give non-biometric data for e-business (e.g. first name, surname, address)

**Pseudonymity and registration** - to get access to social e-communities (e.g. weblog, bulletin board, web album)

**Web forms** - automated fill-in function (to avoid typing errors and to save time)

**Access verification** - to get admittance to restricted areas (e.g. access to fair grounds, to company premises)

# Contact vs Contact-less Platform

## Contact-less Platform

+

- Technology of the future
- Higher comfort
- Durability / Longer Lifetime
- Memory, Speed

-

- Special PED reader QES certified

## Contact Platform

+

- Proven Technology in EU/SK
- Readers availability
- Personalization reliability

-

- Limited usage

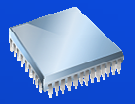
# eID – Security Protocols in Context (GAP)

Chip and eService provider connected via network

1. PACE (contactless chip)
   1. User terminal requires PIN
   2. After successful PIN verification secure messaging is setup to read data from chip
2. eService Provider (Terminal) Authentication

   1. CV certificate is shown and provider is being authenticated with corresponding secret key
   2. After successful certificate verification access to chip data is granted
3. Passive Authentication

   Security object verification is performed to confirm integrity of chip data
4. Chip Authentication (authenticity of chip&data)



   Chip restarts secure messaging between chip and eService provider

# eID – Security Protocols Applications

- Trusted provisioning of electronic identity (identification, authentication) for citizens with regard to eGovernment, eHealth, eBusiness, eBanking
- Document Verification
- Access Control regarding data modification
- Access Control regarding post-personalization
- eID concept guarantees a high level of card holder's data security
  - Reading data from eID card only after card holder's explicit consent via PIN
  - Data from eID card may be required only by certified service providers
  - Data from eID chip are transmitted to a service provider via strongly secured channel

# eID – Privacy Features

- Access control mechanisms
- Secure communication between the card, the middleware and the server
- Selective Disclosure *(EU data protection, Directive 95/46/EC)*
- Verify-only mode
- Privacy-respecting use of unique identifiers
- Domain-specific UIDs (or sector-specific UIDs or sector-specific personal identifiers)
- Pseudonymous authentication

# Security Threats

- Counterfeiting ***(card security features)***
- Skimming ***(BAC, PACE, EAC)***
- Eavesdropping ***(BAC, PACE, EAC)***
- Document fingerprinting ***(not a unique CA or AA key pair)***
- Cloning ***(CA or AA)***
- Alteration ***(PA)***
- Substitution ***(PA)***

# Security Threats cont.

- Man-in-the-middle attacks ***(CA + TA = EAC)***
- Signing a bogus document ***(EAC, QES legislation)***
- User authenticates to a bogus server ***(TA)***
- Loss or Theft of card ***(PIN, PACE)***
- Physical Attacks ***(chip  CC EAL 5)***
- Side-Channel Attacks ***(reader & chip certification CC EAL 5)***
- Location Tracking ***(RI, pseudonyms)***
- Behavioural Profiling ***(RI, pseudonyms)***
- Proving the trustworthiness of personal information to a third party ***(EAC)***

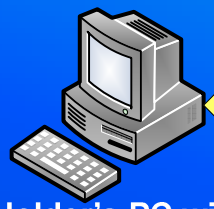
 

# Classification of eServices

- Anonymous – access to public information
- Authenticated – access to own data
- Authorized – access to registers
- QES required – modification of data; transactions

# eService – Distributed Alt.

Holder's PC with chip communication middleware

SSL / TLS

eService Provider

Certify provider

PKI for verification

DVCA

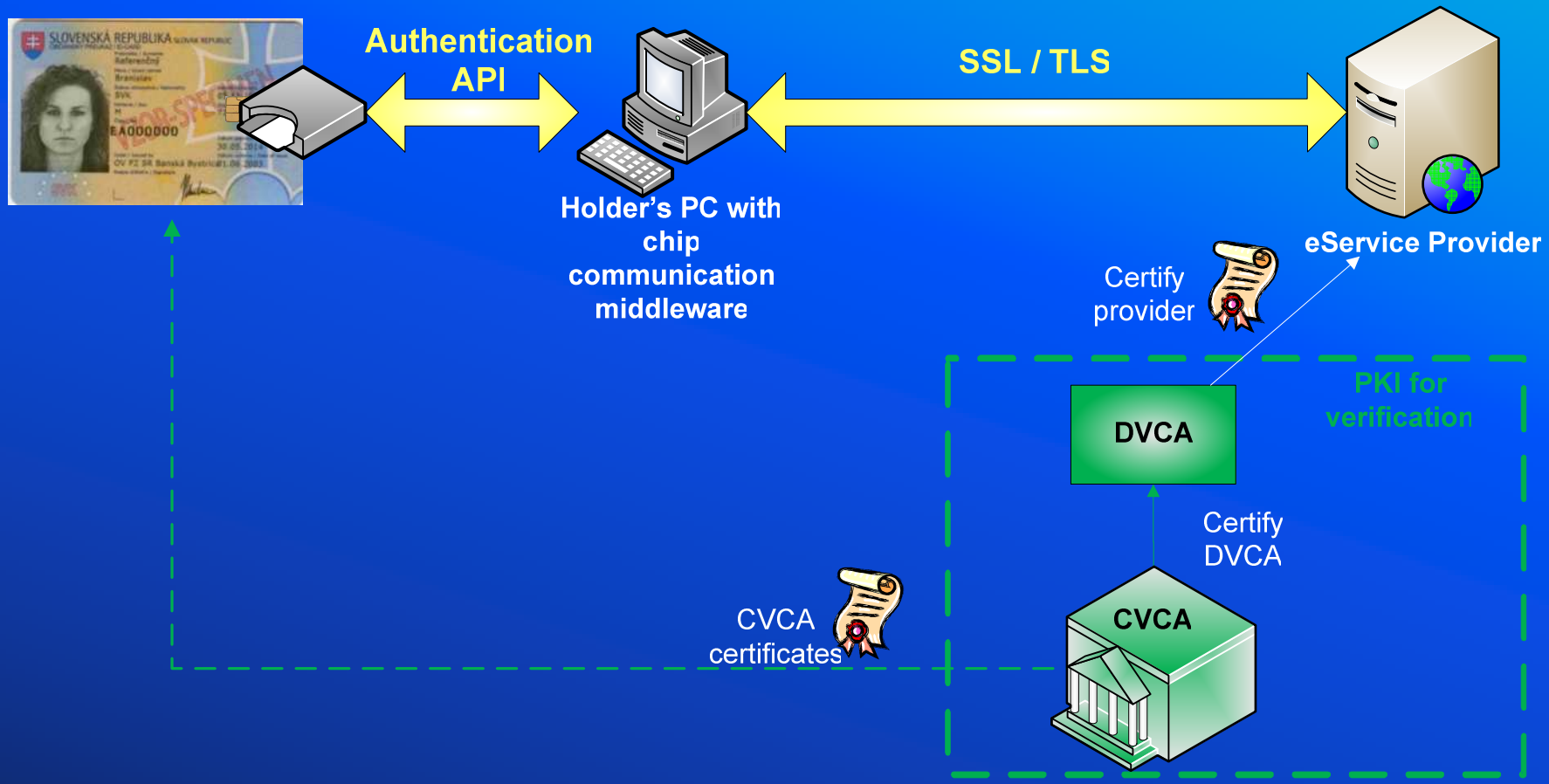
Certify DVCA

CVCA

CVCA certificates

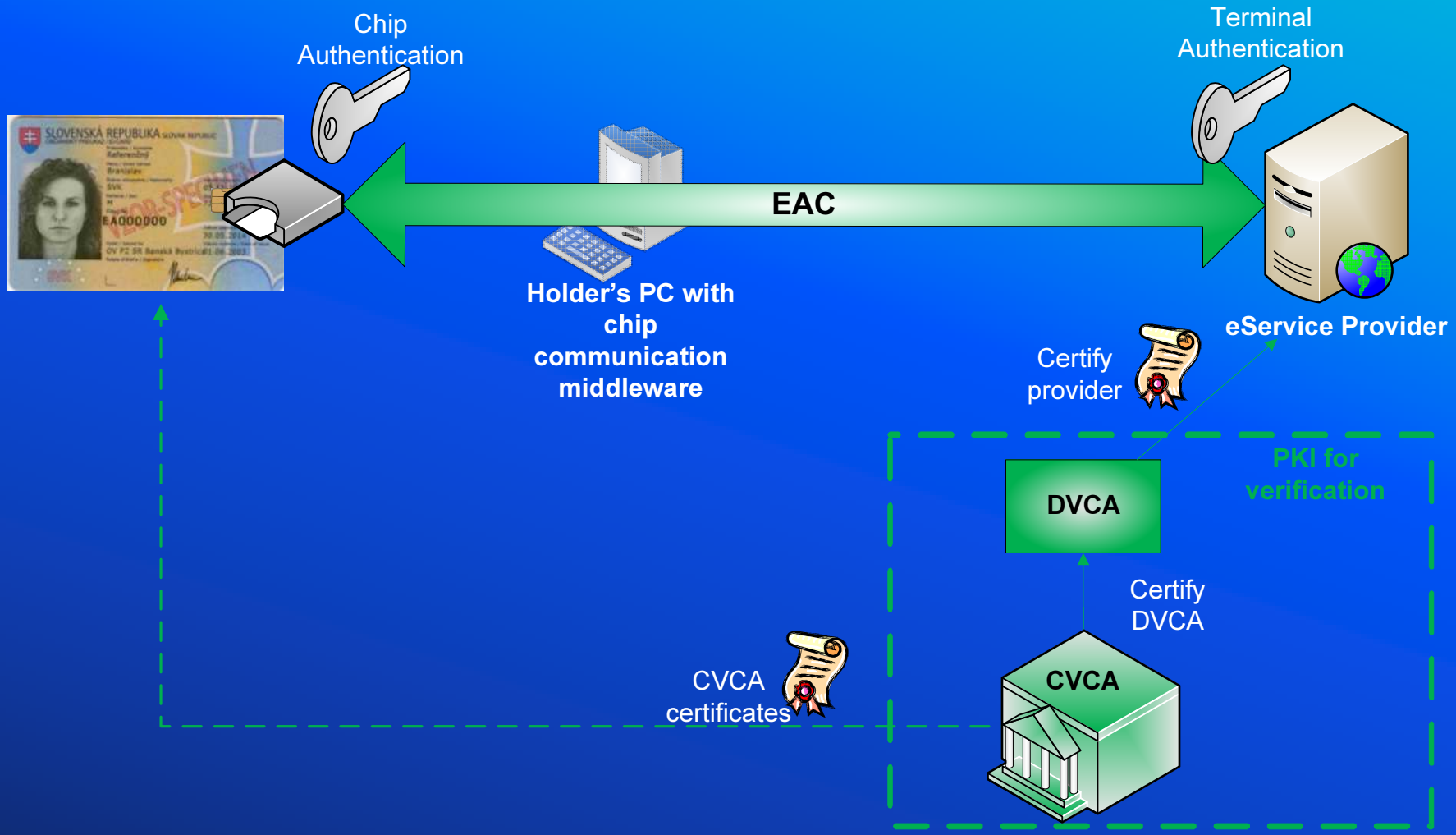
 

# eService – Distributed Alt.



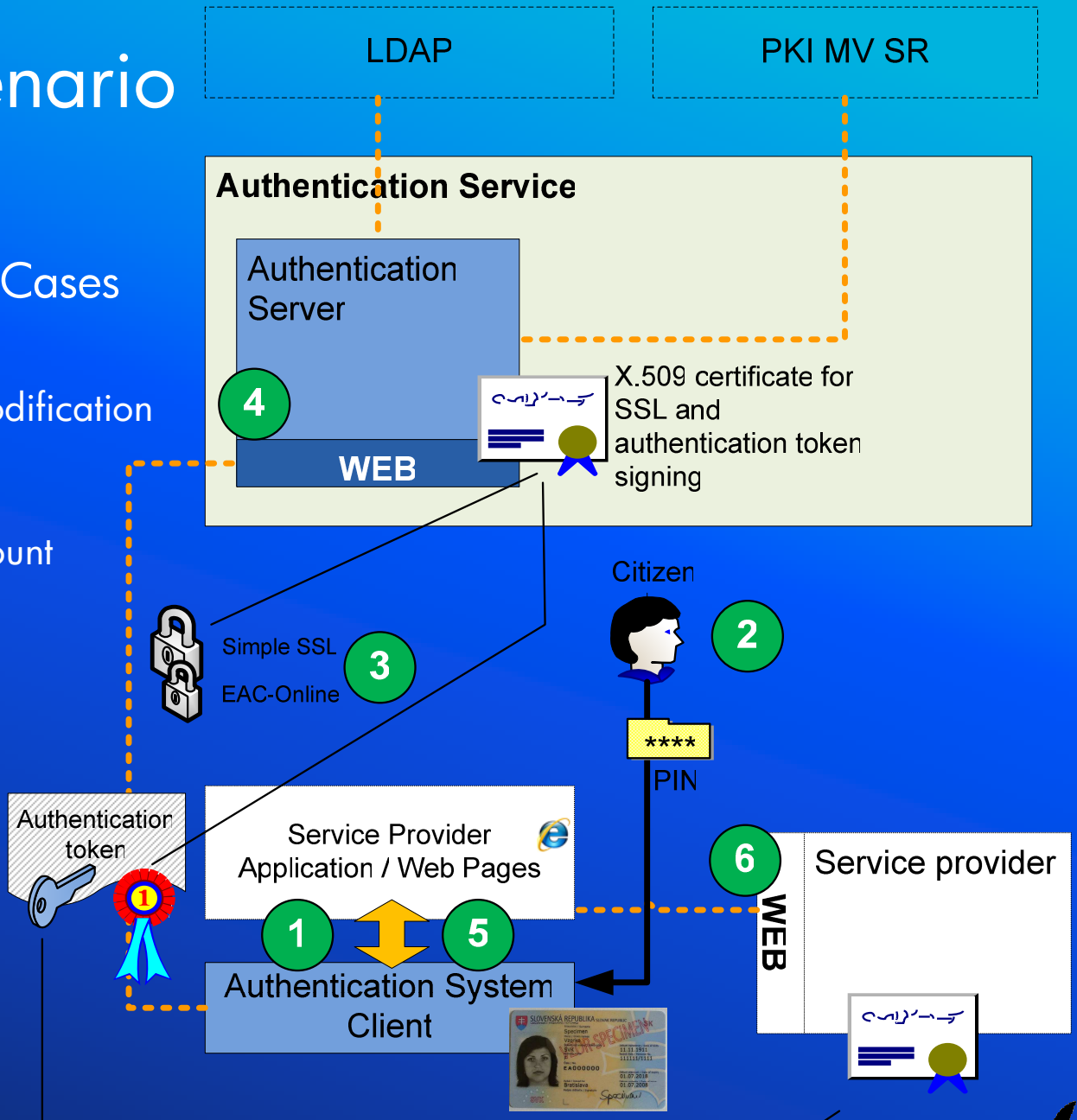
# eService – Distributed Alt.



# eService Scenario Central Alt.

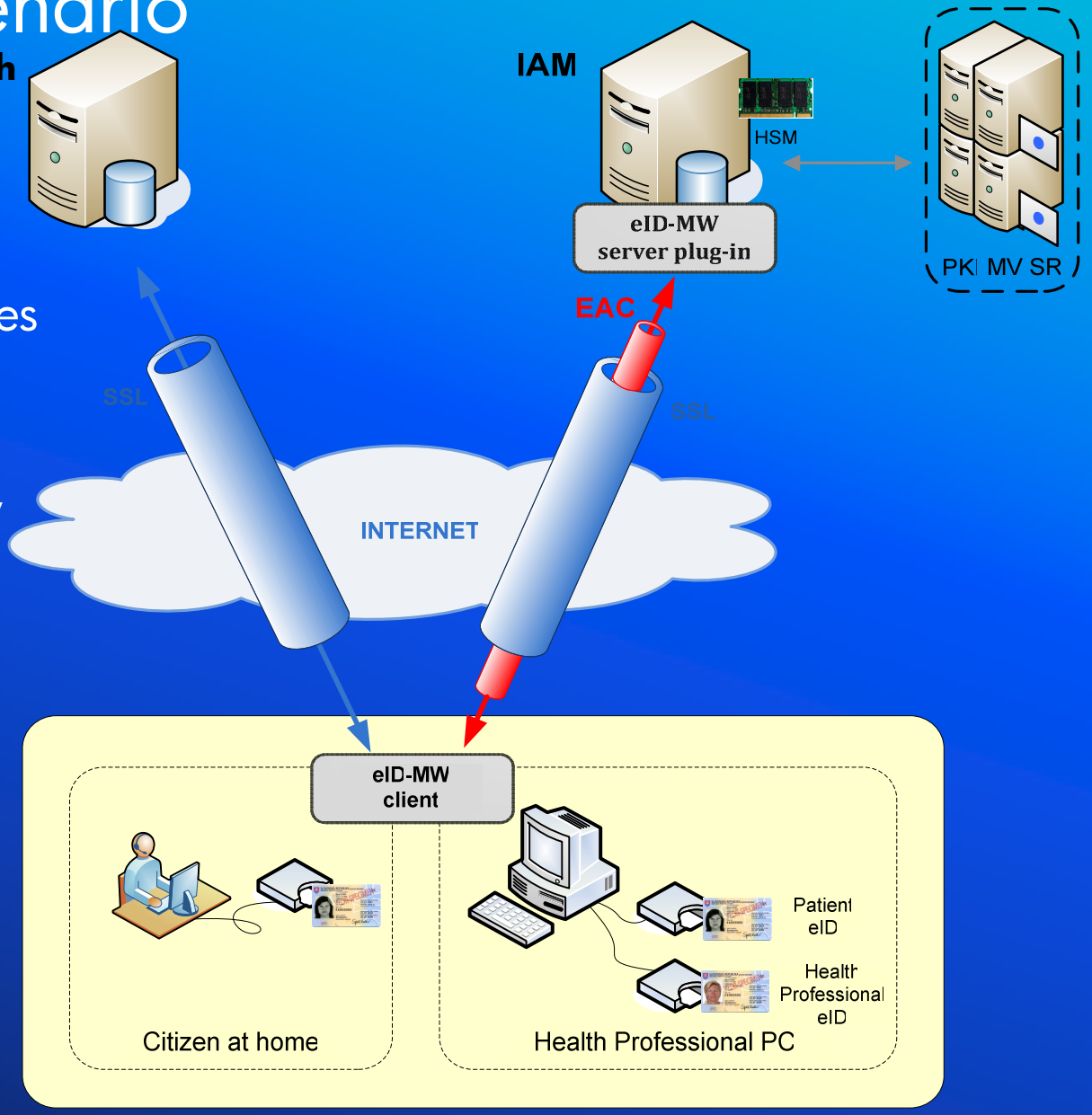
- eGovernment Use Cases
  - Inquiry
  - Data submission / modification
- eBanking
  - Opening a bank account
  - Transferring money from a bank account



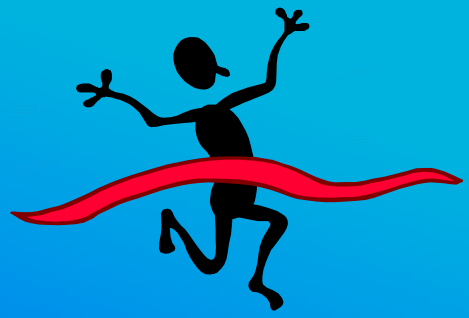
# eHealth Scenario

- eHealth Use Cases
  - Visiting a doctor
  - Diagnostics
  - Visiting a pharmacy
  - Research
  - …



# Conclusions and Outlook



- SK is 10 years behind, no need to start with „cheques“
- Open and multi-application concept
- Security and privacy are the biggest concerns
- Compatibility with ECC profile
- Usage for different sectors: eGovernment, eHealth, eBanking, eVoting, Social Networks, Municipalities, Corparate…