

# From the eCard-API-Framework towards a comprehensive eID-Framework for Europe



**Dr. Detlef Hühnlein**  
secunet Security Networks AG, Germany

Manuel Bach  
Federal Office for Information Security, Germany

## Agenda

- ❑ The German eCard-Strategy
- ❑ The eCard-API-Framework
- ❑ Towards a comprehensive eID-Framework for Europe
- ❑ Summary

## Agenda

- **The German eCard-Strategy**
- The eCard-API-Framework
- Towards a comprehensive eID-Framework for Europe
- Summary

# Goals of the eCard-Strategy

- ❑ Harmonization of different eCard projects (ePA, eGK, eLena, ELSTER ...)
- ❑ Enable smart card interoperability (**arbitrary** cards, **arbitrary** applications, **one** interface)
- ❑ Making electronic services for eBusiness and eGovernment easy, cheap and secure.

# The eCard-Projects

## eCard-Strategy

**eGK**  
Authentication  
optional Signature



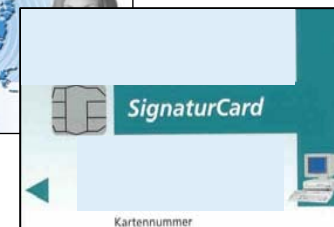
**ePA**  
Authentication  
optional Signature



**eLena  
(JobCard)**  
Signature



**ELSTER**  
Authentication  
Signature



# The eCard-API-Framework

## Agenda

- ❑ The German eCard-Strategy
- ❑ **The eCard-API-Framework**
  - ❑ **Architecture**
  - ❑ ISO/IEC 24727-3
  - ❑ Deployment Options
- ❑ Towards a comprehensive eID-Framework for Europe
- ❑ Summary

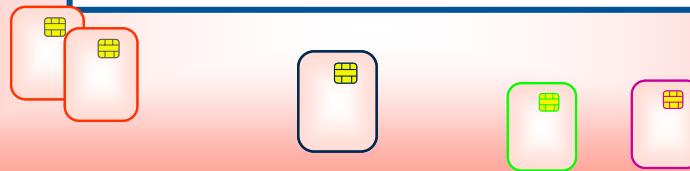
# The goal

arbitrary applications ...

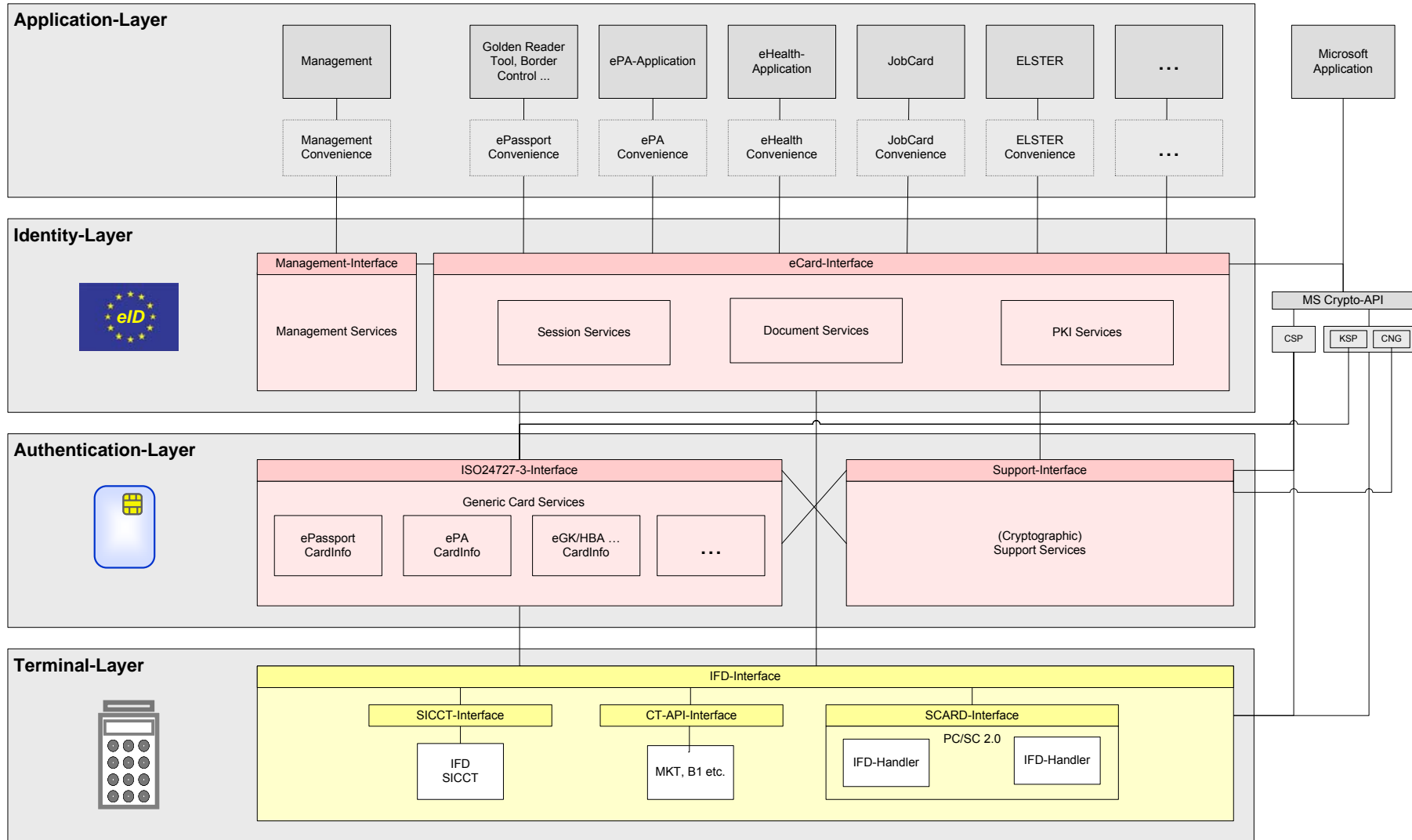


**eCard-API-Framework**

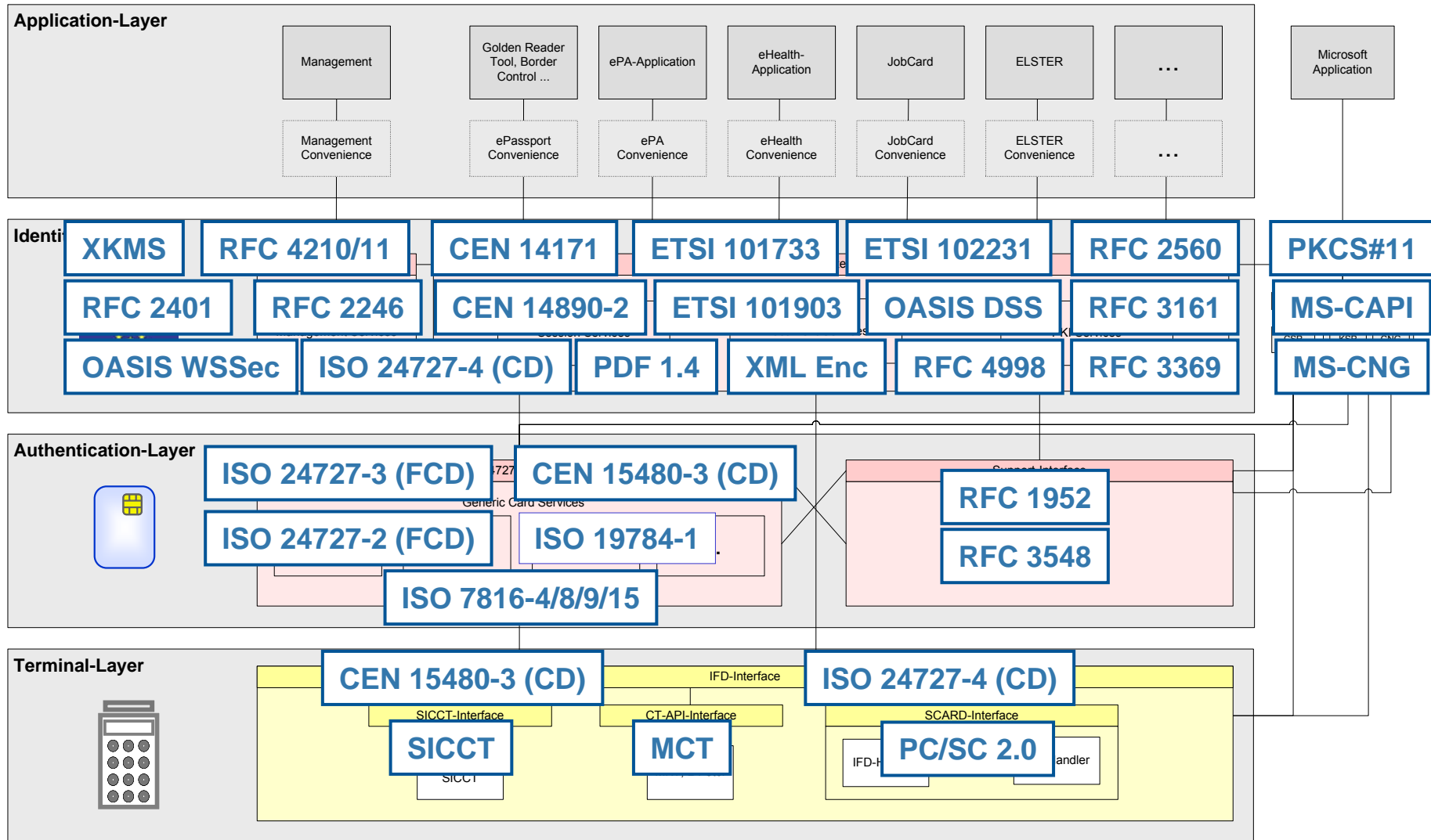
... use arbitrary smart cards and  
readers in a uniform and **easy** way



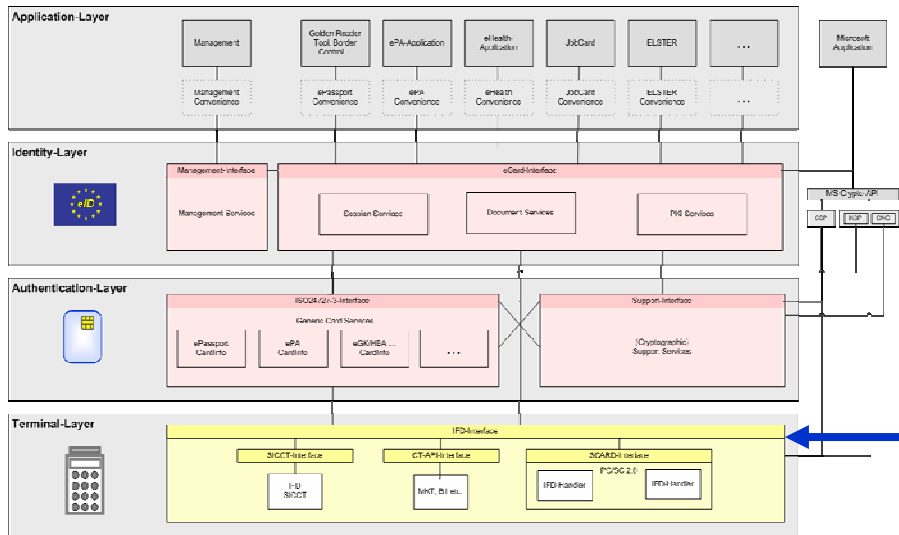
# eCard-API-Framework



# Standards



# Example: IFD-API



Recent agreement in  
CEN TC224 WG15 and  
ISO SC17 TF9 WG4

Reader-Interface  
(eCard-API, v0.6)

Card-Transport-Layer-Interface  
(Onom@topic)

Discussion  
in WG15

eCard-API, v0.8

Interface-Device-API

≈ PC/SC ++

≡

prCEN 15480-3

Discussion  
in WG4

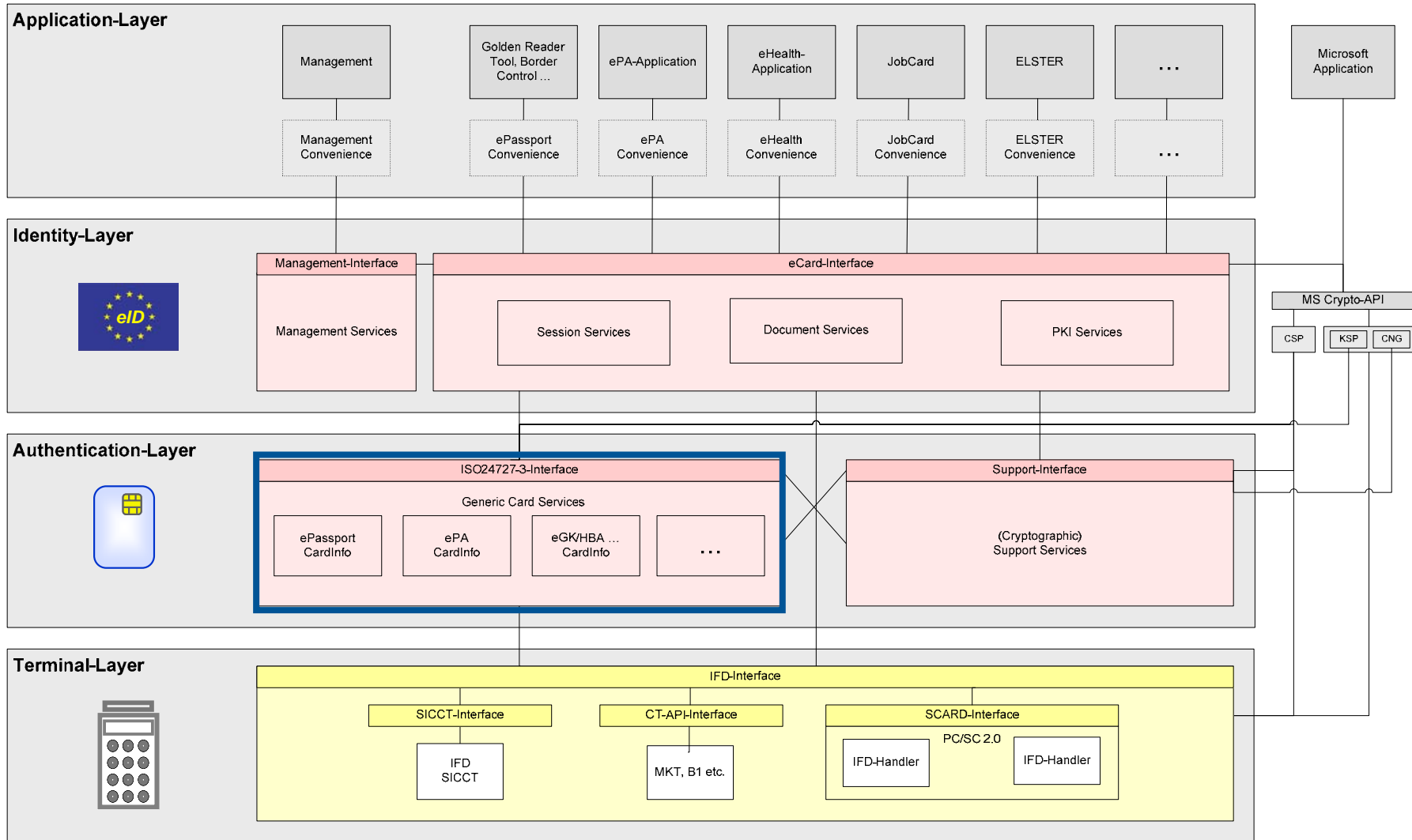
ISO/IEC24727-4



## Agenda

- ❑ The German eCard-Strategy
- ❑ **The eCard-API-Framework**
  - ❑ Architecture
  - ❑ **ISO/IEC 24727-3**
  - ❑ Deployment Options
- ❑ Towards a comprehensive eID-Framework for Europe
- ❑ Summary

# ISO/IEC 24727-3-Interface



# Functions of the ISO24727-3- Interface

## Card-application-service Access

- Initialize
- Terminate
- CardApplicationPath

## Connection-service

- CardApplicationConnect
- CardApplicationDisconnect
- CardApplicationStartSession
- CardApplicationEndSession

## Card-application service

- CardApplicationList
- CardApplicationCreate
- CardApplicationDelete
- CardApplicationServiceList
- CardApplicationServiceCreate
- CardApplicationServiceLoad
- CardApplicationServiceDelete
- CardApplicationServiceDescribe
- ExecuteAction

## Named data service

- DataSetList
- DataSetCreate
- DataSetSelect

- DataSetDelete
- DSIList
- DSICreate
- DSIDelete
- DSIRead
- DSIWrite

## Cryptographic service

- Encipher
- Decipher
- GetRandom
- Hash
- Sign
- VerifySignature
- VerifyCertificate

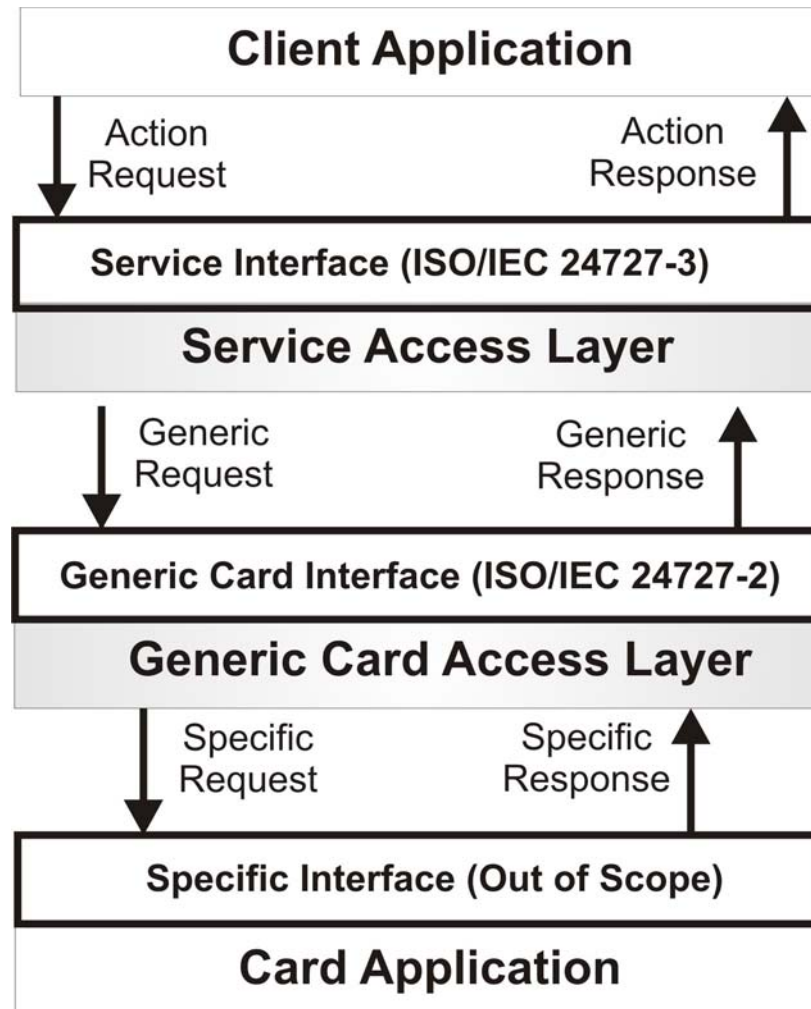
## Differential-identity service

- DIDList
- DIDCreate
- DIDGet
- DIDUpdate
- DIDDelete
- DIDAuthenticate

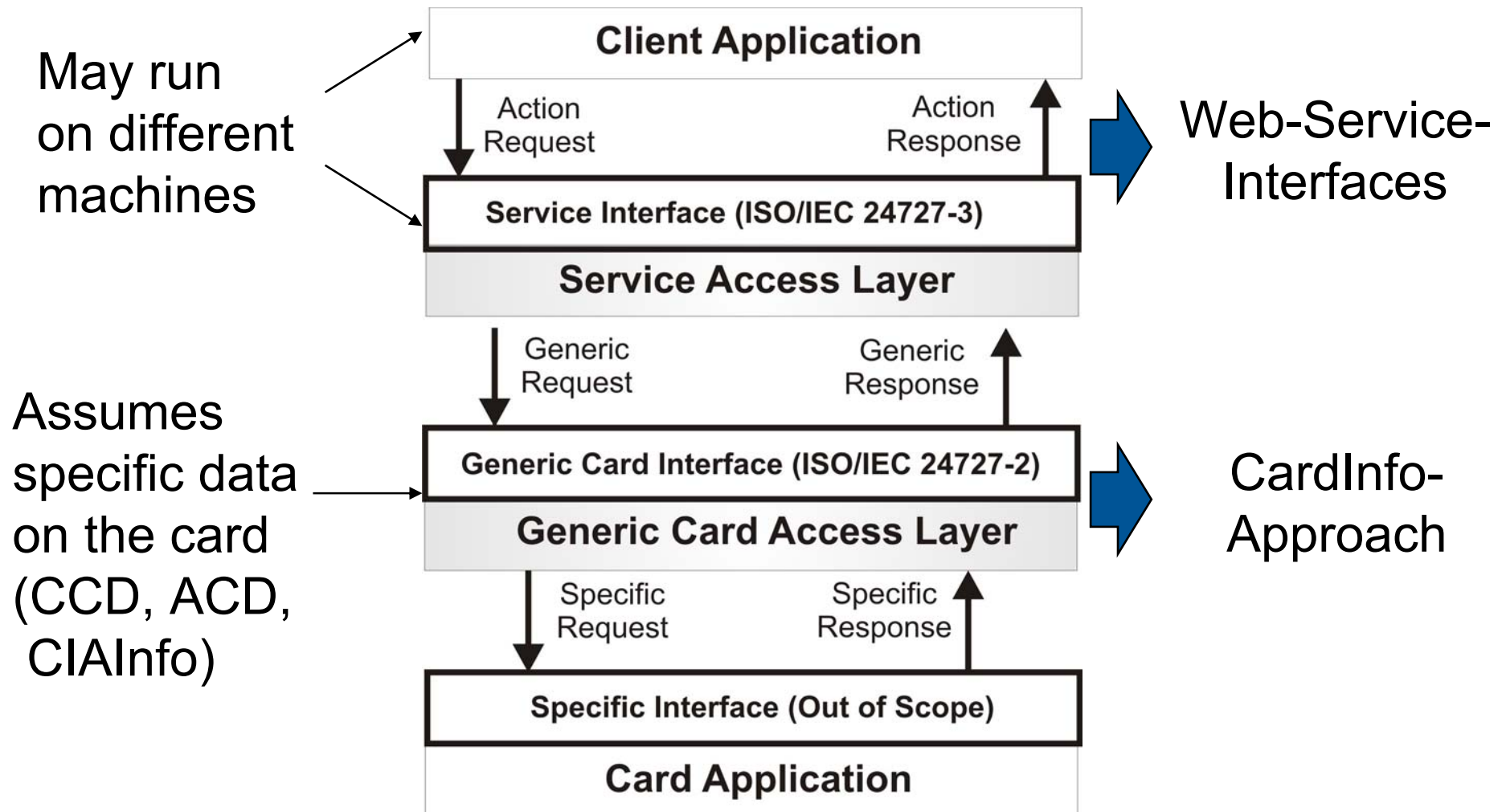
## Authorization service

- ACLList
- ACLModify

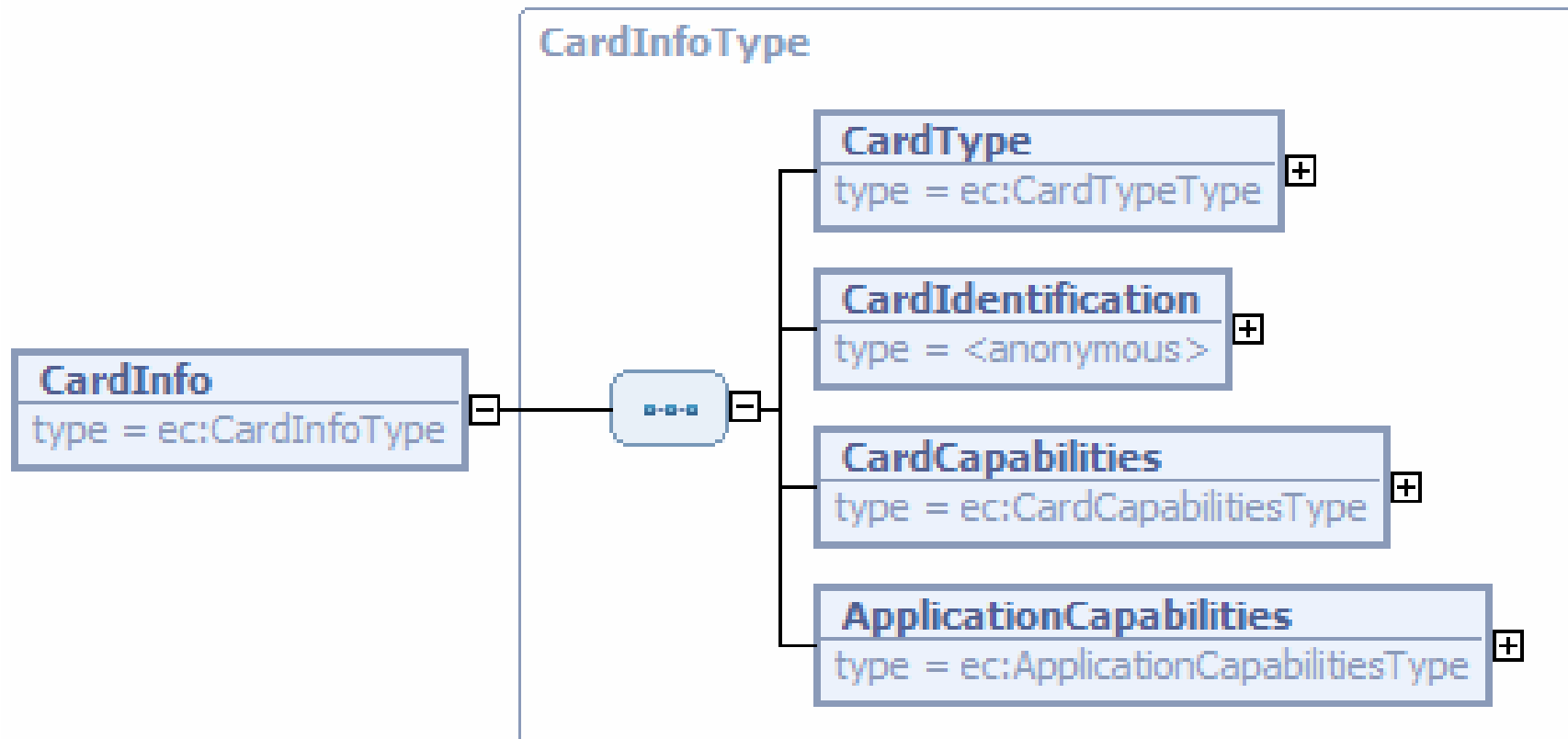
# ISO/IEC 24727-Architecture



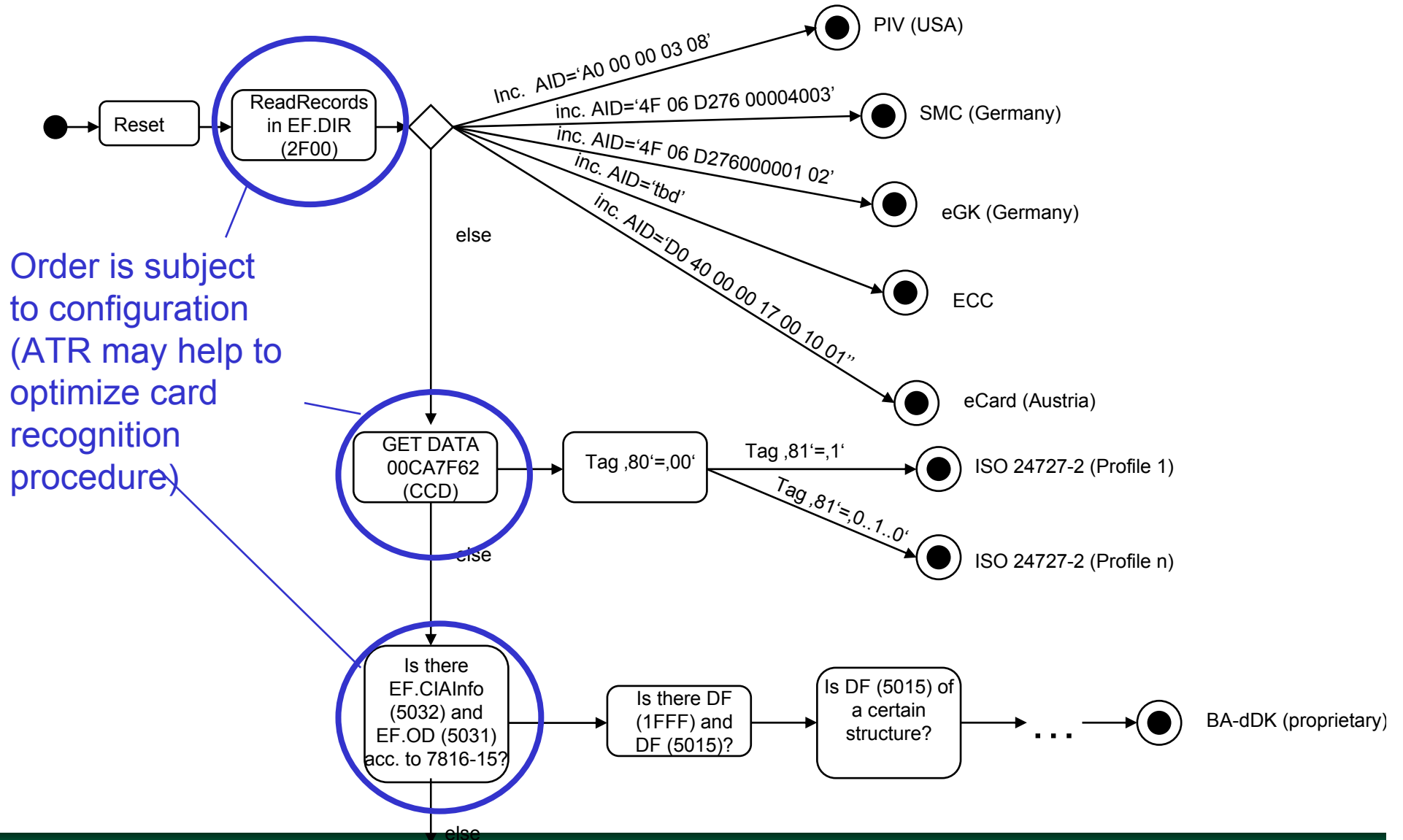
## ... and related issues



# CardInfo

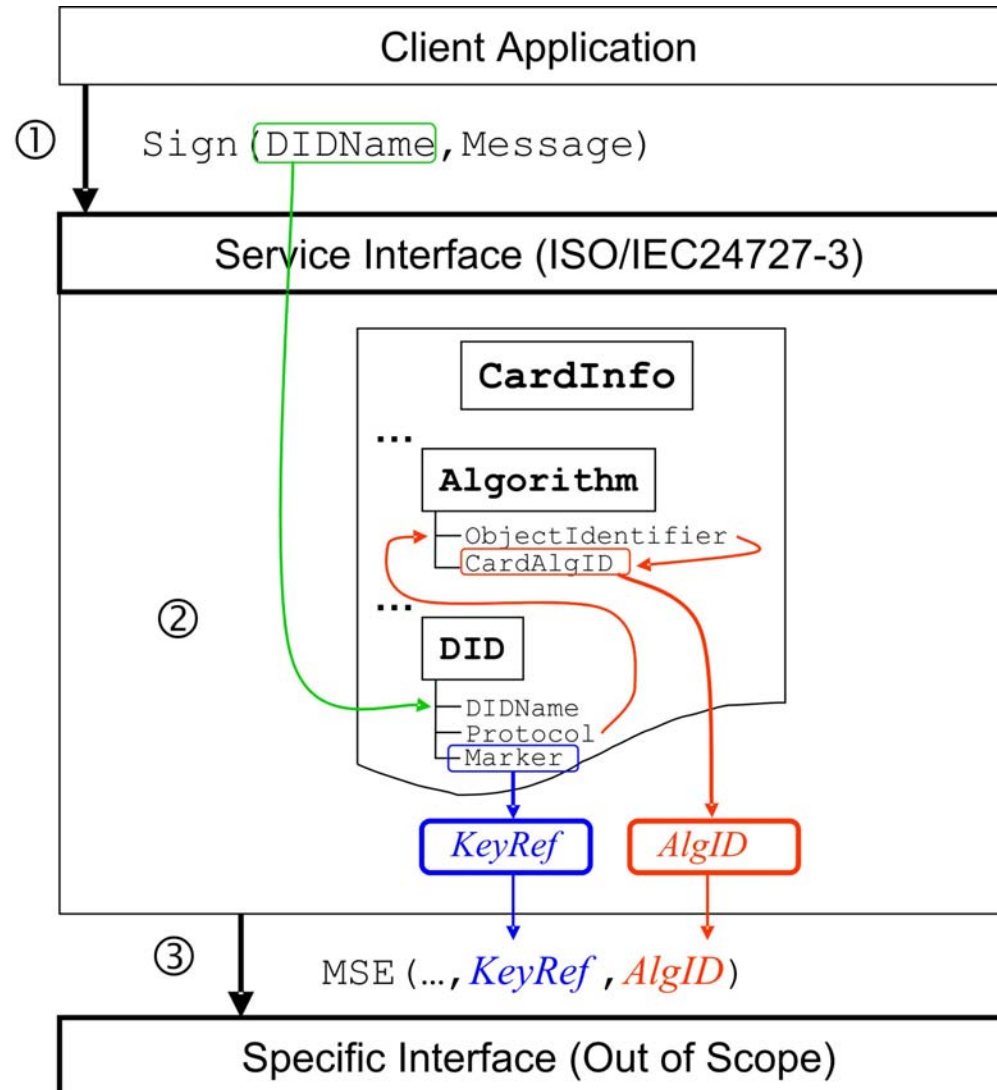


# Example for a „decision tree“



Order is subject to configuration (ATR may help to optimize card recognition procedure)

# Mapping of generic requests to card-specific APDUs



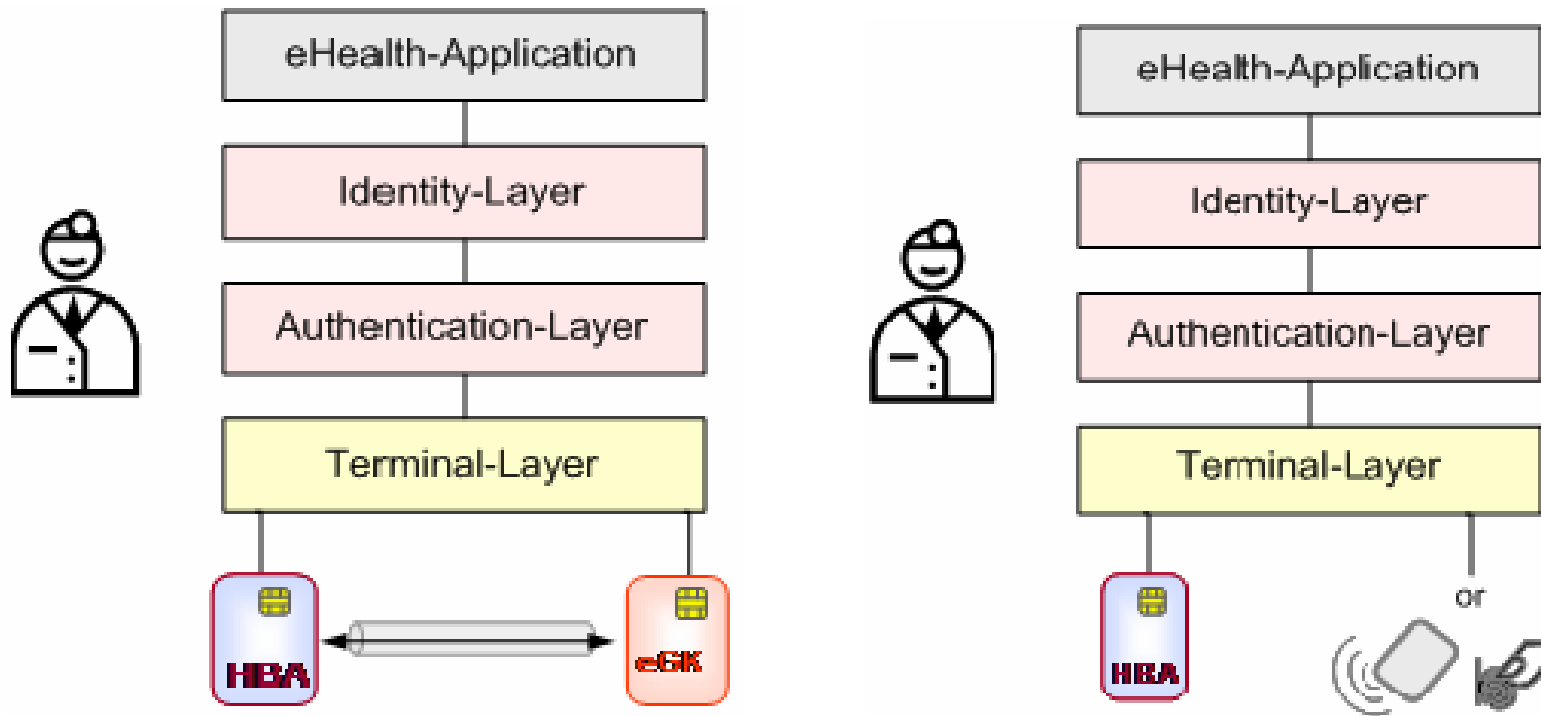
# Advantages of the approach

- ❑ It is possible to support **arbitrary** smart cards **without** changing the executable code of the middleware
  - ❑ The middleware can be evaluated and certified once and for all.
  - ❑ It is possible to support
    - ❑ the European Citizen Card,
    - ❑ cards with the generic card interface according to ISO/IEC 24727-2
    - ❑ **and arbitrary cards** (e.g. SSCDs) which are already distributed
- ❑ It is easy to migrate from one card version to another, as it is only necessary to provide an updated XML-file.

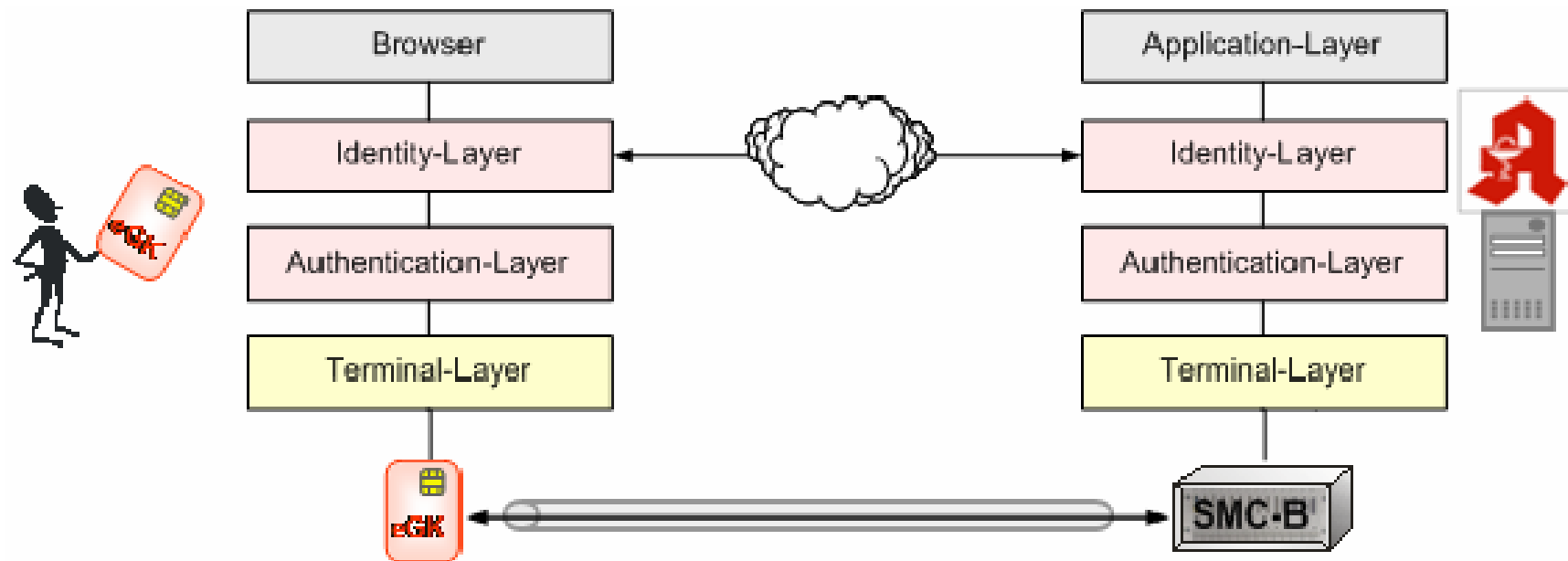
## Agenda

- ❑ The German eCard-Strategy
- ❑ **The eCard-API-Framework**
  - ❑ Architecture
  - ❑ ISO24727-3-Interface
  - ❑ **Deployment Options**
- ❑ Towards a comprehensive eID-Framework for Europe
- ❑ Summary

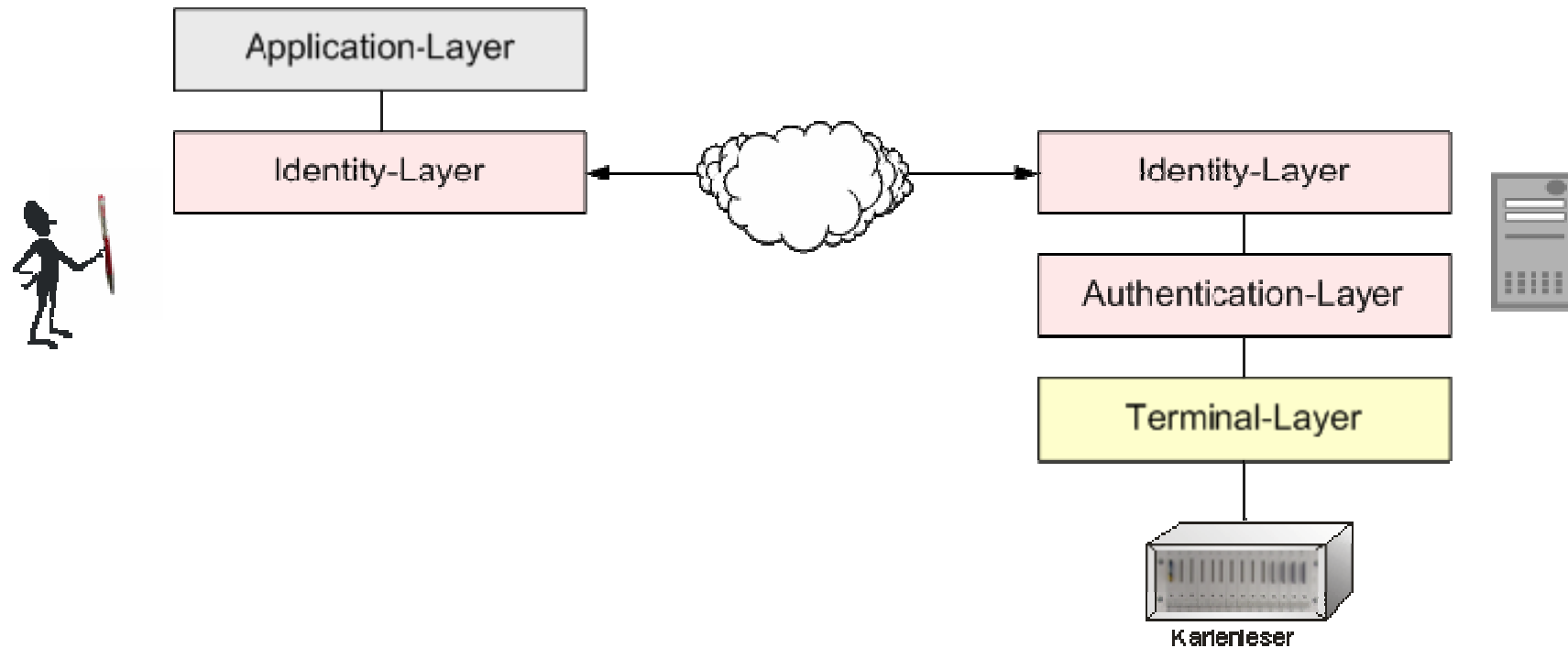
# Loyal Stack



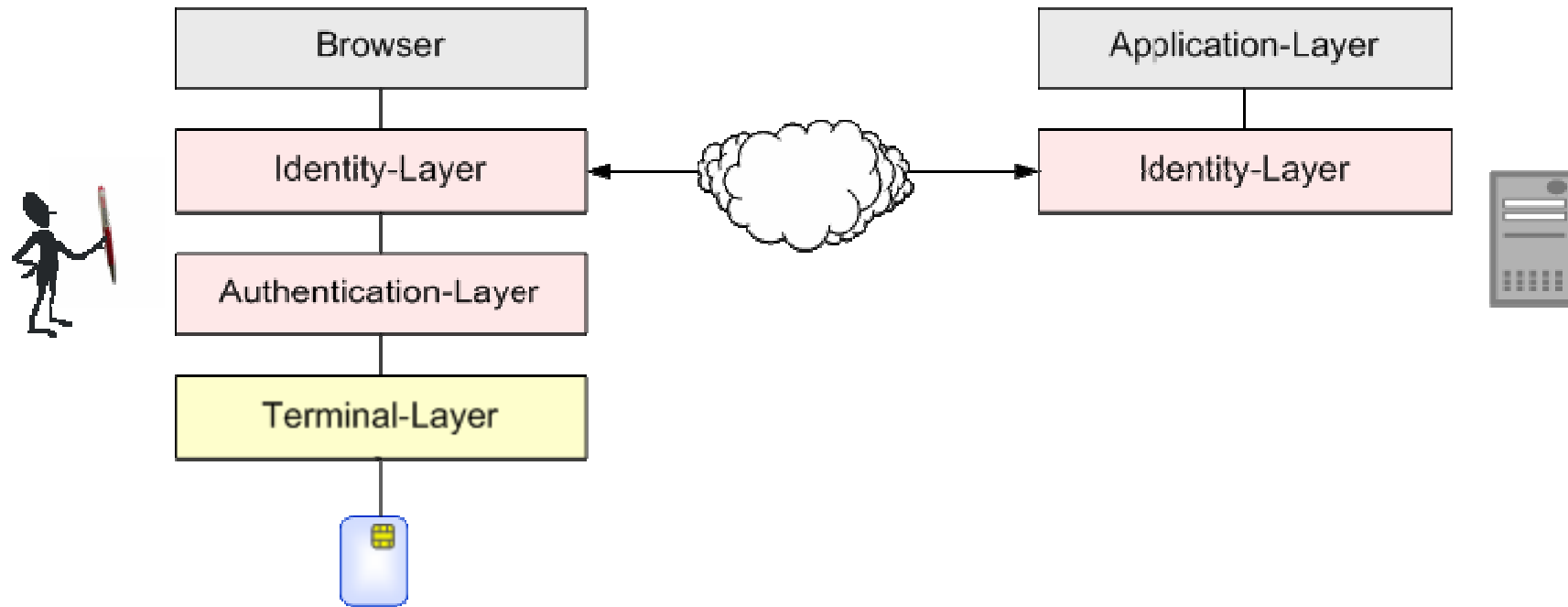
# Remote Loyal Stack (Internet Pharmacy)



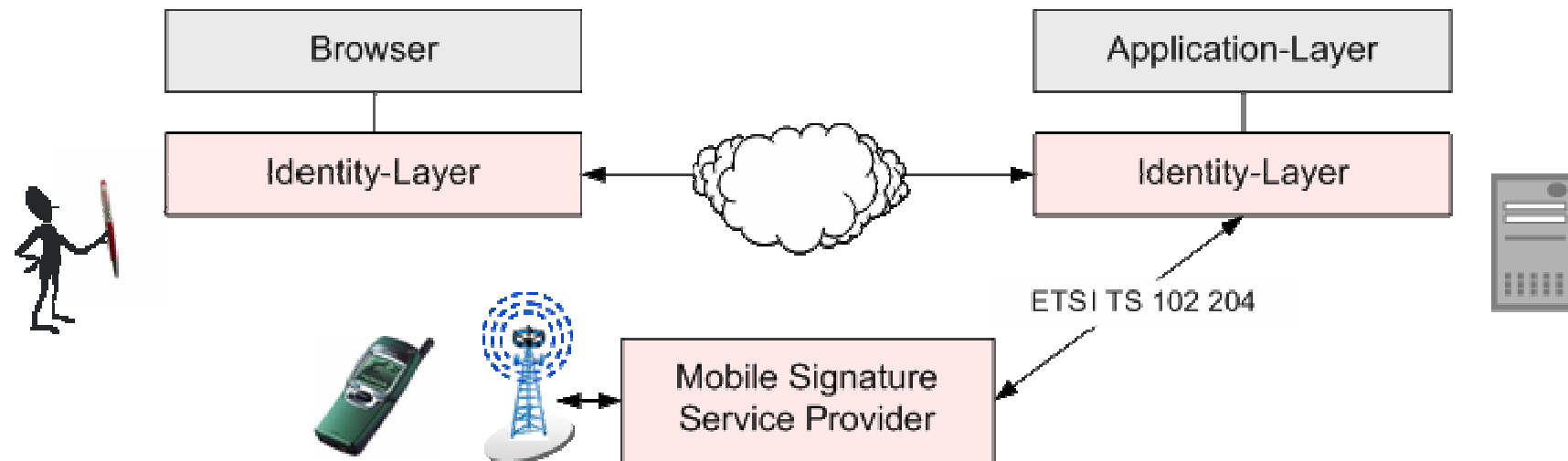
# Remote Loyal Stack (Signature Server)



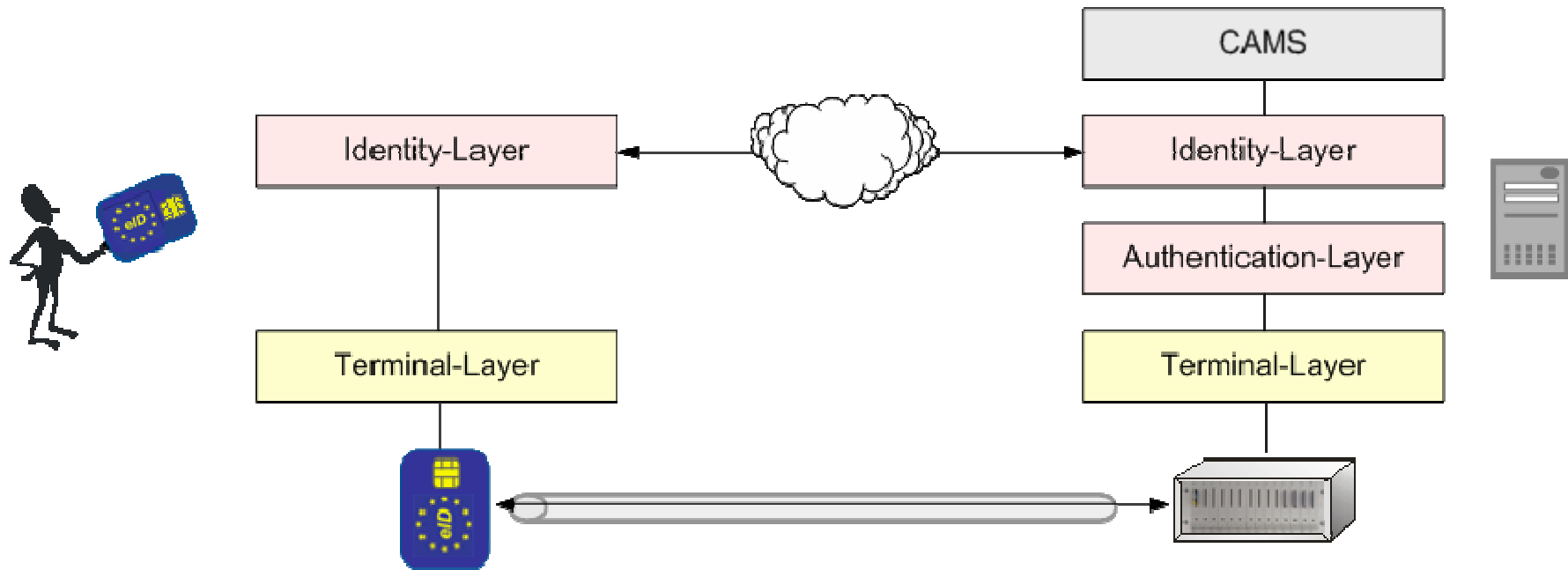
# Remote Loyal Stack (WebSigning)



# Remote Loyal Stack (Mobile Signature)



# Remote ICC Stack (CAMS)



## Agenda

- ❑ The German eCard-Strategy
- ❑ The eCard-API-Framework
- ❑ **Towards a comprehensive eID-Framework for Europe**
- ❑ Summary

# Towards a comprehensive eID-Framework for Europe



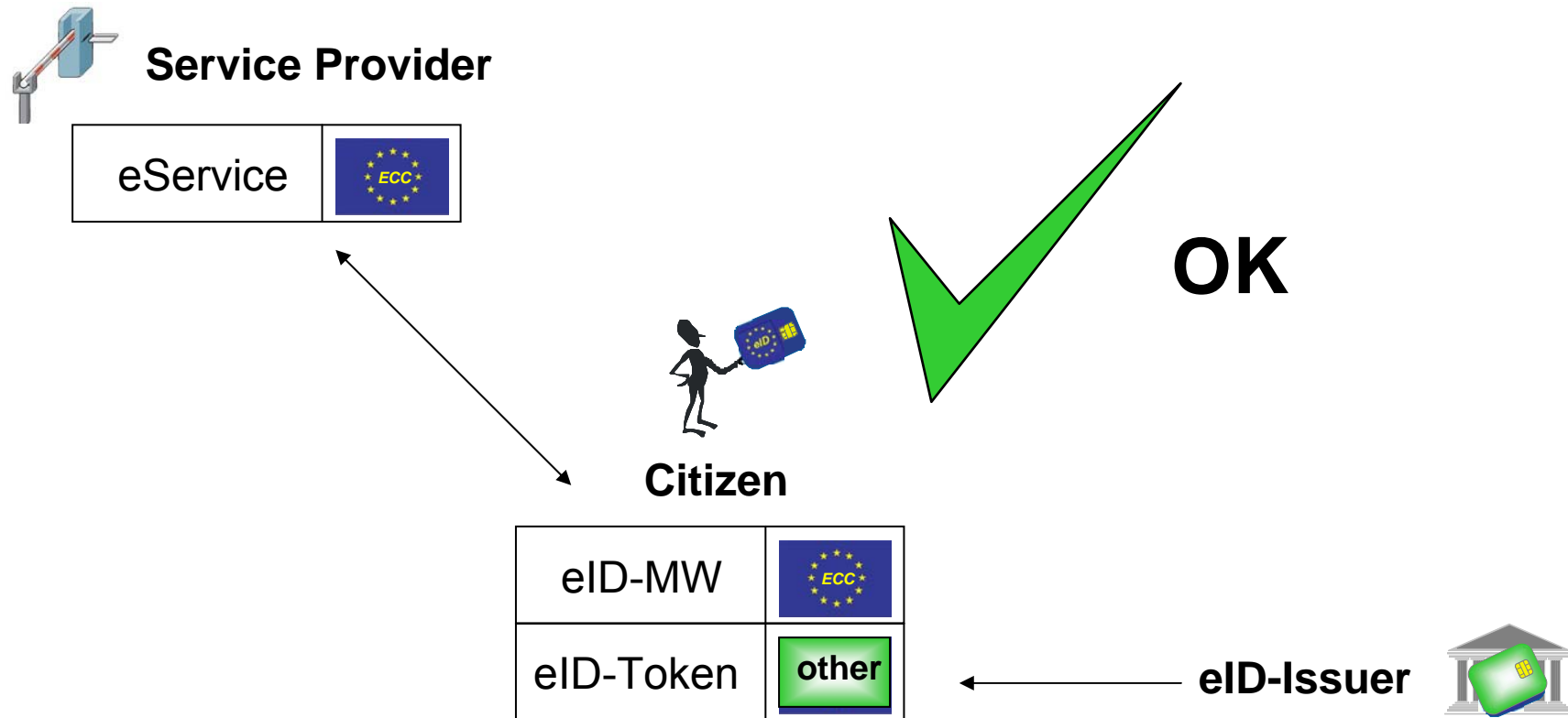
eID Large Scale Pilot



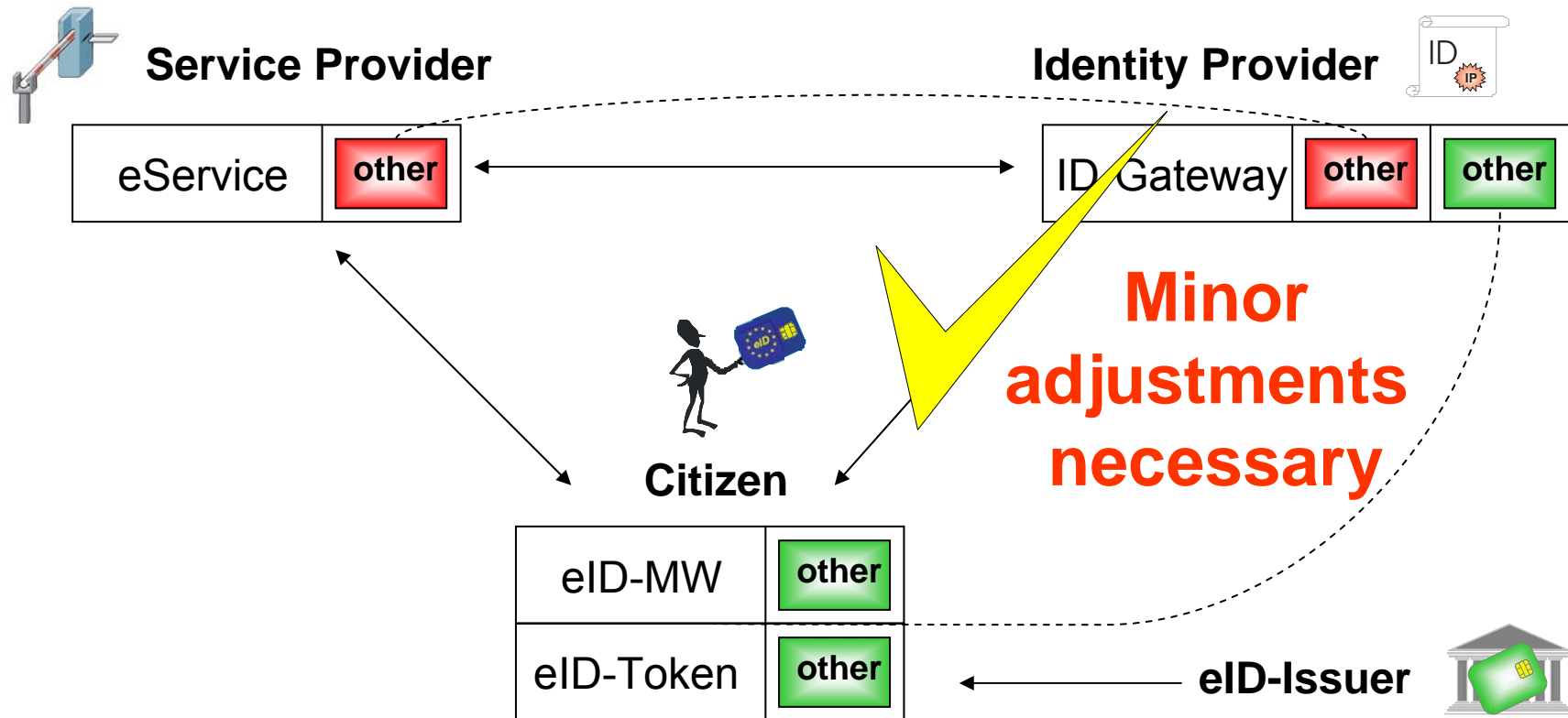
**Middleware-Approach**

**Gateway-Approach**

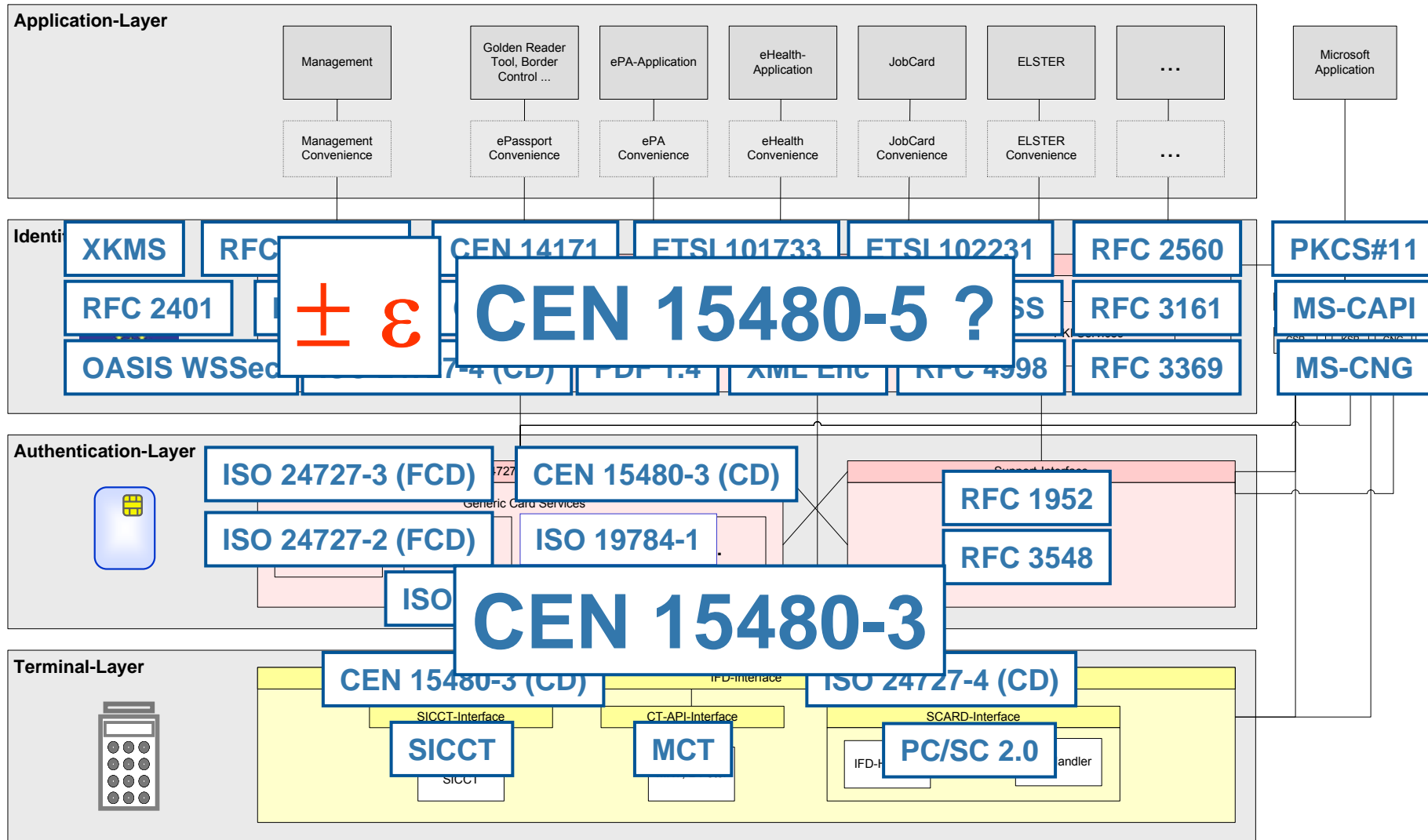
# Middleware-Approach



# Gateway-Approach



# What is missing for a comprehensive eID-Framework for Europe?



## Agenda

- ❑ The German eCard-Strategy
- ❑ The eCard-API-Framework
- ❑ Towards a comprehensive eID-Framework for Europe
- ❑ **Summary**

# Summary

- ❑ **Support of arbitrary smart cards without changing** the executable code (CardInfo-Files)
- ❑ **Easy integration of applications** (“High-Level”-API)
- ❑ **Platform independent** and scalable (Webservice-Interfaces)
- ❑ Support and abstraction of **various card terminal technologies**
- ❑ Considers major **smart card and PKI standards and architectures** e.g. Microsoft’s (CNG) CryptoAPI
- ❑ Currently the eCard-API-Framework is harmonized with emerging eID-standards (e.g. ISO/IEC 24727 and prCEN/TS 15480)
- ❑ May provide a good starting point to define a comprehensive eID-Framework for Europe ...
- ❑ which may be utilized within the EU eID Large Scale Pilot project (STORK)

# Thank you very much for your kind attention!



## Contact:

Dr. Detlef Hühnlein  
secunet Security Networks AG  
[detlef.huehnlein@secunet.com](mailto:detlef.huehnlein@secunet.com)

Manuel Bach  
Federal Office for Information Security  
[manuel.bach@bsi.bund.de](mailto:manuel.bach@bsi.bund.de)