

European Citizen Card Going ahead

Lorenzo Gaston

CEN TC224 WG15

- **Smart-Card based model for e-ID management**
- **User-centric: Card under control of the citizen only**
- **Interoperability based on Middleware/ Open Interfaces**
- **Strong Authentication and Privacy Enhancement key features**
- **Compliant with EU Directive on Electronic Signature**
- **Political Objective not only technical : EU requires common citizenship symbols**

- **Multi-part European Standard in two steps**
- **Implements the Authentication Layer of an e-IDM system**
- **Authentication based on Smart Card + Middleware**
- **Makes smart card security services available to external applications**
- **Specifies:**
 - Complete Smart Card specification, covering physical, electrical and security services
 - Middleware Specification of Implementation
 - Card profiles around a main service (ICAO traveling card, National ID card, e-Government card)

European Citizen Card Progress

Part	Current Status	Publication
5480-1 Hardware Durability	On Publication	Q2 2007
5480-2 AS	On Publication	Q2 2007
5480-3 Middleware -IDM + Testing	4th Working Draft	Q1/Q2 2008
5480-4 ECC Profiles	4th Working Draft	Q1/Q2 2008

Resolution of German and Swiss comments

Fast progress on Middleware Specification for Implementation

Integration of ECC in e-IDM systems

Definition of ECC profiles

Design of ECC Layout ICAO-compatible for Residence Card

Strengthened links with European Commission

Start discussion on new issues: Interoperability Testing, Match-on-Card Biometrics

- The middleware hides the specific details and technology of the European Citizen Card to the external world
- No previous knowledge of the ECC technology is needed to create a new application
- Service Providers does not need to know about the card implementation: The middleware takes care
- The ECC middleware facilitates the coexistence of ECC with other cards enabling the **migration to a common EU approach**

An ambitious approach

- CEN TC224 WG15 is a consensual committee between EU national standards bodies
- Simultaneously, the European Citizen Card interoperability mechanisms are being integrated in ISO Standards: 7816 and 24727
- This process is being done along with US and Japanese industry

ISO / CEN complementarities

CEN TC224

ISO SC17
Cards

ISO SC27
Security

ISO SC37
Biometrics

WG15 ECC

ISO 7816, ISO 24727
ISO 14443 Match on Card

e-ID Management

ISO 19794-2
ISO 24714

WG16 eSign

ISO 7816 4-8-15

ISO 9796, 9797, 9798
ISO 10116 ISO 10118

ISO 19794-2

WG17 PP

ISO 15408 cc 3.0

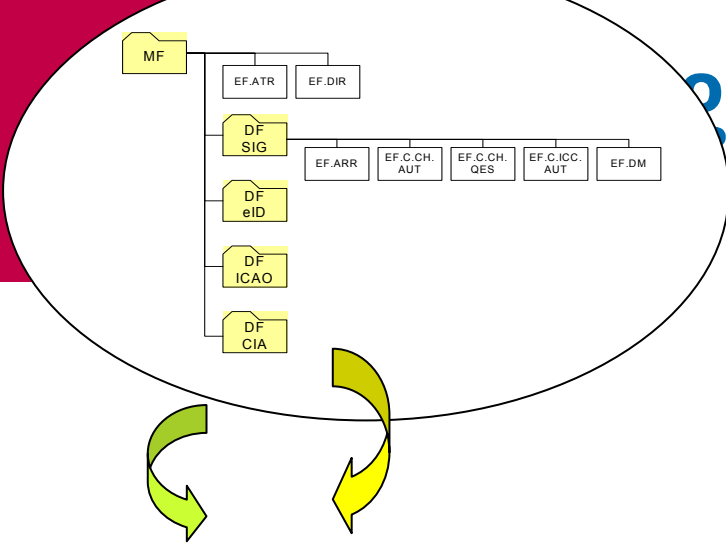
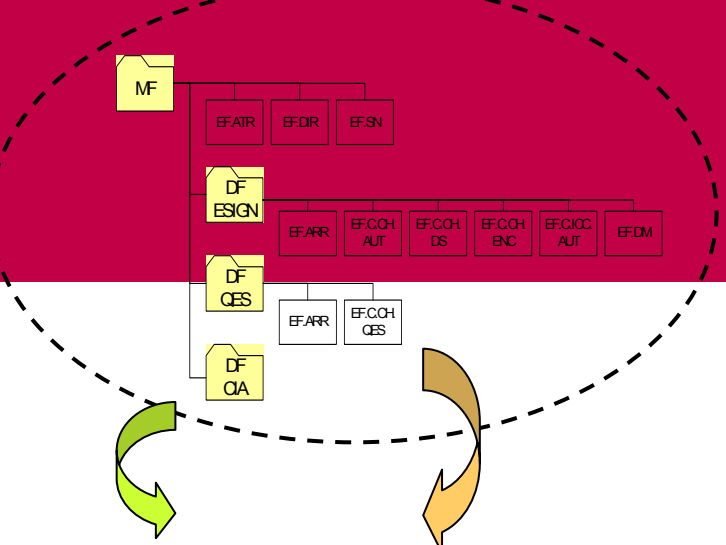
CEN TC 251
eHealth

ISO 7816 3-4-8-15

e-ID Management

Approach: e-ID Interoperability using the ECC

- The Interoperability is achieved with 3 key features:
 - A common set of card commands and data structures specified in the European Citizen Card standard part 2
 - A middleware which makes any ECC look the same for the external world defined in part 3
 - The definition of ECC profiles: e-Government card, National ID card, Traveling ICAO card defined in part 4



DF.CIA (ISO 7816-15)	On-Card Application	EF.DIR ACD 24727-2
☆☆☆ ☆☆ 16 14	4.2 expiry date 5.3 Place/date of issue 6.4 Type of permit 7.5-9 Remarks	14 ☆☆☆☆ 13 OVD 8 Date/Signature/Authorisation

DF.CIA (ISO 7816-15)	On-Card Application	EF.DIR ACD 24727-2
☆☆☆ ☆☆ 16 14	4.2 expiry date 5.3 Place/date of issue 6.4 Type of permit 7.5-9 Remarks	14 ☆☆☆☆ 13 OVD 8 Date/Signature/Authorisation

France e-Government ECC Application

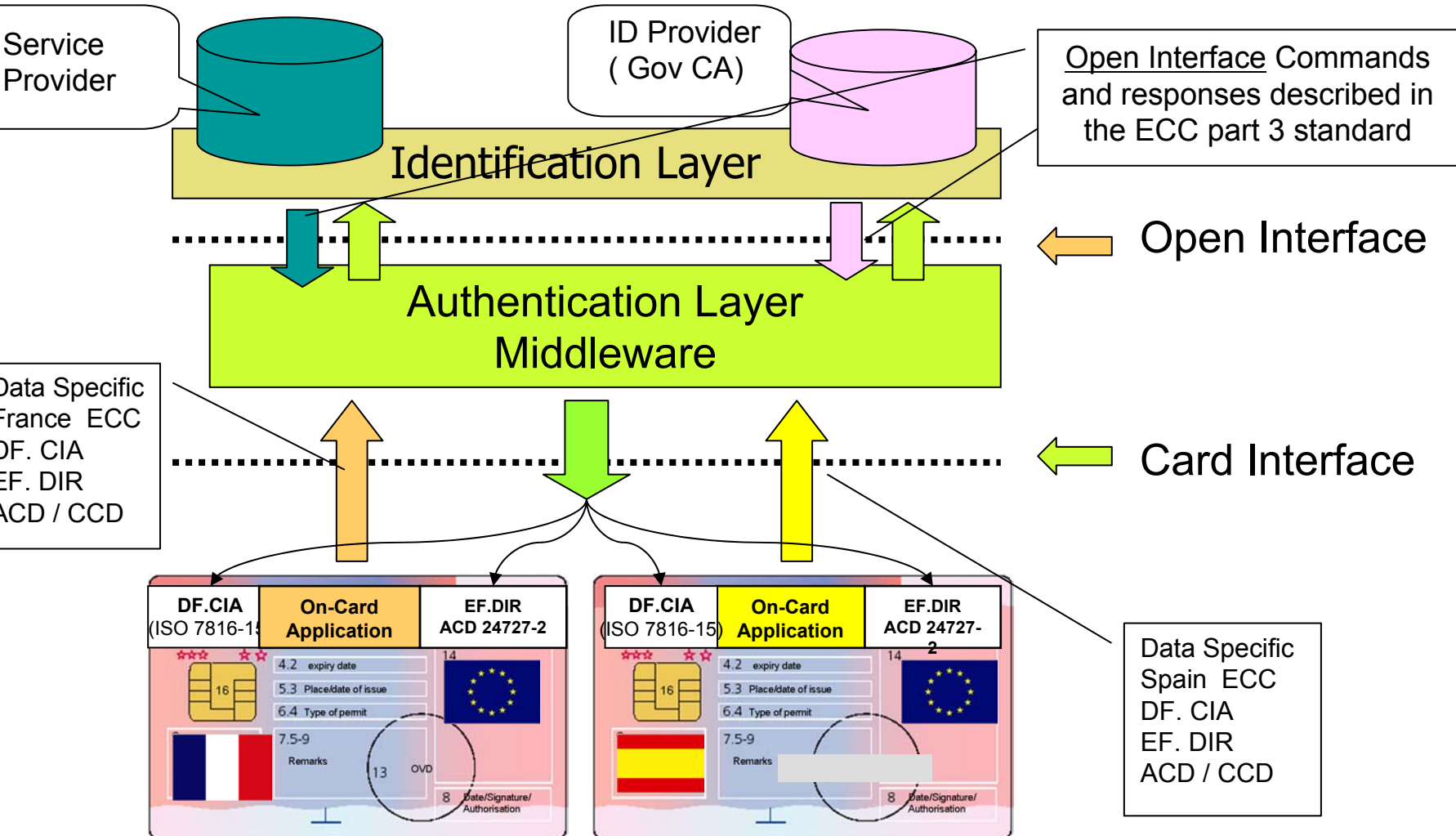
- DF.CIA Data for Middleware
- EF.DIR List of Applications + ECC profile
- ACD Compliance with ISO 24727

Spain e-Government ECC Application

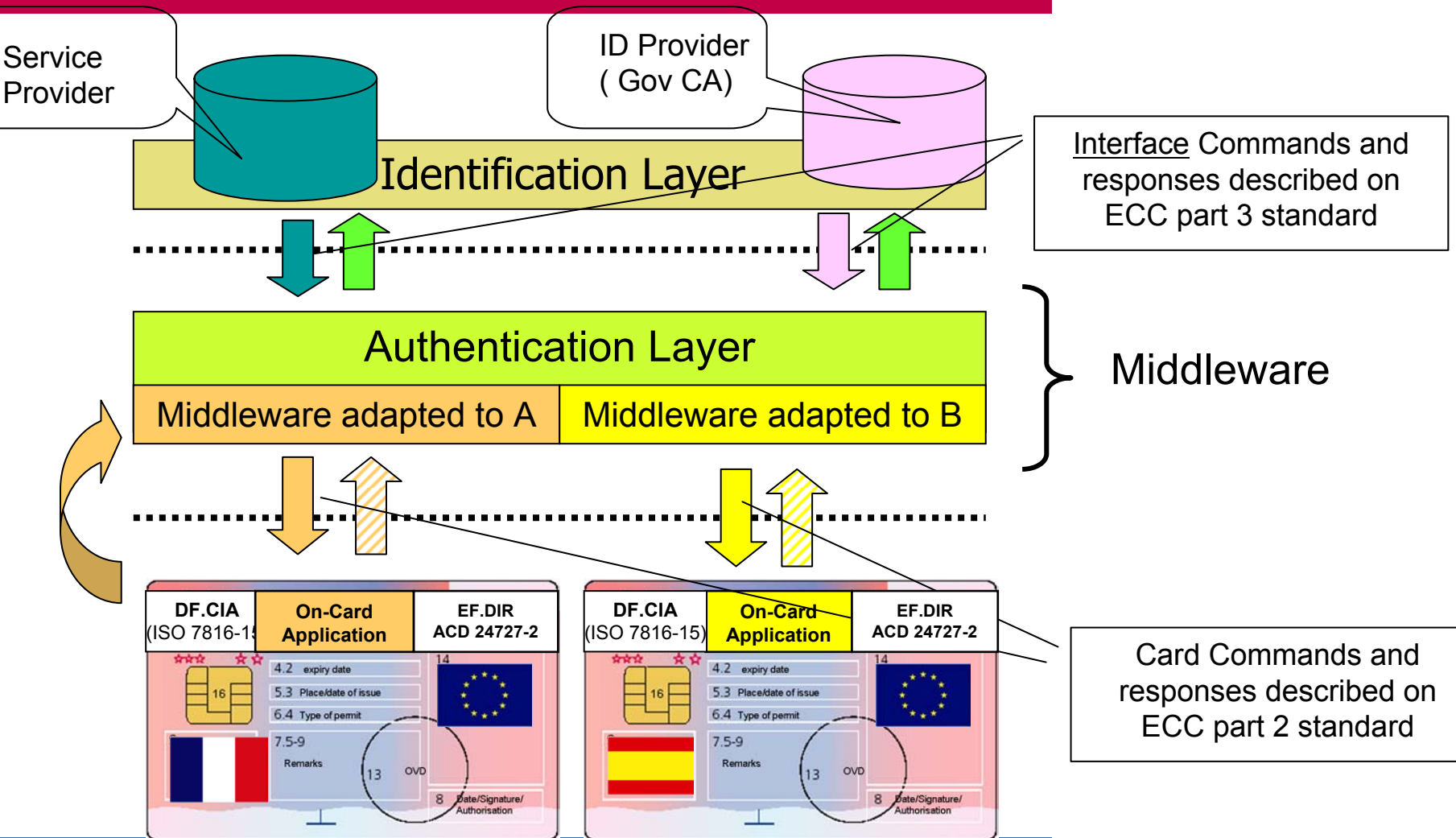
- DF.CIA Data for Middleware
- EF.DIR List of Applications + ECC profile
- ACD Compliance with ISO 24727

- The ECC is integrated in an e-IDM system through a Middleware Stack
- This standard middleware presents **two interfaces**:
 - ➔ An **Open Interface** (or API) that enables an e-Government application **to connect** with the middleware and **to request** a service
 - ➔ A **Card Interface** that connects the middleware with the ECC
- The Authentication Layer of the e-IDM system is implemented using an ECC + Middleware
- This Authentication Layer appears to the Service Provider just as an Open Interface

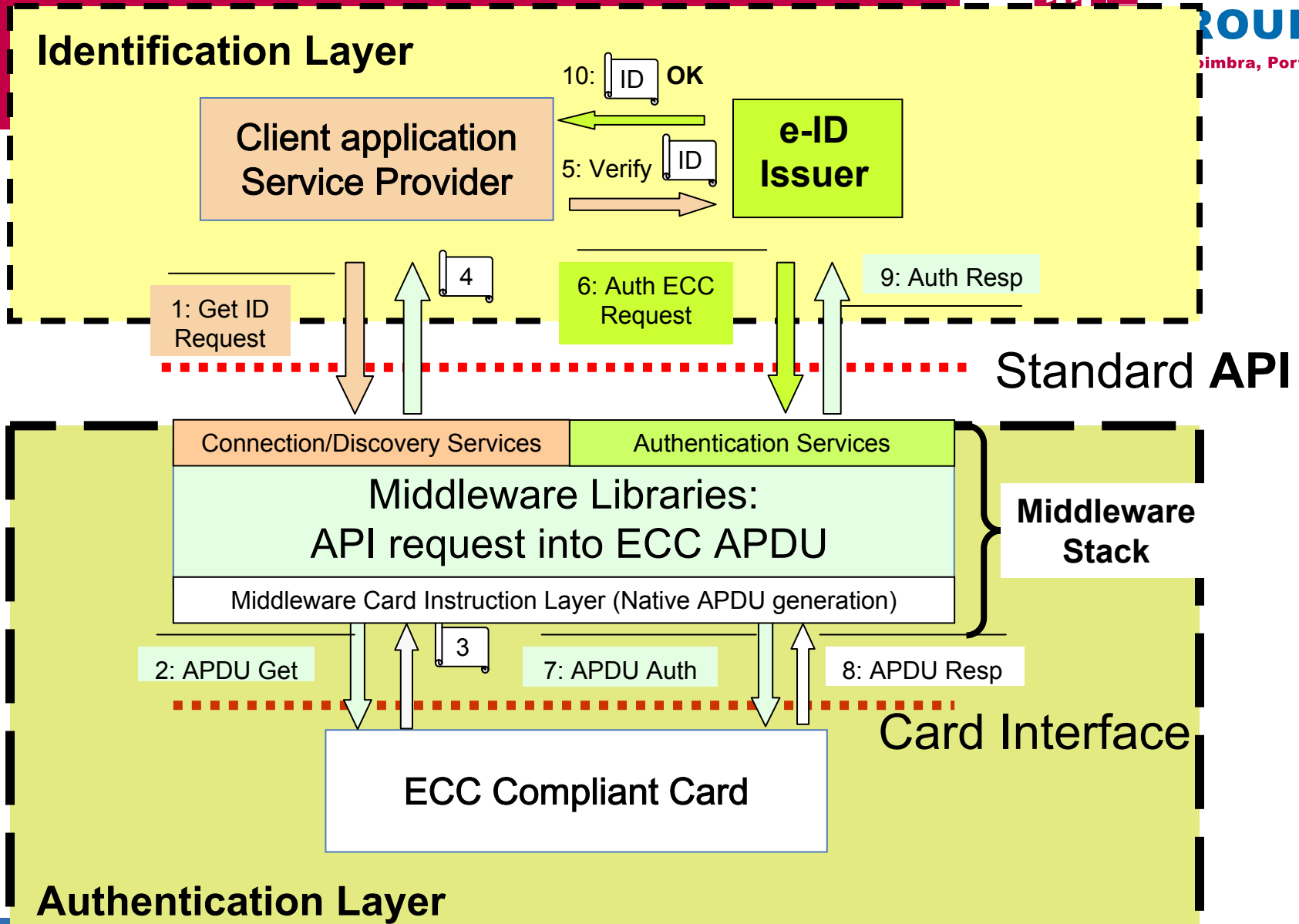
Interoperability T=0: The middleware and the ECC behave the same



The Middleware self-adapts using card data



ECC interoperability scheme



- **Accommodates naturally of any e-IDM scheme based on middleware (eg, TLS)**
- **Provide Authentication services to any e-IDM scheme made up of an ID Agent- ID Provider and Service Provider Federation**

- **The standard is progressing well**
- **We propose an Authentication Layer to e-IDM systems for Interoperability**
- **We intend to play a central role for upcoming e-IDM Pilots**
- **WG15 recommends ECC profiles for IOP**
- **We are making progress on ICAO and GP convergence**
- **Simultaneous European and International standardization process**