

ISO/ CEN Standardization Status European Citizen Card

Lorenzo Gaston

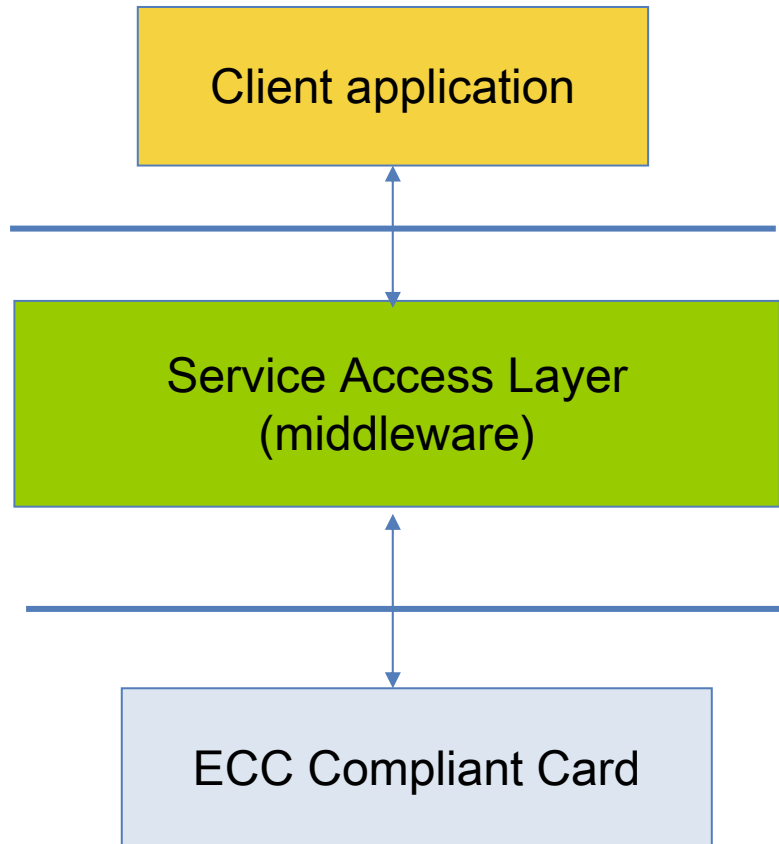
ETSI 16th-17th Jan 2007



CEN/ TC224 WG15 European Citizen Card

- ★ Standardization of ID cards for Public Administration, including but not limited to National Electronic ID cards
- ★ Divided into four parts:
 - 15480-1 “Hardware”: Physical securities and card durability
 - 15480-2 “Software”: Security Architecture and IAS services
 - 15480-3: Middleware and Interoperability Framework for e-ID authentication
 - 15480-4: ECC profiles based on sound use cases)
- ★ Gemalto leadership
- ★ Strong synergies with other CEN and ISO initiatives
- ★ Enable strong relationship with European Commission

Recap of ECC interoperability levels



ECC-4: Use-cases

ECC-3 / ISO 24727 -3:
Application interface (API)

} → For ECC Compact middleware
Merging SAL and GCAL
(see slides 10 and 11)

ECC-1: communication
protocols

ECC-2: APDU interface

2006 and previous years achievements

- ✦ Initial Roadmap achieved
 - Parts 1 and 2 of the standard ready
 - Approval by CEN members of New Work Items parts 3 and 4
- ✦ Solution for Interoperability at system level going on
- ✦ Strong impact on ISO standards
- ✦ Increased participation including Governments
- ✦ European & International Recognition
- ✦ [Onomat@pic](#) project: Proof of the ECC concept being run simultaneously (M. Faher)

Plan for Q4 2006 and 2007 Vision

- ✦ Second submission of Parts 1 and 2 to CEN members for decision on publication
- ✦ Proposal for an e-ID Management Framework for Interoperability including middleware provisions
- ✦ Start work on Match-on-Card Biometrics for ID cards
- ✦ Definition of European Citizen Card Profiles based on Use Cases
- ✦ Start work on Interoperability Testing Methodology
- ✦ Progress on Convergence with on-going ISO standards
- ✦ Set up a stronger liaison with European Commission

European Citizen Card Roadmap

Part	Current Status	Publication
15480-1 ECC Hardware	<ul style="list-style-type: none"> ✦ <u>Approved</u> and Comments Resolved (last WG15 Sept 06) ✦ New Document October 06 	Decision CEN/ TC224 Expected : Jan 2007
15480-2 ECC IAS	<ul style="list-style-type: none"> ✦ <u>Approved</u> and Comments Resolved (last WG15 Sept 06) ✦ New Document October 06 	Decision CEN/ TC224 Expected : Jan 2007
15480-3 ECC IOP middleware	<ul style="list-style-type: none"> ✦ pre-NWI Approved: First Draft Sept 06 ✦ Second Draft: October 06 	Ballot: End 2007
15480-4 ECC Profiles	<ul style="list-style-type: none"> ✦ pre-NWI Approved: First Draft Sept 06 ✦ Second Draft: October 06 	Ballot: End 2007

ISO/IEC 24727

- ✦ Multipart standard specifying a standard card Middleware, with a security architecture and testing methodologies
- ✦ 24727 Middleware stack presents five basic features
 - Bounded by two API:
 - a « high level » API interfacing with a Client Application unaware of the card characteristics
 - A « low level API » directly interfacing with the Card supporting APDU
 - Made up of two separate layers supporting the two API
 - The Service Access Layer (SAL) supports the high-level API
 - The Generic Card Access Layer (GCAL) supports the low-level API
 - Different Implementations possible: ranging from fully distributed architecture up to a card directly supporting the high-level API
 - Intended to support physical/logical Access Control in Secure Environments
 - Card Technology Agnostic: Contact / Contactless, Java/ File Oriented
- ✦ Driven by US Administration, strong international lobby action

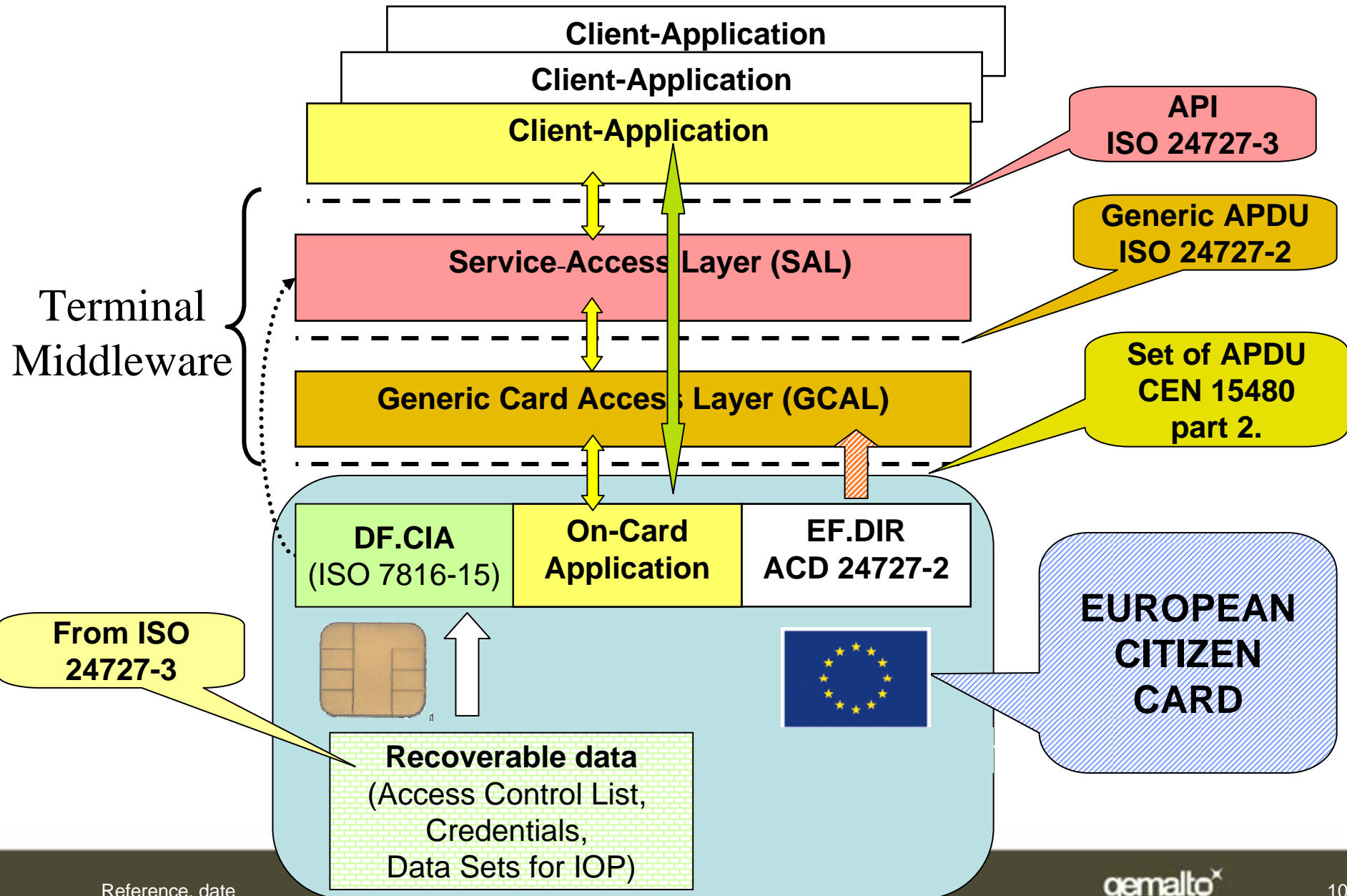
ISO/IEC 24727 Progress

Part	Current Status	Publication
24727-1 General Model	FDIS (Final Draft before publication)	Expected : Q2 2007
24727-2 Low Level API	<u>FCD (Final Committee Draft)</u>	Expected: Q4 2007
24727-3 High-Level API	Second CD (Committee Draft)	Expected: Q1/Q2 2008
24727-4 Security Model	<u>WD (Working Draft)</u>	Expected : Q4 2008
24727-5 Testing	<u>WD (Working Draft)</u>	Expected : Q4 2008

European Citizen Card and ISO 24727

- ✦ The European Citizen Card proposes a middleware taking advantage of ISO/IEC 24727 but adapted to the ECC
- ✦ The basic differences include the following
 - To merge the two middleware sub-layers (SAL and GCAL) so that the middleware directly conveys APDU compliant with 15480-2
 - Define a real end-to-end secure channel (client application- on card application) for unsecure environments (eg, personal PC)
 - Extend the existing API as per 24727-3 to support the European-specific authentication protocols define in 15480-2, including ePassport EAC
- ✦ A simultaneous standardization action is performed therefore at CEN/TC 224 WG15 (ECC) and ISO SC17 WG4 (24727)

CEN 15480-3 Interoperability Model



Conclusions

- ★ The European Citizen Card (CEN/TS 15480) positions as the key standard for public administrations
- ★ Inclusive Objective of the citizen for e-Government access
- ★ Flexible framework enabling the issuance of different types of cards for applications requiring strong citizen authentication
- ★ Concepts that can be reused in other sectors (driving license, eHealth)
- ★ Thinking at system level
 - Convergence with on-going ISO standardization efforts for Middleware
 - Convergence with on-going e-ID Management Systems
- ★ MEDEA + [Onom@topic](#) Project proof of the concept