StarSign® Management Suite Client

ISO 24727 based Middleware

Alexander Winnen

Washington D.C. 12/3/09

Giesecke & Devrient

Creating Confidence.

Why is G&D developing this new Middleware?

- Middleware has become one of the **key differentiating elements in the e-Identity business** - in PKI projects as well as in national ID projects and Company ID. More and more, it is becoming an essential part of our product portfolio.

  Therefore, G&D has decided to develop a smartcard middleware that meets the current requirements of smartcard usage and has already implemented the new standard ISO/IEC 24727.

- What are the main advantages for the customer?
  - **Highly competitive product in terms of functionality and flexibility**
  - **Support of a broad range of applications due to the modular architecture**
  - **Prepared for future requirements**
  - **Time to market will be faster**
  - **More flexibility to fulfil the customer needs**
  - **More reliability**

Why ISO 24727?

- ISO 24727 is becoming increasingly relevant especially in public sector smartcard projects
  - The German government issued the eCard API Framework as basis for all national smartcard projects. ISO 24727 is the core of the smartcard access layer.

- Need for a clean and modern architecture
  - ISO offers a versatile abstraction of the card applications that is not limited to cryptographic use cases
  - PKCS#11 is limited and fulfills many new requirements insufficiently (e.g. multiple PINs)

StarSign® Management Suite Client key differentiators

- ✓ **Multi-platform support**
  32 bit Windows platforms in Version 1, Version 2: Windows 64 bit + Linux, Solaris, Mac
- ✓ **Multi-application support**
  for all conventional PKI application, more than 32 applications are tested in the 1st release
- ✓ **Multi-reader support**
  for all smart cards readers compliant to PC/SC interface
- ✓ **Multi-language support**
- ✓ **Multi-year experience in support and development of Middleware**
  Developers from G&D and Secunet have 7+ years experience and developing, maintaining and supporting PKI Middleware

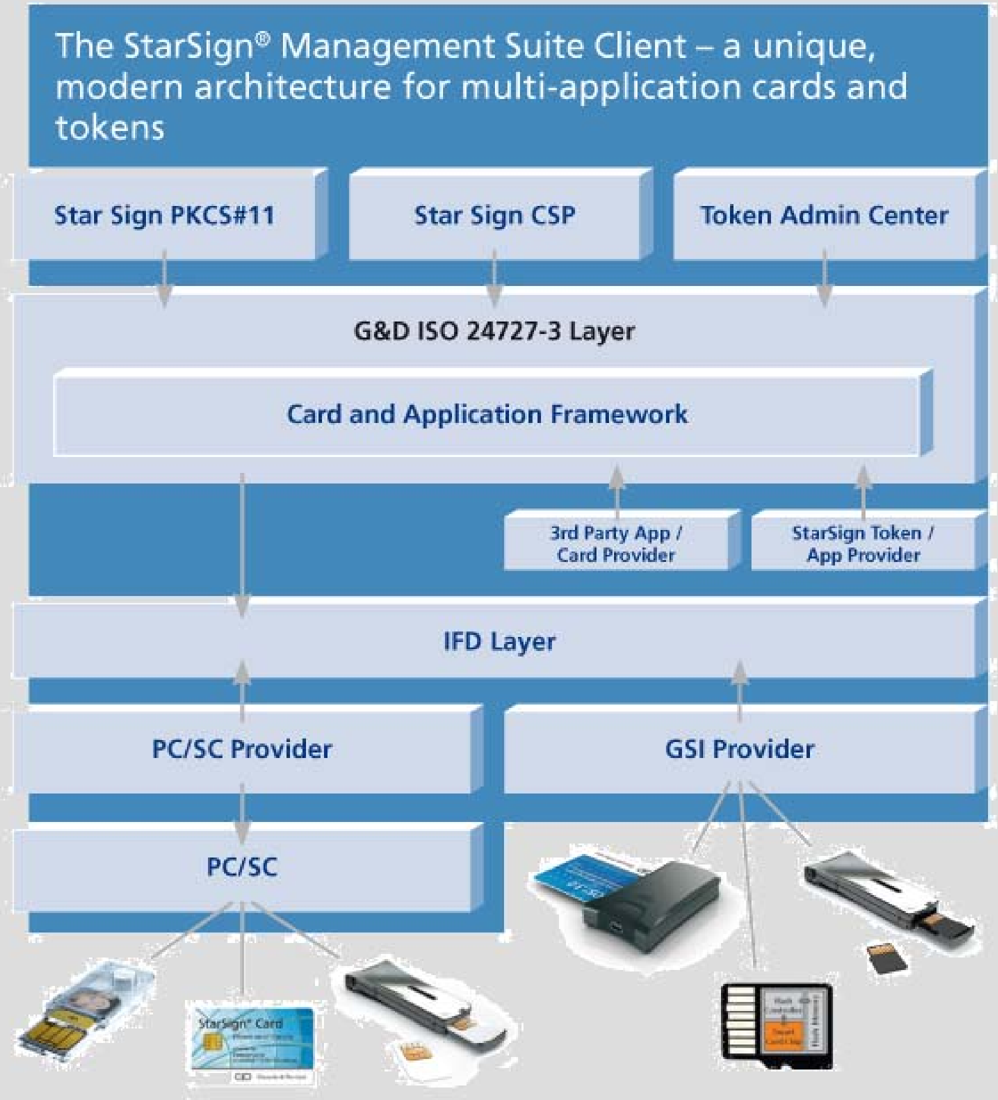
Standard Middleware Features

- ✓ **ISO/IEC 24727 Interface** is the core element of our architecture that provides a comprehensive functionality and guaranteed interoperability with future smartcard applications including PKI and Government
- ✓ **No admin – no install** through our patented GSI interface enables StarSign Mobility Token usage on PC with no administration rights or software installation required
- ✓ **3rd Party Card/Token support:** G&D has developed a card module provider scheme that allows the integration of 3rd party smart cards/token into the StarSign Management Suite Client.
- ✓ Simple configuration through our **Token Administration Centre (TAC)** that allows users to administer and configure tokens by themselves
- ✓ **Strong Authentication** Total security based on e.g. secure channel protocol that enables secure communication between the token and the middleware

StarSign® USP

Giesecke & Devrient

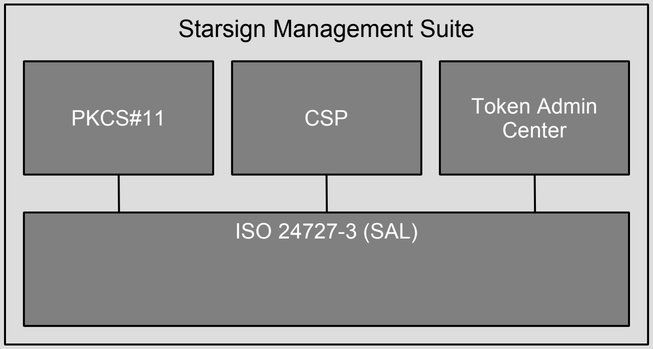
The StarSign® Management Suite Client – a unique, modern architecture for multi-application cards and tokens


The StarSign® Management Suite Client – a unique, modern architecture for multi-application cards and tokens
Star Sign PKCS#11
Star Sign CSP
Token Admin Center
G&D ISO 24727-3 Layer
Card and Application Framework
3rd Party App / Card Provider
StarSign Token / App Provider
IFD Layer
PC/SC Provider
GSI Provider
PC/SC
StarSign® Card

- **No admin – no install** through GSI layer (in combination with StarSign Mobility Token)
- **Multi-on-Token-Application & PIP support**

  supports multi-application cards & tokens including post issuance (e.g. applet loading, certificate and key renewal etc.)
- Based on **ISO 24727-3** Standard
- **Distributed architecture:** different layers can communicate through web server interfaces
- Integration of **3rd Party Card Provider** Modules possible
- Simple configuration through **TAC**

StarSign Management Suite Client – Product Overview

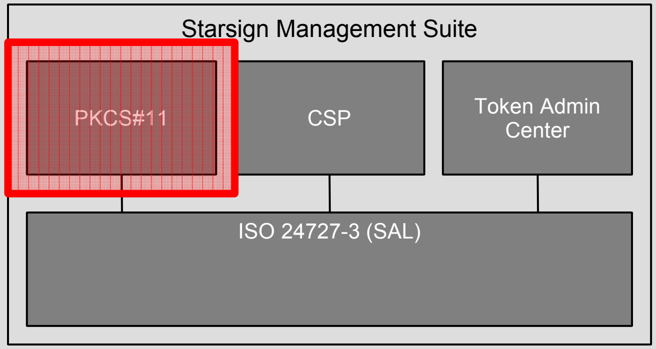


The StarSign middleware contains the following components

- PKCS#11 Library
- CSP Library
- ISO24727-3 Library
- Administration Tool (Token Admin Center)

- Smart card applications (PKCS#15 compatible) and PKI Applet

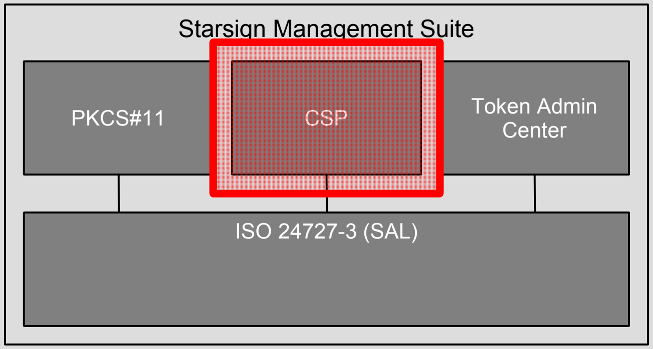
StarSign Management Suite Client – PKCS#11 Interface



PKCS#11 V2.20

- RSA Asymmetric Client Profile
- support of token (re-)initialization
- support of RSA keys, data objects and X.509 certificates

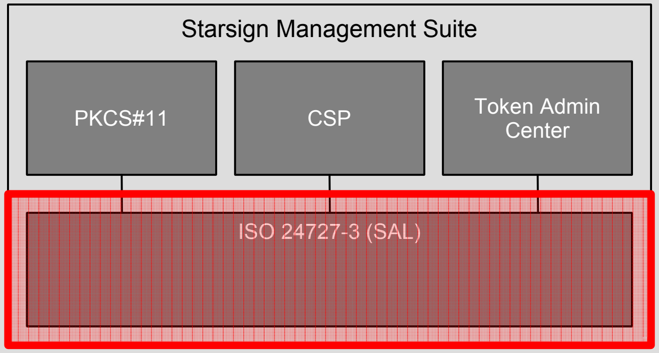
StarSign Management Suite Client – CSP Interface



Microsoft CSP

- Windows Logon
- Certificate Enrollment
- SSL Client Authentication
- Email Signing/Decryption

StarSign Management Suite Client – ISO24727-3 Interface



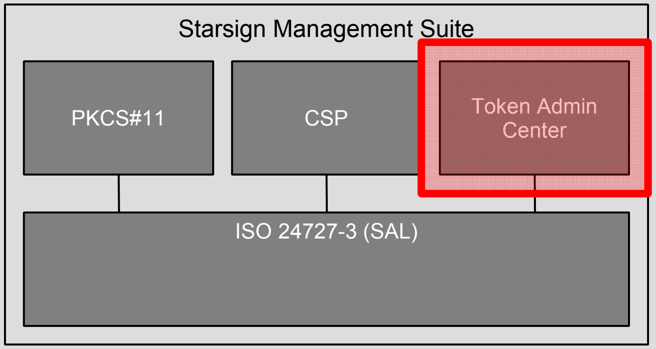
ISO24727-3

- Client/Server Architecture
- C/ASN.1 Interface
- file-based configuration, no Registry settings
- supports access to smart card applications (connections)
- maintains authentication states of multiple client processes using PIN-caching (per connection)
- Supports DIDs, DSIs and Datasets

proprietary extensions:

- Handling of PKCS#11 certificate and data object attributes
- Storage of CSP key container names
- Handling of terminal and card information

StarSign Management Suite Client – Token Admin Center



The Token Admin Center provides a GUI to

Administrate PKI Token functionality such as

- Visualize Token content and configuration
- Import Keys and Certificates (PKCS#12, CER, …)
- Manage PINs and Passwords (Change, Unblock)
- Manage Token element Attributes (labels, …)
- Dump token content for support purposes

Administrate encrypted memory volume on Mobility Token

- Manage Encryption Key and Password
- Manage Partitions

Configure the Management Suite

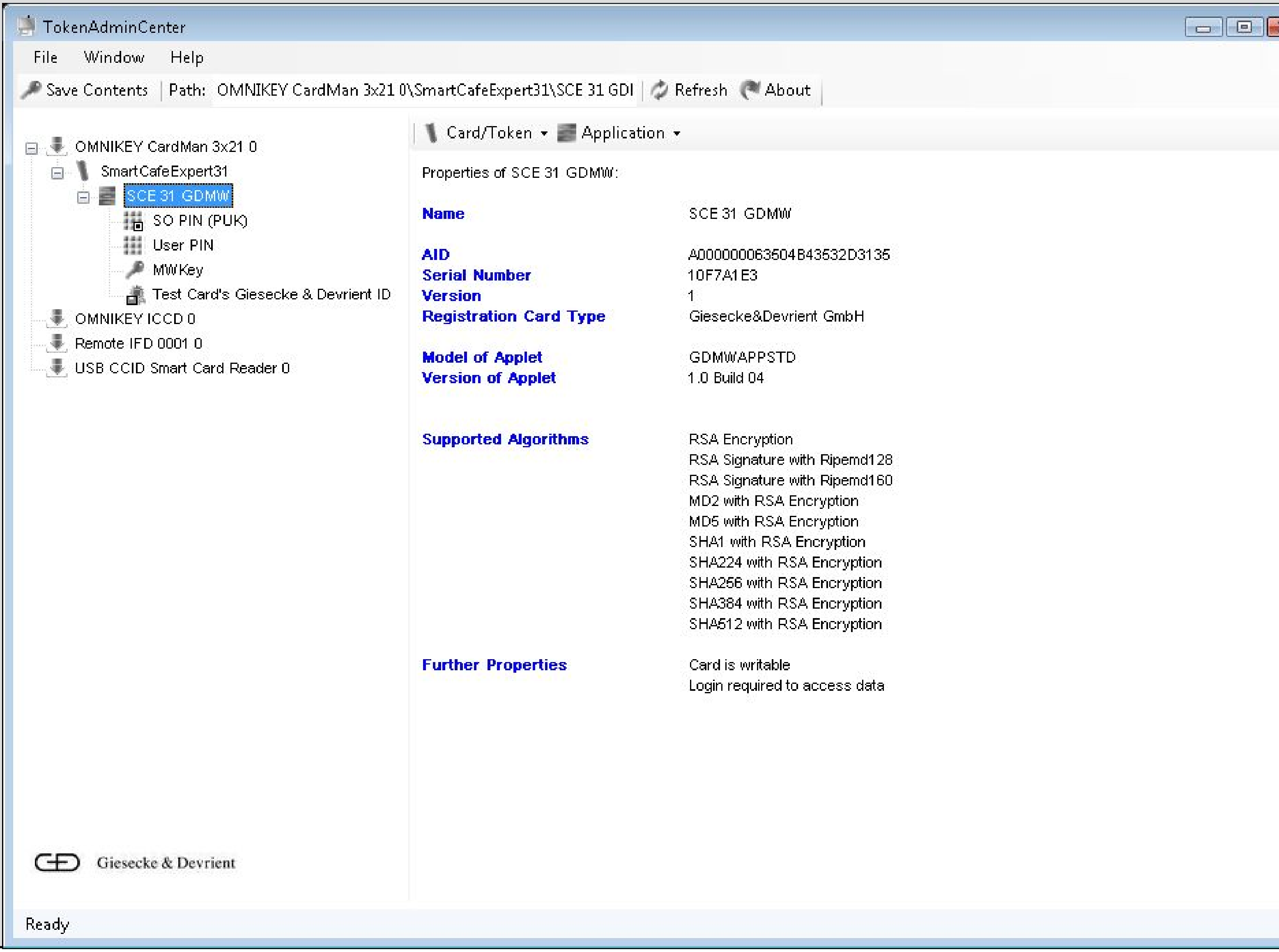
- Configure Smart Card Reader visibility
- Enable/Disable Logging (e.g. for support purposes)

StarSign Management Suite Client – Token Admin Center

Card Overview View:

Display of general card information:

- OS Name and Version
- ISO 24727 Alpha Card-application ID
- Supported Algorithms
- Other administrative information



Properties of SCE 31 GDMW:

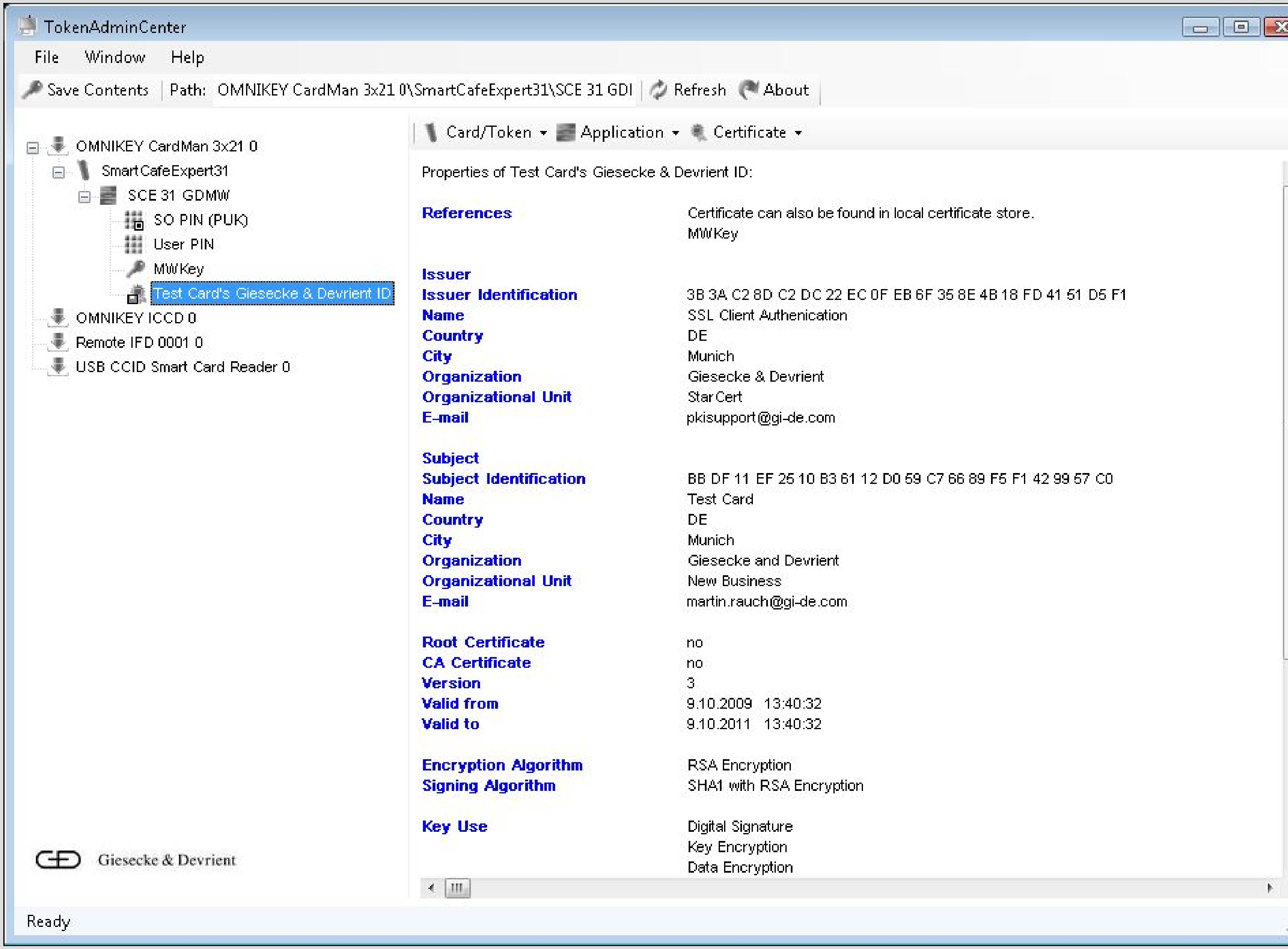
Name	SCE 31 GDMW
AID	A000000063504B43532D3135
Serial Number	10F7A1E3
Version	1
Registration Card Type	Giesecke&Devrient GmbH
Model of Applet	GDMWAPPSTD
Version of Applet	1.0 Build 04
Supported Algorithms	RSA Encryption RSA Signature with Ripemd128 RSA Signature with Ripemd160 MD2 with RSA Encryption MD5 with RSA Encryption SHA1 with RSA Encryption SHA224 with RSA Encryption SHA256 with RSA Encryption SHA384 with RSA Encryption SHA512 with RSA Encryption
Further Properties	Card is writable Login required to access data

StarSign Management Suite Client – Token Admin Center

ertificate View:

Display of certificate elements

- Issuer
- Subject
- Other certificate attributes



Properties of Test Card's Giesecke & Devrient ID:

References	Certificate can also be found in local certificate store. MWKey
Issuer	
Issuer Identification	3B 3A C2 8D C2 DC 22 EC 0F EB 6F 35 8E 4B 18 FD 41 51 D5 F1
Name	SSL Client Authenication
Country	DE
City	Munich
Organization	Giesecke & Devrient
Organizational Unit	StarCert
E-mail	pkisupport@gi-de.com
Subject	
Subject Identification	BB DF 11 EF 25 10 B3 61 12 D0 59 C7 66 89 F5 F1 42 99 57 C0
Name	Test Card
Country	DE
City	Munich
Organization	Giesecke and Devrient
Organizational Unit	New Business
E-mail	martin.rauch@gi-de.com
Root Certificate	no
CA Certificate	no
Version	3
Valid from	9.10.2009 13:40:32
Valid to	9.10.2011 13:40:32
Encryption Algorithm	RSA Encryption
Signing Algorithm	SHA1 with RSA Encryption
Key Use	Digital Signature Key Encryption Data Encryption

Implementation of the ISO 24727-3 Specification

- Development startet in 2007 based on the 0.8 version of the standard
  - Standard was not finalized
  - Important elements required for an implementation were missing

- Introduction of own extensions to the standard
  - Functions to return card / terminal configuration information
  - Functions to de-authenticate single objects
  - Functions to perform special operations on the card
  - „Typed“ datasets

Implementation of the ISO 24727-3 Specification

⑩ 4 Pre-defined Card Applications

- Alpha card app: not implemented on card, card management functions only
- PKCS#15 application: Management of keys and certificates
- Flash encryption key card app: Key management for USB Token encryption
- Security Domain card application: Manages SM between middleware and card

⑩ 8 Pre-defined Data Sets

⑩ Sessions not yet implemented

The reasons for extensions the ISO standard

➓ Different concepts of ISO and PKCS#11/CSP

- P#11/CSP communicate atomic commands between card and application.
  The client applications are responsible for maintaining consistency and logic of the operations performed on the card.
- ISO establishes a connection to the card that performs a defined service consisting of multiple single operations.
- In order to provide a P#11/CSP layer on top of the ISO layer additional functions have to be available to procure this layer with information which is not provided by the ISO functions (e.g. card status information).

Implementation decisions

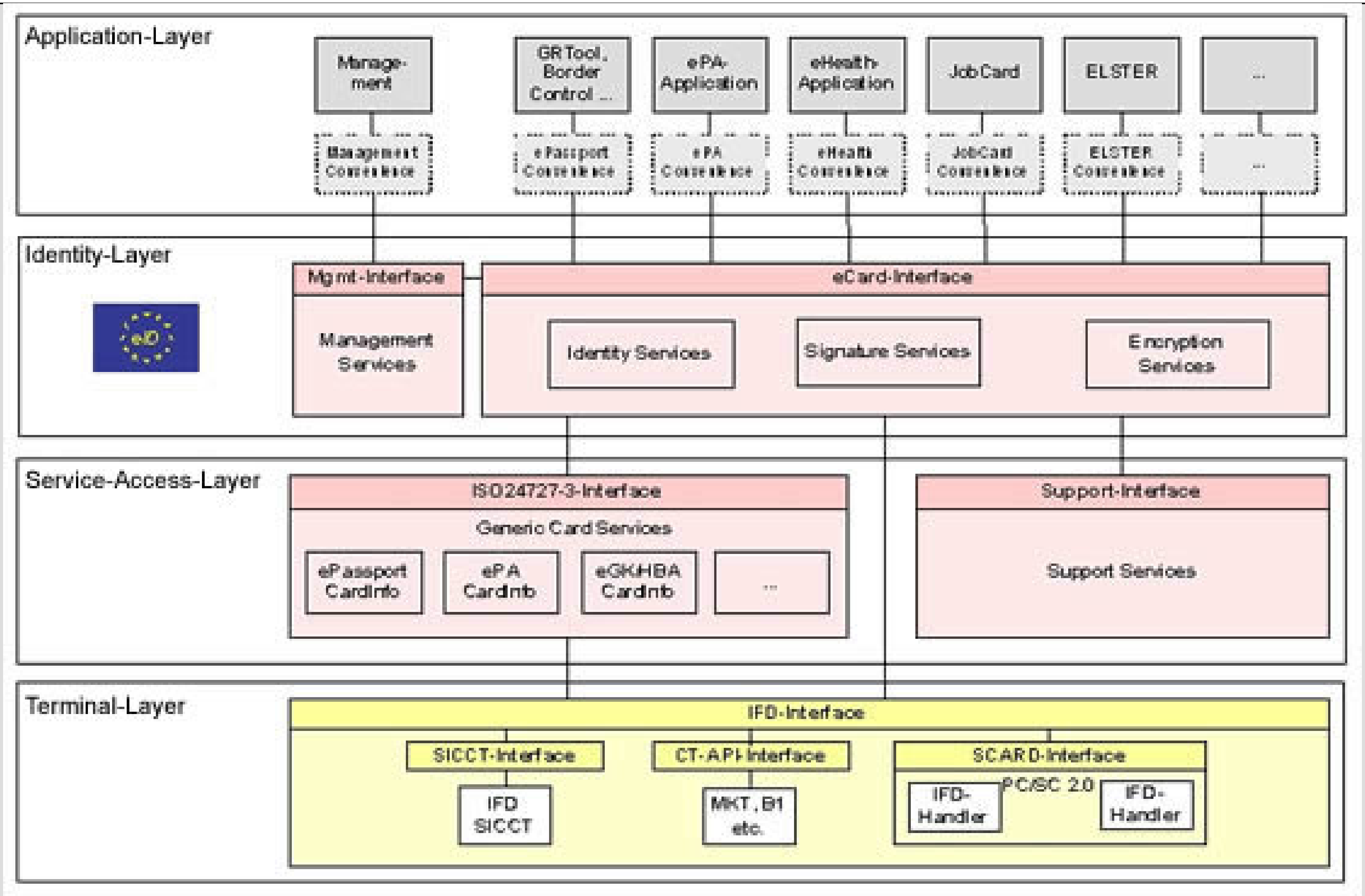
- ISO defines ASN.1 data structures but gives no guideline for an implementation in a specific programming language

- Implementation of the middleware as C API

- Parameters handed over to the C functions have to be ASN.1 formatted

- In most cases implementation follows the eCard API Specification

eCard API – Framework (source: German BSI)



eCard API Framework – Implementation decisions

- Functionality of the ISO interface is provided as Web services
- Definition of a Dataset as a file on the card
- Defines also several other components required in the context of different Public Sector smartcard projects in Germany (ePA, eGK/HBA, …)