



Using ISO/IEC 24727 for mobile devices



Jan Eichholz, Giesecke & Devrient GmbH

Dr. Detlef Hühnlein, secunet Security Networks AG

Manuel Bach, Bundesamt für Sicherheit in der Informationstechnik



ISO/IEC 24727 for mobile devices



Giesecke & Devrient

secunet



Agenda

- ❑ ISO/IEC 24727
- ❑ Using ISO/IEC 24727 for mobile devices
 - ❑ with Mobile Signature Service
 - ❑ in a Java Micro Edition environment
- ❑ Summary



ISO/IEC 24727 for mobile devices



Giesecke & Devrient

secunet

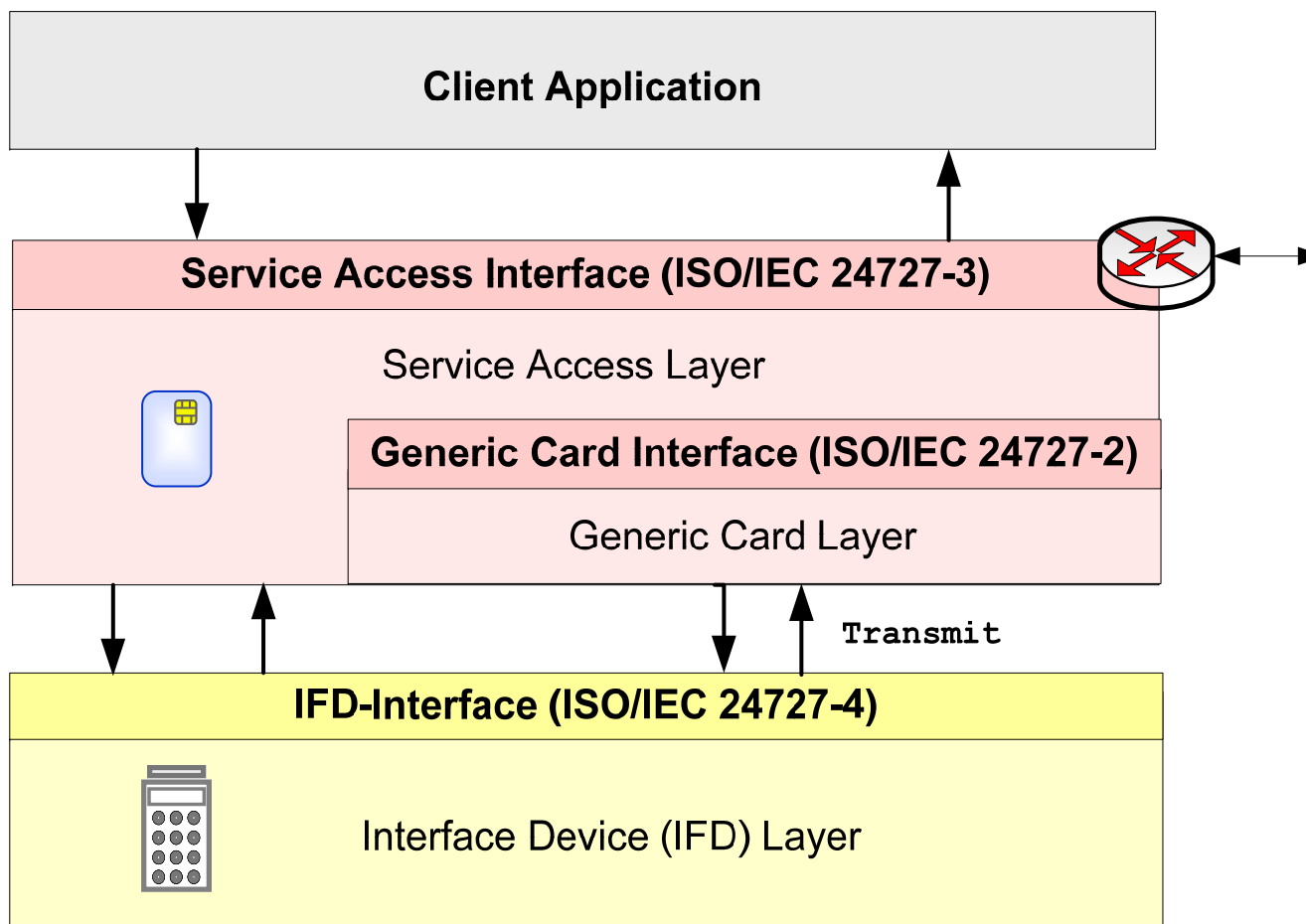


Agenda

- **ISO/IEC 24727**
- Using ISO/IEC 24727 for mobile devices
 - with Mobile Signature Service
 - in a Java Micro Edition environment
- Summary



ISO/IEC 24727 architecture





Functions of the ISO24727-3-Interface



Giesecke & Devrient

secunet



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



First ISO/IEC 24727 deployments





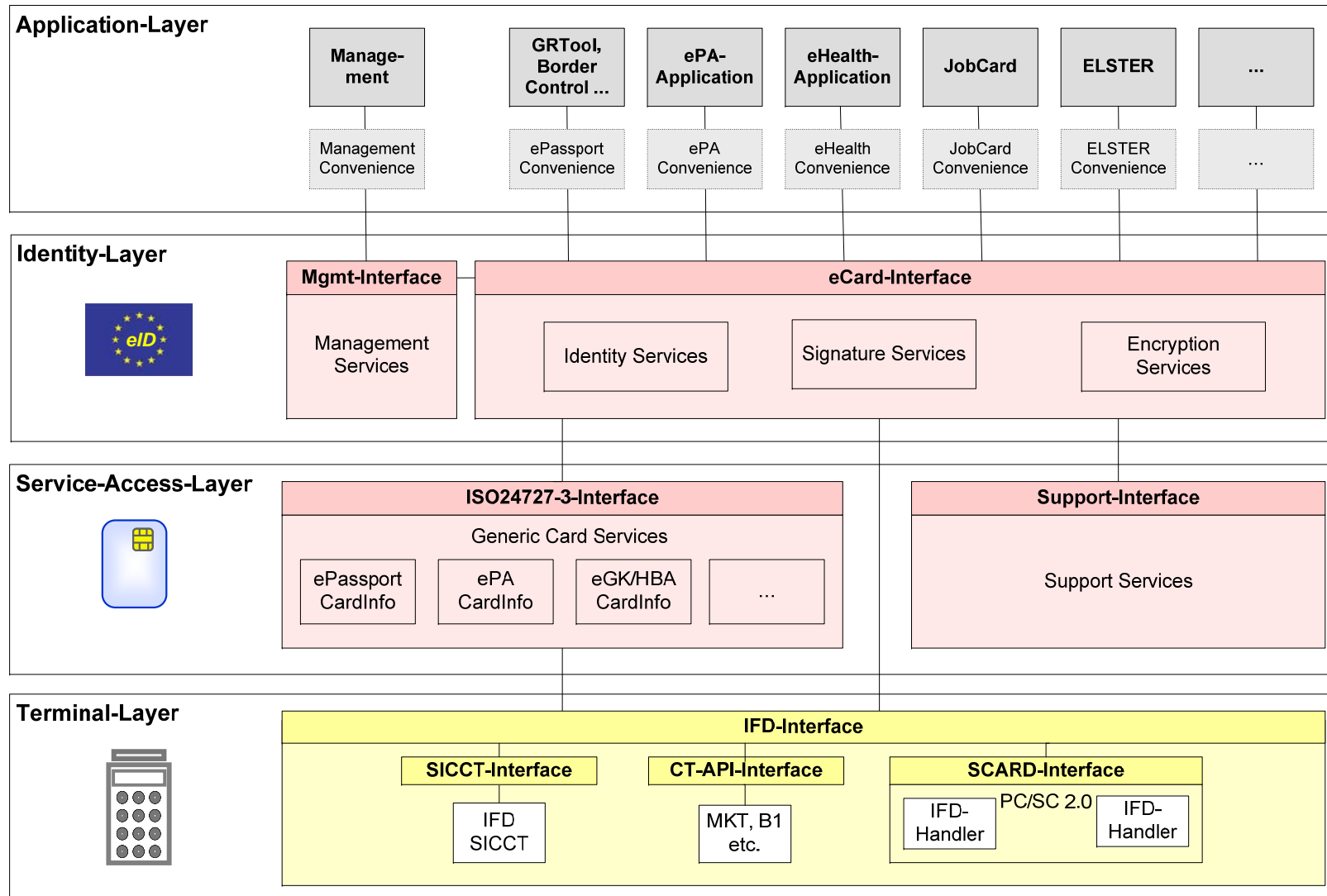
eCard-API-Framework

(BSI TR 03112, <http://www.bsi.de/literat/tr/tr03112/index.htm>)



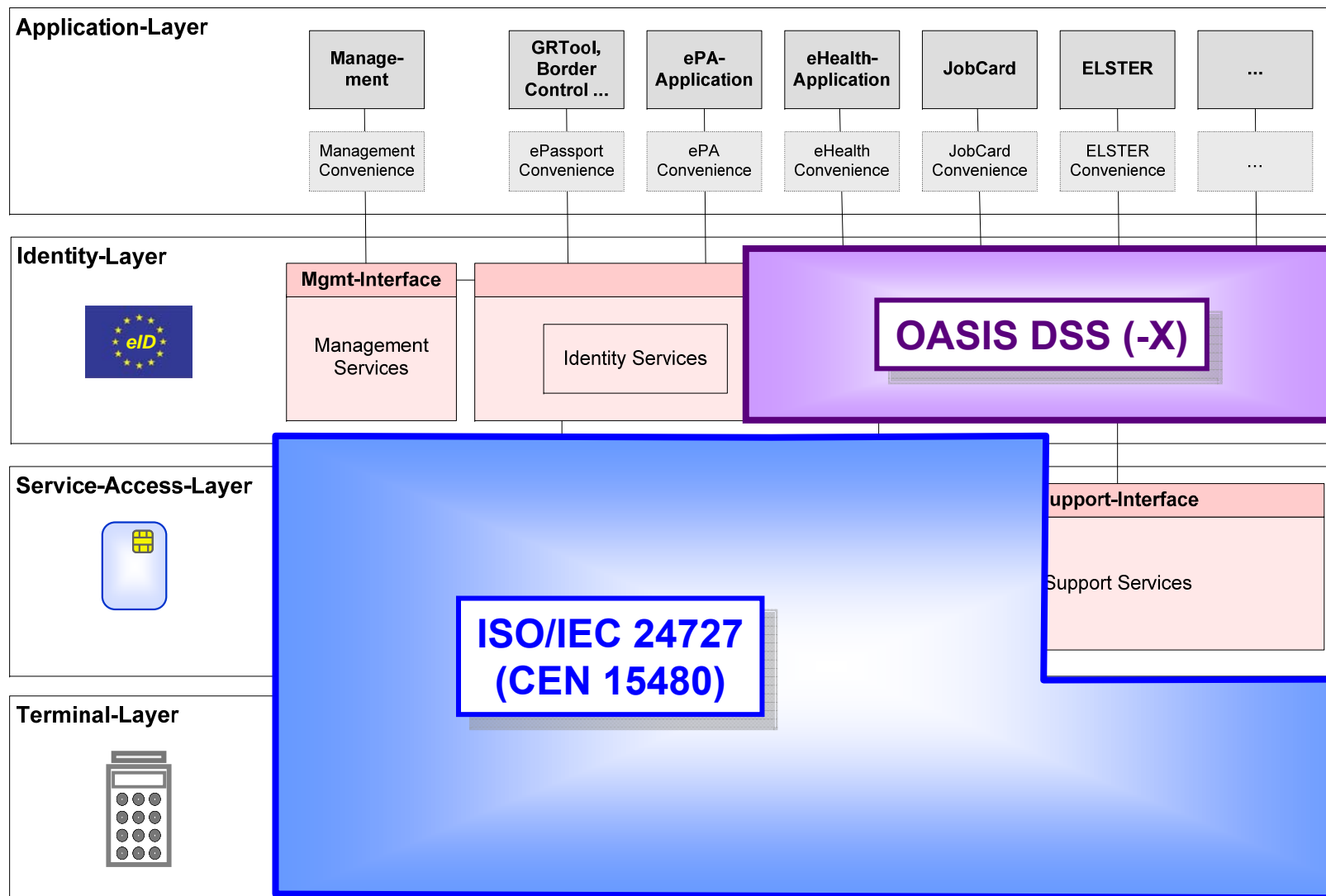
Giesecke & Devrient

secunet



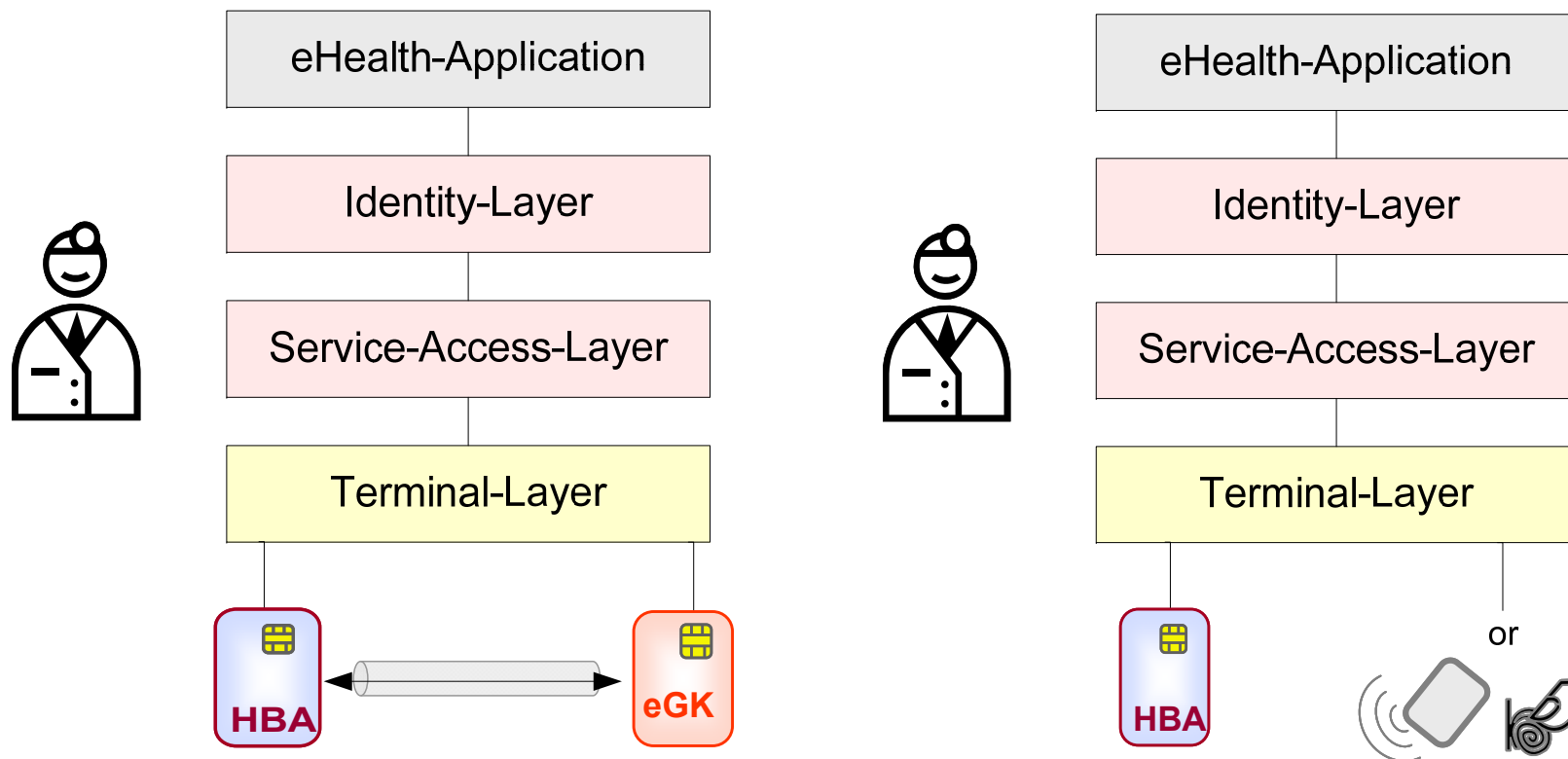


≈ ISO/IEC 24727 + OASIS DSS (-X)



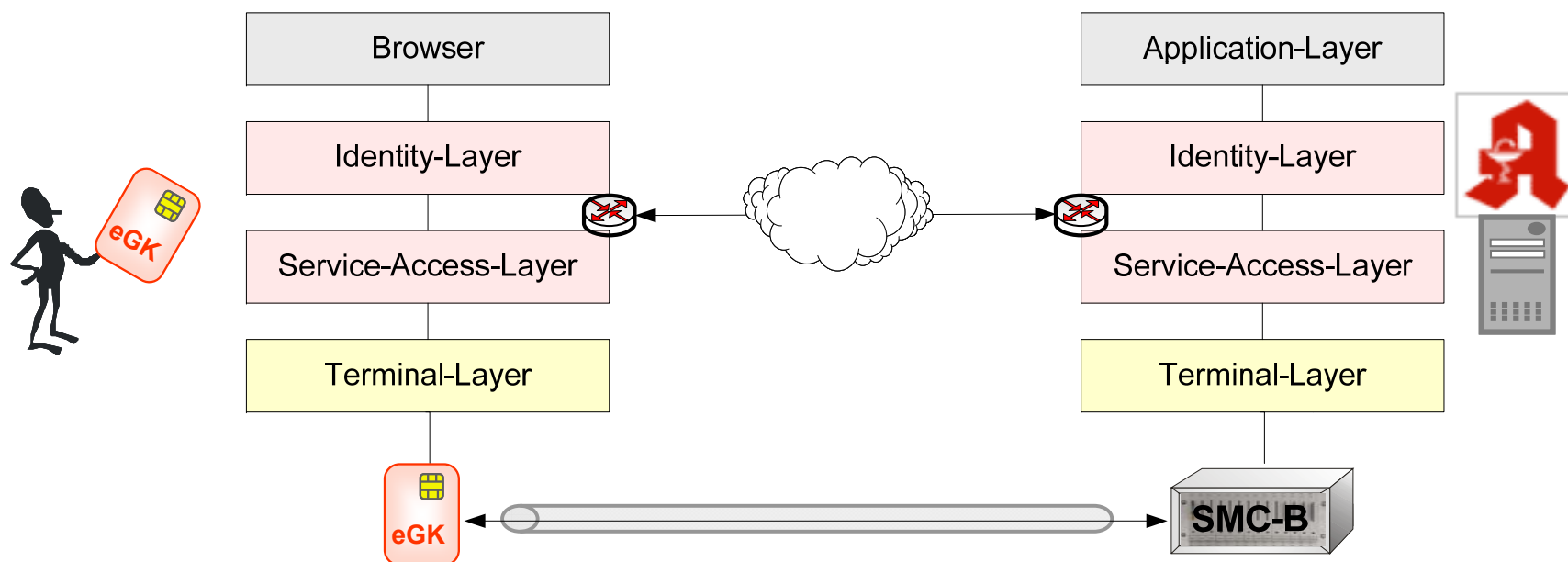


Loyal Stack





Remote Loyal Stack (Internet Pharmacy)



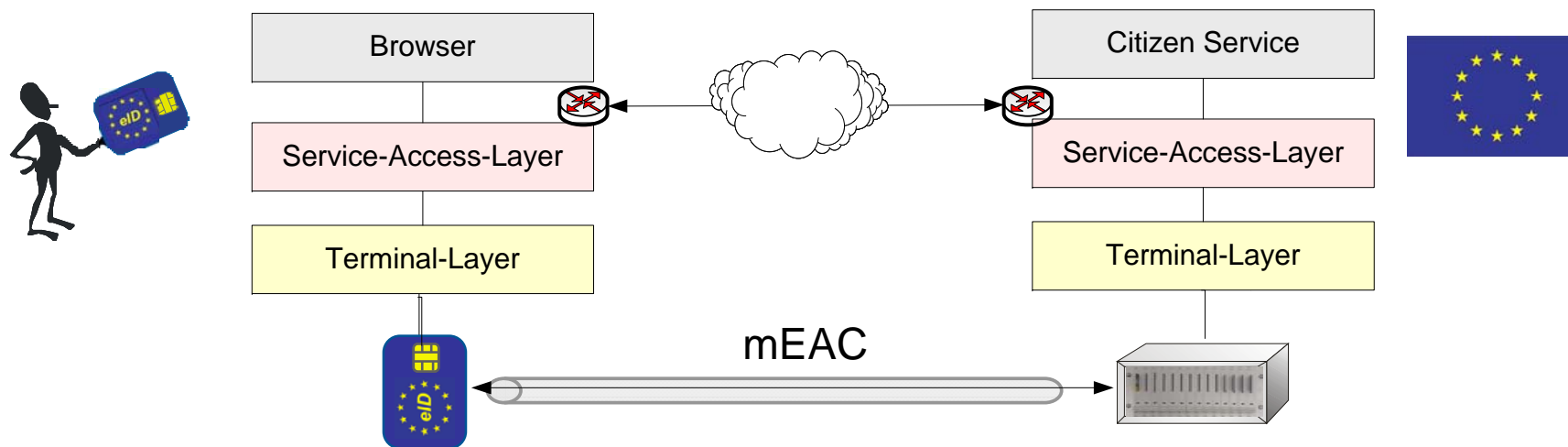


Remote Loyal & ICC Stack (Citizen Services with mEAC)



Giesecke & Devrient

secunet





ISO/IEC 24727 for mobile devices



Giesecke & Devrient

secunet



Agenda

- ISO/IEC 24727
- **Using ISO/IEC 24727 for mobile devices**
 - **with Mobile Signature Service**
 - in a Java Micro Edition environment
- Summary



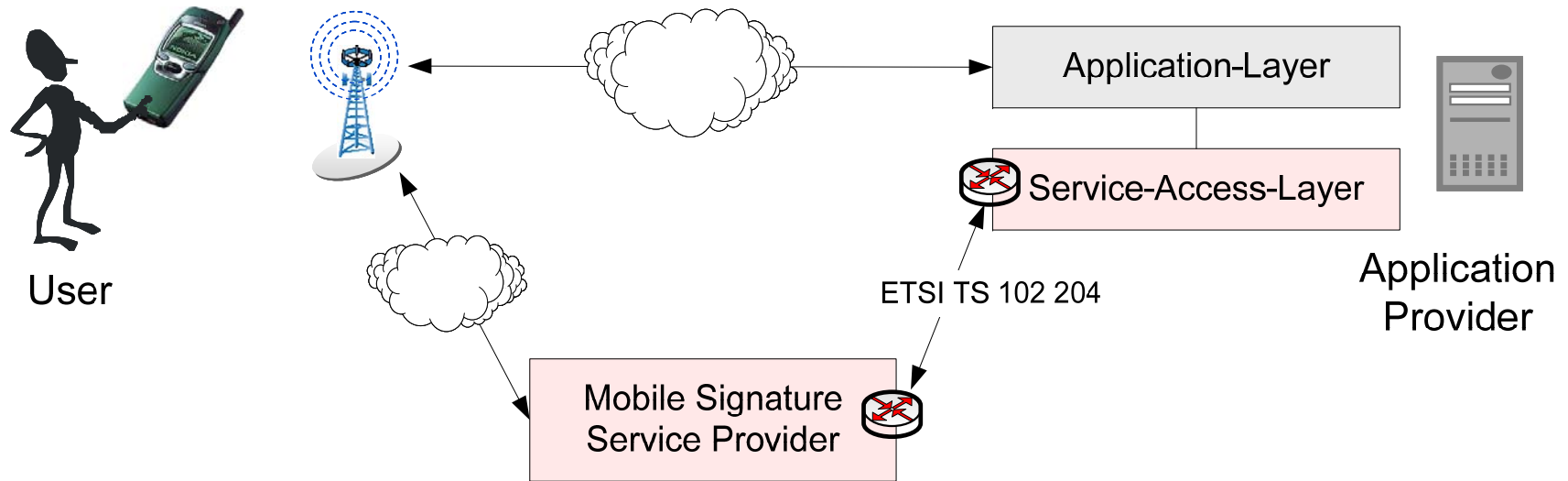
Mobile Signature Service



- ❑ Specifies Web Service Interfaces between
 - ❑ Application Providers (AP) and
 - ❑ Mobile Signature Service Providers (MSSP)which allow to create digital signatures with mobile devices
- ❑ Standardized by ETSI
 - ❑ TR 102 203 (Business & Functional Requirements)
 - ❑ TS 102 204 (Web Service Interface)
 - ❑ TR 102 206 (Security Framework)
 - ❑ TS 102 207 (Specifications for Roaming in M-signature Services)



Mobile Signature Services Integration





Mapping ISO/IEC 24727-3 to ETSI 102204



[ISO24727] Part 3	[ETSI-102204]	Note
CardApplication Path	/	Besides path-information of regular card-applications, CardApplication Path will also return a path to the „virtual card-application“ for [ETSI-102204].
CardApplication StartSession	MSS_HandshakeReq	Using this function the AP and the MSSP agree on security mechanisms for further requests and responses.
DIDCreate / DIDUpdate	MSS_RegistrationReq	The keys of the mobile users are represented as Differential-Identities (DID). Consequently the creation of a DID corresponds to the registration of a user.
DIDGet	MSS_ProfileReq / MSS_StatusReq	DIDGet will be used to obtain information about a user profile and the status of a current transaction.
DIDAuthenticate	MSS_SignatureReq	Using the signing capability of the mobile device it is possible to design a challenge-response protocol for authentication.
Sign	MSS_SignatureReq	The signing capability of the mobile device may be also be used via the Sign function. As in [BSI-TR03112] the low level Sign function may be wrapped by a SignatureRequest according to [OASIS-DSS].



ISO/IEC 24727 for mobile devices



Giesecke & Devrient

secunet



Agenda

- ISO/IEC 24727
- **Using ISO/IEC 24727 for mobile devices**
 - with Mobile Signature Services
 - **in a Java Micro Edition environment**
- Summary



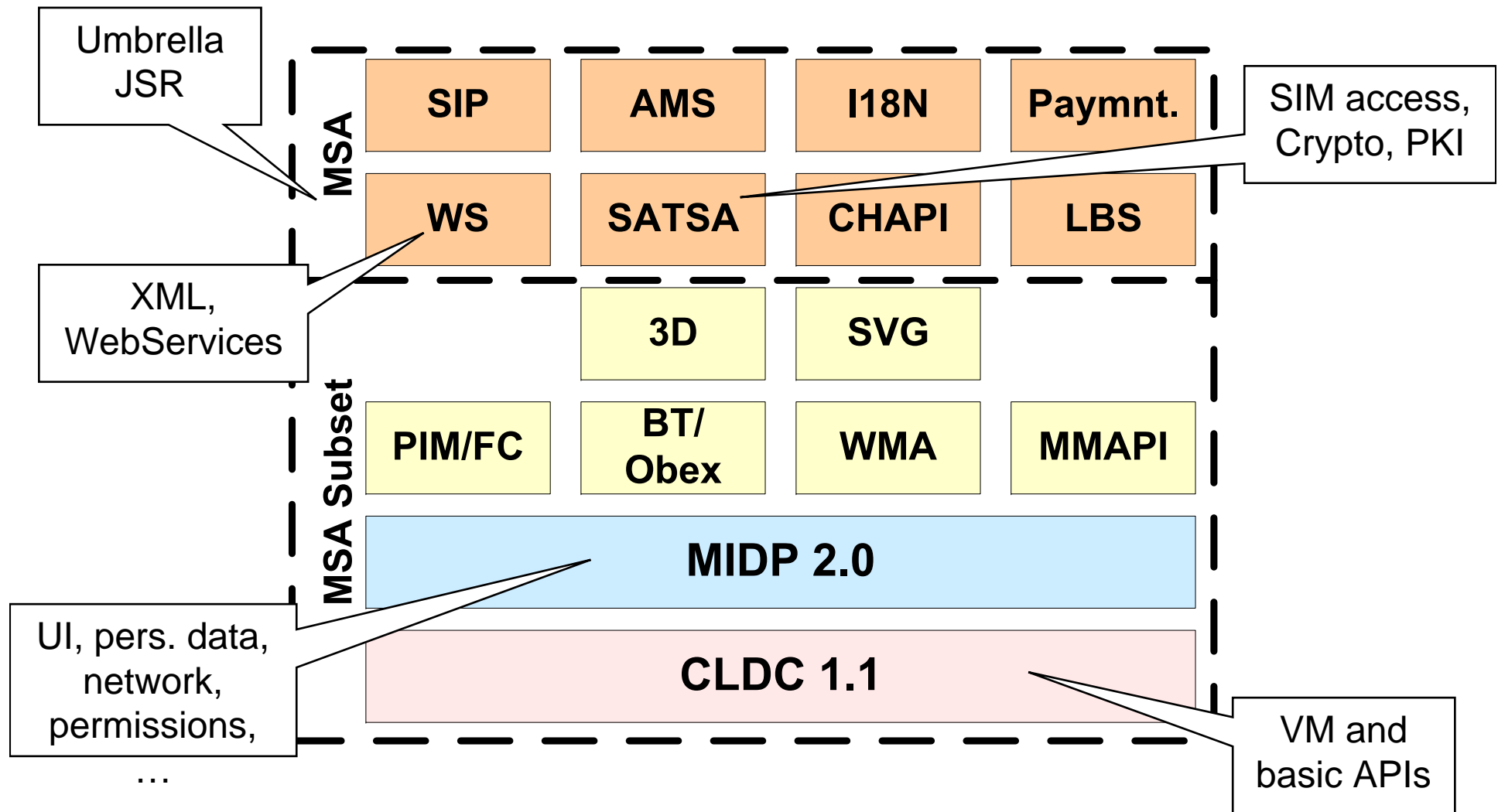
Java™ Micro Edition (JME)

- ❑ Started in Japan in 1999
- ❑ Basic Standards (MIDP 1.0 and CLDC 1.0) available since 2000
- ❑ First MIDP cell phones available since 2000 (e.g. Siemens SL45i)
- ❑ The Mobile Service Architecture defines a powerful platform
- ❑ Lot's of additional API's (SVG, M3G, MMAPI, BT, PIM, CHAPI, SIP, LOCATION, ...)
- ❑ Deployed in over 2.1 billion mobile devices



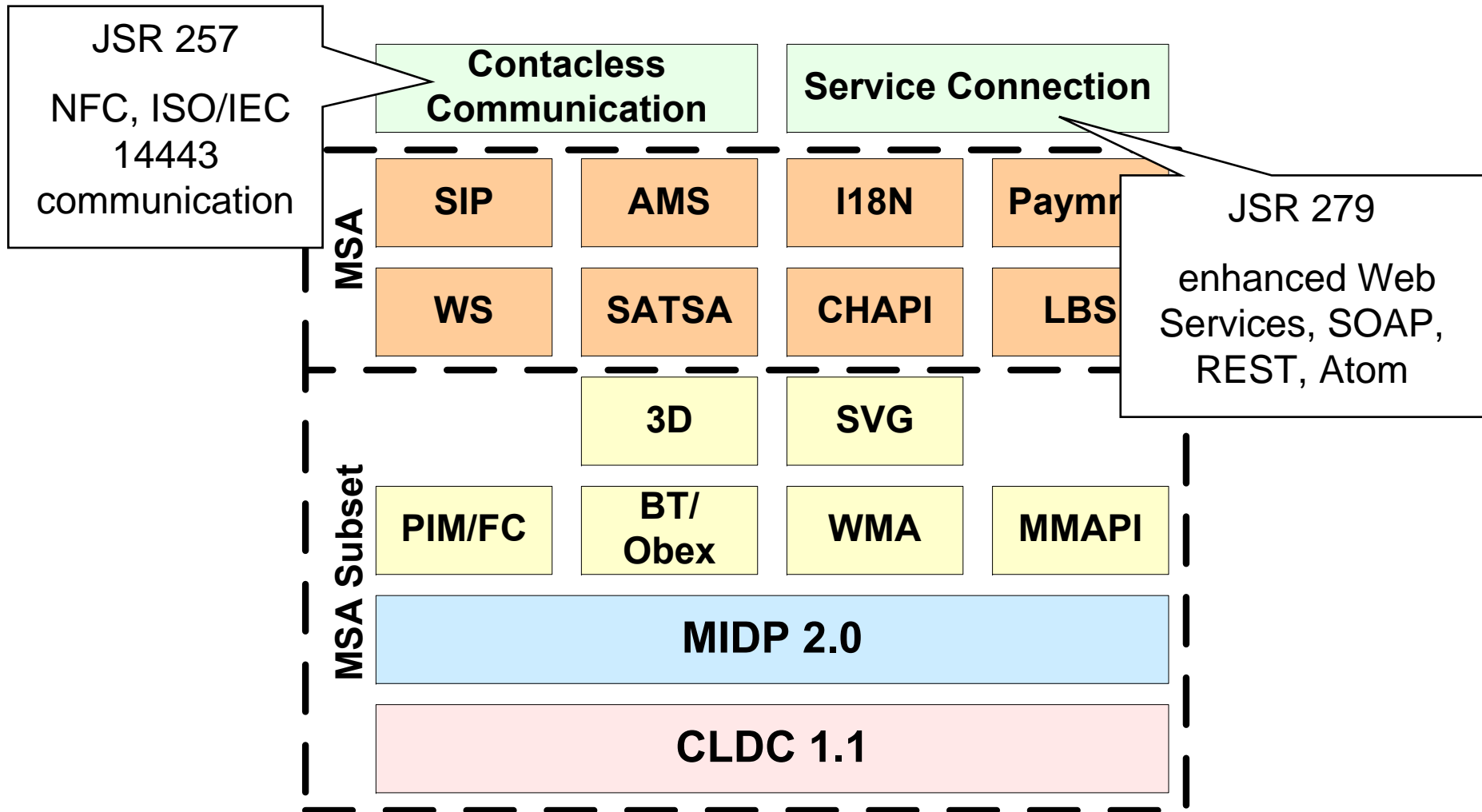
JME Architecture

Mobile Service Architecture (MSA)



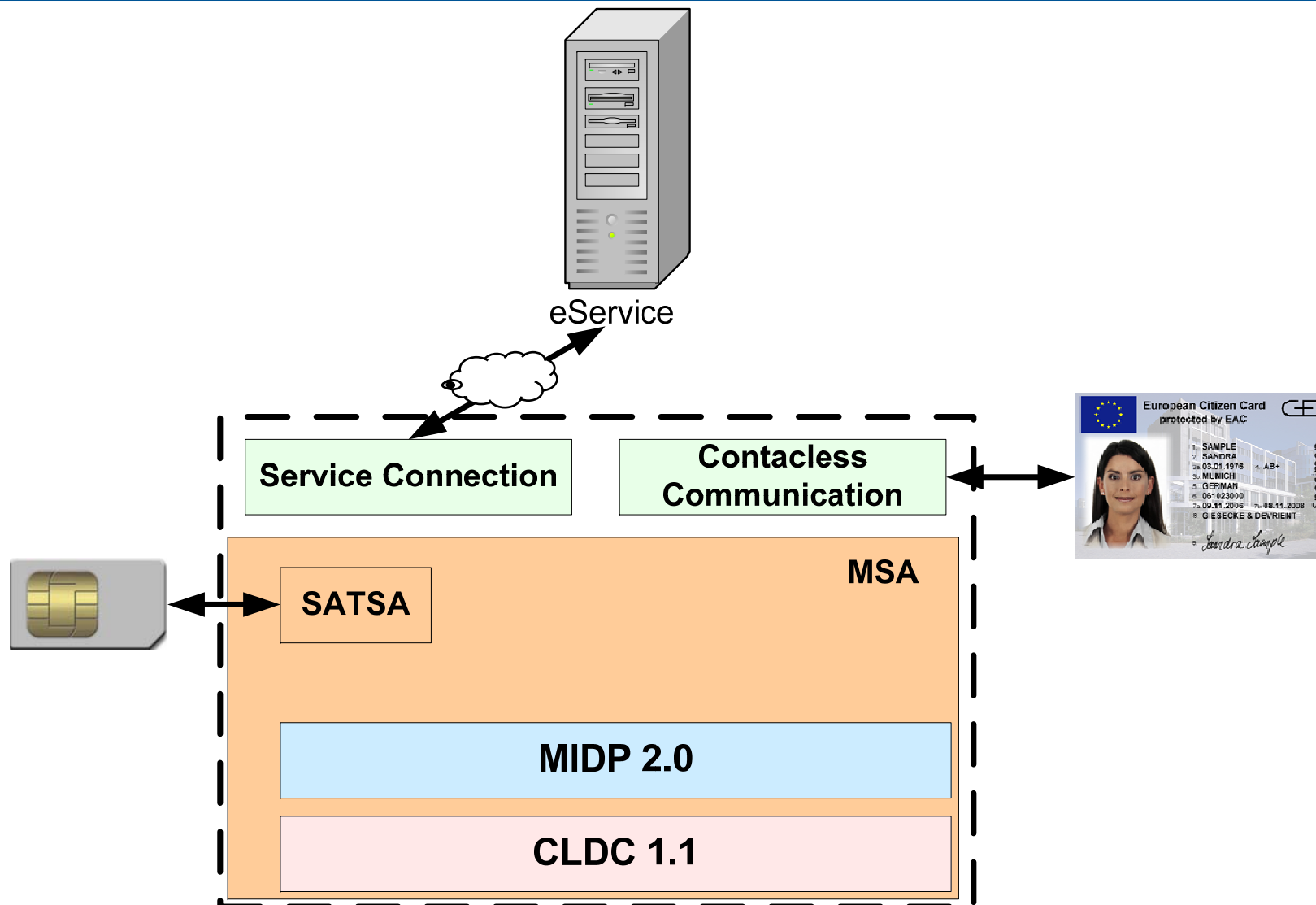


Additional JSR's



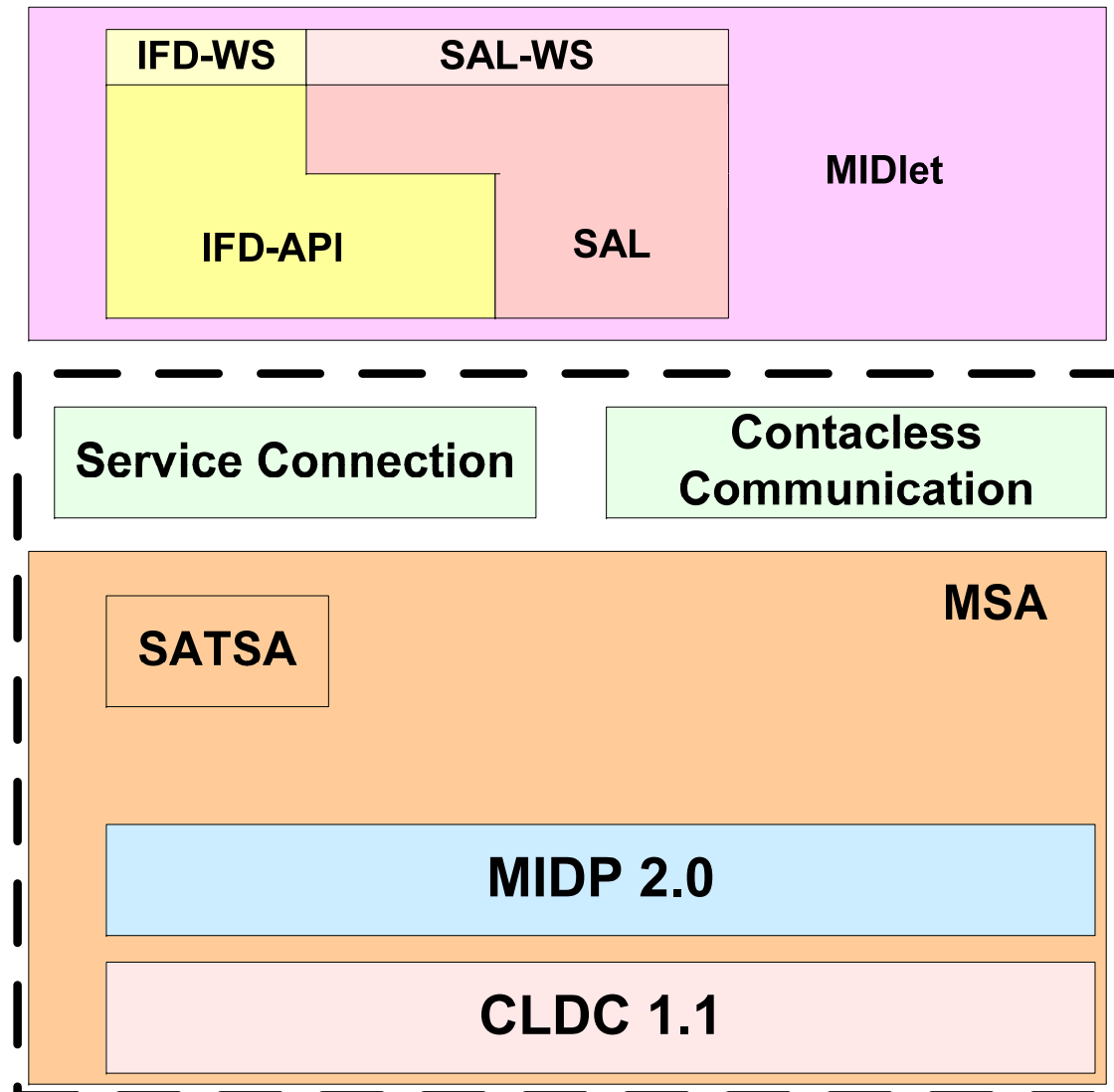


The complete picture





MIDlet Integration of ISO/IEC 24727





ISO/IEC 24727 for mobile devices



Giesecke & Devrient

secunet



Agenda

- ISO/IEC 24727
- Using ISO/IEC 24727 for mobile devices
 - with Mobile Signature Service
 - in a Java Micro Edition environment
- **Summary**



Summary

- ❑ ISO/IEC 24727 about to become *the* global eID-standard
- ❑ MSS-based integration possible with
 - ❑ arbitrary mobile devices,
 - ❑ but requires additional infrastructure services (MSSP)
- ❑ JME offers the necessary functionality to integrate mobile devices into the ISO/IEC 24727 infrastructure
- ❑ NFC will push forward to integrate contactless communications into mobile devices
- ❑ In the mid-term, a JSR for a standardised JME interface to ISO/IEC 24727 would be beneficial



Deadline: 15.05.2008

Call for Papers - BIOSIG 2008

Biometric Border Control & Federated
Identity Management

September 11/12, 2008, Darmstadt

<http://www.biosig.org>



**Thank you very much
for your kind attention!**



Contact:

Dr. Detlef Hühnlein
secunet Security Networks AG
detlef.huehnlein@secunet.com