Integration of Smart Cards in Public Key Infrastructures

Open CAWorkshop

Dr. Stephan Spitz

Stephan.Spitz@gi-de.com

Giesecke & Devrient GmbH

Overview

1. **Why to use Smart Cards in a PKI ?**
2. **Available Interfaces for the Smart Card Integration in a PKI**
3. **Smart Card Integration in Future**

Why Smart Cards ?

- **High physical protection of the stored data, especially the private key**
- **Flexible configuration of access conditions to use the private key for signature operations**
- **Duplication of private keys can be prevented (this is not so with a soft PSE)**
- **Security evaluation according ITSEC E4 high or CC EAL 4+ or even higher**
- **Use of already available smart card infrastructures e.g. future ECC (European Citicen Cards) or eHealth cards**

The Smart Card as a secure Process Environment

- **High performant and secure crypto unit supporting RSA operations and Hash calculations**
- **Secure communication channels to the smart card offer the possibility of a confidential data exchange**
- **On card key generation is possible (RSA, ECC)**
- **Secure runtime environment for small Java Card applications**
- **Multi application and in future multi process environment**

Overview Smart Card Access

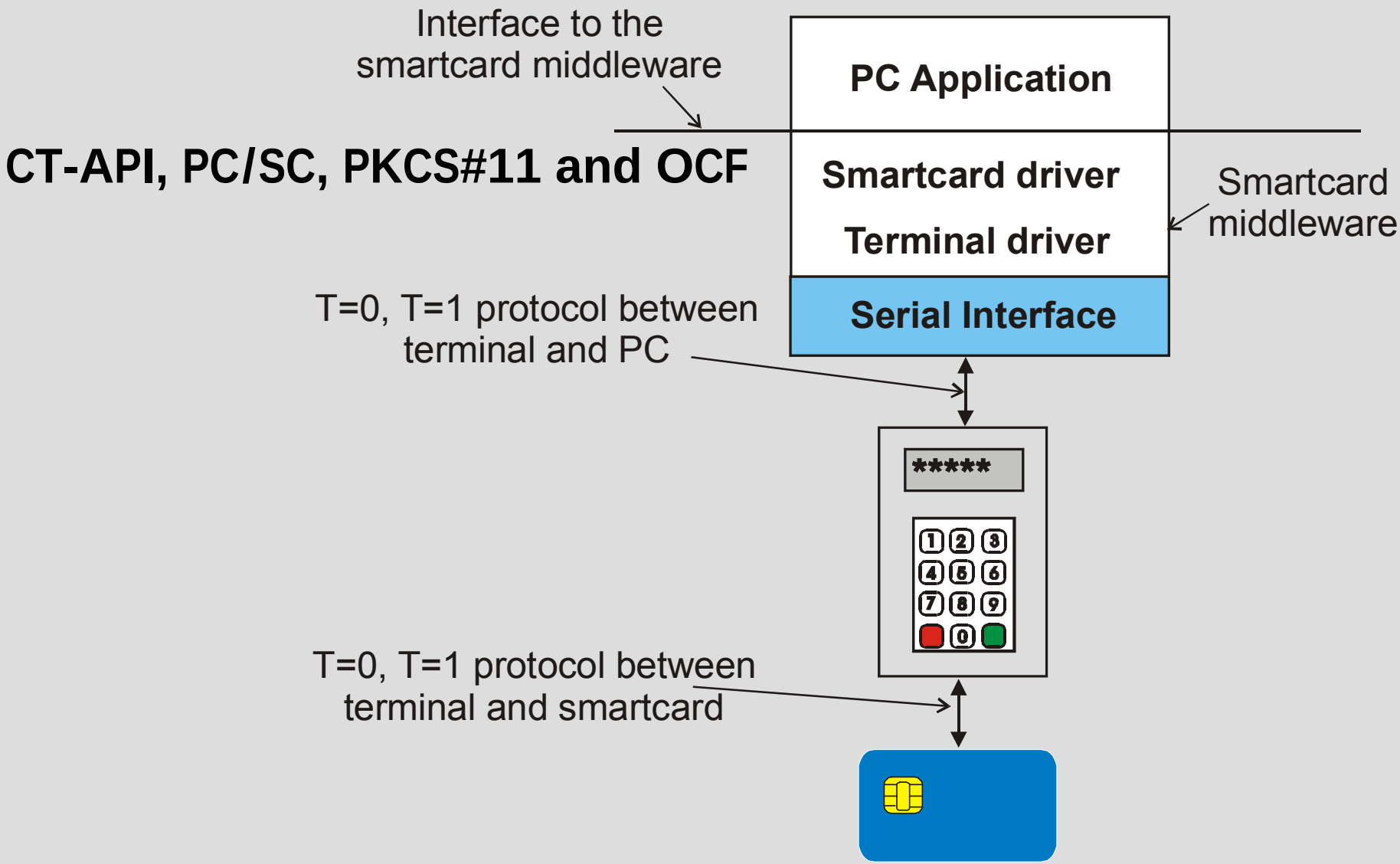
- Currently mainly T=1 protocol is used between PC, terminal and smart card
- Future smart cards will support USB (ICCD, EEM), sMMC and fast serial protocols
- ISO 7816 specification describes T=1, T=0 protocol and smart card application interaction with APDUs
- Smart card middleware and terminals are currently necessary to interact with the smart card
- Future TCP/IP based smart cards/security tokens will not need a terminal and moreover no middleware

Available Interfaces for the Smart Card Integration in PKIs

- **Currently for the interaction with smart cards the following interfaces are used:**
  - **CT-API**
  - **PC/SC**
  - **PKCS#11 and MS CSP**
  - **OCF**

- **Future smart cards will offer interfaces (USB, MMC) which simplify driver installation and can be accessed via TCP/IP**

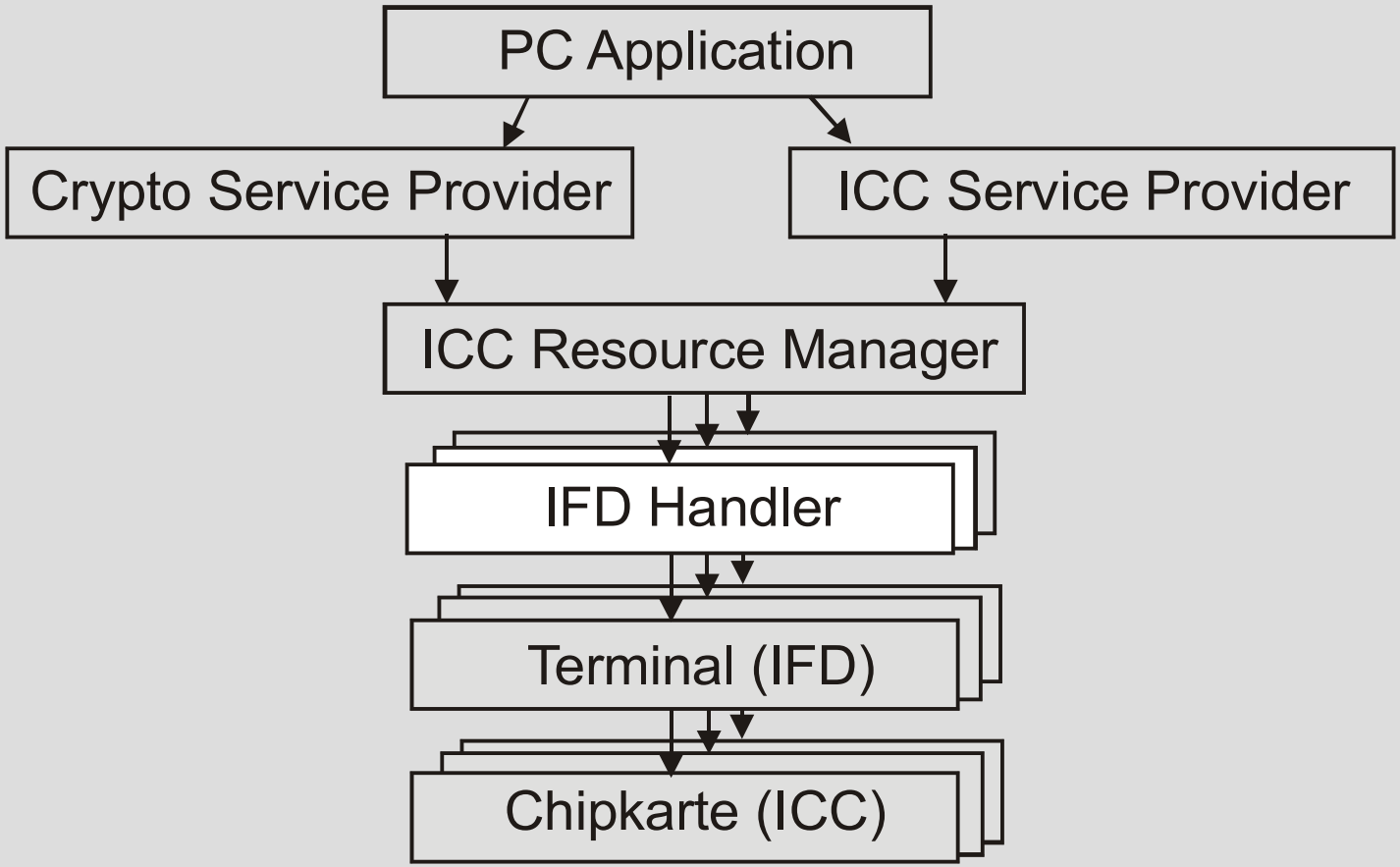
Current Smart Card Access



Card Terminal API

- **Card Terminal API (Application Programming Interface) is a simple API containing only three function calls: CT_init(), CT_close() und CT_data()**
- **PC application is responsible for the generation and handling of ISO7816 APDUs**
- **PC application needs a lot of information about the smartcard operating system, initialization and personalization**
- **Offers a wide variety of smart card functionality but demands a lot of integration work**

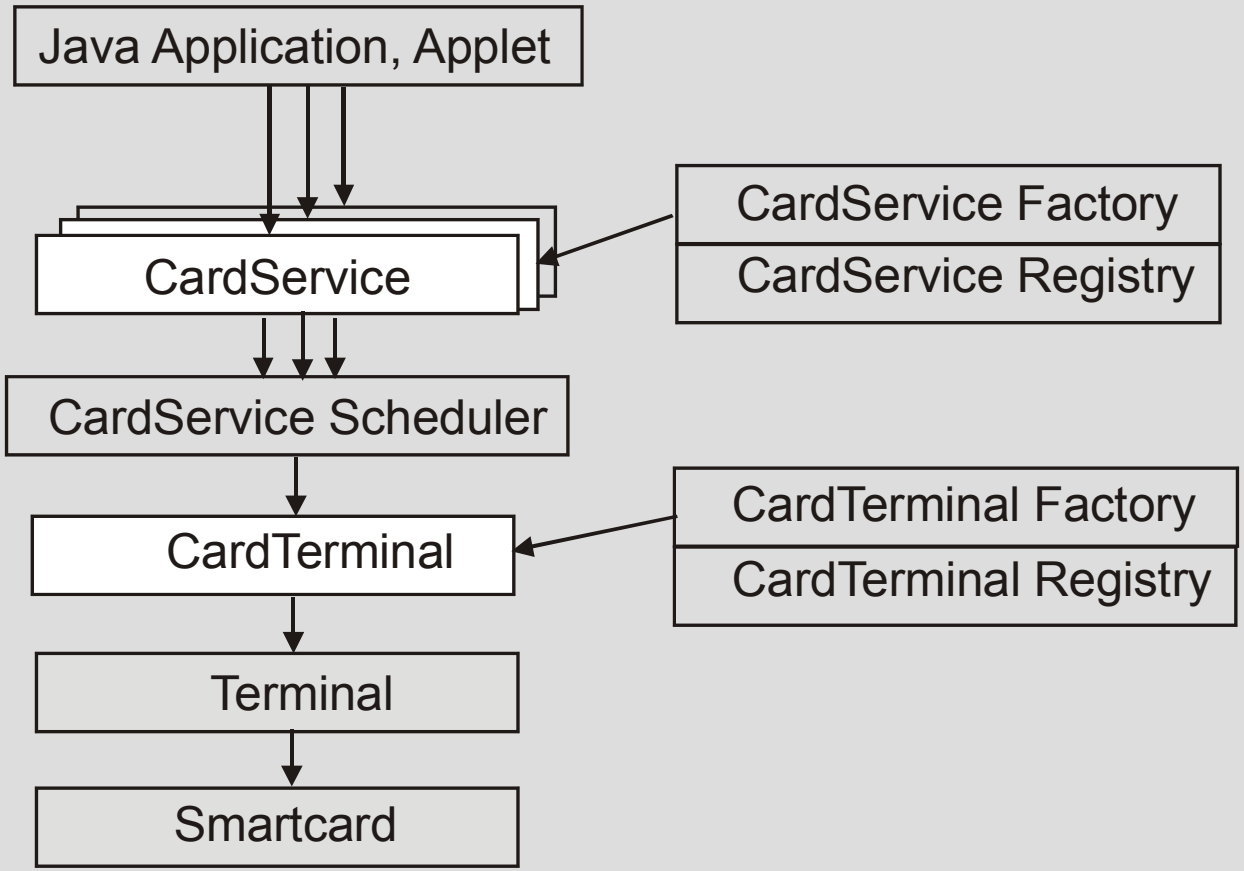
PC/SC Specification



PC/SC Characteristics

- **Personal Computer/Smart Card specification covers the integration of smartcards in a multi user and multi tasking PC operating system**
- **Encapsulation of the smartcard via a Crypto Service Provider and ICC Service Provider**
- **APDU independent integration of smartcards in the PC application**
- **PC/SC driver mostly available for Win platforms**

Open Card Framework (OCF)



OCF Characteristics

- **Java interface for the integration of Smart Cards in Java applications and Applets**
- **Strict separation between terminal (CardTerminal) and smartcard (CardServices) interaction**
- **Dynamic load of OCF drivers via Browser („No-Second Rollout“)**
- **Platform independent because of Java runtime environment**
- **Resource management enables simultaneous use of the Smart Card in different Java applications**

Overview current Smart Card Interfaces

Interface	**Available Smartcard Functionality**	**Supported PC Operating Systems**	**Availability**	**Integration Efforts**	**Timing**
CT-API	Whole smartcard functionality	Always Win32 and on several Unix systems	Available for all smartcards and terminals	Strongly dependent on the desired functionality	Fast smartcard access, but no resource management
PC/SC	Dependence on the ServiceProviders functions	Mostly Win32	Available for the most terminals and smartcards	Different smartcards can be supported	Strongly dependent on the implementation
PKCS#11	Interface only for PKI applications	Win32, Linux, Solaris	Only available for some combinations of smartcards and terminals	Easy to use in combination with PKI applications	Strongly dependent on the implementation
OCF	Strongly dependent on the different Card Services	All systems with a Java runtime environment	Available for a few terminals, all CardServices are seldom implemented	Easy integration in Java applications and Applets	Not very fast, because of Java-Interpreter

The Future

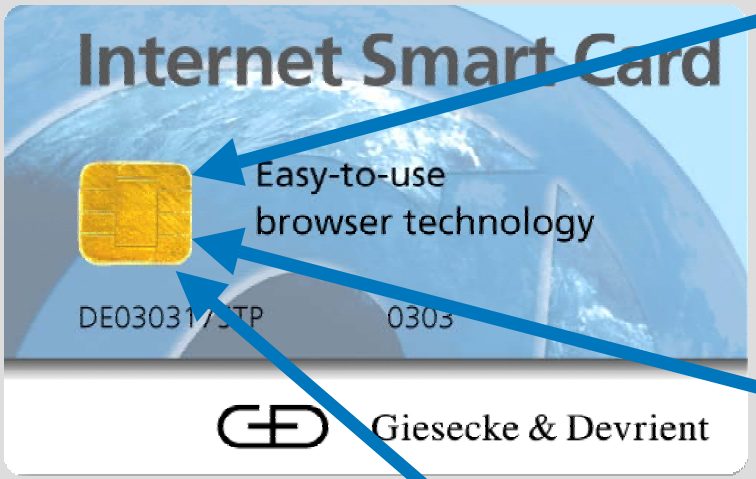

Internet Smart Card
Easy-to-use
browser technology
DE0303175TP
0303
Giesecke & Devrient

What IP Connectivity Means

Future smart cards will act as network devices (server or client):

- **Implementation of a TCP/IP stack on the smart card**
- **Support of network management/configuration**
- **Availability of on-card services via application-level protocols (at least HTTP)**
- **Triggering of different applications via communication channels, allowing concurrent program execution**

What Multiple Channels Means



Web services hosted on the smart card allow the parallel execution of functions.

Multiple servers listening on different TCP ports offer various IP-based services (e.g., FTP, HTTP, etc.).

Multiple connections on the same TCP port allow the execution of different instances of a (Java Card 3) program.

Future Connectivity Profiles According to InspireD

		Low End	High End	M.Media	Contactless	Legacy
7	Application	HTTP	HTTP	HTTP	HTTP	HTTP
6	Presentation					
5	Session					
4	Transport	TCP	TCP	TCP	TCP	TCP
3	Network	IP	IP	IP	IP	IP
2	Data Link	SLIP	RNDIS/CDC EEM	MMC	SLIP	7816-3
1	Physical	USB	USB		NFC/ 14443	

Security Challenges with IP Connectivity (1)

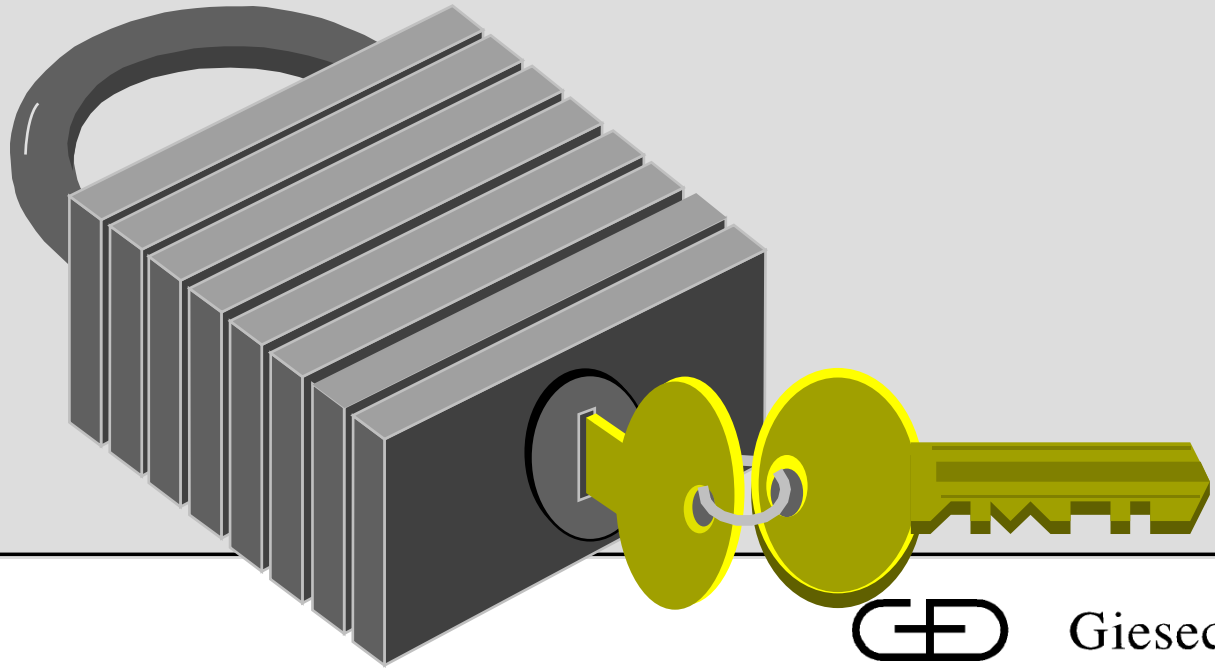
- A simple port scan cannot be misused to analyze the smart card and gain information about active services and servers on the smart card.
- Typical attacks which use buffer overflows in a server to execute malicious code will be impossible on smart cards.
- Unauthorized commands which manipulate input in HTML forms processed by a Common Gateway Interface (CGI) on the smart card will be impossible.

Security Challenges with IP Connectivity (2)

- The network management necessary for organizing the IP connectivity of the smart cards cannot be used for attacks, as the case in other IT systems.
- Authentication and encryption is mandatory for safe connections which are resistant against known attacks (e.g., Man-In-The-Middle prevented from sniffing and spoofing).
- Standard security protocols such as SSL/TLS are used in a high-performance implementation to ensure interoperability to other network devices.

Security Challenges with IP Connectivity

Vendors of smart card operating systems will assure that the wide variety of network attacks (e.g., spoofing, sniffing, fragmentation attacks, session hijacking, D/DoS, etc.) cannot be transferred to the future TCP/IP based smart card world.



Thank you for your attention!