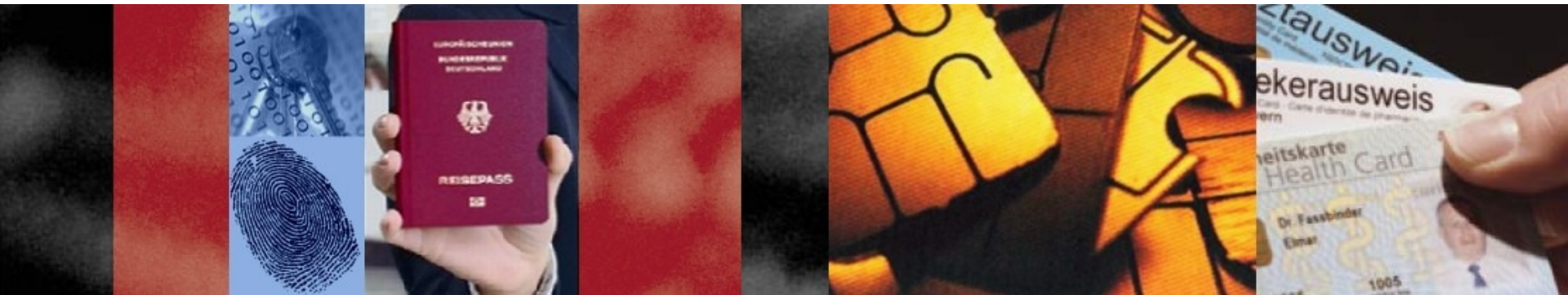




The use of Common Criteria for the German Health System



Dr. Markus Mackenbrock

**Bundesamt für Sicherheit in der Informationstechnik (BSI)
Federal Office for Information Security**



Introduction of the BSI



- National Authority for Information Assurance established by law in 1991
- Certification according to CC and ITSEC
- Development of test requirements like Protection Profiles (PP) and Technical Guidelines (TG)
- Accredited evaluation labs: (12 for CC)
- Types of products certified:
HW, smart card controllers, OS, SW
- Protection Profiles released: >40
- ...

Introduction

The electronic Health Card (eHC):

Due to be rolled-out nation wide in 2009, the electronic health card is one of Germany's most important public sector IT projects.

The card is designed to guarantee the secure exchange of data between

- insured parties
- doctors
- pharmacists and
- health insurance companies

and will serve to validate patient's identity rather than to hold their electronic medical record.

Introduction

The eHC is a microprocessor chipcard (SmartCard) with cryptographic functions.

The personalized eHC contains essential information about the card-holder, the holder's picture and signature.



Introduction

Introduction to the German eHealth Card

Reasons:

Improvement of the quality and availability of health data:

- better information systems for medical service providers
- more efficient communication
- better availability of relevant data for treatment
- prevention against fraud
- increase of treatment quality
- higher cost efficiency



Design of the eHC



Reverse side



Applications

Mandatory applications:

- identity data / cardholder identification
- e-prescription
- EHIC - European Health Insurance Card

Optional applications:

- Emergency data
- Doctor's notes
- Patient's medicine data
- Patient records
- ...

For these optional applications the patient has to give his consent.





Development of IT security testing requirements at the instigation of the government.

- In agreement with different ministries BSI develops evaluation requirements in cooperation with its accredited test laboratories and the IT industry

In detail:

Development of

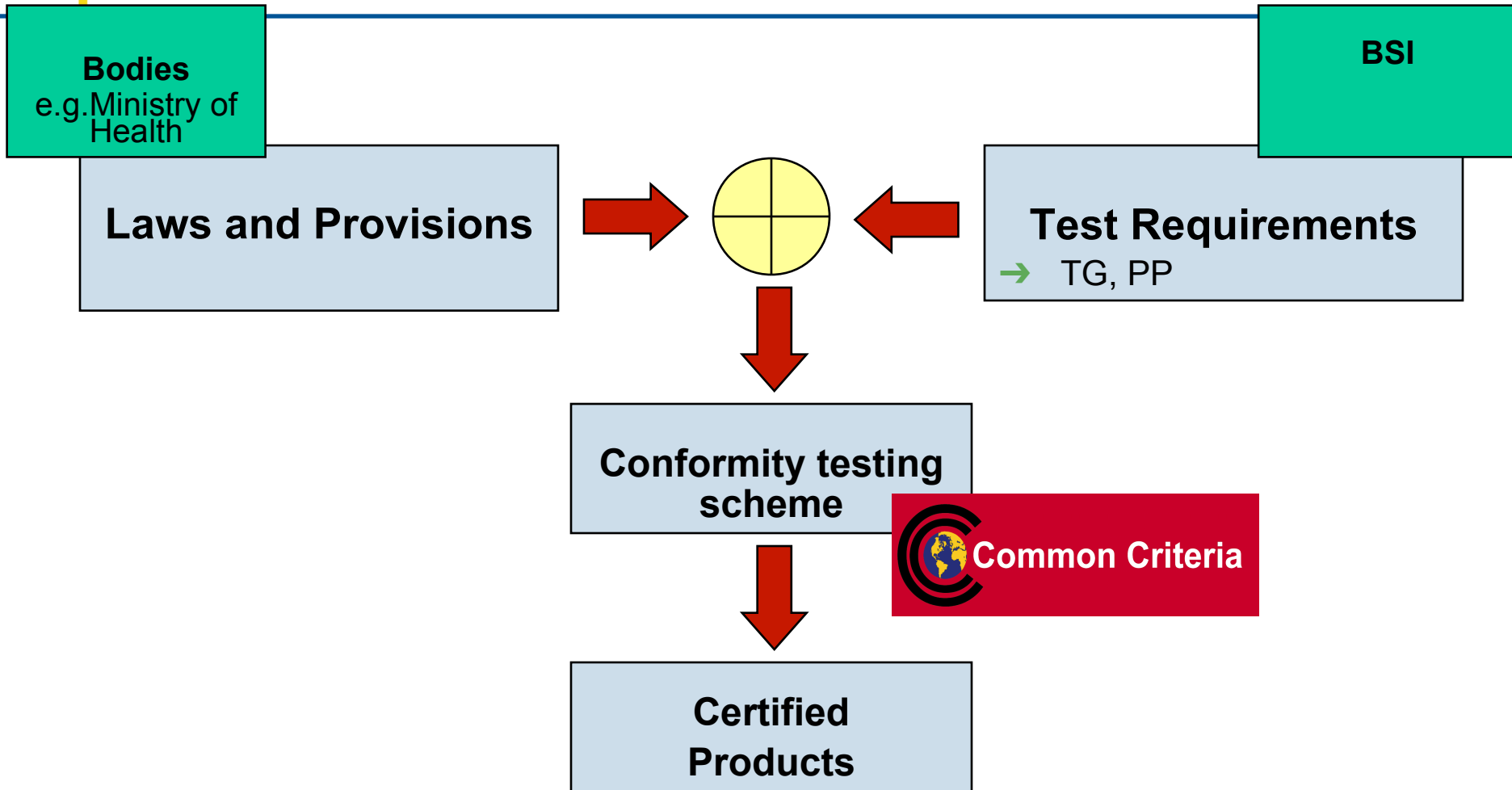
- Protection Profiles and

- Technical Guidelines *(In German: Technische Richtlinien TR)*

for the evaluation and certification of products and components



Testing Requirements/ Protection Profiles

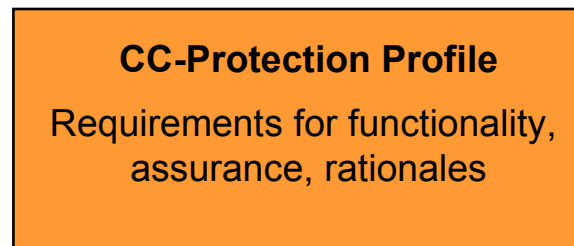




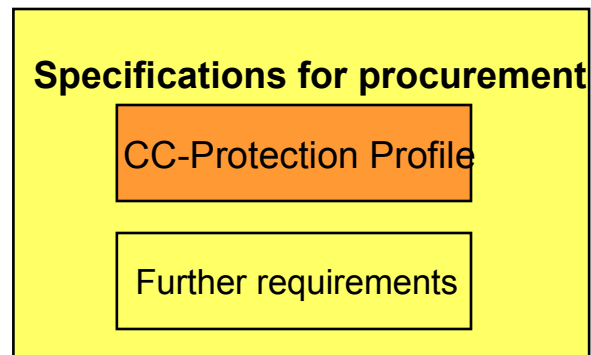
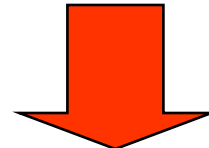
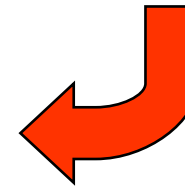
The Concept



**Functional
Requirements**



**Assurance
Requirements**



eHC - Specification

The eHC specification defines:

- ▶ Mandatory commands of the eHC
- ▶ the crypto algorithms used, e.g. RSA, DES, SHA-1
- ▶ Crypto protocols, e.g. Secure Messaging
- ▶ Required data structures within the eHC
- ▶ Data access rules

For a PP these elements have to be defined by the
“Security Functional Requirements” of the CC





Approval of Components for the Telematic- Infrastructure

gematik

Approval body, oversees the German e-health card project

Functional Tests

Functional Tests

Conformity tests
Integration tests
Interoperability tests
by
gematik

Security tests

IT security certification
Approved certification body
BSI

Material tests/ Safety Tests

Electrical, physical and
mechanical tests
Test laboratories

Legal basis for the eHC: § 291 SGB V - Krankenversichertenkarte

Protection Profiles for the German Health System

Key Security Components to be certified:

eHC – Insurance card for 80 mill. patients. It replaces the KVK (magnetic strip only) in 2009

HPC - Health professional card for some 500.000 doctors, pharmacists etc. (for all health care providers and medical service providers)

SMC – Secure module card; card to be used by an institution (doctor's practice, hospital etc.)

Connector – Connects and controls the doctor's practice and the Telematic Infrastructure (access rights etc.)

Card Terminal – Write and read the different cards

eKiosk – Terminal for the patient to read and set permissions on the eHC

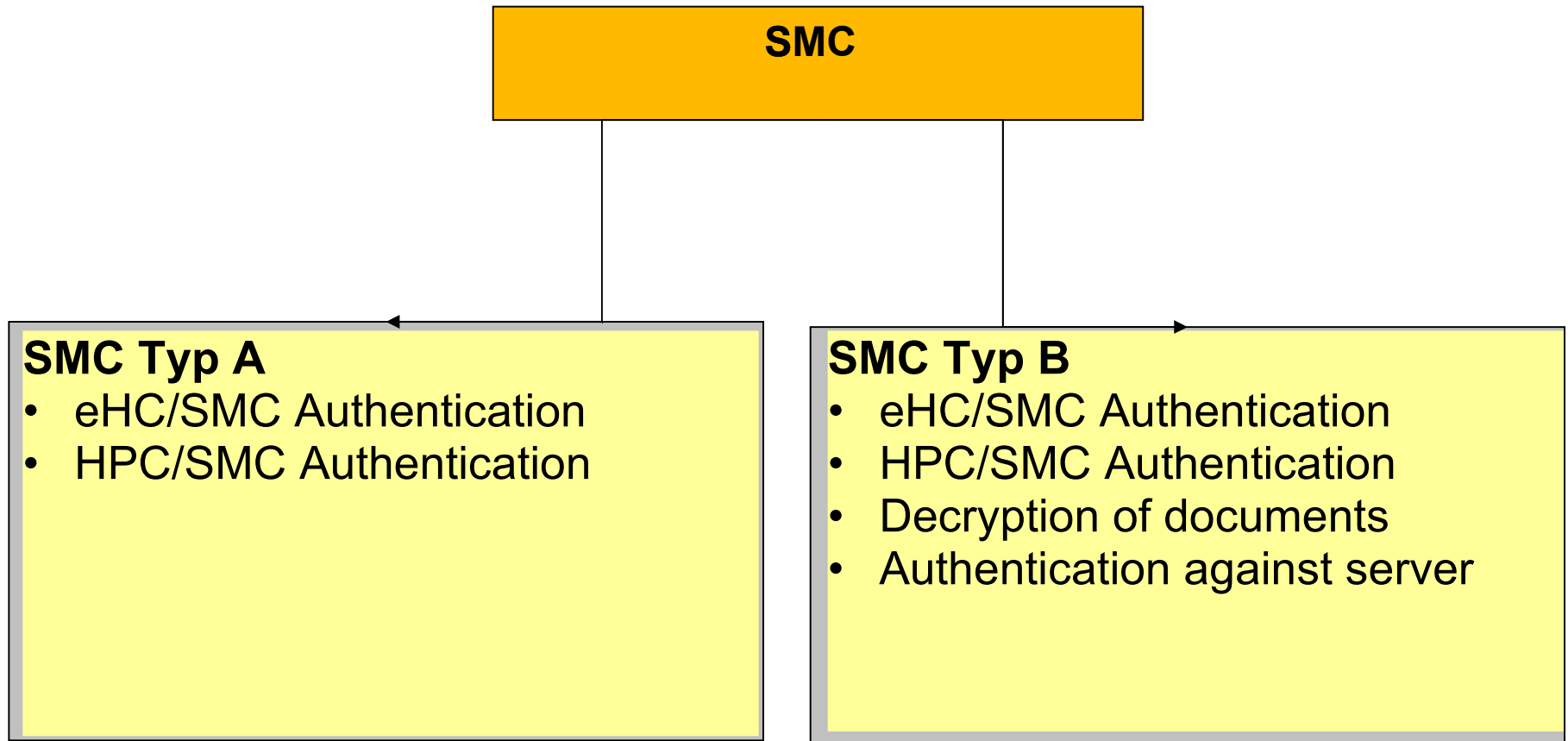


HPC: Functions and Tasks:

- Authentication of the card holder by means of a PIN,
- Mutual authentication between the HPC and an electronic Health Card (eHC)
- Mutual authentication between the HPC and a Security Module Card (SMC)
- Decipherment of health data for external applications
- Client-server authentication for a client
- Qualified electronic signature



SMC (Secure Module Card)



The communications infrastructure is protected against access by several gateways.

The connector provides the functionality of a VPN-client and includes a packet filter.

4 Different connector types/parts:

- SM-K (secure module)
- Network connector
- Application connector “enhanced basic“
- Application connector “high“

Protection Profiles for the German Health System

These PPs are developed for CCv2.3 as well as for CCv3.1.

All PPs for eHC, HPC and SMC require:

CC Version 2.3:

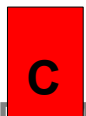
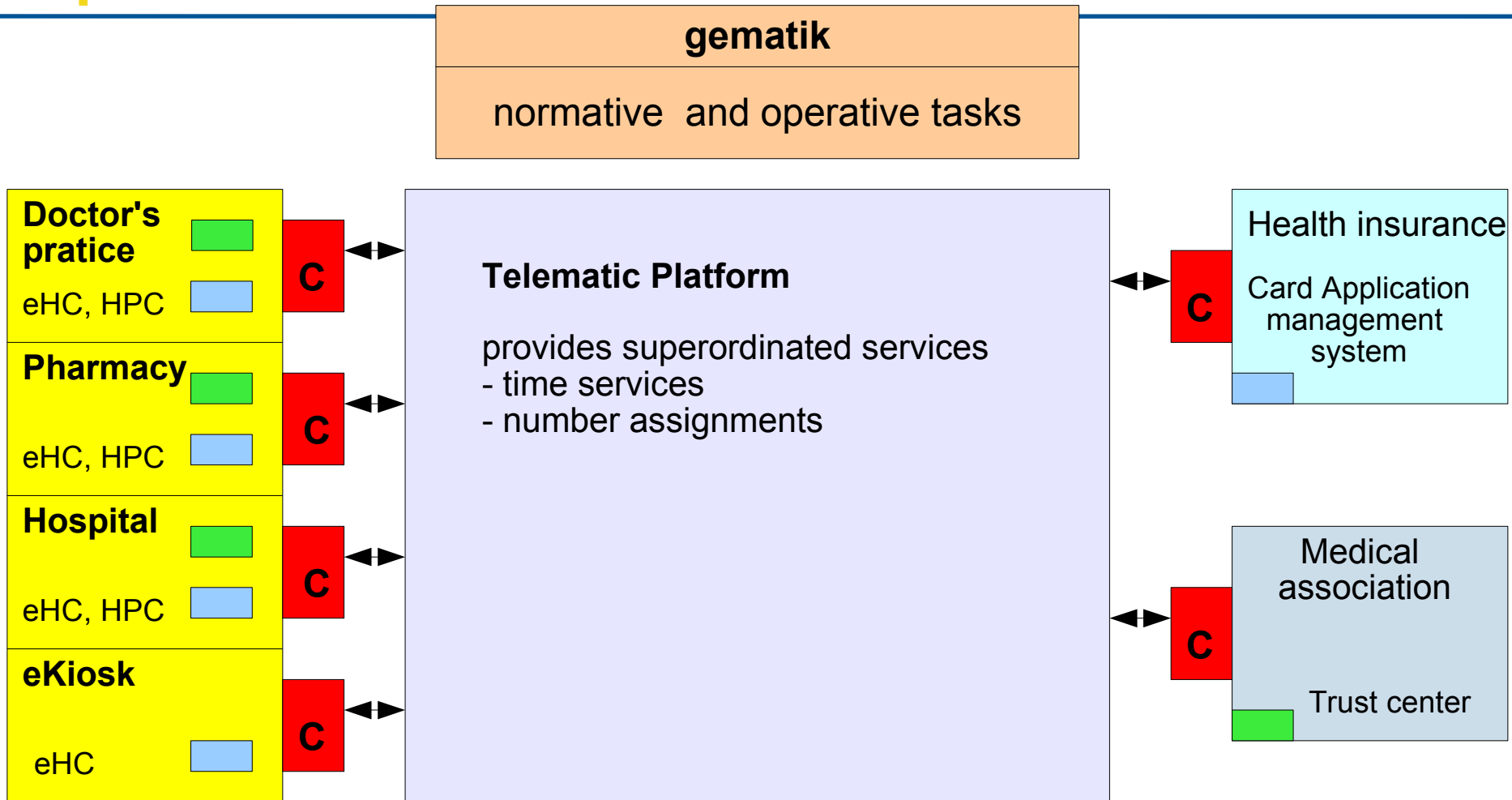
EAL4, SOF high and augmented by AVA_MSU.3 and AVA_VLA.4

CC Version 3.1: EAL4, augmented by AVA_VAN.5

These requirements are state of the art for chip cards/ smart cards.



Infrastructure



Connector



Health Professional Card



electronic Health Card



Special Problem: Number of signatures for prescriptions

Each prescription must be signed by using a qualified electronic signature.

This may be about hundred signatures each day.

The German electronic signature act describes only the single signature in detail.

Other use cases have to be interpreted:

- Batch signature
- Convenience signature

Batch signature

Conventional PIN method:

- each electronic prescription has to be signed electronically by a 6-digit PIN

Batch signature method:

The single input of a 6-digit PIN enables the electronic signature of

- multiple electronic prescriptions within a fixed time scale
- or
- a definite number of electronic prescriptions



Batch Signature

In detail:

A number of documents/lots of data have to be signed

The Secure Viewer Component enables the inspection of the documents to be signed.

- Confirmation of the documents chosen
- One-time input of the PIN on a terminal
- Signing the documents and closing the signature card after completion



Convenience Signature

Input of the PIN (one time) at the beginning of working hours (to activate the signature card).

The number of documents which have to be signed is not yet fixed at this time.

- Selection of documents during working hours
- Possibility to display the document(s)

Activation of the signature during working hours by an additional authentication by a token

- by using a biometric device
or
- by presentation of a shortened PIN (e.g. 3 digits)



A combination of both methods is possible. A batch of documents to be signed can be signed by using the convenience signature method.

This methods will be used for the HPC within the German health system.

BSI has developed two Technical Guidelines (TR 03114 and TR 03115).

The implementation of these methods requires cryptographic functions.

For the application within the German health system BSI has developed and published the Technical Guideline BSI-TR-03116 for all eCard projects of the government.

Product list for the German eHealth System
in evaluation/finalised (June 2009):

Product Type	Products
eHC	7
HPC	8
HSM-module	2
SMC	2
Connector	4
VPN-concentrator	1
Terminals	16



Conclusions

CC are more and more required for public procurements like:
US-Gov't Directive, G8-CIP-Principles, EU, NATO.

In Germany: Health system, electronic signature law, passports,
ID-card...

The concept of Protection Profiles and Technical Guidelines
provides IT developers an adequate specification/method of
their IT security requirements.



Conclusions

The German Health System

All security relevant components of the Telematic Infrastructure will be evaluated and certified, based on testing requirements like PPs and TRs of BSI.

Based on this fact almost every citizen in Germany will own at least one Common Criteria certified product.

This is a big outcome and success for the Common Criteria !





Further Information

- for the Protection Profiles and Technical Guidelines:
www.bsi.bund.de.

- for the functional specifications of the German health system:
www.gematik.de.



Contact



Bundesamt für Sicherheit
in der Informationstechnik (BSI)

Dr. Markus Mackenbrock
Godesberger Allee 185 - 189
D- 53175 Bonn

Tel: +49 228-9582-5334

Fax: +49 228-10-9582-5334

Markus.Mackenbrock@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de