



Evaluation of Cryptographic Implementations in the German CC Scheme

Bernd Kowalski,
Bundesamt für Sicherheit in der Informationstechnik

Wolfgang Killmann,
T-Systems GEI GmbH

11. ICCS Antalya 2010



Overview of the presentation

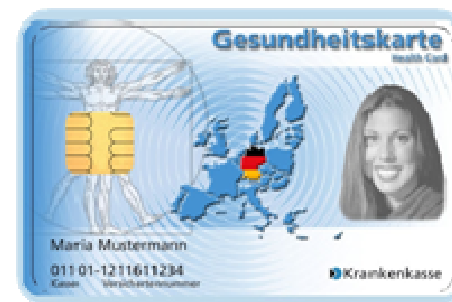
- **Introductory remarks concerning the BSI Certification Scheme (provided at the conference)**
- How does the German Scheme ensure
 - the use of strong cryptographic algorithms and protocols?
 - state of the art cryptographic techniques in development, evaluation and certification?
- How do we evaluate cryptomodules in the German Scheme?
 - Evaluation Scheme documents
 - Skills of evaluators and labs
 - Vulnerability analysis of cryptomodules
- Conclusions



Introductory Remarks

Motivation

- Increasing need for evaluation of cryptographic implementations for commercial and governmental application
- Public projects with relevance to critical national infrastructures
 - ePassport and national eID-CardPublic
 - Health IT-infrastructure
 - Smart Metering in energy networks
- Market requirement for
 - reliable criteria for crypto-implementation
 - better transparency in crypto-evaluation
 - requirements specific to application areas





Instruments

- Technical Recommendations (TR) for
 - Basic algorithms & parameters (based on international standards)
 - Cryptographic requirements for specific applications, e. g. life cycles & lengths of keys
- Protection Profiles
 - Requirements for state of the art cryptographic implementation
 - Vulnerability analysis

Advantages

- Manufacturers, Customers
 - Improved transparency of requirements
 - Improvement for sales and comparability of products
 - Reduced device costs in standard application areas
- Certification Scheme
 - Transparency of evaluation criteria
 - Adjustability of security requirements to cryptographic applications

Endorsed cryptographic algorithms and protocols

- Strength of cryptographic algorithms and protocols
 - Subject of cryptanalysis
 - Cryptanalysis can not be afforded within evaluation process
- BSI certificates may, as a rule, include only endorsed cryptographic algorithms and protocols
 - Strength of these cryptographic algorithms and protocols have been analyzed by BSI crypto experts
- Non-endorsed cryptographic algorithms and protocols may be excluded from certification
- Cryptographic algorithms and protocols are endorsed for
 - governmental application like ePassport, eCard
 - applications supported by government like eHealth projects
 - other applications

Technical guidance

Endorsed algorithms and protocols for general use

- TR-02102 Cryptographic procedures: recommendations and key length

Endorsed algorithms and protocols for specific applications

- TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents
- TR-03116-1 eCard projects of Federal government (eHealths)
- TR-03116-2 eCard projects of Federal government (ID cards)

Other documents

- Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway: Overview of Suitable Algorithms for electronic signatures

➔ Strong Recommendation for Strength of Endorsed algorithms and protocols:
100 security bits



Protection profiles for cryptomodules

- BSI issued a set of protection profiles for cryptographic modules with different levels security functionality and assurance requirements
 - BSI-CC-PP-0045-2009 PP CM „Enhanced“
 - BSI-CC-PP-0042-2009 PP CM „Moderate“
 - BSI-CC-PP-0044-2009 PP CM „Low“
- PPs CM require state of the art cryptographic techniques for cryptographic modules like general purpose cryptoboxes
- The supporting documents for smartcards and similar devices may be relevant for the cryptomodules as well



Cryptographic techniques

- Strength of cryptographic algorithms and protocols will be ensured by assignment of endorsed algorithms and protocols in SFR components of the FCS class
- Key management techniques of key import and export are addressed by refinements of SFR FCS_CKM.1
- Protection against physical invasive attacks is required by SFR of the FPT_PHP family
- Protection against physical invasive attacks as side-channel analysis is required by an extended SFR FPT_EMSEC.1, ADV_ARC.1 (non-bypassability) and subject of vulnerability analysis
- Special requirements for self-test are addressed by an extended component FPT_TST.2
- Other cryptographic techniques are also covered by SFR or SAR like ADV_ARC.1, domain separation



Evaluation process

Scheme documents

- Technical guidance on cryptographic algorithms and protocols
- Guidance documents
 - Random number generators (AIS 20 / 31)
 - TR-03111 Elliptic Curve Cryptography
 - Guidance for Side Channel Analysis of Elliptic Curve Cryptography Implementation
 - Planned: Guidance for Side Channel Analysis of RSA Implementation
- BSI will issue technical evaluation guidance documentation for technical domains
 - Smartcard and similar devices
 - Cryptographic devices
 - Banking terminals



Evaluation process

Kickoff meeting for vulnerability analysis

- Goal of the meeting
 - Agreement about vulnerability analysis between evaluators and certifiers
 - Coordination between lab activities and support from BSI specialists
 - Cryptographic competence centre
 - Side-channel analysis, random number generator
- Content of the meeting
 - Checklist containing specific attacks
 - Evaluators explain how they will address these general attacks for the concrete TOE in their vulnerability analysis
 - Understanding of the TOE based on ADV (ARC, TDS)
 - Agreed plan for vulnerability analysis, may be extended as result of evaluation progress



Evaluation process

Experience of vulnerability analysis

- Lab experience
 - Most evaluation problems of cryptomodules are not of cryptanalytic nature (i.e. do not require mathematic-cryptographic analysis)
 - Specific cryptographic techniques require specialists like for security IC hardware, side-channel analysis or smartcard OS
 - Developers shall strictly follow cryptographic standards and guidance
- How do we deal with problems?
 - Vulnerability analysis might result in new cryptographic questions
 - Side-channel analysis (partially compromised key or parameters)
 - Implementation specific problems especially for protocols
 - Questions can be solved in cooperation with BSI if early enough identified
 - Unsolvable question might result in fail verdict



Certificates

How certificates cover cryptographic procedures

- The strength of cryptographic algorithms are not rated in the course of the evaluation process but the certification report states the suitability of the used cryptographic algorithms („crypto-disclaimer“)
- The certificates issued by the German Scheme may include cryptographic procedures
 - if the TOE uses endorsed procedures only
 - if TOE uses not endorsed procedures but this usage is agreed with CB e.g. CBC-MAC, Retail-MAC, 2KeyTDES, SHA-1



Certificates

How certificates cover cryptographic procedures

- The certificates may not make a statement concerning the strength of cryptographic algorithms
 - if the cryptographic algorithms are suitable for encryption / decryption
 - if ST claims high resistance (AVA_VAN.5) and the TOE uses cryptographic algorithm with strength less 80 security bits
 - if ST claims resistance against basic up to moderate resistance



Conclusions

- The German CC Scheme certifies cryptographic modules using endorsed cryptographic algorithms and protocols
- The German CC Scheme ensures the quality of the evaluation process of cryptographic modules by means of technical guidelines, evaluation guidelines, scheme documents and special oversight
- The German CC Scheme will develop further special methodology guidance documents for the technical domain Cryptographic Devices



Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Bernd Kowalski
Godesberger Allee 185 – 189
53133 Bonn

Tel: +49 (0)22899-9582-5700
Fax: +49 (0)22899-10-9582-5700

bernd.kowalski@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

