

PHILIPS

Leader in Smart Card Security

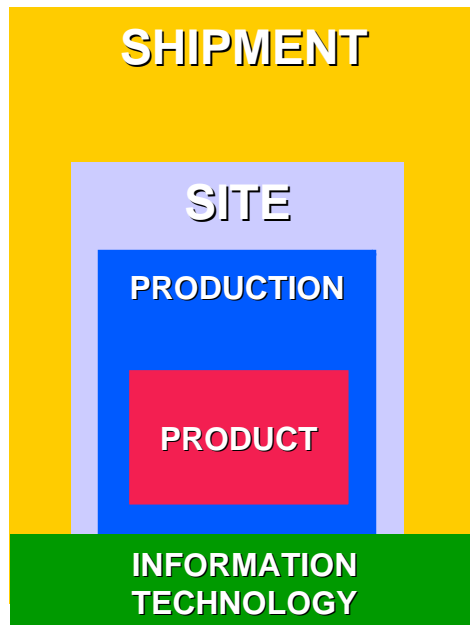
Track Record of Security Evaluations, Certifications and Approvals

Contactless & Embedded Security

PHILIPS Semiconductor - Business Line Identification

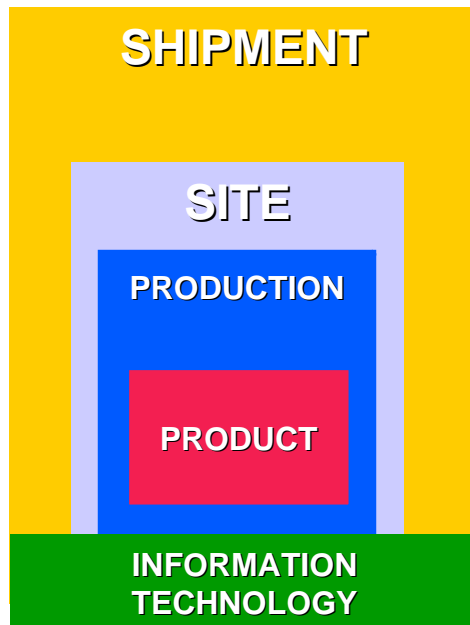
Rev. 1.4 February 2005 M.Ganzera

Security Assessment *General Approach*



- **Product**
to fulfill customer security requirements in the final application
- **Production Flow**
to prevent/detect loss or manipulation of products
- **Site Security**
to prevent unauthorized access to security data, products and facilities
- **Shipment**
to prevent/detect loss or manipulation of security products
- **Information Technology**
to prevent loss of confidentiality and integrity of security data

Security Assessment



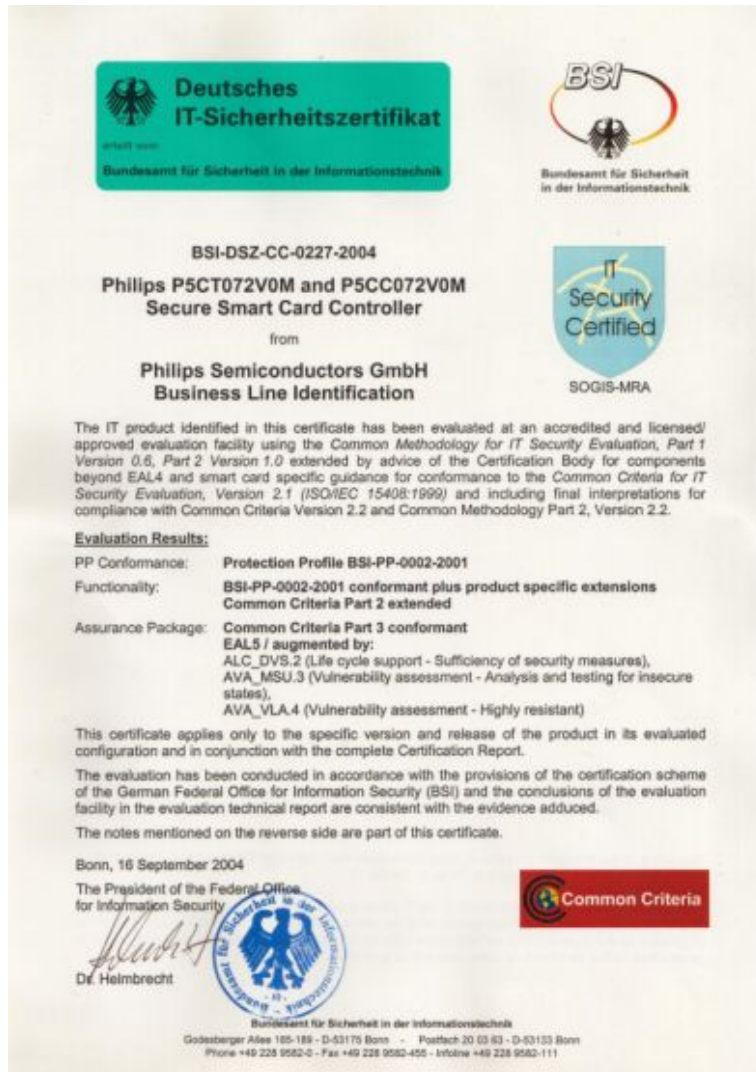
Product

to fulfill customer security requirements in the final application

- ❑ ***Intensive in house investigations***
 - as part of PHILIPS product release procedure

- ❑ ***Independent 3rd party evaluations***
 - well known and recognized labs
 - based on international standards
 - ❑ Common Criteria (EAL5+)
 - ❑ ITSEC
 - ❑ FIPS
 - based on market driven standards
 - ❑ e.g. VISA, MASTERCARD (CAST), JCB
 - ❑ ZKA
 - ❑ MULTOS

CC EAL5+ for SmartMX P5CT072



- Industries 1st CC EAL5+ certified Secure Triple Interface smart card controller
- Platform for several composite evaluations
- Based on smart card protection profile BSI-PP-0002-2001

Security Evaluation *Track Record*



*Certified Smart card controller hardware
based on Smartcard IC Platform Protection Profile (BSI-PP-0002-2001)*

PRODUCT	LEVEL	DATE	EVALUATOR / CERTIFICATION BODY	REMARKS
P8WE5032	EAL3	11/99	debis/BSI	
P8WE6017	EAL5+	07/01	debis/BSI	worlds 1 st smart card controller at EAL5+. Highest level ever reached. also used as basis for formal composite evaluation
P8WE6004	EAL5+	03/02	T-Systems/BSI	also used as basis for formal composite evaluation
P8WE5033	EAL5+	08/02	T-Systems/BSI	
P16WX064	EAL5+	06/03	T-Systems/BSI	worlds 1 st 16 bit smart card controller EAL5+ certified P16 Crypto Library 08/03
P5CT072	EAL5+	09/04	T-Systems/BSI	worlds 1 st Secure Triple Interface smart card controller EAL5+ certified
P5CC072	EAL5+	09/04	T-Systems/BSI	also used as basis for formal composite evaluation
P5CC009	EAL5+	09/04	T-Systems/BSI	also used as basis for formal composite evaluation
P5CC036	EAL5+	10/04	T-Systems/BSI	also used as basis for formal composite evaluation
P5CD036	EAL5+	02/05	T-Systems/BSI	particularly suitable for e-Passport application
P5CD072	EAL5+	02/05	T-Systems/BSI	particularly suitable for e-Passport application
P5CD009	EAL5+	02/05	T-Systems/BSI	

Michael Ganzera

Further information can be found at: <http://www.bsi.bund.de/zertifiz/zert/report.htm>

Security Evaluation *Track Record*

Term 'technology level' not longer used replaced by 'approved'

VISA approval *all smart card controller reached 'technology level 3'*

Product	Date
P8WE5032	1999
P8WE6017	Jan 2001
P8WE5033	Jun 2001
P8WE6008	Sep 2001
P8WE6004	Nov 2001
P8WE5017	May 2002
P8WE6032	Jul 2002
P8WE6018	Nov 2002

Product	Date
P8WE5009	Nov 2002
P8RF5016	Jan 2002
P8RF6005	2003
P8RF6010	2003
P8RF6016	2003
P5CT072	Jul 2004
P5CC036	Aug 2004
P5CC009	Aug 2004

Product	Date
P7CU145	Nov 2004
P7CC145	Nov 2004
P7SC145	Nov 2004
P7SC073	Nov 2004
P7CC073	Nov 2004
P5CD036	Mar 2005
P5CD072	Mar 2005

MASTERCARD CAST approval - *Compliance and security testing*

May 2003

Product	Reg. No.
P8WE6004	ICCN0021
P8WE6017	ICCN0022
P8WE5033	ICCN0020
P8WE5017	ICCN0020
P8WE5009	ICCN0020

May 2004

Product	Reg. No.
P5CT072V0	ICCN0032
P5CD072V0	ICCN0032
P5CC072V0	ICCN0032
P5CD036V0	ICCN0032
P5CC036V0	ICCN0032
P5CD009V0	ICCN0032
P5CC009V0	ICCN0032

August 2004

Product	Reg. No.
P5CC036V1	ICCN0033
P5CC018V1	ICCN0033
P5CC009V1	ICCN0033
P5SC036V1	ICCN0032
P5SC018V1	ICCN0033
P5SC009V1	ICCN0033
P5CC036V1	ICCN0033

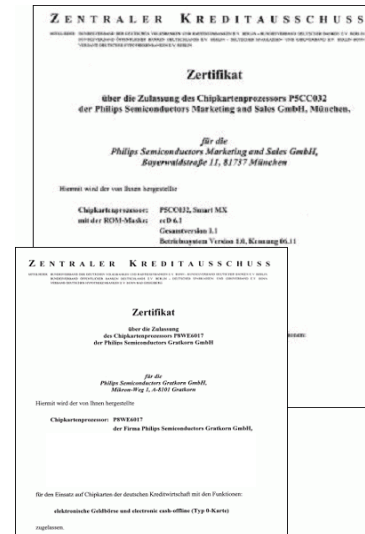
Security Evaluation *Track Record*

ZKA certificates

Product	Date
P8WE5032	1999
P8WE6017	2000
P8WE5033	2002
P5CC032	2003
P5CC036	2004

Composite Evaluations

Crypto Libraries	
SmartXA	SmartMX
On P16WX064 DES3, RSA, SHA-1 RNG (according AIS 31) delivered as Object code EAL5+ certified (8/2003) EAL5+ additional key generation features Q1/2005	DES3, RSA, DSA, SHA-1, ECC RNG (according AIS 31) delivered as Object code for different derivatives CC/EAL4+ Q3/2005



Security Evaluation *Track Record*

NIST FIPS 140-2

Security Requirements for Cryptographic Modules

NIST – National Institutes of Standards and Technology (US)

FIPS - Federal Information Processing Standard

Category of Standard: Computer Security Standard, Cryptography

Explanation:

This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The security requirements cover areas related to the secure design and implementation of a cryptographic module. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated Information (Canada).



PHILIPS hardware was the basis for several FIPS validations performed by our customers

Security Evaluation *Track Record*

FIPS 140-2 level 3 certified


ID-One Cosmo 72K RSA D

Based on SmartMX P5CT072
 native implementation of the latest
 Java Card™ (version 2.2)
 Open Platform (Version 2.1.1)

FIPS-approved algorithms:

- ❑ AES
- ❑ DES
- ❑ DES MAC
- ❑ Triple-DES Triple-DES MAC
- ❑ SHA-1
- ❑ RSA (up to 2048 bit)

FIPS 140-2 Validation Certificate



Certificate No. 449

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority, and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority, hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

ID-One Cosmo 72K RSA D by Oberthur Card Systems

in accordance with the Derived Test Requirements for FIPS 140-2, *Security Requirements for Cryptographic Modules*. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Designated Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

ID-One Cosmo 72K RSA D by Oberthur Card Systems
(Hardware Version: PIN: 77, Firmware Version: E300; Hardware)

and tested by the Cryptographic Module Testing accredited laboratory: **InfoCard Laboratories, Inc., NMLAP LAB CODE 100432-0, CRYPTIK Version 5.5**

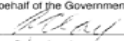
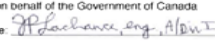
is as follows:

Cryptographic Module Specification:	Level 3	Cryptographic Module Ports and Interfaces:	Level 3
Roles, Services, and Authentication:	Level 3	Finite State Model:	Level 3
Physical Security (Single-Chip):	Level 3	Cryptographic Key Management:	Level 3
EMI/EMC:	Level 3	Self Tests:	Level 3
Design Assurance:	Level 3	Mitigation of Other Attacks:	Level 3
Operational Environment:	Level N/A	tested in the following configuration(s):	N/A

The following FIPS approved Cryptographic Algorithms are used: AES (Cert. #123); DES (Cert. #246); DES MAC (Cert. #246, vendor affirmed); Triple-DES (Cert. #232); Triple-DES MAC (Cert. #232, vendor affirmed); SHA-1 (Cert. #209); RSA (FIPS 186-2, PKCS#1, vendor affirmed)

The Cryptographic module also contains the following non-FIPS approved algorithms: N/A

Overall Level Achieved: 3

Signed on behalf of the Government of the United States	Signed on behalf of the Government of Canada
Signature: 	Signature: 
Dated: <u>8/2/04</u>	Dated: <u>23 July 2007</u>
Chief, Computer Security Division National Institute of Standards and Technology	Director, Information Protection Group The Communications Security Establishment

Michael Ganzera

PHILIPS

