BSI

Developer Site Certification

Trial-Use Results of the Site Certification Process

Thomas Borsch

Bundesamt für Sicherheit in der Informationstechnik /
Federal Office for Information Security

ICCC / September 2006

Agenda

- Benefit of Site Certification
- Information about the Trial Project
- Results from the SW Trial
- Results from the HW Trial
- Conclusions and the way ahead

Site Certification Benefits

- Avoid duplication of ALC related work between different evaluations
- Reduce Evaluation/Certification Costs
- Separate and maintain a Certificate for a Site from a TOE Certificate
- Re-use Site Certificates among different Evaluation Labs and national Certification Bodies

Trial Usage of the Process as part of the Lead Nation Project

- Documentation / Criteria Basis for the Trials:
  - Process Description Version 0.93 available since April 2006
  - AST Criteria for the evaluation of SSTs available since February 2006
- Presentation and discussion of the Process during CCMB and CCDB Meeting January and April 2006
- Start of the Hardware and Software Trials in May 2006

Participants and Scope of the Trial Use Phase

- Purpose of the Trials:
  - Definition of suitable Sites for a Site Certification
  - Development of Site Security Targets (SST)
  - Validation of the Site Certification Process and the SSTs during Audits
- The BSI was supported by the following parties:
  - SW Trials: IBM Corporation,
    atsec information security GmbH
  - HW Trials: Philips Semiconductors,
    T-Systems GEI GmbH

Definition of a „Site“

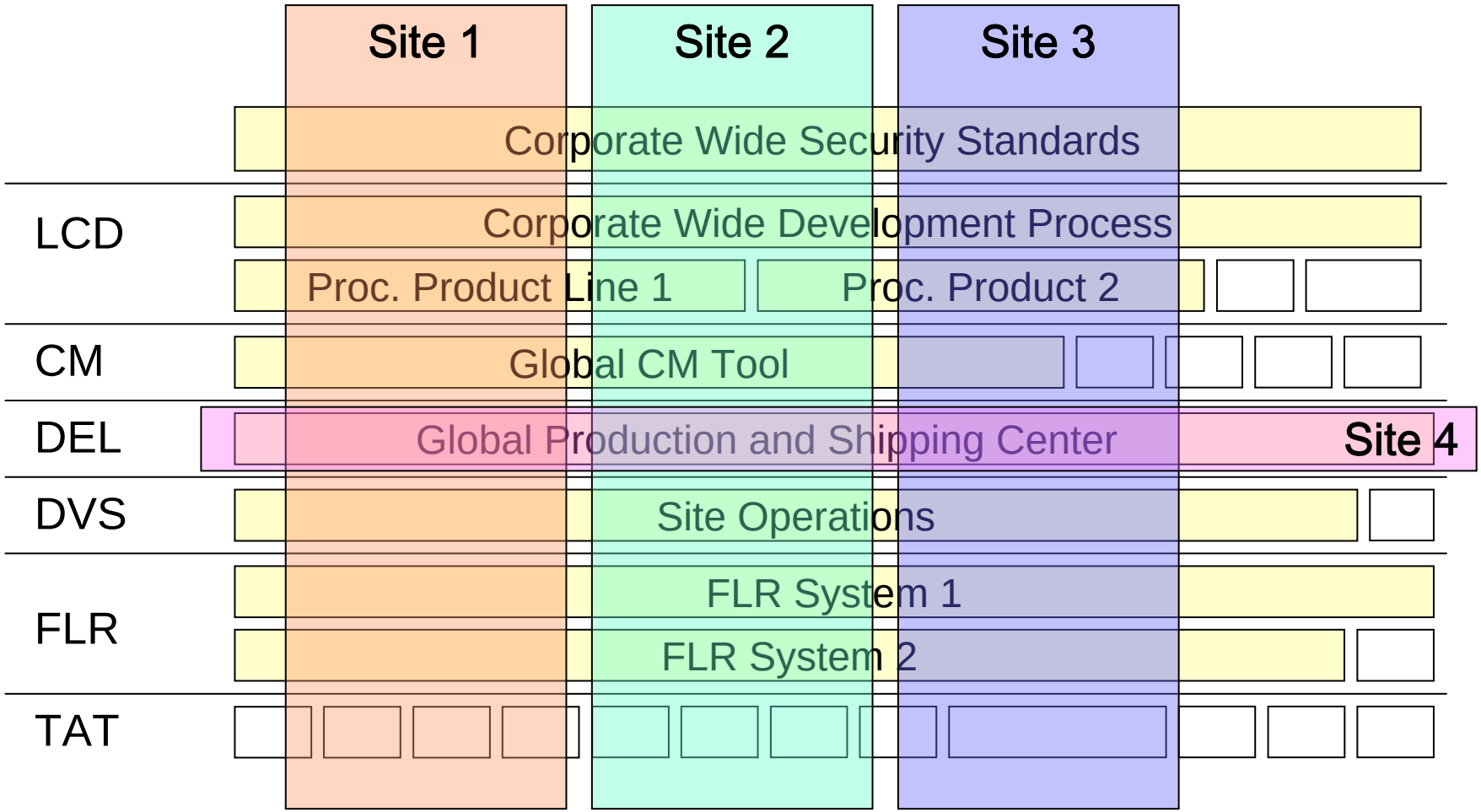
A developer can choose to divide his site into ”Subsites” also called ”Sites”.

- **A Site can be the whole site**
- **A Site may consist of one physical location, may span multiple physical locations, or a Site may be a part of a physical location**
- **A Site may consist of one organizational unit, may span multiple organizational units, or a Site may be a part of an organizational unit.**

SW-Trial
Site Scope

- Software Trial Candidate: IBM Corporation
- One physical location
- Two units at that location with the following life-cycle purpose:
  - Development, Testing and Maintenance of a TOE Subsystem
  - Shipping Division

SW-Trial
Overall Picture
Common Services



SW-Trial
Site Purpose - Details

- Development of Product Subsystem:
  - Software development of a Subsystem which is used as TOE part
  - Testing of the Subsystem
  - Maintenance of the Subsystem (Fixes/Patches)
- Product Shipping & Distribution:
  - Physical Media Production for various products
  - Download Center for various products

SW-Trial
Information about the SST

- SST defines
  - 7 Threats and 5 OSPs which result in 8 Objectives

    => Integrity, Confidentiality is of concern
- ALC Components claimed:
  - CMC.4, CMS.4, DEL.1, DVS.1, LCD.1

    => Site Certificate shall be usable for EAL4 evaluations
- SST has a total number of 31 pages

SST: Threats

Threats address the

- Physical and logical security
  - Access to restricted areas
  - Logical access to critical IT-Systems
  - Access to restricted information
- Development process
  - Modification of code, design, or guidance documents
  - Development mix-up through missing synchronisation
- Delivery
  - Manipulation of delivery items
  - Bypass of verification/review steps

SW-Trial
SST: OSPs and Objectives

- OSPs address
  - Company wide policies, standards and legal instructions
  - Proper Classification of code and documents
- Objectives are derived 1:1 from Threats and OSPs

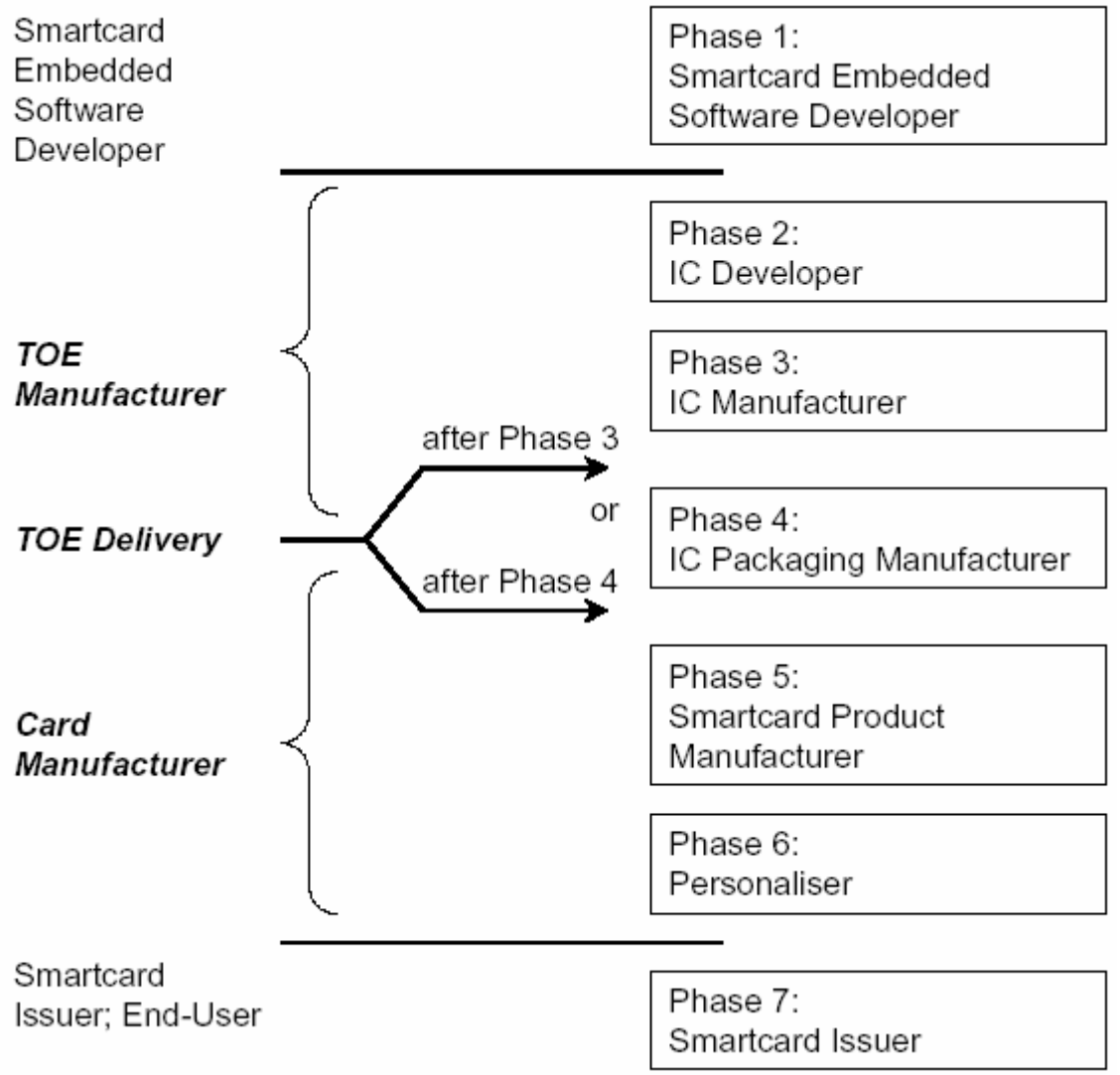
SW-Trial
SST: Security Assurance Requirements

- Site shall be used in Evaluations up to EAL4
- Mandatory Requirements claimed:
  - CMC.4: Production support, acceptance procedures and automation
  - CMS.4: Problem tracking CM coverage
  - DVS.1: Identification of security measures
- Optional Requirements claimed:
  - LCD.1: Developer defined life-cycle model
  - TAT.1: Well-defined development tools
  - DEL.1: Delivery procedures

HW-Trial
Site Scope

- Hardware Trial Candidate: Philips Semiconductors, Business Line Identification
- One physical location
- Two divisions at that location with the following life-cycle purpose:
  - Testing Centre for Smart Card Wafer
  - Shipping Division
- Production and shipment of multiple similar products
  (a lot of them under evaluation/certification at EAL4 or higher)

HW-Trial
Life-Cycle Phase covered



Test of Wafers

Wafer finishing

Shipping of Products

HW-Trial
Site Purpose - Details

- Wafer Testing:
  - Usage of test equipment to stimulate test program stored in each single dice
  - Configuration (pre-personalisation)
  - Guarantee of production authenticity
  - Marking (inking) of defect dices
  - Product finishing (back grinding, sawing), optional
- Product Shipping:
  - Protected storage of products
  - Shipment between wafer fab and/or module assembly and to customer

HW-Trial
Information about the SST

- SST defines
  - 6 Threats and 5 OSPs which result in 12 Objectives

    => Integrity, Confidentiality and Authenticity is of concern
- ALC Components claimed:
  - CMC.4, CMS.5, DEL.1, DVS.2, LCD.1, TAT.2

    => Site Certificate shall be usable for EAL5+ evaluations
- SST has a total number of 18 pages
  (without OBJ to SPD mapping)

HW-Trial
SST: Threats

Threats address the

- Integrity of
  - Test programs, Pre-personalisation Data, Packaging Material
- Confidentiality of
  - Wafers and Dices (good as well as defect/rejected), Authentication Data
- Authenticity of
  - Pre-Personalisation Data, Authentication Data

HW-Trial
SST: OSPs and Objectives

- OSPs address
  - Physical Site Security (Site Access and Monitoring)
  - Automatic Production Flow System
  - Secure Delivery Procedure
- Objectives are derived almost 1:1 from Threats and OSPs

HW-Trial
SST: Security Assurance Requirements

- Site shall be used in Evaluations up to EAL5
- Mandatory Requirements claimed:
  - CMC.4: Production support, acceptance procedures and automation
  - CMS.5: Development tools CM coverage
  - DVS.2: Sufficiency of security measures
- Optional Requirements claimed:
  - LCD.1: Developer defined life-cycle model
  - TAT.2: Compliance with implementation standards
  - DEL.1: Delivery procedures

Trial Usage Conclusions

- The Site Certification Process was easily applicable and worked well for both examples
- The Process is flexible enough to be applied to all kind of development environments
- Expected benefit in general is about 10% and is expected to be higher the more the site can be reused
- The challenge of Site Certification is the “Scoping” of the Sites to be certified
- Balance has to be found between providing information in the SST and just providing references

The way ahead

- Trial Evaluation Results will be used in CC2.3 Evaluations:
  - ALC Transition Guide will be used to provide a Mapping between CC3.1 ALC and CC2.3 ACM, ALC and ADO
  - Mapping will show equivalence between CC2.3 and CC3.1 to allow Re-Usage of Trial Results
- Several Developer would like to see Site Certification be integrated in the CC3.x as soon as possible

Contact Information

Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn

Thomas Borsch
Tel: +49 (0)1888-9582-5467
Fax: +49 (0)1888-10-9582-5467
thomas.borsch@bsi.bund.de