

Experiences gained from the first Site Certification Projects

Christian Krause (BSI)

Thomas Schröder (T-Systems)

Bundesamt für Sicherheit in der Informationstechnik

T-Systems GEI GmbH

10ICCC / 22 September 2009

Overview

- ❑ Status (relevant documents)
- ❑ Site Security Target (SST)
 - ❑ Content of the Site Security Target
 - ❑ Description of the target of evaluation
- ❑ Reuse of the site evaluation results
 - ❑ Information available to the evaluator of a product
 - ❑ Evaluation tasks of the product evaluator
 - ❑ Examples to support the understanding

- ❑ Certification
 - ❑ First Site Certification completed in the German Scheme
 - ❑ Assembly line for smartcard related products
 - ❑ integrated in an ongoing product evaluation
 - ❑ Second Site Certification is in process in the German Scheme

- ❑ Guidance available
 - ❑ Site Security Target Template provided by Eurosmart
 - ❑ Site Certification Guidance for developers and evaluators
 - ❑ AST and ALC Evaluator Report Templates

Content of the Site Security Target

- ❑ Site Security independent of a product considering the assets and the attack potential
- ❑ Configuration management based on process description and internal systems

Content of the Site Security Target

- ❑ The Site Summary Specification (AST_SSS) includes also a list of all evidence to meet the SARs
- ❑ Since the site owner does not want to publish this list of internal site documentation a SST-lite is provided instead of the SST

Content of the Site Security Target

- ❑ Proposal: The requirement *'The Site Summary Specification should identify all evidence that was needed for the site to meet all SARs'* should be removed in the Supporting Document Guidance for Site Certification
- ❑ The identification of all evidence is already required by ALC_CMS

Site Security Target evaluation

- ❑ The evaluation of the Site Security Target covers already quite a number of ALC requirements that are normally evaluated under the respective ALC evaluation report
 - ❑ List of all evidence
 - ❑ Other security aspects
- ❑ The process should be balanced to avoid double work

Site Security Target

Scope of the evaluation

- ❑ Based on the Supporting Document Guidance 'Site Certification' a SST must contain at least:
 - ❑ ALC_CMS.1
 - ❑ ALC_CMC.3
 - ❑ ALC_DVS.1
- ❑ Specific aspects are not relevant for all sites, e.g.
 - ❑ ALC_TAT if no security relevant tools are used
 - ❑ Hence the SST author may exclude ALC_TAT according to the Supporting Document Guidance

Site Security Target

Scope of the evaluation

- ❑ But to omit a ALC component may be risky:
 - ❑ It is only a statement of the site owner
 - ❑ Not verified and confirmed by an evaluator
 - ❑ This aspect has to be verified by the product evaluator and the evaluation could show that the site owner statement was wrong
 - ❑ The client of the site may want to see a statement in the certification report that all ALC aspects relevant for EALx have been successfully evaluated and hence the site supports product evaluations up to EALx

Site Security Target

Scope of the evaluation

- ❑ A better approach is:
 - ❑ Check, which ALC package is required for typical product evaluations of the client and include this ALC package in the SST
 - ❑ The selection of the ALC package is easy if specific Protection Profiles are relevant for the product category
 - ❑ The evaluator carries out the corresponding work units and decides whether these are applicable or not

Site Security Target

Scope of the evaluation

- ❑ The supporting document guidance for Site Certification does not require a guidance for the client of a site
 - ❑ The clients have to consider the assumptions in the SST, but they contain the necessary information only on a high level
- ❑ A guidance for the clients of a site could support the client with a more detailed description about the correct integration of the site
 - ❑ Discussion about a requirement for such a guidance is needed

Aspects covered by site evaluation

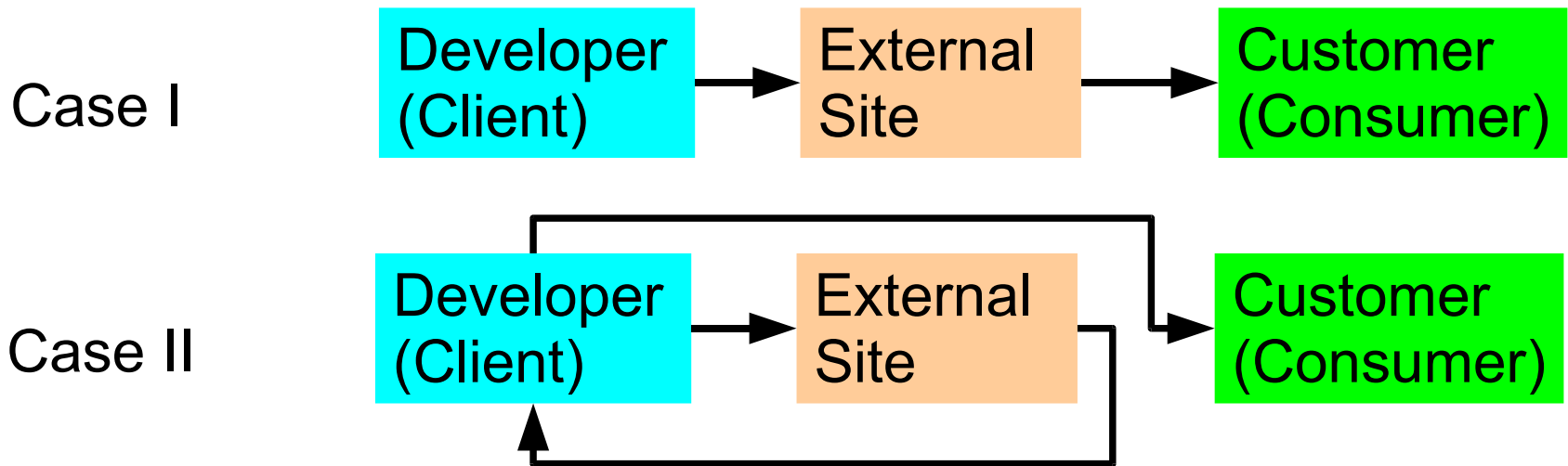
- ❑ Development Environment Security independent of the product
 - ❑ Physical security of the site
 - ❑ Logical security of the site
- ❑ Configuration management evaluated on a process level
 - ❑ Because a concrete TOE is missing it is evaluated whether
 - ❑ The CM system is applicable for the product type
 - ❑ Assets can be managed by the CM system
 - ❑ Change processes are defined
 - ❑ Customer separation is supported
- ❑ Scope of the configuration management is mainly a matter of the evaluation level

Information available to the product evaluator

- ❑ Site Security Target
- ❑ Certification Report
 - ❑ Assumptions including additional information if needed
 - ❑ Reference to Guidance if needed
 - ❑ Hints and stipulations if no separate Guidance is available
- ❑ Product specific information
 - ❑ Specifications and Plans needed at the external site for the production step



Scope of the re-use (ALC-DEL)



- Case I is evaluated including ALC-DEL.1
 - External site is responsible for the delivery to the customer
- Case II is evaluated using ALC-DVS.1 or ALC-DVS.2
 - Transport is considered as internal delivery

- ❑ CC Requirements:
 - ❑ ALC_TAT.x → ADV_IMP.1
 - ❑ Guidances for re-use classifies the work units as product type specific
- ❑ TAT includes all tools and techniques used to generate and produce the TOE
 - ❑ Tools for configuration and initialisation are not considered under ALC_TAT.x
- ❑ Evaluation tasks depend on:
 - ❑ Complexity of the tools
 - ❑ Availability of the development environment
 - ❑ Customisation of tools

Evaluation tasks of the product evaluator

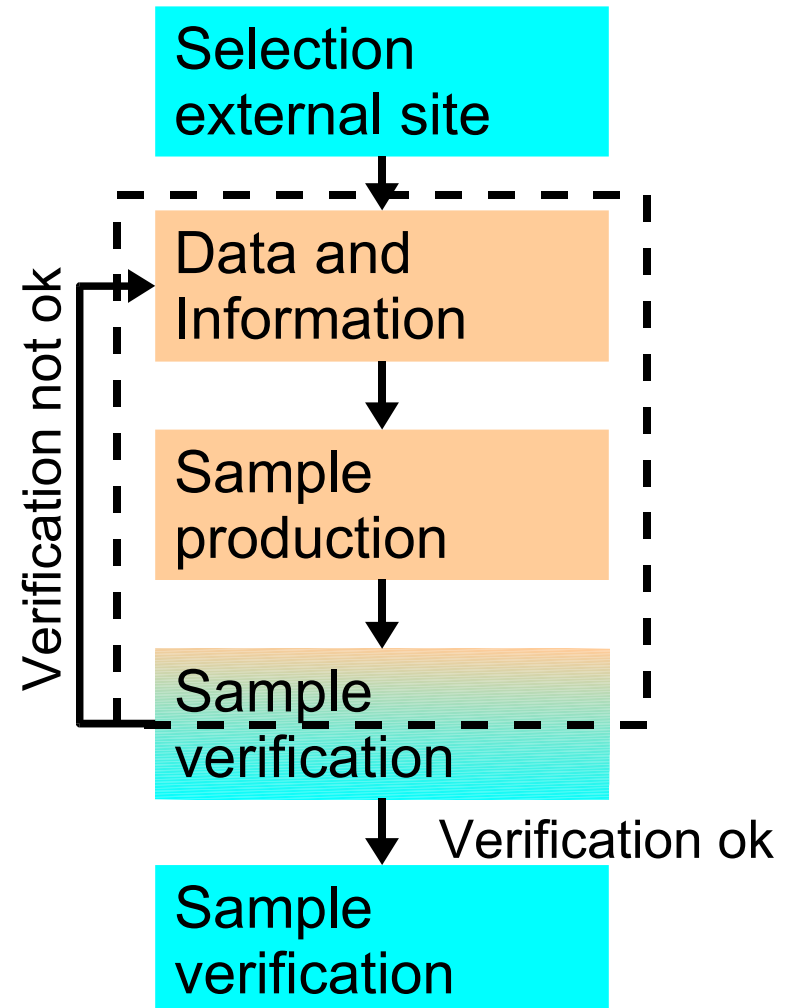
- ❑ Check of the Assets
 - ❑ Are the sensitive deliverables covered by the assets
- ❑ Assumptions (example)
 - ❑ Classification of the product
 - ❑ Product information needed by the external site
 - ❑ Guidance for testing
 - ❑ Test Specifications
 - ❑ Assembly plans
 - ❑ Constraints on the Transport

Evaluation tasks of the product evaluator

- ❑ Considered Threats
 - ❑ Compare Site Security Target and Security Target of the product
- ❑ Life Cycle is usually not complete within a Site Certification
 - ❑ Applicability of the product life cycle described
- ❑ Product specific evidence
 - ❑ Verification tests for configuration or initialisation steps

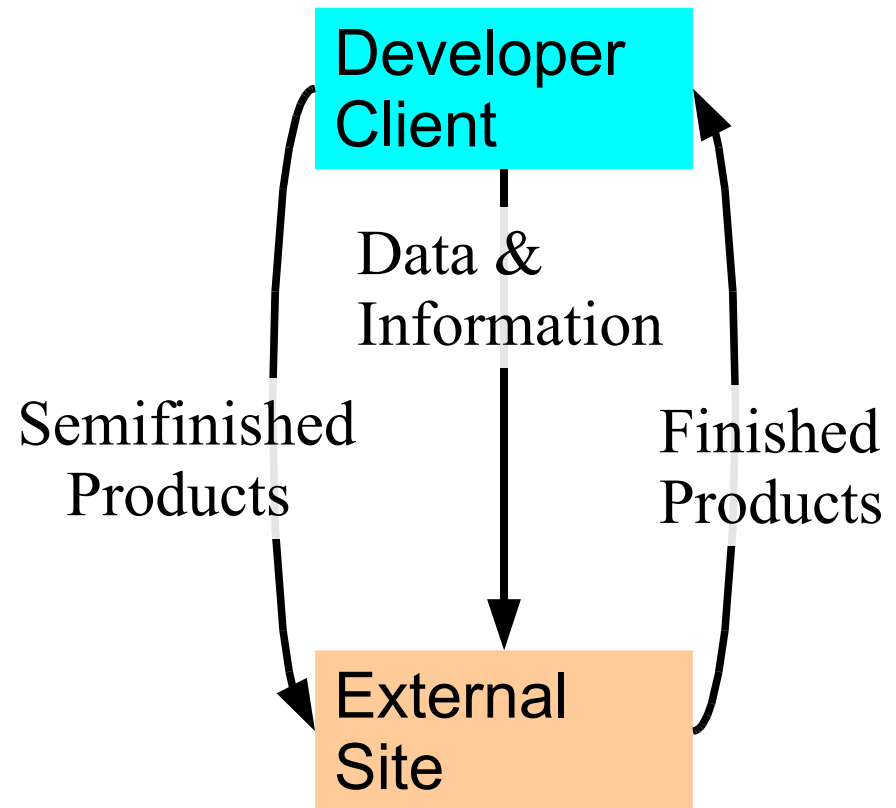
Example Testing Site (including configuration)

- ❑ Data delivered to the external site depend on the set-up
 - ❑ Interface description and test flow
 - ❑ Complete test program for a defined test environment
- ❑ Product specific verification during the product evaluation



Example Assembly Site (only mechanical process)

- ❑ Delivery of parameters and data for the production process
- ❑ No impact on the behaviour of the TOE
- ❑ Verification at the developer based on a go/no go test (reliability not relevant if no impact for the security of the product)



Example Mask Shop

- ❑ Sites that handle design data are of importance
- ❑ However the interfaces are mainly standardised
- ❑ Automated support is state of the art
- ❑ Different verification steps are implemented
- ❑ Challenges
 - ❑ Clients must agree on the same security policy
 - ❑ Comparable evaluation results based on agreed evaluation criteria support the acceptance and re-use
 - ❑ Working groups comprising European certification bodies, evaluation labs and manufacturers are working on this task

Limits of the Site Certification process

- ❑ Site Certification is suitable for sites
 - ❑ Performing standardised processes
 - ❑ Limited involvement in the development process
 - ❑ Mechanical production steps
 - ❑ Verification steps by the client possible
 - ❑ Clients do not require customisation
 - ❑ Product specific steps
 - ❑ Special Transfer requirements

Limits of the Site Certification process

- ❑ Protection Profiles can support the selection of the assurance requirements and the scope of the evaluation
- ❑ The evaluation results are limited to the scope defined in the Site Security Target
- ❑ Changes after the certification process
 - ❑ Maintenance
 - ❑ Re-Certification
- ❑ Validity of a Site Certificate: 2 years
 - ❑ Re-Certification

Summary

- ❑ The process for Site Certification is successfully applied in a first project
- ❑ Additional guidance for the site evaluation is available based on the first processes to support the application
- ❑ Changes of the SST content requirements have to be discussed
- ❑ Necessity for a guidance for the client depends on the task of the site and has to be discussed
- ❑ Specific aspects of the support for re-use may be missing
 - ❑ Guidance on re-use of evaluation results
 - ❑ European working group to standardise the site evaluation tasks in general

Contact

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Christian Krause
Godesberger Allee 185-189
53175 Bonn

Tel.: +49 22899 9582 5116
Fax: +49 22899 10 9582 5116

christian.krause@bsi.bund.de
www.bsi.bund.de

www.bsi-fuer-buerger.de

T-Systems GEI GmbH

Thomas Schröder
Rabinstrasse 8
53111 Bonn

Tel.: +49 228 9841518
thomas.schroeder@t-systems.com

