



Site Certification

another step
to improve the CC process
and to reduce costs

Hans-Gerd Albertsen, NXP Semiconductors Germany GmbH
Jürgen Noller, Infineon Technologies AG

9th ICCS, Sep 23-25, Jeju, Korea



Site Certification *Agenda*

- Motivation
- Overview Site Certification Process
- The real case: Passport Inlay Assembly
- What did we learn ?
- Outlook



Site Certification

Motivation

- Complex manufacturing structure in the Smart Security Industry
 - Security IC or OS & Application SW development
 - Different sites in different countries
 - Maskshops
 - More than one in different countries
 - Waferfabs
 - More than one in different countries
 - Testcenters
 - More than one in different countries
 - Assembly lines
 - Different packages (modules, inlays)
 - Personalisation
 - Different sites in different countries

An example

16 Sites
-3 Dev sites
-4 Maskshops
-2 Waferfabs
-2 Testcentres
-5 Assembly lines



Site Certification

Motivation

Status Quo

- All manufacturing sites are covered during standard product evaluations
- Under responsibility and cost of the developer of the product (TOE)
 - Special bi-lateral agreements may exist
- Frequency of Re-audit depending on customer evaluations
- Visibility on requirements and achievements at the different sites not obvious



Site Certification

Motivation

- Manufacturing Site
 - Visibility of requirements, process and results
 - Site Security Target, CC Process, Evaluator reports, Certification reports
 - (final) Product independent process
 - Under own control & responsibility
 - Reduced cost
 - Done once for all customers
 - To be repeated only every 2 years (just initial effort for 1st ST)
 - More customers
 - Manufacturing process can be easily offered to others
- ‘User’ of the manufacturing site
 - Use of certified sites speeds up certification process
 - No risk if site does not fulfill requirements (rework, further actions)
 - Reduced costs



Site Certification

Overview Site Certification Process

- **Involved Parties**
 - Site
 - Site and Process related documentation
 - Evaluator
 - Audit
 - Evaluation reports
 - Certification Body
 - Evaluation Report and ETR approval
 - Cite Certificate and Certification Report



Site Certification

Overview Site Certification Process

- Process (1)

- Site Security Target (SST)

new

- Describing Threats and Policies, derived Objectives and Assurance Requirements (SAR's)
- Of the site and the processes (services) to be certified
- Site Summary Specification

- Site Documentation

- Covering all ALC aspects
 - Physical and logical measures (ALC_DVS)
 - Process description
 - » Configuration Management (ALC_CMS, ALC_CMC)
 - » Quality & Project Management (ALC_LCD, _TAT, _FLR)



Site Certification

Overview Site Certification Process

- Process (2)
 - Evaluator
 - Performs SST evaluation, new
 - Evaluation of Site documentation, Evaluator reports (Class ALC)
 - Performing the Site Audit
 - Writing evaluation report (ALC) and ETR for the site new
 - Certification Body
 - Approval of ALC evaluation Report and ETR new
 - Issuing the Site Certificate & Certification Report



Site Certification

The real case

- Site Certification

Passport Inlay Manufacturer
HID Global
Erfurt, Germany

Add Inlay picture





Site Certification

Goal

- Performing Site Evaluation and Certification based on
 - CC Supporting Document 'Site Certification Version 1.0, Revision 1, October 2007 CCDB-2007-11-001, www.commoncriteriaport.org
- Derive a Site Security Template
 - Generic document and guidance document
 - Which should serve as basis for further SST's
 - For different sites and different processes
- Pave the way for further Site Certifications
 - Clarify and define which and how specific topics have to be covered in the SST
 - Clarify and define how specific work units have to be satisfied



Site Certification

Roles and responsibilities

- Bundesamt für Sicherheit in der Informationstechnik (BSI, Germany)
 - Certification Body of Germany
 - Author of the CC Supporting Document 'Site Certification Version 1.0, Revision 1, October 2007'
 - Certifier
 - Scheme details, interpretation, certification
 - Sponsor
- Infineon, NXP
 - Manufacturer of Security IC's
 - Using the ePassport Inlay manufacturing site HID Global (Product provider)
 - Support for the evaluation process
 - Goal is to integrate this process into our product evaluation





Site Certification

Roles and responsibilities

T Systems

- T-Systems GEI GmbH
 - Accredited lab at BSI
 - Consultancy
 - Security Target,
 - Evaluator
 - Document review (SST-, ALC evaluation)
 - Audit
 - ETR (Evaluation Technical Report)
 - Writing the Generic SST Template
 - Writing Evaluator Guidance for Site Certification



Site Certification

Roles and responsibilities



- HID Global Erfurt
 - ePassport Inlay manufacturing
 - Contract with evaluator
 - Providing documentation evidence
 - Audit
 - Providing required deliverables to Silicon Manufacturers
- Eurosmart
 - Observer
 - Members are interested in this approach
 - Want to follow
 - Sponsor
 - Security Target Template will be sponsored



Site Certification

Roles and responsibilities

Eurosmart

the Voice of the Smart Security Industry

- Eurosmart is an international non-profit association founded in 1995 and located in Brussels
- Eurosmart represents 24 companies of the Smart Security industry for multi-sectors applications and includes :
manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, application developers and issuers
- through its activities, the Product & System Security Working Group of EUROSMART actively supports the development of the Site Security Target template

In addition EUROSMART is the sponsor of the Site Security Target template development.



Site Certification – The real case

Milestones

- SST draft (generic) 14. July 2008
- SST draft (Erfurt specific) 27. July 2008
- Kick off Meeting at BSI 09. July 2008
- SST (final) 02.Aug. 2008
- Agenda Site Audit 08.Aug. 2008
- Checklist Site Audit -> BSI 08. Aug. 2008
- Single Evaluation Report AST (SST) 15.Aug. 2008
- Single Evaluation Reports ALC (draft) 15.Aug. 2008
- Site Audit Erfurt 26./27. Aug 2008
- Single Evaluation Reports ALC (final) 26. Sept. 2008
- Site Visit Report 03.Oct. 2008
- ETR 10. Oct. 2008
- Certificate 31. Oct. 2008
- SST Template, Evaluator Guidance 30. Nov. 2008



Site Certification – The real case *Observation*

- SST
 - Objectives – how detailed to publish them?
 - O.Security-Control:
Technical security measures like video control, motion sensors and similar kind of sensors are used to enforce access control
OK, as no technical details are published
 - Site Summary Specification:
The main entrance is equipped with sluice and badge with card reader and CCTV surveillance. The CCTV surveillance encloses several cameras and archive with a digital video recorder
Not for publication, as technical details are included
 - The solution may be a SST for the certification process and a SST-lite for publication
Differences:
The SST-lite does not include the section Site Summary Specification of the SST



Site Certification – The real case *Observation*

- **Delivery: ALC_DEL or ALC_DVS ?**
 - Depending on the overall manufacturing flow a site might do internal or external delivery
 - From CC perspective of the be certified product
 - From the Site perspective (and seen as the standalone process) it is always external delivery
 - Clarification in Site Certification Document or Site Certification Guidance might be the solution
- **Guidance for a Site ?**
 - Describes what a user/customer has to provide
 - e.g. classification of the product, testoptions



Site Certification – The real case *Observation*

- How to reflect AVA_VAN.5 ?
 - Currently covered under ALC_DVS.2
 - The security measures of the site are rated by the Evaluator and the Certification body
 - Only national standard, no international recognition yet
 - Definition of an international standard for security measures necessary for the AVA_VAN.x level
 - comparable to the JIL Application of Attack Potential to Smartcards
 - Benefit: international recognition possible
 - JIL Working Group working already working on this subject
 - Site Security Requirements paper in preparation

Problem !

Solution!



Site Certification – The real case

Actual status

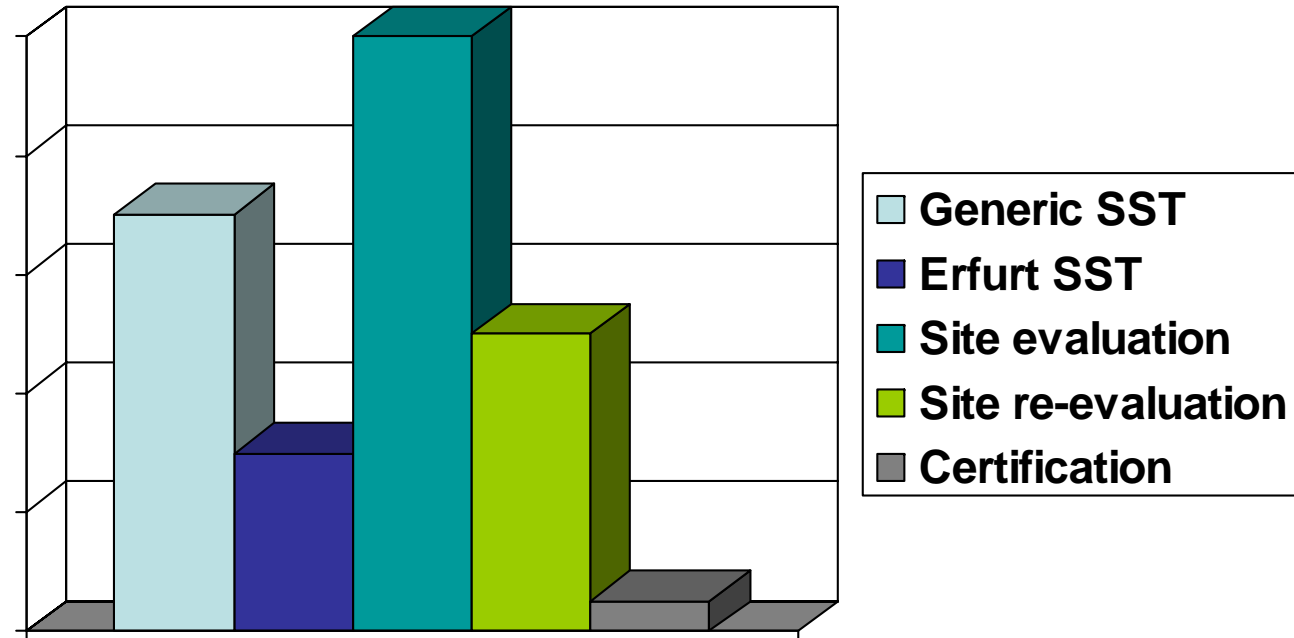
- Status July 24
 - All milestones on schedule
 - Some issues around SST and process identified and discussed
 - Objectives
 - ALC_DEL, ALC_DVS (external/internal delivery)
 - AVA_VAN.5
 - Guidance
 - This slide will be updated just before the conference



Site Certification – The real case

What did we learn ?

- Costs



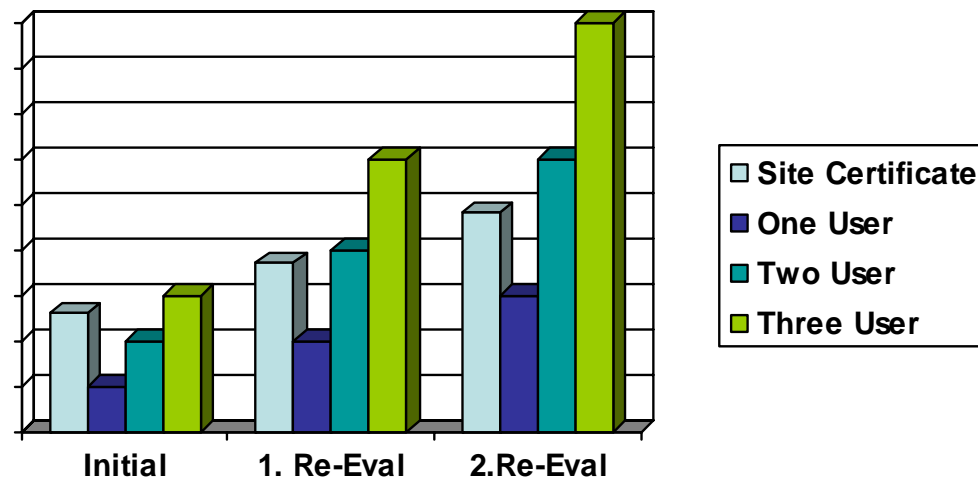


Site Certification – The real case

What did we learn ?

- costs for developing the Generic SST are not relevant for the owner and user of the site
- costs for the Erfurt SST and site evaluation arise only one time per site
- costs for re-evaluation and certification arise every two years per site

Cost site evaluation





Site Certification – The real case

What did we learn ?

Cost savings:

- saving of up to 50%
- by already three users and two re-evaluations

**Benefit by cost and audit time
if the site is used by
more then one customer**



Site Certification – The real case

What did we learn ?

- Targets reached ?
- Formal things (to be) clarified
 - E.g. Objectives, Delivery, Guidance, rating of Site Security Measures)
- Easy to use
 - SST template
 - Defined process with guidelines (for evaluators)
 - No problem with the process itself
- Cost reduction
 - On both sides
- Certificate issued and accepted by BSI
- Site Certificate as part of a product evaluation accepted by MRA members



Site Certification

Outlook

- Process accepted within the CCRA community
- Including the Site Certificate into a product certification process
- Site Certificate for
 - Maskshops, Assembly lines, Personalisation sites...
- Site Security
 - Standardized requirements for security measures
 - JIL Working Group activity (Paper: Site Visits)



Site Certification

Another step to improve the CC process and to reduce costs

Thank you for your attention

Questions ?