



# Site Certification

## Good News & Guidelines

V0.7, Aug 31, 2009

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

10th ICCG, Sep 22-24, Tromso, Norway





# Site Certification *Agenda*

- Site Certification Process - Overview
- Site Certification - 1st trial
- Guidelines and Templates
- Site Security Target Template
- What did we learn
- Next Steps



# Site Certification

## Motivation

- Complex manufacturing structure in the Smart Security Industry
  - Security IC or OS & Application SW development
  - Maskshops, Waferfabs and Testcenters
  - Assembly Lines, Personalization and D
- Status Quo in 2008
  - All manufacturing sites are covered during product evaluations under responsibility and developer of the product
  - Frequency of Re-audit depending on customer evaluations
- Our goal for the future
  - Visibility of requirements, process and results (site certificate)
  - Reduced cost and time for certification process
  - Reduced audit cost for the site

An example

16 Sites

3 Dev sites

4 Maskshops

2 Waferfabs

2 Testcenters

5 Assembly lines



# Site Certification

## *Overview Site Certification Process*

- **Involved Parties**
  - **Site**
    - Site and Process related documentation
    - Customer providing the TOE
  - **Evaluator**
    - Audit
    - Evaluation reports
  - **Certification Body**
    - Evaluation Report and ETR approval
    - Site 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
      - How SAR's are met

- 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, ALC\_TAT)



# Site Certification

## Overview Site Certification Process

- Process (2)

- Evaluator

- Performs SST evaluation,
    - Evaluation of Site documentation (Class ALC)
    - Performing the Site Audit
    - Writing Site Visit Report
    - Writing evaluation report (ALC) and ETR for the site

new

new

- Certification Body

- Accompanying the Site Audit
    - Approval of ALC evaluation Report and ETR
    - Issuing the Site Certificate & Certification Report

new



# Site Certification

*1st trial*

- Site Certification



Passport Inlay Manufacturer

HID Global

Erfurt, Germany





# Site Certification – 1st trial

## *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.commoncriteriaportal.org](http://www.commoncriteriaportal.org)
- Derive a ‘Site Security Target’ Template
  - Generic document incl. application notes
  - Which should serve as basis for further SST’s
  - For different sites and different processes
- Pave the way for further Site Certifications
  - Provide Guidance Documentation for developers & evaluators
  - Provide Templates for evaluators



# Site Certification – 1st trial

## *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 (for some templates & guidance documents)
- 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 – 1st trial

## *Roles and responsibilities*

- 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
    - Incl. application notes to support the writer of a specific SST
  - Writing Guidance & Templates for Site Certification
    - Templates for SST & ALC (Site) evaluation reports (SER's)
    - Guidance Document for Evaluators and Developers
    - Guidance for ETR writing
    - Sponsored by BSI

T Systems



# Site Certification – 1st trial

## *Roles and responsibilities*

- **HID Global Erfurt**
  - ePassport Inlay manufacturing
  - Contract with evaluator
  - Providing documentation evidence
  - Audit
  - Providing required deliverables to Silicon Manufacturers
    - To include Site Certificate into next level evaluation (SST (full), Certification Report, product (TOE))
- **Eurosmart**
  - Observer
    - Members are interested in this approach &
      - wanted to follow
  - Sponsor
    - of the Security Target Template





# Site Certification – 1st trial

## *Roles and responsibilities*

### Eurosmart

## *the Voice of the Smart Security Industry*

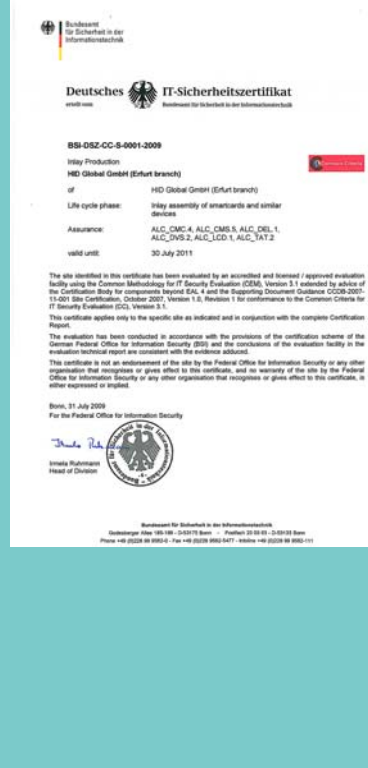
- Eurosmart is an international non-profit association founded in 1995 and located in Brussels
- Eurosmart represents 24 companies of the Smart Security industry for multi-sectors applications and includes :  
manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, 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 – 1st trial

## Milestones

- SST draft (Erfurt) Jun 2008
- Kick off Meeting at BSI Jul 2008
- Single Evaluation Reports ALC (draft) Sep 2008
- Several interim revisions Sep '08 – Feb '09
  - SST, ALC, SVR
- Site Audit Erfurt Sep 2008
- SST (final) Feb 2009
- Single Evaluation Report AST (SST) Feb 2009
- Site Visit Report Feb 2009
- Single Evaluation Reports ALC (final) Mar 2009
- ETR Mar 2009
- Certificate Jul 2009
- Templates, Guidance Doc's Mar 2009
  - Templates for SST (Mar '09) ; ASE & ALC Evaluator Doc's
  - Developer & Evaluator Guidance, ETR Guidance (Sep '09)





# Site Certification – 1st trial

## Costs

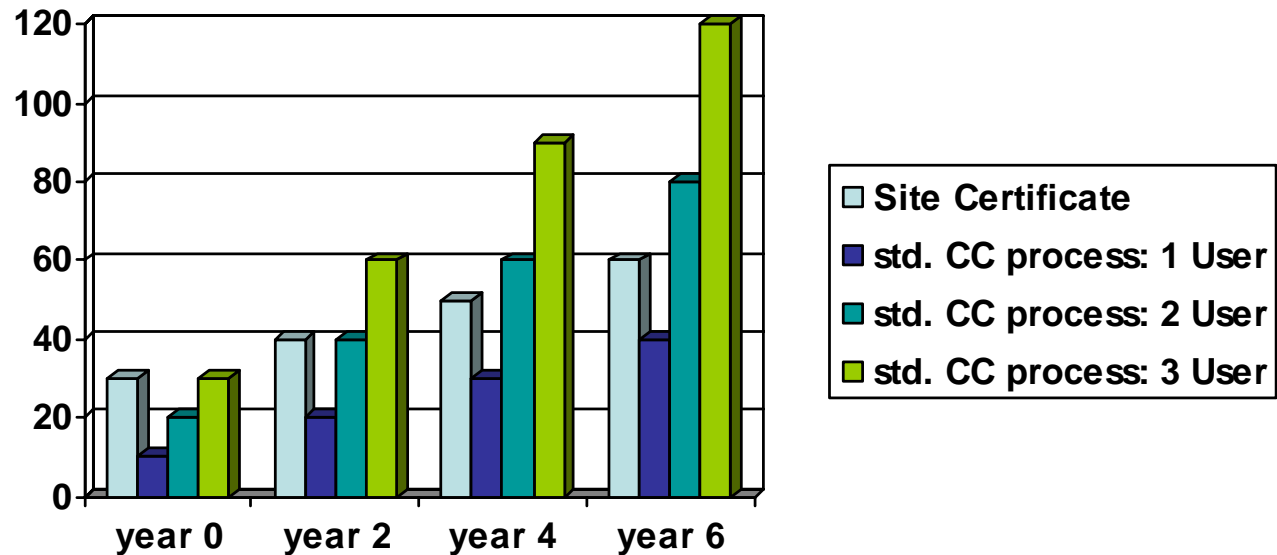
- New process with SST
  - Initial costs for the Site Certification
  - Costs for re-certification and site audit necessary every two years **per site only**
- Old process without SST
  - Initial costs for product certification at the site
  - Costs and time for re-audit necessary every two years for **each user (customer) of the site**
- Benefit for SST process
  - The initial costs for a Site Certification are higher than the initial costs for a product certification, **but**
  - Only one re-certification per site is necessary independently of the number of customers using the site



# Site Certification – 1st trial

## Costs

- Costs site evaluation
  - the initial costs for the SST process are about factor 2,5 higher than the costs for an initial CC audit process for a site
  - the costs for a re-audit of a site are the same as the costs for a re-audit of the SST





# Site Certification – 1st trial

## *Costs*

### Cost savings (example):

- saving of up to 40%
- 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

## *Guidelines & Templates*

- Site Certification Guidance for developers and evaluators
  - Supplement to Site Certification Process Document
  - Hints for developers for proper documentation preparation
  - Work units for evaluators (for aspects not covered in Site certification process manual)
  - How to deal with shortcomings (interpretation, corrections)
- ETR for Site Certification Guidance
  - Guideline for evaluators
  - Describes the content of an ETR for Site Certification
  - Document probably as extension/appendix to ETR like the AIS document of the BSI scheme

Sponsored  
by BSI

Sponsored  
by BSI



# Site Certification

## *Guidelines & Templates*

- **AST Evaluator Report Template**

Sponsored  
by BSI

- Simple link between information and work units
- Define structure and level of detail (of information)
- allow easy check and comparison by certification body
- No CEM replacement or addendum

- **ALC Evaluator Report Template**

Sponsored  
by BSI

- See above

Guidelines & Templates  
available on request

- **Site Security Target Template**

All written by  
T-Systems

- details are given in the next slides



# Site Certification

## *SST Template - content*

- Document Information
- SST Introduction
- Conformance Claim
- Security Problem Definition
  - Assets, Threats, Policies, Assumptions
- Objectives
  - What needs to be achieved
- Assurance Requirements
  - SAR's & refinements
- Site Summary Specification
  - Preconditions, services, rationale

For EAL4+  
easily adaptable  
to EAL5+  
(done for 1<sup>st</sup> run)

No SFR section



# Site Certification

## *SST Template – Security Problem Definition*

- **Assets**
  - Examples given for several sites/processes
    - S/W & IC dev, Maskshop, Test Center,
    - Assembly: wafer, diff packages (e.g modules), spec's, testdata
- **Threats**
  - Theft, manipulation, disclosure (of design data)
    - Incl. IT infrastructure
- **Policies**
  - Requirements derived from ALC assurance class
    - Controlled configuration (e.g. identification, acceptance)
    - Control of security measures (e.g. scrap, zero balancing)
- **Assumptions**
  - Guidance for clients
  - Deliverables needed at the Site
    - interface requirements (e.g. Spec, Identification, Delivery)



# Site Certification

## *SST Template – Security Objectives*

- Related to
  - Physical, IT & organizational security measures
  - Configuration Management & Delivery
- General description of implemented measures
- Examples
  - O.Physical-Access
    - Different levels of access control, organizational measures
  - O.Logical-Access
    - Network separation, firewalls, restricted access
  - O.Zero-Balance
    - The site ensures that all sensitive products (intended TOE of different clients) are separated and traced on a device basis. Automated control and/or two employees acknowledgement during hand over is applied for functional and defective devices. According to the agreed production flow the defect devices are either destroyed at the site or sent to the client or the consumer.
- Mapping Threats/Policies -> Objectives



# Site Certification

## SST Template - Security Objectives

- 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 is a SST for the certification process and a SST-lite for publication. Differences:  
***The SST-lite does not include the rationale section of the Site Summary Specification of the SST (Chapter 8.3)***



# Site Certification

## *SST Template – Assurance Requirements*

- SAR's (EAL4+)
  - ALC\_CMC.4, ALC\_CMS.4, ALC\_DEL.1, ALC\_DVS.2, ALC\_TAT.1 and ALC\_LCD.1
  - To be adapted for EAL5+
- Application Notes & refinements
  - ALC\_TAT.1
    - Site might offer services which need to be covered here
      - Configuration/personalization
    - Describe or argue why not applicable
  - ALC\_DEL vs. ALC\_DVS
    - Depending on the overall manufacturing flow a site might do internal or external delivery
      - From CC perspective of the to be certified product
      - Product view is the right one, therefore it depends on the production flow of the to be certified product
- Mapping Objectives -> SAR's



# Site Certification

## *SST Template - Assurance Requirement*

- 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 this subject
    - Site Security Requirements paper in preparation

Problem !

Solution!



# Site Certification

## *SST Template - Site Summary Specification*

- Preconditions
  - Requirements clients have to meet
  - Justification for assumptions
- Services provided by the site
- Rationale
  - How objectives have been met
    - Not in ST-Lite
  - Why Objectives are suitable to meet SAR's
- Documentation Mapping
  - Which documents relate to which SAR ?
    - Not in ST-Lite



# Site Certification

## *What did we learn ?*

- Site evaluation & certification can be done
- Formal things have been clarified
  - e.g. Objectives, Delivery, Assumptions/Guidance, provided services shall be product independent (ALC\_TAT)
  - 1st trial took long - quite a few clarifications necessary
- Easy to use
  - SST template with application notes for ST writers
  - Defined process with guidelines & templates
    - for developers & evaluators
  - No problem with the process itself
- Cost reduction - on both sides
- Certificate issued by BSI not covered by CCRA
- Site Certificate as part of a product evaluation accepted by CCRA members



# Site Certification

## *Next steps*

- Process accepted within the CCRA community
- Including the Site Certificate into a product certification process
- Site Certificate needed for
  - Maskshops, Assembly lines, Personalization sites, Testcenter, Wafer Fab, ...
- Site Certificate in progress for
  - Module assembly site of NEDCARD
  - Inlay assembly site of SMARTRAC
- Site Security definition
  - Standardized requirements for security measures
  - JIL Working Group activity (Paper: Site Visits)





# Site Certification

## Site Certification

### Good News & Guidelines

**Thank you for your attention**

**Questions ?**

