Site Certification Process

(Status Quo)

Frank Sonnenberg

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

7th ICCC / 2006-09-19

Presentation Content

- **Description of the Site Certification Process**
  Frank Sonnenberg
  BSI, Germany

- **Detailled Information on**
  „How to write a Site Security Target“
  Gerald Krummeck
  atsec information security GmbH, Germany

- **First Trial-Use-Results of the Site Certification Process**
  Thomas Borsch
  BSI, Germany

Background

Certification of a development site

would be a significant benefit for developers who develop multiple products

at one or more sites,

particularly under the same procedures

Motivation

- Increasing demand for development site certificates coming from different developers
- Reduce time and money for evaluations which will be performed within a short time frame under the same product development conditions
- Extention of the CC to ISMS aspects which become more and more important
- Improvement of the acceptance and opening of new markets for the Common Criteria

Further („Side-“) Aspects

There is an obvious imbalance of the criteria between the security provided by the TOE and the Development Environment of the TOE.

The Site Certification Process could achieve a harmonized application of the ALC-Requirements.

Two possible Strategies

1. Re-Use of ALC material

In order to re-use already certified CM system related aspects references to previous TOE evaluation(s) will be made .

2. Developer Site Certification

A separate CC certificate will be issued to confirm that a specific development environment fulfils the CC requirements regarding the related ALC class.
This can be seen independently from a TOE evaluation.
Special ISMS definitions may be taken into account.

Reusability-Problems

- Disadvantages occur when an expensive Site Visit has to be reperformed in the case of Minor Changes of the Development Site
- How to handle Reusability if the Developer changes the Evaluation Lab or the Certification Body
- How can ALC be classified into reusable and not reusable parts and how can the reusable parts be claimed in an evaluation?

Further Development of the Reusability Approach

We have added flexibility and efficiency by:

- Noting that ALC is independent to other CC-Aspects
- Splitting the evaluation between them

The same goes for complex evaluations where:

- parts of the “Site” may be relatively independent

Splitting the site may therefore also help

Main Advantages of Site Certification

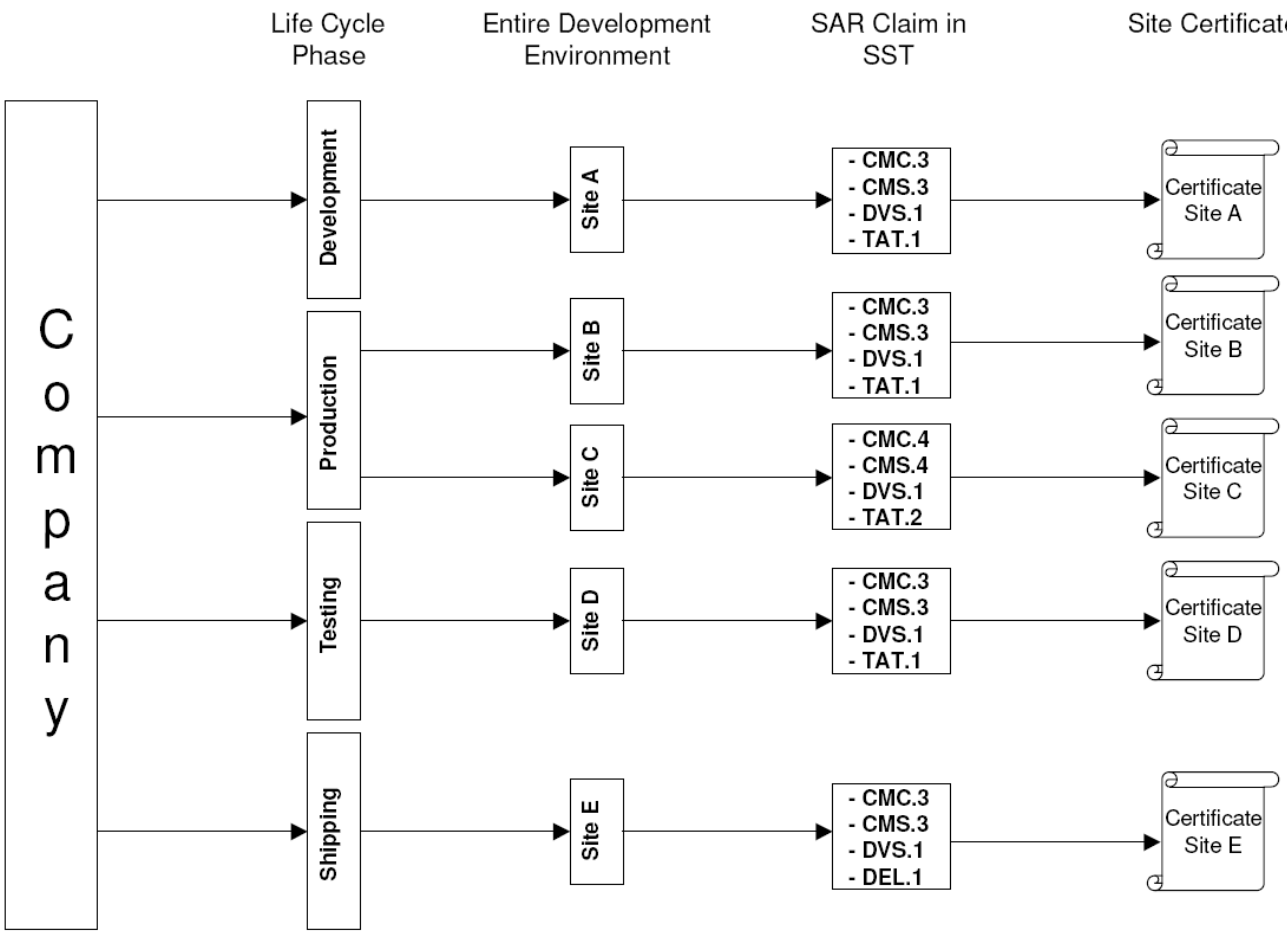
- Site Certificate can be completely separated from the TOE certificate.
- It provides an easy entry into the CC market for a developer. First get a site certificate, then a TOE certificate.
  A ”certificate to hang on the wall” could be a marketing advantage.
- An organization can obtain and maintain its own certificate and provide this to any developer who wants it.

Definition of a „Site“

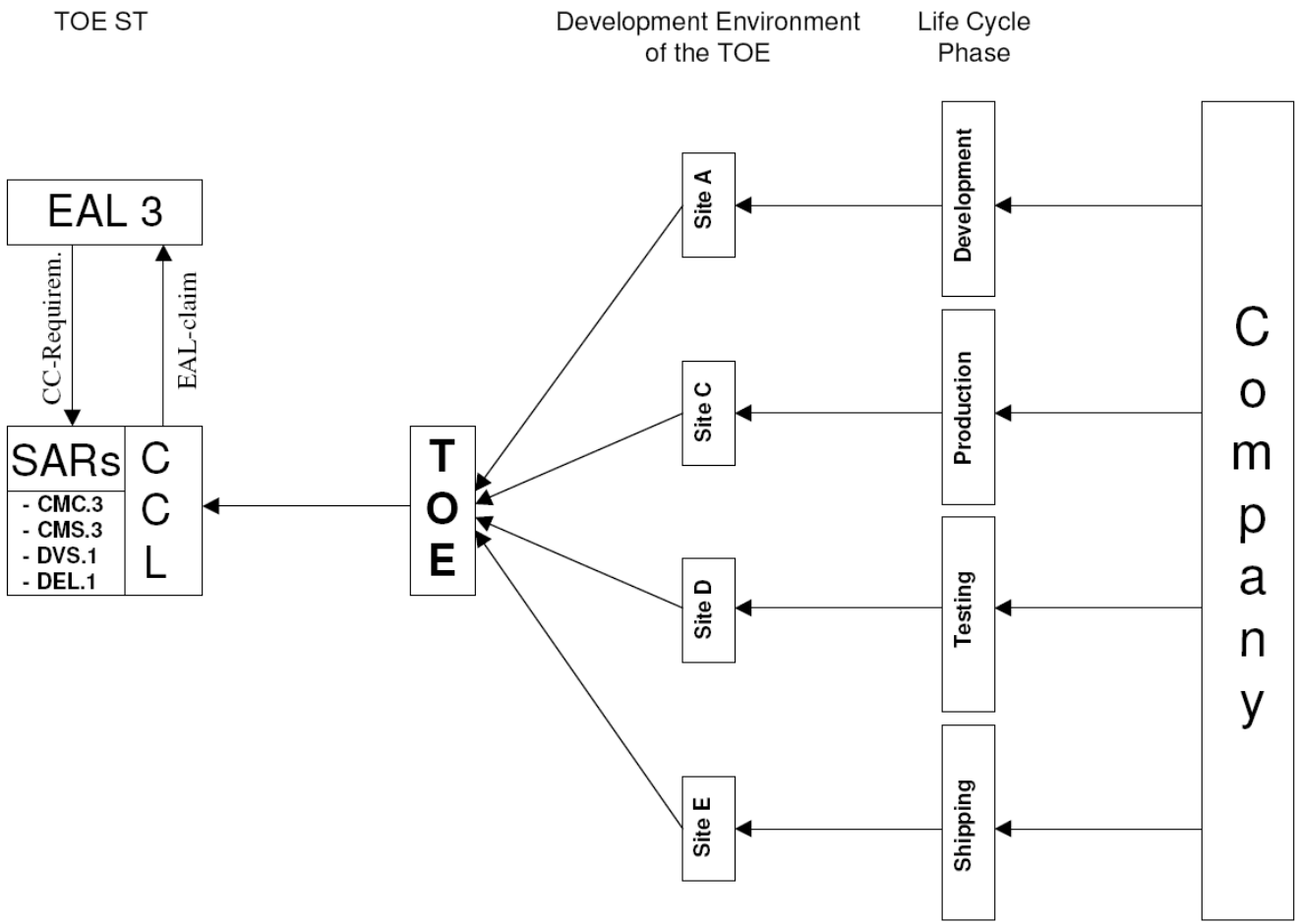
A developer can choose to divide his site into ”Subsites” also called ”Sites”.

- **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.**

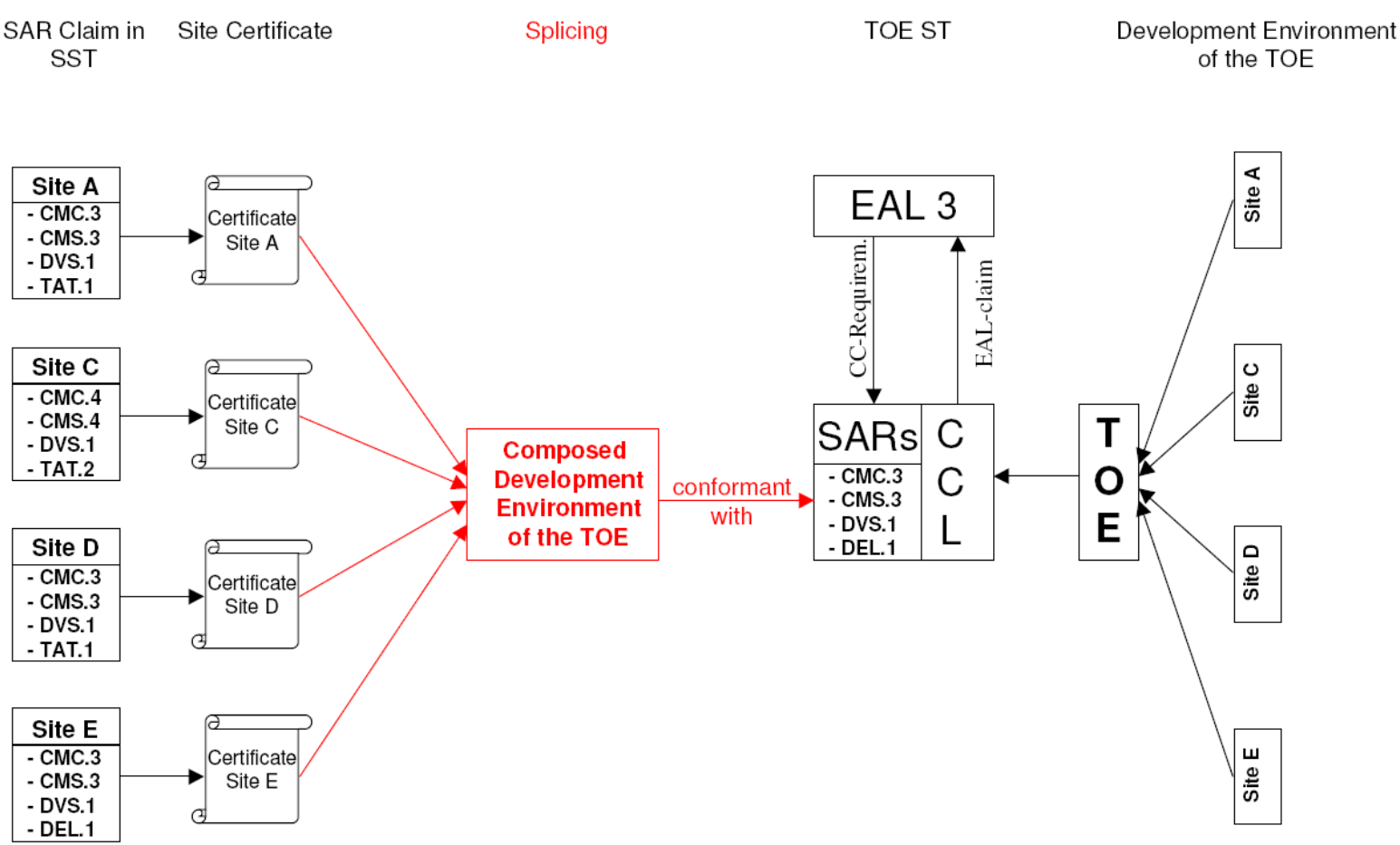
Definition of the Site Scope



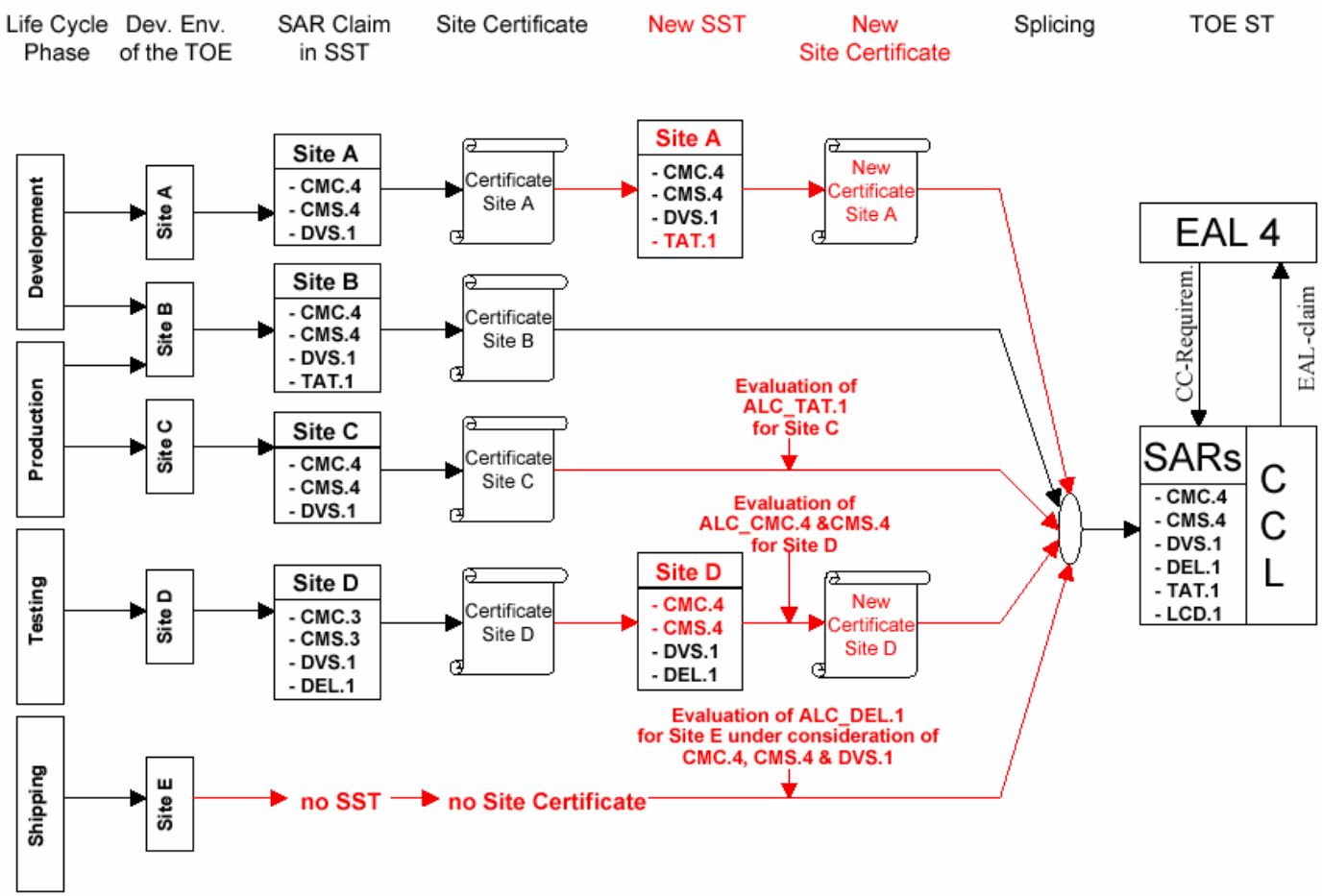
TOE ALC-Evaluation Base



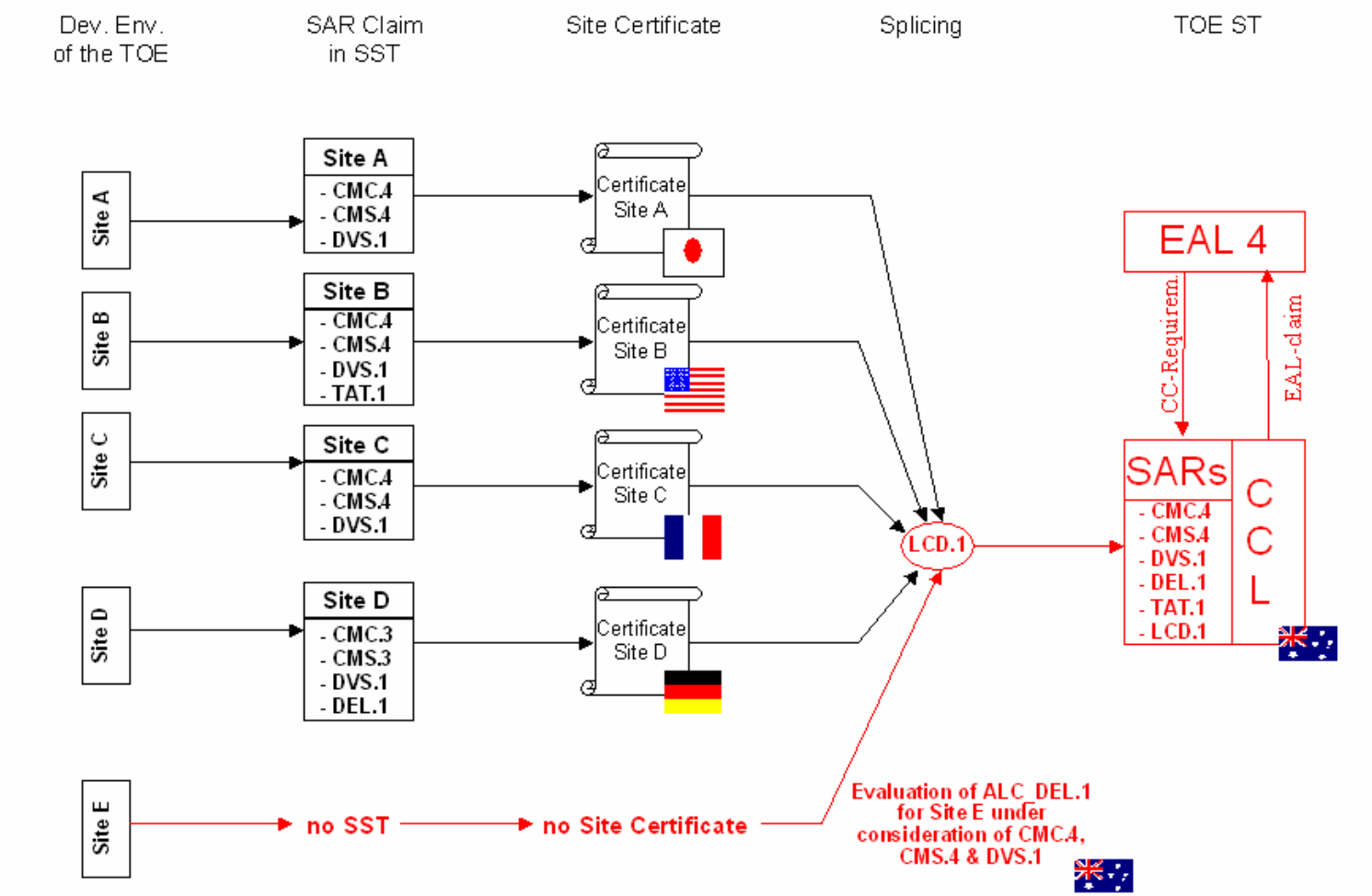
Splicing


SAR Claim in SST
Site Certificate
Splicing
TOE ST
Development Environment of the TOE
Site A
- CMC.3
- CMS.3
- DVS.1
- TAT.1
Site C
- CMC.4
- CMS.4
- DVS.1
- TAT.2
Site D
- CMC.3
- CMS.3
- DVS.1
- TAT.1
Site E
- CMC.3
- CMS.3
- DVS.1
- DEL.1
Certificate Site A
Certificate Site C
Certificate Site D
Certificate Site E
Composed Development Environment of the TOE
conformant with
EAL 3
CC-Requirem.
EAL-claim
SARs
- CMC.3
- CMS.3
- DVS.1
- DEL.1
CCL
TOE
Site A
Site C
Site D
Site E

Integration of non-certified parts



Site Certification throughout Schemes



Minimum & Optional SARs

Minimum SARs:

- CMC.3 (or hierarchically higher)
- CMS.3 (or hierarchically higher)
- DVS.1 (or hierarchically higher)

Optional SARs:

- DEL.1
- TAT.1 (or hierarchically higher)
- LCD.1 (or hierarchically higher)
- FLR.1 (or hierarchically higher)

Content of Site Security Targets

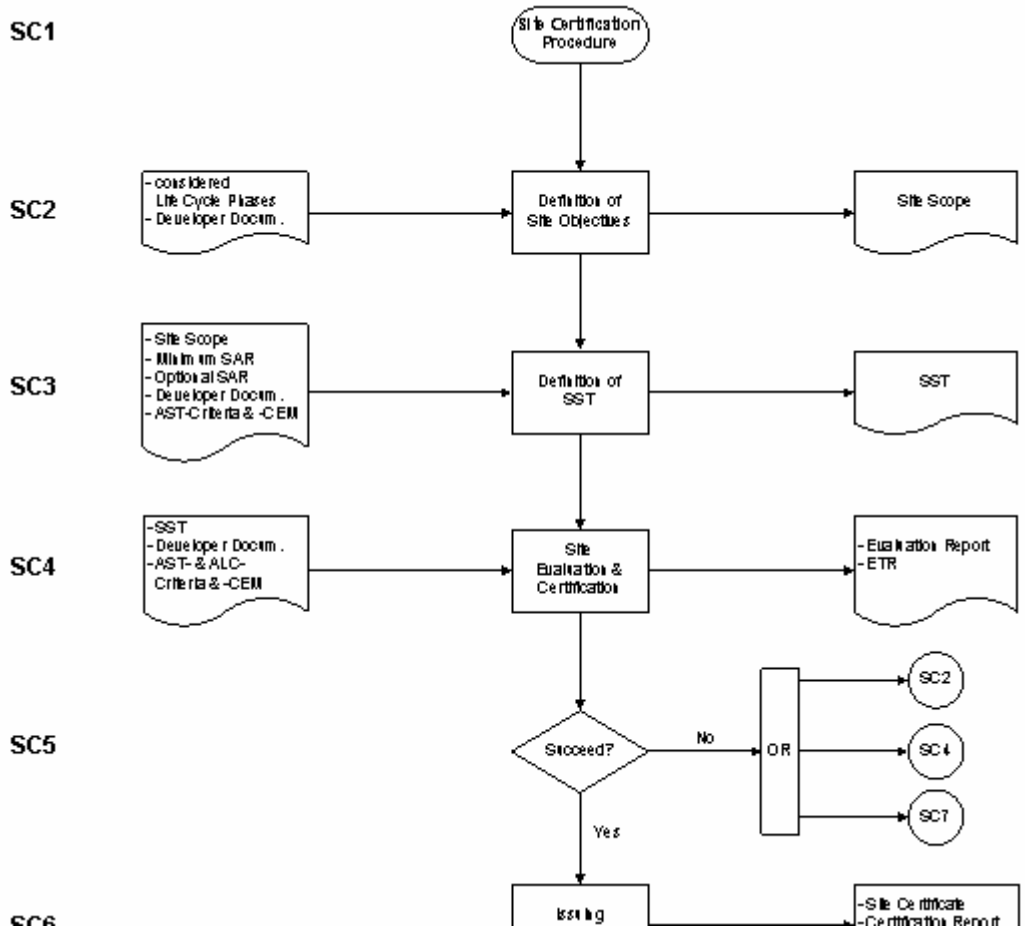
- SST-Introduction
- Conformance Claim
- Security Problem Definition
- Security Objectives for the Development Environment
- Extended Components Definition
- Security Requirements
- Site Summary Specification

Application Notes
for Site Certification

- No changes of the general content of the criteria and/or the methodology of the Common Criteria needed.

- Only adaptations or specific explanations are needed by including Site Certification related Application Notes which give instructions how to use (interpret) certain CC-Requirements (C-Element).

Well Defined Process Struture



Questions to be solved

- How to handle changes of sites which occur all the time?
  That means, do we need specific Maintenance Procedures for Development Sites?
- Is it necessary to add Site Certification to the CCRA?

Summary

- The ALC-Reusability-Approach can only be seen as a first step in saving Evaluation Efforts
- Reusability does only have a limited Applicability since several Technical Problems remain
- Site Certification can solve all these Technical Problems and will save an considerable amount of Evaluation Efforts
- There is an actual need and a new market for the CC to issue Site Certificates

Current Feedback

- Positive Feedback and Acceptance from different Communities/Schemes/Industry
- They would like to see Site Certification as part of the Common Criteria
- Several Developers volunteered for the Trials

Contact Information

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

Dr. Frank Sonnenberg
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)1888-9582-5470
Fax: +49 (0)1888-10-9582-5470

frank.sonnenberg@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de