Jose Emilio Rico
Epoche & Espri
tech@epoche.es

EPOCHE & ESPRI

Single Site Security Target

How to

Agenda

- Site certification
- Current methodology and well known SARs' (ALC) issues in CC.
- The manufacturing model
- The Site Certification process
- Single SST template
- Conclusions

Site Certification

EPOCHE & ESPRI

- Purpose
  - Reusability of results, leads to a significant reduction of time and money efforts.
  - Marketing ➔ Developer image
  - A manufacturing process certification
  - From EAL3
- CC & CEM do not help too much in some aspects of ALC.

Let´s have a look ……..

Current methodology

EPOCHE & ESPRI

- CC part 3 & CEM
- Site Certification Supporting Document
- JIL Minimum DVS requirements for high assurance

Well known SARs' (ALC) issues in CC.

When analyzing the ALC role in CC we found:

- The broken link between SPD & SARs
  - Mapping TOE security capabilities to properties of the security architecture (ADV_ARC).
  - Mapping desirable security properties of the development process and sites to assurance life cycle capabilities (ALC).
  - Mapping AVA_VAN attack potential methodology to security in the development environment.

Well known SARs' (ALC) issues in CC.

EPOCHE & ESPRI

When analyzing the ALC role in CC we found:

- Vague information and references to the development process characteristics in the ST.

ALC_DVS.1.1C, work unit ALC_DVS.1-1

The evaluator determines what is necessary by first referring to the ST for any information that may assist in the determination of necessary protection.

If no explicit information is available from the ST the evaluator will need to make a determination of the necessary measures.

ALC_DEL.1.1C work unit ALC_DEL.1-1

The evaluator shall examine the delivery documentation to determine that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

Interpretation of the term "necessary to maintain security" will need to consider among others:

- **The security objectives provided by the ST**. The emphasis in the delivery documentation is likely to be on measures related to integrity, as integrity of the TOE is always important. However, confidentiality and availability of the delivery will be of concern in the delivery of some TOEs; procedures relating to these aspects of the secure delivery should also be discussed in the procedures.

Well known SARs' (ALC) issues in CC.

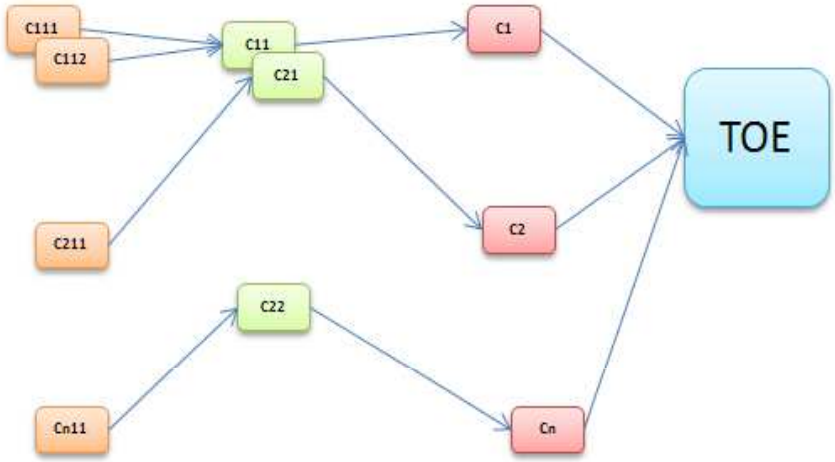
When analyzing the ALC role in CC we found:

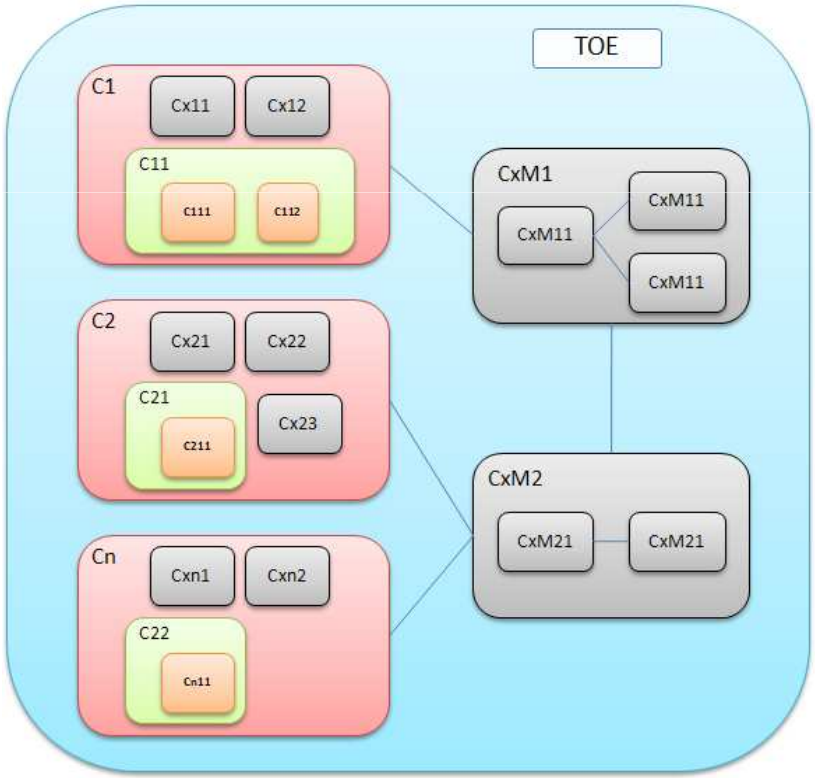
- Minimum requirements for the development sites

[ALC_DVS.1-1]

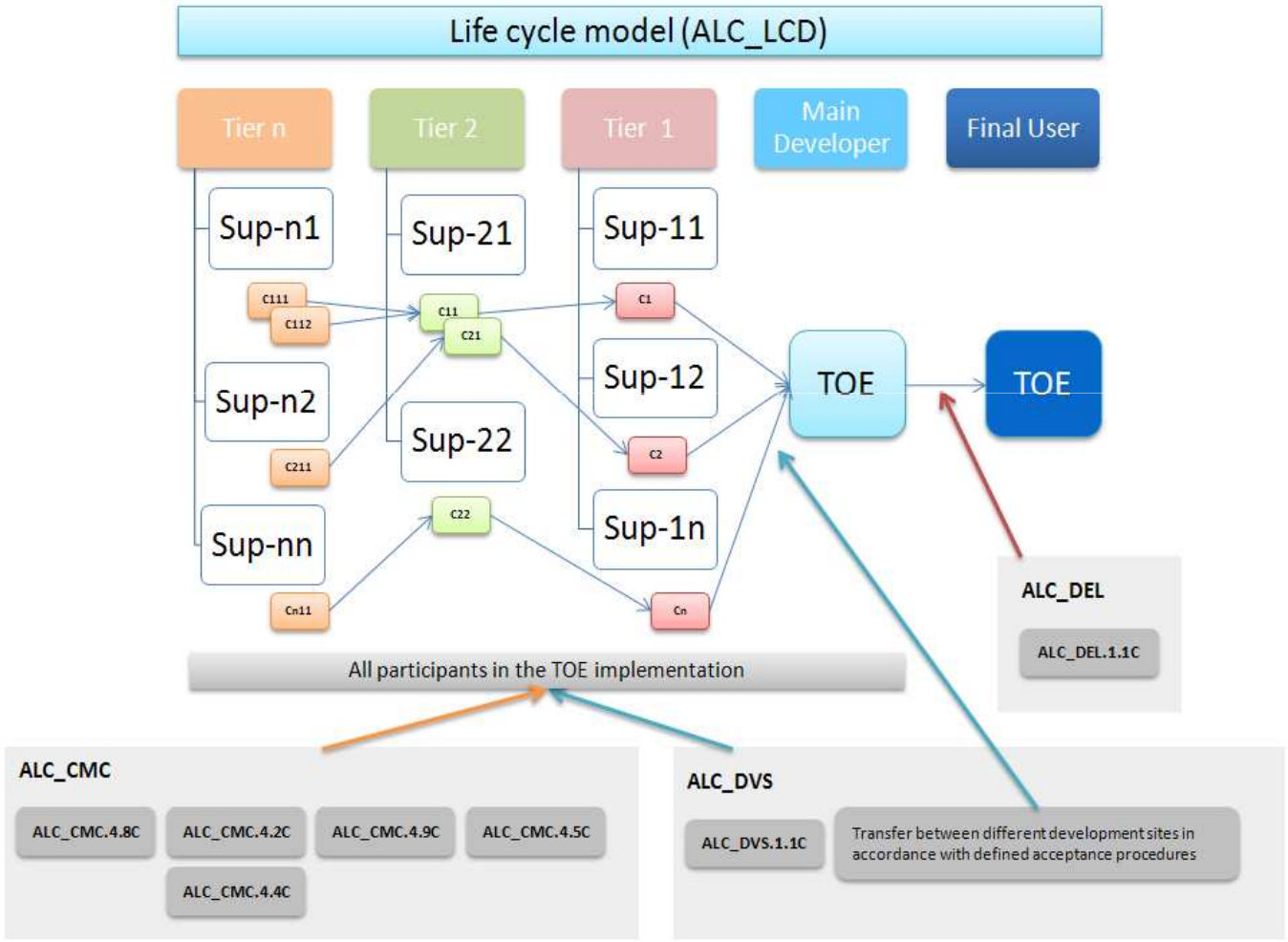
The evaluator determines what is necessary by first referring to the ST for any information that may assist in the determination of necessary protection. ***If no explicit information is available from the ST the evaluator will need to make a determination of the necessary measures.***

The manufacturing model





The manufacturing model



Site Certification process

EPOCHE & ESPRI

- Site evaluation

  AST: SST evaluation → ALC evaluation → ETR

- How to reuse ALC in a later TOE evaluation
  - The TOE-ST defines the scope of the development environment by claiming the ALC requirements.
  - No changes have been made in the certified development environment.
  - The site certificate fulfill all ALC related SARs of the TOE-ST → no additional evaluation efforts are necessary in the TOE evaluation concerning ALC.

Single SST template

EPOCHE & ESPRI

- Site Security target content.
  1. Introduction
  2. Conformance Claim
  3. Security Problem Definition
  4. Security Objectives for the development environment
  5. Extended Components Definition
  6. Security Requirements
  7. Site Summary Specification

Single SST template

EPOCHE & ESPRI

- Common issues in a single SST:
  - Security problem based in Risk analysis
  - Security objectives for the Site
  - ALC SARs: ALC_CMS.1, ALC_CMC.3, ALC_DVS.1
- Distinctive issues:
  - Implementation of the selected SARs

Single SST template

EPOCHE & ESPRI

- Security problem based in Risk analysis: Assets

Id	Asset	Asset value
A.TOE	The products that will be evaluated.	Confidentiality Integrity
A.PROT	Products prototypes or parts of the TOEs before packaging and shipping.	Confidentiality Integrity
A.INFO	All the documentation and information of the products (specifications, designs, guidance, test data, source code, HW drawings) or information related to the processes in whatever format.	Confidentiality Integrity
A.EQUI	Equipment used in the development	Integrity
A.INFOSEC	All the documentation or information regarding the systems and security mechanisms configuration (machines and perimeter protection devices configuration, cryptographic keys, passwords, etc.).	Confidentiality Integrity
A.DEVSEC	Protection devices or mechanisms.	Integrity Availability

Single SST template

EPOCHE & ESPRI

- Security problem based in Risk analysis: Agents
  - Insider with rights
  - Insider without any rights
  - Outsider with rights
  - Outsider without any rights

Single SST template

EPOCHE & ESPRI

- Security problem based in Risk analysis: Threats

Identifier	Description	Affected assets
T.THEFT-PHY	**Physical Theft.** Agents: - Outsider with rights - Outsider without any rights	A.TOE (C) A.INFO (C) A.PROT (C) A.EQUI (I) A.INFOSEC (CI) A.DEVSEC (IA
T.THEFT-LOG	**Logical Theft.** Agents: - Outsider with rights - Outsider without any rights	A.TOE (CI) A.INFO (CI) A.PROT (CI) A.EQUI (I) A.INFOSEC (CI) A.DEVSEC (IA)
T.NEGLIGENT	**Negligent employee.** Agents: - Insider with rights	A.TOE (I)
T.NON_AUTH_ACC	**Non Authorised Access.** Agents: - Insider without rights	A.INFO (C) A.INFOSEC (C)
T.AUTH_ACC	**Authorised Access.** Agents: - Insider with rights	A.TOE (CI) A.INFO (C)

Single SST template

EPOCHE & ESPRI

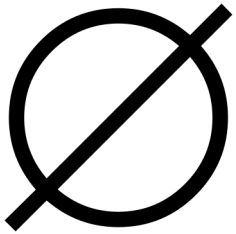
- Security problem: OSPs

Id	Description
P.CM	The organisation has implemented a configuration management system documented in the associated CM plan. The CM system guarantees the assignment of uniquely identifier to the TOEs configuration items, implements version and changes control (by means of procedures and the support of automated access control to the CM system) and provides automated support for the TOE generation and their acceptance. The CM system maintains under configuration management the TOEs, the parts of the TOEs, the implementation representation, the documentation generated and security flaws and their resolution status. The objective of this policy is to contribute to the integrity guarantee of the final product.
P. LCD	The engineer projects development culture of the organisation follows a life cycle model including development and security maintenance phases.
P. TRANSFER	Transfer of protected material out of the development environment and between different development sites is performed in accordance with defined acceptance procedures.
P. BACKUP	Backups will be created, stored and destroyed according to an approved procedure.

Single SST template

EPOCHE & ESPRI

- Security problem: Assumptions.



No assumptions should be included exempting the developer from meeting the ALC requirements.

If needed …….

- ✓ Should be outside the sphere of influence of the developer.
- ✓ Should be requirements for the final customer: security, CMC for maintenance, etc.

Single SST template

EPOCHE & ESPRI

- Security Objectives of the Site vs. Threats (I).

Threats	Security objectives
T.THEFT-PHY	O.SEG.PERIMETERS O.SEG.REVOKING O.SEG.VISITORS O.SEG.CRYPT O.SEG.RIP
T.THEFT-LOG	O.SEG.REVOKING O.SEG.AC O.SEG.PASSWD O.SEG.SEP-NET O.SEG.AC-REM O.SEG.INSTALL O.SEG.CRYPT O.SEG.AVIRUS O.SEG.INTERNET
T. NEGLIGENT	O.SEG.AWARE O.SEG.DEV O.CM.GENERATION

Single SST template

EPOCHE & ESPRI

- Security Objectives of the Site vs. Threats (II).

Threats	Security objectives
T.NON_AUTH_ACC	O.SEG.REVOKING O.SEG.AC O.SEG.PASSWD O.SEG.SEP-NET O.SEG.AC-REM O.SEG.INSTALL O.SEG.CRYPT O.SEG.AVIRUS O.SEG.INTERNET O.SEG.PERIMETERS
T.AUTH_ACC	O.SEG.AWARE O.SEG.DEV O.SEG.CRYPT O.SEG.RIP O.CM.CHANGE-CONTROL O.CM.GENERATION

Single SST template

EPOCHE & ESPRI

- Security Objectives of the Site vs. OSPs.

OSP	Security objectives
P.CM	O.CM.LABEL O.CM.VERSION-CONTROL O.CM.CHANGE-CONTROL O.CM.GENERATION O.CM.ACCEPTANCE O.CM.AUDIT
P. LCD	O.LCD
P. TRANSFER	O.SEG.TRANSFERS
P. BACKUP	O.SEG.BACKUP

Single SST template

EPOCHE & ESPRI

- Security Assurance Requirements to meet Site objectives. Configuration Management System.

Security Objective	SARs	Rationale
O.CM.LABEL	ALC_CMC.4.1/2/3D ALC_CMC.4.1/2/3/6/7C ALC_CMS.4.1D ALC_CMS.4.1/2/3C	CMS - Identification mechanism. The procedures are applied to the CIs.
O.CM.VERSION-CONTROL	ALC_CMC.4.1/2/3D ALC_CMC.4.1/2/3/6/7C ALC_CMS.4.1D ALC_CMS.4.1/2/3C	CMS - Identification mechanism → CI version control. The procedures are applied to the CIs.
O.CM.CHANGE-CONTROL	ALC_CMC.4.2/3D ALC_CMC.4.4/6/7C ALC_CMS.4.1D ALC_CMS.4.1/2/3C	CMS - automated access control mechanism → authorised changes. The procedures are applied to the CIs.
O.CM.GENERATION	ALC_CMC.4.2/3D ALC_CMC.4.5/6/7C	CMS - automated tools for the generation of the TOE.
O.CM.ACCEPTANCE	ALC_CMC.4.2/3D ALC_CMC.4.8/6/7C	The CM plan documents procedures defining the acceptance criteria.
O.CM.AUDIT	ALC_CMC.4.3D ALC_CMC.4.9/10C	The use of the system allows generating records.

Single SST template

EPOCHE & ESPRI

- Security Assurance Requirements to meet Site objectives. Developers security (I).

Security Objectives	SARs	Rationale
O.SEG.PERIMETERS	ALC_DVS.1.1D ALC_DVS.1.1C	Avoid unauthorised access to the company and to the development area.
O.SEG.TRANSFERS	ALC_DVS.1.1D ALC_DVS.1.1C	Protection sensitive material transferred between different areas with the company.
O.SEG.DEV	ALC_DVS.1.1D ALC_DVS.1.1C	Approved management procedure: NDA and training in security procedures to get access rights.
O.SEG.REVOKING	ALC_DVS.1.1D ALC_DVS.1.1C	Rights revocation if someone is removed from the development team due to disciplinary matters or dismissal.
O.SEG.AWARE	ALC_DVS.1.1D ALC_DVS.1.1C	The development team members shall aware of their responsibilities with regard to development security.
O.SEG.VISITORS	ALC_DVS.1.1D ALC_DVS.1.1C	There are security procedures in place for identifying, logging and escorting all visitors to the development.
O.SEG.AC	ALC_DVS.1.1D ALC_DVS.1.1C	Logical access to OS and CMS is based in identification of the individual and not at group level.
O.SEG.PASSWD	ALC_DVS.1.1D ALC_DVS.1.1C	There is a password policy in place guaranteeing the passwords strength.

Single SST template

EPOCHE & ESPRI

- Security Assurance Requirements to meet Site objectives. Developers security (II).

Security Objectives	SARs	Rationale
O.SEG.SEP-NET	ALC_DVS.1.1D ALC_DVS.1.1C	The entry point into the development area's network is protected at the corporate network boundary.
O.SEG.AC-REM	ALC_DVS.1.1D ALC_DVS.1.1C	There are security procedures in place requiring secure communications for remote access to the CM system.
O.SEG.INSTALL	ALC_DVS.1.1D ALC_DVS.1.1C	Secure configuration of the development machines.
O.SEG.CRYPT	ALC_DVS.1.1D ALC_DVS.1.1C	There are security procedures in place requiring that the development equipments HD are encrypted.
O.SEG.AVIRUS	ALC_DVS.1.1D ALC_DVS.1.1C	There are security procedures in place requiring that the development equipments have updated anti-virus.
O.SEG.BACKUP	ALC_DVS.1.1D ALC_DVS.1.1C	There are security procedures in place for creating, storing and destroying backups.
O.SEG.RIP	ALC_DVS.1.1D ALC_DVS.1.1C	Security procedures in place for destroying materials that are no longer used within the development area.
O.SEG.INTERNET	ALC_DVS.1.1D ALC_DVS.1.1C	Development team is aware of the company policy: internet use, material destruction, 'working from home', etc.

Single SST template

EPOCHE & ESPRI

- Security Assurance Requirements to meet Site objectives. Life Cycle model.

Security Objectives	SARs	Rationale
O.LCD	ALC_LCD.1.1/2D ALC_LCD.1.1/2C	Established of a life cycle model covering the development and security maintenance of the TOEs. The model provides the appropriate control over the development and maintenance of the products.

Single SST template

EPOCHE & ESPRI

- Security Assurance Requirements. Application Notes.

CMC

ALC_CMC.4.1D	The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.4.1C	The TOE shall be labelled with its unique reference.
ALC_CMC.4.9C	The evidence shall demonstrate that all configuration items are being maintained under the CM system.

CMS

ALC_CMS.4.1D	The developer shall provide a configuration list for the TOE.
ALC_CMS.4.1C	The **configuration** list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

LCD

ALC_LCD.1.1C	The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.
ALC_LCD.1.2C	The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Single SST template

EPOCHE & ESPRI

- Site Summary Specification (SSS)
  - Identify evidence needed for the Site to meet the SARs and describe how the Site met the SARs.
  - ALC_DVS: how it fulfils the attack potential claimed.
  - The SSS has to describe WHAT but not HOW.
  - Sanitized version of the SST ➔ without SSS.

Single SST template

EPOCHE & ESPRI

- Site Summary Specification (SSS). Attack potential.
  - Attack potential calculation.

Threat Identifier	Attack potential calculation
T.THEFT-PHY	**Physical Theft.** **Agents**: - Outsider with rights - Outsider without any rights **Parameters** - sufficient time to investigate the site from outside - simple equipment to carry out a robbery or manipulate TOE components. **Attack potential** These agents have limited resources but they have enough time to prepare the attack. It is considered an **Enhanced Basic** attack potential.

Conclusions - 1st

- Site certification
  - Reusability: same area, same procedures
    - ✓ Significant reduction of time and money efforts.
    - ✓ Marketing

Conclusions – and 2nd

EPOCHE & ESPRI

- The Single SST template:
  - May derived in a a PP with the common aspects helping in the definition of a set of minimum reqs. for medium assurance (e.g. EAL3 & EAL4).
  - May be extended to cover multiple sites in a supply chain including secure delivery. Main add-ons:
    - ✓ security measures for transfers between sites
    - ✓ acceptance procedures.

EPOCHE & ESPRI

Jose Emilio Rico
tech@epoche.es

Epoche & Espri, S.L.U.
Avda. de la Vega, 1
28108, Alcobendas, Madrid
Spain

Tel: +34 914-902-900
FAX: +34 916-625-344

Epoche & Espri Corporation
4000 Legato Road, Suite 1100
Fairfax, VA 22033
USA

Tel: +1 888-877-9506
FAX: +1 703-227-7189