ALC class - Proposal for minimum assurance requirements

Certification Body - Spain.

14th International Common Criteria Conference.

Luis M. Fernández

Outline

- Proposal to enforce ALC SARs for EAL2 certifications
- Reuse of ALC class efforts applying Site Certification procedures
- Supply chain security assurance within ALC class

Current Situation

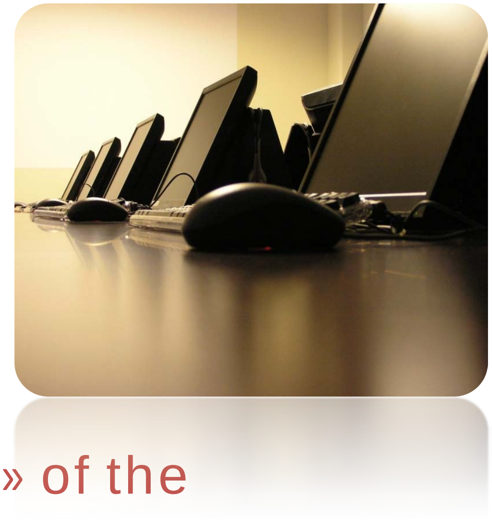
- Vision Statement
  - *The general security level of general ICT COTS certified products needs to be raised without severely impacting price and timely availability of these products*
  - *The level of standardization has to be increased by building Technical Communities (TC) developing collaborative Protection Profiles ("cPPs") and supporting documents, in order to reach reasonable, comparable, reproducible and cost-effective evaluation results*
  - *The existing application of STs and PPs still applies, but its CCRA mutual recognition should be limited to EAL 2.*

Current Situation

- Security Assurance Requirements for ALC class in EAL 2 certifications

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3

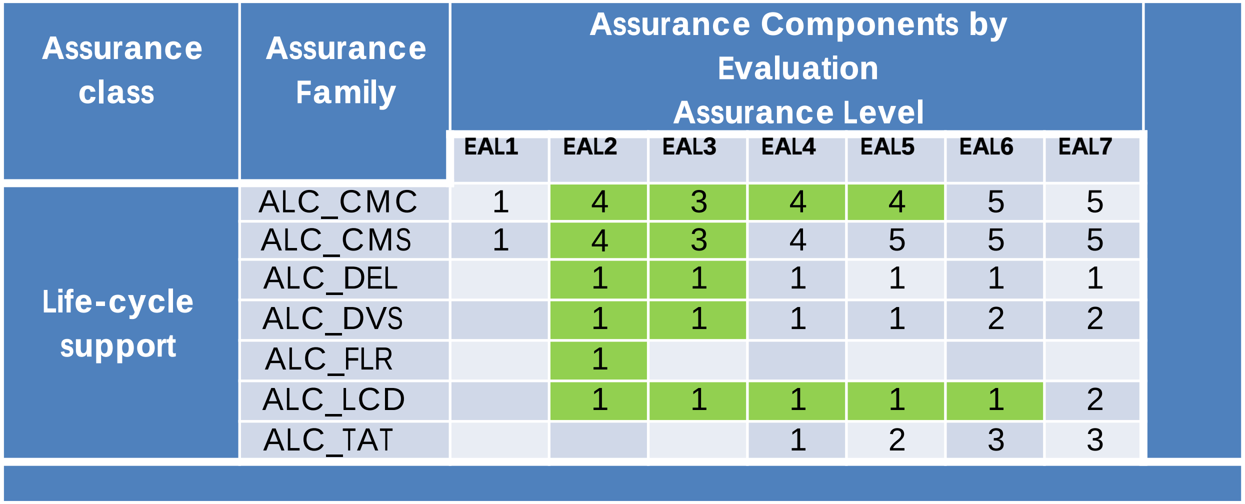
Current Situation



- EAL 2 ALC class components
  - ALC_CMC.2
    - TOE & CI labeled with unique reference.
  - ALC_CMS.2
    - Configuration list composed of the «parts» of the TOE and for each developer must be identified
  - ALC_DEL.1
    - Method of delivery to the TOE consumer. Secure delivery from developer.

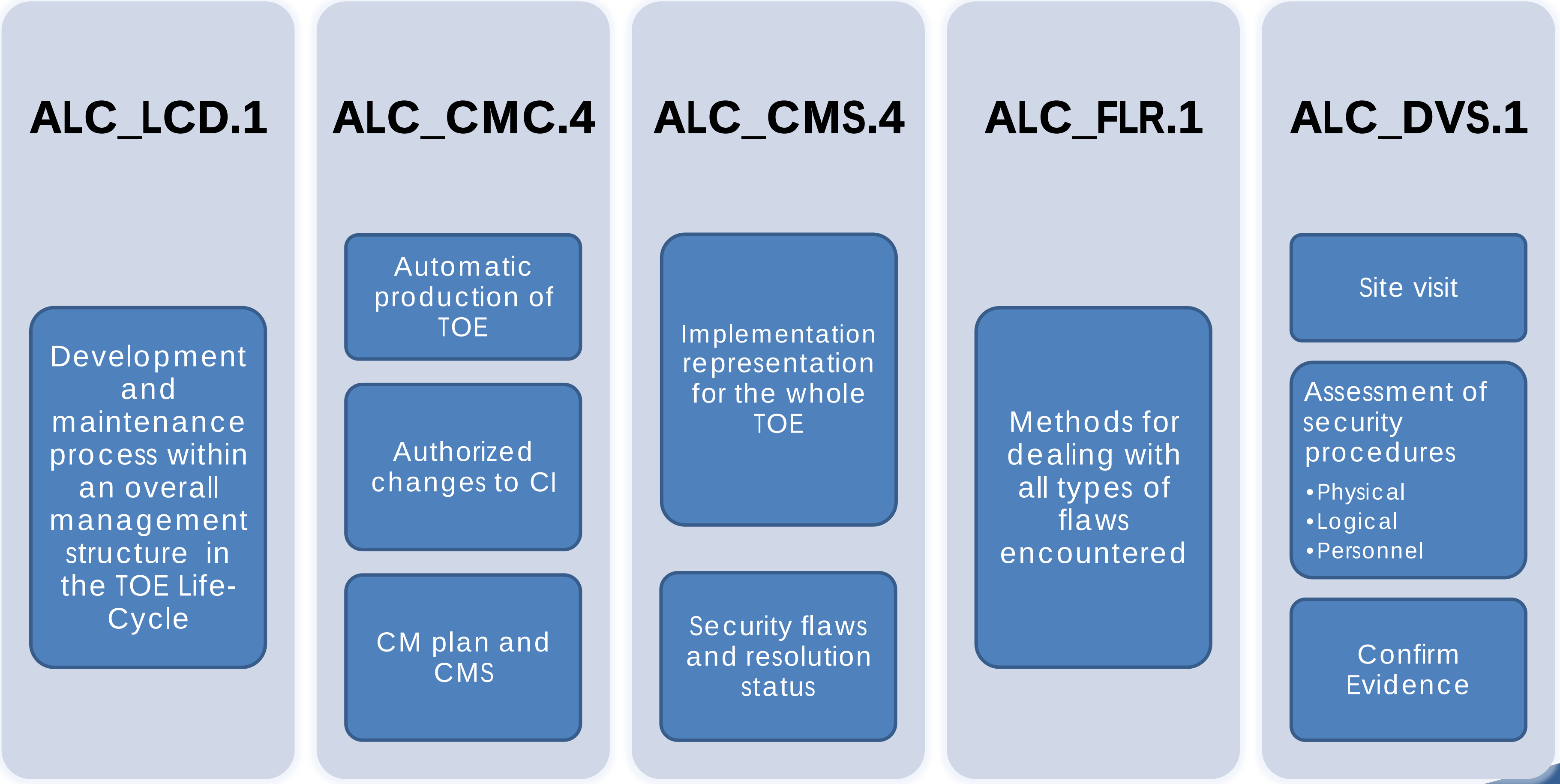
ALC Proposal

- Component rearrangement for EAL2 evaluations according to the Vision Statement.



Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Life-cycle support	ALC_CMC	1	4	3	4	4	5	5
	ALC_CMS	1	4	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS		1	1	1	1	2	2
	ALC_FLR		1					
	ALC_LCD		1	1	1	1	1	2
	ALC_TAT				1	2	3	3

ALC Proposal



ALC_LCD.1

- Development and maintenance process within an overall management structure in the TOE Life-Cycle

ALC_CMC.4

- Automatic production of TOE
- Authorized changes to CI
- CM plan and CMS

ALC_CMS.4

- Implementation representation for the whole TOE
- Security flaws and resolution status

ALC_FLR.1

- Methods for dealing with all types of flaws encountered

ALC_DVS.1

- Site visit
- Assessment of security procedures
  - Physical
  - Logical
  - Personnel
- Confirm Evidence

ALC Proposal

- Outline of security improvements within the proposal
  - Specific Life-cycle definition for the TOE
  - TOE produced by automated means
  - TOE fully identified (source code level) and managed
  - Development site(s) security measures evaluated
  - Procedures to address security flaws

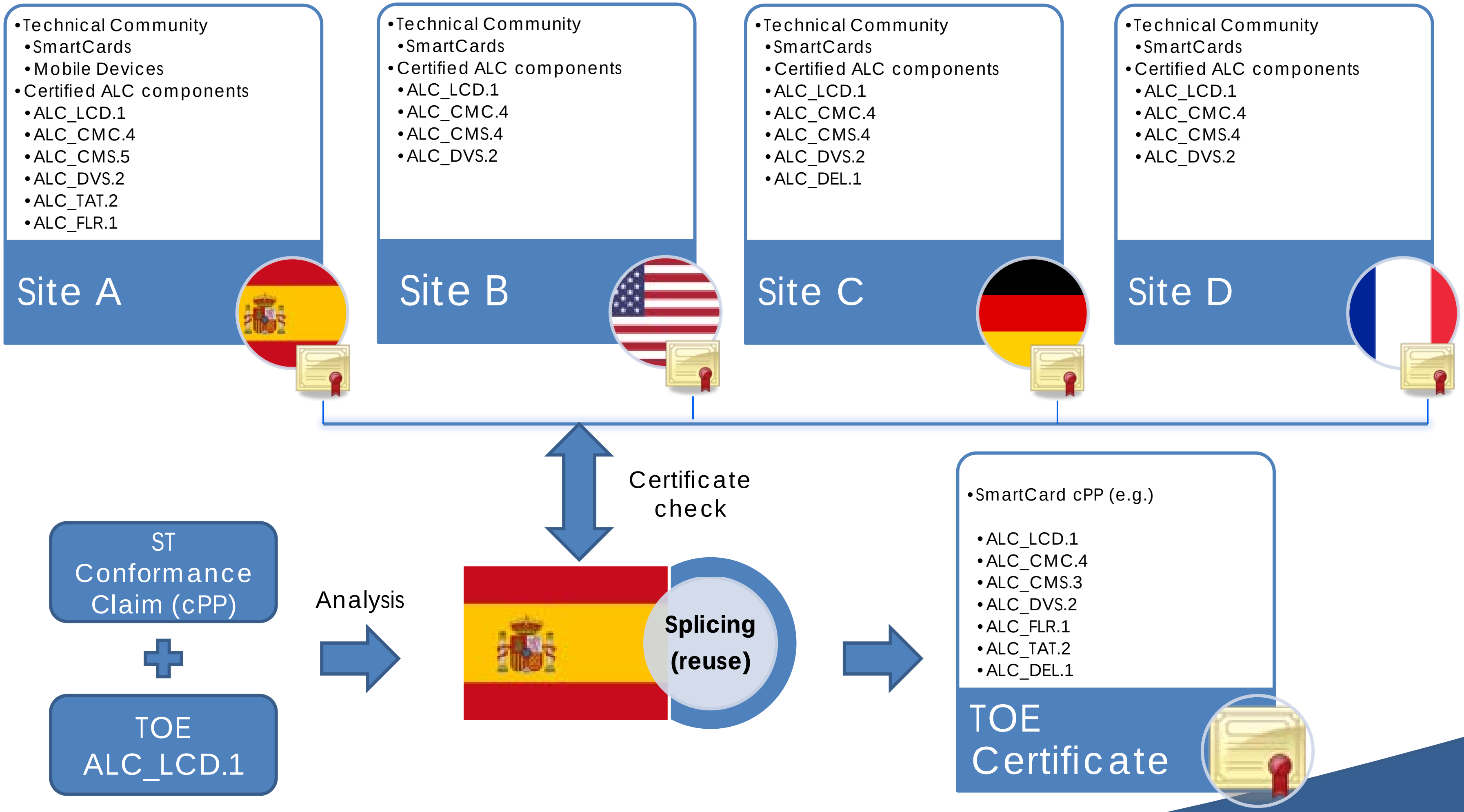
ALC Proposal

- You might think
  - *“This proposal increases the workload for CC certifications”*
  - *“Too much effort for this assurance level”*
- There is a possible answer.
  - ***Re-use the evaluation results.***
- This is not a new idea. There is already a tool to use:
  - **CCDB-2007-11-01 Site Certification**

Site Certification

- Site Certification process according to CCDB-2007-11-01
  - TOE independent CC certification to confirm that a specific development environment fulfills the CC requirements regarding ALC class.
  - These evaluation activities can be reused in a TOE evaluations later on.
  - Based on activities and procedures defined in the Life-cycle (ALC_LCD) and the claimed attack potential.

Site Certification



- Technical Community
  - SmartCards
  - Mobile Devices
- Certified ALC components
  - ALC_LCD.1
  - ALC_CMC.4
  - ALC_CMS.5
  - ALC_DVS.2
  - ALC_TAT.2
  - ALC_FLR.1

Site A

- Technical Community
  - SmartCards
- Certified ALC components
  - ALC_LCD.1
  - ALC_CMC.4
  - ALC_CMS.4
  - ALC_DVS.2

Site B

- Technical Community
  - SmartCards
  - Certified ALC components
  - ALC_LCD.1
  - ALC_CMC.4
  - ALC_CMS.4
  - ALC_DVS.2
  - ALC_DEL.1

Site C

- Technical Community
  - SmartCards
- Certified ALC components
  - ALC_LCD.1
  - ALC_CMC.4
  - ALC_CMS.4
  - ALC_DVS.2

Site D

Certificate check

ST Conformance Claim (cPP)

TOE ALC_LCD.1

Analysis

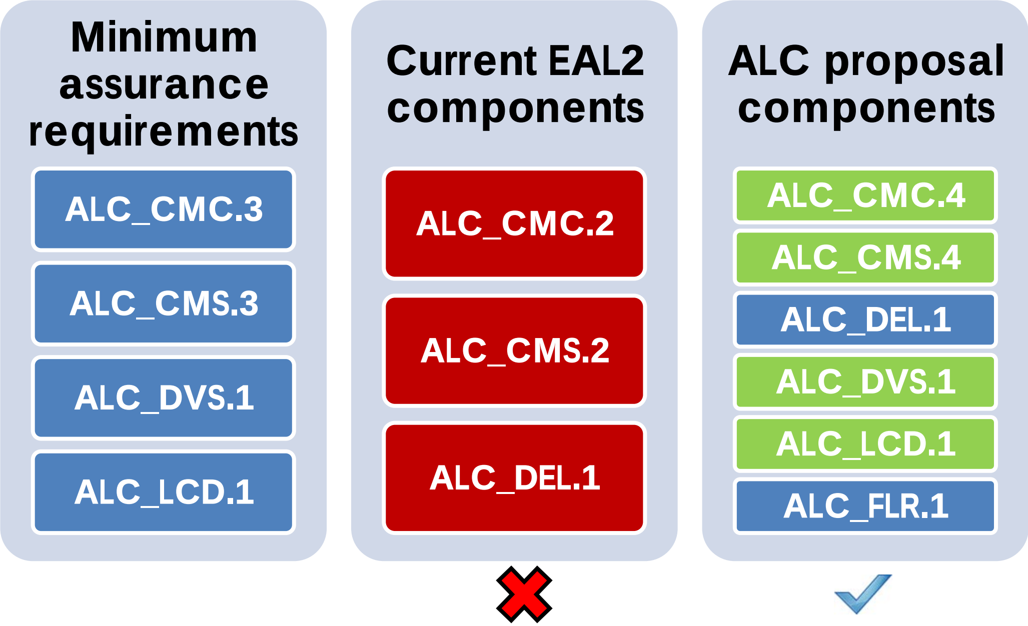
Splicing (reuse)

- SmartCard cPP (e.g.)
  - ALC_LCD.1
  - ALC_CMC.4
  - ALC_CMS.3
  - ALC_DVS.2
  - ALC_FLR.1
  - ALC_TAT.2
  - ALC_DEL.1

TOE Certificate

Site Certification

- Efficiency and reuse of results for ALC class
  - **There is a problem**: Minimum assurance requirements for Site Certification according to CCDB-2007-11-01:



Minimum assurance requirements	Current EAL2 components	ALC proposal components
ALC_CMC.3	ALC_CMC.2	ALC_CMC.4
ALC_CMS.3	ALC_CMS.2	ALC_CMS.4
ALC_DVS.1	ALC_DEL.1	ALC_DEL.1
ALC_LCD.1		ALC_DVS.1
		ALC_LCD.1
		ALC_FLR.1
	✗	✓

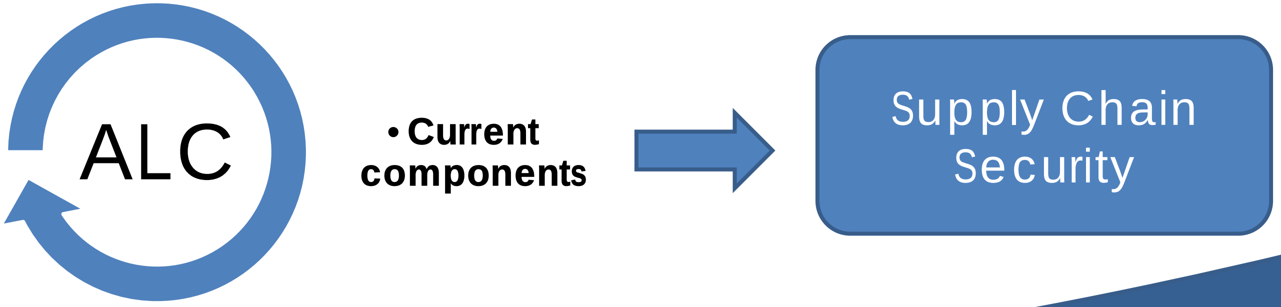
- This proposal makes compatible the Vision Statement with Site Certification processes and supporting documents.

Site Certification

- Benefits
  - For the TOE consumer
    - Security assessment of the whole TOE life-cycle
    - Supply chain assurance (as we'll see later)
  - For the TOE developer
    - Maximum reuse of ALC class documentation
    - Obtain an additional Certificate to certify Development Site Security (similar to ISO 27000 approach)
    - Flexibility: combine certified sites in different countries decreasing ALC class evaluation efforts.

Supply Chain and ALC proposal

- The Council of Supply Chain Management Professionals defines supply chain management as follows:
  - "Supply Chain Management encompasses the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities. Importantly, it also includes coordination and collaboration with channel partners, which can be suppliers, intermediaries, third-party service providers, and customers. […]"
- All this activities are closely related to the TOE Life-Cycle as defined in CC



ALC

- Current components

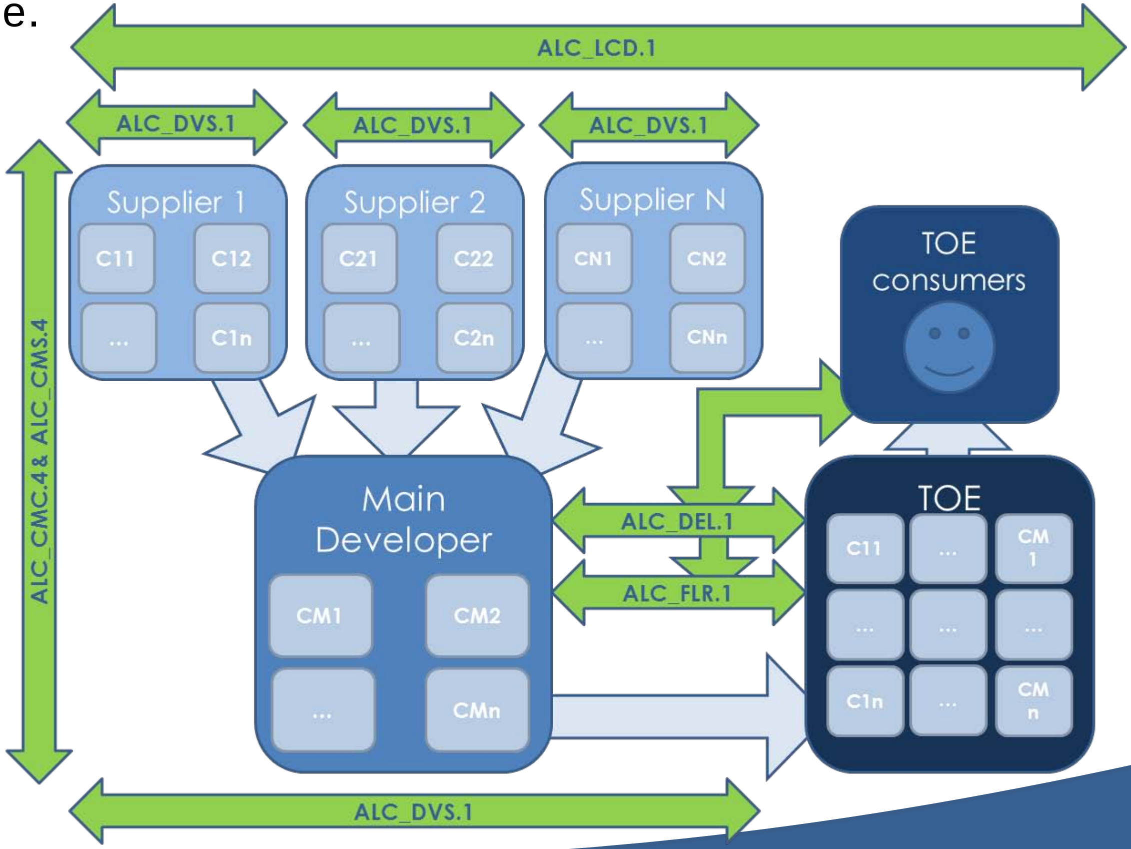
Supply Chain Security

Supply Chain and ALC proposal

- TOE might be composed of different components and parts developed by different entities in different tiers.
- CC considers the TOE as a whole and takes into account each part, so security assessment considers security maintenance processes for each component.
- ALC proposal components supply chain coverage
  - ALC_LCD.1 - provides definitions and procedures of phases on the development and security maintenance of the TOE. Documents should provide information about
    - Where each phase takes place? → **Site**
    - Who is responsible of each phase? → **Organization**
    - What activities are carried out in each phase (inputs/outputs)? → **Policies**
    - How these activities are considered by each actor? → **Processes**

Supply Chain and ALC proposal

- Once this information is provided then all the other ALC components deeply address security issues related to the supply chain in each phase.



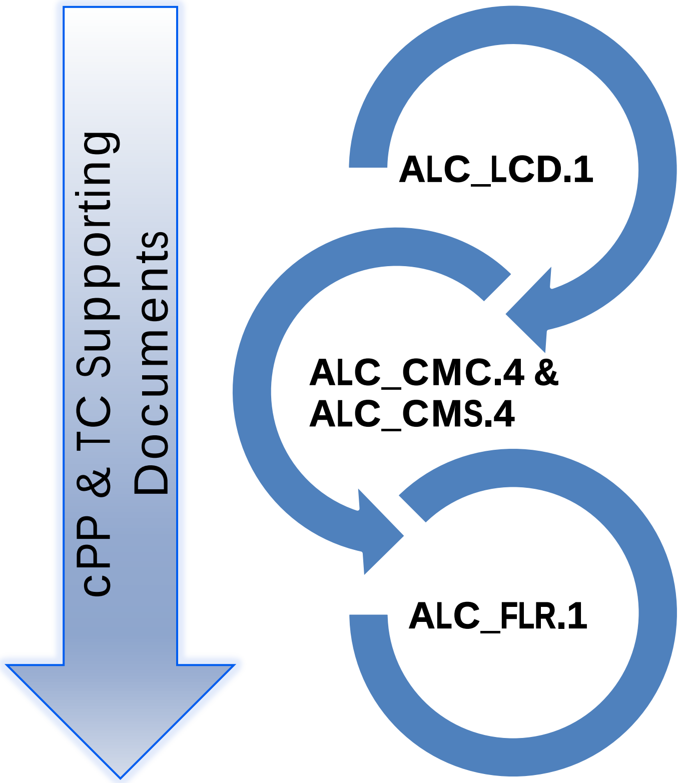
ALC Proposal & Vision Statement

- Refinements to ALC components within iTCs and cPP.
  - iTC can refine ALC requirements and components to better fit them with different technologies.
  - ALC supporting documents aligned with technologies in the scope of a specific iTC.
  - Site Certificate recognition agreements between Schemes in iTC.

- Life-cycle definition
- CI identification measures
- CI Confidentiality & Integrity measures
- Minimum Site Requirements

ALC Proposal & Vision Statement

- Some ideas for refinements to ALC components in TC and cPP.



cPP & TC Supporting Documents

ALC_LCD.1

ALC_CMC.4 & ALC_CMS.4

ALC_FLR.1

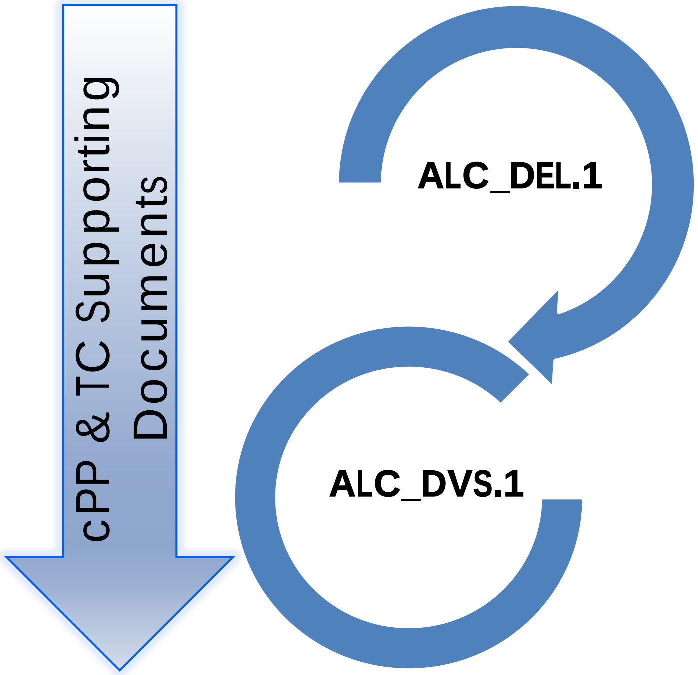
- Development & manufacturing phases
- Actors, roles and responsibilities
- Common Policies and Processes

- Procedures to identify and track CI and TOE components
- Integrity control measures

- Flaw remediation processes to address Supply Chain flaws.

ALC Proposal & Vision Statement

- Refinements to ALC components in TC and cPP.

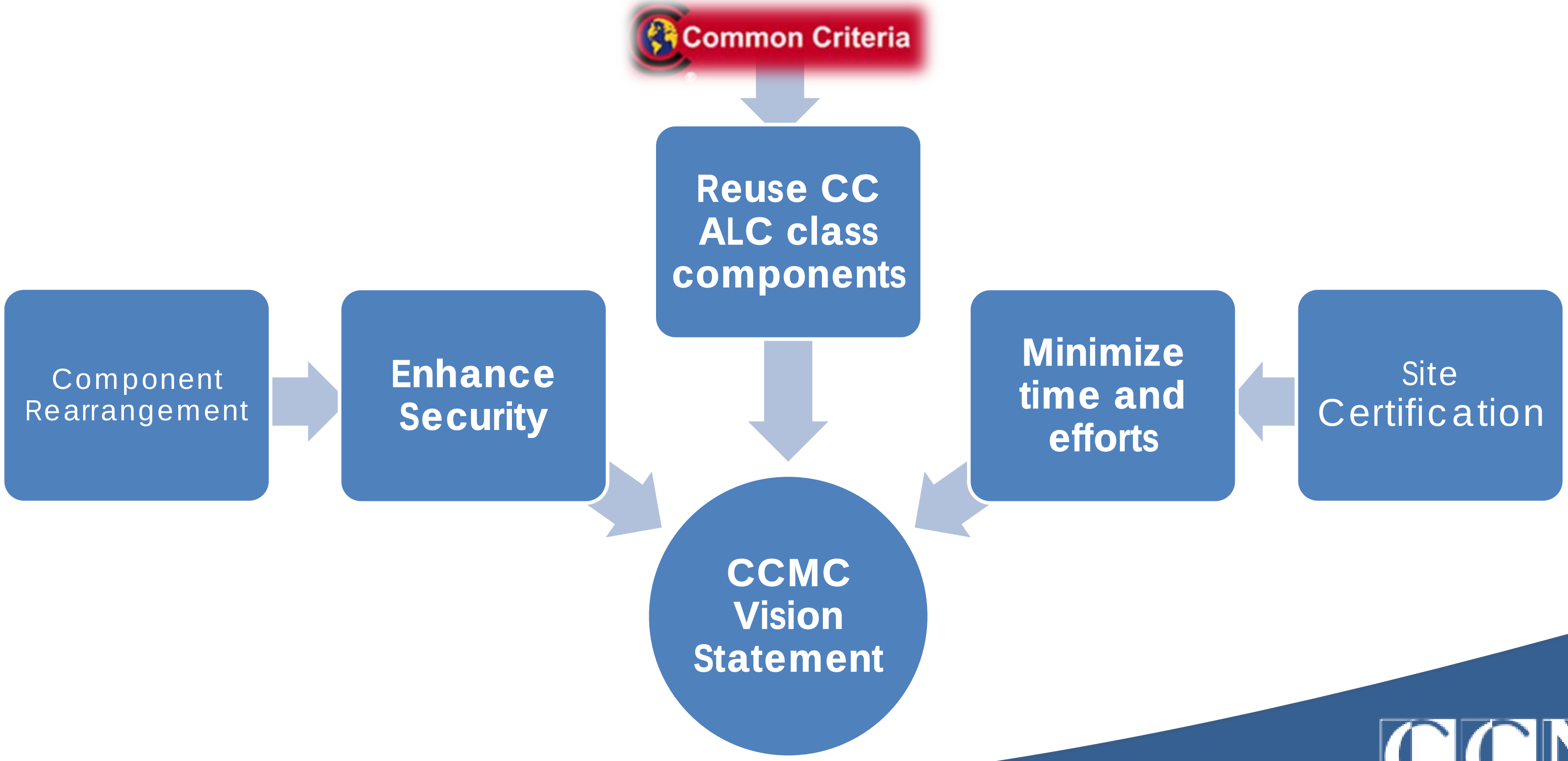


- Protect TOE integrity delivery to consumers
- Traceability in the Supply Chain.

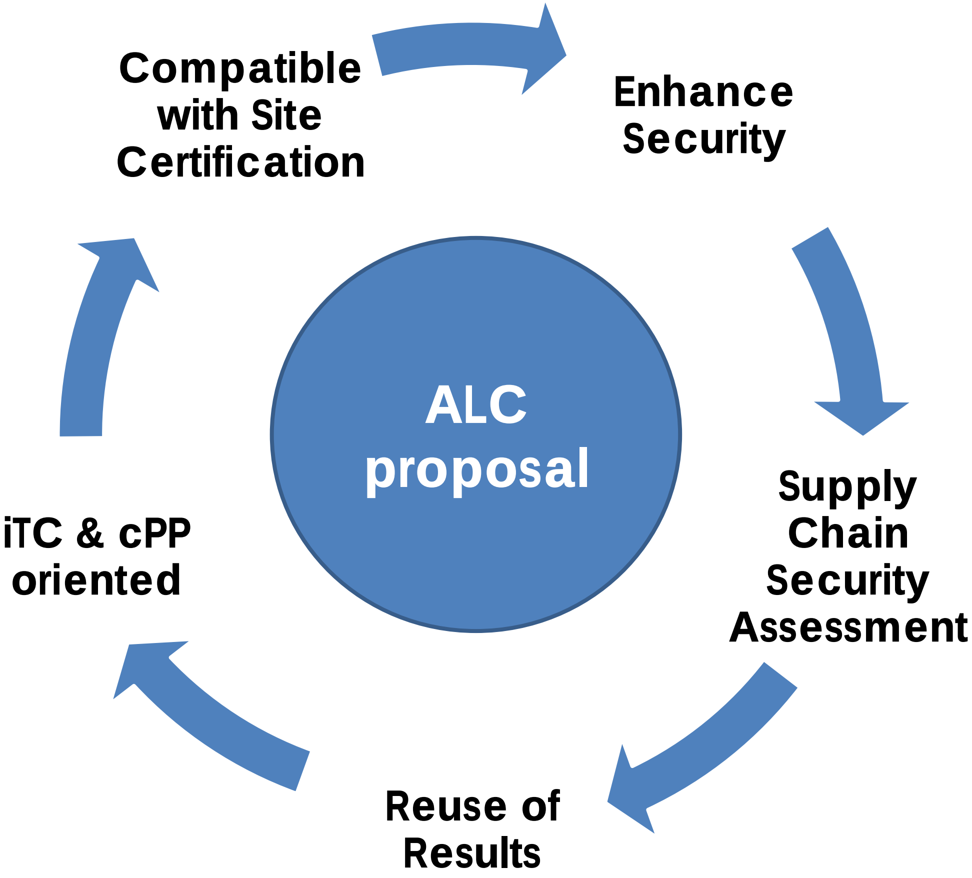
- Minimum site requirements
- Protect TOE CI integrity in internal deliveries (subcontractors and development sites).
- Accountability and traceability of CI
- Rules to reuse Site Certificates depending on the technology area.

ALC Proposal & Vision Statement

- Alignment with the vision statement



Conclusions



ALC proposal

Compatible with Site Certification

Enhance Security

Supply Chain Security Assessment

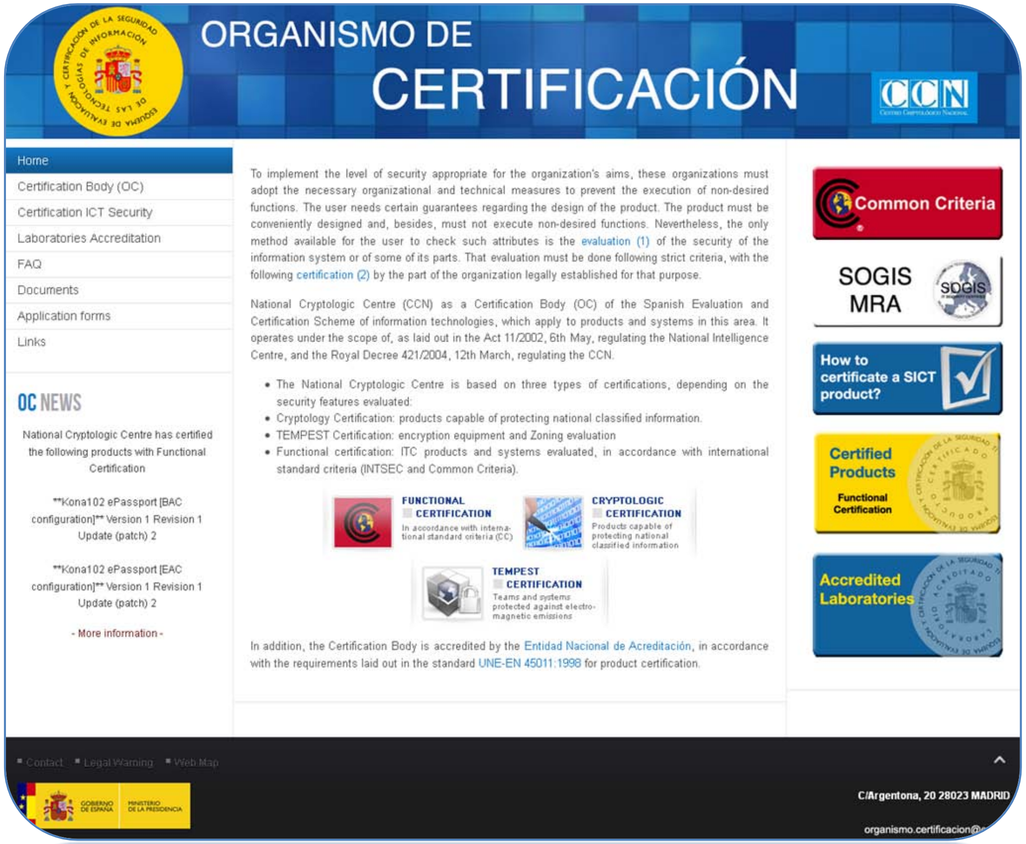
Reuse of Results

iTC & cPP oriented

ALC class - Proposal for minimum assurance requirements

Contact Information

- E-mail
  - organismo.certificacion@cni.es
- Web Site:
  - www.oc.ccn.cni.es



OC NEWS

National Cryptologic Centre has certified the following products with Functional Certification

Kona102 ePassport [BAC configuration] Version 1 Revision 1 Update (patch) 2

Kona102 ePassport [EAC configuration] Version 1 Revision 1 Update (patch) 2

- More information -

To implement the level of security appropriate for the organization's aims, these organizations must adopt the necessary organizational and technical measures to prevent the execution of non-desired functions. The user needs certain guarantees regarding the design of the product. The product must be conveniently designed and, besides, must not execute non-desired functions. Nevertheless, the only method available for the user to check such attributes is the evaluation (1) of the security of the information system or of some of its parts. That evaluation must be done following strict criteria, with the following certification (2) by the part of the organization legally established for that purpose.

National Cryptologic Centre (CCN) as a Certification Body (OC) of the Spanish Evaluation and Certification Scheme of information technologies, which apply to products and systems in this area. It operates under the scope of, as laid out in the Act 11/2002, 6th May, regulating the National Intelligence Centre, and the Royal Decree 421/2004, 12th March, regulating the CCN.

- The National Cryptologic Centre is based on three types of certifications, depending on the security features evaluated:
- Cryptology Certification: products capable of protecting national classified information.
- TEMPEST Certification: encryption equipment and Zoning evaluation
- Functional certification: ITC products and systems evaluated, in accordance with international standard criteria (INTSEC and Common Criteria).

FUNCTIONAL CERTIFICATION In accordance with international standard criteria (CC)

CRYPTOLOGIC CERTIFICATION Products capable of protecting national classified information

TEMPEST CERTIFICATION Teams and systems protected against electro-magnetic emissions

In addition, the Certification Body is accredited by the Entidad Nacional de Acreditación, in accordance with the requirements laid out in the standard UNE-EN 45011:1998 for product certification.

C/Argentona, 20 28023 MADRID
organismo.certificacion@

References

- [CCMB-2012-09-001] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4, Sept. 2012
- [CCMB-2012-09-003] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4, Sept. 2012
- [CCMB-2012-09-004] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4, Sept.2012
- [2012-09-001] Vision statement for the future direction of the application of the CC and the CCRA, version 2.0. Sept. 2012
- [CCDB-2007-11-001] Site Certification, version 1.0. Oct. 2007.