Securing the e-conomy,
We have the key.

# CC-EAL4 Certification of KeyOne v3

Jordi Íñigo Griera
Software Development Manager
Safelayer Secure Communications, S.A.

SAFELAYER

# Index

- Motivation
- Certification Scope
- Procedural improvements
- Product improvements

# Motivation

- Marketing / Management

  → EAL4+

  → CWA-14167-1

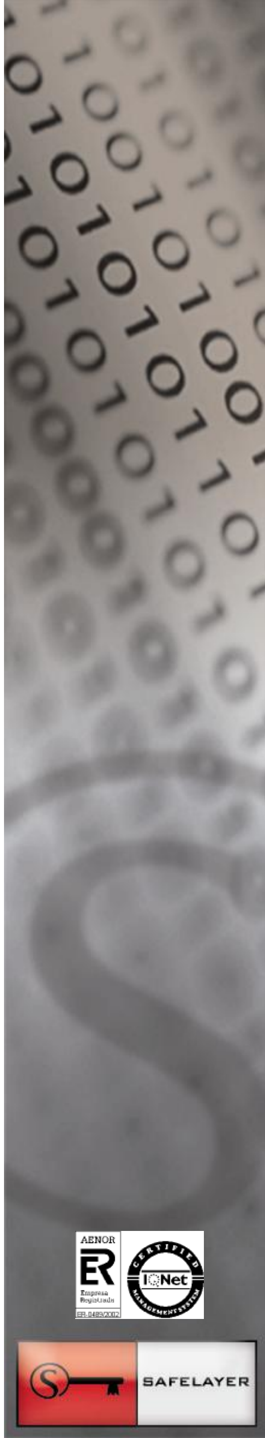
- CWA-14167-1

  → "Qualified Certificates"

- Commercial (NATO)

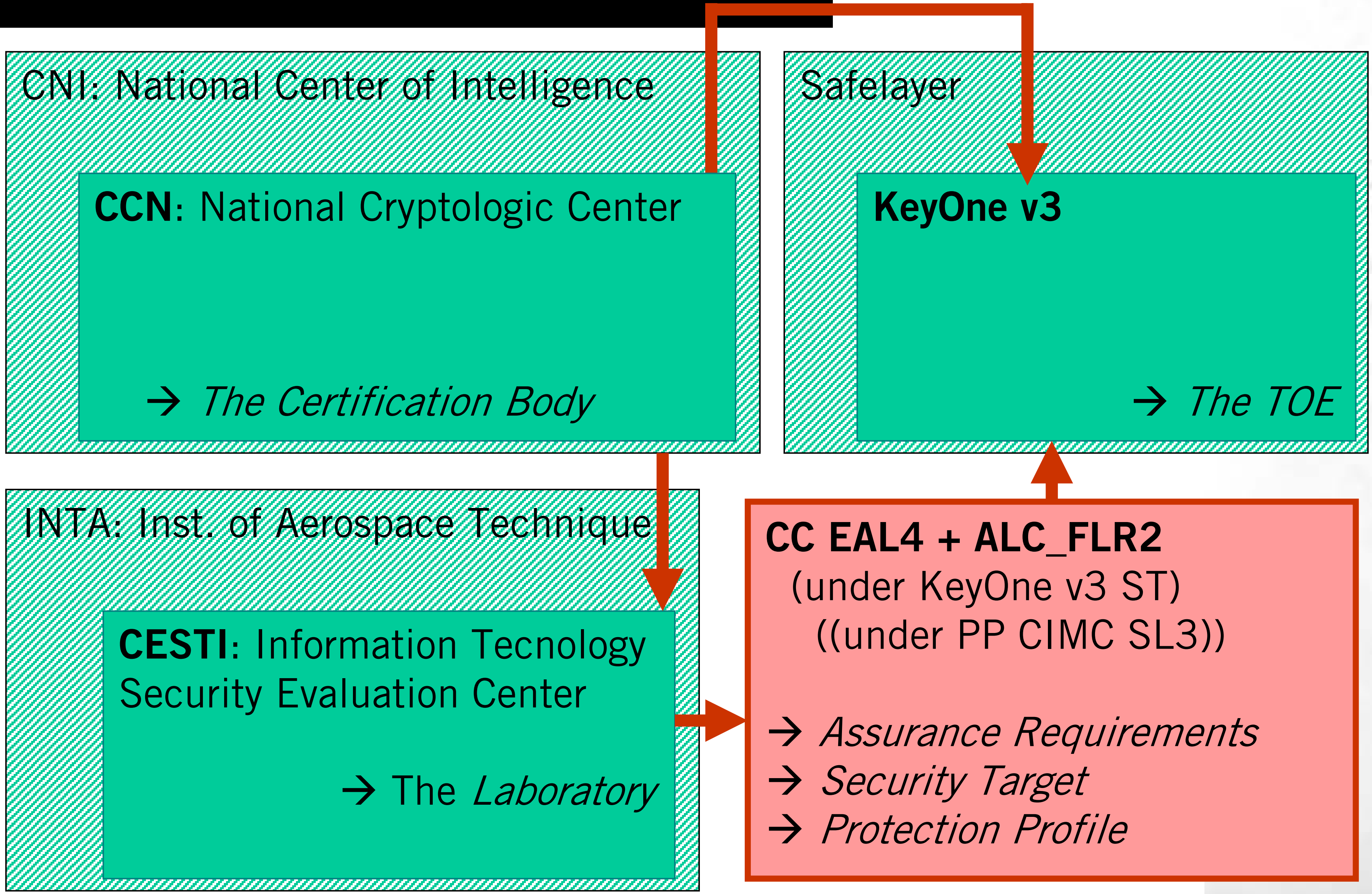
  → "CIMC"

- EAL4+ under PP-CIMC-SL3
  - Approach similar to CWA-14167-1



# CERTIFICATION SCOPE

# Process



CNI: National Center of Intelligence

**CCN**: National Cryptologic Center

→ *The Certification Body*

Safelayer

**KeyOne v3**

→ *The TOE*

INTA: Inst. of Aerospace Technique

**CESTI**: Information Tecnology Security Evaluation Center

→ The *Laboratory*

**CC EAL4 + ALC_FLR2**
(under KeyOne v3 ST)
((under PP CIMC SL3))

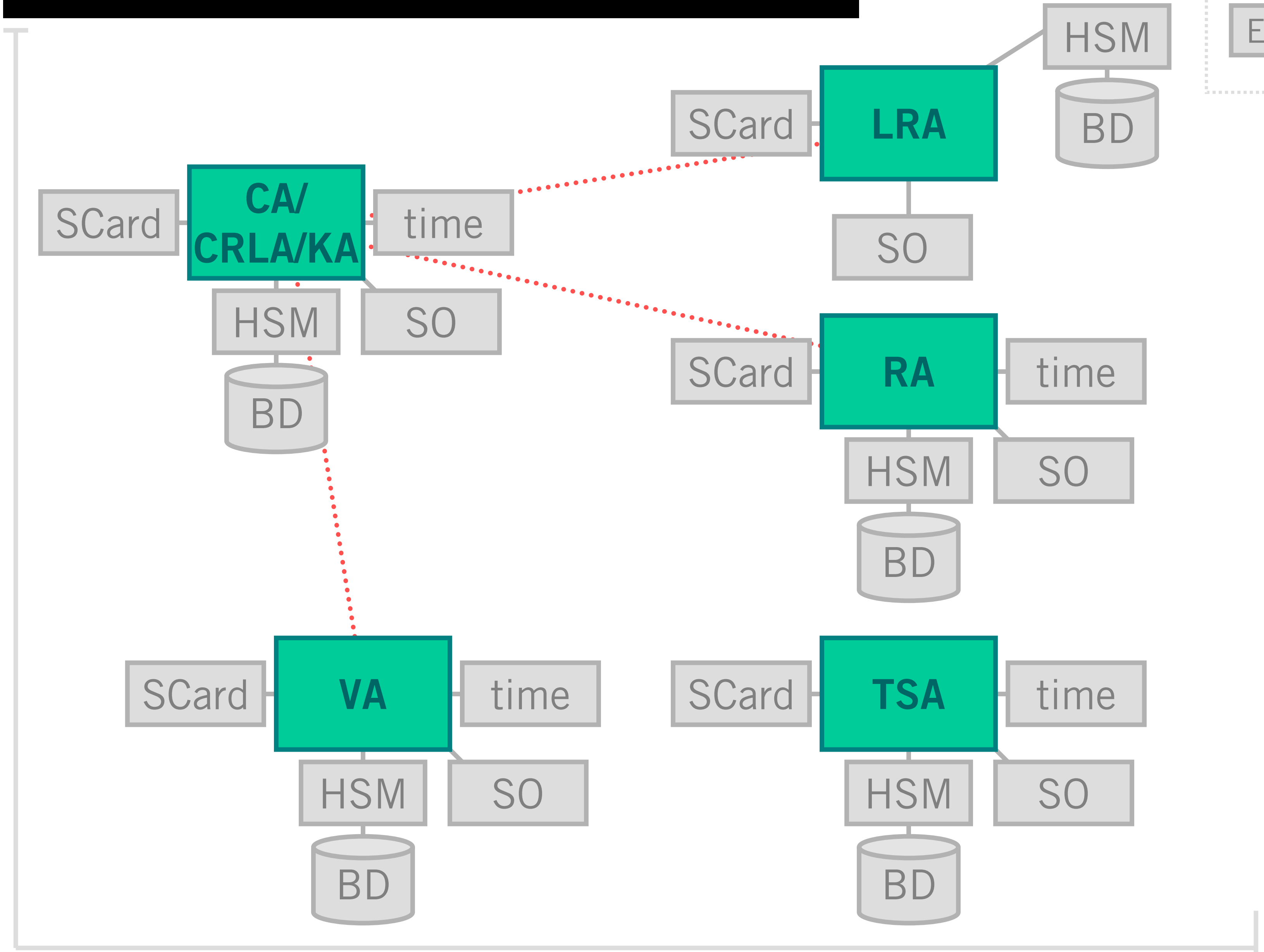
→ *Assurance Requirements*
→ *Security Target*
→ *Protection Profile*

# Certification Scope

- TOE: KeyOne® 3.0 (3.0.04S2R1)
  - PP: Certificate Issuing and Management Components(CIMC), Security Level 3
  - Assurance Requirements for the CC EAL4 plus ALC_FLR.2

- TOE: *subsystems that provide specific functionalities of a PKI, managing certificates for the support of electronic signature*

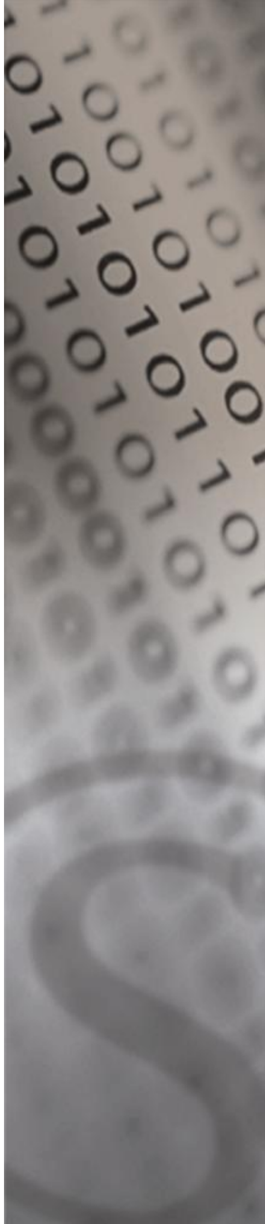
# Certified Products

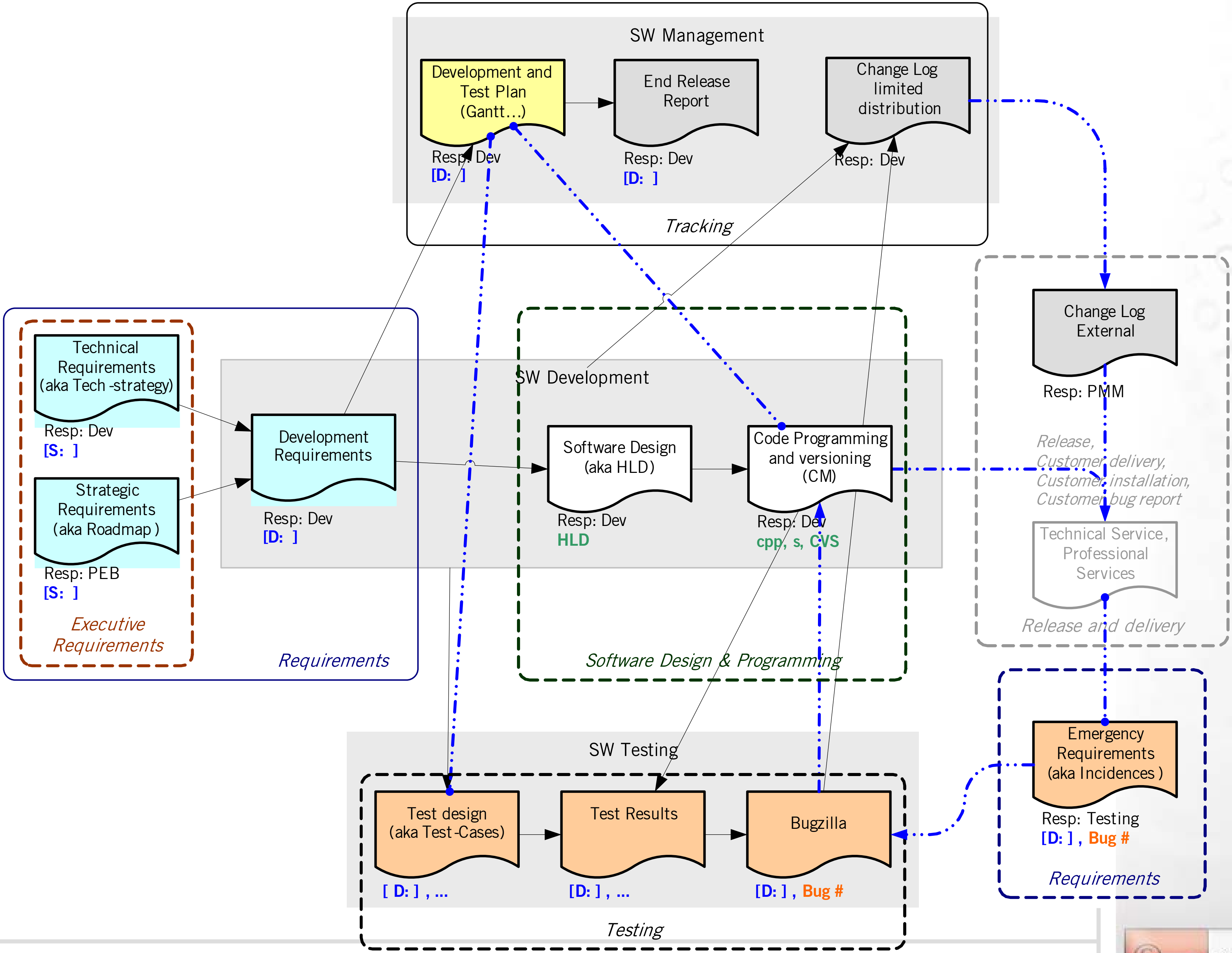


# Procedural improvements

# Development Process

- This system consists of the integration of different tools in a single system
  - Use of labels ( [Project:], [Release:], [S:], [D:], ...)
  - **ATR**$^{SFLY}$, traceability of requirements, planning and tracking
    - Graphic view of executive requirements S:
    - Graphic view of the product architecture
    - Accounting (resources, hours)
    - Tests cases under requirements D:
  - Meeting minute $^{LOTUS/SFLY}$ related to requirements
  - Electronic mail / Design Forum $^{LOTUS}$
    - threads of discussion related to requirements
  - **CVS**$^{GNU}$, implementation of requirements
  - **Documental server**$^{SFLY}$ : versioned and publication of documents
  - **Bugzilla**$^{GNU}$, against requirements





SW Management

Development and Test Plan (Gantt…)
Resp: Dev
[D: ]

End Release Report
Resp: Dev
[D: ]

Change Log limited distribution
Resp: Dev

*Tracking*

Technical Requirements (aka Tech-strategy)
Resp: Dev
[S: ]

Strategic Requirements (aka Roadmap)
Resp: PEB
[S: ]

*Executive Requirements*

Development Requirements
Resp: Dev
[D: ]

*Requirements*

SW Development

Software Design (aka HLD)
Resp: Dev
HLD

Code Programming and versioning (CM)
Resp: Dev
cpp, s, CVS

*Software Design & Programming*

Change Log External
Resp: PMM

*Release, Customer delivery, Customer installation, Customer bug report*

Technical Service, Professional Services

*Release and delivery*

SW Testing

Test design (aka Test-Cases)
[ D: ] , …

Test Results
[D: ] , …

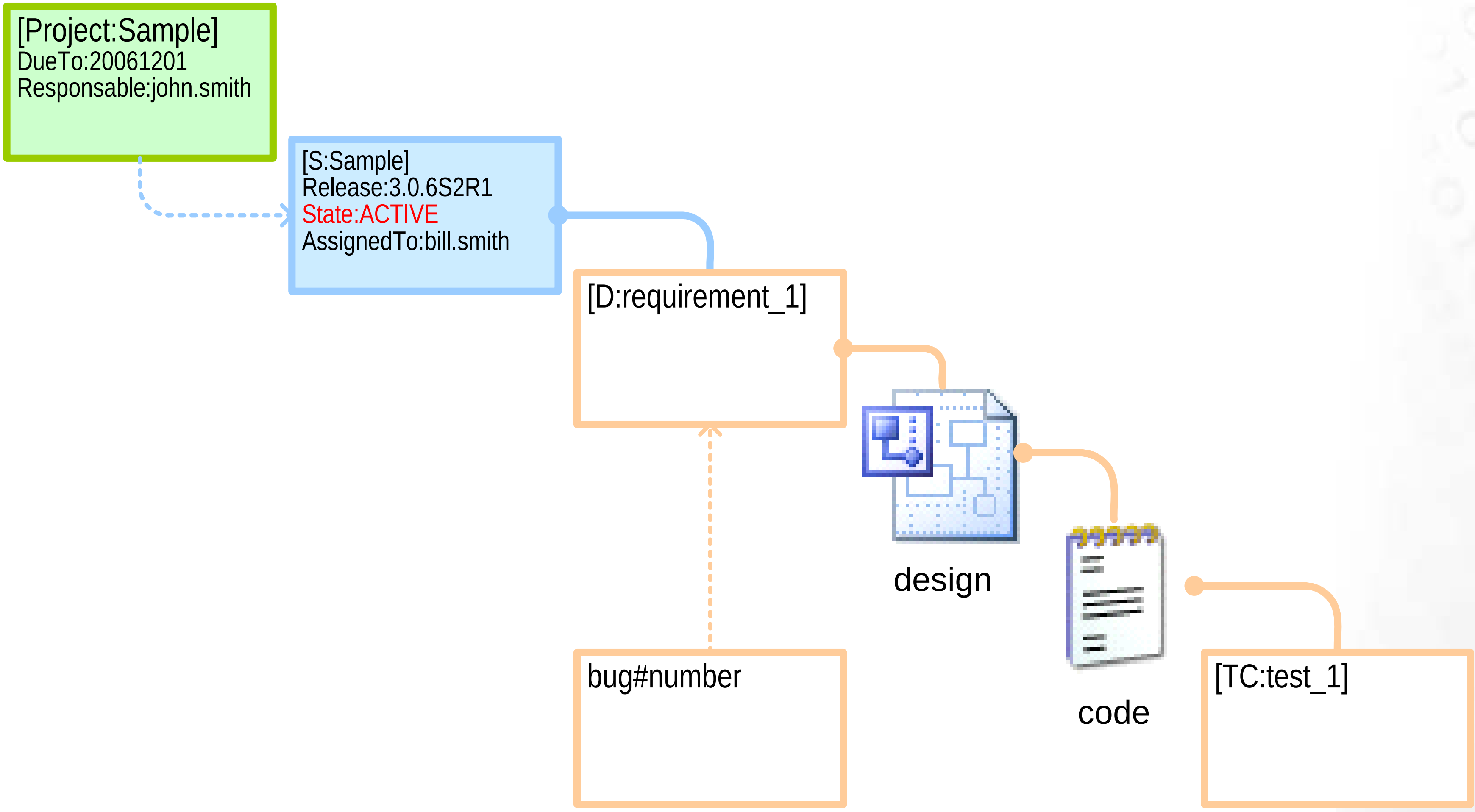
Bugzilla
[D: ] , Bug #

*Testing*

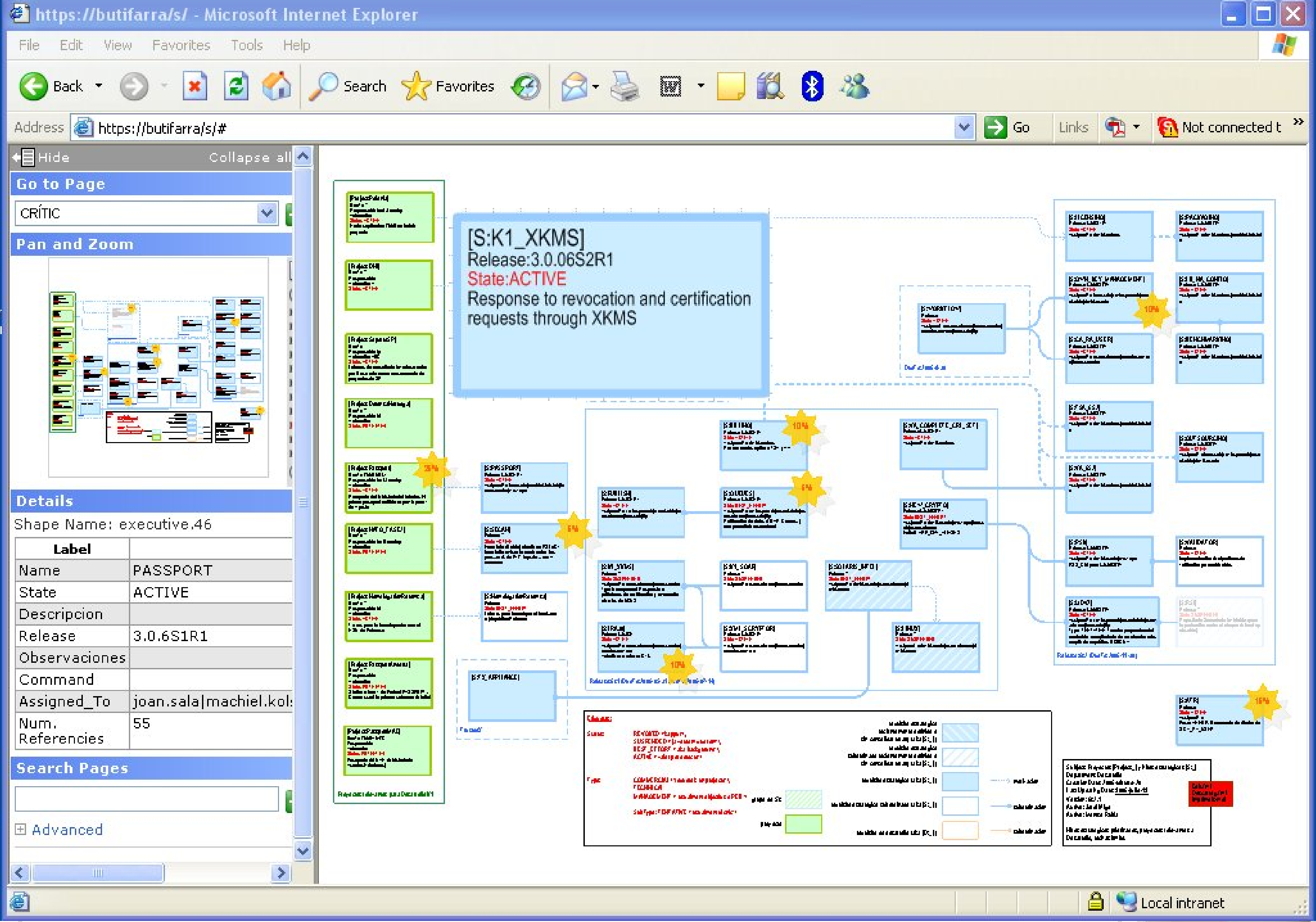
Emergency Requirements (aka Incidences)
Resp: Testing
[D: ] , Bug #

*Requirements*

# Implementation of Traceability



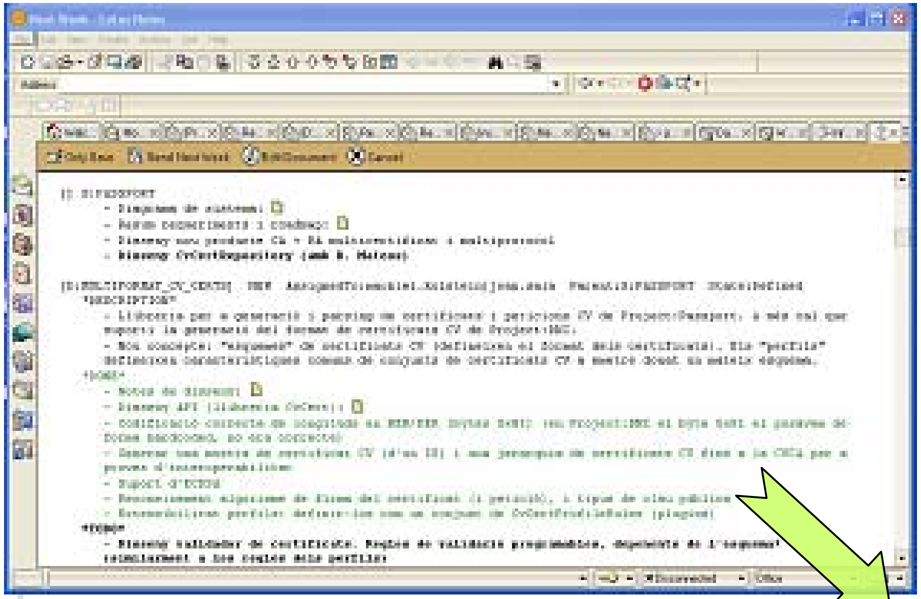
time →



Shape Name: executive.46

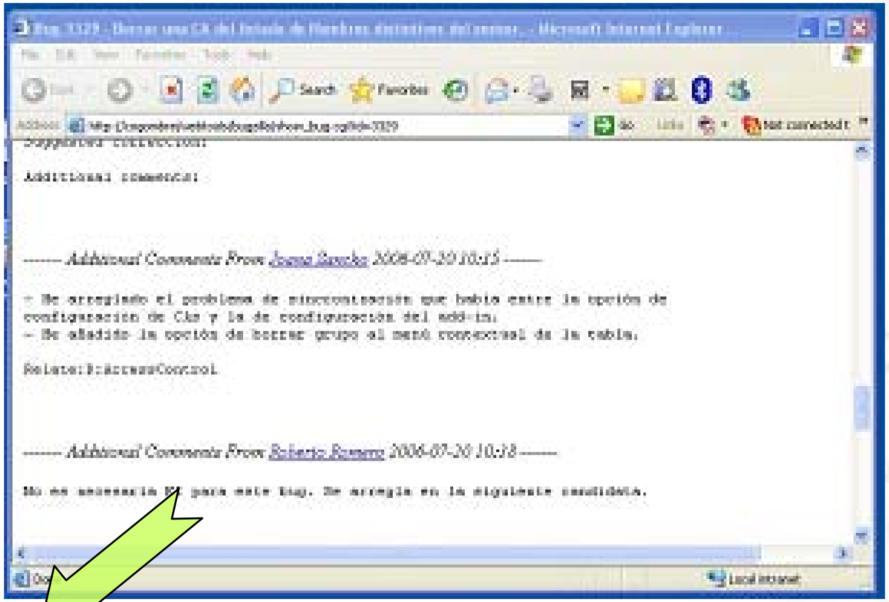
| Label | |
|---|---|
| Name | PASSPORT |
| State | ACTIVE |
| Descripcion | |
| Release | 3.0.6S1R1 |
| Observaciones | |
| Command | |
| Assigned_To | joan.sala\|machiel.kol: |
| Num. Referencies | 55 |

[S:K1_XKMS]
Release:3.0.06S2R1
State:ACTIVE
Response to revocation and certification requests through XKMS



[illegible]

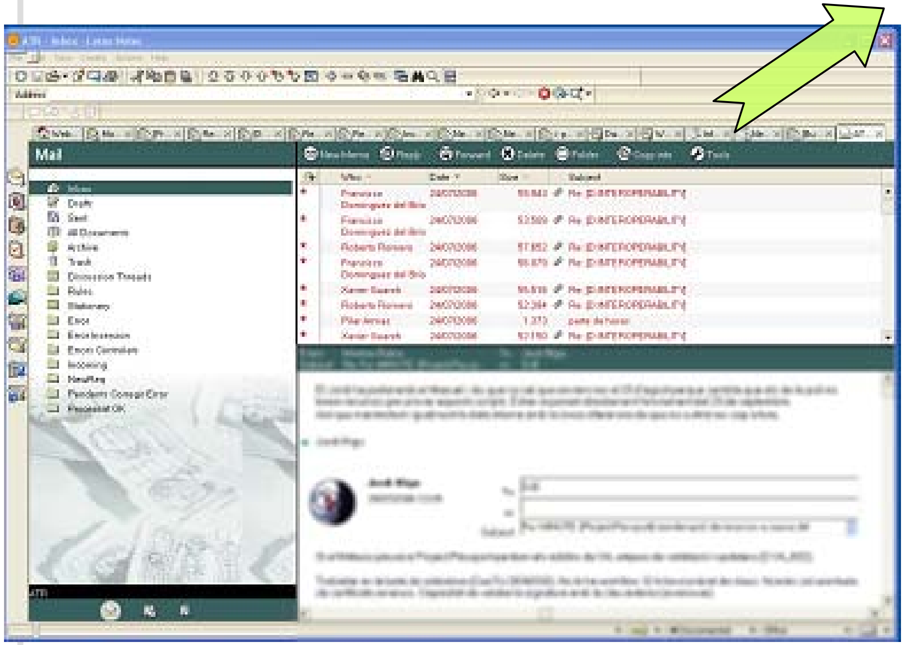
Next Week



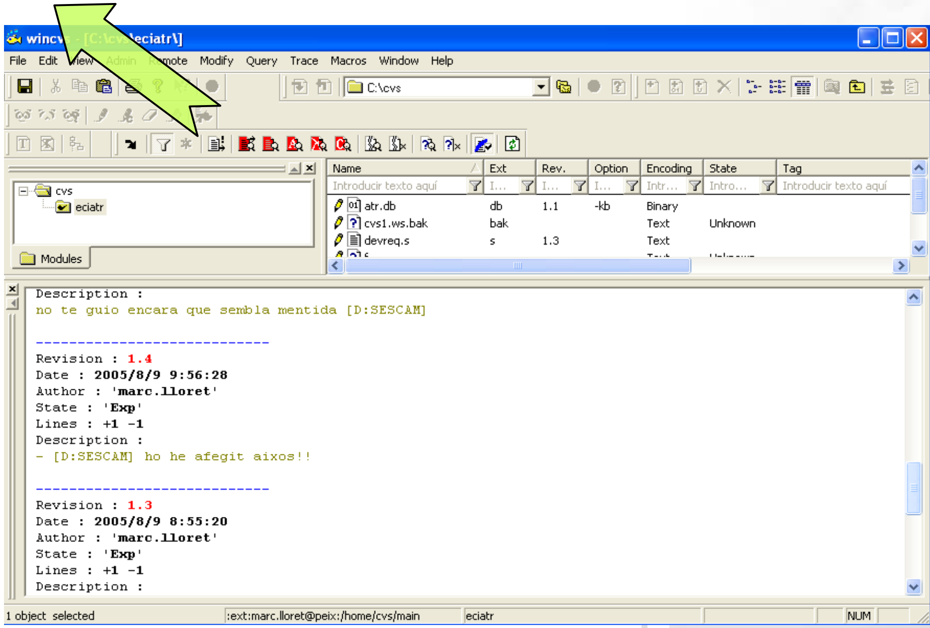
```
Additional comments:


------ Additional Comments From Juana Sancho 2006-07-20 10:15 ------

- Se arreglado el problema de sincronización que había entre la opción de
configuración de CAs y la de configuración del add-in.
- Se añadido la opción de borrar grupo al menú contextual de la tabla.

Relate:P:AccessControl


------ Additional Comments From Roberto Romero 2006-07-20 10:18 ------

No es necesaria NC para este bug. Se arregla en la siguiente candidata.
```

Bugzilla

ATR



Internal E-mails



| Name | Ext | Rev. | Option | Encoding | State | Tag |
|---|---|---|---|---|---|---|
| atr.db | db | 1.1 | -kb | Binary | | |
| cvs1.ws.bak | bak | | | Text | Unknown | |
| devreq.s | s | 1.3 | | Text | | |

```
Description :
no te guio encara que sembla mentida [D:SESCAM]

----------------------------
Revision : 1.4
Date : 2005/8/9 9:56:28
Author : 'marc.lloret'
State : 'Exp'
Lines : +1 -1
Description :
- [D:SESCAM] ho he afegit aixos!!

----------------------------
Revision : 1.3
Date : 2005/8/9 8:55:20
Author : 'marc.lloret'
State : 'Exp'
Lines : +1 -1
Description :
```

1 object selected :ext:marc.lloret@peix:/home/cvs/main eciatr NUM

CVS

# Improvements in configuration management

ACM:Config Management
ADO:Delivery & Operation

- TOE implementation representation
  - Automated versioning tools for:
    - Document Server: versions, changes, author, modification data, rôles (editors, readers, reviewers), status of the document and changes notifications, logs
    - CVS: versions, changes, author, modification data, rôles, logs
  - Better info access control
    - Documental Server: PKI
    - CVS: PKI
- List of configuration items (MPI)
  - Changes of the current MPI (Master Product Index): Implementation representation, security flaws, evaluation evidence required by the assurance components

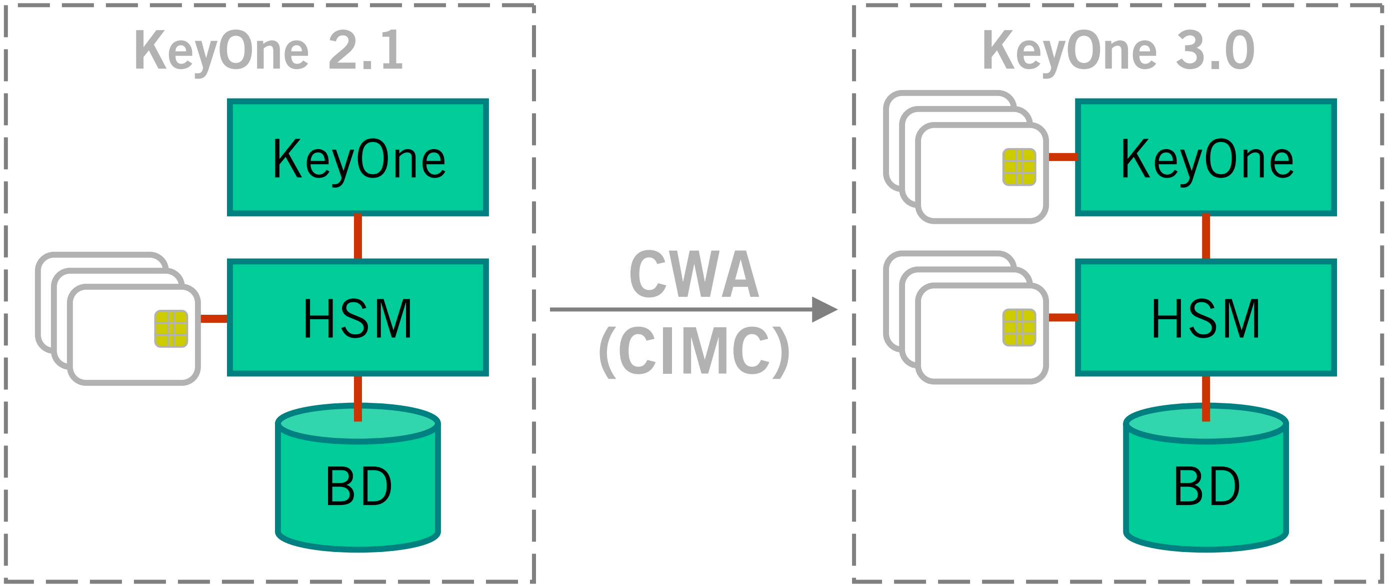
# Improvements on Life Cycle management

- Flaws are corrected and the correction issued to TOE users
  - Improvement of the management of bugs
  - New development rôles
  - Controls and new procedures in the bug resolving process
- Confidentiality and integrity of the TOE design and implementation
  - Improved access control, rôles and logs in CVS and Documental Server

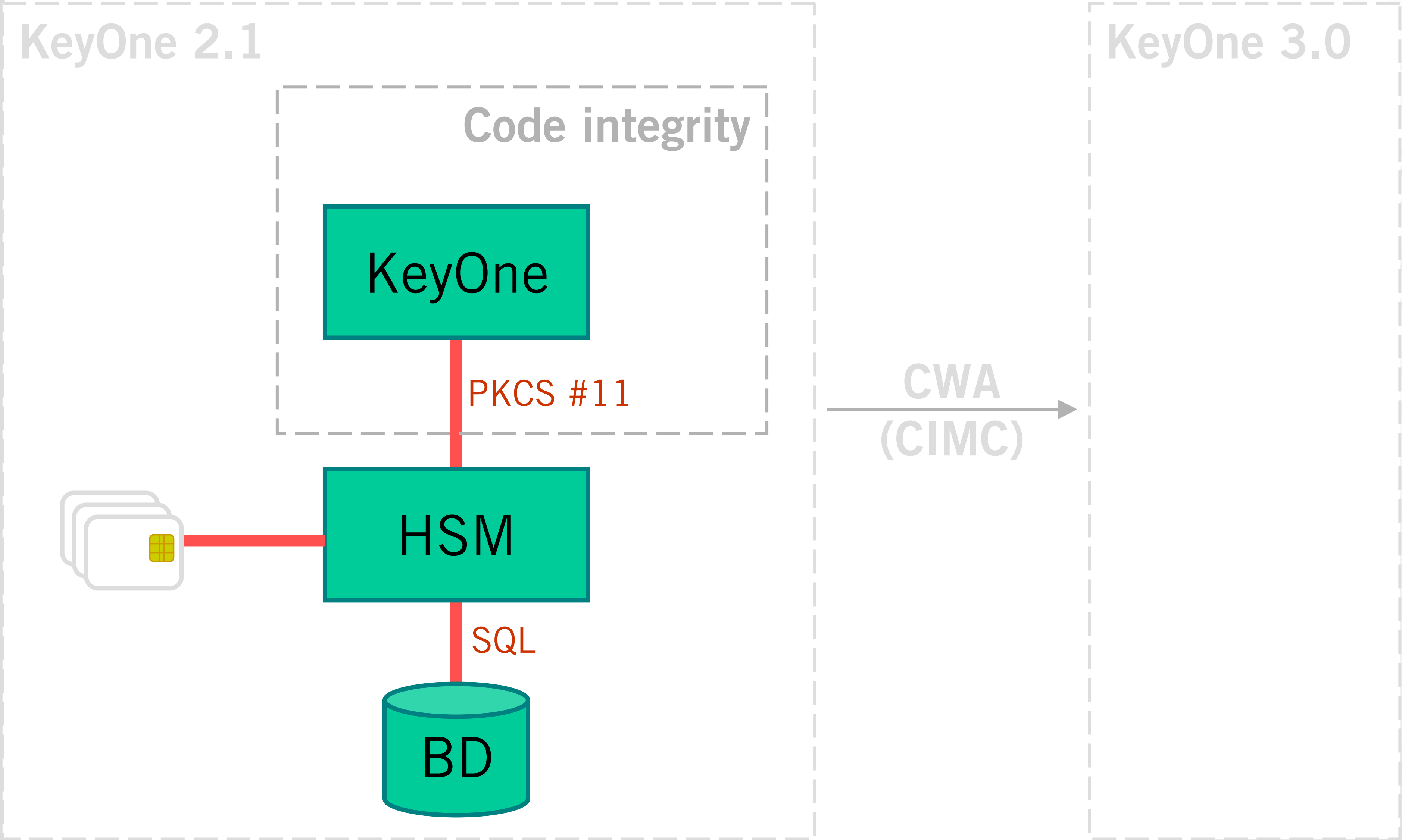
# Product Improvements

# Access Control

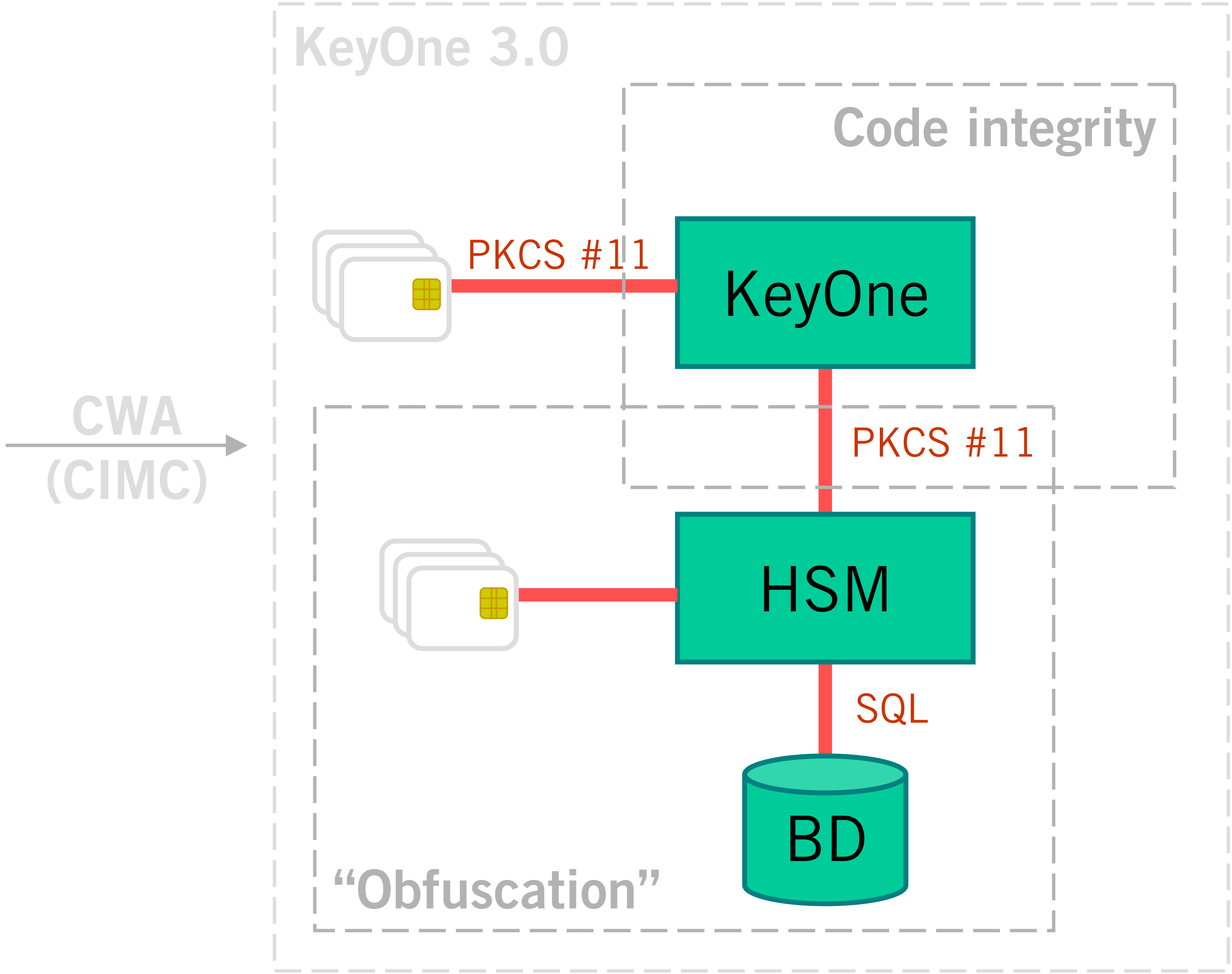
- CWA-14167-1 // CIMC-PP
  - From 2.1: *Security based on sharing the property of keys*
  - To 3.0: *Security based on access control to the system*



# Acceso Control [2.1→...]



# Access Control [...→3.0]



# Access Control

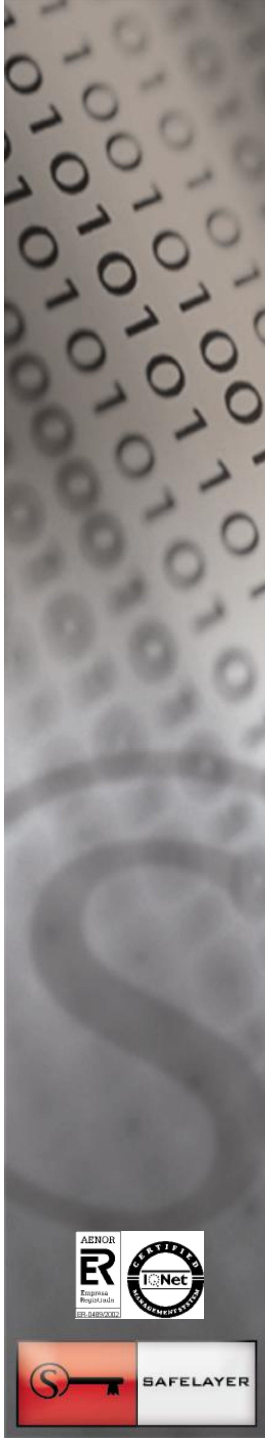
Users → Groups

Application → Actions → Rôles

- Security policy
  - Definition of rôles (actions list)
  - Incompatibilities among rôles
- Available policies
  - PP CIMC SL3 (certificate CC-EAL4+)
  - CWA-14167-1
  - Possibility of ad-hoc development

# Rôles

- PP CIMC SL3
  - Administrator
  - Officer
  - Auditor
- CWA-14167-1
  - Security Officer
  - System Administrator
  - System Operator
  - System Auditor
  - Registration Officer



# Logs Integrity

- 2.1: Full Database Integrity
  - Digital Signature (PKI)
- 3.0: Full Database Integrity
  - Digital Signature (PKI)
  - Transactional Integrity
  - Fault-tolerant integrity

JORDI ÍÑIGO GRIERA
SOFTWARE DEVELOPMENT MANAGER

SAFELAYER SECURE COMMUNICATIONS, S.A.

WWW.SAFELAYER.COM

+34 91 708 04 80
+34 93 508 80 90

©1999-2006 Safelayer Secure Communications, S.A. All the rights reserved.

This material is intellectual propriety of Safelayer Secure Communications S.A.
It is not allowed the total or partial reproduction of this material without the previous consent of Safelayer Secure Communications, S.A.