Application of ALC requirements to Open Source projects

Christophe BLAD
Open Source library for digital signature and PKI services

https://www.cesecore.eu

- Signature
- Key generation
- Certificate generation & revocation
- OCSP
- ...

Initial development by CESeCore consortium:
- PrimeKey (Sweden)
- MultiCert (Portugal)
- E-Imza (Turkey)
- Commfides (Norway)

Result of the CESeCore project sponsored by EUREKA's Eurostars Programme
Partially funded by National public authorities of each participant
Open Source PKI

http://www.primekey.se/Products/EJBCA+PKI/

Project hosted by Primekey (Sweden)

EJBCA branch 5.x based on CESeCore library
EAL+ certification

- EAL4 augmented with ALC_FLR.2, CC 3.1 r3
- Evaluation by Oppida ITSEF (France), Certification by ANSSI (France)
  - All evaluation documents in Wiki format (except the security target)
- Compliance with CIMC PP level 3
• The TOEs are mainly developed by core groups (CESECORE consortium, PrimeKey) but is open to external contributors

• All contributors can develop their own modules with the tools & techniques they want. But contributions are only source code files (not built modules)

• Main steps:
  – Discovery of new features or improvements
  – Requirements analysis by the core group
  – Analysis and design
  – Development
  – Quality assurance (code review & testing)
ALC_CMC.4, ALC_CMS.4: Configuration management

- Use of a “classical” Subversion repository managed by PrimeKey

- CC requirements:
  - Recording of modification (by default in subversion)
  - Contributions accounting

- Requires a reliable identification and authentication of contributors
  - Modification of the contributors registration procedure
  - Review of applications before granting “write” access to the repository

- Requires review of all contributions integration in an official release (systematic code review)
• Java source code

• Edition with any editor

• State-of-the-art continuous integration tools:
  – Subversion
  – MediaWiki for documentation version control
  – Atlassian JIRA for evolution and bug tracking
  – Hudson for continuous integration
  – Clover for testing code coverage assessment
  – …
• Confidentiality is not required (open source)

• Integrity is the main objective: unauthorized modification of the source code must not occur and (if any) must be detected
  – All contributions must be authenticated
  – Access to the source code repository must be strictly controlled
EJBCA was previously hosted by SourceForge

- Incapability to verify the access control system and the physical security of repository servers (~Cloud computing issues)

- The only acceptable solution:
  - Hosting in a auditable Datacenter
    - Physical security under SLA
    - Network and System administration by the project host
  - Central management of contributors accounts
    - Registration of known contributors
    - Revocation of access if needed
Contributors security (client-side)

- All contributors use their own computer
- Major risk: malware installed in their computer
  Alteration of the source code in the contributor’s computer
  Illicit alteration before commit

  ➢ All contributions must be reviewed by a trusted persons (release managers)

- Development of a contributor charter incl. security policy
  Must be signed before access granting
  • Workstation security
  • Probation period
  • Password usage
  • Incident reporting
  • Revocation or legal actions in case of misuse
• The TOE is Source code

• Delivery procedure consists in the provision of the source code to users

• Only `svn over https` distribution mode is certified
  – ssl permits the authentication of the repository
  – Generation of pre-built packages is not evaluated
Classical process
• Discovery
• Notification by email or direct contact
• Investigation
• Resolution (complete retesting due to continuous integration)
• Release

• All notifications are recorded in JIRA
Conclusions

ALC applicable but with constraints on the development conditions

- Requires a strong involvement of the project leader:
  - Strict management of the repository access
  - Strong source code review policy

- Requires the involvement of the configuration management database host
  - Security audit must be possible
Conseil & Expertise
en sécurité des systèmes d'information