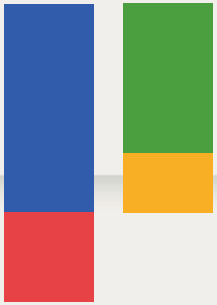


PrimeKey

Tomas Gustavsson, PKI Geek

www.primekey.com

www.ejbca.org

tomas.gustavsson@primekey.com

Assumption

- General knowledge about Common Criteria
  - Security Target, Protection Profiles, etc
- Sponsor, ***Developer***, Lab, Certification Body

A case study on certification and audit of open source security software

The Internet should be a safe place for sensitive information and communication

- EJBCA - Most downloaded PKI in the world, since 2001
- Certificate Authority Software
- >10 billion certificates issued
- Access to source code
- Open standards and Crypto agility
- Easy to get started
- **Common Criteria Certified**

EJBCA
PKI by PrimeKey

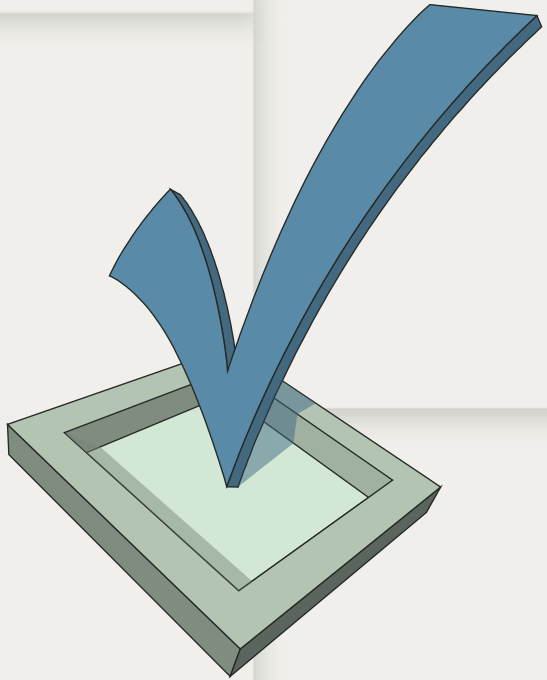
- **14 days free trail in AWS**
- **Community** (basics for free)

Relevant audits and certifications

- WebTrust/CAB Forum
- eIDAS/ETSI
- Common Criteria
- FIPS

It is used

- Public Tenders, World-wide
- Digital Signature Law
- Audits, eIDAS/ETSI & WebTrust
- Marketing & Brand



EJBCA Common Criteria Certification

- 2012
  - NIST, CIMC PP v1.0, security level 3
  - EAL 4+ (ALC_FLR.2)
  - CeSecore and EJBCA - Composite
- 2018
  - NIAP, Protection Profile for Certification Authorities, v2.1
  - No EAL
  - EJBCA

What works?

- Development process
- Protection Profile
- Audit Log
- Improving Quality
- Open is OK

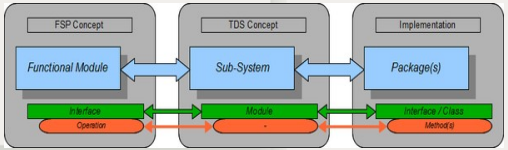
What is broken?

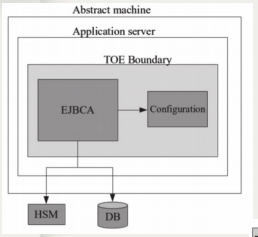
- Impact assessment
- Environment
- User understanding
- Waterfall
- Unused work
- Cost

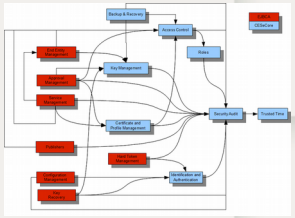
EAL CC Documentation

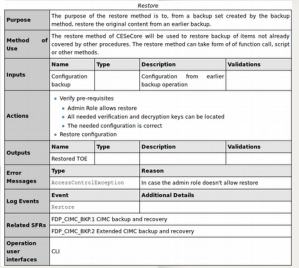
What is actually used?

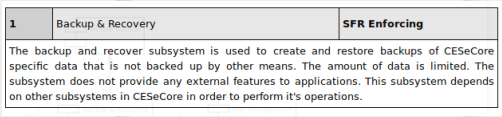
- **Security Target** (ST)
- Functional Specification (FSP)
- Design Specification (TDS)
- Implementation Representation (IMP)
- **Life Cycle Support** (ALC)
- Test Specification (ATE)
- Mapping SFR/Security Functions

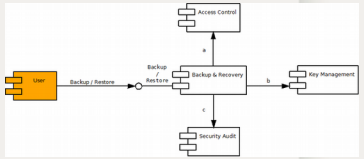


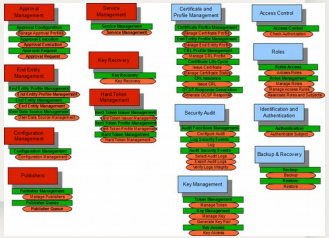












Common Criteria & EJBCA - Result

- **Open Source** works just fine
- Slightly **slower development** per issue
- **Better quality** per issue
- Well defined and tested **Audit Log**
- Improved **development process**
- Product **trustworthiness**
- Some re-usable **documentation**

EJBCA - Summary

- Open Source - LGPL
- Version 1.0, December 2001
- Modern code bas
- 6871 Jira issues May 5 2018
- ~400K lines of code (SLOC)

cPP CC Certification

Test focused vs Documentation focused

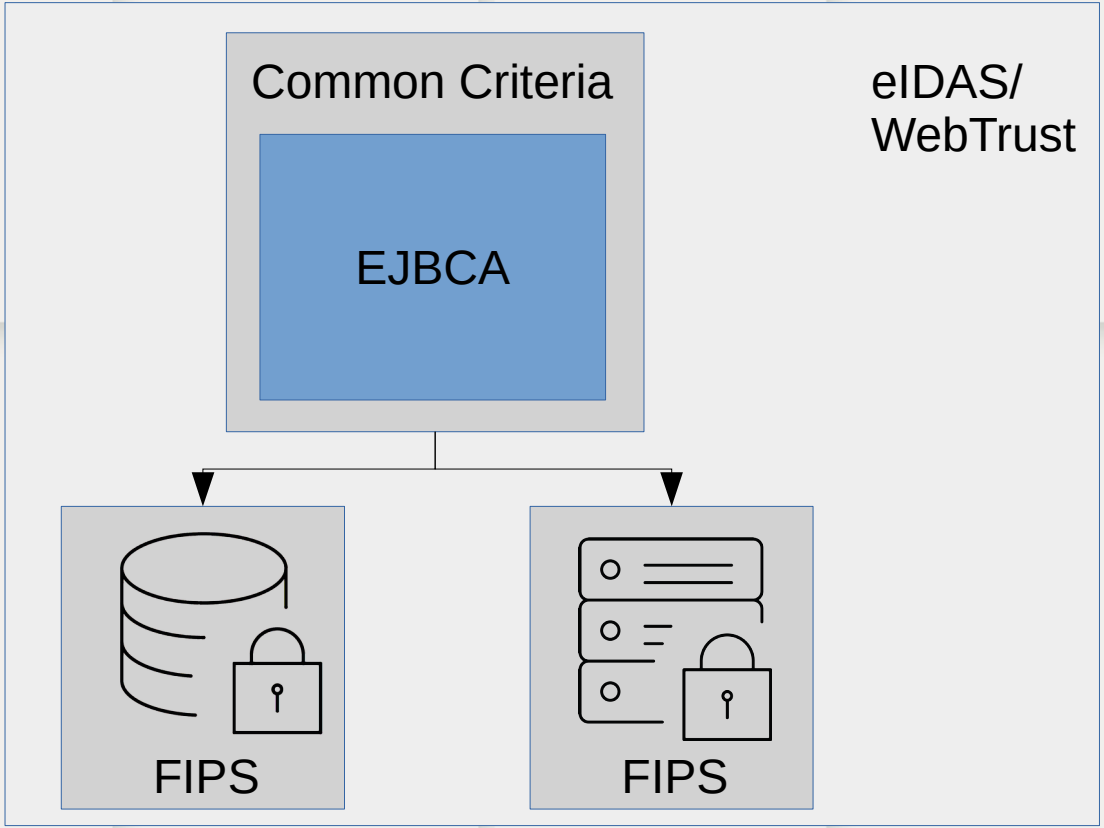
Lightweight documentation, focus on functions

- Security Target (ST)
- Test Specification (ATE)
- Mapping SFR/Security Functions

cPP CC Fears

- Development Process
- Code/Product Integrity
- Tought testing –
  ”*there are always gaps*”

Common Criteria and FIPS



BouncyCastle

Software *should* be CC, but Crypto/HSM *must* be FIPS.

- HSMs (asymmetric keys)
- Software (symmetric keys)

Using BouncyCastle gives both:

- Rapid development using non-FIPS
- Ability to switch in the FIPS provider

HSM FIPS mode issues

Recent issues related to FIPS and HSMs:

- Vendor_1 key generation. Get_MechanismInfo returns max size 4096, even when not in FIPS mode.
- Vendor_2:
  - Need to set *available mechanisms* when generating keys
  - Not possible to have key with sign+encrypt

Almost one year to fix and re-certify!

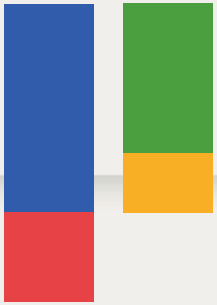
Conclusion

- In general good experience of CC
- Improvement with lightweight process
- Don’t miss out on development process and code integrity
- Remove Impact Assessment in current form
- Make it easier to understand for Users

Should do: Add a user FAQ on Common Criteria Portal

”Will the new certificate for EJBCA be based on an evaluation against TS 419261?”

”We have to use the certified version of EJBCA?”



PrimeKey

Tomas Gustavsson, CTO and PKI Geek

www.primekey.com

www.ejbca.org

tomas.gustavsson@primekey.com