SUSE® Linux Enterprise 12 Security Certifications

Common Criteria, EAL, FIPS, PCI DSS, ... What's All This About?

Matthias G. Eckermann
Senior Product Manager
SUSE Linux Enterprise
mge@suse.com

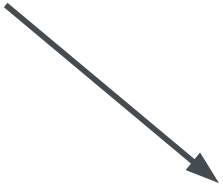
Agenda

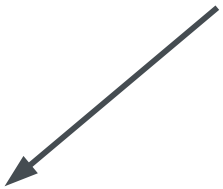
- Evaluation – Validation – Certification
- Details on Certifications and Validations
  - Common Criteria Certification
  - FIPS 140-2
  - NIST SP 800-131A
  - DISA STIG
  - BSI IT Grundschutz
  - Other Certifications and Validations
- SUSE Linux Enterprise 12

Evaluation – Validation – Certification

Evaluation – Validation – Certification

Validation	Evaluation
Compare behavior of the software / module against an existing standard or expected behaviour.	Examine claims made about a target. “Claims” do not need to be based on standards.





Certification

Details on Certifications and Validations

Common Criteria

“How can I be sure to get the security I need?”

- “Common”
  - Accepted by 26 countries all over the world
  - The certification is following a worldwide standard, thus e.g. certifications of certification body B (e.g. BSI) are accepted by certification body N (NIAP/NIST)
    → Common Criteria Recognition Arrangement (CCRA)
- Evaluation Assurance Level 4+
  - Standardized set of test cases
  - Tested at level 4, '+' is an augmentation (e.g. FLR = Flaw Remediation)
  - The highest level for a “commercial” O/S

Common Criteria (2)

- Important abbreviations in this context
  - Security Functional Requirement (SFR)
  - Security Assurance Requirement (SAR)
  - Protection Profile (PP)
  - Security Target (ST)
  - Target of Evaluation (TOE)

- More information

  https://www.niap-ccevs.org/Documents_and_Guidance/cc_docs.cfm

FIPS 140-2

- (US) Federal Information Processing Standard
  - Usage: US FedGov, FISMA, Financial Industry
  - Certificate is issued by NIST and CSEC
- FIPS 140-2 ensures that
  - Crypto algorithms/modes follow the corresponding standard
  - No obvious crypto weakness exists
  - No out dated algorithms are used
  - Key length is sufficient
- Vital
  - Definition of “cryptographic module” (CM), the functional description of the validation target
  - Self test with each invocation of CM
  - Integrity check
  - Checks performed even if module is not in FIPS-140-2 mode!
- Successor FIPS 140-4 in preparation

NIST SP 800-131A

Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths

- Hashing
  - No MD5, no SHA-1 hashing algorithms anymore
  - Use SHA-224, SHA-256, SHA-384, SHA-512
  - See also: FIPS 180-4 Secure Hash Standard (SHS)
- Other cryptography
  - HMAC: key length >= 112bits
  - Signing: DSA or RSA, key length >= 2048bits
  - Symmetric encryption: 3DES, AES
  - Public key encryption: RSA, key length >= 2048 bits
  - See also: FIPS 186-4 Digital Signature Standard (DSS)

DISA STIG

Defense Information Systems Agency (DISA)
defines
Security Technical Implementation Guide (STIG)

Configuration standard → “Hardening” or “Lockdown”

- Purpose
  - Secure Installation
  - Secure Maintenance

- Builds upon other certifications and documentation (e.g. Hardening Guide)

BSI IT Grundschutz (ITGS, Germany)

- Certification of customers' environment and processes
- Covers more than the Operating System
  → an Operating System cannot be ITGS “certified”
- Precondition
  Common Criteria (CC) Certification and
  CC documentation
- SUSE Linux Enterprise Security and Hardening Guide
- More information

  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
  https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.html
  https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.html

PCI DSS (Payment Card Industry)

- Conformance Certification for a customers environment
- Covers more than the Operating System
  → an Operating System cannot be PCI DSS “certified”

- SUSE Status:
  - Does not require changes on SUSE Linux Enterprise Server itself
  - Builds upon parameters and capabilities of SUSE Linux Enterprise
  - Main source for the certification of customers' and partners' environments according to PCI DSS:
    SUSE Linux Enterprise Security and Hardening Guide

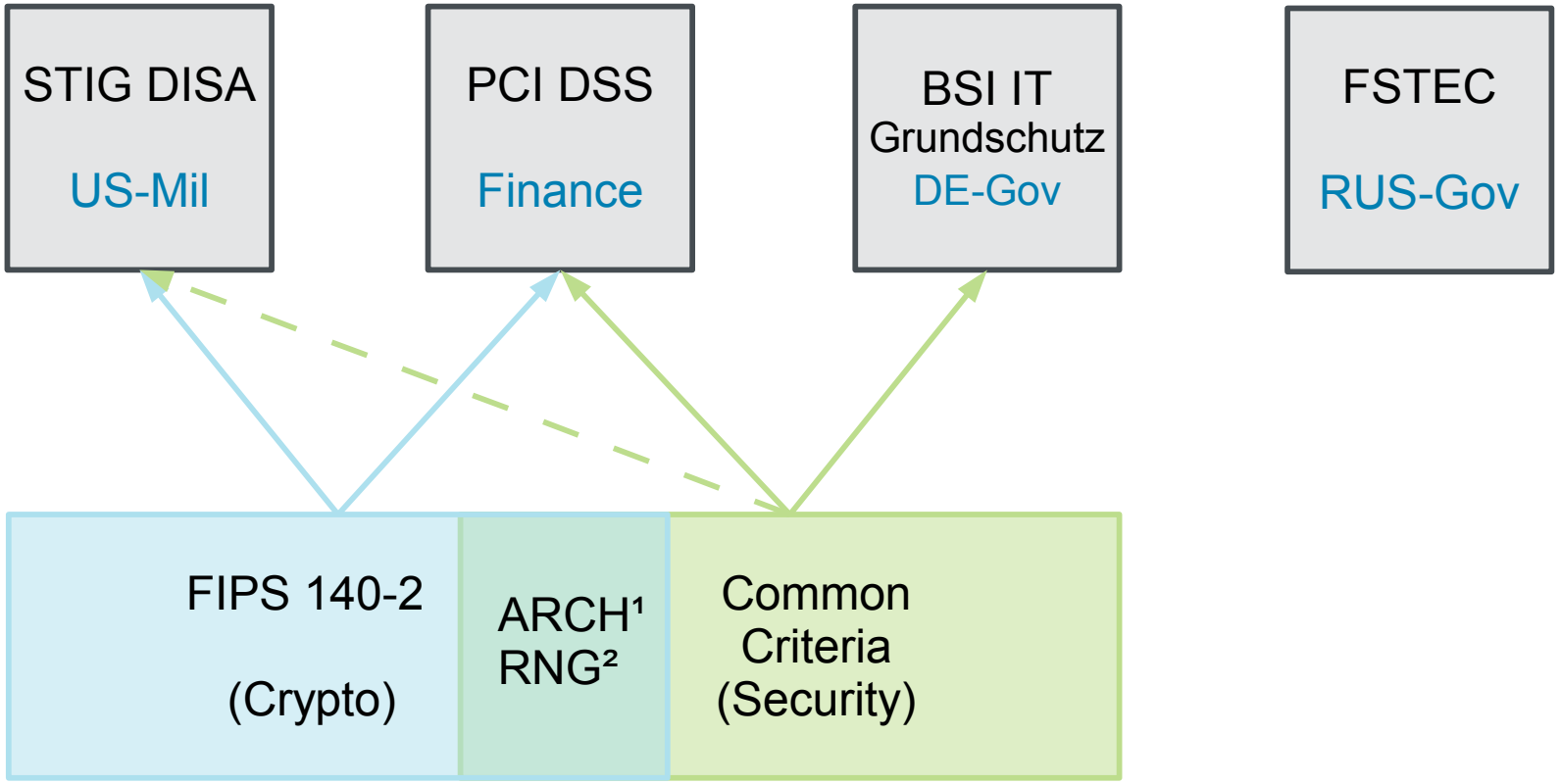
FSTEC (Russia)

- Achieved for SUSE Linux Enterprise Server 10, SUSE Linux Enterprise Server 10 SP3, SUSE Linux Enterprise Server 11 SP1
- Might need refresh according to market needs
- More information:

  http://www.globalsecurity.org/military/world/russia/fstec.htm
  http://www.fstec.ru/
- List of certified systems:

  http://www.fstec.ru/_doc/reestr_sszi/_reestr_sszi.xls

Dependencies of Certifications



[1] ARCH = Security Architecture Document
[2] RNG = Random Number Generator

SUSE Linux Enterprise 12

Common Criteria Certification

Formal Details

- Certification Body: BSI
- Evaluation Lab: atsec information security
- Product (TOE, Target of Evaluation)
  SUSE Linux Enterprise Server 12
- Protection Profile: OSPP-BSI at EAL4 with augmentation (Flaw Remediation).
- Sponsor: SUSE LLC

- Project Lead: Thomas Biege, CSSLP,
  Team Leader MaintenanceSecurity at SUSE

Common Criteria Certification (2)

TOE Configuration

- Architectures
  - x86-64
  - s390x
  - other architectures might follow
- Virtualization (x86-64)
  - KVM and Xen guest
  - KVM host configuration
- Installation via AutoYaST

FIPS 140-2

Architectures

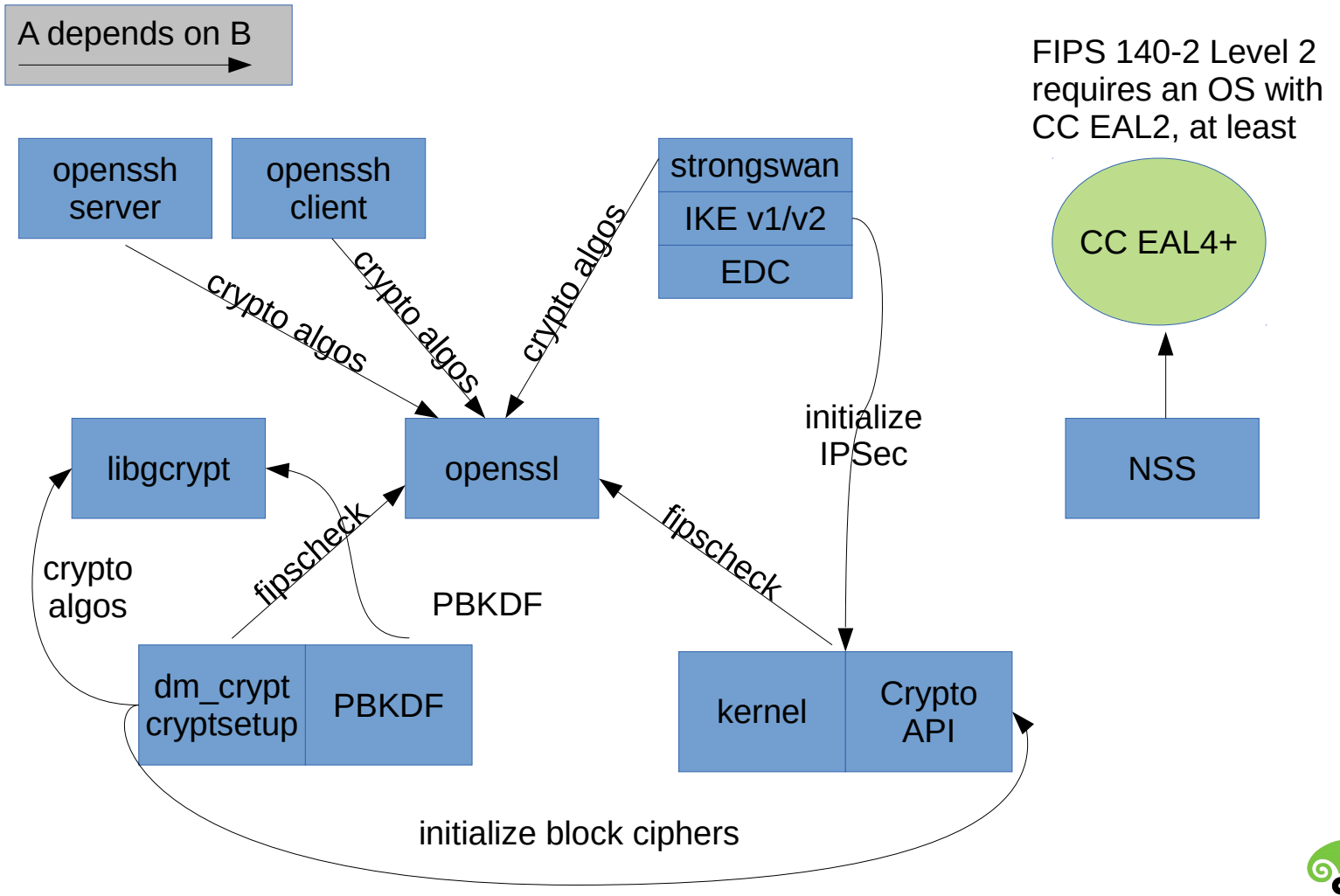
- x86-64
- other architectures might follow

Modules

1. Kernel
2. libgcrypt
3. Disk encryption
4. OpenSSL
5. OpenSSH Client
6. OpenSSH Server
7. NSS
8. StrongSWAN (IPSec)

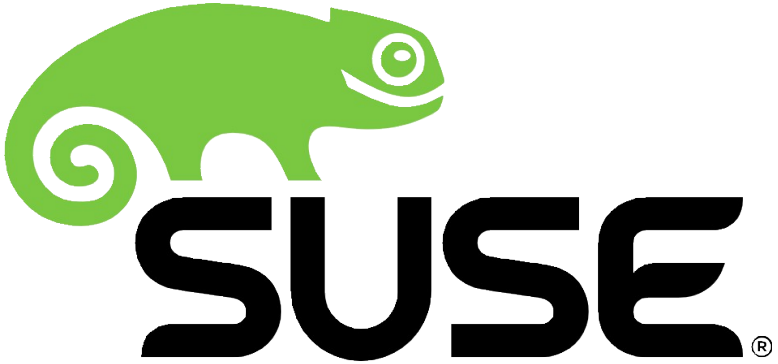
Dependencies of FIPS CSMs

in SUSE Linux Enterprise 12



Your Questions!?

Thank you.



Corporate Headquarters
Maxfeldstrasse 5
90409 Nuremberg
Germany

+49 911 740 53 0 (Worldwide)
www.suse.com

Join us on:
www.opensuse.org