Cryptographic Module Validations
Application Validations
and
Cyber Resilience Act

For relevance

Including a slide about Golang

Contents

- Intro to Cryptographic modules
- Module validation
- Golang
- Security labeling / Classifications
- Application Validation
- Cyber Resiliency Act

What is Cryptography

Cryptography protects sensitive information from disclosure and tampering

- Building blocks
  - Keyless crypto; support routines;
    - random bit generators, and hash-functions
  - Symmetric key crypto: uses same key for sealing and opening, signing and verifying
    - Ciphers, Message Authentication Codes, KDF, PRF
  - Asymmetric key crypto: uses a key pair (public, private)
    - Key agreement (DH, ECDH)
    - Key encapsulation RSA-SVE, RSA-OAEP, ML-KEM
    - Signature RSA-PKCS1v, RSA-PSS, ECDSA, ML-DSA
- Cryptographic protocols are systems built on top of these blocks
  - SSH, TLS, QUIC, IPsec, Signal, CMS, X509, ….

What are “Cryptographic Modules”

- Components that implement some cryptographic functions within their boundaries.
- Software Modules
  - Code implementing crypto with CPU/GPU
  - OpenSSL, Future Golang “crypto” module, …
- Hardware Modules: Smartcards (also payment cards), TPM, HSM, …
  - ASICs, FPGAs
- Hybrid Modules: Systems incorporating software, ASIC’s and CPUs to achieve complex cryptographic functions
  - Combination of SW and HW components in the same enclosure

What is “Validation”

NIST: *Non-validated cryptography provides no protection to the data.*

- Goal of validation is to “Ensure Security and Compliance”
  - Builds confidence in systems and products (market enabler)
  - Builds interoperable basis, avoiding vendor locks at cryptographic level
- Use of validated cryptography is often required on
  - Regulated application domains, such as healthcare and finance (compliance enabler)
  - Governmental and military applications
- Validation gives a second opinion
  - does it really work - does it have backdoors - how error resilient it is?

- The above does not mean non-validated cryptography would be bad

Cryptographic Validations

- CMVP: Cryptographic Module Validation Program; often referenced as `FIPS`
  - Requirements from FIPS 140-3 aka ISO/IEC 19790:2012
  - Driven by US NIST and the Canadian Centre for Cyber Security, also in Japan
- About 1000 active validated modules, most still following older FIPS 140-2.
- Many of these are forks or ports of subsets of OpenSSL FIPS module version 2.0, or current version 3.0
- IEC/15408 Evaluation criteria for IT security, Part 2: Security functional components (Common Criteria)
  - Used as basis in most European countries

CMVP Validation process - standards

- FIPS 140-3: Current standard, accepted from September 22, 2020,
  - Module sunset 5 years after validation
  - Revalidation is lightweight, unless requirements or implementation change.
- FIPS 140-2: Previous standard, accepted until March 31, 2022, sunset Sep 2026 – impacts new procurement

Need to use validated cryptography derives from the following standards:

- FIPS 171; Controlled Unclassified Information
- FIPS 199, FIPS 200; Minimum Security Requirements for Federal Information Systems
- National security systems and certain classified information

CMVP Validation Process - steps

- Submission: (vendor, accredited laboratory, authority) -
- Testing: (vendor and laboratory)
- Reporting: (laboratory, authority)
- Certification: (authority) based on report from laboratory.
- Major cost in terms of time, effort, and money - usually at least one calendar year
  - Some white-label modules available.
  - New platform require new certifications.

Cryptographic Module assurance levels

- Level 1:
  - Production-grade equipment and externally tested algorithms
- Level 2:
  - Includes physical tamper-evidence and role-based authentication.
- Level 3:
  - Adds physical tamper-resistance, identity-based authentication, and requires secure key management.
- Level 4:
  - Adds multi-factor authentication (MFA) and tamper-active features, resistant to fault injection.

Cryptographic Module assurance aspects

- Requirements
  - Secure design, documentation implementation, and operations.
- Interfaces between cryptographic modules and other systems.
- Roles, services, and authentication mechanisms within module.
- Logical Security of software and firmware within module.
- Physical Security measures to protect cryptographic modules from attacks.
  - Resilience against non-invasive attacks, such as side-channel attacks.
  - Mitigation of Other Attacks such as invasive mechanisms (given enough time nothing is secure)
- Self-Tests for integrity and functionality of cryptographic modules.
  - Installation, Startup, Continuous runtime
  - Ensure the secure life cycle.

Downsides on Validated Crypto

- Validated crypto != state-of-the-art crypto
  - innovations are slow to get to standards
  - PQC was “quick”, only two years from selection to standard
- Lock-down to exact version – change process is slow
  - Only original vendor is allowed to make changes
  - You are not the vendor
  - minor changes (bug fixes) via vendor-affirmation
  - major changes and features requires re-certification.

FIPS 140-3 and Golang

The Go Cryptographic Module v1.0.0 is part of Golang 1.24

- Module under test at CMVP-accredited laboratory (not certified yet)
- `crypto/internal/fips140` …
- Public API transparently uses the FIPS module when `GODEBUG=fips140=on`
- Cryptographic operations may either panic of fail on error, and will get slower (continuous self-tests)
- Will only use FIPS approved algorithms, limiting interoperability

FIPS 140-3 and Golang alternatives

- Go with BoringCrypto
  - BoringCrypto is Google minimized and certified OpenSSL
  - Not supported outside Google
  - Go with BoringCrypto is incompatible with the native FIPS 140-3 mode.

- RedHat Go Toolset
  - Uses system OpenSSL
  - Pretty much dead recently

- Microsoft build of Go
  - Uses system OpenSSL
  - Uses windows native CNG (Cryptography; Next Generation)
  - Active development – an alternative to Native FIPS provider

Microsoft fork is the way go if underlying cryptographic module is to be shared/re-used with non-Golang components

FIPS 140-3 and Golang conclusions

Applications that have no need for FIPS 140-3 compliance can

- ***and should -***

safely ignore this topic

FIPS compliancy is costly, and is not necessary a business enabler

Certified cryptography vs State-of-the-Art cryptography

- Certified Cryptography
  - Meets regulatory compliance
  - Required in certain industries, government, finance, and healthcare.
  - Proven (or validated) Security: Rigorous validation to meet standards.
  - Assurance that the cryptographic module works as intented.
- State-of-the-Art Cryptography
  - Leverage the latest advancements in research and technology.
  - Improved performance, efficiency, and security

About "Security Classifications"

- EU TOP SECRET (TRÈS SECRET UE) == COSMIC TOP SECRET
  - Exceptionally grave prejudice to the interests of document domain
- EU SECRET (SECRET UE) == SECRET
  - Seriously harm the essential interests of document domain
- EU CONFIDENTIAL (CONFIDENTIEL UE) == CONFIDENTIAL
  - Harm the essential interests of the document domain
- EU RESTRICTED (RESTREINT UE) == RESTRICTED
  - Disadvantageous to the interests document domain

Who sets the classifications

- Document producer or owner decides the classification
- May be derived from processing environment
- Often documents are “over-classified”.
  - Rules are vague, determining impact is hard
  - Material is labelled as “Secret” just in case
  - Labelling is cheap, but processing such document is expensive

- Confidential Unclassified Information
  - Usually similar classifications as on governmental – rules depend on organization and regulation
  - Personal or Financial information
  - Company secrets, trade secrets, business agreements

“Application Validations”

Several aspects are considered on Operative Validations:

- Personnel Security: individuals having proper clearances.
- Physical Security: premises used for data processing
- Information Assurance: measures to protect CIA triad.
- Industrial Security: third party compliance.
- "Application Validation" for information processing systems

“Application Validations” Examples

- (Global PCI DSS) Payment Card Industry Data Security Standard
  - Payment card and related processing elements security requirements
- (US SOX) Sarbanes-Oxley
  - Financial data and reporting integrity applications and operations
- (EU NIS2) Network and Information Security Directive
  - Critical Infrastructure cybersecurity operations
- (EU DORA) Digital Operational Resilience Act (Jan 17/2023->)
  - Cybersecurity resilience for financial sector applications and operations
- (EU CRA) Cyber Resiliency Act (Dec 11/2027->)
  - Cybersecurity for products with “digital elements”

Basics of the CRA - Cyber Resiliency Act

Ensure manufacturers and retailers maintain cybersecurity throughout the product lifecycle

In force since Dec, 2024, with main obligations apply from Dec, 2027

Applies to all products connected directly or indirectly to another device or network, with some exclusions

- Mandatory cybersecurity requirements for manufacturers and retailers.
- Third-party assessment for critical products.
- CE marking to indicate compliance.

CRA Essential Cybersecurity Requirements

- Risk based design
  - Dependency security
  - CI pipeline security
  - Use industry best practices; create secure designs; utilize Weakness Enumerations (CWE)
- Secure by default configuration
- Software and Data life cycle management
  - Ship without know vulnerabilities (CVE)
  - Do not collect unnecessary information and provide data removal
  - Prepare for security incidents - they will happen
- Continuous maintenance and obligation to report and fix
  - Know and actively monitor your dependencies; SBOM, CBOM
  - Know your users and customers – let them know – also let CSIRT and ENISA know
  - EU Declaration of Conformity

CRA Overall Impact

- CRA applies to
  - Consumer systems
  - Industrial IoT systems
  - Servers and services used by these
- CRA does not apply
  - Medical systems
  - National security systems and defense systems
  - Systems for processing classified information
  - Open-source software - but OSS user takes responsibility!

CRA - Product lifecycle

- The product is developed
  - Network connected software or device is being developed
  - Risk assessment is performed, risks are recorded.
- Conformity is assessed
  - determine how the conformity of the product must be assessed
  - some use cases require assessment by a notified body (lab) or
  - obtaining a cybersecurity certificate from CAA (use of *Validated Crypto is a plus* in this case)
  - conformity assessment must pass to comply with the Cyber Resilience Act.
- The product is placed on the market
  - An EU declaration of conformity and the necessary technical available
  - A CE marking and support period are attached to the product.
- Post-market monitoring
  - repair vulnerabilities of the product in accordance with the risk assessment.
  - report any vulnerabilities to the CSIRT and to ENISA
  - if significant changes are made reassess and update documentation

CRA Annex 3 - Important products (Class 1)

System intended for consumer use (not industrial use); **Vendor assurance; notified body**

- Identity management systems software and privileged access management software;
- Standalone and embedded browsers
- Password managers, credential management systems
- Antivirus/antimalware software
- Network management systems, configuration management tools, traffic monitoring systems
- Security information and event management (SIEM) systems, other monitoring systems.
- Update management and application configuration management systems
- Remote access/sharing software, remote management systems
- VPN systems, firewalls, routers, modems, and other components not for industrial use
- Microprocessors and Microcontrollers not for industrial use, network interface components.
- ASIC, and FPGA intended for the use by essential entities on NIS2
- Personal wearable that monitor health, or are intended for children

CRA Annex 3 - Important products (Class 2)

Requires third party validation if applied in industrial/critical infrastructure use; **notified body**

- Operating systems, hypervisors and container runtime systems
- Public key infrastructure
- Firewalls, routers, modems, and other components intended for industrial use
- Routers, modems, and switches, intended for industrial use
- General purpose microprocessors, microprocessors for integration in programmable logic controllers and secure elements
- Industrial Automation & Control Systems (IACS, SCADA), programmable logic controllers (PLC), distributed control systems (DCS), numeric controllers (CNC)
- Robot sensing and actuator components and robot controllers
- Smart meters

CRA Annex 4

Issues on critical products have wide impact throughout the society; official validation by **CAA**

- Firewalls, and intrusion detection systems (deep packet inspection)
- Tamper resistant microprocessors, microprocessors
- PKI systems, Secure elements, Hardware Security Modules (HSMs), Smartcards, readers and tokens
- Industrial Automation & Control Systems (IACS, SCADA), programmable logic controllers (PLC), distributed control systems (DCS), numeric controllers (CNC)
- Smart meters and related infrastructure

Thanks for your valuable time

BR.

Tero M

Principal Engineer Cryptography and Protocols

Approved Algorithms

- Ciphers; AES, (3DES)
- Hashes SHA-1 (limited), SHA-2 family, (SHA-3)
- Message authentication codes: CMAC, HMAC, (KMAC)
- Pubkey
  - Sign: RSA-PSS (2k+), ECDSA (256+), EDDSA 255+, ML-DSA
  - Agree & Encapsulate: FFDHE, ECDHE, EDDH X255+, ML-KEM
- KDF generic HASH, HMAC; applications (TLS,IKE,SSH)