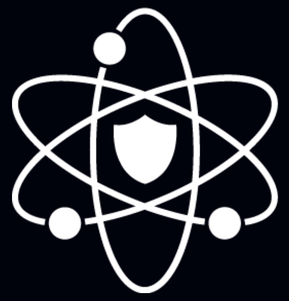


Post-Quantum
Cryptography Alliance

Advancing CBOM: Hands-On with CycloneDX v1.7 and PKI Extensions

Time	Session	Speakers
9:00 – 9:15	Welcome & Introductions *Introduction to Linux Foundation PQCA*	*Hart Montgomery,* Linux foundation
9:15-9:45	CBOM Fundamentals	
09:15- 09:30	. *Overview of CBOMs and their purpose* . *Progress of international standardization* . *Relationship between SBOMs and CBOMs*	*Mike Osborne* *IBM Research*
09:30-09:45	*An update on the CycloneDX standard, including PKI*	*Basil Hess, IBM Research*
9:45-10:30	CBOM Use Cases	
9:45-10:15	. *Telco Example (GSMA)* . *Product Use Cases*	*Lory Thorpe / Mike Osborne* *IBM Research*
10:15 - 10:30	. *Open Source Software Use Case*	*Sean Egan, SCANOSS*
10:30 - 10:50	*BREAK*	*ALL*

Time	Session	Speakers
10:30 - 10:50	*BREAK*	*ALL*
	Open-Source Tooling	
10:50 -11:20	SCANOSS Open Source . *Introduction* . *Software demonstration*	*Sean Egan* *SCANOSS*
11:20 - 12:00	Linux Foundation CBOM Toolkit . *Source Code / End Point* . *Findings Analysis* . *Integration into CI/CD pipelines*	*Mike/Basil* *IBM Research*
12:00-12:30	Discussion and Next Steps . *Other contributions* . *Contributing to the Linux Foundation* . *Alignment with SPDX*	*Hart Montgomery* Linux foundation *Audience and other vendors*

Intro Outline

1. The Linux Foundation
2. What is the Post-Quantum Cryptography Alliance?
3. Project details and how to get involved

We are behind some of the most critical projects in the world

We are a global organization committed to the free exchange of data, code, and innovation

3,000+
Universities, NGOs, Members 41 Countries

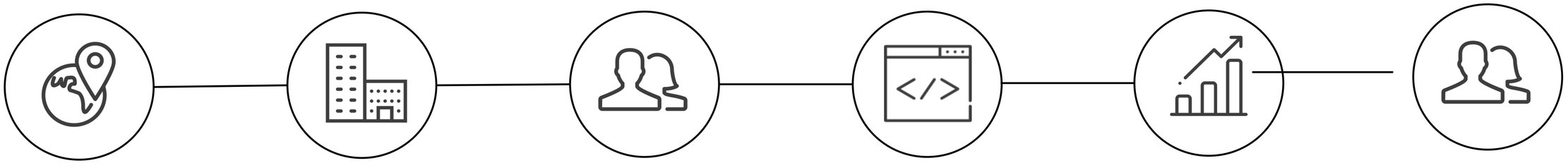
100%
of Fortune 100 Tech & Telecom

830K+
Developers Contributing Code

980+
Critical Open Source Projects

$100B
Shared Value

2M
Developers Trained



The Linux Foundation is a critical part of modern technology

Across our foundations: hundreds of projects, lines of code in the billions

110M
Lines of Code Added Weekly

14.4M
Lines of Code Removed Weekly

722,330
Technical Contributors

118,556
Ecosystem Contributors

12,925
Contributing Companies

12,899
Repositories

12.2M
Commits

1.4M
Pull Requests

2.1M
Builds Monitored

933,150
Logged Issues

11.2B
Container Downloads

236,499
Vulnerabilities Detected

4.4M
Email Messages

5.1M
Chat Messages

32,517
CLA Contributors

82,939
Event Attendees (12 months)

1100+
Project Domains

28,028
Community Meetings

Open Source Business Rationale

- Increase market opportunity
- Take market share through de facto standards
- Decrease costs
- Create new markets with entirely new technologies

...but most of you probably aren't business people.

Why Work in the Linux Foundation?

The Linux Foundation solves a **core technical collaboration problem**:

Imagine a situation where there are **multiple companies, people or organizations that want to collaborate on open source development** but **no organization is trusted by all of the others to fully own the collaboration**.

The Linux Foundation serves as a neutral home, solving this problem.

Introducing the PQCA

The Linux Foundation’s open source umbrella for post-quantum cryptography.

Mission

Post-Quantum Cryptography Alliance

To advance the adoption of post-quantum cryptography, by producing high-assurance software implementations of standardized algorithms, and supporting the continued development and standardization of new post-quantum algorithms with software for evaluation and prototyping.

Post-Quantum Cryptography Alliance

PREMIER

aws
cisco
Google
IBM
NVIDIA

GENERAL

EigenQ
Global Data Quantum
Information Security Corporation
intellect EU
Meta
QAN
QRL
QuSecure
SANDBOXAQ
THALES
TRAIL OF BITS

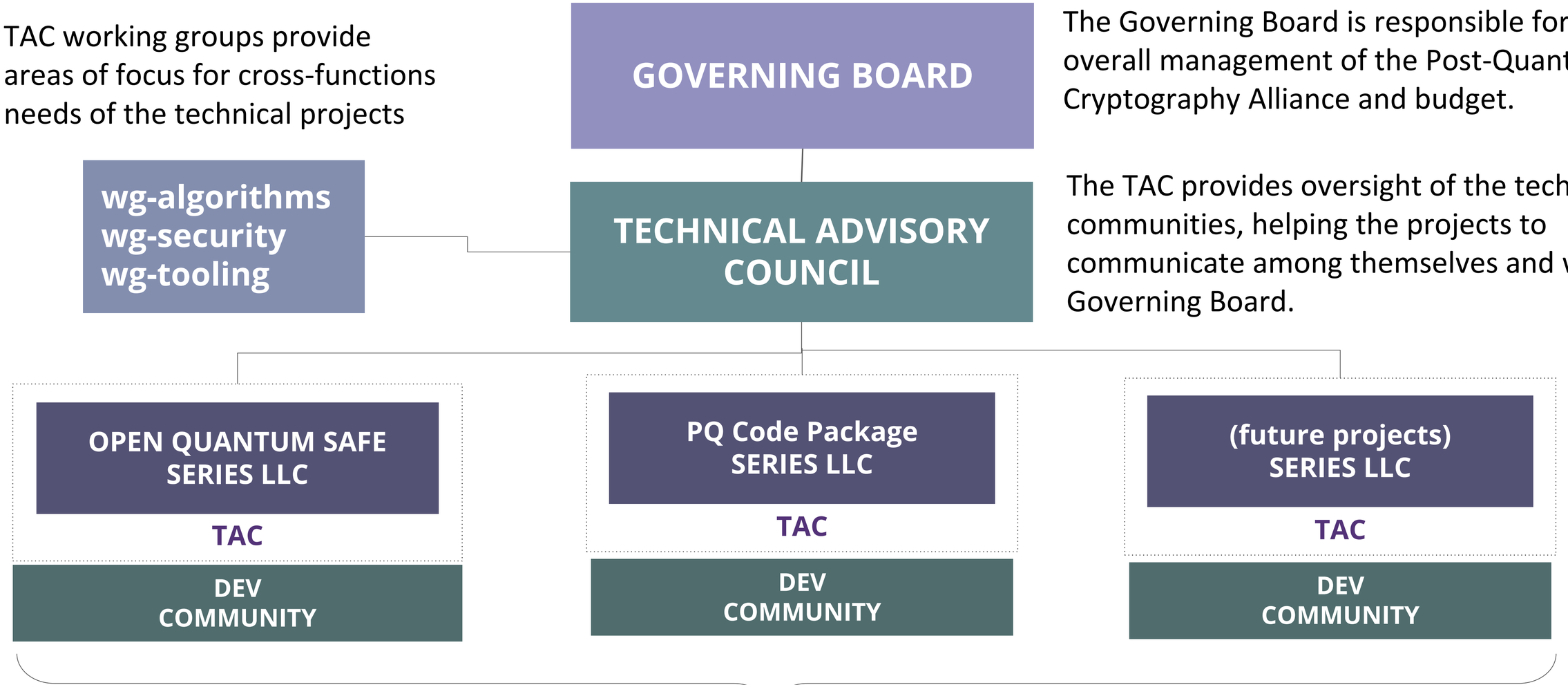
ASSOCIATE

QUANTUM VILLAGE
Rensselaer
上海期智研究院 SHANGHAI QI ZHI INSTITUTE
UNIVERSITY OF WATERLOO
GSA U.S. General Services Administration
USP
Veilid

Post-Quantum Cryptography Alliance Structure

Post-Quantum Cryptography Alliance

TAC working groups provide areas of focus for cross-functions needs of the technical projects



The Governing Board is responsible for the overall management of the Post-Quantum Cryptography Alliance and budget.

The TAC provides oversight of the technical communities, helping the projects to communicate among themselves and with the Governing Board.

Each supported technical project will have its own project governance and may contain multiple sub-projects

Projects Overview

Open Quantum Safe Project (OQS)

liboqs

Library of many PQ algorithms

- Main profile: standards-track algorithms
- Experimental profile: new algorithms, NIST signatures on-ramp etc.

OQS demos

Prototype integrations of PQ into protocols and applications to support experiments, standardization, interoperability

OQS OpenSSL 3 Provider

Integration of PQ + hybrid algorithms from liboqs into OpenSSL 3 via OpenSSL provider interface

- TLS key exchange, authentication
- X.509
- S/MIME, CMS, CMP

PQ Code Package Project (PQCP)

PQPC

High-assurance production source-code implementations of Kyber

- C, x86_64, ARMv8, …
- Rust, Go, …
- audited/certified/formally verified

Plus appropriate wrappers / providers, e.g. Kyber OpenSSL 3 provider

CBomKit

- A toolset for dealing with cryptography bill of materials.
- Not a project, but may become one soon.

Projects Overview

Technical Participation is Completely Open!

Anyone can use code, contribute to code, or contribute a new project! No membership or other commitment required!

roject (PQCP)

lib

Library of
algorithms
- Main pr
standar
algorith
- Experim
new alg
signatu
etc.

uction

yber
8, …

/form

ppers
r

CBomKit

- A toolset for dealing with cryptography bill of materials.
- Not a project, but may become one soon.

Open Quantum Safe project (OQS)

Goal: Provide an open-source software for evaluating and using post-quantum cryptography.

Main Components:

- **liboqs:** A cryptographic library in C providing implementations of standards-track post-quantum signature schemes and public key encryption / KEM schemes, plus support for testing and evaluating new experimental PQ algorithms.
- **OQS Provider:** An OpenSSL 3 provider adding post-quantum algorithms from liboqs into OpenSSL 3-based applications, providing support for post-quantum and hybrid TLS, X.509, and S/MIME/CMS.
- **OQS Demos:** Provide prototype integrations of post-quantum algorithms into protocols and applications, to support experiments and interoperability by early adopters and assist in protocol-level standardization.

Github: https://github.com/open-quantum-safe

Website: https://openquantumsafe.org/

TSC Page: https://github.com/open-quantum-safe/tsc/blob/main/README.md#members

PQ Code Package (PQCP)

Goal: Develop and maintain high-assurance, production implementations of Kyber for a variety of target architectures (ARMv7, ARMv8, x86_64, ...) and languages (C, Rust, Go, ...), distributed primarily as source code. Aim for implementations to be audited and/or formally verified.

Project Track: Production

Intended Audience: Implementers of cryptographic libraries and tools that need to add Kyber to their software as source code. The Kyber code package should be organized in a way that allows for easy tracking of changes and integration into software development lifecycles.

Starting Points:

- Portable C (PQCrystals, PQClean, eventually HACL*)
- x86_64 AVX2 (libjade / Jasmin)
- x86_64 non-AVX2 (libjade / Jasmin)
- ARM64 (neon-ntt?)
- ARM32 (pqm4, eventually libjade)
- Rust
- Go
- OpenSSL 3 provider for Kyber

Github: https://github.com/pq-code-package

Website: https://docs.pqcodepackage.org/main/

TSC Page: https://github.com/pq-code-package/tsc/blob/main/README.md

CBomKit

CBOMkit is a toolset for dealing with Cryptography Bill of Materials (CBOM). CBOMkit includes a

Main Components:

- CBOM Generation (CBOMkit-hyperion, CBOMkit-theia): Generate CBOMs from source code by scanning private and public git repositories to find the used cryptography.
- CBOM Viewer (CBOMkit-coeus): Visualize a generated or uploaded CBOM and access comprehensive statistics.
- CBOM Compliance Check: Evaluate CBOMs created or uploaded against specified compliance policies and receive detailed compliance status reports.
- CBOM Database: Collect and store CBOMs into the database and expose this data through a RESTful API.

Github: https://github.com/PQCA/cbomkit

Note: not officially a full project.

Topic of Today's Workshop!

Post-Quantum
Cryptography Alliance

PKIC – CBOM Workshop

Agenda

1. CBOM Fundaments
2. CBOM Use Cases
3. Open Source Tooling
4. Discussion Next Steps

Introduction

CBOM Fundamentals

Cryptographic Governance

Cryptographic governance refers to the framework and practices an organization implements to effectively manage and control its cryptographic assets and operations.

~~Cryptographic~~ Governance
Data

~~Cryptographic~~ Governance Data

Data Governance is the practice of controlling and protecting information in an organization.

Cryptographic Governance

What we have

- ✓ Regulations and Polices
- ✓ Standards (AES, DSA, ECC, ...)
- ✓ Key Management (Systems)
- ✓ Certificate Lifecycle Management (CLM)

What we miss

- ❑ Standard for collecting and sharing cryptographic information
- ❑ Automated Compliance Checks
- ❑ Cryptographic Inventory
- ❑ Cryptographic Agility

Standard for collecting cryptographic information

Standard for collecting cryptographic information

CBOM

Justification

There has been no standard for clearly reporting cryptographic information

Example: NIST SP 800-52 R EV . 2 Interpreting Cipher Suite Names

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

Cryptography is complex, without a common standard, **Inventory Building**, **Governance** and **Automation** are difficult and error prone

Crypto Formats

Domain / Protocol	Format Type	Example	Encoding Type
PKI / X.509	OID	1.2.840.113549.1.1.11	ASN.1 numeric
TLS	IANA Suite	TLS_AES_256_GCM_SHA384	Text / Codepoint
SSH	String	curve25519-sha256	UTF-8 text
JOSE / JWA	JSON Token	"RS256"	Text
COSE	Integer	-8 (EdDSA)	CBOR int
IPsec	Transform ID	20 (ENCR_AES_GCM_16)	Integer
XMLDSig	URI	http://www.w3.org/2001/04/xmlenc#aes128-cbc	Text URI
OpenSSL	NID / Short Name	sha256WithRSAEncryption	Numeric / Text
FIPS	Label	"CTR_DRBG (AES-256)"	Text

TLS Cipher-suites

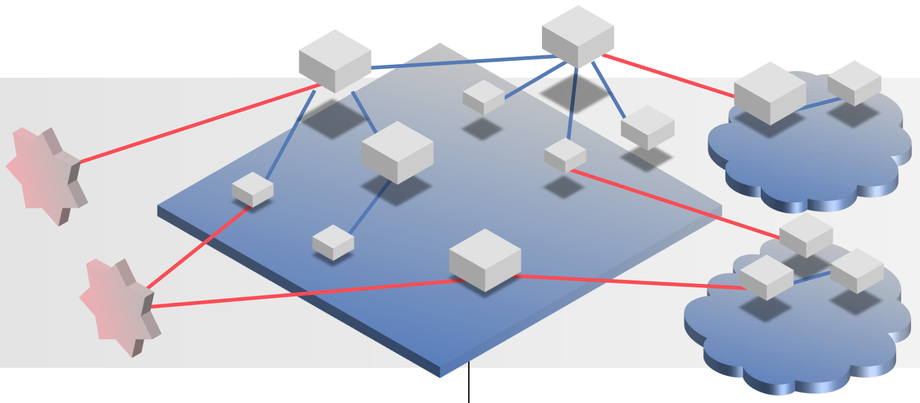
Library / Stack	Cipher Definition Style	Example	Based On
OpenSSL / Python	Colon-separated string / filters	ECDHE-RSA-AES256-GCM-SHA384	OpenSSL
Java (JSSE)	IANA-style underscore names	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	IANA
Go	Constants (typed uint16)	tls.TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	IANA
GnuTLS	Priority strings + modifiers	"NORMAL:+AES-256-GCM:+AEAD"	GnuTLS
Mozilla NSS	Prefixed enable/disable flags	:+TLS_AES_256_GCM_SHA384	NSS

Most cryptography is in vendor software and hardware

Reporting vs Scanning

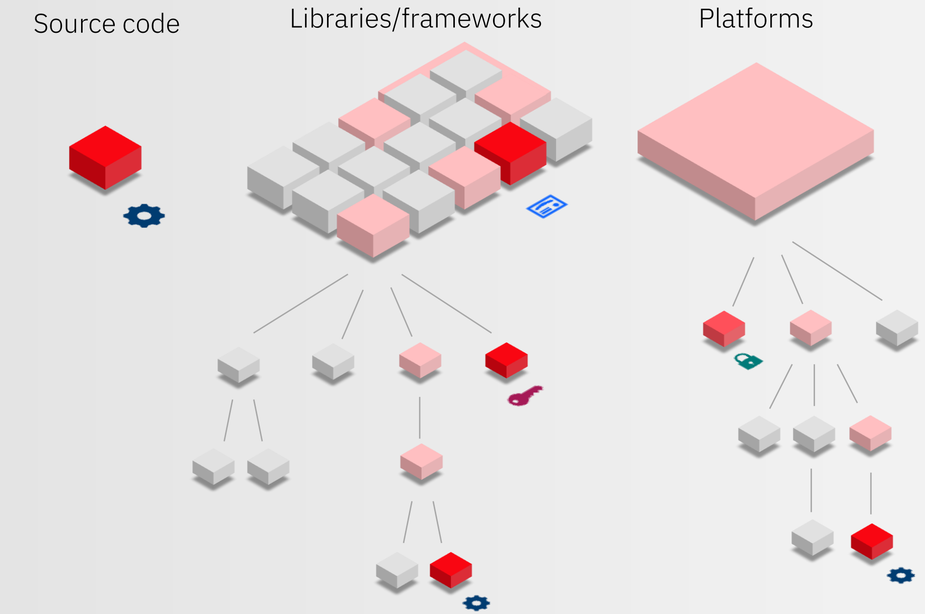
IT Enterprise context

IT Assets



By scanning the network, key stores, etc.

Applications & Services



By scanning code …

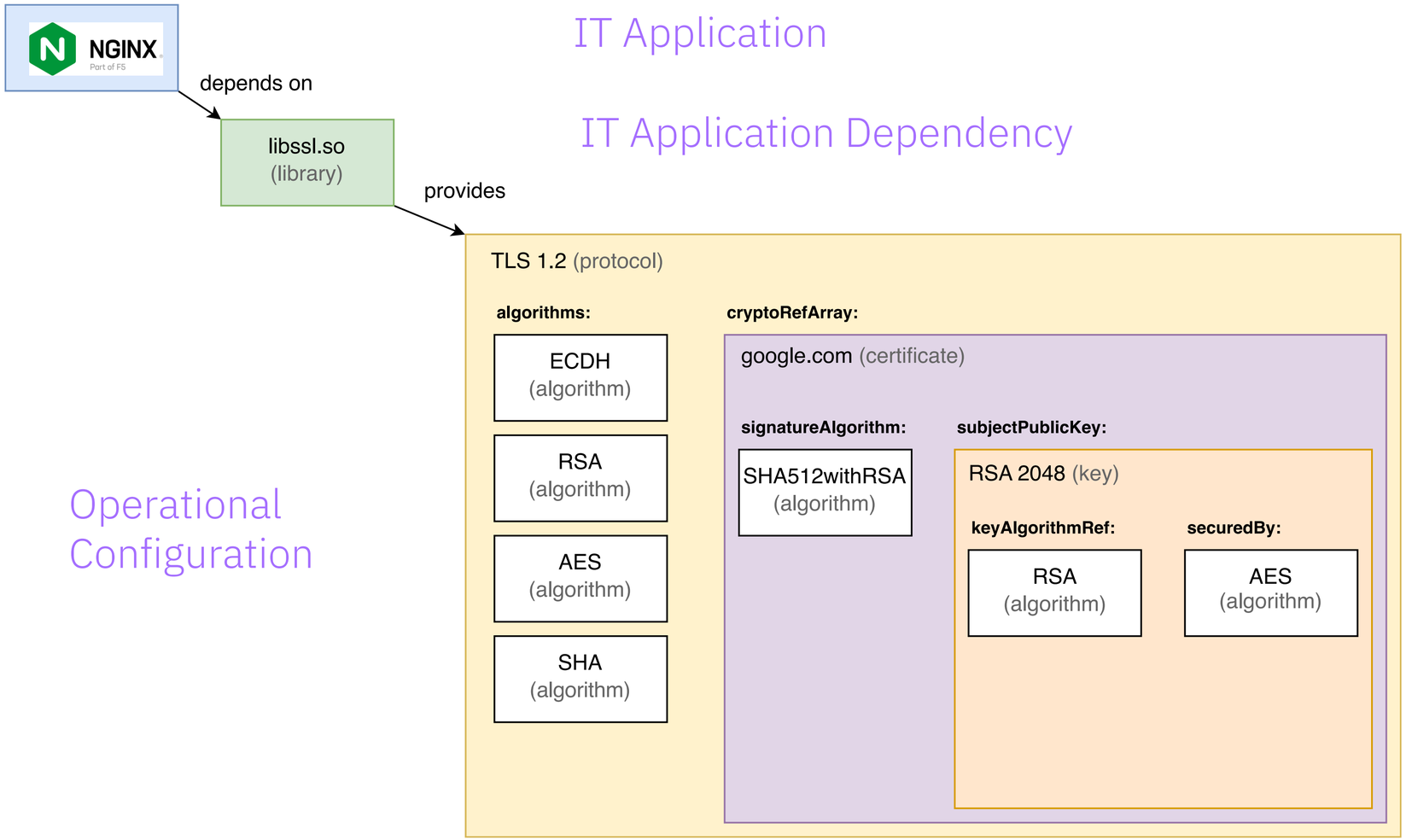
But: No organization has access to all the source code in use.

So it needs to be reported

CBOMS Need Context

We want to clearly report the crypto context

IT component context

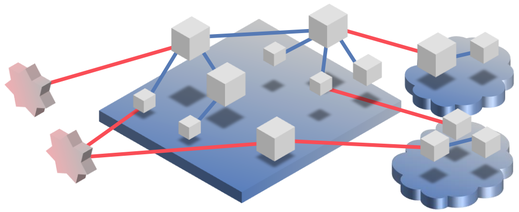


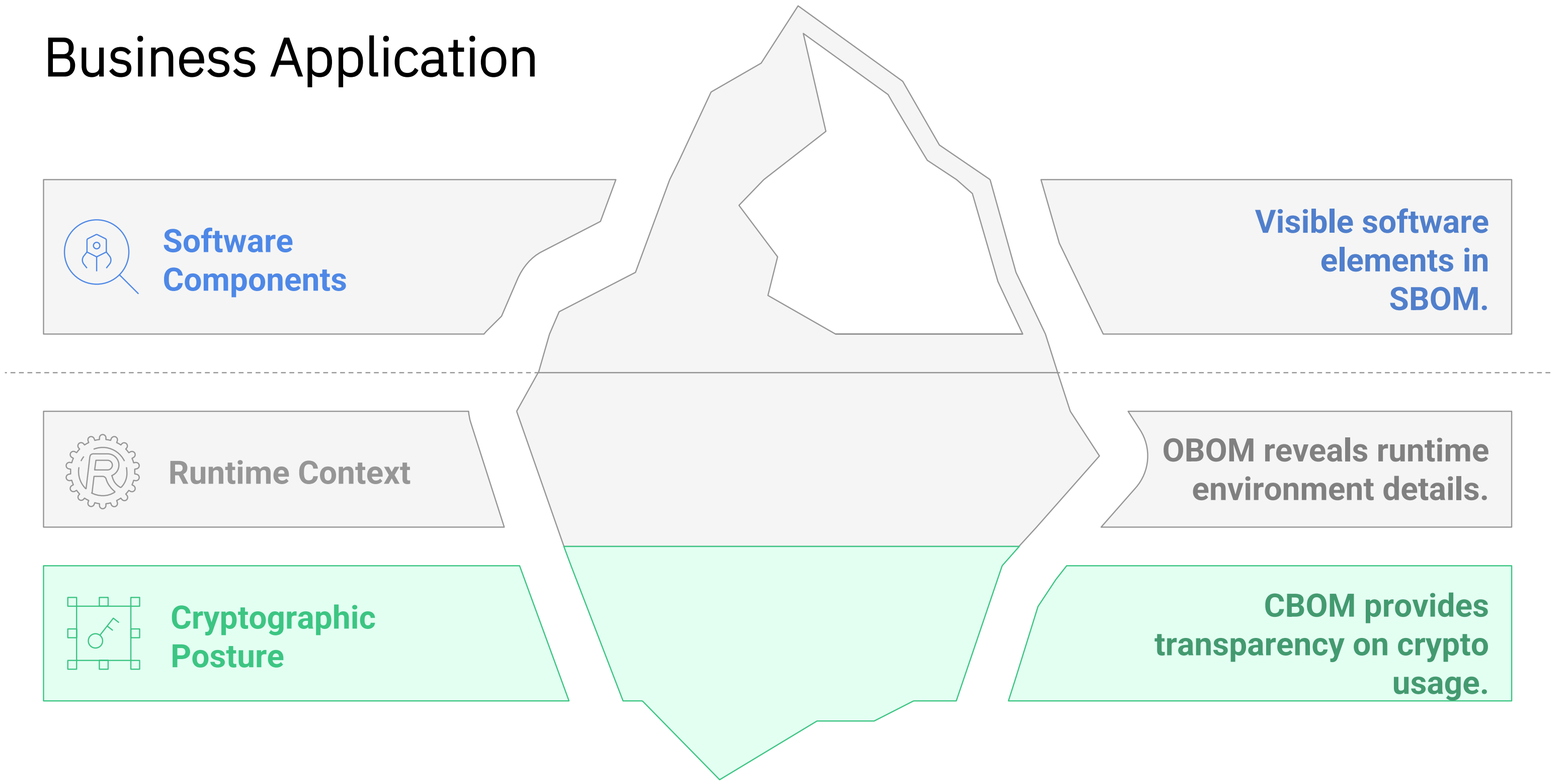
There are <u>many</u> ways to build and configure cryptography in applications:
Examples: NGINX

- Build-time linking (OpenSSL/BoringSSL/FIPS)
- TLS directives (ssl_*, ssl_protocols, ssl_ciphers)
- Certificate & key handling (files, HSM, PKCS#11)
- Session and ticket management
- Stream and HTTP modules
- Scripting (Lua/njs) for app-level cryptography
- System or FIPS crypto policies

We want to clearly report the crypto context

IT Enterprise context





We want to clearly understand the Enterprise context

Enterprise context

Business Assets

Determine criticality/risk

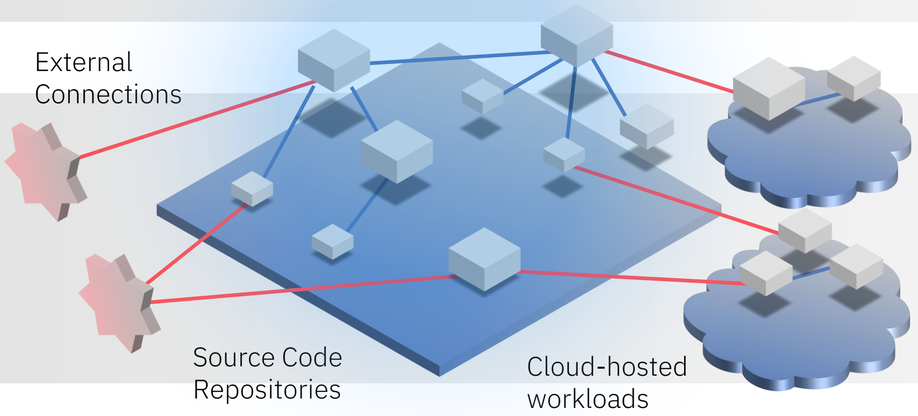
- Assets
- Data
- Processes

Impact is at the business level

Dependencies & Data Flows

Identify affected components

- Dependencies
- Exposure
- Constraints



Its tricky modelling risk through ICT dependencies?

Cryptographic Artifacts

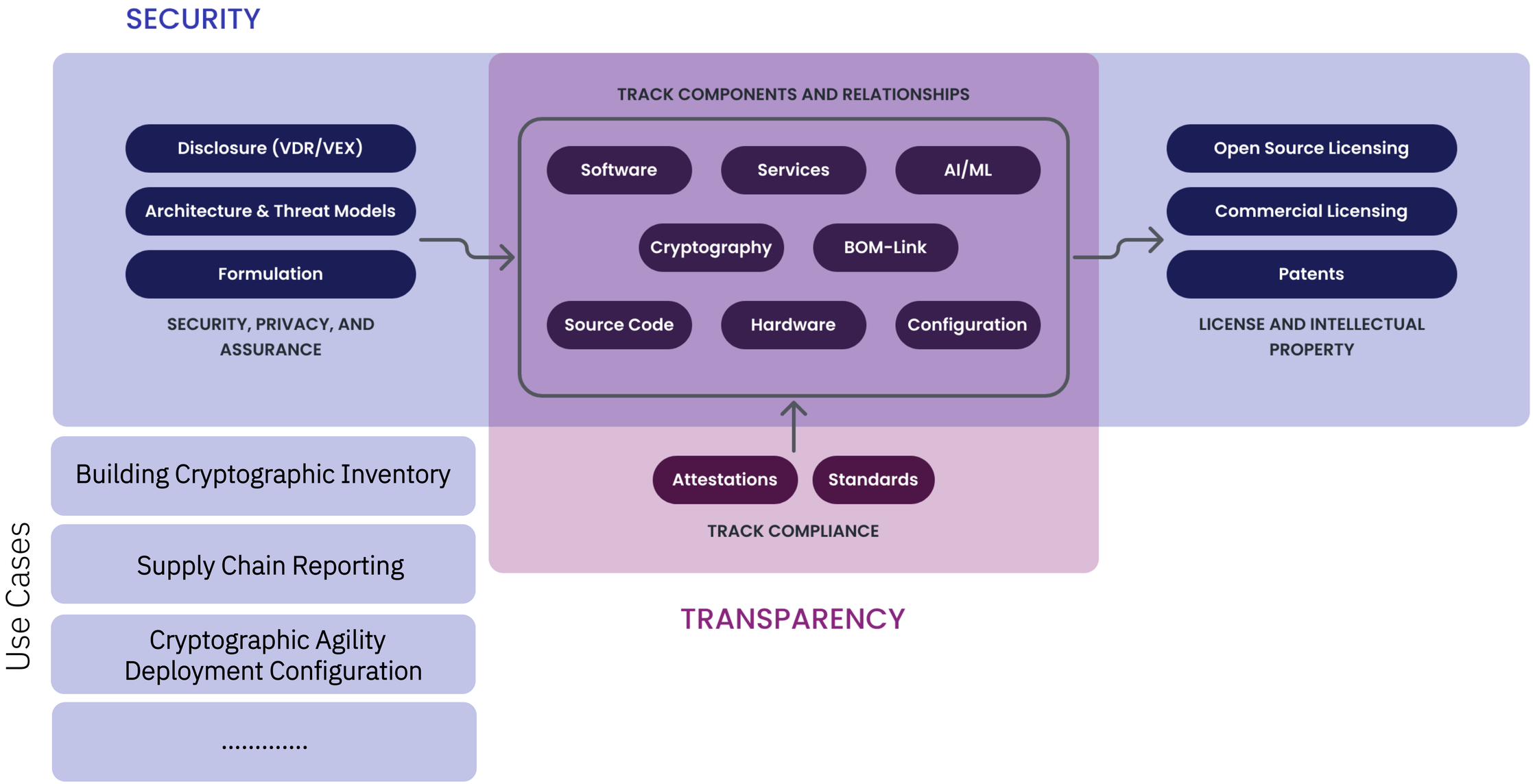
Manage and track Posture

- Cryptographic artifacts
- Asset/vendor readiness
- Hybrid readiness

Cryptographic Artifacts (algorithms, protocols, certificates, keys, etc.)

Quantum threat is to cryptography

Different Use Cases need different data


SECURITY
TRACK COMPONENTS AND RELATIONSHIPS
Disclosure (VDR/VEX)
Architecture & Threat Models
Formulation
SECURITY, PRIVACY, AND ASSURANCE
Software
Services
AI/ML
Cryptography
BOM-Link
Source Code
Hardware
Configuration
Open Source Licensing
Commercial Licensing
Patents
LICENSE AND INTELLECTUAL PROPERTY
Attestations
Standards
TRACK COMPLIANCE
TRANSPARENCY
Use Cases
Building Cryptographic Inventory
Supply Chain Reporting
Cryptographic Agility Deployment Configuration
.....

CBOM Use Cases