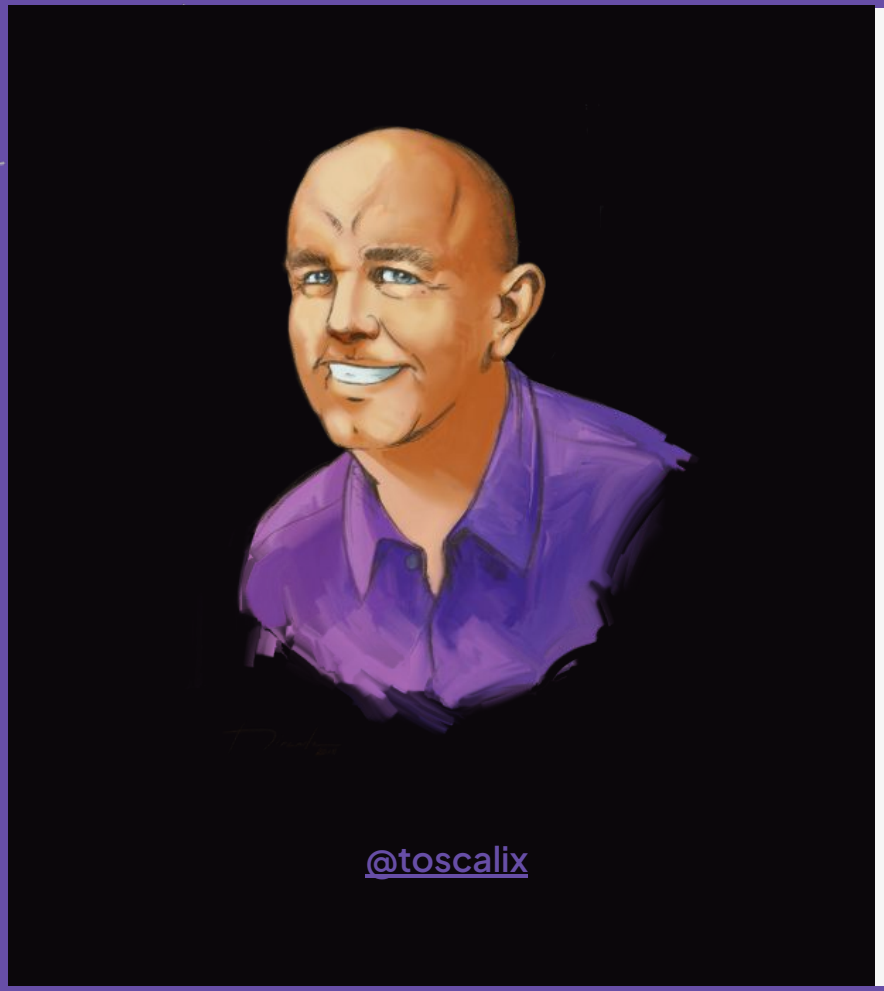
SPDX Crypto Algorithms List

State of the art

SPDX tech-team Meeting
2026-02-17

Agustín Benito Bethencourt
Independent Consultant
Sponsored by STF



@toscalix

Agustín Benito Bethencourt

- FLOSS, Business Intelligence, Continuous Delivery, agility and remote work advocate
- SPDX interim Cryptography Group coordinator. Sponsored by STF
- Independent consultant helping companies in two ways:
  - Applying business intelligence to the production of SW defined products to increase delivery performance, partnering with Bitergia: Delivery Performance Analytics
  - Increasing their organizational performance by becoming good open source citizens: Software Transparency Foundation (STF)...
- More about Agustín:
  - Background: MBition (Mercedes Benz), SUSE, Eclipse Foundation, Linaro, Codethink...
  - Blog - About - Talks - Contact

SPDX License List

- SPDX License List is an essential component of SPDX specifications
- It enables "efficient and reliable identification of such licenses and exceptions"
- Multiformat list managed through git repos
- A unique (machine & human)-readable identifier for every Open Source license
- By adding those id to your source code, licenses can be detected, identified, declared and introduced in SBOMs, so audited.

SPDX Crypto Algorithms List

Modeled after the SPDX License List, this list provides a shared and unambiguous vocabulary for identifying and referencing cryptographic algorithms in Bills of Materials (BOM), SPDX documents, and related tooling.

The SPDX Cryptographic Algorithm List includes a standardized short identifier, the full name, OID, cryptoClass, and references.

The purpose of the SPDX Cryptographic Algorithm List is to enable efficient and reliable identification of Cryptographic Algorithms in an SPDX document, in source files or elsewhere.

Why a SPDX Crypto Algorithms List?

- **Collecting and structuring** *all used* crypto algorithms with open (source) implementations has, by itself, value
- Standardizing how crypto algorithms are **identified** and **declared** will enable developers, projects and organizations to add those to SBOMs…
- … turning **detection** and **auditing** crypto algorithms within any SW composition into an achievable task.
- This List expands collaboration opportunities for SPDX in SCA, security auditing, static analysis, export control, quantum safety readiness… markets

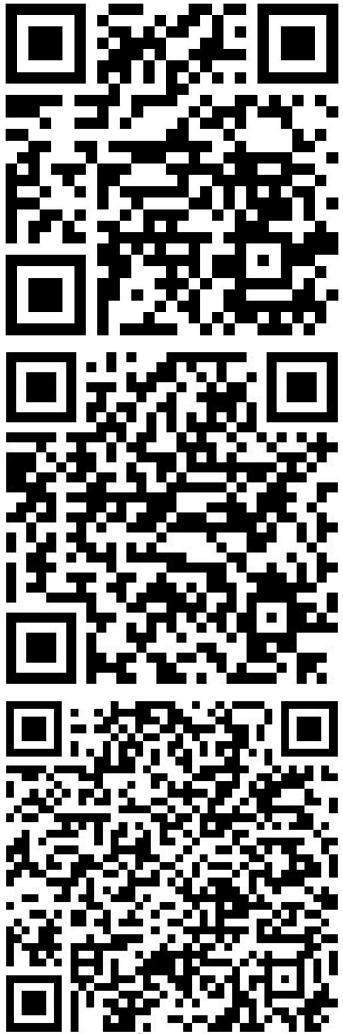
SPDX Crypto Algorithms List Group

The SPDX Cryptographic Algorithms List is developed and maintained by the SPDX Cryptography Group who…

- …started this effort in May 2025
- …supports the broader SPDX Project by:
  - Aligning the list's format and structure with current and future SPDX specifications.
  - Promoting the adoption of the list and its identifiers across the software ecosystem.
  - Fostering collaboration and interoperability with standards bodies and open source communities.

SPDX Crypto Algorithms List today

- A list of +120 algorithms
  - Unique ids, full name and other properties for each algorithm
  - Structured in 3 main categories: Cryptographic-Hash-Function, Symmetric-Key-Algorithm and Asymmetric-Key-Algorithm
    - Several subcategories (under review)
  - Developed in .yaml for simplicity, so low contribution threshold
- A description of the properties used on the list
  - id, name, oid, commonKeySize, specifiedkeySize, cryptoClass and reference
- Other content: example algorithm for new algorithms requests…



SPDX Crypto Algorithms List today

- Algorithm detection and SPDX Security Profile as main use cases
- Meeting regularly: meetings repo, cryptography folder
- Current activities
  - Publishing the List on the website? Scope
  - Completeness: adding references (parameter)
  - First parameter: mode
  - Several open discussions. Conclusions are frequently deferred…
    - To focus on the next small batch
    - To learn more about topic and implications

Challenges

- Completeness: it will require some time to complete the information corresponding to the properties of the current algorithms. Example
- The security profile requires the addition of algorithm “parameters” to the list. We do not fully understand yet the scope and impact.
    a. We will include a first parameter as soon as possible
- The inclusion of certificates might challenge the current structure
- Small group (risk):
    a. We welcome a cryptographer that can advise the existing teamLately more people are showing up to meetings
    b. Not yet at the activation point

CycloneDX cryptographic assets

- CycloneDX created an overview of "cryptographic assets", defining a:
  a. 4 cryptographic assets types: algorithm, certificate, protocol and related-crypto-material
  b. Cryptographic definition schema
  c. Cryptographic definitions
     i. 80 different algorithms "families"
     ii. 254 elliptic curves variants
     iii. Last update on 2025-03-22
- CycloneDX definitions and schema are part of the specification
- When it comes to algorithms, focus on the most relevant only, specially from the standardization bodies perspective

CycloneDX definitions vs SPDX C.A. List

- Specification vs project resource
- Cryptographic assets vs algorithm list
- Focus on standardised algorithms vs widely used algorithms

The cryptography team agreed on using the same id as CycloneDX by default.

- When not possible/desired, compatibility mechanism

Why is SPDX creating the List?

Next steps

- Publishing the list on the website?
  - Release process
  - Tooling and procedures
  - Complementary content
- Add the first parameter: mode
- Keep working on completeness
- A new contribution from SCANOSS is on its way: bulk of algorithms
- Adding new contributors: awareness
- Mature open discussions

SPDX Crypto Algorithms List Use Case

SPDX Security Profile

Summary

- SPDX Cryptographic Algorithm List, inspired by the SPDX License List
- The List has been driven so far by two main use cases: algorithm detection and SPDX Security Profile
- Cryptographic algorithm id and full name as main asset
- The List is under heavy development but, mature enough to be perceived as a credible effort, so it can go on the SPDX website?
- Similar motivations but different scope and approach than CycloneDX. Sharing ids is a foundational goal
- The Group is working on the preps. For publishing on the SPDX website

Call for Participation

- We welcome all contributors to review the list and provide feedback, especially:
  - Engineer who wants to drive the publishing effort technically
  - Individuals with expertise in cryptography
  - SCA tooling developers and open standards professionals

How can the list work for you? New use cases?

- Join our regular meetings, on Wednesdays at 15:00 UTC
- Contribute to our GitHub repository
- Connect with us through the SPDX community channels.

SPDX Crypto Algorithms List

State of the art

SPDX tech-team Meeting
2026-02-17

Agustín Benito Bethencourt
Independent Consultant
Sponsored by STF