SCANOSS

Cryptography definitions

Open Data

OpenChain Webinar (online)

2024-03-12

Julian Coccia

SCANOSS CTO

About SCANOSS

About us

- A **data** company
- **IP:** Knowledge Base and Mining Network
- Knowledge Base of **published** OSS
  - **No** proprietary software
  - **No** unpublished OSS

About us

- An **Open Source Software** company
- Our software is here: **https://github.com/scanoss**
- Our Knowledge Base is made using **OSS only**
- With our OSS, you can create **your own Knowledge Base**

Our Memberships

- **OpenChain** Partner
  - OpenChain Tooling WG
  - OpenChain Export Control WG
- **Eclipse Foundation** Sponsor
  - Eclipse SDV Member
- **Software Heritage** Sponsor

Growing Ecosystem

Open Source SCA

fossology

OSS Review Toolkit

scancode

FOSSLight

Commercial SCA vendors

Trust Source

+ others

Auditing firms

ARRAY

Fossity

+ others

Universities

UNIVERSIDAD DE MÁLAGA | uma.es

ITIS SOFTWARE UNIVERSIDAD DE MÁLAGA

BAES Blockchain Lab

HELLENIC REPUBLIC UNIVERSITY OF MACEDONIA

Courts

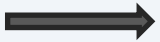
REPVBBLICA ITALIANA

SCANOSS

The Journey to Open Data

Our Journey to Open Data

- 2021 Launched OSSKB
  https://osskb.org



- 2022 Launched PURL2CPE
  https://github.com/scanoss/purl2cpe

- 2024 Launched Crypto Algorithms (Open Data)
  https://github.com/scanoss/crypto_algorithms_open_dataset

Building and maintaining a knowledge base

- The Knowledge Base **is BIG**
  - >2Pb downloaded
  - 210M URLs
  - 100B files
  - 3T lines of code
- Creating and maintaining a KB **is expensive**
  - Dedicated team of data scientists/engineers
  - Dedicated team of curators
- Providing a reliable data access at scale **is expensive**
  - Dedicated operations team
  - High hosting costs

SCANOSS

Crypto Algorithm Definitions

Crypto Algorithms (Open Data)

crypto_algorithms_open_dataset Private

Edit Pins | Watch 4

main | 3 Branches | 0 Tags | Go to file | Code

toscalix Merge pull request #2 from scanoss/toscalix-patch-quantum-safe e73f310 · 41 minutes ago 6 Commits

.idea	Initial commit	2 days ago
definitions	Initial commit	2 days ago
utilities	Initial commit	2 days ago
.gitignore	Initial commit	2 days ago
CODE_OF_CONDUCT.md	Initial commit	2 days ago
CONTRIBUTING.md	Initial commit	2 days ago
LICENSE	Initial commit	2 days ago
README.md	Update README.md	yesterday

README | Code of conduct | CC0-1.0 license

Cryptographic Algorithms Open Dataset

This data set, which includes a list of cryptography algorithms with an open source implementation, was originally the output of SCANOSS mining efforts across its entire data base, which includes all relevant open source software published. Today, the intention is to turn this repository into a collaborative project to enrich and maintain this data set, not just for export control, the original target activity, but for other purposes as well, like quantum safe.

CC0-1.0 License

Crypto Algorithms (Open Data)

Files

main

Go to file t

- ASN1.yaml
- CMAC.yaml
- README.md
- X509.yaml
- aes.yaml
- aria.yaml
- bcrypt.yaml
- blakex.yaml
- blowfish.yaml
- blum-goldwasser.yaml
- camellia.yaml
- cast.yaml
- chacha(salsa).yaml
- cmea.yaml
- cms.yaml
- cobra.yaml

crypto_algorithms_open_dataset / definitions / camellia.yaml

eeisegn Initial commit

Code Blame 21 lines (21 loc) · 531 Bytes

```yaml
algorithm: camellia
strength: '256'
keywords:
    - camellia.core
    - CIPHERCAMELLIA256
    - CAMELLIA-256-CBC
    - Camellia_cfb8_encrypt
    - Camellia_ctr128_encrypt
    - Camellia_set_key
    - Camellia_EncryptBlock_Rounds
    - Camellia_DecryptBlock
    - Camellia_decrypt
    - Camellia_DecryptBlock_Rounds
    - Camellia_cfb128_encrypt
    - Camellia_Ekeygen
    - Camellia_EncryptBlock
    - Camellia_cbc_encrypt
    - Camellia_cfb1_encrypt
    - Camellia_ecb_encrypt
    - Camellia_encrypt
    - Camellia_ofb128_encrypt
```

- Algorithm list
- Detection definitions
- Attributes
- Reference code

Crypto Algorithms (Open Data)

- Use it!
- Contribute!
  - New Definitions
  - New Attributes
- Use in SBOM

Use cases

- Export Control (ECCN, Trade Compliance)
- Quantum safe area
- CAVP compliance (NIST)

SCANOSS

Crypto Algorithm Definitions

For Export Control

Bridging the gap together

Seeking Consensus on

- How to **declare** these open source algorithms
  - Initial step towards **standardization**
- Algorithm **classification and attributes**
- Bringing declarations **into SBOMs**
  - Simpler distribution, consumption and management.
- Just like we (as a community) did with license compliance
  - Reducing overall **costs and risks**
  - Improving **transparency and efficiency**

Next Steps

- **Enrich** and **maintain** the published **data** and **tool** sets
- Define and **ontology** to declare crypto algorithms
  SPDX?

Is OpenChain Export Control WG interested in making this data set part of its commons?

FYI: SCANOSS is.

SCANOSS

Thank you!

https://scanoss.com