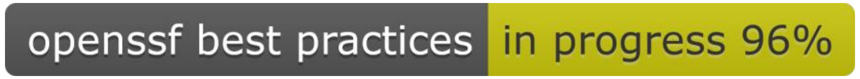
Project Veraison

Attestation Verification Components

CCC TAC review 2024

VERAISON

Project Submission deltas

- No change from last year
- Budget usage
    - Travel: IETF Hackathon / Fosdem / CC Summit
    - Infrastructure: no budget usage yet
- Core team have completed Inclusive Open Source Community Orientation training
- 
  openssf best practices in progress 96%
- Sandbox level is still appropriate

VERAISON

Technical Progress - codebase

- Support for multiple Attestation schemes
  - CCA / AMD SEV-SNP / PSA / TPM / DICE / Oracle CC
  - Parsec + CCA key attestation plugin
  - Major refactor to promote code reuse across similar profiles
- Extensibility framework for CoRIM
  - in collaboration with Oracle & Intel
- Full REST API
  - https support
  - authentication & authorization via Keycloak integration
- New policy manager service
- Container Deployment or Native Deployment scripting
- Added functionality in CLI tools
- Improved user documentation
- Increased use of RUST
  - Added standalone CCA token, EAR, keybroker demo crates
- Introduced a lightweight versioning scheme with monthly tags

VERAISON

Technical Progress - standards

- Standards Co-authoring & reference implementations
- CoRIM (model for endorsement / ref value supply to Verifier)
  - IETF / TCG
- Entity Attestation Results (data model for results from Verifier)
  - IETF – builds on AR4SI claim normalization work
- Attested TLS – demo & unification work
- IETF RATS EAT contributions
  - Architecture / Media Types / Conceptual Message Wrapper

VERAISON

github stats

- 36 individual contributors (+14)
  - 15 organisations (+6)
- Community split:
  - Veraison services: 22 stars, 14 forks, 7 contributors
  - CoRIM: 8 stars, 7 forks, 7 contributors
  - go-cose: 49 stars, used by 143 other projects, 16 contributors
- All repo stats:
  - 174 PRs merged in past year
  - 72 issues closed in past year
  - 103 stars
  - 68 forks

Community

- Active weekly meetings
  - Keylime project collaboration
- Active services deployments in preparation (Oracle, Siemens)
- Academic project integrations (IISEC Japan for OpTEE)
- OSS project integration (CoCo, OpenEuler)
- It’s believed that CoRIM tooling is in active use

- Conference presentations: OC3, FOSDEM, CCS, IETF hackathon

VERAISON

VERAISON

https://github.com/veraison/