Project Veraison

Attestation Verification Components

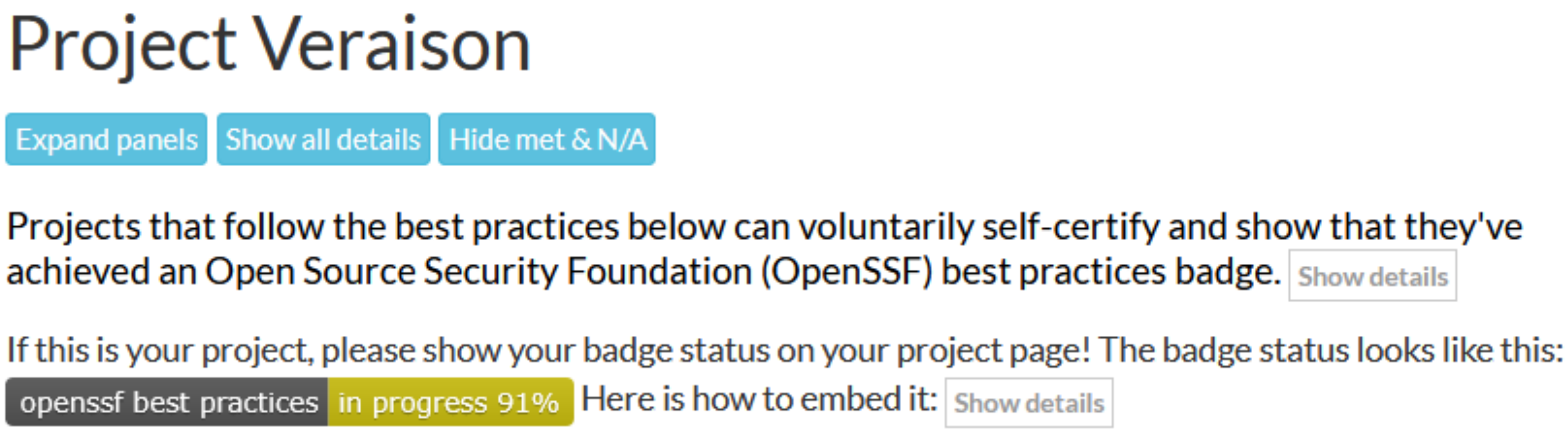
CCC TAC review 2023

VERAISON

Project Submission deltas

- Minimal deltas from original
    - Some URLs have changed due to a repo reorg, but info remains the same
        - Updated doc published on Veraison github
    - Details of 3rd party dependencies have changed but minor in effect
        - License scan published on Veraison github
- Budget usage
    - Travel: IETF Hackathon / Fosdem / CCC Summit
    - Infrastructure: no budget usage yet
- Most of core team have completed Inclusive Open Source Community Orientation
- Sandbox level is still appropriate

Open Source Best Practices



Project Veraison

Projects that follow the best practices below can voluntarily self-certify and show that they've achieved an Open Source Security Foundation (OpenSSF) best practices badge.

If this is your project, please show your badge status on your project page! The badge status looks like this: Here is how to embed it:

https://bestpractices.coreinfrastructure.org/en/projects/7428

VERAISON

Technical Progress - codebase

- Support for multiple Attestation schemes (PSA / CCA / TPM / DICE)
  - others pending
- Full REST API
- Deployable Appraisal Policy pass
- Container Deployment
- CLI tools for experiments & test construction
- First implementation of standard ‘EAT Attestation Results’ data model
- Experimental deployment ‘in TEE’ with proofs
- Options to deploy without (external) plugin framework to reduce TCB

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 / EAT Collections

Community

- Individual Contributors grows from 4 to 22
  - 9 organisations involved
- 552 PRs merged in the last year
- Issues: total: 404, 270 closed
- Community split: Veraison services / Standards / go-cose
- Collaboration:
  - Multiple organisations attend the public meetings
  - Some orgs are restricted on OSS contributions
  - Exploring collaboration with Keylime
- Conference presentations: OC3, FOSDEM, TPM.dev, IETF hackathon

VERAISON

https://github.com/veraison/