

Project Veraison

Attestation Verification Components

CCC TAC review 2025

Project Submission deltas

- No change from last year
- Budget usage (to date CY25)
 - Travel: no budget usage
 - Infrastructure: no budget usage
- Sandbox level is still appropriate

openssf best practices **passing**

Technical Progress - codebase

- Support for multiple Attestation schemes
 - CCA / AMD SEV-SNP / PSA / TPM / DICE / Oracle CC / Intel TDX
- Golang is used for most components but there is an increased use of RUST
- Deployment
 - Native Service deployment tweaks
 - AWS service deployment
 - RPM build
- Documentation 'Book'
- RATS
 - CMW
 - Device Assignment EAT
 - CoSERV endorsement distribution prototype
 - CoRIM verifier / generation
 - Python-EAR *
 - Provisioning of Signed CoRIM *
- ratsd
- * projects completed in LF mentorship

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
- New for 2025: CoSERV + prototype
- Veraison – the ‘RATS verifier’

github stats

- 51 individual contributors (+15)
 - 21 organisations (+6)
- Community split:
 - Veraison services: 29 stars, 23 forks, 11 contributors
 - CoRIM: 13 stars, 20 forks, 14 contributors
 - go-cose: 55 stars, 28 forks, used by 143 other projects, 17 contributors
- All repo stats:
 - 243 PRs merged in past year
 - 119 issues closed in past year
 - 219 stars
 - 138 forks

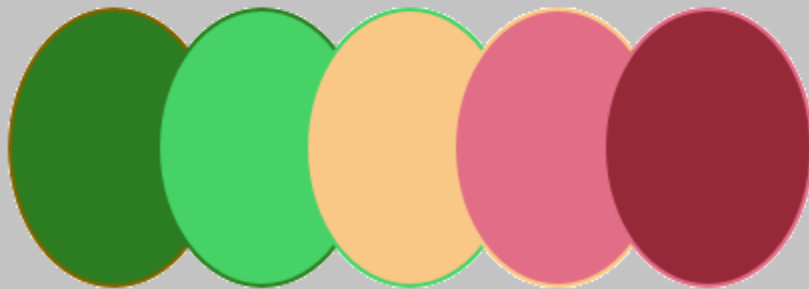
Community

- Active weekly meetings
 - Regular attendance from multiple organisations, commercial + academic
- 2 LF mentorship projects
- Active services deployments: Oracle, Linaro
- Subject of academic paper
 - [Standard-Based Remote Attestation: The Veraison Project](#)
- OSS project integration (CoCo, Keylime)
- CoRIM tooling is in active use
 - Cocli referenced in vendor docs
- Conference presentations:
 - OC3, FOSDEM, CCS24, IETF meetings, Google transparency summit

Roadmap

- Endorsement / Reference Value distribution
 - IETF RATS 'CoSERV'
- Endorsement lifecycle management (provisioned store)
- Multi Verifier interactions for compound attestations
 - RATS WG work

VERAISON



<https://github.com/veraison/>