Remote Attestation in the Cloud

With Veraison

Jagannathan Raman

Software Developer

Oracle

Feb 02, 2025

Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied
upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Oracle Team

Liam Merwick

liam.merwick@oracle.com

Jag Raman

jag.raman@oracle.com

Ian Ching Wang

ian.chin.wang@oracle.com

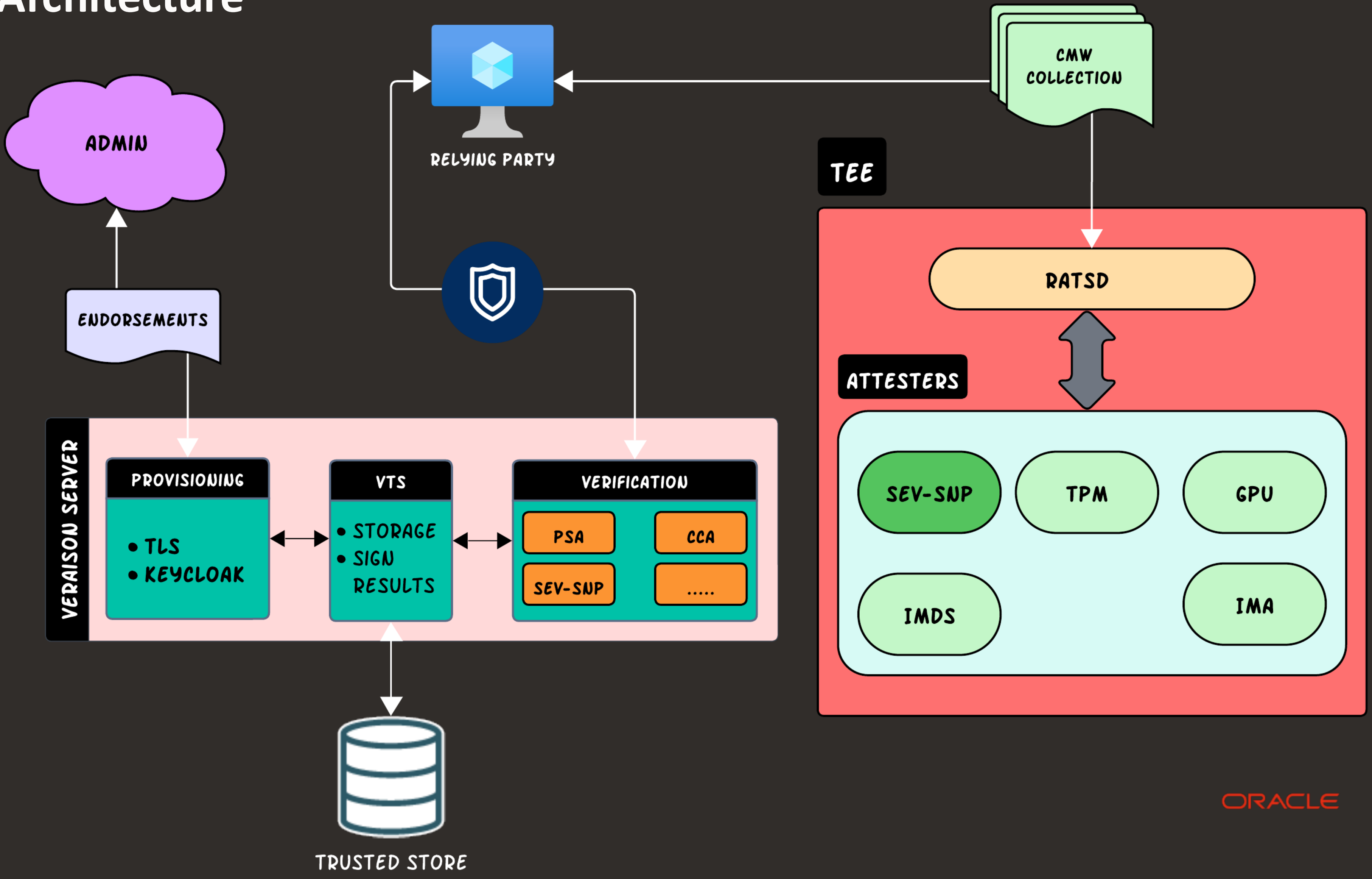
Agenda

- Veraison
- Architecture
- Endorsements
- Evidence format
- Verification
- Result format
- Oracle contribution
- Demo
- Upcoming features
- Acknowledgements

Veraison

- IETF RATS compliance
- Software components
  - Server
  - RATSd, go-gen-ref, cocli, evcli
- Support for token formats and attestation protocols
  - CoRIM (Concise Reference Integrity Manifest)
  - EAT (Entity Attestation Token) / CMW (Conceptual Message Wrapper)
- Scalable
- Interoperable
- Open-source

System Architecture



ORACLE

SEV-SNP Endorsements

- Trust Anchors
  - Root Keys (eg. ARK & ASK)
- CoRIM Reference Values
- SEV-SNP profile
  - IETF draft
  - SEV-SNP Attestation Report
  - Mkeys
- `go-gen-ref` generates reference values
  - Compute launch measurement

```
{
  "lang": "en-GB",
  "tag-identity": {
    "id": "da3c7818-55ef-4aaa-a465-1f59d2872b1e"
  },
  "triples": {
    "reference-values": [
      {
        "environment": {
          "class": {
            "id": {
              "type": "oid",
              "value": "1.3.6.1.4.1.3704.3.1"
            }
          },
          "instance": {
            "type": "bytes",
            "value":
"wqZSi3Nk4H6fXGU6s6oNvXOE+agN/eVMxkPdu4nYk2Ql/4oyVoym7XcQINw5wzzP+ztD
ysDFAaAJPK1gEt/T7Q=="
          }
        },
```

SEV-SNP Endorsements

- Trust Anchors
  - Root Keys (eg. ARK & ASK)
- CoRIM Reference Values
- SEV-SNP profile
  - IETF draft
  - SEV-SNP Attestation Report
  - Mkeys
- `go-gen-ref` generates reference values
  - Compute launch measurement

```
 "measurements":  [
          {
            "key": {
              "type": "uint",
              "value": 641
            },
            "value": {
              "digests": [
                "sha-
384;C8yFu/d5q8TGw/OyKF6JFxTqmRnGT1QhkuWbnKSefWGRIqnylmWiQ52i4IVkHN1+"
              ]
            }
          },
          {
            "key": {
              "type": "uint",
              "value": 3330
            },
            "value": {
              "version": {
                "value": "1.55.40”,
                "scheme": "semver"
              }
            }
          }
        ]
      }
    ]
  }
}
```

SEV-SNP Evidence

- Evidence formats
- CMW collection
- Registered TSM report media-type with IANA: “application/vnd.veraison.tsm-report+cbor”
- RATSd: https://github.com/veraison/ratsd

CMW collection

```
{
    "__cmwc_t":
”application/vnd.oracle.VMStandardE5Flex",
    "sevsnp": [
        {
            "type": "application/vnd.veraison.tsm-
report+cbor",
            "value": "<< tsm-report >>"
        }
    ],
    "tpm": [
        {
            "type": "application/vnd.tcg.tpm",
            "value": "<< TPMS_ATTEST >>"
        }
    ]
}
```

IANA recognizes "application/vnd.veraison.configfs-tsm+json”.

Yet to register ”application/vnd.oracle.VMStandardE5Flex” & "application/vnd.tcg.tpm

SEV-SNP Evidence

- Evidence formats
- CMW collection
- Registered TSM report media-type with IANA: “application/vnd.veraison.tsm-report+cbor”
- RATSd: https://github.com/veraison/ratsd

tsm-report

```
tsm-report = {
  ? auxblob: binary-string
  outblob: binary-string
  provider: tstr
  ? service-report
}

service-report = ((
  manifestblob: binary-string
  service_provider: tstr
) // service_provider: tstr)

binary-string = base64url-string .feature "json" / bstr
.feature "cbor"

base64url-string = tstr .b64u bstr
```

Attestation Result

- EAR (EAT Attestation Result)
- Trustworthiness vector
- Description of various aspects of security

Result

```
"ear.appraisal-policy-id": "policy:SEVSNP",
     "ear.status": "affirming",
     "ear.trustworthiness-vector": {
       "configuration": 0,
       "executables": 0,
       "file-system": 0,
       "hardware": 2,
       "instance-identity": 0,
       "runtime-opaque": 2,
       "sourced-data": 0,
       "storage-opaque": 0
     }
```

Oracle’s contribution

- SEV-SNP plugin for the server: `https://github.com/jraman567/services`
- go-gen-ref to build reference values: `https://github.com/jraman567/go-gen-ref`
- RATSd tool to compose evidence, WIP: `https://github.com/veraison/ratsd`
- Oracle Linux deployment of Veraison
- Active community collaboration

Demo

Upcoming features

- Support for more attestation schemes
- RATSd
- Endorsement and Reference Value distribution
- Authorization

Acknowledgement

- Dionna Amalie Glaze (dionnaglaze@google.com)
- Sergei Trofimov (Sergei.Trofimov@arm.com)
- Thomas Fossati (thomas.fossati@linaro.org)
- Yogesh Deshpande (Yogesh.Deshpande@arm.com)

Thank you