STI CT

draft-wendt-stir-certificate-transparency-03

Chris Wendt, Somos
Rob Sliwa, Somos
Alec Fenichel, TransNexus
Vinit Anil Gaikwad, Twilio

STIR Working Group
IETF 120 - 07/22/2024

SOMOS®

STIR CT Overview

- As STIR is maturing and there is more adoption across different eco-systems of certificates, in particular delegate certificates with TNs in the TNAuthList, a broader mechanism is needed to validate certificates generated with different TNAuthLists (including SPC) can be explicitly trusted.

- Certificate transparency and transparency more generally provide a general framework for verifiable mechanisms to assure the eco-system that all of the CA participants and their customers are following the policies, and there isn't any mis-issuance of certificates with duplicate or unintended SPC or telephone number resources, whether unintentional or with fraudulent intent.

- This has the benefit of providing trust and uniqueness both within and cross STIR eco-systems that either follow different policies or simply want to provide external transparency for greater trust and guaranteeing uniqueness of STIR certificates created based on rules of SPC or telephone number administration for different jurisdictions.

SOMOS®

STIR CT Discussion

- Based on feedback from IETF 119 discussion, we have abandoned aligning with RFC9162 other than using concepts of certificate transparency more generally.
- STIR certificate eco-systems generally follow prescriptive flows and STIR has PASSporTs which are convenient mechanisms to deliver multiple SCT certificate receipts.
- So, STIR CT document is very opinionated on not including SCT in certificate.
- We define a specified API for submission to logs, getting SCT, and for monitoring of logs.
- We don’t specify a specific append-only log implementation and really only use the definition of SCT based on STIR certificate chain from RFC9162.

SOMOS®

Vesper Token

draft-wendt-stir-vesper-00

Chris Wendt, Somos
Rob Sliwa, Somos

STIR Working Group
IETF 120 - 07/22/2024

SOMOS®

Vesper Overview

- Vesper tokens - Verifiable STI Personas are intended to provide a protocol and extensible format to represent a framework for the selective disclosure of information about an entity associated with a telephone number.
- There has been a lot of industry discussion about vetting and KYC/KYB by third party Vetting Agents. Vesper is meant to align these concepts into a specific framework that vesper tokens can be used as a signed token with interesting characteristics for selective disclosure for different scenarios of proving different information to a called party, their telephone service provider, or many other potential use-cases, like vcon and others.
- It is intended to align with many of the three party (issuer, holder, verifier) models being discussed in SPICE and SCITT as well, but specific to telephone numbers and some of the unique cases required in the telecom environment.

SOMOS®

Vesper Overview - Key Components

- Selectively Disclosable Token: Contains vetted information that can be selectively disclosed.
- Transparency Append-only Log: Publicly verifiable log that records the issuance and updates of the token.
- Transparency Receipt: A verifiable proof of the token's existence and its contents at a given time.
- Each component plays a crucial role in maintaining the security and integrity of the VESPER protocol.

SOMOS®

Vesper Overview - Roles

- VESPER involves three primary roles:
- Vetting Agent (VA): Acts as the issuer. Performs the vetting of persona related information and issues the VESPER token.
- Vetting Entity (VE): Acts as the holder. The entity whose information is vetted and who holds the VESPER token.
- Vetting Verifier (VV): Acts as the verifier. The party that verifies the authenticity and integrity of the VESPER token.

SOMOS®

Vesper Overview - Vetting of Personas

- The vetting process involves verifying the identity and credentials of a persona.
- Issuer's Role: The issuer, known as a Vetting Agent (VA), validates the information and creates a VESPER token.
- Use of JWT and SD-JWT: Utilizes JSON Web Tokens (JWT) and Selective Disclosure JWT (SD-JWT) for persona-related information.

Vesper Overview - Telephone number validation

- The VESPER token associates a vetted persona with the right to use (RTU) a specific telephone number.
- Verification: Ensures that the telephone number is authorized for use by the vetted persona.
- Preventing Fraud: Helps combat unauthorized usage and fraudulent activity by ensuring that only vetted personas can use the telephone numbers.

SOMOS®

Vesper Overview - Verifiability

- Verification Methods: Tools and methods available for the public to verify the authenticity of the VESPER token.
- Append-only Log: Ensures all updates and issuances are recorded and cannot be altered.
- Transparency Receipt: Provides proof of the token's validity and integrity.
- Eco-system Verifiability: Allows anyone to verify the authenticity of the VESPER token, ensuring accountability and trust in the system.
- Standard APIs for transparency logs

SOMOS®

Vesper Example

- Vetted Claims Example


```
{
  "sub": "Business_42",
  "telephone_number_rtu": [
    +18001231234,
    +18881231234
  ],
  "rcd": [
    {"nam":"Business_42","icn":"https://example.com/logo.png"}
  ]
  "business_ids": [
    {"EIN":"123456789"}
  ]
  "address": {
    "street_address": "123 Main St",
    "locality": "Anytown",
    "region": "Anystate",
    "country": "US"
  },
  "contact_given_name": "John",
  "contact_family_name": "Doe",
  "contact_email": "johndoe@example.com",
  "contact_phone_number": "+12025550101"
}
```


SOMOS®

Vesper Example

- Vesper Token SD-JWT Example


```
{
  "_sd": [
    "CrQe7S5kqBAHt-nMYXgc6bdt2SH5aTY1sU_M-PgkjPI",
    "JzYjH4svliH0R3PyEMfeZu6Jt69u5qehZo7F7EPYlSE",
    "PorFbpKuVu6xymJagvkFsFXAbRoc2JGlAUA2BA4o7cI",
    "TGf4oLbgwd5JQaHyKVQZU9UdGE0w5rtDsrZzfUaomLo",
    "XQ_3kPKt1XyX7KANkqVR6yZ2Va5NrPIvPYbyMvRKBMM",
    "XzFrzwscM6Gn6CJDc6vVK8BkMnfG8vOSKfpPIZdAfdE",
    "gbOsI4Edq2x2Kw-w5wPEzakob9hV1cRD0ATN3oQL9JM",
    "jsu9yVulwQQlhFlM_3JlzMaSFzglhQG0DpfayQwLUK4"
  ],
  "iss": "https://vetting-agent.example.com",
  "iat": 1683000000,
  "exp": 1883000000,
  "sub": "Business_42",
  "telephone_number_rtu": [
    +18001231234,
    +18881231234
  ],
  "rcd": [
    {
      "...": "pFndjkZ_VCzmyTa6UjlZo3dh-ko8aIKQc9DlGzhaVYo"
    }
  ],
  "business_ids": [
    {
      "...": "7Cf6JkPudry3lcbwHgeZ8khAv1U1OSlerP0VkBJrWZ0"
    }
  ],
  "kyc_data_hash": "8khAv1U1OSlerP0VkBJrWZ07Cf6JkPudry3lcbwHgeZ",
  "transparency_receipt": "dh-ko8aIKQc9DlGzhaVYopFndjkZ_VCzmyTa6UjlZo3",
  "_sd_alg": "sha-256",
  "cnf": {
    "jwk": {
      "kty": "EC",
      "crv": "P-256",
      "x": "TCAER19Zvu3OHF4j4W4vfSVoHIP1ILilDls7vCeGemc",
      "y": "ZxjiWWbZMQGHVWKVQ4hbSIirsVfuecCE6t4jT9F2HZQ"
    }
  }
}
```


SOMOS®

sipcore-callinfo-rcd Update

draft-ietf-sipcore-callinfo-rcd-12

STIR Working Group
IETF 120 - 07/22/2024

SOMOS®

call-info RCD update

- A lot of recent thought and review has been put into latest updates in terms of RCD implementation.
- Focus has been on use of Call-Info specific to a trusted UNI interface between terminating provider and UE to enforce local policy on what RCD information is sent to UE.
- Recent updates include “verified” and “integrity” parameters
- “verified” is a simple indication that the sender (who should be assumed to be trusted in UNI case) has explicitly verified the RCD information from sender
- “integrity” allows the ‘rcdi’ hash to be sent to the UE, so that when a URI is followed, for a logo for example, an integrity check can be performed, because a verification service will likely not download content from a URI to verify it. (Don’t download twice).

SOMOS®

call-info RCD update status

- version -12 was uploaded this morning that includes minor editorial fixes and clarification based on mailing list comments from Paul and some offline comments/ review received directly.

- Any questions/comments?

SOMOS®