06 November 2023

Supply Chain Integrity, Transparency, and Trust (SCITT)

This session is being recorded

Agenda

- Welcome and Introduction (5 min): Chairs
- Why SCITT is COOL (5 mins): Henk Birkholz
- Recap since 117 (5 mins): Henk Birkholz
- Registration Policies (15 mins): Jon/Cedric
- API & Receipt Updates (15 mins): Orie Steele
- Hackathon Report (15 min): Jon
- Next Steps and WG operations for 119 (15 min): Chairs
- AOB Open Mic (20 min – BE CONCISE!): All
- Wrap-up and Conclusion (5 min): Chairs

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

I E T F®

Note Really Well

- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, please talk to the Ombudsteam, who are available if you need confidentiality to raise concerns confident about harassment or other conduct in the IETF.
- The IETF strives to create and maintain an environment in which people of many different backgrounds and identities are treated with dignity, decency, and respect. Those who participate in the IETF are expected to behave according to professional standards and demonstrate appropriate workplace behavior.
- IETF participants must not engage in harassment while at IETF meetings, virtual meetings, social events, or on mailing lists. Harassment is unwelcome hostile or intimidating behavior—in particular, speech or behavior that is aggressive or intimidates.
- If you believe you have been harassed, notice that someone else is being harassed, or have any other concerns, you are encouraged to raise your concern in confidence with one of the Ombudspersons.

IETF

IETF-118 Links

- Agenda
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information
  https://www.ietf.org/how/meetings/preparation
- If you need technical assistance, see the Reporting Issues page:
  https://www.ietf.org/how/meetings/issues/

Any Volunteers?

HedgeDoc

IETF

Agenda

- Welcome and Introduction (5 min): Chairs
- Why SCITT is COOL (5 mins): Henk Birkholz
- Recap since 117 (10 mins): Henk Birkholz
- Registration Policies (15 mins): Jon/Cedric
- API & Receipt Updates (15 mins): Orie Steele
- Hackathon Report (15 min): Jon
- Next Steps and WG operations for 119 (15 min): Chairs
- AOB Open Mic (20 min – BE CONCISE!): All
- Wrap-up and Conclusion (5 min): Chairs

IETF

Why is SCITT Cool

Henk Birkholz

Why is SCITT Cool

It's a simple and scalable authenticity layer for endorsements* of your products moving along supply chains!**

*such as SBOMs, SLSA, etc. **actually, directed value creation graphs.

https://emojipedia.org/animated-noto-color-emoji/14.0/heart-on-fire

Why is SCITT Cool (some more detail)

One compact (CBOR), well-profiled (CDDL) signing mechanism (COSE) that enables:

1. a thin, minimalistic authenticity layer wrapped around your supply chain statements
2. registration (aka notarization) of your supply chain statements for later audits after the fact
3. off-line verifiable receipts that prove you are honest about being transparent with your product statements (and under which conditions these statement were made transparent)

Recap Since 117

Henk Birkholz

Architecture Updates

- PR #94: Signed Statement Issuance, Registration
- PR #95: BCP 14 rules for SHOULD/SHOULD NOT
- PR #105: Cleanup of remaining references to Claims
- PR #107: Clarification of Feed purpose and differentiate from reg_info
- PR #108: Use CWT Claims in Headers
- PR #113: Proposal to rephrase the Reg_Info definition
- PR #114: Rename Feed to Subject
- PR # 119: Clarify Consumer/Verifier Terminology

Use Case Updates

- Detailed Software Supply Chain Uses Cases for SCITT
- PR #4: Add Versioning Use Case
- Use Case: WGLC still on this week
  - Feedback via scitt@ietf.org

Registration Policies

Jon Geater
Cedric Fournet

Context

Registration Policy *"is a simple set of rules evaluated by the Transparency Service to determine admissibility of a Statement"*

Assumed Requirements

- We need to stay payload-agnostic and interoperable
- We cannot predict all use cases or data inputs, so while some defined conventions are a good idea, the structures must be extensible
- General access control concerns:
  - API implementation concerns
  - Anti-spamming
  - Mandatory identification of statement issuers
    (note protocol clients and message-based signing + DID are *not the same*)

- Specific Statement registration concerns:
  - The owner of a Feed (now original Issuer of a Subject) should be able to limit which other Issuers can write to that feed
  - Where Statements are related to each other or to the real world in ways that the Issuer or Client cannot reasonably know or evaluate, the Transparency Service should be able to decide to reject the Statement
  - Verifiers can see what Registration Policy was in force when a Transparent Statement was created

Direction of Travel

- Observing recent progress there's an opportunity for Registration Policies to be worked out between now and –119

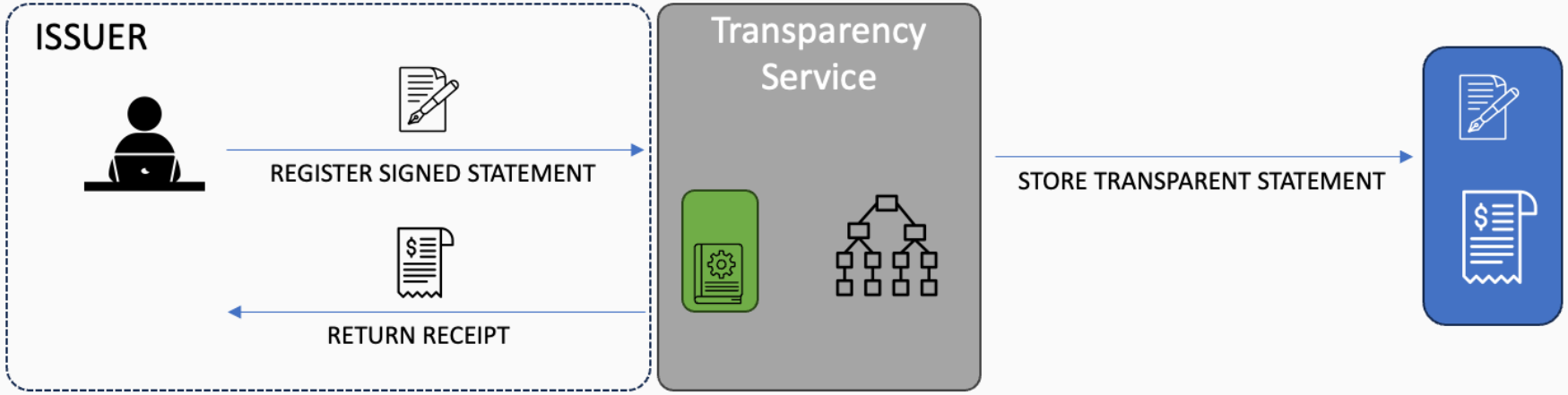
- Splitting the concerns signposts a route towards progress one-bite-at-a-time

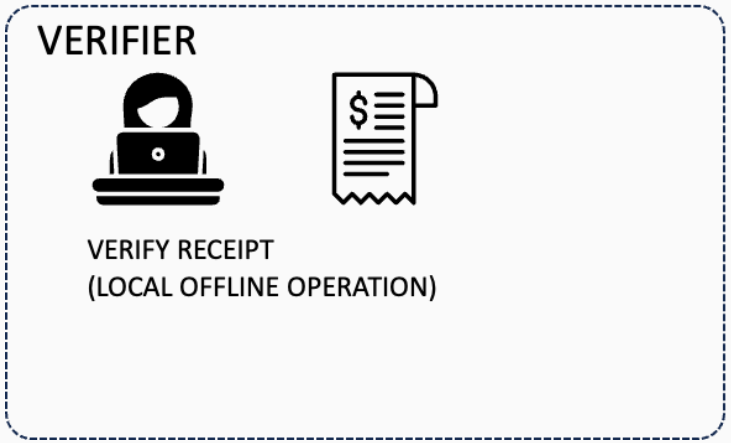
  - Very specific Registration Policy concepts: Protocol elements sufficient to enable the signaling from the Issuer to the Transparency Service for semantic evaluation of Statement admissibility
    (but ONLY syntactic interoperability, not semantic inference, Transparency Service operation or specific policy languages)

  - Protocol elements and architecture guidance sufficient to enable simple front-edge access control for identification of protocol clients and anti-spamming, etc.
    (This may obviate itself through development of SCRAPI??)

IETF

Challenge from the Hackathon

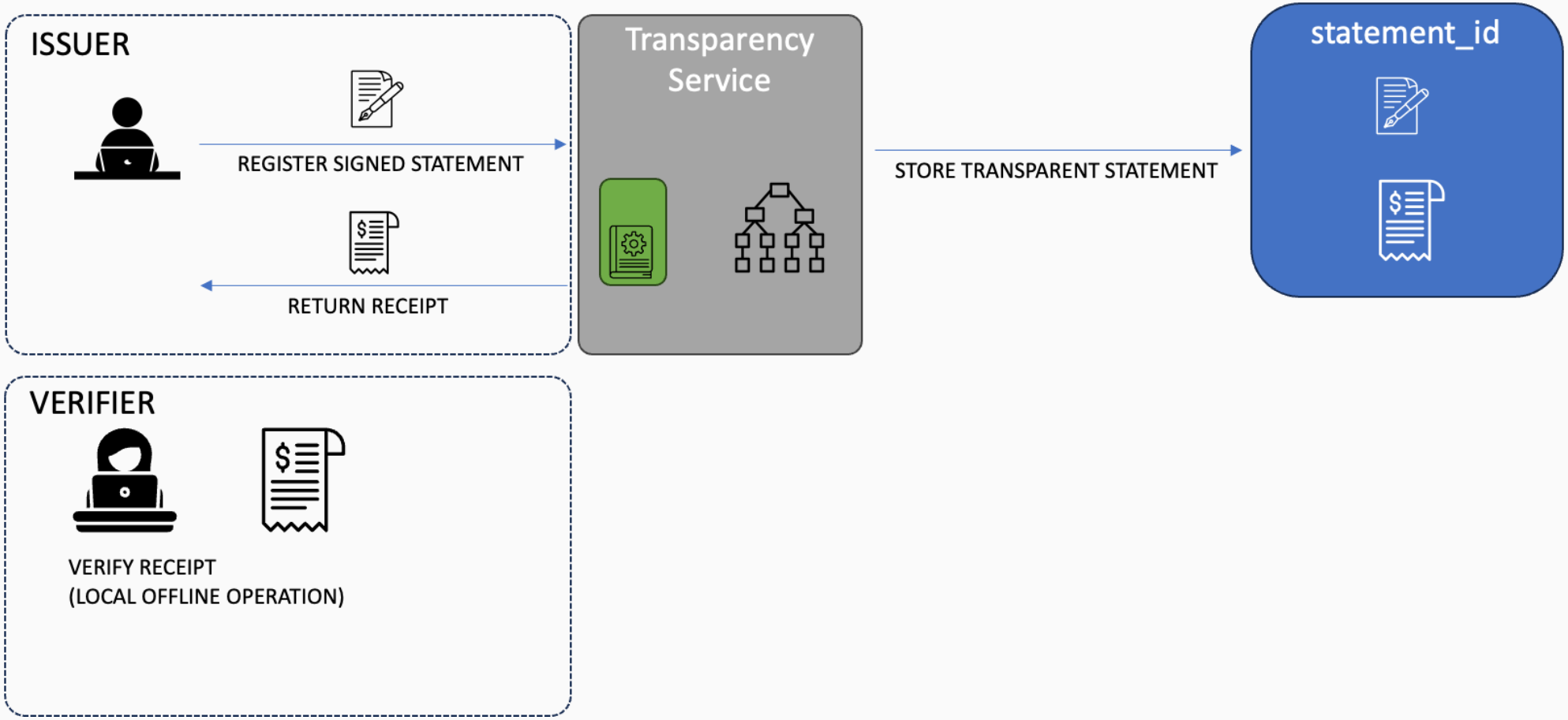




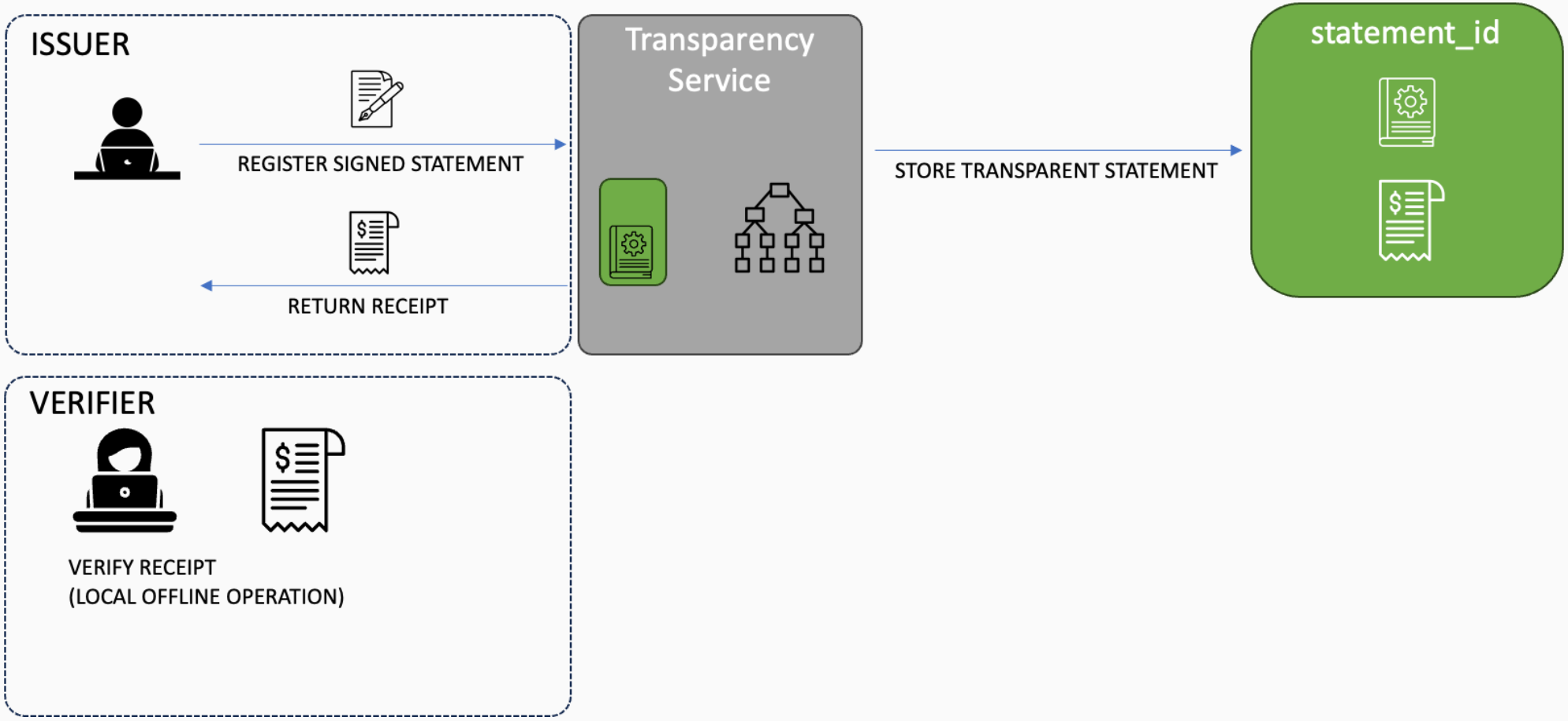
Problem statement

Although the receipt allows users to verify statements offline, we also desire to know what configuration was in force when that statement was registered

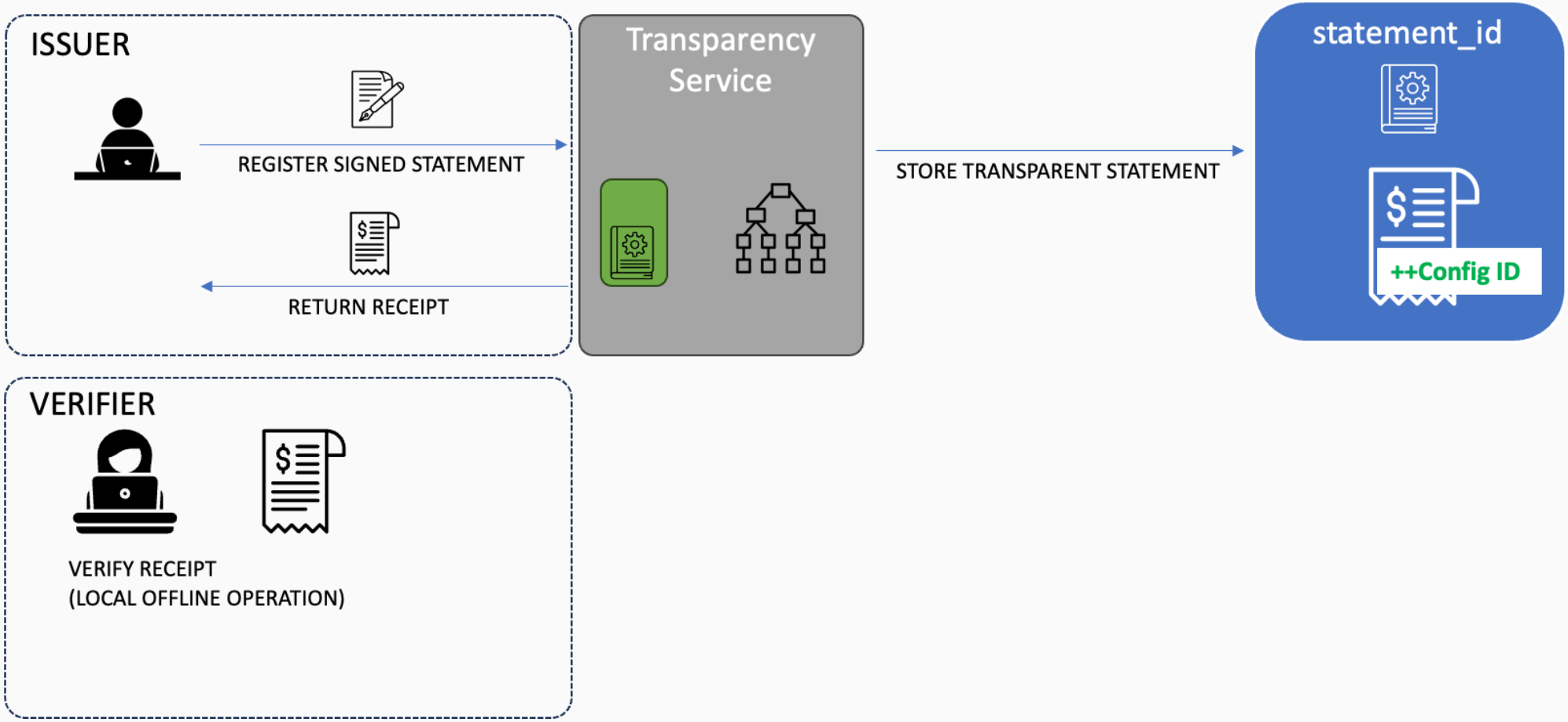
Response part 1: Each Transparent Statement gets an ID



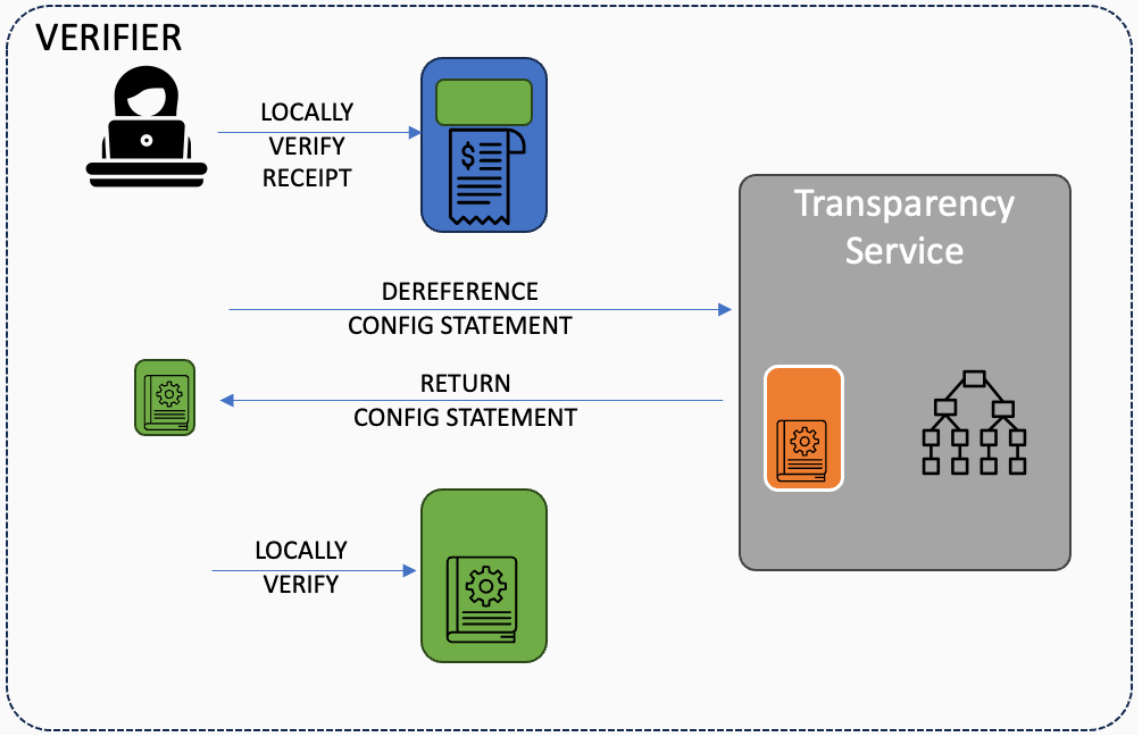
Response part 2: Store Config Changes as Transparent Statements



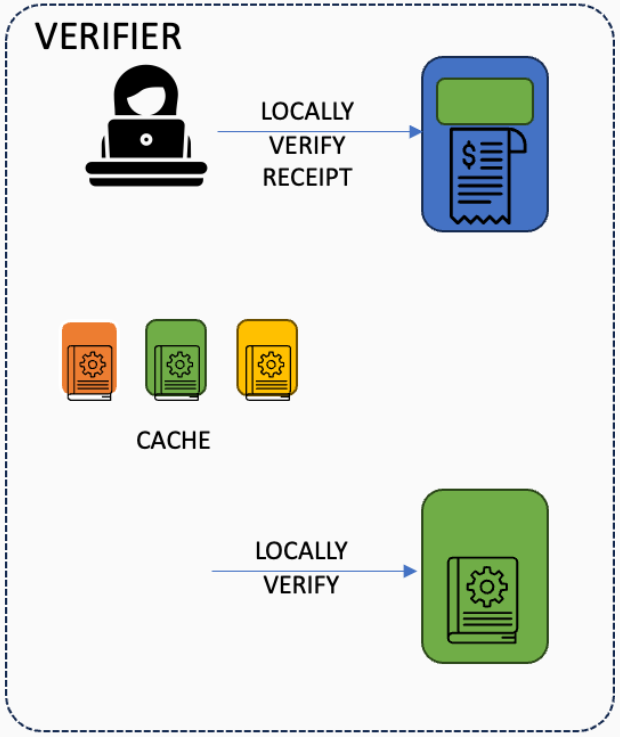
Response part 3: Embed ID Pointing To Config in Every Receipt



Response part 4: If in Doubt, Verify Both!



Response part 4A: Caching (And Other Techniques) Possible



Summary

- Great news! Reduce and simplify!
  - Drinking our own champagne is very satisfying.
    Proves that the SCITT structures are useful!
  - Increases overall system discoverability and transparency
  - Removes bulk and complexity from the architecture doc

- One big open question over the integrity of the Statement ID
  - Do we need to trust the Transparency Service to return the correct ID?
    Looking for ways to improve the integrity of this process.

Other Open Questions / Work to Be Done

- Is 'Registration Policy' the right name anymore? Is ‘configuration' better?
- Does this meet our need for application profiles?
  - Propose a couple of informative conventions for known common policies, see how it develops
- Example Registration Policies: SVN, supported issuer IDs, etc need to be added to the architecture.
  - Make sure we have clear use cases and people understand the value. Push for common use cases. Can be refined later.
- Control and updates to the Registration Policy.
  - Deliberately left Transparency Service specific for now—recording Registration Policy and its updates as Transparent Statements with unique IDs is a big step forward on its own.
- The content of a Registration Policy is (mostly) opaque to the SCITT layer: i.e., it is Transparency Service specific.
  - Can be refined later, but it's a huge piece of work and does not need to stall the progress the group has made with the other changes.

IETF

CBOR API

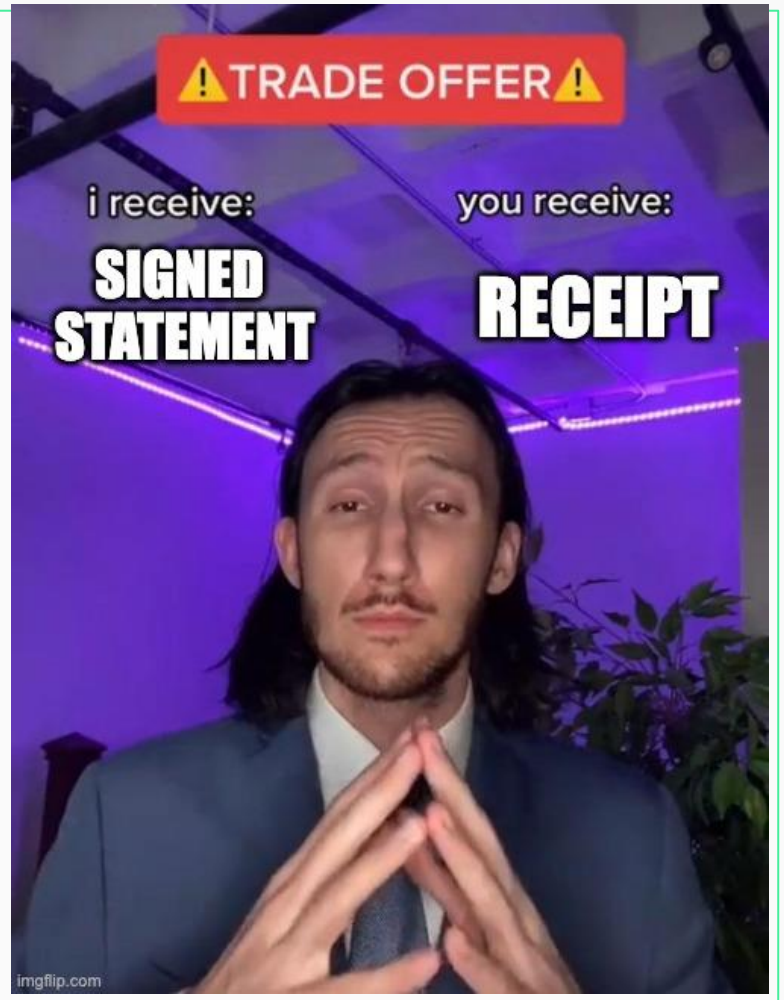
Orie Steele

High Level Pseudo-CBOR API

statement = a file or artifact that is relevant to a supply chain

signed statement = issue(
  statement,
  issuer claims,
  issuer signing key
)

receipt = registration(
  signed statement,
  registration policy,
  transparency log,
  notary claims,
  notary signing key
)



transparent statement = signed statement with a receipt

Signed Statement Protected Header

```
{
  1: -35,                       / Signature Algorithm        /
  3: application/json,          / Content type               /
  4: h'75726e3a...4b755a59',    / Key identifier             /
  TBD 0: {                      / CWT Claims                 /
    1: software.vendor,         / Issuer                     /
    2: product.version          / Subject                    /
  },
  393: {                        / Registration Info          /
    TBD 1: 74635                / Secure Version Number      /
  },
  33: [                         / X.509 Certificate Chain    /
    h'308201b4...b4e9b233',     / X.509 Certificate          /
    h'308201bf...4eb5f42d’      / X.509 Certificate          /
  ]
}
```

Transparent Statement

```
18(                                 / COSE Sign 1       /
  [
    h'a4012603...6d706c65',         / Protected         /
    {                               / Unprotected       /
      -333: [                       / Receipts (1)      /
        h'd284586c...8f1ff150'      / Receipt 1         /
      ]
    },
    nil,                            / Detached payload  /
    h'bcbb3bfe...9fc99291'          / Signature         /
  ]
)
```

Receipt

```
18(
  [
    h'a4012604...6d706c65',          / Protected            /
    {
      -222: {                        / Proofs               /
        -1: [                        / Inclusion proofs (1) /
          h'83080783...32568964’     / Inclusion proof 1    /
        ]
      },
    },
    nil,                             / Detached payload     /
    h'9621ab96...8f1ff150'           / Signature            /
  ]
)
```

Receipt Protected Header

```
{
  1: -35,                       / Signature Algorithm        /
  4: h'75726e3a...4b755a59',    / Key identifier             /
  TBD 0: 1                      / RFC9162 Transparency Log.  /
  TBD 1: {                      / CWT Claims                 /
    1: transparency.service,    / Issuer                     /
    2: registration event id    / Subject                    /
  },
}
```

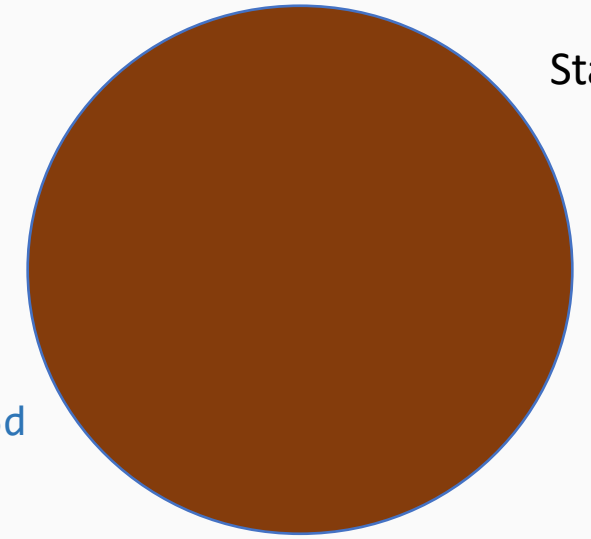
REST API

Orie Steele

High Level API

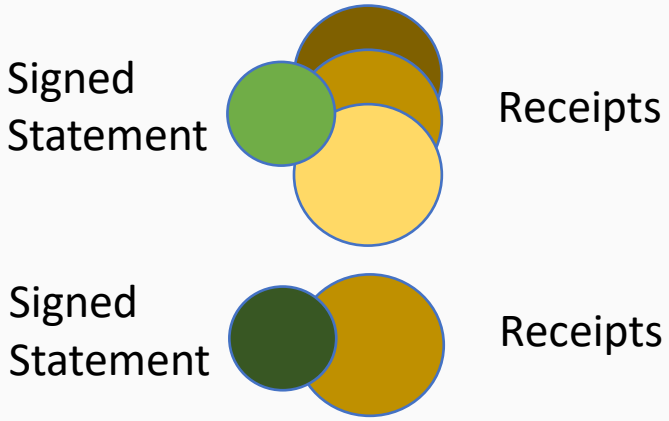
```
curl -X POST https://... /statements
-H "Authorization: Bearer ..."
-F "@path/to/local/statement.xml"
-F "@path/to/local/signed-statement.cbor"

curl -X GET https://... /receipts/urn:uuid:3cb97c51-...-f61b260f245d
-H "Authorization: Bearer ..."
-O -J  #
receipt.cbor
```




```
scitt up-transparency
  …/statement.xml

  …/signed-statement.cbor
  …/receipt.cbor
  …/transparent.cbor
```



Subscribe for Receipts About a Topic

Subscribe to a feed

```
https://... /receipts
https://... /receipts/urn:uuid:3cb97c51-...-f61b260f245d
```

```
https://... /product/.../suppliers
https://... /product/.../ingredients
https://... /product/.../ingredients/456/lab-test-results
https://... /product/.../origin-certificates
```

IETF

Consuming Upstream Feeds

Supplier 1

https://supplier1.example/products/gtin/00611628927558
- Where are they grown?
- Organic or GMO?
- Ethical Labour/ Sustainable Agriculture Certifications?

Supplier 2

https://supplier2.example/products/gtin/0076808516135
- What kind of wheat?
- Where was the wheat grown?
- Where were the noodles made?

Supplier 1

https://supplier1.example/products/gtin/00611628950426
- Where are they grown?
- How long since they were harvested?
- Allergy details?

IETF

Producing a Downstream Feed

https://.../products/gtin/0024739160217

https://.../products/gtin/0024739160217/suppliers
- Which suppliers contribute to this product?
- Have the certifications for any of these suppliers expired recently?
- Has supplier authentication or identity information change recently?

https://.../products/gtin/0051000038852/ingredients
- Have any of these ingredients recently been recalled?
- Are these ingredients from a region that is experiencing natural disasters or political disruptions?

IETF

Using Feeds to Make Trust Decisions

https://vendor.example/products/LDevID/000bd910...27acc9f9478ac

- Has the device been certified?

- Have there been any vulnerabilities reported for this device identity, since the product was packaged and shipped?

- Has the regulatory landscape changed, is the product still considered safe to operate?

- Has the product been recalled?

- Is there an upgrade oath for the installed firmware?

- Is the device still supported?

- Are there any unpatched CVEs?

IETF

Using Feeds to Make Trust Decisions

Wabbit Networks: Net Monitor V1

1. SPDX SBOM
2. CycloneDX SBOM
3. SLSA
4. VEX
5. Vendor Response File
6. VEX (Update)
7. Revocation/Alert
8. New Version Available
9. End of Life Date (EOL)

IETF

Hackathon Report

Jon Geater

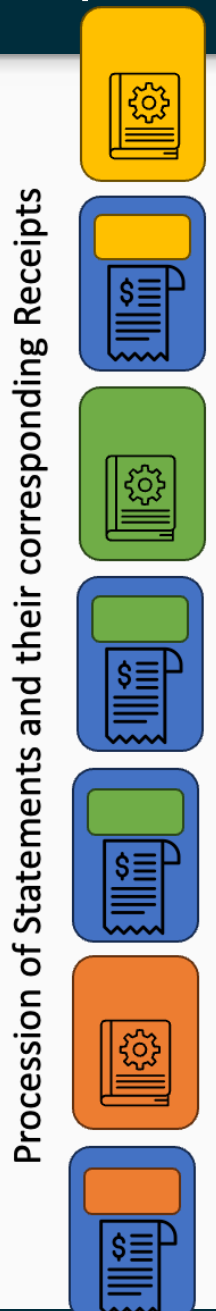
Experience from the Hackathon

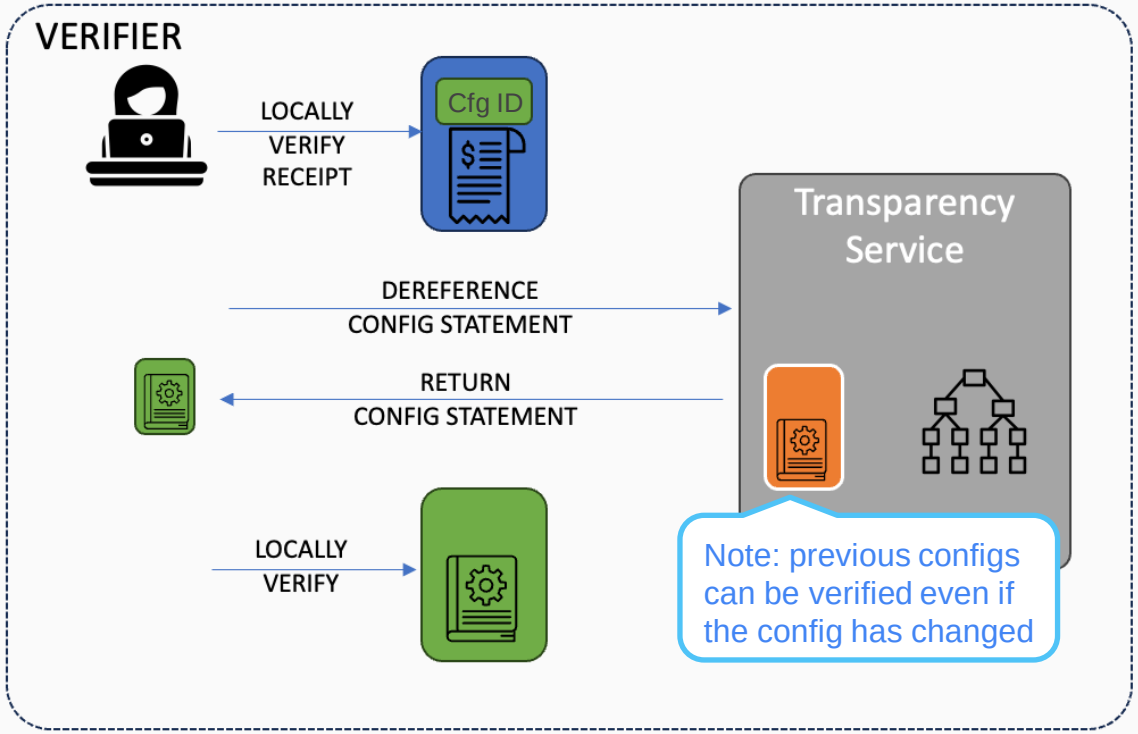
Jon Geater

Hackathon -118

- Strong participation
  - Full table with folks from other groups coming and going
- Much more spec focused than code focused

Spec Progress





- Registration Policies
- Eliminated a complex area and replaced with usage of the existing structures!
- Open questions remain but overall great progress

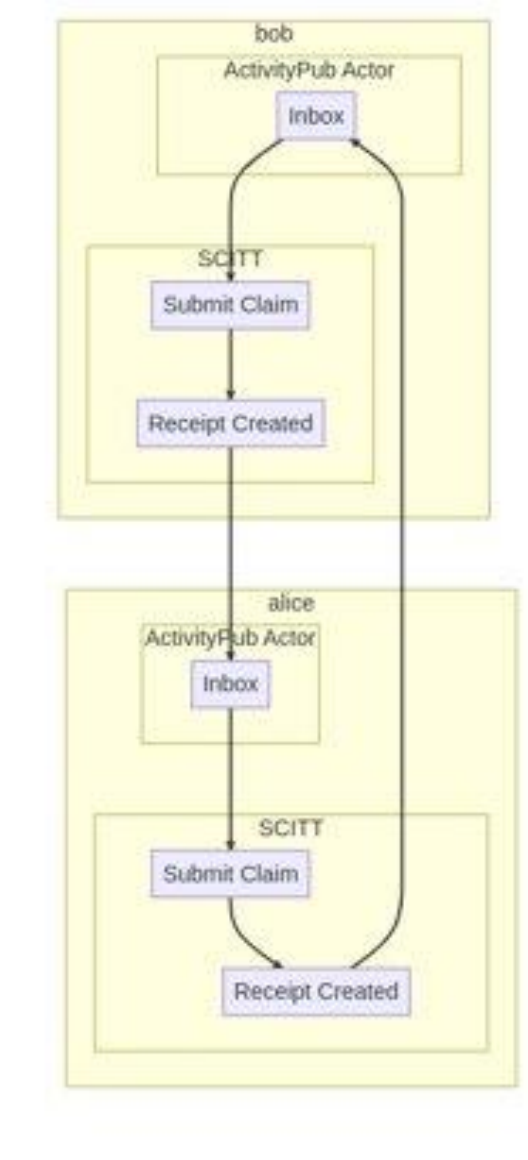
Code Progress

https://github.com/scitt-community/scitt-api-emulator

https://github.com/scitt-community/scitt-examples

- A bit fragmented and distracted by intense discussions on Registration Policies. The good news is a lot of topics have been touched. The trade-off is that nothing quite got finished.
  - Furthered work on federation
  - Furthered work on API access control
  - Proved out DID resolution and verification
  - RKVST implementation eliminated need for translation proxy
  - Begun collecting illustrative examples to help know when the building blocks satisfy the use cases

Federation Hackathon POC Overview



- Federation is
  - service-to-service communication of Transparency Service statements
- Claims registered in federating Transparency Services
  - Trigger a submission attempt within receiving services
  - Evaluate to target TS registration policy to determine applicability of receipt creation

Federation Hackathon POC Demo

```
(.venv) $ scitt-emulator server     --workspace ${HOME}/Documents/fediverse
/scitt_federation_bob/workspace_bob/ --tree-alg CCF --port 6000     --middl
eware scitt_emulator.federation_activitypub_bovine:SCITTFederationActivityP
ubBovine     --middleware-config-path ${HOME}/Documents/fediverse/scitt_fed
eration_bob/config.json
```

```
(.venv) $ scitt-emulator server     --workspace ${HOME}/Documents/fediverse
/scitt_federation_alice/workspace_alice/ --tree-alg CCF --port 7000     --m
iddleware scitt_emulator.federation_activitypub_bovine:SCITTFederationActiv
ityPubBovine     --middleware-config-path ${HOME}/Documents/fediverse/scitt
_federation_alice/config.json --log debug
```

```
(.venv) $ git log -n 1
commit e327d431718554c1e46c1cc136b33af78d9d716f (HEAD -> federation_activitypub_bovine, origin/federation_activitypub_bovine)
Author: John Andersen <johnandersenpdx@gmail.com>
Date:   Mon Nov 6 07:04:30 2023 +0100

    It works! Successful federation of claim submitted to Alice federated to Bob, retreived from Bob and verified using his service parameters

    Asciinema: https://asciinema.org/a/619499
    Signed-off-by: John Andersen <johnandersenpdx@gmail.com>
(.venv) $ bash ~/demo-client.sh
```

```
[0] 0:bash  1:bash* 2:ssh- 3:ssh                                    "hat-1" 09:22 06-Nov-23
```

https://asciinema.org/a/619517

Next Steps and WG Operations

Jon Geater

WG Operations

Seeking to make the WG more effective in its primary goal of producing specs for interoperable building blocks.

A few themes have arisen over the past weeks which we should seek to address together:

- Communications channels
- Interim meeting cadence
- New co-chair

SCITT Drafts

- Software Supply Chain Uses Cases
  https://datatracker.ietf.org/doc/draft-ietf-scitt-software-use-cases/
- SCITT Architecture
  https://datatracker.ietf.org/doc/draft-ietf-scitt-architecture
- Countersigning COSE Envelopes in Transparency Services
  https://datatracker.ietf.org/doc/draft-birkholz-scitt-receipts
- **SC**ITT **R**eference **API** (SCRAPI)
  https://github.com/ietf-scitt/draft-birkholz-scitt-scrapi

Next Steps

- Related IETF drafts
  - RFC 8152 - **C**BOR **O**bject **S**igning and **E**ncryption (COSE)
    https://datatracker.ietf.org/doc/html/rfc8152
  - **R**emote **AT**testation **P**rocedure**S** (RATS)
    https://datatracker.ietf.org/wg/rats/documents/
  - **C**BOR **W**eb **T**oken (CWT) Claims in COSE Headers
    https://datatracker.ietf.org/doc/draft-ietf-cose-cwt-claims-in-headers
- Resources
  - scitt.io
  - scitt-api-emulator
    https://github.com/scitt-community/scitt-api-emulator
  - SCITT REST Emulator
    https://scitt.xyz

IETF

AOB (Open Mic)

Wrap-Up