

IETF 117

# IETF Hackathon – SCITT code hack

IETF 117

22-23 July 2023

San Francisco, California

<date>

22-23 july 2023

san francisco  
37° 47'08.6"N 122°24'37.6"W



I E T F

## SCITT high level promises

A scalable and flexible, decentralized architecture to enhance auditability and accountability across various existing and emerging supply chains. It achieves this goal by enforcing the following complementary security guarantees:

1. Statements made by Issuers about supply chain Artifacts must be identifiable, authentic, and non-repudiable;
2. such Statements must be registered on a secure append-only Log, so that their provenance and history can be independently and consistently audited;
3. Issuers can efficiently prove to any other party the Registration of their Signed Statements; verifying this proof ensures that the Issuer is consistent and non-equivocal when producing Signed Statements.



**I E T F**

## SCITT high level promises

A scalable and flexible, decentralized architecture to enhance auditability and accountability across various existing and emerging supply chains. It achieves this goal by enforcing the following complementary security guarantees:

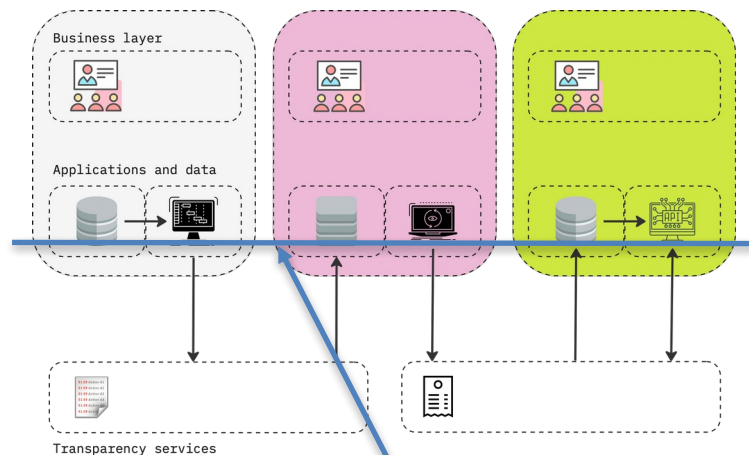
1. Statements made by Issuers about supply chain Artifacts must be identifiable, authentic, and non-repudiable;
2. such Statements must be registered on a secure append-only Log, so that their provenance and history can be independently and consistently audited;
3. Issuers can efficiently prove to any other party the Registration of their Signed Statements; verifying this proof ensures that the Issuer is consistent and non-equivocal when producing Signed Statements.

# Intent of the code hack

Use the RKVST implementation of the SCITT API and COSE Merkle tree receipts to show the practicality of building systems on top of the SCITT building blocks that solve the problems the SCITT WG set out to solve.

## Planned activity:

- Continue building on the open interop client
- Add initial creation of signed claims to the emulator client (not in a very secure way, but just to illustrate the steps required for a generalized solution)
- Experimenting with various application layer payloads, but particularly the Vendor Response Form
- Show different models for storage and retrieval of payloads and receipts.



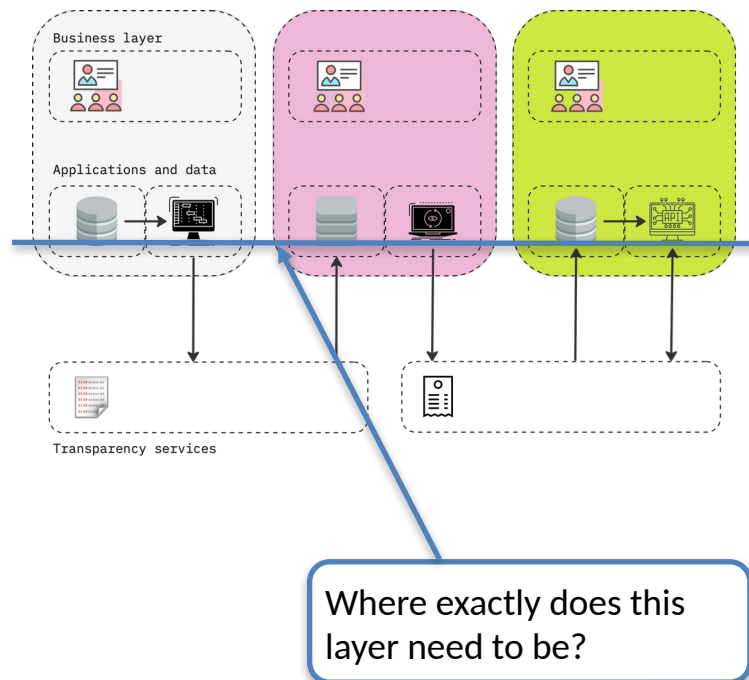
Where exactly does this layer need to be?

# Outcome of the code hack

Use the RKVST implementation of the SCITT API and COSE Merkle tree receipts to show the practicality of building systems on top of the SCITT building blocks that solve the problems the SCITT WG set out to solve.

## Hoped-for outcomes:

- Successful end-to-end demonstration of attesting and verifying a Vendor Response Form
- Driving the spec forward in understanding the different places where company identifiers might show up
- Driving the spec forward in understanding which higher level concepts (especially storage, 'indexing' and 'searching' of stuff) need to be brought into scope, and which stay up in some unspecified application layer.

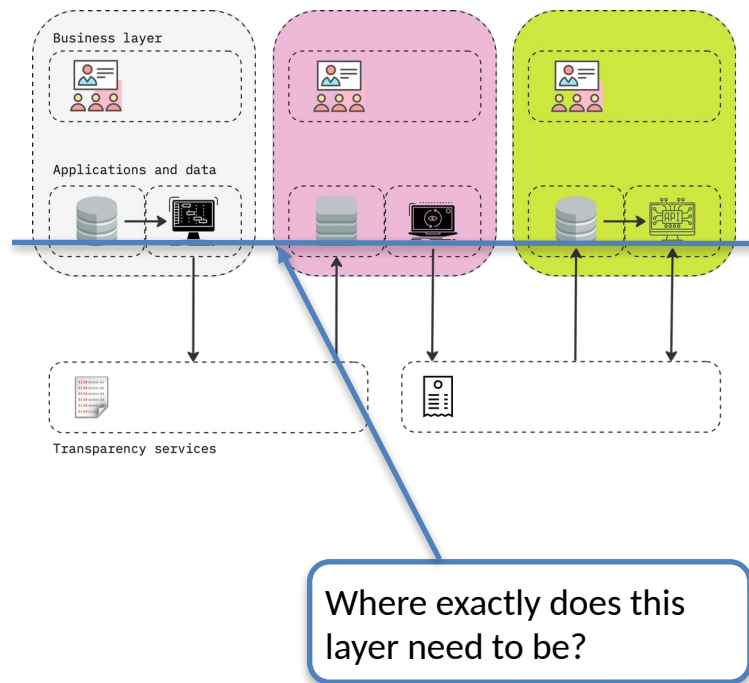


# Outcome of the code hack

Use the RKVST implementation of the SCITT API and COSE Merkle tree receipts to show the practicality of building systems on top of the SCITT building blocks that solve the problems the SCITT WG set out to solve.

## Hoped-for outcomes:

- [?] Successful end-to-end demonstration of attesting and verifying a Vendor Response Form
- [?] Driving the spec forward in understanding the different places where company identifiers might show up
- [?] Driving the spec forward in understanding which higher level concepts (especially storage, 'indexing' and 'searching' of stuff) need to be brought into scope, and which stay up in some unspecified application layer.







# SCITT Registered VRF

▼ VendorResponse:	
VendorLegalName:	"Reliable Energy Analytics LLC"
SupplierID:	"dns:reliableenergyanalytics.com"
StreetAddress:	"23 Linda Drive"
City:	"Westfield"
StateOrProvince:	"Massachusetts"
ZipCode:	"01085"
Country:	"USA"
WebsiteURL:	" <a href="https://reliableenergyanalytics.com/">https://reliableenergyanalytics.com/</a> "
ContactTelephone:	"978-696-1788"
ContactEmail:	"dick@reliableenergyanalytics.com"
ContactPerson:	"Dick Brooks"
DUNSNumber:	"111509681"
NAESBEIRID:	"REAL"
CyberSecPolicyURL:	" <a href="https://softwareassuranceguardian.com/CyberSecPolicy.html">https://softwareassuranceguardian.com/CyberSecPolicy.html</a> "
▼ FinancialDataURL:	" <a href="https://softwareassuranceguardian.com/FinancialData.html">https://softwareassuranceguardian.com/FinancialData.html</a> "
▼ CompanyDataURL:	" <a href="https://softwareassuranceguardian.com/CompanyData.html">https://softwareassuranceguardian.com/CompanyData.html</a> "
▼ Products:	
▼ 0:	
LicensorName:	"Reliable Energy Analytics LLC"
ProductName:	"SAG-PM (TM)"
Version:	"1.2"
▼ SBOM:	
type:	"cycloneDX"
version:	"1.4"
format:	"XML"
▼ DigitalSignatureURL:	" <a href="https://softwareassuranceguardian.com/SAG-PM_SBOM_V1_2.xml.sig">https://softwareassuranceguardian.com/SAG-PM_SBOM_V1_2.xml.sig</a> "
▼ URL:	" <a href="https://softwareassuranceguardian.com/SAG-PM_SBOM_V1_2.xml">https://softwareassuranceguardian.com/SAG-PM_SBOM_V1_2.xml</a> "
SourceLocationURL:	" <a href="https://softwareassuranceguardian.com/sag-pm.zip">https://softwareassuranceguardian.com/sag-pm.zip</a> "
DigitallySigned:	"y"
UnsolvedVulnerabilities:	"N"
▼ KnownVulnInfoURL:	
DocFormat:	"XML"
▼ DigitalSignatureURL:	" <a href="https://softwareassuranceguardian.com/SAG-PM_VulnDisclosure_V1_2.xml.sig">https://softwareassuranceguardian.com/SAG-PM_VulnDisclosure_V1_2.xml.sig</a> "
▼ URL:	" <a href="https://softwareassuranceguardian.com/SAG-PM_VulnDisclosure_V1_2.xml">https://softwareassuranceguardian.com/SAG-PM_VulnDisclosure_V1_2.xml</a> "
▼ SDLCPolicyURL:	" <a href="https://softwareassuranceguardian.com/SAG-PM-V1_2_SDLc-POLICY-NIST.SP.000-218.SSDF-table.pdf">https://softwareassuranceguardian.com/SAG-PM-V1_2_SDLc-POLICY-NIST.SP.000-218.SSDF-table.pdf</a> "
▼ SDLCEvidenceDataURL:	" <a href="https://softwareassuranceguardian.com/SAG-PM_SDLCEvidenceData_V1_2.html">https://softwareassuranceguardian.com/SAG-PM_SDLCEvidenceData_V1_2.html</a> "
▼ CyberSecLabelURL:	" <a href="https://softwareassuranceguardian.com/SAGCTR_inquiry/getSAGScore?FileHash=94E0B27E1995370E9003EE0A0A12D0A7DE2E8D45E6B63C31A97C04215A817186">https://softwareassuranceguardian.com/SAGCTR_inquiry/getSAGScore?FileHash=94E0B27E1995370E9003EE0A0A12D0A7DE2E8D45E6B63C31A97C04215A817186</a> "
CommercialStatus:	"Available"
SupportStatus:	"Supported"
LastModifiedDateTimeUTC:	"2022-09-22T16:23:00"

# Use of SCITT Registered VRF in C-SCRM Risk Assessment

```
Evidence Data for VendorData :
----> SAGDatabaseURL : file:///C:\\Users\\dick\\SAGPM_database\\SAGPM_Vendor_Data.csv
----> Vendor_Name : Reliable Energy Analytics LLC
----> Product_Name : SAG-PM (TM)
----> Product_Version : 1.2
----> Source_Location_URL : https://softwareassuranceguardian.com/sag-pm.zip
----> SL_CN_Name : softwareassuranceguardian.com
----> SL_CA_Name : Go Daddy Secure Certificate Authority - G2
----> Access_Control : BasicAuth
----> NATF_Response_File_URL : https://app.rkvst.io/_api/archivist/v2/attachments/publicassets/517b02c0-1274-40d6-a85d-fe402aa8275e/384d1461-6e2c-4a8b-9abd-f9eb14b6c89c
----> X509SKID : 5DDB670A484E5AFCDC3D7B6435EBC9C8047C75E6
----> PGPfingerprint : 2C17B5D1A50EA9144AAF8DD6D4EB22CCB8A6A3AB
----> NATF_ResponseDigSigURL : https://softwareassuranceguardian.com/SAG-PM_VendorResponse_V1_2.xml.sig
----> VENDOR_FOUND : True
```

# All Evidence Files in SCITT Registered VRF were Downloaded/Used

2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc_SAGPMTM_1,2	7/23/2023 8:02 AM	Text Document	17 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc-CompanyDataURL-File	7/23/2023 7:52 AM	Firefox HTML Doc...	1 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc-CyberSecPolicyURL-File	7/23/2023 7:52 AM	Firefox HTML Doc...	1 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc-FinancialDataURL-File	7/23/2023 7:52 AM	Firefox HTML Doc...	1 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc-KnownVulnInfoDigSigURL-File_SAGPMTM_1,2	7/23/2023 7:52 AM	UNKNOWN File	1 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc-KnownVulnInfoURL-File_SAGPMTM_1,2	7/23/2023 7:52 AM	XML File	35 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338baccMpCmdRun	7/23/2023 7:55 AM	Text Document	5 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc-NATF_Response_File_URL-File_SAGPMTM_1,2	7/23/2023 7:52 AM	UNKNOWN File	3 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc-NATF_ResponseDigSigURL-File_SAGPMTM_1,2	7/23/2023 7:52 AM	UNKNOWN File	1 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc-SAGScoreLabel	7/23/2023 8:02 AM	PNG File	37 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc-SAGScorethumbprint	7/23/2023 8:02 AM	PNG File	3 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc-SBOM-SAG-PM_SBOM_V1_2	7/23/2023 7:52 AM	XML File	45 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc-SBOMsignature-File_SAGPMTM_1,2	7/23/2023 7:52 AM	UNKNOWN File	1 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc-SDLCEvidenceDataURL-File_SAGPMTM_1,2	7/23/2023 7:52 AM	Firefox HTML Doc...	1 KB
2023-07-23_11_52_02_391120_ONLINE_c08114b9-1d97-45ab-aab1-72705338bacc-SDLCPolicyURL-File_SAGPMTM_1,2	7/23/2023 7:52 AM	Adobe Acrobat D...	233 KB

DOWNLOADED SCITT REGISTERED VRF FILE

# Outcomes of the code hack

## POSITIVES

- VRF use case end-to-end proven [?]
- Other very different use cases discussed and also seem to be supported without much fuss
- Core fundamentals continue to be strong
- Highlighted (relatively) simple next step in terms of Feed specification

## CHALLENGES

- Not nearly as much time to hack as I'd hoped – didn't get interoperable submission working, because...
- ...Feeds are a moving target (but at least they ARE a target [?])
- Client/emulator risks rotting: consider significant maintenance and quality updates alongside new API spec doc