An Architecture for Trustworthy and Transparent Digital Supply Chains
draft-birkholz-scitt-architecture-00

Abstract

Traceability of physical and digital artifacts in supply chains is a long-standing, but increasingly serious security concern. The rise in popularity of verifiable data structures as a mechanism to make actors more accountable for breaching their compliance promises has found some successful applications to specific use cases (such as the supply chain for digital certificates), but lacks a generic and scalable architecture that can address a wider range of use cases.

This memo defines a generic and scalable architecture to enable transparency across any supply chain with minimum adoption barriers for producers (who can register their claims on any TS, with the guarantee that all consumers will be able to verify them) and enough flexibility to allow different implementations of Transparency Services with various auditing and compliance requirements.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 September 2022.
Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction ....................................................... 3
   1.1. Requirements Notation ...................................... 5
2. Use Cases .......................................................... 5
   2.1. Software Bill of Materials (SBOM) .......................... 5
   2.2. Confidential Computing ...................................... 6
   2.3. Cold Chains for Seafood .................................... 7
3. Terminology ....................................................... 7
4. Definition of Transparency ........................................ 8
5. Architecture Overview ............................................. 9
   5.1. Claim Issuance ............................................... 10
      5.1.1. Issuer Identity ......................................... 11
      5.1.2. Naming Artifacts ...................................... 11
      5.1.3. Claim Metadata ......................................... 11
   5.2. Transparency Service (TS) .................................. 12
      5.2.1. Service Identity, Remote Attestation, and Keying ... 12
      5.2.2. Registration Policies .................................. 13
      5.2.3. Ledger Security Requirements .......................... 15
   5.3. Verifying Transparent Claims ............................... 17
6. Claim Issuance, Registration, and Verification ..................... 18
   6.1. Envelope and Claim Format .................................. 18
   6.2. Claim Issuance ............................................... 20
   6.3. Registering Signed Claims .................................. 20
   6.4. Validation of Transparent Claims ........................... 21
7. Federation .......................................................... 22
8. Transparency Service API ........................................... 22
   8.1. Messages .................................................... 22
      8.1.1. Register Signed Claims ................................. 22
      8.1.2. Retrieve Registration Receipt ......................... 23
9. Privacy Considerations ............................................. 24
10. Security Considerations .......................................... 24
11. IANA Considerations .............................................. 25
12. References ........................................................ 25
1. Introduction

This document describes a scalable and flexible decentralized architecture to enhance auditability and accountability in 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 ledger 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 claims; verifying this proof ensures that the issuer is consistent and non-equivocal when making claims.

The first guarantee is achieved by requiring issuers to sign their statements and associated metadata using a distributed public key infrastructure. The second guarantee is achieved by storing the signed statement on an immutable, append-only, transparent ledger. The last guarantee is achieved by implementing the ledger using a verifiable data structure (such as a Merkle Tree), and by requiring a transparency service (TS) that operates the ledger to endorse its state at the time of registration.

The guarantees and techniques used in this document generalize those of Certificate Transparency [RFC9162], which can be re-interpreted as an instance of this architecture for the supply chain of X.509 certificates. However, the range of use cases and applications in this document is much broader, which requires much more flexibility in how each TS implements and operates its ledger. Each service may enforce its own policy for authorizing entities to register their claims on the TS. Some TS may also enforce access control policies to limit who can audit the full ledger, or keep some information on the ledger encrypted. Nevertheless, it is critical to provide global interoperability for all TS instances as the composition and configuration of involved supply chain entities and their system components is ever changing and always in flux.
A TS provides visibility into claims issued by supply chain entities and their sub-systems. These claims are called Digital Supply Chain Artifacts (DSCA). A TS vouches for specific and well-defined metadata about these DSCAs. Some metadata is selected (and signed) by the issuer, indicating, e.g., "who issued the DSCA" or "what type of DSCA is described" or "what is the DSCA version"; whereas additional metadata is selected (and countersigned) by the TS, indicating, e.g., "when was the DSCA registered in the ledger". The DSCA contents can be opaque to the TS, if so desired: it is the metadata that must always be transparent in order to warrant trust.

Transparent claims provide a common basis for holding issuers accountable for the DSCA they release and (more generally) principals accountable for auxiliary claims they make about DSCAs. Hence, issuers may register new claims about their artifacts, but they cannot delete or alter earlier claims, or hide their claims from third parties such as auditors.

Trust in the TS itself is supported both by protecting their implementation (using, for instance, replication, trusted hardware, and remote attestation of systems) and by enabling independent audits of the correctness and consistency of its ledger, thereby holding the organization accountable that operates it. Unlike CT, where independent auditors are responsible for enforcing the consistency of multiple independent instances of the same global ledger, we require each TS to guarantee the consistency of its own ledger (for instance, through the use of a consensus algorithm between replicas of the ledger), but assume no consistency between different transparency services.

The TS specified in this architecture caters to two types of audiences:

1. DSCA Issuers: entities, stakeholders, and users involved in supply chain interactions that need to release DSCAs to a definable set of peers; and

2. DSCA Consumers: entities, stakeholders, and users involved in supply chain interactions that need to access, validate, and trust DSCAs.
DSCA Issuers rely on being discoverable and represented as the responsible parties for released DSCAs by the TS in a believable manner. Analogously, DSCA Consumers rely on verifiable trustworthiness assertions associated with DSCAs and their processing in a believable manner. If trust can be put into the operations that record DSCAs in a secure, append-only ledger via an online operation, the same trust can be put into a corresponding receipt that is the result of these online operations issued by the TS and that can be validated in offline operations.

The TS specified in this architecture can be implemented by various different types of services in various types of languages provided via various variants of API layouts.

The global interoperability enabled and guaranteed by the TS is enabled via core components (architectural constituents) that come with prescriptive requirements (that are typically hidden away from the user audience via APIs). The core components are based on the Concise Signing and Encryption standard specified in [RFC8152], which is used to sign released DSCAs and to build and maintain a Merkle tree that functions as the append-only ledger for DSCAs. The format and verification process for ledger-based transparency receipts are described in [I-D.birkholz-scitt-receipts].

1.1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Use Cases

This section presents representative and solution-agnostic use cases to illustrate the scope of SCITT and the processing of Digital Supply Chain Artifacts.

2.1. Software Bill of Materials (SBOM)

As the ever increasing complexity of large software projects requires more modularity and abstractions to manage them, keeping track of their full Trusted Computing Base (TCB) is becoming increasingly difficult. Each component may have its own set of dependencies and libraries. Some of these dependencies are binaries, which means their TCB depends not only on their source, but also on their build environment (compilers and tool-chains). Besides, many source and binary packages are distributed through various channels and
repositories that may not be trustworthy.

Software Bills of Materials (SBOM) help the authors, packagers, distributors, auditors and users of software understand its provenance and who may have the ability to introduce a vulnerability that can affect the supply chain downstream. However, the usefulness of SBOM in protecting end users is limited if supply chain actors cannot be held accountable for their contents. For instance, consider a package repository for an open source operating system distribution. The operator of this repository may decide to provide a malicious version of a package only to users who live in a specific country. They can write two equivocal SBOMs for the honest and backdoored versions of the package, so that nobody outside the affected country can discover the malicious version, but victims are not aware they are being targeted.

2.2. Confidential Computing

Confidential Computing can leverage hardware-protected trusted execution environments (TEEs) to operate cloud services that protect the confidentiality of data that they process. It relies on remote attestation, which allows the service to prove to remote users what is the hash of its software, as measured and signed by the hardware.

For instance, consider a speech recognition service that implements machine learning inference using a deep neural network model. The operator of the service wants to prove to its users that the service preserves the user’s privacy, that is, the submitted recordings can only be used to detect voice commands but no other purpose (such as storing the recordings or detecting mentions of brand names for advertisement purposes). When the user connects to the TEE implementing the service, the TEE presents attestation evidence that includes a hardware certificate and a software measurement for their task; the user verifies this evidence before sending its recording.

But how can users verify the software measurement for their task? And how can operators update their service, e.g., to mitigate security vulnerabilities or improve accuracy, without first convincing all users to update the measurements they trust?

A supply chain that maintains a transparent record of the successive software releases for machine-learning models and runtimes, recording both their software measurements and their provenance (source code, build reports, audit reports,...) can provide users with the information they need to authorize these tasks, while holding the service operator accountable for the software they release for them.
2.3. Cold Chains for Seafood

Once seafood is caught, its quality is determined -- amongst other criteria -- via the integrity of a cold chain that ensures a regulatory perspective freshness mandating a continuous storing temperature between 1 °C and 0 °C (or -18 °C and lower for frozen seafood). The temperature is recorded by cooling units adhering to certain compliance standards automatically. Batches of seafood can be split or aggregated before arriving in a shelf so that each unit can potentially have a potentially unique cold chain record whose transparency impacts the accuracy of the shelf-life associated with it. Especially in early links of the supply chain, Internet connection or sophisticated IT equipment are typically not available and sometimes temperature measurements are recorded manually and digital records are created in hindsight.

3. Terminology

The terms defined in this section have special meaning in the context of Supply Chain Integrity, Transparency, and Trust throughout this document. When used in text, the corresponding terms are capitalized. To ensure readability, only a core set of terms is included in this section.

Artifact: the physical or non-physical item that is moving along the supply chain.

Statement: any serializable information about an Artifact. To help interpretation of Statements, they must be tagged with a media type (as specified in [RFC6838]).

Claim: an identifiable and non-repudiable Statement about an Artifact made by an Issuer. In SCITT, Claims are encoded as COSE signed objects; the payload of the COSE structure contains the Statement.

Issuer: creator of Claims submitted to a Transparency Service for Registration. The Issuer may be the owner or author of the Artifact, or a completely independent third party.

Envelope: the metadata added to the Statement by the Issuer to make it a Claim. It contains the identity of the Issuer and other information to help Verifiers identify the Artifact referred in the Statement. A Claim binds the Envelope to the Statement. In COSE, the Envelope consists of protected headers.

Feed: An identifier chosen by the Issuer for the Artifact. For
every Issuer and Feed, the Ledger on a Transparency Service contains a sequence of Claims about the same Artifact. In COSE, Feed is one header attributes in the protected header of the Envelope.

Ledger: the verifiable data structure that stores Claims in a transparency service. SCITT supports multiple Ledger formats to accommodate different transparency service implementations, such as historical Merkle Trees and sparse Merkle Trees.

Transparency Service: the entity that maintains and extends the Ledger, and endorses its state. A Transparency Service can be a complex distributed system, and SCITT requires the TS to provide many security guarantees about its Ledger. The identity of a TS is captured by a public key that must be known by Verifiers in order to validate Receipts.

Receipt: a Receipt is a special form of COSE countersignature for Claims that embeds cryptographic evidence that the Claim is recorded in the Ledger. It consists of a Ledger-specific inclusion proof, a signature by the Transparency Service of the state of the Ledger, and additional metadata (contained in the countersignature protected headers) to assist in auditing.

Registration: the process of submitting a Claim to a Transparency Service, applying its registration policy, storing it in the Ledger and producing the Receipt returned to the submitter.

Transparent Claim: a Claim that is augmented with a Receipt of its registration. A Transparent Claim remains a valid Claim (as the Receipt is carried in the countersignature), and may be registered again in a different TS.

Verifier: the entity that consumes Transparent Claims, verifying their proofs and inspecting their Statements, either before using their Artifacts, or later to audit their supply chain.

4. Definition of Transparency

In this document, we use a definition of transparency built over abstract notions of Ledgers and Receipts. Existing transparency systems such as Certificate Transparency are instances of this definition.

A Claim is an identifiable and non-repudiable Statement made by an Issuer. The Issuer selects additional metadata and attaches a proof of endorsement (in most cases, a signature) using the identity key of the Issuer that binds the Statement and its metadata. Claims can be
made transparent by attaching a proof of Registration by a TS, in the form of a Receipt that countersigns the Claim and witnesses its inclusion in the Ledger of a TS. By extension, we may say an Artifact (e.g. a firmware binary) is transparent if it comes with one or more Transparent Claims from its author or owner, though the context should make it clear what type of Claim is expected for a given Artifact.

Transparency does not prevent dishonest or compromised Issuers, but it holds them accountable: any Artifact that may be used to target a particular user that checks for Receipts must have been recorded in the tamper-proof Ledger, and will be subject to scrutiny and auditing by other parties.

Transparency is implemented by a Ledger that provides a consistent, append-only, publicly available record of entries. Implementations of TS may protect their Ledger using a combination of trusted hardware, replication and consensus protocols, and cryptographic evidence. A Receipt is an offline, universally-verifiable proof that an entry is recorded in the edger. Receipts do not expire, but it is possible to append new entries that subsume older entries.

Anyone with access to the Ledger can independently verify its consistency and review the complete list of Claims registered by each Issuer. However, the Ledgers of separate Transparency Services are generally disjoint, though it is possible to take a Claim from one Ledger and register it again on another (if its policy allows it), so the authorization of the Issuer and of the Ledger by the Verifier of the Receipt are generally independent.

Reputable Issuers are thus incentivized to carefully review their Statements before signing them into Claims. Similarly, reputable TS are incentivized to secure their Ledger, as any inconsistency can easily be pinpointed by any auditor with read access to the Ledger. Some Ledger formats may also support consistency auditing through Receipts, that is, given two valid Receipts the TS may be asked to produce a cryptographic proof that they are consistent. Failure to produce this proof can indicate that the TS operator misbehaved.

5. Architecture Overview
The SCITT architecture consists of a very loose federation of Transparency Services, and a set of common formats and protocols for issuing, registering and auditing Claims. In order to accommodate as many TS implementations as possible, this document only specifies the format of Claims (which must be used by all Issuers) and a very thin wrapper format for Receipts, which specifies the TS identity and the Ledger algorithm. Most of the details of the Receipt’s contents are specific to the Ledger algorithm. The [I-D.birkholz-scitt-receipts] document defines two initial Ledger algorithms (for historical and sparse Merkle Trees), but other Ledger formats (such as blockchains, or hybrid historical and indexed Merkle Trees) may be proposed later.

In this section, we describe at a high level the three main roles and associated processes in SCITT: Issuers and the Claim issuance process, transparency Ledgers and the Claim Registration process, and Verifiers and the Receipt validation process.

5.1. Claim Issuance
5.1.1. Issuer Identity

Before an Issuer is able to produce Claims, it must first create its decentralized identifier (https://www.w3.org/TR/did-core) (also known as a DID). A DID can be _resolved_ into a _key manifest_ (a list of public keys indexed by a _key identifier_) using many different DID methods.

Issuers MAY choose the DID method they prefer, but with no guarantee that all TS will be able to register their Claim. To facilitate interoperability, all Transparency Service implementations SHOULD support the did:web method from [https://w3c-ccg.github.io/did-method-web/]. For instance, if the Issuer publishes its manifest at https://sample.issuer/user/alice/did.json, the DID of the Issuer is did:web:sample.issuer:user:alice.

Issuers SHOULD use consistent decentralized identifiers for all their Artifacts, to simplify authorization by Verifiers and auditing. They MAY update their DID manifest, for instance to refresh their signing keys or algorithms, but they SHOULD NOT remove or change any prior keys unless they intend to revoke all Claims issued with those keys. This DID appears in the Issuer header of the Claim’s Envelope, while the version of the key from the manifest used to sign the Claim is written in the kid header.

5.1.2. Naming Artifacts

Many Issuers issue Claims about different Artifacts under the same DID, so it is important for everyone to be able to immediately recognize by looking at the Envelope of a Claim what Artifact it is referring to. This information is stored in the Feed header of the Envelope. Issuers MAY use different signing keys (identified by kid in the resolved key manifest) for different Artifacts, or sign all Claims under the same key.

5.1.3. Claim Metadata

Besides Issuer, Feed and kid, the only other mandatory metadata in the Claim is the type of the Payload, indicated in the cty Envelope header. However, this set of mandatory metadata is not sufficient to express many important Registration policies. For example, a Ledger may only allow a Claim to be registered if it was signed recently. While the Issuer is free to add any information in the payload of the Claim, the TS (and most of its auditor) can only be expected to interpret information in the Envelope.
Such metadata, meant to be interpreted by the TS during Registration policy evaluation, should be added to the reg_info header. While the header MUST be present in all Claims, its contents consist of a map of named attributes. Some attributes (such as the Issuer’s timestamp) are standardized with a defined type, to help uniformize their semantics across TS. Others are completely customizable and may have arbitrary types. In any case, all attributes are optional so the map MAY be empty.

5.2. Transparency Service (TS)

The role of TS can be decomposed into several major functions. The most important is maintaining a Ledger, the verifiable data structure that records Claims, and enforcing a Registration policy. It also maintains a service key, which is used to endorse the state of the Ledger in Receipts. All TS MUST expose standard endpoints for Registration of Claims and Receipt issuance, which is described in Section 8.1. Each TS also defines its Registration policy, which MUST apply to all entries in the Ledger.

The combination of Ledger, identity, Registration policy evaluation, and Registration endpoint constitute the trusted part of the TS. Each of these components SHOULD be carefully protected against both external attacks and internal misbehavior by some or all of the operators of the TS. For instance, the code for policy evaluation, Ledger extension and endorsement may be protected by running in a TEE; the Ledger may be replicated and a consensus algorithm such as Practical Byzantine Fault Tolerance (pBFT [PBFT]) may be used to protect against malicious or vulnerable replicas; threshold signatures may be use to protect the service key, etc.

Beyond the trusted components, Transparency Services may operate additional endpoints for auditing, for instance to query for the history of Claims made by a given Issuer and Feed. Implementations of TS SHOULD avoid using the service identity and extending the Ledger in auditing endpoints; as much as practical, the Ledger SHOULD contain enough evidence to re-construct verifiable proofs that the results returned by the auditing endpoint are consistent with a given state of the Ledger.

5.2.1. Service Identity, Remote Attestation, and Keying

Every TS MUST have a public service identity, associated with public/private key pairs for signing on behalf of the service. In particular, this identity must be known by Verifiers when validating a Receipt.
This identity should be stable for the lifetime of the service, so that all Receipts remain valid and consistent. The TS operator MAY use a distributed identifier as their public service identity if they wish to rotate their keys, if the Ledger algorithm they use for their Receipt supports it. Other types of cryptographic identities, such as parameters for non-interactive zero-knowledge proof systems, may also be used in the future.

The TS SHOULD provide evidence that it is securely implemented and operated, enabling remote authentication of the hardware platforms and/or software TCB that run the TS. This additional evidence SHOULD be recorded in the Ledger and presented on demand to Verifiers and auditors.

For example, consider a TS implemented using a set of replicas, each running within its own hardware-protected trusted execution environments (TEEs). Each replica SHOULD provide a recent attestation report for its TEE, binding their hardware platform to the software that runs the Transparency Service, the long-term public key of the service, and the key used by the replica for signing Receipts. This attestation evidence SHOULD be supplemented with transparency Receipts for the software and configuration of the service, as measured in its attestation report.

5.2.2. Registration Policies

*Editor’s note*

The initial version of this document assumes Registration policies are set for the lifetime of the Ledger, and that they apply to all Issuers and Feeds uniformly. There is an ongoing discussion on how to make the design more flexible to allow per-Issuer and per-Feed Registration policies, and whether such policies should be updatable or if a policy change requires a Feed change. Please contribute your comments to the SCITT mailing list.

Each TS is initially configured with a set of Registration policies, which will be applied for the lifetime of the Ledger. A Registration policy represents a predicate that takes as input the current Ledger and the Envelope of a new Claim to register (including the reg_info header which contains customizable additional attributes), and returns a Boolean decision on whether the Claim should be included on the Ledger or not. A TS MUST ensure that all its Registration policies return a positive decision before adding a Claim to the Ledger.
While Registration policies are a burden for Issuers (some may require them to maintain state to remember what they have signed before) they support stronger transparency guarantees, and they greatly help Verifiers and auditors in making sense of the information on the Ledger. (This is particularly relevant for parties that verify Receipts on their own, without accessing the Ledger.) For instance, if a TS doesn’t apply any policy, Claims may be registered in a different order than they have been issued, and old Claims may be replayed, which makes it difficult to understand the logical history of an Artifact, or to prevent rollback attacks.

There are two kinds of Registration policies: (1) named policies have standardized semantics that are uniform across all implementations of SCITT Transparency Services, while (2) custom policies are opaque and may contain pointers to (or even inlined) policy descriptions (declarative or programmable).

Transparency services MUST advertise the Registration policies enforced by their service, including the list of reg_info attributes they require, both to minimize the risk of rejecting Claims presented by Issuers, and to advertise the properties implied by Receipt verification. Implementations of Receipt Verifiers SHOULD persist the list of Registration policies associated with a service identity, and return the list of Registration policies as an output of Receipt validation. Auditors MUST re-apply the Registration policy of every entry in the Ledger to ensure that the Ledger applied them correctly.

Custom policies may use additional information present in the Ledger outside of Claims. For instance, Issuers may have to register on the TS before Claims can be accepted; a custom policy may be used to enforce access control to the Transparency Service. Verifying the signature of the Issuer is also a form of Registration policy, but it is globally enforced in order to separate authentication and authorization, with policy only considering authentic inputs.

Table 1 defines an initial set of named policies that TS may decide to enforce. This may be evolved in future drafts.
<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Required attributes</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>TimeLimited</td>
<td>register_by: uint</td>
<td>Returns true if now () &lt; register_by. The Ledger MUST store the Ledger time at Registration along with the Claim, and SHOULD indicate it in Receipts.</td>
</tr>
<tr>
<td>Sequential</td>
<td>sequence_no: uint</td>
<td>First, lookup in the Ledger for Claims with the same Issuer and Feed. If at least one is found, returns true if and only if the sequence_no of the new Claim is the highest sequence_no in the existing Claims incremented by one. Otherwise, returns true if and only if sequence_no = 0.</td>
</tr>
<tr>
<td>Temporal</td>
<td>issuance_ts: uint</td>
<td>Returns true if and only if there is no Claim in the Ledger with the same Issuer and Feed with a greater issuance_ts.</td>
</tr>
<tr>
<td>NoReplay</td>
<td>None</td>
<td>Returns true if and only if the Claim doesn’t already appear in the Ledger.</td>
</tr>
</tbody>
</table>

Table 1: An Initial Set of Named Policies

5.2.3. Ledger Security Requirements

There are many different candidate verifiable data structures that may be used to implement the Ledger, such as chronological Merkle Trees, sparse/indexed Merkle Trees, full blockchains, and many other variants. We only require the Ledger to support concise Receipts (i.e. whose size grows at most logarithmically in the number of entries in the Ledger). This does not necessarily rule out blockchains as a Ledger, but may necessitate advanced Receipt schemes that use arguments of knowledge and other verifiable computing techniques.

Since the details of how to verify a Receipt are specific to the data structure, we do not specify any particular Ledger format in this document. Instead, we propose two initial formats for Ledgers in...
[I-D.birkholz-scitt-receipts] using historical and sparse Merkle Trees. Beyond the format of Receipts, we require generic properties that should be satisfied by the components in the TS that have the ability to write to the Ledger.

5.2.3.1. Finality

The Ledger is append-only: once a Claim is registered, it cannot be modified, deleted, or moved. In particular, once a Receipt is returned for a given Claim, the Claim and any preceding entry in the Ledger become immutable, and the Receipt provides universally-verifiable evidence of this property.

5.2.3.2. Consistency

There is no fork in the Ledger: everyone with access to its contents sees the same sequence of entries, and can check its consistency with any Receipts they have collected. TS implementations SHOULD provide a mechanism to verify that the state of the Ledger encoded in an old Receipt is consistent with the current Ledger state.

5.2.3.3. Replayability and Auditing

Everyone with access to the Ledger can check the correctness of its contents. In particular,

* the TS defines and enforces deterministic Registration policies that can be re-evaluated based solely on the contents of the Ledger at the time of registration, and must then yield the same result.

* The ordering of entries, their cryptographic contents, and the Ledger governance may be non-deterministic, but they must be verifiable.

* The TS SHOULD store evidence about the resolution of distributed identifiers into manifests.

* The TS MAY additionally support verifiability of client authentication and access control.
5.2.3.4. Governance and Bootstrapping

The TS needs to support governance, with well-defined procedures for allocating resources to operate the Ledger (e.g., for provisioning trusted hardware and registering their attestation materials in the Ledger) and for updating its code (e.g., relying on Transparent Claims about code updates, secured on the Ledger itself, or on some auxiliary TS).

Governance procedures, their auditing, and their transparency are implementation specific. The TS SHOULD document them.

* Governance may be based on a consortium of members that are jointly responsible for the TS, or automated based on the contents of an auxiliary governance TS.

* Governance typically involves additional records in the Ledger to enable its auditing. Hence, the Ledger may contain both Transparent Claims and governance entries.

* Issuers, Verifiers, and third-party auditors may review the TS governance before trusting the service, or on a regular basis.

5.3. Verifying Transparent Claims

For a given Artifact, Verifiers take as trusted inputs:

1. the distributed identifier of the Issuer (or its resolved key manifest),

2. the expected name of the Artifact (i.e. the Feed),

3. the list of service identities of trusted TS.

When presented with a Transparent Claim for the Artifact, they verify its Issuer identity, signature, and Receipt. They may additionally apply a validation policy based on the protected headers present both in the Envelope or in the countersignature and the Statement itself, which may include security-critical Artifact-specific details.

Some Verifiers may systematically resolve the Issuer DID to fetch their latest DID document. This strictly enforces the revocation of compromised keys: once the Issuer has updated its document to remove a key identifier, all Claims signed with this kid will be rejected. However, others may delegate DID resolution to a trusted third party and/or cache its results.
Some Verifiers may decide to skip the DID-based signature verification, relying on the TS’s Registration policy and the scrutiny of other Verifiers. Although this weakens their guarantees against key revocation, or against a corrupt TS, they can still keep the Receipt and blame the Issuer or the TS at a later point.

6. Claim Issuance, Registration, and Verification

This section details the interoperability requirements for implementers of Claim issuance and validation libraries, and of Transparency Services.

6.1. Envelope and Claim Format

The formats of Claims and Receipts are based on CBOR Object Signing and Encryption (COSE). The choice of CBOR is a trade-off between safety (in particular, non-malleability: each Claim has a unique serialization), ease of processing and availability of implementations.

At a high-level that is the context of this architecture, a Claim is a COSE single-signed object (i.e. COSE_Sign1) that contains the correct set of protected headers. Although Issuers and relays may attach unprotected headers to Claims, Transparency Services and Verifiers MUST NOT rely on the presence or value of additional unprotected headers in Claims during Registration and validation.

All Claims MUST include the following protected headers:

* algorithm (label: 1): Asymmetric signature algorithm used by the Claim Issuer, as an integer, for example -35 for ECDSA with SHA-384, see COSE Algorithms registry (https://www.iana.org/assignments/cose/cose.xhtml);

* Issuer (label: TBD, to be registered): DID (Decentralized Identifier, see W3C Candidate Recommendation (https://www.w3.org/TR/did-core/)) of the signer, as a string, for example did:web:example.com;

* Feed (label: TBD): the Issuer’s name for the Artifact, as a string;

* payload type (label: 3): Media type of payload as a string, for example application/spdx+json

* Registration policy info (label: TBD): a map of additional attributes to help enforce Registration policies;
* DID key selection hint (label: TBD): a DID method-specific selector for the signing key, as a bytestring.

Additionally, Claims MAY carry the following unprotected headers:

* Receipts (label: TBD, to be registered): Array of Receipts, defined in [I-D.birkholz-scitt-receipts]

In CDDL [RFC8610] notation, the Envelope is defined as follows:

SCITT_Envelope = COSE_Sign1_Tagged

COSE_Sign1_Tagged = #6.18(COSE_Sign1)

COSE_Sign1 = [
  protected : bstr .cbor Protected_Header,
  unprotected : Unprotected_Header,
  payload : bstr,
  signature : bstr
]

Reg_Info = {
  ? "register_by": uint,
  ? "sequence_no": uint,
  ? "issuance_ts": uint,
  * tstr => any
}

; All protected headers are mandatory, to protect against faulty implementations of COSE
; that may accidentally read a missing protected header from the unprotected headers.

Protected_Header = {
  1 => int ; algorithm identifier
  3 => tstr ; payload type
  258 => tstr ; DID of Issuer
  259 => tstr ; Feed
  260 => Reg_Info ; Registration policy info
  261 => bstr ; key selector
}

Unprotected_Header = {
  ? 257 => SCITT_Receipt / [+ SCITT_Receipt]
}
6.2. Claim Issuance

There are many types of Statements (such as SBOMs, malware scans, audit reports, policy definitions) that Issuers may want to turn into Claims. The Issuer must first decide on a suitable format to serialize the Statement, such as: - JSON-SPDX - CBOR-SPDX - SWID - CoSWID - CycloneDX - in-toto - SLSA

Once the Statement is serialized with the correct content type, the Issuer should fill in the attributes for the Registration policy information header. From the Issuer’s perspective, using attributes from named policies ensures that the Claim may only be registered on Transparency Services that implement the associated policy. For instance, if a Claim is frequently updated, and it is important for Verifiers to always consider the latest version, Issuers SHOULD use the sequence_no or issuer_ts attributes.

Once all the Envelope headers are set, the Issuer MAY use a standard COSE implementation to produce the serialized Claim (the SCITT tag of COSE_Sign1_Tagged is outside the scope of COSE, and used to indicate that a signed object is a Claim).

6.3. Registering Signed Claims

The same Claim may be independently registered in multiple TS. To register a Claim, the service performs the following steps:

1. Client authentication. This is implementation-specific, and MAY be unrelated to the Issuer identity. Claims may be registered by a different party than their Issuer.

2. Issuer identification. The TS MUST store evidence of the DID resolution for the Issuer protected header of the Envelope and the resolved key manifest at the time of Registration for auditing. This MAY require that the service resolve the Issuer DID and record the resulting document, or rely on a cache of recent resolutions.

3. Envelope signature verification, as described in COSE signature, using the signature algorithm and verification key of the Issuer DID document.

4. Envelope validation. The service MUST check that the Envelope has a payload and the protected headers listed above. The service MAY additionally verify the payload format and content.
5. Apply Registration policy: for named policies, the TS should check that the required Registration info attributes are present in the Envelope and apply the check described in Table 1. A TS MUST reject Claims that contain an attribute used for a named policy that is not enforced by the service. Custom Claims are evaluated given the current Ledger state and the entire Envelope, and MAY use information contained in the attributes of named policies.

6. Commit the new Claim to the Ledger

7. Sign and return the Receipt.

The last two steps MAY be shared between a batch of Claims recorded in the Ledger.

The service MUST ensure that the Claim is committed before releasing its Receipt, so that it can always back up the Receipt by releasing the corresponding entry in the Ledger. Conversely, the service MAY re-issue Receipts for the Ledger content, for instance after a transient fault during Claim Registration.

6.4. Validation of Transparent Claims

This section provides additional implementation considerations, the high-level validation algorithm is described in Section 5.3, with the Ledger-specific details of checking Receipts are covered in [I-D.birkholz-scitt-receipts].

Before checking a Claim, the Verifier must be configured with one or more identities of trusted Transparency Services. If more than one service is configured, the Verifier MUST return which service the Claim is registered on.

In some scenarios, the Verifier already expects a specific Issuer and Feed for the Claim, while in other cases they are not known in advance and can be an output of validation. Verifiers SHOULD offer a configuration to decide if the Issuer’s signature should be locally verified (which may require a DID resolution, and may fail if the manifest is not available or if the key is revoked), or if it should trust the validation done by the TS during Registration.

Some Verifiers MAY decide to locally re-apply some or all of the Registration policies if they have limited trust in the TS. In addition, Verifiers MAY apply arbitrary validation policies after the signature and Receipt have been checked. Such policies may use as input all information in the Envelope, the Receipt, and the payload, as well as any local state.
Verifiers SHOULD offer options to store or share Receipts in case they are needed to audit the TS in case of a dispute.

7. Federation

We explain how multiple, independent Transparency Services can be composed to distribute supply chains without a single transparency authority trusted by all parties.

Multiple SCITT instances, governed and operated by different organizations.

For example, - a small, simple SCITT instance may keep track specifically of the software used for operating SCITT services. - an air-gapped data center may operate its own SCITT Ledger to retain full control and auditing of its software supplies.

How? - Policy-based. Within an organization, local Verifiers contact an authoritative SCITT that records the latest policies associated with classes of Artifacts; these policies indicate which Issuers and Ledgers are trusted for verifying signed Transparent Claims for these Artifacts.

* Other federation mechanisms?

We’d like to attach multiple Receipts to the same signed Claims, each Receipt endorsing the Issuer signature and a subset of prior Receipts. This involves down-stream Ledgers verifying and recording these Receipts before issuing their own Receipts.

8. Transparency Service API

Editor’s Note: this may be moved to appendix.

8.1. Messages

8.1.1. Register Signed Claims

8.1.1.1. Request

POST <Base URL>/entries

Body: SCITT COSE_Sign1 message

8.1.1.2. Response

One of the following:
HTTP Status 201 - Registration was tentatively successful pending service consensus.

HTTP Status 400 - Registration was unsuccessful.
  - Error code AwaitingDIDResolutionTryLater
  - Error code InvalidInput

[TODO] Use 5xx for AwaitingDIDResolutionTryLater

The 201 response contains the x-ms-ccf-transaction-id HTTP header which can be used to retrieve the Registration Receipt with the given transaction ID. [TODO] this has to be made generic

[TODO] probably a bad idea to define a new header, or is it ok? can we register a new one? https://www.iana.org/assignments/http-fields/http-fields.xhtml

The 400 response has a Content-Type: application/json header and a body containing details about the error:

json { "error": { "code": "<error code>", "message": "<message>" } }

AwaitingDIDResolutionTryLater means the service does not have an up-to-date DID document of the DID referenced in the Signed Claims but is performing or will perform a DID resolution after which the client may retry the request. The response may contain the HTTP header Retry-After to inform the client about the expected wait time.

InvalidInput means either the Signed Claims message is syntactically malformed, violates the signing profile (e.g. signing algorithm), or has an invalid signature relative to the currently resolved DID document.

8.1.2. Retrieve Registration Receipt

8.1.2.1. Request

GET <Base URL>/entries/<Transaction ID>/receipt

8.1.2.2. Response

One of the following:

* HTTP Status 200 - Registration was successful and the Receipt is returned.
* HTTP Status 400 - Transaction exists but does not correspond to a Registration Request.
  - Error code TransactionMismatch

* HTTP Status 404 - Transaction is pending, unknown, or invalid.
  - Error code TransactionPendingOrUnknown
  - Error code TransactionInvalid

The 200 response contains the SCITT_Receipt in the body.

The 400 and 404 responses return the error details as described earlier.

The retrieved Receipt may be embedded in the corresponding COSE_Sign1 document in the unprotected header, see TBD.

[TODO] There’s also the GET <Base URL>/entries/<Transaction ID> endpoint which returns the submitted COSE_Sign1 with the Receipt already embedded. Is this useful?

9. Privacy Considerations

Unless advertised by the TS, every Issuer should treat its Claims as public. In particular, their Envelope and Statement should not carry any private information in plaintext.

10. Security Considerations

On its own, verifying a Transparent Claim does not guarantee that its Envelope or contents are trustworthy---just that they have been signed by the apparent Issuer and counter-signed by the TS. If the Verifier trusts the Issuer, it can infer that the Claim was issued with this Envelope and contents, which may be interpreted as the Issuer saying the Artifact is fit for its intended purpose. If the Verifier trusts the TS, it can independently infer that the Claim passed the TS Registration policy and that has been persisted in the Ledger. Unless advertised in the TS Registration policy, the Verifier should not assume that the ordering of Transparent Claims in the Ledger matches the ordering of their issuance.

Similarly, the fact that an Issuer can be held accountable for its Transparent Claims does not on its own provide any mitigation or remediation mechanism in case one of these Claims turned out to be misleading or malicious---just that signed evidence will be available to support them.
Issuers SHOULD ensure that the Statements in their Claims are correct and unambiguous, for example by avoiding ill-defined or ambiguous formats that may cause Verifiers to interpret the Claim as valid for some other purpose.

Issuers and Transparency Services SHOULD carefully protect their private signing keys and avoid these keys for any purpose not described in this architecture. In case key re-use is unavoidable, they MUST NOT sign any other message that may be verified as an Envelope.

11. IANA Considerations

See Body Section 4.

12. References

12.1. Normative References


12.2. Informative References
[I-D.birkholz-scitt-receipts]


Appendix A.  Attic
Not ready to throw these texts into the trash bin yet.

Authors’ Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
64295 Darmstadt
Germany
Email: henk.birkholz@sit.fraunhofer.de

Antoine Delignat-Lavaud
Microsoft Research
21 Station Road
Cambridge
CB1 2FB
United Kingdom
Email: antdl@microsoft.com

Cedric Fournet
Microsoft Research
21 Station Road
Cambridge
CB1 2FB
United Kingdom
Email: fournet@microsoft.com
Abstract

A transparent and authentic ledger service in support of a supply chain’s integrity, transparency, and trust requires all peers that contribute to the ledgers operations to be trustworthy and authentic. In this document, a countersigning variant is specified that enables trust assertions on merkle-tree based operations for global supply chain ledgers. A generic procedure how to produce payloads for signing and validation is defined and leverages solutions and principles from the Concise Signing and Encryption (COSE) space.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 September 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document.
This document defines a method for issuing and verifying
countersignatures on COSE_Sign1 messages included in an authenticated
data structure such as a Merkle Tree.

We adopt the terminology of architecture (pointer) for Claim,
Envelope, Transparency Service, Ledger, Receipt, and Verifier.
Do we need to explain or introduce them here? We may also define Tree (our shorthand for authenticated data structure), Root (a succinct commitment to the Tree, e.g., a hand) and use Issuer instead of TS.

From the Verifier’s viewpoint, a Receipt is similar to a countersignature V2 on a single signed message: it is a universally-verifiable cryptographic proof of endorsement of the signed envelope by the countersigner.

Compared with countersignatures on single COSE envelopes, - Receipts countersign the envelope in context, providing authentication both of the envelope and of its logical position in the authenticated data structure. - Receipts are proof of commitment to the whole contents of the data structure, even if the Verifier knows only some of its contents. - Receipts can be issued in bulk, using a single public-key signature for issuing a large number of Receipts.

1.1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Common Parameters

Verifiers are configured by a collection of parameters to identify a Transparency Service and verify its Receipts. These parameters MUST be fixed for the lifetime of the Transparency Service and securely communicated to all Verifiers.

At minimum, these parameters include:

* a Service identifier: An opaque identifier (e.g. UUID) that uniquely identifies the service and can be used to securely retrieve all other Service parameters.

* The Tree algorithm used for issuing receipts, and its additional global parameters, if any. This document creates a registry (see Section 9.2.1) and describes an initial set of tree algorithms.

[TODO] The architecture also has fixed TS registration policies.
3. Generic Receipt Structure

A Receipt represents a countersignature issued by a Transparency Service.

The Receipt structure is a CBOR array with two items, in order:

* service_id: The service identifier as tstr.
* contents: The proof as a CBOR structure determined by the tree algorithm.

Receipt = [
  service_id: tstr,
  contents: any
]

Each tree algorithm MUST define its contents type and procedures for issuing and verifying a receipt.

4. COSE_Sign1 Countersigning

While the tree algorithms may differ in the way they aggregate multiple envelopes to compute a digest to be signed by the TS, they all share the same representation of the individual envelopes to be countersigned (intuitively, their leaves).

This document uses the principals and structure definitions of COSE_Sign1 countersigning V2 ([I-D.ietf-cose-countersign]). Each envelope is authenticated using a Countersign_structure array, recalled below.

Countersign_structure = [
  context: "CounterSignatureV2",
  body_protected: empty_or_serialized_map,
  sign_protected: empty_or_serialized_map,
  external_aad: bstr,
  payload: bstr,
  other_fields: [
    signature: bstr
  ]
]

The body_protected, payload, and signature fields are copied from the COSE_Sign1 message being countersigned.
The sign_protected field is provided by the TS, see Section 4.1 below. This field is included in the Receipt contents to enable the Verifier to re-construct Countersign_structure, as specified by the tree algorithm.

By convention, the TS always provides an empty external_aad: a zero-length bytestring.

Procedure for reconstruction of Countersign_structure:

1. Let Target be the COSE_Sign1 message that corresponds to the countersignature. Different environments will have different mechanisms to achieve this. One obvious mechanism is to embed the Receipt in the unprotected header of Target. Another mechanism may be to store both artifacts separately and use a naming convention, database, or other method to link both together.

2. Extract body_protected, payload, and signature from Target.

3. Create a Countersign_structure using the extracted fields from Target, and sign_protected from the Receipt contents.

4.1. Countersigner Header Parameters

The following parameters MUST be included in the protected header of the countersigner (sign_protected in Section 4):

* Issued At (label: TBD): The time at which the countersignature was issued as the number of seconds from 1970-01-01T00:00:00Z UTC, ignoring leap seconds.

5. CCF 2 Tree Algorithm

The CCF 2 tree algorithm specifies an algorithm based on a binary Merkle tree over the sequence of all ledger entries, as implemented in the CCF version 2 framework (see [CCF_Merkle_Tree]).

5.1. Additional Parameters

The algorithm requires that the TS define additional parameters:

* Hash Algorithm: The hash algorithm used in its Merkle Tree (see Section 9.2.2).

* Signature Algorithm: The signature algorithm used (see Section 9.2.3).
* Service Certificate: The self-signed X.509 certificate used as trust anchor to verify signatures generated by the transparency service using the Signature Algorithm.

All definitions in this section use the hash algorithm set in the TS parameters (see Section 5.1). We write HASH to refer to this algorithm, and HASH_SIZE for the fixed length of its output in bytes.

5.2. Cryptographic Components

Note: This section is adapted from Section 2.1 of [RFC9162], which provides additional discussion of Merkle trees.

5.2.1. Binary Merkle Trees

The input of the Merkle Tree Hash (MTH) function is a list of n bytestrings, written \( D_n = \{d[0], d[1], \ldots, d[n-1]\} \). The output is a single HASH_SIZE bytestring, also called the tree root hash.

This function is defined as follows:

The hash of an empty list is the hash of an empty string:

\[
MTH(\{\}) = \text{HASH}().
\]

The hash of a list with one entry (also known as a leaf hash) is:

\[
MTH(\{d[0]\}) = \text{HASH}(d[0]).
\]

For \( n > 1 \), let \( k \) be the largest power of two smaller than \( n \) (i.e., \( k < n \leq 2k \)). The Merkle Tree Hash of an \( n \)-element list \( D_n \) is then defined recursively as:

\[
MTH(D_n) = \text{HASH}(MTH(D[0:k]) || MTH(D[k:n])),
\]

where:

* \( || \) denotes concatenation
* \( : \) denotes concatenation of lists
* \( D[k1:k2] = D'_{-(k2-k1)} \) denotes the list \( \{d'[0] = d[k1], d'[1] = d[k1+1], \ldots, d'[k2-k1-1] = d[k2-1]\} \) of length \( k2 - k1 \).
5.2.2. Merkle Inclusion Proofs

A Merkle inclusion proof for a leaf in a Merkle Tree is the shortest list of intermediate hash values required to re-compute the tree root hash from the digest of the leaf bytestring. Each node in the tree is either a leaf node or is computed from the two nodes immediately below it (i.e., towards the leaves). At each step up the tree (towards the root), a node from the inclusion proof is combined with the node computed so far. In other words, the inclusion proof consists of the list of missing nodes required to compute the nodes leading from a leaf to the root of the tree. If the root computed from the inclusion proof matches the true root, then the inclusion proof proves that the leaf exists in the tree.

5.2.2.1. Verifying an Inclusion Proof

When a client has received an inclusion proof and wishes to verify inclusion of a leaf_hash for a given root_hash, the following algorithm may be used to prove the hash was included in the root_hash:

recompute_root(leaf_hash, proof):
    h := leaf_hash
    for [left, hash] in proof:
        if left
            h := HASH(hash || h)
        else
            h := HASH(h || hash)
    return h

5.2.2.2. Generating an Inclusion Proof

Given the MTH input D_n = {d[0], d[1], ..., d[n-1]} and an index i < n in this list, run the MTH algorithm and record the position and value of every intermediate hash concatenated and hashed first with the digest of the leaf, then with the resulting intermediate hash value. (Most implementations instead record all intermediate hash computations, so that they can produce all inclusion proofs for a given tree by table lookups.)

5.3. Encoding Signed Envelopes into Tree Leaves

This section describes the encoding of signed envelopes and auxiliary ledger entries into the leaf bytestrings passed as input to the Merkle Tree function.

Each bytestring is computed from three inputs:
* internal_hash: a string of HASH_SIZE bytes;

* internal_data: a string of at most 1024 bytes; and

* data_hash: either the HASH of the CBOR-encoded Countersign_structure of the signed envelope, using the CBOR encoding described in Section 6, or a bytestring of size HASH_SIZE filled with zeroes for auxiliary ledger entries.

as the concatenation of three hashes:

\[
\text{LeafBytes} = \text{internal_hash} \ || \ \text{HASH(internal_data)} \ || \ \text{data_hash}
\]

This ensures that leaf bytestrings are always distinct from the inputs of the intermediate computations in MTH, which always consist of two hashes, and also that leaf bytestrings for signed envelopes and for auxiliary ledger entries are always distinct.

The internal_hash and internal_data bytestrings are internal to the CCF implementation. Similarly, the auxiliary ledger entries are internal to CCF. They are opaque to receipt Verifiers, but they commit the TS to the whole ledger contents and may be used for additional, CCF-specific auditing.

5.4. Receipt Contents Structure

The Receipt contents structure is a CBOR array. The items of the array in order are:

* signature: the signature over the Merkle tree root as bstr.

* node_certificate: a DER-encoded X.509 certificate for the public key for signature verification. This certificate MUST be a valid CCF node certificate for the service; in particular, it MUST form a valid X.509 certificate chain with the service certificate.

* inclusion_proof: the intermediate hashes to recompute the signed root of the Merkle tree from the leaf digest of the envelope.

  - The array MUST have at most 64 items.

  - The inclusion proof structure is an array of [left, hash] pairs where left indicates the ordering of digests for the intermediate hash computation. The hash MUST be a bytestring of length HASH_SIZE.
* leaf_info: auxiliary inputs to recompute the leaf digest included in the Merkle tree: the internal hash, the internal data, and the protected header of the countersigner.

  - internal_hash MUST be a bytestring of length HASH_SIZE;
  - internal_data MUST be a bytestring of length less than 1024.

The inclusion of an additional, short-lived certificate endorsed by the TS enables flexibility in its distributed implementation, and may support additional CCF-specific auditing.

The CDDL fragment that represents the above text follows.

ReceiptContents = [
    signature: bstr,
    node_certificate: bstr,
    inclusion_proof: [+ ProofElement],
    leaf_info: LeafInfo
]

ProofElement = [
    left: bool
    hash: bstr
]

LeafInfo = [
    internal_hash: bstr,
    internal_data: bstr,
    sign_protected: empty_or_serialized_map
]

5.5. Receipt Verification

Given the TS parameters, a signed envelope, and a Receipt for it, the following steps must be followed to verify this Receipt.

1. Verify that the Receipt Content structure is well-formed, as described in Section 5.4

2. Construct a Countersign_structure as described in Section 4, using sign_protected from the leaf_info field of the receipt contents.

3. Compute LeafBytes as the bytestring concatenation of the internal hash, the hash of internal data, and the hash of the CBOR-encoding of Countersign_structure, using the CBOR encoding described in Section 6.
LeafBytes := internal_hash || HASH(internal_data) || HASH(cbor(Countersign_structure))

4. Compute the leaf digest.

LeafHash := HASH(LeafBytes)

5. Compute the root hash from the leaf hash and the Merkle proof using the Merkle Tree Hash Algorithm found in the service’s parameters (see Section 5.1):

root := recompute_root(LeafHash, inclusion_proof)

6. Verify the certificate chain established by the node certificate embedded in the receipt and the fixed service certificate in the TS parameters (see Section 5.1) using the Issued At time from sign_protected to verify the validity periods of the certificates. The chain MUST enable the use of the public key in the receipt certificate for signature verification with the Signature Algorithm of the TS parameters.

7. Verify that signature is a valid signature value of the root hash, using the public key of the receipt certificate and the Signature Algorithm of the TS parameters.

The Verifier SHOULD apply additional checks before accepting the countersigned envelope as valid, based on its protected headers and payload.

5.6. Receipt Generation

This document provides a reference algorithm for producing valid receipts, but it omits any discussion of TS registration policy and any CCF-specific implementation details.

The algorithm takes as input a list of entries to be jointly countersigned, each entry consisting of internal_hash, internal_data, and an optional signed envelope. (This optional item reflects that a CCF ledger records both signed envelopes and auxiliary entries.)

1. For each signed envelope, compute the Countersign_structure as described in Section 4.

2. For each item in the list, compute LeafBytes as the bytestring concatenation of the internal hash, the hash of internal data and, if the envelope is present, the hash of the CBOR-encoding of Countersign_structure, using the CBOR encoding described in Section 6, otherwise a HASH_SIZE bytestring of zeroes.
3. Compute the tree root hash by applying MTH to the resulting list of leaf bytestings, keeping the results for all intermediate HASH values.

4. Select a valid node_certificate and compute a signature of the root of the tree with the corresponding signing key.

5. For each signed envelope provided in the input,
   * Collect an inclusion_proof by selecting intermediate hash values, as described above.
   * Produce the receipt contents using this inclusion_proof, the fixed node_certificate and signature, and the bytestings internal_hash and internal_data provided with the envelope.
   * Produce the receipt using the Service Identifier and this receipt contents.

6. CBOR Encoding Restrictions

   In order to always regenerate the same byte string for the "to be signed" and "to be hashed" values, the core deterministic encoding rules defined in Section 4.2.1 of [RFC8949] MUST be used for all their CBOR structures.

7. Privacy Considerations

   TBD

8. Security Considerations

   TBD

9. IANA Considerations

9.1. Additions to Existing Registries

9.1.1. New Entries to the COSE Header Parameters Registry

   IANA is requested to register the new COSE Header parameters defined below in the "COSE Header Parameters" registry.

9.1.1.1. COSE_Sign1 Countersign receipt

   Name: COSE_Sign1 Countersign receipt

   Label: TBD
9.1.1.2. Issued At

Name: Issued At
Label: TBD
Value Type: uint
Description: The time at which the signature was issued as the number of seconds from 1970-01-01T00:00:00Z UTC, ignoring leap seconds.

9.2. New SCITT-Related Registries

IANA is asked to add a new registry "TBD" to the list that appears at https://www.iana.org/assignments/.

The rest of this section defines the subregistries that are to be created within the new "TBD" registry.

9.2.1. Tree Algorithms

IANA is asked to establish a registry of tree algorithm identifiers, named "Tree Algorithms", with the following registration procedures:

The "Tree Algorithms" registry initially consists of:

| Identifier | Tree Algorithm       | Reference     |
|------------+----------------------+---------------|
| CCF-2      | CCF 2 tree algorithm | This document |

Table 1: Initial content of Tree Algorithms registry

The designated expert(s) should ensure that the proposed algorithm has a public specification and is suitable for use as [TBD].

9.2.2. Hash Algorithms

IANA is asked to establish a registry of hash algorithm identifiers, named "Hash Algorithms", with the following registration procedures:

TBD
The "Hash Algorithms" registry initially consists of:

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Hash Algorithm</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-256</td>
<td>SHA-256</td>
<td>[RFC6234]</td>
</tr>
</tbody>
</table>

Table 2: Initial content of Hash Algorithms registry

The designated expert(s) should ensure that the proposed algorithm has a public specification and is suitable for use as a cryptographic hash algorithm with no known preimage or collision attacks. These attacks can damage the integrity of the ledger.

9.2.3. Signature Algorithms

IANA is asked to establish a registry of signature algorithm identifiers, named "Signature Algorithms", with the following registration procedures: TBD

The "Signature Algorithms" registry initially consists of:

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Signature Algorithm</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES256</td>
<td>Deterministic ECDSA (NIST P-256)</td>
<td>[RFC6979]</td>
</tr>
<tr>
<td></td>
<td>with HMAC-SHA256</td>
<td></td>
</tr>
<tr>
<td>ED25519</td>
<td>Ed25519 (PureEdDSA with the edwards25519 curve)</td>
<td>[RFC8032]</td>
</tr>
</tbody>
</table>

Table 3: Initial content of Signature Algorithms registry

The designated expert(s) should ensure that the proposed algorithm has a public specification and is suitable for use as a cryptographic signature algorithm.

10. References

10.1. Normative References
10.2. Informative References

[CCF_Merkle_Tree]
Microsoft Research, ., "CCF - Merkle Tree", n.d.,
<https://microsoft.github.io/CCF/main/architecture/
merkle_tree.html>.

[I-D.ietf-cose-countersign]
Schaad, J. and R. Housley, "CBOR Object Signing and
Encryption (COSE): Countersignatures", Work in Progress,
Internet-Draft, draft-ietf-cose-countersign-05, 23 June
2021, <https://www.ietf.org/archive/id/draft-ietf-cose-
countersign-05.txt>.
Authors’ Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
64295 Darmstadt
Germany
Email: henk.birkholz@sit.fraunhofer.de

Maik Riechert
Microsoft
United Kingdom
Email: Maik.Riechert@microsoft.com

Antoine Delignat-Lavaud
Microsoft
United Kingdom
Email: antdl@microsoft.com

Cedric Fournet
Microsoft
United Kingdom
Email: fournet@microsoft.com
Abstract

This document is intended to inform the development of the proposed Encrypted Client Hello (ECH) standard that encrypts Server Name Indication (SNI) and other data. Data encapsulated by ECH (i.e., data included in the encrypted ClientHelloInner) is of legitimate interest to on-path security actors including anti-virus software, parental controls and consumer and enterprise firewalls.

The document includes observations on current use cases for SNI data in a variety of contexts. It highlights how the use of that data is important to the operators of private networks and shows how the loss of access to SNI data will cause difficulties in the provision of a range of services to many millions of end-users.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 September 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.
1. Introduction

As noted above, this document includes observations on current use cases for SNI data in a variety of contexts. It highlights how the use of that data is important to the operators of private networks and shows how the loss of access to SNI data will cause difficulties in the provision of a range of services to many millions of end-users.

The Internet was envisaged as a network of networks, each able to determine what data to transmit and receive from their peers. Developments like ECH mark a fundamental change in the architecture of the Internet, allowing opaque paths to be established from endpoints to commercial services, some potentially without the knowledge or permission of the device owners. This change should not be undertaken lightly given both the architectural impact on the Internet and potentially adverse security implications for end users. Given these implications, it certainly should not be undertaken without either the knowledge or consultation of end users, as outlined in RFC 8890 [RFC8890].
NB Whilst it is reasonable to counter that VPNs also establish opaque paths, a primary difference is that the use of a VPN is a deliberate act by the user, rather than a choice made by client software, potentially without either the knowledge and/or consent of the end-user or device owner.

RFC 7258 [RFC7258] discusses the critical need to protect users’ privacy when developing IETF specifications and also recognises that making networks unmanageable to mitigate pervasive monitoring is not an acceptable outcome.

RFC 8404 [RFC8404] discusses current security and network operations as well as management practices that may be impacted by the shift to increased use of encryption to help guide protocol development in support of manageable and secure networks. As RFC 8404 notes, "the implications for enterprises that own the data on their networks or that have explicit agreements that permit the monitoring of user traffic are very different from those for service providers who may be accessing content in a way that violates privacy considerations".

This document considers the implications of ECH for private network operators including enterprises and education establishments. The data encapsulated by ECH is of legitimate interest to on-path security actors including anti-virus software, parental controls and consumer and enterprise firewalls. This document will focus specifically on the impact of encrypting the SNI data by ECH on private networks, but it should be noted that other elements will be relevant for some on-path security methods.

2. Encrypted Server Name Indication

RFC 8744 [RFC8744] describes the general problem of encrypting the Server Name Identification (SNI) TLS extension. The document includes a brief description of what it characterises as "unanticipated" usage of SNI information (section 2.1) as well as a brief (two paragraph) assessment of alternative options in the event that the SNI data is encrypted (section 2.3).
The text in RFC 8744 suggests that most of the unanticipated SNI usage "could also be implemented by monitoring DNS traffic or controlling DNS usage", although it does then acknowledge the difficulties posed by encrypted DNS protocols. It asserts, with limited evidence, that "most of [the unanticipated usage] functions can, however, be realized by other means", although without considering or quantifying the affordability, operational complexity, technical capability of affected parties or privacy implications that might be involved. It is unclear from the document whether any stakeholders that may be impacted by the encryption of SNI data have been consulted; it does not appear to be the case.

The characterisation of "unanticipated usage" of SNI data could be taken to imply that such usage was not approved and therefore inappropriate in some manner. The reality is that the development of the Internet has many examples of permissionless innovation and so these should not be dismissed as lacking in importance.

This document is intended to address the above limitations of RFC 8744 by providing more information about the issues posed by the introduction of ECH due to the loss of visibility of SNI data on private networks. To do so it considers the situation within schools and enterprises, building on information previously documented in a report from a roundtable discussion [ECH_Roundtable].

3. The Education Sector

3.1. Context

Focusing specifically on the education sector, the primary issue caused by ECH is that it is likely to circumvent the safeguards applied to protect children through content filtering, whether in the school or home environments, adding to adverse impacts already introduced through the use of encrypted DNS protocols such as DNS over HTTPS [RFC8484].

Content filtering that leverages SNI information is used by education establishments to protect children from exposure to malicious, adult, extremist and other content that is deemed either age-inappropriate or unsuitable for other reasons. Any bypassing of content filtering by client software on devices will be problematic and may compromise duties placed on education establishments: for example, schools in the England and Wales have obligations to provide "appropriate filtering systems in place" [KCSE]; schools in the US use Internet filters and implement other measures to protect children from harmful online content as a condition for the receipt of certain federal funding, especially E-rate funds [CIPA].
3.2. Why Content Filtering Matters to Schools

The impact that ineffective content filtering can have on an educational institution should not be underestimated. For example, a coroner in the UK in 2021 ruled that a school’s failure to prevent a pupil from accessing harmful material online on its equipment contributed to her taking her own life [Coroner]. In this particular case, the filtering software installed at the school was either faulty or incorrectly configured but it highlights the harmful risks posed if the filtering is bypassed by client software using ECH.

3.3. Mitigations

Whilst it may be possible for schools to overcome some of the issues ECH raises by adopting similar controls to those used by enterprises, it should be noted that most schools have a very different budget for IT compared to enterprises and usually have very limited technical support capabilities. Therefore, even where technical solutions exist that may allow them to continue to meet their compliance obligations, affordability and operational expertise will present them with significant difficulties.

Absent funding and technical expertise, schools will need to consider the best way forward that allows them to remain compliant. If client software does not allow ECH to be disabled, any such software that implements support for ECH may need to be removed from school devices and replaced, assuming that suitable alternatives are available. This will have a negative impact on budgets and maybe operationally challenging if institutions have made a significant investment in the deployment and use of particular applications and technologies.

There are instances where policies in education establishments allow for the use of equipment not owned by the institution, including personal devices and the devices of contractors and site visitors. These devices are unlikely to be configured to use the institution’s proxy but can nevertheless connect to the school network using a transparent proxy (see below). Transparent proxies used for filtering will typically use SNI data to understand whether a user is accessing inappropriate data, so encrypting the SNI field will disrupt the use of these transparent proxies.

In the event that transparent proxies are no longer effective, institutions will either have to require more invasive software to be installed on third party devices before they can be used along with ensuring they have the capability to comprehend and adequately manage these technologies or will have to prevent those devices from operating. Neither option is desirable.
4. Transparent Proxies

A proxy server is a server application that acts as an intermediary between a client requesting a resource and the server providing that resource. Instead of connecting directly, the client directs the request to the proxy server which evaluates the request before performing the required network activity. Proxies are used for various purposes including load balancing, privacy and security.

Traditionally, proxies are accessed by configuring a user’s application or network settings, with traffic diverted to the proxy rather than the target destination. With "transparent" proxying, the proxy intercepts packets directed to the destination, making it seem as though the request is handled by the target destination itself.

A key advantage of transparent proxies is that they work without requiring the configuration of user devices or software. They are commonly used by organisations to provide content filtering for devices that they don’t own that are connected to their networks. For example, some education environments use transparent proxies to implement support for BYOD without needing to load software on third-party devices.

Transparent proxies use SNI data to understand whether a user is accessing inappropriate content without the need to inspect data beyond the SNI field. Because of this, encryption of the SNI field, as is the case with ECH, will disrupt the use of transparent proxies.

5. Enterprises

Filtering is an important tool within many enterprises, with uses including the prevention of accidental access to malicious content due to phishing etc. In the enterprise market, a number of vendors use transparent proxy solutions, often combined with DNS filtering, to give stronger protections, with the proxy capability requiring unencrypted SNI information. BYOD is arguably even more important with the current reliance on remote working, which is another area where the use of transparent proxies can help. Alternative solutions are available but will require the use of more invasive software to be installed onto the guest device.
Any restrictions on the use of BYOD will also affect contractors and other third parties that need to connect to one or more enterprise networks on a temporary basis. In such circumstances, requiring software or custom configurations to be installed on those devices may be problematic, especially for contractors that work across multiple organisations. One solution could be for dedicated equipment for each client, however this will have potentially significant cost considerations.

Clear audit trails of any communications between parties are required in the finance sector amongst others for compliance purposes. If it becomes possible for communications to take place without an audit trail or any visibility to the enterprise, then there is increased scope for abuse to take place, including insider trading or fraud.

In addition to concerns about the loss of visibility of deliberate activity by users, the loss of visibility of potential command and control and other activity by malicious software is of concern to enterprises. In such cases, the lack of visibility from these privacy protections could lead to negative impacts on security and privacy for the enterprise, its employees, suppliers and customers.

When considering the operational and cost implications for enterprises, it should be remembered that the resources available will vary significantly between a multinational organisation and a small to medium-sized enterprise. It should not be assumed that a solution that can be absorbed financially and operationally by the former is practical for the latter. The needs of both need to be taken into account when evaluating potential solutions.

6. Threat Detection

[To be completed, additional input welcome]

RFC 8404 identifies a number of issues arising from increased encryption of data, some of which apply to ECH. For example, it notes that an early trigger for DDoS mitigation involves distinguishing attacker traffic from legitimate user traffic; this become more difficult if traffic sources are obscured.

The various indicators of compromise (IoCs) are documented in draft-ietf-opsec-indicators-of-compromise-00, which also describes how they are used effectively in cyber defence. For example, section 4.1.1 of the document describes the importance of IoCs as part of a defence-in-depth strategy; in this context, SNI is just one of the range of indicators that can be used to build up a resilient defence (see section 3.1 in the same document on IoC types and the 'pyramid of pain').
In the same Internet-Draft, section 6.1 expands on the importance of the defence in depth strategy. In particular, it explains the role that domains and IP addresses can play, especially where end-point defences are compromised or ineffective, or where endpoint security isn’t possible, such as in BYOD, IoT and legacy environments. SNI data plays a role here, in particular where DNS data is unavailable because it has been encrypted; if SNI data is lost too, alongside DNS, defences are weakened and the attack surface increased.

7. Mitigations

Access to SNI data is sometimes necessary in order for institutions, including those in the education and finance sectors, to discharge their compliance obligations. The introduction of ECH in client software poses operational challenges that could be overcome on devices owned by those institutions if policy settings are supported within the software that allows the ECH functionality to be disabled.

Third-party devices pose an additional challenge, primarily because the use of ECH will render transparent proxies inoperable. The most likely solution is that institutions will require the installation of full proxies and certificates on those devices before they are allowed to be connected to the host networks. They may alternatively determine that such an approach is impractical and instead withdraw the ability for network access by third-party devices.

An additional option that warrants further consideration is the development of a standard that allows a network to declare its policy regarding ECH and other such developments. Clients would then have the option to continue in setting up a connection if they are happy to accept those policies, or to disconnect and try alternative network options if not. Such a standard is outside of the scope of this document but may provide a mechanism that allows the interests and preferences of client software, end-users and network operators to be balanced.

8. Security Considerations

In addition to introducing new operational and financial issues, the introduction of SNI encryption poses new challenges for threat detection which this document outlines. These do not appear to have been considered within either RFC 8744 or the current ECH Internet-Draft [draft-ietf-tls-esni-14] and should be addressed fully within the latter’s security considerations section.
9. Acknowledgements

In addition to the authors, this document is the product of an informal group of experts including the following people:

10. Informative References


Updates to the Cipher Suites in Secure Syslog
draft-ciphersuites-in-sec-syslog-01

Abstract


Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 2 August 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.
1. Introduction


Both [RFC5425] and [RFC6012] MUST support certificates as defined in [RFC5280].

[RFC5425] requires that implementations "MUST" support TLS 1.2 [RFC5246] and are "REQUIRED" to support the mandatory to implement cipher suite TLS_RSA_WITH_AES_128_CBC_SHA (Section 4.2).

[RFC6012] requires that implementations "MUST" support DTLS 1.0 [RFC4347] and are also "REQUIRED" to support the mandatory to implement cipher suite TLS_RSA_WITH_AES_128_CBC_SHA (Section 5.2).

The TLS_RSA_WITH_AES_128_CBC_SHA cipher suite has been found to be weak and the community is moving away from it and towards more robust suites.
The DTLS 1.0 transport [RFC4347] has been deprecated by [BCP195] and the community is moving to DTLS 1.2 [RFC6347] and DTLS 1.3 [I-D.ietf-tls-dtls13].

This document updates [RFC5425] and [RFC6012] to deprecate the use of TLS_RSA_WITH_AES_128_CBC_SHA and to make new recommendations to a mandatory to implement cipher suite to be used for implementations. This document also updates [RFC6012] to make a recommendation of a mandatory to implement secure datagram transport.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Support for Updating

[I-D.salowey-tls-rfc8447bis] generally reminds us that cryptographic algorithms and parameters will be broken or weakened over time. Blindly implementing the cryptographic algorithms listed in any specification is not advised. Implementers and users need to check that the cryptographic algorithms specified continue to provide the expected level of security.

As the Syslog Working Group determined, Syslog clients and servers MUST use certificates as defined in [RFC5280]. Since both [RFC5425] and [RFC6012] REQUIRE the use of TLS_RSA_WITH_AES_128_CBC_SHA, it is very likely that RSA certificates have been implemented in devices adhering to those specifications. [BCP195] notes that ECDHE cipher suites exist for both RSA and ECDSA certificates, so moving to an ECDHE cipher suite will not require replacing or moving away from any currently installed RSA-based certificates.

[I-D.saviram-tls-deprecate-obsolete-kex] documents that the cipher suite TLS_RSA_WITH_AES_128_CBC_SHA has been found to be weak. As such, the community is moving away from that and other weak suites and towards more robust suites such as TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, which is also listed as a currently Recommended algorithm in [I-D.salowey-tls-rfc8447bis].
Along those lines, [I-D.ietf-uta-rfc7525bis] notes that
TLS_RSA_WITH_AES_128_CBC_SHA does not provide forward secrecy, a
feature that is highly desirable in securing event messages. That
document also goes on to recommend
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as a cipher suite that does
provide forward secrecy.

Therefore, the mandatory to implement cipher suites listed in
[RFC5425] and [RFC6012] must be updated so that implementations of
secure syslog are still considered to provide an acceptable and
expected level of security.

Additionally, [BCP195] [RFC8996] deprecates the use of DTLS 1.0
[RFC4347], which is the mandatory to implement transport protocol for
[RFC6012]. Therefore, the transport protocol for [RFC6012] must be
updated.

4. Updates to RFC 5425

Implementations of [RFC5425] MUST NOT offer
TLS_RSA_WITH_AES_128_CBC_SHA. The mandatory to implement cipher
suite is REQUIRED to be TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.

Implementations of [RFC5425] MUST continue to use TLS 1.2 [RFC5246]
as the mandatory to implement transport protocol.

Implementations of [RFC5425] MAY use TLS 1.3 [RFC8446] as a transport
as long as they support the currently recommended cipher suites.

EDITOR’s NOTE: Need to address 0-RTT considerations.

5. Updates to RFC 6012

Implementations of [RFC6012] MUST NOT offer
TLS_RSA_WITH_AES_128_CBC_SHA. The mandatory to implement cipher
suite is REQUIRED to be TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.

As specified in [BCP195], implementations of [RFC6012] must not use
DTLS 1.0 [RFC4347]. Implementations MUST use DTLS 1.2 [RFC6347].

DTLS 1.2 [RFC6347] implementations are REQUIRED to support the
mandatory to implement cipher suite, which is
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.

Implementations of [RFC6012] MAY use DTLS 1.3 [I-D.ietf-tls-dtls13]
as a transport as long as they support the currently recommended
cipher suites.
EDITOR’s NOTE: Need to address 0-RTT considerations.

6. Authors Notes

This section will be removed prior to publication.

This is version -01. Comments were received regarding the -00 version that this document should not imply that the use of DTLS1.0 is being deprecated by this I-D since that was done by RFC 8996. Edits have been made to clarify that. Also, the authors want this document to update RFC 6012 because it says more about cipher suites than RFC 8996 and, since there will be 1.3, we’re saying ya’ gotta use 1.2 (for now).

Members of IEC 62351 TC 57 WG15, who prompted this work, have proposed the following text to be inserted into their documents.

The selection of TLS connection parameters such as cipher suites, session resumption and renegotiation shall be reused from IEC 62351-3 specification. Note that port TCP/6514 is assigned by IANA to RFC 5425 (syslog-tls). The RFC requires the support of TLS1.2 and a SHA-1 based cipher suite, but does not mandate its use. The cipher does not align with IEC 62351-3 Ed.2 for profiling TLS. Nevertheless, RFC 5425 does not rule out to use stronger cipher suites. With this, clients and server supporting the selection of cipher suites stated in IEC 62351-3 Ed2 will not experience interoperability problems. Caution has to be taken in environments in which interworking with existing services utilizing syslog over TLS is intended. For these, the syslog server needs to be enabled to support the required cipher suites. This ensures connectivity with clients complying to this document and others complying to RFC 5425. Note that meanwhile the work on an update of RFC 5425 and RFC 6012 has started. It targets the adoption of stronger cipher suites for TLS and DTLS to protect syslog communication.

Comments on this text are welcome.

7. Acknowledgments

The authors would like to thank Arijit Kumar Bose, Steffen Fries and the members of IEC TC57 WG15 for their review, comments, and suggestions. The authors would also like to thank Tom Petch and Juergen Schoenwaelder for their comments and constructive feedback.
8. IANA Considerations

This document makes no requests to IANA.

9. Security Considerations

[BCP195] deprecates an insecure DTLS transport protocol from [RFC6012] and deprecates insecure cipher suites from [RFC5425] and [RFC6012]. This document specifies mandatory to implement cipher suites to those RFCs and the latest version of the DTLS protocol to [RFC6012].

10. References

10.1. Normative References


<https://www.rfc-editor.org/info/bcp14>


<https://www.rfc-editor.org/info/bcp195>


10.2. Informative References

[I-D.ietf-tls-dtls13]

[I-D.ietf-uta-rfc7525bis]

[I-D.salowey-tls-rfc8447bis]

Authors’ Addresses

Chris Lonvick
Email: lonvick.ietf@gmail.com

Sean Turner
sn3rd
Email: sean@sn3rd.com

Joe Salowey
Salesforce
Email: joe@salowey.net
Abstract

This document describes the key consistency and correctness requirements of protocols such as Privacy Pass, Oblivious DoH, and Oblivious HTTP for user privacy. It discusses several mechanisms and proposals for enabling user privacy in varying threat models. In concludes with discussion of open problems in this area.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the mailing list (), which is archived at .

Source for this draft and an issue tracker can be found at https://github.com/chris-wood/key-consistency.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 5 September 2022.
1. Introduction

Several proposed privacy-enhancing protocols such as Privacy Pass [PRIVACY-PASS], Oblivious DoH [ODOH], and Oblivious HTTP [OHTTP] require clients to obtain and use a public key for execution. For example, Privacy Pass public keys are used by clients for validating privately issued tokens for anonymous session resumption. Oblivious DoH and HTTP both use public keys to encrypt messages to a particular server.
User privacy in these systems depends on users receiving a key that many, if not all, other users receive. If a user were to receive a public key that was specific to them, or restricted to a small set of users, then use of that public key could be used to learn targeted information about the user. Users also need to receive the correct public key.

In this document, we elaborate on these core requirements, and survey various system designs that might be used to satisfy them. The purpose of this document is to highlight challenges in building and deploying solutions to this problem.

1.1. Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Terminology

This document defines the following terms:

Key Consistency and Correctness System (KCCS): A mechanism for providing clients with a consistent view of cryptographic key material within a period of time.

Reliant System: A system that embeds one or more key consistency and correctness systems.

The KCCS’s consistency model is dependent on the implementation and reliant system’s threat model.

3. Core Requirements

Privacy-focused protocols which rely on widely shared public keys typically require keys be consistent and correct. Informally, key consistency is the requirement that all users who communicate with an entity share the same view of the key associated with that entity; key correctness is that the key’s secret information is controlled by the intended entity and is not known to be available to an external attacker.
Some protocols depend on large sets of users with consistent keys for privacy reasons. Specifically, all users with a consistent key represent an anonymity set wherein each user of the key in that set is indistinguishable from the rest. An attacker that can actively cause inconsistent views of keys can therefore compromise user privacy.

An attacker that can cause a user to use an incorrect key will likely compromise the entire protocol, not just privacy.

Reliant systems must also consider agility when trying to satisfy these requirements. A naive solution to ensuring consistent and correct keys is to only use a single, fixed key pair for the entirety of the system. Users can then embed this key into software or elsewhere as needed, without any additional mechanics or controls to ensure that other users have a different key. However, this solution clearly is not viable in practice. If the corresponding key is compromised, the system fails. Rotation must therefore be supported, and in doing so, users need some mechanism to ensure that newly rotated keys are consistent and correct.

Operationally, servers rotating keys may likely need to accommodate distributed system state-synchronization issues without sacrificing availability. Some systems and protocols may choose to prioritize strong consistency over availability, but this document assumes that availability is preferred to total consistency.

4. Consistency and Correctness at Key Acquisition

There are a variety of ways in which reliant systems may build key consistency and correct systems (KCCS), ranging in operational complexity to ease-of-implementation. In this section, we survey a number of possible solutions. The viability of each varies depending on the applicable threat model, external dependencies, and overall reliant system's requirements.

We do not include the fixed public key model from Section 3, as this is likely not a viable solution for systems and protocols in practice. In all scenarios, the server corresponding to the desired key is considered malicious.

4.1. Direct Discovery

In this model, users would directly query servers for their corresponding public key, as shown below.
The properties of this solution depend on external mechanisms in place to ensure consistency or correctness. Absent any such mechanisms, servers can produce unique keys for users without detection. External mechanisms to ensure consistency here might include, though are not limited to:

* Presenting a signed assertion from a trusted entity that the key is correct.

* Presenting proof that the key is present in some tamper-proof log, similar to Certificate Transparency ([RFC6962]) logs.

* User communication or gossip ensuring that all users have a shared view of the key.

The precise external mechanism used here depends largely on the threat model. If there is a trusted external log for keys, this may be a viable solution.

4.2. Single Proxy Discovery

In this model, there exists a proxy that fetches keys from servers on behalf of multiple users, as shown below.
If this proxy is trusted, then all users which request a key from this server are assured they have a consistent view of the server key. However, if this proxy is not trusted, operational risks may arise:

* The proxy can collude with the server to give per-user keys to clients.

* The proxy can give all users a key owned by the proxy, and either collude with the server to use this key or retroactively use this key to compromise user privacy when users later make use of the key.

Mitigating these risks may require tamper-proof logs as in Section 4.1, or via user gossip protocols.

4.3. Multi-Proxy Discovery

In this model, users leverage multiple, non-colluding proxies to fetch keys from servers, as shown below.
These proxies are ideally spread across multiple vantage points. Examples of proxies include anonymous systems such as Tor. Tor proxies are general purpose and operate at a lower layer, on arbitrary communication flows, and therefore they are oblivious to clients fetching keys. A large set of untrusted proxies that are aware of key fetch requests (Section 4.2) may be used in a similar way. Depending on how clients fetch such keys from servers, it may become more difficult for servers to uniquely target individual users with unique keys without detection. This is especially true as the number of users of these anonymity networks increases. However, beyond Tor, there does not exist a special-purpose anonymity network for this purpose.

4.4. Database Discovery

In this model, servers publish keys in an external database and clients fetch keys from the database, as shown below.
Figure 4: Database Discovery Example

The database is expected to have a table that asserts mappings between server names and keys. Examples of such databases are as follows:

* An append-only, audited table similar to that of Certificate Transparency [RFC6962]. The log is operated and audited in such a way that the contents of the log are consistent for all users. Any reliant system which depends on this type of KCCS requires the log be audited or users have some other mechanism for checking their view of the log state (gossiping). However, this type of system does not ensure proactive security against malicious servers unless log participants actively check log proofs. This requirement may impede deployment in practice. Experience with Certificate Transparency shows that most implementations have chosen not to check SignedCertificateTimestamps before using (that is, accepting as valid) a corresponding TLS certificate.

* A consensus-based table whose assertions are created by a coalition of entities that periodically agree on the correct binding of server names and key material. In this model the agreement is achieved via a consensus protocol, but the specific consensus protocol is dependent on the implementation.

For privacy, users should either download the entire database and query it locally, or remotely query the database using privacy-preserving queries (e.g., a private information retrieval (PIR) protocol). In the case where the database is downloaded locally, it
should be considered stale and re-fetched periodically. The frequency of such updates can likely be infrequent in practice, as frequent key updates or rotations may affect privacy; see Section 5 for details. Downloading the entire database works best if there are a small number of entries, as it does not otherwise impose bandwidth costs on each client that may be impractical.

5. Minimum Validity Periods

In addition to ensuring that there is one key at any time, or a limited number keys, any system needs to ensure that a server cannot rotate its keys too often in order to divide clients into smaller groups based on when keys are acquired. Such considerations are already highlighted within the Privacy Pass ecosystem, more discussion can be found at [PRIVACY-PASS-ARCH]. Setting a minimum validity period limits the ability of a server to rotate keys, but also limits the rate of key rotation.

6. Separate Consistency Verification

The other schemes described here all attempt to directly limit the number of keys that a client might accept. However, by changing how keys are used, clients can impose costs on servers that might discourage key diversity.

Protocols that have distinctly separate processes for acquiring and using keys might benefit from moving consistency checks to the usage part of the protocol. Correctness might be guaranteed through a relatively simple process, such obtaining keys directly from a server. A separate correctness check is then applied before keys are used.

6.1. Independent Verification

Anonymous queries to verify key consistency can be used prior to use of keys. A request for the current key (or limited set of keys) will reveal if the key that was acquired is different than the original. If the key that was originally obtained is not included, the client can abort any use of the key.

It is important that any validation process not carry any information that might tie it to the original key discovery process or that the system providing verification be trusted. A proxy (see Section 4.2) might be sufficient for providing anonymity, though more robust anonymity protections (see Section 4.3) could provide stronger guarantees. Querying a database (see Section 4.4) might provide independent verification if that database can be trusted not to provide answers that change based on client identity.
6.2. Key-Based Encryption

Key-based encryption has a client encrypt the information that it sends to a server, such as a token or signed object generated with the server keys. This encryption uses a key derived from the key configuration, specifically not including any form of key identifier along with the encrypted information. If key derivation for the encryption uses a pre-image resistant function (like HKDF), the server can only decrypt the information if it knows the key configuration. As there is no information the server can use to identify which key was used, it is forced to perform trial decryption if it wants to use multiple keys.

These costs are only linear in terms of the number of active keys. This doesn’t prevent the use of multiple keys, it only makes their use incrementally more expensive. Trial decryption costs can be increased by choosing a time- or memory-hard function such as [ARGON2] to generate keys.

Encrypting this way could provide better latency properties than a separate check.

7. Future Work

The model in Section 4.3 seems to be the most lightweight and easy-to-deploy mechanism for ensuring key consistency and correctness. However, it remains unclear if there exists such an anonymity network that can scale to the widespread adoption of and requirements of protocols like Privacy Pass, Oblivious DoH, or Oblivious HTTP. Existing infrastructure based on technologies like Certificate Transparency or Key Transparency may work, but there is currently no general purpose system for transparency of opaque keys (or other application data).

8. Security Considerations

This document discusses several models that systems might use to implement public key discovery while ensuring key consistency and correctness. It does not make any recommendations for such models as the best model depends on differing operational requirements and threat models.

9. References

9.1. Normative References
9.2. Informative References


Authors’ Addresses

Alex Davidson
Brave Software
Email: alex.davidson92@gmail.com

Matthew Finkel
The Tor Project
Email: sysrqb@torproject.org

Martin Thomson
Mozilla
Email: mt@lowentropy.net

Christopher A. Wood
Cloudflare
101 Townsend St
San Francisco,
United States of America
Email: caw@heapingbits.net
This specification updates the requirements for adding new entries to the IANA Secure Shell (SSH) Protocol Parameters registry. Currently, the requirement is generally for "IETF Review", as defined in RFC 8126, although a few portions of the registry require "Standards Action". This specification will change that former requirement to "Expert Review".
1. Introduction

The IANA Secure Shell (SSH) Protocol Parameters registry was populated by several RFCs including [RFC4250], [RFC4716], [RFC4819], and [RFC8308]. Outside of some narrow value ranges that require Standards Action in order to add new values or are marked for private use, all other portions of the registry require IETF Review [RFC8126]. This specification changes the requirement for sections currently requiring IETF Review to Expert Review.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. SSH Protocol Parameters Affected

The following table lists the SSH protocol parameters that changed from IETF Review to Expert Review. Where this change applies to a specific range of values within the particular parameter, that range is given in the notes column.
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>RFC</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Channel Connection Failure Reason Codes and Descriptions</td>
<td>[RFC4250]</td>
<td>0x00000001-0xFDFFFFFF (inclusive)</td>
</tr>
<tr>
<td>Compression Algorithm Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Connection Protocol Channel Request Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Connection Protocol Channel Types</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Connection Protocol Global Request Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Connection Protocol Subsystem Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Disconnection Messages Reason Codes and Descriptions</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Encryption Algorithm Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Extended Channel Data Transfer data_type_code and Data</td>
<td>[RFC4250]</td>
<td>0x00000001-0xFDFFFFFF (inclusive)</td>
</tr>
<tr>
<td>Extension Names</td>
<td>[RFC8308]</td>
<td></td>
</tr>
<tr>
<td>Key Exchange Method Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>MAC Algorithm Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Pseudo-Terminal Encoded Terminal Modes</td>
<td>[RFC4250]</td>
<td></td>
</tr>
<tr>
<td>Public Key Algorithm Names</td>
<td>[RFC4250]</td>
<td></td>
</tr>
</tbody>
</table>
Table 1: Secure Shell (SSH) Protocol Parameters Affected

<table>
<thead>
<tr>
<th>Protocol Parameter</th>
<th>RFC Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publickey Subsystem Attributes</td>
<td>[RFC4819]</td>
</tr>
<tr>
<td>Publickey Subsystem Request Names</td>
<td>[RFC4819]</td>
</tr>
<tr>
<td>Publickey Subsystem Response Names</td>
<td>[RFC4819]</td>
</tr>
<tr>
<td>Service Names</td>
<td>[RFC4250]</td>
</tr>
<tr>
<td>Signal Names</td>
<td>[RFC4250]</td>
</tr>
<tr>
<td>SSH Public-Key File Header Tags</td>
<td>[RFC4716]</td>
</tr>
</tbody>
</table>

3. Designated Expert Pool

Expert Review [RFC8126] registry requests are registered after a three-week review period on the <ssh-reg-review@ietf.org> mailing list, on the advice of one or more designated experts. However, to allow for the allocation of values prior to publication, the designated experts may approve registration once they are satisfied that such a specification will be published.

Registration requests sent to the mailing list for review SHOULD use an appropriate subject (e.g., "Request to register value in SSH protocol parameters <specific parameter> registry").

Within the review period, the designated experts will either approve or deny the registration request, communicating this decision to the review list and IANA. Denials SHOULD include an explanation and, if applicable, suggestions as to how to make the request successful. Registration requests that are undetermined for a period longer than 21 days can be brought to the IESG’s attention (using the <iesg@ietf.org> mailing list) for resolution.

Criteria that SHOULD be applied by the designated experts include determining whether the proposed registration duplicates existing functionality, whether it is likely to be of general applicability or useful only for a single application, and whether the registration description is clear.
IANA MUST only accept registry updates from the designated experts and SHOULD direct all requests for registration to the review mailing list.

It is suggested that multiple designated experts be appointed who are able to represent the perspectives of different applications using this specification, in order to enable broadly informed review of registration decisions. In cases where a registration decision could be perceived as creating a conflict of interest for a particular Expert, that Expert SHOULD defer to the judgment of the other Experts.

4. Acknowledgements

The impetus for this specification was a February 2021 discussion on the CURDLE mailing list.

5. IANA Considerations

This memo is wholly about updating the IANA SSH Protocol Parameters registry.

6. Security Considerations

This memo does not change the Security Considerations for any of the updated RFCs.

7. References

7.1. Normative References


Author’s Address

Peter E. Yee
AKAYLA
Mountain View, Calif. 94043
United States of America

Email: peter@akayla.com