Network Working Group
Internet-Draft
Intended status: Informational
Expires: 21 August 2025

D. Avrilionis
Compellio S.A.
T. Hardjono
MIT Connection Science

17 February 2025

Asset Schema Architecture for Asset Exchange
draft-avrilionis-satp-asset-schema-architecture-06

Abstract

A management architecture for asset schemas and profiles is needed to enable entities in the tokenized assets ecosystem to instantiate tokens within one or more asset networks. An asset network may be constrained to support only a select class or type of token to be present in the network. In the SATP protocol, the receiving gateway at the destination network is assumed in its preparatory stages to evaluate the transfer request of a tokenized asset from the sending gateway at the origin network. In order to evaluate the proposed transfer, the receiving gateway must have access to the asset definition schema upon which the token was based in the origin network. The current document discusses the management architecture for the asset definition schema and the schema-profiles derived from the definition schema.

Editorial Note

Discussion of this draft takes place on the SATP mailing list (sat@ietf.org), which has its home page at https://datatracker.ietf.org/wg/satp/about/.

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 21 August 2025.

Table of Contents

1. Introduction

One of the significant challenges facing many decentralized asset networks is the compatibility of the token as the digital representation of value (i.e., asset). The recent EU MiCA Regulation [1] recognizes asset-referenced tokens (ART) as a means to represent real-world assets (RWA) that are located outside the network and pre-exists before the token is instantiated on the network.

However, currently, there are no technical mechanisms to digitally express the definition of tokenizable assets. Such a definition is relevant for asset transfer protocols such as SATP [2] that utilize

gateways to transfer tokenized assets from one network to another. This is because if an asset (value) is to be transferable across distinct networks then both networks must share a common definition of what constitutes a tokenizable asset.

The semantic definition of the tokenizable real-world assets is referred to as the asset definition schema (or “asset schema” for short). Certain industry verticals or narrow use cases may define a subset of the larger asset definition schema. These derived schemas are called schema-profiles (or simply “profile”).

There are currently no protocols for the management of these asset schemas and profiles that can be utilized by gateways to retrieve and validate schemas, before executing the secure asset transfer protocol.

A management architecture for asset schemas and profiles must include mechanisms to enable designated authorities in a jurisdiction or community to publish an asset definition schema in such a way that is easily accessible. Furthermore, the schema management architecture must provide standard protocols to enable any entity or community to easily derive narrower profiles and enable them to mint tokens that are compliant with the profile and thus to the asset definition schema. This approach enables an equivalent comparison between two tokens in different networks to be performed if they are compliant to the same schema-profile.

An asset schema management architecture should provide a logical arrangement of the roles, functions and the interaction flows of the entities and asset-related Artifacts within the ecosystem.

2. Terminology

Real World Asset (RWA)
: This is the asset in the real-world whose value pre-exists before they are tokenized. A given RWA may be a physical asset (e.g. commodities, oil, gold) or it may be a digital-only asset (e.g. digital-only artwork). Any discrete object that bears economic, cultural, intellectual or any other form of value can be considered an RWA, making it subject to identification, ownership or trade among physical persons or legal entities. A physical asset exists physical world in a non-digitized form.

Asset Definition Schema (or Asset Schema)
: This is a data structure that defines the class or type of real-world assets (RWA) in a jurisdiction or community that can be tokenized. It defines the structure and the legal elements and attributes of an asset token.

(Asset) Schema-Profile (or Profile)
This is a data structure that is a subset of an Asset Definition Schema that is relevant to a given industry or vertical. A profile must include a reference to the parent schema from which it was derived. A profile may be published by the same entity as the Asset Schema Authority, or it may be published by a different entity.

Asset Schema Authority (ASA)
This is a legal entity in a jurisdiction that is recognized by other entities in the ecosystem as being the competent authority to publish one or more asset schemas under a given namespace.

Digitized Asset Record (DAR)
A digital representation (data structure) of a real-world asset that is primarily stored off-network or off-chain (e.g. traditional centralized depositories, registries, etc.). It is static information that is independent of the mechanism used to store it. In some cases, the DAR may be a digitized version of an existing paper certificate (note). For convenience, a digitized asset record may be copied onto the ledger of a given network for ease of accessibility (e.g. accessible smart contract), but its utility is independent of any technology used to store it. A DAR may hold reference to attestations issued by one or more Asset Record Authority. In the context of SATP, a DAR is typically hosted in a Network - a DAR is what is often quoted as "asset" in SATP Core.

Asset Record Authority
This is a legal entity in a jurisdiction that is recognized by other entities in the ecosystem as being the competent authority to attest to the existence of the real-world asset being represented as a DAR. Examples of asset record authorities include the traditional centralized certificates depository (e.g. DTCC, Clearstream, Euroclear), municipal land registries, and others [3].

Tokenized Asset Record (TAR)
This is a data structure used to instantiate (“tokenize”) a RWA based on both the DAR and the Schema-Profile that the creator of the token claims adherence to. The TAR must “point to” (carry references to) both the DAR (which states that the real-world asset truly exists) and the Schema-Profile (that defines the semantic and legal recognition) of the tokenization process. A TAR is stored in a registry and must be accessible to processes that mint the Asset-Token, because the record provides the semantic meaning of the Asset-Token. We refer to the TAR as “smart pointer” because it maintains one-to-one mapping with a

DAR. A TAR does not carry ownership information. In the context of SATP, a DAR is typically recorded in a Registry - a TAR is part of the SATP transfer context established during SATP Setup stage (a.k.a "Stage 0"). A TAR has a standardized identification format so Gateways have a uniform way to identify assets, independently from the specific DAR identification method used in each Network.

Asset-Token (or Token)
: This is the data structure on the network (i.e. on-chain) that represents the real-world asset through its association with the TAR and DAR based on the Schema-Profile. A given asset token must have a permanent immutable link (reference) to a tokenized asset record because the record provides the semantic context behind the asset token. Since the asset token is an on-chain construct, it can be managed by a smart contract or other similar programs that interact with the ledger of the network. Any SATP gateway or any entity that views a given asset token must be able to fetch the corresponding tokenized asset record and schema-profile in order to validate the legitimacy of the asset token.

Asset Provider
: This is the party (person or legal entity) in a jurisdiction or community that issues an Asset-Token based on a TAR and the related Schema-Profile.

Token Issuance Authorization
: In some jurisdictions, the Asset Provider may be required to obtain authorization from one or more Asset Schema Authorities in that jurisdiction to create (mint) Asset-Tokens on a network. An issuance-authorization protocol must be utilized that provides proof that the Asset Provider obtained authorization.

Asset Metadata Artifacts (or Asset Artifacts)
: For simplicity, the schemas, profiles, tokenized asset records, and other data structures that assist in the creation and management of asset-tokens on the network are referred to as asset-related artefacts (metadata). Being metadata, the artefacts exclude the asset token itself.

Artefacts Registry (or Registry)
: This is a location on the Internet or on other asset-related networks and systems where the Asset Metadata Artifacts can be registered and obtained (fetched). This includes services where the artefact’s integrity (signature) and author source authenticity can be verified. SATP gateways utilize the registries to retrieve (fetch) and/or validate a given asset schema or profiles derived from that schema.

Asset-related Network (or Network)
: Any system that maintains DARs. A Network can be based on DLT technology, it can be a traditional application running as SaaS software, or it can be a stand-alone enterprise application.

Gateway
: A software system that implements the SATP protocol to transfer assets between two Networks. Transfers are based on tokenized assets where validations can occur before the execution of the transfer, to ensure consistency.

3. Basic Concepts

3.1. Goal of asset schema management architecture

When a given Asset Provider seeks to tokenize a real-world asset (RWA) on a given network, contextual information must accompany and guide the token creation process. This background contextual information consists of a range of data and artefacts that may exist on-network (on-chain) and off-network (off-chain). Access to the relevant artifacts enable other entities in the tokenized assets ecosystem to validate the economic value represented by the asset token.

The need for data and artefacts to support the legal standing of an asset token in a jurisdiction means that these artefacts are as crucial as the token itself, and therefore the proper management of these artefacts using standardized mechanisms is core to the value proposition of the tokenized assets ecosystem.

Thus, the goal of an asset schema management architecture is to provide secure, persistent and reliable management of the relevant data and artefacts so that Asset-Tokens can be created, traded and decommissioned with transparency and consistency across networks globally.

3.2. Semantic consistency of asset-tokens

In order for communities to accept the tokenized representation of real-world assets, there must be an agreed syntax and semantic definition of what constitutes a tokenizable real-world asset. An agreed definition enables a token in one network to be acceptable in a different network, and therefore transferrable across networks. A disciplined and structured approach to defining the semantics of tokenizable real-world assets is therefore fundamental to the viability of a tokenized assets ecosystem.

The term used to refer to this semantic definition is the Asset Definition Schema (or simply Asset Schema). Similar to other data schemas (e.g. JSON schema, DTD in XML), the asset-schema, in addition to other processing properties/capabilities, defines the structure and the legal elements and attributes of an asset token such that the token is legally accepted as a financial instrument in a given jurisdiction. For certain industry verticals that are concerned only with specific types or classes of real-world assets, a subset of the Asset Schema. We refer to this subset as the Schema-Profile (or simply as the asset “profile”).

In order for Asset Schema to be acceptable to a community of stakeholders, the Asset Schema must be agreed upon by the community and be published (digitally signed) by an authority that is accepted by the community. This authority is referred to as the Asset Schema Authority (ASA). Similarly, a Schema-Profile must be published by the appropriate authority in the industry or vertical that utilizes that profile. How these authorities are selected and governed is outside the scope of this document.

3.3. Artifacts enabling the tokenization

For a real-world asset (RWA) to be represented as a token on a network (i.e. "on-chain") based on an Asset Schema and Schema-Pofile, there are several supporting data structures or “artifacts” that must be created, published and managed over time:

(a) Evidence of the existence of the physical real-world asset: A record of the existence of the real-world asset must be produced, digitized, and signed by the relevant entity that attests to the record. This entity is referred to as the Asset Record Authority, while the record is referred to as the Digitized Asset Record (DAR). Such DAR must be able to be stored off-network (off-chain) or on-network (on-chain), without affecting the veracity of the claims or assertions made in the record.

(b) Binding of the record to the schema: A DAR can be represented as an Asset Token (i.e. it is tokenizable) only in the context of an Asset Schema or Schema-Profile. In other words, tokenization only makes logical sense if sufficient data about the structure, legal elements and attributes (following the structure of the Schema) is defined for the type of asset listed in a record holding all these data.

The binding between a Schema-Profile and the DAR (in order to mint a token) is referred to as the Tokenized Asset Record (TAR). The TAR can be said to be a “smart pointer” because it

must carry a reference (pointer) to both the Schema-Profile and the DAR. In other words, the TAR is the data structure that enables the creation (minting) of the Asset Token.

Both of these references/pointers must be resolvable, and the relevant data structures at the endpoint of the references must be signed and be current/fresh (i.e. not expired). The TAR is stored in a Registry Service because it contains static artefact information, and unlike the asset token it does not carry ownership information (i.e. not tradeable).

(c) Transitivity conferred value to an Asset-Token by the TAR: Within a Network (on-chain), an Asset-Token must reference (point to) a corresponding TAR because the record is the technical means by which economic value is conferred upon the on-chain Asset-Token.

Thus, one can say that the economic value of the RWA is conferred transitively to the asset token from the DAR through the TAR. The TAR is the middleman construct that holds things together.

(d) Asset-token as the ownership mechanism: The ownership of the tokenized RWA is defined through the control of the Network of the Asset-Token. Usually, this entails control over the public key pair (address) on the network associated with the Asset-Token.

Thus, one can say that the economic value of the RWA is conferred transitively to the asset token from the DAR through the TAR. The TAR is the middleman construct that holds things together.

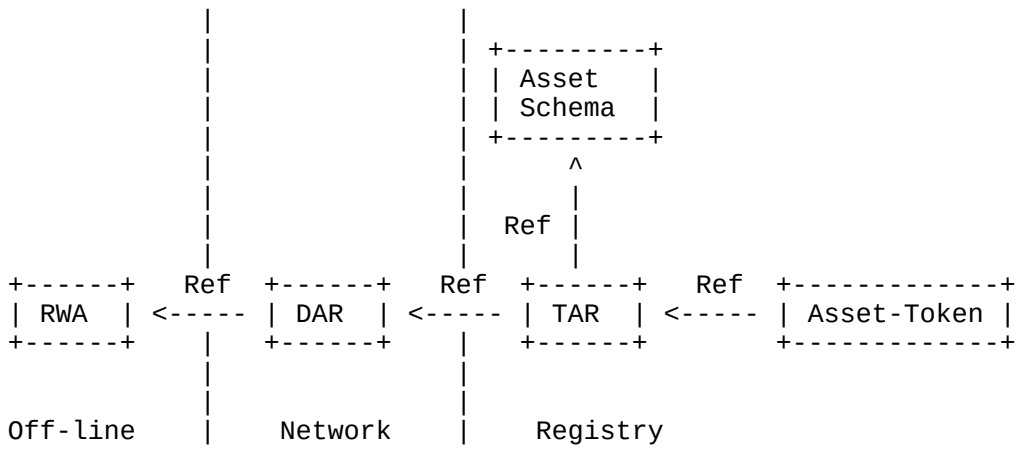

Figure 1: Basic concepts

3.4. System components enabling the tokenization

In order for a real-world asset (RWA) to be represented as a token on a network (i.e. “on-chain”) based on an asset schema and profile, there are several supporting data structures or “artefacts” that must be created, published and managed over time.

Asset Schema Authorities as well as Asset providers (collectively referred to as “Parties”) are defined by way of a digital record call “Party Definition” . A Party Definition should contain at least a cryptographic public key that would be used by the party for any proof operation related to creating Asset artefacts. However, to ensure immutability of the identity of a Party, the identifier of a Party Definition should not be derived from any Party key pair (for example, in order to avoid modification of the identity of the Party in case of key rotation).

Asset Providers can request a Token Issuance Authorisation from the relevant Asset Schema Authority at any time.

Token Issuance Authorisations may be valid for a given period (e.g. like SSL/TLS certificates, or oauth2.0 tokens).

4. Component architecture for asset artifacts and asset schema management

4.1. Registries

Registries, Networks and Gateways are system components that participate in asset transfers. Among these three components, the Registry plays a central role in the management of asset artifacts and asset schemas.

Registries are acting as persistent storage locations for Asset Schemas, Asset Schema Profiles, Asset Providers, Asset Schema Authorities and Tokenised Asset Records.

Asset Schemas (or Schema-Profiles), once registered, cannot be removed. New versions are appended in the Registry without removing previous versions (append-only principle).

4.2. Registry usage

Asset Schema Authorities as well as Asset providers can freely register themselves in a given Registry without any permission from any other central organization.

Updates of a Party Definition are append-only. Party Definitions may contain new as well as revoked public keys. It may also contain integrity keys (see below). Appends are transactions that are signed using the private key of the Party.

Key rotation is done by appending a new Party Definition containing the new key, and subsequently, a new update of the Party Definition revoking the old public key.

New Asset Schemas/Profiles (or new versions of existing Asset Schemas/Profiles) can be appended to the Registry by any Party without previous authorisation by any other Party. As part of its Definition, an Asset Provider can self-declare several key pairs that would be used as integrity verification keys for Tokenized Asset Records.

When issuing a Tokenized Asset Record, an Asset Provider should sign that record data with an integrity key. Integrity keys are declared as part of an Asset Provider Definition

A Token Issuance Authorisation Request (TIAR) is created by an Asset Provider (i.e. signed by the private key of the Asset Provider). It is a data structure containing information about an Asset Provider including a cryptographic public key (that is part of its Asset Provider Definition), a reference to a Network (a Network ID), and a reference to the Asset Schema-Profile (an Asset Schema-Profile ID). (note: A TIAR is similar to a Certificate Signing Request in the context of SSL)

The TIAR becomes a Token Issuance Authorisation (TIA) when signed by an Asset Schema Authority. TIAs allow Asset Providers to issue TARs in a specific Registry, which are valid for a given Asset Schema Profile.

Note: It is assumed that the Asset Provider holds the authorisation from an Asset Record Authority to issue DARs in a given network. This authorisation is eventually part of the attributes of the DAR. Issuance of DAR authorisations is outside of the scope of the present draft.

Based on the TIA the Asset Provider Issues a TAR in the given Registry. Such TAR contains references to the underlying Digitised Asset Record, the specific Asset Schema-Profile as well as to the TIA.

4.3. Registry governance

The current draft does not impose the existence of a central Registry. Many different registries may exist either in the same or in different jurisdictions. Asset Schema Authorities as well as Asset providers can freely register themselves at a given Registry without any permission from any central organisation. Asset Providers can request an Asset Issuance Authorisation from the relevant Asset Schema Authority at any time.

4.4. DAR issuance

In order for an Asset Provider to issue valid DARs and related TARs a series of processing steps occur. Before such processing sequence the following initial state must exist:

* The Asset Schema Authority is self-declared in the Registry

* The Asset Provider is self-declared in the Registry

* The Asset Schema (Profile) is issued and stored in the Registry by the Asset Schema Authority

* It is also assumed that the Asset Provider holds an authorisation to issue DARs in the given Network

Given the above initial state, the processing sequence is described in the sequence diagram below:

1. The Asset Provider fetches the definition of the Asset Schema Authority related to a given Asset Profile from the Registry

2. The Asset Provider submits a Token Issuance Authorization Request (TIAR) for the given Asset Profile to the Asset Schema Authority

3. Assunming there is approval of the TIAR from the The Asset Schema Authority, the Asset Schema Authority registers the Token Issuance Authorization in the Registry

4. The TIA is then delivered to the Asset Provider

5. The DAR is created in the given Network (This step is optional, as the DAR might have already been created)

6. The TAR is issued on the given Registry

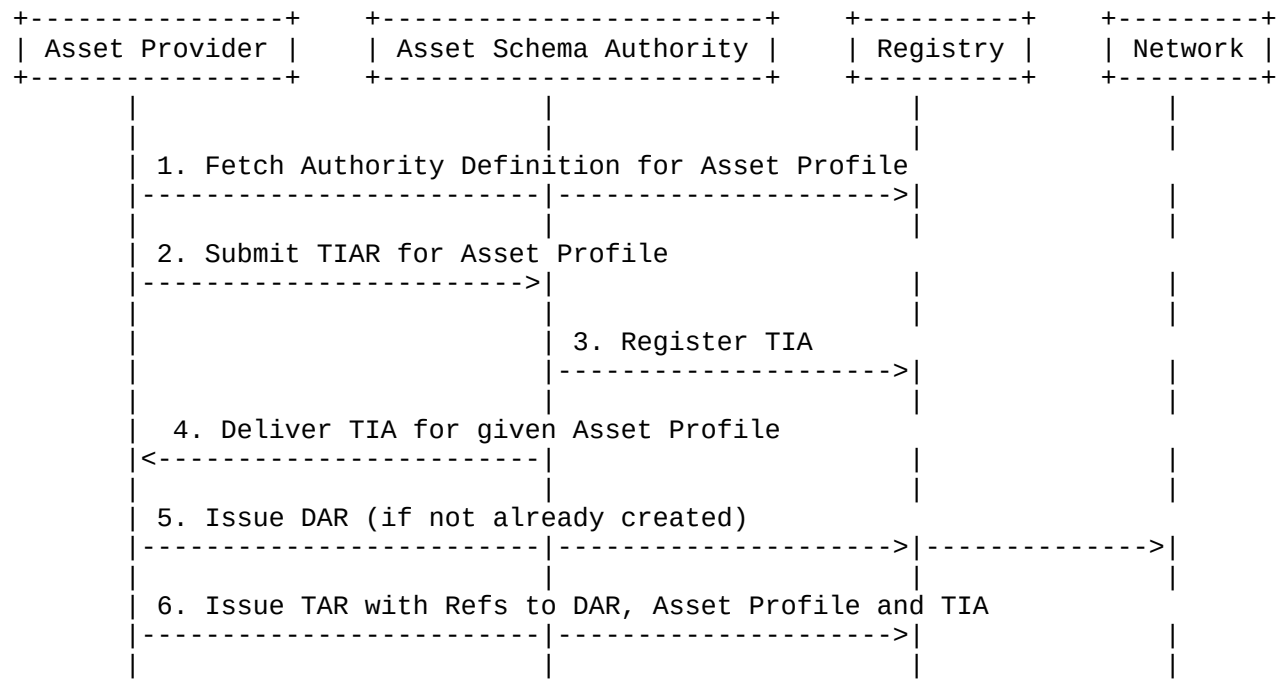

Figure 2: DAR Issuance

5. Gateways and Cross-Network Asset Transfers

The SATP Architecture defines a secure asset transfer protocol between networks, where the transfer is performed by peered gateways using the burn-mint paradigm and the classic two-phase commit protocol.

5.1. Pre-Transfer Validation

An important requirement for the recipient gateway (G2) at the destination network (NW2) is to validate that the asset-token (AT1) to be transferred via the sending gateway (G1) in the origin network (NW1) satisfies several requirements.

The validation of these requirements must occur pre-transfer before the first stage of the transfer commences. This preparatory stage is referred to as Stage-0 in the SATP Architecture [REF?]. Some of the information to be validated includes identity of originator and beneficiary, the destination address at the destination network (NW2), and asset-related information.

With regard to asset-related information, the recipient gateway (G2) must verify that the Asset-Token (AT1) in the origin network (NW1) is recognized within the destination network (NW2). This means that gateway G2 must obtain the relevant artifacts pertaining to the asset token AT1.

5.2. Validating Asset Metadata Artifacts

As part of the pre-transfer preparatory stage (Stage-0), gateway G1 must deliver metadata that is present within the asset token AT1 to gateway G2. However, since network NW1 may be private/closed, this means that gateway G2 may be unable to access the ledger on network NW1 and thus must rely on the information within the Transfer Proposal Claims (carrying this metadata) from gateway G1. This is one reason why the Transfer Proposal Claims (in SATP-Core protocol) must be digitally signed gateway G1.

The following is a list of tasks related to the proposed transfer of asset token AT1 from the origin network NW1 to the destination network NW2:

(a) Delivery of reference values of asset-token AT1 in network NW1: The gateway G1 must deliver a copy of the references found in the asset-token AT1 to gateway G2. Notably, this includes the reference to the TAR that underlies Asset-Token AT1.

(b) Validating Tokenized Asset Record (TAR1) corresponding to asset-token AT1: Upon receiving the reference to the Tokenized Asset Record, the gateway G2 must resolve (de-reference) the reference to the correct Registry Service (RG1) where the Tokenized Asset Record (TAR1) is stored. Gateway G2 then fetches a copy of the TAR1 from the Registry Service (RG1) and validates the signature of on TAR1.

(c) Validating Schema Profile (SP1) corresponding to Tokenized Asset Record (TAR1): Since the Tokenized Asset Record (TAR1) carries a reference to the Schema Profile (SP1), gateway G2 must use that reference to fetch a copy of the Schema Profile SP1 from the correct Registry Service (RG0).

(d) Policy Verification of Schema Profile SP1: Using the Schema Profile SP1 obtained from Registry Service RG0 the gateway G2 is now able to compare the asset definitions found in SP1 against its own network-wide policies regarding asset types and classes permitted to enter the destination network NW2.

6. Working with Registries

Below we give a list of elements that must be considered when working with Registries

* Any Party (Asset Provider or Asset Schema Authority) appears in the Registry via a “Party Definition” record. Such self-declared Party Definition (Asset Provider Definition or Asset Schema Authority Definition) should contain a cryptographic public key that would be used by the party for any proof operation related to creating Asset Schemas and Asset Instances (see below).

* The identifier of a Party Definition should not be derived from any Party key pair.

* Updates of a Party Definition are append-only. Party Definitions may contain new as well as revoked public keys. It may also contain integrity keys (see below). Appends are transactions that are signed using the private key of the Party.

* Key rotation is done by appending a new Party Definition containing the new key, and subsequently, a new update of the Party Definition revoking the old public key.

* New Asset Schemas/Profiles (or new versions of existing Asset Schemas/Profiles) can be appended in the Registry by any Party without previous authorisation by any other Party.

* As part of its Definition, an Asset Provider can self-declare several key pairs that would be used as integrity verification keys for Digitized Asset Records and Tokenized Asset Records.

* When issuing a TAR, an Asset Provider should sign the TAR data with an integrity key. Integrity keys are declared as part of an Asset Provider Definition.

* A Token Issuance Authorisation Request (TIAR) is created by an Asset Provider (i.e. signed by the private key of the Asset Provider). It is a data structure containing information about an Asset Provider including a cryptographic public key (that is part of its Asset Provider Definition), a reference to a Network (a Network ID), and a reference to the Asset Schema (an Asset Schema ID). (note: A TIAR is similar to a Certificate Signing Request in the context of SSL).

* The TIAR becomes a Token Issuance Authorisation (TIA) when signed by a key belonging to the Asset Schema Authority (Such key is part of the Asset Schema Authority Definition).

* Any third party can verify the validity of a DAR or a TAR as they are publically available and can be retrieved from the related Registries and Networks.

* Any third party can verify the validity of a DAR or a TAR as they are publically available and can be retrieved from the related Registries and Networks.

* An Digitized Asset Record is valid when all the following conditions apply (assuming a given Network and Registry):

  - The Tokenized Asset Record associated to the Digitized Asset Record is signed by an integrity key of a given Asset Provider.

  - The integrity key can be found in the Asset Provider Definition of the Asset Provider.

  - A TIA related to the Asset Schema of that TAR is linked/ embedded to the TAR.

  - The TIA contains the public key of the Asset Provider.

  - The Asset Schema Authority that has signed the TIA has also created the Asset Schema/Profile (or the specific Asset Schema/{Profile version).

7. References

[1] European Parliament, "MiCA Regulation", 2022, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>.

[2] Hardjono, T., "SATP Architecture", Work in Progress, Internet-Draft, draft-SATP, 2022, <https://datatracker.ietf.org/doc/html/draft-SATP>.

[3] Clearstream, D. E., "Advancing the Digital Asset Era, Together: An Industry Paper from DTCC / Clearstream / Euroclear", 2023, <https://www.dtcc.com/-/media/Files/Downloads/WhitePapers/FMI-Standards-WP.pdf>.

Authors' Addresses

Denis Avrilionis
Compellio S.A.
Email: denis@compell.io

Thomas Hardjono
MIT Connection Science
Email: hardjono@mit.org