Spherity GmbH

ATP Credentialing Pilot

Utilizing Verifiable Credentials to establish **A**uthorized **T**rading **P**artner Status

Supporting Drug Supply Chain Security Act (DSCSA) compliance

PUBLIC

ATP Public Architecture Handbook

Draft v0.81

3-12-2021

Contents

Authors
Carsten Stöcker, Spherity GmbH
Bob Celeste, Center for Supply Chain Studies
Sam Smith, Spherity GmbH
Georg Jürgens, Spherity GmbH

Document Updates

Version	Date	Author	Comments
V0.10	06 June 2020	Carsten Stöcker, Spherity GmbH	Initial version
V0.20	11 July 2020	Carsten Stöcker, Spherity GmbH	First Draft
V0.21	16 July 2020	Carsten Stöcker, Spherity GmbH	First version for review of chapters 1) to 4)
V0.30	17 July 2020	Carsten Stöcker, Spherity GmbH	Transferred to Google Doc for feedback from the group
V0.40	10 August 2020	Carsten Stöcker, Spherity GmbH	Resolved all comments and feedback from the ATP technical working group and updated chart. Switched to DSCSA terms “wholesale distributor” and “manufacturer”.
V0.50	27 November 2020	Georg Jürgens, Spherity GmbH	Update of AH of domain language and pilot implementation
V0.60	23 February 2021	Carsten Stöcker, Spherity GmbH	Chapter 5,6, 7 and 8
V0.71	25 February 2021	Carsten Stöcker, Spherity GmbH	Formatting of the document
v0.80	8 March	Carsten Stöcker, Spherity GmbH	Final Review
V0.81	12 March	Bob Celeste	Updated Figure 23: Replaced DEA icon with DEA Signing Certificate icon and minor punctuation corrections (Word spelling and punctuation applied).

1 Introduction

1.1 Purpose

This Architecture Handbook describes the design of the Health Distribution Alliance (HDA) pilot project for demonstrating compliance solution options for the US Drug Supply Chain Security Act (DSCSA) requirement for the **verification of Saleable Returns** and the **verification of Authorized Trading Partners** (ATP).

The focus of the Architecture Handbook is

1. to briefly document the current end-to-end architecture landscape for sending, receiving, and responding to Product Identity (PI) verification messages between **wholesale distributors** (WHO) and **manufacturers** (MAN),
2. to describe how trading partner authentication using ATP credentials can be augmented within existing Verification of Saleable Returns infrastructures, in a minimally invasive way, and
3. to outline architecture and roadmap alternatives for a secure and efficient approach for industry-wide adoption of an ATP credentialing solution.

As the existing technology solutions of WHOs, MANs, and Verification Request Service (VRS) providers are based on different software packages, the architecture handbook introduces an abstraction architecture, and as such will be transferable to the various individual software implementations of the parties involved in the Verification of Saleable Returns process.

Note: US DSCSA and FDA are using the terms **wholesale distributor** and **manufacturer**. In DSCSA manufacturer also refers to legal constructs such as marketing authorization holder (MAH), co-licensor, or manufacturer partnership.

It shall be understood that the ATP credentialing solution can be also applied for **dispensers**. In this case the requester of a PI verification request shall be the dispenser instead of the wholesale distributor. The ATP credentialing solution shall therefore be able to **abstract from the entity type of the requester**, either wholesale manufacturer or dispenser.

1.1.1 Status Quo of existing industry solutions for addressing US DSCSA

Per the DSCSA as of November 2019, wholesale distributors are required to verify the product-level serial number on saleable returns before selling the product back into the supply chain. The manufacturer must make the serial numbers available for verification. It is estimated that 2 to 4% of pharmaceutical products sold in the US are returned to the wholesale distributors and are eligible to be sold back into the supply chain upon verification.

Due to this high volume, an industry-wide PI verification system was implemented to allow wholesale distributors to perform the verification. The existing PI verification system allows the exchange of messages between WHOs and MANs via various VRS service providers as the primary method for the verification of so-called **serialized GTINs** (sGTIN) automatically, with a sub-second messaging roundtrip requirement. The sGTIN is encoded in a GS1 2D DataMatrix and encodes the following data objects: GTIN, Expiration Date, Batch Number, and Serial Number (S/N). Response times in the actual system are up to 2 seconds.

VRS services are cloud-based, multi-tenant solutions that are integrated with the systems of wholesale distributors and manufacturers. To allow a seamless exchange of PI verification messages among WHOs, MANs, and VRS providers, the industry adopted the **GS1 Lightweight Messaging Standard** as a communication protocol among these systems.

When a saleable return arrives at the warehouse of a wholesale distributor, the 2D DataMatrix of each individual package needs to be scanned. After scanning a 2D DataMatrix in the warehouse system of the WHO, the WHO initiates a **PI verification request** (VR). This PI verification is sent to the WHO VRS service provider, which then determines a routing path by looking up a service endpoint URL and forwarding the PI request using a **Look-up Table and Routing Service Network** (e.g. MediLedger) to the VRS of the MAN service provider. The MAN VRS queries PI data from the MAN system and then sends a PI verification request response (VR/R) back to the wholesale distributor.

The Look-up Table and Routing Service Network stores and maintains look-up data for mapping any sGTIN to the service endpoint of the relevant MANs.

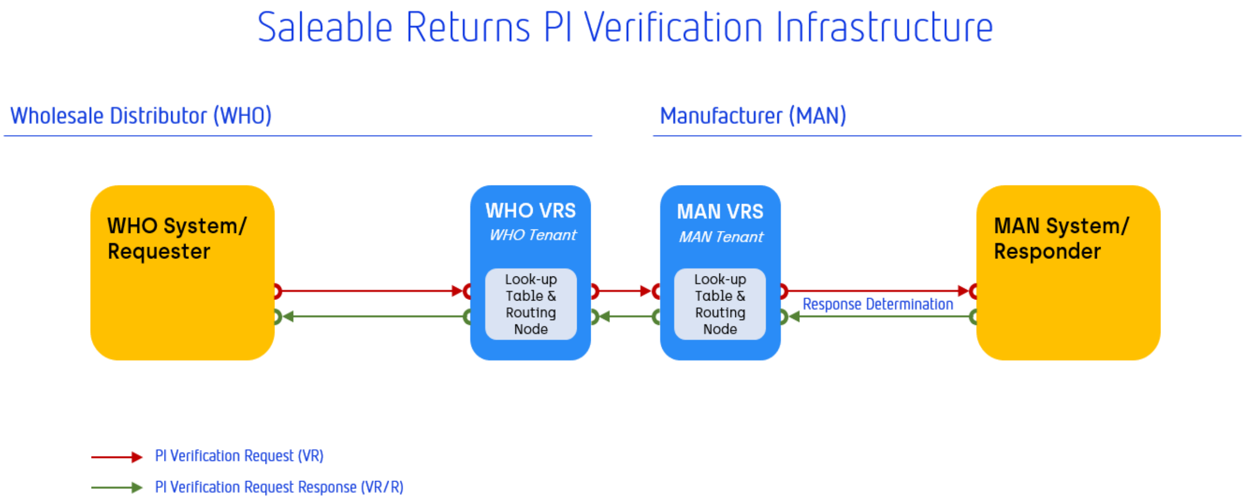

Saleable Returns PI Verification Infrastructure
Wholesale Distributor (WHO)
Manufacturer (MAN)
WHO System/ Requester
WHO VRS
WHO Tenant
Look-up Table & Routing Node
MAN VRS
MAN Tenant
Look-up Table & Routing Node
Response Determination
MAN System/ Responder
PI Verification Request (VR)
PI Verification Request Response (VR/R)

Figure 1 Existing PI Verification Infrastructure & VRS Services (source: Spherity)

1.1.2 Project Statement of ATP Pilot

The current saleable returns solution does not fulfill all DSCSA requirements. The ATP Pilot team recognizes that:

- The DSCSA requires manufacturers, repackagers, wholesale distributors and dispensers to only trade with companies that meet the DSCSA defined “Trading Partner” and “Authorized” definition.
- Compliance with the DSCSA will require supply chain companies to digitally interact with supply chain companies where the company identity and whether they meet the DSCSA defined “Trading Partner” and “Authorized” definition will be unknown at the time of interaction.

- To complete the interaction, it is essential for companies at both ends of a DSCSA digital interaction to know the identity of the other company and if the other company meets the DSCSA defined “Trading Partner” and “Authorized” definition.

The pilot team seeks to pilot the use of W3C (World Wide Web Consortium) standard decentralized Identifiers (DIDs) and verifiable credentials (VCs) in conjunction with the GS1 Lightweight Messaging Standard to:

- Know the identity of PI Verification requesters and responders,
- Verify that the requestor or responder meets the DSCSA definition of “Trading Partner” and “Authorized”.

To fulfill the DSCSA requirements, the pilot team seeks to test the use of the following new components:

- W3C Decentralized Identifiers (DIDs),
- W3C Verifiable Credentials (VCs), and
- Identity Wallets.

These components are described in more detail in the following sections.

1.2 Objectives

The objectives of the ATP pilot are to provide evidence about:

1. The feasibility of meeting DSCSA ***compliance goals*** with a DID, VC credential, and Identity Wallet approach in a minimally invasive way,
2. ***Operational goals*** such as response times, scalability, and ease of integration with existing business processes, and
3. ATP credential verifiability in a ***digital chain of trust***.

Compliance goals:

Wholesale Distributor (WHO)	Manufacturer (MAN)
● Know who responds to a verification request ● Determine whether they meet the ATP threshold ● Prevent bad actors from interacting ● Credential: ○ Acceptable by regulator ○ Meets Due Diligence goals ○ Meets the frequency occurrence goal	● Know who is requesting verification ● Determine whether they meet the ATP threshold ● Prevent bad actors from interacting ● Credential: ○ Acceptable by regulator ○ Meets Due Diligence goals ○ Meets the frequency occurrence goal

Operational goals:

- < 1 sec end-to-end round-trip time
- Benchmark against VC-free scenario
- Analyze different VC data structures and types (e.g., Identity Verification VC, ATP VC, VCs on corporate level or on facility level)
- Provide performance metrics for comparison
- Comparison between alternative business logic (batch vs real time, 1st contact vs subsequent)

Digital Chain of Trust goals:

- Pilot establishes a digital "chain of trust" based on agreed due diligence standards and cryptographically verifiable identifiers and credentials that validate compliance with them.
- This digital "chain of trust" is the key to the value of the system and interacting with it meaningfully becomes the gateway to operating in the supply chain.
- The critical points are where trust proof crosses over from the physical world to the digital world (the due diligence). These trust proofs shall be analyzed in this project.

1.3 Scope

The ATP pilot shall deploy and analyze a solution encompassing business as usual operations, exception handling, and nefarious actor scenarios.

#	Scope Type	Description
1	Business as usual operations	● DID Creation ● DID Maintenance ● Credential Acquisition ● PI Verification Request ● PI Verification Response ● Credential Maintenance ● Audit Scenario
2	Exception handling	● Unidentified credential Issuer ● Credential is revoked ● Credential is suspended ● License has lapsed beyond grace period; governance decision or issuer decision on grace periods (may be per state or per issuer) ● No credential provided in request ● No credential provided in response

		● Poorly formed credential (wrong attributes) ● Credential verification failure ● Expired License ● Expired Credential
3	Nefarious actor scenarios	● Nefarious actor attempts to represent themselves as a legitimate wholesale distributor to the Issuing body ● Nefarious Actor passes a legitimate company's credential for its own in PI Verification process ● Wholesale distributor sends PI Verification to nefarious actor (handled by current VRS routing)

1.4 System Overview

The ATP credentialing system will integrate the three **new components** (DID, VC, and Identity Wallet) with components of the existing PI verification infrastructure (GS1 Lightweight Messaging standard and Distributed Ledger).

Integration of these components requires the implementation of the following artefacts:

1. Identity wallets for trading partners and verification issuers using W3C DIDs and VCs
2. Wallet-to-Wallet Exchange Protocol for acquiring credentials from a verification issuer
3. Root-of-trust instruments for verification of issuers
4. Enrichment of the GS1 Lightweight Messaging standard
5. Distributed ledger as trust fabric for anchoring DIDs

The ATP identity wallets are cloud-based multi-tenant solutions that acquire, store, and present verifiable credentials. There are multiple options to integrate identity wallets with either the system of a trading partner or their respective VRS tenants. As the integration of wallets requires customization of a trading partner's system, industry-wide adoption can be driven much faster by integrating the wallets with the respective VRS system tenants with much less overall system customization efforts. In a longer-term solution, trading partners might choose to either outsource their wallets to the VRS or integrate their own wallet solution. Wallet integration options will be assessed under architecture alternatives.

For acquiring ATP credentials, wallets of trading partners interact with wallets of verifiable credential issuers.

Root-of-trust instruments will be established to anchor the identity of verifiable credential issuers so that each verifier can trust the authenticity of a credential issued by a verifiable credential issuer.

To be minimally invasive, the solution will integrate identity wallets and the credentials they verify and store with both the GS1 Lightweight Messaging standard and existing systems. Therefore, the ATP credentialing pilot system aims to implement ATP credential verification by enriching GS1 lightweight messages without any change to this standard. It will validate that ATP credentials can be embedded into the header of compliant GS1 lightweight messages without changing the VR and VR/R payload bodies' data structure.

1.5 New Component Details: DIDs, VCs, and Identity Wallets

The ATP pilot adopts decentralized public key infrastructure (PKI) technology and blockchain identity anchoring to establish the verifiable digital identity of the enterprises involved in the ATP verification process. To establish privacy-respecting cooperation, most enterprise communication is being done off-chain with a small amount of static data anchored on an immutable ledger.

An open, interoperable, portable, decentralized identity framework is a key requirement for establishing trust, verifiability, and auditability among the WHOs and MANs involved in the DSCSA ATP ecosystem.

Both the abstract concepts and the concrete implementations of verifiable credentials (VCs) using decentralized identifiers (DIDs) have been gaining momentum and acceptance. The primary loci of activity in developing interoperable open standards for these are the W3C, the Hyperledger Foundation, the Sovrin Foundation, and the Decentralized Identity Foundation (DIF). Working groups at the W3C authored, host, and maintain the W3C Verifiable Credential Data Model 1.0 specification. The W3C VC Standard is now a W3C recommendation (the most mature stage of the W3C standards process). Verifiable credentials (VCs) are issued against identifiers that may be associated with cryptographic operations, be they DIDs, self-certifying identifiers, or legacy identities backed with traditional PKI.

The most important class of identifier for verifiable credentials, however, is a decentralized identifier (DID). The W3C also hosts the Decentralized Identifier Working Group which is responsible for the Decentralized Identifiers (DIDs) 1.0 specification, soon to become a W3C recommendation as well.

1.5.1 Introduction to Decentralized Identifiers (DIDs)

Decentralized identifiers (DIDs) are a new type of identifier for verifiable, decentralized digital identity. DIDs can be used to digitally identify an enterprise, a human, an object, a machine, or data.

While their operations or storage may or may not be distributed in a topological sense, decentralized identifiers are defined by decentralization of their control mechanism, which differs sharply from traditional PKI centered on a hierarchical authority to issue and verify keys. Decentralized identifiers can be self-maintained and proven without the intervention (or knowledge) of their original issuers. Furthermore, decentralized identifiers and their infrastructure are sourced or controlled by more than one entity. This control may lie anywhere on a scale from highly centralized to highly decentralized, depending on the architecture of that particular "DID method" (see below) and system.

This definition is especially relevant to the ATP architecture which involves multiple entities that must use interoperable identifiers and their supporting infrastructure. Decentralized identifiers with decentralized supporting infrastructure provide flexible mechanisms for secure interoperability that traverse entity control boundaries and domains. This work may often use the term decentralized identifier as an abstract concept to mean an identifier under decentralized control. However, unless otherwise indicated, this work will use the term to refer to the **W3C DID (Decentralized Identifier)** specification or to a specific implementation.

The principal use case for a digital identity system is to provide a secure overlay for digital network interactions and transactions. A decentralized identifier with its supporting infrastructure is often referred to as a decentralized digital identity system. The security of an identifier and its supporting infrastructure are inextricably linked to the mechanisms of control over the identifier. Consequently, understanding the mechanisms for establishing authoritative control over each identifier in a decentralized identity system is a vital part of the ATP architecture design.

Within a decentralized identity system, disparate entities control some of the identifiers but in an interoperable way. Each entity may control a set of identifiers (in one or more namespaces), but the other entities still recognize those identifiers. In other words, each entity may be the sole controller of a set of different identifiers. Ideally, a decentralized identifier is one that the user issues and controls without deference to or permission from any other administrative organization.

Today, decentralized identity systems typically use one or more distributed-consensus ledgers in common (blockchains and/or DLTs) to anchor trust. The security properties of properly implemented distributed-consensus ledgers make exploits extremely difficult and costly, while enabling decentralized control over both the associated identifiers and the supporting infrastructure. One limitation of using a distributed consensus ledger as the trust basis for a decentralized identity system is that many times, the associated identifiers are locked to that ledger without portability and backwards-compatibility after a porting event from one ledger to another ledger. This places constraints on secure interoperability among participants. Either all participants must use identifiers from the same ledger, or all participant applications must provide support for the various trust bases engendered by each ledger, effectively federating a multi-fabric system.

DID methods actually have great flexibility and variety in how they store, delegate control over, and resolve DIDs. However, some can be used with multiple ledgers, or no ledger at all. A system that uses multiple DID methods needs to navigate and account for differing **security guarantees** of the associated DID methods before accepting them as equivalent or imposing limitations on their mutual recognition. These issues will be discussed in more detail below in the architecture sections.

The most secure decentralized identifiers are those whose root-of-trust is a **self-certifying identifier**. A self-certifying identifier is uniquely derived via cryptographic one-way functions from one or more public keys from asymmetrical (aka "public/private") key-pairs used in a cryptographic digital signature scheme. The derivation effectively cryptographically binds the identifier to the key-pairs(s), making the controller of the key-pairs(s) the sole controlling authority over the identifier and the source of truth for any of the identifiers cryptographic operations or data traces, including rotating its own key material. Thus, the identifiers are not only self-certifying, but the controller is the administrator, thus making the identifiers self-administrating. Originally proposed in the 1990's as a mechanism to avoid the centralization of the current DNS certificate authority system, self-certifying identifiers are inherently compatible with decentralized identity systems and provide a secure root-of-trust that is not dependent on administrative operational infrastructure.

DID documents are simple documents (technically, resolution transcripts, analogous to cached DNS records) that describe how that specific DID can be used to verify signatures, initiate communications, query a lookup table, etc. Each DID document may express **cryptographic material**, **verification methods**, and/or **service endpoints**. These also provide at least one mechanism for its controller to prove control. Service endpoints enable trusted interactions with the DID subject, with all the security and privacy considerations incumbent on a published, crawlable record of such addressable references. In the ATP credentialing pilot, we work with public DIDs representing '*enterprise identities*' for issuers and trading partners only.

The following diagrams illustrate key aspects of W3C DIDs:

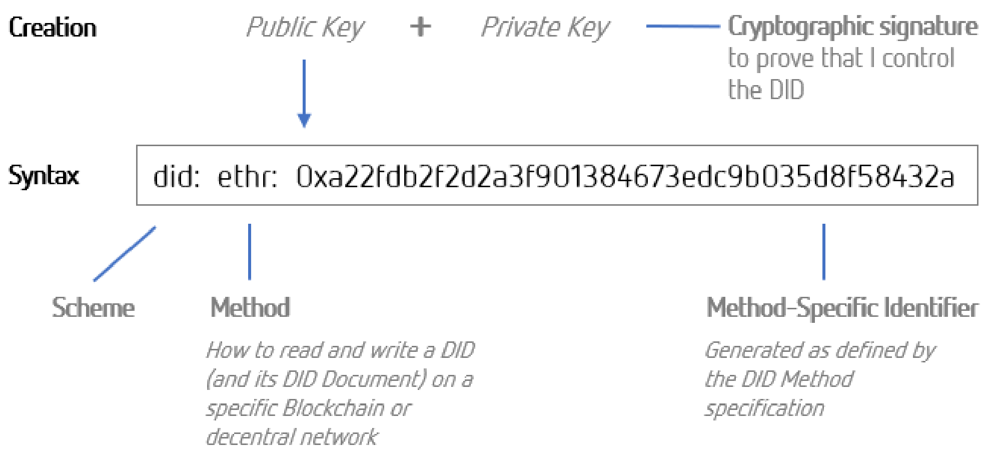

Creation
Public Key
+
Private Key
Cryptographic signature to prove that I control the DID
Syntax
did: ethr: 0xa22fdb2f2d2a3f901384673edc9b035d8f58432a
Scheme
Method
How to read and write a DID (and its DID Document) on a specific Blockchain or decentral network
Method-Specific Identifier
Generated as defined by the DID Method specification

Figure 2 DID Syntax

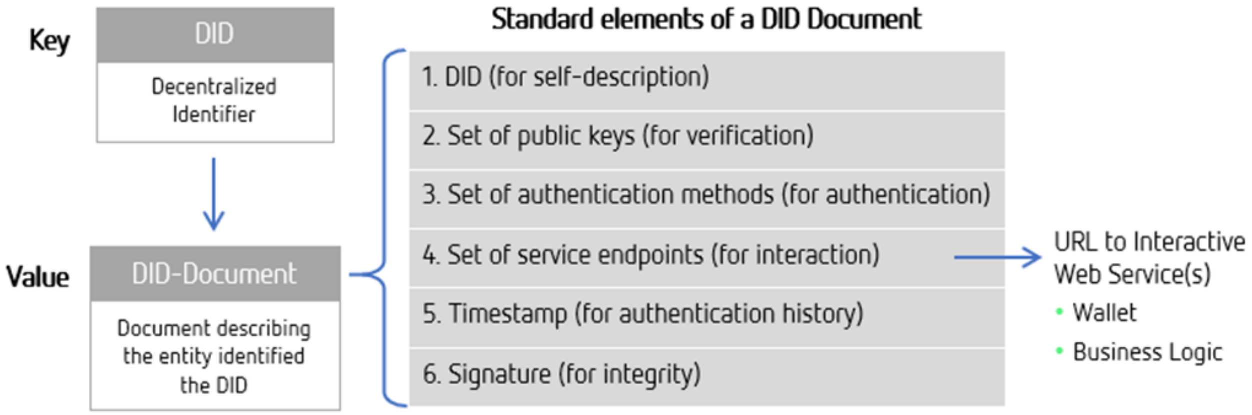

Key
DID
Decentralized Identifier
Value
DID-Document
Document describing the entity identified the DID
Standard elements of a DID Document
1. DID (for self-description)
2. Set of public keys (for verification)
3. Set of authentication methods (for authentication)
4. Set of service endpoints (for interaction)
5. Timestamp (for authentication history)
6. Signature (for integrity)
URL to Interactive Web Service(s)
Wallet
Business Logic

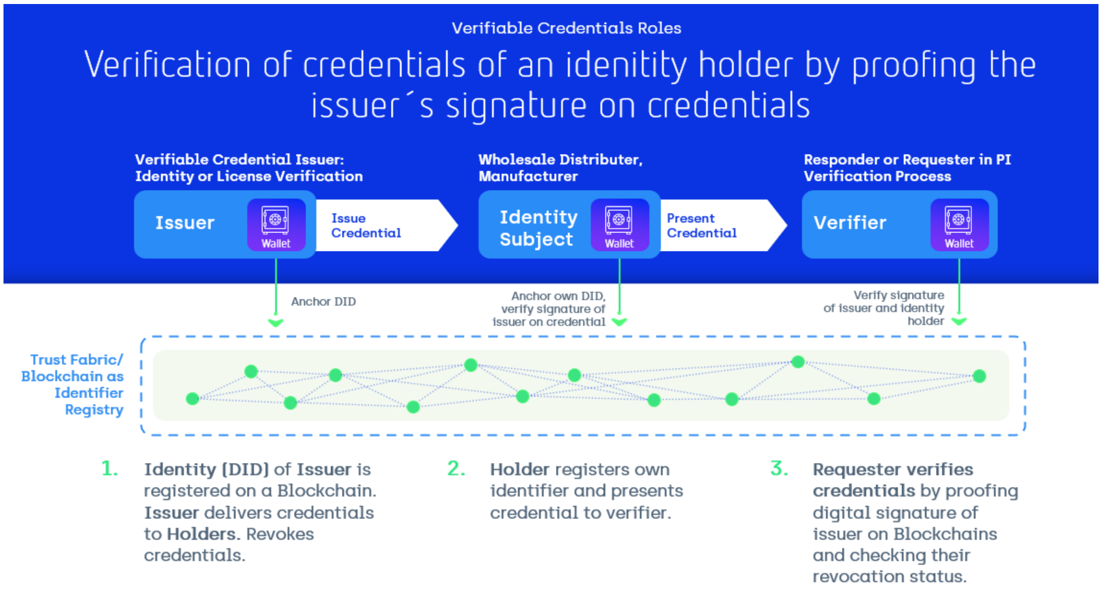
Figure 3 DID Document Structure

1.5.2 Introduction to Verifiable Credentials (VCs)

The term **Verifiable Credential (VC)** was first popularized by the W3C verifiable credential working group and is strongly associated with the W3C VC standard. In this work, Verifiable Credential (VC) both abstractly and concretely refers to the W3C standard depiction unless specifically indicated otherwise. For example, an “ersatz verifiable credential” would have similar functionality but may not follow the standard specification. The core concept of a verifiable credential is that it is a block of verifiable data attributes cryptographically bound to the identities of the owner, the issuer, and optionally to other parties.

A verifiable credential is not limited to conventional credentialing applications like a university transcript or a business license but may be used for any application where data benefits from being **verifiable**. In this context, asymmetric digital signatures make any payload's provenance and authorship cryptographically verifiable, and in most implementations, strongly timestamped.

The signature on each verifiable credential provides two essential properties. The first is **data integrity**. Any changes to the block of data will cause the signature verification to fail. So, any tampering with the data will be detectable by the verifier. The second property is **non-repudiation**. If kept private, only the controller of the private key may create a signature that is verifiable against the public key. The controller-and-signer can therefore not repudiate (deny) their signature. In this sense, any digitally signed data is verifiable data insofar as it is anchored to a trusted PKI. The VC standard, however, specifies interoperability features including privacy, in addition to mere verifiability, and offers much implementation freedom relative to how these guarantees are secured.



Verifiable Credentials Roles

Verification of credentials of an idenitity holder by proofing the issuer´s signature on credentials

Verifiable Credential Issuer: Identity or License Verification
Wholesale Distributer, Manufacturer
Responder or Requester in PI Verification Process
Issuer
Wallet
Issue Credential
Identity Subject
Wallet
Present Credential
Verifier
Wallet
Anchor DID
Anchor own DID, verify signature of issuer on credential
Verify signature of issuer and identity holder
Trust Fabric/ Blockchain as Identifier Registry

1. **Identity (DID)** of **Issuer** is registered on a Blockchain. **Issuer** delivers credentials to **Holders**. Revokes credentials.
2. **Holder** registers own identifier and presents credential to verifier.
3. **Requester verifies credentials** by proofing digital signature of issuer on Blockchains and checking their revocation status.

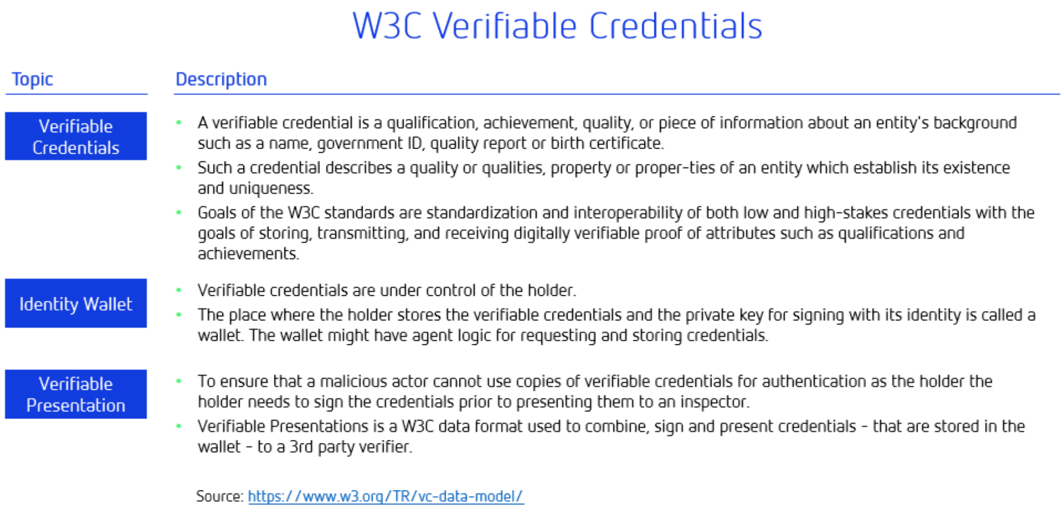
Figure 4 Verifiable Credential Roles

There are three participants in the VC operational mode: **Issuer**, **Holder**, and **Verifier**. The Issuer first creates and signs a VC designated for a given Holder and then issues it to the Holder, usually synonymous with the data subject. The Holder may then "carry" the VC, choosing when and where to present it for verification to any given Verifier. The Verifier may then establish that the VC is valid without interacting with the Issuer. This enables privacy for the Holder, with respect to the Issuer, in the Holder's usage of its VCs. In the diagram depicted above, the identity subject and verifier can both be either a "responder" or "requester".

VCs may be described as an **interoperable** and widely **portable** vessel for verifiable data. Standard VCs are most represented in JWT, JSON-LD or CBOR encodings. JWT is more lightweight and backwards-compatible, while JSON-LD enables extensible data schema for interoperability and semantic agility. By registering a schema, a VC Issuer may publish the semantics of the data attributes of a given credential or credential class.

VCs are presented as so-called **W3C verifiable presentations** which might include data derived from one or more verifiable credentials, issued by one or more issuers, that is shared with a specific verifier. A verifiable presentation is a tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. In the ATP credentialing pilot, we are planning to use one VCs in a verifiable presentation only (e.g., verifiable presentation with one ATP credential). Registered or published schemata are one way of helping Holders to combine data attributes from multiple credentials into a single **verifiable presentation** to a Verifier. The Verifier may then validate that the attributes share the same semantics, even if the source credentials come from different issuers, encodings, and trust fabrics. This type of semantic interoperability (enforced at the point of presentation/verification rather than at the level of storage) makes VCs usable for almost any application where data is shared across entity application domains. However, it must still be cryptographically verifiable both in syntax and semantics. Verifiable presentations are more dynamic and ephemeral than verifiable credentials, more like events than documents, but they can be cached or even generate new verifiable credentials making different claims at different levels of assurance or trust and anchored to other trust fabrics.

A VC uses several identifiers. These include the identifier of the Issuer, and the identifier of the Holder to whom the VC is issued. (If the Holder is not the data subject, implementations and regulatory frameworks differ, but usually a third identifier is needed for clean and explicit distribution of responsibilities.). Depending on the application, a VC may include other identifiers as well, including complex references related to the above-mentioned semantic portability features. All of these identifiers must be bound to asymmetric cryptographic (public, private) key-pairs. Decentralized Identifiers (DIDs) are a natural fit for VCs, especially when multiple entities need to interoperate in a decentralized environment and/or where privacy is important, but legacy identifiers bound less structurally to cryptographic key material are also easily incorporated as needed by the application.



W3C Verifiable Credentials

Topic	Description
Verifiable Credentials	• A verifiable credential is a qualification, achievement, quality, or piece of information about an entity's background such as a name, government ID, quality report or birth certificate. • Such a credential describes a quality or qualities, property or proper-ties of an entity which establish its existence and uniqueness. • Goals of the W3C standards are standardization and interoperability of both low and high-stakes credentials with the goals of storing, transmitting, and receiving digitally verifiable proof of attributes such as qualifications and achievements.
Identity Wallet	• Verifiable credentials are under control of the holder. • The place where the holder stores the verifiable credentials and the private key for signing with its identity is called a wallet. The wallet might have agent logic for requesting and storing credentials.
Verifiable Presentation	• To ensure that a malicious actor cannot use copies of verifiable credentials for authentication as the holder the holder needs to sign the credentials prior to presenting them to an inspector. • Verifiable Presentations is a W3C data format used to combine, sign and present credentials - that are stored in the wallet - to a 3rd party verifier.

Source: https://www.w3.org/TR/vc-data-model/

Figure 5 Introduction to Verifiable Credentials

A credential is a set of one or more claims made by an issuer about a data subject, which is usually the holder. In the ATP pilot, we will have two primary types of credentials:

1. Identity verification credential (enterprise Know Your Customer (KYC))
2. ATP credential for both WHOs (State license) and MANs (FDA Establishment Identifier (FEI)

Note: In a later stage of the ATP credentialing roll-out, delegated authority credentials might be introduced. For instance, a VRS service provider could present a credential on behalf of a WHO or MAN, like a "power of attorney" to sign certain kinds of transactions or credentials.

To establish an efficient **verifiable presentation protocol** for enabling the underlying credentials to be maximally portable and flexible, we have designed a custom verifiable presentation instrument specific to this pilot that incorporates the VRS process as it stands today and takes advantage of existing opaque serialization methods and correlation unique user IDs (corrUUIDs). This is particularly important to forward-compatibility, regardless of when or whether other VC-based credentialing systems become central to other cross-silo data exchange systems in the pharmaceutical industry.

Verifiable credentials include an **expiration date** that is validated when the underlying credential is verified. (Similarly, verifiable presentations often include instructions about when and for how long they are expected to be cached.) Besides, VCs are subject to a **revocation mechanism** to enable an issuer to revoke (cancel) a credential. A revocation mechanism will be used in the ATP pilot project, such as in the case that a State Board of Pharmacy revokes a state license. Checking to ensure that a VC has not been revoked is part of the validation process at the time a VC is presented.

When a **credential or presentation** is being **verified**, the verifier needs to check first and foremost the identity of the credential issuer (i.e., does the DID really belong to the VC issuer). This means that a verifier needs to have the instruments to check the DID (e.g., by looking it up in a registry governed by a trusted source or requesting a verifiable identity credential about the VC issuer which can in turn be verified the same way). We recommend adopting the IETF 'well-known' standard developed by Internet Engineering Task Force (IETF) to establish **trust anchors** for the verifiers and describe options for establishing the root of trust in the alternative architecture sections.

1.5.3 Definition of Roles with regard to VC Credentialing

A **credential** is a digital assertion containing a set of claims (e.g., about a state license or FDA Establishment Identifier) made by an entity about itself or another entity. Credentials are a subset of identity data. The entity described by the claims is called the **subject** of the credential.

A **holder** can refer to the subject, or to others who hold a credential on behalf of its subject, or to third parties authorized to cache or hold a credential that has been presented to them. The holder may or may not be the subject of the credential. There are many use cases in which the holder is not the subject, e.g., a birth certificate where the subject is a baby, and both the mother and father may be holders.

An **issuer** is an entity that creates a credential for use by its intended holder.

A **relying party** or **verifier** is generally the entity to whom a verifiable credential is presented (i.e., the party making decisions based on the claims and its degree of trust in the credential). A verifier requests a credential or proof from a holder and verifies it to make a trust decision about the subject entity.

A **regulatory body** is an entity that establishes a legal requirement for the subject to be registered or licensed in a particular field (i.e., the FDA or State Board of Pharmacy.) An issuer is responsible for checking the status of such registrations and licenses prior to issuing VCs to WHO and MAN entities.

1.5.4 Introduction to Identity Wallets

Enterprise identity using DIDs, and VCs requires a digital identity wallet that manages and protects the public/private key pairs, to prove control over DIDs, to sign access tokens for authenticating an entity's identity, and to issue verifiable credentials and presentations. In some systems, this last function is handled by a distinct issuer/verifier module, but they are integrated into a more usable, combined interface in this solution.

At its core, an **identity wallet** is a software module, and optionally an associated hardware module, for securely storing and accessing private keys, link secrets, other sensitive cryptographic key material, and other private data used by an entity. Most wallets also handle, present, and verify credentials and different kinds of information as well.

A wallet is accessed and controlled by a **software agent**. This software agent provides ways to request, accept, store, and navigate credentials, as well as issue/delegate verifiable credentials. The agent provides further ways of authenticating humans and enterprise systems and controlling access to the data used by the agent. In this handbook, the software combining key management, credential management, issuance, and a cloud agent is referred to **holistically** as an "Identity Wallet". The agent contains a DID driver to connect to a blockchain for DID document anchoring, credential schema/definition anchoring, and interaction with verifiable registries.

As the terminology is still evolving and the identity wallet also stores and exchanges data in the form of verifiable credentials it shall be understood that other terms refer to the same concept as well: Identity Vault, Data Vault, Secure Data Vault, Identity Hub or Secure Data Storage.

In the ATP Credentialing Pilot implementation, the identity wallet will integrate the infrastructures of both:

- the Verifiable Credential Issuers, and
- the VRS service providers.

The PI verification process will be fully automated. The wallet credentials process will be integrated via APIs with the VRS systems. This means that there is no direct UI integration between a wallet and a WHO or MAN required for the PI verification process.

WHO or MAN business administrators have access to their respective wallets via a **simple browser-based user interface** to perform wallet administration tasks, acquire ATP credentials, and review their credentials' status. Verifiable Credential Issuers will use a similar UI to administer their wallet, receive credential requests, and issue credentials. The processes of the Verifiable Credential Issuers will be a manual workflow in the ATP pilot phase.

1.6 Participating Stakeholders & their Roles in the ATP Pilot Project

It is foreseen that the following stakeholders will participate in the ATP pilot project:

#	Role	Description	Primary Roles wrt/ VCs	Company
1	Verifiable Credential Issuer (VCI)	● Perform identity verification ● Perform state license verification ● Perform FEI license verification	● Issuer	Legisym
2	Wholesaler (WHO)	● Acquire, store, present, verify ATP credentials	● Identity and credential holder ● Verifier	AmerisourceBergen
3	Manufacturer (MAN)	● Acquire, store, present, verify ATP credentials	● Identity and credential holder ● Verifier	Bristol-Myers Squibb, Johnson & Johnson, Merck, Novartis
4	VRS Service Provider	● Provide Saleable Return Verification Requests and Responses ● Enrich Verification Requests and Responses with ATP credentials through integration of wallet APIs ● Verify ATP credentials	● Create PI Verification Message ● Enriched GS 1 message with Credential Presentation	Rfxcel, SAP
5	Identity Wallet Provider	● Provide Identity Wallets to create Enterprise Identities (DIDs) for WHOs, MANs and Verifiable Credential issuers ● Provide functionality to request, issue, revoke and verify ATP credentials	● Wallet infrastructure provider ● Permissioned test ledger operator	Spherity
6	State Board of Pharmacy	● Act as simulated governance body	● Governance body	./.
7	FDA	● Act as simulated governance body	● Governance body	./.

2 Enterprise Architecture Context

2.1 Business Architecture Context

Per the United States Drug Supply Chain Security Act (DSCSA), wholesale distributors are required to verify the serial number on saleable returns before selling the product back into the supply chain. Manufacturers must make the serial number data available for verification.

The industry is aligned on an ecosystem that consists of multiple Verification Routing Services (VRS) provided by various solution providers. Within this ecosystem, a wholesale distributor (requester) initiates a verification request (VR) that its VRS solution provider potentially routes to another VRS and from there to a repository that holds the required information to provide a response (VRR) which is owned by a Manufacturer (MAN, responder).

In this context, it must be ensured that both parties, wholesale distributor and manufacturer alike, are strongly identified to be the authorized entity. This authentication effectively excludes bad actors from the ecosystem.

The verification process's challenge is that the receivers of verification requests or responses do not know if the sender of such a request holds a valid state or FDA license to indicate that they are an authorized trading partner. Today, manufacturers receive a verification request (VR) without any reliable information about the sender and must manually authenticate them out of band. The VR only includes a GLN (Global Location Number) which is **NOT** a reliable and secure identifier, as GLNs are basically public and can be used by anyone.

As the interactions for Saleable Return Verification are not necessarily executed among established business relationships, no one can strongly identify the requester or responder of a request. There is no unique and verifiable identifier of a legal entity attached to the interaction. As a result, it cannot be guaranteed that interactions for PI verification purposes are taking place only among authorized trading partners as required by the DSCSA.

In the context of verification of saleable returns, the industry uses the terms **requester** and **responder**. A MAN responds to verification requests, acting as a responder, while a wholesale distributor (or a dispenser) requests PI verification, thus acting as a requester. Within this architecture handbook, the terms "requester" and "responder" are referenced to identify the users' roles in a PI verification process. Therefore, the acronym WHO can be understood as a synonym for the requester and the acronym MAN as a synonym for the responder.

2.1.1 Overview

The implementation of new business capabilities is not foreseen with this ATP pilot. Instead, the existing capabilities will be enhanced with new functionalities such as Authorized Trading Partner verification in the Verification of Saleable Returns process. This section includes an abstraction of the Business Capabilities of the WHO and MAN roles, and is not intended to describe a particular WHO or MAN.

The ATP credentialing features can be mapped to existing WHO and MAN business capabilities as highlighted in the model below.

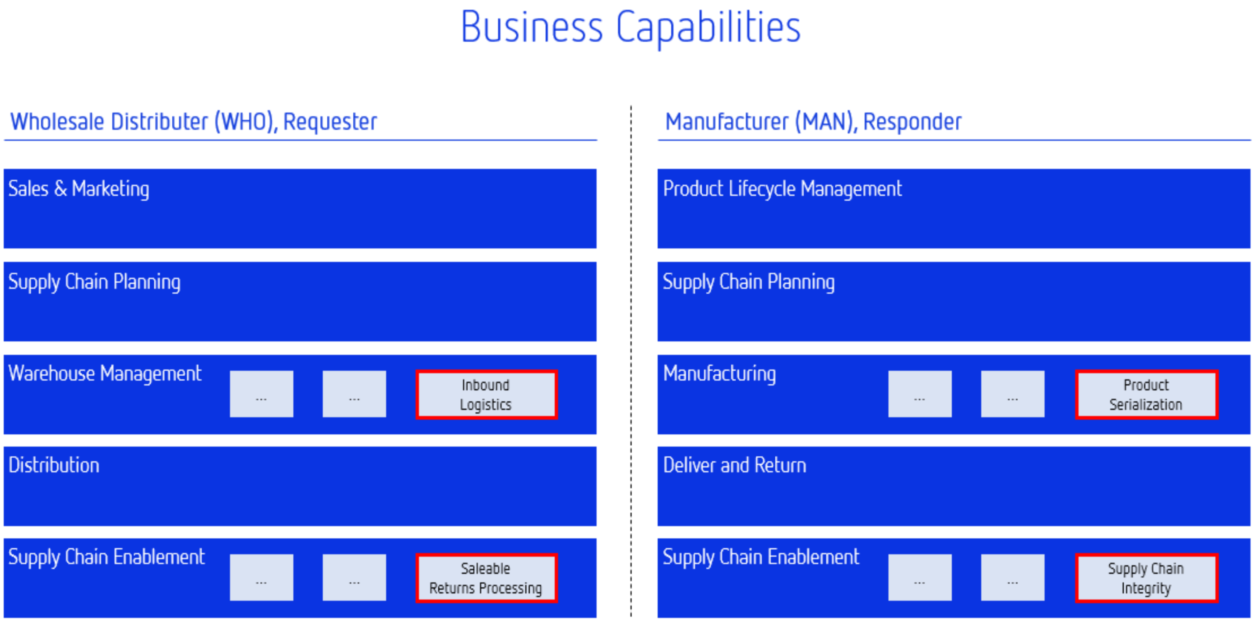


Figure 6 Business Capability Overview

2.1.2 Details: Business Capabilities

This table outlines Business Capabilities and Processes in scope of ATP credentialing pilot:

#	Business Capability / Process	Entity	In Scope	Purpose
1	Saleable Returns Processing	WHO	Yes	Ability to plan, manage and control saleable return transactions and their respective logistics.
2	Inbound Logistics	WHO	Yes	Ability to plan, manage, track and verify inbound logistics transactions and events.
3	Product Serialization	MAN	Yes	Ability to apply a unique serial number to each individual product sales pack. The unique number on the sales pack is created by using “entropy” and is used to register product locations and trading partners in a cross-industry database, from packaging site to pharmacy level.
4	Supply Chain Integrity	MAN	Yes	Ability to comply with drug serialization and reporting requirements – and fight counterfeiting and illicit trade. Track and trace systems platform integrates serialization data to provide country-ready reporting packages, minimizing the cost of compliance, increasing pharma supply chain security, improving patient safety, and managing Saleable Returns processes.
5	Compliance Management	VCI	Yes	Ability to verify a State Board of Pharmacy or FDA license status of either a WHO or MAN.

The ATP pilot will implement add-ons to the existing saleable returns processes:

- ATP Credential Management (WHO, MAN)
- ATP Saleable Return PI Verification (WHO, MAN)
- ATP Verifiable Credential Issuance (VCI)

#	Sub-Capability / Process	Entity	In Scope	Purpose
1	Saleable Returns Processing – ATP Credential management, ATP Credential acquisition and maintenance	WHO	Yes	Ability to acquire and manage the enterprise identity (DID) and the ATP credentials (VCs). Ability to report discrepancies in the license status of responding MANs.
2	Inbound Logistics – ATP Saleable Return PI Verification	WHO	Yes	Ability to add an ATP credential to inbound PI verification request and to process the PI verification via a VRS provider. Ability to verify an ATP credential of the MAN in a PI verification request response.
3	Product Serialization – ATP Saleable Return PI Verification	MAN	Yes	Ability to check the license status of a requesting WHO prior to answering a PI verification request that is orchestrated via a VRS provider. Ability to add an ATP credential to the verification request response.
4	Supply Chain Integrity – License Management, ATP Credential Acquisition	MAN	Yes	Ability to acquire and manage the enterprise identity (DID) and the ATP credentials (VCs). Ability to report discrepancies in the ATP status of requesting WHOs.
5	License verification – ATP Verifiable Credential Issuance	VCI	Yes	Ability to issue ATP credentials in form of a W3C VC after verification of enterprise identity, its corresponding DID, and license status.

2.1.3 Details: ATP Credential Issuance

In the ATP pilot, WHO and MAN shall manage their ATP credentials. In case they do not have a credential, a credential expires, or it was revoked, they will request a (new) ATP credential.

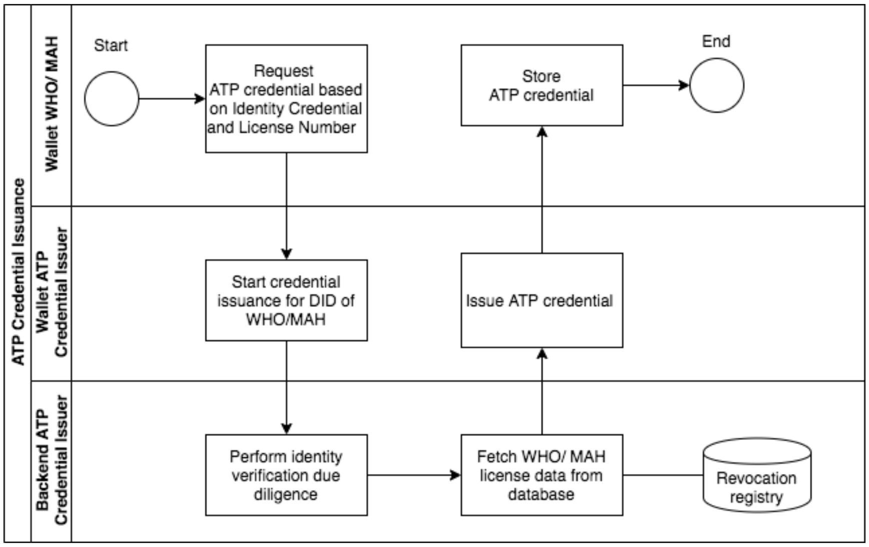

ATP Credential Issuance
Wallet WHO/ MAH
Wallet ATP Credential Issuer
Backend ATP Credential Issuer
Start
Request ATP credential based on Identity Credential and License Number
Store ATP credential
End
Start credential issuance for DID of WHO/MAH
Issue ATP credential
Perform identity verification due diligence
Fetch WHO/ MAH license data from database
Revocation registry

Figure 7 ATP Credential Acquisition & Issuance Process

Enterprise Identity Verification:

Prior to credential issuance, the WHO or MAN's DID identifier needs to be verified by following an **identity verification process**.

The enterprise identity verification can be done either by the VCI or by a 3rd party identity verifier provider. In the pilot, the VCI may use existing identity certificates such as the DEA signing certificate or DIDs in combined with manual, paper-based identity verification processes to prove the WHO or MAN's digital identity.

In an alternative implementation, a 3rd party identity verifier of a different type (e.g., GLEIF in the financial sector or GS1) will perform an enterprise identity verification and issue identity credentials. The introduction of other means (GLEIF specifically) means that the governance body needs to decide based on the new method's due diligence SOP. Their decision to include other methods will impact the ATP credential due diligence and cost.

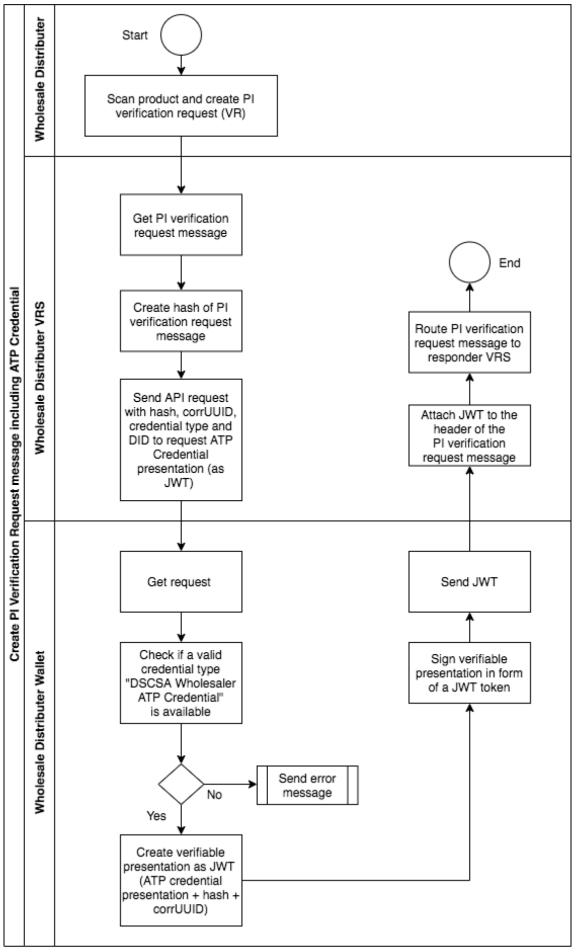
As of now, the assumption is that the VCI will do this enterprise identity process. The enterprise identity verification process is NOT shown in the diagram above; options for identity verification will be discussed under architecture alternatives.

The VCI will issue enterprises identity credentials which are used in the pilot as the root of trust for the ecosystem. If it was to be removed via governance decision, then the due diligence performed for identity credentials will move to the ATP credential process. We consider such a combination of identity and ATP credentials into one credential not as best practice as this is an inefficient process when working with different credential types for different use cases.

2.1.4 Details: ATP Saleable Return License Verification Process Flow

GS1 provides a standardized Lightweight Verification Message format that can be easily implemented by all VRS providers. The required credentials can be added to the message header, leaving the message body unchanged, to ensure quick implementation with this approach, the ATP credentials can augment the existing PI verification request and response process flows to minimize the impact on any other automated or manual processes.

The PI request process is depicted in the figure below:


Create PI Verification Request message including ATP Credential
Wholesale Distributer
Start
Scan product and create PI verification request (VR)
Wholesale Distributer VRS
Get PI verification request message
Create hash of PI verification request message
Send API request with hash, corrUUID, credential type and DID to request ATP Credential presentation (as JWT)
End
Route PI verification request message to responder VRS
Attach JWT to the header of the PI verification request message
Wholesale Distributer Wallet
Get request
Check if a valid credential type "DSCSA Wholesaler ATP Credential" is available
No
Send error message
Yes
Create verifiable presentation as JWT (ATP credential presentation + hash + corrUUID)
Send JWT
Sign verifiable presentation in form of a JWT token

**) Other credential types:*
• DSCSA Manufacturer ATP Credential
• DSCSA Dispenser ATP Credential

Figure 8 PI Request Message Augmentation

For recurring requests to create a verifiable presentation, the ATP credential can be **cached** in memory so that the API latency will be reduced to just the time required to sign a verifiable credential and associated hash.

Prior to creating a PI request-response, the ATP credential in the PI request header will be verified:

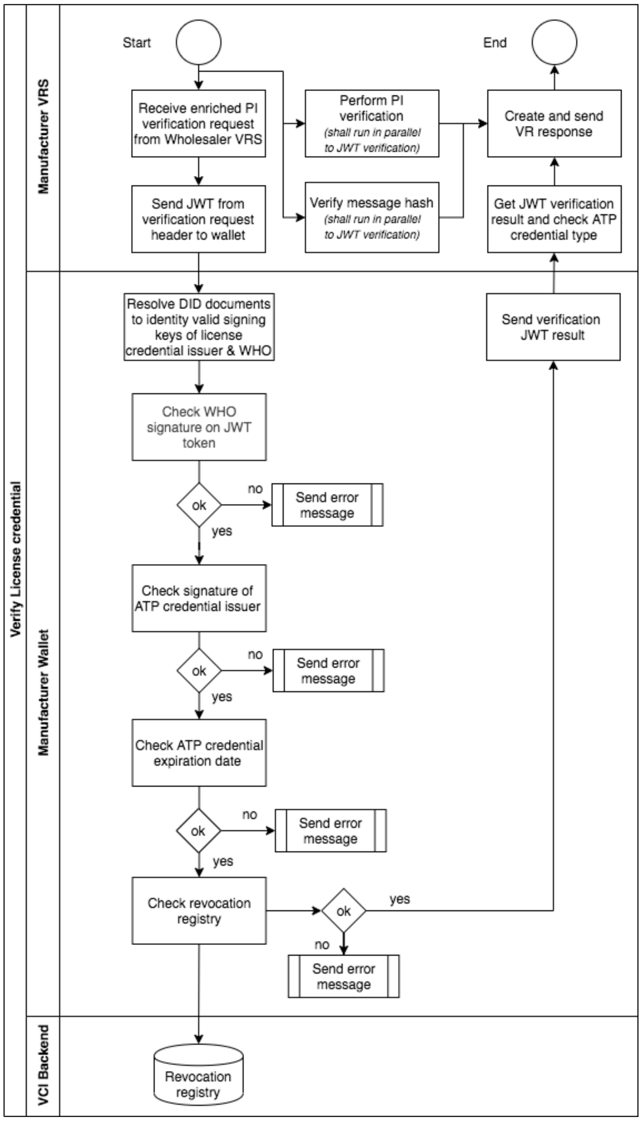

Verify License credential
Manufacturer VRS
Manufacturer Wallet
VCI Backend
Start
End
Receive enriched PI verification request from Wholesaler VRS
Perform PI verification (shall run in parallel to JWT verification)
Create and send VR response
Send JWT from verification request header to wallet
Verify message hash (shall run in parallel to JWT verification)
Get JWT verification result and check ATP credential type
Resolve DID documents to identity valid signing keys of license credential issuer & WHO
Send verification JWT result
Check WHO signature on JWT token
ok
no
yes
Send error message
Check signature of ATP credential issuer
ok
no
yes
Send error message
Check ATP credential expiration date
ok
no
yes
Send error message
Check revocation registry
ok
yes
no
Send error message
Revocation registry

Figure 9 ATP credential verification

It shall be understood that the ATP credential (ATP credential presentation in form of a JWT token) verification can be **run in parallel** to the regular PI verification as it is today. Also, the VRS business logic shall verify the message hash and whether the right credential type for a given use case (here: ATP verification) was provided in the request. For recurring ATP verification requests, the DID resolution and the revocation check can be cached to prevent additional latency for recurring verifications.

The PI ATP credential verification must be compliant with **audit and national reporting requirements**. That means that the PI verification events, and data sets must be archived in accordance with audit and data retention and archiving requirements.

It shall be understood that in the PI Request Message Augmentation workflow, the VRS system can provide either the entire message body or a hash of the message body to the wallet. For security and data minimization, it is recommended to provide only the **message hash** to the wallet to create a verifiable presentation. We recommend using **SHA256** as a secure NIST-compliant hash-function

for hashing the message body.

The charts above describe the ATP status verification when the wholesale distributor sends a PI verification request to the manufacturer. According to DSCSA the wholesale distributor must also check the manufacturer's ATP status that is sending the PI verification response. As this is a **symmetric** ATP verification requirement, a very similar process will be performed to augment the manufacturer's ATP credential with the PI verification response.

All possible ATP check cases shall be addressed by the system’s business logic:

Cases	PI Request by Wholesale Distributor		Pi Response by Manufacturer		PI VRS Request		Result
	ok	failed	ok	failed	ok	failed	
1	x		x		x		VRS ok
2	x		x			x	VRS failed
3	x			x	x		VRS failed
4	x			x		x	VRS failed
5		X	x		x		VRS failed
6		x	x			x	VRS failed
7		x		x	x		VRS failed
8		x		x		x	VRS failed

For future pharmaceutical supply chain use cases, the solution will be more extensible, allowing the attachment of **different credential types** and/or **multiple/chained credentials** in the form of a verifiable presentation for the PI verification process. This requires implementing **business logic** on the VRS side to select the correct credential for a given use case and verify that the right credential type was presented on the verifier side as well.

The system shall be designed in a way that it supports FDA or state credential types or other derived credentials so that it can be reused for other contexts and use cases as well:

1. PI Verify - Salable Returns *(scope of the ATP credentialing pilot project)*
2. TI Verify - Investigations
3. TI Transfer
4. TI Request
5. Drop Shipments

2.2 Application Architecture Context

The Application Architecture Context defines how the existing WHO and MAN (and VCI) systems integrate with the additional functional ATP credentialing processes and the supporting identity wallet and credential infrastructure.

2.2.1 Overview

The diagram below describes how enterprise identity wallets for ATP credential management are integrated with the existing PI verification systems of WHO, MAN, VRS provider, and VCI.

The VRS systems support various integration capabilities, such as content-based routing and mapping of the PI verification requests, and several connectivity options, providing standardized integration with other VRS providers. VRS systems are cloud-based multi-tenant solutions. Each WHO or MAN customer will have its own tenant that is integrated via APIs with the respective backend system of the WHO or MAN.

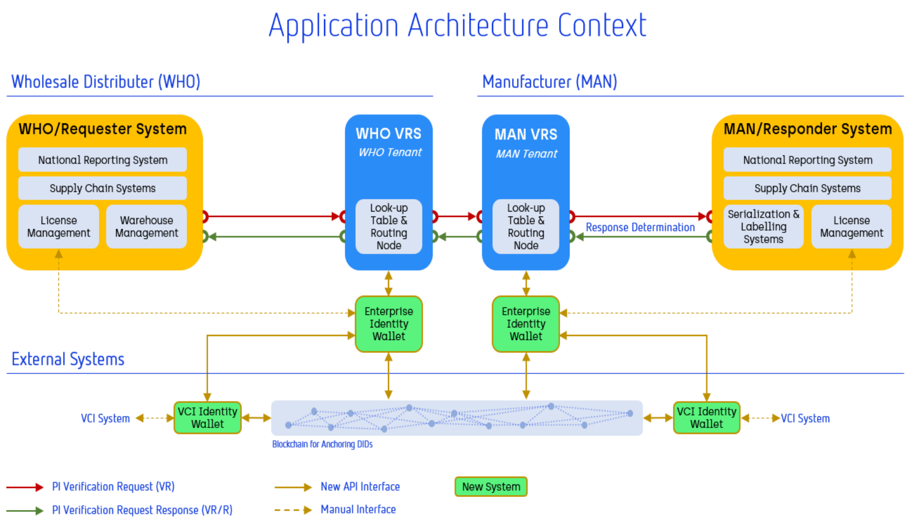

Application Architecture Context
Wholesale Distributer (WHO)
Manufacturer (MAN)
WHO/Requester System
National Reporting System
Supply Chain Systems
License Management
Warehouse Management
WHO VRS
WHO Tenant
Look-up Table & Routing Node
MAN VRS
MAN Tenant
Look-up Table & Routing Node
Response Determination
MAN/Responder System
National Reporting System
Supply Chain Systems
Serialization & Labelling Systems
License Management
Enterprise Identity Wallet
Enterprise Identity Wallet
External Systems
VCI System
VCI Identity Wallet
Blockchain for Anchoring DIDs
VCI Identity Wallet
VCI System
PI Verification Request (VR)
PI Verification Request Response (VR/R)
New API Interface
Manual Interface
New System

Figure 10 High Level Application Architecture Context

Following the minimally invasive adoption principle, the identity wallets will be integrated via APIs to the VRS provider system so that ATP credentials can be attached to the GS1 lightweight verification protocol in a very efficient way. For the management of ATP credentials, a web UI and manual process will be implemented. Consequently, there will be minimal customization requirements and changes to the WHO and MAN's existing infrastructures.

Additional API integration will be implemented between the enterprise wallets and the Verifiable Credential Issuers' wallets for ATP credentials acquisition.

In the longer-term manual processes, tighter control, and integration of the Enterprise Identity Wallet with the WHO and MAN infrastructure can be implemented. These options will be described under architecture alternatives in this handbook.

2.3 Data Architecture Context

2.3.1 Overview

As the pilot will focus on a minimally invasive integration of ATP credentials with existing VRS systems and PI verification processes, the high-level data architecture context can be described as below:

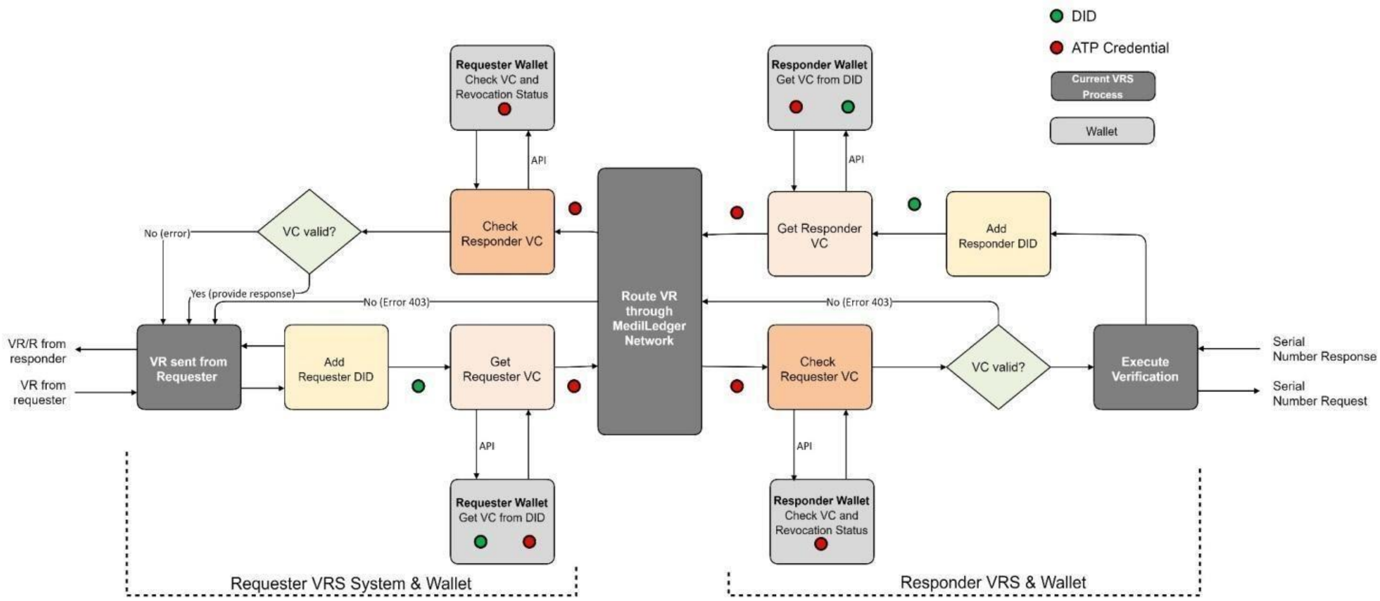


Figure 11 High Level Data Architecture Context for Requester-Responder ATP Credentialing

2.3.2 Details

The following figure describes the broader data architecture context in more detail:

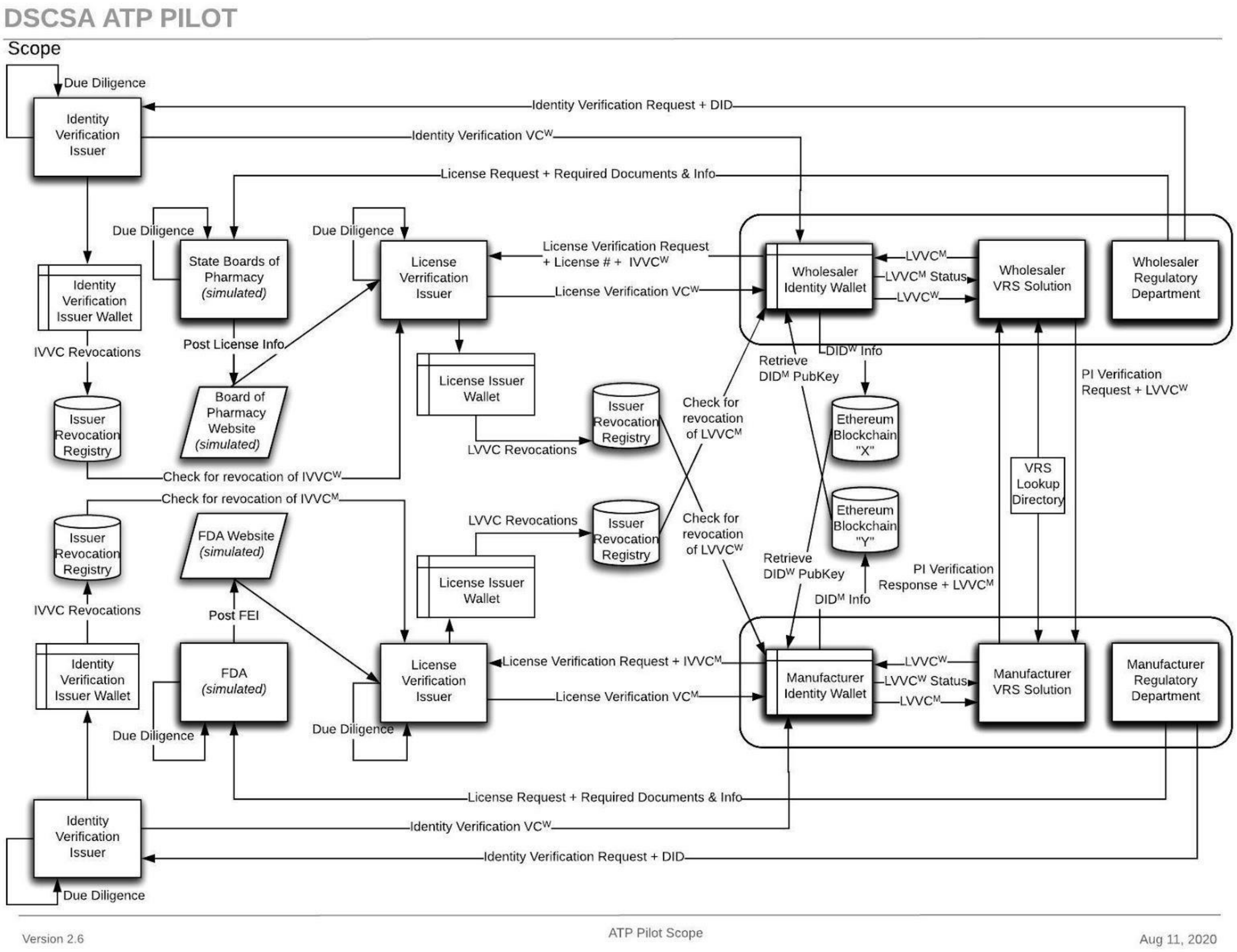

DSCSA ATP PILOT
Scope
Due Diligence
Identity Verification Issuer
Identity Verification Request + DID
Identity Verification VC^{W}
License Request + Required Documents & Info
Due Diligence
State Boards of Pharmacy (simulated)
Due Diligence
License Verification Issuer
License Verification Request + License # + IVVC^{W}
License Verification VC^{W}
Identity Verification Issuer Wallet
Post License Info
IVVC Revocations
Issuer Revocation Registry
Board of Pharmacy Website (simulated)
License Issuer Wallet
LVVC Revocations
Issuer Revocation Registry
Check for revocation of IVVC^{W}
Check for revocation of IVVC^{M}
Check for revocation of LVVC^{M}
Wholesaler Identity Wallet
LVVC^{M}
LVVC^{M} Status
LVVC^{W}
Wholesaler VRS Solution
Wholesaler Regulatory Department
Retrieve DID^{M} PubKey
DID^{W} Info
Ethereum Blockchain "X"
PI Verification Request + LVVC^{W}
VRS Lookup Directory
Issuer Revocation Registry
FDA Website (simulated)
LVVC Revocations
Issuer Revocation Registry
Check for revocation of LVVC^{W}
Ethereum Blockchain "Y"
Retrieve DID^{W} PubKey
PI Verification Response + LVVC^{M}
DID^{M} Info
IVVC Revocations
Post FEI
License Issuer Wallet
Identity Verification Issuer Wallet
FDA (simulated)
License Verification Issuer
License Verification Request + IVVC^{M}
License Verification VC^{M}
Manufacturer Identity Wallet
LVVC^{W}
LVVC^{W} Status
LVVC^{M}
Manufacturer VRS Solution
Manufacturer Regulatory Department
Due Diligence
Due Diligence
License Request + Required Documents & Info
Identity Verification Issuer
Identity Verification VC^{W}
Identity Verification Request + DID
Due Diligence
Version 2.6
ATP Pilot Scope
Aug 11, 2020

Figure 12 Detailed Data Architecture Context

In the above figure, the Verifiable Credential Issuer is depicted as two separate entities - one which issues an identity credential (Identity Verification Issuer) and one which issues an ATP credential (License Verification Issuer.) This separation serves three important purposes:

1. It allows license-checking organizations in the industry to offer their services without requiring them to undertake the much more onerous task of becoming an identity certifying authority,
2. It allows onboarding of trading partners well ahead of the point at which they need to present an ATP credential, and
3. It dramatically reduces the time required to issue an ATP credential.

The ATP credentialing workflow's overall objective is to prove that a trading partner is authorized by presenting an ATP credential that reflects that the trading partner has one or more valid state or ATP credentials.

The ATP pilot project plans to use company identity verification credentials to prove the trading partner's identity and the ATP credentials. Credentials in the ATP pilot project will be constructed in accordance with the following list of data objects summarized in the table below (draft list of credential attributes):

#	Company Identity Credential	ATP credential
1	Credential ID	Credential ID
2	Credential Type	Credential Type
3	Issuer DID	Issuer DID
4	Credential Issuance Date	Credential Issuance Date
5	Credential Expiration Date	Credential Expiration Date
6	Subject Company DID	Subject Company DID
7	Subject Company Name	Subject Company Name
8	Subject Company Address	Subject Company Address
9	Subject Company Contact	Corporate Entity GLN (optional)
10	Due Diligence Source (DEA Signing Cert., Corp Documents)	Revocation Status
11	Due Diligence Signature	Issuer Signature
12	Revocation Status	./.
13	Issuer Signature	./.

The exact credential data structure will be defined in the ATP pilot design phase. In addition to the data structure the granularity of the credentials (corporate level vs location) still needs to be decided by the project.

The Identity and License verification credentials can potentially be combined in a PI verification process. However, the ATP credential alone will suffice when the VCI who issued the credential is accepted as a root of trust.

To achieve data portability, the credential's data structure will be formalized in a **credential schema**. In a best-case scenario, the industry will agree on schemas that will also be acceptable by the State Boards of Pharmacy or the FDA. For the pilot, the schemas will be designed with the VCI and the pilot team.

2.4 Technology Architecture Context

2.4.1 Overview

Wallets are the only add-on technology to the existing system for Saleable Returns. All the other technology components remain unchanged.

The identity wallet is bundling the following technologies and providing APIs that can be consumed by the VRS system (or the VCI system).

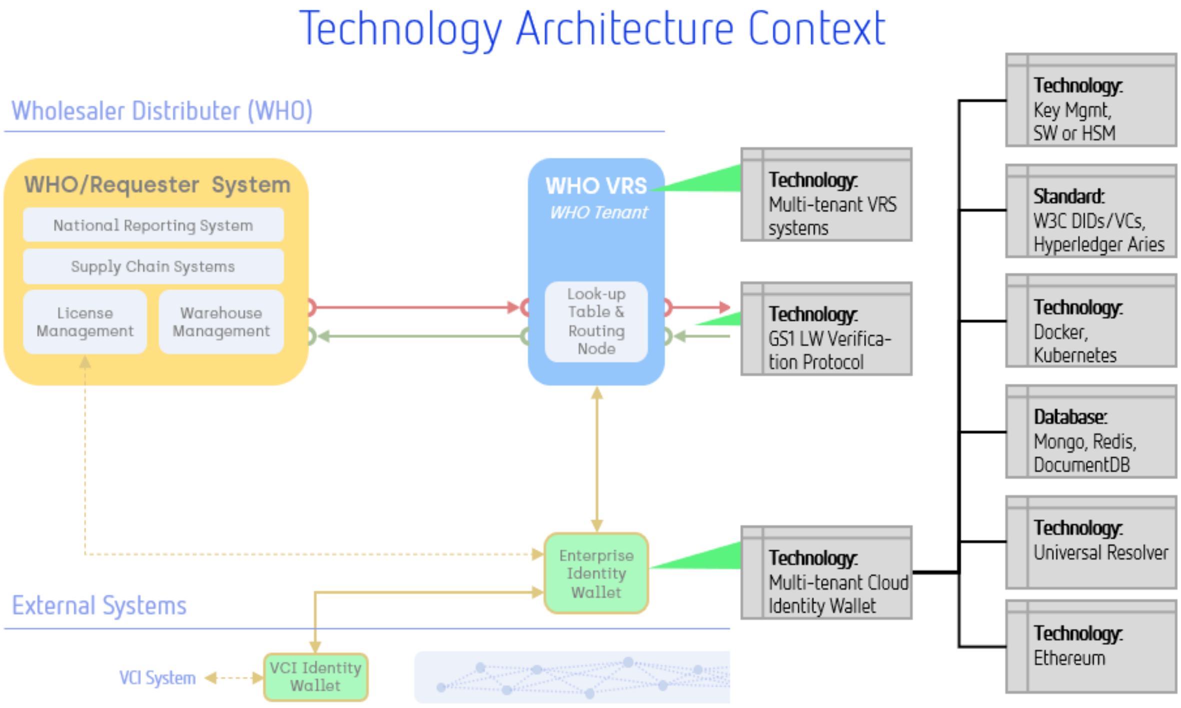

Technology Architecture Context
Wholesaler Distributer (WHO)
WHO/Requester System
National Reporting System
Supply Chain Systems
License Management
Warehouse Management
WHO VRS
WHO Tenant
Look-up Table & Routing Node
Enterprise Identity Wallet
External Systems
VCI System
VCI Identity Wallet
Technology: Multi-tenant VRS systems
Technology: GS1 LW Verification Protocol
Technology: Multi-tenant Cloud Identity Wallet
Technology: Key Mgmt, SW or HSM
Standard: W3C DIDs/VCs, Hyperledger Aries
Technology: Docker, Kubernetes
Database: Mongo, Redis, DocumentDB
Technology: Universal Resolver
Technology: Ethereum

Figure 13 Identity Wallet Technology Components

Cloud-based identity wallets are an emerging technology that is built on W3C standards for DIDs and VCs as well as further open standards for wallet-to-wallet interoperability and semantics.

2.4.2 Details

This table outlines add-on Technology components in scope:

#	System	Description	Purpose	Foreseen changes
1	VRS	Routing and mapping of the PI verification requests. Providing connectivity options and integration interfaces with other VRS providers. VRS systems often provide individual tenants for each trading partner.	To process and route a PI verification request among trading partners. To provide a means to verify the ATP status among trading partners.	Integration of wallet APIs for augmenting the GS1 lightweight messages.
2	API Gateway	Infrastructure system for connecting cloud services and publishing web application programming interfaces (APIs) for internal and external connections. Enforcing usage policies, controlling access, collecting and analysing usage statistics, and reporting on performance. The gateway is a server that acts as an API front-end, receives API requests, enforces throttling and security policies, passes requests to the back-end service and then passes the response back to the requester.	To support authentication, authorization, security, audit and regulatory compliance.	It may be foreseen that VRS systems and identity SaaS wallets are connected via an API gateway service. In case the wallet is implemented as a docker container into the virtual private cloud of the VRS the API Gateway is not required. Alternatively, the wallet SW is directly deployed into the VRS systems. *Note: Integration of wallet with VRS providers via an API Gateway to be evaluated in the pilot.*
3	Cloud Identity Wallet	Identity wallet for managing W3C DIDs and VC credentials.	To manage the ATP credentials via a Web UI	Implementation in the pilot project
4	Database	E.g., Mongo or DocumentDB, Redis	To store configurations & audit trails in the wallet and enable caching of DID documents and revocation status data (Redis)	To be provided with the wallet solution
5	Cloud HSM[1]	Cloud HSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption and signing keys.	To protect private keys and to provide a secure and easy to integrate means for key management using FIPS 140-2 Level 3 validated HSMs.	Because of cost considerations, Cloud HSM will NOT be integrated in the pilot. SW secret stores will be used in the pilot. It is an important option to be considered later for a production system.
6	Ethereum	Blockchain ledger with a DID identity registry (ERC 1056 lightweight identity).	To anchor and publish DID documents.	Implementation in the pilot project
7	Universal Resolver	Infrastructure component and software to resolve DIDs. Universal resolver is part of the wallet SW.	To resolve DIDs and their DID documents.	Implementation in the pilot project

[1] Out of scope for pilot phase because of cost consideration.

8	Hyperledger Aries RfCs	Protocol for widely interoperable wallet-to-wallet communications, i.e., for acquiring or requesting credentials or verifiable presentations	To establish a secure and open protocol standard for wallet-to-wallet communication.	Implementation in the pilot project
9	GS1 LW Verification Protocol	Protocol for exchanging and routing verification messages.	To establish a standard for PI requests and responses.	Augmentation of the protocol with ATP credentials in the pilot project

Cloud wallets can be provided as either a SaaS service or as a **docker container** that can run in a container manager of a VRS provider. Docker containers shall be orchestrated by Kubernetes.

Database Tooling:

- In a VC workflow, the data in the VC payload, not the data in the database, is the normative (authoritative). This means that changing values in a database has an effect on only the next issuance of a verifiable credential.
- For a change to the database to be authoritative, it must **trigger a revocation and reissuance of the associated VC.**
- In general, VC workflows use databases differently from conventional database-driven applications. This requires the business logic or the cloud wallet to update the database tooling.

Data Workflow Management:

- Data workflow management with VCs may induce changes to the auditing and compliance requirements for the system.
- The DSCSA requires secure lookback for 6 years from ship date and/or 6 years from inspection date. This means a maximum look back of up to 12 years.
- In a VC workflow, the system of record or source of truth is the issued VCs, not the change log to the database. This means issued VCs must be archived.
- To enable transaction audits, the message queue of the wallet shall be archived as well.
- This may be simpler than archiving changelogs for the database. If applications already archive event logs or use event sourcing, the VC issuance and revocation events may be added to those event logs.

3 Principles and Requirements

3.1 Principles

The principles below have been identified for the ATP credentialing pilot:

Category	Business
Name	Ensure Compliance with Law (US DSCSA – Authorized Trading Partners)
Statement	Enterprise IT processes comply with all relevant laws, policies, and regulations
Rationale	Enterprise policy is to abide by laws, policies, and regulations. This will not preclude business process improvements that lead to changes in policies and regulations
Implication	The enterprise must be mindful to comply with laws, regulations, and external policies regarding the collection, retention, and management of data. Remaining DSCSA requirements for saleable returns will be addressed: ● DSCSA requires manufacturers, re-packagers, wholesale distributors, and dispensers to trade with only companies that meet the DSCSA defined “Trading Partner” and “Authorized” definition. ● Compliance with the DSCSA will require supply chain companies to digitally interact with supply chain companies where the company identity and whether they meet the DSCSA defined “Trading Partner” and “Authorized” definition will be known at the time of interaction. ● In order to complete the interaction, it is essential for companies at both ends of a DSCSA digital interaction to know the identity of the other company and whether the other company meets the DSCSA defined “Trading Partner” and “Authorized” definition.
Implication	Primary focus will be given ATP and GxP compliance, and the design shall be minimally invasive regarding changes to the existing infrastructure. Costs for the entire ecosystem shall be minimized while fulfilling compliance requirements.
Priority	5

Category	Business
Name	Increase Business Velocity & Agility
Statement	Increase business velocity and application agility by applying leading architecture practices and effective solutions for regulatory compliance.
Rationale	The US pharma supply chain industry requires effective and ecosystem-wide adoption to comply with the DSCSA ATP requirements for saleable returns.
Implication	To realize effective integration with adoption, a strategy shall be implemented that scales across the entire ecosystem by retrofitting existing WHO and MAN systems and processes with minimal customizations.
Priority	5

Category	Integration
Name	Selecting and enforcing re-usability of integration patterns
Statement	Re-usability of current and future integration patterns will reduce complexity and cost, while reducing duplicate data.
Rationale	The solution’s effectiveness relies on a robust integration architecture which avoids complexity and performance issues and can be continuously adapted for future requirements.
Priority	5

Category	Data
Name	Manage Data as an Enterprise Asset
Statement	Data is an asset that has value to the enterprise and is managed accordingly – data will be accurate, secure, shared, accessible, governed, and categorized.
Rationale	The level of data availability and quality directly impacts the value of the system as a whole, thus data management and governance must be part of the overall design from the beginning.
Implications	Apply the data minimization principle when sharing data with VRS or wallet services.
Priority	5

Category	Technology
Name	Cloud first
Statement	Reusable Cloud-based solutions are preferred
Rationale	Beyond the specific benefits of cloud-based solutions (cost efficiency, infrastructure and operation footprint, fast delivery ...), cloud-based solutions are most appropriate generally to support the augmentation of ATP credentials with the existing cloud-based VRS systems.
Implications	SaaS is favored for the target solution
Priority	5

Category	Technology
Name	Ease of Integration with 3rd Parties
Statement	Wallet Solution shall use standards and simple APIs to make integration with 3rd parties easy with existing legacy infrastructures such as IAM, API Gateways, VRS, or systems of WHOs, MANs and VCIs.
Rationale	Use of IT standards, easy to integrate APIs that can be integrated with existing applications, customizable authentication features that can be integrated with existing security and IAM infrastructures, customizable web front end, customizable authorization features and ATP semantic standard.
Implications	3rd parties should be able to integrate the wallet with their existing solutions
Priority	5

Category	Technology
Name	No lock-in; interoperability and data portability
Statement	The solution should conform to defined standards that promote interoperability and portability for data, applications, and technology. The solution should be designed to allow interoperability with identity wallets of other VRSs, WHOs, MANs, and VCIs.
Rationale	The solution shall interact with existing systems providing a seamless user experience. In addition, the solution will use interoperability recommendations for the interaction with the wallets of other parties. The solution shall be flexible to integrate with DID/VC identity interoperability standards that are expected to be endorsed in the future.
Implications	Open standards will be followed unless there is a compelling business reason to implement a non-standard solution. Standards: W3C DIDs, W3C VCs, Hyperledger Aries.
Priority	5

Category	Technology
NIST	NIST-compliant elliptical curves
Statement	Spherity's wallet Solution shall use NIST-compliant cryptography (such as SHA-3 signature suites) wherever feasible.
Rationale	As full NIST compliance is required for some government contracts, SHA-3-based audit trails and hash verifications are preferable to other commercial alternatives.
Implications	Verifiable Credentials should use SHA-3 hashes rather than Keccak-256 ones for PI matching capabilities.
Priority	5

3.2 Architecture-Significant Requirements

The principal activities in ATP credentialing are establishment and management of decentralized identifiers (W3C DIDs) as well as establishing and exchange of VC based license

A. issuance,

B. holding/navigation,

C. presentation,

D. verification, and

E. revocation.

Decentralized Identifiers (W3C DIDs)

The requirements for decentralized identifiers include:

- creation and management of self-certifying identifiers (DID) using public/private key pairs
- creation, usage and maintenance of DID Documents

VC Licenses (W3C VCs)

The VC license requirements induce abstracted, architecturally significant requirements for the VC management:

A) Issuance

VCs are issued by and to entities (including data) identified by DIDs. This requires infrastructure for verifiable control establishment over DID creation, derivation, issuance, delegation, and transfer. The core requirements include identifying the roots-of-trust (ledger or self-certification), the sources-of-truth, and the loci-of-control. These also include key creation, storage, and signing infrastructure. Often wallets provide these functions, so the selection of wallet technology is a requirement. In order to verify DIDs there must be infrastructure to support DID discovery, DID:Doc resolution and dereferencing, and DID registration and anchoring.

To trust the underlying identifiers in a VC, there must be infrastructure to perform identity proofing on the entities that provide DIDs. VC issuance also requires infrastructure to provide the data attributes included in the VC, i.e., the actual verifiable data payload of the VC. The data should be provided in compliance with the licensing requirements. Issuance also requires the creation and specification, registration, and anchoring of the data schema or VC schema used in the VC. Issuance also requires processing infrastructure to compute the cryptographic operations such as signatures involved in the VC's issuance.

B) Holding/Navigation

VCs are typically held, navigated, and monitored in wallets controlled by the holding entity. Monitoring VCs will check accuracy, expiration, and revocation status. In case of discrepancies, the holder might want to acquire renewed VCs. The UX for these wallets is often application-specific and should be designed to ensure usage in accordance with proper workflows.

C) Presentation

The holding entity presents a proof of the verifiable data attributes for verification by the verifier. This presentation proof may be an aggregate of verifiable attributes from multiple VCs. The presentation requires the discovery of the necessary data attributes and matching against existing issued and held credentials. This may require searching, or the business logic for these wallets is often application-specific and should be designed to ensure usage in accordance with proper workflows. The presentation also includes signing or other cryptographic operations to create the proof. This also means specifying key storage and signing infrastructure.

D) Verification

VC verification may be the most demanding task for the system from a performance point of view. VC verification requires discovery, resolution and dereferencing, and verification of every DID and DID:Doc used in a VC. It also requires discovery, lookup, and verification of a DID schema used for the VC. In addition, VC verification requires discovery and lookup of revocation status for each VC. The actual cryptographic verification requires computing infrastructure. Finally, the data payload in the verified VC must be validated against the verification requested data both by the semantics of the data schema and the actual content values. This validation must be performed against business logic or use case requirements for the given workflow.

E) Revocation

The issuer has an obligation to revoke a credential if the prerequisites or requirements for a credential that has been issued are not met anymore after the credential was issued. The issuer shall revoke the credential by using a revocation mechanism. Any verifier that checks the validity of a verifiable credential shall check the revocation status of this credential.

3.2.1 Functional Requirements

The following diagrams depict the overview of the main use cases of the solution that infer architecturally significant functional/non-functional requirements.

We distinguish between use cases from three perspectives:

1. Perspective of the Verifiable Credential Issuer
2. Perspective of the Trading Partner (WHO, MAN)
3. Perspective of the VRS System for automated PI verification processing

1. Perspective of the Verifiable Credential Issuer

The VCI will have an identity wallet for managing its own enterprise identity and for issuing identity and ATP credentials to other wallet holders. Before issuing credentials to other wallet holders, the VCI requires the entity to present a proof that they are who they say. This proof can be in the form of a digital signature via a certificate issued by a trusted certifying authority (such as the DEA or another certified VCI), or in the form of physical documents and picture identification. This identity proofing process is what comprises the due diligence for identity credential.

Before issuing an ATP credential, the VCI performs a different due diligence process of proving that the entity possesses a valid license. This license proofing process consists of checking publicly available state license databases and/or FDA registration databases.

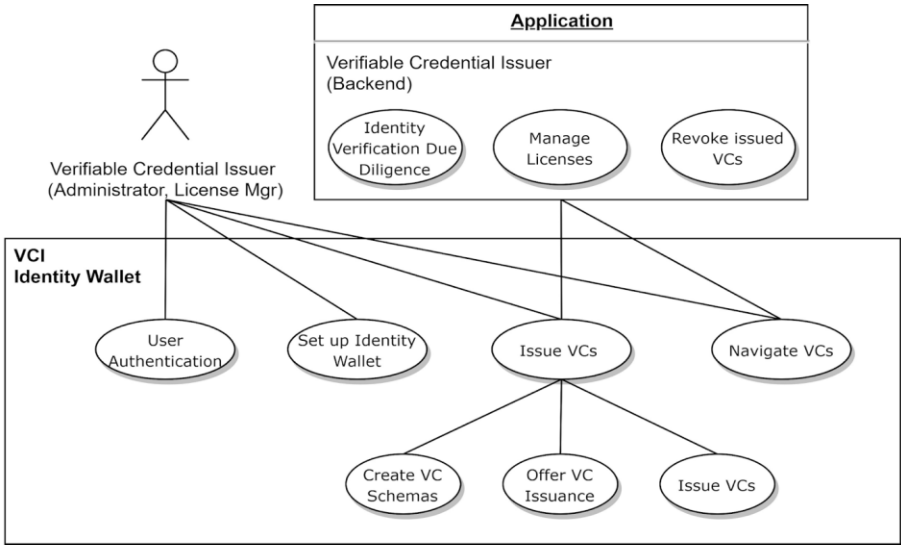


Figure 14 Perspective of Verifiable Credential Issuer - Identity Wallet Use Cases

2. Perspective of the Trading Partner (WHO, MAN)

The trading partner can manage their enterprise identities and acquire and navigate credentials. The trading partner can give his VRS access to his Identity Wallet. The VRS providers can have the permission to access the Identity Wallet APIs to generate or verify ATP Credentials.

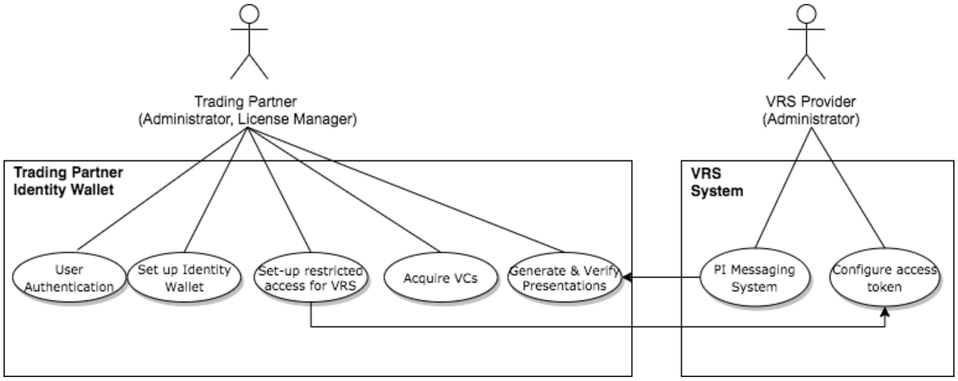

Trading Partner (Administrator, License Manager)
VRS Provider (Administrator)
Trading Partner Identity Wallet
User Authentication
Set up Identity Wallet
Set-up restricted access for VRS
Acquire VCs
Generate & Verify Presentations
VRS System
PI Messaging System
Configure access token

Figure 15 Perspective of Trading Partner Wallet - Identity Wallet Use Cases

3. Perspective of the VRS System for automated PI verification processing

When ATP credentials are acquired and stored in the identity wallet of a given trading partner, the VRS system needs to be authenticated. The VRS system augments credentials in PI verification requests and responses.

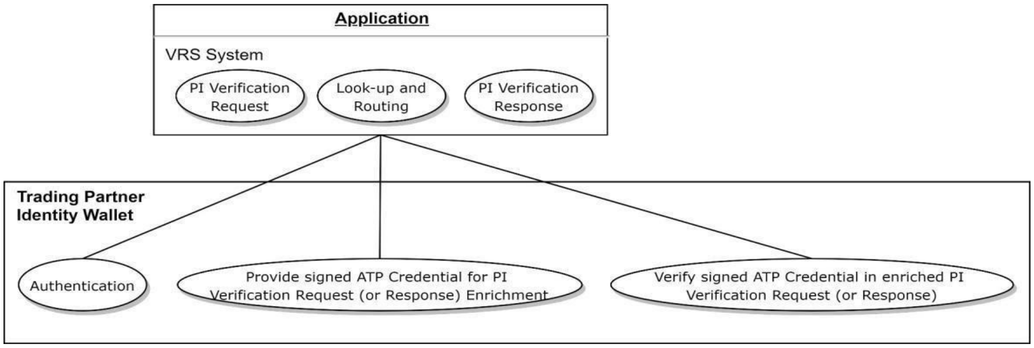

Application
VRS System
PI Verification Request
Look-up and Routing
PI Verification Response
Trading Partner Identity Wallet
Authentication
Provide signed ATP Credential for PI Verification Request (or Response) Enrichment
Verify signed ATP Credential in enriched PI Verification Request (or Response)

Figure 16 Perspective of VRS System – Automated PI Verification Processing

The following table outlines Use Cases in scope of the ATP credentialing pilot:

ID	Use Case	Brief Description
UC1.1	User Authentication	Secure user authentication
UC1.2	Set up Identity Wallet	Configure and manage DID and wallet parameters
UC1.3	Issue VCs	Create a VC schema (semantics), offer credential and issue credentials
UC1.4	Navigate & Assign VCs	Administrators, license managers or APIs shall be able to navigate VCs in the wallet including VCs that have been issued or VCs that have been acquired. It is expected that trading partners have multiple license or derived credentials in their wallet. This might include credentials for other use cases. License managers shall be able to assign credentials for being used for a given use case. Note: In a future set-up it is foreseen that users navigate credentials not via the wallet UX, but via an enterprise system that accesses the credentials via an API.
UC2.0	Deploy Wallet Tenant	Process to deploy and connect an identity wallet tenant for the customers of the VRS
UC2.1	User Authentication	*Same as UC1.1*
UC2.2	Set up Identity Wallet	*Same as UC1.2*
UC2.3	Set up restricted access for VRS provider	Authorize VRS provider via restricted API access to Identity Wallet to generate and verify JWT
UC2.4	Acquire VCs	Acquire credentials from the VCI
UC2.5	Navigate VCs	*Same as UC1.3*
UC3.1	Authentication	Secure authentication of the VRS system
UC3.2	Provide signed ATP Credential for PI Verification Request (or Response) Enrichment	Create verifiable presentation for the augmented PI request
UC3.3	Verify signed ATP Credential in enriched PI Verification Request (or Response)	Verify verifiable presentation of the augmented PI request
UC4[2]	Monitor counterparty ATP status	Check list of all counterparties and their ATP credential status to prove DSCSA ATP compliance

[2] UC4 and UC5 are not depicted in a specific diagram.

UC5[6]	Monitor ATP credential exchange	Check individual ATP credential transactions and DSCSA ATP compliance

Verifiable Presentations in augmented GS1 Lightweight Messages

In the automated PI verification, the processing of ATP credentials will be incorporated into the GS1 Lightweight Messaging Standard for Verification.

By merging the hash of the message request or response body with the ATP credential, the process establishes a so-called verifiable presentation. Verifiable presentations require a **nonce** (i.e., an arbitrary random number) provided by the verifier to protect them against credential reuse attacks.

The existing random **serial numbers** and the **corrUUIDs** will be used as a nonce that is provided and known by the verifier. As these data are part of the message body hash, the credential reuse/replay vector is mitigated in the proposed solution.

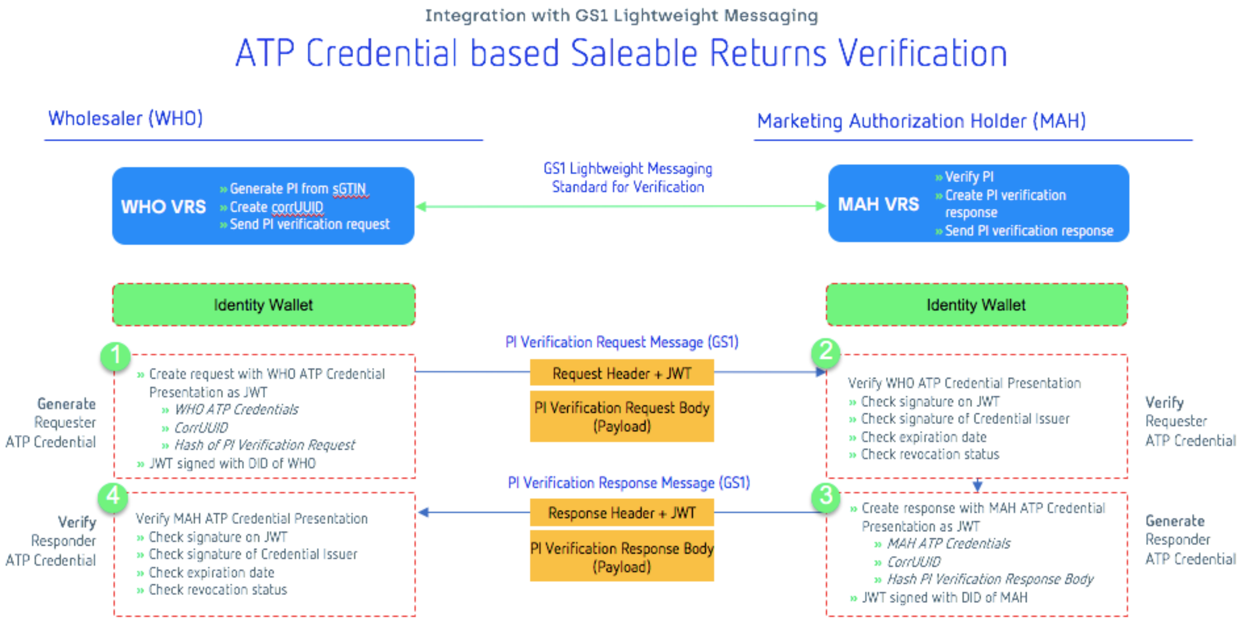

Integration with GS1 Lightweight Messaging
ATP Credential based Saleable Returns Verification
Wholesaler (WHO)
Marketing Authorization Holder (MAH)
WHO VRS
» Generate PI from sGTIN
» Create corrUUID
» Send PI verification request
GS1 Lightweight Messaging Standard for Verification
MAH VRS
» Verify PI
» Create PI verification response
» Send PI verification response
Identity Wallet
Identity Wallet
PI Verification Request Message (GS1)
Request Header + JWT
PI Verification Request Body (Payload)
PI Verification Response Message (GS1)
Response Header + JWT
PI Verification Response Body (Payload)
1
Generate Requester ATP Credential
» Create request with WHO ATP Credential Presentation as JWT
» WHO ATP Credentials
» CorrUUID
» Hash of PI Verification Request
» JWT signed with DID of WHO
2
Verify WHO ATP Credential Presentation
» Check signature on JWT
» Check signature of Credential Issuer
» Check expiration date
» Check revocation status
Verify Requester ATP Credential
3
» Create response with MAH ATP Credential Presentation as JWT
» MAH ATP Credentials
» CorrUUID
» Hash PI Verification Response Body
» JWT signed with DID of MAH
Generate Responder ATP Credential
4
Verify Responder ATP Credential
Verify MAH ATP Credential Presentation
» Check signature on JWT
» Check signature of Credential Issuer
» Check expiration date
» Check revocation status

Figure 17 GS1 Lightweight Messages augmented with ATP Credential Presentations

It shall be understood that the process to create and verify a verifiable presentation WHO JWT in the VR request is **symmetrical** to the create and verify a verifiable presentation MAN JWT in the VR/R response. This means that processing in 1) and 2) is the same as in 3) and 4) only with different message data.

The GS1 lightweight verification message protocol standards is using **JSON** for message serialization.

As the ATP credentialing is augmented with the existing GS1 lightweight verification message protocol, we propose to use **JSON Web Token (JWT)** for VC and VP encoding. JWT is more lightweight compared to

JSON-LD. CBOR or CBOR-LD would add further complexity as the GS1 protocol is using JSON, and the use of an additional message serialization standard would not be beneficial for the overall architecture design.

4 Architecture Elaboration

4.1 System Context

The following context diagram shows the solution represented as a single object and identifies its human actor and system (internal/external) interfaces (IF) with the corresponding flow of data and information.

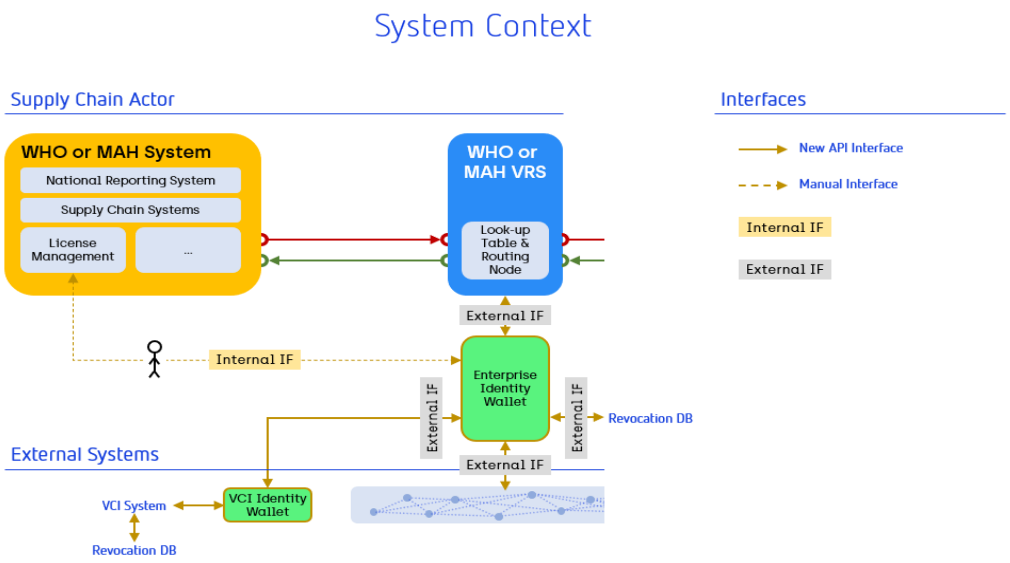


Figure 21 System Context

4.1.1 Human Actors

The following table describes actors from the System Context Diagram in more detail:

Actor Name	Actor Description	User Class	Authentication Type
Administrator	● Administrating the wallet set-up ● Enterprise identity configuration ● User and role management	Internal User	Username & Password in Pilot Phase (2 Factor Authentication, SSO in production)
Auditor	● Monitoring the ATP interactions ● Investigating ATP interactions	Internal User	Username & Password in Pilot Phase (2 Factor Authentication, SSO in production)

Credential Manager	● Requesting Identity and ATP credentials ● Managing existing credentials	Internal User	Username & Password in Pilot Phase (2 Factor Authentication, SSO in production)

4.1.2 External Systems

The following table describes all external systems:

System Name	System Description	System Type	System Owner
VRS	Verification routing service provider: Routing and mapping of the PI verification requests to VRS providers of other supply chain actors.	Look-up and message routing system	VRS Service Provider
Revocation DB	In case of identity or ATP status changes, the verifiable credentials must be revocable by the Verifiable Credential Issuer	Database with verifiable credential revocation status information	Credential Issuer
Trust network for DID Registry	DID information of the counterparties such as key material and service end-points are stored on a public ledger	Distributed Ledger Technology	Spherity for test network in pilot, will be a public ledger in production
Credential Issuer Identity Wallet	Creating decentralized identifiers, managing keys, managing credentials, performing enterprise identity verification issuing ATP credentials.	Enterprise Identity Wallet	Identity Wallet Provider
Credential Issuer System	Receives verifiable credential requests and issues identity and ATP credentials, creates entries and updates for the revocation registry	Backend System	Verifiable Credential Issuer (VCI)

4.1.3 Interfaces

The following diagrams shows the interfaces of the identity wallet:

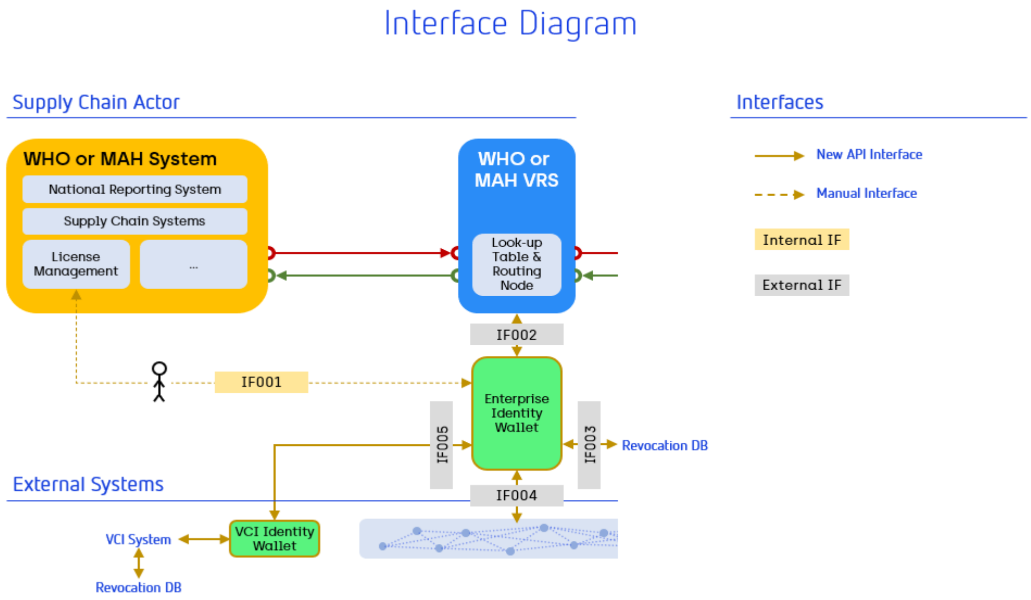


Figure 22 Interface Diagram

4.2 Architecture Vision

Early in the pilot, the team established that trading partners must not only establish that they hold ATP status but establish their identity with each other. Establishing identity and ATP status is key to mitigating nefarious actors from posing as legitimate trading partners and gaining business intelligence from digitally interacting with legitimate trading partners.

The diagram below illustrates the Credentialing Architecture Vision and how the credentialing is embedded into a trusted domain (e.g., DEA via signing certificates). We expect that in future ATP credentialing solutions ATP credentials will be used for further supply chain track & trace use cases and that supply chain credentials will be linked into trust domains such as DEA, GS1, GLEIF, FDA or state government entities.

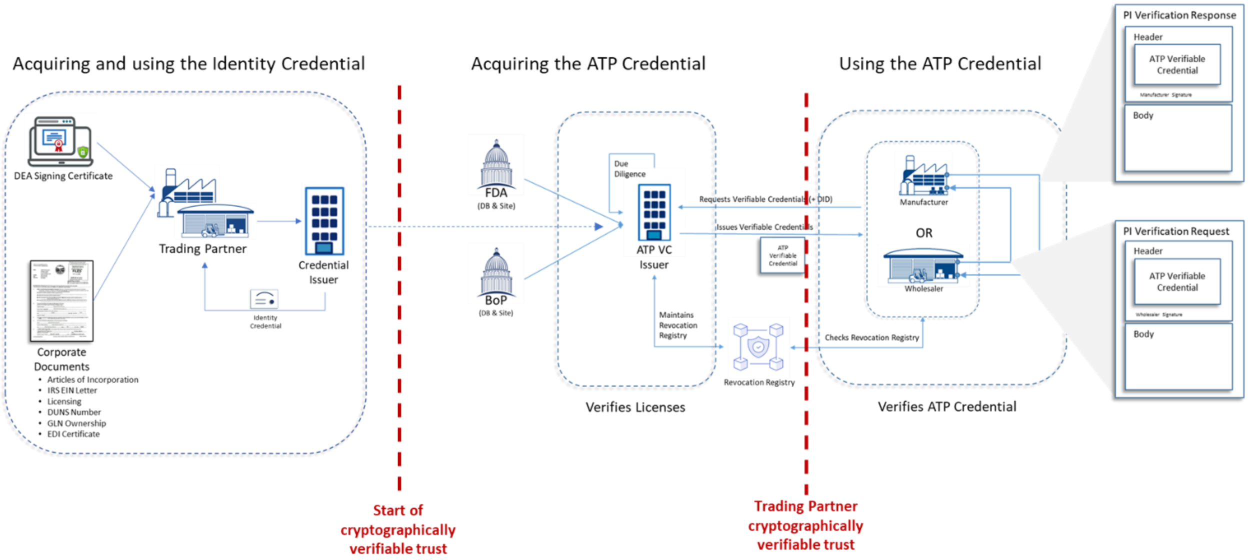


Figure 23 Target Application Architecture

The diagram illustrates the credentials issuer's due diligence in verifying either the trading partner's DEA signing certificate or corporate documents to establish an identity credential. That identity credential is verified in the ATP Credential issuing due diligence along with verifying the trading partner's licenses required. After receiving their Identity and ATP Credential (in their digital identity wallet), trading partners can use the ATP credential in Product Information Verification interactions to prove their ATP status and verify their trading partner's ATP status. The solution shall enable interoperability and data portability of the ATP credentials.

4.3 Application Architecture

The following diagram outlines the target application architecture and its interfaces (IF) for the Enterprise Identity Wallet:

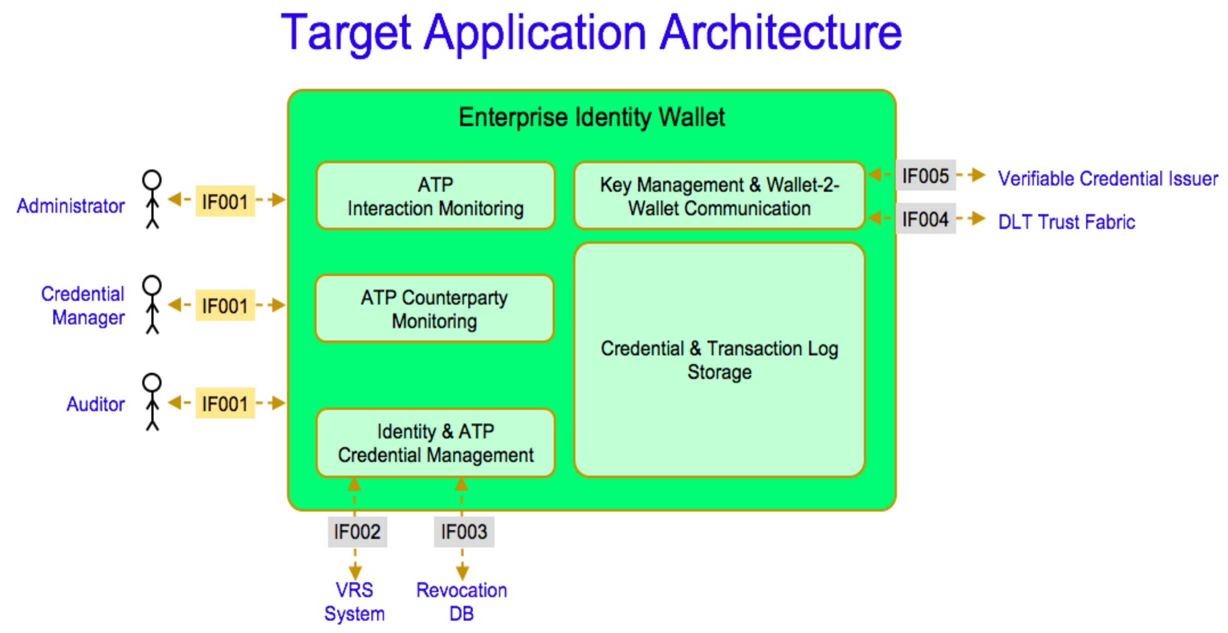


Figure 24 Target Application Architecture

4.3.1 Interoperability and Data Portability Realization

A key objective of the solution and the architecture vision is to enable interoperability and data portability among arbitrary actors in the US pharma supply chain using standards for the wallet-2-wallet communication, digital signatures, and credential management:

ID	Use Case Requirement	Involved components	Realization
S1	Interoperability & Data Portability	Identifier	W3C DIDs ETHR DID Method Spec
S2	Interoperability & Data Portability	Credential Structure	W3C VCs
S3	Interoperability & Data Portability	Credential Schemas	W3C VCs
S4	Interoperability & Data Portability	Schemas	GS1 Web Vocab (tbd)
S5	Interoperability & Data Portability	Signatures	JSON Web Signature 2020 using Secp256k1 curve
S6	Interoperability & Data Portability	Verification Method	JSON Web Key 2020 using Secp256k1 curve
S7	Interoperability & Data Portability	Wallet to Wallet communication	Aries RFCs (key ones) ● Issue Credential Protocol v2 ● Credential Manifest ● Present Proof Protocol v2 ● Presentation Exchange Decentralized Identity Foundation specs ● DIDComm Messaging v2 ● Credential Manifest ● Presentation Exchange
S8	Interoperability & Data Portability	Messaging Standard for PI Verification	GS1 Lightweight Messaging Standard
S9	Interoperability & Data Portability	Interaction between Credential Issuer Identity Wallet and Trading Partner Identity Wallet	Open APIs

S10	Interoperability & Data Portability	Interaction between Trading Partner Identity Wallet and PI Verification messaging service (VRS)	Open APIs
S11	Interoperability & Data Portability	Caching	Redis based open-source caching solution
S12	Interoperability & Data Portability	Revocation	LDAP-based revocation method (standardization in progress)

5 Architecture Assumptions

Assumptions made during the Architecture elaboration:

ID	AA-001
Description	The Identity Credential is the Root of Trust. The trading partners established the due diligence expected of the Credential Issuer. The credential issuer exercised this due diligence prior to issuing credentials. The due diligence contained automated and manual processes.
Implications	The entire solution depends on the process verifying the company identity and the issuance process of the Identity Credential.
Dependency / Impact	The root of trust depends on the due diligence process of the credential issuer.
State	Basic Assumption

ID	AA-002
Description	Custodial approach for wallet infrastructure
Implications	Wallets including key management can be provided as a service. SaaS can be integrated with VRS providers.
Dependency / Impact	If this assumption is not true, more effort needs to be invested to establish wallets under full control in the WHO or MAH infrastructure
State	Basic Assumption

6 Architecture Decisions

The following table summarizes the Architecture Decisions taken during the Architecture elaboration. Architecture decisions will be captured here pending confirmation with regard to the Architecture Alternatives outlined above.

ID	Decision
D-001	Public blockchain will be used for production (e.g. Ethereum).
D-002	Credential revocation will be done via LDAP solution provided by VCIs. LDAP solution shall be standardized.
D-003	Identity and ATP credential schemas shall be standardized.
D-004	Caching will be used to reduce latency times.
D-005	Selective privacy features are not required, as the solution shall establish full disclosure for a give credential set for audit purposes.
D-006	DID:web will be used to establish .well-know of the VCI identifiers

7 References

This Architecture Handbook was developed with information from the following documents:

ID	Document Title	Storage Location
Ref-Doc.1	ATP Pilot User Journey	https://docs.google.com/document/d/1JKUmAnE7e9yvl01NS2XNOQU_8OMayuCzc0bb_DSC-CY/edit?usp=sharing
Ref-Doc.2	ATP Credentialing - Audit Requirements	https://docs.google.com/document/d/1LhmyXWUuCU7ra2Xt6vGy6lBvrMOb693F/edit
Ref-Doc.3	ATP Credentialing Pilot – Security Analysis	https://docs.google.com/document/d/1pwAqMsIGGCZfZdA6D-IT8TeBcVG6RNTv/edit
Ref-Doc.4	Identity Wallet API Documentation	https://documenter.getpostman.com/view/11378415/T17FAToR?version=latest#intro
Ref-Doc.5	Explainer video	https://www.youtube.com/watch?v=y7aWEPUgYbA&feature=youtu.be
Ref-Doc.6	Step through demo	https://xd.adobe.com/view/7d0d1ee6-44e7-437f-b39e-ec4d2dc8acdd-285e/?fullscreen

8 Glossary

Abbreviations used as part of the Architecture Handbook and its process description are described in Abbreviations.

Abbreviation	Meaning
ATP	Authorized Trading Partner
DEA	Drug Enforcement Agency
DID	Decentralized Identifier
FEI	FDA Entity Identifier
GLN	GS1 Global Location Number is an identifier for an enterprise location, a legal entity or an organizational department
GTIN	GS1 Global Trade Item Number is an identifier for trade items
HDA	Health Distribution Alliance
HTTPS	Hypertext Transfer Protocol Secure
IAM / IDAM	Identity Access Management
JSON	JavaScript Object Notation
JWT	JSON Web Token
VCI	Verifiable Credential Issuer
MAH	Marketing Authorization Holder, responsible legal entity for selling a product to the market
MAN	Manufacturer and legal constructs in scope of the respective DSCSA definition. In DSCSA manufacturer also refers to a marketing authorization holder, co-licensor, or manufacturer partnership.
ML	MediLedger
PAM	Privileged Access Management
PI	Product Identity, Product Information
PII	Personal Identifiable Information
sGTIN	Serialized GTIN = GTIN + Expiration Date + Batch Number + Serial Number (S/N), sGTIN encoded on a GS1 2D DataMatrix
SSO	Single Sign On
TLS	Transport Layer Security
VC	Verifiable Credential
VP	Verifiable Presentation
VR	Verification Request
VR/R	Verification Request & Response
VRS	Verification Routing Services
VSP	VRS Service Endpoint, this service endpoint of a VRS service shall not be confused with a service endpoint in a W3C DID document
W3C	World Wide Web Consortium
WHO	Wholesale Distributor

WM	Warehouse Management