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 End to End User Journey for Trading Partners

Version 1.3

3-12-2021

Contents

About this Document

The objective of this document is to documents the end-to-end process for PI Verifications using ATP Credentials. Based on user stories, the process of acquiring credentials and using them in PI Verifications is explained. The Saleable Return Verification between a Wholesaler and a Manufacturer is used as an example.

Related Documents

- Architecture Handbook
- ATP Credentialing - Draft Audit Requirements
- ATP Security Analysis - GS1 Lightweight Messaging Protocol & Overall Architecture Attack
- Spherity Wallet API Documentation

1 High Level ATP Project Scope

Requirement Specification	User Stories
VC (Verifiable Credential) Issuer can issue the Company Identity Verification Credential	• VC Issuer onboards new trading partner via Website to start the Company Identity Verification Credential issuance process. • VC Issuer performs internal due diligence on the company identity based on DEA Signing Certificate ○ Due diligence on notarized documents is out of scope • VC Issuer can request Verifiable Presentation of Company Identity Verification Credential from trading partner wallet before starting the ATP credential issuance process
VC Issuer can issue the DSCSA Wholesaler ATP Credential, DSCSA Manufacturer ATP Credential, DSCSA Dispenser ATP Credential to trading partner DID	• VC issuer decides based on his backend system if an ATP credential issuance is required • VC Issuer performs internal due diligence on the license status and defines the status and expiration of the credential • VC Issuer can revoke credential on own revocation registry • Schemas for Verifiable Credentials are stored with Spherity and provided to all Pilot participants
VRS interactions in saleable returns verification between SAP and RFXCEL	• Creation of Verification Request Message incl. credential type ATP Credential • Creation of Verification Request Response Message incl. credential type ATP Credential • Routing of GS1 Messages between service endpoint of two VRS providers (SAP and RFXCEL)
Trading Partner has Identity Wallet Web Application for managing credentials or perform audits on ATP interactions	• Create enterprise identity (DID) • Manage credentials • Monitoring the Wallet interactions • Dashboard for audit scenario

2 Pilot Implementation Assumptions

- Trading Partner has one VC Issuer contracted to issue ATP and Company Identity Verifiable Credentials
- Trading Partner has one VRS provider
- Trading Partner provides his VRS provider a restricted access to access Wallet APIs to get and verify the ATP Credential
- The DID of the VC issuer is known and whitelisted within the Trading Partner wallet to request credential presentations or push new credentials in the Trading Partner wallet

3 Use Case Overview

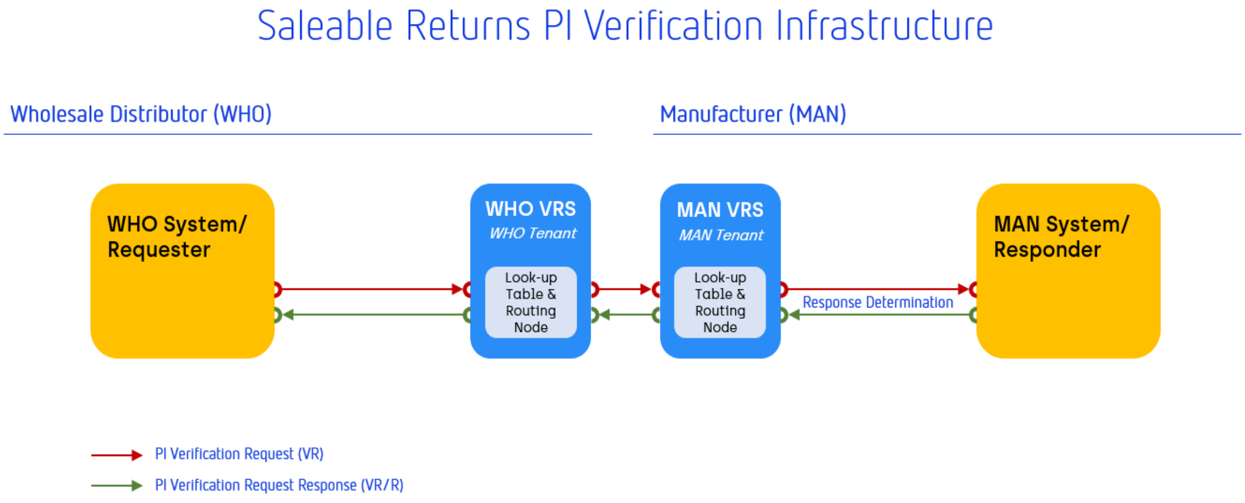
Saleable Returns PI Verification Infrastructure
Wholesale Distributor (WHO)
Manufacturer (MAN)
WHO System/ Requester
WHO VRS
WHO Tenant
Look-up Table & Routing Node
MAN VRS
MAN Tenant
Look-up Table & Routing Node
Response Determination
MAN System/ Responder
PI Verification Request (VR)
PI Verification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

Figure 1 Existing PI Verification Infrastructure & VRS Services

4 Pilot Participants

The following stakeholders will participate in the Pilot for testing the usage of Identity Wallets in the Saleable Returns Verification.

#	Role	Description	Primary Roles wrt/ VCs	Company
1	Verifiable Credential Issuer (VCI)	• Perform identity verification • Perform state license verification • Perform labeler license verification	• Issuer	Legisym
2	Wholesaler	• Acquire, store, present, verify ATP credentials	• Identity and credential holder	AmerisourceBergen

			- Verifier	
3	Manufacturer	- Acquire, store, present, verify ATP credentials	- Identity and credential holder - Verifier	Bristol-Myers Squibb, Johnson & Johnson, 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	- GS 1 message enrichment credential issuer - Enriched GS 1 message verifier	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

4.1 Personas

Role	Persona	Description
VRS	VRS Administrator	Works at VRS provider
		Responsible for new system integrations
		Configuration and monitoring of customer system
VC Issuer	Administrator	Works at VC Issuer
		Responsible for new system integrations
		Configuration and monitoring of customer system
	Key Account Manager	Works at VC Issuer
		Key account manager for customers
		Interface between customer and internal team
Identity Wallet provider	Administrator	Works at Identity Wallet provider
		Responsible for new system integrations
		Configuration and monitoring of customer system
Trading Partner	Administrator	Works at Trading Partner
		Manages own IT systems
	Credential Manager	Works at Trading Partner
		Holder of a DEA Signing Certificate

		Responsible for valid ATP licenses
	Auditor	Works at Trading Partner
		Performs Audits and investigations

5 End to End User Journey in Pilot

The following user journey describes the process that will be analyzed in the ATP Pilot. This process is designed for the ATP Pilot. Based on learnings from the pilot, the process will be adjusted for a productive implementation.

5.1 Identity Wallet Initialization

The Wholesaler, Manufacturer and the VC Issuer need an Identity Wallet to manage credentials and their decentralized identifiers. The VRS Provider does not need an Identity Wallet

Persona	Description	System Interaction
Identity Wallet initialization for Wholesaler/ Manufacturer		
Trading Partner Credential Manager	Agreement with VRS provider to use Identity Wallets for ATP Verification in Pilot.	
Identity Wallet Provider Administrator	Creates an Identity Wallet account including a DID for the Trading Partner. Identity Wallet Provider sends credential data to access the account to Wholesaler/Manufacturer contact person.	Identity Wallet UI, Email
Trading Partner Credential Manager	Authorizes his VRS provider to communicate with the required APIs from the Identity Wallet. The authorization is technically done by providing API credentials to the VRS provider.	Email/ Document
Identity Wallet Provider Administrator	The Trading Partner´s VRS provider gets restricted access for the Trading Partner Wallet. Login data will be sent to the nominated VRS Administrator.	Email
Identity Wallet initialization for VC Issuer		
VC Issuer Key Account	Requests an account at Wallet Provider.	Email
Identity Wallet Provider Administrator	Creates an Identity Wallet with an account for the email address received. The account includes the DID for the VC Issuer. Wallet Provider sends credential data to VC Issuer.	Identity Wallet UI, Email
Usage of Identity Wallets		
Trading Partner Credential Manager	Trading Partner can access his Identity Wallet via web UI, to • know the own DID	Identity Wallet UI

& Trading Partner Administrator	- Monitor ATP interactions - Investigate ATP interactions	
VC Issuer Key Account & VC Issuer Administrator	VC Issuer can access his Identity Wallet via web UI, to - know the own DID - Monitor activities within the own identity wallet Remark: - The VC Issuer will manage the wallet via API integration.	Identity Wallet UI
Technical Operations of Identity Wallets (in Pilot)		
Identity Wallet Provider Administrator	- Each Identity Wallet is operated, hosted and maintained by Spherity. - Key Management is done by encrypted key storage - For production alternative private key management solutions can be provided (e.g. storing private key in (cloud) HSM system of trading partner, Multi-Party Computation).	/

5.2 Verification of Trading Partner´s DID

Company Identity Verification Credential

Within the pilot, each participating wholesaler and manufacturer has to request the VC Issuer to get onboarded via an online service. The VC Issuer will request enterprise data and ask the requestee use a DEA Signing Certificate to confirm that he acts on behalf of the enterprise. Based on the provided data and the DEA Signing Certificate, the VC Issuer is able issue a Company Identity Verification Credential.

Persona	Description	System interaction
Issue Company Identity Verification Credential to Trading Partner		
Trading Partner Credential Manager	- Trading Partner needs to fill in requested company data on VC Issuer website - Trading Partner needs to copy DID from his Identity Wallet and enter it to the Website Form - Website form is submitted to VC Issuer	- Wallet UI - VC Issuer Backend with Wallet API
VC Issuer Key Account	- Backend Process is triggered to establish Wallet to Wallet connection. Based on whitelisted DIDs, it is ensured that only permissioned DID communicate with each other	

	• When Wallet to Wallet communication is established, VC Issuer Key Account performs a due diligence on the provided data (DEA Signing Certificate) • After successful due diligence, VC Issuer issues Company Identity Verification Credential	

5.3 Issuance of ATP Credential

There are three kind of ATP credentials that can be issued by the VC Issuer:

- DSCSA Wholesaler ATP Credential
- DSCSA Manufacturer ATP Credential
- DSCSA Dispenser ATP Credential

Persona	Description	System Interaction
ATP Credential Issuance to Wholesaler or Manufacturer		
Trading Partner Credential Manager	Based on a service contract the VC Issuer checks frequently if a new credential issuance is required. The VC Issuer checks • if an ATP credential was issued before • Existing ATP credential is valid and not revoked VC Issuer requests the presentation of the latest Company Identity Verification Credential. After this, the due diligence on an existing license starts. The VC Issuer defines the ATP status and the expiration date of the credential.	VC Backend with Wallet APIs

5.4 ATP Credential Revocation

Persona	Description	System Interaction
Credential Revocation of Wholesaler/Manufacturer Credential		
VC Issuer Key Account	VC Issuer revokes issued credential on the Credential ID. VC Issuer has its own revocation registry	VC Backend with Wallet APIs

5.5 Saleable Returns Verification with ATP credentials

The VRS provider has a restricted access to the Identity Wallet of his customer to get the presentation of an ATP Credential from his customer or to verify incoming ATP credential presentations. Technically, these presentations are JSON Web Token that are attached to the header of the Verification Request and Response messages (standardized by GS1).

5.5.1 Successful roundtrip for a PI verification

The Wholesaler is the requester of a PI Verification, whereas the Manufacturer is the responder. Both use VRS providers to process the PI Verification. This process can start, when the Wholesaler and Manufacturer have an Identity Wallet and the VC Issuer issued an Identity and ATP credential to the respective enterprise identity DID.

Additionally, the Wholesaler/ Manufacturer needs to provide the contracted VRS Provider authorization to access two APIs of his Identity Wallet:

- Generate Signed Verifiable Presentation (JWT)
- Verify Signed Verified Presentation (JWT)

Based on the authorization, the VRS Provider can enrich the header of the GS1 Verification Request / Response message with a JWT containing the ATP credential.

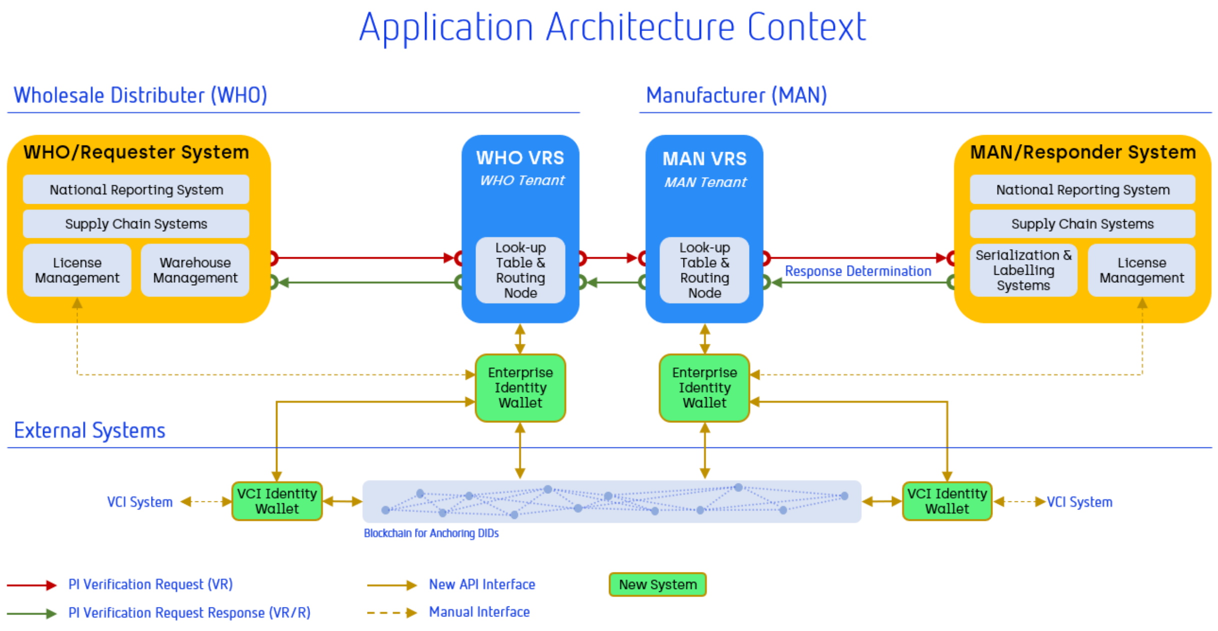
Application Architecture Context
Wholesale Distributer (WHO)
Manufacturer (MAN)
WHO/Requester System
National Reporting System
Supply Chain Systems
License Management
Warehouse Management
WHO VRS
WHO Tenant
Look-up Table & Routing Node
MAN VRS
MAN Tenant
Look-up Table & Routing Node
MAN/Responder System
National Reporting System
Supply Chain Systems
Serialization & Labelling Systems
License Management
Response Determination
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 2 Application Architecture Context

We start the process with a request from the Wholesaler. As this process is symmetrical, it could also be vice versa.

Role	Description	System interaction
VRS Wholesaler creates Verification Request enriched with DSCSA Wholesaler ATP Credential		
Wholesaler	Sends a Product Information with Request for Verification to his VRS Provider	Wholesaler backend (ERP)
VRS Provider Wholesaler	VRS Provider Wholesaler receives verification request from wholesaler backend	Wholesaler backend <-> VRS Wholesaler
VRS Provider Wholesaler	VRS Provider Wholesaler creates hash and sends **Hash of Verification Request, corrUUID,** and **credential type** to the Identity Wallet of the Wholesaler (DID), to get a JWT back	VRS Wholesaler <-> Identity Wallet Wholesaler
Identity Wallet Provider Wholesaler	Identity Wallet of the Wholesaler checks if **valid credential type "DSCSA Wholesaler ATP Credential" is available.** • If not, send an error message.	Identity Wallet Wholesaler
Identity Wallet Provider Wholesaler	Wholesaler wallet creates verifiable presentation of ATP credential **"DSCSA Wholesaler ATP Credential" and hash of Verification Request** as JWT and signs the verifiable presentation. Sends JWT to VRS	Identity Wallet Wholesaler <-> VRS Wholesaler
VRS Provider Wholesaler	VRS Provider Wholesaler attaches the JWT to the header of the Verification Request. Resolve JWT to check the content.	VRS Wholesaler
VRS Provider Wholesaler	Sends enriched PI Verification request message to the endpoint of the VRS Manufacturer.	VRS Wholesaler <-> VRS Manufacturer
VRS Manufacturer receives PI Verification Request		
VRS Provider Manufacturer	VRS Provider Manufacturer receives enriched PI verification request from Wholesaler VRS	VRS Manufacturer
VRS Provider Manufacturer	VRS Provider Manufacturer Perform PI verification (shall run in parallel to JWT verification)	VRS Manufacturer
VRS Provider Manufacturer	VRS Provider Manufacturer verifies message hash and ATP Credential Type (shall run in parallel to JWT verification)	VRS Manufacturer
VRS Provider Manufacturer	**Send JWT** from PI verification request header **to manufacturer wallet.**	VRS Manufacturer <->

		Identity Wallet Manufacturer
Identity Wallet Provider Manufacturer	Identity Wallet Manufacturer resolve DID documents of identity and get valid signing keys of license credential issuer & WHO • **Check signature on JWT** ○ Error message • **Check signature of credential issuer** on ATP Credential ○ Error message • **Check ATP credential expiration date** ○ Error message • **Check revocation registry** ○ Error message • **Send verification JWT result**	Identity Wallet Manufacturer
VRS Provider Manufacturer	Get JWT verification result	VRS Manufacturer
VRS Manufacturer creates Verification Request Response enriched with DSCSA Manufacturer ATP Credential		
	VRS Manufacturer creates PI Verification Request Response message	VRS Manufacturer
VRS Manufacturer	VRS Manufacturer sends **Hash of Verification Request, corrUUID** and **Credential Type** to the Identity Wallet of the Manufacturer (DID), to get a JWT back	VRS Wholesaler <-> Identity Wallet Manufacturer
Identity Wallet Provider Manufacturer	Identity Wallet of the Manufacturer checks if **valid credential type "DSCSA Manufacturer ATP Credential" is available.** • If not, send an error message.	Identity Wallet Manufacturer
Identity Wallet Provider Manufacturer	Identity Wallet of the Manufacturer creates verifiable presentation of ATP credential **"DSCSA Manufacturer ATP Credential" and hash of Verification Request** and signs the verifiable presentation. Sends JWT to VRS	Identity Wallet Manufacturer <-> VRS Manufacturer
VRS Manufacturer	VRS Manufacturer attaches the JWT to the header of the Verification Request	VRS Manufacturer
VRS Manufacturer	Sends enriched PI Verification response message to the endpoint of the VRS Wholesaler.	VRS Manufacturer <-> VRS Wholesaler

VRS of Wholesaler receives Verification Request Response enriched with ATP Credential Presentation of Manufacturer		
VRS Provider Wholesaler	VRS Provider Wholesaler receives enriched PI verification response from Manufacturer VRS	VRS Wholesaler
VRS Provider Wholesaler	VRS Provider Wholesaler verifies message hash and ATP Credential Type (shall run in parallel to JWT verification)	VRS Wholesaler
VRS Provider Wholesaler	VRS Provider Wholesaler **sends JWT** from PI verification request header **to wholesaler wallet.**	VRS Wholesaler <-> Identity Wallet Wholesaler
Identity Wallet Provider Wholesaler	Identity Wallet Wholesaler resolves DID documents of identity and get valid signing keys of license credential issuer & WHO ● **Check signature on JWT** ○ Error message ● **Check signature of credential issuer** on ATP Credential ○ Error message ● **Check ATP credential expiration date** ○ Error message ● **Check revocation registry** ○ Error message ● **Send verification JWT result**	Identity Wallet Wholesaler
VRS Provider Wholesaler	VRS Wholesaler Get JWT verification result	VRS Wholesaler
VRS Provider Wholesaler	Send PI Verification result to Wholesaler	VRS Wholesaler <-> Wholesaler

5.5.2 Possible cases combining ATP checks and PI Request

All possible ATP check cases shall be addressed by the system's business logic.

Cases	ATP Check for Wholesaler		ATP Check for 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

5.6 Trading Partner monitors Wallet interactions for Audit purposes

Spherity provides for the trading partner a wallet web application that enables every pilot participant to manage their enterprise identity, credentials and investigate every ATP interaction (test cases).

Persona	Description	System interaction
Manage enterprise identity and credentials		
Trading Partner Credential Manager	Create new DID for enterprise and see all identifier data	Wallet User Interface
Trading Partner Credential Manager	Overview with all stored credentials that are issued to the trading partners DID	Wallet User Interface
Monitoring Wallet interactions		
Trading Partner Credential Manager	Monitoring page with all ATP interactions and the status if the associated ATP Credentials • PI Verification Requests • PI Verification Responses	Wallet User Interface

Trading Partner Credential Manager	Inspect single ATP interactions based on the corrUUID and the credential ID	Wallet User Interface
Trading Partner Credential Manager	Overview with all ATP names and DID that send PI Verification requests or responses. Option to request identity credential, so that validity of credential is guaranteed.	Wallet User Interface