

OCI Architecture

Introduction
v07

The Open Credentialing Initiative (OCI) architecture is based on W3C Standard Decentralized Identifiers, Verifiable Credentials and Verifiable Presentations (of Verifiable Credentials).

This document provides an overview of the OCI Credentialing components and their use in PI Verification.

This architecture was piloted in 2021, has been tested and implemented by industry trading partners and solution providers and will be part of the Verification Routing Service (VRS) testing in Q2, 2022.

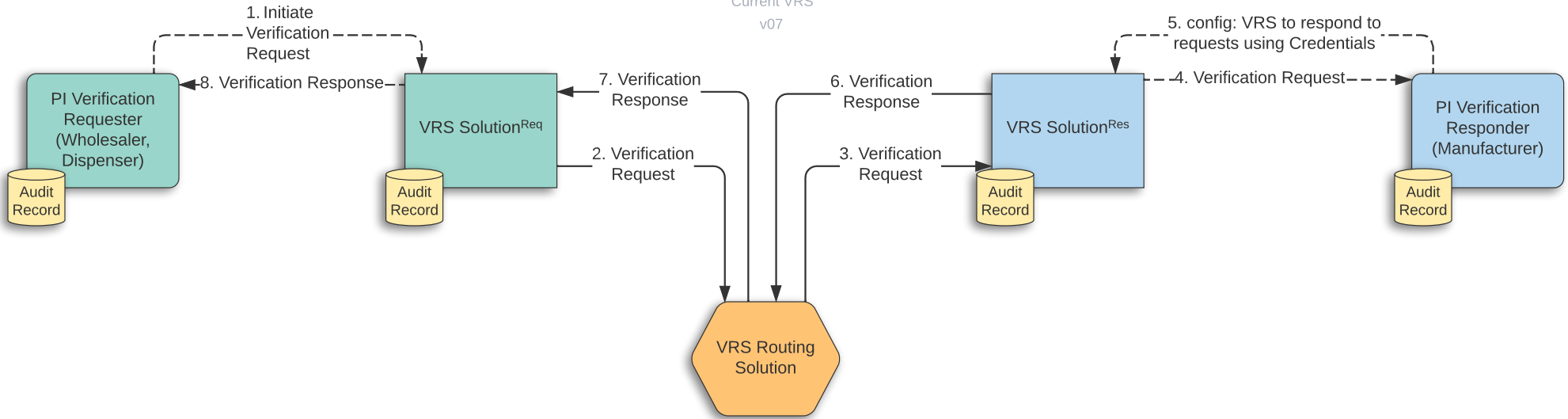
Release 1.2 of the GS1 US Implementation Guide for Applying the GS1 Lightweight Messaging Standard for DSCSA Verification¹ includes a HTTP header field (ATP-Authorization) of the Verification Request and Response to convey the Requester's and Responder's ATP Credential. The OCI ATP Credential is wrapped in a W3C Standard Verifiable Presentation and inserted in the ATP-Authorization field.

Recommendations have been developed for using OCI based credentials based on the PDG Tracing model.

1. https://www.gs1us.org/documents?Command=Core_Download&EntryId=1897

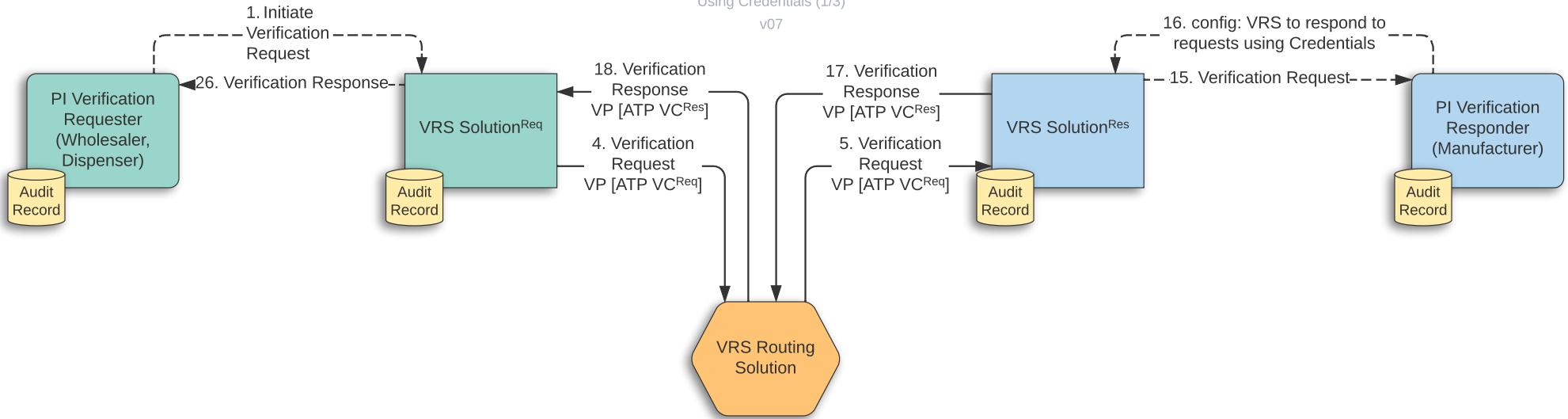
OCI Participant Interactions for DSCSA PI Verification

Current VRS
v07



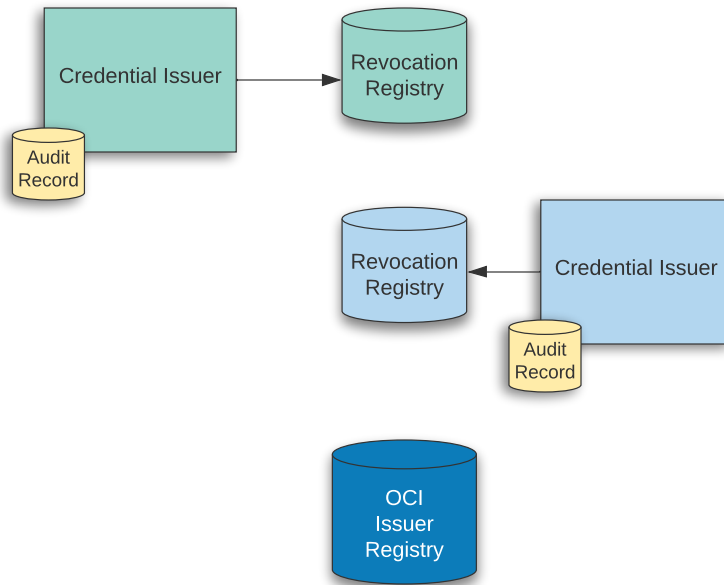
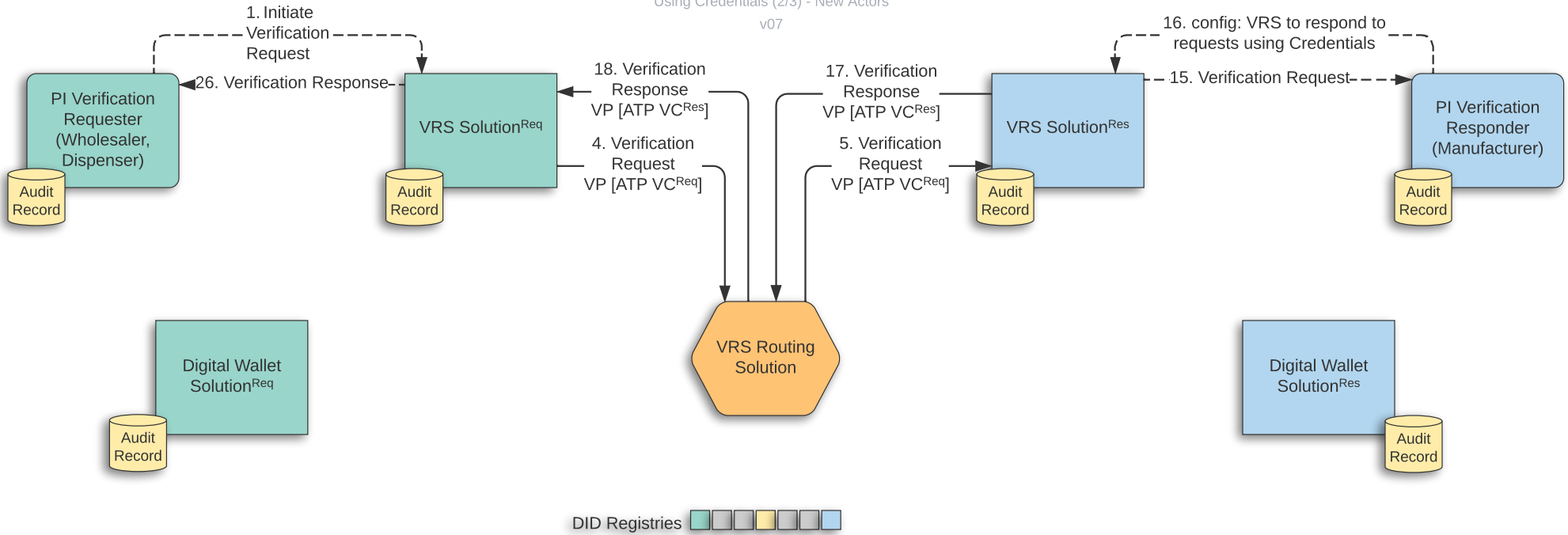
OCI Participant Interactions for DSCSA PI Verification

Using Credentials (1/3)
v07



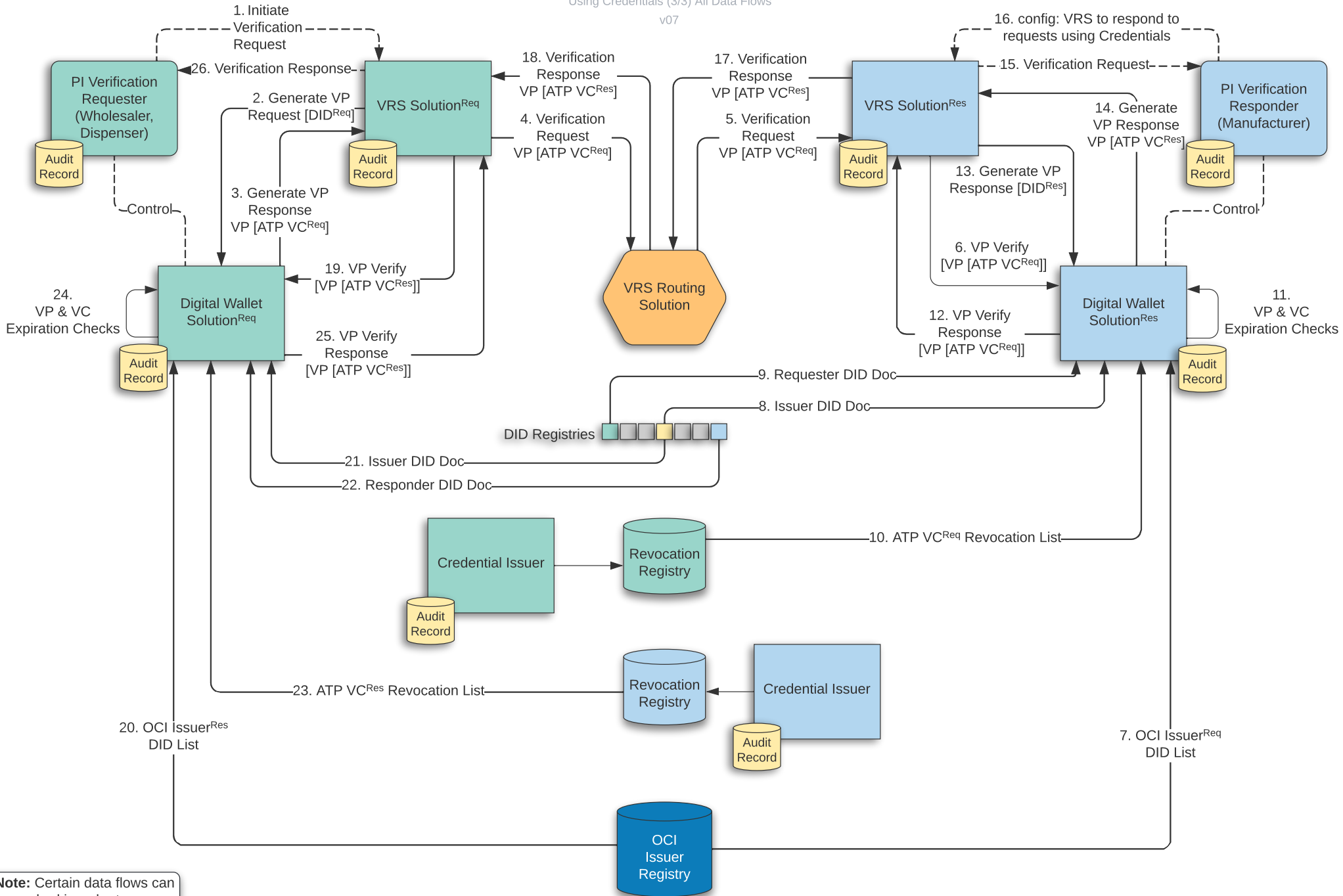
OCI Participant Interactions for DSCSA PI Verification

Using Credentials (2/3) - New Actors
v07



OCI Participant Interactions for DSCSA PI Verification

Using Credentials (3/3) All Data Flows
v07



Note: Certain data flows can be cached in order to improve end-to-end PI Verification performance.

OCI Participant Interactions for DSCSA PI Verification

PI Verification when Requester and Responder service by same Solution
v07

