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

Audit Requirements
Version 1.2
3-12-2021

Contents

About this Document

The objective of this document is to **gather and consolidate audit requirements** for the integration of identity wallets and credentials into the PI Verification process. This documents **maps all identified audit requirements**.

Authors
Carsten Stöcker, Spherity GmbH

1 Secure User & System Authentication & Authorization

- Users of the wallet (either humans or systems) must authenticate prior to getting access to the wallet.
- VRS System Users have access to authorized APIs only. The wallet API access for a VRS system is restricted to access "generate JWT" and "Verify JWT" API only
- All authentication events must be logged and auditable
- All transactions shall be linked to authenticated users or systems in the audit log

2 Data Workflow Management/ Data Retention

- Data workflow management with VCs may induce changes to the auditing and compliance requirement for the system.
- The DSCSA has a requirement for secure lookback (data retention / archiving) for 6 years from ship date and/or 6 years from inspection date. This means a maximum lookback 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 in wallet-to-wallet communication shall be archived as well.
- This may be simpler than archiving change logs 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 Auditability

- All of the following processes must be auditable and logged:
    - VC issuance events in wallet-to-wallet communication
        - Message threads identifier is used to establish correlatability (Thread ID)
        - VC request, issuance, and storing events
    - Revocation events
        - Revocation events shall be logged in the system of the VC Issuer (VCI)
        - Revocation verification events will be logged in the wallet
    - ATP VP signing and verification events
        - ATP VP issuance events (PI msg hash ⇔ nonce, corrUUID, credential type, JWT VP, timestamp, request creator/account name)
        - ATP VP verification events (PI msg hash ⇔ nonce, JWT VP, corrUUID, credential type, revocation result, verification result, timestamp, request creator/account name)
- In addition,
    - wallet authentication events must be logged (for users and systems)
    - wallet admin and configuration events must be logged
- Some instruments on the backend that the owner of a credential can restrict and see what VP Tx are signed for a given credential.
    - Restricted access for VRS Systems for interacting with a limited set of APIs only (e.g. ATP VP signing API and ATP VP verification API)
    - Logging and monitoring of VP signing transactions
    - Authorization of the wallet for each signing corrUUID Tx by the back-end system of the trading partner prior to signing (possibly a future requirement)

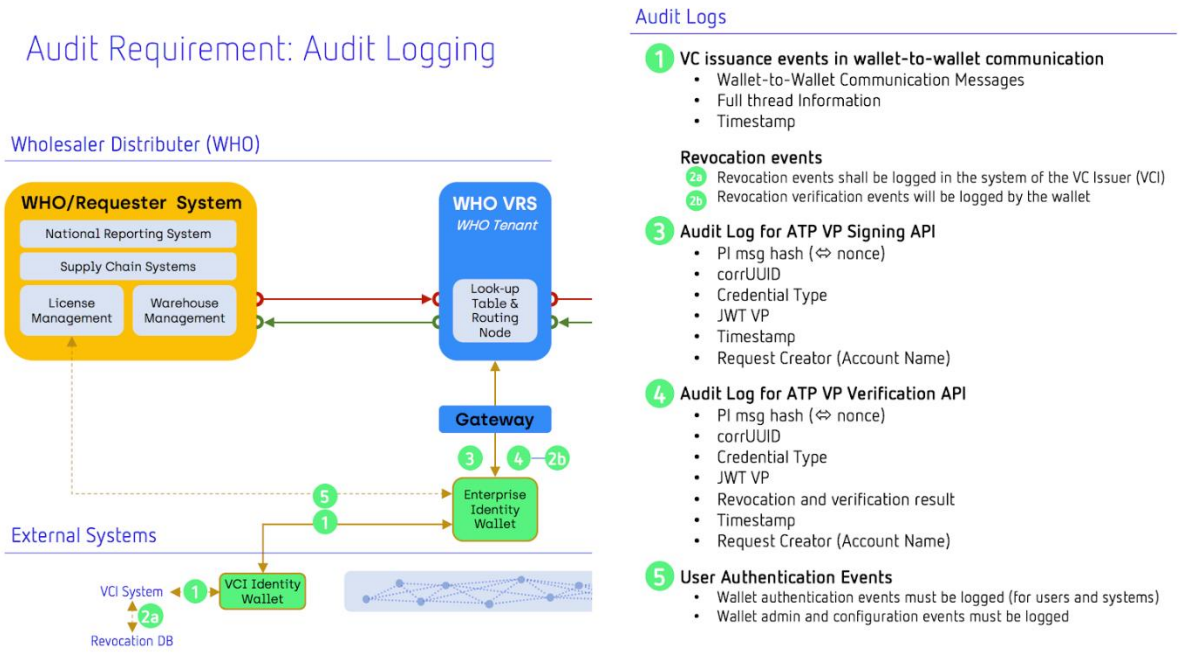

Figure 1 Audit Logging

4 Audit Log Correlatability

- All issuance events shall be correlatable between wallet of issuer and identity holder. A **threadUUID** is used to correlate credential issuance messages in wallet-to-wallet communication
- All revocation events shall be correlatable between the system of the issuer and wallet of the verifier. The identifier in the revocation list entry for a credential will be the credential id that is designated by Legisym at the time the credential is issued. Correlation will be done via credential ID.
- All ATP request response process flow shall be correlatable via the **existing corrUUID** among the following systems:
    - Requester
    - VRS Requester
    - VRS Responder
    - Responder
    - Wallet of Requester
    - Wallet of Responder
    - ➔ This means that
        - **corrUUID** must be part of the wallet API calls, and the JWT VP (tbc)
        - **corrUUID** must be part of the ATP VP issuance process done inside respective wallet that creates a VP for being added to the GS1 lightweight message
        - **corrUUID** must be part of the ATP VP verification process
        - both processes, ATP VP issuance and verification must be logged for audit purposes.

Audit Requirement: Correlation of ATP Credential Issuance & PI Verify Tx

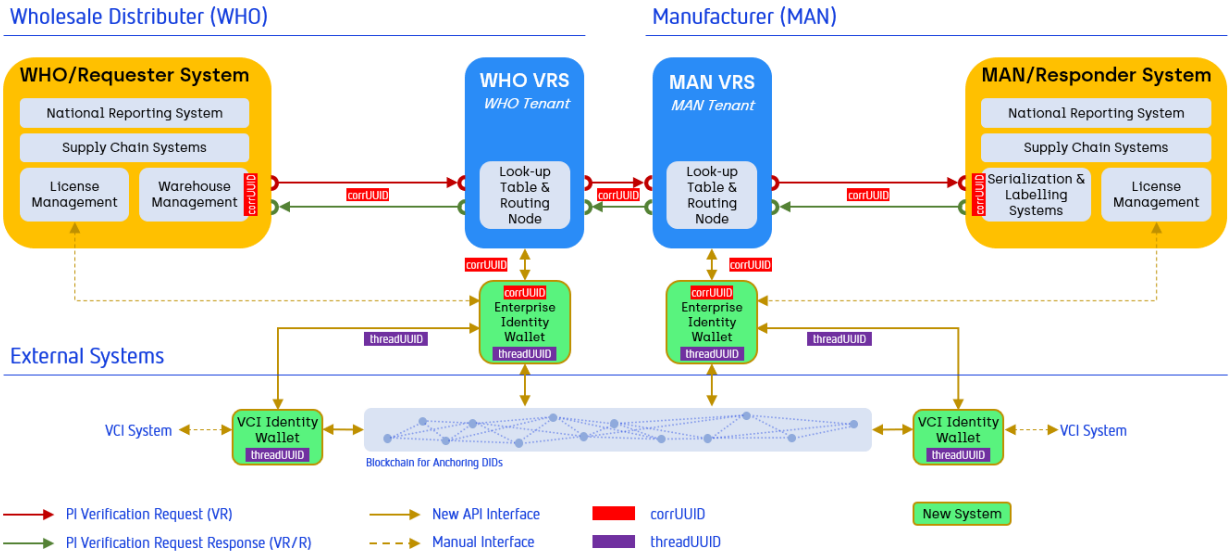

Figure 1 Correlation of ATP Credential Issuance & PI Verify Tx

5 Audit Formats

- All messages shall be logged
  - ➔ How should we do this? Using a message queue that will be archived?
- Audit log format shall be built upon standardized tools for investigators/auditors
- Tools such as "splunk" might be useful in cloud hosting for parsing text strings in the audit log
  - ➔ Check with SAP and Rfxcel if there is an industry standard log format already established or what they us as a best practice

6 Private key in wallet, controlled by wallet

- Private key in wallet, controlled by wallet
- Signing Tx with private key only accessible for authenticated and authorized system or human users
- Open requirements from the ATP Pilot: Root Keys, Key Rotation, Delegated and Signing Keys, Key Back-up and Recovery

7 Electronic Records, Electronic Signatures (ERES) - Code of Federal Regulations Title 21

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm

https://www.ecfr.gov/cgi-bin/ECFR?page=browse

https://www.ecfr.gov/cgi-bin/text-idx?SID=35d122b28f65c50621b5feaab5394b7b&mc=true&tpl=/ecfrbrowse/Title21/21tab_02.tpl

21 CFR Part §11 - ERES Requirements (Source Novartis TPRM)

Note: Most of the following controls will be addressed using 'verifiable credentials'. Implementation of the controls will be analyzed and designed in detail in the **User Requirement Specification (URS)** document.

Req. ID	Requirement Type	Citation	Requirement Description	Comment	In Scope Y/N
UR-<req. Type>-nnnn	ER	21 CFR Part §11.10(a)	System must ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	*Recommend that this requirement be addressed by one or more of the following types of actions:* *Documented tests of add/change/delete transactions and whether the audit trail accurately discerns those changes.* *If tools outside of the application software can be used to add/change/delete records, documented tests to determine if these changes can be detected.* *Review of the system design/implementation to determine if there is some combination of edit checks, security, and/or data validation that prevents or detects record altering or invalid records.*	
UR-<req. Type>-nnnn	ER	21 CFR 11.10(b)(c)	System must ensure ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying throughout the records retention period	*Key Questions to consider in assessing compliance include:* *Will supplanted hardware/software be archived to read data? Or will all previously collected data be converted for use in future revisions/replacements of this computerized system? Preamble Comment #30.* *Can Novartis supply all or any part of the audit trail (in electronic format) to an inspector? In paper format?* *If requested, is it possible for an inspector to review the hardware, software, system-related documentation, and/or audit trail information?* *Are there specific predicate rules requirements for record retention and availability?* *Are there business requirements for the data beyond regulatory requirements?*	
UR-<req. Type>-nnnn	ER	21 CFR §11.10(d)(f)(g)	System must limit access, approvals, and use to authorized individuals and enforce only permitted sequencing of steps and events.	*"The agency advises that the purpose of performing operational checks is to ensure that operations(such as manufacturing production steps and signings to indicate initiation or completion of those steps) are not executed outside of the predefined order established by the operating organization." Preamble Comments #79 - #81*	

UR-<req. Type>-nnnn	ER	21 CFR §11.10(e)	System must employ secure, computer-generated, time-stamped audit trails to independently record the date and local time of operator entries and actions that create, modify, or delete electronic records.	*When assessing compliance, use the following questions:* *Are audit trails secured at the "system administrator" level (i.e., not available as a user function)?* *Are audit trail records updatable manually in order to, for example, delete individual audit trail entries and compromise audit trail integrity?* *Are audit trails capable of undetected add/change/delete by using the application software or application software-related maintenance utilities?* *Are audit trails capable of undetected add/change/delete by using external tools (such as debuggers, database maintenance utilities, etc.)?* *System administrator privilege should be restricted to individuals without a conflict of interest regarding the data.*	
UR-<req. Type>-nnnn	ER	21 CFR §11.10(e)	System must assure that record changes (create, modify, delete) do not obscure previously recorded information by implementing secure, computer-generated, time-stamped audit trails. These audit trails must be retained for as long as the subject electronic records and be available for review and copying.	*When assessing compliance, consider the following:* *Required audit trails must not be turned off.* *Audit trails review (frequency, method, and extent based on risk) must be defined and performed.*	
UR-<req. Type>-nnnn	ES	21 CFR §11.50	All signed electronic records must securely and permanently link all signatures with the local time and date of execution, signature meaning, and printed names of any signature owners.	*Consider the following when assessing Signature Manifestation (§11.50) compliance:* *Identify every display screen and report generated by the computerized system where an electronic signature is represented; each occurrence must be separately assessed for compliance.* *FDA advises that the purpose of this section is not to protect against inaccurate entries, but to provide unambiguous documentation of the signer, when the signature was executed, and the signature's meaning.* *It is unacceptable to display other information, such as employee ID or user ID, as a substitute for the printed name of the signer.* **[ ] 21 CFR §11.50 is not applicable (i.e.,for Electronic Records without Signatures) per Risk Assessment: *<refer to risk assessment>* *[REF]***	

UR-<req. Type>-nnnn	ER	21 CFR §11.70	System must ensure that electronic signatures and handwritten signatures executed to electronic records be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	*Consider the following when assessing Signature / Record Linking (§11.70) compliance:* *"…because it is relatively easy to copy an electronic signature to another electronic record and thus compromise or falsify that record, a technology-based link is necessary [….] The agency does not believe that procedural or administrative controls alone are sufficient." Preamble Comment #107.* *"The agency acknowledges that, despite elaborate system controls, certain determined individuals may find a way to defeat anti-falsification measures […] the agency's intent is to require measures that prevent electronic records falsification by ordinary means." Preamble Comment #108.* **[ ] 21 CFR §11.70 is not applicable (i.e., for Electronic Records without Signatures) per Risk Assessment: *<refer to risk assessment> [REF]***	
UR-<req. Type>-nnnn	ER	21 CFR §11.30	"Open" system must employ controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt and include additional measures such as document encryption and use of appropriate digital signature standards	*Consider the following when assessing Open System (§11.30) compliance:* *Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.* *The agency advises that 11.30 requires additional controls, beyond those identified in 11.10 "[…] to ensure record authenticity, integrity, and confidentiality for open systems." Preamble Comment #94.* **[ ] 21 CFR Part §11.30 -- Controls for "Open" Systems are not applicable per Risk Assessment:** *<refer to risk assessment> [REF]*	
UR-<req. Type>-nnnn	ES	21 CFR §11.100(a) & §11.300(a)	System must ensure that each electronic signature be unique to one individual and not reused by, or reassigned to, anyone else.	**[ ] 21 CFR Part 11 - Subpart C—Electronic Signatures (§11.100 -§11.300) is not applicable per Risk Assessment:** *<refer to risk assessment> [REF]* *[URS-ERES-9 through URS-ERES-16 correspond to this Subpart. (i.e., If this is N/A, so are 10-16)]* *If a system does not provide unique user accounts, an alternate approach (e.g., a logbook) must be in place.*	
UR-<req. Type>-nnnn	ES	21 CFR Part §11.200(a, 1)	System must assure that any electronic signature not based on biometrics must employ at least two distinct components (e.g., ID code and password)	*Consider the following when assessing compliance:* *"The agency believes that using a password alone...would clearly increase the likelihood that one individual, by chance or deduction, could enter a password that belonged to someone else and thereby...impersonate that individual." Preamble Comment #124.* *The combination of these 2 components must be unique. Any possible combinations of this two-factor authentication method are permissible. Preamble Comment #125.*	
UR-<req. Type>-nnnn	ES	21 CFR §11.200(a, 1, i)	System must ensure that the first signature of a series always include all electronic signature components, and that subsequent signings use at least one electronic signature component.	*Consider the following when assessing compliance:* *"The agency advises that 'each signing' means each time an individual executes a signature...For example, in the case of a laboratory employee who performs a number of analytical tests...it is permissible for one signature to indicate the performance of a group of tests (21 CFR 211.194(a)(7))." Preamble Comment #126.*	

UR-<req. Type>-nnnn	ES	21 CFR §11.200(a, 1, ii)	System must enforce workflows such that an individual executing one or more signings not performed during a single, continuous period of controlled system access, will execute each signing using all of the electronic signature components.	*Consider the following when assessing compliance:* *"The agency's concern here is the possibility that, if a person leaves the workstation, someone else could access the workstation and impersonate the legitimate signer by entering an identification code or password." Refer to Preamble comment #124*	
UR-<req. Type>-nnnn	ES	21 CFR Part §11.200(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners	*Consider the following when assessing compliance:* *The key word is "designed". The agency believes that a properly designed and implemented biometric-based electronic signature system makes it highly unlikely that any electronic signature could be falsified.* *"The agency notes that the rule does not require the use of biometric-based electronic signatures." Refer to Preamble Comment #128.* **[ ] 21 CFR §11.200(b) Controls for Electronic Signatures based on Biometrics is not applicable per Risk Assessment:** *<refer to risk assessment> [REF]*	
UR-<req. Type>-nnnn	ES	21 CFR Part §11.300(a)	System must assure the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	*Describe whether or not the system maintains the password or if, for example, LDAP is used*.	
UR-<req. Type>-nnnn	ES	21 CFR Part §11.300(d)	System must employ transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect any attempts at their unauthorized use	*Consider the following when assessing compliance:* *Does the computerized system contain any functionality to detect and report possible unauthorized use of the system?* *Has testing been conducted to ensure that "inactive" user accounts cannot be activated by unauthorized persons?* *"The agency advises that a simple typing error may not indicate an unauthorized use attempt, although a pattern of such errors, especially in short succession... could signal a security problem that should not be ignored". Refer to Preamble Comment #135.*	
UR-<req. Type>-nnnn	ER	21 CFR Part §11.300(e)	Any devices that bear or generate identification code or password information must be tested to ensure that they function properly and have not been altered in an unauthorized manner.	*Consider the following when assessing compliance:* *"Testing for system access alone could fail to discern significant unauthorized device alterations. If, for example, a device has been modified to change the identifying information, system access may still be allowed, which would enable someone to assume the identity of another person." Preamble Comment #138.* *"Because validation of electronic signature systems would not cover unauthorized device modifications, or subsequent wear and tear, validation would not obviate the need for periodic testing." Preamble Comment #138.*	

8 Data Integrity Requirements (GMP) - (Source Novartis TPRM)

All data generated by the wallet are stored as signed data in the form of verifiable credentials (VCs) or verifiable presentations (VPs), including a time stamp, signing ID and signature.

Note: Most of the following controls will be addressed using authentication logs, DIDs, 'verifiable credentials' and 'schemas'. Implementation of the controls will be analyzed and designed in detail in the **User Requirement Specification (URS)** document.

Req. ID	Require-ment Type	Citation	Requirement Description	Comment	In Scope Y/N
UR-<req. Type>-nnnn	DI	MHRA DI Definitions & Guidance v1.1:ALCOA	System must require data to be Attributable to the person generating the data.	*For examples of "Attributable" see 21 CFR Parts: §§ 211.68(b), 211.188(b)(11), 211.194(a)(7)(8), 212.50(c)(10)).*	
UR-<req. Type>-nnnn	DI	MHRA DI Definitions & Guidance v1.1:ALCOA	System must display or print data in a Legible (human-readable) format throughout its retention period.	*For examples of "Legible" see 21 CFR Parts: §§ 211.180(e), 212.110(b)*	
UR-<req. Type>-nnnn	DI	MHRA DI Definitions & Guidance v1.1:ALCOA	System must be designed to ensure that the execution of critical operations are recorded Contemporaneously (at the time of execution) by the user.	*For examples of "Contemporaneous" see 21 CFR Parts: §§ 211.100(b), 211.160(a)*	
UR-<req. Type>-nnnn	DI	MHRA DI Definitions & Guidance v1.1:ALCOA	System must ensure that Original data remains accessible and readable throughout the retention period of the data.	*For examples of "Original" see 21 CFR Parts: §§ 211.180, 211.194(a)*	
UR-<req. Type>-nnnn	DI	MHRA DI Definitions & Guidance v1.1:ALCOA	System must Accurately save data at the time the data is generated and in a manner that prevents the original data from be altered, obscured or deleted.	*For examples of "Accurate" see 21 CFR Parts: §§ 211.22(a), 211.68, 211.188, 212.60(g)*	
UR-<req. Type>-nnnn	DI	MHRA DI Definitions & Guidance v1.1:Primary Record	Data must be retained in a dynamic form where this is critical to its integrity or later verification.	*Data may be static (e.g. a 'fixed' record such as paper or pdf) or dynamic (e.g. an electronic record which the user / reviewer can interact with).*	
UR-<req. Type>-nnnn	DI	MHRA DI Definitions & Guidance v1.1:Original Record / True Copy	System must maintain the original data when technically feasible to do so. Otherwise, data must be output as a report validated as a true and accurate representation of all original data and metadata, one that preserves the integrity (accuracy, completeness, content and meaning) of the record.	*Original records and true copies must preserve the integrity (accuracy, completeness, content and meaning) of the record. Exact (true) copies of original records may be retained in place of the original record (e.g. scan of a paper record), provided that a documented system is in place to verify and record the integrity of the copy.* *Reference 21 CFR § 211.180 for additional detail.* *In the case of basic electronic equipment which does not store electronic data, or provides only a printed data output (e.g. balance or pH meter), the printout constitutes the original record.*	
UR-<req. Type>-nnnn	DI	MHRA DI Definitions & Guidance v1.1: Data Retention - Archival	System must assure long term, permanent retention of completed data and relevant metadata in its final form for the purposes of reconstruction of the process or activity.	*Reference 21 CFR § 211.68 & §212.110(b) for additional detail*	
UR-<req. Type>-nnnn	DI	MHRA DI Definitions & Guidance v1.1:Data Retention - Backup	System must assure that a copy of current data, metadata and system configuration settings be maintained for the purpose of disaster recovery.	*Reference 21 CFR § 211.68 & § 212.110(b) for additional detail*	