


# CredEntry

Powered by 

## APPENDIX H.4

### TECHNICAL STANDARD

### PLATFORM CONFIGURATION

### MANAGEMENT

## Table of Contents

PC-1: Configurable Encryption and Secure Deletion .....	2
PC-2: PKI/HSM Integration.....	2
PC-3: Role-Based Access Control .....	2
PC-4: Single Sign-On for Platform Access .....	2
PC-5: Identity Provider Integration for Credential Workflows .....	3
PC-6: Wallet Allow Lists .....	3
PC-7: Credential Copy Limits.....	3
PC-8: Configurable Dashboards and Metrics Export .....	3
PC-9: Revocation of Trust .....	4
PC-10: Administrative Audit Logs .....	4
PC-11: Wallet Attribute Schema Template.....	4
PC-12: OIDC Attribute Obfuscation .....	4
PC-13: Administrator Web Portal .....	4

# Technical Standard PC: Platform Configuration Management

## PC-1: Configurable Encryption and Secure Deletion

### **Requirement:**

The platform must allow for configuration of encryption algorithms, key rotation policies, access control policies for credential storage, and secure deletion/revocation procedures.

**Standards:** ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 19790

### **Implementation by CredEntry:**

CredEntry supports configurable encryption algorithms aligned with international cryptographic standards. Administrators can define and enforce key rotation policies, ensuring cryptographic agility. Credential storage is protected by configurable access controls, with full support for secure deletion and revocation procedures to guarantee credentials are invalidated safely.

## PC-2: PKI/HSM Integration

### **Requirement:**

The platform must allow for configuration of integration with external PKI/Hardware Security Module (HSM) infrastructure for key protection and signing operations.

**Standards:** ISO/IEC 19790

### **Implementation by CredEntry:**

CredEntry integrates with external PKI and HSM infrastructures for secure key management and signing. Signing operations are executed within FIPS 140-3 compliant HSMs, ensuring private keys remain hardware-protected and compliant with ISO/IEC 19790 requirements.

## PC-3: Role-Based Access Control

### **Requirement:**

The platform must allow for configuration of role-based access control mechanisms to dictate which roles can view, issue, manage, or present specific types of credentials.

**Standards:** ISO/IEC 27001, ISO/IEC 27002

### **Implementation by CredEntry:**

CredEntry implements configurable role-based access control (RBAC), allowing fine-grained assignment of permissions across credential lifecycle activities. Policies ensure only authorised roles can view, issue, manage, or present specific credentials, enforcing least privilege access.

## PC-4: Single Sign-On for Platform Access

### **Requirement:**

The platform must be configurable to use single sign-on from an OIDC or SAML identity provider for platform access itself.

**Standards:** OID4VCI

### **Implementation by CredEntry:**

CredEntry enables integration with OIDC or SAML-based identity providers for Single Sign-On (SSO). This centralises authentication for administrators and operators, ensuring streamlined and secure access management aligned with OID4VCI.

## PC-5: Identity Provider Integration for Credential Workflows

**Requirement:**

The platform must be configurable to use standalone OIDC or SAML identity providers for credential workflows.

**Standards:** OID4VCI, SAML 2.0

**Implementation by CredEntry:**

CredEntry allows credential workflows to leverage standalone OIDC or SAML identity providers, supporting interoperability and federation across trusted identity ecosystems.

## PC-6: Wallet Allow Lists

**Requirement:**

The platform must enable configuration of an allow list of target wallets a credential is able to be issued to.

**Standards:** eIDAS 2.0

**Implementation by CredEntry:**

CredEntry administrators can configure allow lists that restrict credential issuance to approved wallet providers, ensuring compliance with eIDAS 2.0 and preventing delivery to untrusted or non-compliant wallets.

## PC-7: Credential Copy Limits

**Requirement:**

The platform should enable configuration of the number of copies of an 'active credential' an identity is able to issue to their devices.

**Standards:** ISO/IEC 18013-5, ISO/IEC 23220-2, eIDAS 2.0

**Implementation by CredEntry:**

CredEntry provides configuration options to limit the number of active credential copies issued to a user's devices. This reduces misuse, prevents uncontrolled duplication, and ensures adherence to ISO/IEC and eIDAS standards.

## PC-8: Configurable Dashboards and Metrics Export

**Requirement:**

Platform dashboards must be configurable and enable regular metric exports for external dashboarding of key events and activities.

**Standards:** ISO/IEC 27001, ISO/IEC 27002

**Implementation by CredEntry:**

CredEntry provides configurable administrative dashboards with role-specific views. Key operational metrics can be exported via API or scheduled exports, enabling integration with external monitoring and reporting systems.

## PC-9: Revocation of Trust

### **Requirement:**

Platform must enable the revocation of trust for a compromised or untrusted Issuer or Verifier, rendering their credentials or verification attempts invalid across the ecosystem.

**Standards:** eIDAS 2.0

### **Implementation by CredEntry:**

CredEntry administrators can revoke Issuer or Verifier trust relationships. Once revoked, associated credentials or verification attempts are invalidated across the ecosystem, with trust registry updates propagated automatically.

## PC-10: Administrative Audit Logs

### **Requirement:**

Platform must generate audit logs for all administrative actions including user, action and timestamp.

**Standards:** ISO/IEC 27001, ISO/IEC 27002

### **Implementation by CredEntry:**

CredEntry produces tamper-resistant audit logs for all administrative actions. Logs capture user identity, action performed, and timestamps, ensuring accountability and traceability in line with ISO/IEC standards.

## PC-11: Wallet Attribute Schema Template

### **Requirement:**

A template for defining and managing the wallet attribute schema must be provided as part of the product design documentation suite.

**Standards:** ISO/IEC 23220-3, eIDAS 2.0

### **Implementation by CredEntry:**

CredEntry includes schema templates for defining and managing wallet attributes. Templates support consistent schema governance and align with ISO/IEC 23220-3 and eIDAS 2.0.

## PC-12: OIDC Attribute Obfuscation

### **Requirement:**

OIDC attributes (including PII) must be obfuscated when stored.

**Standards:** eIDAS 2.0, OIDC4VP, ISO/IEC 29100

### **Implementation by CredEntry:**

CredEntry ensures all stored OIDC attributes, including PII, are obfuscated using strong pseudonymisation and encryption techniques, in compliance with international privacy and data protection standards.

## PC-13: Administrator Web Portal

### **Requirement:**

A secure web-based dashboard should be available for administrator monitoring, reporting, governance and analytics.

**Standards:** ISO/IEC 27001/27002, ISO/IEC 29003, eIDAS 2.0, TDIF

### **Implementation by CredEntry:**

CredEntry provides a secure web-based administrator portal with MFA and RBAC enforcement. The portal enables monitoring, governance, reporting, and analytics, ensuring compliance with ISO/IEC, eIDAS 2.0, and TDIF standards.