


CredEntry

Powered by 

APPENDIX H.2

TECHNICAL STANDARD

COMPLIANCE REPORTING

Table of Contents

CR-1: ISO/IEC 18013 & ISO/IEC 23220 Conformance	2
CR-2: eIDAS 2.0 Conformance Testing	2
CR-3: Cyber Security Incident Reporting	2
CR-4: Maintenance of Information Security Certifications.....	3
CR-5: Entity Information Security	3
CR-6: Secure Disposal or Return of Information.....	3
CR-7: SLA Service Credits for Breaches	3
CR-8: SLA Framework for Incident Response	4

Compliance Requirements and Implementation

CR-1: ISO/IEC 18013 & ISO/IEC 23220 Conformance

- **Requirement:** The platform must undertake regular conformance activities against ISO/IEC 18013 and ISO/IEC 23220 to ensure ongoing compliance and interoperability.
- **Implementation by CredEntry:**
 - Conformance test activities will be integrated into the platform's continuous integration (CI/CD) pipeline.
 - Automated test harnesses aligned with ISO/IEC 18013-5 and ISO/IEC 23220 standards will be executed quarterly.
 - Reports generated from these tests will be documented and submitted as part of periodic compliance reporting.
 - Any deviations or non-compliance issues will be logged, investigated, and resolved under CredEntry's Quality Management System (QMS).

CR-2: eIDAS 2.0 Conformance Testing

- **Requirement:** The platform must undertake regular conformance activities against eIDAS 2.0 technical test suites.
- **Implementation by CredEntry:**
 - The platform has been architected for interoperability with the European Wallet Conformance (EWC) RFC100 profiles.
 - Conformance testing against eIDAS 2.0 technical test suites will be conducted during the Pilot Phase, followed by annual retesting.
 - Results will be documented, reviewed by independent auditors, and submitted to the relevant authority as part of compliance obligations.

CR-3: Cyber Security Incident Reporting

- **Requirement:** Service providers must report any cyber security incidents within 24 hours of detection.
- **Implementation by CredEntry:**
 - Incident response procedures are aligned with the WA Cyber Security Policy (2024).
 - Detection is supported by real-time monitoring via SIEM (Security Information and Event Management) and automated alerting.
 - Confirmed incidents are logged, risk-assessed, and reported within 24 hours to the Department's designated contact point.
 - Post-incident reviews and root cause analyses are documented and used to strengthen preventive controls.

CR-4: Maintenance of Information Security Certifications

- **Requirement:** Suppliers must maintain independent security certifications.
- **Implementation by CredEntry:**
 - Current certifications include **ISO/IEC 27001** and **SOC 2 Type 2** (roadmap).
 - Engagement with ACSC IRAP assessors has been added in the roadmap.
 - CredEntry commits to maintaining and renewing all certifications annually for the duration of the contract.

CR-5: Entity Information Security

- **Requirement:** Entity information must be adequately secured for the duration of the contract.
- **Implementation by CredEntry:**
 - Data security is enforced using **AES-256 encryption at rest** and **TLS 1.3 in transit**.
 - Role-based access control (RBAC) is implemented, with least-privilege principles applied across all services.
 - Logging and monitoring ensure all access to entity data is tracked and auditable.
 - Compliance with ISO/IEC 27001 and GDPR is maintained through formal security controls and audits.

CR-6: Secure Disposal or Return of Information

- **Requirement:** Supplier must ensure secure disposal or transfer of entity information upon contract termination.
- **Implementation by CredEntry:**
 - Documented processes for secure data destruction are in place, aligned with **NIST 800-88** media sanitization guidelines.
 - On contract termination, entity data can be securely exported back to the Organisation in structured, encrypted formats.
 - Disposal certificates will be issued once sanitization or transfer has been completed.

CR-7: SLA Service Credits for Breaches

- **Requirement:** Provisions for customer service credits when SLAs are breached.
- **Implementation by CredEntry:**
 - SLA framework defines measurable service commitments for uptime, response times, and vulnerability remediation.
 - Service credits will be automatically applied for breaches of managed services or SDK remediation timeframes.
 - SLA tracking and credit calculations will be transparent and reported quarterly.

CR-8: SLA Framework for Incident Response

- **Requirement:** Supplier must provide draft SLA framework aligned to ITIL for incident response and remediation.
- **Implementation by CredEntry:**
 - SLA framework defines:
 - **Incident Severity Levels** (Critical, High, Medium, Low).
 - **Response Timeframes** (e.g., 1 hour for Critical, 4 hours for High).
 - **Remediation Commitments** (e.g., patch deployment for Critical vulnerabilities within 48 hours).
 - SLA is aligned with **ITIL 4 principles** to ensure continual service improvement and resilience.
 - Framework will be finalized during the Pilot Phase and agreed with the contracting entity.