# Assessment Evidence: Credential

Assessor’s Notes

* CRWI.01 to CRWI.11 are PSP PCTF only
* The remaining criteria are part of CAN/CIOSC 103-1

| **103-1/PSP PCTF ID** | **Qualifier(s)** | ***Conformance Criteria***  **Evidence** |
| --- | --- | --- |
| **CRWI** |  | **Credential Wide** General requirements for credential domain atomic processes |
| **CRWI.01** | C1 | The entity under assessment SHOULD adhere to applicable credential management controls, standards, and guidelines, and SHOULD have an auditable process to demonstrate adherence. |
| **CRWI.02** | C2,C3 | The entity under assessment MUST adhere to applicable credential management controls, standards, and guidelines, and MUST have an auditable process to demonstrate adherence. |
| **CRWI.03** | C2,C3 | The entity under assessment MUST provide a list of the applicable credential management controls, standards, and guidelines that are in effect. |
| **CRWI.04** | C2,C3 | The entity under assessment MUST demonstrate the equivalency of the applicable credential management controls, standards, and guidelines to those used by the assessor. |
| **CRWI.05** | C1 | The entity under assessment SHOULD monitor for indications of credential misuse or compromise. |
| **CRWI.06** | C2,C3 | The entity under assessment MUST monitor for indications of credential misuse or compromise. |
| **CRWI.07** | C1,C2,C3 | The entity under assessment MUST notify the Holder of any changes to credential information (e.g., updating the expiry date). |
| **CRWI.08** | C1 | The entity under assessment SHOULD log and retain for a predefined period of time all credential events. |
| **CRWI.09** | C2,C3 | The entity under assessment MUST log and retain for a predefined period of time all credential events. |
| **CRWI.10** | C1,C2,C3 | The entity under assessment MUST have in place policies and procedures to detect the misuse of the identity information of a person. |
| **CRWI.11** | C2,C3 | The entity under assessment MUST adhere to applicable credential management controls, standards, and guidelines, and MUST have an auditable process to demonstrate adherence. |
| **CRCB** |  | **Credential Claims Binding** Credential Claims Binding is the process of associating a credential with one or more claims about one or more Subjects. |
| **CRCB.01** | C1 | The entity under assessment SHOULD ensure that there is a tamper-evident process in place. |
| **CRCB.02** | C2,C3 | The entity under assessment MUST ensure that there is a tamper-evident process in place. |
| **CRIS** |  | **Credential Issuance** Credential Issuance is the process of creating a Credential from a set of Claims and assigning the Credential to a Holder. |
| **CRIS.01** | C1,C2,C3 | The entity under assessment MUST ensure that a credential is referenceable to a relevant event or activity. |
| **CRIS.02** | C1,C2,C3 | The entity under assessment MUST ensure that a credential identifies the Issuer. |
| **CRIS.03** | C1,C2,C3 | The entity under assessment MUST ensure that a credential has a defined validity period. |
| **CRIS.04** | C1 | The entity under assessment SHOULD ensure that a credential is tamper-evident. |
| **CRIS.05** | C2,C3 | The entity under assessment MUST ensure that a credential is tamper-evident. |
| **CRIS.06** | C1,C2,C3 | The entity under assessment MUST ensure that a credential is unique within a specified population. |
| **CRIS.07** | C1,C2,C3 | The entity under assessment MUST ensure that a credential is provided to the rightful Holder. |
| **CRAB** |  | **Credential Authenticator Binding** Credential Authenticator Binding is the process of associating a credential issued to a Holder with one or more authenticators. This process also includes authenticator life-cycle activities such as suspending authenticators (caused by a forgotten password or a lockout due to successive failed authentications, inactivity, or suspicious activity), removing authenticators, binding new authenticators, and updating authenticators (e.g., changing a password, updating security questions and answers, having a new facial photo taken). |
| **CRAB.01** | C1,C2,C3 | The entity under assessment MUST ensure that at least one authenticator is bound to a credential. |
| **CRAB.02** | C1,C2,C3 | The entity under assessment MAY provide to the Holder the ability to update the authenticators bound to a credential issued to the Holder. In this case, Credential Validation and Credential Verfication processes MUST be performed first. |
| **CRAB.03** | C1,C2,C3 | The entity under assessment MAY provide to authorized personnel the ability to update the authenticators bound to a credential. |
| **CRAB.04** | C1 | The entity under assessment SHOULD require the Holder to complete any administrator-initiated credential authenticator binding (e.g., the Holder must supply a new password when the administrator initiates a password reset). |
| **CRAB.05** | C2,C3 | The entity under assessment MUST require the Holder to complete any administrator-initiated credential authenticator binding (e.g., the Holder must supply a new password when the administrator initiates a password reset). |
| **CRVA** |  | **Credential Validation** Credential Validation is the process of verifying that the issued credential is valid (e.g., not tampered with, corrupted, modified, suspended, or revoked). The validity of the issued credential can be used to generate a level of assurance. |
| **CRVA.01** | C1,C2,C3 | The entity under assessment MUST ensure, using acceptable methods, that a credential is not tampered with, corrupted, or modified. Examples of acceptable methods are cryptographic methods or examination by a trained examiner. |
| **CRVA.02** | C1,C2,C3 | The entity under assessment MUST ensure that a credential is not suspended or revoked. |
| **CRVE** |  | **Credential Verification** Credential Verification is the process of verifying that a Holder has control over an issued credential. Control of an issued credential is verified by means of one or more authenticators. The degree of control over the issued credential can be used to generate a level of assurance. |
| **CRVE.01** | C1,C2,C3 | The entity under assessment MUST ensure that the Holder has demonstrated control over a credential by means of one or more authenticators. |
| **CRVE.02** | C1,C2,C3 | The entity under assessment MUST inform the Holder when the Holder has demostrated control over a credential by means of one or more authenticators. |
| **CRVE.03** | C1,C2,C3 | The entity under assessment MUST indicate an authentication failure when a credential is suspended or revoked, or when credential misuse or compromise is detected. |
| **CRMA** |  | **Credential Maintenance** Credential Maintenance is the process of updating the credential attributes (e.g., expiry date, status of the credential) of an issued credential. |
| **CRMA.01** | C1,C2,C3 | The entity under assessment MUST ensure that credential attributes are updated in a timely manner. |
| **CRMA.02** | C1,C2,C3 | The entity under assessment MAY provide to authorized personnel the ability to update the credential attributes of a credential. |
| **CRMA.03** | C1,C2,C3 | The entity under assessment MUST record the initiating party for a credential attribute modification, and date of modification. |
| **CRSU** |  | **Credential Suspension** Credential Suspension is the process of transforming an issued credential into a suspended credential by flagging the issued credential as temporarily unusable. |
| **CRSU.01** | C1,C2,C3 | The entity under assessment MUST have the ability to suspend the use of a credential (for example, due to an expiry date having been exceeded or the detection of suspicious activity). |
| **CRSU.02** | C1,C2,C3 | The entity under assessment SHOULD provide to the Holder the ability to suspend the use of a credential issued to the Holder. |
| **CRSU.03** | C1 | The entity under assessment SHOULD undertake a reassessment of a credential relationship, potentially leading to suspension, when evidence of a potential change to underlying identity attributes or credential attributes is made known from an acceptable information provider. |
| **CRSU.04** | C2,C3 | The entity under assessment MUST undertake a reassessment of a credential relationship, potentially leading to suspension, when evidence of a potential change to underlying identity attributes or credential attributes is made known from an acceptable information provider. |
| **CRSU.05** | C1,C2,C3 | The entity under assessment MUST record the following suspension information: the effective date of suspension, the reason for suspension, and the initiating party for a suspension. |
| **CRSU.06** | C1,C2,C3 | The entity under assessment SHOULD inform the Holder of the change in credential status. |
| **CRSU.07** | C1,C2,C3 | The entity under assessment MUST make available suspension information to the Holder and any Verifier. |
| **CRSU.08** | C1,C2,C3 | The entity under assessment MUST ensure that a suspended credential undergoes a timely revalidation, based on the entity's formal policy and procedures, for the purposes of either Recovery or Revocation. |
| **CRSU.09** | C1,C2,C3 | The entity under assessment MUST initiate a process to render a credential unusable, potentially leading to revocation, if it detects indications of compromised information or compromised automated processing components. |
| **CRRC** |  | **Credential Recovery** Credential Recovery is the process of transforming a suspended credential back to a usable state (i.e., an issued credential). |
| **CRRC.01** | C1,C2,C3 | The entity under assessment MUST have the ability to recover a suspended credential. |
| **CRRC.02** | C1,C2,C3 | The entity under assessment SHOULD provide to the Holder the ability to request the recovery of a suspended credential. |
| **CRRC.03** | C1,C2,C3 | The entity under assessment MUST perform Identity Verification of the Holder prior to credential recovery. |
| **CRRC.04** | C1,C2,C3 | The entity under assessment MUST record the following recovery information: the effective date of recovery and the initiating party for the recovery action. |
| **CRRC.05** | C1,C2,C3 | The entity under assessment SHOULD inform the Holder of the change in relationship status. |
| **CRRC.06** | C1,C2,C3 | The entity under assessment MUST make available recovery information to the Holder and any Verifier. |
| **CRRC.07** | C1,C2,C3 | The entity under assessment MUST ensure that recovery of a credential can only occur after revalidation based on currently valid evidence and execution of the requirements in Credential Validation. |
| **CRRC.08** | C1,C2,C3 | The entity under assessment MUST ensure that recovery processes apply only to those credentials in a suspended state (i.e., revoked credentials cannot be recovered, they must be reissued). |
| **CRRV** |  | **Credential Revocation** Credential Revocation is the process of ensuring that an issued credential is permanently flagged as unusable. |
| **CRRV.01** | C1,C2,C3 | The entity under assessment MUST have the ability to revoke a credential (for example, due to an expiry date having been exceeded or the detection of suspicious activity). |
| **CRRV.02** | C1,C2,C3 | The entity under assessment SHOULD provide to the Holder the ability to revoke a credential issued to the Holder. |
| **CRRV.03** | C1,C2,C3 | The entity under assessment MUST record the following revocation information: the effective date of revocation, the reason for revocation, and the initiating party for a revocation. |
| **CRRV.04** | C1,C2,C3 | The entity under assessment MUST inform the Holder of the change in relationship status. |
| **CRRV.05** | C1,C2,C3 | The entity under assessment MUST make available the revocation information to the Holder and any Verifier. |
| **CRRV.06** | C1,C2,C3 | The entity under assessment MUST ensure that revocation can only occur based on contravention of relevant policy, law, or regulation. |
| **CRRV.07** | C1,C2,C3 | The entity under assessment MAY immediately revoke a credential without prior suspension in cases where it deems the risk or evidence warrants revocation. |