# **Assessment Evidence**: Credential

|  |  |  |
| --- | --- | --- |
| **PSP CCP V1.5 ID** | **Qualifiers** | ***Conformance Criteria*** |
| **CRDG** |  | **General requirements for the credential domain atomic processes.** |
| **CRDG.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. |
| **CRDG.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. |
| **CRDG.03** | C2,C3 | The entity under assessment MUST provide a list of the applicable credential management controls, standards, and guidelines that are in effect. |
| **CRDG.04** | C1 | The entity under assessment SHOULD monitor for indications of credential misuse or compromise. |
| **CRDG.05** | C2,C3 | The entity under assessment MUST monitor for indications of credential misuse or compromise. |
| **CRDG.06** | C1,C2,C3 | The entity under assessment SHOULD notify the Holder of any changes to credential information (e.g., updating the expiry date). |
| **CRDG.07** | C1 | The entity under assessment SHOULD log and retain for a predefined period of time all credential events. |
| **CRDG.08** | C2,C3 | The entity under assessment MUST log and retain for a predefined period of time all credential events. |
| **CRIS** |  | ***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 the credential is referenceable to a relevant event or activity. |
| **CRIS.02** | C1,C2,C3 | The entity under assessment MUST ensure that the credential identifies the Issuer. |
| **CRIS.03** | C1,C2,C3 | The entity under assessment MUST ensure that the credential has a defined validity period. |
| **CRIS.04** | C1 | The entity under assessment SHOULD ensure that the credential is tamper-evident. |
| **CRIS.05** | C2,C3 | The entity under assessment MUST ensure that the credential is tamper-evident. |
| **CRIS.06** | C1,C2,C3 | The entity under assessment MUST ensure that the credential is unique within a specified population. |
| **CRIS.07** | C1,C2,C3 | The entity under assessment MUST ensure that the credential is provided to the rightful Holder. |
| **CRAB** |  | ***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 the credential. |
| **CRAB.02** | C1,C2,C3 | The entity under assessment MAY provide to the Holder the ability to update the authenticators bound to the credential. In this case, the Credential Validation and Credential Verification 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 the 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 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 the 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 be able to determine if the credential is suspended or revoked. |
| **CRVE** |  | ***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 | The entity under assessment MUST ensure that the Holder has demonstrated control over the credential by means of one or more authenticators. |
| **CRVE.02** | C1,C2 | The entity under assessment MUST inform the Holder when the Holder has demonstrated control over the credential by means of one or more authenticators. |
| **CRVE.03** | C3 | The entity under assessment MUST ensure that the Holder has demonstrated control over the credential by means of two or more authenticators. |
| **CRVE.04** | C3 | The entity under assessment MUST inform the Holder when the Holder has demonstrated control over the credential by means of two or more authenticators. |
| **CRVE.05** | C1,C2,C3 | The entity under assessment MUST indicate an authentication failure when the credential is suspended or revoked, or when credential misuse or compromise is detected. |
| **CRMA** |  | ***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 the credential attributes of the credential 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 the credential. |
| **CRMA.03** | C1,C2,C3 | The entity under assessment MUST record the initiating party of the credential attribute modification, and the date of modification. |
| **CRSU** |  | ***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 credential *(for example, due to the expiry date having been exceeded or the detection of suspicious activity).* |
| **CRSU.02** | C1,C2,C3 | The entity under assessment MUST suspend the credential if the entity under assessment detects indications of compromised information or compromised automated processing components. |
| **CRSU.03** | C1,C2,C3 | The entity under assessment MAY provide to the Holder of the credential the ability to request the suspension of the credential. |
| **CRSU.04** | C1,C2,C3 | If the person making the credential suspension request is unable to demonstrate control over the credential, the entity under assessment MUST perform Identity Verification of that person. |
| **CRSU.05** | C1 | The entity under assessment SHOULD undertake a reassessment of the credential, potentially leading to suspension, when evidence of a potential change to the identity attributes or credential attributes is made known from an acceptable information provider. |
| **CRSU.06** | C2,C3 | The entity under assessment MUST undertake a reassessment of the credential, potentially leading to suspension, when evidence of a potential change to the identity attributes or credential attributes is made known from an acceptable information provider. |
| **CRSU.07** | C1,C2,C3 | The entity under assessment SHOULD record the following credential suspension information: the effective date of the credential suspension, the reason for the credential suspension, and the initiating party of the credential suspension. |
| **CRSU.08** | C1,C2,C3 | The entity under assessment SHOULD inform the Holder of the change in credential status. |
| **CRSU.09** | C1,C2,C3 | The entity under assessment MAY make available the credential suspension information to the Holder and any Verifier. |
| **CRSU.10** | C1,C2,C3 | The entity under assessment MUST ensure that the suspended credential undergoes a timely reassessment, based on the entity under assessment's formal policy and procedures, leading to either credential recovery or credential revocation. |
| **CRRC** |  | **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 the suspended credential. |
| **CRRC.02** | C1,C2,C3 | The entity under assessment MAY provide to the Holder of the credential the ability to request the recovery of the suspended credential. |
| **CRRC.03** | C1,C2,C3 | The entity under assessment MUST perform Identity Verification of the Holder making the credential recovery request. |
| **CRRC.04** | C1,C2,C3 | The entity under assessment MUST ensure that recovery of the credential can only occur after appropriate administrative action. |
| **CRRC.05** | C1,C2,C3 | The entity under assessment MUST ensure that credential recovery only applies to those credentials that are in a suspended state (i.e., revoked credentials cannot be recovered, they must be reissued). |
| **CRRC.06** | C1,C2,C3 | The entity under assessment SHOULD record the following credential recovery information: the effective date of the credential recovery and the initiating party of the credential recovery. |
| **CRRC.07** | C1,C2,C3 | The entity under assessment SHOULD inform the Holder of the change in credential status. |
| **CRRC.08** | C1,C2,C3 | The entity under assessment MAY make available the credential recovery information to the Holder and any Verifier. |
| **CRRV** |  | ***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 the credential *(for example, due to the expiry date having been exceeded or the detection of suspicious activity).* |
| **CRRV.02** | C1,C2,C3 | The entity under assessment MAY immediately revoke the credential without prior suspension in cases where the entity under assessment determines that the risk or evidence warrants revocation. |
| **CRRV.03** | C1,C2,C3 | The entity under assessment MAY provide to the Holder of the credential the ability to request the revocation of the credential. |
| **CRRV.04** | C1,C2,C3 | The entity under assessment MUST perform Identity Verification of the Holder making the credential revocation request. |
| **CRRV.05** | C1,C2,C3 | The entity under assessment MUST ensure that credential revocation can only occur based on relevant policy, law, or regulation. |
| **CRRV.06** | C1,C2,C3 | The entity under assessment SHOULD record the following credential revocation information: the effective date of the credential revocation, the reason for the credential revocation, and the initiating party of the credential revocation. |
| **CRRV.07** | C1,C2,C3 | The entity under assessment MUST inform the Holder of the change in the credential status. |
| **CRRV.08** | C1,C2,C3 | The entity under assessment MAY make available the credential revocation information to the Holder and any Verifier. |