***Contributo di Trust Technologies***

**Premessa.**

Per la verifica di conformità e la dimostrazione del soddisfacimento dei requisiti della ISO/IEC 29115 relativamente ai rispettivi Livelli SPID , il documento del Gestore Trust descrive, nelle tre fasi identificate dallo standard (Enrolment, management, authentication phase) , come i controlli richiesti dallo standard siano stati implementati.

|  |  |  |
| --- | --- | --- |
| **ID** | **SPID Liv 1** | **Rispondenza al requisito** |
| 1.1 | corrisponde al LoA2 ISO/IEC 29115 | Per il Livello di sicurezza 1 SPID (LoA2 dello standard ISO/IEC 29115) l’autenticazione è effettuata tramite un singolo fattore. |
| 1.2 | sistemi di autenticazione informatica a un fattore, quale la password | Per il Livello di sicurezza 1 SPID l’autenticazione è effettuata tramite ***User ID*** e ***Password*** |
| 1.3 | Ulteriori requisiti da Regolamento AgID | [Controllo ***StrongPassword***   * **Livelli 1-2** (LoA2-3). La password policy impostata sulla piattaforma di identity & access management segue le Best Practices in materia, **coerentemente con quanto disposto da AgID nelle modalità attuative SPID**. ] |
| 1.4 | Successful authentication shall be dependent upon the entity proving, through a secure authentication protocol, that the entity has control of the credential | Sono stati implementati i controlli e le misure necessari per garantire la conformità e per mitigare le minacce descritte al paragrafo **10.1.2** del l’ISO/IEC 29115 (Enrolment phase).  [*Esempio:*  *…*  *Controllo* ***IdentityProofing:PolicyAdherence***   * ***Livelli 1-2-3*** *(LoA2-3-4). Le modalità di identificazione previste dal Gestore (“de-visu”, con firma digitale qualificata) sono conformi con quanto definito all’Art.7 comma 2 lettere a) e d) del decreto SPID; la procedura di verifica delle informazioni di identità sono conformi con quanto definito all’Art.7, comma 6 e 7 del decreto SPID.* ]   Sono stati implementati i controlli e le misure necessari per garantire la conformità e per mitigare le minacce descritte al paragrafo **10.2.2** del l’ISO/IEC 29115 (management phase).  *[ESEMPI …..*  *Controllo* ***AppropriateCredentialIssuance***   * ***Livelli 1-2*** *(LoA2-3). Il processo di emissione e consegna delle credenziali al titolare avviene utilizzando due canali – email ed SMS – che appartengono legittimamente al titolare in quanto già verificate dal Gestore in fase di registrazione.*   *Controllo* ***ActivatedByEntity***   * ***Livello 1*** *(LoA2). La credenziale viene attivata dal titolare solo al suo primo utilizzo: difatti in tale occasione il titolare è obbligato a cambiare la password ed a definirne una nuova, personale, secondo le policy di sicurezza previste dalla normativa in materia (e dal DPCM SPID).*   *……*  *Controllo* ***EncryptedSession***   * ***Livelli 1-2*** *(LoA2-3). Tutte le sessioni di autenticazione utilizzano TLS 1.0 come protocollo di trasporto. ]* |
| 1.5 | Controls should be in place to reduce the effectiveness of eavesdropper and online guessing attacks | Sono stati implementati i controlli e le misure necessari per garantire la conformità e per mitigare le minacce descritte al paragrafo **10.3.2** del l’ISO/IEC 29115.  [*Online Guessing :*  *- StrongPassword*  *- CredentialLockOut*  *- DefaultAccountUse*  *- AuditAndAnalyze*  - …… ]  Per ciascuna minaccia è stato descritto il controllo implementato.  [Esempi  *Controllo* ***StrongPassword***   * ***Livelli 1-2*** *(LoA2-3). La password policy impostata sulla piattaforma di identity & access management segue le Best Practices in materia, coerentemente con quanto disposto da AgID nelle modalità attuative SPID.*   *Controllo* ***CredentialLockout***   * ***Livello 1*** *(LoA2). La piattaforma di identity management implementa un meccanismo di blocco temporaneo della credenziale dopo un numero – configurabile – di tentativi falliti di immissione della password.*   *……*  *…..*   * ] |
| 1.6 | Controls shall be in place to protect against attacks on stored credentials | Come sopra. |

|  |  |  |
| --- | --- | --- |
| **ID** | **SPID Liv 2** | **Rispondenza al requisito** |
| 2.1 | corrisponde al LoA3 ISO/IEC 29115 | Per il Livello di sicurezza 2 SPID (LoA3 dello standard ISO/IEC 29115) l’autenticazione è effettuata tramite due fattori. |
| 2.2 | sistemi di autenticazione informatica a due fattori, non basati necessariamente su certificati digitali | Per il Livello di sicurezza 2 SPID l’autenticazione a due fattori tramite ***User ID*** & ***Password (Livello 1)* + *OTP via SMS***. |
| 2.3 | Regolamento AgID (Art. 15) |  |
| 2.4 | shall employ multifactor authentication | Sono stati implementati i controlli e le misure necessari per garantire la conformità e per mitigare le minacce descritte al paragrafo 10.3.2 del l’ISO/IEC 29115.  Per ciascuna minaccia è stato descritto il controllo implementato.  *[esempio.*  *……*  *Controllo* ***CredentialLockout***  ***Livello 2*** *(LoA3). Si applica quanto indicato a Livello 1 (LoA2). Inoltre la piattaforma di identity management implementa un meccanismo di annullamento del codice OTP dopo un numero – configurabile – di tentativi falliti di immissione.*  *……]* |
| 2.5 | Any secret information exchanged in authentication protocols shall be cryptographically protected in transit and at rest (although LoA3 does not require the use of a cryptographic-based challenge-response protocol) | *Controllo* ***EncryptedSession***  ***Livelli 1-2*** *(LoA2-3). Tutte le sessioni di autenticazione utilizzano TLS 1.0 come protocollo di trasporto* |
| 2.6 | no requirements concerning the generation or storage of credentials; they may be stored or generated in general purpose computers or in special purpose hardware | Sono stati implementati i controlli e le misure necessari per garantire la conformità e per mitigare le minacce descritte al paragrafo **10.2.2** del l’ISO/IEC 29115 (management phase).  [*ESEMPI*.  *…..*  *Controllo* ***AppropriateCredentialCreation***   * ***Livello 1*** *(LoA2). La creazione delle credenziali avviene attraverso un processo automatico ed atomico che prevede la creazione contestuale di UserID e Password durante la stessa transazione; ciò viene performato dal sistema di Credential Management e le credenziali vengono memorizzate in un “repository” interno.* * ***Livello 2*** *(LoA3). Si applica quanto previsto a Livello 1 (LoA2): nello specifico la credenziale di livello 2 (LoA3) prevista dal Gestore (UserID&Password + OTP via SMS) viene effettuata con una combinazione multi-token attraverso l’utilizzo di un “token con segreto memorizzato” di Livello 1 (LoA2 Password) + un “token out-of-band” di Livello 1 (OTP ricevuto via SMS al numero di telefono cellulare del titolare). In tal modo non è necessario alcun vincolo aggiuntivo di protezione contro la manomissione per credenziali di Livello 2 (LoA3), come prevede lo standard ISO/IEC 29115 per token di Livello 2 (LoA3).*   *…..*  *Controllo* ***CredentialSecureStorage***   * ***Livello 1*** *(LoA2). Le credenziali di Livello 1 (LoA2 Password) vengono memorizzate “hashed” sui sistemi che le custodiscono, pertanto non contengono segreti in chiaro. In aggiunta l’accesso logico a tali sistemi (repository) è consentito solo agli Amministratori di Sistema – nominati direttamente dal Responsabile della Sicurezza e sottoposti a revisione continua – ed in nessun caso è possibile l’accesso dall’esterno a tali sistemi.*   *Infine, la policy di gestione delle Password di Livello 1 (LoA2) è descritta nelle cosiddette “Condizioni generali di utilizzo del servizio SPID” che il titolare ha accettato e sottoscritto – con firma autografa o digitale – al momento dell’adesione al servizio.*   * ***Livello 2*** *(LoA3). Si applica quanto indicato a Livello 1 (LoA2). Nello specifico il Livello 2 (LoA3) per la credenziale prevista dal Gestore (UserID&Password + OTP via SMS) viene attuato tramite combinazione multi-token attraverso l’utilizzo di un “token con segreto memorizzato” di Livello 1 (LoA2 Password) + un “token out-of-band” di Livello 1 (OTP ricevuto via SMS al numero di telefono cellulare del titolare), in tal modo non è necessario proteggere crittograficamente la credenziale di Livello 1 (LoA2 Password) come prevede lo standard ISO/IEC 29115 per token di Livello 2 (LoA3).* |

|  |  |  |
| --- | --- | --- |
| **ID** | **SPID Liv 3** | **Rispondenza al requisito** |
| 3.1 | corrisponde al LoA4 ISO/IEC 29115 |  |
| 3.2 | sistemi di autenticazione informatica a due fattori basati su certificati digitali |  |
| 3.3 | le chiavi private del sistema di autenticazione sono custodite su dispositivi che soddisfano i requisiti dell'Allegato 3 della Direttiva 1999/93/CE  + regolamento AgID (Art. 15) |  |
| 3.4 | shall employ multifactor authentication |  |
| 3.5 | use of tamper-resistant hardware devices for the storage of all secret or private cryptographic keys |  |
| 3.6 | all Personally Identifiable Information and other sensitive data included in authentication protocols shall be cryptographically protected in transit and at rest |  |
| 3.7 | in-person identity proofing for human entities |  |