SERVIZIO SPID

Controlli e Procedure di conformità

Indice degli argomenti

[1 Scopo del Documento 3](#_Toc421180524)

[2 Gestione delle credenziali 4](#_Toc421180525)

[2.1 Premessa 4](#_Toc421180526)

[2.2 Credenziali di Livello 1 SPID (LoA2) 4](#_Toc421180527)

[2.2.1 Descrizione 4](#_Toc421180528)

[2.2.2 Consegna 4](#_Toc421180529)

[2.3 Credenziali di Livello 2 SPID (LoA3) 4](#_Toc421180530)

[2.3.1 Descrizione 4](#_Toc421180531)

[2.3.2 Consegna 4](#_Toc421180532)

[2.4 Credenziali di Livello 3 SPID (LoA4) 4](#_Toc421180533)

[2.4.1 Descrizione 4](#_Toc421180534)

[2.4.2 Consegna 4](#_Toc421180535)

[3 Autenticazione 5](#_Toc421180536)

[3.1 Premessa 5](#_Toc421180537)

[3.2 Meccanismi di autenticazione informatica a Livello 1 SPID (LoA2) 5](#_Toc421180538)

[3.3 Meccanismi di autenticazione informatica a Livello 2 SPID (LoA3) 5](#_Toc421180539)

[3.4 Meccanismi di autenticazione informatica a Livello 3 SPID (LoA4) 5](#_Toc421180540)

[4 Descrizione dei controlli necessari per la protezione delle identità digitali in conformità alla ISO/IEC 29115 6](#_Toc421180541)

[4.1 Tipologie di minacce e controlli necessari per la fase di Gestione credenziali 6](#_Toc421180542)

[4.1.1 Descrizione dei controlli/contromisure implementati dal Gestore (gestione delle credenziali) 8](#_Toc421180543)

[4.2 Tipologie di minacce e controlli necessari per la fase di Autenticazione 9](#_Toc421180544)

[4.2.1 Descrizione dei controlli/contromisure implementati dal Gestore (autenticazione) 11](#_Toc421180545)

# Scopo del Documento

Questo documento illustra le procedure e i controlli……

.

# Gestione delle credenziali

## Premessa

La fase di **gestione delle credenziali** comprende tutti i processi relativi alla gestione del ciclo di vita di una credenziale. Alcuni di questi processi dipendono dal fatto se le credenziali sono trasportate o meno su un dispositivo hardware.

Il processo di ***emissione*** delle credenziali è il processo di fornire o in altri termini di associare una identità digitale con una credenziale: alla convalida della procedura di Registrazione, il sistema del Gestore crea e personalizza le credenziali assegnate al Richiedente (che sono in uno stato non attivo per motivi di sicurezza).

Il processo di ***consegna*** rappresenta l’ultima fase relativamente al processo di rilascio di una identità digitale: la complessità varia con il livello di Assurance (LoA) necessario.

**DESCRIZIONE DELLE CREDENZIALI FORNITE DAL GESTORE PER CIASCUN LIVELLO…..**

## Credenziali di Livello 1 SPID (LoA2)

#### Descrizione

**DESCRIZIONE DELLE CREDENZIALI …..**

#### Consegna

**DESCRIZIONE DEL PROCESSO DI CONSEGNA DELLE CREDENZIALI …..**

## Credenziali di Livello 2 SPID (LoA3)

#### Descrizione

**DESCRIZIONE DELLE CREDENZIALI …..**

#### Consegna

**DESCRIZIONE DEL PROCESSO DI CONSEGNA DELLE CREDENZIALI …..**

## Credenziali di Livello 3 SPID (LoA4)

#### Descrizione

**DESCRIZIONE DELLE CREDENZIALI …..**

#### Consegna

**DESCRIZIONE DEL PROCESSO DI CONSEGNA DELLE CREDENZIALI …..**

# Autenticazione

## Premessa

Il processo di **autenticazione** prevede l'uso di un protocollo per dimostrare il possesso e/o il controllo di una credenziale per stabilire la fiducia in una identità.

I requisiti del protocollo di autenticazione variano a seconda del *Livello di Assurance* (*LoA*) applicabile. L’autenticazione a più fattori è richiesta ai livelli LoA3 e LoA4.

Il processo di verifica delle credenziali utente (l’**autenticazione**) è in grado di assicurare i seguenti livelli di sicurezza:

* **Livello di sicurezza 1 (LoA2 dello standard ISO/IEC 29115)** – sistemi di autenticazione informatica ad un fattore (password o parola chiave);
* **Livello di sicurezza 2 (LoA3 dello standard ISO/IEC 29115)** – sistemi di autenticazione informatica a due fattori, non basati necessariamente su certificati digitali le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all’Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo;
* **Livello di sicurezza 3 (LoA4 dello standard ISO/IEC 29115)** – sistemi di autenticazione informatica a due fattori basati su certificati digitali, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all’Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo.

**DESCRIZIONE DEI MECCANISMI DI AUTENTICAZIONE MESSI A DISPOSIZIONE DAL GESTORE PER CIASCUN LIVELLO…..**

## Meccanismi di autenticazione informatica a Livello 1 SPID (LoA2)

***Descrizione***

**DESCRIZIONE DEI MECCANISMI DI AUTENTICAZIONE DI LIVELLO 1**

## Meccanismi di autenticazione informatica a Livello 2 SPID (LoA3)

***Descrizione***

**DESCRIZIONE DEI MECCANISMI DI AUTENTICAZIONE DI LIVELLO 2**

## Meccanismi di autenticazione informatica a Livello 3 SPID (LoA4)

***Descrizione***

**DESCRIZIONE DEI MECCANISMI DI AUTENTICAZIONE DI LIVELLO 3**

# Descrizione dei controlli necessari per la protezione delle identità digitali in conformità alla ISO/IEC 29115

Questa sezione analizza le tipologie di minacce così come descritte nello standard ISO/IEC DIS 29115 per ognuna delle fasi: **Gestione credenziali e** **Autenticazione**; descrive inoltre i controlli/contromisure necessari previsti per i livelli LoA2, LoA3 e LoA4 dello standard corrispondenti rispettivamente ai Livelli 1, 2 e 3 di SPID.

## Tipologie di minacce e controlli necessari per la fase di Gestione credenziali

La tabella seguente identifica e descrive le minacce previste in fase di Gestione delle credenziali.

|  |  |
| --- | --- |
| **Minaccia** | **Descrizione** |
| CredentialCreation: Tampering | Un utente malintenzionato altera le informazioni che passano dal processo di registrazione al processo di creazione delle credenziali (manomissione). |
| CredentialCreation: UnauthorizedCreation | Un utente malintenzionato porta il Gestore a creare una credenziale basata su una persona fittizia. |
| CredentialIssuance: Disclosure | Una credenziale creata dal Gestore per un'utente viene copiata da un attaccante quando viene consegnata dal Gestore all'utente durante la gestione delle credenziali (divulgazione/rivelazione). |
| CredentialActivation: Unauthorized Possession | Un utente malintenzionato ottiene una credenziale che non appartiene a lui/lei e mascherandosi come utente legittimo porta il Gestore ad attivare la credenziale (emissione non autorizzata). |
| CredentialActivation: Unavailability | 1. L’utente associato ad una credenziale non è nella posizione usuale e non è in grado di autenticare in modo adeguato la propria identità al Gestore. 2. La consegna di una credenziale è ritardata, e non è possibile l'attivazione entro il termine prescritto. |
| CredentialStorage: Disclosure | Credenziali memorizzate in un file system vengono rivelate (ad esempio, un record di nomi utente e password è acceduto da un utente malintenzionato). |
| CredentialStorage: Tampering | Il file che mappa i nomi utente con le credenziali è compromesso in modo tale che le mappature vengono modificate, e le credenziali esistenti sono sostituite da credenziali cui un utente malintenzionato ha accesso. |
| CredentialStorage: Duplication | Un utente malintenzionato utilizza informazioni memorizzate per creare una credenziale duplicata che può essere utilizzata da un'utente non autorizzato. |
| CredentialStorage: DisclosureByEntity | L'utente mantiene una traccia scritta del nome utente e della password in un luogo che può essere acceduto da altri. |
| CredentialRevocation: DelayedRevocation | La diffusione delle informazioni di revoca non è tempestivo comportando una minaccia agli utenti con credenziali revocate ma ancora in grado di autenticare prima che vengano aggiornate le ultime informazioni di revoca. |
| CredentialRevocation: UseAfterDecommissioning | Gli account utente non vengono eliminati quando i dipendenti lasciano una organizzazione portando ad un possibile uso improprio dei vecchi account da parte di persone non autorizzate.  Una credenziale memorizzata in un dispositivo hardware viene utilizzata dopo che le sue chiavi crittografiche sono state revocate. |
| CredentialRenewal: Disclosure | Una credenziale rinnovata dal Gestore per un'utente viene copiata da un attaccante nel momento in cui viene trasportata. |
| CredentialRenewal: Tampering | Una nuova credenziale creata da un utente viene modificata da un attaccante mentre viene sottoposta al Gestore la sostituzione di una credenziale scaduta. |
| CredentialRenewal: UnauthorizedRenewal | Un utente malintenzionato è in grado di trarre vantaggio da una procedura debole di rinnovo delle credenziali per prorogare il periodo di validità delle credenziali per un'utente corrente.  Un utente malintenzionato inganna il Gestore in emissione di una nuova credenziale per un'utente corrente, e la nuova credenziale lega l’identità dell'utente corrente alla credenziale fornita dall'attaccante. |
| CredentialRecordkeeping: Repudiation | L'utente afferma o sostiene che una credenziale legittima è fraudolenta o contiene informazioni errate negando falsamente di aver utilizzato le credenziali. |

Tabella 1. Minacce previste in fase di Gestione credenziali

La tabella seguente identifica i controlli necessari per la protezione contro le minacce previste per la fase di Gestione delle credenziali, per ogni Livello di sicurezza. Nella tabella sotto il simbolo ‘✓’ indica che il controllo - in conformità alla ISO - deve essere applicato al Livello corrispondente, ‘N/A’ indica che il controllo non è applicabile al Livello corrispondente. Infine, ‘N/D’ indica che il Livello corrispondente non è disponibile; mentre le celle con una linea diagonale indicano che il rispettivo controllo non è applicabile al Livello corrispondente perché non richiesto.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minaccia** | **Controlli** | **Controlli Richiesti** | | |
| **Livello 1 SPID (LoA2)** | **Livello 2 SPID (LoA3)** | **Livello 3 SPID (LoA4)** |
| CredentialCreation: Tampering | *AppropriateCredentialCreation* | ✓ | ✓ | ✓ |
| *HardwareOnly* | ✓ | ✓ | ✓ |
| *StateLocked* | ✓ | ✓ | ✓ |
| CredentialCreation: UnauthorizedCreation | *TrackedInventory* | ✓ | ✓ | ✓ |
| CredentialIssuance: Disclosure | *AppropriateCredentialIssuance* | ✓ | ✓ | ✓ |
| CredentialActivation: UnauthorizedPossession  CredentialActivation: Unavailability | *ActivatedByEntity* | ✓ | ✓ | ✓ |
| CredentialStorage: Disclosure  CredentialStorage: Tampering  CredentialStorage: Duplication  CredentialStorage: DisclosureByEntity | *CredentialSecureStorage* | ✓ | ✓ | ✓ |
| CredentialRevocation: DelayedRevocation  CredentialRevocation: UseAfterDecommissioning | *CredentialSecureRevocation&Destruction* | ✓ | ✓ | ✓ |
| CredentialRenewal: Disclosure  CredentialRenewal: Tampering  CredentialRenewal: UnauthorizedRenewal | *CredentialSecureRenewal* | ✓ | ✓ | ✓ |
| CredentialRecordkeeping: Repudiation | *RecordRetention* | ✓ | ✓ | ✓ |

Tabella 2. Controlli richiesti in fase di Gestione credenziali ad ogni LoA

**DI SEGUITO LA DESCRIZIONE DI COME SONO STATI IMPLEMENTATI I CONTROLLI NECESSARI AL PROCESSO DI GESTIONE DELLE CREDENZIALI NELLA SOLUZIONE DEL GESTORE PER OGNI SPECIFICO LIVELLO…..**

### Descrizione dei controlli/contromisure implementati dal Gestore (gestione delle credenziali)

Il seguente paragrafo descrive come i controlli necessari sono implementati per garantire la conformità allo standard ISO/IEC DIS 29115.

Controllo ***AppropriateCredentialCreation***

* **Livello 1** (LoA2). …
* **Livello 2** (LoA3). ….
* **Livello 3** (LoA4). ….

Controllo ***HardwareOnly***

* **Livello 1** (LoA2). …
* **Livello 2** (LoA3). ….
* **Livello 3** (LoA4). ….

Controllo ***StateLocked***

* **Livello 1** (LoA2). …
* **Livello 2** (LoA3). ….
* **Livello 3** (LoA4). ….

Controllo ***TrackedInventory***

* **Livello 1** (LoA2). …
* **Livello 2** (LoA3). ….
* **Livello 3** (LoA4). ….

Controllo ***AppropriateCredentialIssuance***

* **Livello 1** (LoA2). …
* **Livello 2** (LoA3). ….
* **Livello 3** (LoA4). ….

Controllo ***ActivatedByEntity***

* **Livello 1** (LoA2). …
* **Livello 2** (LoA3). ….
* **Livello 3** (LoA4). ….

Controllo ***CredentialSecureStorage***

* **Livello 1** (LoA2). …
* **Livello 2** (LoA3). ….
* **Livello 3** (LoA4). ….

Controllo ***CredentialSecureRevocation&Destruction***

* **Livello 1** (LoA2). …
* **Livello 2** (LoA3). ….
* **Livello 3** (LoA4). ….

Controllo ***CredentialSecureRenewal***

* **Livello 1** (LoA2). …
* **Livello 2** (LoA3). ….
* **Livello 3** (LoA4). ….

Controllo ***RecordRetention***

* **Livello 1** (LoA2). …
* **Livello 2** (LoA3). ….
* **Livello 3** (LoA4). ….

## Tipologie di minacce e controlli necessari per la fase di Autenticazione

Le possibili minacce alla fase di autenticazione includono sia minacce associate all'uso di credenziali durante l'autenticazione sia minacce generiche per l'autenticazione. Queste ultime includono, ma non sono limitate a: software malevolo (ad esempio, virus, Trojan, worms, spyware); ingegneria sociale (ad esempio, shoulder surfing, furto di dispositivi hardware e pin); errori utente (ad esempio, password deboli, incapacità di proteggere le informazioni di autenticazione); falso ripudio; intercettazione non autorizzata e/o modifica dei dati di autenticazione durante la trasmissione; e carenze procedurali.

Con l'eccezione dell'uso di autenticazione a più fattori, controlli per minacce generiche per l'autenticazione esulano dal contenuto del presente documento, che si concentra sulle minacce associate all'uso di credenziali per l'autenticazione, descrive tali minacce, ed elenca i controlli previsti per ogni tipo di minaccia.

La tabella seguente identifica e descrive le minacce previste in fase di Autenticazione.

|  |  |
| --- | --- |
| **Minaccia** | **Descrizione** |
| General threats | Minacce generiche per l'autenticazione includono molte categorie di minacce alla sicurezza comuni a qualsiasi tipo di ICT. Alcuni esempi includono *keystroke logger*, ingegneria sociale, ed errori degli utenti. Si noti che l'autenticazione a più fattori non protegge contro tutte le possibili minacce generiche. |
| Online Guessing | Un utente malintenzionato si connette al sito del verificatore online ed esegue ripetuti tentativi di accesso provando ad indovinare il token valido (ad esempio attacchi online basati su dizionari o password note). |
| Offline Cracking | Il *cracking* della password si basa spesso su metodi di *brute force*, come ad esempio l'utilizzo di attacchi del dizionario. Ad esempio una chiave viene estratta utilizzando tecniche di analisi differenziale su token hardware rubati oppure un token software PKI può essere soggetto ad attacchi da dizionario per identificare la password corretta da usare per decifrare la chiave privata. |
| Credential Duplication | La credenziale dell’utente viene illegittimamente copiata. Un esempio potrebbe essere la copia non autorizzata di una chiave privata. |
| Phishing | L'utente viene ingannato e crede che l'aggressore sia il fornitore di servizi o di identità (sito civetta). L’utente è attratto ad interagire con un verificatore contraffatto, e indotto a rivelare a lui/lei la propria password o dati personali sensibili che possono essere utilizzati per mascherarsi come utente. Un esempio è quando ad un utente viene inviata una e-mail che lo reindirizza su un sito web fraudolento e chiede all'utente di loggarsi utilizzando la propria username e password. |
| Eavesdropping | Un utente malintenzionato ascolta passivamente la transazione di autenticazione per acquisire le informazioni che possono essere utilizzate in un successivo attacco per mascherarsi come utente. |
| Replay Attack | Un utente malintenzionato è in grado di riprodurre messaggi precedentemente catturati (ad esempio tra un soggetto legittimo e un Service Provider) per autenticarsi come tale soggetto al SP. |
| Session Hijack | Un utente malintenzionato è in grado di inserire se stesso tra un utente ed un verificatore in seguito ad uno scambio di autenticazione avvenuto con successo tra questi ultimi. L'attaccante è in grado di porsi come un utente per controllare lo scambio dei dati di sessione. Un esempio è quando un attaccante è in grado di acquisire una sessione già autenticata con l’intercettazione o prevedere il valore del cookie di autenticazione utilizzato per contrassegnare le richieste HTTP inviate dall'utente. |
| Man-In-The-Middle | L'attaccante si posiziona tra l'utente e il verificatore in modo da poter intercettare e modificare il contenuto dei messaggi del protocollo di autenticazione. L'attaccante tipicamente impersona il verificatore all'utente e contemporaneamente impersona l'utente al verificatore. Condurre uno scambio attivo con entrambe le parti contemporaneamente può consentire all’attaccante di utilizzare i messaggi di autenticazione inviati da una parte legittima per autenticarsi con successo all'altra parte. |
| Credential Theft | Un dispositivo che genera o contiene credenziali viene rubato da un utente malintenzionato (ad esempio furto di un cellulare, dispositivo fisico, ecc.). |
| SpoofingAndMasquerading | Spoofing e mascheramento si riferiscono a situazioni in cui un attaccante impersona un altro utente, al fine di consentire al malintenzionato di eseguire un'azione che non sarebbe altrimenti in grado di eseguire (ad esempio, ottenere l'accesso a un bene altrimenti inaccessibile). Questo può essere fatto facendo uso delle credenziali di un’utente o altrimenti ponendosi come l’utente. |

Tabella 3. Minacce previste in fase di Autenticazione

Fatta eccezione per l’obbligo di utilizzare l'autenticazione a più fattori per i livelli LoA3 e LoA4 dello standard ISO/IEC DIS 29115 (corrispondenti, rispettivamente, ai livelli di sicurezza 2 e 3 di SPID), gli altri controlli non sono specifici in termini di LoA ma possono essere applicati ad un qualsiasi livello in funzione del contesto di riferimento.

La tabella seguente identifica i controlli necessari previsti per la protezione contro le minacce per la fase di Autenticazione, per ogni Livello. Nella tabella sotto il simbolo ‘✓’ indica che il controllo - in conformità alla ISO - deve essere applicato al Livello corrispondente, ‘N/A’ indica che il controllo non è applicabile al Livello corrispondente. Infine, ‘N/D’ indica che il Livello corrispondente non è disponibile; mentre le celle con una linea diagonale indicano che il rispettivo controllo non è applicabile al Livello corrispondente perché non richiesto.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Minaccia** | **Controlli** | **Controlli Richiesti** | | |
| **Livello 1 SPID (LoA2)** | **Livello 2 SPID (LoA3)** | **Livello 3 SPID (LoA4)** |
| General threats | *MultiFactorAuthentication* |  | ✓ | ✓ |
| Online Guessing | *StrongPassword*  *CredentialLockOut*  *DefaultAccountUse*  *AuditAndAnalyze* | ✓  ✓  ✓  ✓ | ✓  ✓  ✓  ✓ | ✓  ✓  ✓  ✓ |
| Offline Cracking | *HashedPassword* | ✓ | ✓ | ✓ |
| Credential Duplication | *AntiCounterfeiting* | ✓ | ✓ | ✓ |
| Phishing | *DetectPhishingFromMessages*  *AdoptAntiPhishingPractice*  *MutualAuthentication* | ✓  ✓  ✓ | ✓  ✓  ✓ | ✓  ✓  ✓ |
| Eavesdropping | *NoTransmitPassword*  *EncryptedAuthentication*  *DifferentAuthenticationParameter* | ✓  ✓  ✓ | ✓  ✓  ✓ | ✓  ✓  ✓ |
| Replay Attack | *DifferentAuthenticationParameter*  *Timestamp*  *PhysicalSecurity* | ✓  ✓  ✓ | ✓  ✓  ✓ | ✓  ✓  ✓ |
| Session Hijacking | *EncryptedSession*  *FixProtocolVulnerabilities*  *CryptographicMutualHandshake* | ✓  ✓  ✓ | ✓  ✓  ✓ | ✓  ✓  ✓ |
| Man-In-The-Middle | *MutualAuthentication*  *EncryptedSession* | ✓  ✓ | ✓  ✓ | ✓  ✓ |
| Credential Theft | *CredentialActivation* | ✓ | ✓ | ✓ |
| SpoofingAndMasquerading | *CodeDigitalSignature*  *LivenessDetection* | ✓  ✓ | ✓  ✓ | ✓  ✓ |

Tabella 4. Controlli richiesti in fase di Autenticazione ad ogni LoA

**DI SEGUITO LA DESCRIZIONE DI COME SONO STATI IMPLEMENTATI I CONTROLLI NECESSARI AL PROCESSO DI AUTENTICAZIONE NELLA SOLUZIONE DEL GESTORE PER OGNI SPECIFICO LIVELLO…..**

### Descrizione dei controlli/contromisure implementati dal Gestore (autenticazione)

Il seguente paragrafo descrive come i controlli necessari sono implementati per garantire la conformità allo standard ISO/IEC DIS 29115.

Controllo ***MultiFactorAuthentication***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***StrongPassword***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***CredentialLockout***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***DefaultAccountUse***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***AuditAndAnalyze***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***HashedPassword***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***Anticounterfeiting***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***DetectPhishingFromMessages***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***AdoptAntiPhishingPractice***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***MutualAuthentication***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***NoTransmitPassword***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***EncryptedAuthentication***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***DifferentAuthenticationParameter***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***Timestamp***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***PhysicalSecurity***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***EncryptedSession***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***FixProtocolVulnerabilities***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***CryptographicMutualHandshake***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***CredentialActivation***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***CodeDigitalSignature***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...

Controllo ***LivenessDetection***

* **Livello 1** (LoA2). …..
* **Livello 2** (LoA3)…….
* **Livello 3** (LoA4). …...