L'AUTENTICAZIONE ELETTRONICA O IDENTITÀ DIGITALE

Digital Identity or Electronic Authentication (e-authentication)

Autore: Aldo Pedico – Enterprise Security & Privacy

Contatto: pedicoaldo@gmail.com

PREMESSA

L'identità digitale presenta una sfida tecnica perché spesso implica la verifica delle persone e la loro autenticazione su una rete aperta. Ciò presenta molteplici attacchi che possono portare ad affermazioni fraudolente dell'identità digitale di un soggetto.

Uno dei principali obiettivi dell'identità digitale è l'associazione di un insieme di attività ad una singola entità specifica. Ci sono tuttavia situazioni in cui ciò non è richiesto o è addirittura indesiderabile (ad esempio, casi d'uso in cui sono richiesti l'anonimato o lo pseudonimo), ci sono altri casi in cui è importante stabilire in modo affidabile un'associazione con un soggetto della vita reale, ad esempio l'ottenimento dell'assistenza sanitaria e l'esecuzione di transazioni finanziarie.

Ed ancora, la necessita che un fiduciario (RELYING PARTY - RP) *sappia qualcosa sull'interessato che esegue una transazione, senza conoscerne l'identità nella vita reale.*

A. CHE COSA È

L'Autenticazione Elettronica (E-AUTHENTICATION) *è il processo necessario per stabilire la sicurezza delle identità degli utenti presentate elettronicamente a un sistema informativo.*

Tale processo si avvale di uno o più autenticazioni utilizzate per stabilire l'identità digitale.

E-AUTHENTICATION *è la rappresentazione univoca di un soggetto impegnato in una transazione online e* dovrebbe stabilire che il soggetto in questione sia effettivamente chi afferma di essere. **(La certezza matematica del rischio zero non esiste: l'uso del condizionale è d'obbligo!)**

B. PERCHÉ È NECESSARIA

*Per i servizi in cui è applicabile, l'*E-AUTHENTICATION *fornisce delle ragionevoli garanzie sul rischio che il soggetto, che opera on line, sia sempre lo stesso che ha avuto accesso al servizio in precedenza e che lo sarà nel futuro (ad esempio, furto di identità).*

C. COME AVVIENE

*L'*E-AUTHENTICATION *dell'interessato viene eseguita mediante controlli di uno o più autenticatori (denominati* TOKEN*) associati alla persona interessata.*

D. RISULTATI ATTESI DALLA VERIFICA DELL'IDENTITÀ

- ✓ *Univocità ed unicità dell'identità dichiarata nel contesto della popolazione di utenti serviti dal* CSP *(*CREDENTIAL SERVICE PROVIDER*).*
- ✓ *Convalida di tutte le prove fornite (corrette e autentiche: ad esempio, non contraffatte o sottratte indebitamente).*
- ✓ *Convalida dell'esistenza dell'identità dichiarata nel mondo reale.*
- ✓ *Verifica che l'identità dichiarata sia associata alla persona reale che fornisce la prova dell'identità.*

INDICE DEGLI ARGOMENTI

1. DIGITAL IDENTITY MODEL

OVERVIEW

L'identità digitale è la rappresentazione univoca di un soggetto impegnato in una transazione online.

*Il processo utilizzato per verificare l'associazione di un soggetto con la sua identità nel mondo reale è chiamato "***IDENTITY PROOFING***" e la parte da verificare è chiamata "***APPLICANT***" (il richiedente).*

*Quando il richiedente completa con successo il processo di correzione, viene indicato come "***SUBSCRIBER***" (l'interessato).*

La forza della verifica dell'identità è descritta da una misurazione ordinale chiamata IAL *(*IDENTITY ASSURANCE LEVEL*).*

Il livello IAL1 *non richiede la verifica dell'identità, quindi qualsiasi informazione sugli attributi fornita dal richiedente è auto-affermata o dovrebbe essere trattata come auto-affermata e non verificata (anche se fornita da un CSP a un RP).*

IAL2 *e* IAL3 *richiedono la verifica dell'identità e l'RP può richiedere informazioni sull'asserzione CSP sull'interessato, come valori di attributo verificati, riferimenti di attributo verificati o identificatori pseudonimi.*

Queste informazioni aiutano il PR nel prendere decisioni di autorizzazione.

Un RP può decidere di richiedere IAL2 o IAL3, ma può aver bisogno solo di attributi specifici, con il risultato che il soggetto mantiene un certo grado di pseudonimo.

Questo approccio di miglioramento della privacy ha il vantaggio di separare la forza del processo di VERIFICA da quella del processo di AUTENTICAZIONE.

Un RP può anche impiegare un approccio di identità federata in cui il RP esternalizza tutta la verifica dell'identità, la raccolta degli attributi e l'archiviazione degli attributi ad un CSP.

*In questo trattato, la parte da autenticare è chiamata "***CLAIMANT***" (Ricorrente) e la parte che verifica tale identità è chiamata "***VERIFIER***" (Verificatore).*

Quando un ricorrente dimostra con successo il possesso e il controllo di uno o più autenticatori a un verificatore tramite un protocollo di autenticazione, il verificatore può constatare che il richiedente sia un interessato valido.

Il verificatore trasmette un'asserzione sull'interessato (pseudonimo o non pseudonimo) al PR.

Tale asserzione include un identificatore e può includere informazioni sull'identità dell'interessato, come il nome o altri attributi che sono stati raccolti nel processo di registrazione.

Se il verificatore è anche l'RP, l'asserzione può essere implicita.

L'RP può utilizzare le informazioni autenticate fornite dal verificatore per prendere decisioni di autorizzazione.

L'autenticazione stabilisce la certezza che il richiedente sia in possesso di uno o più autenticatori vincolati alla credenziale, e in alcuni casi nei valori degli attributi del sottoscrittore.

La forza del processo di autenticazione è descritta da una misura ordinale chiamata AAL.

AAL1 richiede l'autenticazione a fattore singolo ed è consentito con una varietà di diversi tipi di autenticatore.

In AAL2, l'autenticazione richiede due fattori di autenticazione per una sicurezza aggiuntiva.

L'autenticazione al livello più alto AAL3 richiede inoltre l'uso di un autenticatore basato su hardware e una resistenza alla rappresentazione del verificatore.

Le varie entità e interazioni che compongono il modello di identità digitale qui utilizzato sono illustrate nella Figura 4-1

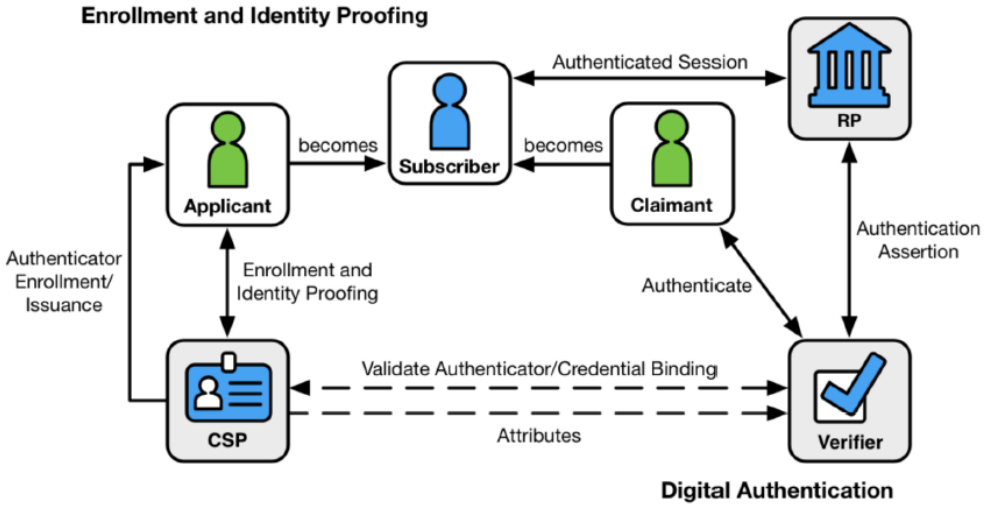

Figure 4-1 Digital Identity Model

Il lato sinistro della Figura 4-1 mostra la registrazione, il rilascio delle credenziali, le attività di gestione del ciclo di vita e i vari stati di un processo di verifica dell'identità e autenticazione.

La consueta sequenza di interazioni è la seguente:

1. *Un richiedente* (APPLICANT) *fa richiesta a un CSP attraverso un processo di iscrizione.*
2. *L'identità del CSP prova tale richiedente. In caso di esito positivo della prova, il richiedente diventa un interessato* (SUBSCRIBER).
3. *Tra il CSP e l'interessato si inseriscono gli autenticatori e le credenziali corrispondenti.*
4. *Il CSP conserva la credenziale, il suo stato e i dati di registrazione raccolti per tutta la durata della credenziale (almeno). L'interessato mantiene i suoi autenticatori.*

Il lato destro della Figura 4-1 mostra le entità e le interazioni coinvolte nell'utilizzo di un autenticatore per eseguire l'autenticazione digitale.

Un interessato è00000 definito ricorrente (CLAIMANT) *quando deve autenticarsi presso un verificatore.*

Le interazioni sono le seguenti:

1. *Il richiedente* (APPLICANT) *dimostra al verificatore* (VERIFIER) *il possesso e il controllo dell'autenticatore o degli autenticatori tramite un protocollo di autenticazione.*
2. *Il verificatore interagisce con il CSP per convalidare la credenziale che lega l'identità dell'interessato al suo autenticatore e per ottenere facoltativamente gli attributi del richiedente.*
3. *Il CSP o verificatore fornisce un'asserzione sull'interessato alla RP, che può utilizzare le informazioni nell'asserzione per prendere una decisione di autorizzazione.*

4. *Viene stabilita una sessione autenticata tra l'interessato e il RP.*

AUTHENTICATORS

Il paradigma classico per i sistemi di autenticazione individua tre fattori come capisaldi di autenticazione:

- *Qualcosa che conosci (ad es. una password).*
- *Qualcosa in tuo possesso (ad es. un badge identificativo o una chiave crittografica).*
- *Qualcosa che sei (ad esempio, un'impronta digitale o altri dati biometrici).*

MFA (MULTI-FACTOR AUTHENTICATION) *si riferisce all'uso di due o più fattori.*

Altri tipi di informazioni, come i dati sulla posizione o l'identità del dispositivo, possono essere utilizzati da un responsabile della protezione o da un verificatore per valutare il rischio in un'identità dichiarata, ma non sono considerati fattori di autenticazione.

I segreti contenuti negli autenticatori si basano su coppie di chiavi pubbliche, chiavi asimmetriche, (PUBLIC KEY PAIRS - ASYMMETRIC KEYS) *o segreti condivisi, chiavi simmetriche* (SHARED SECRETS - SYMMETRIC KEYS).

Una chiave pubblica e una relativa chiave privata costituiscono una coppia di chiavi pubbliche.

La chiave privata è memorizzata nell'autenticatore ed è utilizzata dal richiedente per dimostrare il possesso e il controllo dell'autenticatore.

Un verificatore, conoscendo la chiave pubblica del richiedente attraverso alcune credenziali (in genere un certificato di chiave pubblica), può utilizzare un protocollo di autenticazione per verificare l'identità del richiedente dimostrando che il richiedente ha il possesso e il controllo dell'autenticatore della chiave privata associato.

I segreti condivisi archiviati negli autenticatori possono essere chiavi simmetriche o segreti memorizzati (ad es. password e PIN), a differenza delle chiavi asimmetriche che gli abbonati non devono condividere con il verificatore.

Le chiavi simmetriche sono generalmente memorizzate in hardware o software che l'interessato controlla, mentre le password sono destinate ad essere memorizzate dall'interessato.

I fattori di autenticazione classificati come qualcosa che conosci non sono necessariamente segreti.

La biometria non costituisce un segreto.

L'uso della biometria per l'autenticazione è consentita solo quando fortemente vincolata a un autenticatore fisico.

L'autenticazione basata sulla conoscenza, in cui al richiedente è chiesto di rispondere a domande che sono presumibilmente note solo al richiedente, non costituisce un segreto accettabile per l'autenticazione digitale.

Un sistema di autenticazione digitale può incorporare più fattori in due modi:

1. *Il sistema può essere implementato in modo che al verificatore vengano presentati più fattori; oppure*
2. *Alcuni fattori possono essere utilizzati per proteggere un segreto che verrà presentato al verificatore.*

Ad esempio, il primo modo può essere soddisfatto abbinando un segreto memorizzato (quello che sai) con un dispositivo di banda (quello che hai). Entrambi gli output dell'autenticatore vengono presentati al verificatore per autenticare il ricorrente.

Il secondo modo considera un componente hardware (l'autenticatore) che contiene una chiave crittografica (il segreto dell'autenticatore) in cui l'accesso è protetto da un'impronta digitale. Se utilizzata con il biometrico, la chiave crittografica produce un output che viene utilizzato per autenticare il ricorrente.

Come notato sopra, la biometria, quando impiegata come singolo fattore di autenticazione, non costituisce segreti accettabili per l'autenticazione digitale, ma hanno il loro posto nell'autenticazione delle identità digitali.

AUTHENTICATION PROCESS

Il processo di autenticazione inizia con il ricorrente che dimostra al verificatore il possesso e controllo di un autenticatore che è vincolato all'identità asserita tramite un protocollo di autenticazione.

Una volta dimostrato il possesso e il controllo, il verificatore si accerta che la credenziale rimanga valida, di solito, interagendo con il CSP.

I meccanismi situati presso il verificatore possono mitigare gli attacchi online contro segreti, come password e PIN, limitando la velocità con cui un aggressore può effettuare tentativi di autenticazione o ritardare in altro modo tentativi errati. In genere, ciò viene fatto tenendo traccia e limitando il numero di tentativi non riusciti, poiché la premessa di un attacco online è che la maggior parte dei tentativi fallirà.

Il verificatore è un ruolo funzionale, ma è spesso implementato in combinazione con il CSP, il RP, o entrambi. Se il verificatore è un'entità separata dal CSP, è spesso desiderabile garantire che il verificatore non conosca il segreto dell'autenticatore dell'interessato nel processo di autenticazione, o garantire almeno che il verificatore non abbia accesso illimitato ai segreti archiviati dal CSP.

RELYING PARTIES

Un RP si basa sui risultati di un protocollo di autenticazione per stabilire la fiducia nell'identità o negli attributi di un interessato allo scopo di condurre una transazione online.

Gli RP possono utilizzare l'identità autenticata di un interessato (pseudonimo o non pseudonimo), IAL, AAL e FAL (FAL che indica la forza del protocollo di asserzione) e altri fattori per decidere l'autorizzazione.

Il verificatore e l'RP possono essere la stessa entità o possono essere entità separate. Se sono entità separate, l'RP normalmente riceve un'asserzione dal verificatore.

L'RP garantisce che l'asserzione provenga da un verificatore di fiducia dell'RP.

L'RP elabora anche qualsiasi informazione aggiuntiva nell'asserzione, come attributi personali o tempi di scadenza.

L'RP è l'arbitro finale riguardo al fatto che una specifica asserzione presentata da un verificatore soddisfi i criteri stabiliti dall'RP per l'accesso al sistema indipendentemente da IAL, AAL o FAL.

2. PROCESS FLOW

Flusso di base per la verifica dell'identità.

1°. RESOLUTION: *raccolta degli attributi e delle prove.*

- ✓ *Distinzione univoca dell'individuo.*
- ✓ *Esempi*
  - *a. Il CSP raccoglie le PII dal richiedente (ad esempio nome, indirizzo, data di nascita, e-mail e numero di telefono).*
  - *b. Il CSP raccoglie anche due forme di prova dell'identità, come la patente di guida e il passaporto. Ad esempio, utilizzando la fotocamera di un laptop, il CSP può acquisire una foto di entrambi i lati di entrambi i documenti di identità.*

2°. VALIDATION: *validazione degli attributi e delle prove raccolte.*

- ✓ *Autenticità, validità e accuratezza delle informazioni sull'identità della persona.*
- ✓ *Esempi*
  - *a. Il CSP convalida le informazioni raccolte precedentemente verificandone una fonte autorevole.*
  - *b. Il CSP interroga le fonti emittenti dei documenti e convalida le corrispondenze delle informazioni.*

3°. VERIFICATION: *verifica degli attributi e delle prove raccolte.*

- ✓ *Confermato e accertato il collegamento tra l'identità dichiarata e l'esistenza del soggetto che presenta le prove.*
- ✓ *Esempi*
  - *a. Il CSP invia un codice di registrazione al numero di telefono convalidato del richiedente, l'utente fornisce il codice di registrazione al CSP e il CSP conferma la corrispondenza, verificando che l'utente sia in possesso e controllo del numero di telefono convalidato.*
  - *b. Il richiedente è stato verificato con successo.*

3. IDENTITY RESOLUTION, VALIDATION, AND VERIFICATION

Questa sezione elenca i requisiti per risolvere, convalidare e verificare un'identità e qualsiasi prova di identità fornita.

I requisiti hanno lo scopo di garantire che l'identità dichiarata sia l'identità effettiva del soggetto che tenta di iscriversi al CSP e che gli attacchi scalabili che colpiscono una vasta popolazione di individui iscritti richiedano tempi e costi maggiori rispetto al valore delle risorse che il sistema sta proteggendo.

IDENTITY RESOLUTION

L'obiettivo della risoluzione dell'identità è distinguere in modo univoco un individuo all'interno di una data popolazione o contesto.

La risoluzione effettiva dell'identità utilizza il più piccolo insieme di attributi necessari per risolvere un individuo univoco. Fornisce al CSP un importante punto di partenza nel processo complessivo di

verifica dell'identità, per includere l'individuazione iniziale di potenziali frodi, ma non rappresenta in alcun modo una transazione completa e di successo per la verifica dell'identità.

IDENTITY EVIDENCE COLLECTION AND VALIDATION

L'obiettivo della convalida dell'identità è raccogliere le prove di identità più appropriate (ad esempio, passaporto o patente di guida) dal richiedente e determinarne l'autenticità, la validità e l'accuratezza.

L'obiettivo della convalida dell'identità è raccogliere le prove di identità più appropriate (ad esempio, passaporto o patente di guida) dal richiedente e determinarne l'autenticità, la validità e l'accuratezza.

La convalida dell'identità si compone di tre fasi del processo:

1. *raccolta delle prove di identità appropriate,*
2. *conferma che le prove sono autentiche e genuine,*
3. *conferma che i dati contenuti nelle prove di identità siano validi, attuali e relativi a un soggetto reale.*

La tabella accanto (vedi tabella 5-1 del NIST SP 800-63A) elenca i punti di forza, che vanno da UNACCEPTABLE *a* SUPERIOR, *delle prove di identità raccolte per stabilire un'identità valida.*

Salvo diversa indicazione, per ottenere una data forza l'evidenza DEVE (SHALL), *come minimo, soddisfare tutte le qualità elencate.*

TABLE 5-1 STRENGTHS OF IDENTITY EVIDENCE

Strength	Qualities of Identity Evidence
Unacceptable	No acceptable identity evidence provided.

Weak	• The issuing source of the evidence did not perform identity proofing.
	• The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the applicant.
	• The evidence contains:
	  ○ At least one reference number that uniquely identifies itself or the person to whom it relates, **OR**
	  ○ The issued identity evidence contains a photograph or biometric template (of any modality) of the person to whom it relates.

Fair	• The issuing source of the evidence confirmed the claimed identity through an identity proofing process.
	• The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the person to whom it relates.
	• The evidence:
	  ○ Contains at least one reference number that uniquely identifies the person to whom it relates, **OR**
	  ○ Contains a photograph or biometric template (any modality) of the person to whom it relates, **OR**
	  ○ Can have ownership confirmed through KBV.
	• Where the evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed.
	• Where the evidence includes physical security features, it requires proprietary knowledge to be able to reproduce it.
	• The issued evidence is unexpired.

Strong	• The issuing source of the evidence confirmed the claimed identity through written procedures designed to enable it to form a reasonable belief that it knows the real-life identity of the person. Such procedures are subject to recurring oversight by regulatory or publicly-accountable institutions. For example, the Customer Identification Program guidelines established in response to the USA PATRIOT Act of 2001 or the Red Flags Rule, under Section 114 of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act). • The issuing process for the evidence ensured that it was delivered into the possession of the subject to whom it relates. • The issued evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the issued evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names.

	• The:
	  ○ Issued evidence contains a photograph or biometric template (of any modality) of the person to whom it relates, **OR**
	  ○ Applicant proves possession of an AAL2 authenticator, or equivalent, bound to an IAL2 identity, at a minimum.
	• Where the issued evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed.
	• Where the issued evidence contains physical security features, it requires proprietary knowledge and proprietary technologies to be able to reproduce it.
	• The evidence is unexpired.

Superior	• The issuing source of the evidence confirmed the claimed identity by following written procedures designed to enable it to have high confidence that the source knows the real-life identity of the subject. Such procedures are subject to recurring oversight by regulatory or publicly accountable institutions. • The issuing source visually identified the applicant and performed further checks to confirm the existence of that person;. • The issuing process for the evidence ensured that it was delivered into the possession of the person to whom it relates. • The evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names. • The evidence contains a photograph of the person to whom it relates. • The evidence contains a biometric template (of any modality) of the person to whom it relates. • The evidence includes digital information, the information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed. • The evidence includes physical security features that require proprietary knowledge and proprietary technologies to be able to reproduce it. • The evidence is unexpired.

VALIDATING IDENTITY EVIDENCE

Il CSP ottiene le prove di identità (accuracy, authenticity, integrity) ed effettua la verifica presso fonti autorevoli affinché:

- *sia autentico e non contraffatto o falso;*
- *contenga informazioni corrette;*
- *contenga informazioni relative a un argomento della vita reale.*

La tabella 5-2 (del NIST SP 800-63A) elenca i punti di forza, che vanno da UNACCEPTABLE *a* SUPERIOR, *della convalida dell'identità eseguita dal CSP per convalidare le prove presentate per l'attuale sessione di copertura e le informazioni ivi contenute.*

Table 5-2 Validating Identity Evidence

Strength	Method(s) Performed by the CSP
Unacceptable	• Evidence validation was not performed, or validation of the evidence failed.
Weak	• All personal details from the evidence have been confirmed as valid by comparison with information held or published by an authoritative source.
Fair	• Attributes contained in the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s), **OR** • The evidence has been confirmed as genuine using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** • The evidence has been confirmed as genuine by trained personnel, **OR** • The evidence has been confirmed as genuine by confirmation of the integrity of cryptographic security features.
Strong	• The evidence has been confirmed as genuine: o using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** o by trained personnel and appropriate technologies, confirming the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** o by confirmation of the integrity of cryptographic security features. • All personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).
Superior	• The evidence has been confirmed as genuine by trained personnel and appropriate technologies including the integrity of any physical and cryptographic security features. • All personal details and evidence details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).

IDENTITY VERIFICATION

L'obiettivo della verifica dell'identità è di confermare e di stabilire un collegamento tra l'identità dichiarata e l'esistenza reale del soggetto che presenta le prove.

IDENTITY VERIFICATION METHODS

La Tabella 5-3 descrive in dettaglio i metodi di verifica necessari per ottenere un livello di qualità della verifica.

Il CSP DEVE (SHALL) *aderire ai requisiti indicati nel capitolo immediatamente successivo se* KBV *utilizzato per verificare un'identità.*

Table 5-3 Verifying Identity Evidence

Strength	Identity Verification Methods
Unacceptable	Evidence verification was not performed or verification of the evidence failed. Unable to confirm that the applicant is the owner of the claimed identity.
Weak	The applicant has been confirmed as having access to the evidence provided to support the claimed identity.
Fair	• The applicant's ownership of the claimed identity has been confirmed by: o KBV. See Section 5.3.2. for more details, **OR** o a physical comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3, **OR** o biometric comparison of the applicant to the identity evidence. Biometric comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3.
Strong	• The applicant's ownership of the claimed identity has been confirmed by: o physical comparison, using appropriate technologies, to a photograph, to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3, **OR** o biometric comparison, using appropriate technologies, of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Biometric comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3.
Superior	The applicant's ownership of the claimed identity has been confirmed by biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity, using appropriate technologies. Biometric comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3.

KNOWLEDGE-BASED VERIFICATION (KBV) REQUIREMENTS

I seguenti requisiti si applicano ai passaggi di verifica dell'identità per IAL2.

1. *Il CSP* NON DEVE (SHALL NOT) *utilizzare* KBV (KNOWLEDGE-BASED VERIFICATION) *per verificare l'identità di un richiedente rispetto a più di un elemento di prova dell'identità convalidato.*
2. *Il CSP* DEVE (SHALL) *utilizzare solo informazioni che si prevede siano note solo al richiedente e la fonte autorevole, per includere tutte le informazioni necessarie per iniziare il processo KBV.*
   Le informazioni accessibili liberamente, a pagamento di pubblico dominio o tramite il mercato nero NON DEVONO essere utilizzate.
3. *Il CSP* DEVE (SHALL) *consentire a un'identità risolta e convalidata di rinunciare a KBV e sfruttare un altro processo per la verifica.*

4. CSP DOVREBBE (SHOULD) *eseguire KBV verificando la conoscenza della storia delle transazioni recenti in cui il CSP è un partecipante.*
   Il CSP DEVE (SHALL) *garantire che le informazioni sulle transazioni hanno almeno 20 bit di entropia. Ad esempio, per raggiungere i requisiti minimi di entropia, il CSP potrebbe chiedere al richiedente la verifica dell'importo/i e del/i numero/i di transazione/i di un micro-deposito/i su un conto bancario valido, purché il numero totale di cifre è sette o più.*
5. *Il CSP* PUÒ (MAY) *eseguire KBV ponendo al richiedente domande per dimostrare di essere il proprietario delle informazioni richieste.*
   Tuttavia, si applicano i seguenti requisiti:
   a. *KBV* DOVREBBE (SHOULD) *essere basato su più fonti autorevoli.*
   b. *CSP* DEVE (SHALL) *richiedere un minimo di quattro domande KBV, ognuna delle quali richiede una risposta corretta per completare con successo il passaggio KBV.*
   c. *CSP* DOVREBBE (SHOULD) *richiedere domande KBV a risposta libera.*
      Il CSP PUÒ (MAY) *consentire domande a scelta multipla, tuttavia, se vengono fornite domande a scelta multipla, il CSP* DEVE (SHALL) *richiedere un minimo di quattro opzioni di risposta per domanda.*
   d. *CSP* DOVREBBE (SHOULD) *consentire due tentativi al richiedente per completare il KBV ma non più di tre.*
   e. *CSP* DEVE (SHALL) *far scadere le sessioni KBV dopo due minuti di inattività per domanda. In caso di timeout della sessione, il CSP* DEVE (SHALL) *riavviare l'intero processo KBV e considerarlo un tentativo fallito.*
   f. *CSP* NON DEVE (SHALL NOT) *presentare la maggior parte delle domande KBV diversive (cioè quelle in cui "nessuna delle precedenti" è la risposta corretta).*
   g. *CSP* NON DOVREBBE (SHOULD NOT) *porre le stesse domande KBV nei tentativi successivi.*
   h. *CSP* NON DEVE (SHALL NOT) *porre una domanda KBV che fornisca informazioni che potrebbero aiutare a rispondere a qualsiasi futura domanda KBV in una singola sessione o in una sessione successiva dopo un tentativo fallito.*
   i. *CSP* NON DEVE (SHALL NOT) *utilizzare domande KBV per le quali le risposte non cambiano (ad esempio, "Qual è stata la tua prima auto?").*
   j. *CSP* DEVE (SHALL) *garantire che qualsiasi domanda KBV non riveli una* PII (PERSONALLY IDENTIFIABLE INFORMATION) *che il richiedente non abbia già fornito, né informazioni personali che, se combinate con altre informazioni in una sessione KBV, potrebbero comportare un'identificazione univoca.*

REQUIREMENTS FOR SUPERVISED REMOTE IN-PERSON PROOFING

I CSP possono utilizzare processi di verifica remota per raggiungere livelli comparabili di fiducia e sicurezza agli eventi di persona.

La verifica dell'identità remota e le transazioni di registrazione DEVONO (SHALL) *soddisfare i seguenti requisiti, oltre ai requisiti di convalida e verifica IAL3 specificati nella tabella "*TABLE 4-1 IAL REQUIREMENTS SUMMARY*" descritta più avanti, il CSP:*

1. DEVE (SHALL) *monitorare l'intera sessione di verifica dell'identità, dalla quale il richiedente* NON DEVE (SHALL NOT) *discostarsi, ad esempio mediante una trasmissione video continua ad alta risoluzione del richiedente.*
2. DEVE (SHALL) *avere un operatore live che partecipi a distanza con il richiedente per l'intera sessione di verifica dell'identità.*
3. DEVE (SHALL) *richiedere che tutte le azioni intraprese dal richiedente durante la sessione di verifica dell'identità siano chiaramente visibili all'operatore remoto.*
4. DEVE (SHALL) *richiedere che tutte le verifiche digitali delle prove (ad esempio, tramite chip o tecnologie wireless) siano eseguite da scanner e sensori integrati.*
5. DEVE (SHALL) *richiedere agli operatori di aver seguito un programma di formazione per rilevare potenziali frodi e per eseguire correttamente una sessione di verifica remota supervisionata.*
6. DEVE (SHALL) *impiegare il rilevamento di manomissioni fisiche e le caratteristiche di resistenza appropriate per l'ambiente in cui si trova.*
7. DEVE (SHALL) *garantire che tutte le comunicazioni avvengano su un canale protetto reciprocamente autenticato.*

4. IDENTITY ASSURANCE LEVELS (IAL)

La garanzia dell'identità di un interessato è descritta utilizzando uno dei tre IAL*:*

- IAL1: *non è necessario collegare il richiedente a una specifica identità.*
  Tutti gli attributi forniti in combinazione con le attività del soggetto sono auto-affermati o dovrebbero essere trattati come auto-affermati (compresi gli attributi che un CSP asserisce a un RP).
  Gli attributi auto-affermati non sono né convalidati né verificati.
- IAL2: *le prove supportano l'esistenza nel mondo reale dell'identità dichiarata e verificano che il richiedente sia adeguatamente associato a questa identità.*
  IAL2 introduce la necessità di una verifica dell'identità remota o fisicamente presente. Gli attributi potrebbero essere asseriti dai CSP agli RP a sostegno dell'identità pseudonima con attributi verificati.
  Un CSP che supporta IAL2 può supportare le transazioni IAL1 se l'utente acconsente.
- IAL3: *La presenza fisica è richiesta per la prova dell'identità.*
  Gli attributi identificativi devono essere verificati da un rappresentante CSP autorizzato e formato.

La tabella seguente riassume i requisiti per ciascuno dei livelli di garanzia dell'autenticatore.

TABLE 4-1 IAL REQUIREMENTS SUMMARY

Requirement	IAL1	IAL2	IAL3
Presence	No Requirements	In-person and unsupervised remote.	In-person and supervised remote.
Resolution	No Requirements	• The minimum attributes necessary to accomplish identity resolution. • KBV may be used for added confidence.	Same as IAL2
Evidence	No identity evidence is collected.	• One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation occurs with issuing source, **OR** • Two pieces of STRONG evidence, **OR** • One piece of STRONG evidence plus two (2) pieces of FAIR evidence.	• Two pieces of SUPERIOR evidence, **OR** • One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source, **OR** • Two pieces of STRONG evidence plus one piece of FAIR evidence.
Validation	No validation	Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented.	Same as IAL2
Verification	No verification	Verified by a process that is able to achieve a strength of STRONG.	Verified by a process that is able to achieve a strength of SUPERIOR.
Address Confirmation	No requirements for address confirmation	Required. Enrollment code sent to any address of record. Notification sent by means different from enrollment code.	Required. Notification of proofing to postal address.
Biometric Collection	No	Optional	Mandatory
Security Controls	N/A	• SP 800-53 • Moderate Baseline (or equivalent federal or industry standard).	• SP 800-53 • High Baseline (or equivalent federal or industry standard).

5. AUTHENTICATOR ASSURANCE LEVELS (AAL)

La capacità di una transazione di autenticare è caratterizzata da una misura ordinale nota come AAL (AUTHENTICATOR ASSURANCE LEVEL)*.*

Un'autenticazione più forte (un AAL *più alto) richiede che gli attori malintenzionati dispongano di capacità migliori e impieghino maggiori risorse per sovvertire con successo il processo di autenticazione.*

Di seguito viene fornita una sintesi di alto livello dei requisiti tecnici per ciascuno degli AAL*.*

- AAL 1: *fornisce una certa garanzia che il richiedente controlli un autenticatore associato all'account dell'interessato.*

  AAL1 *richiede l'autenticazione a un fattore o a più fattori utilizzando un'ampia gamma di tecnologie di autenticazione disponibili.*

  L'autenticazione valida richiede che l'interessato dimostri il possesso e il controllo dell'autenticatore attraverso un protocollo di autenticazione sicuro.

  AAL1 *richiede l'autenticazione a un fattore o a più fattori utilizzando un'ampia gamma di tecnologie di autenticazione disponibili.*

L'autenticazione riuscita obbliga il richiedente a dimostrare il possesso e il controllo dell'autenticatore tramite un protocollo di autenticazione sicuro.

- AAL 2: *fornisce un'elevata sicurezza che il richiedente controlli gli autenticatori collegati all'account dell'interessato.*
  La prova del possesso e del controllo di due diversi fattori di autenticazione è richiesta tramite il/i protocollo/i di autenticazione sicuro.
  Sono richieste tecniche crittografiche approvate.

- AAL 3: *fornisce un'elevata sicurezza che il richiedente controlli gli autenticatori collegati all'account dell'interessato.*
  L'autenticazione presso AAL3 si basa sulla prova del possesso di una chiave tramite un protocollo crittografico.
  L'autenticazione AAL3 richiede un autenticatore basato su hardware e un autenticatore che fornisca resistenza alla rappresentazione del verificatore.
  Per autenticarsi presso AAL3, i richiedenti sono tenuti a dimostrare il possesso e il controllo di due distinti fattori di autenticazione tramite protocolli di autenticazione sicuri.
  Sono necessarie tecniche crittografiche approvate.

SUMMARY OF REQUIREMENTS

La tabella seguente riassume i requisiti per ciascuno degli AAL

Requirement	AAL1	AAL2	AAL3
Permitted Authenticator Types	Memorized Secret; Look-Up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus: • Look-Up Secret • Out-of-Band • SF OTP Device • SF Crypto Software • SF Crypto Device	MF Crypto Device; SF Crypto Device plus Memorized Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorized Secret
FIPS 140 Verification	Level 1 (Government agency verifiers)	Level 1 (Government agency authenticators and verifiers)	Level 2 overall (MF authenticators) Level 1 overall (verifiers and SF Crypto Devices) Level 3 physical security (all authenticators)
Reauthentication	30 days	12 hours or 30 minutes inactivity; MAY use one authentication factor	12 hours or 15 minutes inactivity; SHALL use both authentication factors
Security Controls	SP 800-53 Low Baseline (or equivalent)	SP 800-53 Moderate Baseline (or equivalent)	SP 800-53 High Baseline (or equivalent)
MitM Resistance	Required	Required	Required
Verifier-Impersonation Resistance	Not required	Not required	Required
Verifier-Compromise Resistance	Not required	Not required	Required
Replay Resistance	Not required	Not required	Required
Authentication Intent	Not required	Recommended	Required
Records Retention Policy	Required	Required	Required
Privacy Controls	Required	Required	Required

6. AUTHENTICATOR AND VERIFIER REQUIREMENTS

In questo capitolo si fornisce una indicazione sui requisiti specifici per ogni tipo di autenticatore.

REQUIREMENTS BY AUTHENTICATOR TYPE

MEMORIZED SECRETS

Un autenticatore segreto memorizzato, comunemente indicato come PASSWORD *o, se numerico,* PIN*, è un valore segreto destinato a essere scelto e memorizzato dall'utente.*

I segreti memorizzati devono essere di complessità e segretezza tali da non consentire a un utente malintenzionato di indovinare o scoprire in altro modo il valore corretto del segreto.

*Un segreto memorizzato è qualcosa "*CHE CONOSCI*"* (Vedi MULTI-FACTOR AUTHENTICATION MFA).

I segreti memorizzati DEVONO (SHALL) *essere lunghi almeno 8 caratteri se scelti dall'interessato, quelli scelti casualmente dal CSP o dal verificatore* DEVE (SHALL) *avere una lunghezza minima di 6 caratteri e* POSSONO (MAY) *essere interamente numerici.*

Se il CSP o il verificatore non consente un segreto memorizzato scelto in base alla sua comparsa su una lista nera di valori compromessi, l'interessato DEVE (SHALL) *scegliere un segreto memorizzato diverso.*

Non DOVREBBERO (SHOULD) *essere imposti altri requisiti di complessità per i segreti memorizzati.*

LOOKUP SECRETS

Un autenticatore segreto di ricerca è un record fisico o elettronico che memorizza una serie di segreti condivisi tra il richiedente e il CSP.

Il richiedente utilizza l'autenticatore per cercare i segreti appropriati necessari per rispondere a una richiesta del verificatore. Ad esempio, il verificatore può chiedere a un richiedente di fornire un sottoinsieme specifico delle stringhe numeriche o di caratteri stampati su una carta in formato tabella.

Un'applicazione comune dei segreti di ricerca è l'uso di "Recovery Keys" *memorizzate dall'interessato per l'uso in caso di smarrimento o malfunzionamento di un altro autenticatore.*

*Un segreto di ricerca è qualcosa "*CHE HAI*"* (Vedi MULTI-FACTOR AUTHENTICATION MFA).

I CSP che creano autenticatori segreti di ricerca DEVONO (SHALL) *utilizzare un generatore di bit casuale approvato per generare l'elenco dei segreti e* DEVONO (SHALL) *consegnare l'autenticatore in modo sicuro all'interessato.*

I segreti di ricerca DEVONO (SHALL) *avere almeno 20 bit di entropia e* POSSONO (MAY) *essere distribuiti dal CSP di persona, per posta all'indirizzo di registrazione dell'interessato o tramite distribuzione online.*

Se distribuiti online, i segreti di ricerca DEVONO (SHALL) *essere distribuiti su un canale sicuro in conformità con i requisiti vincolanti post-iscrizione.*

Se l'autenticatore utilizza i segreti di ricerca in sequenza da un elenco, l'interessato PUÒ (MAY) *disporre dei segreti utilizzati, ma solo dopo una corretta autenticazione.*

OUT OF BAND DEVICES

Un autenticatore OUT-OF-BAND *è un dispositivo fisico indirizzabile in modo univoco e in grado di comunicare in modo sicuro con il verificatore su un canale di comunicazione distinto, denominato canale secondario.*

Il dispositivo è posseduto e controllato dal richiedente e supporta la comunicazione privata su questo canale secondario, separato dal canale principale per l'autenticazione elettronica (E-AUTHENTICATION).

Un autenticatore OUT-OF-BAND *è qualcosa che* (CHE HAI). (Vedi MULTI-FACTOR AUTHENTICATION MFA).

L'autenticatore OUT-OF-BAND *può funzionare in uno dei seguenti modi:*

- *Il richiedente trasferisce un segreto ricevuto dal dispositivo Out-of-Band tramite il canale secondario al verificatore utilizzando il canale principale.*
  Ad esempio, il richiedente può ricevere il segreto sul proprio dispositivo mobile e digitarlo (in genere un codice a 6 cifre) nella sessione di autenticazione.
- *Il richiedente trasferisce un segreto ricevuto tramite il canale principale al dispositivo Out-of-Band per la trasmissione al verificatore tramite il canale secondario.*
  Ad esempio, il richiedente può visualizzare il segreto nella sessione di autenticazione e digitarlo in un'app sul proprio dispositivo mobile o utilizzare una tecnologia come un codice a barre o un codice QR per effettuare il trasferimento.
- *Il richiedente confronta i segreti ricevuti dal canale principale e dal canale secondario e conferma l'autenticazione tramite il canale secondario.*

Lo scopo del segreto è associare in modo sicuro l'operazione di autenticazione sul canale primario e secondario.

Quando la risposta avviene tramite il canale di comunicazione primario, il segreto stabilisce anche il controllo del ricorrente sul dispositivo OUT-OF-BAND.

L'autenticatore OUT-OF-BAND DEVE (SHALL) *stabilire un canale separato con il verificatore per recuperare il segreto o la richiesta di autenticazione.*

Questo canale è considerato OUT-OF-BAND *rispetto al canale di comunicazione principale (anche se termina sullo stesso dispositivo) a condizione che il dispositivo non trasmetta informazioni da un canale all'altro senza l'autorizzazione del richiedente.*

Il dispositivo OUT-OF-BAND DOVREBBE (SHOULD) *essere indirizzabile in modo univoco e la comunicazione sul canale secondario* DEVE (SHALL) *essere crittografata a meno che non sia inviata tramite la rete telefonica pubblica commutata* (PUBLIC SWITCHED TELEPHONE NETWORK - PSTN).

I metodi che non dimostrano il possesso di un dispositivo specifico, come VOICE-OVER-IP (VOIP) *o* E-MAIL, SHALL NOT *essere utilizzati per l'autenticazione OUT-OF-BAND.*

SINGLE-FACTOR OTP DEVICE

Un dispositivo OTP *(*ONE TIME PASSWORD*) a fattore singolo genera OTP.*

Questa categoria include dispositivi hardware e generatori OTP basati su software installati su dispositivi come i telefoni cellulari.

Questi dispositivi hanno un segreto incorporato che viene utilizzato come "seme" per la generazione di un OTP *e non richiede l'attivazione tramite un secondo fattore.*

L'OTP viene visualizzato sul dispositivo e immesso manualmente per la trasmissione al verificatore, **dimostrando così il possesso e il controllo del dispositivo**.

*Un dispositivo OTP a fattore singolo è qualcosa (*CHE POSSIEDI*).* (Vedi MULTI-FACTOR AUTHENTICATION MFA)

I dispositivi OTP a fattore singolo sono simili agli autenticatori segreti di ricerca con l'eccezione che i segreti sono generati crittograficamente e indipendentemente dall'autenticatore e dal verificatore e confrontato dal verificatore.

*Il segreto è calcolato in base a un "*NONCE*" che può essere basato sul tempo o da un contatore sull'autenticatore e sul verificatore.*

Gli autenticatori OTP a fattore singolo contengono due valori persistenti.

1st. *È una chiave simmetrica interna che rimane per tutta la vita del dispositivo.*

2nd. *È un "*NONCE*" modificato ogni volta che è utilizzato l'autenticatore oppure si basa su un orologio in tempo reale.*

La chiave segreta e il suo algoritmo DEVE *(*SHALL*) fornire almeno il livello di sicurezza minimo specificato nell'ultima revisione di SP 800-131A (112 bit alla data di questa pubblicazione).*

Il NONCE DEVE *essere di lunghezza sufficiente per garantire che sia univoco per ogni operazione del dispositivo nel corso della sua vita.*

Gli autenticatori OTP, in particolare i generatori OTP basati su software, DOVREBBERO *(*SHOULD*) scoraggiare e* NON DEVONO *(*SHALL NOT*) facilitare la clonazione della chiave segreta su più dispositivi.*

L'output dell'autenticatore si ottiene utilizzando un cifrario a blocchi o una funzione HASH *per combinare la chiave e il* NONCE *in modo sicuro.*

L'output dell'autenticatore PUÒ *(*MAY*) essere troncato a un minimo di 6 cifre decimali (circa 20 bit di entropia).*

Se il NONCE *utilizzato per generare l'output dell'autenticatore è basato su un orologio in tempo reale, esso* DEVE *(*SHALL*) essere cambiato almeno una volta ogni 2 minuti.*

Il valore OTP associato a un dato NONCE DEVE *(*SHALL*) essere accettato una sola volta.*

MULTI-FACTOR OTP DEVICE

Un dispositivo OTP a più fattori genera OTP da utilizzare nell'autenticazione dopo l'attivazione tramite un fattore di autenticazione aggiuntivo.

Ciò include dispositivi hardware e generatori OTP basati su software installati su dispositivi come i dispositivi mobili telefoni.

Il secondo fattore di autenticazione può essere ottenuto attraverso una sorta di pad di ingresso integrato, un lettore biometrico integrato (ad es. interfaccia del computer (ad es. porta USB).

L'OTP viene visualizzato sul dispositivo e immesso manualmente per la trasmissione al verificatore.

*Ad esempio, un dispositivo OTP può visualizzare 6 caratteri alla volta, dimostrando così "*IL POSSESSO E IL CONTROLLO*" del dispositivo.*

*Il dispositivo OTP a più fattori è qualcosa "*CHE HAI*" e* DEVE (SHALL) *essere attivato da qualcosa che "*TU SAI*" o qualcosa "*CHE SEI*".* (Vedi MULTI-FACTOR AUTHENTICATION MFA)

Gli autenticatori OTP a più fattori funzionano in modo simile agli autenticatori OTP a fattore singolo, tranne per il fatto che richiedono l'inserimento di un segreto memorizzato o l'uso di una biometria per ottenere l'OTP dall'autenticatore. Ogni utilizzo dell'autenticatore DEVE (SHALL) *richiedere l'input del fattore aggiuntivo.*

Oltre alle informazioni di attivazione, gli autenticatori OTP a più fattori contengono due valori persistenti.

1st. *È una chiave simmetrica che persiste per tutta la vita del dispositivo.*

2nd. *È un* NONCE *che viene modificato ogni volta che viene utilizzato l'autenticatore o si basa su un orologio in tempo reale.*

La chiave segreta e il suo algoritmo DEVONO (SHALL) *fornire almeno il livello di sicurezza minimo specificato nell'ultima revisione di SP 800-131A (112 bit alla data di questa pubblicazione).*

Il NONCE DEVE (SHALL) *essere di lunghezza sufficiente per garantire che sia univoco per ogni operazione del dispositivo nel corso della sua vita.*

Gli autenticatori OTP, in particolare i generatori OTP basati su software, DOVREBBERO (SHOULD) *scoraggiare e* NON DEVONO (SHALL NOT) *facilitare la clonazione della chiave segreta su più dispositivi.*

L'output dell'autenticatore è ottenuto utilizzando un cifrario a blocchi approvato o una funzione hash per combinare la chiave e il NONCE *in modo sicuro e* PUÒ (MAY) *essere troncato a un minimo di 6 cifre decimali (circa 20 bit di entropia).*

Se il NONCE *utilizzato per generare l'output dell'autenticatore è basato su un orologio in tempo reale, il nonce* DEVE (SHALL) *essere modificato almeno una volta ogni 2 minuti.*

Il valore OTP associato a un dato nonce DEVE (SHALL) *essere accettato solo una volta.*

Qualsiasi segreto memorizzato utilizzato dall'autenticatore per l'attivazione DEVE (SHALL) *essere un segreto numerico scelto casualmente con una lunghezza di almeno 6 cifre decimali oppure un altro segreto memorizzato e* DEVE (SHALL) *essere limitato in base alla frequenza come specificato nel capitolo "*RATE LIMITING (THROTTLING)*" descritto più avanti.*

Un fattore di attivazione biometrico DEVE (SHALL) *soddisfare i requisiti indicati nel capitolo "*USE OF BIOMETRIC*" descritto più avanti, compresi i limiti su il numero di errori di autenticazione consecutivi.*

La chiave non crittografata e il segreto di attivazione o il campione biometrico – e qualsiasi dato biometrico derivato dal campione biometrico come una sonda prodotta attraverso l'elaborazione del segnale – DEVONO (SHALL) *essere azzerati immediatamente dopo che è stata generata una OTP.*

SINGLE-FACTOR CRYPTOGRAPHIC SOFTWARE

Un autenticatore crittografico software a fattore singolo è una chiave crittografica archiviata su disco o su un altro supporto "soft".

L'autenticazione è eseguita dimostrando il possesso e il controllo della chiave.

L'output dell'autenticatore dipende fortemente dal protocollo crittografico specifico, ma generalmente è un tipo di messaggio firmato.

*L'autenticatore crittografico software a fattore singolo è qualcosa "*CHE HAI*". (Vedi* MULTI-FACTOR AUTHENTICATION MFA*).*

Gli autenticatori crittografici software a fattore singolo incapsulano una o più chiavi segrete univoche per l'autenticatore.

La chiave DEVE (SHALL) *essere archiviata in un archivio adeguatamente sicuro e disponibile per l'applicazione di autenticazione (ad es. archivio chiavi,* TPM *- Trusted Platform Module -oppure* TEE *- Trusted Execution Environment -se disponibile).*

La chiave DEVE (SHALL) *essere fortemente protetta contro la divulgazione non autorizzata mediante l'uso di controlli di accesso che limitano l'accesso alla chiave solo ai componenti software sul dispositivo che richiedono l'accesso.*

Gli autenticatori software crittografici a fattore singolo DOVREBBERO (SHOULD) *scoraggiare e* DEVONO (SHALL) *facilitare la clonazione della chiave segreta su più dispositivi.*

SINGLE-FACTOR CRYPTOGRAPHIC DEVICES

Un dispositivo crittografico a fattore singolo è un dispositivo hardware che esegue operazioni crittografiche utilizzando chiavi crittografiche protette e fornisce l'output dell'autenticatore tramite connessione diretta all'endpoint utente.

Il dispositivo utilizza chiavi crittografiche simmetriche o asimmetriche incorporate e non richiede l'attivazione tramite un secondo fattore di autenticazione.

L'autenticazione è eseguita dimostrando il possesso del dispositivo tramite il protocollo di autenticazione.

L'output dell'autenticatore è fornito dalla connessione diretta all'endpoint utente ed è fortemente dipendente dal dispositivo e dal protocollo crittografici specifici, ma in genere è un tipo di messaggio firmato.

*Un dispositivo crittografico a fattore singolo è qualcosa "*CHE HAI*". (Vedi* MULTI-FACTOR AUTHENTICATION MFA*).*

SINGLE-FACTOR CRYPTOGRAPHIC DEVICE AUTHENTICATORS

Gli autenticatori di dispositivi crittografici a fattore singolo incapsulano una o più chiavi segrete univoche per il dispositivo e NON DEVONO (SHALL NOT) *essere esportabili (ovvero, non possono essere rimosse dal dispositivo).*

L'autenticatore opera firmando un CHALLENGE NONCE *presentato tramite un'interfaccia diretta del computer (ad esempio, una porta USB).*

In alternativa, l'autenticatore potrebbe essere un processore adeguatamente sicuro integrato con l'endpoint dell'utente stesso (ad esempio, un TPM hardware).

Sebbene i dispositivi crittografici contengano software, differiscono dagli autenticatori di software crittografico in quanto sono tutti incorporati il software è sotto il controllo del CSP o dell'emittente e che l'intero autenticatore è soggetto a tutti i requisiti FIPS 140 applicabili presso l'AAL in fase di autenticazione.

La chiave segreta e il suo algoritmo DEVONO (SHALL) *fornire almeno la lunghezza minima di sicurezza specificata nell'ultima revisione di SP 800-131A (112 bit alla data di questa pubblicazione).*

Il CHALLENGE NONCE DEVE (SHALL) *avere una lunghezza di almeno 64 bit.*

Gli autenticatori di dispositivi crittografici a fattore singolo DOVREBBERO (SHOULD) *richiedere un input fisico (ad esempio, la pressione di un pulsante) per funzionare.*

Ciò fornisce una difesa contro il funzionamento involontario del dispositivo, che potrebbe verificarsi se l'endpoint a cui è connesso viene compromesso.

SINGLE-FACTOR CRYPTOGRAPHIC DEVICE VERIFIERS

I verificatori di dispositivi crittografici a fattore singolo generano un CHALLENGE NONCE, *lo inviano all'autenticatore corrispondente e utilizzano l'output dell'autenticatore per verificare il possesso del dispositivo.*

L'output dell'autenticatore dipende fortemente dal dispositivo crittografico e dal protocollo, ma generalmente è un tipo di messaggio firmato.

Il verificatore dispone di chiavi crittografiche simmetriche o asimmetriche corrispondenti a ciascun autenticatore.

Mentre entrambi i tipi di chiavi DEVONO (SHALL) *essere protetti contro la modifica, le chiavi simmetriche* DEVONO (SHALL) *essere inoltre protette contro la divulgazione non autorizzata.*

Il CHALLENGE NONCE DEVE (SHALL) *avere una lunghezza di almeno 64 bit e* DEVE (SHALL) *essere unico per l'intero ciclo di vita dell'autenticatore oppure statisticamente univoco.*

L'operazione di verifica DEVE (SHALL) *utilizzare la crittografia approvata.*

MULTI-FACTOR CRYPTOGRAPHIC SOFTWARE

Un autenticatore crittografico software a più fattori è una chiave crittografica archiviata su disco o su un altro supporto "soft" che richiede l'attivazione tramite un secondo fattore di autenticazione.

L'autenticazione viene eseguita dimostrando il possesso e il controllo della chiave.

L'output dell'autenticatore dipende fortemente dal protocollo crittografico specifico, ma generalmente è un tipo di messaggio firmato.

L'autenticatore crittografico software a più fattori è qualcosa "CHE HAI" e DEVE *(*SHALL*) essere attivato da qualcosa "CHE CONOSCI" o qualcosa "CHE SEI".* (Vedi MULTI-FACTOR AUTHENTICATION MFA)

Gli autenticatori crittografici software a più fattori incapsulano una o più chiavi segrete univoche per l'autenticatore e accessibili solo attraverso l'input di un fattore aggiuntivo, un segreto memorizzato o una biometria.

La chiave DOVREBBE *(*SHOULD*) essere conservata in un luogo adeguatamente sicuro disponibile per l'applicazione di autenticazione (ad esempio, archiviazione portachiavi, TPM, TEE).*

La chiave DEVE *(*SHALL*) essere fortemente protetta contro la divulgazione non autorizzata mediante l'uso di controlli di accesso che limitano l'accesso alla chiave solo ai componenti software sul dispositivo che richiedono l'accesso.*

Gli autenticatori software crittografici a più fattori DOVREBBERO *(*SHOULD*) scoraggiare e* NON DEVONO *(*SHALL NOT*) facilitare la clonazione della chiave segreta su più dispositivi.*

Ogni operazione di autenticazione che utilizza l'autenticatore DEVE *(*SHALL*) richiedere l'input di entrambi i fattori.*

Qualsiasi segreto memorizzato utilizzato dall'autenticatore per l'attivazione DEVE *(*SHALL*) essere un valore numerico scelto casualmente di almeno 6 cifre decimali di lunghezza o un altro segreto memorizzato che soddisfi i requisiti indicati nel precedente capitolo "*MEMORIZED SECRETS*" e* DEVE *(*SHALL*) essere limitato in base alla frequenza come specificato nel capitolo "*RATE LIMITING (THROTTLING)*" descritto più avanti.*

Un fattore di attivazione biometrico DEVE *(*SHALL*) soddisfare i requisiti indicati nel capitolo "*USE OF BIOMETRIC*" descritto più avanti, compresi i limiti al numero di fallimenti di autenticazione consecutivi.*

La chiave non crittografata e il segreto di attivazione o il campione biometrico (compresi tutti i dati biometrici derivati dal campione biometrico come una sonda prodotta attraverso l'elaborazione del segnale) DEVONO *(*SHALL*) essere azzerati immediatamente dopo l'avvenuta transazione di autenticazione.*

*I requisiti di un verificatore di software crittografico a più fattori sono identici a quelli di un verificatore di dispositivi crittografici a fattore singolo, descritti nel precedente capitolo "*SINGLE-FACTOR CRYPTOGRAPHIC DEVICES*".*

La verifica dell'output da un autenticatore software crittografico a più fattori dimostra l'uso del fattore di attivazione.

MULTI-FACTOR CRYPTOGRAPHIC DEVICES

Un dispositivo crittografico a più fattori è un dispositivo hardware che esegue operazioni crittografiche che utilizzano una o più chiavi crittografiche protette e richiede l'attivazione tramite un secondo fattore di autenticazione.

L'autenticazione viene eseguita dimostrando il possesso del dispositivo e il controllo della chiave.

L'output dell'autenticatore è fornito dalla connessione diretta all'endpoint utente ed è fortemente dipendente dal dispositivo e dal protocollo crittografici specifici, ma in genere è un tipo di messaggio firmato.

Il dispositivo crittografico multifattoriale è qualcosa "CHE HAI" e DEVE (SHALL) essere attivato da qualcosa "CHE CONOSCI" o qualcosa "CHE SEI". (Vedi MULTI-FACTOR AUTHENTICATION MFA)

Gli autenticatori di dispositivi crittografici a più fattori utilizzano hardware a prova di manomissione per incapsulare una o più chiavi segrete uniche per l'autenticatore e accessibili solo attraverso l'immissione di un fattore aggiuntivo, un segreto memorizzato o un biometrico.

L'autenticatore opera utilizzando a chiave privata che è stata sbloccata dal fattore aggiuntivo per firmare una sfida nonce presentata tramite un'interfaccia diretta del computer (ad esempio, una porta USB).

In alternativa, l'autenticatore potrebbe essere un processore adeguatamente sicuro integrato con l'endpoint dell'utente stesso (ad esempio, un TPM hardware).

Sebbene i dispositivi crittografici contengano software, differiscono dal software crittografico autenticatori in quanto tutto il software incorporato è sotto il controllo del CSP o dell'emittente e che il l'intero autenticatore è soggetto a qualsiasi requisito FIPS 140 applicabile all'AAL selezionato.

La chiave segreta e il suo algoritmo DEVONO (SHALL) *fornire almeno la lunghezza minima di sicurezza specificata nell'ultima revisione di SP 800-131A (112 bit alla data di questa pubblicazione).*

Il CHALLENGE NONCE DEVE (SHALL) *avere una lunghezza di almeno 64 bit e* DEVE (SHALL) *essere utilizzata la crittografia approvata.*

Ogni operazione di autenticazione che utilizza l'autenticatore DOVREBBE (SHOULD) *richiedere l'input del fattore aggiuntivo.*

L'input del fattore aggiuntivo PUÒ (MAY) *essere effettuato tramite input diretto sul dispositivo o tramite una connessione hardware (ad es. USB, smartcard).*

Qualsiasi segreto memorizzato utilizzato dall'autenticatore per l'attivazione DEVE (SHALL) *essere scelto casualmente valore numerico di almeno 6 cifre decimali di lunghezza o altro segreto memorizzato che soddisfi i requisiti indicati nel precedente capitolo "*LOOK-UP SECRETS*" e* DEVE (SHALL) *essere limitato in base alla velocità come specificato nel capitolo "*RATE LIMITING (THROTTLING)*" descritto più avanti.*

Un fattore di attivazione biometrico DEVE (SHALL) *soddisfare i requisiti indicati nel capitolo "*USE OF BIOMETRIC*" descritto più avanti, compresi i limiti al numero di fallimenti di autenticazione consecutivi.*

La chiave non crittografata e il segreto di attivazione o il campione biometrico (compresi tutti i dati biometrici derivati dal campione biometrico come una sonda prodotta attraverso l'elaborazione del segnale) DEVONO (SHALL) *essere azzerati immediatamente dopo l'avvenuta transazione di autenticazione.*

*I requisiti per un verificatore di dispositivi crittografici a più fattori sono identici a quelli per un verificatore di dispositivi crittografici a fattore singolo, descritti nel precedente capitolo "*SINGLE-FACTOR CRYPTOGRAPHIC DEVICES*".*

La verifica dell'output dell'autenticatore da un dispositivo crittografico a più fattori dimostra l'uso del fattore di attivazione.

GENERAL AUTHENTICATOR REQUIREMENTS

Di seguito si descrivono i requisiti generali per gli autenticatori.

PHYSICAL AUTHENTICATORS

Il CSP DEVE *(*SHALL*) fornire agli interessati istruzioni su come proteggere adeguatamente l'autenticatore contro furto, comportamento o smarrimento.*

Inoltre, DEVE *(*SHALL*) fornire un meccanismo per revocare o sospendere l'autenticatore immediatamente dopo la notifica da parte dell'interessato che si sospetta la perdita o il furto dell'autenticatore.*

RATE LIMITING (THROTTLING)

Quando richiesto dalle descrizioni del tipo di autenticatore, il verificatore DEVE *(*SHALL*) implementare i controlli per proteggersi dagli attacchi di ipotesi online.*

Se non diversamente specificato nella descrizione di un dato autenticatore, il verificatore DEVE *(*SHALL*) limitare i tentativi di autenticazione falliti consecutivi su un singolo account a non più di 100.*

Tecniche aggiuntive POSSONO *(*MAY*) essere utilizzate per ridurre la probabilità che un utente malintenzionato blocchi il legittimo richiedente a causa della limitazione della velocità.*

Queste includono:

- *Richiedere al richiedente di completare il* CAPTCHA (COMPLETELY AUTOMATED PUBLIC TURING TEST TO TELL COMPUTER AND HUMANS APART) *prima di tentare l'autenticazione.*
- *Richiedere al richiedente di attendere in seguito a un tentativo fallito per un periodo di tempo che aumenta man mano che l'account si avvicina al limite massimo consentito per tentativi falliti consecutivi (ad esempio, da 30 secondi a un'ora).*
- *Accettare solo le richieste di autenticazione che provengono da una lista bianca di indirizzi IP da cui l'interessato è stato autenticato in precedenza con successo.*
- *Utilizzare altre tecniche di autenticazione basate sul rischio o adattive per identificare se il comportamento dell'utente rientra o non rientra nelle norme tipiche. Queste potrebbero, ad esempio, includere l'uso dell'indirizzo IP, la geolocalizzazione, i tempi dei modelli di richiesta o i metadati del browser.*

Quando l'interessato si autentica con successo, il verificatore DOVREBBE *(*SHOULD*) ignorare qualsiasi precedente tentativo fallito per quell'utente dallo stesso indirizzo IP.*

USE OF BIOMETRICS

*L'uso della biometria (qualcosa "*CHE SEI*") nell'autenticazione include sia la misurazione di caratteristiche fisiche (ad es. impronte digitali, iride, caratteristiche facciali) e caratteristiche comportamentali (ad es. cadenza di battitura).*

*Entrambe le classi sono considerate modalità biometriche, sebbene modalità diverse possano differire nella misura in cui stabiliscono l'intento di autenticazione come descritto nel capitolo "*AUTHENTICATION INTENT*" descritto più avanti.*

Di seguito alcune motivazioni per un uso limitato della biometria nella AUTENTICAZIONE.

1. *Il False Match Rate (FMR) biometrico non fornisce fiducia nell'autenticazione dell'interessato stesso. Inoltre, FMR non tiene conto degli attacchi di spoofing.*

2. *Il confronto biometrico è probabilistico, mentre gli altri fattori di autenticazione sono deterministici.*
3. *Gli schemi di protezione dei modelli biometrici forniscono un metodo per revocare le credenziali biometriche paragonabile ad altri fattori di autenticazione (ad esempio, certificati PKI e password).*
4. *Le caratteristiche biometriche non costituiscono segreti.*
   Possono essere ottenute online o tramite una foto di qualcuno con un telefono con fotocamera (ad es. immagini facciali) con o senza la loro consapevolezza, da oggetti toccati da qualcuno (ad es. impronte digitali latenti) o catturata con immagini ad alta risoluzione (ad es. modelli dell'iride).
   Sebbene le tecnologie di rilevamento degli attacchi di presentazione (PRESENTATION ATTACK DETECTION PAD) *(ad es. rilevamento della vitalità) possano mitigare il rischio di questi tipi di attacchi, è necessaria un'ulteriore fiducia nel sensore o nell'elaborazione biometrica per garantire che il PAD operi in conformità con le esigenze del CSP e dell'interessato.*

Per l'uso della biometria in combinazione con altre tecniche di autenticazione, vedi NIST SP 800-63B.

ATTESTATION

Un'attestazione è un'informazione trasmessa al verificatore in merito a una persona direttamente collegata all'autenticatore o all'endpoint coinvolto in un'operazione di autenticazione.

Le informazioni trasmesse dall'attestazione POSSONO *(*MAY*) includere anche:*

- *la provenienza (ad es. certificazione del produttore o del fornitore), la salute e l'integrità del autenticatore ed endpoint;*
- *funzionalità di sicurezza dell'autenticatore;*
- *caratteristiche di sicurezza e prestazioni dei sensori biometrici;*
- *modalità del sensore.*

Le informazioni di attestazione POSSONO *(*MAY*) essere utilizzate come parte della decisione di autenticazione basata sul rischio di un verificatore.*

VERIFIER IMPERSONATION RESISTANCE

*Gli attacchi di simulazione del verificatore, a volte indicati come "***ATTACCHI DI PHISHING***", sono tentativi da parte di verificatori e* RP *(*RELYING PARTY*) fraudolenti per ingannare un richiedente incauto inducendolo ad autenticarsi su un sito Web di impostori.*

Un protocollo di autenticazione resistente alla rappresentazione del verificatore DEVE *(*SHALL*) stabilire un canale protetto autenticato con il verificatore e* DEVE *(*SHALL*) legare in modo forte e irreversibile un identificatore di canale che è stato negoziato per stabilire il canale protetto autenticato all'output dell'autenticatore (ad esempio, firmando i due valori insieme utilizzando una chiave privata controllata dal richiedente la cui chiave pubblica è nota al verificatore).*

Il verificatore DEVE *(*SHALL*) convalidare la firma o altre informazioni utilizzate per dimostrare la resistenza al tentativo di simulazione del verificatore. Ciò impedisce all' impostore, anche se ha ottenuto un certificato che rappresenta il verificatore effettivo, di riprodurre tale autenticazione su un diverso canale protetto autenticato.*

Gli algoritmi crittografici approvati DEVONO *(*SHALL*) essere utilizzati per stabilire la resistenza alla rappresentazione del verificatore laddove richiesto.*

Le chiavi utilizzate a questo scopo DEVONO (SHALL) *fornire almeno il livello di sicurezza minimo specificato nell'ultima revisione di SP 800-131A (112 bit alla data di questa pubblicazione).*

Un esempio di protocollo di autenticazione resistente alla rappresentazione del verificatore è l'autenticazione del client TLS, perché il client firma l'output dell'autenticatore insieme ai messaggi precedenti dal protocollo univoco per la particolare connessione TLS negoziata.

Gli autenticatori che comportano l'inserimento manuale di un output dell'autenticatore, come gli autenticatori fuori banda e OTP, NON DEVONO (SHALL NOT) *essere considerati resistenti alla rappresentazione del verificatore perché l'immissione manuale non vincola l'output dell'autenticatore alla sessione specifica da autenticare.*

In un attacco MitM (Man in the Middle), *un verificatore impostore potrebbe riprodurre l'output dell'autenticatore OTP al verificatore e autenticarsi correttamente.*

VERIFIER-CSP COMMUNICATIONS

Nelle situazioni in cui il verificatore e il CSP sono entità separate (come mostrato dalla linea tratteggiata nella figura 4-1 (vedi NIST SP 800-63-3), le comunicazioni tra il verificatore e il CSP DEVONO (SHALL) *avvenire attraverso un canale sicuro autenticato reciprocamente (come un client - connessione TLS autenticata) utilizzando la crittografia approvata.*

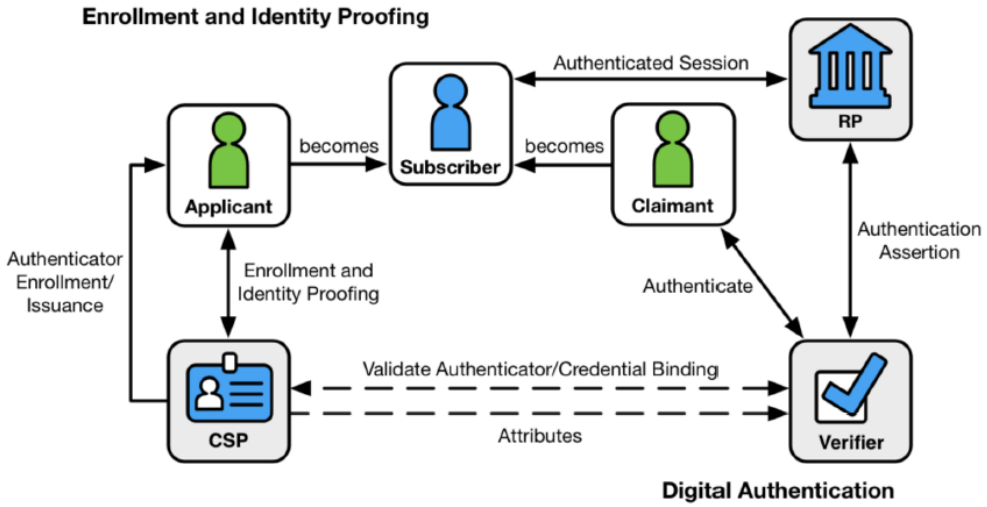

Figure 4-1 Digital Identity Model

VERIFIER-COMPROMISE RESISTANCE

L'utilizzo di alcuni tipi di autenticatori richiede che il verificatore memorizzi una copia del segreto dell'autenticatore. Ad esempio, un autenticatore OTP richiede che il verificatore generi in modo indipendente l'output dell'autenticatore per il confronto con il valore inviato dal richiedente.

A causa della possibilità che il verificatore venga compromesso e che i segreti archiviati vengano rubati, i protocolli di autenticazione, che non richiedono al verificatore di archiviare in modo permanente i segreti che potrebbero essere utilizzati per l'autenticazione, sono considerati più forti.

Un verificatore potrebbe essere compromesso in un modo diverso, ad esempio essere manipolato per accettare sempre un particolare output dell'autenticatore.

La resistenza alla compromissione del verificatore può essere ottenuta in diversi modi, ad esempio:

- *utilizzare un autenticatore crittografico che richieda al verificatore di memorizzare una chiave pubblica corrispondente a una chiave privata detenuta dall'autenticatore;*
- *memorizzare l'output previsto dell'autenticatore in forma hash.*

Per essere considerate resistenti alla compromissione del verificatore, le chiavi pubbliche memorizzate dal verificatore DEVONO *(*SHALL*) essere associate all'uso di algoritmi crittografici approvati e* DEVONO *(*SHALL*) fornire almeno il livello di sicurezza minimo specificato nell'ultima revisione di SP 800-131A (112 bit alla data di questa pubblicazione).*

REPLAY RESISTANCE

Un processo di autenticazione resiste agli attacchi di REPLAY *se è impraticabile ottenere con successo l'autenticazione registrando e riproducendo un precedente messaggio di autenticazione.*

La resistenza alla riproduzione si aggiunge alla natura resistente alla riproduzione dei protocolli del canale protetto autenticato, poiché l'output potrebbe essere rubato prima dell'ingresso nel canale protetto.

I protocolli che utilizzano NONCE *o* CHALLENGE *per dimostrare la "freschezza" della transazione sono resistenti agli attacchi di* REPLAY *poiché il verificatore rileverà facilmente quando i vecchi messaggi del protocollo sono riprodotti poiché non conterranno i* NONCE *appropriati o i dati sulla tempestività.*

Esempi di autenticatori resistenti alla riproduzione sono i dispositivi OTP, gli autenticatori crittografici e i segreti di ricerca. Al contrario, i segreti memorizzati non sono considerati resistenti alla riproduzione perché l'output dell'autenticatore, il segreto stesso, viene fornito per ogni autenticazione.

AUTHENTICATION INTENT

Un processo di autenticazione dimostra L'INTENTO *se richiede al soggetto di rispondere esplicitamente a ciascuna richiesta di autenticazione o riautenticazione.*

L'obiettivo dell'intento di autenticazione è di rendere più difficile l'uso degli autenticatori fisici collegati direttamente (ad es. dispositivi) all'insaputa del soggetto, ad esempio tramite malware sull'endpoint.

L'intento di autenticazione PUÒ *(*MAY*) essere stabilito in diversi modi:*

- *i processi di autenticazione che richiedono l'intervento del soggetto: ad esempio, un richiedente che inserisce un output di autenticazione da un dispositivo OTP;*
- *i dispositivi crittografici che richiedono l'azione dell'utente: ad esempio, la pressione di un pulsante.*

A seconda della modalità, la presentazione di una biometria può o meno stabilire l'autenticazione intento. La presentazione di un'impronta digitale normalmente stabilirebbe l'intento, mentre l'osservazione del volto del ricorrente utilizzando una fotocamera normalmente non lo sarebbe da sola. Allo stesso modo, è meno probabile che la biometria comportamentale stabilisca l'intento di autenticazione perché non sempre richiedono un'azione specifica da parte del richiedente.

RESTRICTED AUTHENTICATORS

L'uso di un autenticatore RESTRICTED *(Limitato) richiede che l'organizzazione attuatore valuti, comprenda e accetti i rischi associati a tale autenticatore e riconosca che il rischio probabilmente aumenti nel tempo.*

È responsabilità dell'organizzazione determinare il livello di rischio accettabile per i propri sistemi e dati associati e definire eventuali metodi per mitigare i rischi eccessivi.

Se in qualsiasi momento l'organizzazione determina che il rischio per qualsiasi parte è inaccettabile, allora tale autenticatore NON DOVRÀ (SHALL NOT) *essere utilizzato.*

Inoltre, il rischio di un errore di autenticazione è in genere sostenuto da più parti, tra cui l'organizzazione di attuazione, le organizzazioni che si affidano alla decisione di autenticazione e l'interessato.

Poiché l'interessato può essere esposto a rischi aggiuntivi quando un'organizzazione accetta un autenticatore RESTRICTED *e l'interessato può avere una comprensione e una capacità limitate di controllare tale rischio, il CSP* DEVE (SHALL):

1. *offrire agli interessati almeno un autenticatore alternativo che non sia* RESTRICTED *e può essere utilizzato per l'autenticazione all'AAL richiesto;*
2. *fornire un avviso significativo agli abbonati in merito ai rischi per la sicurezza dell'autenticatore* RESTRICTED *e alla disponibilità di alternative non* RESTRICTED;
3. *affrontare qualsiasi rischio aggiuntivo per gli interessati nella sua valutazione del rischio;*
4. *Sviluppare un piano di migrazione per garantire la possibilità che l'autenticatore* RESTRICTED *non sia più accettabile in futuro e includere questo piano di migrazione nella sua dichiarazione di accettazione dell'identità digitale.*

7. SESSION MANAGEMENT

Una volta che si è verificato un evento di autenticazione, è spesso desiderabile consentire all'interessato di continuare a utilizzare l'applicazione attraverso più interazioni successive senza richiedere loro di ripetere l'evento di autenticazione. Per facilitare questo comportamento, una sessione può essere avviata in risposta a un evento di autenticazione e continuare la sessione fino al momento in cui viene terminata.

SESSION BINDING

Si verifica una sessione tra un interessato, tramite browser, e l'RP o CSP a cui l'interessato sta accedendo (ovvero l'host della sessione).

Un segreto di sessione DEVE (SHALL) *essere condiviso tra i software dell'interessato e il servizio a cui si accede. Questo segreto lega le due estremità della sessione, consentendo all'interessato di continuare a utilizzare il servizio nel tempo.*

Il segreto DEVE (SHALL) *essere presentato direttamente dal software dell'interessato oppure il possesso del segreto* DEVE (SHALL) *essere dimostrato utilizzando un meccanismo crittografico.*

Il segreto utilizzato per il binding della sessione DOVREBBE (SHOULD) *essere generato dall'host della sessione in risposta diretta a un evento di autenticazione.*

Una sessione DOVREBBE (SHOULD) *ereditare le proprietà AAL dell'evento di autenticazione che ha attivato la sua creazione.*

Una sessione PUÒ (MAY) *essere considerata ad un AAL inferiore rispetto all'evento di autenticazione ma* NON DEVE (SHALL NOT) *essere considerata a un AAL superiore rispetto all'evento di autenticazione.*

I segreti utilizzati per l'associazione della sessione sono:

1. DEVE (SHALL) *essere generato dall'host di sessione durante un'interazione, in genere immediatamente dopo l'autenticazione;*
2. DEVE (SHALL) *essere generato da un generatore di bit casuale e contenere almeno 64 bit di entropia.*
3. DEVE (SHALL) *essere cancellato o invalidato dal soggetto della sessione quando l'interessato si disconnette.*
4. DOVREBBE (SHOULD) *essere cancellato sull'endpoint dell'interessato quando l'utente si disconnette o quando si ritiene che il segreto sia scaduto.*
5. NON DOVREBBE (SHOULD NOT) *essere collocato in posizioni non sicure come l'archiviazione locale HTML5 a causa della potenziale esposizione dell'archiviazione locale ad attacchi* **XSS (CROSS-SITE SCRIPTING)**.
6. DEVE (SHALL) *essere inviato e ricevuto dal dispositivo utilizzando un canale protetto autenticato.*
7. DEVE (SHALL) *scadere e non essere accettato dopo i tempi specificati e appropriato per l'AAL.*
8. NON DEVE (SHALL NOT) *essere disponibile per comunicazioni non sicure tra l'host e l'endpoint dell'interessato.*
   Le sessioni autenticate NON DEVONO (SHALL NOT) *ricorrere a un trasporto non sicuro, come da* **HTTPS** *a* **HTTP**, *dopo l'autenticazione.*

Gli URL o POST DEVE (SHALL) *contenere un identificatore di sessione che* DEVE (SHALL) *essere verificato dall'RP per assicurarsi che le azioni intraprese al di fuori della sessione non influiscano sulla sessione protetta.*

BROWSER COOKIES

I cookie del browser sono il meccanismo predominante mediante il quale sarà creata e tracciata una sessione per un interessato che accede a un servizio.

Il Cookie:

1. DEVE (SHALL) *essere contrassegnato per essere accessibile solo su sessioni sicure (HTTPS).*
2. DEVE (SHALL) *essere accessibile al minimo insieme pratico di nomi host e percorsi.*
3. DOVREBBE (SHOULD) *essere contrassegnato per essere inaccessibile tramite JavaScript (Http Only).*
4. DOVREBBE (SHOULD) *essere contrassegnato per scadere al, o subito dopo, il periodo di validità della sessione.*
   Questo requisito ha lo scopo di limitare l'accumulo di cookie, ma NON DEVE (SHALL NOT) *imporre timeout di sessione.*

REAUTHENTICATION

La continuità delle sessioni autenticate DEVE (SHALL) *essere basata sul possesso di un segreto di sessione rilasciato dal verificatore al momento dell'autenticazione ed eventualmente aggiornato durante la sessione.*

La natura di una sessione dipende dall'applicazione, tra cui:

1. *una sessione del browser web con un cookie di "sessione", oppure*
2. *un'istanza di un'applicazione mobile che conserva un segreto di sessione.*

I segreti di sessione DEVONO (SHALL) *essere non persistenti, cioè,* NON DEVONO (SHALL NOT) *essere mantenuti dopo un riavvio dell'applicazione associata o un riavvio del dispositivo host.*

La riautenticazione periodica delle sessioni DEVE (SHALL) *essere eseguita per confermare la presenza continua dell'interessato a una sessione autenticata (cioè, senza che l'interessato non si sia disconnesso).*

Prima della scadenza della sessione, il limite di tempo per la riautenticazione DEVE (SHALL) *essere esteso richiedendo all'interessato il/i fattore/i di autenticazione specificato nella Tabella 7-1.*

Quando una sessione è stata terminata, a causa di un timeout o di un'altra azione, all'utente DEVE (SHALL) *essere richiesto di stabilire una nuova sessione autenticandosi nuovamente.*

Nota: in AAL2, è richiesto un segreto memorizzato o biometrico, e non un autenticatore fisico, perché il segreto della sessione è qualcosa che "HAI" ed è necessario un fattore di autenticazione aggiuntivo per continuare la sessione.

Table 7-1 - AAL Reauthentication Requirements

AAL	Requirement
1	Presentation of any one factor
2	Presentation of a memorized secret or biometric
3	Presentation of all factors

8. THREATS AND SECURITY CONSIDERATIONS

Esistono due categorie generali di minacce al processo di registrazione: furto d'identità e compromissione o illecito del fornitore dell'infrastruttura.

Per motivi pratici, c si concentra sulle minacce di imitazione o furto d'identità, poiché le minacce all'infrastruttura sono affrontate dai tradizionali controlli di sicurezza.

Le minacce al processo di registrazione o presentazione dell'interessato al sistema includono attacchi di rappresentazione e minacce ai meccanismi di trasporto per la verifica dell'identità, l'associazione dell'autenticatore e il rilascio delle credenziali.

La Tabella 7-1 elenca le minacce relative alla registrazione e alla verifica dell'identità.

Table 7-1 Enrollment and Identity Proofing Threats

Activity	Threat/Attack	Example
Enrollment	Falsified identity proofing evidence	An applicant claims an incorrect identity by using a forged driver's license.
	Fraudulent use of another's identity	An applicant uses a passport associated with a different individual.
	Enrollment repudiation	A subscriber denies enrollment, claiming that they did not enroll with the CSP.

AUTHENTICATOR THREAT

Le minacce agli autenticatori possono essere classificate in base agli attacchi ai tipi di fattori di autenticazione che comprendono l'autenticatore.

TABLE 8-1 AUTHENTICATOR THREATS

Authenticator Threat/Attack	Description	Example
Assertion Manufacture or Modification	The attacker generates a false assertion	Compromised CSP asserts identity of a claimant who has not properly authenticated
	The attacker modifies an existing assertion	Compromised proxy that changes AAL of an authentication assertion
Theft	A physical authenticator is stolen by an Attacker.	A hardware cryptographic device is stolen.
		An OTP device is stolen.
		A look-up secret authenticator is stolen.
		A cell phone is stolen.

- *Qualcosa che "CONOSCI" potrebbe essere divulgato a un malintenzionato.*
  L'attaccante potrebbe indovinare un segreto memorizzato.
  Se l'autenticatore è un segreto condiviso, l'autore dell'attacco potrebbe ottenere l'accesso al CSP o al verificatore e ottenere il valore del segreto o eseguire un attacco del dizionario su un hash di tale valore.
  Un malintenzionato può osservare l'immissione di un PIN o di un codice di accesso, trovare una registrazione scritta o una voce di registro di un codice di accesso, un codice di accesso, installare del software malevolo (ad esempio, un registratore di tastiera) per acquisire il segreto.
  Inoltre, un utente malintenzionato può determinare il segreto tramite attacchi offline su un database di password gestito dal verificatore.
- *Qualcosa che "POSSIEDI" potrebbe essere perso, danneggiato, rubato al proprietario o clonato da un malintenzionato.*
  Ad esempio, un malintenzionato che ottiene l'accesso al computer del proprietario potrebbe copiare un autenticatore software.
  Un autenticatore hardware potrebbe essere rubato, manomesso o duplicato.
  I segreti Out-of-Band possono essere intercettati da un malintenzionato e utilizzati per autenticare la propria sessione.
- *Qualcosa che "SEI" potrebbe essere replicato.*
  Ad esempio, un utente malintenzionato può ottenere una copia del l'impronta digitale dell'interessato e costruire una replica.

Nella tabella seguente è elencata solo la parte iniziale delle minacce all'autenticatore per l'autenticazione digitale; la tabella completa è nel capitolo 8.1 del NIST SP 800-63B.

THREAT MITIGATION STRATEGIES

TABLE 7-1 ENROLLMENT AND IDENTITY PROOFING THREATS

La tabella 7-1 (vedi NIST SP 800-63A) elenca le strategie per mitigare le minacce al processo di iscrizione e rilascio.

Le minacce di registrazione possono essere scoraggiate rendendo più difficile la rappresentazione o aumentando la probabilità di rilevamento.

Questa raccomandazione riguarda principalmente i metodi per rendere più difficile la rappresentazione; tuttavia, prescrive alcuni metodi e procedure che possono aiutare a dimostrare chi ha perpetrato una rappresentazione.

Ad ogni livello, vengono impiegati metodi per determinare che esiste una persona con l'identità dichiarata, che il richiedente è la persona avente diritto all'identità dichiarata e che il richiedente non può in seguito ripudiare l'iscrizione.

Con l'aumentare del livello di sicurezza, i metodi impiegati forniscono una crescente resistenza all'imitazione casuale, sistematica e dall'interno.

Activity	Threat/Attack	Mitigation Strategy
Enrollment	Falsified identity proofing evidence	CSP validates physical security features of presented evidence.
		CSP validates personal details in the evidence with the issuer or other authoritative source.
	Fraudulent use of another's identity	CSP verifies identity evidence and biometric of applicant against information obtained from issuer or other authoritative source.
		Verify applicant-provided non-government-issued documentation (e.g., electricity bills in the name of the applicant with the current address of the applicant printed on the bill, or a credit card bill) to help achieve a higher level of confidence in the applicant's identity.
	Enrollment repudiation	CSP saves a subscriber's biometric.

TABLE 8-2 MITIGATING AUTHENTICATOR THREATS

I meccanismi correlati che aiutano a mitigare le minacce identificate sopra sono riassunti nella Tabella 8-2 qui accanto.

Nella tabella è elencata solo la parte iniziale delle azioni necessarie a mitigare le minacce; la tabella completa è nel capitolo 8.2 del NIST SP 800-63B.

Authenticator Threat/Attack	Threat Mitigation
Theft	Use multi-factor authenticators that need to be activated through a memorized secret or biometric.
	Use a combination of authenticators that includes a memorized secret or biometric.
Duplication	Use authenticators from which it is difficult to extract and duplicate long-term authentication secrets.
Eavesdropping	Ensure the security of the endpoint, especially with respect to freedom from malware such as key loggers, prior to use.
	Avoid use of non-trusted wireless networks as unencrypted secondary out-of-band authentication channels.

Diverse altre strategie possono essere applicate per mitigare le minacce descritte nella Tabella 8-1:

- *Molteplici fattori rendono più difficili da realizzare gli attacchi riusciti. Se un utente malintenzionato deve rubare un autenticatore crittografico e indovinare un segreto memorizzato, il lavoro per scoprire entrambi i fattori potrebbe essere troppo elevato.*
- *Possono essere impiegati meccanismi di sicurezza fisica per proteggere un autenticatore rubato dalla duplicazione. I meccanismi di sicurezza fisica possono fornire prove di manomissione, rilevamento e risposta.*
- *Richiedere l'uso di segreti memorizzati a lungo che non compaiono nei dizionari comuni può costringere gli aggressori a provare ogni possibile valore.*
- *È possibile utilizzare controlli di sicurezza del sistema e della rete per impedire a un utente malintenzionato di accedere a un sistema o installare software dannoso.*
- *La formazione periodica può essere eseguita per garantire che gli abbonati comprendano quando e come segnalare una compromissione – o sospetto di compromissione – o in altro modo riconoscere modelli di comportamento che potrebbero indicare che un utente malintenzionato sta tentando di compromettere il processo di autenticazione.*
- *È possibile utilizzare tecniche fuori banda per verificare la prova del possesso di dispositivi registrati (ad es. telefoni cellulari).*

9. RIFERIMENTI

1) NIST SP 800-63-3 – Implementation Resources
2) NIST SP 800-63A - Digital Identity Guidelines Enrollment and Identity Proofing
3) NIST SP 800-63B - Digital Identity Guidelines Authentication and Lifecycle Management
4) NIST SP 800-63C – Federation and Assertion