Framework per l'Autenticazione ISO/IEC 29115:2013

VINCENZO CALABRÒ

Indice

Standard per l'Autenticazione ISO/IEC 29115:2013

- Definizioni
- Obiettivi
- Level of Assurance
- Attori
- Fasi
- Minacce e controlli
- Conclusioni

Finalità

- L'adozione di una norma internazionale serve a realizzare numerosi servizi e soluzioni tecniche connessi alla sua applicazione, in linea con l'attuazione dell'Agenda digitale europea e italiana
- La norma è utilizzata in diversi provvedimenti, come riferimento per i livelli di garanzia dell'identificazione elettronica «*Regolamento europeo N. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno»*, e come riferimento per i livelli di garanzia nell'ambito del DPCM 24 ottobre 2014 «*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)*».

Standard per l’Autenticazione: ISO/IEC 29115

- È uno standard internazionale che fornisce un quadro di riferimento per gestire l'autenticazione di entità (umane e non) in un contesto determinato.
- In particolare, specifica quattro livelli di garanzia (LoA) relativi all'autenticazione delle entità e i criteri e linee guida per ottenere ciascuno dei quattro livelli.

Approfondimenti

1. Definizioni
2. Confronto con altri standard di autenticazione

Overview del Framework ISO29115

Technical			Management & Organizational
Enrolment phase	• Application and initiation • Identity proofing • Identity verification	• Record-keeping recording • Registration	• Service establishment • Legal and contractual compliance • Financial provisions • Information security management and audit • External service components • Operational infrastructure • Measuring operational capabilities
Credential management phase	• Credential creation • Credential pre-processing • Credential initialization • Credential binding • Credential issuance • Credential activation	• Credential storage • Credential suspension, revocation, and/or destruction • Credential renewal and/or replacement • Record-keeping	
Entity authentication phase	• Authentication • Record-keeping		

ISO/IEC 29115: obiettivi

Lo Standard ISO/IEC 29115:

- specifica 4 livelli di garanzia (LoA) utilizzabili per l'autenticazione delle entità.
- specifica i criteri e le linee guida per ottenere ciascuno dei quattro livelli di garanzia attinenti all'autenticazione dell'entità.
- fornisce una guida per la mappatura con altri schemi di garanzia dell'autenticazione rispetto ai quattro LoA.
- fornisce una guida per l'interscambio dei risultati di autenticazione basati sui quattro LoA.
- fornisce una guida sui controlli che si dovrebbero utilizzare per mitigare le minacce relative al processo di autenticazione.

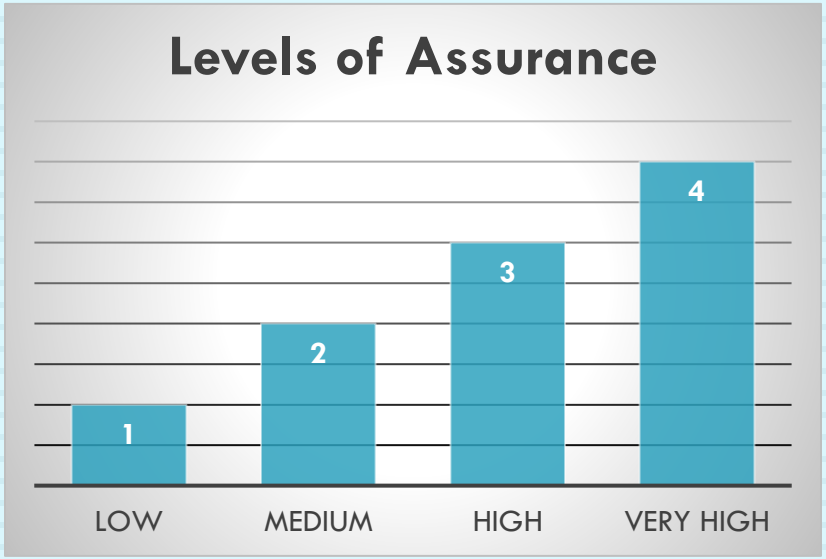
ISO/IEC 29115: Level of Assurance

Ogni LoA descrive un grado di fiducia del processo di autenticazione e fornisce la certezza che l'entità, che rivendica una determinata identità, sia realmente quella a cui è stata assegnata.

Il LoA 1 è il livello più basso di garanzia, mentre il LoA 4 è il livello più alto.

La scelta di quale sia il LoA appropriato in una determinata situazione dipende da molteplici fattori. Quello principale è legato al rischio: le conseguenze di un errore di autenticazione e/o l'uso improprio delle credenziali, il danno e l'impatto che possono derivare e la loro probabilità di accadimento.

Caveat



Level of assurance 1 (LoA1)

- Nel LoA1 è garantita una fiducia minima, in relazione all'identità asserita dall'entità, che aumenta nel caso di eventi di autenticazione consecutivi.
- Questo LoA è utilizzato quando il rischio di un'autenticazione errata è minimo.
- Non esiste un requisito specifico utilizzato per il meccanismo di autenticazione e non richiede l'uso di metodi crittografici.

Ad esempio il LoA1 può essere applicato per l'autenticazione nel caso in cui un'entità utilizza il nome utente o la password autoregistrati ad un sito Web oppure per le transazioni che coinvolgono siti Web che richiedono la registrazione per l'accesso a strumenti e documentazione, come le notizie o la documentazione dei prodotti. Anche un indirizzo MAC può soddisfare il requisito di autenticazione di un'entità-dispositivo.

Level of assurance 2 (LoA2)

- Nel LoA2 è assicurata una certa fiducia all'identità asserita dall'entità.
- Questo LoA è utilizzato quando il rischio di un'autenticazione errata è moderato.
- È accettata l'autenticazione a fattore singolo.
- L'autenticazione è corretta quando l'entità dimostra, attraverso un protocollo di autenticazione sicuro, che ha il controllo delle proprie credenziali. Devono essere previsti controlli per ridurre le intercettazioni e gli attacchi alle credenziali archiviate.

Ad esempio, un fornitore di servizi online potrebbe gestire un sito Web per consente ai propri clienti di modificare il proprio indirizzo (fisico o elettronico) di registrazione. La transazione in cui un beneficiario modifica l'indirizzo di registrazione può essere considerata una transazione di autenticazione LoA2. Questa transazione comporta un rischio moderato poiché le comunicazioni ufficiali vengono inviate all'indirizzo di registrazione del beneficiario, la transazione comporta inoltre un rischio moderato di rilascio non autorizzato di informazioni personali. Di conseguenza, il fornitore dovrebbe ottenere almeno una garanzia di autenticazione prima di consentire l'esecuzione di questa transazione.

Level of assurance 3 (LoA3)

- Nel LoA3 è garantita una fiducia alta sull'identità affermata dall'entità.
- Questo LoA è utilizzato laddove il rischio di un'autenticazione errata è sostanziale.
- Deve utilizzare l'autenticazione a più fattori.
- Le procedure di verifica dell'identità dipendono dalla verifica delle informazioni sull'identità. Qualsiasi informazione segreta scambiata dai protocolli di autenticazione deve essere protetta crittograficamente. Non ci sono requisiti sulla generazione o sull'archiviazione delle credenziali.

Ad esempio, una transazione in cui un soggetto invia elettronicamente informazioni riservate ad un altro può richiedere una autenticazione di LoA3. Una divulgazione impropria sarebbe sanzionabile.

Altri esempi di transazioni LoA3 includono l'accesso online ad un conto economico che consente il pagamento di competenze, l'approvazione da parte di un dirigente di un trasferimento di fondi dalla tesoreria di un'organizzazione (fino a un limite definito) o l'utilizzo da parte di un contraente di un sistema remoto per accedere alle informazioni personali dei clienti.

Level of assurance 4 (LoA4)

- Nel LoA4 è assicurata una fiducia altissima dell'identità affermata dall'entità.
- Questo LoA è utilizzato quando il rischio di un'autenticazione errata è elevato.
- Il LoA4 fornisce il massimo livello di garanzia di autenticazione dell'entità definito dallo Standard.
- Il LoA4 è simile al LoA3, aggiunge dei requisiti sul controllo in presenza dell'identità per le entità umane e l'uso di dispositivi hardware, a prova di manomissione, per l'archiviazione di tutte le chiavi crittografiche segrete o private. Tutte le informazioni personali e i dati sensibili inclusi nei protocolli di autenticazione devono essere protetti crittograficamente.

Ad esempio, la dispensazione di un farmaco può richiedere la protezione LoA4. Il farmacista deve avere la certezza che un medico qualificato ha prescritto il farmaco. Oppure, l'approvazione da parte di un dirigente di un significativo trasferimento di fondi di un'organizzazione può essere considerata una transazione LoA4.

Con LoA4 possono essere utilizzati i certificati digitali per autenticare un'Entità non-umana, quali laptop, telefoni cellulari, stampanti, fax e altri dispositivi collegati ad una rete. Ad esempio, il processo di registrazione di uno smartphone potrebbe richiedere l'implementazione dei certificati digitali sullo smartphone.

ISO/IEC 29115: attori

Gli attori coinvolti comprendono l'Entity, il Credential service provider (CSP), la Registration authority (RA), il Relying party (RP), il Verifier e il Trusted third party (TTP).

Questi attori possono appartenere ad un'unica organizzazione o ad organizzazioni separate.

- **Entità / Entity**

  Un'entità (umana o tecnologica) che può avere la sua identità autenticata.
  La capacità di autenticare un'entità dipende da una serie di fattori.
  Nel contesto di questo Framework, la capacità di autenticare un'entità implica che l'entità sia registrata, siano emesse le credenziali da un CSP e sia specificato il protocollo di autenticazione.
  Durante l'autenticazione, l'entità può far valere la propria identità.

- **Fornitore di servizi credenziali / Credential service provider**

  Un fornitore di servizi di credenziali (CSP) emette le credenziali e/o gestisce l'hardware, il software e i dati utilizzati per produrre credenziali.
  Un CSP può anche emettere e gestire i dati utilizzati per autenticare le credenziali.

ISO/IEC 29115: attori

- **Autorità di registrazione / Registration authority**

  L'autorità di registrazione (RA) stabilisce e/o verifica e garantisce l'identità di un'entità a un CSP.
  Il RA deve affidarsi al CSP per eseguire la fase di registrazione e gestire le entità in modo da consentirgli l'assegnazione delle credenziali.
  Ogni RA deve eseguire la verifica dell'identità secondo una procedura specifica. Ciò avviene in genere attraverso la valutazione delle informazioni sull'identità o la verifica dei record nei database.

- **Parte fiduciaria / Relying party**

  Un RP inoltra una richiesta o una conferma di identità. La parte può richiedere un'identità per vari scopi, come la gestione dell'account, il controllo degli accessi, la scelta di autorizzazione, ecc.

- **Verificatore / Verifier**

  Il verificatore conferma le informazioni sull'identità. Il verificatore può essere una parte fiduciaria o un'altra parte che funge da terza parte fidata nei confronti del PR.

- **Terza parte fidata / Trusted third party**

  Una terza parte fidata (TTP) è un'autorità considerata attendibile da altri attori in base alle attività legate alla sicurezza. Per questo Framework un TTP è considerato attendibile da un'entità e/o da un verificatore ai fini dell'autenticazione.

ISO/IEC 29115: fasi

Lo standard fornisce i requisiti e le linee guida per l'implementazione dei quattro LoA.

In particolare, fornisce i requisiti per l'implementazione dei processi delle seguenti fasi:

a) **Registrazione** (ad es. prova dell'identità, verifica dell'identità, registrazione)

b) **Gestione delle credenziali** (ad es. emissione ed attivazione delle credenziali)

c) **Autenticazione dell'entità**.

Il modello delle fasi e dei processi di autenticazione sono tecnologicamente neutrali.

Le organizzazioni che adottano questo framework stabiliscono politiche e procedure che forniscono il necessario supporto ai processi che soddisfano i requisiti stabiliti. Questi potranno variare a seconda del ruolo scelto da una particolare organizzazione come, ad esempio, dai contratti di servizio ai quali un'organizzazione fornisce le credenziali.

Fase 1: Registrazione

La fase di registrazione consta di quattro processi:

1. Richiesta e iniziazione;
2. Prova d'identità;
3. Verifica dell'identità;
4. Conservazione e tenuta dei registri.

Questi processi possono essere eseguiti interamente da una singola organizzazione, oppure possono consistere in una moltitudine di attività fornite da più organizzazioni, inclusi i componenti, i sistemi o i servizi condivisi o interagenti.

I processi richiesti devono differire in base ai requisiti chiesti dal LOA applicabile.

Nel caso di un'entità che si iscrive a LoA1, questi processi devono essere minimi (ad esempio, un individuo può fare clic su un pulsante "nuovo utente" su una pagina Web e creare un nome utente e una password). In altri casi, i processi di iscrizione possono essere estesi. Ad esempio, l'iscrizione a LoA4 richiede un incontro di persona tra l'entità e l'AR, nonché una prova dell'identità certificata.

Fase 2: Gestione delle credenziali

La fase di gestione delle credenziali comprende tutti i processi rilevanti per il ciclo di vita di una credenziale, o gli strumenti per generare credenziali, e consente all'utente di partecipare ad un'attività o un contesto.

La fase di gestione delle credenziali può comportare i seguenti processi:

- creazione delle credenziali,
- emissione delle credenziali o degli strumenti per produrre credenziali,
- attivazione delle credenziali o degli strumenti per produrre credenziali,
- memorizzazione delle credenziali,
- revoca e/o distruzione delle credenziali o degli strumenti per produrre credenziali,
- rinnovo e/o sostituzione delle credenziali o degli strumenti per produrre credenziali
- tenuta dei registri.

Alcuni di questi processi dipendono dal fatto che le credenziali siano trasferite su un device hardware.

Fase 3: Autenticazione dell’entità

Durante la fase di autenticazione dell'entità, quest’ultima utilizza le proprie credenziali per affermare la propria identità ad un RP (Relying party).

Il processo di autenticazione riguarda esclusivamente l'accertamento (o meno) della fiducia della richiesta di identità e non ha alcun rapporto o relazione con le azioni che dovrà intraprendere.

Considerazione gestionali e organizzative

Questo framework nasce non solo da fattori tecnici, ma anche da regolamenti, accordi contrattuali e considerazione su come deve essere gestita e organizzata la fornitura del servizio.

Una soluzione tecnicamente rigorosa, che non contempli gli aspetti gestionali e organizzativi, può intaccare il potenziale di sicurezza offerto dallo standard.

I criteri specifici e la valutazione della conformità per le considerazioni gestionali e organizzative non rientrano nel campo di applicazione della presente raccomandazione, ma dovrebbe essere forniti all'interno di un framework di fiducia.

Di seguito sono descritte le considerazioni organizzative e gestionali che riguardano questo standard.

Minacce e controlli: fase registrazione

Nelle tabelle sottostanti sono descritte le principali minacce che possono accadere durante le fasi di Registrazione, Gestione e Autenticazione e i controlli che possono essere attivati per la mitigazione e il monitoraggio delle stesse.

Minaccia	Descrizione	Controlli
Impersonation	Alcuni esempi di sostituzione di identità si verificano quando un'entità rivendica illegittimamente l'identità di un'altra entità utilizzando una patente di guida contraffatta o quando un dispositivo si registra in una rete utilizzando un indirizzo MAC contraffatto (Media Access Control).	• Identity Proofing Policy • Identity Proofing Local • Identity Proofing Authoritative Information

Minacce e controlli: fase gestione 1/5

Minaccia	Descrizione	Controlli
Credential Creation Unauthorized Creation	Un utente malintenzionato fa in modo tale che un CSP crei una credenziale basata su un'entità fittizia.	• Tracked Inventory
Credential Creation Tampering	Un utente malintenzionato modifica le informazioni mentre si passa dal processo di registrazione al processo di creazione delle credenziali.	• Appropriate Credential Creation • State Locked • Hardware Only
Credential Issuance Disclosure	Una password, creata dal CSP per un'entità, è copiata da un utente malintenzionato mentre è trasferita dal CSP all'entità durante la creazione delle credenziali.	• Appropriate Credential Issuance
Credential Activation In The Possession	Un utente malintenzionato ottiene una credenziale che non appartiene a lui e si maschera da entità legittima affinchè il CSP attivi la credenziale.	• Activated From Entity

Minacce e controlli: fase gestione 2/5

Minaccia	Descrizione	Controlli
Credential Activation Unavailability	L'entità associata a una credenziale non si trova nello stato normale e non è in grado di autenticare adeguatamente la propria identità al CSP. Inoltre, la consegna di una credenziale è ritardata e non è possibile attivarla entro il termine prescritto.	• Activated From Entity
Credential Storage Disclosure	Vengono prelevati nomi utente e password memorizzati in un file di sistema.	• Credential Secure Storage
Credential Storage Tampering	Il file che associa i nomi utente alle password è compromesso in modo da modificare il mapping e le password esistenti vengono sostituite con password note all'attaccante	• Credential Secure Storage
Credential Storage Duplication	Un utente malintenzionato utilizza le informazioni archiviate per creare una credenziale duplicata che può essere utilizzata da un'entità non intenzionale.	• Credential Secure Storage

Minacce e controlli: fase gestione 3/5

Minaccia	Descrizione	Controlli
Credential Storage Disclosure By Entity	L'entità memorizza una registrazione scritta del nome utente e della password in un luogo accessibile a terzi.	• Credential Secure Storage
Credential Revocation Delayed Revocation	Gli elenchi di revoca dei certificati non aggiornati consentono agli account (che avrebbero dovuto essere bloccati a seguito della revoca delle credenziali) di essere utilizzati da un utente malintenzionato.	• Credential Secure Revocation & Destruction
Credential Revocation Use After Decommissioning	Gli account utente non vengono eliminati quando i dipendenti lasciano un'azienda e ciò porta ad un possibile utilizzo 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.	• Credential Secure Revocation & Destruction

Minacce e controlli: fase gestione 4/5

Minaccia	Descrizione	Controlli
Credential Renewal Disclosure	La password rinnovata dal CSP per un'entità viene copiata da un utente malintenzionato mentre viene trasferita.	• Credential Secure Renewal
Credential Renewal Tampering	La nuova password creata da un'entità è modificata da un utente malintenzionato mentre viene inviata al CSP per sostituire una password scaduta.	• Credential Secure Renewal
Credential Renewal Unauthorized Renewal	L'attaccante inganna il CSP nell'emissione di una nuova credenziale per un'entità corrente e la nuova credenziale lega l'identità dell'entità corrente con una credenziale fornita dall'aggressore. L'attaccante è in grado di sfruttare il protocollo di rinnovo delle credenziali per estendere il periodo di validità delle credenziali per un'entità corrente.	• Credential Secure Renewal

Minacce e controlli: fase gestione 5/5

Minaccia	Descrizione	Controlli
Credential Management Recordkeeping Repudiation	Un'entità afferma che una credenziale legittima è fraudolenta o contiene informazioni errate al fine di negare erroneamente di aver utilizzato la credenziale.	• Record Retention
Credential Unauthorized Control	Le minacce non mitigate possono consentire che, un utente malintenzionato, acquisisca il controllo di una credenziale e si mascheri con l'entità per cui è stata effettivamente emessa la credenziale.	

Minacce e controlli: fase autentic. 1/3

Minaccia	Descrizione	Controlli
General	Le minacce sull'autenticazione comprendono molte categorie generiche. Esempio: i logger di battitura dei tasti, l'ingegneria sociale e gli errori degli utenti.	• Multi Factor Authentication
Online Guessing	Un utente malintenzionato esegue ripetuti tentativi di accesso indovinando i possibili valori della credenziale.	• Strong Password • Credential Lock Out • Default Account Use • Audit And Analyze
Offline Guessing	I segreti associati alla generazione delle credenziali sono esposti utilizzando metodi analitici al di fuori della transazione di autenticazione.	• Hashed Password With Salt
Credential Duplication	Le credenziali dell'entità o degli strumenti per generare credenziali sono state copiate illegittimamente. Un esempio potrebbe essere la copia non autorizzata di una chiave privata.	• Anti Counterfeiting

Minacce e controlli: fase autentic. 2/3

Minaccia	Descrizione	Controlli
Phishing	Un'entità è attratta ad interagire con un verificatore contraffatto e indotta a rivelare la propria password o dati personali sensibili che possono essere utilizzati per mascherarsi entità.	• Detect Phishing From Messages • Adopt Anti Phishing Practice • Mutual Authentication
Eavesdropping	Un utente malintenzionato capta la transazione di autenticazione per acquisire informazioni che possono essere utilizzate in un successivo attacco.	• No Transmit Password • Encrypted Authentication • Different Authentication Parameter
Replay Attack	Un utente malintenzionato è in grado di riprodurre i messaggi acquisiti in precedenza (tra un'entità legittima e un RP) per autenticarsi come tale entità.	• Different Authentication Parameter • Timestamp • PhysicalSecurity
Session Hijack	Un utente malintenzionato è in grado di inserirsi tra un'entità e un verificatore in seguito ad uno scambio di autenticazione riuscito tra le ultime due parti.	• EncryptedSession • Fix TCPIP Vulnerabilities • Cryptographic Mutual Handshake

Minacce e controlli: fase autentic. 3/3

Minaccia	Descrizione	Controlli
Man In The Middle	L'aggressore si posiziona tra l'entità e il RP in modo da poter intercettare e modificare il contenuto dei messaggi del protocollo di autenticazione.	• Mutual Authentication • Encrypted Session
Credential Theft	Un dispositivo che genera o contiene credenziali viene rubato da un utente malintenzionato.	• Credential Activation
Spoofing And Masquerading	Lo spoofing e il mascheramento si riferiscono a situazioni in cui un attaccante impersona un'altra entità al fine di consentire all'attaccante di compiere un'azione che altrimenti non sarebbe in grado di eseguire (ad esempio, ottenere l'accesso a un'attività altrimenti inaccessibile). Questo può essere fatto facendo uso delle credenziali di un'entità o ponendosi in altro modo come entità.	• Code Digital Signature • Liveness Detection

Conclusioni

- Lo standard fornisce un quadro di riferimento per gestire l'autenticazione di entità (umane e non) in determinati contesti.
- In particolare, specifica 4 livelli di garanzia (LoA) relativi all'autenticazione delle entità, i criteri e le linee guida per ottenere ciascuno dei 4 livelli.
- Le normative europee e nazionali hanno sviluppato altri modelli (eIDAS, SPID) che si ispirano alla stessa norma ISO 29155.
- È necessario trovare una sintesi tra i vari modelli affinché si possano sviluppare procedure di autenticazione universalmente accettate e si diffondano la identità digitali.

Approfondimento 1: Definizioni 1/3

Asserzione: dichiarazione rilasciata da un'entità senza comprovare la sua validità.
Autenticazione: prestazione di garanzia dell'identità dichiarata da un'entità.
Fattore di autenticazione: informazioni e processo utilizzati per autenticare o verificare l'identità di un'entità.
I fattori di autenticazione sono divisi in quattro categorie:

- qualcosa che un'entità ha (ad es. firma del dispositivo, passaporto, dispositivo hardware contenente una credenziale, chiave privata);
- qualcosa che un'entità conosce (ad es. password, PIN);
- qualcosa che un'entità è (ad esempio, caratteristica biometrica);
- qualcosa che un'entità tipicamente fa (ad esempio, modello di comportamento).

Protocollo di autenticazione: sequenza definita di messaggi tra un'entità e un verificatore che consente al verificatore di confermare l'identità dell'entità.
Fonte autorevole: repository riconosciuto come una fonte di informazione accurata e aggiornata.
Affermazione: dichiarare qualcosa, senza essere in grado di fornire prove.
Contesto: ambiente in cui le entità esistono e interagiscono.
Credenziale: insieme di dati presentati come prova di un'identità e/o diritti.
Fornitore di servizi credenziali: attore di fiducia che emette e/o gestisce le credenziali.

Approfondimento 1: Definizioni 2/3

Entità: qualcosa che ha un'esistenza separata e distinta e che può essere identificata in un contesto.
Assicurazione dell'autenticazione dell'entità: grado di fiducia raggiunto nel processo di autenticazione secondo il quale l'entità è ciò che afferma di essere o si prevede che sarà.
Identificatore: uno o più attributi che caratterizzano in modo univoco un'entità in un contesto specifico.
Identità: insieme di attributi relativi a un'entità.
Verifica di identità: processo mediante il quale la Registration Authority (RA) acquisisce e verifica informazioni. sufficienti per identificare un'entità a un livello di affidabilità specificato o compreso.
Attacco man-in-the-middle: attacco in cui un utente malintenzionato è in grado di leggere, inserire e modificare messaggi tra due parti a loro insaputa.
Autenticazione a più fattori: autenticazione con almeno due fattori di autenticazione indipendenti.
Autenticazione reciproca: autenticazione di identità delle entità che fornisce ad entrambe le garanzia dell'identità reciproca.
Non ripudio: capacità di proteggere la negazione da parte di una delle entità coinvolte in un'azione di aver partecipato a tutta o parte dell'azione.
Autorità di registrazione: attore di fiducia che stabilisce e/o verifica e garantisce l'identità di un'entità a un CSP.

Approfondimento 1: Definizioni 3/3

Ripudio: rifiuto da parte di un'entità di un evento o azione rivendicati.
Salt: valore non segreto, spesso casuale, utilizzato in un processo di hashing.
Segreto condiviso: segreto utilizzato nell'autenticazione noto solo all'entità e al verificatore.
Timestamp: parametro di variante temporale affidabile che indica un punto nel tempo rispetto a un riferimento comune.
Transazione: evento discreto tra un'entità e un fornitore di servizi che supporta uno scopo commerciale o programmatico.
Trust Framework: insieme di requisiti e meccanismi di applicazione per le parti che scambiano informazioni sull'identità.
Terzo affidato: autorità o un suo agente, affidato ad altri attori in relazione alle attività legate alla sicurezza.
Periodo di validità: periodo di tempo durante il quale un'identità può essere utilizzata in una o più transazioni.
Verifica: processo di controllo delle informazioni attraverso il confronto tra le informazioni fornite con le informazioni precedentemente confermate e il legame con l'entità.
Verificatore: attore che conferma le informazioni sull'identità.
Verificare: validazione delle informazioni attraverso il confronto delle informazioni fornite con le informazioni precedentemente confermate e il legame con l'entità.

Approfondimento 2: Confronto con altri standard

ISO/IEC 29115:2013 Framework per garantire l'autenticazione delle entità	**SPID (Legge 98 del 2013)** Sistema Pubblico di Identità Digitale	**eIDAS (Reg UE 910/2014)** Regolamento europeo per l'identificazione elettronica
LoA 1	---	---
LoA 2	Livello 1	Basso
LoA 3	Livello 2	Significativo
LoA 4	Livello 3	Elevato

Approfondimento:
Levels of assurance

Approfondimento

- Selezione del livello di affidabilità appropriato
- Mappatura LOA ed interoperabilità
- Scambio dei risultati di autenticazione basati sui 4 LoA

Approfondimento 3: Selezione del LoA appropriato

La selezione del LOA appropriato si basa sulla valutazione del rischio dei servizi per i quali le entità saranno autenticate.

La scelta di ciò che costituisce un rischio (basso, moderato, significativo o elevato) dipende dai criteri di rischio definiti dall'organizzazione che utilizza questo standard.

La valutazione del rischio di una transazione può essere condotta come parte della valutazione globale del rischio per la sicurezza delle informazioni dell'organizzazione (ad es. ISO / IEC 27001).

Potential impact of authentication errors	Level of assurance*			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Min	Mod	Sub	High
Financial loss or agency liability	Min	Mod	Sub	High
Harm to the entity, its programs, or public interests	N/A	Min	Mod	High
Unauthorized release of sensitive information	N/A	Mod	Sub	High
Personal safety	N/A	N/A	Min Mod	Sub High
Civil or criminal violations	N/A	Min	Sub	High
* Min=Minimum; Mod=Moderate; Sub=Substantial; High=High				

Approfondimento 4: Mappatura LOA ed interoperabilità

Domini diversi possono definire i LoA in modo diverso.
Ad esempio, un dominio può adottare un modello a 4 livelli e un altro dominio può adottare un modello a 5 livelli.

Per ottenere l'interoperabilità tra i diversi modelli di LoA, ogni dominio dovrebbe esplicitare in che modo il suo schema si riferisce ai LoA:

a) Sviluppare una metodologia ben definita di verifica dell'autenticazione dell'entità, comprese le categorie LOA;

b) Pubblicare questa metodologia in modo che le organizzazioni che desiderano stipulare accordi di tipo federativo possano comprendere chiaramente i processi e la terminologia.

La metodologia LoA deve tenere conto e definire:

a) Minacce attese;

b) Livelli di impatto (ovvero basso, medio, alto, molto alto) qualora le minacce diventassero realtà;

c) Individuazione delle minacce che devono essere controllate in ciascun LOA;

d) Tecnologie e processi di sicurezza raccomandati per l'uso nell'implementazione dei controlli in ciascun LOA;

e) Criteri per la determinazione dell'equivalenza di diverse combinazioni di fattori di autenticazione che tengano conto sia delle prove di identità che delle credenziali associate.

Approfondimento 5:
Scambio dei risultati di autenticazione

Gli attori che partecipano ad una transazione di autenticazione potrebbero dover scambiare informazioni per completare la transazione o l'attività stessa. La gamma di azioni include:

a) Consentire ad un Richiedente di esprimere i requisiti in cui un'entità dovrebbe essere autenticata;

b) Consentire ad un'entità di indicare il LOA effettivo nelle sue risposte;

c) Autorizzare un'entità a pubblicare i LOA per i quali sono stati certificati i requisiti associati a tale LOA.

Gli attori di un'autenticazione devono concordare il protocollo, la semantica, il formato e la struttura delle informazioni da scambiare. I requisiti tipici includono:

a) La necessità di specificare se accetterà qualsiasi risposta di autenticazione diversa da quella richiesta;

b) La necessità di specificare i requisiti per la protezione delle credenziali da parte delle entità.

Mentre i certificati digitali sono un modo consolidato per trasmettere informazioni sulla garanzia delle credenziali, i metadati sono sempre più utilizzati come metodo per comunicare i requisiti di garanzia delle parti.

Una classe di contesto, come una classe di autenticazione SAML (Security Assertion Markup Language) sotto forma di un URI, è un meccanismo ben noto per le parti per esprimere le classi relative alla garanzia di autenticazione nelle richieste di autenticazione e nelle asserzioni.

Approfondimento Fase 1: Registrazione

Approfondimento

- Richiesta e iniziazione
- Prova d'identità
- Verifica dell'identità
- Conservazione e tenuta dei registri
- Registrazione

Approfondimento 6: Richiesta e iniziazione

La fase di Registrazione può avvenire in diversi modi. Può essere avviata sulla base di una richiesta avanzata da un'entità che cerca di ottenere determinate credenziali, oppure è possibile che il processo venga avviato da una terza parte per conto dell'entità o dallo stesso CSP.

In ogni caso, il processo di iscrizione per gli esseri umani può comportare la compilazione di un modulo di registrazione. Questo modulo può richiedere informazioni sufficienti a garantire l'identificazione univoca dell'entità in un contesto in cui verrà emessa la credenziale.

Per le entità non umane, come ad esempio un dispositivo mobile, la registrazione può richiedere l'inizializzazione tramite la distribuzione delle credenziali sul dispositivo, ciò consentirebbe al dispositivo di essere identificato in maniera univoca e ricevere le impostazioni ad hoc tramite un profilo di configurazione crittografato.

I CSP stabiliscono i termini in base ai quali è fornita la registrazione e quali servizi devono essere utilizzati. Questi ultimi possono essere stabiliti in base ad un framework di fiducia.

Approfondimento 7: Prova d'identità

La prova di identità è il processo di acquisizione e verifica delle informazioni sufficienti ad identificare un'entità per un determinato livello di garanzia. A secondo del contesto, alcune informazioni relative all'identità possono provenire da fonti autorevoli e soddisfare i requisiti di prova dell'identità. Le informazioni sull'identità presentate per soddisfare i requisiti di prova dell'identità variano a seconda del contratto di servizio.
La prova può includere il controllo fisico dei documenti presentati per rilevare possibili frodi, manomissioni o contraffazioni. Il controllo dell'identità può includere il controllo che la stessa identità venga utilizzata in altri contesti. Più è alto il valore minimo richiesto, più saranno rigorosi i requisiti di prova dell'identità. Se il processo fosse avviato da remoto, i controlli saranno ancora più rigorosi.
La severità dei requisiti si basa sugli obiettivi che devono essere raggiunti per ciascun LOA.

Nel LoA1 l'obiettivo è garantire che l'identità sia unica nel contesto previsto. L'identità non deve essere associata a due entità diverse.

Nel LoA2 devono essere raggiunti due obiettivi: l'identità deve essere unica e l'entità a cui appartiene l'identità deve oggettivamente esistere. Ad esempio, la verifica dell'identità umana in LoA2 può includere il controllo dei registri delle nascite e delle morti per garantire una certa provenienza. Allo stesso modo, la verifica dell'identità presso LoA2 per non umani può includere la verifica del numero di serie presso il produttore del dispositivo.

LoA3 soddisfa gli obiettivi di LoA1 e LoA2, nonché l'esigenza di verificare le informazioni sull'identità attraverso una o più fonti autorevoli. Tuttavia, non vi è alcuna garanzia che le informazioni sull'identità siano in possesso del proprietario reale o legittimo dell'identità. Per gli esseri umani, LoA4 richiede alle entità di essere presenti di persona per proteggersi dallo scambio di persona.

I processi di prova di identità di un LOA superiore devono includere i processi dei LOA inferiori.

Approfondimento 8: Verifica dell'identità

È il processo di verifica delle informazioni che si concretizza attraverso il confronto delle informazioni fornite e confermate precedentemente dall'entità.

Sia il processo di prova dell'identità, che il processo di verifica, vengono eseguiti per raggiungere un alto livello di fiducia nell'identità di un'entità prima che questa sia registrata come entità particolare.

La verifica dell'identità differisce dalla prova dell'identità perché comporta la conferma delle informazioni sull'identità da fonti aggiuntive (interne o esterne).

Approfondimento 9: Conservazione e tenuta dei registri

È il processo che conclude la registrazione di un'entità.

Viene completata la registrazione della fase di iscrizione.

Il record deve includere le informazioni e la documentazione che sono state raccolte (e che possono essere memorizzate), le informazioni sul processo di verifica dell'identità, i risultati di questi passaggi e gli altri dati pertinenti.

Approfondimento 10: Registrazione

La registrazione è il processo attraverso il quale un'entità chiede di utilizzare un servizio o una risorsa.

Può essere eseguito durante o immediatamente dopo l'iscrizione, oppure in un secondo momento successivo alla fase di iscrizione.

È probabile che l’iscrizione sia necessaria una sola volta, mentre la registrazione può essere necessaria ogni qualvolta un'entità chiede l'accesso ad un servizio o ad una risorsa.

Approfondimento Fase 2: Gestione delle credenziali

Approfondimento

- Creazione delle credenziali
- Emissione delle credenziali
- Attivazione delle credenziali
- Memorizzazione delle credenziali
- Sospensione, revoca e/o distruzione delle credenziali
- Rinnovo e/o sostituzione delle credenziali
- Tenuta del registro

Approfondimento 11: Creazione delle credenziali

Il processo di creazione delle credenziali comprende tutti i processi necessari per creare per la prima volta una credenziale o gli strumenti per produrre una credenziale,.

Questi processi possono includere:, e.

- Preelaborazione: alcune credenziali richiedono una preelaborazione prima dell'emissione, come la personalizzazione. La personalizzazione può assumere molte forme diverse a seconda delle credenziali. Ad esempio, la personalizzazione di una smart card può comportare la stampa (all'esterno della scheda) o la scrittura (nel chip della scheda) del nome dell'entità a cui verrà consegnata la scheda.
- Inizializzazione: comprende tutti i passaggi che garantiscono che uno strumento per produrre una credenziale sia in grado di supportare le funzionalità richieste.
- Associazione: è il processo di associazione tra una credenziale o gli strumenti per produrre una credenziale e l'entità per la quale è stata emessa. Il legame e la fiducia nell'associazione con il LOA.

Approfondimento 12: Emissione delle credenziali

L'emissione delle credenziali è il processo di fornitura o di associazione di un'altra entità ad una particolare credenziale o strumento per produrre una credenziale.

La complessità di questo processo varia in base al LOA richiesto. Per i LoA più elevati può comportare la consegna di persona di un dispositivo hardware (ad es. una smart card) che detiene una credenziale. In caso di LOA inferiori il processo di emissione potrebbe essere più semplice come l'invio di una password o di un PIN all'indirizzo fisico o all'e-mail dell'entità.

I processi di emissione per i dispositivi con LoA più elevati in genere iniziano quando il produttore del dispositivo ordina i certificati digitali in blocco ad un provider di servizi di credenziali (CSP) associati ad un elenco di numeri di identificazione univoci dei dispositivi per ciascuno dei certificati digitali. Il CSP risponde fornendo i certificati e le chiavi private al produttore in un formato crittografato. Durante il processo di costruzione, il produttore può includere un certificato digitale in ciascun dispositivo, creando un identificatore univoco del dispositivo.

Approfondimento 13: Attivazione delle credenziali

L'attivazione delle credenziali è il processo mediante il quale una credenziale o uno strumento per produrre credenziali viene reso pronto all'uso.

Il processo di attivazione può comportare una varietà di misure a seconda delle credenziali. Ad esempio, una credenziale o uno strumento per produrre credenziali ,dopo la sua inizializzazione, potrebbe essere stato rilasciato "bloccato" fino al momento dell'emissione all'entità per evitare abusi. In questo caso, l'attivazione può comportare lo "sblocco" delle credenziali (ad esempio, con l'uso di una password). Una credenziale, o lo strumento per produrre credenziali, può essere attivato anche dopo una sospensione in cui la sua validità viene temporaneamente interrotta.

Approfondimento 14: Memorizzazione delle credenziali

L'archiviazione delle credenziali è il processo mediante il quale le credenziali o gli strumenti per la produzione delle credenziali vengono memorizzati in modo sicuro per proteggerne l'utilizzo non autorizzato. L'archiviazione delle credenziali interessa l'entità e le azioni necessarie per impedire l'uso non autorizzato di una credenziale.

L'archiviazione delle credenziali non include necessariamente la protezione delle informazioni utilizzate per verificare che una credenziale sia legittima.

La protezione delle informazioni, come le tabelle delle password in formato hash, è richiesta nei LoA superiori.

Approfondimento 15: Sospensione, revoca e/o distruzione

La revoca è il processo mediante il quale la validità di una credenziale è definitivamente terminata.

La sospensione è un processo correlato in base al quale la validità di una credenziale viene temporaneamente interrotta. La revoca può avvenire nei seguenti casi:

a) la credenziale è stata dichiarata persa, rubata o comunque compromessa;

b) la credenziale è scaduta;

c) I presupposti per la credenziale non ci sono più (ad esempio, quando un dipendente lascia il lavoro);

d) la credenziale è stata utilizzata per scopi non autorizzati;

e) è stata emessa una credenziale diversa per sostituire la credenziale in questione.

Il periodo che passa tra l'avviso di un evento, la richiesta e il completamento del processo di revoca è determinato dalla politica organizzativa. In caso di LOA più elevati il periodo di tempo consentito per la revoca è generalmente più breve. Alcune credenziali, come quelle contenute nelle smart card, possono essere fisicamente distrutte in caso di revoca.

Approfondimento 16:
Rinnovo e/o sostituzione delle credenziali

Il rinnovo è il processo con cui viene prolungata la durata di una credenziale esistente.

La sostituzione è il processo mediante il quale un'entità riceve una nuova credenziale, o uno strumento per produrre una credenziale, per rimpiazzare una credenziale precedentemente revocata.

Un esempio di credenziale sostitutiva è quando un CSP invia una password temporanea all'indirizzo e-mail dell'entità che consente all'entità di creare una nuova password dopo aver fornito la password temporanea. La rigorosità dei processi di rinnovo e sostituzione delle credenziali varia in base al LOA.

Approfondimento 17: Tenuta del registro

Le registrazioni devono essere conservate per tutto il ciclo di vita di una credenziale.

I registri devono essere conservati per documentare almeno le seguenti informazioni:

a) il fatto che sia stata creata una credenziale;

b) l'identificatore della credenziale (ove applicabile);

c) l'entità alla quale è stata emessa la credenziale (ove applicabile);

d) lo stato della credenziale (ove applicabile).

I registri devono essere conservati per ogni processo (applicabile) coinvolto nella fase di gestione delle credenziali.

Laddove le credenziali sono rilasciate a soggetti umani, è probabile che la tenuta di registri comporti l'elaborazione di informazioni personali.

Approfondimento Fase 3: Autenticazione dell’entità

Approfondimento

- Autenticazione
- Tenuta del registro

Approfondimento 18: Autenticazione

Il processo di autenticazione prevede l'uso di un protocollo che consente di dimostrare il possesso e/o il controllo di una credenziale al fine di stabilire la fiducia del possesso di una determinata identità.

I requisiti del protocollo di autenticazione variano a seconda del LOA definito.

Ad esempio, per un LOA inferiore l'autenticazione può comportare l'uso di una password. In un LoA superiore l'autenticazione può comportare l'utilizzo di un protocollo challenge-response basato sulla crittografia.

Nei LOA più elevati può essere richiesta l'autenticazione a più fattori perché non tutti i fattori di autenticazione forniscono la stessa affidabilità e, pertanto, vengono utilizzati più fattori per aumentare la sicurezza.

Approfondimento 19: Tenuta del registro

Il monitoraggio e la tenuta dei registri degli eventi della fase di autenticazione possono essere necessari per una varietà di scopi, quali la fornitura dei servizi, la conformità ad altri standard, la verifica della responsabilità e/o dei requisiti legali.

Per quanto riguarda le entità umane le informazioni contenute in questi registri possono includere informazioni sensibili. Pertanto, devono essere gestiti in modo tale che si tenga conto della necessità di protezione dei dati e di limitare le informazioni personali contenute.

Approfondimento sulle Considerazione gestionali e organizzative

Approfondimento

- Istituzione dei servizi
- Conformità legale e contrattuale
- Disponibilità finanziaria
- Gestione e controllo della sicurezza delle informazioni
- Componenti di servizio esterni
- Infrastruttura operativa
- Misurare la capacità operativa

Approfondimento 20: Istituzione dei servizi

L’istituzione dei servizi si rivolge sia allo status giuridico del fornitore di servizi, che allo stato della fornitura dei servizi. Ad esempio, sapere che il fornitore dei servizi di gestione e di autenticazione dell'identità è un'entità legalmente registrata dà la certezza che il CSP è un'impresa riconosciuta nella giurisdizione in cui opera. Ciò diventa significativo quando i componenti del servizio sono gestiti da persone giuridiche diverse.

Sebbene i requisiti di base siano gli stessi per tutti i LOA, quelli più elevati dovrebbero avere una maggiore attenzione al fatto che la prestazione del servizio sia completa e affidabile. Ad esempio, nel LoA3 e superiore, si dovrebbe richiedere la conoscenza dei suoi legami aziendali e la comprensione del livello di indipendenza.

Approfondimento 21: Conformità legale e contrattuale

Tutti gli attori devono comprendere e rispettare i requisiti legali previsti dalla normative vigenti in relazione al funzionamento e alla fornitura del servizio.

Ciò ha implicazioni sui tipi di informazioni che possono essere cercate, il modo in cui viene condotta la prova dell'identità e quali informazioni possono essere memorizzate.

Il trattamento dei data personali è uno di questi aspetti.

È necessario tenere conto di tutte le giurisdizioni in cui operano gli attori.

Nel LoA2 e superiori, dovrebbero essere identificati anche i requisiti di policy e contrattuali.

Approfondimento 22: Disponibilità finanziaria

Nel caso in cui è necessario offrire il servizio a lungo termine deve essere dimostrata la stabilità finanziaria, in modo tale che questa sia sufficiente a garantire il proseguimento dell'attività del servizio ed a sottoscrivere il grado di esposizione di responsabilità.

Per i servizi e l'affidabilità del LoA1 è improbabile che tali disposizioni vengano prese in considerazione, mentre per i servizi che supportano transazioni più significative, in LoA2 e superiori, dovrebbero rispondere a tali esigenze.

Approfondimento 23:
Gestione e controllo della sicurezza inf.

Nel LoA2 e versioni superiori, gli attori dovrebbero disporre di protocolli sulla gestione della sicurezza delle informazioni, di politiche, di approcci alla gestione dei rischi e gli altri controlli riconosciuti, in modo da garantire che esistano misure efficaci. Per il LoA3 e versioni superiore, è necessario utilizzare un sistema formale di gestione della sicurezza delle informazioni (ad es. ISO/IEC serie 27000).

In base agli accordi di conformità legale, contrattuale e tecnica, gli attori dovrebbero garantire che le parti rispettino gli impegni e possano fornire una tutela nel caso in cui non siano rispettate.

In LoA2 e versioni superiori, questa garanzia dovrebbe essere supportata dai controlli di sicurezza, sia interni che esterni, e dalla conservazione sicura delle registrazioni degli eventi significativi. A tal fine può essere utilizzato un controllo per verificare se le pratiche delle parti siano in linea con quanto concordato.

Approfondimento 24: Componenti di servizio esterni

Quando un'organizzazione dipende da organizzazioni terze per alcune parti del suo servizio, il modo in cui coordina le azioni di tali parti e le attività di supervisione contribuiranno a garantire la sicurezza globale della prestazione del servizio.

La natura e l'estensione delle disposizioni dovrebbero essere proporzionali al LoA richiesto e al sistema di gestione della sicurezza delle informazioni applicato.

In LoA1 tale garanzia dovrebbe avere un effetto minimo, ma da LoA2 in poi queste misure contribuiscono alla qualità complessiva della fornita.

Approfondimento 25: Infrastruttura operativa

Per abilitare le reti di fiducia su larga scala è possibile utilizzare un framework di fiducia.

In questo contesto gli attori supportano il flusso di informazioni tra entità, fornitori di servizi di identità (ad es. RA, CSP) e RP.

Questi attori aggiuntivi possono essere chiamati a garantire che tutte le parti rispettino gli impegni e possano fornire una via legale nel caso in cui si verificasse un disservizio.

Approfondimento 26: Misurare la capacità operativa

I responsabili delle policy stabiliscono i requisiti tecnici e contrattuali per i framework di fiducia.

Questi dovrebbero includere, ad esempio, i livelli di versione del prodotto, la configurazione del sistema, le impostazioni e i protocolli, mentre i requisiti contrattuali potrebbero essere orientati verso pratiche di informazione corrette.

Quando si stabiliscono questi requisiti, i responsabili delle policy dovrebbero includere dei criteri in base ai quali misurare le potenziali entità del framework di fiducia.

Anziché sviluppare gli stessi criteri, potrebbero rifarsi a criteri standard che altri esperti hanno già elaborato. Se i responsabili di policy utilizzassero i criteri standard in diversi framework, sarà più facile comprendere e applicare i criteri in modo coerente.

Grazie!
Domande?

VINCENZOCALABRO.IT