Normativa di riferimento

UNI CEN ISO/IEC 17000:2005

UNI CEN ISO/IEC 17025:2005

ISO/IEC 27000 - serie

ISO/IEC 29115 Entity Authentication Assurance Framework

ISO/IEC 24760 Framework for Identity Management

ISO/IEC 29100 Privacy Framework

ISO/IEC 29101 Privacy Reference Architecture

NIST 800-63-2 Electronic Authentication Guideline

FICAM Trust Framework Provider Adoption Process (TFPAP) version 2.02

FIPS 140-2 → Common Criteria EAL

Dlgs n. 82 del 7 marzo 2005 e smi

DPCM 24 ottobre 2014 pubblicato su GU n. 285 del 9 dicembre 2014

Dlgs n. 196 del 30 giugno 2003 e smi

Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014

Regolamento (bozza per il garante Privacy) per modalità attuative SPID

Definizioni (ad integrazione Regolamento per modalità attuative SPID)

Asserzione: una dichiarazione dall'IdP al SP che contiene informazioni (anche attributi associati) relative ad una identità digitale.

Aggressore: una parte che agisce allo scopo di provocare un danno (ed eventualmente ricavarne un profitto)

Cookie: stringhe di caratteri, poste nella memoria del browser, che sono disponibili ai siti web all'interno dello stesso dominio Internet per eseguire autenticazioni automatiche, tracciatura di sessioni e memorizzazione di informazioni .

Entropia: una misura della quantità di incertezza che un aggressore deve affrontare per dedurre il valore di un segreto.

Man in the Middle Attack: un attacco sul protocollo di autenticazione nel quale l'aggressore si pone tra il richiedente e l'IdP in modo da poter intercettare ed alterare i dati che transitano.

Nonce: un valore usato nei protocolli di sicurezza che non è mai ripetuto con la stessa chiave.

Personal Identifiable Information (PII): qualsiasi informazione relative ad un individuo che possono essere usate per distinguerlo o tracciarlo come ad es. nome, codice fiscale, data e luogo di nascita, nome della madre da nubile, dati biometrici o qualsiasi altra informazione che può essere associata ad un individuo come ad es. informazioni scolastiche, lavorative, finanziarie, mediche ecc.

Pharming: un attacco in cui l'aggressore si infiltra in un servizio infrastrutturale come ad esempio il DNS (Domain Name Service) causando l'indirizzamento verso IdP contraffatti.

Phising: un attacco in cui il richiedente viene indotto (normalmente attraverso una e-mail) ad interagire con un IdP o SP contraffatto in modo da fornire informazioni utili a mascherare l'aggressore come legittimo richiedente al vero IdP.

Salt: un valore non segreto che è usato in un processo crittografico allo scopo di assicurare che il risultato di un calcolo per una istanza non può essere riusato dall'aggressore.

Spoofing: nel contesto della sicurezza di rete, un attaco spoofing è una situazione in cui un aggressore (persona o programma) maschera un altro falsificandone i dati.

Token: qualcosa che il richiedente possiede e controlla (un modulo crittografico o una password) e che viene usato nel processo di autenticazione.

Premessa

Lo scopo del presente documento consiste nell'indicazione di uno schema, ovvero regole e controlli che potrebbero essere adottati per la corretta valutazione di conformità dei processi e delle soluzioni tecnologiche per la fase di gestione delle credenziali e per la fase di autenticazione, ai fini del rilascio dell'attestazione di conformità ai livelli di sicurezza SPID 1, 2 e 3 (corrispondenti ai LoA, level of assurance, 2, 3 e 4 della norma ISO/IEC 29115).

Controlli generali

Si suggerisce che i gestori delle identità digitali SPID (IdP) siano in possesso/abbiano attivato procedura, per questa particolare tipologia di servizio, della certificazione ISO/IEC 27001:2013 emessa da Enti Certificatori indipendenti e riconosciuti (v. IAF e Accredia) a seguito del completamente con esito positivo di un formale processo di audit.

I responsabili della sicurezza IdP dovranno quindi realizzare (e mantenere) un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI, nella letteratura tecnica Information Security Management Systems - ISMS) basandosi sulle migliori pratiche indicate dalla ISO/IEC 27002:2013 allo scopo di garantire la triade C-I-A ovvero la confidenzialità (assicurando che l'informazione sia accessibile solo a chi è stato autorizzato), integrità (salvaguardando la completezza e l'accuratezza delle informazioni e dei metodi di elaborazione) e disponibilità (consentendo l'accesso agli utenti autorizzati alle informazioni e risorse associate quando richiesto).

In sintesi i controlli generali saranno effettuati in un dominio composto dalle seguenti 14 aree:

1. Procedure e Politiche di sicurezza
2. Organizzazione
3. Risorse Umane
4. Gestione beni/risorse
5. Controllo accessi
6. Crittografia
7. Sicurezza fisica e ambientale
8. Sicurezza operativa
9. Sicurezza delle comunicazioni

10. Acquisizione, sviluppo e manutenzione dei sistemi
11. Relazioni con i fornitori
12. Gestione degli incidenti di sicurezza
13. Business Continuity
14. Conformità (sia ai requisiti interni che a quelli esterni, norme e legislazione corrente).

Dal punto di vista strettamente operativo, deve essere prestata particolare attenzione alle infrastrutture tecnologiche adottate, alle componenti esterne del sistema ed alla misurazione continua della capacità operativa allo scopo di garantire prestazioni, disponibilità e scalabilità.

Pratiche di sicurezza, privacy e interoperabilità

Possono essere considerati (rif. FICAM Trust Framework Solutions v. 2.02.2) sette livelli di fiducia/trust:

a. registrazione ed emissione: relativa a come l'IdP registra e prova l'identità del soggetto richiedente ed a come invia/consegna le credenziali al soggetto validato.

b. tecnologia dei token, in pratica a come la tecnologia resiste a frodi, manomissioni, furti o altri attacchi.

c. gestione delle credenziali, come l'IdP gestisce e protegge, durante il ciclo di vita completo, le credenziali e token associati

d. processo di autenticazione, quanto è sicuro il processo di autenticazione adottato dall'IdP

e. asserzioni, come l'IdP protegge le asserzioni, se usate, e quanta informazione è fornita nell'asserzione.

f. verifiche e controlli continui, quali controlli addizionali sono effettuati dall'IdP allo scopo di assicurare un controllo continuo dell'identità digitale e dell'uso corretto delle credenziali

g. privacy, assicurare che le politiche sulla privacy adottate dall'IdP siano in linea con la normativa vigente, la regolamentazione europea, le raccomandazioni e quanto definito dal Garante privacy in Italia.

Il caso a. è da considerarsi fuori ambito per gli scopi di questo documento.

Nei paragrafi che seguono sarà fornita una schematizzazione, regole e controlli da applicare alla tecnologia, alla gestione delle credenziali, al processo di autenticazione, ai controlli continui, alle asserzioni ed alla privacy (si noti esplicitamente che questi ultimi due punti sono stati inseriti per completezza ma potrebbero essere, in parte, fuori ambito dagli obiettivi di certificazione delle soluzioni tecnologiche).

Tecnologia token

Le potenziali minacce associate all'utilizzo di token sono:

- Furto (ad es. è stato rubato lo smartphone, un dispositivo OTP ecc.)
- Scoperta (ad es. domande banali, del tipo liceo frequentato facilmente rilevabili su siti web sociali)
- Duplicazione (password scritte su "pizzini" o su file elettronici)
- Osservare di nascosto (software tipo keylogger o semplicemente osservando)
- Offline cracking (uso di metodologie analitiche per estrarre chiavi da informazioni disponibili o intercettate)
- Phising
- Pharming
- Social Engineering: (ad es. convincere il legittimo proprietario dell'identità digitale a rilevare credenziali o segreti associati)
- Provare ad indovinare (ad es. basati su dizionari)

Per mitigare queste minacce devono essere previsti:

a. meccanismi di sicurezza fisica
b. rigorosi controlli di sicurezza logica per la rete ed i sistemi
c. addestramento periodico (per gli addetti ai lavori e per gli utilizzatori)

Inoltre l'imposizione di regole di complessità, l'adozione di tecniche multi-fattore e fuori banda possono ridurre sensibilmente i rischi associati alle minacce sopra elencate.

A titolo esemplificativo, e non esaustivo, dipendentemente dalla tipologia di token utilizzati devono essere applicate le seguenti tecniche.

Numero minimo di bit di entropia in funzione del tipo di token (ad es. almeno 20 bit per token conoscenza pre-registrata e 64 bit per token con look-up secret)

Meccanismi di limitazione (throttling) sul numero di tentativi di autenticazione.

Per token out of band, su un canale separato dal canale primario usato per l'autenticazione elettronica e almeno 64 bit di entropia (ridotti a 20 se l'IdP adotta meccanismi di limitazione sul numero massimo consentito di tentativi di autenticazione).

Per token a fattore singolo con dispositivi OTP (one-time password):

- il token deve utilizzare un meccanismo di cifratura o funzione hash approvata in modo da combinare la chiave simmetrica memorizzata sul dispositivo con un valore che non sarà mai ripetuto con la stessa chiave (nonce) in modo da generare una password OTP
- la password OTP deve avere una durata veramente limitata, nell'ordine di qualche minuto
- si propone che il modulo crittografico che esegue le funzioni di verifica sia validato almeno a livello EAL 2+ (o superiore al livello 1 del FIPS 140-2)

Per i dispositivi crittografici a fattore singolo:

anche in questo caso si suggerisce che il modulo crittografico sia validato almeno a livello EAL 2+ (o superiore al livello 1 del FIPS 140-2) e devono essere previsti almeno 64 bit di entropia per il nonce o per challenge basato su valori casuali.

Con uno schema di autenticazione multi-token , il livello di sicurezza SPID può essere determinato in analogia con quanto indicato nella tabella A riportata alla pagina successiva (rif. tabella 7 Assurance Levels for Multi-Token E-Authentication Schemes del documento NIST 800-63-2).

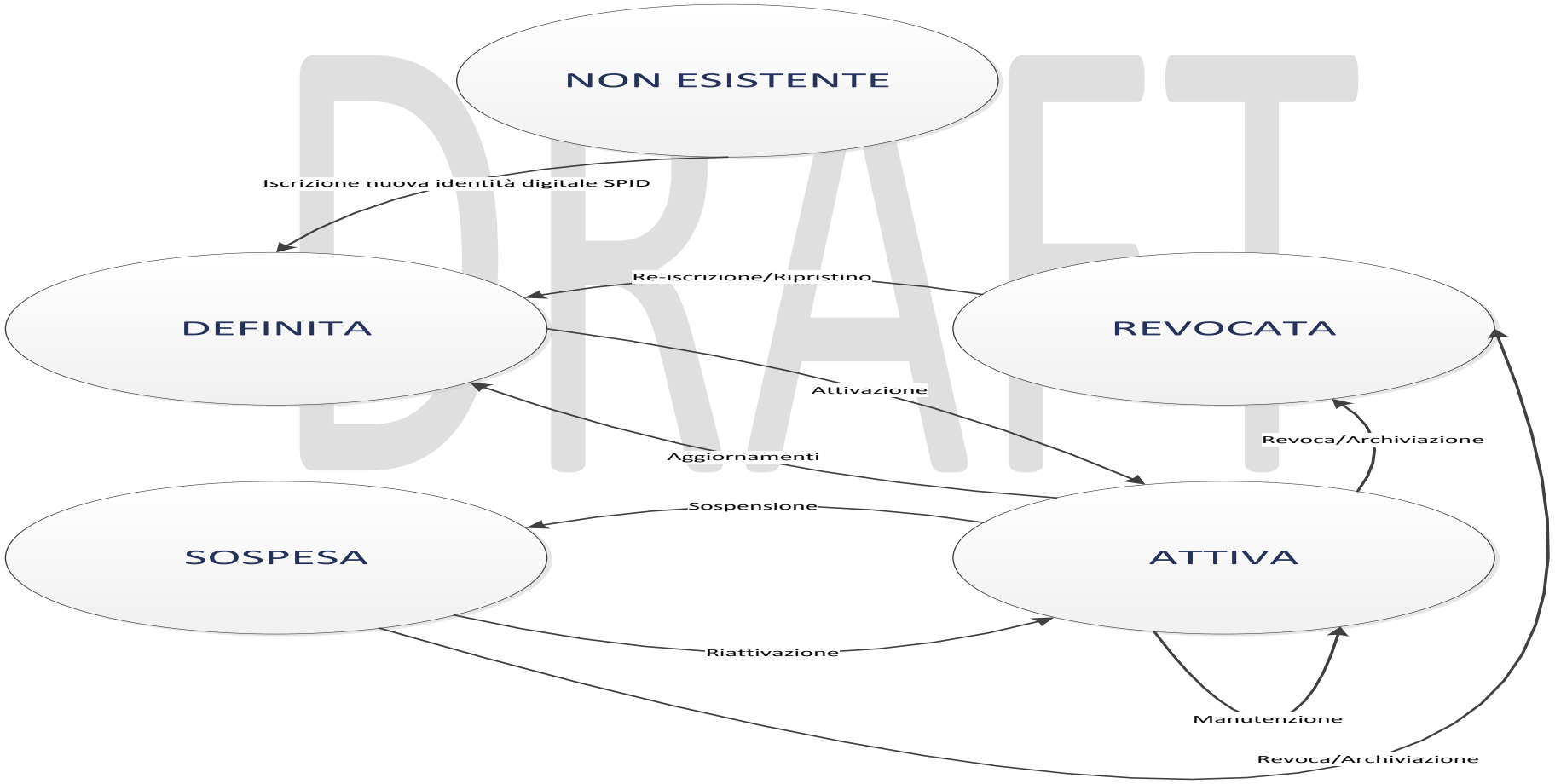
	Token con segreto memorizzato	Token con conoscenza pre-registrata	Token con tabella dei codici/segreti	Token out of band	Dispositivo a singolo fattore (SF) del tipo One-Time Password (OTP)	Dispositivo Crittografico a singolo fattore (SF)	Token crittografico software multi-fattore (MF)	Dispositivo multi-fattore (MF) del tipo One –Time Password (OTP)	Dispositivo Crittografico multi-fattore (MF)
Token con segreto memorizzato	Livello 1 SPID	Livello 1 SPID	Livello 2 SPID	Livello 2 SPID	Livello 2 SPID	Livello 2 SPID	Livello 3 SPID	Livello 2 SPID	Livello 3 SPID
Token con conoscenza pre-registrata	X	NA	NA	NA	NA	Livello 1 SPID	Livello 3 SPID	Livello 2 SPID	Livello 3 SPID
Token con tabella dei codici/segreti	X	X	NA	NA	NA	Livello 1 SPID	Livello 3 SPID	Livello 2 SPID	Livello 3 SPID
Token out of band	X	X	X	NA	NA	Livello 1 SPID	Livello 3 SPID	Livello 2 SPID	Livello 3 SPID
Dispositivo a singolo fattore (SF) del tipo One-Time Password (OTP)	X	X	X	X	NA	Livello 1 SPID	Livello 3 SPID	Livello 2 SPID	Livello 3 SPID
Dispositivo Crittografico a singolo fattore (SF)	X	X	X	X	X	X	Livello 3 SPID	Livello 2 SPID	Livello 3 SPID
Token crittografico software multi-fattore (MF)	X	X	X	X	X	X	Livello 3 SPID	Livello 3 SPID	Livello 3 SPID
Dispositivo multi-fattore (MF) del tipo One –Time Password (OTP)	X	X	X	X	X	X	X	Livello 2 SPID	Livello 3 SPID
Dispositivo Crittografico multi-fattore (MF)	X	X	X	X	X	X	X	X	Livello 3 SPID

Tabella A - Schema livello sicurezza SPID / multi-token

Si noti esplicitamente che un processo di autenticazione multi-stadio, in cui un token a fattore singolo viene usato per ottenere un secondo token, non costituisce un modello di autenticazione multi fattore in quanto il livello di sicurezza SPID associato alla soluzione composta è dato dal livello di sicurezza del token più debole.

Schema - Regole e Controlli - fase di gestione delle credenziali

Per la fase di gestione delle credenziali possiamo considerare il seguente diagramma di stato che illustra il ciclo di vita completo delle identità digitali SPID



Dove i cinque stati possibili sono così definiti:

NON ESISTENTE: nessuna informazione è presente nel registro delle identità digitali SPID usato per identificare un'entità (cittadino/impresa).

DEFINITA: le informazioni relative all'identità digitale sono state verificate durante in processo di iscrizione dell'entità, sono state generate informazioni addizionali (ad es. identificativo) e tutte le informazioni sono state registrate.

ATTIVA: le informazioni relative all'identità digitali sono presenti nel sistema di gestione delle identità in modo da consentire all'entità di interagire con i servizi abilitati e utilizzare le risorse disponibili nel dominio delle applicazioni consentite.

SOSPESA: le informazioni sono presenti ma è indicato che l'entità non può utilizzare nessun servizio e risorsa del dominio.

REVOCATA: le informazioni sono ancora presenti nel registro delle identità SPID anche se l'entità, di fatto, non esiste più nel dominio non potendo utilizzare alcun servizio o risorsa. Le informazioni archiviate possono essere utilizzate per scopi statistici, verifiche e controlli ma NON sono disponibili per il riconoscimento dell'entità ad eccezione di verifiche ed integrazioni per eventuali richieste di re-iscrizione. Si noti esplicitamente che quando l'entità si re-iscrive al registro delle identità digitali SPID, DEVE ESSERE definita una NUOVA identità che può includere alcune informazioni precedentemente archiviate (ripristino).

Per la gestione del ciclo di vita delle credenziali devono essere considerati gli stati di identità DEFINITA, ATTIVA, SOSPESA e REVOCATA ed associate transizioni e processi (si noti esplicitamente che il processo di iscrizione è fuori ambito dallo scopo di questo documento).

Un gestore di identità SPID emette e gestisce credenziali, in generale l' hardware, il software e i dati che possono essere usati per la produzione delle credenziali.

Le credenziali che sono emesse e supportate, incluso i dispositivi di sicurezza implementati, dal gestore di identità digitali sono fattori chiave per la determinazione del livello di sicurezza (da 1 a 3) SPID.

Nella fase di gestione delle credenziali, come da norma ISO 29115 devo essere considerate le seguenti potenziali minacce:

Alterazione/duplicazione delle credenziali (1) per accesso ai file che contengono le credenziali (ad es. sostituzione delle password con password note all'aggressore) e (2) durante le fasi di generazione/emissione/rinnovo delle credenziali.

Divulgazione non autorizzate delle credenziali possono avvenire (1) nella fase di emissione delle credenziali, (2) durante la rigenerazione/rinnovo delle credenziali, (3) per non sicura memorizzazione sui sistemi del gestore delle identità SPID e (4) per causa dell'entità che non ha conservato le credenziali in modo sicuro (ad es. scrittura di username e password in un posto accessibile da potenziali aggressori).

Attivazione fraudolenta delle credenziali nei casi in cui un aggressore ottiene delle credenziali che non gli appartengono e finge di essere la legittima entità richiedendone l'attivazione al gestore delle identità SPID.

Attivazione ritardata delle credenziali nei casi in cui un aggressore riesce a ritardare la consegna delle credenziali, o degli strumenti necessari per la generazione, e quindi a rendere impossibile il completamento del processo di attivazione nel prescritto periodo di tempo.

Revoca ritardata, in questo caso si rende possibile l'utilizzo di credenziali (che in teoria dovevano essere bloccate per effetto della revoca) da parte di potenziali aggressori.

Ripudio, un'entità sostiene che un valido uso delle credenziali è invece fraudolento o contiene informazioni non corrette allo scopo di negarne falsamente l'uso.

E quindi per la protezione dalle minacce sopra citate devono essere previste le seguenti azioni , regole e controlli.

A. Processi formalizzati, e ben documentati, per l'emissione delle credenziali. Se le credenziali non sono consegnate direttamente alla persona fisica, deve essere prevista una procedura per poter controllare l'esistenza dell'indirizzo di consegna e la legittima associazione all'entità richiedente.

B. Inoltre a partire dal livello 2 SPID, se le credenziali non sono consegnate di persona allora come recapito di consegna deve essere previsto un canale sicuro (ad es. e-mail registrata) e un meccanismo di riconoscimento per la ricezione delle credenziali.

C. Se le credenziali includono un dispositivo hardware, questo deve essere posto in uno stato bloccato alla fine del processo di creazione.

D. Se le credenziali, o i mezzi per la produzione delle credenziali, sono mantenute in un dispositivo hardware, questo deve essere conservato in un luogo fisicamente sicuro e deve esserne prevista una corretta tracciatura (inventario dei dispositivi). Ad esempio, nel caso di smart card deve essere prevista

la conservazione in posti sicuri e la registrazione dei numeri seriali in modo da garantire adeguata protezione contro furti e successivi tentativi di creazione di credenziali non autorizzate.

E. Per quanto riguarda la conservazione, le password, o in generale qualsiasi "segreto condiviso", devono essere protetti da un sistema di controllo che limiti l'accesso solo agli amministratori ed alle applicazioni necessari; in ogni caso i file che contengono "segreti condivisi" non devono MAI essere in chiaro (ad es. per le password deve essere previsto l'adozione di algoritmo di hash con salt in modo da impedire attacchi del tipo "forza bruta" o "tabella arcobaleno").

F. I requisiti e le condizioni per la protezione delle credenziali da parte delle entità devono essere descritti nella documentazione resa disponibile alle entità e deve esserne richiesto comprensione, assenso e condivisione. Nel caso di livello di sicurezza 3 di SPID, dovrà essere richiesto la firma di un documento da parte dell'entità coinvolta in modo da esplicitarne il riconoscimento.

G. Il gestore delle identità digitali SPID deve prevedere la revoca o distruzione (laddove possibile, ad es. azzerando le informazioni contenute nei token in modo che non sia presente alcuna informazione residua che potrebbe essere usata da un aggressore per poter ricavare valori validi di token) delle credenziali entro un ben definito e limitato periodo di tempo.

H. La documentazione della registrazione, storia e stato di ogni credenziale (incluso la revoca) deve essere mantenuta e conservata dal gestore delle identità digitali per un periodo di 20 anni dalla data di attivazione.

Schema - Regole e Controlli - fase di autenticazione

Il processo di autenticazione include l'uso di protocolli per dimostrare il possesso e/o il controllo delle credenziali in modo da acquisire sicurezza per l'identità richiesta.

Nella fase di autenticazione, come da norma ISO 29115 devono essere considerate le seguenti potenziali minacce:

- minacce comuni ICT ad es. social engineering, errori utente, keystroke logger
- furto delle credenziali
- provare ad indovinare (online e offline)
- replica di messaggi precedentemente catturati
- duplicazione
- appropriazione e/o dirottamento della sessione
- osservare di nascosto
- phising/pharming
- man in the middle
- spoofing

I seguenti controlli devono essere applicati nella fase di autenticazione e in dipendenza della tipologia delle credenziali e del livello di sicurezza SPID:

- non devono MAI essere conservati o tramessi in chiaro segreti o password.
- i dati necessari all'autenticazione devono essere cifrati durante il transito o per mezzo di un canale di comunicazione cifrato (ad es. TLS)

- ogni messaggio deve avere marcatura temporale e questa marcatura (timestamp) non deve essere alterabile
- devono essere previsti meccanismi di sicurezza fisica (ad es. evidenza della manomissione)
- adozione delle regole di complessità per le password come da Regolamento (bozza per il garante Privacy) per modalità attuative SPID
- deve essere previsto (e mandatorio) un servizio di attivazione per l'uso delle credenziali
- devono essere previsti meccanismi di blocco (o quantomeno di rallentamento/slowdown)dopo un certo numero di tentativi falliti dell'uso della password
- devono essere previsti misure di anti-contraffazione (ad es. ologrammi, microstampe) per i dispositivi che contengono le credenziali
- le password devono essere trattate con algoritmi di hashing con salt per mitigare gli attacchi del tipo tabelle arcobaleno o di forza bruta
- per prevenire attacchi da sistemi automatici deve essere prevista l'implementazione di Reverse Turing test durante il processo di autenticazione ← da valutare impatto su utente
- deve essere prevista analisi e audit di tutti i login falliti per verificare provenienza e pattern utilizzati
- adeguati controlli possono essere implementati per la rilevazione di attacchi di phising (ad es, filtri bayesiani per il blocco dello spam, blacklist IP, filtri basati su URL, schemi euristici), inoltre possono essere adottate delle buone pratiche come ad es. la disabilitazione delle immagini e iperlink per sorgenti non fidate
- le sessioni di autenticazione devono essere cifrate
- deve essere utilizzata una piattaforma tecnologica per le patch a correzione delle vulnerabilità TCP/IP
- per livello SPID > 1 devono essere adottati criteri di autenticazione ad almeno due fattori(ad es. una combinazione di qualcosa che si possiede con qualcosa che si conosce)
- devono essere previste tecniche di rilevazione di vita per resistere all'uso di caratteristiche biometriche artificiali (ad es. contraffazione delle impronte)

Controlli Continui

Verifica dell'identità con altri dati forniti out of band per le attività di manutenzione dell'identità digitale

Geo-localizzazione: per bloccare tentativi di autenticazione e di accesso da aree improbabili o anomale per storia recente accessi

IP reputation: bloccare (con l'utilizzo di tabelle IP blacklist) connessioni con server da indirizzi IP noti o sospetti per attività fraudolente

Out of wallet question: realizzare meccanismi che sfruttano dati non residenti in database pubblici per autorizzare transazioni a maggiore rischio

Anomaly detection: la capacità di rilevare comportamenti anomali e potenzialmente fraudolenti (ad es. velocità della transazione, storia e comportamento ecc.)

Asserzioni

come l'IdP protegge le asserzioni

quanta informazione è fornita nell'asserzione

da approfondire 1: in order for the RP to consider the assertion to be a Level 4 assertion of identity, the interaction between the CSP and the RP must comply with the holder-of-key provisions as documented in the FICAM SAML 2.0 Web Browser SSO Profile.

da approfondire 2: use an ICAM (SPID nel ns. Caso)-adopted authentication scheme.

Privacy trust criteria

Da considerare che oltre alla fase di iscrizione e per tutto il ciclo di vita della gestione delle credenziali anche durante le fasi di autenticazione sono monitorati e registrate una serie di eventi che possono essere necessari per diversi scopi come ad esempio la corretta erogazione del servizio e/o accesso a risorse, regole di conformità, per responsabilità ed altri obblighi legali.

Tutte queste informazioni possono includere anche dati sensibili che devono essere gestiti (1) secondo il principio del minimo necessario e (2) in modo da garantirne la protezione.

Al riguardo oltre alle regole definite dal Garante Privacy, ulteriori linee guide per la protezione dei dati PII (personal identifiable information) possono essere trovate in:

- ISO/IEC 29100 che descrive i principi base per la privacy: Scelta e Consenso, Specifica dell'uso e per quali scopi, Limitazioni sulla conservazione, Uso, Ritenzione, Limiti di Divulgazione, Minimizzazione dei dati, Accuratezza, Qualità, Trasparenza. Partecipazione individuale, Accesso, Responsabilità, Controlli di sicurezza e Conformità. In aggiunta all'esecuzione periodica di un risk assessment per una corretta analisi delle minacce, gli IdP dovrebbero condurre un **privacy impact assessment** (considerando anche rischi per azioni involontarie) per valutare quali componenti del loro sistema richiedono una particolare cura ed attenzione in termini di misure di protezione della privacy.

- ISO/IEC 29101 che fornisce le migliori pratiche e linee guida per la costruzione di una architettura ICT che che includa, in modo semplificato ed ottimale, la corretta gestione dei dati PII.

Per indicazioni più dettagliate sui principi, prerequisiti, la progettazione dei sistemi ed i controlli relativi alla protezione dei dati PII si consiglia di fare direttamente riferimento ai due standard sopra indicati.