

- Deve visualizzare, al completamento della procedura di autenticazione, la data, l'ora e le informazioni sull'ultimo sistema (indirizzo IP/FQDN) che ha completato con successo la fase di log-on per una specifica utenza;
- Deve visualizzare nella console dell'amministratore o nei file di log, i dettagli di tutti i precedenti tentativi infruttuosi di accesso per una specifica utenza;
- L'autenticazione non deve mai essere un processo convalidato lato client.

#### **5.7.4 Account standard**

L'applicazione non deve essere rilasciata da chi la sviluppa, con account utente standard di tipo amministrativo/operativo o con account protetti tramite password di default.

#### **5.7.5 Autorizzazione**

L'applicazione deve sempre operare un controllo sui reali privilegi d'accesso dell'utente prima di autorizzare qualsiasi operazione in lettura, scrittura, esecuzione o cancellazione.

L'autorizzazione non deve mai essere un processo convalidato lato client.

#### **5.7.6 Generazione dei token**

I token dell'applicazione devono essere generati utilizzando algoritmi true random ed analizzati ogniqualvolta l'utente richiede autorizzazione a svolgere una qualsiasi azione, al fine di determinarne permessi e privilegi.

#### **5.7.7 Generazione dei cookie**

Nelle applicazioni web i cookie di sessione applicativa devono essere cifrati, non persistent, avere il flag secure attivato e l'attributo HttpOnly impostato.

#### **5.7.8 Contenuto del cookie**

Un cookie non deve contenere informazioni critiche quali password o essere composto da parti predicibili come username o valori elaborati basandosi su algoritmi sequenziali. L'identificatore della sessione nel cookie deve avere un'entropia pari almeno a 128 bit.

#### **5.7.9 Scadenza del cookie**

Nelle applicazioni web, ciascun cookie generato deve essere soggetto a un tempo di scadenza oltre il quale non deve più essere considerato valido.

#### **5.7.10 Logout utente**

Quando un utente ha effettuato il log-out, la sessione relativa deve essere invalidata sia sul server (sganciandola nella Entry Table delle sessioni attive) che sul client (ad esempio rimuovendo il cookie o svuotando il suo contenuto).

#### **5.7.11 Timeout di sessione**

L'applicazione deve prevedere il rilascio della sessione utente dopo un certo periodo configurabile di inattività della sessione stessa.

#### **5.7.12 Isolamento delle funzioni dall'applicazione**

È vietata l'implementazione della sicurezza attraverso l'oscuramento delle funzioni a livello di presentazione. È obbligatorio invece isolare e rendere inutilizzabili le funzioni che non devono essere rese accessibili agli utenti, direttamente a livello logico (es: imponendo la consultazione del token della sessione per determinarne i reali privilegi di esecuzione).

### **5.8 Password, chiavi e certificati**

Per la gestione di dati quali password, chiavi e certificati, si raccomanda l'adozione dei criteri riportati di seguito.