- Scopo della funzione;
- Parametri di input e output a/dalla funzione;
- Valori di ritorno dei parametri di output;
- Tracciamento degli aggiornamenti del codice della funzione (data ultima modifica).
- Le parentesi graffe, nel codice, devono essere apposte sulla riga superiore e inferiore rispetto alla dichiarazione del costrutto linguistico (struttura, classe, funzione, metodo, etc.).
- È raccomandato che ogni funzione assolva un unico compito, in maniera efficiente ed efficace.

5.3.2 Algoritmi

Nell'ottica di rendere l'applicazione conforme agli standard internazionali è richiesto l'utilizzo esclusivo di algoritmi riconosciuti nell'industria del software. Gli standard internazionali devono essere strettamente seguiti per lo sviluppo di algoritmi crittografici e processi di autenticazione.

5.3.3 Utilizzo funzioni di gestione delle stringhe

Tutto l'input utente processato dall'applicazione deve passare per funzioni sicure di gestione delle stringhe che ne prevedono il bound-checking (controllo del range di validità). L'applicazione deve risultare immune da problematiche di tipo stack overflow, off by one/off by few overflow o heap overflow.

5.3.4 Specifica del formato delle stringhe

Nei sorgenti dell'applicazione il formato delle stringhe deve essere sempre specificato nei parametri delle funzioni che lo prevedono e mai dato per assunto. L'applicazione deve risultare immune da problematiche di tipo format string overflow.

5.3.5 Casting e variabili numeriche

L'input utente deve essere filtrato in modo che alle variabili o strutture dati interne dell'applicazione non sia possibile assegnare valori negativi (ad esempio dichiarando array come signed integer) ad eccezione dei casi previsti e per i quali sia stata pianificata la gestione. In fase di comparazione di due variabili numeriche dove il contenuto di almeno una deriva da input utente, il casting o l'assegnazione di un valore da una variabile all'altra deve avvenire in base alla stessa tipologia (ad esempio assegnare un valore intero a una variabile di tipo short è un errore). L'applicazione deve risultare immune da problematiche di tipo integer overflow, cambi di segno, troncamento di valori numerici o altri errori di programmazione logico-computazionali.

5.4 Tracciamento e Raccomandazioni di "Alarm Detection"

Per il tracciamento degli eventi di "Alarm Detection" si raccomanda l'adozione dei criteri generali riportati nei paragrafi (Cfr. [5.4.1- 5.4.4]) che seguono.

5.4.1 Tracciamento eventi

L'applicazione deve essere predisposta sia per il tracciamento di attività "anomale" sia per le "eccezioni" verificatesi sui sistemi.
Il tracciamento degli eventi può essere attivato su:

- Eventi andati a buon fine;
- Eventi non andati a buon fine;
- Errori di sistema o utente;
- La configurazione del sistema di tracciamento e detection degli allarmi sarà predisposta sulla base delle policy stabilite nell'ambito dei requisiti dell'applicazione.

Gli eventi per i quali è richiesto il tracciamento riguardano:

- Autenticazione e processi correlati;
- Start e Stop delle componenti dell'applicazione;
- Violazioni dei criteri o delle policy configurate;