**ARCHITETTURA GENERALE**

**Architettura del Remote SIM Provisioning System**Caso in cui LPA è embeddato nel dispositivo (LPAd):

Immagine che contiene diagramma

Descrizione generata automaticamente

-> **CI** = Certificate Issuer: è un’entità autorizzata a rilasciare certificati digitali.  
-> **EUM** = eUICC Manufacturer: è il fornitore delle eUICC e del software residente (e.g. firmware e OS).  
-> **LDSd** = Local Discovery Service (quando LPA è nel dispositivo).  
-> **LPDd** = Local Profile Download (quando LPA è nel dispositivo).  
-> **LUId** = Local User Interface (quando LPA è nel dispositivo).

**Enhanced = potenziato**

Caso in cui LPA è embeddato nell’eUICC (LPAe):

Immagine che contiene diagramma

Descrizione generata automaticamente

-> **LDSe** = Local Discovery Service (quando LPA è nell’eUICC).  
-> **LPDe** = Local Profile Download (quando LPA è nell’eUICC).  
-> **LUIe** = Local User Interface (quando LPA è nell’eUICC).

**Architettura dell’eUICC**  
Immagine che contiene diagramma

Descrizione generata automaticamente

-> **CASD** = Controlling Authority Security Domain.  
-> **ECASD** = eUICC Controlling Authority Security Domain: è il componente responsabile dello storage sicuro delle credenziali richieste per supportare i domini di sicurezza necessari sull’eUICC. Dovrebbe essere unico nell’eUICC e dovrebbe essere personalizzato dall’EUM durante la produzione dell’eUICC. Contiene la chiave privata dell’eUICC per creare le signature ECDSA, il certificato dell’eUICC, la chiave pubblica del CI per verificare i certificati delle controparti, il certificato dell’EUM e il set di chiavi dell’EUM per rinnovare chiavi/certificati in uso. In definitiva, fornisce all’ISD-R servizi come la creazione della firma eUICC e la verifica dei certificati mediante la chiave pubblica della CI.  
-> **ES6** = interfaccia tra l’operatore e l’eUICC usata dall’operatore per la gestione dei servizi dell’operatore.  
-> **ES8+** = interfaccia tra SM-DP+ e l’eUICC che fornisce un canale end-to-end sicuro tra SM-DP+ e l’eUICC per l’amministrazione dell’ISD-P e del profilo associato.  
-> **ES9+** = interfaccia tra SM-DP+ e LPD usata per fornire trasporto sicuro tra SM-DP+ e LPA.  
-> **ES10a** = interfaccia tra LDSd e l’eUICC usata per gestire una Discovery Request.  
-> **ES10b** = interfaccia tra LPDd e l’eUICC usata per trasferire un Bound Profile Package (BPP – un Protected Profile Package crittograficamente collegato all’eUICC) all’interno dell’eUICC.  
-> **ES10c** = interfaccia tra LUId e l’eUICC usata per la gestione locale del profilo da parte dell’end user.  
-> **ES11** = interfaccia tra LDS e SM-DS usata da LDS per recuperare gli Event Record (i.e. set di informazioni salvate su SM-DS per uno specifico evento) per il rispettivo eUICC.  
-> **ESeu** = interfaccia tra l’end user e la LUI che è specifica per le relazioni di business.  
-> **ISD-P** = Issuer Security Domain Profile: è un contenitore sicuro che ospita un unico profilo. Nessun componente al di fuori dell’ISD-P (eccetto l’ISD-R) dovrebbe avere visibilità o accesso al profilo; inoltre, il profilo non dovrebbe avere visibilità o accesso ad alcun componente al di fuori del proprio ISD-P; infine, un ISD-P non dovrebbe avere visibilità o accesso ad alcun altro ISD-P.  
-> **ISD-R** = Issuer Security Domain Root: è il componente responsabile della creazione di nuovi ISD-P e della gestione del loro ciclo di vita. Dovrebbe essere unico nell’eUICC, dovrebbe essere personalizzato dall’EUM durante la produzione dell’eUICC e non può essere eliminato o disabilitato.  
-> **LPA Services** = i seguenti 4 servizi: trasferimento del BPP da LPAd all’ISD-P; ottenimento della lista dei profili installati; recupero dell’EID (eUICC ID); ottenimento delle operazioni di gestione del profilo locale (Local Profile Management Operations).  
-> **MNO-SD** = Mobile Network Operator Security Domain: è la parte del profilo (posseduta dall’operatore) che fornisce il canale sicuro alla piattaforma dell’operatore Over The Air (OTA); viene usato per gestire il contenuto di un profilo una volta che è stato abilitato.  
-> **NAAs** = Network Access Applications.  
-> **Profile Package Interpreter** = servizio dell’OS dell’eUICC che traduce i dati del Profile Package in un profilo installato all’interno dell’ISD-P codificato usando il formato interno dell’eUICC target.  
-> **SSD** = Supplementary Security Domain.  
-> **Telecom Framework** = servizio dell’OS che fornisce algoritmi di autenticazione di rete standardizzati ai NAAs ospitati negli ISD-P. Inoltre, fornisce la capacità di configurare gli algoritmi con i parametri necessari all’interno del profilo abilitato.

Caratteristiche dell’eUICC:  
- Dovrebbe essere resistente al tampering dei componenti hardware.  
- Dovrebbe supportare SHA-1.  
- Dovrebbe supportare TUAK (che è un particolare algoritmo crittografico 3GPP).  
- Dovrebbe supportare Milenage (che è un set di funzioni 3GPP di autenticazione e di key generation).  
- Tutte le funzioni crittografiche dovrebbero essere resistenti al tampering e agli attacchi side-channel.

[PAGINA 26]