**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.

**Protezione e delivery dei profili**  
Qui viene descritto come un profilo di un operatore (Operator Profile) viene protetto all’interno di un Profile Package prima di essere scaricato in un eUICC. Abbiamo diversi formati di Profile Package:  
-> Unprotected Profile Package (UPP): viene generato da SM-DP+ all’interno della Profile Package Generation function, che prende come input le specifiche del profilo stabilite con l’operatore. Tale Profile Package consiste in una sequenza di Profile Element (PE) di tipo TLV (Type-Length-Value).  
-> Protected Profile Package (PPP): viene generato da SM-DP+ all’interno della Profile Package Protection function. Dovrebbe essere protetto col protocollo **SCP03** (**Secure Channel Protocol 03**, che prevede l’uso di una serie di chiavi simmetriche dette Static Keys); a tal proposito, potrebbero essere utilizzate le **chiavi di sessione** (S-ENC, S-MAC) generate dal key agreement con l’eUICC oppure le **random key per Profile** (PPK-ENC, PPK-MAC) generate da SM-DP+. L’eUICC dovrebbe supportare entrambe le alternative, anche se l’uso delle random key per Profile garantisce la Profile Package Protection senza avere alcuna conoscenza dell’eUICC, il che può fornire una migliore scalabilità di SM-DP+.  
-> Bound Profile Package (BPP): viene generato da SM-DP+ all’interno della Profile Package Binding Function. Il suo scopo è collegare un Protected Profile Package a un particolare eUICC, il che è fatto con un key agreement tra l’eUICC e SM-DP+.  
-> Segmented Bound Profile Package (SBPP): è generato da LPAd, il quale trasferisce il Bound Profile Package all’eUICC usando l’interfaccia locale ES10b e suddividendo i Profile Element in più segmenti composti da al più 255 byte.

Profile Installation Result:  
È codificato in un oggetto ASN.1 e contiene i seguenti dati:  
- **Notification Metadata**: metadati che includono informazioni come il sequence number e l’ICCID (integrated circuit card identifier).  
- **Transaction ID**: identificatore fornito all’eUICC durante la procedura di scaricamento e installazione.  
- **Final Result**: fornisce l’esito dell’installazione del profilo.  
- **SM-DP+ OID** (opzionale): object identifier di SM-DP+ fornito all’eUICC durante la procedura di scaricamento e installazione.  
- **Signature**: viene creata dall’eUICC con lo scopo di garantire l’autenticità e l’integrità del Profile Installation Result.

Il Profile Installation Result dovrebbe essere creato dall’eUICC dopo l’esecuzione dell’ultimo TLV del BPP oppure dopo l’esecuzione dell’eventuale TLV del BPP che dà errore. Dopodiché, dovrebbe essere mantenuto dall’eUICC finché non verrà eliminato esplicitamente dall’LPA (dopo averlo consegnato con successo a SM-DP+). Prima dell’eliminazione, il Profile Installation Result potrebbe essere recuperato in qualunque momento dall’LPA. Quando viene avviato un nuovo scaricamento e installazione di un profilo, l’eUICC potrebbe eliminare eventuali vecchi Profile Installation Result che sono ancora memorizzati.

**Security overview**  
Certificazione delle entità:  
- L’eUICC dovrebbe essere certificato con l’eUICC Protection Profile.  
- L’EUM, SM-DP+ e SM-DS dovrebbero essere certificati con la GSMA SAS certification.

Remote Secure Communication:  
L’ecosistema RSP (Remote SIM Provisioning) si basa sulla comunicazione remota sicura per poter fare uso delle richieste dell’esecuzione di funzioni e dello scambio di dati. Qualunque comunicazione remota definita per RSP dovrebbe seguire le regole sottostanti.  
-> **Mutua autenticazione**: il server (e.g. SM-DP+) dovrebbe essere autenticato per primo dal client; l’autenticazione dovrebbe includere la verifica di un Server Certificate valido firmato da un Certificate Issuer di GSMA. D’altra parte, il client dovrebbe essere autenticato dal server in un secondo momento; nel caso in cui il client sia l’eUICC, l’autenticazione dovrebbe includere la verifica di certificati eUICC ed EUM validi firmati da un Certificate Issuer di GSMA.  
-> **Privacy dei dati**: l’eUICC, in quanto client, non deve rivelare alcuna informazione privata a un server non autenticato. Inoltre, non deve generare materiale firmato prima di essersi autenticato al server.  
-> **Protezione della comunicazione**: dopo aver completato la mutua autenticazione, le due controparti dovrebbero negoziare una suite crittografica minimale (e.g. chiavi simmetriche) per proseguire la comunicazione. Quest’ultima dovrebbe essere protetta dall’integrità dei messaggi, dalla cifratura e dall’autenticazione del mittente. Quando possibile, dovrebbe valere la proprietà di **Forward Secrecy**, secondo cui se una chiave a lungo termine viene compromessa, le chiavi di sessione generate a partire da essa vengono comunque riservate.  
-> **Autorizzazione**: sulla base dell’autenticazione, il server dovrebbe sempre verificare che il client che invia le richieste sia effettivamente autorizzato prima di far partire l’esecuzione della funzione richiesta.

Public Key Infrastructure:  
Ciascun certificato ha una validation chain la cui root è il certificato del Certificate Issuer di GSMA; viene usato per l’autenticazione delle entità mediante una signature creata con la chiave privata associata a esso (al certificato), dove la signature dovrebbe essere fatta con ECDSA. I certificati possono essere revocati.

Protocollo per la protezione dei profili e il binding all’eUICC:  
Ciascun Profile è protetto mediante meccanismi di sicurezza basati sul protocollo **SCP11a** (**Secure Channel Protocol 11**), che ha le seguenti caratteristiche:  
- La mutua autenticazione viene fatta con uno shared secret calcolato da coppie di ephemeral key.  
- Le ephemeral key possono essere utilizzate più di una volta e salvate in memoria non volatile.  
- ISD-R non deve memorizzare in modo persistente alcuna chiave pubblica SM-DP+.  
- La procedura per stabilire le chiavi di sessione dovrebbe usare solo lo shared secret generato da coppie di ephemeral key.  
- I primi TLV che seguono i dati relativi alla procedura per stabilire le chiavi sono protetti con le chiavi di sessione generate nel key agreement.  
- Opzionalmente, le chiavi di sessione possono essere rimpiazzate dalle chiavi di protezione del profilo. Queste ultime sono a loro volta protette proprio dalle chiavi di sessione.

Lunghezza delle chiavi e funzioni hash:

Immagine che contiene Rettangolo

Descrizione generata automaticamente

Immagine che contiene testo

Descrizione generata automaticamente

Elliptic Curves Algorithms:  
Per facilitare l’interoperabilità, le specifiche prevedono solo tre curve ellittiche: NIST P-256, brainpoolP256r1 e FRP256V1. L’eUICC dovrebbe supportare almeno due curve ellittiche, i cui parametri vengono precaricati dall’EUM durante la fabbricazione dell’eUICC. D’altra parte, un server RSP dovrebbe supportare tutte e tre le curve ellittiche.  
Gli algoritmi principalmente usati per le curve ellittiche sono:  
-> **ECDSA**: algoritmo usato per generare le signature.  
-> **ECKA**: algoritmo usato in RSP per stabilire le chiavi di sessione tra l’eUICC e SM-DP+.

**Revocazione dei certificati**  
I seguenti certificati possono essere revocati in qualunque momento:  
- Certificato del GSMA CI (Certificate Issuer).  
- Certificato EUM.  
- Certificati SM-DP+.  
- Certificato TLS di SM-DP+.  
- Certificato SM-DS.  
- Certificato TLS di SM-DS.  
Ciascun GSMA CI dovrebbe gestire lo status di revocazione dei certificati che aveva rilasciato. Tale status di revocazione viene esposto a tutte le entità RSP sottoforma di Certificate Revocation List (CRL). D’altro lato, la gestione della revoca dei certificati è opzionale per l’eUICC. Se tale capability non è supportata all’interno dell’eUICC, l’LPA non deve passare la CRL all’eUICC stesso.

[2.9 PAGINA 38]