Università degli Studi di Roma Tor Vergata

DIPARTIMENTO DI INGEGNERIA CIVILE E INGEGNERIA DELL'INFORMAZIONE
Corso di Laurea Magistrale in Ingegneria Informatica

Titolo della tesi

Candidato:
Matteo Fanfarillo
Matricola 0316179

Relatore:
Giuseppe Bianchi

Correlatore:
Francesco Gringoli

Anno Accademico 2023/2024

[Citazione]

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Introduzione

1.1 Panoramica sull'eSIM

La eSIM (embedded-SIM) non è altro che una SIM virtuale: grazie a lei, quando l'utente vuole cambiare operatore, non deve più acquistare fisicamente una nuova SIM card presso un negozio del nuovo operatore, bensì gli è sufficiente ricevere via e-mail un profilo, ossia una "SIM digitale" che può essere caricata subito sul telefono mediante la scansione di un QR code. Si tratta di una soluzione molto più pratica rispetto a recarsi fisicamente presso il negozio dell'operatore, tant'è vero che negli ultimi anni si sta diffondendo sempre di più: uno studio di Juniper Research stima che il numero di telefoni che utilizzano la connettività eSIM aumenterà dai 986 milioni attuali ai 3.5 miliardi entro il 2027 [1]. Per questi motivi, e poiché le informazioni associate alla comunicazione tra eSIM sono sensibili, è fondamentale garantire un livello di sicurezza sufficientemente elevato per il funzionamento dell'eSIM sia a run-time che a boot-time.

1.2 Obiettivo del lavoro

La presente trattazione si propone di effettuare un'analisi di sicurezza e delle vulnerabilità della eSIM e del suo funzionamento e, successivamente, di tentare di sfruttare, anche con delle attività di laboratorio, le eventuali vulnerabilità trovate.

1.3 Definizioni preliminari

- **eUICC (embedded Universal Integrated Circuit Card)**: è un chip utilizzato all'interno dei telefoni all'interno del quale è embeddato il software dell'eSIM. È integrato direttamente nei dispositivi (i.e. non è rimovibile) ed è progettato per essere programmato a distanza. Può contenere uno o più profili eSIM.
- **LPA (Local Profile Assistant)**: è un'applicazione che vive nel telefono dell'utente ed è responsabile della gestione dei profili all'interno della rete mobile, inclusi la creazione, l'aggiornamento e la cancellazione.
- **SM-DP+ (Subscription Manager Data Preparation plus)**: è un protocollo che rappresenta una tecnica di provisioning usata per configurare le eSIM in modo automatico e remoto. Rispetto alla versione base SM-DP, offre delle funzionalità aggiuntive come un sistema di crittografia più avanzato e un'architettura di rete più flessibile.

1.4 Panoramica sui capitoli successivi

Nel capitolo 2 verrà svolta una trattazione dettagliata sull'architettura e sulle interfacce dell'eSIM, con lo scopo di fornire al lettore gli strumenti per comprendere appieno le tematiche centrali del lavoro. Nel capitolo 3 verrà effettuata un'analisi della sicurezza dell'eSIM a run-time, mentre nel capitolo 4 si procederà con l'analisi della sicurezza dell'eSIM a boot-time (i.e. durante la

fase di configurazione). Infine, nel capitolo 5 verranno mostrati i risultati finali, verranno tratte delle conclusioni sul lavoro svolto e verrà fornita una panoramica sui possibili progetti futuri che potranno essere intrapresi a partire dai risultati ottenuti attraverso questo lavoro.

Capitolo 2

Interfacce e funzionamento dell'eSIM

2.1 Architettura di RSP

Per comprendere appieno come funziona e come si interfaccia l'eSIM all'interno dei dispositivi mobili, è necessario introdurre il protocollo RSP, anche perché la eSIM si colloca proprio all'interno dell'architettura di RSP.
RSP (Remote SIM Provisioning) è un protocollo utilizzato dal protocollo SM-DP+ per gestire la comunicazione tra il server SM-DP+ e la scheda eSIM del dispositivo mobile (i.e. l'eUICC). In particolare, definisce le operazioni di provisioning specifiche per la comunicazione dell'eUICC. Quest'ultimo comprende i dati sia dell'operatore che dell'utente che, nel caso delle SIM tradizionali, verrebbero appunto memorizzati su una SIM card fisica. Entrando più nel dettaglio sul funzionamento di RSP, l'end user che vuole ottenere un profilo eSIM offerto da un particolare operatore (nel quale viene definito un piano tariffario), deve pagare l'operatore affinché esso gli fornisca un codice QR. Dopodiché, deve effettuare la scansione di tale codice QR per avviare lo scaricamento (operazione di Download) e l'installazione (operazione di Install) del profilo eSIM: a questo punto, la connessione tra end user (col relativo profilo eSIM) e operatore è completata. Se in un secondo momento l'end user ha la necessità di ottenere e utilizzare un secondo profilo eSIM, gli è sufficiente ripetere i medesimi passaggi appena descritto, e questo secondo profilo può essere installato all'interno del medesimo eUICC che ospita già il primo profilo. Tale meccanismo è illustrato nella figura 2.1 tratta da [2].
Per quanto riguarda l'architettura interna di RSP nello specifico, esistono due soluzioni diverse [3].

1. **LPA embeddato nel dispositivo mobile ma non all'interno dell'eUICC (LPAd)**: oltre alla comunicazione tra l'applicazione LPA e SM-DP+, si utilizzano delle apposite interfacce anche per la comunicazione tra l'eUICC e l'applicazione LPA, come mostrato nella figura 2.2 tratta da [3]. Di seguito è riportato un breve glossario che chiarisce il significato di alcuni componenti appartenenti all'architettura di RSP raffigurata in 2.2.

   - **CI** = Certificate Issuer: è un'entità autorizzata a rilasciare certificati digitali.
   - **Device App** = una qualunque applicazione installata nel dispositivo mobile.
   - **Enterprise** = impresa (i.e. azienda, organizzazione o entità governativa) che si iscrive ai servizi mobili che devono essere utilizzati dai dipendenti a supporto dell'impresa stessa.
   - **EUM** = eUICC Manufacturer: è il fornitore delle eUICC e del software residente (e.g. firmware, sistema operativo); svolge anche il ruolo di certificate authority subordinata al CI e rilascia certificati all'eUICC [4].
   - **HRI Server** = server che fornisce le High Resolution Icon, che sono icone che vengono create per essere visualizzate in alta risoluzione.
   - **LDSd** = Local Discovery Service (quando LPA non è nell'eUICC).
   - **LPDd** = Local Profile Download (quando LPA non è nell'eUICC).
   - **LUId** = Local User Interface (quando LPA non è nell'eUICC).

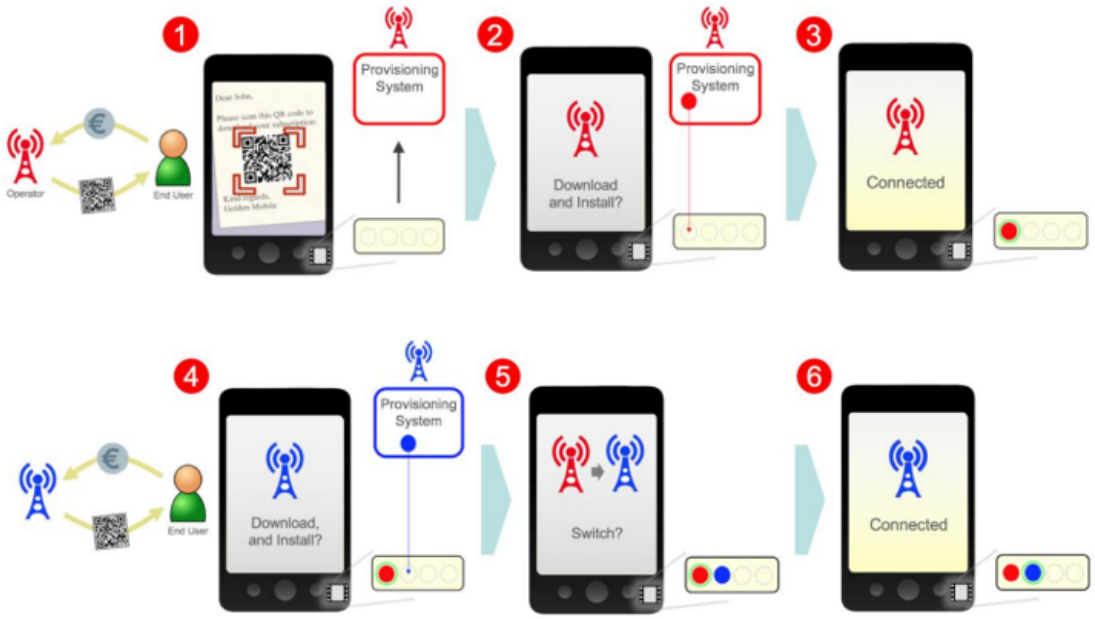

Figura 2.1: Comunicazione tra end user e operatore nel contesto del Remote SIM Provisioning.

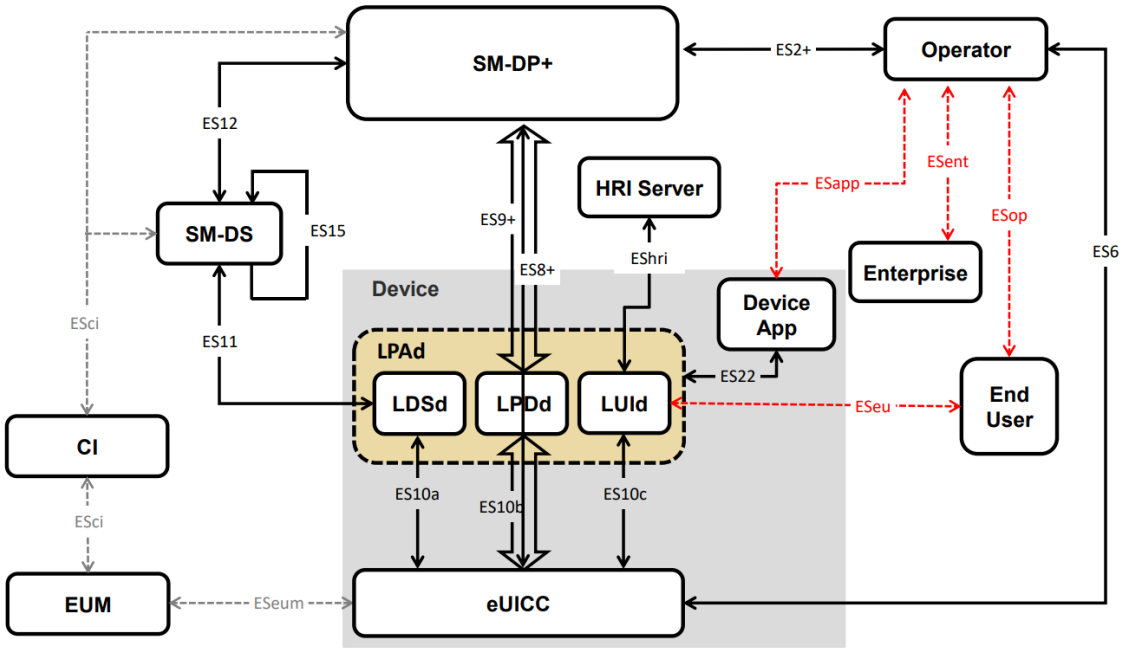

Figura 2.2: Architettura di RSP nel caso di LPA non embeddato nell'eUICC.

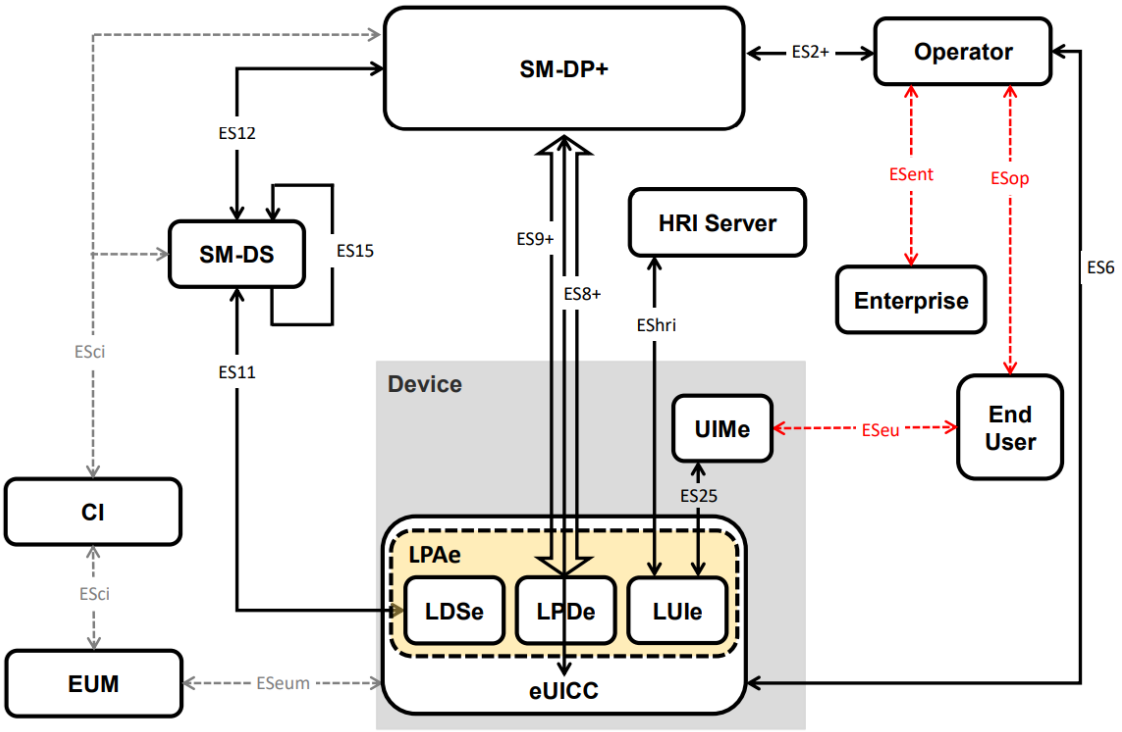

Figura 2.3: Architettura di RSP nel caso di LPA embeddato nell'eUICC.

- **SM-DS** = Subscription Manager Discovery Server: è il componente che fornisce un mezzo a SM-DP+ per raggiungere l'eUICC senza dover sapere a quale rete il dispositivo è connesso.

2. **LPA embeddato all'interno dell'eUICC (LPAe)**: sono necessarie solo delle interfacce tra l'eUICC e SM-DP+, come mostrato nella figura 2.3 tratta da [3]. Successivamente è riportato un breve glossario che chiarisce il significato di alcuni componenti appartenenti all'architettura di RSP raffigurata in 2.3.

   - **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).
   - **UIMe** = User Inteface Module.

2.1.1 Interfacce presenti nell'architettura di RSP

Sono illustrate nella tabella 2.1, costruita a partire da informazioni tratte da [3].

**Un Profile Package è un pacchetto di dati associato a un profilo che contiene le informazioni di configurazione necessarie per attivare e utilizzare quel profilo all'interno di una scheda eSIM. Esistono diversi tipi di Profile Package: l'Unprotected Profile Package (UPP) è un pacchetto di dati non protetto da alcun meccanismo di sicurezza, come l'autenticazione o la crittografia; il Protected Profile Package (PPP) è un pacchetto di dati protetto da alcuni meccanismi di sicurezza; il Bound Profile Package (BPP) è un pacchetto di dati legato a un particolare dispositivo o a una piattaforma di servizi; il Segmented Bound Profile Package (SBPP), infine, non è altro che un BPP suddiviso in molteplici segmenti che possono essere utilizzati in modo indipendente e separato.*
***ISD-P (Issuer Security Domain Profile) è un contenitore sicuro che ospita un unico profilo.*
****Root SM-DS è il server primario utilizzato da un operatore di rete mobile per gestire le attivazioni e le disattivazioni delle sottoscrizioni e per gestire funzionalità come l'autenticazione e l'autorizzazione degli utenti. D'altra parte, si hanno gli Alternative SM-DS, che sono server di backup a cui si ricorre quando il Root SM-DS non è disponibile.*

Tabella 2.1: Interfacce in RSP

Interfaccia	Componente 1	Componente 2	Descrizione
ES2+	Operatore	SM-DP+	Viene usata dall'operatore per invocare la preparazione del Profile Package*.
ES6	Operatore	eUICC	Viene usata dall'operatore per gestire il contenuto dei profili.
ES8+	SM-DP+	eUICC	Fornisce un canale end-to-end sicuro tra SM-DP+ e l'eUICC per l'amministrazione dell'ISD-P** e del relativo profilo durante il download e l'installazione.
ES9+	SM-DP+	LPD	Viene usata per fornire trasporto sicuro tra SM-DP+ e LPD per la consegna del Profile Package.
ES10a	LDSd	eUICC	Viene usata da LPAd per ottenere gli indirizzi configurati dall'eUICC per Root SM-DS*** (gestione di una Discovery Request).
ES10b	LPDd	eUICC	Viene usata da LPAd per trasferire un Profile Package all'eUICC.
ES10c	LUId	eUICC	Viene usata da LPAd per la gestione locale dei profili installati sull'eUICC da parte dell'end user (e.g. Enable, Disable, Delete).
ES11	LDS	SM-DS	Viene usata per l'ottenimento di eventi.
ES12	SM-DP+	SM-DS	Viene usata per la gestione degli eventi.
ES15	SM-DS	SM-DS	Viene usata per connettere gli SM-DS tra loro nel caso in cui ce ne sia più di uno.
ES22	LPAd	Device App	Viene usata da un'applicazione del dispositivo mobile per interoperare con l'LPA.
ES25	UIMe	LUIe	Viene usata per trasferire verso l'LPA le interazioni dell'end user.
ESop	Operatore	End user	È specifica per le relazioni di business tra l'operatore e l'end user.
ESeu	End user	LUI	È specifica per le relazioni di business tra l'end user e la LUI.
ESeum	eUICC	EUM	È specifica per le relazioni di business tra l'eUICC e l'EUM.
ESci	CI	SM-DP+, SM-DS, EUM	Viene usata per richiedere certificati.
EShri	LUI	HRI Server	Viene usata per recuperare le High Resolution Icon.
ESent	Operatore	Enterprise	È un'interfaccia che prescinde dagli scopi del presente documento.
ESapp	Operatore	Device App	È un'interfaccia che prescinde dagli scopi del presente documento.

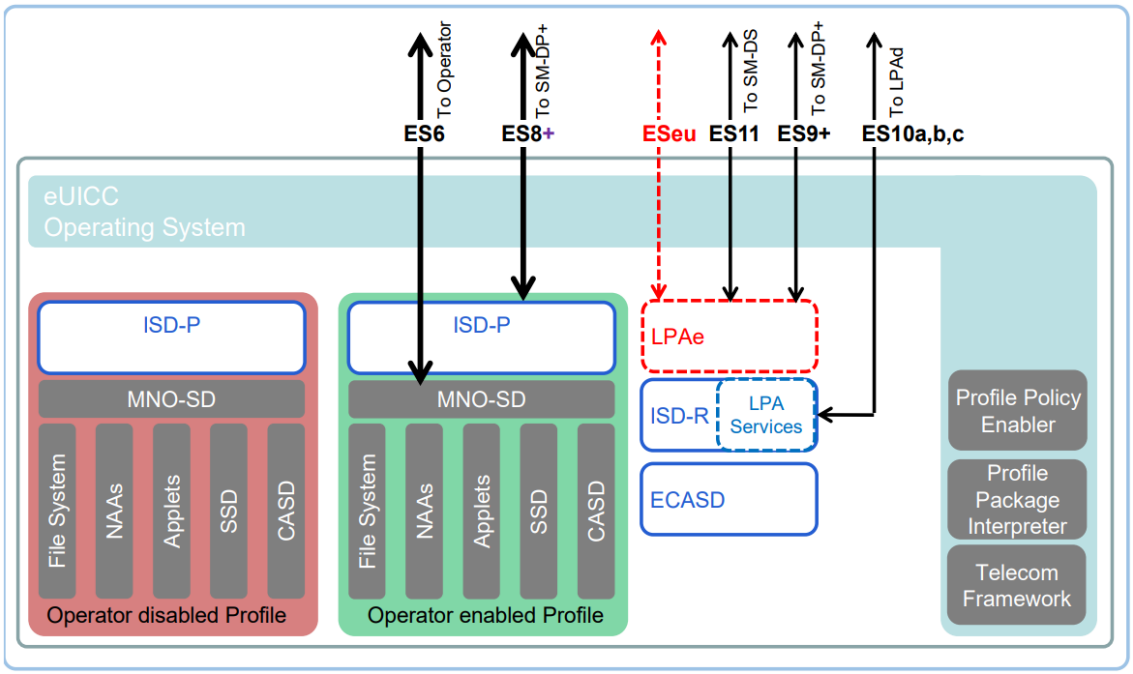

Figura 2.4: Architettura dell'eUICC.

2.2 Architettura dell'eUICC

Nella figura 2.4 tratta da [3] è schematizzata l'architettura interna del chip eUICC, dove i riquadri e le frecce in rosso sono relativi rispettivamente ai componenti e alle interfacce che, nell'ambito dell'eUICC, sono presenti esclusivamente nel caso in cui l'applicazione LPA sia effettivamente embeddata all'interno dell'eUICC (LPAe).
Di seguito, invece, è riportato un breve glossario che chiarisce il significato di alcuni componenti appartenenti all'architettura dell'eUICC raffigurata in 2.4.

- **CASD** = Controller Authority Security Domain: è un'area di storage sicura all'interno dell'ISD-P in cui vengono memorizzate le credenziali richieste per supportare le funzionalità di sicurezza sensibili.
- **ECASD** = Embedded Controller Authority Security Domain: è il componente CASD direttamente incapsulato all'interno dell'eUICC.
- **ISD-R** = Issuer Security Domain Root: è il componente responsabile della creazione di nuovi ISD-P e della gestione del loro ciclo di vita.
- **LPA Services** = i seguenti quattro servizi: trasferimento del Bound Profile Package 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 all'operatore Over The Air (OTA) un canale di comunicazione sicuro; viene usato per gestire il contenuto di un profilo una volta che è stato abilitato.
- **NAAs** = Network Access Applications: sono le applicazioni che consentono l'accesso alla rete.
- **Profile Package Interpreter** = servizio del sistema operativo dell'eUICC che traduce i dati del Profile Package in un profilo installato all'interno dell'ISD-P codificando usando il formato interno dell'eUICC.
- **Profile Policy Enabler** = componente che verifica che un il profilo eSIM possa essere installato sull'eUICC.

- **SSD** = Supplementary Security Domain: è un'area di memoria protetta all'interno dell'ISD-P che viene utilizzata per l'esecuzione di funzioni di sicurezza come le operazioni crittografiche. Di fatto, il suo scopo principale è quello di proteggere le informazioni riservate dell'utente (i.e. chiavi, password) da accessi non autorizzati e attacchi esterni.
- **Telecom Framework** = servizio del sistema operativo dell'eUICC che fornisce algoritmi di autenticazione di rete standardizzati alle applicazioni NAAs ospitate nei rispettivi ISD-P.

2.2.1 Caratteristiche hardware e software dell'eUICC

1. Deve essere resistente al tampering dei componenti hardware.
2. Supporta SHA-1.
3. Supporta TUAK, che è un particolare algoritmo crittografico di 3GPP, dove 3GPP (Third Generation Partnership Project) è il consorzio industriale che definisce gli standard per la tecnologia 5G .
4. Supporta Milenage, che è un set di funzioni 3GPP di autenticazione e di key generation.
5. Tutte le funzioni crittografiche devono essere resistenti al tampering e agli attacchi side-channel.

2.3 Interazione tra eUICC, LPA, SM-DP+ e operatore

2.3.1 Sicurezza TLS

Il protocollo TLS, la cui versione 1.2 è definita in RFC 5246 [5] e la cui versione 1.3 è definita in RFC 8446 [6], è utilizzato per proteggere il traffico sulle interfacce ES2+ (tra server SM-DP+ e operatore) e ES9+ (tra server SM-DP+ e LPA). In particolare, in ES2+ è prevista la mutua autenticazione tra le parti, mentre in ES9+ è prevista solo l'autenticazione del server. La documentazione di GSMA di riferimento [3] sottolinea l'obbligatorietà di fare uso di TLS v1.2 sia per gli algoritmi di autenticazione e autorizzazione, sia per l'integrità dei messaggi, sia per la confidenzialità. In realtà, introduce anche la possibilità (e suggerisce) di utilizzare TLS v1.3, che è la versione più recente di TLS e risolve le vulnerabilità che caratterizzano TLS v1.2, per cui, in linea di principio, dovrebbe risultare particolarmente difficoltoso da penetrare. Tuttavia, attualmente sembra essere solo un suggerimento, per cui nei capitoli successivi potrebbe essere necessario verificare a livello pratico qual è la versione di TLS utilizzata per proteggere la comunicazione tra LPA e server SM-DP+.
Un discorso analogo vale per l'interazione che si ha nella mutua autenticazione tra l'eUICC e il server SM-DP+, dove le due parti interagiscono tra loro tramite un TLS tunnel [4]. Per quanto invece riguarda la comunicazione tra eUICC e applicazione LPA, è richiesto l'utilizzo di un pairwise secure channel (ovvero di un canale di comunicazione sicuro rispetto alla confidenzialità e all'autenticazione dei messaggi) che collega le due parti all'interno del dispositivo mobile [4]. Tuttavia, non esiste una specifica universale che imponga l'utilizzo di un particolare protocollo di crittografia per proteggere il pairwise secure channel; il protocollo più utilizzato a tal proposito rimane TLS ma, di nuovo, potrebbe essere necessario stabilire con un approccio pratico se nel canale di comunicazione tra eUICC e LPA viene utilizzato TLS oppure un protocollo differente.

2.3.2 Dettagli sull'interazione in RSP

L'interazione tra le parti, nel contesto del protocollo RSP, avviene in quattro fasi distinte: profile ordering, download initialization, common handshake e profile download [4].

- **Profile ordering & download initialization**: nella prima fase, l'operatore richiede al server SM-DP+ di preparare un profilo eSIM, e il server gli restituisce dei download initialization pointer (che possono essere rappresentati ad esempio da un codice di attivazione). Nella seconda fase, invece, l'operatore consegna i download initialization pointer all'LPA in modo tale che poi sia possibile effettuare il download vero e proprio del profilo. Per questi primi due step, si possono seguire tre tipi di approcci differenti:

1. Default server approach: la figura 2.5 tratta da [4] mostra questo approccio. L'operatore (indicato con MNO - Mobile Network Operator) pre-condivide con l'eUICC l'indirizzo S del server. Quando vuole effettuare una nuova sottoscrizione e ottenere così un nuovo profilo, l'end user contatta l'operatore (messaggio 0), il quale ordina al server SM-DP+ il profilo per l'identificatore U dell'eUICC target (messaggio 1). Il server crea il nuovo profilo e lo invia all'operatore (messaggio 2), il quale notifica l'utente (messaggio 3). A tal punto, l'applicazione LPA viene avviata e, tramite un'operazione di get, recupera S dall'eUICC.
2. Activation code approach: la figura 2.6 tratta da [4] mostra questo secondo approccio. L'operatore ordina al server SM-DP+ dei profili (messaggio 1), e il server li rende disponibili con un codice di attivazione (tipicamente un codice QR) e li restituisce all'operatore (messaggio 2). Il codice di attivazione include l'indirizzo S del server, l'identificatore I_{ac} del profilo e, opzionalmente, l'OID, ovvero l'identificatore del server SM-DP+. Quando l'end user vuole effettuare una nuova sottoscrizione e ottenere così un nuovo profilo, contatta l'operatore (messaggio 0, che può essere inviato sia prima che dopo l'interazione tra operatore e SM-DP+ server appena descritta), il quale restituisce il codice di attivazione opportuno (messaggio 3).
3. SM-DS assisted approach: è un approccio analogo all'activation code, con la differenza che SM-DP+ si appoggia sui server SM-DS per comunicare con l'eUICC.

- **Common handshake**: la figura 2.7 tratta da [4] mostra i dettagli di questa fase, che coinvolge tre attori fondamentali: il server SM-DP+, l'applicazione LPA e l'eUICC. Lo stato iniziale delle tre entità è descritto qui di seguito.

  – Il server SM-DP+ è dotato di tre certificati, tutti e tre rilasciati dal CI: $Cert_{St}$ è il certificato TLS, $Cert_{Sa}$ è il certificato usato per autenticarsi all'eUICC e $Cert_{Sp}$ è il certificato che permette di rilasciare i profili eSIM. Il server possiede anche il profilo P che l'utente deve scaricare e il relativo identificatore *mnoId* dell'operatore. Infine, ha l'identificatore U dell'eUICC target, l'identificatore I_{ac} del profilo oppure entrambi.

  – L'applicazione LPA conosce l'indirizzo S del server e, opzionalmente, l'identificatore I_{ac} del profilo e l'identificatore OID del server.

  – L'eUICC ha una catena di certificati composta da $Cert_U$ e $Cert_{EUM}$.

  L'obiettivo per il server SM-DP+ e l'eUICC è quello di autenticarsi vicendevolmente all'interno di un tunnel TLS. Per iniziare questo processo, l'end user chiede all'eUICC di generare un nonce N_U (messaggio 1) e l'eUICC replica con N_U e la chiave SKI_{CI} che determina la curva ellittica che verrà usata per i certificati, le firme e l'ECDH (elliptic-curve Diffie-Hellman) key exchange (messaggio 2). L'applicazione LPA inoltra queste due informazioni al server insieme a S (messaggio 3). Il server genera così un identificatore di sessione I_t fresh e risponde all'LPA con un messaggio firmato con la propria chiave privata SK_{Sa} che comprende I_t, il nonce N_U, un altro nonce N_S e il proprio indirizzo S (messaggio 4). L'LPA verifica l'autenticità delle informazioni contenute nel digest, ad esempio controllando il valore di S, e in caso di successo inoltra il messaggio all'eUICC con l'identificatore I_{ac} del profilo (messaggio 5). Anche l'eUICC invia il proprio digest firmato con la propria chiave privata SK_U che contiene I_t, il nonce N_S, l'indirizzo S del server e I_{ac} (messaggio 6), e l'LPA inoltra tale messaggio al server (messaggio 7); è importante notare che I_{ac} è non nullo solo nell'approccio activation code. Dopodiché, il server seleziona il profilo per l'eUICC in base a I_{ac} (caso activation code) oppure in base all'identificatore U dell'eUICC presente in $Cert_U$ (caso default server). A questo punto, invia la signature di I_t firmata con SK_{Sp} (messaggio 8) e l'LPA, quando la riceve, la inoltra a sua volta all'eUICC (messaggio 9). Quest'ultimo, infine, verifica che la signature sia autentica e che i certificati $Cert_{Sa}$ e $Cert_{Sp}$ facciano riferimento allo stesso identificatore OID del server, in modo da assicurarsi che il server stesso sia effettivamente quello autorizzato.

- **Profile download**: la figura 2.8 tratta da [4] mostra i dettagli di quest'ultima fase, che non è altro che una continuazione della common handshake. I messaggi 10, 11, 12, 13 si occupano di portare a termine un key exchange basato su elliptic-curve key agreement (ECKA), tramite il quale viene calcolato uno shared secret da cui, mediante una key derivation function (KDF), saranno derivate le chiavi di sessione k (per la cifratura) e k' (per l'integrità dei dati).

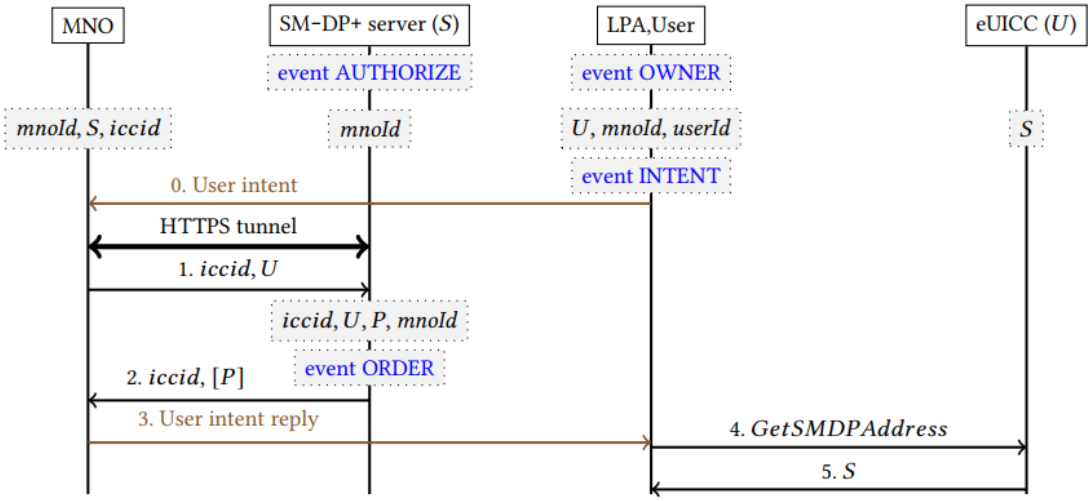

Figura 2.5: Approccio default server per le fasi di profile ordering e download initialization.

Contestualmente all'authenticated key exchange, avviene il download del profilo eSIM, in cui il server SM-DP+ invia all'LPA il profilo cifrato con la chiave k e l'identificatore *mnoId* dell'operatore (messaggio 12), dove entrambe le informazioni sono firmate singolarmente con la chiave k' mediante il meccanismo di message authentication code (MAC). Dopodiché, l'LPA mostra l'identificatore *mnoId* all'utente, che dovrà stabilire se fa riferimento all'operatore giusto: se sì, l'LPA inoltra tutte le informazioni all'eUICC (messaggio 13) il quale, dopo aver derivato le chiavi di sessione k, k', dovrà decriptare il profilo P, che risulterà finalmente essere utilizzabile. A questo punto l'eUICC elimina le chiavi k, k' e invia all'LPA un messaggio firmato con la chiave SK_U che, tra le varie cose, comprende anche un sequence number *Seq* (messaggio 14). L'LPA può decidere di inoltrare immediatamente il messaggio al server (messaggio 15) oppure di aspettare una quantità di tempo prefissata. Il server verifica che il sequence number *Seq* del messaggio è maggiore dell'ultimo sequence number precedentemente inviato dal medesimo eUICC: in caso affermativo, risponde all'LPA con HTTP OK (messaggio 16), cosicché l'LPA richieda all'eUICC di rimuovere la notifica associato al sequence number *Seq* (messaggio 17). Infine, l'eUICC replica all'LPA con un acknowledgement (messaggio 18).

In definitiva, in questa sezione è emerso come l'LPA svolga principalmente il ruolo di relay nell'interazione tra server SM-DP+ ed eUICC. Non solo: l'LPA è fondamentale anche per verificare l'autenticità del server durante la fase di common handshake e per permettere all'utente di stabilire se si sta per scaricare un profilo eSIM associato all'operatore corretto o meno. Dunque, svolge delle importanti funzioni di sicurezza e di gestione dei dati durante la comunicazione tra il server e l'eUICC.

2.3.3 Regole per la comunicazione in RSP

Qualunque comunicazione remota definita per RSP, oltre a prevedere il meccanismo di mutua autenticazione descritto in precedenza, deve far fede alle regole riportate di seguito [3].

- **Privacy dei dati**: l'eUICC, in quanto client, non deve rivelare alcuna informazione privata a un server SM-DP+ non autenticato. Inoltre, non deve generare materiale firmato prima del completamento del processo di autenticazione del server.

- **Protezione della comunicazione**: quando possibile, la comunicazione tra eUICC e server SM-DP+, oltre a essere protetta dall'integrità dei messaggi, dalla cifratura e dall'autenticazione del mittente, dovrebbe essere caratterizzata dalla proprietà di Perfect Forward Secrecy. Secondo tale proprietà, se anche una chiave a lungo termine viene compromessa, le chiavi di sessione generate a partire da essa rimangono comunque riservate.

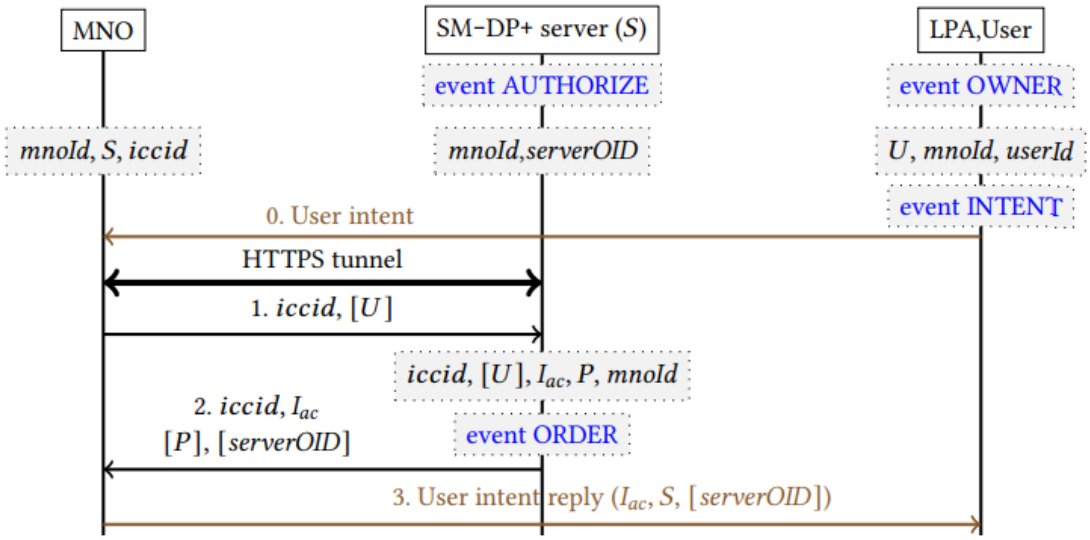

Figura 2.6: Approccio activation code per le fasi di profile ordering e download initialization.

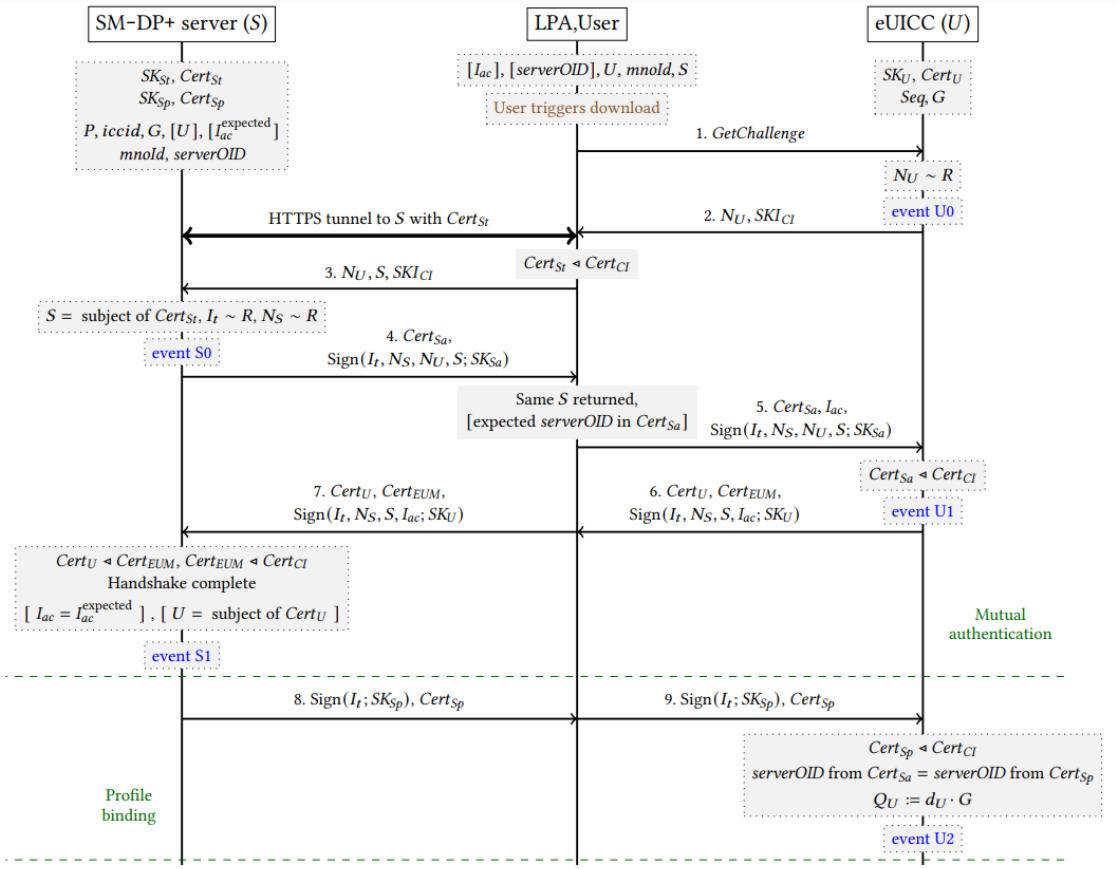

Figura 2.7: Fase di common handshake.

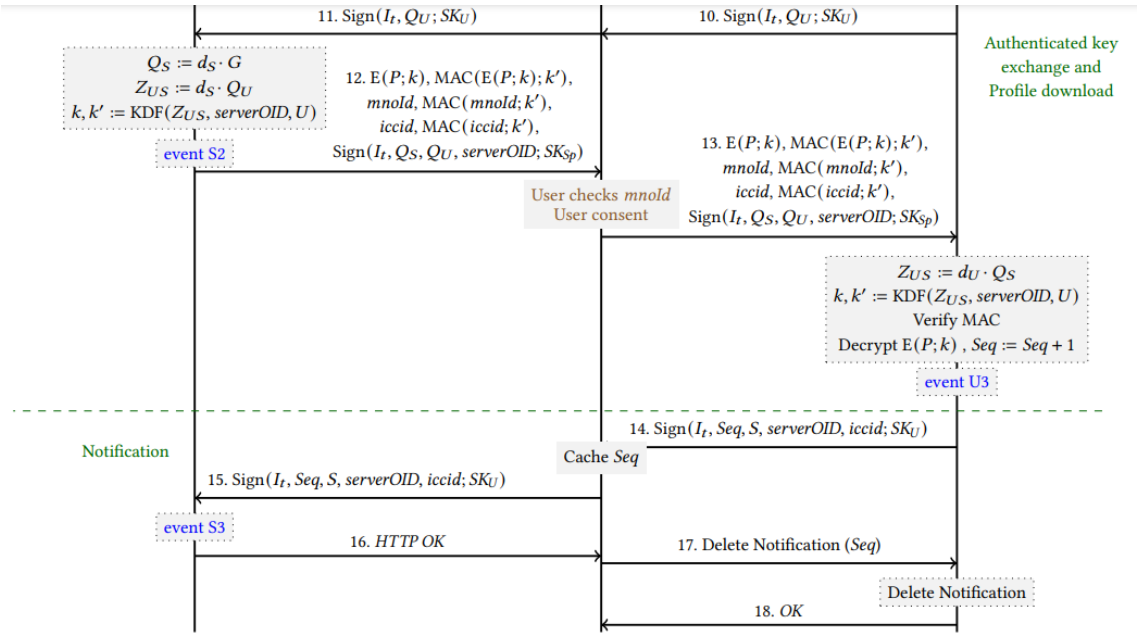

Figura 2.8: Fase di profile download.

- **Autorizzazione**: il server SM-DP+ deve sempre verificare che il client che ha inviato una richiesta sia effettivamente autorizzato prima di far partire l'esecuzione della funzione desiderata.

2.4 Chiavi crittografiche e certificati

2.4.1 Chiavi crittografiche

Le chiavi utilizzate dai principali componenti che partecipano all'interazione data dal protocollo RSP hanno tutte un nome di tipo ¡XX¿.¡YY¿.¡ZZ¿ [3], dove:

- <**XX**>: indica la natura della chiave (i.e. chiave pubblica PK, chiave privata SK, chiave pubblica one-time otPK, chiave privata one-time otSK).
- <**YY**>: indica il proprietario della chiave.
- <**ZZ**>: indica il tipo di utilizzo della chiave (i.e. digital signature SIG, key agreement KA, TLS).

Le chiavi di maggiore rilievo, comunque sia, sono riportate nella tabella 2.2 tratta da [8].

2.4.2 Certificati

I certificati propri dei principali componenti che partecipano all'interazione data dal protocollo RSP sono riportate nella tabella 2.3 tratta da [3].
La figura 2.9 tratta da [3] definisce uno schema riassuntivo della catena di certificati definita dalla Public Key Infrastructure (PKI) di RSP. All'interno della PKI, il Certificate Issuer di GSMA (CI) è la Root Certification Authority del servizio RSP e, di conseguenza, rappresenta il nodo radice della catena. La figura 2.9, inoltre, rimarca bene come tutti i certificati siano rilasciati dal CI, fatta eccezione di CERT.EUICC.ECDSA che, invece, viene rilasciato dall'EUM. Tutti i certificati rilasciati direttamente dal CI possono essere revocati in qualunque momento, in particolar modo se le entità corrispondenti (CI, EUM, SM-DP+, SM-DS) vengono compromesse. D'altra parte, i certificati eUICC (CERT.EUICC.ECDSA) non vengono revocati in modo individuale: di fatto, è difficile che un singolo eUICC venga compromesso. Piuttosto, è più verosimile che un modello eUICC o un intero batch di produzione di eUICC venga dichiarato come compromesso; quando ciò avviene, quello che si fa è revocare direttamente il certificato EUM (CERT.EUM.ECDSA) associato a quel modello o batch di produzione di eUICC [3].

Tabella 2.2: Chiavi crittografiche in RSP

Nome	Descrizione
PK.EUICC.SIG	Chiave pubblica dell'eUICC usata per verificare le signature dell'eUICC. È inclusa nel certificato CERT.EUICC.SIG.
SK.EUICC.SIG	Chiave privata dell'eUICC usata per generare le signature. Corrisponde alla chiave SK_U citata nella sottosezione 2.3.2.
PK.DPauth.SIG	Chiave pubblica del server SM-DP+ usata per verificare le signature del server. È inclusa nel certificato CERT.DPauth.SIG.
SK.DPauth.SIG	Chiave privata del server SM-DP+ usata per generare le signature per autenticarsi all'eUICC. Corrisponde alla chiave SK_{Sa} citata nella sottosezione 2.3.2.
PK.DPpb.SIG	Chiave pubblica del server SM-DP+ usata per verificare le signature del server comprese nel BPP. È inclusa nel certificato CERT.DPpb.ECDSA.
SK.DPpb.SIG	Chiave privata del server SM-DP+ usata per generare le signature per il binding dei profili. Corrisponde alla chiave SK_{Sp} citata nella sottosezione 2.3.2.
PK.DSauth.SIG	Chiave pubblica del server SM-DS usata per verificare le signature di SM-DS. È inclusa nel certificato CERT.DSauth.SIG.
SK.DSauth.SIG	Chiave privata del server SM-DS usata per generare le signature per autenticarsi all'eUICC.
PK.EUM.SIG	Chiave pubblica dell'EUM usata per verificare i certificati degli eUICC. È inclusa nel certificato CERT.EUM.SIG.
SK.EUM.SIG	Chiave privata dell'EUM usata per firmare i certificati degli eUICC.
PK.CI.SIG	Chiave pubblica del CI usata per verificare i certificati dell'EUM dei server SM-DS e del server SM-DP+.
SK.CI.SIG	Chiave privata del CI usata per firmare i certificati dell'EUM dei server SM-DS e del server SM-DP+.
otPK.EUICC.KA	Chiave pubblica one-time dell'eUICC usata per il key agreement.
otSK.EUICC.KA	Chiave privata one-time dell'eUICC usata per il key agreement.
otPK.DP.KA	Chiave pubblica one-time del server SM-DP+ usata per il key agreement.
otSK.DP.KA	Chiave privata one-time del server SM-DP+ usata per il key agreement.
PK.DP.TLS	Chiave pubblica del server SM-DP+ usata per verificare le signature TLS del server. È inclusa nel certificato CERT.DP.TLS.
SK.DP.TLS	Chiave privata del server SM-DP+ usata per generare le signature per autenticarsi all'LPA. Corrisponde alla chiave SK_{St} citata nella sottosezione 2.3.2.
PK.DS.TLS	Chiave pubblica del server SM-DS usata per verificare le signature TLS di SM-DS. È inclusa nel certificato CERT.DS.TLS.
SK.DS.TLS	Chiave privata del server SM-DS usata per generare le signature per autenticarsi all'LPA.

Il CI fornisce una Certificate Revocation List (CRL), che è la lista dei certificati revocati tra tutti i certificati non scaduti che erano stati rilasciati da quello stesso CI. Ciascun CI, per giunta, deve pubblicare la propria CRL sia periodicamente, sia ogni volta che viene revocato un particolare certificato [3].
In realtà, i certificati relativi alla PKI di RSP di cui si è discusso finora non sono gli unici certificati utilizzati per effettuare il deployment dei profili eSIM: esiste anche un certificato per firmare l'applicazione LPA e un certificato da inserire in ciascun profilo eSIM da distribuire all'end user. Dove entrano in gioco tali certificati? Con riferimento alla guida di Android per le API e per l'implementazione del deployment dei profili eSIM [7], l'interazione tra un'applicazione LPA e l'interfaccia all'eUICC (legata al componente EuiccManager in [7]) può avvenire solo se l'applicazione dispone dei privilegi dell'operatore. Di norma, tali privilegi sono conferiti all'applicazione se il certificato usato per firmarla coincide col certificato presente nel profilo fornito da SM-DP+.

Tabella 2.3: Certificati in RSP

Nome	Descrizione	Note
CERT.CI.SIG	Certificato GSMA CI	Viene firmato e rilasciato da se stesso.
CERT.CISubCA.SIG	Certificato GSMA CI subordinato	Se esistente, viene firmato e rilasciato dal CI root.
CERT.EUM.SIG	Certificato EUM	Viene firmato e rilasciato dal CI root. Corrisponde al certificato $Cert_{EUM}$ citato nella sottosezione 2.3.2.
CERT.EUMSubCA.SIG	Certificato EUM subordinato	Se esistente, viene firmato e rilasciato dall'EUM root.
CERT.DPSubCA.SIG	Certificato SM-DP+ subordinato	Viene firmato e rilasciato dal CI root.
CERT.DPauth.SIG	Certificato SM-DP+ per autenticarsi all'eUICC	Viene firmato e rilasciato dal SM-DP+ subordinato. Corrisponde al certificato $Cert_{Sa}$ citato nella sottosezione 2.3.2.
CERT.DPpb.SIG	Certificato SM-DP+ per rilasciare e firmare i profili eSIM	Viene firmato e rilasciato dal SM-DP+ subordinato. Corrisponde al certificato $Cert_{Sp}$ citato nella sottosezione 2.3.2.
CERT.DP.TLS	Certificato TLS di SM-DP+	Viene firmato e rilasciato dal SM-DP+ subordinato. Corrisponde al certificato $Cert_{St}$ citato nella sottosezione 2.3.2.
CERT.DSSubCA.SIG	Certificato SM-DS subordinato	Viene firmato e rilasciato dal CI root.
CERT.DSauth.SIG	Certificato SM-DS	Viene firmato e rilasciato dal SM-DS subordinato.
CERT.DS.TLS	Certificato TLS di SM-DS	Viene firmato e rilasciato dal SM-DS subordinato.
CERT.EUICC.SIG	Certificato eUICC	Viene firmato e rilasciato dall'EUM root.

2.5 Ciclo di vita dei profili in SM-DP+

La tabella 2.4 tratta da [3][8] fornisce un elenco degli stati in cui ciascun profilo eSIM può trovarsi nell'arco della sua esistenza.

Tabella 2.4: Stati dei profili eSIM

Nome	Descrizione
Available	Il profilo è disponibile nell'inventory del server SM-DP+.
Allocated	Il profilo è riservato per il download senza essere linkato a un EID (eUICC ID).
Linked	Il profilo è riservato per il download ed è linkato a un EID.
Confirmed	Il profilo è riservato per il download (che sia esso linkato o non linkato a un EID) col matching ID (i.e. il codice che identifica la transazione di download) e il codice di conferma (i.e. il codice che deve essere inserito dall'end user), se richiesti.
Released	Il profilo è pronto per il download e l'installazione dopo che l'operatore ha effettuato la configurazione di rete.
Downloaded	Il profilo è stato consegnato all'LPA (i.e. è stato scaricato).
Installed	Il profilo è stato installato sull'eUICC con successo.
Error	Il profilo non è stato installato a causa di una condizione di errore.
Unavailable	Il profilo non può essere più riutilizzato da SM-DP+.

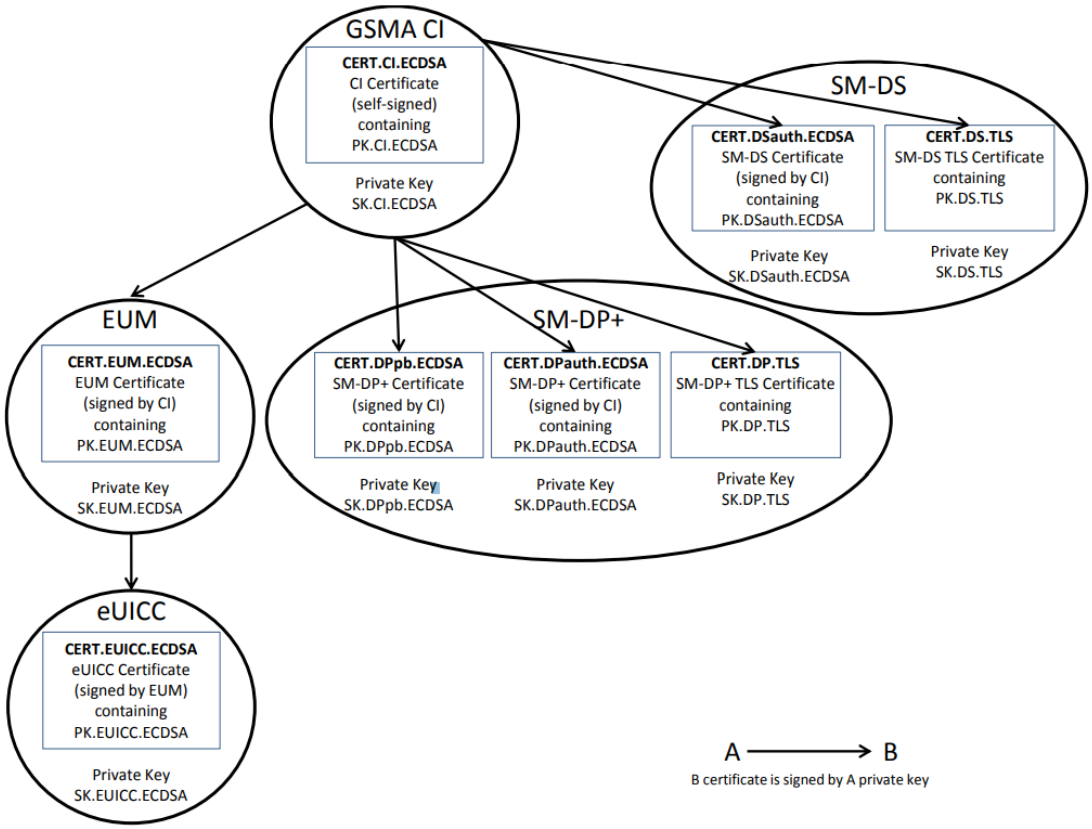

Figura 2.9: Catena di certificati definita dalla PKI di RSP.

Nelle figure 2.10, 2.11 tratte da [3][8] sono mostrati due diagrammi a stati finiti che illustrano per bene il ciclo di vita dei profili in SM-DP+.
Con riferimento alla figura 2.10, a partire dallo stato Available:

- Si passa allo stato Allocated se si effettua l'ordine di download senza specificare l'EID.
- Si passa allo stato Linked se si effettua l'ordine di download specificando l'EID.

A partire dallo stato Allocated:

- Si passa allo stato Confirmed se si conferma l'ordine di download con releaseFlag=false.
- Si passa allo stato Released se si conferma l'ordine di download con releaseFlag=true.

A partire dallo stato Linked:

- Si passa allo stato Confirmed se si conferma l'ordine di download con releaseFlag=false.
- Si passa allo stato Released se si conferma l'ordine di download con releaseFlag=true.

A partire dallo stato Confirmed:

- Si passa allo stato Released se si effettua il rilascio del profilo in modo tale che sia effettivamente pronto per il download e l'installazione.

A partire dallo stato Released:

- Si passa allo stato Downloaded se il profilo viene consegnato all'LPA con successo.
- Si passa allo stato Error se si ha un errore nel consegnare il profilo all'LPA.

A partire dallo stato Downloaded:

- Si passa allo stato Installed se il profilo viene installato sull'eUICC con successo.

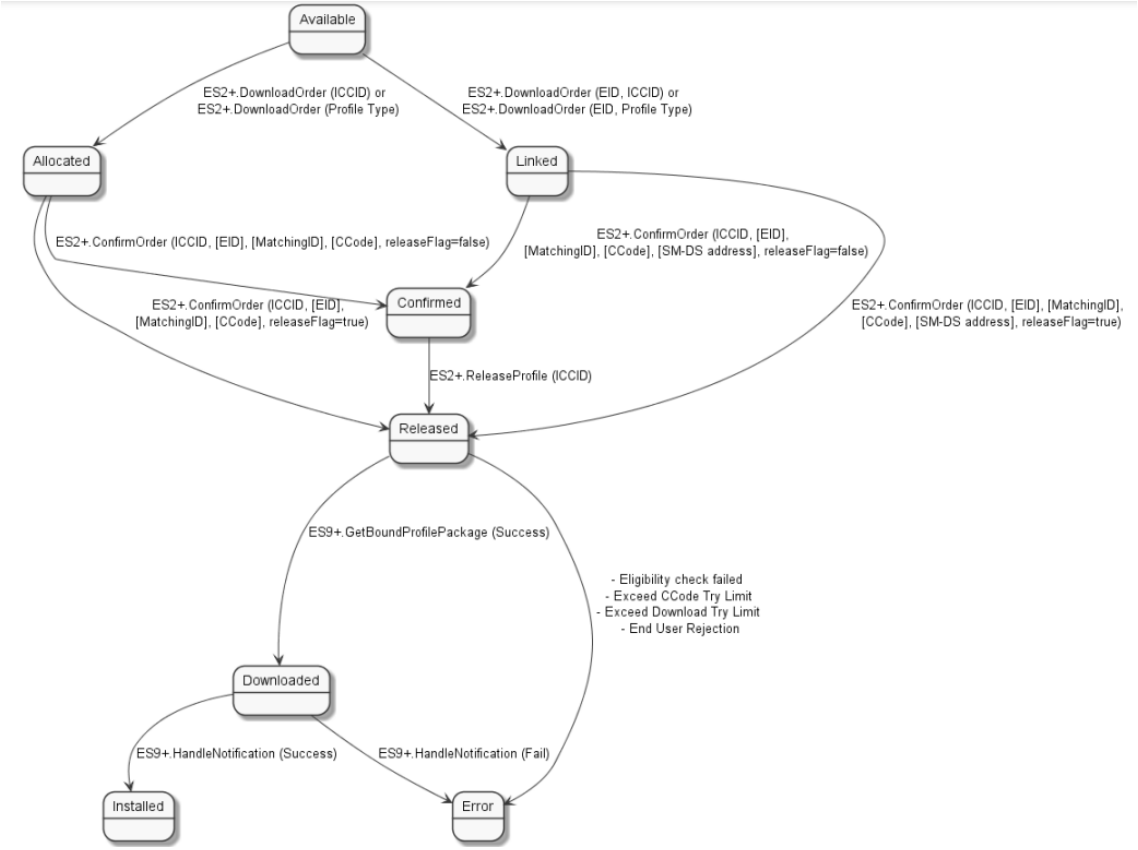

Figura 2.10: Primo diagramma a stati per i profili eSIM.

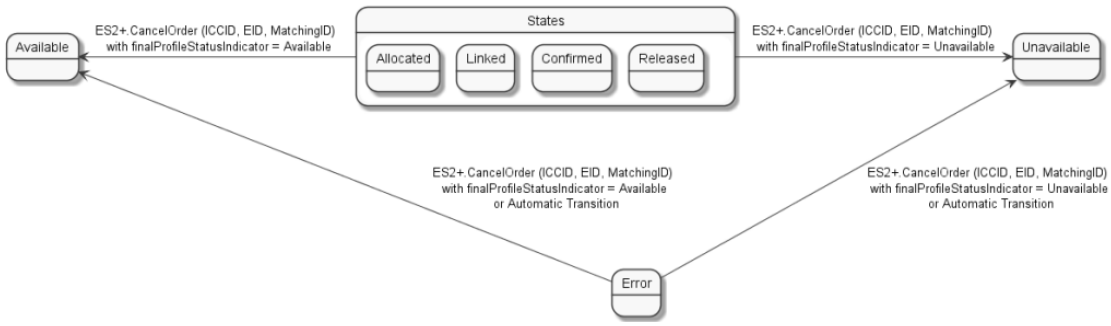

Figura 2.11: Secondo diagramma a stati per i profili eSIM.

- Si passa allo stato Error se si ha un errore nell'installare il profilo sull'eUICC.

Con riferimento alla figura 2.11, a partire dagli stati Allocated / Linked / Confirmed / Released:

- Si torna allo stato Available se l'ordine di download viene annullato con finalProfileStatusIndicator=Available.
- Si passa allo stato Unavailable se l'ordine di download viene annullato con finalProfileStatusIndicator=Unavailable.

A partire dallo stato Error:

- Si torna allo stato Available in modo automatico oppure se l'ordine di download viene annullato con finalProfileStatusIndicator=Available.
- Si passa allo stato Unavailable in modo automatico oppure se l'ordine di download viene annullato con finalProfileStatusIndicator=Unavailable.

Capitolo 3

Sicurezza dell'eSIM a run-time

[TODO]

Capitolo 4

Sicurezza dell'eSIM a boot-time

4.1 Funzionamento del boot dell'eSIM

[TODO]

4.2 Potenziali vulnerabilità

[TODO]

4.3 Prove sperimentali

[TODO]

Capitolo 5

Conclusione

[TODO]

Bibliografia

[1] Corcom. *"Telefonia mobile, cosa sono le eSim? E perché sono più sicure?"*, 2023. https://corrierecomunicazioni.it/telco/telefonia-mobile-cosa-sono-le-esim-e-perche-sono-piu-sicure/.

[2] GSM Association. *"The what and how of Remote SIM Provisioning"*, 2018. https://gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf.

[3] GSM Association. *"RSP Technical Specification Version 3.0"*, 2022. https://gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf.

[4] Abu Shohel Ahmed, Aleksi Peltonen, Mohit Sethi, and Tuomas Aura. *"Security Analysis of the Consumer Remote SIM Provisioning Protocol"*, 2022. https://arxiv.org/pdf/2211.15323.pdf.

[5] IETF. *"The Transport Layer Security (TLS) Protocol Version 1.2"*, 2008. https://rfc-editor.org/rfc/rfc5246.

[6] IETF. *"The Transport Layer Security (TLS) Protocol Version 1.3"*, 2018. https://rfc-editor.org/rfc/rfc8446.

[7] Team di Android. *"Implementing eSIM"*, 2023. https://source.android.com/docs/core/connect/esim-overview.

[8] GSM Association. *"RSP Technical Specification Version 2.0"*, 2016. https://gsma.com/newsroom/wp-content/uploads/SGP.22_v2.0.pdf.

Ringraziamenti

[TODO]