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

L'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 del 2023 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 dell'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 nei 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 dell'eSIM e sul protocollo di comunicazione tra eUICC, LPA e server SM-DP+, 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). Nel capitolo 5 verranno mostrati i risultati ottenuti. Infine, nel capitolo 6 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 l'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 memorizzati su una SIM card fisica. 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 del 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 un secondo profilo eSIM, gli è sufficiente ripetere i medesimi passaggi appena descritti, 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: nota anche come eSIM CA RootCA, 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 [3][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).
    - **SM-DS** = Subscription Manager Discovery Server: è il componente che consente a SM-DP+ di raggiungere l'eUICC senza dover sapere a quale rete il dispositivo è connesso.

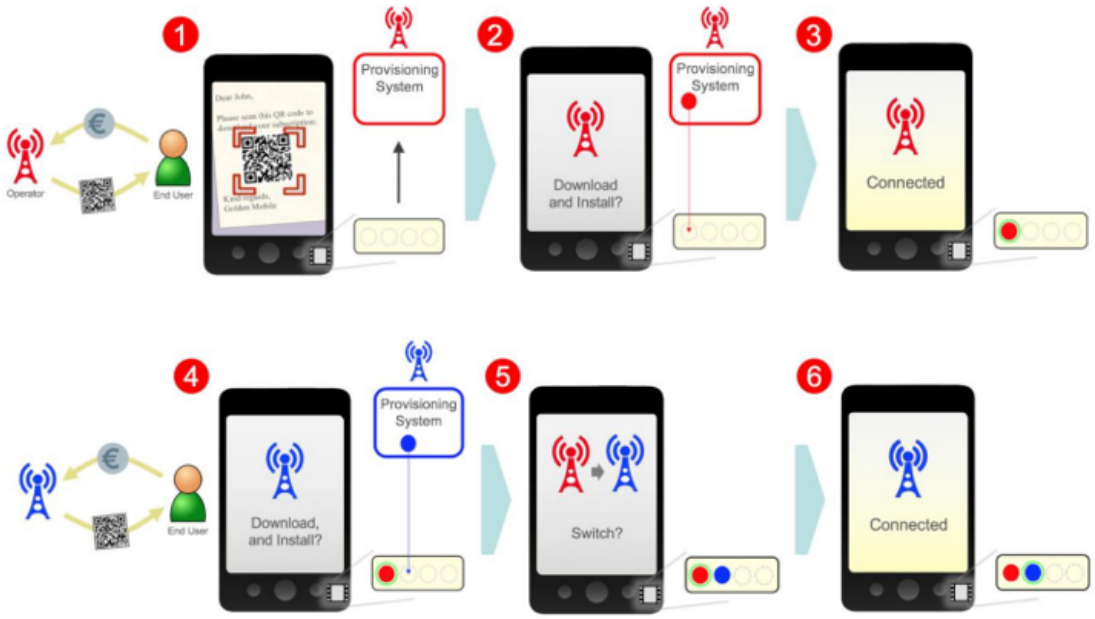

Figura 2.1: Comunicazione tra end user e operatore nel contesto del Remote SIM Provisioning.

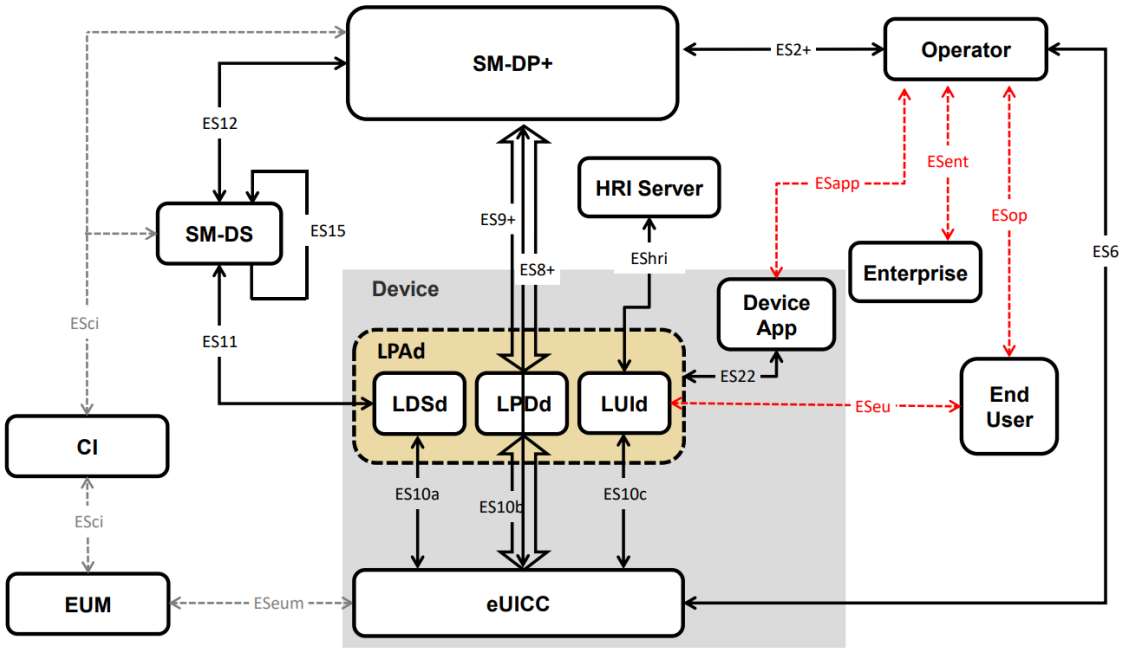

Figura 2.2: Architettura di RSP nel caso di LPA non embeddato nell'eUICC.

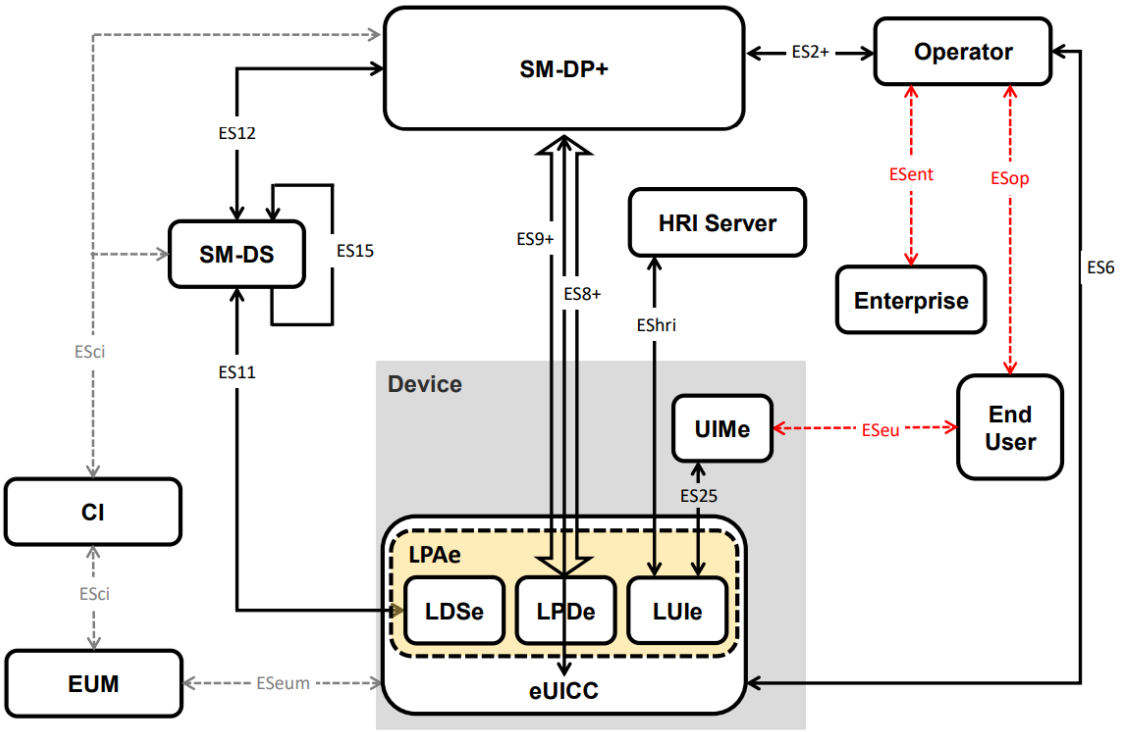

Figura 2.3: Architettura di RSP nel caso di LPA embeddato nell'eUICC.

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; il Protected Profile Package (PPP) è un pacchetto di dati protetto da alcuni meccanismi di sicurezza, come l'autenticazione e/o la crittografia; 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.

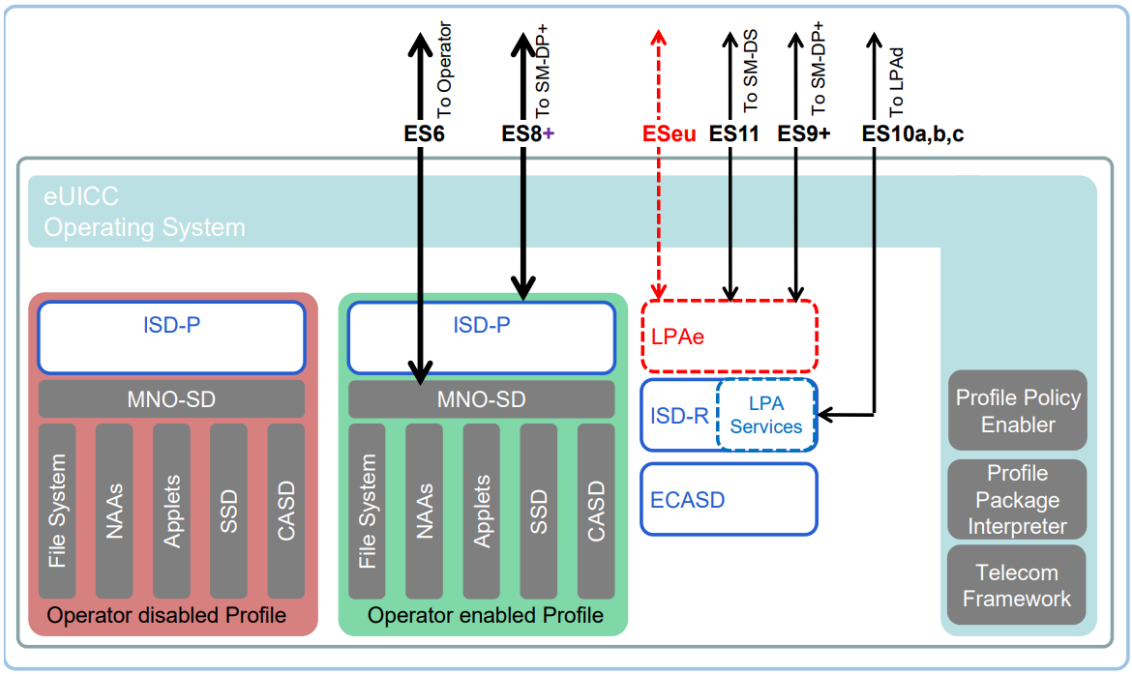

Figura 2.4: Architettura dell'eUICC.

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 (i.e. chiavi, certificati) 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 usando il formato interno dell'eUICC.
- **Profile Policy Enabler** = componente che verifica che 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. Contiene un unico ECASD (eUICC Controlling Authority Security Domain).
3. Supporta SHA-1.
4. Supporta Milenage, che è un set di funzioni di autenticazione e di generazione di chiavi.
5. Tutte le funzioni crittografiche devono essere resistenti al tampering e agli attacchi side-channel.

2.3 Chiavi crittografiche e certificati

2.3.1 Chiavi crittografiche

I principali attori che interagiscono nel protocollo RSP sono l'eUICC, l'LPA e il server SM-DP+. Le chiavi utilizzate da loro 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 l'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 [5].

2.3.2 Certificati

I certificati propri dei principali componenti che partecipano all'interazione data dal protocollo RSP sono riportati nella tabella 2.3 tratta da [3].

La figura 2.5 tratta da [5] definisce uno schema riassuntivo della struttura originale della catena di certificati definita dalla Public Key Infrastructure (PKI) di RSP.
Attualmente, invece, la struttura della certificate chain è più complessa e introduce molteplici varianti differenti (i.e. presenza o meno di GSMA CI subordinati, presenza o meno di EUM subordinati, presenza o meno di SM-DP+ intermediari, presenza o meno di SM-DS intermediari). Di seguito, per semplicità, più porzioni distinte della catena verranno analizzate separatamente.

- Porzione della catena comprendente il CI, l'EUM e l'eUICC: è riportata nella figura 2.6 tratta da [3] e prevede quattro varianti differenti.
  - **Variante O (originale)**: il CI root rilascia certificati per l'EUM root, il quale rilascia a sua volta certificati per l'eUICC.
  - **Variante A**: il CI root rilascia certificati per l'EUM root; l'EUM root rilascia certificati per l'EUM subordinato; l'EUM subordinato, infine, rilascia certificati per l'eUICC.
  - **Variante B**: il CI root rilascia certificati per il CI subordinato; il CI subordinato rilascia certificati per l'EUM root; l'EUM root, infine, rilascia certificati per l'eUICC.
  - **Variante C**: il CI root rilascia certificati per il CI subordinato; il CI subordinato rilascia certificati per l'EUM root; l'EUM root rilascia certificati per l'EUM subordinato; l'EUM subordinato, infine, rilascia certificati per l'eUICC.

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.
PK.DPauth.SIG	Chiave pubblica del server SM-DP+ usata per verificare le signature del server in fase di autenticazione. 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.
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.SIG.
SK.DPpb.SIG	Chiave privata del server SM-DP+ usata per generare le signature per il binding dei profili.
PK.DSauth.SIG	Chiave pubblica del server SM-DS usata per verificare le signature di SM-DS in fase di autenticazione. 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 TLS per autenticarsi all'LPA.
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 TLS per autenticarsi all'LPA.

- Porzione della catena comprendente il CI e i certificati di tipo SIG di SM-DP+ e SM-DS: è riportata nella figura 2.7 tratta da [3] e prevede quattro varianti differenti.
  - **Variante O (originale)**: il CI root rilascia direttamente i certificati CERT.DPauth.SIG, CERT.DPpb.SIG, CERT.DSauth.SIG.
  - **Variante A**: il CI root rilascia certificati per l'SM-DP+ intermediario e l'SM-DS intermediario; l'SM-DP+ intermediario rilascia i certificati CERT.DPauth.SIG, CERT.DPpb.SIG; l'SM-DS intermediario rilascia il certificato CERT.DSauth.SIG.
  - **Variante B**: il CI root rilascia certificati per il CI subordinato, il quale rilascia a sua volta i certificati CERT.DPauth.SIG, CERT.DPpb.SIG, CERT.DSauth.SIG.
  - **Variante C**: il CI root rilascia certificati per il CI subordinato; il CI subordinato rilascia certificati per l'SM-DP+ intermediario e l'SM-DS intermediario; l'SM-DP+ intermediario rilascia i certificati CERT.DPauth.SIG, CERT.DPpb.SIG; l'SM-DS intermediario rilascia il certificato CERT.DSauth.SIG.
- Porzione della catena comprendente il CI e i certificati TLS di SM-DP+ e SM-DS: è riportata nella figura 2.8 tratta da [3] e prevede quattro varianti differenti.

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 esiste, viene firmato e rilasciato dal CI root.
CERT.EUM.SIG	Certificato EUM	Viene firmato e rilasciato dal CI (root o subordinato).
CERT.EUMSubCA.SIG	Certificato EUM subordinato	Se esiste, viene firmato e rilasciato dall'EUM root.
CERT.DPSubCA.SIG	Certificato SM-DP+ intermediario	Viene firmato e rilasciato dal CI (root o subordinato).
CERT.DPauth.SIG	Certificato SM-DP+ per autenticarsi all'eUICC	Viene firmato e rilasciato dal SM-DP+ intermediario o dal CI (root o subordinato).
CERT.DPpb.SIG	Certificato SM-DP+ per rilasciare e firmare i profili eSIM	Viene firmato e rilasciato dal SM-DP+ intermediario o dal CI (root o subordinato).
CERT.DP.TLS	Certificato TLS di SM-DP+	Viene firmato e rilasciato dal SM-DP+ intermediario o dal CI (root o subordinato).
CERT.DSSubCA.SIG	Certificato SM-DS intermediario	Viene firmato e rilasciato dal CI (root o subordinato).
CERT.DSauth.SIG	Certificato SM-DS	Viene firmato e rilasciato dal SM-DS intermediario o dal CI (root o subordinato).
CERT.DS.TLS	Certificato TLS di SM-DS	Viene firmato e rilasciato dal SM-DS intermediario o dal CI (root o subordinato).
CERT.EUICC.SIG	Certificato eUICC	Viene firmato e rilasciato dall'EUM (root o subordinato).
CERT.CA.SIG	Certificato di una qualunque CA pubblica	Può firmare e rilasciare certificati TLS.

  - **Variante O (originale)**: il CI root rilascia direttamente i certificati CERT.DP.TLS, CERT.DS.TLS.
  - **Variante A**: il CI root rilascia i certificati per l'SM-DP+ intermediario e l'SM-DS intermediario; l'SM-DP+ intermediario rilascia il certificato CERT.DP.TLS; l'SM-DS intermediario rilascia il certificato CERT.DS.TLS.
  - **Variante B**: il CI root rilascia certificati per il CI subordinato, il quale rilascia a sua volta i certificati CERT.DP.TLS, CERT.DS.TLS.
  - **Variante C**: il CI root rilascia certificati per il CI subordinato; il CI subordinato rilascia certificati per l'SM-DP+ intermediario e l'SM-DS intermediario; l'SM-DP+ intermediario rilascia il certificato CERT.DP.TLS; l'SM-DS intermediario rilascia il certificato CERT.DS.TLS.

Per quanto riguarda i certificati TLS, al posto del CI, può esserci come root qualunque CA pubblica, come mostrato nella figura 2.9 tratta da [3]. Anche con questa soluzione esistono diverse varianti.

- **Prima variante OO (originale)**: la CA pubblica root rilascia direttamente i certificati CERT.DP.TLS, CERT.DS.TLS.
- **Seconda variante OO**: la CA pubblica root rilascia certificati per la CA pubblica subordinata, la quale rilascia a sua volta i certificati CERT.DP.TLS, CERT.DS.TLS.
- **Prima variante AA**: la CA pubblica rilascia certificati per l'SM-DP+ intermediario e l'SM-DS intermediario; l'SM-DP+ intermediario rilascia il certificato CERT.DP.TLS; l'SM-DS intermediario rilascia il certificato CERT.DS.TLS.

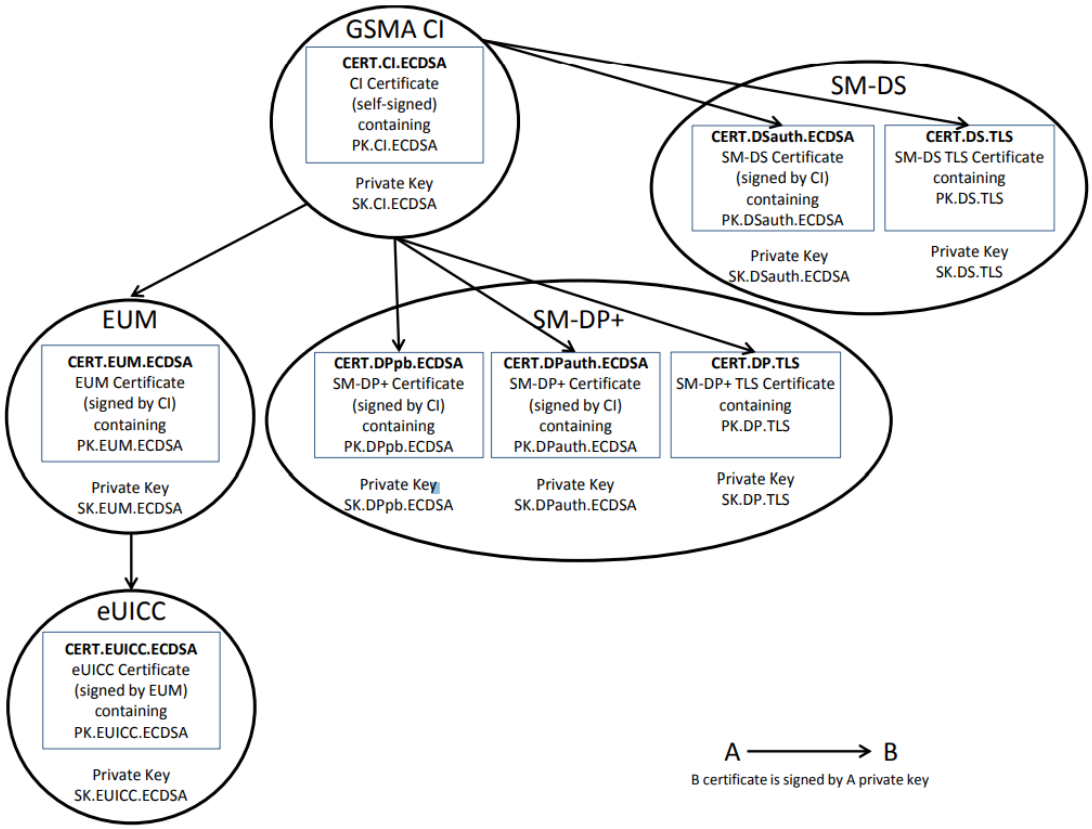

Figura 2.5: Catena di certificati definita originariamente dalla PKI di RSP.

- **Seconda variante AA**: la CA pubblica rilascia certificati per la CA pubblica subordinata; la CA pubblica subordinata rilascia certificati per l'SM-DP+ intermediario e l'SM-DS intermediario; l'SM-DP+ intermediario rilascia il certificato CERT.DP.TLS; l'SM-DS intermediario rilascia il certificato CERT.DS.TLS.

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. Inoltre, tutti i certificati possono essere rilasciati direttamente dal CI (root o subordinato), fatta eccezione di CERT.EUICC.SIG che, invece, viene rilasciato dall'EUM (root o subordinato). Tutti i certificati che possono essere rilasciati direttamente dal CI hanno la possibilità di 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.SIG) 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.SIG) associato a quel modello o batch di produzione di eUICC [3].
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 [6], l'interazione tra un'applicazione LPA e l'interfaccia all'eUICC (legata al componente EuiccManager in [6]) 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+.

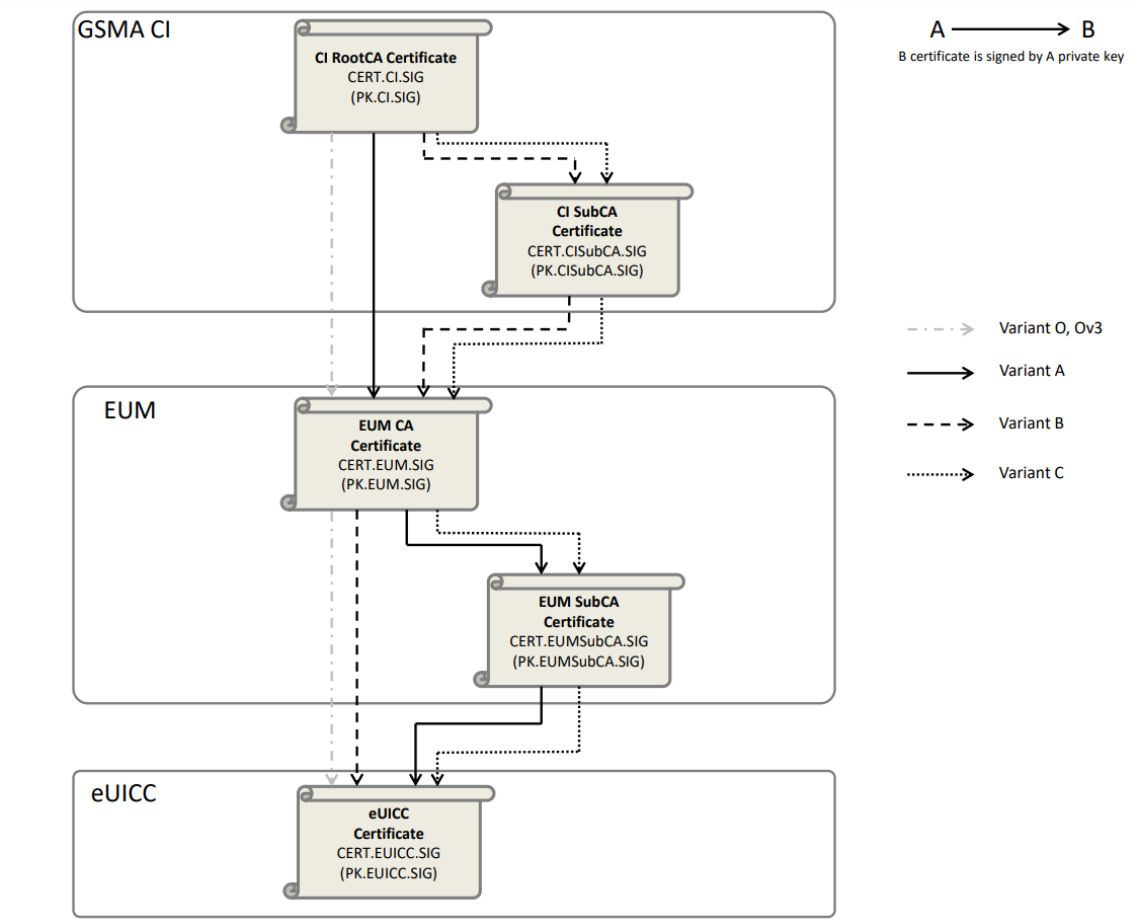

Figura 2.6: Prima porzione dell'attuale catena di certificati definita dalla PKI di RSP.

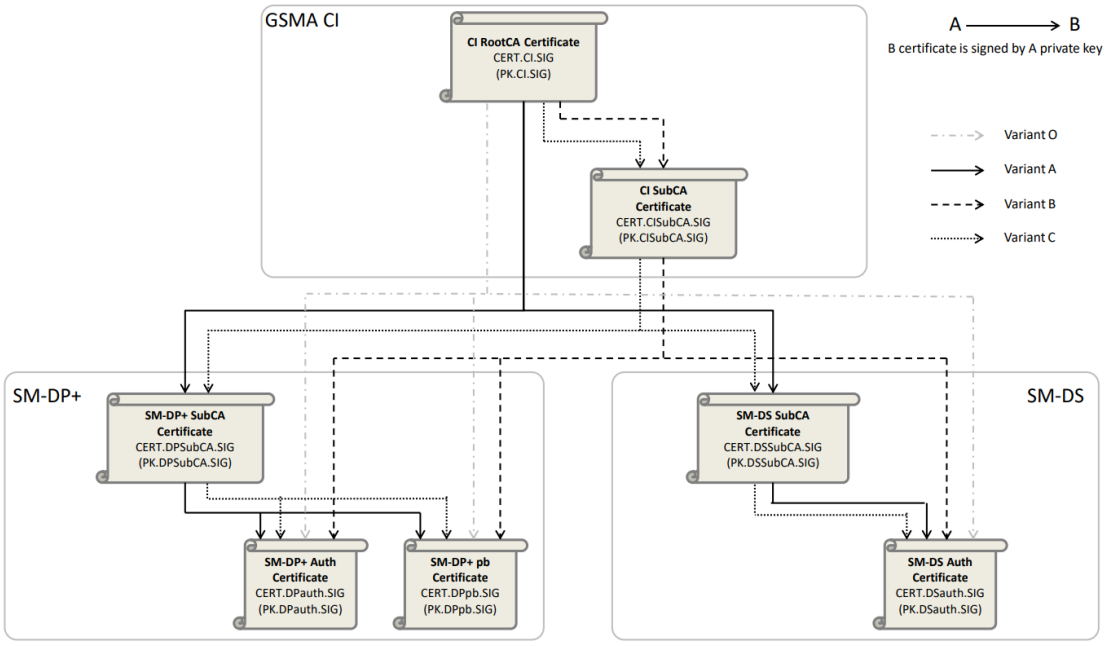

Figura 2.7: Seconda porzione dell'attuale catena di certificati definita dalla PKI di RSP.

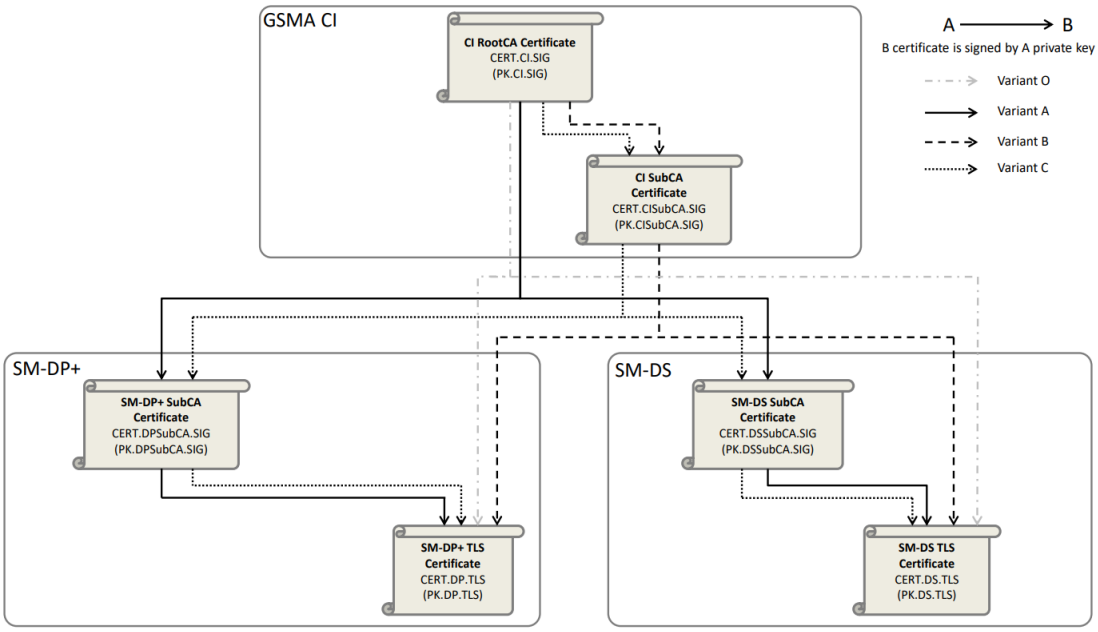

Figura 2.8: Terza porzione dell'attuale catena di certificati definita dalla PKI di RSP.

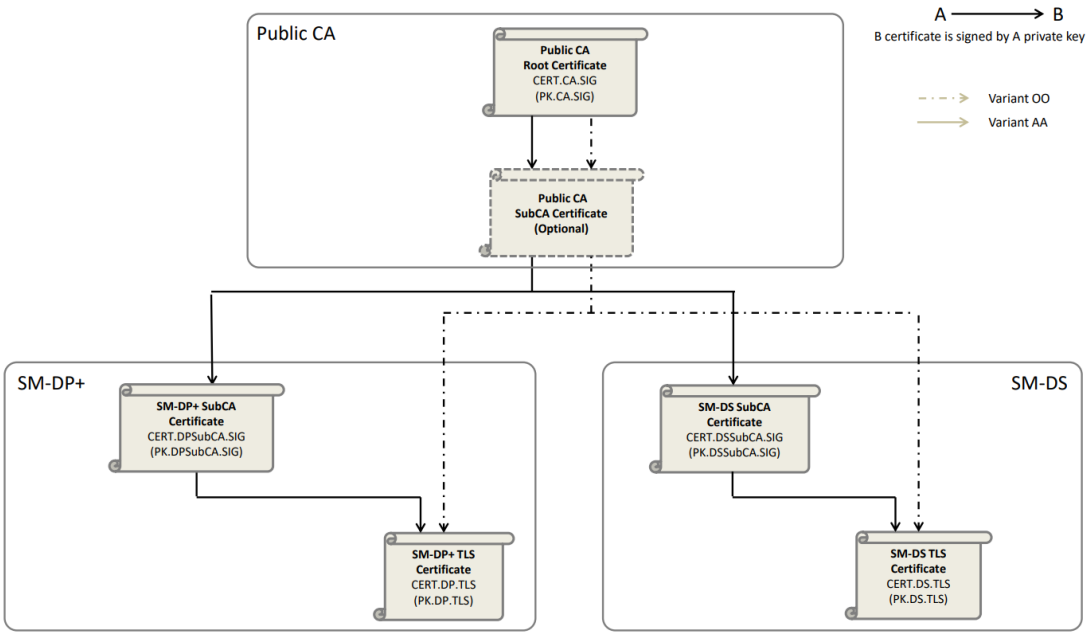

Figura 2.9: Quarta porzione dell'attuale catena di certificati definita dalla PKI di RSP.

2.3.3 Aggiornamento delle chiavi pubbliche nell'eUICC

L'eUICC può fornire un meccanismo per aggiornare il set di chiavi pubbliche memorizzate nell'ECASD dell'eUICC (che sono chiavi a lunga durata). L'implementazione di tale meccanismo è lasciata all'EUM o al produttore del dispositivo mobile e, stando alla guida ufficiale di GSMA [3], deve essere sicura. Tuttavia, nel momento in cui un'implementazione è affidata a terze parti, nessuno può garantire con certezza che la prescrizione sulla sicurezza venga rispettata, poiché non vengono seguite delle linee guida standard e consolidate. Di conseguenza, nei capitoli successivi potrebbe essere utile approfondire mediante degli esperimenti pratici il funzionamento dell'aggiornamento del set di chiavi poste nell'ECASD e stabilire così se esiste qualche vulnerabilità da sfruttare a vantaggio di un attaccante.

Contenuto dell'ECASD

Tutti gli eUICC devono avere un ECASD che contenga [3]:

- la chiave privata dell'eUICC (SK.EUICC.SIG);
- il certificato dell'eUICC (CERT.EUICC.SIG) contenente la chiave PK.EUICC.SIG, che è la chiave pubblica dell'eUICC;
- la chiave pubblica del CI root (PK.CI.SIG);
- il certificato dell'EUM (CERT.EUM.SIG) e, opzionalmente, il certificato degli EUM subordinati (CERT.EUMSubCA.SIG);
- un keyset dell'EUM per il rinnovo di chiavi e certificati.

Quando avviene l'aggiornamento delle chiavi?

La necessità di rinnovare le chiavi contenute nell'ECASD può presentarsi in due casi [3].

- L'applicazione LPA ha determinato che il Public Key identificator (i.e. la rappresentazione in esadecimale dell'identificatore della chiave pubblica) del CI non è supportato dall'eUICC.
- Durante la procedura di Common Mutual Authentication, il server SM-DP+ ha restituito un certificato CERT.DPauth.SIG che ha come parent un Root Certificate non supportato dall'eUICC.

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

2.4.1 Sicurezza TLS

Il protocollo TLS, la cui versione 1.2 è definita in RFC 5246 [7] e la cui versione 1.3 è definita in RFC 8446 [8], è utilizzato per proteggere il traffico sulle interfacce ES2+ (tra server SM-DP+ e operatore) e ES9+ (tra server SM-DP+ e LPA), dove è prevista la mutua autenticazione tra le parti. 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.

2.4.2 Regole per la comunicazione in RSP

Qualunque comunicazione remota definita per RSP deve far fede alle regole riportate di seguito [3].

- **Mutua autenticazione tra eUICC e server SM-DP+**: il server deve essere autenticato per primo da parte dell'eUICC, dove il processo di autenticazione deve includere la verifica di una catena di certificati del server. D'altra parte, l'eUICC deve essere autenticato in un secondo momento da parte del server, dove il processo di autenticazione, di nuovo, deve includere la verifica di una catena di certificati dell'eUICC; l'autenticazione dell'eUICC non si applica all'LPA.
- **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.
- **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.

2.4.3 Step dell'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, 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 2.10 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 2.11 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**: questa fase, nota anche come Common Mutual Authentication, coinvolge tre attori fondamentali: il server SM-DP+, l'applicazione LPA e l'eUICC. I relativi dettagli sono riportati nella sezione 2.4.5.

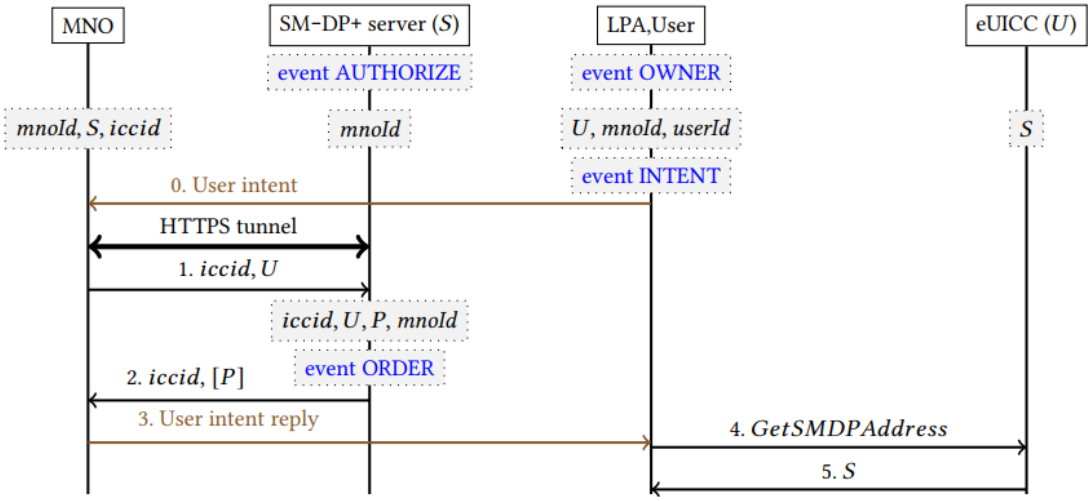

Figura 2.10: Approccio default server per le fasi di profile ordering e download initialization.

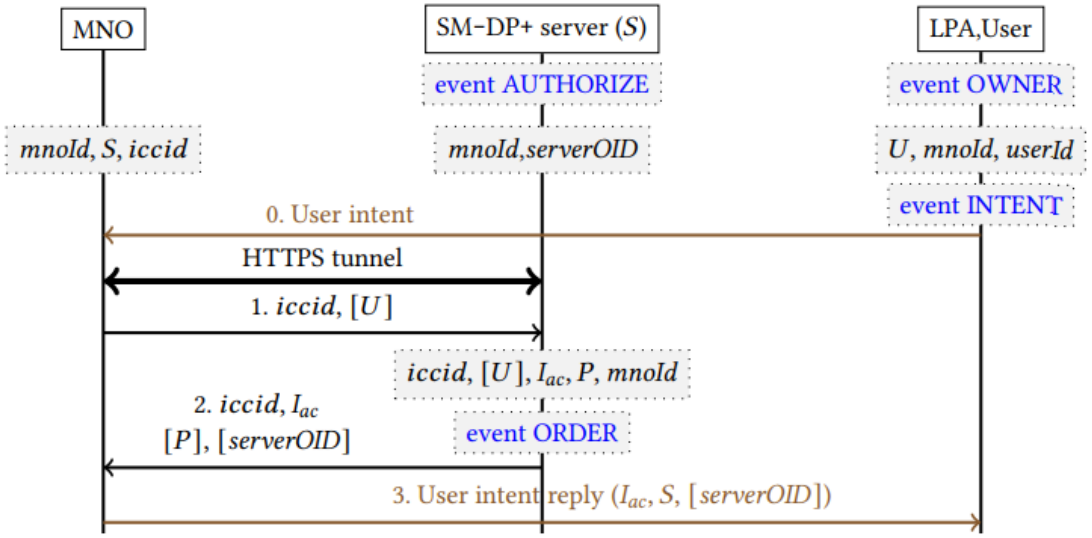

Figura 2.11: Approccio Activation Code per le fasi di profile ordering e download initialization.

- **Profile download**: in quest'ultima fase, i cui dettagli sono riportati nella sezione 2.4.6, 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). Avviene poi il download del profilo eSIM, in cui il server SM-DP+ invia all'LPA il profilo cifrato con la chiave k e l'operatore di riferimento, dove entrambe le informazioni sono firmate singolarmente con la chiave k' mediante il meccanismo di message authentication code (MAC). Dopodiché, l'LPA mostra l'operatore all'utente, che dovrà stabilire se è corretto: se sì, l'LPA inoltra tutte le informazioni all'eUICC il quale, dopo aver derivato a sua volta le chiavi di sessione k, k', dovrà decriptare il profilo P, che risulterà finalmente essere utilizzabile.

2.4.4 Ciclo di vita dei profili in SM-DP+

Prima di approfondire più nel dettaglio l'interazione in RSP, è bene illustrare il ciclo di vita dei profili eSIM.
La tabella 2.4 tratta da [3][5] fornisce un elenco degli stati in cui ciascun profilo eSIM può trovarsi nell'arco della sua esistenza. Nelle figure 2.12, 2.13 tratte da [3][5], invece, sono mostrati due diagrammi a stati finiti che illustrano per bene il ciclo di vita dei profili in SM-DP+.

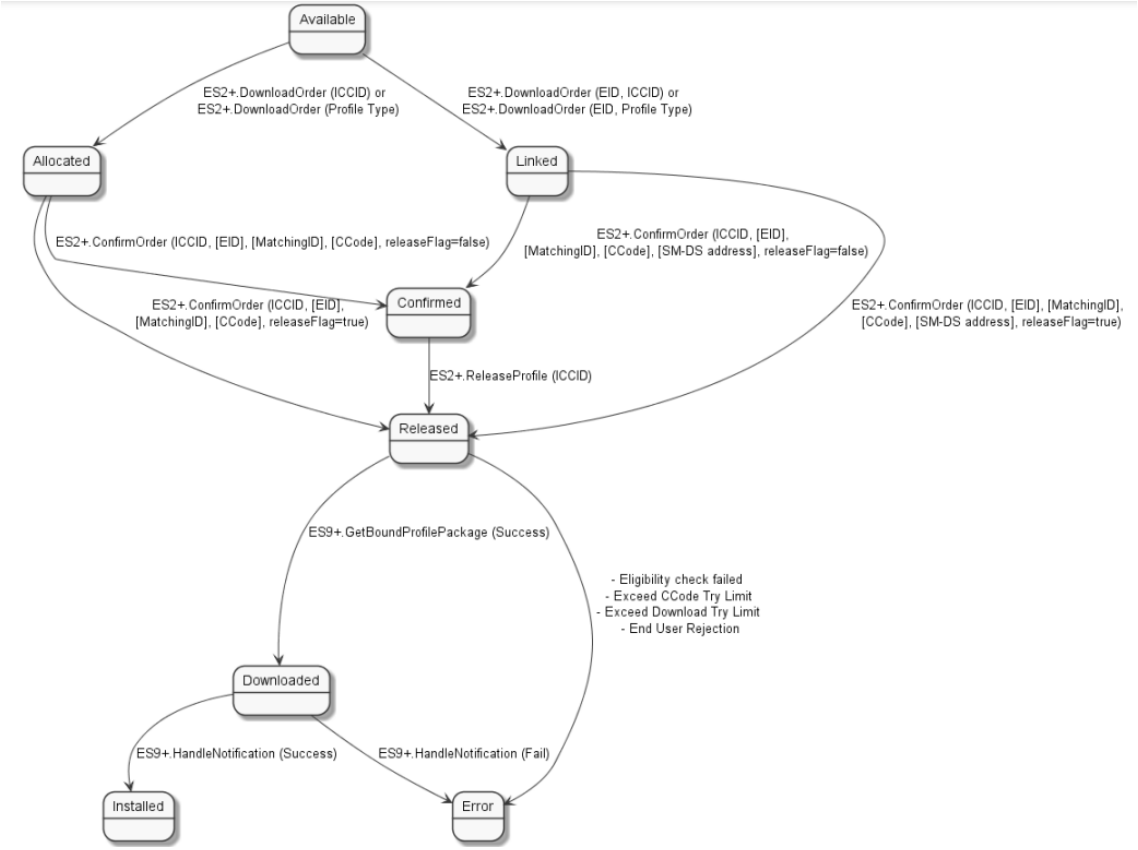

Figura 2.12: Primo diagramma a stati per i profili eSIM.

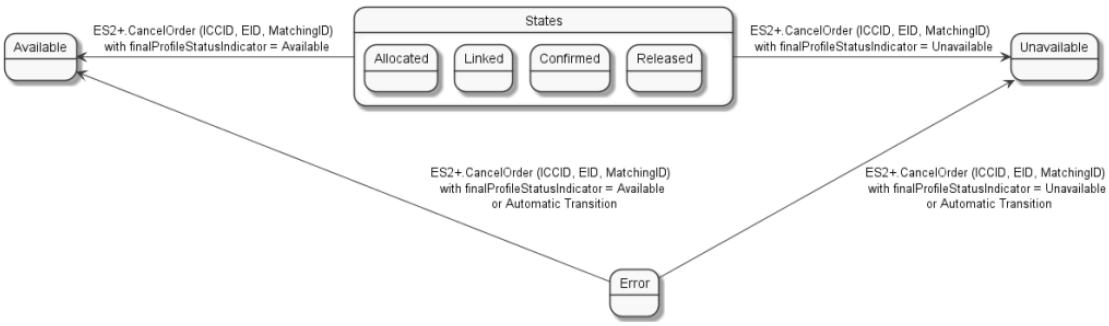

Figura 2.13: Secondo diagramma a stati per i profili eSIM.

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+.

Con riferimento alla figura 2.12, 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.
- Si passa allo stato Error se si ha un errore nell'installare il profilo sull'eUICC.

Con riferimento alla figura 2.13, 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 con una transizione automatica oppure se l'ordine di download viene annullato con finalProfileStatusIndicator=Available.
- Si passa allo stato Unavailable con una transizione automatica oppure se l'ordine di download viene annullato con finalProfileStatusIndicator=Unavailable.

2.4.5 Dettagli sulla Common Mutual Authentication

La figura 2.14 ripresa da [3] illustra tutti i messaggi che il server SM-DP+, l'LPA e l'eUICC si scambiano tra loro e le operazioni che queste tre entità svolgono durante la procedura di Common Mutual Authentication. Tutti i relativi dettagli [3] sono spiegati nelle sottosezioni successive. Si osservi che l'intero meccanismo resta valido e invariato se si ha un server SM-DS al posto del server SM-DP+.

Condizioni iniziali

- Il server SM-DP+ è dotato di:
  - certificato CERT.DPauth.SIG;
  - chiave privata SK.DPauth.SIG;
  - certificato del CI (CERT.CI.SIG);
  - certificato TLS CERT.DP.TLS;
  - chiave privata TLS SK.DP.TLS;
  - certificati di SM-DP+ intermediari, se esistenti (CERT.DPSubCA.SIG).
- L'eUICC, d'altra parte, è dotato di:
  - certificato CERT.EUICC.SIG;
  - chiave privata SK.EUICC.SIG;
  - certificato dell'EUM (CERT.EUM.SIG);
  - certificati di CI subordinati, se esistenti (CERT.CISubCA.SIG);
  - certificati di EUM subordinati, se esistenti (CERT.EUMSubCA.SIG);
  - chiave pubblica del CI (PK.CI.SIG).

Procedimento

1. Il primo step, che è opzionale, si articola in tre punti:
   a) Se non lo aveva già fatto in un momento precedente, l'LPA richiede le informazioni dell'eUICC (i.e. Specification Version Number e identificatori delle chiavi pubbliche del CI che possono essere utilizzate per autenticare il server e per firmare i propri dati) identificate dalla variabile euiccInfo1.
   b) L'eUICC restituisce euiccInfo1 all'LPA.
   c) Se esiste una restrizione sulle chiavi pubbliche consentite del CI, l'LPA crea una nuova istanza di euiccInfo1 senza le chiavi pubbliche non compatibili del CI. Se dopo questa operazione rimane una lista vuota di chiavi pubbliche, l'LPA informa l'end user che la procedura di mutua autenticazione deve terminare.
2. L'LPA richiede all'eUICC una challenge (euiccChallenge).
3. L'eUICC genera la challenge che successivamente dovrà essere firmata dal server SM-DP+ per l'autenticazione del server stesso.
4. L'eUICC restituisce la challenge all'LPA.
5. L'LPA stabilisce una nuova connessione HTTPS col server SM-DP+. Il setup della sessione TLS, poiché non può riutilizzare le chiavi da una sessione precedente, deve prevedere un nuovo key exchange, che avviene nella fase del TLS handshake. Qui il server fornisce all'LPA un certificato CERT.DP.TLS e l'LPA deve verificarne la validità; se l'LPA non riesce a effettuare la verifica, il server deve inviargli un certificato CERT.DP.TLS differente, e così via, fin tanto che l'LPA non sarà riuscito a validare un certificato oppure il numero di tentativi per ritrasmettere il certificato non avrà raggiunto il limite massimo. In questo secondo caso l'LPA interrompe la procedura di Common Mutual Authentication.
6. L'LPA invoca la funzione *InitiateAuthentication* passandovi come parametri le proprie capability, euiccChallenge, euiccInfo1 e l'indirizzo SM-DP+, il quale viene usato dall'LPA per accedere al server.

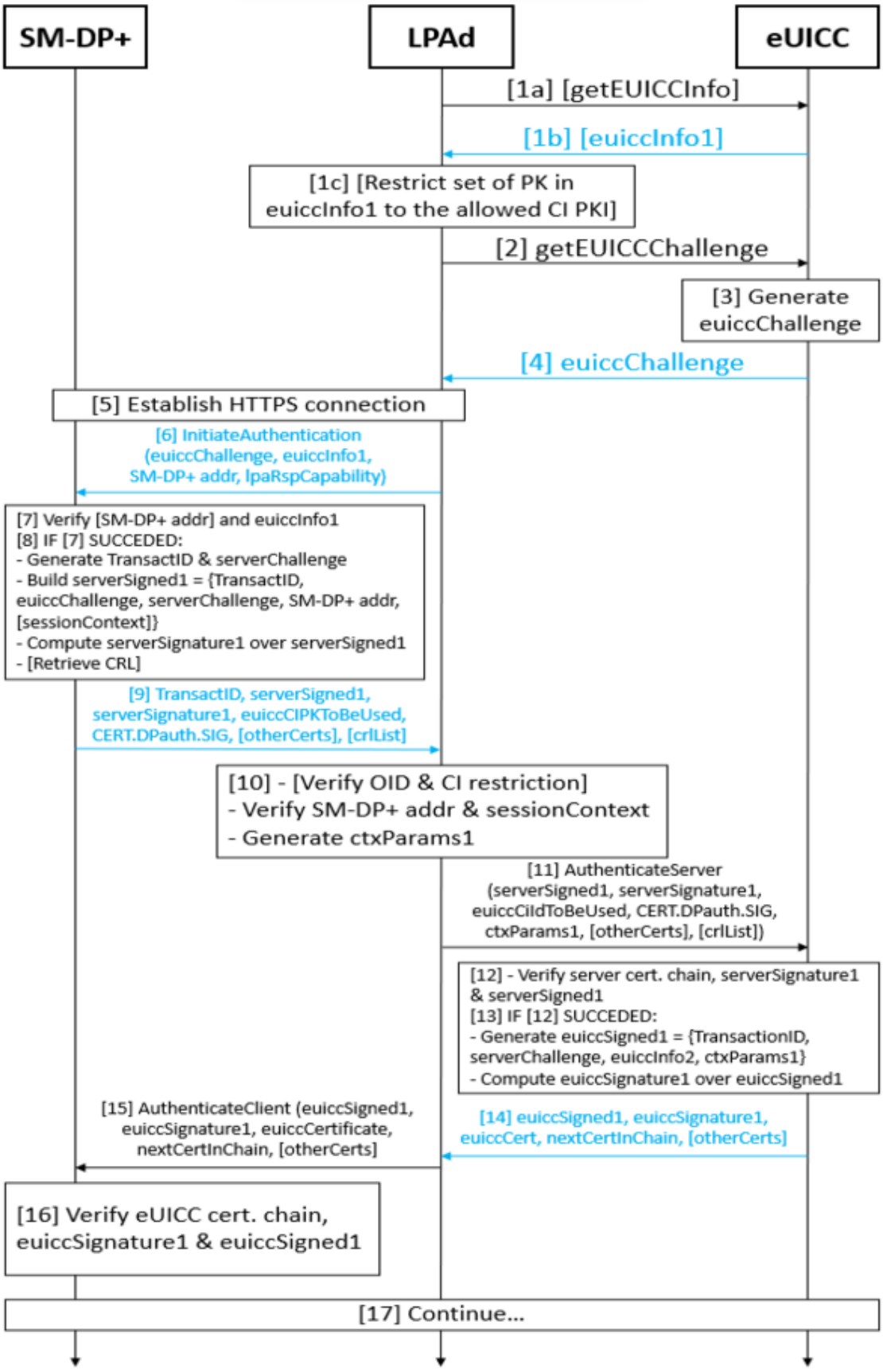

Figura 2.14: Sequence diagram che descrive la Common Mutual Authentication.

7. Il server SM-DP+ esegue le seguenti operazioni:

   - Verificare che l'indirizzo SM-DP+ inviato dall'LPA sia valido.
   - Verificare il contenuto della variabile euiccInfo1, incluse le chiavi pubbliche del CI, tra cui deve essercene almeno una che può essere accettata dal server stesso.

   Se anche solo uno di questi controlli non va a buon fine, il server restituisce una condizione di errore e l'LPA interrompe la procedura di Common Mutual Authentication.

8. Il server SM-DP+ esegue le seguenti altre operazioni:

   - Generare un ID di transazione che serve per identificare la sessione RSP.
   - Generare una challenge (serverChallenge) che dovrà essere firmata dall'eUICC per l'autenticazione dell'eUICC stesso.
   - Generare una struttura dati serverSigned1 a partire dall'ID di transazione, da euiccChallenge, da serverChallenge, dall'indirizzo SM-DP+ ed eventualmente dal contesto di sessione.
   - Calcolare la serverSignature1 a partire da serverSigned1, utilizzando la chiave privata SK.DPauth.SIG.
   - Se sia l'eUICC che l'LPA prevedono il crlStaplingV3Support, che è la funzionalità che permette al server di fornire una Certificate Revocation List (CRL), il server deve anche recuperare la CRL per ciascun certificato che abbia l'estensione CRLDistributionPoints (i.e. per ciascun certificato che dà informazioni su dove è possibile ottenere una CRL).

9. Il server SM-DP+ restituisce all'LPA alcune informazioni, tra cui l'ID della transazione, serverSigned1, serverSignature1, euiccCIPKToBeUsed (che dovrà corrispondere alla chiave pubblica del CI accettata tra quelle proposte dall'eUICC), il certificato CERT.DPauth.SIG, eventuali altri certificati ed eventualmente la CRL.

10. L'LPA esegue le seguenti operazioni:

    - Verificare l'OID, che è l'Object Identifier del server SM-DP+ (se fornito in precedenza).
    - Verificare che l'indirizzo SM-DP+ restituito dal server (incapsulato in serverSigned1) matchi con l'indirizzo SM-DP+ che l'LPA aveva inviato allo step (6).
    - Verificare che la chiave pubblica associata al certificato CERT.DPauth.SIG sia inclusa in euiccInfo1.
    - Effettuare altre verifiche sui certificati che non verranno approfondite in questa sede.

    Se anche solo uno di questi controlli non va a buon fine, l'LPA interrompe la procedura di Common Mutual Authentication. In caso contrario, procede col generare la struttura dati ctxParams1, che dovrà essere inviata all'eUICC affinché venga poi inclusa tra i dati firmati.

11. L'LPA invoca la funzione *AuthenticateServer* passandovi come parametri serverSigned1, serverSignature1, euiccCiIdToBeUsed, il certificato CERT.DPauth.SIG, eventuali altri certificati, ctxParams1 ed eventualmente la CRL.

12. L'eUICC esegue le seguenti operazioni:

    - Verificare il certificato CERT.DPauth.SIG e altri eventuali certificati nella catena.
    - Verificare serverSignature1.
    - Verificare che l'euiccChallenge contenuta in serverSigned1 matchi con la challenge generata dall'eUICC stessa allo step (3).
    - Verificare che la chiave pubblica del CI sia effettivamente supportata.
    - Se il contesto di sessione prevede il crlStaplingV3Support, l'eUICC deve anche verificare la validità della CRL e assicurarsi che nessun certificato all'interno della certificate chain sia stato revocato.

    Se anche solo uno di questi controlli non va a buon fine, la procedura di Common Mutual Authentication deve essere interrotta. In caso contrario, il server SM-DP+ risulta autenticato all'eUICC.

13. L'eUICC esegue le seguenti altre operazioni:

    - Generare la struttura dati euiccSigned1 a partire dall'ID di transazione, dall'indirizzo del server SM-DP+, da serverChallenge, da euiccInfo2 e da ctxParams1, dove euiccInfo2 è un sovrainsieme di euiccInfo1 e comprende le informazioni complete dell'eUICC. Si noti che euiccChallenge non è incluso in euiccSigned1.
    - Calcolare la euiccSignature1 a partire da euiccSigned1, utilizzando la chiave privata SK.EUICC.SIG.

14. L'eUICC restituisce all'LPA alcune informazioni, tra cui euiccSigned1, euiccSignature1 e la catena di certificati dell'eUICC.

15. L'LPA invoca la funzione *AuthenticateClient* passandovi come parametri euiccSigned1, euiccSignature1 e la catena di certificati dell'eUICC.

16. Il server SM-DP+ esegue le seguenti operazioni:

    - Verificare che l'ID di transazione contenuto in euiccSigned1 corrisponda a quello comunicato dal server stesso allo step (9).
    - Verificare che il certificato root della certificate chain comunicata dall'eUICC corrisponda con quella selezionata dal server stesso (euiccCIPKToBeUsed) durante l'esecuzione della funzione *InitiateAuthentication*.
    - Verificare che la certificate chain dell'eUICC sia valida.
    - Verificare euiccSignature1.
    - Verificare che la serverChallenge contenuta in euiccSigned1 matchi con la challenge generata dal server stesso allo step (8).

    Se anche solo uno di questi controlli non va a buon fine, il server restituisce una condizione di errore e l'LPA interrompe la procedura di Common Mutual Authentication. In caso contrario, l'eUICC risulta autenticato al server SM-DP+.

In definitiva, in questa sezione è emerso come l'LPA svolga sì il ruolo di relay nell'interazione tra server SM-DP+ ed eUICC, ma svolge anche delle importanti funzioni di sicurezza. Infatti, com'è stato già menzionato, si occupa anzitutto di verificare che il certificato CERT.DP.TLS sia valido e, in un secondo momento, effettua altri controlli sull'OID, sull'indirizzo del server SM-DP+, sulla chiave pubblica associata al certificato CERT.DPauth.SIG e sulla certificate chain del server nello specifico. Tale caratteristica implica la necessità di considerare l'applicazione LPA come un'entità trusted, il che non è fortemente indicato dal punto di vista della sicurezza.

2.4.6 Dettagli su download e installazione dei profili

La figura 2.15 ripresa da [3] illustra tutti i messaggi che l'operatore, il server SM-DP+, l'LPA e l'eUICC si scambiano tra loro e le operazioni che queste quattro entità svolgono durante la procedura di download e installazione dei profili. Tutti i relativi dettagli [3] sono spiegati nelle sottosezioni successive. Anche qui l'intero meccanismo resta valido se si ha un server SM-DS al posto del server SM-DP+, a meno di variazioni di poco conto.

Condizioni iniziali

- L'applicazione LPA potrebbe aver recuperato l'indirizzo del server SM-DP+ e l'identificativo della chiave pubblica del CI Root consentita; se tale identificativo viene effettivamente recuperato a partire dall'eUICC, allora l'LPA deve restringere l'insieme degli identificativi delle chiavi pubbliche dei CI Root compatibili a quel valore.

- Per ogni profilo nello stato Released il server SM-DP+ mantiene un contatore dei tentativi di download di quel profilo e un contatore dei tentativi di immissione del codice di conferma. Di fatto, il server deve limitare il valore di questi due contatori.

- Se è richiesto l'Activation Code per il download e l'installazione del profilo, l'end user deve averlo già immesso all'LPA.

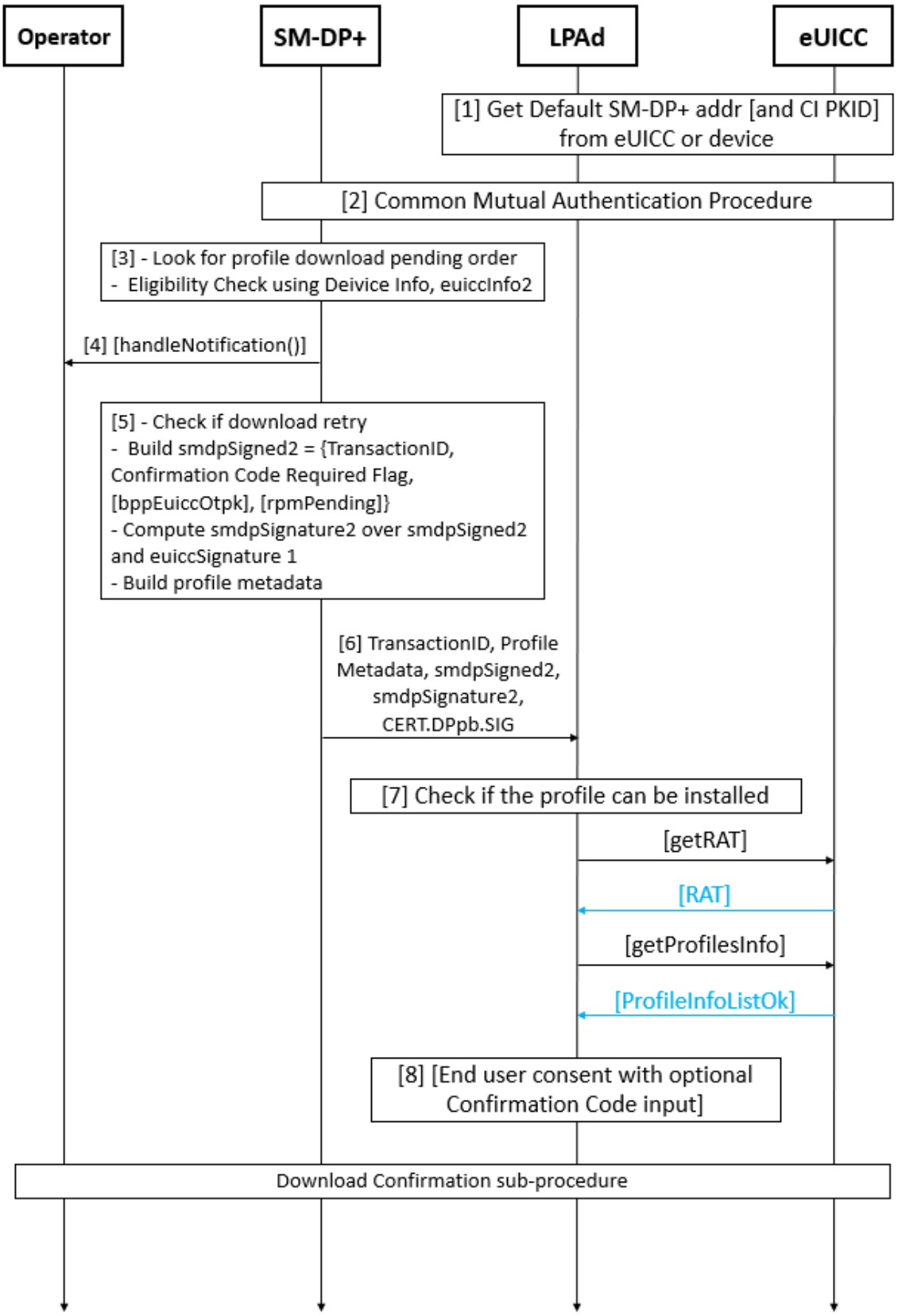

Figura 2.15: Sequence diagram che descrive il download e l'installazione dei profili.

Procedimento

1. Se non lo ha già fatto in precedenza e se è necessario, l'applicazione LPA effettua il parsing dell'Activation Code: così ottiene l'indirizzo del server SM-DP+ e, opzionalmente, l'OID del server SM-DP+ e l'identificativo della chiave pubblica del CI Root.

2. Viene eseguita la procedura di Common Mutual Authentication definita nella sezione 2.4.5. In particolare, nel messaggio *AuthenticateClient*, l'LPA deve specificare il Matching ID, che è l'identificatore della transazione di download corrente e, dunque, individua esattamente il profilo che si vuole installare.

3. Il server SM-DP+ esegue le seguenti operazioni:

   - Verificare che esista un profilo correlato al Matching ID ricevuto in *AuthenticateClient*.
   - Se l'ordinazione di download del profilo è già linkato a un EID, verificare che quest'ultimo corrisponda all'EID dell'eUICC appena autenticato.
   - Verificare che il profilo sia nello stato Released o, nel caso di retry a seguito del fallimento di un'installazione precedente, nello stato Downloaded.

   Se anche solo uno di questi controlli non va a buon fine, la procedura di download e installazione del profilo deve essere interrotta. In caso contrario, il server SM-DP+ deve procedere con le seguenti altre azioni:

   - Incrementare il contatore dei tentativi di download del profilo target. Se il numero massimo di tentativi viene sforato, il server deve notificare l'operatore del fallimento del download e l'intera procedura deve terminare.
   - Effettuare i check di idoneità opportuni.

4. Il server SM-DP+ notifica l'operatore con l'esito dei check di validità mediante la funzione *handleNotification* (step opzionale). La comunicazione tra server e operatore è protetta dall'uso di un pairwise secure channel, come nell'interazione tra eUICC e LPA; anche qui il protocollo più utilizzato è TLS ma non viene imposto dallo standard di GSMA. Di conseguenza, potrebbe essere nuovamente utile stabilire empiricamente se nel canale di comunicazione tra server SM-DP+ e operatore viene utilizzato TLS o meno.

5. Se i check di idoneità falliscono, allora il server SM-DP+ esegue le seguenti operazioni:

   - Portare il profilo target allo stato Error.
   - Restituire uno status di errore all'LPA in modo tale che l'intera procedura termini.

   In caso contrario, il server SM-DP+ esegue le seguenti altre operazioni:

   - Determinare se è richiesto un codice di conferma (Confirmation Code) per l'ordinazione pendente.
   - Generare una struttura dati smdpSigned2 che contiene le proprie informazioni.
   - Calcolare smdpSignature2, che è un fingerprint ottenuto da smdpSigned2 ed euiccSignature1, dove euiccSignature1 è un'informazione che è stata scambiata durante la fase di Common Mutual Authetication.
   - Generare i metadati del profilo target.

6. Il server SM-DP+ fornisce all'LPA la risposta ad *authenticateClient* (funzione invocata durante la procedura di Common Mutual Authentication), che comprende transactionId, i metadati del profilo, smdpSigned2, smdpSignature2 e CERT.DPpb.SIG.

7. L'LPA verifica se il profilo può essere effettivamente installato. Per far ciò, deve ricorrere a un'apposita struttura dati detta Rules Authorisation Table (RAT) e/o alla lista dei profili installati. Se non dispone già di queste informazioni, deve richiederle all'eUICC invocando le funzioni *getRAT* e/o *getProfilesInfo*.

8. Se richiesto, l'LPA richiede all'end user di inserire il codice di conferma che l'operatore gli aveva fornito. In caso contrario, l'LPA richiede una conferma semplice (Simple Confirmation) sul download del profilo, che può prevedere poche semplici opzioni di risposta come 'Yes',

'No', 'Not now'. Se l'end user non inserisce correttamente il codice di conferma o non risponde positivamente alla conferma semplice, si procede con la cancellazione della sessione (Common Cancel Session Procedure); altrimenti, l'installazione del profilo può completarsi con successo mediante la sotto-procedura di Download Confirmation, che verrà illustrata qui di seguito.

2.4.7 Sotto-procedura di Download Confirmation

La figura 2.16 ripresa da [3] illustra tutti i messaggi che l'operatore, il server SM-DP+, l'LPA e l'eUICC si scambiano tra loro e le operazioni che queste quattro entità svolgono durante la sotto-procedura di Download Confirmation, che conclude la procedura di download e installazione dei profili introdotta poc'anzi. Tutti i relativi dettagli [3] sono spiegati nelle sottosezioni successive. Ancora una volta i passaggi rimangono gli stessi se si ha un server SM-DS al posto del server SM-DP+.

Condizioni iniziali

- L'end user ha consentito con successo il download del profilo target.

Procedimento

1. L'LPA invoca la funzione *prepareDownload* passandovi come parametri le informazioni precedentemente ricevute del server SM-DP+ (come smdpSigned2, smdpSignature2 e il certificato CERT.DPpb.SIG) e opzionalmente l'hash del codice di conferma (Confirmation Code).
2. L'eUICC esegue le seguenti operazioni:
   - Verificare che CERT.DPpb.SIG sia un certificato valido.
   - Verificare che CERT.DPauth.SIG e CERT.DPpb.SIG appartengano alla medesima entità e siano state rilasciate dalla medesima CA.
   - Verificare smdpSignature2.
   - Verificare che l'ID di transazione contenuto in smdpSigned2 corrisponda con l'ID di transazione che identifica la sessione RSP corrente.

   Se anche solo uno di questi controlli non va a buon fine, l'eUICC deve restituire uno stato di errore e la procedura di download e installazione del profilo deve essere interrotta.
3. L'eUICC prosegue con le seguenti altre azioni:
   - Generare una coppia di chiavi one-time (otPK.EUICC.KA, otSK.EUICC.KA).
   - Generare la struttura dati euiccSigned2, che comprende l'ID di transazione, otPK.EUICC.KA ed eventualmente l'hash del Confirmation Code.
   - Calcolare euiccSignature2.
4. L'eUICC restituisce all'LPA la risposta a *prepareDownload*.
5. L'LPA invoca la funzione *getBoundProfilePackage* passandovi come parametri euiccSigned2 ed euiccSignature2.
6. Il server SM-DP+ verifica euiccSignature2 e stabilisce se è richiesto il codice di conferma: se sì, si procede con lo step (7), altrimenti si passa allo step (9).
7. Il server SM-DP+ esegue le seguenti operazioni:
   - Recuperare l'hash del Confirmation Code ottenuto dalla funzione *confirmOrder* relativa alle fasi di profile ordering & download initialization, e calcolarne il valore atteso come SHA256(hash del Confirmation Code — TransactionID).
   - Verificare che l'hash del Confirmation Code ricevuto all'interno di euiccSigned2 corrisponda col valore hash atteso.
   - Se la verifica dell'hash del Confirmation Code fallisce, incrementare di un'unità il contatore dei tentativi di immissione del codice di attivazione e verificare che tale contatore non sfori il numero massimo ammissibile.

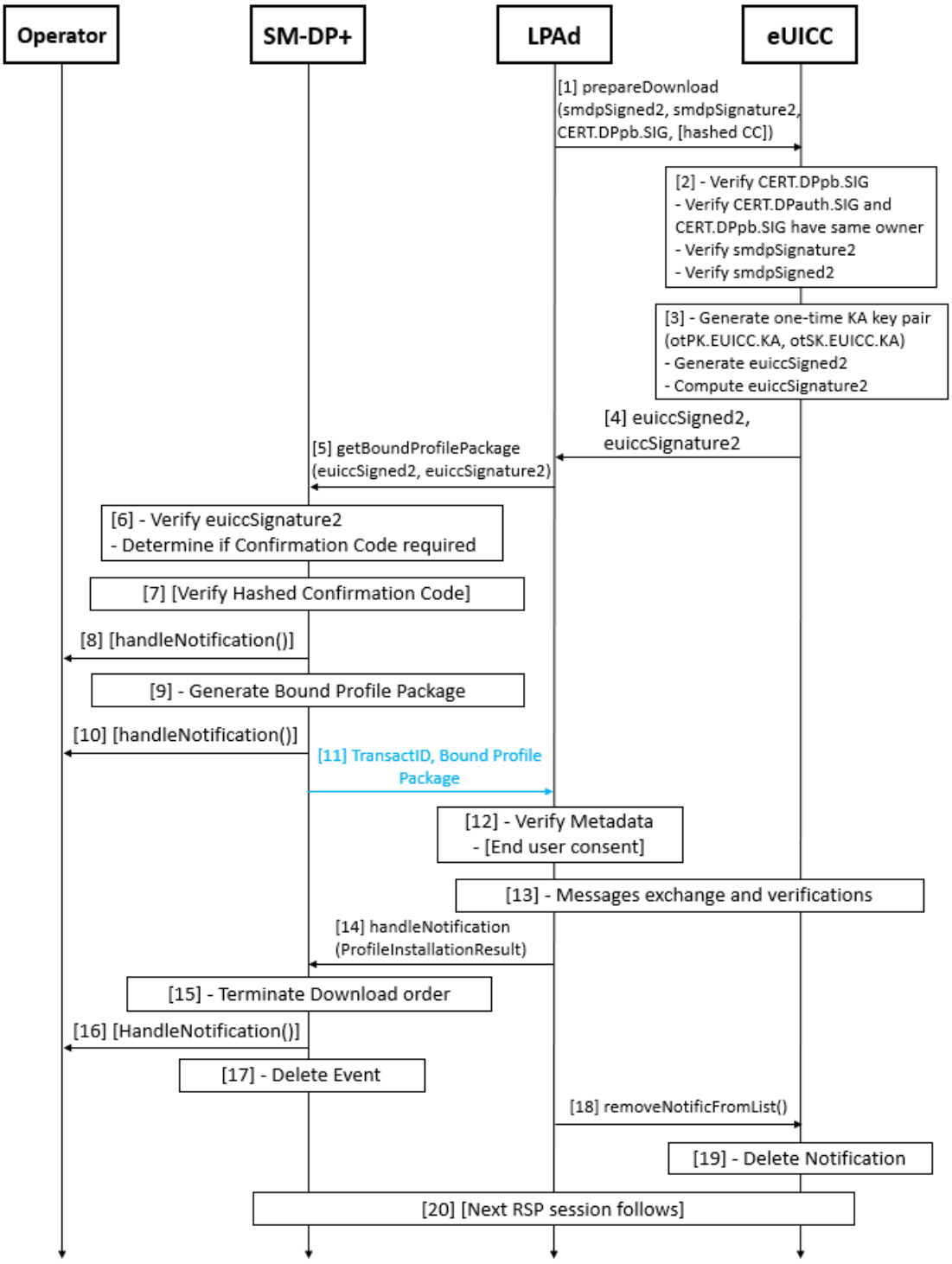

Figura 2.16: Sequence diagram che descrive la sotto-procedura di Download Confirmation.

Se anche solo uno di questi controlli non va a buon fine, il server SM-DP+ deve restituire uno stato di errore e la procedura di download e installazione del profilo deve essere interrotta. Più precisamente, se fallisce il controllo sul contatore dei tentativi di immissione del codice di attivazione, è necessario anche impostare il profilo target nello stato Error e passare allo step (8) prima di interrompere la procedura. Se invece i controlli vanno tutti a buon fine, si passa allo step (9).

8. Se il numero di tentativi di immissione del codice di attivazione supera il massimo stabilito, il server SM-DP+ informa l'operatore del fallimento mediante la funzione *handleNotification*; dopodiché, la procedura di download e installazione del profilo viene interrotta.

9. Il server SM-DP+ genera un Bound Profile Package.

2.4.8 Cambio di dispositivo

La figura 2.17 ripresa da [3] illustra tutti i messaggi che l'end user, l'LPA installata nel vecchio dispositivo, l'eUICC presente nel vecchio dispositivo, il server SM-DP+, l'LPA installata nel nuovo dispositivo, l'eUICC presente nel nuovo dispositivo e l'operatore (qui indicato come Service Provider) si scambiano tra loro e le operazioni che queste sette entità svolgono durante la procedura di trasferimento di un profilo dovuto al cambio di dispositivo. Tutti i relativi dettagli [3] sono spiegati nelle sottosezioni successive.

Condizioni iniziali

- Il Service Provider ha fornito al server SM-DP+ la configurazione e altre informazioni rilevanti per il cambio di dispositivo. Tutti questi dati devono essere contenuti anche nel profilo all'interno del vecchio dispositivo.

- L'end user possiede sia un vecchio dispositivo contenente un profilo, sia un nuovo dispositivo.

- L'eUICC e l'LPA del vecchio dispositivo supportano il cambio di dispositivo.

Procedimento

1. L'end user dà inizio all'operazione di cambio di dispositivo a partire dall'LPA del vecchio dispositivo e seleziona il profilo da installare nel nuovo dispositivo.

2. L'LPA del vecchio dispositivo recupera DeviceChangeConfiguration dai metadati del profilo. Se DeviceChangeConfiguration indica requestToDp, allora si passa allo step (3); se invece DeviceChangeConfiguration indica usingStoredAc, allora si passa allo step (17).

3. L'LPA del vecchio dispositivo determina l'indirizzo del server SM-DP+ a partire da DeviceChangeConfiguration.

4. Se DeviceChangeConfiguration indica che è richiesto l'EID e/o la TAC (Type Allocation Code, che è un codice a 8 cifre univoco per il dispositivo) del nuovo dispositivo, allora l'LPA del vecchio dispositivo recupera l'EID e/o la TAC dal nuovo dispositivo.

5. L'LPA del vecchio dispositivo dà inizio alla procedura di Common Mutual Authentication definita nella sezione 2.4.5.

6. Se la funzione *handleDeviceChangeRequest* è configurata nel Service Provider, allora il server SM-DP+ la invoca passandovi come parametri l'ICCID (Integrated Circuit Card ID, che è l'identificativo del profilo) ed eventualmente l'EID e la TAC del nuovo dispositivo. D'altro canto, però, se il server SM-DP+ non supporta il cambio di dispositivo o il cambio di dispositivo non è consentito per il profilo, allora il server risponde con un messaggio di errore e la procedura termina.

7. Il Service Provider risponde al server SM-DP+ col booleano isNewProfileRequired e, opzionalmente, un messaggio di Service Provider per il cambio di dispositivo e un codice di conferma.

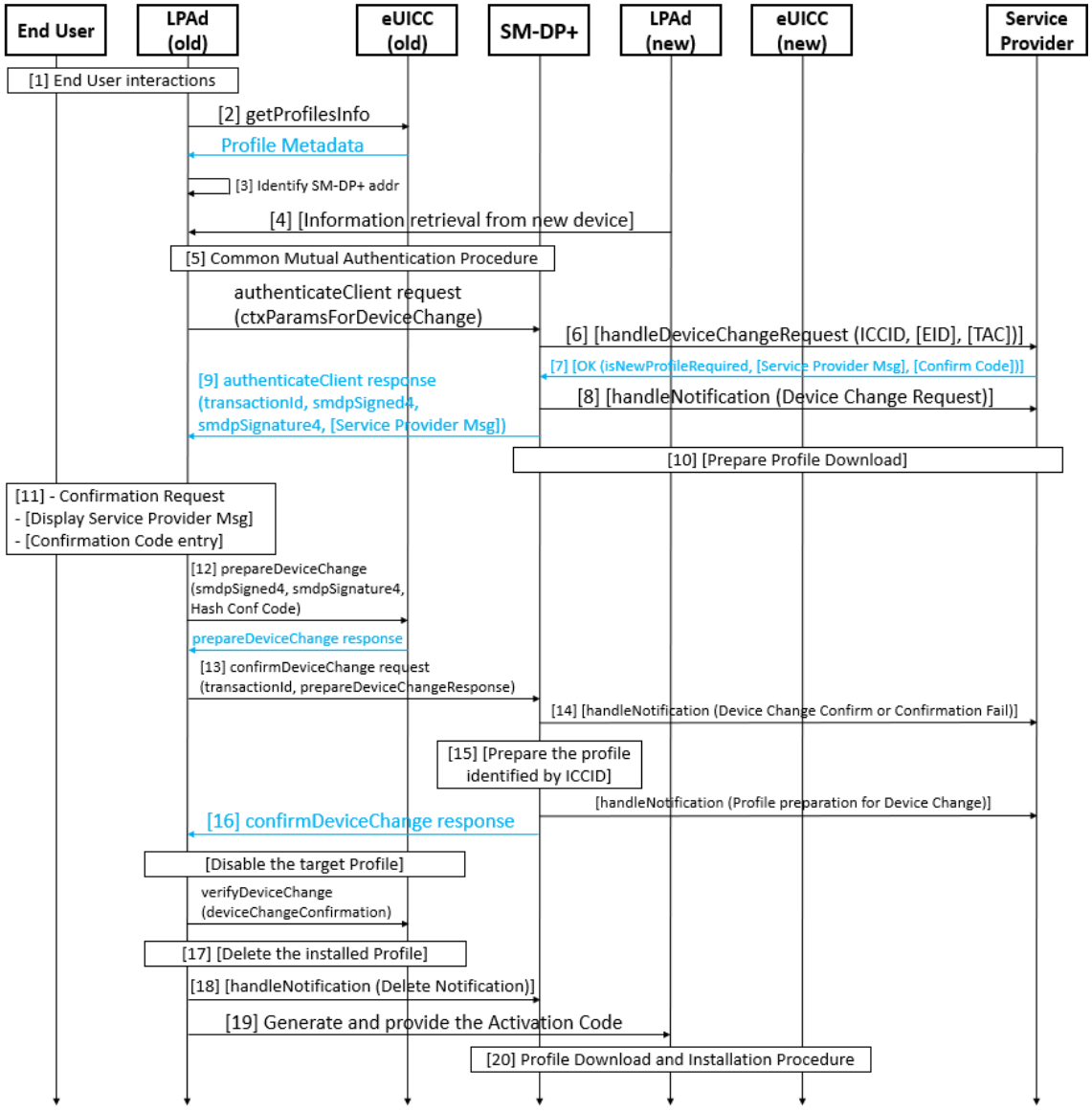

Figura 2.17: Sequence diagram che descrive il trasferimento di un profilo.

8. Se la funzione *handleNotification* è configurata nel Service Provider, il server SM-DP+ la invoca per notificare il Service Provider riguardo la richiesta del cambio di dispositivo.

9. Il server SM-DP+ restituisce all'LPA del vecchio dispositivo la risposta ad *authenticateClient* che comprende transactionId (l'identificativo della transazione), smdpSigned4 (informazioni del server SM-DP+), smdpSignature4 (signature di smdpSigned4) ed eventualmente il messaggio di Service Provider per il cambio di dispositivo.

10. Se il booleano isNewProfileRequired fornito dal Service Provider nello step (7) vale TRUE, allora il Service Provider esegue il Download Preparation Process (processo di preparazione del download) e opzionalmente il Subscription Activation Process (processo di attivazione della sottoscrizione al profilo).

11. L'LPA del vecchio dispositivo effettua una richiesta di conferma per il cambio di dispositivo. In particolare, se il Service Provider nello step (7) ha fornito il messaggio di Service Provider per il cambio di dispositivo, quest'ultimo viene presentato all'end user. Inoltre, se smdpSigned4 ha il campo ccRequiredFlag pari a TRUE, allora l'LPA del vecchio dispositivo chiede all'end user di inserire il codice di conferma fornito dal Service Provider nello step (7). Se l'end user non inserisce correttamente il codice di conferma entro un timeout prestabilito, si procede con la cancellazione della sessione (Common Cancel Session Procedure).

12. L'LPA del vecchio dispositivo invoca la funzione *prepareDeviceChange* passandovi come parametri smdpSigned4, smdpSignature4 ed eventualmente l'hash del codice di conferma. Quest'ultimo viene calcolato come SHA256(SHA256(ConfirmationCode) — transactionID).

13. L'LPA del vecchio dispositivo invoca la funzione *confirmDeviceChange* passandovi come parametri transactionId e prepareDeviceChangeResponse.

14. Se il booleano isNewProfileRequired fornito dal Service Provider nello step (7) vale TRUE, allora il server SM-DP+ invoca la funzione *handleNotification* per notificare il Service Provider riguardo l'esito della conferma del cambio di dispositivo da parte dell'end user. Se l'end user ha accettato il cambio di dispositivo, allora si passa allo step (15); altrimenti la procedura termina.

15. Se il booleano isNewProfileRequired vale FALSE, allora il server SM-DP+ prepara il profilo per il download e il Matching ID associato al profilo. Inoltre, se nello step (5) è stato fornito un EID, allora il server lo collega al download del profilo preparato. Infine, il server invoca la funzione *handleNotification* per notificare il Service Provider riguardo l'esito della preparazione del profilo.

16. Il server SM-DP+ restituisce all'LPA del vecchio dispositivo la risposta a *confirmDeviceChange* che comprende l'esito del cambio di dispositivo. Se tale risposta contiene encryptedDeviceChangeData, l'LPA del vecchio dispositivo disabilita il profilo target. Dopodiché l'LPA verifica la signature del server SM-DP+ invocando la funzione *verifyDeviceChange*.

17. Se previsto, l'LPA del vecchio dispositivo elimina il profilo target dall'eUICC del vecchio dispositivo. Inoltre, se DeviceChangeConfiguration indica requestToDp e il server SM-DP+ nello step (16) ha indicato di supportare la recovery dei profili eliminati, allora l'LPA del vecchio dispositivo dovrebbe memorizzare alcune informazioni del profilo eliminato, come l'ICCID. Se invece l'eliminazione del profilo non è richiesta, si passa direttamente allo step (19).

18. L'LPA del vecchio dispositivo invia al server SM-DP+ la notifica di eliminazione del profilo. Se l'invio della notifica fallisce, la procedura termina.

19. L'LPA del vecchio dispositivo genera il codice di attivazione (Activation Code) e lo fornisce all'LPA del nuovo dispositivo. Inoltre, dovrebbe fornire al nuovo dispositivo lo stato attuale del profilo in modo tale da consentire all'LPA del nuovo dispositivo di ripristinare correttamente tale stato.

20. Il profilo viene scaricato nel nuovo dispositivo a partire dal server SM-DP+ mediante la procedura di download e installazione del profilo, che è stata definita nella sezione 2.4.6.

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

Risultati ottenuti

[TODO]

Capitolo 6

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

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

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

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

Ringraziamenti

[TODO]