M2M Remote SIM Provisioning Report

Generated on: 2025-03-19 13:53:48

1. Process Overview

The M2M Remote SIM Provisioning (RSP) process allows for the remote provisioning and management of embedded SIMs (eUICC) in M2M devices. The implementation follows the GSMA SGP.02 specification and consists of the following key steps:

1. Root CA initialization - Certificate authority setup for secure communication
2. SM-DP and SM-SR setup - Subscription Manager entities initialization
3. eUICC registration - Device registers with SM-SR using PSK-TLS
4. Profile preparation - SM-DP prepares the profile data package
5. Key establishment - Secure ECDH key exchange for end-to-end encryption
6. ISD-P creation - Creation of security domain for profile installation
7. Profile transmission - Profile data securely transmitted from SM-DP to SM-SR
8. Profile installation - SM-SR delivers and installs profile on eUICC

2. Performance Measurements

The following table shows the time taken for each step of the process:

Process Step	Time (seconds)	Bottleneck
eUICC Registration Process	0.102	No
ISD-P Creation Process	0.082	No
ECDH Key Establishment Process	0.203	No
Profile Preparation Process	0.508	Yes
Profile Installation Process	0.307	Yes
Total Process Time	**1.202**	

2.1 Bottleneck Analysis

The following steps were identified as bottlenecks in the M2M RSP process (taking more than 20% of the total process time):

• Profile Preparation Process: 0.508 seconds (42.3% of total time)

Profile preparation involves packaging, encryption, and signing operations. Possible optimizations include: - Caching precomputed profile templates - Optimizing ASN.1 encoding/decoding operations - Using hardware acceleration for cryptographic operations

• Profile Installation Process: 0.307 seconds (25.5% of total time)

3. M2M RSP Process Flow

The M2M Remote SIM Provisioning process follows a specific sequence of operations to securely provision profiles to embedded SIMs. The implementation follows the GSMA SGP.02 specification with the following key steps:

1. eUICC Registration at SM-SR

The eUICC sends an eUICC Information Set (EIS) to the SM-SR for registration. The EIS contains the eUICC certificate, capabilities, and other information needed for secure communication. This step establishes a PSK-TLS channel between the eUICC and SM-SR.

2. ISD-P Creation

The SM-SR creates an ISD-P (Issuer Security Domain for Profile) on the eUICC. The ISD-P acts as a secure container for profile installation and management.

3. Key Establishment & Mutual Authentication

The eUICC and SM-DP perform ECDH key agreement with mutual authentication to establish secure session keys for profile protection and transmission.

4. Profile Download & Installation

The profile is prepared by the SM-DP, transmitted securely to the eUICC via the SM-SR, and installed in the ISD-P using SCP03t secure channel protocol.

5. Profile Enabling

The newly installed profile is enabled on the eUICC, making it operational. This step involves executing ES8 commands over the PSK-TLS channel between the SM-SR and eUICC.

4. System Diagnostics

4.1 Component Status

Component	Status	Response Time (seconds)
SM-DP	Offline	0.000
SM-SR	Offline	0.000
eUICC	Offline	0.000