

# M2M Remote SIM Provisioning Report

Generated on: 2025-03-24 11:51:20

## 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. ISD-P creation - Creation of security domain for profile installation
- 5. Key establishment - Secure ECDH key exchange for end-to-end encryption
- 6. Profile preparation - SM-DP prepares the profile data package
- 7. Profile installation - SM-SR delivers and installs profile on eUICC
- 8. Profile enabling - Newly installed profile is enabled on the eUICC

## 2. Performance Measurements

The following table shows the accurate time taken for each step of the process from detailed measurements:

| Process Step                              | Time (seconds) | Bottleneck |
|---|----------------|------------|
| eUICC Registration Process                | 0.014          | No         |
| ISD-P Creation Process                    | 0.017          | No         |
| ECDH Key Establishment Process            | 0.043          | No         |
| Profile Preparation Process               | 10.042         | Yes        |
| Profile Download and Installation Process | 0.077          | No         |
| Profile Enabling Process                  | 10.056         | Yes        |
| Status Check Process                      | 0.042          | No         |
| ECDH Key Generation                       | 0.000          | No         |
| SM-DP Key Signing                         | 0.000          | No         |
| ECDH Shared Secret Computation            | 0.001          | No         |
| SM-DP Shared Secret Computation           | 0.000          | No         |
| Profile Data Preparation                  | 0.000          | No         |
| PSK-TLS Encryption                        | 0.058          | No         |
| PSK Key Derivation (AES-128)              | 0.054          | No         |
| AES-128 Encryption                        | 0.002          | No         |
| HMAC Generation                           | 0.000          | No         |
| PSK-TLS Decryption                        | 0.035          | No         |

|  |        |    |
|--|--------|----|
| PSK Key Derivation for MAC (AES-128)           | 0.021  | No |
| HMAC Verification                              | 0.000  | No |
| PSK Key Derivation for Decryption (AES-128)    | 0.012  | No |
| AES-128 Decryption                             | 0.000  | No |
| Total Process Operations                       | 20.475 |    |
| Total Protocol Time (including network delays) | 26.346 |    |

### 3. Connectivity and System Diagnostics

#### 3.1 Component Status

| Component | Status | Response Time |
|-----------|--------|---------------|
| SM-DP     | Online | 0.013 seconds |
| SM-SR     | Online | 0.014 seconds |
| eUICC     | Online | 0.002 seconds |

#### 3.2 Detailed Process Timeline

| Process                           | Entity | Duration (s) | Status  |
|-----------------------------------|--------|--------------|---------|
| eUICC Registration                | eUICC  | 0.000        | success |
| ISD-P Creation                    | SM-SR  | 0.000        | success |
| ECDH Key Establishment            | eUICC  | 0.000        | success |
| Profile Preparation               | SM-DP  | 0.000        | success |
| Profile Download and Installation | eUICC  | 0.000        | success |
| Profile Enabling                  | SM-SR  | 0.000        | success |
| Status Check                      | SYSTEM | 0.000        | success |