TS-M2M-0003v3.10.2
セキュリティ技術の適用
Security Solutions

アブストラクト：
本技術仕様書は、M2M システムにおけるセキュリティ仕様を定義する。

目次：

- デバイス認証フレームワーク（MAF）

９章　セキュリティフレームワークの手順と設定パラメータ

本章では、8 章で記述したフレームワークにおける手順や設定パラメータについて記述する。

１０章 プロトコル、及びアルゴリズムの詳細

本章では、プロトコルやアルゴリズムの詳細について記述する。証明書ベースセキュリティフレームワーク、TLS(Transport Layer Security)・DTLS(Datagram Transport Layer Security)、鍵のエクスポート・導出に関する記述を含む。

１１章 PPM (Privacy Policy Manager)を用いたプライバシー保護アーキテクチャ

本章では、ユーザの設定情報を基にしたパーソナルデータの管理フレームワークである PPM を使用したアーキテクチャについて記述する。内容としては、ユーザのプリファレンスの登録、プライバシーポリシーへの同意取得、PPM を使用したアクセス制御の流れを記述する。

１２章 oneM2M におけるセキュリティ関連のデータタイプ定義

本章では、本セキュリティ仕様書（TS-0003）にのみ使用されるデータタイプの定義について記述する。

付則 A（情報）3GPP(3rd Generation Partnership Project) GBA(Generic Bootstrapping Architecture)用語のマッピング

本付則では、3GPP 規格の GBA で用いられる用語と、oneM2M で用いられる用語の対応について記述する。

付則 B（情報）一般的な相互認証メカニズム

本付則では、oneM2M の相互認証メカニズムについて記述する。複数 Entity のグループ認証に関する記述を含む。

付則 C（規則）特定のセキュア領域に関連したセキュリティプロトコル

本付則では、特定のセキュア領域に関連したセキュリティプロトコルについて記述する。UICC(Universal Integrated Circuit Card)、ISO7816 インターフェース関連、TEE(Trusted Execution Environment)、セキュア領域と CSE(Common Service Entity)の対応付けに関する記述を含む。

付則 D（規則）共通鍵ベースの oneM2M サービスをサポートする UICC セキュリティフレームワーク

本付則では、M2M サービスレイヤセキュリティに UICC を用いる際の適用事項について記述する。

付則 E（情報）M2M サービスをサポートする UICC フレームワークの詳細

本付則では、付則 D にて記述した oneM2M に向けた UICC フレームワークに関連した実用的な情報について記述する。

付則 F（規則）位置ベースアクセス制御のための位置情報の取得

本付則では、位置ベースアクセス制御のための位置情報の取得方法について記述する。

付則 G（情報）アクセス制御判定要求

本付則では、6 章に記述した認可アーキテクチャにおけるアクセス制御判定リクエストについて記述する。

付則 H（情報）実装の手引き、及びソリューションの索引

本付則では、本仕様書で定義したセキュリティ仕様を利用する際の参照章番号について記述する。

付則 I（情報）参考文献

本付則は、参考文献のリストを提供する。

付則 J（規則）プライバシーポリシー記述言語

本付則は、プライバシーポリシーへの同意取得するための記述言語を記載する。内容としては、データの種類（非パーソナルデータ、匿名加工済みデータ、パーソナルデータ）、データの収集頻度（イベント発生時、定期的、リアルタイム）、データの保存先（国内、国外）、データ利用理由（サービス向上、第 3 者提供）、データの保存期間（利用後削除、一定期間）等を記載する。

付則 K（情報）サービス規約記述言語の実装ルール

本付則は、サービス規約記述言語を用いたサービス規約の実装に関するルールを記述する。

付則 L（規則）非対称鍵をサポートする耐タンパーセキュア領域のフレームワーク

本付則は、デバイスの認証などに、PKI を耐タンパー性のあるセキュア領域で実施するためのフレームワークについて記述する。

付則 M（情報）SCEP（Simple Certificate Enrolment Protocol）の実装例

SCEP を用いた証明書のプロビジョニングに関する実装例について記述する。

Summary:

The TS defines security solutions for M2M systems.

The present document defines security solutions applicable within the M2M system.