TS-M2M-0003v2.4.1
oneM2M 技術仕様書 －セキュリティ技術の適用－
oneM2M Technical Specification －Security Solutions－

サマリ（和文）：

アブストラクト：
本仕様書は、M2M システムに適用可能なセキュリティ技術について定義する。

目次：
１章　所掌範囲（目的）
本仕様書は、M2M システムに適用可能なセキュリティ技術について定義する。
２章　引用文献
３章　定義、略語と頭字語
４章　表記法
５章　セキュリティアーキテクチャ
本章では、セキュリティアーキテクチャの概要について記述する。本アーキテクチャは次のレイヤで構成される。
- セキュリティ機能レイヤ
- セキュリティ環境抽象化レイヤ
- セキュリティ環境レイヤ
６章　セキュリティサービスとインタラクション
本章では、oneM2M のイベントフローにおけるセキュリティ機能の実現、セキュリティサービスレイヤ、及びセキュア環境抽象化レイヤの構成要素について記述する。
７章　認可
本章では、アクセス制御機構、AE(Application Entity)なりすましの防止、ダイナミック認可、ロールを使用するアクセス制御について記述する。
８章　セキュリティフレームワーク
本章では、M2M システムにおいてセキュリティを確保する様々な方法をサポートするフレームワークについて記述しており、以下に関する記述を含む。
- セキュリティアソシエーション確立
- リモートセキュリティ設定のフレームワーク
- プリミティブなエンド・ツー・エンド・セキュリティ(ESPrim)
- エンド・ツー・エンド・セキュリティのデータ方式（ESData）
- エンド・ツー・エンド・セキュリティのリモートセキュリティ・フレームワーク
- エンド・ツー・エンドの認証ベースの鍵生成(ESCertKE)
- MAF セキュリティフレームワークの詳細
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 を用いたプライバシ保護アーキテクチャ

本章では、ユーザのプレファレンスを基にしたパーソナルデータ管理フレームワークの 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。

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 SE(Secure Environment)技術に関連したセキュリティプロトコル

本付則では、特定の SE 技術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)、SE・CSE(Common Service Entity)の対応付けに関する記述を含む。

付則 D（規則） 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（情報）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（規則）アクセス制御判定要求

本付則では、6.2.2 にて記述した認可アーキテクチャに導入された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、セキュリティソリューション実装の際の参照箇所について記述する。

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）参考文献

本付則は、参考文献のリストを提供する。

サマリ（英文）：

Abstract：

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