3F-1

スマートデバイスに搭載したセキュリティモジュールへの鍵配送方式の考案

山﨑裕紀† 相川慎† 川連嘉晃† 福島真一郎† 高見穣†
†株式会社 日立製作所

1 緒言

スマートデバイスに搭載される SIM やセキュア SD カード等のセキュリティモジュールは、種々のサービス事業者による決済サービスや認証サービスでの利用が進んでいる。サービス事業者がこれらのセキュリティモジュールに OTA(Over the Air)で秘密鍵を配送する際には、通信事業者や TSM(Trusted Service Manager)等の第三者が提供するネットワークやサーバ等を用いる必要がある。そのため、サービス事業者の秘密鍵をこれらの第三者から秘匿しつつ、セキュリティモジュールに配送する技術が求められている。これを受け、本研究は、OTA による秘密鍵の配送をより安全に行うための鍵配送システムの検討を目的とする。

2 従来方式の課題と検討目標

2．1 従来の OTA の概要

無線ネットワークを通じてセキュリティモジュールにアクセスする技術を OTA(Over the Air)と呼ぶ。OTA の一例を GlobalPlatform(GP)が仕様化している[1]。GP による従来の OTA では、主に表 1に示すプレイヤーで役割を分担することが考えられている。このうちセキュリティモジュール管理事業者や鍵配送事業者は TSM(Trusted Service Manager)と呼ばれる。

サービス事業者は、ユーザを識別したり、サービスに関する機密情報を秘匿したりするために、ユーザのセキュリティモジュールに秘密鍵を格納する。秘密鍵はアプリケーション自身に設定されるか、もしくは、秘密鍵の管理を行うセキュリティドメインに設定される。

サービス事業者の秘密鍵の配送は、サービス事業者に代わって鍵配送事業者が行う。セキュリティモジュールに秘密鍵の設定を行う際の認証や暗号化に用いる鍵はセキュリティモジュール管理事業者が発行する。

表 1: OTA のプレイヤー

	プレイヤー	概要
A	サービス事業者	サービス主体。秘密鍵所持
B	鍵配送事業者	サービス事業者の秘密鍵をセキュリティモジュールに配送
C	セキュリティモジュール管理事業者	スマートデバイスのセキュリティモジュールを管理
D	通信事業者	無線ネットワークの提供

Investigation of Key Deployment System for Secure Modules in Smart Device

Hiroki YAMAZAKI†, Makoto AIKAWA†, Yoshiaki KAWATSURA†, Shinichiro FUKUSHIMA† and Yutaka TAKAMI†
†Hitachi, Ltd.
{hiroki.yamazaki.nt, makoto.aikawa.vm, yoshiaki.kawatsura.ct, shinichiro.fukushima.ct, yutaka.takami.xx}@hitachi.com

2．2 従来の OTA の課題

従来の OTA の処理概要とその課題を図 1に示す。GP 仕様に則った従来の OTA では、サービス事業者の秘密鍵を鍵配送事業者に預託する必要があるため、技術的には鍵配送事業者が秘密鍵の値を知ることが可能となる。また、セキュリティモジュール管理事業者は、秘密鍵を設定するための通信路暗号鍵を所持していることから、これを復号することで秘密鍵の情報を得ることができる。

したがって、従来方式ではサービス事業者の秘密鍵が他のプレイヤーに漏洩するおそれがあると考える。そのためサービス事業者の秘密鍵を他の OTA のプレイヤーから秘匿することが課題となる。

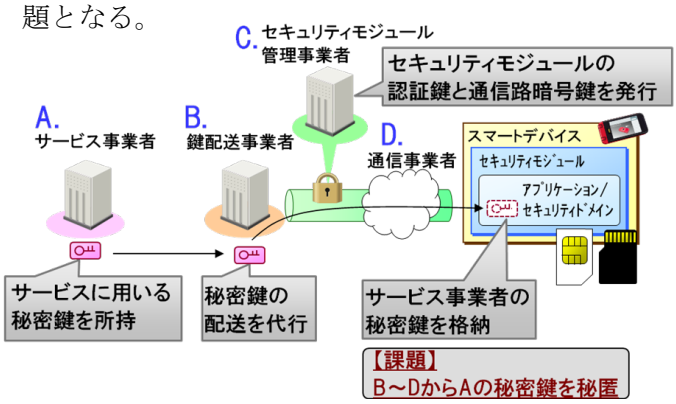

図 1: 従来の OTA の処理概要とその課題

2．3 検討目標

前項で述べた課題を解決しようとする際に、セキュリティモジュールの OS やサービス事業者のアプリケーションの改変を要するような方式を用いると、セキュリティモジュール管理事業者やサービス事業者のコスト負担の増大に繋がる。そこで、既存の OS やアプリケーションを改変することなく適用できる鍵配送システムを検討することが必要となる。

上述した内容から、検討目標を表 2の通り設定し、鍵配送システムの検討を行うこととした。

表 2: 検討目標

	目標
1	OTAに関わる全てのプレイヤーからサービス事業者の秘密鍵を秘匿すること
2	既存のOSやアプリケーションを変更せずにサービス事業者の秘密鍵を配送すること

3 鍵配送システムの検討

従来方式の課題を踏まえ、本研究では新たな方式の鍵配送システムを考案した。本方式では、セキュリティモジュール内で生成する公開鍵ペアを用い、PKI での鍵配送を行う。さらに、セキュリティモジュールに搭載するアプリケーションとして、鍵配送アプリケーションを用意する。鍵配送アプリケーションは、サービス事業者の秘密鍵を公開鍵暗号で暗号化した上で一時的に受け取り、これをアプリケーションやセキュリティドメインに設定する。本方式の概要を図 2 に示す。

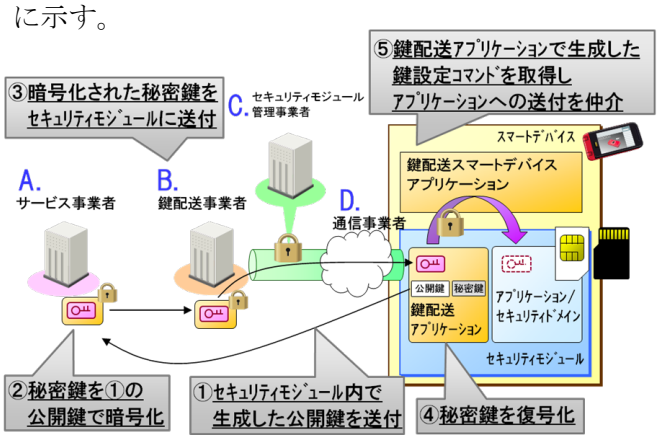

図 2: 本検討による鍵配送システム

鍵配送の手順を、図 2に基づき説明する。まずセキュリティモジュールの内部で公開鍵暗号の鍵ペアを生成し、公開鍵をサービス事業者に送付する(①)。図 2では公開鍵に対する証明書の付与や検証等の記述を省いているが、PKI として用を成すための諸手順は適宜実施する。サービス事業者の秘密鍵は公開鍵により暗号化され(②)、鍵配送事業者によってセキュリティモジュールに配送される(③)。サービス事業者の秘密鍵は公開鍵のペアとなる秘密鍵によってセキュリティモジュールの内部で復号される(④)。鍵配送アプリケーションは、秘密鍵を設定するための鍵設定コマンドを内部で生成する。生成された鍵設定コマンドは、鍵配送スマートデバイスアプリケーションによって読み取られ、対象となるアプリケーションやセキュリティドメインに送付される(⑤)。

⑤において、鍵配送アプリケーションと、アプリケーションもしくはセキュリティドメインは、鍵配送スマートデバイスアプリケーションの仲介処理により、鍵設定コマンドの送受信を行う。このとき鍵設定に必要な所定の認証や暗号通信を両者間で実施する。図 2では省略しているが、この認証や暗号通信を実施するための鍵は、サービス事業者の秘密鍵と合わせて、公開鍵で暗号化して鍵配送アプリケーションに配送する。

4 検討結果の考察

前節で検討した鍵配送システムについて、検討目標 1 及び検討目標 2 に関し考察する。サービス事業者の鍵はセキュリティモジュールに格納されるまで、一貫して公開鍵で暗号化されている。これを復号できる公開鍵暗号秘密鍵は、鍵配送アプリケーションの内部にのみ存在する。したがって鍵配送事業者、セキュリティモジュール管理事業者及び通信事業者のいずれもサービス事業者の秘密鍵を復号できない。またスマートデバイスは End-to-End で暗号化された通信を仲介するのみにとどまっており、サービス事業者の秘密鍵を復号することはできない。以上の考察から検討した鍵配送システムは検討目標 1 を達成することができる。

また、鍵配送アプリケーションの導入はセキュリティモジュールの既存の OS に何ら変更を要するものではない。更に、秘密鍵を設定すべきアプリケーションやセキュリティドメインにとっては、既存の鍵設定の方法で秘密鍵が設定される場合と何ら違いがない。したがって本方式によって検討目標 2 を達成することができる。なお、本方式では目標 2 の達成のために鍵配送アプリケーションを考案したが、将来的には、内部生成した公開鍵を鍵配送に用いる機能をセキュリティモジュールの OS に含めることも考えられる。

5 結言

本研究では、サービス事業者の秘密鍵を OTA でより安全に配信するための鍵配送システムを検討することを目的とし、OTA のプレイヤーから秘密鍵を秘匿すること、並びにセキュリティモジュールの既存の OS やアプリケーションに改変を加えないことを検討目標とした。従来方式では検討目標を達成困難であることを示した上で、新たな鍵配送システムを考案し、PKI による鍵配送アプリケーションをセキュリティモジュールに搭載することで検討目標達成の見込みを得た。実装による実現性の検証が今後の課題である。

6 参考文献

[1]Secure Element Remote Application Management Version 1.0, GlobalPlatform, 2011