Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 4, 2018

D. Liu
Q. Fang
Alibaba Group

July 3, 2017

A Protocol for Dynamic Trusted Execution Environment Enablement
draft-liu-opentrustprotocol-usecase-01

Abstract

This document describes features of a open trust protocol and related use cases. With the Open Trust Protocol, see https://tools.ietf.org/html/draft-pei-opentrustprotocol-03, we have been trying to develop this application layer security protocol that allows the management of credentials and the update of such applications.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 4, 2018.

Copyright Notice

Table of Contents

1. Acronyms

CA	Certificate Authority
OTrP	Open Trust Protocol
REE	Rich Execution Environment
SD	Security Domain
SP	Service Provider
SBM	Secure Boot Module
TA	Trusted Application
TEE	Trusted Execution Environment
TFW	Trusted Firmware
TSM	Trusted Service Manager

2. Introduction

Chips used on smart phones, tablets, and many consumer appliances today have built-in support for a so-called Trusted Execution Environment (TEE). The TEE is a security concept that separates normal operating systems, like Linux, from code that requires higher security protection, like security-related code. The underlying idea of this sandboxing approach is to have smaller code that is better reviewed and test and to provide it with more rights. They run on the so-called Secure World (in comparison to the Linux operating system that would run in the Normal World).

TEEs have been on the market for a while and have been successfully used for a number of applications, such as payment. However, the technology hasn’t reached its full potential since ordinary developers who could make use of such functionality have a hard time getting access to it, and to write applications for it .

The industry has been working on an application layer security protocol that allows to configure security credentials and software running on a Trusted Execution Environment (TEE) for sometime. Today, TEEs are, for example, found home routers, set-top boxes, smart phones, tablets, wearables, etc. Unfortunately, there have been mostly proprietary protocols used in this environment.

This document describes features of a open trust protocol and related use cases.

3. Terminology

Client Application: An application running on a rich OS, such as an Android, Windows, or iOS application, provided by a SP.

Device: A physical piece of hardware that hosts symmetric key cryptographic modules

OTrP Agent: An application running in the rich OS allowing communication with the TSM and the TEE.

Rich Application: Alternative name of "Client Application". In this document we may use these two terms interchangably.

Rich Execution Environment (REE) An environment that is provided and governed by a rich OS, potentially in conjunction with other supporting operating systems and hypervisors; it is outside of the TEE. This environment and applications running on it are considered un-trusted.

Secure Boot Module (SBM): A firmware in a device that delivers secure boot functionality. It is also referred as Trusted Firmware (TFW) in this document.

Service Provider (SP): An entity that wishes to supply Trusted Applications to remote devices. A Service Provider requires the help of a TSM in order to provision the Trusted Applications to the devices.

Trust Anchor: A root certificate that a module strusts. It is usually embedded in one validating module, and used to validate the trust of a remote entity’s certificate.

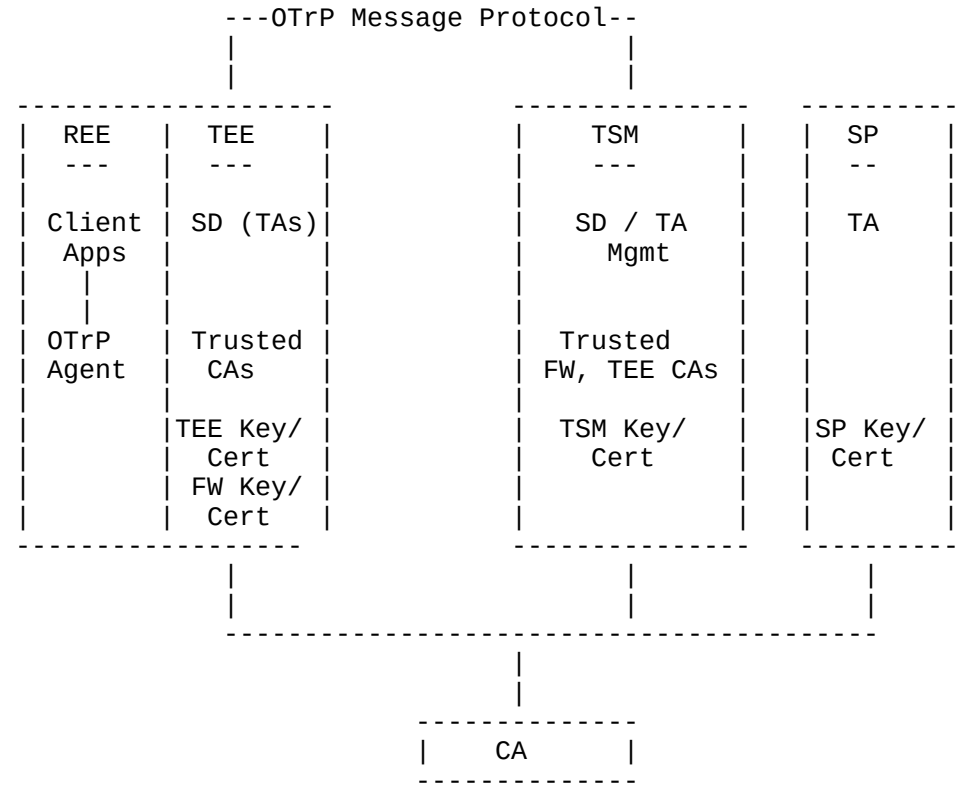
Trusted Application (TA): Application that runs in TEE.

Trusted Execution Environment (TEE): An execution environment that runs alongside but isolated from an REE. A TEE has security capabilities and meets certain security-related requirements: It protects TEE assets from general software attacks, defines rigid safeguards as to data and functions that a program can access, and resists a set of defined threats. There are multiple technologies that can be used to implement a TEE, and the level of security achieved varies accordingly.

4. Scenario and usecase of OtrP

OTrP Message is an open interoperable protocol that allows trustworthy TSM to manage security domains and contents running in different Trusted Execution Environment (TEE) of various devices.

Figure 1: OTrP System Diagram



TEE is usually used to solve the following security issues.In theory, in order to solve the above security issues, TEE which can exist in the corresponding TA to complete the corresponding security features.In conjunction with the description in Figure 1, the SP is responsible for developing the appropriate security application and becoming the end user of the OTrP protocol.

o The use of open environments: In general, some new kind device will be equipped with open environment to provide the operating system. This has the advantage that users can add applications at any time, and there is little need to worry about their impact on the stability and security of the device. However, the open environment makes the device face more and more foreign attacks. Device manufacturers want to take advantage of this operating system, but need to effectively control the behavior of the software running on the device.

- Verification: The traditional user authentication method requires a username and password. At present, this approach is increasingly considered safe, after all, consumers will use a less confidential password or re-use the existing password, and hackers are increasingly able to invade the consumer's account. Because an application or service provider typically stores personal verification and sensitive information on its own server, such hacking is the headline of the news, causing consumers to fear and shaken business confidence. Therefore, there is a need for a more sophisticated validation mechanism to ensure that the openers of the application enjoy the necessary flexibility while protecting the consumer.

- Privacy: The device stores more and more personal information (such as contact information, photos, photos and video clips), and even sensitive data (including credentials, passwords, medical data, etc.). In order to prevent this information from being exposed to loss, theft, malware or other negative events, we need adequate security to store, process and distribute such personal data.

- Content protection: Today, more and more devices with high-definition (HD) video playback and video streaming, mobile TV playback and host 3D games and other functions. They can even become content gateway devices, and to replace the traditional set-top boxes or game consoles. In this case, the playback function of the device becomes less important, and the security requirements are more and more prominent. Therefore, not only to protect the mobile device on the full HD or ultra-high-definition content, but also to protect the device to send the content to the TV through the channel.

- Enterprise Data Access: Enterprise IT professionals often exercise caution when opening access to their internal network, fearing that the device will carry malware, the device will be stolen, or when used outside the company, there will be attacks from the internal network The As a result, IT departments often establish green lists and red lists of equipment based on the security performance of the device. They are also concerned about the characteristics of these devices always open and the implementation of password protection and device lockout functions in shutdown mode.

- Financial risk: Financial transactions through networking devices, especially mobile devices, are becoming increasingly common. These transactions include booking, remote payments, near-field payments and financial electronic transactions. Moreover, the use of mobile devices in the retail outlets shopping has become

increasingly common. Moreover, mobile devices become a point-of-sale terminal, especially mobile point of sale, and this use case is now growing.

OTrP can be more efficient than the traditional OTA model, which can also reduce management overhead.The following two scenarios are used to explain why OTrP is required instead of OTA:

- Use Case 1 - Security vulnerability fixes:Imagining a fingerprint application stored in TEE appear an error, OTrP can help to fix this by several programers in one small team, but OTA may need to update the whole application by several teams in a company.

- Use Case 2 - Personalization data update: In IoT,there are lots of scenes that only need to update the personalized data without having to update the entire application like OTA.

Based on current research, this document provides an example of the application in the payment and IoT industry.

4.1. Use Case 1 - Payment

Payment technology(Especially mobile payments) is growing rapidly, in which the payment system continues to expand their trusted payment applications through existing technology and new technologies.

The TEE-based identity authentication application has a strong need for using otrp. The types of TA involved mainly include the following two kinds.

- Identification:Personal identification password and biometric.Because TEE can provides larger amount of memory and data transfer, TEE can store a trusted application that is used to complete a personal password acquisition or biological identification.For the development of the relevant TA of SP, the use of OTrP can easily send the latest trusted application to the device. At the same time, because TA and REE applications are independent of each other, REE side of the corresponding application only need to make little changes because of the OTrP.

- Security interface:Mobile payment is inseparable from the security interaction between end users and consumer devices. For example, the user needs to confirm the sensitive information displayed on the screen and enter the sensitive information (such as a password) through the keyboard.A TA such as keyboard in tee is needed.When designing a keyboard in tee, you should consider how to make a timely update when an application has a vulnerability to

ensure that user sensitive data is not compromised.In this case, it is necessary to use OTrP

4.2. Use Case 2 - IoT

In the field of Internet of Things, the purpose of TA is to use TEE to perform the functions of storing and managing sensitive data (eg, encryption keys) and performing sensitive operations (eg, authentication or encryption) in a secure environment in devices

In the smart home industry, a lot of security equipment are used TEE program to protect users of sensitive data, such as smart door locks. Some smart door locks even use biometrics, which makes this application in smart home very similar to the payment industry. Similarly, security products also need a secure and trusted remote update protocol to update the TA program in the device.

In the automotive (and bike) sharing industry, smart door locks use TEE technology to protect users' identity information. Operators who share automotive products need to remotely update trusted applications in smart locks.

Some high-value consumer electronics devices also have the need to use TEE and complete TA remote updates.For example, UAV devices use TEE to store sensitive operational instructions to prevent hackers from controlling the UAV's takeoff or landing by tampering with GPS location information.The manufacturer of the UAV needs to consider the easy management of the safety instructions in the UAV. For example, when the geographical location information of the prohibited flight area is changed, the equipment manufacturer should be able to update all the Corresponding information stored in the device .

In the automotive (and bike) sharing industry, smart door locks use TEE technology to protect users' identity information. Operators who share automotive products need to remotely update trusted applications in smart locks.

5. The functional requirements generated by the scenario and usecase

OTrP need to consider the requirements of OEM, SP, CA, TEE manufacturers, it will be helpfull to analysis the scenario and usecase to improve the functions of OTrP and solve the problems encountered in the deployment process.

The following lists the scenarios that OTrP users have already submitted. This section will continue to update according to the actual deployment of OTrP.

5.1. Use Case 1 - Resource-constrained interaction and multicast

In draft-pei-opentrustprotocol-03,OTrP is defined with a protocol which relies on IETF-defined end-to-end security mechanisms, namely JSON Web Encryption (JWE), JSON Web Signature (JWS), and JSON Web Key(JWK). Using JSON makes OTrP easier to accept by the developer, but in the case of limited resources, the use of Json is not a good choice, especially Json need to do some of the contents of the base64 transcoding.

As mentioned earlier, in the shared automotive industry, smart door locks have the requirement to use OTrP. In this scenario, the update of TA in the smart door locks is facing with the problem of communication bandwidth limitation and multicast demand. software and firmware updates often comprise quite a large amount of data. Therefore, it can overload a LLN that is otherwise typically used to deal with only small amounts of data, on an infrequent base. Rather than sending software and firmware updates as unicast messages to each individual device, multicasting such updated data to a larger group of devices at once displays a number of benefits.Binary solutions will be a better choice in the scenario such as low-power and lossy networks (LLNs),Low Power Personal Area Network(LWPAN)and Low Power Wide Area Network (LWAN).

As descrypted above, public key infrastructure (PKI) is used to do identiy authentication and securely exchange data over network. But, this is not a good choice for resource-constrained devices, especailly for IoT, to manage certificates and process TLS protocols, which need much memory and processing time.

5.2. Use Case 2 - TA and SD management owned by OEM and SP

There are three permission settings to manage TA and SD in TEE:

- The OEM wants to ensure that no service provider can talk to the TEE without the OEM’s prior approval. Once approved, the Service Provider is allowed to create security domains and install trusted apps. The OEM doesn’t require to be involved in that phase.

- The OEM wants to ensure that no service provider can talk to the TEE without the OEM’s prior approval. Once approved, the Service Provider is allowed to perform lifecycle management of trusted apps within a particular security domain but cannot create any new security domains without the OEM being involved and agreeing to it.

- The OEM and Service provider both want to be involved in every transaction with the TEE, and only when they both agree should the TEE accept the OTrP message and perform the action.

The first kind of permission setting can give SP manufacturers greater management authority, which can be very convenient management of SD and TA, but the security between SDs which set up by different vendors will not be able to be protected.

The second permission setting can give SP manufacturers a certain degree of control, TA can be easily issued to SD by SP. But at the same time, how to protect the security of TAM platform and TEE terminal should be considered.

The third permission setting can guarantee the management right of the OEM to the terminal, and avoid the terminal security risk caused by the insecurity of the TA program to a certain extent. However, in this authority set, the service provider to maintain the convenience of TA will be significantly reduced.

5.3. Use Case 3 - Batch mode

In draft-pei-opentrustprotocol-03, the following steps have to be done for deploying TA to device: establish trust between TEE and TSM, create Security Domain, and finally install TA in the device. This procedure will take at least three back and forth between TSM server and the device. While there are huge amount of IoT devices, this mechanism will make the burden of TSM server raise considerably.

In order to reduce the burden of TSM server, this procedure can be simplified by batch mode: TSM server will sign every command which runs in the device, pack them together in a command package, and send this package to a batch of devices. This one-time communication can significantly reduce the burden of TSM server. To make this happen, the DSI of these devices should be the same. DSI information can be organized by manufacture or by device model.

5.4. Use Case 4 - personalization data management

In many scenes, TAM only need to manage TA and SD personalization data, without having to update the entire TA or SD. Therefore, personalization data management function is required.The detail functions involved are as follows:

- Service provider key management(SD personalization data management). For example: In the field of IoT,a hotel(Service provider)an use this function to update a pair of keys to the lock of the door and the IoT device of customer.

- o TUI management(TA personalization data management).For example:In the field of financial, a bank can use this function to update the keyboard(Or other Trusted User Interfaces) of E-banking.

- o Other business data management.For example:In the field of payment,a company can use this function to update the QR code stored in TEE which is used for payment.

6. IANA Considerations

This memo includes no request to IANA.

7. Security Considerations

TBD.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <http://www.rfc-editor.org/info/rfc7515>.

[RFC7516] Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, DOI 10.17487/RFC7516, May 2015, <http://www.rfc-editor.org/info/rfc7516>.

[RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <http://www.rfc-editor.org/info/rfc7517>.

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <http://www.rfc-editor.org/info/rfc7518>.

8.2. Informative References

[GPTEE] Global Platform, "Global Platform, GlobalPlatform Device Technology: TEE System Architecture, v1.0", 2013.

Authors' Addresses

Dapeng Liu
Alibaba Group
Beijing
Beijing

Phone: +86-1391788933
Email: maxpassion@gmail.com

Qiang Fang
Alibaba Group
Beijing
Beijing

Phone: +86-15210569677
Email: qiangwu.fq@alibaba-inc.com