Electronic Design

MARC CANEL, Vice President of Security Systems,
ARM, www.arm.com

Exploring the Open Trust Protocol

Leading technology security experts recently collaborated together to assess the security challenges of connecting billions of devices across multiple sectors.

A group of leading technology security experts led by ARM, Intercede, Solacia, and Symantec recently released the results of a collaborative effort that set out to assess the security challenges of connecting billions of devices across multiple sectors, including industrial, home, health services, and transportation. Their conclusion was that any system could be compromised unless a system-level root of trust was established. And for the continued development of a truly connected world, there must be trust between all devices and service providers.

To deal with the risk, the companies collaborated on the Open Trust Protocol (OTrP), which combines a secure architecture with trusted code management. It leverages technologies proven in large-scale banking and sensitive data applications on mass-market devices such as smartphones and tablets.

Here, we explore the objectives of OTrP, how the technology works, its use cases, and the ecosystem delivering it.

WHY OTrP?

The objectives of developing OTrP were threefold:

1. Create an open international protocol defining how devices trust each other in a connected environment. The protocol would be based on existing open technologies with proven robustness and commercial attractiveness in existing markets. The Public Key Infrastructure (PKI) architecture, including the mature concepts around certificate authorities, was selected as the basic underlying system.

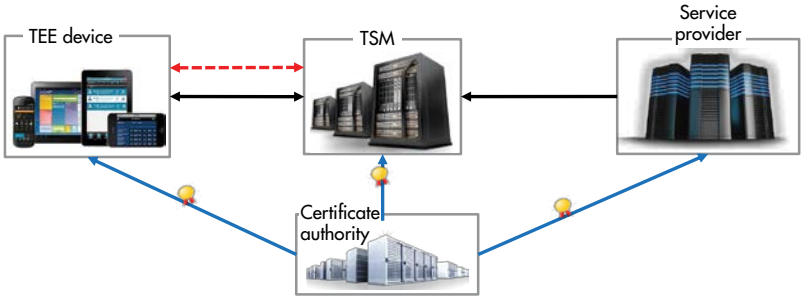
2. Given the reuse of the PKI architecture, it was imperative to create an open market for the certificates that would enable applications to authenticate resources in devices. It was a key requirement to have a mechanism by which certificate authorities can all compete and access devices in which they push their certificates to authenticate resources. In other words, having an open market for certificates was a key objective of the project.

3. With an open protocol, it's possible for multiple vendors to create either client or server solutions. This strategy enables an open and active market of developers of both client and server solutions.

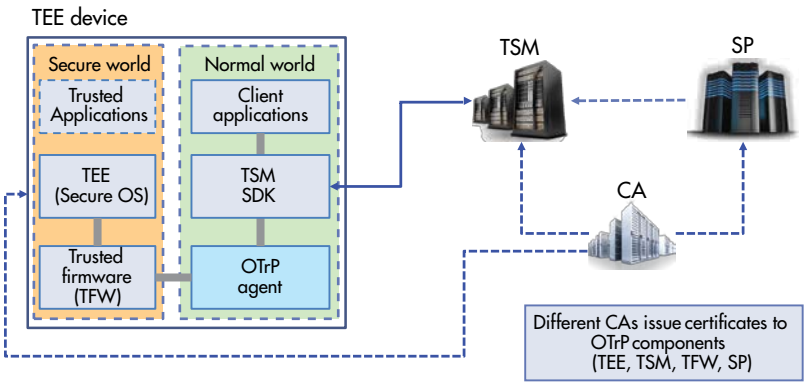
Collaboration began in early 2015, and membership of the OTrP Alliance soon grew to 13 companies. To encourage widespread adoption, the alliance also worked with international standards bodies such as the IETF and Global Platform to get OTrP adopted as a protocol within their organizations.

THE OTrP TECHNOLOGY

As a protocol, OTrP adds a messaging layer on top of the PKI architecture. OTrP reuses the Trusted Execution Environment (TEE) concept that increases security and robustness in the system by physically separating the regular operating system of a device from its security-sensitive applications. Given the heterogeneity of the devices in the connected world, Trusted Services Managers (TSMs) are used to manage keys in the devices to create security domains, authenticate resources,



1. The OTrP Ecosystem is composed of a Trusted Services Manager, a certificate authority, and a trusted execution environment.



2. The keys are generated by the certificate authority and provisioned during manufacturing.

and load applications.

OTrP defines a protocol between a TSM and a TEE and relies on IETF-defined end-to-end security mechanisms, namely JSON Web Encryption (JWE), JSON Web Signature (JWS), and JSON Web Key (JWK). The specification assumes that a device utilizing OTrP is equipped with a TEE and is pre-provisioned with a device-unique public/private key pair, which is securely stored. This key pair is referred to as the "root of trust." A service provider uses such a device to run Trusted Applications (TAs).

The key components of the OTrP system *(Fig.1)* are:

• *Trusted Services Manager (TSM):* The TSM is responsible for originating and coordinating lifecycle management activity on a particular TEE. It's at the core of the protocol and manages the trust in the devices on behalf of service providers. In addition, the TSM provides security domain management and TA management in a device, in particular over-the-air updates to keep TAs up to date.

• *Certificate authority:* Mutual trust between a device, a TSM, and services providers is based on certificates. A device embeds a list of root certificates, called trust anchors, from trusted certificate authorities that will be used to validate a TSM. A TSM will remotely validate a device by checking that a device comes with a certificate from a trusted certificate authority.

• *Trusted Execution Environment in the device:* The TEE resides in the device chip security zone and is responsible for protecting applications from attack, enabling them to perform secure operations.

OTrP establishes appropriate trust anchors to enable TEEs and TSMs to communicate in a secure way when performing lifecycle management transactions. The main trust relationships between the components are:

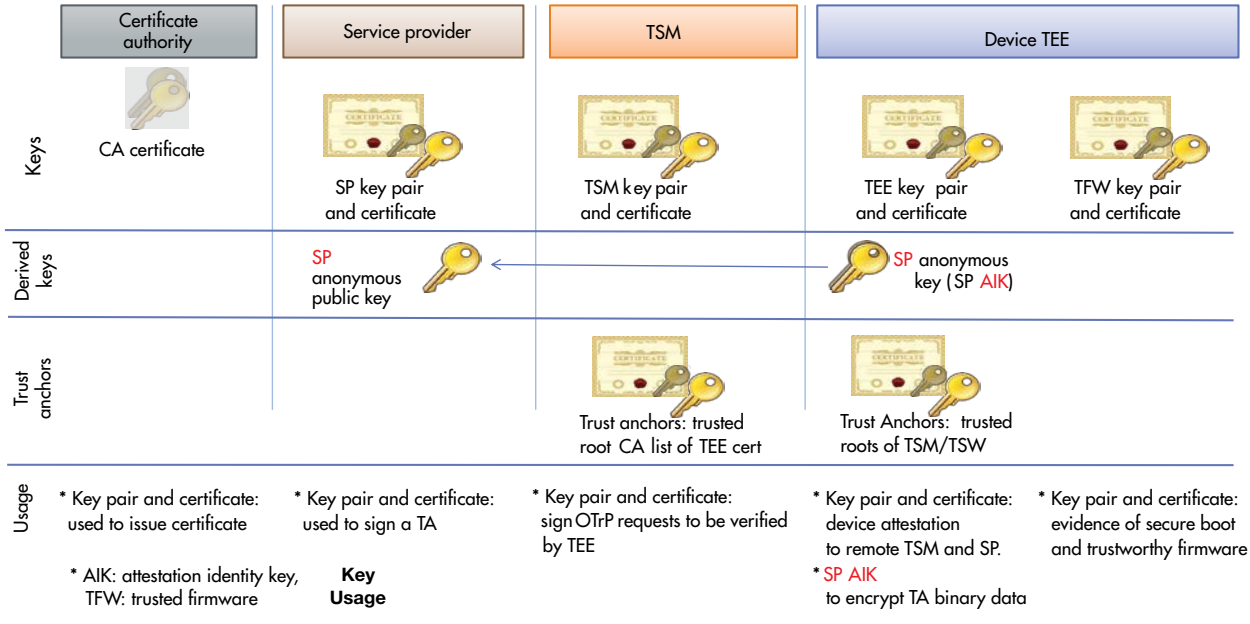
• The TSM must be able to ensure that a TEE is genuine.

• The TEE must be able to ensure that a TSM is genuine.

• The secure boot sequence of the TEE device must be able to ensure that the TEE is genuine.

TRUST MODEL OF THE OTrP

To establish trust between the various entities, OTrP assumes that certificates will be used to attest the identities of the key elements within the protocol. The certificate authority issues certificates to all the main components listed below and



3. The trust model is based on the architecture of keys.

the keys are typically provisioned during manufacturing *(Fig. 2)*:

- Service provider
- TSM
- Within the TEE device, two certificates are issued: one for the trusted boot sequence (also referred to as the trusted firmware), and one for the TEE .

OTrP builds a trust model based on the architecture of keys between the elements of the system *(Fig. 3)*.

SYSTEM ARCHITECTURE OF THE OTrP

OTrP assumes a system architecture with the following operations and building blocks *(Fig. 4)*:

- CA issues certificates to all OTrP components (SP, TSM, Device (TEE, Trusted Firmware)).
- The TSM vendor provides the SDK to communicate with TSM from a client application.
- TSM communicates with OTrP agent to relay the OTrP message between TSM and TEE. The OTrP agent is developed and distributed by the TEE vendor. It's responsible for routing OTrP messages to the appropriate TEE and implementing an interface as a service, SDK, etc.

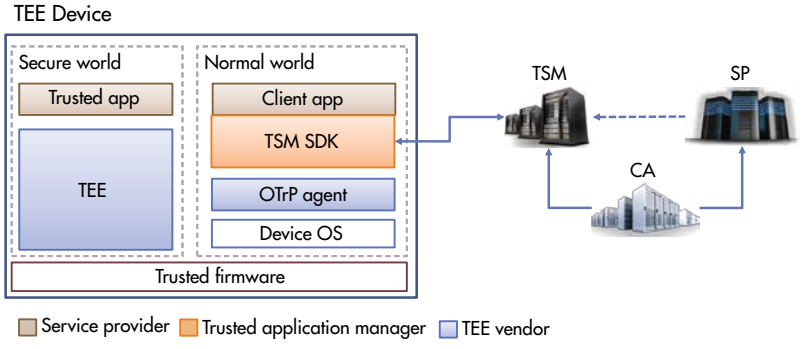
The OTrP Protocol

The protocol defines JSON messages for trust and remote TA management between a TSM and TEE:

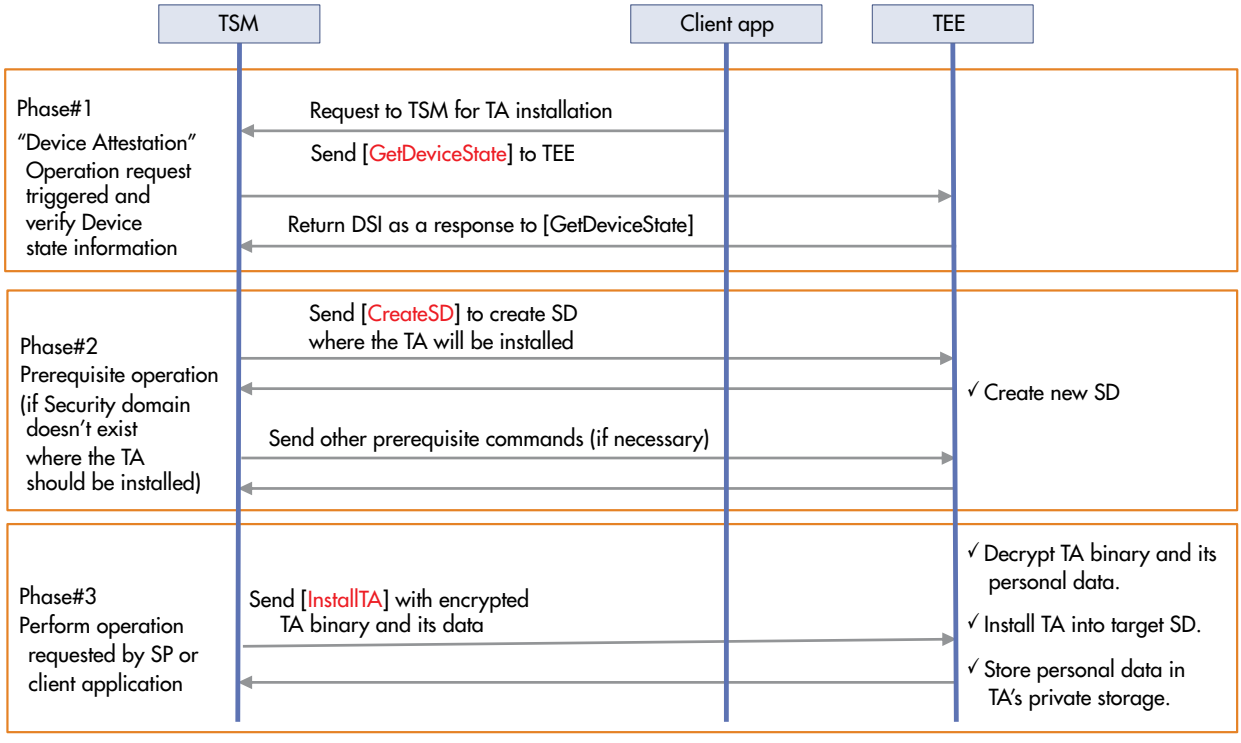
- Messages for device attestation (device integrity check) by a TSM and a device to trust a TSM.
- Messages for security domain management and trusted application management.
- Network communication among entities are left to implementations (OTrP is strictly a high-level messaging protocol and the implementation selects the communications stack) .

OTrP uses standard JSON messages and JSON security RFCs:

1. JSON signing and encryption RFCs
   a. RFC 7515, JSON Web Signature (JWS)
   b. RFC 7516, JSON Web



4. The OTrP system is based on an architecture of software building blocks.



5. The protocol flow is based on JSON messages.

Encryption (JWE)

c. RFC 7517, JSON Web Key (JWK)

d. RFC 7518, JSON Web Algorithms (JWA)

2. Currently supported encryption algorithms

a. A128CBC-HS256

b. A256CBC-HS512

3. Currently supported signing algorithms

a. RS256 (RSA 2048-bit key)

b. ES256 (ECC P-256)

The security of the protocol is enhanced by applying the following three measures:

1. Verifies validity of message sender's certificate.

2. Verifies signature of message sender to check immutability.

3. Encrypted to guard against exposure of sensitive data.

Figure 5 illustrates the protocol flow.

USE CASES

Examples of use cases for OTrP span both the mobile and the Internet of Things (IoT) marketplace. They're based on the dynamic loading of a security-sensitive application into the TEE of a client device via a TSM to perform a task for a server system. Here's a small subset:

- Identity management for enterprise systems
- Strong authentication and display protection for payment systems
- Enterprise systems: VPN, secure access to web sites
- Digital Rights Management applications
- Automotive systems: authentication, pay as you drive, in-application purchasing
- Healthcare: authentication, privacy management
- Home automation: authentication, privacy

OTrP ECOSYSTEM AND BUSINESS MODEL

By identifying the key components in the system, OTrP defines an ecosystem of partners that deliver trust in the applications of the devices. The TSM plays a central role in enabling trust between the partners.

OTrP as a protocol doesn't define a business model; it only defines the entities that take part in the ecosystem. The protocol integrates all of the tracking elements to enable any business model selected by the partners. In other words, the business model can be TSM-centric, or TEE-centric, or certificate-authority-centric, or application-centric, with either one of these entities having the ability to control the pricing of the trust services.

The protocol is available for download from the IETF website today for prototyping and testing.

Marc Canel has extensive experience in the mobile devices industry, driving software projects for the past 25 years, focusing on how mobile devices work with the enterprise world. He has served as Vice President of Security Systems at ARM Inc. for the past two and a half years, leading the next generation of security architectures to become the foundation for enterprise applications in a connected world. He promoted the definition of Trust systems and standards for devices in the internet. And he defined the architecture for the next generation Root of Trust for applications in devices.

Prior to ARM, he was Vice President of Software & Security Systems at Qualcomm, where he spent 18 years focusing on the features that make Qualcomm products more attractive to enterprises. He led the company to become a leader in the area of content protection and privacy management. He also worked on Qualcomm's software ecosystem management, supporting OEMs' customers looking for complete solutions. Prior to Qualcomm, he worked at IBM for 12 years, where he had various roles in product development and management roles in data networking products.

References:

https://www.arm.com/about/newsroom/connected-devices-need-e-commerce-standard-security-say-cyber-security-experts.php

http://www.ietf.org/id/draft-pei-opentrustprotocol-03.txt