Whitepaper

THE WISEKEY-OISTE ROOT OF TRUST AND ITS UNIQUE TRUST MODEL

A holistic approach to secure identities and transactions in the internet for people, applications and objects

WISeKey

Contents

Introduction

The Four Pillars of the Security for Electronic Transactions

An electronic transaction can be considered secure if one or several of the following criteria can be met:

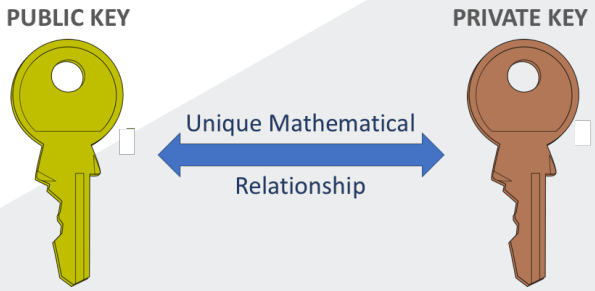
- Authenticity: We can assure the origin of the transaction (e.g. the person that signed an electronic document).
- Integrity: We can ensure that the transaction has not been tampered (e.g. the electronic signature)

What is a pki?

A Public Key Infrastructure (PKI) is commonly defined as "a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates", but the understanding of this definition requires us to explain some base concepts.

Public Key Cryptography

PKI uses cryptographic techniques based in public/private key pairs—two keys with a unique mathematical relationship. Public-key cryptography works in such a way that a message encrypted with the public key can only be decrypted with the private key, and, conversely, a message signed with a private key can be verified with the public key. This technology is the foundation to build the four pillars of transaction security: confidentiality, authentication, integrity, and nonrepudiation. We'll come later to these concepts.



*"What is encrypted with the **Private Key** can only decrypted with the **Public Key**, and what is encrypted with the **Public Key** can only decrypted with the **Private Key**"*

A subscriber or "end entity" (person, application or object) will have a Key Pair, where the private key must be kept secret, whereas the public key may be made widely available, usually presented in the form of a "Digital Certificate" that binds the public key with the identity of the subscriber, and that ensures that other parties can have confidence on the identity to which the public key belongs.

Using Public Key Cryptography for Encryption and Digital Signatures

There are multiple techniques to encrypt information, basically around two operational concepts:

- Symmetric Encryption: The same Key is used to encrypt and decrypt
- Asymmetric Encryption: We use one key to encrypt and another to decrypt

As described in the previous section, the private key is only known by the subscriber, therefore, if we want to encrypt a document or email and ensure that only the authorized person can read it, we will use the public key of that person (we could use our own public key if we want to encrypt something for our eyes only).

When we validate the digital signature of a document, we use the public key of the signer to decrypt the signature and be certain that only the person that controls the corresponding private key was the one producing the signature. Also, when encrypting a confidential document or email we will use the public key of the recipient person, and we want also to ensure that only that person will be able to decrypt the information with its private key. All these operations rely, therefore, on being sure beyond any reasonable doubt that we use the public key of the real person that signed the document or can decrypt an email.

PKI facilitates the secure electronic transfer of information for a range of network activities including, but not limited to, e-commerce, internet banking and confidential email. PKI enables parties to identify one another by providing authentication with digital certificates and allows reliable business communications by providing confidentiality through the use of encryption, and authentication data integrity and a reasonable basis for nonrepudiation through the use of digital signatures.

The concept of “Trust”

eSecurity and Trust

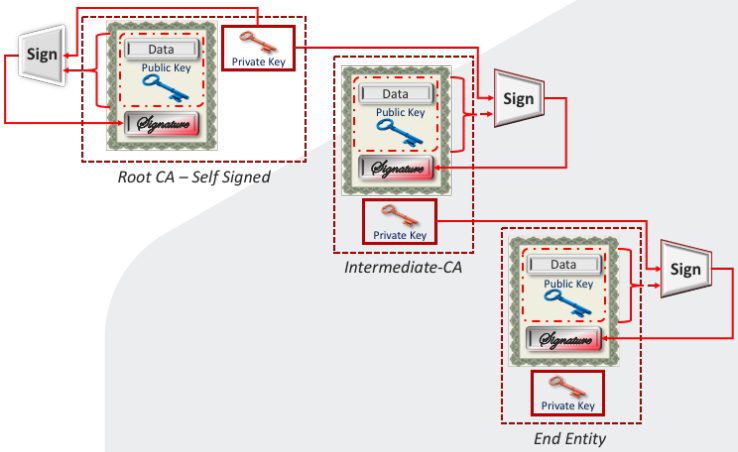
Trust and Information Security (or **eSecurity**) are concepts intimately linked:

- Applying eSecurity techniques is required to bring trust to electronic transactions. For example, applying a Digital Signature to a document will authenticate its origin and deems it worth of trust by the person receiving the document
- Most eSecurity techniques require the participants to Trust that the encryption key is really associated to its owner. For example to validate a digital signature, it’s required to use the public key of the user, being critical to be able to ensure that the key really belongs to him

To solve this dichotomy, we apply the concept of the “**Root of Trust**”, as a way to define the cornerstone of eSecurity.

Electronic transactions and the “Software Root of Trust”

In PKI the assurance on the owner of a private key is achieved by using an X.509 “Digital Certificate” that contains not only the public key but also the identity of the person that has the corresponding private key, together with an attestation issued by an entity that verified the identity of the person according to a series of security practices. The entity that makes the attestation is known as the “Certification Authority” (CA) and the attestation itself has the form of a digital signature, generated with the private key of the CA. **This implies in one of the first concepts around Trust: we can Trust in a Digital Certificate of an entity (person, application or object) only if we Trust the CA that signed the Digital Certificate.**



Typically, a PKI is built as a hierarchy of Certification Authorities, in such a way that the CA that issues the Digital Certificate of an entity is itself endorsed by a higher-level CA. This chain has two or three levels and at the top level we’ll find what is called the “Root Certification Authority” (Root CA). **This brings the second concept around Trust: We can Trust the whole hierarchy if we Trust the Root CA.**

Public Trust Vs Private Trust

The trust in a Root Certification Authority can be “Explicit” or “Implicit”.

For an Explicit Trust it will be required that the “Relying Party”, so the entity who will trust the digital certificates issued under that Root CA, performs some voluntary approval of the Root CA before trusting it. For example, the first time that a new Root CA is used, the user could be requested to accept the Root.

On the other side, we can also have an Implicit Trust if the Root is already preconfigured in the Software or Operating System. In this case the user can automatically Trust any certificate under that Root without any manual action.

In all operating systems and internet browsers it exists what is called a “Root Certificate Trust List”, this list contains a number of Root CAs that the software manufacturer embeds by default, and that the users can trust without any Explicit action. For a Root CA to be in the list, the software vendor requires compliance with their Root Certificate Program, being the most important Requirement for the Root CAs to fulfill an Independent Audit against some international standard like Webtrust or ETSI.

Microsoft, Apple, Google, Mozilla, Adobe and Java have such these programs and maintain a **Trust List** that includes a number of Root CAs that are trusted by their software when using digital certificates when browsing the internet (e.g. using SSL/TLS certificates to connect to a web site with HTTPS) or securing electronic transactions (to validate a digital signature in an email or PDF document).

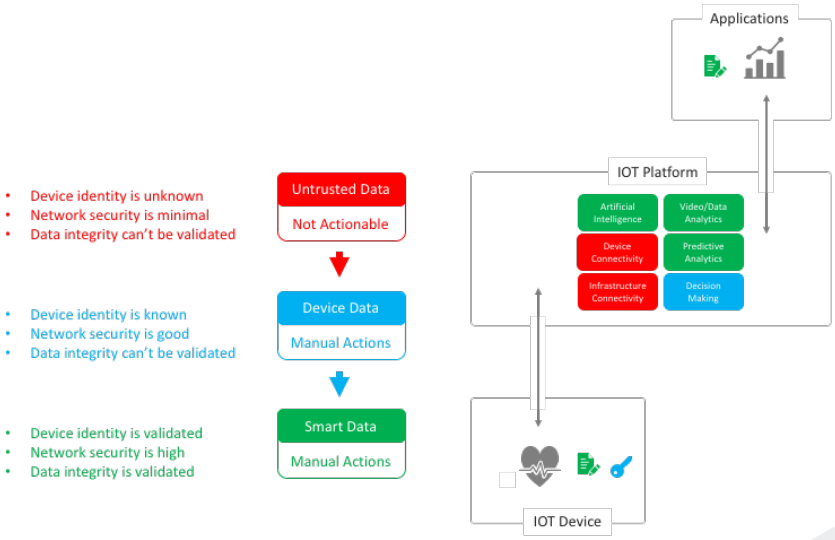
Most Governments also apply criteria on the CAs that should be trusted by citizens when doing eGovernment transactions or for a digital signature to be considered legally binding. These Governments will either impose a “National Root” or will define an accreditation process for a CA to be added in the “**National Trust List**”. These National Trust Lists can be consolidated in regional lists, as it’s the case of the European Union, which maintain an “European Trust List”.

It is understood that a Root CA can be “Publicly Trusted” when it is included in one of these Trust Lists, and “Privately Trusted” when there’s no compliance with the audit standards and the user is required to manually express trust in a Root. Of course, being in as many of these Trust Lists as possible ensures for a Root CA the usability and ubiquity required to reach any worldwide internet user and application.

IoT security and the “hardware Root of Trust”

The Internet of Things and the new classes of connected devices have more and more impact in our daily life. From an Intelligent Fridge to an Autonomous Car, everything trends to be connected and this creates new attack vectors and risks, as is not only about trusting data but also about taking automated decisions based on the data sent to or received from these devices, that can even put human lives at risk.

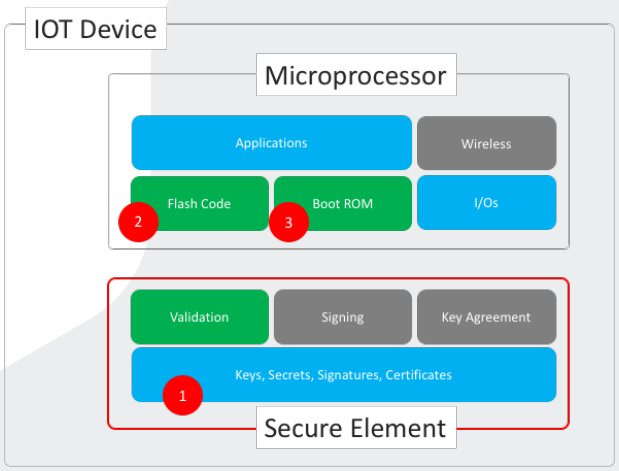
There are three classes of data sent by IoT devices, that require different levels of Trust:



For data to be fully actionable (so, take decisions based on it) we imperatively need to Trust this data, and this can only be achieved when we are sure that:

- We can trust on the Identity of the Device,
- We can ensure that the firmware running in the device has not been modified, and
- We can ensure that the data sent by the device has not been manipulated at any moment during the process.

In order to achieve the above, the traditional Digital Identity might be insufficient to protect an IoT device, as we require additional security mechanisms to ensure that the cryptographic operations and the secret keys used during encryption and digital signatures can be trusted during the whole life-cycle of the device.



A full “Hardware Root of Trust” will bring these benefits:

- [1] The core anchor that establishes the chain of trust for the device.
- [2] Protection of the firmware code and data.
- [3] Safeguards at boot time that ensures that the operating environment hasn’t been tampered with

WISeKey, through it’s “WISeKey Semiconductors” division, proposes a complete portfolio of solutions based in our Hardware Secure Element product families. These Secure Microcontrollers offer a reliable and cost-effective solution to protect the secret keys, cryptographic operations and device firmware.

The OISTE-WISeKey Trust Model

The OISTE Foundation

Founded in Switzerland in 1998, OISTE was created with the objectives of promoting the use and adoption of international standards to secure electronic transactions, expand the use of digital certification and ensure the interoperability of certification authorities' e-transaction systems. The OISTE Foundation is a not for profit organization based in Geneva, Switzerland, regulated by article 80 et seq. of the Swiss Civil Code. OISTE is an organization in special consultative status with the Economic and Social Council of the United Nations (ECOSOC) and belongs to the Not-for-Profit constituency (NPOC) of the ICANN. More information: http://www.oiste.org

OISTE as the owner of the Root of Trust

OISTE is the sole owner of a set of Root Certification Authorities, ensuring the independence of the Trust Model and isolating the users of the WISeKey Trust Services of possible changes in the ownership of WISeKey.

As owner of the Roots, OISTE delegates in WISeKey the role of "**Operator of the Trust Model**". Under this assignment, WISeKey operates the PKI and provides commercial trust services, but always under the supervision of the Foundation, who has the ultimate responsibilities to:

- Approve and Control the Subordinate Certification Authorities operating under the OISTE Roots
- Define the Certificate Policies that regulate the different types of identities that can be issued under the Trust Model: Identities for Persons, Applications and Objects
- Define the Certificate Practices Statement, that estipulate how the Certification Authorities will operate

OISTE allows third parties to operate under the Roots, and act as Subordinate Certification Authority, always when all the internal and external regulations are met, and when this compliance is demonstrated by means of an independent audit.

Both OISTE and WISeKey are subject periodically to these independent audits.

Our Unique Trust Model

WISeKey has developed a novel institutional and trust management framework that enables the Entity using it to convey trust through the segregation of ownership of components of the technological infrastructure, intellectual property rights, and policy creation authority among entities that are, by law, structured differently and in a manner that reinforces the management of trust. The institutional framework is composed of the following entities:

- Foundation: a legal entity in the form of a foundation as legally structured in Switzerland or its functional equivalent in other jurisdictions or internationally (herein the "Foundation");
- Operator: A separate legal entity contractually bound to pursue the objectives of the Foundation (herein the "Operator");
- Auditor: The independent auditor directly or indirectly designated by the Foundation;
- Supervisory Authority: The supervisory authority of the Foundation (in Switzerland this is the Swiss Federal Government);
- Policy Approval Authority: The PAA is a committee within the Foundation that has the mandate of drafting, adopting and maintaining the policies applicable to the Trust Management Infrastructure;
- Users: These are the communities of trust or individuals of such communities that form part of the Trust Management Infrastructure as clients of the Operator that wish to form part of or wish to be connected in some form or another to the Trust Management Framework and are accepted by the Operator to form part of it. They can be public or private sector entities, interoperable or not, in vertical sectors or across sectors (e.g. biometric passports, electronic ID systems, digital TV authentication systems, employee ID cards, etc.).
- The Trust Communities or Users of the Trust Management Infrastructure installed by, serviced by or the users of other such infrastructures that wish to form part of the institutional framework and are accepted as members by the Foundation.

In accordance with the Swiss law (and the law of many other jurisdictions), foundations do not have shareholders but are composed of capital and have an objective they must pursue. Under Swiss law, foundations are subject to annual audits by qualified and certified auditors and to supervision by the Swiss federal government to ensure that the capital of the foundation is used in conformity with the objectives of the foundation (Art. 84 Swiss Civil Code).