The Internet of Things

The Internet of Things (IoT) is a new vision of the Internet in which any type of object or thing that generates or consumes data on the network can be connected. It is the evolution of the original idea of the network of networks as the Internet of People (IoP), in which only people generated traffic, which later gave rise to the Internet of Services (IoS).

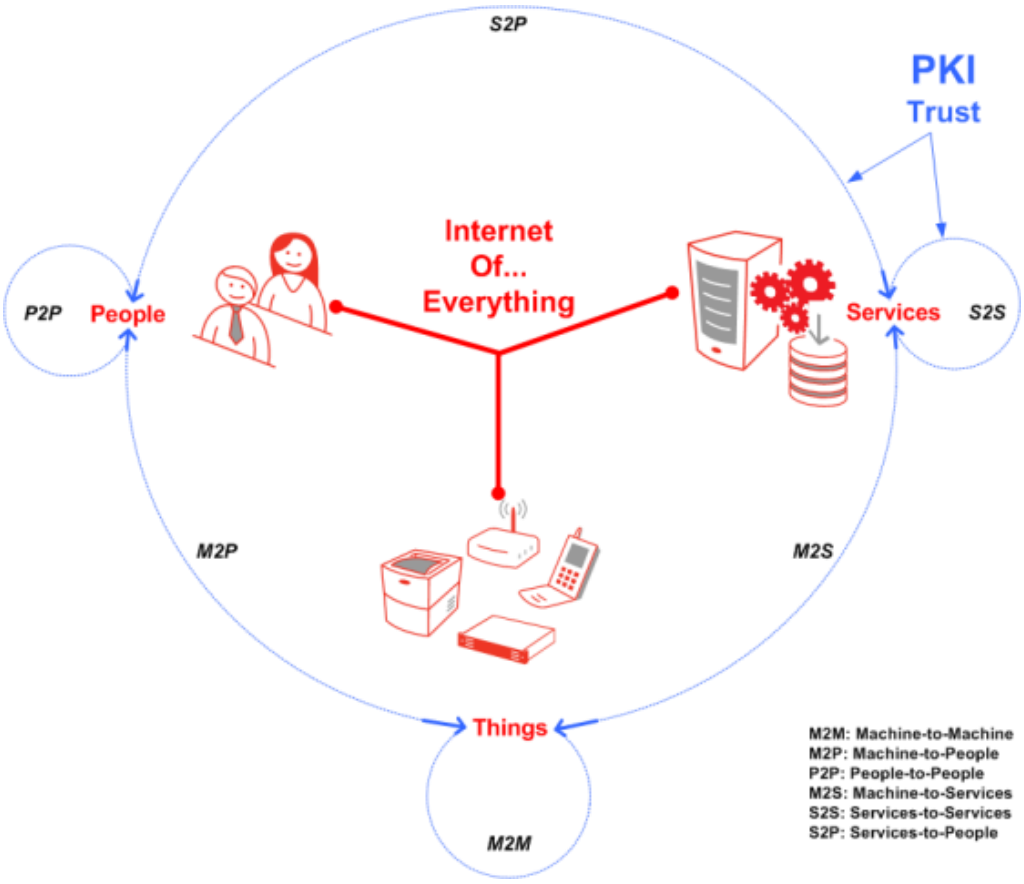
This new conception of the Internet of Things coupled with the advantages of the mobility factor have seen a new ICT ecosystem emerge that promises to revolutionize all industry sectors and all corners of society. It is estimated that currently 1,000 million users access Facebook via smartphone, and analysts expect 50,000 million objects to be connected to the Internet by 2020 and 1 billion by 2025. The fact that many things are connected to the Internet does not only suppose a challenge for network capacity. It will also change how people and services interact.

Why Security and Privacy Matters in the IoT

Things will talk to each other via Machine-to-Machine (M2M) communication. Some things will sample certain factors in the environment, for instance, temperature, brightness, a person's blood pressure, etc., and others will receive multiple samples and generate other events based on which big data will be created to feed Services via Machine-to-Service (M2S) communication, which in turn will provide valuable information to people directly via Machine-to-People (M2P) communication or indirectly and in more detail via Service-to-People (S2P) communication. For example, a sensor takes the blood pressure of a person and sends the data to a mobile app that the person has connected in a personal area network (PAN). The app does some basic data processing to detect blood pressure spikes and warns the user in real time, but it also sends the data to a remote service for storage and intelligent processing to be able to provide the most adequate health advice to the person based on their vital signs.

The Internet of Things and mobility also impact on interpersonal relationships. As well as things interacting with people (M2P), people will also interact with each other (P2P) via, and in collaboration with, things. For instance, ad hoc wireless networks will be spontaneously created between people's mobile devices and other things for them to

interact when they are in proximity, which will give rise to new forms of relationships and value-added services.



This new ecosystem also provides benefits to industry, from the known cases in the energy industry with smart metering, smart grid, green energy, etc.; the telecom industry with intelligent networks; the transport and automobile industry; the logistics sector; and the consumer goods sector with intelligent lighting, electrical appliances (TVs, fridges, etc.), entertainment (consoles, tablets, etc.), health, tourism, smart office, smart cities, etc., all making up what is known as the home grid, home area network (HAN) or smart home.

Without a doubt, all the potential of this new active ecosystem of things and people necessarily depends on the communications and information being secure so the system can transmit the trust and privacy required to the users and competent authorities regulating the different sectors.

PKI Technology the Best Guarantee of Trust in the IoE

It is well known that PKI technology is the most secure option for communications and interactions between People and Services (S2P), between Services and Services (S2S) and between People and People (P2P) via Services. Take, for instance, the TLS/SSS standards for secure channels, electronic signatures for protecting content, etc. Along the same lines, the industry and community in the Internet of Everything (IoE) is made up by the Internet of the Things (IoT). This includes:

Classic examples:

- PKIX and SCEP protocols for provisioning PKI material to network devices: routers, firewalls, etc., and mobile devices in some operating systems.
- 3GPP standards for LTE/4G mobile telecommunications antennas.

Newer examples:

- Smart Energy Profile 2 (SEP2), which includes the majority of the industry through the HomePlug® Alliance, Wi-Fi Alliance®, HomeGridForum® and ZigBee® Alliance alliances, including Bluethooth®SpecialInterestGroup, which recommend a PKI based on elliptic curves and X.509 certificates.
- The AllJoyn open source framework in the AllSeen Alliance that recommends PKI technology based on X.509 certificates as the most secure authentication method.
- The EST (EnrollmentoverSecureTransport) proposal as an advance and improvement on classic protocols such as SCEP for provisioning PKI material in devices.
- Etc.

New KeyOne Functions for Managing Digital Certificates

With this new functionality, the KeyOne PKI platform supports managing the registration of certificates required for the development of trust in the IoE. KeyOne provides a complete solution with all the components for supporting any provisioning scenario and the management of the life-cycle of certificates, either from a single CA, a hierarchy of CAs or multiple hierarchies. The solutions adapt to the range of PKI scenarios possible, i.e., for:

People and Services, for which sophisticated certification policies are needed with requirements for interoperability and trust in open communities of any size (from a few thousand to millions of users). Certificate revocation, validation and renewal are also required.

Things in general and devices in particular, for which deployments are usually in a closed environment without requirements for revocation, validation or renewal, however,

on a scale of millions of units. This requires meeting the very highest requirements of quality, availability and speed, especially in production lines in which the PKI material is provisioned to devices in real-time.

In any case, for People, Services or Things, KeyOne provides the highest security assurance via CC EAL4+ certification and the use of specialized hardware (HSM) as a result of collaboration with its technology partners SafeNet and Thales, which also have certified solutions.

Social

With Facebook and Google leading the way, the social networks and major Internet service providers are, in actual fact, the biggest identity providers (IdP) that have existed. There is nothing comparable in the history of identity and access management (IAM) to the capacity of these social IdPs. With Facebook alone, 1,300 million registered users can collaborate through single sign-on (SSO) via millions of integrated third-party applications. Users can even have various social eIDs (Facebook, Google, Twitter, etc.) and, through identity federation techniques, an even greater number of users and applications can be reached to provide ubiquitous access to any content, from anywhere, from any device, at any time.

Furthermore, like IdPs, these major providers implement a user-centric paradigm that allows users to manage a range of identity information and attributes that they can share in a controlled manner with the applications and services they access, which enables them to protect their privacy.

Mobile

The mobile device is becoming the direct link between individuals and the digital society. Of little surprise, then, are all the predictions that wireless traffic (on Wi-Fi and via mobiles) and the rate of applications created for these environments will surpass the traditional wired environments.

From the point of view of identity and the user's exclusive control over it, the mobile device is the perfect tool. Until now, no other electronic device was kept so close to the user, both from a service perspective and with regard to security and privacy. Based on these premises, the mobile device is also an important security factor for electronic transactions as it can enable physically providing the user with "something you have" and "something you are" factors. This last factor is increasingly present through the use of biometric fingerprint and image and voice recognition systems integrated in mobile devices.

Cloud

The adoption of Cloud technologies is considered unstoppable. Hybrid deployments appear to be the most widely adopted, not only during the transition to the cloud, but permanently. Mainly because organizations have sensitive systems and data they do not

want to store externally and manage in the Cloud. This includes corporate identity data and information.

Organizations want to make their existing on-premises systems compatible with the new applications and services in the cloud, but they also want to manage the identities of their user population in a unified manner. In this sense, it is becoming more common for organizations to acquire new IT and software as services for their corporate users to whom they offer, in a unified manner, both the on-premises and external resources in the Cloud, making compatible corporate access control and single sign-on (SSO).

Safelayer's eIDAS Platform

Safelayer's eIDAS (electronicIDentity, Authentication and Signature) platform was designed and built to take into account the successful factors of the social, mobile and cloud phenomenon. This value proposal intends to facilitate trust and convenience in electronic transactions. Therefore, the platform has adopted the following SoMoClo principles and values:

- Full support for World Wide Web standards and practices
- User-centric paradigm that observes privacy.
- New model of economies of scale and value creation known as the API Economy.
- Dynamic adapting of security and user convenience based on risk.
- Mobile device as the future user eID in the digital societypar excellence.
- Hybrid cloud-based model that uses identity federation as the link to the company