Internet de las cosas

La Internet de las Cosas (IoT) es una nueva visión de Internet en la que se conecta cualquier tipo de objeto o cosa que genera datos en, o los consume de, la red. Se trata de la evolución de la concepción inicial de la red de redes como la Internet de las Personas (IoP), en la que sólo los humanos generaban tráfico, que posteriormente dio cabida a la Internet de los Servicios (IoS).

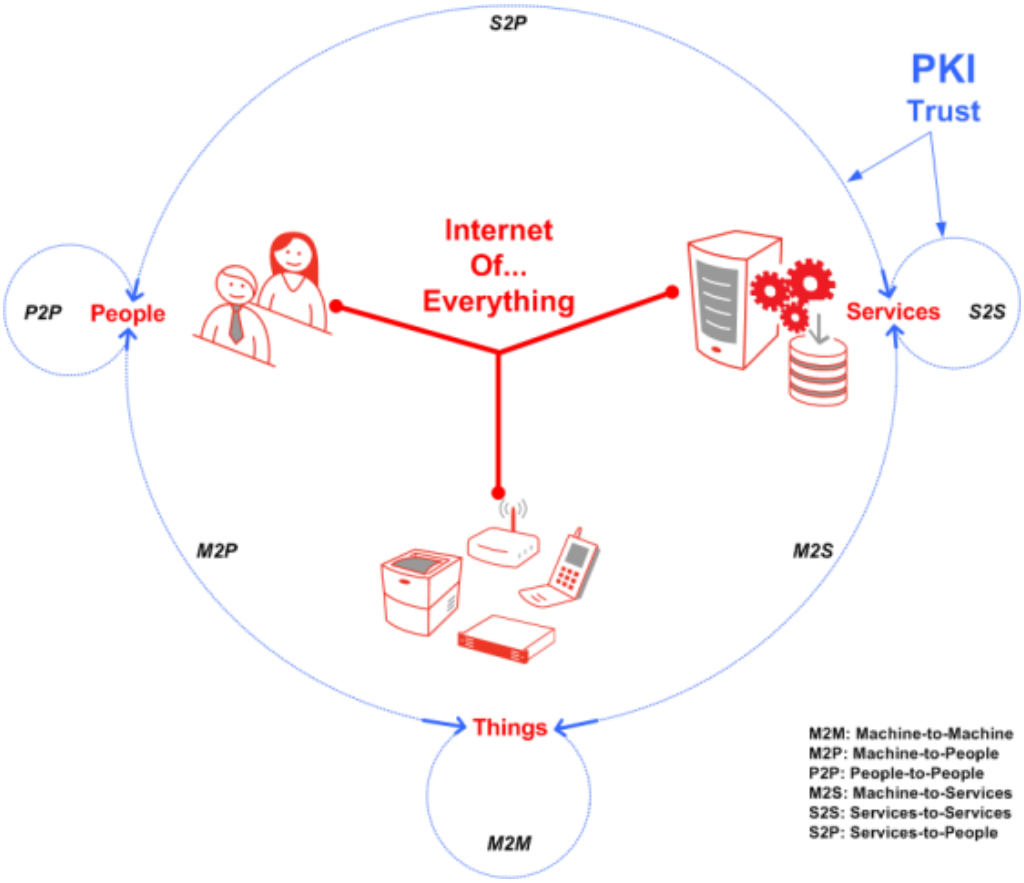
La nueva concepción de Internet de la Cosas (IoT) junto a la tracción del factor movilidad en las Personas han dado lugar a un nuevo ecosistema TIC que promete revolucionar todos los sectores de la industria, así como todos los recovecos de la sociedad. Actualmente, se estima que 1.000 millones de usuarios acceden a Facebook mediante un teléfono inteligente, y los analistas dicen que para el año 2020 se prevé que habrá conectados a Internet 50.000 millones de objetos, y para 2025 se espera 1 billón de objetos. El hecho que existan muchas cosas conectadas a Internet no sólo supone un reto a la capacidad de la red, sino que también cambiará el modo en que las personas y los servicios interaccionen.

Por qué la seguridad y la privacidad en la IoT son importantes

Las cosas dialogarán entre ellas en una forma de comunicación denominada Machine-to-Machine (M2M) de modo que algunas cosas simplemente muestrearán el ambiente, por ejemplo, la temperatura, la luminosidad, la presión sanguínea de una persona, etc. y otras cosas recibirán múltiples muestras y generarán otros eventos a partir de estos, en definitiva, dango lugar a un volumen masivo de información (Big Data) cuyo procesado inteligente, alimentará a Servicios -Machine-to-Service (M2S)- que a su vez proporcionará información valiosa a las personas de forma directa –Machine-to-People (M2P)- o indirecta y más elaborada –Service-to-People (S2P)-. Por ejemplo, un sensor toma muestras de la presión sanguínea de una persona y envía los datos a una App móvil que la persona tiene conectada en una red personal –Personal Area Network (PAN)-. La App hace un mínimo procesado de los datos que le sirve para detectar picos de presión y avisar al usuario en tiempo real, y además, re-envía dichos datos a un servicio remoto para su almacenamiento y procesado inteligente de forma que pueda recomendar a la persona una pauta de salud más adecuada a su ritmo vital.

La relación inter-personal también cambia con la Internet de las Cosas y la movilidad. No solo las cosas se relacionarán con las personas (M2P), sino que las personas se relacionarán entre ellas (P2P) a través de, y en colaboración con, las cosas. Por

ejemplo, se crearán espontáneamente redes ad-hoc inalámbricas entre dispositivos móviles de personas y otras cosas que les permitirán interaccionar en proximidad dando lugar a nuevas formas de relaciones y servicios de valor añadido.Desde el punto de vista de la identidad y del exclusivo control del usuario sobre ésta, el dispositivo móvil es la herramienta perfecta. Hasta el momento, no existe ningún otro dispositivo electrónico más apegado al usuario, tanto desde el punto de vista de servicio como de preocupación en cuanto a su seguridad y privacidad. Con estas premisas, el dispositivo móvil se convierte también en un factor de seguridad importante para las transacciones electrónicas pudiendo aportar físicamente al usuario factores “algo que se tiene” y “algo que se es”, éste último cada vez más presente con los sistemas biométricos de huella dactilar, reconocimiento de imagen y voz integrados en el dispositivo móvil.



Mencionar también los beneficios en la industria que proporciona este nuevo ecosistema, desde los conocidos casos en la industria de la energía, Smart Metering, Smart Grid, Green Energy, etc. la industria de las telecomunicaciones con las redes inteligentes, la industria del transporte y automoción, la industria de la logística, o la industria del consumo con luces inteligentes, electrodomésticos (TV, frigoríficos, …), entretenimiento (consolas, tabletas, …), Salud, Turismo, Smart Office, Smart Cities, etc. todo ello conformando lo que se conoce como Home Grid, Home Area Network (HAN) o casa inteligente.

Sin duda, todo el potencial de este nuevo ecosistema activo de cosas y personas depende necesariamente de que las comunicaciones y la información sean seguras

para que el sistema pueda transmitir la confianza y privacidad necesaria a los usuarios y autoridades competentes que regulan los diferentes sectores.

La tecnología PKI como el mejor soporte a la confianza en la IoE

Ya es bien conocido que la tecnología PKI es la opción más segura para las comunicaciones y relaciones entre Personas y Servicios (S2P), entre Servicios y Servicios (S2S), y entre Personas y Personas (P2P) a través de Servicios. Véanse las prácticas con los estándares TLS/SSL en securización del canal, firmas electrónicas para proteger contenidos, etc. Y en la misma línea, la industria y comunidad en la Internet de Todo (IoE) está conformando la Internet de las Cosas (IoT). Algunos ejemplos:

- Los ya clásicos:
  - Protocolos PKIX y SCEP para el aprovisionamiento de material PKI en dispositivos de red: routers, firewalls, etc., así como dispositivos móviles en algunos sistemas operativos.
  - Estándares 3GPP para antenas de telecomunicaciones móviles LTE/4G.
- O los nuevos:
  - Smart Energy Profile 2 (SEP2) que aglutina la mayor parte de la industria alrededor de las alianzas HomePlug® Alliance, Wi-Fi Alliance®, HomeGrid Forum® y ZigBee® Alliance, incluyendo Bluethooth® Special Interest Group, recomiendan una infraestructura PKI basada en curvas elípticas y certificados X.509.
  - El framework de open source AllJoyn dentro de AllSeen Alliance el cual recomienda la tecnología PKI basada en certificados X.509 como el mecanismo de autenticación más seguro.
  - La propuesta EST (Enrollment over Secure Transport) como avance y mejora de protocolos clásicos como SCEP para el aprovisionamiento de material PKI en dispositivos.
  - Etc.

Nuevas funciones de gestión de certificados digitales de KeyOne

Con esta nueva funcionalidad, la **plataforma PKI KeyOne de Safelayer** permite gestionar el registro de certificados requerido para el desarrollo de la confianza en la IoE. Es una solución completa con todos los componentes para soportar cualquier escenario de aprovisionamiento y gestión del ciclo de vida de los certificados, ya sea en una única CA, una jerarquía de CAs o múltiples jerarquías. Se acomoda a los diferentes escenarios PKI posibles, a saber, para:

- Personas y Servicios, en los que se deben desplegar políticas de certificación sofisticadas con requisitos de interoperabilidad y confianza en comunidades

abiertas de cualquier tamaño (entre unos pocos miles a millones de usuarios), revocación, validación y renovación de certificados.

- Cosas en general, y dispositivos en particular, en los que los despliegues se suelen realizar en un entorno cerrado, sin requisitos de revocación, validación ni renovación, no obstante, en una escala de millones de unidades. Aquí, se requiere cumplir con los más altos requisitos de calidad, disponibilidad y velocidad, sobre todo en las líneas de producción en los que se aprovisiona el material PKI a dispositivos en tiempo real.

En cualquier caso, ya sean Personas, Servicios o Cosas, **KeyOne** cumple con el mayor grado de garantía de seguridad mediante la certificación CC EAL4+ de la solución así como con el uso de hardware especializado (HSM) fruto de la colaboración con partners tecnológicos SafeNet y Thales, también con soluciones certificadas.