LIBRO ELECTRÓNICO

¿NECESITA SEGURIDAD? TODO LO QUE NECESITA ES PKI

digicert®

ÍNDICE

DE LA FRONTERA DE ALASKA A LOS CONFINES DEL ESPACIO EXTERIOR

En 2013, un lluvioso día de verano, una avioneta equipada con flotadores se estrelló cuando sobrevolaba a baja altura una zona montañosa situada cerca de Petersburg (Alaska, Estados Unidos). La aeronave, con seis pasajeros a bordo, se dirigía al glaciar LeConte en una excursión turística. Cuando comenzó a ascender por los acantilados de Horn Cliff a través del puerto de montaña, el piloto calculó mal, perdió el control de la avioneta y, tras varias vueltas de campana, se precipitó sobre el suelo llevándose por delante los gigantescos árboles de hoja perenne que encontró a su paso.

Los pasajeros que sobrevivieron al accidente, heridos y atrapados en mitad del acantilado, no tenían la menor esperanza de salir de la montaña con vida por sí solos. Faltaban muy pocas horas para que cayera la noche y, en Alaska, incluso en pleno junio, la oscuridad es sinónimo de heladas en un lugar sin cobertura móvil ni carreteras. Solo un equipo de rescate aéreo podría salvarlos entre los escombros.

Ochocientos kilómetros sobre sus cabezas, la constelación de satélites Iridium captó la señal de la radiobaliza de emergencia del vehículo y transmitió la llamada de socorro y la ubicación a las autoridades de búsqueda y salvamento. El dispositivo, que era compatible con el satélite Iridium, no solo había enviado una llamada de mayday por GPS o radio, sino que había rastreado todos los movimientos de la aeronave desde el despegue hasta el accidente, trazando una pista digital de todo el vuelo de principio a fin. Esto fue posible gracias a que cada uno de los 66 satélites de Iridium describe una órbita perfectamente coreografiada alrededor de la Tierra, comunicándose entre la superficie terráquea y entre sí para cubrir cada milímetro del planeta durante todo el día. En la red de la constelación Iridium, los dispositivos en condiciones de funcionamiento son visibles a cualquier hora del día en cualquier lugar del mundo: desde la Antártida hasta Alaska.

Aunque este particular tipo de dispositivos de rastreo y señalización de emergencias no es obligatorio en todos los aviones, cada vez son más los pilotos y propietarios que lo instalan, sobre todo cuando se trata de avionetas tras recorrer grandes distancias.

La mayoría lo hace para estar tranquilo, pero en algunos casos supone la diferencia entre la vida y la muerte.

De esta forma, localizar el lugar del accidente con precisión permitió a la guardia costera estadounidense llegar hasta allí con sus helicópteros y, en cuestión de unas pocas horas, rescatar a todos los supervivientes. Tras sacarlos de los escombros y trasladarlos a los servicios médicos, Alaska Public Media[1] entrevistó al portavoz de la guardia costera,

[1] https://www.alaskapublic.org/2013/06/05/one-dead-six-survive-float-plane-crash-near-petersburg/

Grant DeVuyst. A propósito del dispositivo de señalización de emergencias, afirmó: «Si no hubiese sido por él, nunca nos habríamos enterado de que había problemas. Fue el único motivo por el que nos acercarnos hasta allí y pudimos encontrarlos».

En estas infrecuentes emergencias, cuando hay vidas en juego, un piloto tiene que saber que la red de satélites Iridium rastreará el vuelo y recibirá la señal de auxilio para que un equipo de rescate pueda acudir en su ayuda.

La señal debe estar protegida de intercepciones, el dispositivo de emergencia debe estar autenticado y la red debe estar a salvo de interrupciones. Si falla alguna parte de la constelación Iridium, el riesgo de perder vidas es mayor. Es un nivel de confianza máximo y no puede haber margen de error; por eso, la constelación de satélites Iridium está protegida con infraestructura de clave pública (PKI, por sus siglas en inglés).

«LA INFRAESTRUCTURA DE CLAVE PÚBLICA ES DE TOTAL CONFIANZA PARA PROTEGER DESDE LAS PROFUNDIDADES DEL OCÉANO HASTA LOS CONFINES DEL ESPACIO EXTERIOR».

Brian Trzupek
Vicepresidente de producto de DigiCert

LA CONFIANZA ES UNA NECESIDAD DINÁMICA

Cuando los criptólogos británicos James Ellis y Clifford Cocks desarrollaron por vez primera la idea de «cifrado no secreto» en la década de 1970, no podían ni imaginar que esa idea se utilizaría en decenas de millones de sitios web de todo el mundo. Por aquellos tiempos, Internet no era más que un proyecto de la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA, por sus siglas en inglés) estadounidense, con un uso más bien limitado para que los investigadores universitarios pudieran compartir datos y resultados entre sí.

Décadas después, el mundo había cambiado para siempre y la infraestructura de clave pública de Ellis y Cocks cobraría impulso en plena era de la información como escudo de protección frente a las técnicas de hackeo y el fraude. Todavía hoy, si un sitio web es de confianza es gracias a la infraestructura PKI.

Pero la invención de la red de redes —que, por sí misma hubiera sido suficiente para definir una era de desarrollo humano— se vio seguida de inmediato por una segunda revolución de dispositivos conectados. De la noche a la mañana, como quien dice, todo (desde los refrigeradores hasta las aplicaciones de banca online) pasó a formar parte de un ecosistema global de redes, dispositivos, aplicaciones y usuarios, comunicándose de una punta del mundo a la otra.

La velocidad de crecimiento fue, y continúa siendo, tan rápida que solo puede medirse en órdenes de magnitud. En un momento en el que cientos de miles de personas están volcadas en el desarrollo de nuevas ideas para conectar a millones de personas a miles de millones de cosas, la necesidad de una mayor seguridad ha aumentado a un ritmo exponencial.

Pero, con todo lo bueno que ha traído la era de la información —en términos de intercambio cultural o de avances en el campo de la medicina, por ejemplo—, esta descomunal red de comunicaciones ha abierto nuevas posibilidades para oportunistas y delincuentes, quienes se aprovechan de nuestros usuarios y su buena fe.

La solución a esta amenaza es muy sencilla: dotar a todo lo que se conecta de la máxima seguridad posible. Y la infraestructura de clave pública proporciona esa seguridad fundacional. Una solución de seguridad e identidades que sea lo suficientemente confiable como para proteger los datos más sensibles, pero lo suficientemente flexible como para funcionar en las invenciones más vanguardistas. La infraestructura PKI deja vía libre para disfrutar sin preocupaciones de las ventajas de un mundo que puede comunicarse de forma prácticamente instantánea en todo el planeta… y hasta en el espacio.

LA INFRAESTRUCTURA DE CLAVE PÚBLICA PROPORCIONA ESA SEGURIDAD FUNDACIONAL.

Un mundo cada vez más amenazado

Cada día surgen nuevas e ingeniosas ideas que, basadas en la conectividad, mejoran la supervisión, la eficiencia y la seguridad de computadoras, aplicaciones y dispositivos. Pero cada nueva conexión representa una nueva vulnerabilidad, un potencial punto de entrada a todo lo que se comunica con esa aplicación o dispositivo.

Los riesgos financieros son conocidos. Llevamos años viendo lo que ocurre cuando los ciberdelincuentes explotan una brecha de seguridad. En 2017, una conocidísima firma de préstamos al consumo fue condenada a pagar una indemnización de 700 millones de dólares estadounidenses por los daños y perjuicios ocasionados por una gran brecha de datos.[2] Un estudio llevado a cabo por Ponemon/IBM en 2019 concluyó que el costo medio de una brecha de datos podía ascender, en el mejor de los casos, a 4 millones de dólares[3]. Y, ese mismo año, el estudio Consumer Breach Report de ForgeRock[4] documentó una pérdida de 17 760 millones de dólares solo en el sector de la atención médica. De hecho, el sanitario, que acaparó para sí el 45 por ciento de las brechas, fue el sector más atacado en 2019.

Pero si bien el costo financiero del sector sanitario es, de por sí, escalofriante, lo que llama más la atención quizá es el número de ataques y sus características.

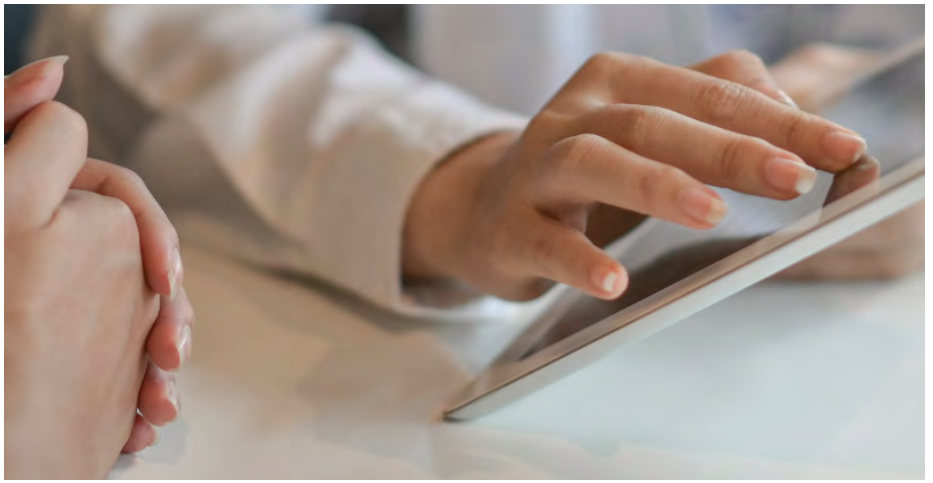
[2] https://investor.equifax.com/news-and-events/press-releases/2019/07-22-2019-125543228 [3] https://digitalguardian.com/blog/whats-cost-data-breach-2019 [4] https://healthitsecurity.com/news/health-sector-most-targeted-by-hackers-breach-costs-rise-to-17.76b

Estas pérdidas se repartieron entre 382 brechas distintas, dirigidas a las redes de organizaciones sanitarias mediante el uso de diversos métodos. A diferencia del pasado, cuando las principales víctimas de los ataques a redes y sitios web eran los bancos y las transacciones entre empresas y consumidores, ahora los ciberdelincuentes se dedican a explotar las vulnerabilidades de los dispositivos y usuarios menos formados para extraer valor de la información como tal.

Todo esto significa que, pese a que los recursos no han aumentado al mismo nivel que las amenazas, la seguridad es una carga cada vez mayor para las organizaciones. Por mucho que las historias médicas digitales, los monitores conectados y las herramientas terapéuticas inteligentes hayan revolucionado la asistencia médica, los profesionales que los utilizan no son expertos en las vulnerabilidades de seguridad, por lo que los departamentos de TI tienen que ser hábiles a la hora de negociar los desafíos que conllevan las restricciones presupuestarias, las nuevas tecnologías y la normativa local y nacional.

Corren tiempos interesantes y prometedores en el sector de la información y todo el mundo, sin excepción, tanto para el pequeño consumidor como para las grandes multinacionales y los estados, que se benefician de los avances tecnológicos a los que nos conectamos. Pero para los profesionales informáticos, que trabajan tras bambalinas, comprender las amenazas que surgen con las nuevas tecnologías e implementar soluciones manejables para eliminar el riesgo puede ser una tarea abrumadora.

Para combatir esta realidad en la que las amenazas proliferan sin control, los profesionales de la seguridad necesitan una solución flexible que pueda implementarse rápidamente, fácil de gestionar y con la capacidad de responder a cualquier ataque, aun mientras se amplía o actualiza para adaptarse a las necesidades de crecimiento y cambio de la organización. La infraestructura PKI cumple todos los requisitos y va más allá



Para combatir esta realidad en la que las amenazas proliferan, los profesionales de la seguridad necesitan una solución flexible que pueda implementarse rápidamente, fácil de gestionar y con la capacidad de manejar cualquier ataque.

CASO DE ESTUDIO (FLORENCE, ALABAMA, ESTADOS UNIDOS)

Un pez gordo en un pequeño estanque

En julio de 2019, hubo una gran filtración de datos bancarios que afectó a 100 millones de clientes de todo el mundo.[5] Un ejemplo más de robo de información a nivel internacional.

Pero al mismo tiempo que se producía esta brecha, los ciberdelincuentes atacaban a víctimas más modestas, buscando vulnerabilidades por aquí y por allá, para extraer algún tipo de ganancia en sitios en los que escaseaban los recursos de seguridad. Cada vez más, encontraron este tipo de vulnerabilidades en pequeños organismos públicos, donde la limitación de los recursos dificultaba la protección de todos los sistemas y usuarios.

En lugar de atacar a empresas multimillonarias, en las que los departamentos de TI son grandes y están bien dotados, estos delincuentes se introdujeron en redes informáticas municipales, donde instalaban ransomware para secuestrar los datos de los ayuntamientos.

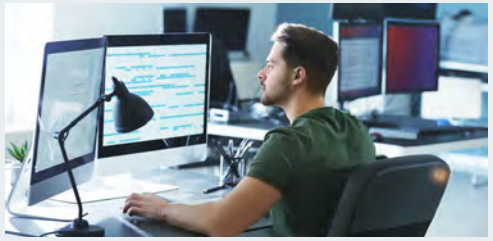
Esto es lo que pasó en junio de 2020 en la localidad de Florence (Alabama, Estados Unidos). Situada a orillas del río Tennessee, en la frontera septentrional del estado, esta localidad de 40 000 habitantes es conocida por su Feria del Renacimiento anual y por ser la ciudad natal de uno de los padres del blues, W. C. Handy. A finales de mayo, los funcionarios del ayuntamiento recibieron aviso de una potencial brecha, pero para entonces ya era demasiado tarde. El delincuente que hackeó la red de Florence había conseguido acceder a ella un mes antes y trabajando todo ese tiempo para secuestrar los sistemas del municipio. El 5 de junio, el hacker lanzó su ataque y pidió un rescate en forma de bitcoins.

Tras consultar con los expertos en seguridad que estaban familiarizados con los hábitos de este delincuente en serie, el gobierno de Florence decidió pagar el rescate de 300 000 dólares. Pero Florence no estaba sola en esto. Tan solo cuatro meses antes de esta brecha, el New York Times publicaba un informe según el cual los ataques de ransomware habían aumentado un 41 por ciento[6] entre 2018 y 2019 y, entre sus víctimas, se contaban decenas de ciudades y municipios.

Aunque las brechas de datos grandes son las que acaparan los titulares, una facción de delincuentes ha fabricado un lucrativo esquema con el que perseguir a víctimas vulnerables más proclives a pagar. Estos peces gordos en un pequeño estanque se están aprovechando de las comunidades mediante la implementación de ciberataques sofisticados contra quienes menos recursos tienen para defenderse.

PKI, a diferencia de otras soluciones de seguridad e identidad, es lo suficientemente flexible como para funcionar tan bien con las redes como con el correo electrónico e Internet. Las soluciones de PKI simplifican las implementaciones de seguridad ofreciendo al personal de TI y seguridad la capacidad de emitir y gestionar certificados de cifrado y autenticación en diversos sistemas, dispositivos y usuarios.

La solución, que ya funciona para proteger los sitios web, también puede servir para garantizar la seguridad de redes, dispositivos, correos electrónicos, documentos y usuarios, bloqueando los ataques de ransomware y simplificando el ecosistema de seguridad.



[5] https://www.capitalone.com/facts2019/ [6] https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html

CAPÍTULO 2

LO QUE TAL VEZ NO SEPA DE LA INFRAESTRUCTURA PKI

El reto del mundo actual conectado es la complejidad.

Cuando no se trata de ataques sofisticados, se trata de proteger ecosistemas complejos en los que interactúan tecnologías nuevas con otras que no lo son tanto. Y, cuando los ecosistemas son más simples, se trata de proteger un sistema en el que los usuarios no siempre están al tanto de amenazas más compleja.

En todo el mundo, los consultores y analistas de seguridad: necesitan una solución que sea fácil de configurar y gestionar, por un lado, y en la que puedan confiar de una vez y para siempre, por otro.

Y aquí es donde la infraestructura de clave pública entra en acción.

Si tiene ciertas nociones de seguridad en Internet, ya sabrá lo que es la infraestructura PKI. Probablemente la conozca desde hace mucho tiempo, pues PKI lleva ya dos décadas siendo la solución de seguridad para sitios web de confianza: primero con el protocolo SSL y ahora, TLS. La base de confianza, no obstante, sigue siendo la misma que hace veinte años.

Pero a mucha gente le sorprende saber que la infraestructura PKI no solo protege la Web. También protege aplicaciones. Protege código, relojes inteligentes, contratos, camas de hospital, satélites… Resulta que la solución de seguridad que lleva dos décadas demostrando ser fiable en Internet también lo es en los artilugios conectados más recientes e innovadores.

PKI ha demostrado ser confiable

Pese al hecho de que el mundo conectado evoluciona todos los días, la infraestructura PKI ha demostrado ser tan eficaz en la protección de los dispositivos IoT más avanzados hoy como lo fue en la red de redes cifrada de hace veinte años.

La genialidad de la infraestructura PKI es su sencillez: unas simples parejas de claves que utilizan cifrado asimétrico. En el cifrado asimétrico, una parte protege los datos y los transmite a la otra sin compartir un secreto común. Por lo tanto, descifrar el código de una de las claves no resuelve el cifrado de la otra. Para leer los datos, es necesario descifrar ambas claves.

El resultado es un sistema de confianza que lleva décadas demostrando ser confiable.

PKI es flexible

En los ecosistemas de hoy en día, los profesionales tienen que proteger un sitio web junto con una aplicación, por ejemplo, o firmar un documento de forma segura mientras se autentica el teléfono inteligente de un empleado. Una empresa puede necesitar una solución para los robots automatizados de una línea de ensamblado mientras otra tiene que proteger los números de las tarjetas de pago de sus clientes. Una solución que funcione de una forma pero no de otra, o un día pero no al siguiente, no solo sobrecarga de trabajo al equipo de TI responsable de gestionar la seguridad, sino que pone a la organización en peligro.

A diferencia de otros tipos de soluciones de seguridad, la infraestructura PKI es increíblemente flexible. Dado que su funcionamiento está basado en una pareja de claves asimétricas y que el proceso de seguridad puede validar con la misma facilidad con que cifra, PKI puede implementarse en cualquier número de entornos para proteger una amplia gama de conexiones. Las soluciones de PKI pueden ampliarse o reducirse, ejecutarse en la nube, de forma local o en entornos híbridos, proteger sitios web o el correo electrónico, mañana un modelo

de uso de dispositivos personales en el trabajo y pasado el IoT. Es una solución comodín capaz de cubrir un amplio espectro de necesidades de seguridad.

La infraestructura PKI proporciona confianza pública y privada

PKI, más que un simple sistema de cifrado, vincula la identidad a una clave a través de un proceso de firma. La firma la emite la raíz para que cualquiera que tenga la clave pública de esa raíz sepa que la firma vinculada al certificado PKI es válida y confiable.

En algunos casos, esa raíz es pública, es decir, se ha distribuido a un repositorio de confianza alojado por un navegador web, como Chrome o Firefox, o por un sistema operativo, como Microsoft Windows o Apple MacOS. En otros, la raíz es privada, es decir, confían en ella todos los sistemas que quiera utilizar una organización de manera interna o en un pequeño grupo de empresas. La criptografía es la misma en ambos casos, pero poder implementar tanto opciones públicas como privadas convierte la infraestructura PKI en una especialmente versátil.

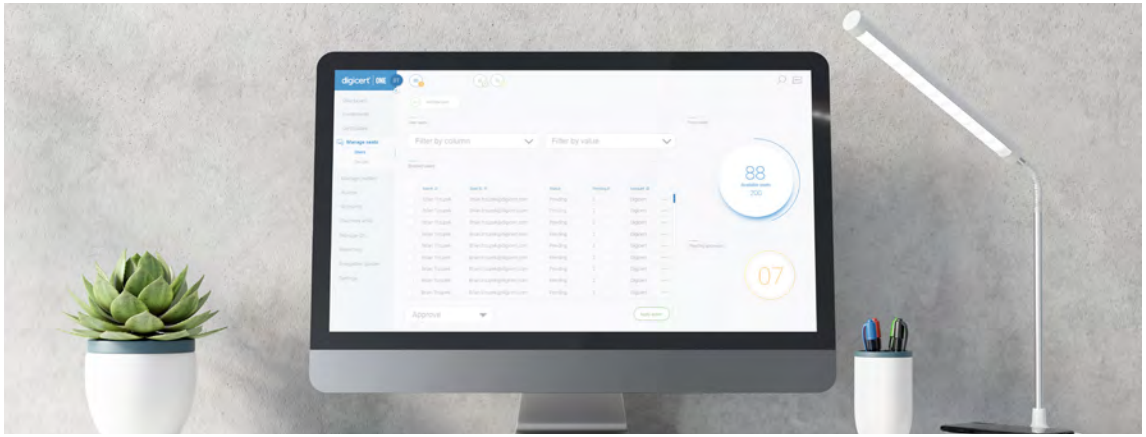
Esta flexibilidad permite tender un puente entre la confianza pública y la privada con PKI. Es suficientemente potente y segura como para ser una solución privada de identidad y cifrado digna de la confianza de muchos gobiernos y, al mismo tiempo, la solución pública para dispositivos IoT de consumo.

LA INFRAESTRUCTURA PKI PROPORCIONA CONFIANZA PÚBLICA Y PRIVADA.

La infraestructura PKI puede ser sencilla

Antes, la infraestructura PKI era una cosa muy complicada. Sin acceso a expertos y plataformas ni herramientas que simplificaran la gestión, los profesionales informáticos tenían que desarrollar a ciegas soluciones de PKI internas sin el conocimiento especializado necesario para hacerlo correctamente. Aunque su confiabilidad convierte a PKI en la solución ideal —si funciona, claro—, llegar hasta ahí solía ser una carrera de obstáculos y, a menudo, daba más problemas de los que resolvía.

Afortunadamente, esos días han quedado atrás. Hoy en día, PKI puede ser fácil de configurar y usar, si se hace bien. Ahora, hay muchas herramientas sofisticadas para implementar y supervisar las soluciones de PKI que funcionan en una plataforma de inicio de sesión único. Y, gracias a que PKI es tan versátil, resulta sencillo ejecutar soluciones para muchos retos de seguridad distintos en un solo lugar. En lugar de tener que asumir la complejidad de diseñar y desarrollar una solución de PKI para un solo uso, ahora es posible implementar y gestionar varias soluciones de seguridad en un único lugar, sin necesidad de ayuda experta para mantener y ejecutar su entorno de PKI.



Cuatro malentendidos sobre la infraestructura PKI

¿La gente sigue usando PKI?

Lo viejo vuelve a ser novedoso. No es que PKI se siga utilizando; es que está en estado de gracia. El valor de PKI reside en su flexibilidad, unida a su largo historial de confianza. Los ingenieros, que encuentran cada vez más conexiones en las que la infraestructura PKI les ofrece la mejor solución, pueden implementar una solución de seguridad e identidad de PKI sabiendo que la tecnología lleva años demostrando ofrecer una protección robusta.

¿Y el problema que hubo con Chrome? ¿PKI no ha pasado a mejor vida?

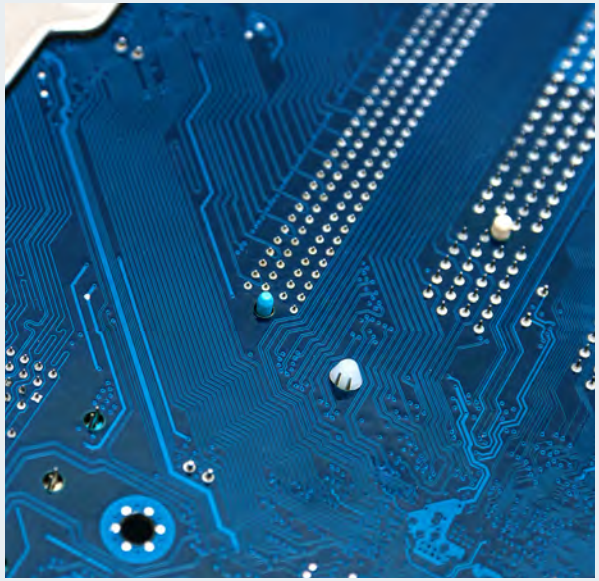
El historial de PKI es sólido en lo que a la seguridad se refiere. La manera de implementarlo, sin embargo, depende de la entidad que emita el certificado. En 2017, Google anunció[7] que dejaría de confiar en una serie de certificados emitidos por Symantec debido a que esos certificados no cumplían con los requisitos básicos del CA/Browser Forum.

Se trata de un ejemplo poco afortunado de unapráctica empresarial desfasada con graves consecuencias. En reacción a una posible brecha en la seguridad mundial, Symantec y Google empezaron

[7] https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

a buscar a una autoridad de certificación capaz de mantener el nivel de confianza e infraestructura necesario para gestionar una reemisión a gran escala. Optaron por DigiCert y acordaron pasar los certificados de Symantec a las raíces de confianza de DigiCert, de manera que los usuarios de Chrome no tuvieran que ver interrumpido el acceso a los sitios web protegidos con PKI.

Hoy, cuando se cumplen justo veinte años, PKI sigue siendo la solución de confianza para proteger la comunicación web, incluso en Chrome.



PKI no funciona en muchos dispositivos.

Sería más exacto decir que PKI funciona en cualquier dispositivo con capacidad suficiente para ejecutarlo. El emparejamiento de claves asimétrico requiere velocidad de procesamiento, memoria y espacio en discos suficientes como para ejecutar la acción. Por supuesto, PKI lleva más de veinte años en uso, así que si los procesadores de finales de los noventa podían cifrar las claves, lo lógico sería que cualquier dispositivo de reciente creación tuviera potencia suficiente como para ejecutar PKI. Sin embargo, aun con los avances en los microprocesadores, las características de rendimiento de algunos dispositivos IoT son tan rudimentarias que no siempre son capaces de generar las claves rápidamente o de firmar el canal de comunicaciones.

Afortunadamente, a los expertos en PKI se les suelen ocurrir alternativas inteligentes que no ponen en peligro la seguridad. Estas soluciones comprimen el contenido de los certificados de PKI para que el escaso ancho de banda y el procesamiento básico de ciertos dispositivos IoT sean capaces de gestionarlo. También hay proveedores de software que proporcionan sistemas de generación de claves o de CSR para dispositivos de baja potencia.

Con el paso del tiempo, cada vez serán menos los dispositivos con problemas de compatibilidad con PKI. Los nuevos procesos de fabricación permiten a los fabricantes de dispositivos integrar claves en el silicio, para que la seguridad se incorpore a la cadena de suministro al principio del proceso. La integración en el silicio no solo resuelve los problemas de compatibilidad, sino que también acelera la fabricación mientras refuerza la seguridad y la identidad de los dispositivos a lo largo de todo su ciclo de vida.

¿PKI no era simplemente un tipo de tecnología SSL para sitios web?

Si lleva varios años en el mundo de la seguridad conectada, seguramente sabrá que PKI es un método de protección de capa de transporte o SSL. SSL se remonta al año 1995, cuando su primera versión funcional sirvió como protocolo criptográfico de Netscape. En 1999, SSL quedó descatalogado a favor de su sucesor, Transport Layer Security (TLS), que era similar. Todavía hoy, TLS sigue siendo el protocolo de cifrado de confianza para sitios web.

TLS/SSL es la implementación de PKI más extendida, pero este no es más que uno de entre decenas de usos. En realidad, PKI está en todas partes y se utiliza de forma confiable en casi cualquier tipo de conexión. De hecho, PKI ahora protege todo tipo de cosas que el equipo de Netscape no podía ni imaginar cuando anunció SSL hace un cuarto de siglo.

LA PRUEBA DE CONFIANZA ESTÁ EN TODAS PARTES

Hasta los ingenieros y expertos en seguridad que desarrollan soluciones de PKI se sorprenden por la creatividad con que algunas personas utilizan la infraestructura PKI para proteger sus inventos. PKI, como una hebra tejida a través de tecnologías dispares y sectores inconexos, aparece en algunos de los lugares más inusitados. Sin embargo, independientemente de su uso, siempre se repite la misma necesidad: una confianza incondicional.

PRIMER CASO DE ESTUDIO

AeroMACS

De total confianza

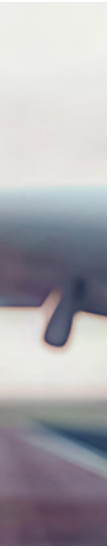
Un piloto de avión comercial tiene acceso a más datos de sensores conectados de los que usaron los astronautas Young y Crippen para sacar de órbita el *Columbia* durante la misión inaugural del transbordador espacial en 1981.

Pero el componente sigue siendo hoy igual de importante que hace cuarenta años. Para aterrizar esa máquina colosal de forma segura, la persona que está a los mandos necesita la mayor cantidad de información precisa posible.

La mayoría de los accidentes aéreos se producen al despegar y al aterrizar. Esos son los momentos en que el avión es más vulnerable a las fuerzas —tanto humanas como de la naturaleza— que afectan al complicado acto de manejar 60 toneladas de metal, combustible, equipaje y pasajeros en el aire. Una cizalladura, un error de sincronización, la pérdida de visibilidad…

Durante el aterrizaje y la aproximación final, los pilotos de avión utilizan información vital, recogida por sensores y retransmitida a través de lecturas en cabina y los técnicos de las torres de control, para realizar los ajustes necesarios y proteger los viajes aéreos. Toda esa información vital lleva desde 2016 transmitiéndose a través de sensores IoT de aeronaves protegidos por la tecnología de PKI a torres y aviones de todo el mundo.

La mayoría de los accidentes aéreos se producen al despegar y al aterrizar. Esos son los momentos en que el avión es más vulnerable a las fuerzas —tanto humanas como de la naturaleza— que afectan al complicado acto de manejar 60 toneladas de metal, combustible, equipaje y pasajeros en el aire.



TODA LA INFORMACIÓN VITAL LLEVA DESDE 2016 TRANSMITIÉNDOSE A TRAVÉS DE SENSORES IoT DE AERONAVES PROTEGIDOS POR LA TECNOLOGÍA DE PKI A TORRES Y AVIONES DE TODO EL MUNDO.

Todos para uno y uno para todos

De aquí a 2025, se espera que el número de aviones en el aire se duplique. Cada vez hay más aviones y vuelos; de hecho, el Aeropuerto Internacional de Pekín vio un aumento de pasajeros del 5 por ciento entre 2017 y 2018, y el Aeropuerto de Dallas Love Field (Estados Unidos) acogió un 90 por ciento más de pasajeros entre 2010 y 2020.

EL SISTEMA AERONÁUTICO DE COMUNICACIONES INALÁMBRICAS PARA AVIONES AeroMACS (AERONAUTICAL MOBILE AVIATION COMMUNICATION SYSTEM) ES UN ENLACE DE DATOS INALÁMBRICOS DE BANDA ANCHA Y GRAN CAPACIDAD QUE TRANSMITE DATOS DE SENSORES IoT PARA TORRES DE CONTROL Y AVIONES.

Aunque se están construyendo nuevos aeropuertos por todo el mundo, los actuales destinos en los que se gestionan más vuelos solo tienen una solución: incrementar la eficiencia de la coordinación del tráfico aéreo y garantizar la integridad de los despegues y los aterrizajes.

¿Qué es AeroMACS?

El sistema aeronáutico de comunicaciones inalámbricas para aviones AeroMACS (Aeronautical Mobile Aviation Communication System) es un enlace de datos inalámbricos de banda ancha y gran capacidad que transmite datos de sensores IoT para torres de control y aviones. Desde la temperatura y los indicadores de viento hasta sistemas de visualización de la información de vuelo —e incluso información sobre la manipulación de equipajes—, si un dispositivo forma parte de la superficie del aeropuerto, sus datos se comunican a través del sistema AeroMACS.

Pero este sistema no se reduce a unos cuantos artilugios. Representa los ojos y los oídos de lo que ocurre en tierra. Desempeña un papel fundamental en la coordinación de los planes de vuelo y las programaciones. Es un elemento nuclear de las operaciones aeroportuarias. Si sufre un ataque, alguien podría utilizarlo para transmitir información falsa al avión y al piloto. Y, dado que cada vez hay más vuelos y pasajeros, proteger la información de AeroMACS de la manipulación resulta esencial para garantizar que los aviones despeguen, vuelen y aterricen en condiciones de seguridad.

Agregue PKI a la lista de control de despegue

En sectores con ecosistemas complejos, formados por muchos componentes conectados, con

dispositivos heterogéneos y limitados en cuanto a su potencia, se necesita una solución adaptable y confiable. En el caso de los viajes aéreos, entran en juego todos estos factores, pero también surge la necesidad de proteger la confidencialidad de los datos. Al igual que el dispositivo, es preciso proteger la información que se transmite entre la tierra y el avión para impedir que se produzca una manipulación con implicaciones catastróficas.

Una infraestructura PKI capaz de proteger estos dispositivos y los datos que transmiten permite a los pilotos y torres de control reunir, comunicar y utilizar una gran variedad de información para garantizar que los aviones despeguen y aterricen de forma segura, independientemente de la aeronave o del aeropuerto. Si está en AeroMACS, funciona exactamente igual —y con la misma confiabilidad— en un pequeño aeropuerto de Estados Unidos que en un gran aeropuerto de Australia.

Implementación: el mundo

Las soluciones de PKI protegen la red AeroMACS, el estándar de comunicaciones aeronáuticas que de manera inminente será utilizado por casi cualquier aeropuerto del mundo.

Necesidad primordial: confianza

Con miles de vuelos operando en el aire a todas horas, los aeropuertos, compañías aéreas y pilotos confían en AeroMACS para garantizar que millones de personas viajen en condiciones de seguridad y lleguen puntuales a su destino todos los días.

SEGUNDO CASO DE ESTUDIO

AUSTRALIA GATEKEEPER

Con la confianza de las administraciones públicas para proteger a la ciudadanía

Probablemente, la gran mayoría de los australianos no sean conscientes de la solución de seguridad e identidad que protege su información y muchas de las transacciones más importantes que llevan a cabo en su día a día. Si ha comprado una casa recientemente en Australia, ha utilizado Gatekeeper. Si ha importado algún bien, ha utilizado Gatekeeper.

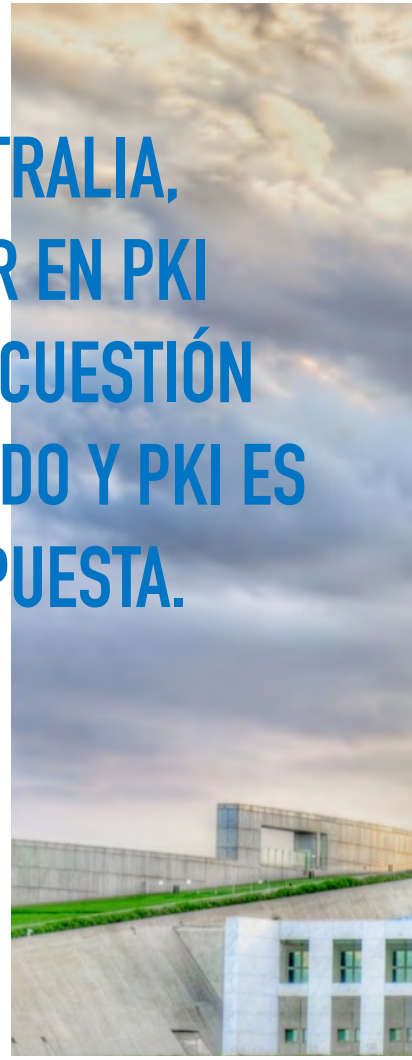
El marco de desarrollo Gatekeeper Public Key Infrastructure, que ya va por su tercera década, «gobierna la forma en que el estado australiano utiliza las claves y los certificados digitales para proteger la identidad de las personas suscritas a los servicios de autenticación».Las soluciones de PKI, mediante tecnologías de cifrado y autenticación, protegen desde documentos legales importantes hasta contratos, fronteras, información bancaria y muchas de las áreas públicas de confianza más delicadas.

La seguridad de todo un país

A finales del siglo pasado, el estado australiano empezó a buscar un mecanismo para proteger de forma confiable la información que rellenaba cada vez más y más documentos y transacciones digitales. Al principio, ciertas agencias implementaron de forma puntual soluciones desarrolladas internamente, pero enseguida descubrieron que gestionar la seguridad por sí mismas a alto nivel resultaba costoso en términos de tiempo, complejidad y riesgos.

En consecuencia, el comité del marco de desarrollo definió una solución capaz de cubrir la necesidad de proteger a toda una nación mientras minimizaba el tiempo y los recursos necesarios para gestionar el ecosistema.Hoy en día, el marco de desarrollo de Gatekeeper «proporciona integridad, interoperabilidad, autenticidad y confianza entre las agencias de las administraciones públicas y sus clientes».

EN AUSTRALIA, CONFIAR EN PKI ES UNA CUESTIÓN DE ESTADO Y PKI ES LA RESPUESTA.



Invisible, pero siempre presente

Muchas veces, es precisamente la tecnología que no vemos la que tiene el mayor impacto en nuestras vidas. Redes eléctricas, sistemas de bombeo de agua, operaciones bancarias… Damos por sentada la importancia de la confiabilidad de estos sistemas que funcionan entre bastidores. Para los australianos, Gatekeeper es más que un sistema que debe dar confianza. Además de hacer que los procesos sean más cómodos y eficientes, está detrás de muchas funciones públicas vitales. Sin la seguridad que ofrece PKI, la información personal de millones de australianos podría verse expuesta a robos, muchas transacciones y procesos legales importantes se verían demorados o, directamente, interrumpidos, y las agencias públicas que controlan las aduanas y las inversiones correrían peligro. En Australia, confiar en PKI es una cuestión de estado y PKI es la respuesta.

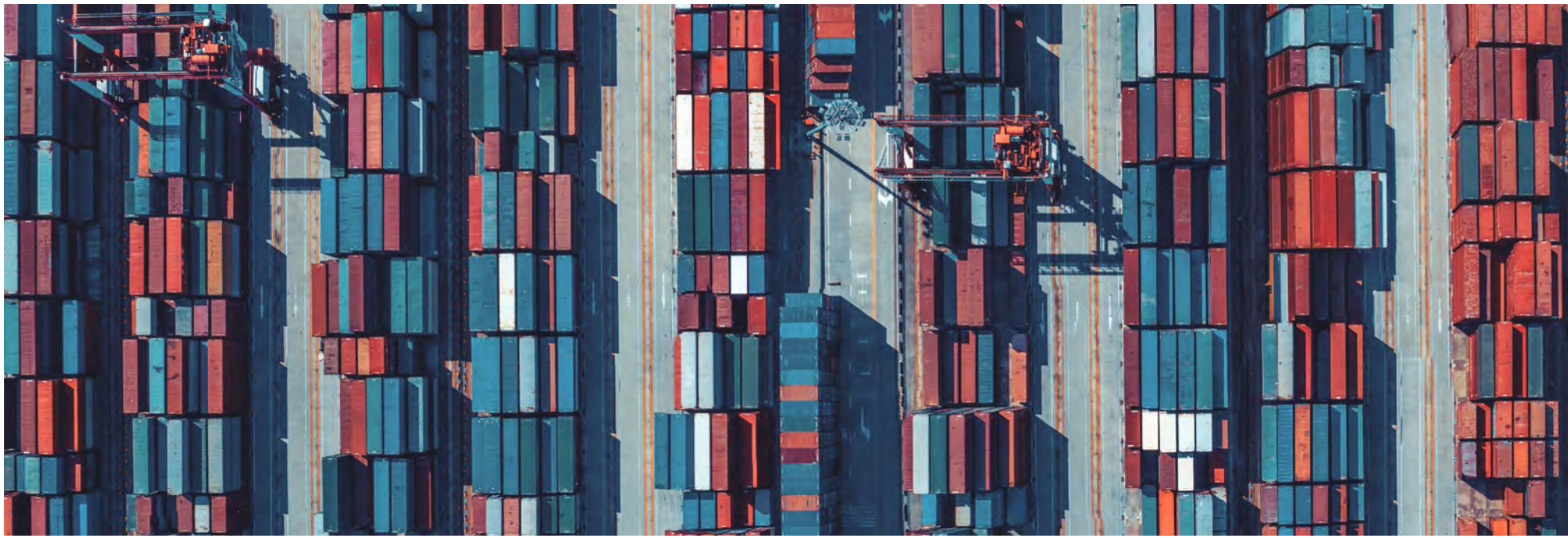
TIENE QUE FUNCIONAR DE MANERA ININTERRUMPIDA.

Implementación: Australia

Una solución de seguridad e identidad nacional que funciona en varias agencias estatales y protege muchos de los espacios de confianza públicos más confidenciales.

Necesidad primordial: integridad

Desde la banca y la propiedad inmobiliaria hasta la seguridad fronteriza, no hay margen para el error y la exposición de información. Tiene que funcionar de manera ininterrumpida.



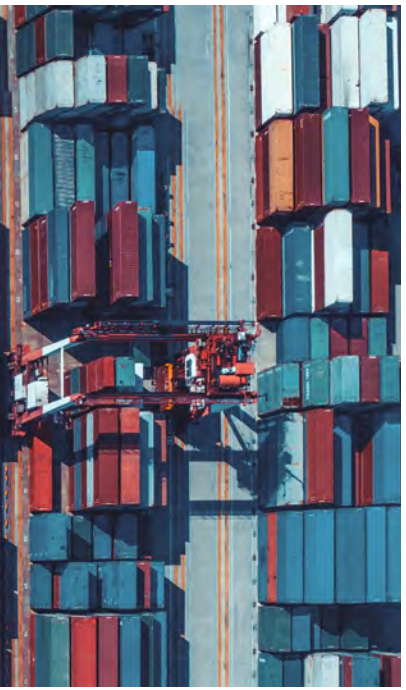
TERCER CASO DE ESTUDIO

TRANSPORTE MUNDIAL

Confiable a escala planetaria

Imagine tener que localizar un contenedor de transporte concreto —uno entre millones— en su periplo de un puerto a otro, entre continentes y a través de los océanos. Ahora, imagine que tiene que localizar ese mismo contenedor de envío utilizando bases de datos y registros de carga.

La cadena de suministro mundial es como un reloj muy complejo: para que el mecanismo funcione, todos y cada uno de los dientes, muelles y ruedas tienen que estar en su lugar y funcionar según lo previsto. Los retrasos en los envíos frenan la actividad de toda la cadena. Los envíos perdidos pueden romper la cadena y costar dinero a las empresas, tanto por la pérdida de materiales como por la pérdida de ingresos.



Todos los años se desplazan más de 11 000 millones de toneladas de bienes a través del mar. Hoy, hay más de 50 000 buques portacontenedores en el mundo.

A la vista digital

Todos los años se desplazan más de 11 000 millones de toneladas de bienes a través del mar. Hoy, hay más de 50 000 buques portacontenedores en el mundo. Aunque ingente, el comercio transoceánico es también dinámico. El movimiento es constante, con todo el globo salpicado de buques de carga como un mapa de la noche estrellada.

Por cada buque navegando, hay aún más contenedores. Localizar y rastrear cada uno de estos contenedores en tiempo real —y de forma segura— es una tarea descomunal.

El reto de transportar mercancías a este nivel es autenticar los dispositivos mutuamente en el ámbito de la nube, donde se controlan los activos. Si el sistema se ve atacado, la empresa transportista puede perder de vista la localización de los contenedores o recibir información falsa acerca de ellos. Una solución de seguridad, para que sea efectiva, no solo debe proteger el dispositivo, sino también la información que transmite. Asimismo, tiene que ser escalable y capaz de proteger decenas de miles de dispositivos a la vez sin cometer fallos.

En cualquier rincón del mundo

Con la autenticación de PKI, los contenedores de transporte se pueden rastrear de forma segura a lo largo de toda la ruta, desde la salida del puerto hasta su llegada a destino. Y, dado el incremento de dispositivos y envíos todos los años, la necesidad de seguridad es cada vez mayor. Gracias a la escalabilidad de la tecnología de PKI, la cadena siempre satisface la demanda.

¿El resultado? Todos los envíos y los datos quedan protegidos y los contenedores se rastrean, con independencia de su paradero. Esto reduce la posibilidad de que se produzcan robos o pérdidas, y ayuda a garantizar que los bienes se trasladen de un puerto a otro de manera eficiente. La cadena de suministro funciona de forma ininterrumpida, y tanto las empresas como los consumidores disfrutan de las ventajas de una mayor disponibilidad de los bienes por un costo inferior.

Implementación: el mundo

En el centro de la cadena de suministro mundial, los contenedores de transporte conectados desplazan bienes y materias primas entre todos los continentes del planeta.

Necesidad primordial: autenticación

Las soluciones de PKI, más que un simple rastreo, ofrecen autenticación segura en tiempo real para que la empresa pueda localizar e identificar el dispositivo conectado a cada contenedor de mercancías.

CON LA INFRAESTRUCTURA PKI, LOS CONTENEDORES DE TRANSPORTE SE PUEDEN RASTREAR DE FORMA SEGURA A LO LARGO DE TODA LA RUTA.

CUARTO CASO DE ESTUDIO:

IBM

La empresa de confianza de las tecnológicas

A menudo, cuanto más grande es la empresa, mayor es el desafío. Es más, a veces el verdadero desafío es el tamaño de la empresa. Por ejemplo, ¿cómo protege una organización a cada uno de sus usuarios, quienes no solo desempeñan distintas funciones en diferentes oficinas de todo el mundo, sino que además utilizan distintos dispositivos, cada uno con su propio sistema operativo y aplicaciones?

Para IBM, esto no fue un mero ejercicio intelectual. Fue un problema real. Y ese problema afectó a medio millón de empleados.

Utilice el dispositivo que sea

Autenticar, identificar y proteger a más de 500 000 usuarios.

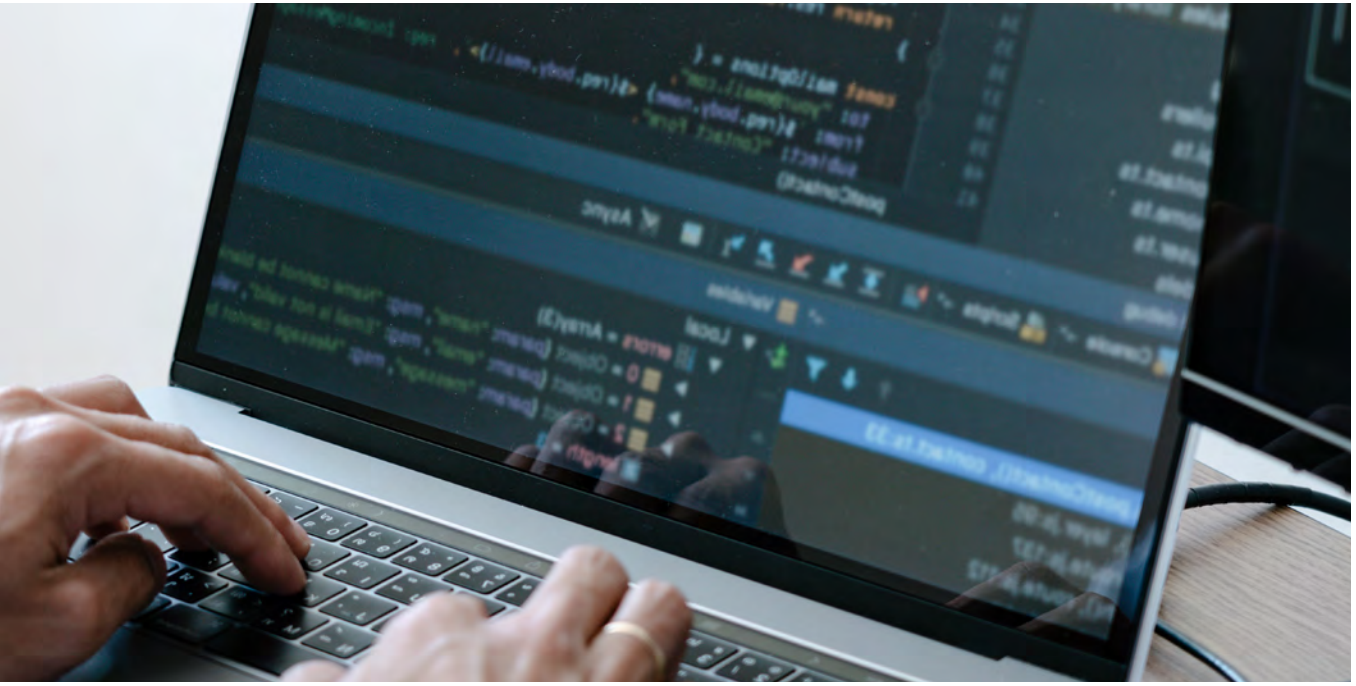
Aquí, la expresión «flexible y escalable» no podía ser una simple descripción teórica: tenía que ser una función real de una solución de PKI operativa. Pero, si bien el número de usuarios presenta todo un desafío, no es mayor que el que plantea el número de tipos de dispositivos y aplicaciones que esos usuarios traen al trabajo. Una computadora portátil propiedad de la empresa. Un teléfono inteligente que pertenece al usuario. Un modelo de iPad antiguo. Si quiere ofrecer a sus empleados, proveedores y contratistas la flexibilidad de utilizar los dispositivos que les facilitan el trabajo, pero no quiere introducir vulnerabilidades en la red, necesita una solución de seguridad que sea robusta y, al mismo tiempo, fácil de adaptar.

La tecnología de PKI es flexible y escalable. Esto significa que la infraestructura de clave pública no solo puede autenticar cualquier número dado de dispositivos, con independencia de quién sea su propietario o de qué software ejecuten, sino que también puede autenticar los dispositivos de cientos de miles de usuarios a la vez, independientemente del lugar en que se encuentren.
Y los usuarios —los 500 000— ni se enteran.

Cuando confianza es sinónimo de confiabilidad

Las soluciones de identidad de PKI han prestado servicios ininterrumpidos en más de 170 países en solo una empresa.

LA TECNOLOGÍA DE PKI ES FLEXIBLE Y ESCALABLE.



La confiabilidad es tan necesaria como la confianza. A esta escala, la autenticación del software como servicio debe ser lo suficientemente robusta como para funcionar todo el tiempo en todas partes.En todo el mundo, 24 horas al día, 7 días a la semana, cientos de miles de usuarios necesitan acceder de forma segura a la red de IBM desde el dispositivo de turno, sea cual sea. Es seguro y directo, por lo que no es necesario pensar en ello ni la empresa preocuparse por las vulnerabilidades.

Implementación: el mundo

Miles de oficinas repartidas por todo el mundo llevan la compañía de un veterano líder internacional en hardware y software.

Necesidad primordial: flexibilidad

La tecnología de PKI, en el caso de las operaciones críticas, ofrece una solución de autenticación, protección e identificación para medio millón de empleados repartidos por todo el globo.

QUINTO CASO DE ESTUDIO

EL SECTOR SANITARIO

Un salvavidas

Para la mayoría de nosotros, un componente conectado ofrece un extra, una ventaja más. Una conexión Bluetooth nos permite comprobar la temperatura y el nivel de humedad del salón. Con una conexión Wi-Fi entre un iPad ubicado en la cocina y un televisor inteligente situado en el salón, podemos elegir un episodio para retomar la serie por donde la dejamos mientras se hace la cena en el horno. Casi siempre, los dispositivos conectados son deseables, pero no necesarios. En algunos casos, sin embargo, una conexión no solo ofrece un extra o comodidad. Para algunas personas, una conexión es una cuestión de vida o muerte.

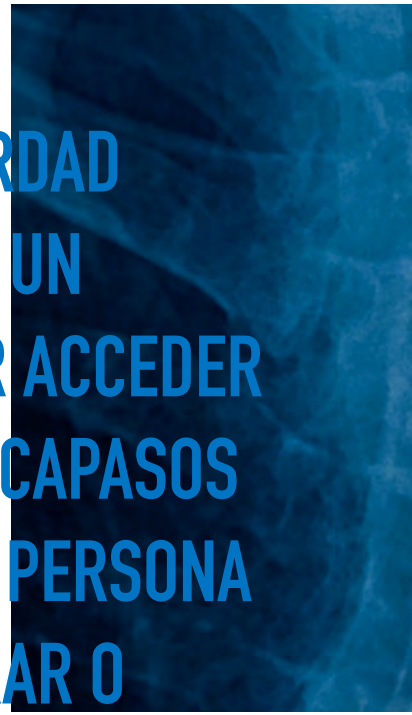
Hace unos años, los ingenieros médicos presentaron un nuevo tipo de marcapasos. Este modelo concreto era «inteligente». Al conectar un monitor externo y una aplicación al teléfono del paciente a través de Bluetooth, el marcapasos no solo podía enviar las señales eléctricas necesarias para que el corazón siguiera latiendo, sino que también podía decir al paciente y al médico que el marcapasos estaba operativo.

¿Funciona el marcapasos correctamente? ¿Cuánta batería le queda? Para responder estas preguntas, era necesario que el paciente se desplazara hasta el hospital y, a veces, incluso que se sometiera a una operación. Ahora, todo esto puede monitorizarse, registrarse y comunicarse de manera automática y continua.

Los marcapasos conectados no son una simple comodidad. Las vidas de miles de personas dependen de estos dispositivos. Pero, como con cualquier conexión, existe la posibilidad de que se produzcan interferencias. Y, como cualquier otro dispositivo IoT, un marcapasos conectado necesita un cifrado integral seguro.

Cuando «vida o muerte» es literal

En agosto de 2017, un titular inédito[8] se repetía en los teletipos; inédito, al menos, para cualquiera que no trabaje en el mundo del IoT. La Administración de Alimentos y Medicamentos (FDA, por sus siglas en inglés) de Estados Unidos tuvo que retirar una serie de marcapasos debido a una amenaza de seguridad informática. En lo que parecía una historia más sobre los riesgos del hackeo en Internet, la FDA avisó que ciertos marcapasos podrían «ser vulnerables a intrusiones y exploits de ciberseguridad».



¿DE VERDAD PODRÍA UN HACKER ACCEDER AL MARCAPASOS DE UNA PERSONA Y ALTERAR O INTERRUMPIR SU FUNCIONAMIENTO? SÍ.

[8] https://thehealthcareblog.com/blog/2019/07/29/security-crisis-of-cardiac-pacemakers-paves-the-way-for-iot-security-evolution-in-cardiology/

Era una idea extraña, parecía la trama de una película de ciencia ficción. ¿De verdad podría un hacker acceder al marcapasos de una persona y alterar o interrumpir su funcionamiento? Sí.

La invención de formas novedosas y valiosas de conectar herramientas terapéuticas —desde camas de hospital inteligentes hasta glucómetros— por parte de los fabricantes de dispositivos médicos disparó los beneficios para los pacientes. Al mismo tiempo, surgieron preocupaciones sobre la protección de los datos de los pacientes recopilados por los dispositivos conectados y, hasta cierto punto, sobre posibles intrusiones que podían hacer fallar el dispositivo.

Los marcapasos ofrecían ese punto de intrusión que los hackers buscaban. Los fabricantes cifraron la comunicación entre el marcapasos y el monitor de pacientes a pie de cama, pero el monitor en sí no estaba protegido. Con acceso al monitor, estos hackers podían enviar comandos al marcapasos sin parar hasta agotar la batería. Y lo que es peor, podían ordenar al marcapasos que provocara un choque cardiocirculatorio en el paciente. Al buscar una respuesta para proteger no solo el dispositivo sino la seguridad general del paciente, muchos fabricantes pusieron la vista sobre la infraestructura PKI.

El valor de la tecnología de PKI en los dispositivos médicos no solo tiene que ver con su largo historial de cifrado sólido, sino también con la identidad integrada.

UNA SOLUCIÓN DE SEGURIDAD QUE PROTEGE LA INTEGRIDAD DE LOS DATOS DEL DISPOSITIVO Y DEL PACIENTE, Y LO SUFICIENTEMENTE FIABLE COMO PARA CONFIARLE LAS VIDAS HUMANAS.

Los dispositivos médicos serán más pequeños e inteligentes, pero la solución de seguridad que protegerá los datos —y la vida— de los pacientes continuará siendo PKI.

La infraestructura PKI facilita la protección de los datos del dispositivo mientras lo autentica con un identificador cifrado. Esto significa que un dispositivo puede protegerse durante su fabricación y hacer llegar esa seguridad al hospital y, después, al paciente. Aunque el dispositivo en sí haya completado distintas fases de su ciclo de vida y las personas encargadas de supervisar la seguridad hayan cambiado, esa seguridad permanece intacta durante todo el tiempo.

El futuro de los dispositivos médicos es más inteligente todavía

Recientemente, ha habido nuevas autorizaciones de financiación y de entidades sanitarias para que inviertan recursos de I+D para crear dispositivos más pequeños y sofisticados. Ya se están utilizando marcapasos sin plomo lo suficientemente pequeños como para poder insertarlos a través de un catéter femoral e implantarlos directamente en el corazón. Así, deja de ser necesario aplicar una cirugía más invasiva o utilizar cables de plomo, que son más susceptibles al desgaste provocado por la contracción del tejido cardíaco como resultado de los millones o miles de millones de latidos del corazón.

La próxima ola de marcapasos seguirá siendo, por supuesto, sin plomo y más inteligente. Conectados a unos pequeños desfibriladores, no solo supervisarán el estado de salud del dispositivo, sino también el del corazón, que será capaz de decir al desfibrilador a través de Bluetooth que envíe una descarga eléctrica si el corazón falla. Transmitirán los datos al cardiólogo del paciente, quien podrá reajustar el dispositivo en tiempo real, sin necesidad de cirugía, para que la salud cardíaca del paciente pueda mejorar sin intervención quirúrgica alguna y sin moverse del sofá.

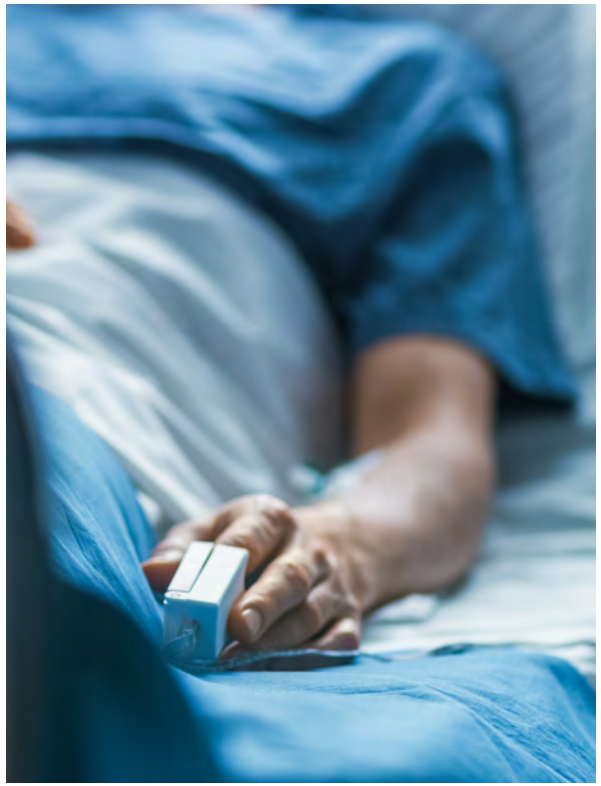
Hoy, miles de personas tienen la tranquilidad de saber que hay un sistema de supervisión cómodo y seguro que garantiza que su marcapasos continúe funcionando y les avise en el caso de que surja algún problema. En el futuro próximo, las funciones de la tecnología cardíaca seguirán aumentando y ofrecerán más opciones a pacientes y personal médico para que cuenten con mejores datos y asistencia inmediata sin cirugías ni visitas al hospital. Los dispositivos médicos serán más pequeños e inteligentes, pero la solución de seguridad que protegerá los datos —y la vida— de los pacientes continuará siendo PKI.

Implementación: varios países, el mundo

Miles de hospitales y centros de atención ambulatoria, y millones de personas, con distintos estándares de implementación y cumplimiento normativo, para uso de proveedores y pacientes por igual.

Necesidad primordial: confiabilidad

Una solución de seguridad que protege la integridad de los datos del dispositivo y del paciente, y lo suficientemente fiable como para confiarle las vidas humanas.



CAPÍTULO 3

LO QUE IGNORA PUEDE HACERLE DAÑO.

Sí, PKI es una tecnología confiable y lleva décadas siéndolo. Pero esa confianza se basa en el conocimiento y la experiencia. Al fin y al cabo, si una solución de PKI no se implementa correctamente, las vulnerabilidades de un sistema sin proteger pueden llegar a plantear un gran riesgo.

Dado que PKI es una tecnología con varios años de antigüedad, los técnicos y científicos informáticos llevan ya bastante tiempo estudiando su funcionamiento en situaciones reales. Aunque es un sistema casi perfecto y hay incontables ejemplos de implementaciones inteligentes e innovadoras, también se dan casos de intentos fallidos en los que, debido a errores de diseño o de gestión, la implementación no funciona.

Cada vez que se implementa PKI, tenemos una oportunidad más de ver cómo se comporta la implementación, especialmente si se produce en un entorno novedoso o se incorpora a una nueva tecnología. Y, cada vez que algo sale bien, los técnicos de PKI aprenden más sobre la forma más inteligente y segura de utilizar esta tecnología.

Unas cuantas cosas que los expertos de seguridad saben hoy acerca de PKI

Claves bien protegidas

La tecnología de PKI solo puede ser tan buena como la clave privada utilizada para firmar la cadena de certificados. Por lo general, se trata de una clave para la autoridad de certificación raíz y la autoridad certificadora intermedia (ICA). Si alguna de las claves —o ambas— se genera o se almacena de forma insegura, los certificados de PKI emitidos no serán del todo confiables. Esto puede ocurrir en el entorno empresarial, por ejemplo, si un profesional de TI crea claves en texto sin cifrar en un servidor gestionado mediante software descargado de Internet y, acto seguido, transfiere dichas claves a la CA que se ejecuta en la red para que haya una copia de seguridad. En este caso, el sistema de PKI es enormemente inseguro porque las claves —que nunca están protegidas— son fáciles de robar. Lo único que garantiza que toda la jerarquía de PKI sea de confianza es contar con una protección adecuada.

Estado de los certificados

Los sistemas de PKI deben proporcionar al dispositivo o al navegador una forma de determinar si el certificado sigue siendo válido y utilizable. Cuando la tecnología de PKI no se implementa adecuadamente, la jerarquía suele carecer de la información necesaria para la revocación o esa información no existe. En algunos casos, el sistema no gestiona correctamente las solicitudes cuando la información está presente y es correcta. Independientemente de la causa, el resultado es un sistema poco confiable.

Configuración defectuosa

Las configuraciones del certificado o la cadena de certificados, además de requerir que los sistemas estén configurados correctamente, suelen necesitar una serie de configuraciones para que PKI proteja el software y el hardware. En el caso de implementaciones «caseras», no es raro encontrar configuraciones alternativas que resuelven un problema concreto mientras el certificado queda abierto a otros riesgos, como la elusión del tráfico, la falsificación o el mal uso.

SÍ, PKI ES UNA TECNOLOGÍA CONFIABLE Y LLEVA DÉCADAS SIÉNDOLO. PERO ESA CONFIANZA SE BASA EN EL CONOCIMIENTO Y LA EXPERIENCIA.

Cuatro errores que hay que evitar al configurar el cifrado de PKI

No planificar futuras iteraciones

Muchas veces, cuando un técnico de seguridad configura soluciones de PKI desarrolladas internamente para su organización, desestima los cambios que se producen a lo largo del tiempo. Cuando las organizaciones evolucionan, los objetivos empresariales cambian, aparecen nuevos productos y se forman nuevos equipos, una solución de PKI que no sea adaptable o que no se haya creado para admitir nuevas implementaciones corre el riesgo de volverse obsoleta o, en el peor de los casos, convertirse en un lastre.

Intentar gestionar todo un ecosistema de PKI de manera interna

La sencillez de la confiabilidad de la infraestructura de PKI puede ser engañosa. Sí, es flexible, escalable, rápida y confiable, pero solo si se integra y se implementa de manera adecuada. Las soluciones creadas internamente suelen terminar siendo medidas de seguridad rígidas que consumen muchos recursos. Sin una instalación experta y una supervisión avanzada, resulta difícil controlar dónde se implementa la infraestructura PKI, su estado y qué es susceptible de fallos. Las infraestructuras PKI gestionadas y las plataformas centralizadas resuelven todos estos problemas y eliminan tanto la necesidad de dedicar un tiempo innecesario a la supervisión como las preocupaciones acerca de los fallos de seguridad, el extravío de claves o los errores humanos.

Diseñar una infraestructura PKI que no cumpla la normativa

Si hay algo que diferencia a la infraestructura PKI —y una de sus grandes ventajas— es la cantidad de posibilidades de implementación flexible que ofrece. Hay un sinfín de modelos, desde la implementación local hasta la nube. No solo es importante saber qué opción es la mejor para el negocio, la seguridad y las necesidades de los usuarios de una organización, sino también cuál es la que ofrece un tipo de seguridad conforme con la regulación local, regional y nacional. También es importante saber cómo encaja la solución de PKI en la estrategia general de seguridad de una organización y un sector.

No prepararse para la próxima revolución PQC

La informática postcuántica está abandonando rápidamente el terreno de la ciencia ficción para convertirse en la nueva realidad de la tecnología. Además de ventajas, la informática postcuántica tiene sus peligros. Pero aún se desconoce hasta qué punto es posible utilizar computadoras cuánticas para descifrar códigos imposibles desde el punto de vista matemático. Uno de los errores que puede cometer un profesional de la seguridad es esperar hasta que la informática cuántica esté aquí para empezar a preparar su entorno para potenciales amenazas. Ya existen soluciones sobre las que asentar la protección de los sistemas en el mundo de la criptografía postcuántica. Cualquier técnico debidamente formado sabe lo importante que es empezar a conocer y probar sistemas que protejan los activos cuando la informática cuántica sea la nueva realidad de la vida diaria.

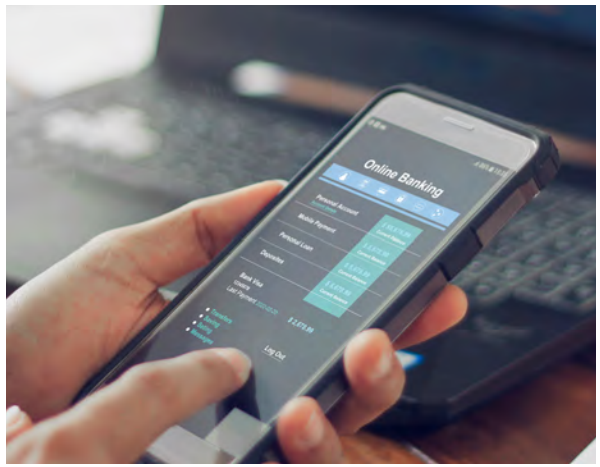
CUESTIÓNESE TODO LO QUE SABE. ESTO ES LA TECNOLOGÍA DE PKI MODERNA.

¿A qué se debe el resurgimiento de una tecnología de varias décadas de antigüedad con una reputación cimentada en la confiabilidad? La respuesta no está en un cambio en la tecnología, sino en un cambio en la forma en que el mundo utiliza la tecnología.

La infraestructura PKI funciona. Ha demostrado ser una solución confiable para la protección de la seguridad y de las identidades que se remonta a Netscape y los módem 33.6k. Aunque los protocolos se han actualizado y ha habido pequeñas modificaciones para adaptarse a los cambios experimentados en otras partes del mundo informático, la tecnología de PKI de hoy sigue siendo esencialmente la misma que la de ayer.

En 1996, la gente que trabajaba con PKI pensaba en proteger los resultados de búsqueda de Excite y las compras realizadas en eBay. Todavía hoy siguen siendo mayoría quienes creen que PKI solo sirve para eso. Sin embargo, no se dan cuenta de que la tecnología de PKI moderna se está utilizando para evitar accidentes de trenes o para impedir que los hackers roben información personal de los relojes inteligentes de los consumidores. Todo, sin dejar de cifrar eBay.

La infraestructura PKI moderna ha evolucionado con la tecnología y se ha ampliado para cubrir necesidades de seguridad en todo el mundo, en todo tipo de sectores, organizaciones y organismos públicos, así como en el hogar. Al fin y al cabo, la función que desempeña la tecnología de PKI en las balizas de rescate de emergencia no tiene un impacto menor que el hecho de que todos los días, gracias a esta misma tecnología, millones de personas puedan realizar transacciones bancarias online sin que nadie les robe el número de la tarjeta de débito. En ambos casos, no hay que subestimar la importancia de la confianza. PKI es la amalgama perfecta entre una tecnología acreditada y una solución que proporciona seguridad e identidad para las cosas que la gente inventa hoy y con las que sueña para el futuro. Con independencia de lo que venga después, PKI continuará brindando una confianza acreditada y flexible.



LA INFRAESTRUCTURA PKI MODERNA HA EVOLUCIONADO CON LA TECNOLOGÍA Y SE HA AMPLIADO PARA CUBRIR NECESIDADES DE SEGURIDAD EN TODO EL MUNDO.

Acerca de DigiCert

La mejor manera de hacer las cosas no se convierte en una práctica habitual hasta que alguien la descubre.

En DigiCert, todo nuestro afán ha sido, desde nuestras raíces, encontrar la mejor manera de proteger Internet. Es por eso que el 89 % de las empresas que forman parte de la lista de Fortune 500, el 97 % de los principales bancos internacionales y el 81 % del comercio electrónico mundial confían en nuestros certificados TLS/SSL. Es por eso que las reseñas de nuestros clientes sobre nuestros servicios y asistencia son las que reciben más calificaciones de cinco estrellas del sector, encuesta tras encuesta. Es por eso que estamos modernizando la infraestructura PKI mediante la creación de la plataforma DigiCert ONE y herramientas de gestión que ayudan a las empresas a proteger sus identidades, accesos, servidores, redes, correo electrónico, código, firmas, documentos y dispositivos IoT. En cuestión de soluciones de SSL, IoT, PKI —por poner solo unos ejemplos—, DigiCert ofrece algo único. Somos, en definitiva, lo opuesto al denominador común.

¿Conoce a alguien que esté utilizando la infraestructura PKI de forma innovadora? Nos encantaría publicar su caso. ¿Le gustaría conocer mejor las soluciones de PKI de DigiCert? Se las enseñamos encantados.
PKI_Info@digicert.com