DIGITAL TRUST PARA EL MUNDO REAL

digicert®

ÍNDICE

DESDE LAS MONTAÑAS DE ALASKA HASTA EL LÍMITE DEL ESPACIO

Un lluvioso día del verano de 2013, un hidroavión que sobrevolaba a poca altitud una zona montañosa cercana a Petersburg, en Alaska, entró en pérdida y se estrelló. A bordo iban seis pasajeros de camino a una visita turística del glaciar LeConte. Cuando intentaba un ascenso para franquear un desfiladero de los acantilados de Horn Cliffs, el piloto cometió un error de cálculo y perdió el control del aparato, que comenzó a dar vueltas antes de empezar a caer en picado e impactar contra las gigantes coníferas que encontró a su paso.

Para los supervivientes del accidente, heridos y atrapados en terreno escarpado, no había ninguna esperanza de escapar de la montaña por su propio pie. No faltaba mucho para que cayera la noche y, en Alaska, con la oscuridad llegan las temperaturas gélidas, incluso en junio. Y, por si fuera poco, no había carreteras. Hacía falta un equipo de rescate que sacase a los supervivientes de lo que quedaba del avión y los pusiera a salvo; pero en ese remoto lugar no había cobertura móvil, y la de radio eramuy limitada.

Afortunadamente, el avión estaba conectado a la constelación de satélites Iridium, que orbita a casi 800 km de distancia. Una baliza de emergencia envió una llamada de socorro y la posición de la aeronave a los equipos de búsqueda y rescate a través de una señal digital protegida. El dispositivo conectado a la constelación Iridium había estado siguiendo cada movimiento del avión, desde el despegue hasta el momento en que empezó a caer, trazando su recorrido segundo a segundo durante el tiempo que permaneció en vuelo —un sistema claramente superior al mero envío de coordenadas GPS o los avisos por radio—. Esto fue posible porque cada uno de los 66 satélites de Iridium establece un vínculo digital no solo con los dispositivos, sino también con los demás satélites de la constelación, lo que garantiza la comunicación y visibilidad de los dispositivos en todo momento y en cualquier lugar del planeta, desde la Antártida hasta Alaska.

Al conocer la ubicación exacta en la que se había estrellado el monomotor, la Guardia Costera de EE. UU. pudo llegar al lugar del accidente y, en

pocas horas, sus helicópteros ya habían rescatado a todos los supervivientes.

Cuando ya los habían liberado y trasladado para que recibieran asistencia médica, Alaska Public Media entrevistó al portavoz de los guardacostas, Grant DeVuyst. En referencia al dispositivo de señal de emergencia, afirmó: «Esa es la única razón por la que sabíamos que algo iba mal y la única razón por la que fuimos capaces de llegar al lugar del accidente y encontrarlos».

Normalmente, al hablar de interacciones digitales pensamos en cosas que hacemos desde el ordenador o el móvil, como comprar, mandar correos o utilizar aplicaciones; pero, hoy en día, el límite entre lo digital y lo real se ha desdibujado. Por todas partes hay conexiones que supervisan y generan grandes cantidades de datos, y que además garantizan el funcionamiento de un sinfín de dispositivos de todo el mundo.

En emergencias así en las que hay vidas en juego, el piloto necesita saber que la red satelital Iridium estará supervisando el vuelo y recibirá la señal de socorro y la retransmitirá a un equipo de rescate. Es una necesidad que trasciende el tráfico web, las comunicaciones por correo electrónico y lo que tradicionalmente entendemos como «conexión» o «cifrado de datos». La conexión y las comunicaciones entre estas balizas deben ofrecer el máximo nivel de fiabilidad en cualquier lugar del planeta, de modo que puedan responder de inmediato y en las condiciones más extremas para salvar vidas en el mundo real. Por eso la constelación de satélites Iridium se basa en la confianza digital.

«LA CONFIANZA DIGITAL ES CLAVE PARA LA SEGURIDAD DE TODAS LAS COSAS CONECTADAS, DESDE EL FONDO DEL MAR HASTA EL LÍMITE DEL ESPACIO».

Brian Trzupek
Vicepresidente sénior de productos, DigiCert

LA REALIDAD ES DIGITAL Y LO DIGITAL ES REAL

Hoy en día, todo está conectado. Ya hablemos de neveras o de teletrabajadores, cada vez más, todo lo que utilizamos o con lo que interactuamos está conectado a otras cosas. Los dispositivos son Internet, Internet son las aplicaciones móviles, los coches son ordenadores, las visitas médicas son virtuales y el entretenimiento es contenido en streaming. O, dicho de otro modo: ya no hay un límite entre lo real y lo digital.

En este contexto de conexiones omnipresentes, la confianza es la base de la comunicación digital. Las interacciones entre los distintos sistemas, dispositivos y usuarios son muy variadas y coexisten en espacios reales y virtuales, entretejidas en una red global cada vez más compleja. Si bien los métodos tradicionales de seguridad digital siguen siendo importantes, el cifrado por sí solo no basta. Para garantizar la comunicación y el buen funcionamiento del mundo conectado real, hace falta una arquitectura mucho más flexible y fiable que incorpore la tecnología, las normas y las prácticas en un sistema global de confianza digital.

¿Qué es la confianza digital?

La confianza digital hace referencia al marco, el software y las prácticas que garantizan la autenticidad de las interacciones entre el mundo digital y los negocios, gobiernos, consorcios e individuos. En esencia, la confianza digital responde a las necesidades del mundo conectado, protege de las amenazas y anticipa el crecimiento y la evolución de las tecnologías digitales. Para ello, se apoya en cuatro pilares:

Un organismo de normalización

Un conjunto de expertos y organizaciones líderes en el sector que establecen los protocolos, las tecnologías y los requisitos de identidad en materia de confianza digital. Por ejemplo, el CA/Browser Forum define los estándares aplicables a los certificados TLS/SSL y un marco común para verificar las identidades y el cifrado en Internet.

Cumplimiento y operaciones

Para garantizar el cumplimiento, hacen falta políticas y auditorías continuas que comprueben si las operaciones se realizan con arreglo a los estrictos estándares definidos por el organismo regulador pertinente. En lo que respecta a las operaciones —muy ligadas a los centros de datos—, habrá que validar el estado de los certificados mediante OCSP u otros protocolos.

Gestión del ciclo de vida de los certificados

Un software que centraliza la visibilidad y el control de los ciclos de vida de los certificados digitales para garantizar la confianza pública o privada dentro de una organización.

Aplicación en todos los ecosistemas

Se garantiza la confianza en cadenas de suministro complejas, a lo largo de todo el ciclo de vida de un dispositivo y a la hora de determinar si los contenidos publicados en un foro se utilizan con permiso de quien tiene los derechos digitales, así como en cualquier otro ámbito en el que haya objetos conectados.

UNA CONFIANZA REAL PARA EL MUNDO REAL

La noción de «confianza» entre dos puntos de una conexión digital es tan antigua como la comunicación digital en sí; pero, con demasiada frecuencia, ha habido un gran trecho entre la teoría y la práctica (o la tecnología). A los principios de la confianza les han faltado soluciones de hardware y software consonantes, y viceversa. La confianza digital es, a partes iguales, un concepto, una serie de procesos y un conjunto de herramientas. Es el punto en el que confluyen la tecnología digital y los ideales de confianza para ofrecer valor añadido y resultados reales.

SE NECESITA UNA ARQUITECTURA QUE INCORPORE LA TECNOLOGÍA, LOS ESTÁNDARES Y LAS PRÁCTICAS EN UN SISTEMA DE CONFIANZA DIGITAL.

CAPÍTULO 2

LA CONFIANZA ESTÁ PATENTE MIREMOS DONDE MIREMOS

Incluso a los padres de nuestras soluciones, ingenieros y expertos en seguridad, les sorprenden muchas veces las formas tan creativas que tiene la gente de utilizar la confianza digital. Como un hilo que hilvana tecnologías y sectores a priori dispares y sin relación, la confianza digital se convierte en el tejido en el que nos comunicamos, nos movemos y trabajamos en el mundo real.

AVIACIÓN

Despegues y aterrizajes seguros

En sectores con ecosistemas complejos, formados por muchas piezas conectadas con limitaciones en la potencia de los dispositivos y variación entre los tipos de dispositivos, hace falta una solución de seguridad adaptable y fiable. En el caso del tráfico aéreo, además de todos estos factores, hay que tener también en cuenta la necesidad de garantizar la confidencialidad de los datos.

La información transmitida entre la torre de control y el avión debe estar protegida, y el dispositivo en sí debe ser seguro. De lo contrario, podrían producirse manipulaciones cuyas consecuencias podrían ser catastróficas.

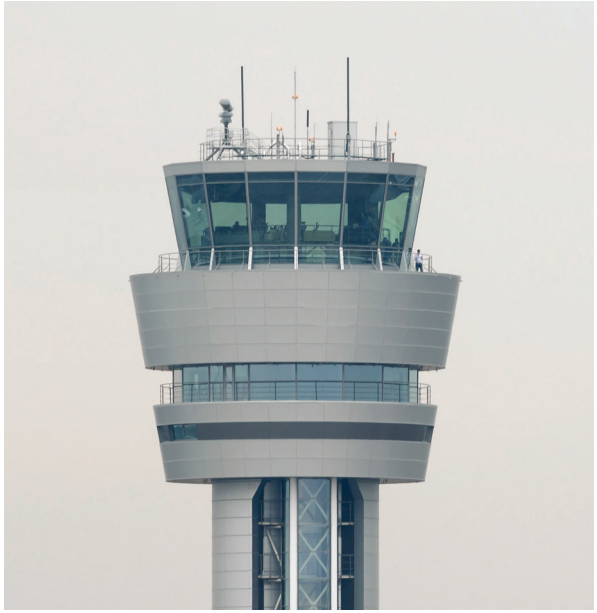
Cuando estos dispositivos y los datos que transmiten están protegidos por soluciones de confianza digital, los pilotos y los controladores pueden recopilar, compartir y utilizar de forma segura distintos tipos de información que les permiten garantizar la seguridad de los despegues y aterrizajes de cualquier avión y en cualquier aeropuerto. Si se utiliza el sistema AeroMACS, el resultado y el nivel de fiabilidad serán los mismos tanto en un pequeño aeropuerto de EE. UU. como en uno de los más grandes de Australia.

Implementación: en todo el mundo

Las soluciones de DigiCert protegen la red AeroMACS, el estándar para las comunicaciones aeronáuticas que muy pronto utilizarán casi todos los aeropuertos del mundo.

Necesidad principal: autenticación

En cualquier momento del día, hay miles de aviones en vuelo. Para proteger a los millones de pasajeros que cogen un avión cada día, y garantizar que lleguen a su destino a tiempo, los aeropuertos, las aerolíneas y los pilotos recurren a AeroMACS.



DESDE 2016, LOS SENSORES IoT DE LAS AERONAVES, PROTEGIDOS CON CONFIANZA DIGITAL, HAN TRANSMITIDO INFORMACIÓN DE VITAL IMPORTANCIA A LAS TORRES DE CONTROL Y LOS AVIONES.

CADENA DE SUMINISTRO

Ningún eslabón sin identificar

Imagine tener que localizar un contenedor en concreto entre los millones que, en un momento dado, viajan de un puerto a otro, cruzando océanos y bordeando distintos continentes. ¿Se imagina tener que hacerlo con bases de datos y registros de mercancías como única ayuda?

La cadena de suministro global vendría a ser como un reloj complejo: para que el mecanismo funcione, cada engranaje, muelle y rueda deben estar en su sitio y cumplir la función que les corresponde. Los retrasos en los envíos tienen un efecto dominó en toda la cadena Y los cargamentos extraviados pueden interrumpir la cadena y costar dinero a las empresas, debido a la pérdida tanto de materiales como de ingresos.

Campo de visión digital

Cada año, se transportan por mar más de 11 000 millones de toneladas de mercancías. Hoy hay más de 50 000 portacontenedores en el mundo.

La escala del comercio marítimo es gigantesca, y también dinámica. El movimiento es constante, y los cargueros salpican los mares como si fueran cuerpos celestes en una noche estrellada. Y por cada barco que hay navegando, hay aún más contenedores. Localizar y llevar un seguimiento de cada uno de estos contenedores en tiempo real y de forma segura es una tarea titánica.

La dificultad de los envíos a tal escala reside en la autenticación mutua entre los dispositivos sobre el terreno y la nube, desde donde se supervisan los activos. Una naviera que sea víctima de un ataque podría dejar de ver la posición de los contenedores o recibir información falsa acerca de estos. Para ser eficaz, una solución de seguridad no solo debe proteger el dispositivo, sino también la información que este transmite.

Además, debe ser capaz de adaptarse para proteger decenas de miles de dispositivos a la vez, sin excepción.

Cualquier ruta del mundo

Gracias a la confianza digital, es posible realizar un seguimiento seguro de los contenedores a lo largo de toda la ruta, desde que el barco leva anclas hasta que amarra en el puerto de destino, independientemente del número de viajes que haga o de en qué parte del mundo se encuentre. Así, hay menos probabilidades de que se produzcan robos o pérdidas y se garantiza una circulación eficiente de mercancías entre los distintos puertos.

Implementación: en todo el mundo

Los contenedores, elemento central de la cadena de suministro global, transportan mercancías y materiales entre todos los continentes.

Necesidad principal: autenticación

Las soluciones de DigiCert van más allá del mero seguimiento de los contenedores: ofrecen un método de autenticación seguro y en tiempo real para que las empresas puedan localizar e identificar el dispositivo asociado a cada uno de ellos.

GRACIAS A LA CONFIANZA DIGITAL, ES POSIBLE REALIZAR UN SEGUIMIENTO SEGURO DE LOS CONTENEDORES A LO LARGO DE TODA LA RUTA, DESDE QUE EL BARCO LEVA ANCLAS HASTA QUE AMARRA EN EL PUERTO DE DESTINO, INDEPENDIENTEMENTE DEL NÚMERO DE VIAJES QUE HAGA O DE EN QUÉ PARTE DEL MUNDO SE ENCUENTRE.

PLANTILLAS GLOBALES

Todos los usuarios, en cualquier momento y lugar

En ocasiones, gestionar el tamaño de una empresa es igual de complejo que gestionar sus productos. Por ejemplo: ¿cómo se protege a los usuarios, cuando cada uno trabaja en lo suyo y desde distintas oficinas repartidas por todo el mundo; y no solo eso, sino que además utilizan distintos sistemas operativos, aplicaciones y dispositivos (muchos de ellos personales)?

Para IBM, esto no era un simple ejercicio teórico; Era un problema real al que tuvieron que poner remedio mucho antes de que la pandemia de COVID-19 obligara a muchísimas más empresas a adoptar soluciones para el teletrabajo.

Uso de cualquier dispositivo para trabajar

Autenticar, identificar y proteger a más de 500.000 usuarios. Tal era la tarea que tenían entre manos.

En casos así, los términos «flexible» y «escalable» no pueden limitarse a meras descripciones teóricas: deben ser características reales de una solución de confianza digital eficaz. Sin duda el número de usuarios supone un reto importante; pero tan importante, o más, es el reto que presenta la cantidad de tipos de dispositivos y aplicaciones que esos usuarios utilizan para trabajar (el portátil de la empresa, su teléfono personal, un viejo iPad, etc.). Si quiere que sus empleados, proveedores y contratistas tengan flexibilidad para trabajar con los dispositivos con los que se sientan más cómodos, pero sin arriesgarse a introducir vulnerabilidades en su red, necesita una solución de seguridad que sea adaptable y robusta al mismo tiempo.

En este caso, la flexibilidad y la escalabilidad son trascendentales, y también dos atributos fundamentales de la confianza digital. IBM recurrió a soluciones de confianza digital para poder autenticar un número ilimitado de dispositivos, independientemente del propietario o de los programas que ejecuten. Además, la empresa puede también autenticar varios dispositivos a la vez, sin importar dónde se encuentren los cientos de miles de usuarios que trabajan con ellos. Y lo mejor es que los más de 500 000 usuarios ni se enteran.

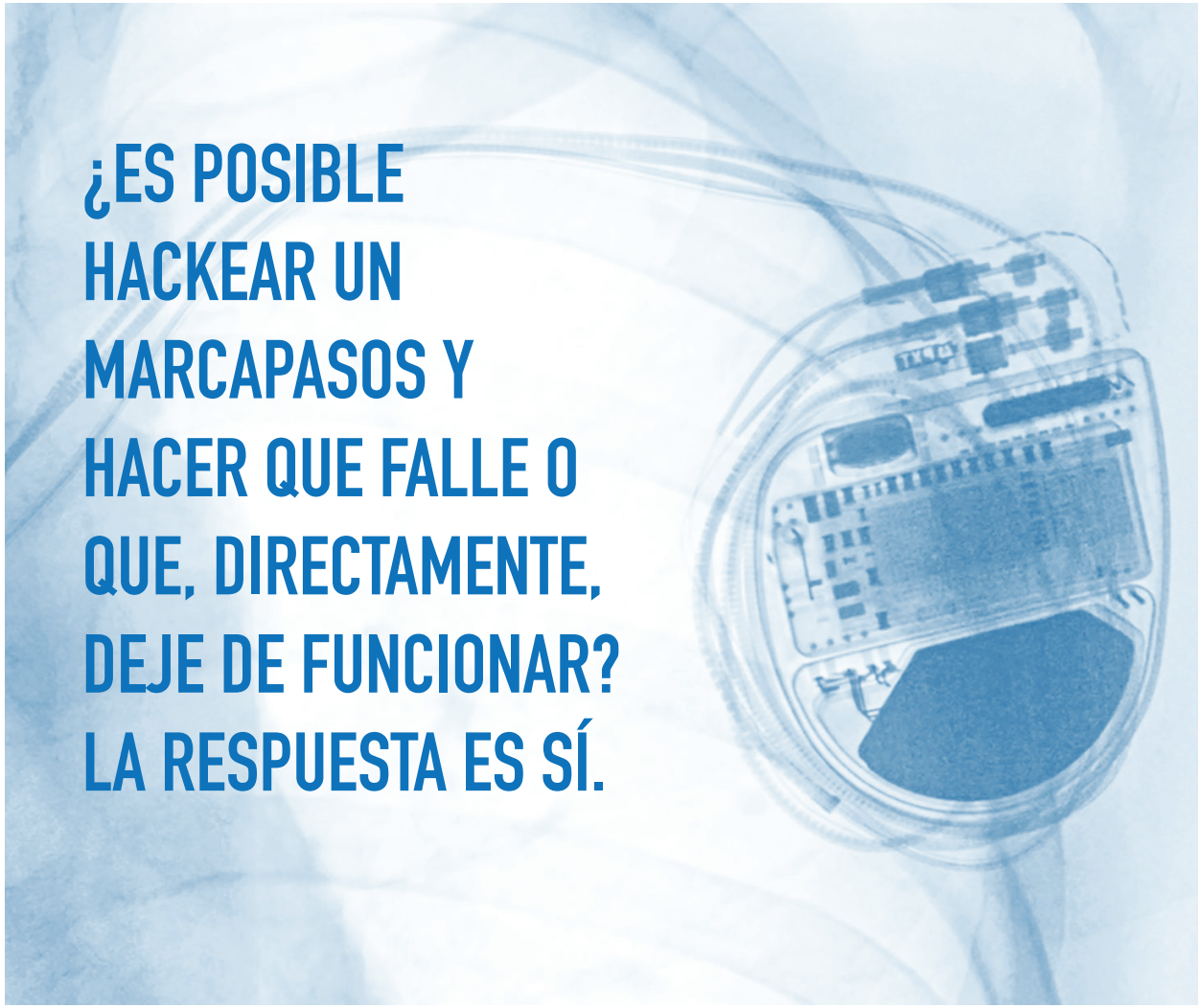
Implementación: en todo el mundo

Son miles las oficinas repartidas por todo el planeta que mantienen vivo a un más que consolidado líder mundial en software y hardware.

Necesidad principal: flexibilidad y escalabilidad

Cuando hay que garantizar la continuidad de las operaciones críticas, la PKI ofrece una solución para autenticar, proteger e identificar a medio millón de usuarios empresariales repartidos por todo el mundo.

EN ENTORNOS EN LOS QUE LOS SISTEMAS, EMPLEADOS, PROVEEDORES Y CONTRATISTAS ESTÁN CONECTADOS, LA SEGURIDAD HA DE SER ADAPTABLE Y ROBUSTA.



SANIDAD

La confianza como pieza central de la atención sanitaria

A la mayoría de nosotros, los dispositivos digitales nos hacen la vida más cómoda. Por ejemplo, gracias a una conexión por Bluetooth podemos comprobar la temperatura y humedad del jardín, y la conexión wifi entre la tele inteligente del salón y el iPad que nos llevamos a la cocina nos permite retomar el capítulo que estábamos viendo mientras hacemos la cena. Son conexiones que agradecemos, pero que, la mayoría de las veces, no necesitamos. Sin embargo, para algunas personas, este tipo de conexiones pueden suponer la diferencia entre vivir o morir.

Hace unos años, unos ingenieros médicos presentaron un nuevo tipo de marcapasos: el marcapasos inteligente. Este dispositivo se conecta por Bluetooth a un monitor externo y a una aplicación instalada en el teléfono del paciente, lo que le permite no solo enviar las señales eléctricas que necesita el corazón para seguir latiendo, sino también informar tanto al paciente como al médico del estado del marcapasos (por ejemplo, si está funcionando como es debido o cuánta batería le queda).

Antes, para determinar o corregir estos datos era necesario acercarse al hospital, cuando no someterse a una operación quirúrgica. Con el marcapasos inteligente, todo esto podía supervisarse, registrarse y comunicarse de forma automática y continua.

Los marcapasos conectados son mucho más que una comodidad, porque miles de personas dependen de ellos para seguir con vida. Lo malo es que, como con cualquier otra conexión, existe el riesgo de interferencia. Para los pacientes que tienen este tipo de marcapasos, la confianza digital es una necesidad imperiosa y muy real.

Una cuestión de vida o muerte (literalmente)

En agosto de 2017, una inusual noticia acaparaba titulares (inusual, al menos, para quienes no trabajan en el ámbito del IoT): la Administración de Alimentos y Medicamentos de Estados Unidos anunciaba la «retirada» de casi medio millón de marcapasos por cuestiones de ciberseguridad. En lo que parecía un caso más de riesgo de piratería informática, la FDA advirtió de que algunos marcapasos podrían «ser vulnerables a exploits e intrusiones de ciberseguridad». Sonaba muy raro, como a película de ciencia ficción. ¿De verdad era posible hackear un marcapasos y hacer que fallase o que, directamente, dejase de funcionar? La respuesta es sí.

A medida que los fabricantes de dispositivos médicos discurrían nuevas formas de conectar estos aparatos —desde camas de hospital inteligentes hasta monitores de glucosa de funcionamiento continuo—, se disparaban los beneficios para los pacientes. Pero con ellos aumentaban también la preocupación por proteger los datos que recopilaban los dispositivos conectados sobre los pacientes y, más adelante, el temor de que una intrusión provocase el fallo de estos dispositivos.

Y el temor no era infundado: los hackers vieron en los marcapasos una vía de intrusión. Los fabricantes cifraban las comunicaciones entre el marcapasos y el monitor colocado en la mesilla de noche, pero el monitor en sí carecía de protección. Al tener acceso al monitor, los hackers podían mandar instrucciones al marcapasos repetidamente, lo que acababa agotando su batería. Y peor aún: esas instrucciones podían ser que el aparato alterase las descargas eléctricas administradas al paciente, causándole problemas o incluso llevándolo a la muerte. Para cubrir la necesidad de proteger no solo el dispositivo, sino también al paciente, muchos fabricantes decidieron recurrir a una solución de confianza digital.

En la actualidad, miles de pacientes disfrutan de la tranquilidad de saber que cuentan con un sistema de supervisión seguro y cómodo que garantiza el buen funcionamiento de su marcapasos y los avisa si se produce cualquier tipo de problema. A corto plazo, la tecnología cardiovascular seguirá incorporando nuevas funciones y ofreciendo a más pacientes (y a sus médicos) más opciones para mejorar los datos, así como asistencia inmediata, sin necesidad de pisar el hospital ni pasar por el quirófano. También cambiarán los dispositivos médicos, que serán cada vez más pequeños e inteligentes, pero la solución de seguridad que protegerá los datos y la vida de los pacientes seguirá siendo la misma: la confianza digital.

Implementación: en varios países de todo el mundo

Miles de hospitales y centros de atención médica, y millones de personas, sujetos a distintas normas de cumplimiento e implementación; uso destinado tanto a proveedores como a pacientes.

Necesidad principal: fiabilidad

Una solución de seguridad que proteja la integridad del dispositivo y los datos de los pacientes y que ofrezca suficientes garantías como para confiarle vidas humanas.

BASADA EN TECNOLOGÍAS DE EFICACIA PROBADA

Sin la tecnología para sustentarla, la confianza digital no es más que una quimera. Para implementar la confianza digital en el mundo real, se necesitan programas de software y sistemas que permitan establecer conexiones seguras a lo largo y ancho de este ecosistema tan amplio y complejo. Pero no vale cualquier tecnología. Para que la confianza cumpla su cometido en el mundo real, las conexiones deben tener ciertas características y estar basadas en protocolos y software de seguridad de eficacia probada.

Los tres principios de las conexiones seguras

Identidad

Las personas, los negocios, las máquinas, las cargas de trabajo, los contenedores, los servicios y cualquier otra cosa que se conecte deben estar autenticados con una identidad única desde el punto de vista criptográfico.

Integridad

Para utilizar y transmitir objetos, es necesario prevenir las manipulaciones y contar con herramientas que verifiquen que dicho objeto no ha sufrido modificaciones.

Cifrado

Es necesario proteger los datos mientras se transmiten.

PARA QUE LA CONFIANZA CUMPLA SU COMETIDO EN EL MUNDO REAL, LAS CONEXIONES DEBEN BASARSE EN PROTOCOLOS Y SOFTWARE DE SEGURIDAD DE EFICACIA PROBADA.

LA PKI COMO PIEDRA ANGULAR

Durante décadas, la infraestructura de clave pública ha demostrado ser muy eficaz a la hora de proteger sitios web. Con los años, y a medida que evolucionaba el mundo conectado, los expertos en seguridad digital se dieron cuenta de que esa misma tecnología de eficacia probada que se utilizaba para cifrar los sitios web servía también para verificar la identidad digital y la autenticidad de los datos. Y los certificados pueden emitirse para prácticamente cualquier objeto digital, desde las redes y el código hasta los correos electrónicos y los documentos; e incluso para los usuarios y los dispositivos. Por su propia naturaleza, la PKI garantiza el cifrado, la integridad y la identidad en las conexiones digitales, de ahí que destaque como un componente básico de la confianza digital que siempre está a la altura de cualquier desafío.

Versatilidad

En los ecosistemas de hoy en día, los profesionales necesitan tener la capacidad de, por ejemplo, proteger el sitio web y las aplicaciones o de firmar un documento de forma segura y autenticar al mismo tiempo el teléfono de un empleado. Una empresa podría necesitar una solución para los robots automatizados de la cadena de producción y otra, un sistema para proteger los números de las tarjetas de crédito de sus clientes.

Cualquier solución que permita hacer una cosa, pero no la otra, o que hoy funcione y mañana no, no solo contribuye a la carga de trabajo de los responsables de gestionar la seguridad, sino que además pone en riesgo la empresa.

A diferencia de otros tipos de soluciones de seguridad, la PKI es extremadamente versátil. Como utiliza pares de claves asimétricos y el proceso de seguridad puede cifrar al igual que validar, es posible implementarla en un número ilimitado de entornos y sirve para proteger una gran variedad de conexiones. Las soluciones de PKI pueden ampliarse o reducirse según sea necesario, ejecutarse en la nube, en local o en entornos híbridos, y utilizarse hoy para proteger la web y el correo electrónico y mañana, los dispositivos IoT y personales. Es una sola solución que permite cubrir un sinfín de necesidades en materia de seguridad.

Confianza pública y privada

La PKI va más allá del cifrado: vincula la identidad a una clave mediante un proceso de firma.

La firma la emite el certificado raíz, por lo que cualquiera que tenga la clave pública de este sabrá que la firma vinculada al certificado PKI es válida y de confianza.

En algunos casos, ese certificado raíz es público, es decir, está incluido en un almacén de confianza alojado en un navegador web (como Chrome o Firefox) o en un sistema operativo (como Windows de Microsoft o macOS de Apple). En otros, es privado, lo que significa que se utiliza únicamente para los sistemas internos de la empresa o para un grupo reducido de empresas. Desde el punto de vista criptográfico no hay ninguna diferencia, pero el hecho de poder elegir entre la opción pública y la privada confiere una gran versatilidad a la PKI.

Es gracias a esta versatilidad que la PKI tiende un puente entre la confianza pública y la privada. Es lo suficientemente segura y avanzada como para haberse ganado la confianza de muchas administraciones públicas en todo el mundo, que la han elegido como su solución privada para el cifrado y la identidad, y de los fabricantes de dispositivos IoT, que la han adoptado como solución pública.

PONGA LA CONFIANZA DIGITAL A SU SERVICIO

Lo más importante acerca de la confianza digital suele ser también lo que más se pasa por alto: que «digital» ya no significa lo mismo que antes. La razón de ser de la confianza digital tiene que ver con lo que durante miles de años ha sido la base de los negocios, los acuerdos, los contratos sociales e incluso simples interacciones humanas. Y es que, ya hablemos del espacio físico o del espacio virtual, necesitamos tener la certeza de que nuestras interacciones son auténticas, de que nuestras comunicaciones están protegidas y de que la información que intercambiamos es legítima y no ha sufrido manipulaciones.

La confianza digital es mucho más que un ideal y que un software de seguridad: es poder confiar en las interacciones entre cualquier persona o cosa que se conecte a Internet. En ese sentido, lo importante de la confianza digital no es tanto lo que es, sino lo que hace.

Acerca de DigiCert

DigiCert es un proveedor líder de confianza digital. Gracias a él, los usuarios individuales, las empresas, las administraciones públicas y los consorcios pueden utilizar Internet con la tranquilidad de saber que su presencia en el mundo digital está protegida.

La plataforma DigiCert® ONE, garantía de confianza digital, protege los sitios web, los accesos y comunicaciones empresariales, el software, las identidades, el contenido y los dispositivos, entre otros elementos, para que las empresas respondan a toda una gama de necesidades en materia de confianza digital con una visibilidad y un control centralizados. Su galardonado software y su liderazgo en el sector de los estándares, la asistencia y las operaciones convierten a DigiCert en el proveedor al que recurren las grandes empresas de todo el mundo que apuestan por la confianza digital.

¿Quiere poner la confianza digital al servicio de su empresa? Póngase en contacto con sales@digicert.com para obtener más información.