EBOOK

QUI DIT CONFIANCE, DIT PKI

digicert®

SOMMAIRE

DES FRONTIÈRES DE L'ALASKA AUX CONFINS DE L'ESPACE

Un jour d'été pluvieux de 2013, un hydravion décroche en plein air alors qu'il vole à basse altitude au-dessus d'une zone montagneuse près de Petersburg, en Alaska. À son bord, six passagers en route pour une visite touristique du glacier LeConte. Suite à une erreur de jugement en tentant de franchir les Horn Cliffs, le pilote perd le contrôle de l'appareil qui se retourne alors sur lui-même avant de piquer droit vers le sol et de percuter les conifères géants situés juste en-dessous.

Blessés et pris au piège sur un terrain escarpé, les survivants du crash ne peuvent espérer quitter la montagne sans l'intervention des secours. La nuit est sur le point de tomber. Or, même en juin, l'obscurité en Alaska est synonyme de températures glaciales. Et il n'y a ni réseau, ni route à cet endroit. Seule une équipe de sauvetage aérien serait en mesure de sortir les passagers de l'épave et de les ramener en sécurité.

À environ 800 km du sol, Iridium, un système de maillage satellitaire, capte le signal de la balise d'urgence de l'avion et transmet l'appel de détresse et l'emplacement aux autorités. Plus qu'un simple GPS ou un système d'appels d'urgence, un satellite Iridium avait suivi les mouvements de l'avion du décollage au crash, dessinant en temps réel la trajectoire du vol. Cette prouesse technologique, on la doit aux 66 satellites Iridium orbitant la Terre dans un mouvement soigneusement chorégraphié. Ces satellites communiquent entre eux et avec la surface pour couvrir à chaque seconde le moindre recoin de la planète. Sur le réseau de la constellation Iridium, toute balise fonctionnelle est visible à tout moment, partout dans le monde, de l'Antarctique à l'Alaska.

Tous les avions ne sont pas équipés de ce type de dispositif de traçage et de signalisation d'urgence. Mais de plus en plus de compagnies et de pilotes, notamment ceux qui volent sur des aéronefs de petite taille ou traversent des zones reculées, en ont un à bord.

Dans la plupart des cas, il ne sert qu'à rassurer. Mais il a parfois fait toute la différence entre la vie et la mort.

Sachant exactement où l'avion s'était écrasé, les gardes côtes américains ont pu atteindre le lieu de l'accident et, en quelques heures, des hélicoptères avaient secouru tous les rescapés. Une fois les passagers extirpés de la carlingue et évacués vers l'hôpital le plus proche, l'Alaska

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

Public Media[1] a interviewé Grant DeVuyst, porte-parole des gardes-côtes. Concernant le dispositif de signalisation d'urgence, celui-ci a déclaré : « Sans lui, nous n'aurions pas su qu'il y avait eu un problème et encore moins nous rendre à temps sur les lieux. »

Dans ces rares cas d'urgence, où des vies sont en jeu, un pilote doit avoir la certitude que le réseau satellite Iridium suivra le vol et captera le signal de détresse pour le relayer à une équipe de secours. Le signal doit être protégé des interceptions, le dispositif d'urgence authentifié et le réseau préservé de toute interruption de service. Toute défaillance dans le système Iridium peut entraîner la perte de vies humaines. Ici, la confiance est un enjeu vital dans tous les sens du terme, et aucune erreur n'est permise. C'est pourquoi la constellation de satellites Iridium est sécurisée par PKI.

« DES PROFONDEURS DES OCÉANS AUX CONFINS DE L'ESPACE, LA SÉCURITÉ PKI INTERVIENT SUR TOUS LES FRONTS. »

Brian Trzupek
SVP produits, DigiCert

CHAPITRE 1

LA CONFIANCE, UN BESOIN EN PERPÉTUELLE ÉVOLUTION

Dans les années 70, lorsque les cryptologues britanniques James Ellis et Clifford Cocks ont pour la première fois émis l'idée d'un « chiffrement non secret », ils n'imaginaient pas un jour le voir appliqué sur des dizaines de millions de sites web dans le monde. À cette époque, Internet n'était encore qu'un projet de la DARPA, utilisé occasionnellement pour permettre aux chercheurs universitaires de partager des données ou des résultats d'études.

En quelques décennies, l'infrastructure à clés publiques (PKI, Public Key Infrastructure) d'Ellis et Cocks s'est imposée comme un bouclier contre le piratage et la fraude dans une nouvelle ère de l'information. Aujourd'hui, tout site web considéré comme fiable doit ce capital confiance à la technologie PKI.

Or, l'invention du web – qui, à elle seule, aurait suffi à définir une époque entière dans le développement humain – a été immédiatement suivie d'une seconde révolution, celle des objets connectés. Des réfrigérateurs aux applications bancaires, toutes sortes d'appareils sont devenus du jour au lendemain partie intégrante d'un écosystème mondial de réseaux, d'équipements, d'applications et d'utilisateurs capables de communiquer à distance.

Ce phénomène a été, et demeure, si rapide qu'on ne peut l'exprimer que par des superlatifs. Et tandis que des centaines de milliers d'idées émergent pour connecter des millions de personnes à des milliards d'objets, le besoin d'une sécurité robuste augmente, lui, à un rythme exponentiel.

Des échanges culturels aux progrès médicaux, l'ère de l'information a certes eu un impact extrêmement positif sur l'humanité. Mais comme toute médaille a son revers, ce vaste réseau de communication donne également libre cours aux criminels et autres opportunistes pour abuser de la confiance des utilisateurs dans tout ce qui a trait aux technologies.

Il faut donc redonner le plus haut niveau d'assurance possible dans tout ce qui est connecté. L'infrastructure PKI apporte cette garantie de confiance. Elle offre une solution de sécurité et d'identification suffisamment fiable pour protéger les données les plus sensibles, et suffisamment flexible pour fonctionner sur les inventions les plus récentes. Grâce aux infrastructures PKI, nous pouvons enfin profiter en toute sérénité des avantages d'un monde capable de communiquer en quasi-instantané sur toute la planète – voire dans l'espace.

L'INFRASTRUCTURE PKI APPORTE CETTE GARANTIE DE CONFIANCE.

Des menaces en pleine expansion

Chaque jour, de nouvelles idées sont développées pour renforcer la surveillance, l'efficacité et la fiabilité des ordinateurs, des applications et des appareils. Or, qui dit nouvelle connexion, dit nouvelle vulnérabilité. Une vulnérabilité est un point d'entrée potentiel dans tout élément avec lequel une application ou un appareil communique.

Les risques financiers sont bien connus. Depuis des années, nous voyons tout le mal que les cybercriminels peuvent faire à leurs victimes. En 2017, un grand organisme de crédit à la consommation s'est vu condamné à verser 700 millions de dollars de dommages et intérêts suite à une compromission de données massive[2]. Une étude Ponemon/IBM de 2019 a quant à elle révélé que le coût moyen d'une compromission de données était d'un peu moins de 4 millions de dollars[3]. La même année, le Consumer Breach Report de ForgeRock[4] a fait état d'une perte de 17,76 milliards de dollars dans le secteur de la santé. Celui-ci a en effet été le plus ciblé en 2019, avec 45 % de toutes les compromissions recensées.

Le coût financier pour toute la branche médicale peut paraître stupéfiant en soi, mais le nombre et la nature des attaques le sont probablement encore plus.

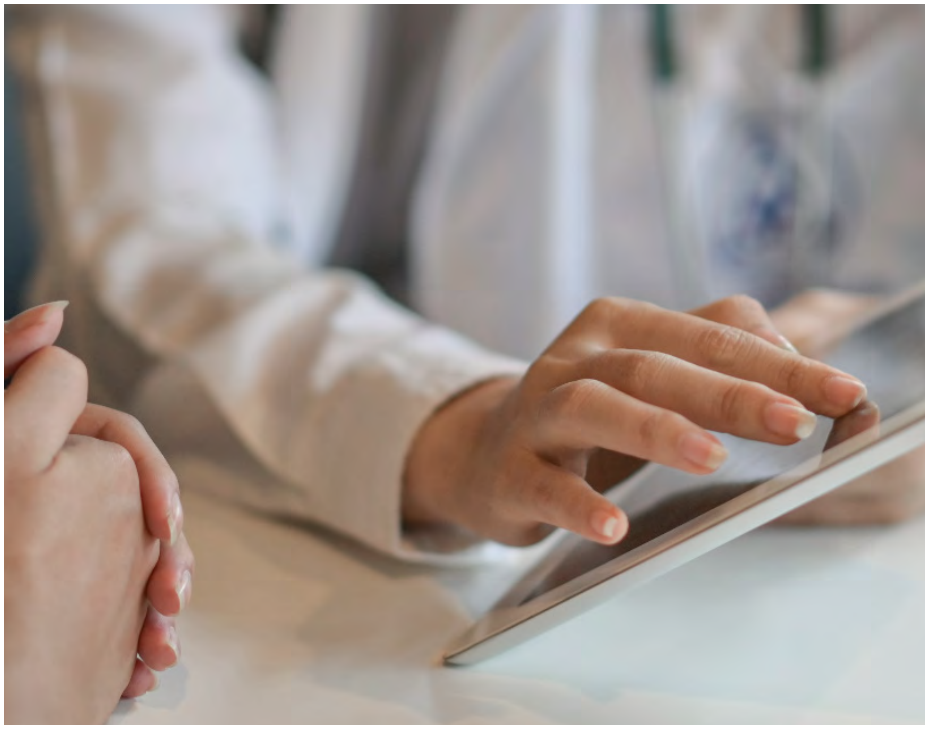
[2] https://investor.equifax.com/news-and-events/press-releases/2019/07-22-2019-125543228 [3] https://digitalguardian.com/blog/whats-cost-data-breach-2019 [4] https://healthitsecurity.com/news/health-sector-most-targeted-by-hackers-breach-costs-rise-to-17.76b

Ces pertes ont été réparties sur 382 compromissions utilisant diverses méthodes pour cibler les réseaux des établissements de santé. Hier, la norme était de pirater les réseaux et les sites web pour cibler les transactions des banques et des consommateurs. Aujourd'hui, les cybercriminels exploitent les vulnérabilités d'appareils peu sécurisés et d'utilisateurs peu aguerris pour monétiser l'information extirpée.

Résultat : à ressources égales, les organisations sont aujourd'hui confrontées à un nombre de menaces beaucoup plus élevé. La numérisation des analyses, les moniteurs connectés et les outils de traitement intelligents révolutionnent les soins médicaux. Or, les professionnels de santé qui les utilisent ne sont pas des experts en sécurité. Quant aux équipes informatiques, elles doivent se livrer à un exercice d'équilibriste entre restrictions budgétaires, nouvelles technologies et resserrement du cadre réglementaire.

Le monde de l'information traverse une période passionnante et pleine de promesses. Des consommateurs aux États, en passant par les entreprises transnationales, tout le monde devrait bénéficier des énormes retombées du tout-connecté. Mais pour les professionnels IT qui œuvrent en coulisses, cerner les menaces et trouver des solutions de sécurité efficaces prend souvent de allures de parcours du combattant.

Face à des menaces en perpétuelle évolution, les professionnels de la sécurité ont besoin d'une solution flexible, rapide à déployer, facile à gérer et capable de neutraliser n'importe quelle attaque, tout en évoluant au rythme des besoins de leur organisation. C'est là toute la mission de l'infrastructure PKI.



Face à des menaces en perpétuelle évolution, les professionnels de la sécurité ont besoin d'une solution flexible, rapide à déployer, facile à gérer et capable de neutraliser n'importe quelle attaque.

ÉTUDE DE CAS – FLORENCE (ALABAMA)

Un gros poisson dans une petite mare

En juillet 2019, la nouvelle d'une compromission massive des données d'une banque affectant 100 millions de clients s'est répandue comme une traînée de poudre à travers toute la planète[5]. Il s'agissait d'un énième cas de vol de données à l'échelle mondiale.

Pendant ce temps-là, d'autres cybercriminels s'affairaient à tester la résistance de cibles plus petites, cherchant ici et là des opportunités d'exploiter des systèmes faiblement sécurisés. Les collectivités locales ou territoriales, où le manque de moyens rend difficile la protection de tous les systèmes et utilisateurs, semblent être soumises à ce genre de vulnérabilités.

Plutôt que de s'attaquer à des grands groupes, dont les services informatiques sont à la fois bien développés et bien équipés, ces criminels préfèrent s'immiscer sur les réseaux de municipalités et autres petites collectivités pour y déployer des ransomwares et ainsi tenir les autorités en otage.

C'est exactement ce qui s'est passé en juin 2020, à Florence, dans l'Alabama. Située sur les rives du Tennessee, à la frontière nord de l'État, cette ville de 40 000 habitants est connue pour sa foire annuelle de la Renaissance et pour avoir vu naître W. C. Handy, pionnier de la musique blues.

À la fin du mois de mai, les responsables municipaux sont avertis d'une éventuelle compromission en gestation. Mais à ce moment-là, il est déjà trop tard. Le malfaiteur s'était infiltré dans le réseau environ un mois plus tôt et avait peu à peu étendu son emprise sur les systèmes de la ville. Ce dernier passe à l'offensive le 5 juin, paralysant tous les serveurs et exigeant une rançon sous forme de bitcoins.

Après consultation auprès d'experts en sécurité très au fait des habitudes de ce criminel notoire, les responsables de la ville ont décidé de payer les 300 000 dollars réclamés. Florence n'était toutefois pas un cas isolé. À peine quatre mois avant, le New York Times faisait état d'une hausse de 41 % des attaques par ransomware, entre 2018 et 2019,[6] et de dizaines de villes victimes de compromissions.

Alors que les attaques de plus grande envergure sont souvent largement reprises dans les médias, une autre faction de criminels s'est fait une spécialité de prendre en otage des entités plus vulnérables et plus susceptibles de céder à leur chantage. À l'image d'un gros poisson dans une petite mare, ils déploient leurs tentacules sur des structures mal défendues afin d'en soustraire une rançon souvent juteuse.

Contrairement à d'autres solutions d'identification et de sécurité, une infrastructure PKI est suffisamment flexible pour fonctionner aussi bien pour les réseaux et les e-mails que pour le web. Pour simplifier le déploiement des environnements de sécurité, les solutions PKI donnent aux responsables IT et sécurité la possibilité d'émettre et de gérer des certificats de chiffrement et d'authentification pour une variété de systèmes, de périphériques et d'utilisateurs.

La solution qui protège déjà vos sites web peut également sécuriser vos réseaux, appareils, e-mails, documents et utilisateurs. Elle prévient ainsi les attaques par ransomware tout en simplifiant votre écosystème de sécurité.

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

CHAPITRE 2

PKI : CE QUE VOUS NE SAVIEZ PEUT-ÊTRE PAS

Le grand défi du monde connecté d'aujourd'hui se résume en un mot : complexité.

Quand ce n'est pas le défi lié à la complexité accrue des attaques, c'est celui d'écosystèmes complexes que la cohabitation de technologies d'ancienne et de nouvelle génération rend difficile à protéger. Et quand ce n'est pas le défi de la complexité des écosystèmes, c'est celui de la sécurité d'environnements où les utilisateurs ne sont pas toujours conscients des menaces plus complexes et sophistiquées qui les guettent.

Partout dans le monde, les consultants et analystes en sécurité entendent ce même refrain : les professionnels de l'informatique et de la sécurité ont besoin d'une solution simple à configurer et à gérer, et réellement digne de confiance.

C'est ici que l'infrastructure à clés publiques (PKI, Public Key Infrastructure) entre en jeu.

Si vous avez des notions en sécurité Internet, vous savez déjà ce qu'est une infrastructure PKI. Et vous connaissez probablement le PKI depuis longtemps, car cela fait vingt ans que cette infrastructure s'impose comme une solution de confiance pour la sécurité des sites web. D'abord avec la technologie SSL, puis désormais avec le TLS. Elle offre aujourd'hui la même garantie de confiance qu'il y a vingt ans.

Mais ce que beaucoup de gens ne savent souvent pas, c'est qu'une infrastructure PKI ne protège pas uniquement le web. Elle protège également les applications. Elle protège le code. Elle protège les montres connectées, les voitures, les contrats, les lits d'hôpitaux et les satellites. Cette solution de sécurité, testée et éprouvée depuis deux décennies sur le web, s'avère tout aussi fiable et efficace sur les technologies connectées les plus récentes et les plus innovantes.

Une solution qui a fait ses preuves

Dans un monde connecté qui évolue au quotidien, les infrastructures PKI se montrent aussi efficaces dans la sécurisation des tout derniers appareils IoT qu'il y a vingt ans avec le chiffrement des sites web.

Tout leur génie se situe dans la simplicité du chiffrement asymétrique à deux clés. Dans un chiffrement asymétrique, une partie peut sécuriser les données et les transmettre à une autre partie sans partager de secret commun. Le craquage du code d'une clé n'affecte donc pas le chiffrement de l'autre. Il faut les deux clés de la paire pour pouvoir déchiffrer les données.

C'est ainsi que les infrastructures PKI apportent invariablement la preuve de leur fiabilité depuis des décennies.

Une solution flexible

Les écosystèmes actuels exigent de pouvoir sécuriser un site web en même temps qu'une application, ou encore de signer un document de manière sécurisée tout en authentifiant le smartphone d'un collaborateur. Une entreprise aura besoin d'une solution pour les robots automatisés de sa ligne de production, tandis qu'une autre devra de protéger les numéros de carte bancaire de ses clients. Une solution qui fonctionne dans un sens mais pas dans l'autre, ou un jour mais pas le lendemain, non seulement augmente la pression sur les équipes de sécurité, mais expose également toute l'organisation aux plus grands dangers.

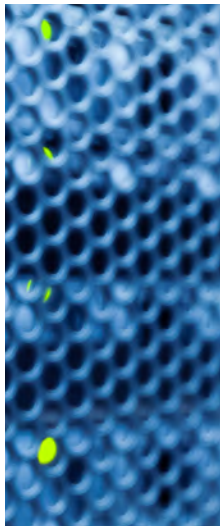
Contrairement aux autres modes de sécurité, une infrastructure PKI est extrêmement flexible. Parce qu'elle repose sur des paires de clés asymétriques et que le processus de sécurité peut valider ces clés aussi facilement que chiffrer les données, une solution PKI peut être déployée dans un nombre incalculable d'environnements pour assurer la protection d'un large éventail de connexions. Les solutions PKI évoluent de manière élastique, fonctionnent dans le cloud, sur site et dans les environnements hybrides. Garantes de la sécurité du web et des e-mails aujourd'hui, elles assureront la protection du BYOD et de l'IoT demain. Bref, elles répondent à tous les besoins de sécurité.

Une solution de confiance en public comme en privé

Plus qu'une simple solution de chiffrement, un certificat PKI relie des identités à des clés via un processus de signature. La signature est émise par la racine. Ainsi, toute personne disposant de la clé publique de cette racine sait que la signature rattachée au certificat PKI est valide et approuvée.

Cette racine est parfois publique, c'est-à-dire qu'elle est distribuée dans un Trust Store hébergé par un navigateur web (Chrome, Firefox, etc.) ou un système d'exploitation (Microsoft Windows, Apple MacOS, etc.). Et elle est parfois privée. Autrement dit, elle est considérée comme fiable par tous les systèmes qu'une organisation souhaite utiliser en interne ou dans un groupe restreint d'entités. La cryptographie utilisée est la même dans tous les cas, mais le fait de pouvoir déployer des solutions PKI dans des environnements publics et privés rend ces dernières particulièrement polyvalentes.

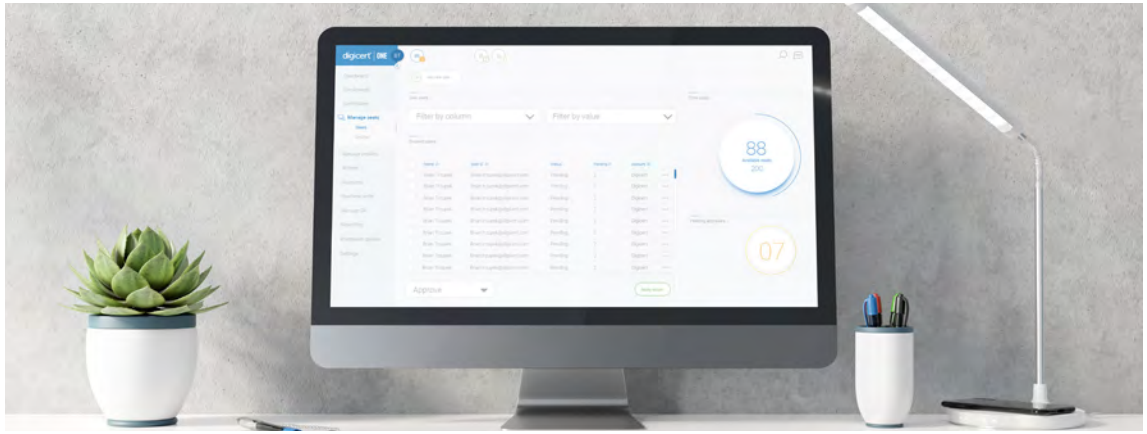
C'est grâce à cette flexibilité qu'une infrastructure PKI parvient à combler le fossé de confiance existant entre environnements publics et privés. Elle est suffisamment puissante et sécurisée pour s'imposer à la fois comme la solution privée de chiffrement et d'identification pour les gouvernements de nombreux pays, et la solution publique pour les appareils IoT grand public.



Une solution simplifiée

Hier, une infrastructure PKI était une véritable usine à gaz. Faute d'accès à des experts, des outils et des plateformes de gestion simplifiés, les informaticiens se risquaient à développer des solutions PKI en interne, sans toutefois maîtriser les connaissances pointues nécessaires à ce type de déploiement. Une fois opérationnelles, la fiabilité des infrastructures PKI en faisait la solution toute indiquée. Mais parvenir à ce stade était un vrai parcours du combattant, apportant souvent plus de problèmes que de solutions.

Heureusement, cette époque est révolue. Aujourd'hui, une infrastructure PKI peut être simple à configurer et à utiliser, à condition bien sûr de procéder dans les règles de l'art. Les outils avancés de déploiement et de surveillance des solutions PKI s'exécutent désormais sur une plateforme avec authentification unique (SSO). Et compte tenu de leur polyvalence, les solutions PKI peuvent résoudre de nombreuses problématiques de sécurité en un seul et même endroit. Au lieu de devoir passer par la création complexe d'une solution PKI unidimensionnelle, vous pouvez désormais déployer et gérer plusieurs solutions de sécurité depuis une console centralisée. Et aucune expertise particulière n'est requise pour gérer votre environnement PKI.



Infrastructures PKI : les quatre grandes idées reçues

L'infrastructure PKI est-elle vraiment toujours utilisée ?

Le PKI retrouve aujourd'hui une nouvelle jeunesse. Non seulement les infrastructures PKI sont toujours utilisées, mais elles ne cessent d'évoluer. Toute leur valeur se situe dans leur flexibilité et dans la confiance dont elles sont su se faire les gardiennes au fil des ans. Ce n'est donc pas par hasard si les ingénieurs y font de plus en plus appel pour leurs besoins de sécurité et d'identification, convaincus qu'ils sont par le long héritage de protection de cette technologie.

Qu'en est-il du problème avec Chrome ? La technologie PKI n'est-elle pas dépassée ?

Les solutions PKI affichent un bilan irréprochable en matière de sécurité. Toutefois, la fiabilité de leur déploiement dépend de l'organisme émetteur du certificat. En 2017, Google a annoncé[7] son intention de signaler comme non fiables une série de certificats émis par Symantec, ces derniers n'étant pas conformes aux exigences de base du CA/Browser Forum.

Il s'agit là d'un exemple regrettable de pratiques latitudinaires dont l'onde de choc a fait vaciller

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

toute l'industrie. Pour éviter une crise mondiale de la sécurité, Symantec et Google se sont mis à la recherche d'une Autorité de certification (AC) capable de fournir le niveau de confiance et l'infrastructure nécessaires à la gestion d'une réémission massive de certificats. Les deux entreprises se sont alors tournées vers DigiCert et ont décidé de transférer les certificats Symantec vers les racines de confiance DigiCert. Les utilisateurs de Chrome n'ont ainsi eu à subir aucune interruption dans l'accès aux sites web sécurisés par PKI.

Aujourd'hui, comme il y a vingt ans, l'infrastructure PKI reste la solution de confiance pour sécuriser les communications web, y compris sur Chrome.

Un grand nombre d'appareils ne sont pas compatibles.

Il serait plus exact de dire qu'une solution PKI fonctionne sur tout appareil suffisamment puissant pour l'exécuter. L'appairage de clés asymétriques nécessite une vitesse de traitement, une quantité de mémoire et un espace disque suffisants. Les solutions PKI sont utilisées depuis plus de vingt ans. Par conséquent, si les processeurs de la fin des années 90 pouvaient gérer le chiffrement par clé, il est logique que tout appareil plus récent puisse exécuter une solution PKI. Toutefois, malgré les progrès en matière de microprocesseurs, certains objets connectés (IoT) sont parfois si rudimentaires qu'ils peuvent être incapables de générer rapidement les clés ou de signer le canal de communication.

Heureusement, les experts PKI ont trouvé la parade à cette contrainte sans toutefois compromettre la sécurité. Le principe consiste à réduire le contenu des certificats PKI, de sorte qu'ils soient suffisamment légers pour être traités par un grand nombre d'appareils à la bande passante et aux capacités de traitement réduites. Par ailleurs, certains éditeurs de logiciels fournissent des systèmes de génération de clés ou de génération de CSR pour les appareils de faible puissance.

À terme, il existera donc de moins en moins d'appareils peu ou pas compatibles PKI. De nouveaux processus de production permettent en effet aux fabricants d'injecter des clés directement dans le silicium de manière à intégrer la sécurité très en amont dans la supply chain. Cette injection résout non seulement les problèmes de compatibilité, mais accélère également la fabrication tout en renforçant la sécurité et l'identification des appareils tout au long de leur cycle de vie.

Je croyais que la technologie PKI se limitait au SSL pour le web ?

Si vous travaillez dans le monde de la sécurité connectée depuis plusieurs années, vous associez probablement le PKI au SSL (Secure Sockets Layer). Le SSL remonte à 1995 avec sa première version fonctionnelle ayant servi de protocole cryptographique pour Netscape. Dès 1999, le SSL a été progressivement remplacé par le TLS (Transport Layer Security) qui, à ce jour, reste le protocole de chiffrement de confiance pour le web.

Le chiffrement TLS/SSL est le domaine d'application le plus connu du PKI. Pourtant, il en existe des dizaines d'autres. En réalité, les solutions PKI sont partout, protégeant à peu près tous les types de connexions qui existent dans le monde. Les solutions PKI sécurisent aujourd'hui des technologies que l'équipe Netscape était loin d'imaginer lorsqu'elle lança le SSL il y a un quart de siècle.

CONFIANCE : LA PREUVE PAR MILLE

Même les ingénieurs et créateurs de solutions PKI sont eux-mêmes souvent surpris par la créativité avec laquelle leur invention est aujourd'hui utilisée. Le PKI parvient donc à s'imposer dans des secteurs et sur des technologies apparemment sans aucun lien, et même parfois là où on ne l'attend pas. Peu importe l'usage qui en est fait, chaque cas reflète un besoin profond et commun, celui d'une confiance sans compromis.

ÉTUDE DE CAS N° 1

AeroMACS

La solution de confiance face à des enjeux vitaux

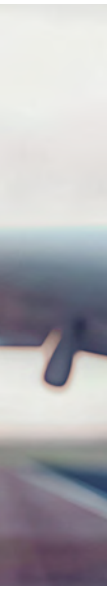
Aujourd'hui, un pilote de ligne a accès à plus de données de capteurs connectés que les astronautes Young et Crippen n'en avaient pour sortir la navette spatiale *Columbia* de l'orbite terrestre lors de sa mission inaugurale en 1981.

Or, tout comme le facteur humain était crucial pour cette prouesse spatiale il y a quarante ans, il reste un enjeu de sécurité majeur à l'heure actuelle. La personne aux commandes d'un avion de ligne doit disposer d'un maximum d'informations précises pour poser cette énorme machine en toute sécurité.

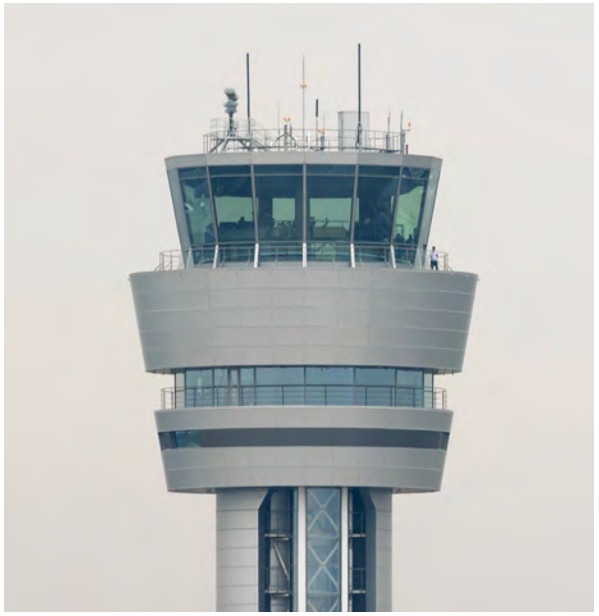
La majorité des accidents aériens se produisent au décollage et à l'atterrissage. C'est à ce moment que l'avion est le plus vulnérable aux forces humaines et naturelles qui influencent l'acte complexe consistant à faire voler 60 tonnes de métal, de carburant, de bagages et de passagers. Une bourrasque de vent, un mauvais timing, une perte de visibilité…

Au moment de décoller et d'atterrir, les pilotes de ligne utilisent des informations essentielles, issues de capteurs et relayées par les écrans du poste de pilotage et les techniciens de la tour de contrôle, pour effectuer les ajustements nécessaires à un vol sans encombre. Depuis 2016, ces informations vitales sont transmises aux tours de contrôle et avions du monde entier via des capteurs IoT placés dans les avions et sécurisés par PKI.

La majorité des accidents aériens se produisent au décollage et à l'atterrissage. C'est à ce moment que l'avion est le plus vulnérable aux forces humaines et naturelles qui influencent l'acte complexe consistant à faire voler 60 tonnes de métal, de carburant, de bagages et de passagers.



DEPUIS 2016, DES INFORMATIONS VITALES SONT TRANSMISES AUX AVIONS ET AUX TOURS DE CONTRÔLE DU MONDE ENTIER VIA DES CAPTEURS IOT PLACÉS DANS LES AVIONS ET SÉCURISÉS PAR PKI.



Faire plus avec moins

Le nombre d'avions en vol devrait doubler d'ici 2025. De plus en plus d'avions, de plus en plus de vols… Entre 2017 et 2018, l'aéroport international de Pékin-Capitale a enregistré une augmentation de 5 % du nombre de passagers. Pour le Dallas Love Field Airport, ce chiffre a même bondi de 90 % entre 2010 et 2020.

AeroMACS EST UNE LIAISON SANS FIL HAUT DÉBIT ET HAUTE CAPACITÉ DESTINÉE À TRANSMETTRE LES DONNÉES DES CAPTEURS IOT DES AÉROPORTS AUX AVIONS ET AUX TOURS DE CONTRÔLE.

Alors que de nouveaux aéroports sortent de terre dans le monde entier, les destinations existantes n'ont d'autre choix que de gagner en efficacité pour gérer l'augmentation du nombre de vols et garantir l'intégrité des atterrissages et des décollages.

Qu'est-ce qu'AeroMACS ?

Le système de communication mobile aéronautique d'aéroport (AeroMACS) est une liaison sans fil haut débit et haute capacité destinée à transmettre les données des capteurs IoT des aéroports aux tours de contrôle et aux avions. Relevés de température, vitesse du vent, systèmes d'affichage des informations de vol, manutention des bagages... tout système rattaché à l'aéroport transmet ses données via AeroMACS.

AeroMACS ne se résume pas à une série de widgets. Il représente les yeux et les oreilles indispensables au sol. Il est le poumon de la coordination des horaires et des plans de vol. Et il est le cœur des opérations aéroportuaires. De fait, toute compromission du système AeroMACS pourrait servir à fournir de fausses informations aux avions et aux pilotes. Compte tenu du nombre de vols et de passagers que cela concerne, on comprend à quel point la protection des informations AeroMACS est essentielle pour garantir un décollage et un atterrissage des avions en toute sécurité.

Ajouter PKI à la checklist d'avant décollage

Une solution de sécurité adaptable et fiable est indispensable dans les secteurs aux écosystèmes complexes, caractérisés par des interconnexions multiples d'appareils variés et parfois limités

en puissance. Hormis tous ces facteurs, les acteurs du transport aérien doivent également tenir compte des enjeux de confidentialité des données. Concrètement, les informations transmises entre le sol et l'avion doivent être sécurisées au même titre que l'appareil lui-même pour éviter toute manipulation frauduleuse aux conséquences catastrophiques.

En misant sur le PKI pour protéger les appareils et les données qu'ils transmettent, les pilotes et les tours de contrôle peuvent collecter, communiquer et exploiter une variété d'informations en toute sécurité pour garantir des décollages et des atterrissages sans encombre, quel que soit l'appareil ou l'aéroport. Autre grand avantage, une solution PKI intégrée à un système AeroMACS sera aussi fiable et opérationnelle dans un petit aérodrome des États-Unis que dans un grand aéroport d'Australie.

Déploiement : planétaire

Les solutions PKI protègent le réseau AeroMACS, une norme de communication aéronautique appelée à se généraliser dans presque tous les aéroports du monde.

Principale mission : la confiance

Avec des milliers d'avions en vol à chaque instant, les aéroports, les compagnies aériennes et les pilotes s'appuient sur AeroMACS pour garantir la sécurité et la ponctualité des vols pour des millions de voyageurs.

ÉTUDE DE CAS N° 2

LE GARDIEN DE L'AUSTRALIE

Protection des citoyens

La majorité des Australiens n'a probablement pas conscience de la solution de sécurité et d'identification qui protège leurs informations et la plupart de leurs transactions les plus importantes. Si vous avez récemment acheté une maison en Australie, vous avez utilisé Gatekeeper. Idem si vous y avez importé des marchandises.

Depuis plus de 30 ans, le Gatekeeper Public Key Infrastructure Framework « régit la manière dont le gouvernement australien utilise les clés et les certificats numériques pour garantir l'identité des abonnés aux services d'authentification. » Contrats, documents juridiques, protection des frontières, opérations bancaires… bon nombre des domaines publics de confiance les plus sensibles sont chiffrés et authentifiés à l'aide de solutions PKI.

La sécurité de toute une nation

À la fin du siècle dernier, le gouvernement australien s'est mis en quête d'un mécanisme capable de protéger de manière fiable les informations d'un nombre croissant de documents et de transactions numériques. Différentes administrations ont d'abord déployé des solutions internes, mais elles se sont très vite rendues compte qu'une gestion intra-muros de la sécurité était à la fois difficile, chronophage et risquée.

La commission-cadre a alors dressé le cahier des charges d'une solution capable de protéger les usagers des services publics de toute une nation, tout en réduisant le temps et les ressources nécessaires à la gestion de l'écosystème. Aujourd'hui, le framework Gatekeeper « assure l'intégrité, l'interopérabilité, l'authenticité et la confiance entre les agences gouvernementales et leurs usagers ».

EN AUSTRALIE, LA CONFIANCE EN LA SÉCURITÉ PKI EST UN ENJEU NATIONAL. PROMESSE TENUE.

Souvent invisible, toujours opérationnel

Souvent, ce sont les technologies que l'on ne voit pas qui ont le plus grand impact sur nos vies. Réseaux électriques, systèmes hydrauliques, réseaux bancaires… nous prenons souvent pour acquis la fiabilité et la disponibilité de ces systèmes dits « d'importance vitale ». Pour les Australiens, Gatekeeper en fait partie. À la fois simple et efficace, Gatekeeper est au cœur de nombreuses fonctions administratives essentielles. Sans Gatekeeper et son infrastructure PKI, les informations personnelles de millions d'Australiens seraient exposées au vol, les transactions importantes et les processus juridiques seraient ralentis ou stoppés, et les agences chargées des douanes et des investissements seraient exposées à toutes sortes de compromissions. En Australie, la confiance en la sécurité PKI est un enjeu national. Promesse tenue.

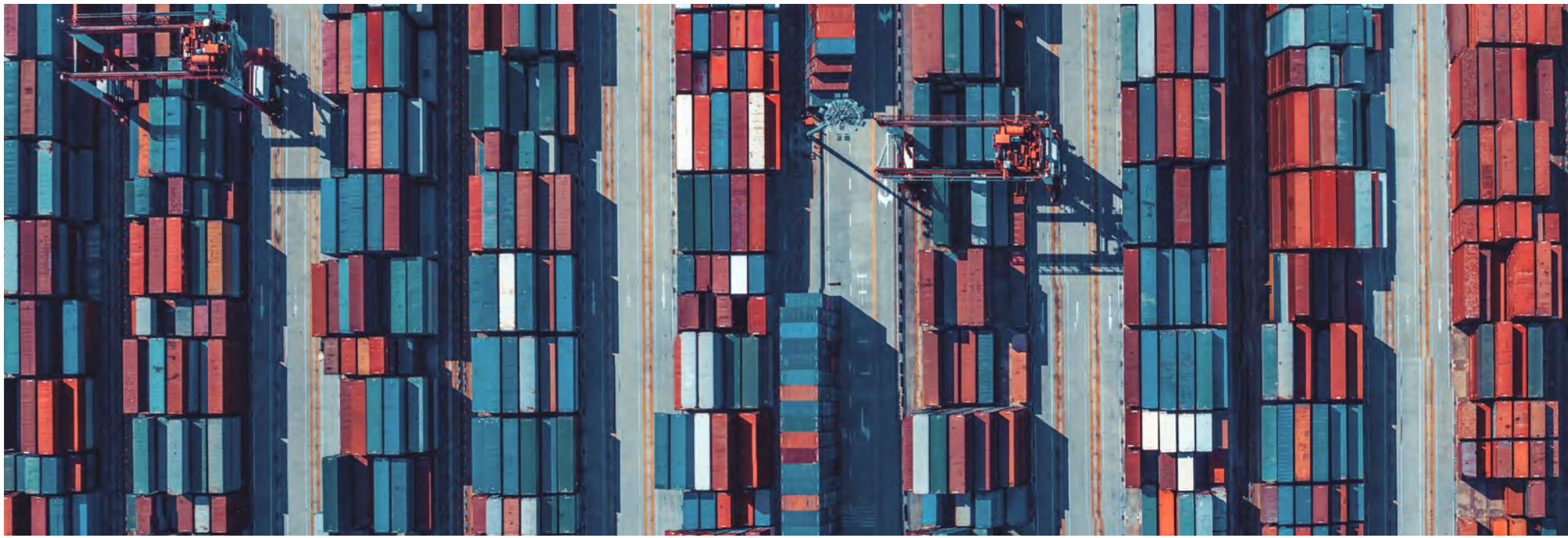
TOUT DOIT ÊTRE OPÉRATIONNEL À TOUT MOMENT.

Déploiement : Australie

Une solution de sécurité et d'identification déployée à l'échelle nationale, exploitée par de nombreuses agences gouvernementales et assurant la protection des domaines publics de confiance parmi les plus sensibles.

Principale mission : l'intégrité

Des opérations bancaires aux acquisitions immobilières, en passant par la sécurité des frontières, il n'y a de place ni pour les défaillances, ni pour les compromis. Tout doit être opérationnel à tout moment.



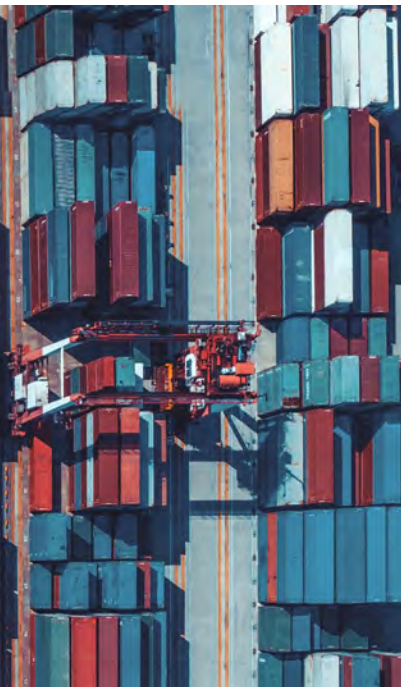
ÉTUDE DE CAS N° 3

TRANSPORT MONDIAL

Une confiance à l'échelle mondiale

Imaginez devoir localiser un conteneur parmi des millions, alors qu'il se déplace d'un port à un autre, d'un continent à un autre et d'un océan à un autre. Pour y parvenir, vous devrez accéder à d'énormes bases de données et consulter les systèmes de suivi du fret.

La supply chain mondiale est un peu comme une grande horloge. Pour que le mécanisme tourne, chaque pignon, ressort et rouage doit être à sa place et remplir son rôle comme prévu. Un simple retard d'expédition, et c'est l'ensemble de la chaîne qui se grippe. Les pertes financières se chiffrent alors tant en termes matériels qu'en de chiffre d'affaires.



Plus de 11 milliards de tonnes de marchandises transitent par voie maritime chaque année, et on compte aujourd'hui plus de 50 000 porte-conteneurs dans le monde.

Traçabilité numérique

Plus de 11 milliards de tonnes de marchandises transitent par voie maritime chaque année, et on compte aujourd'hui plus de 50 000 porte-conteneurs dans le monde. Le commerce maritime est à la fois gigantesque et en perpétuel mouvement. Les cargos qui sillonnent le globe forment des constellations qui ne sont pas sans rappeler un ciel étoilé.

Pour chaque cargo sur les flots, il faut compter des centaines de conteneurs. Autant dire que la localisation et le suivi en temps réel et sécurisé de chacun d'entre eux est un véritable travail de fourmi.

La grande difficulté avec des expéditions à cette échelle réside dans l'authentification des balises embarquées faisant remonter des informations vers le cloud, là où s'effectue le tracking. En cas de compromission, la compagnie maritime peut perdre toute visibilité sur ses conteneurs, ou encore recevoir de fausses informations sur leur positionnement. Une solution de sécurité efficace doit non seulement protéger les balises, mais également les informations transmises. Elle se doit également d'être évolutive et capable de sécuriser simultanément des dizaines de milliers d'appareils en toute fiabilité.

Tous les couloirs maritimes de la planète

L'authentification PKI permet de suivre des conteneurs en toute sécurité tout au long de leur trajet, du chargement jusqu'au port de destination. Et compte tenu de l'augmentation du trafic, des cargaisons et des équipements connectés à bord, le besoin d'une sécurité renforcée augmente également chaque année. Le PKI est suffisamment évolutif pour répondre à cette demande.

Ainsi, quel que soit le nombre d'expéditions, les données sont sécurisées et les conteneurs suivis, où qu'ils se trouvent sur la planète. Le PKI réduit les risques de vol ou de perte et contribue à assurer l'efficacité du mouvement des marchandises d'un port à l'autre. La supply chain reste fluide et les produits peuvent être fabriqués à moindre coût. Entreprises et consommateurs : tout le monde est gagnant.

Déploiement : planétaire

Au cœur de la supply chain mondiale, les conteneurs maritimes connectés acheminent des marchandises et des matériaux vers tous les continents.

Principale mission : l'authentification

Plus qu'un simple outil de suivi, les solutions PKI fournissent une authentification sécurisée en temps réel pour permettre aux entreprises de localiser et d'identifier les balises rattachées à chaque conteneur.

LES SOLUTIONS PKI PERMETTENT UN SUIVI SÉCURISÉ DES CONTENEURS TOUT AU LONG DE LEUR TRAJET.

IBM

Le choix de confiance des leaders de la tech

Les plus grandes entreprises sont souvent celles qui font face aux plus grands défis. En fait, le défi vient parfois de la taille même de l'entreprise. Rôles des utilisateurs ; multiplicité des sites et implantations à l'échelle mondiale ; diversité des appareils, systèmes d'exploitation et applications... tant de variables entrent dans l'équation de la sécurité qu'elle peut paraître insoluble.

Pour IBM, ce n'était pas seulement une extraordinaire gymnastique intellectuelle. C'était aussi un vrai problème. Un problème qui touchait un demi-million de collaborateurs.

BYOx (Bring Your Own Anything)

Comment authentifier, identifier et protéger plus de 500 000 utilisateurs ?

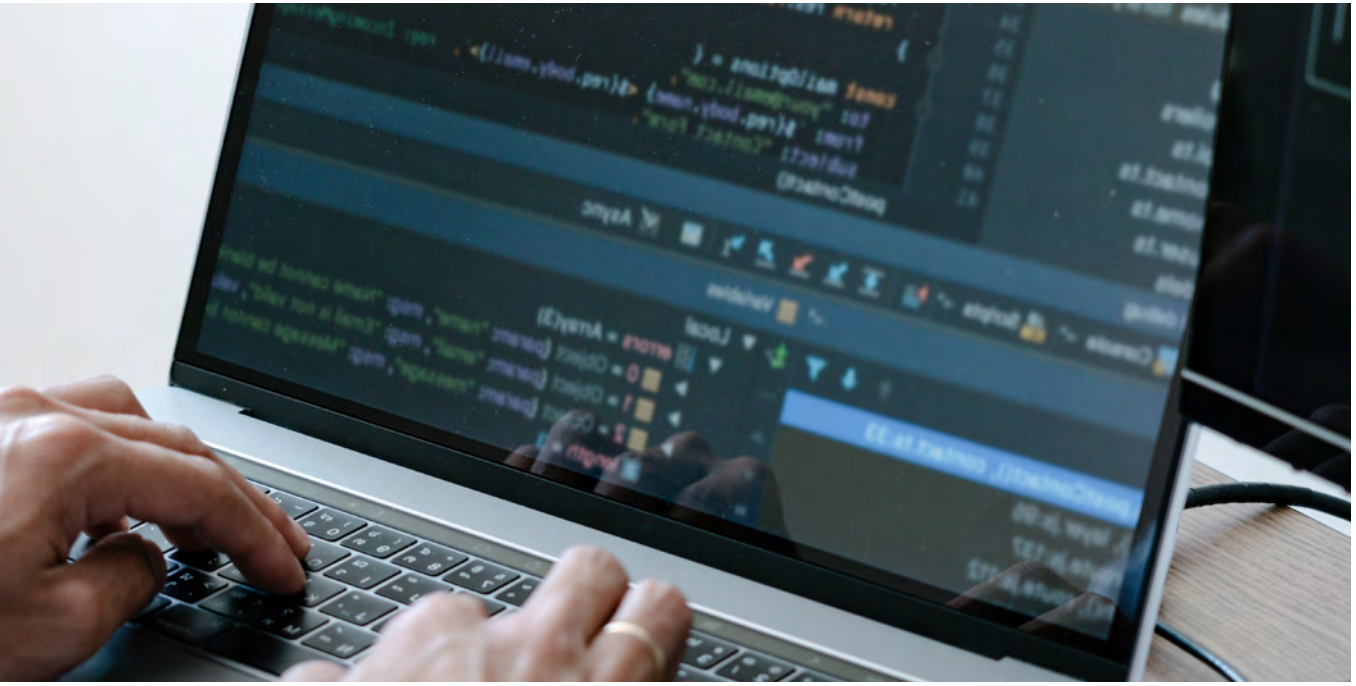
Dans le cas d'IBM, les mots « flexible » et « évolutif » ne devaient pas se limiter à de simples avantages théoriques, ils devaient se refléter très concrètement dans la solution PKI déployée. Si le nombre d'utilisateurs constitue un défi, la quantité et la variété d'appareils et d'applications utilisés sur leur lieu de travail l'est au moins tout autant. Ordinateur portable fourni par l'entreprise, smartphone personnel, iPad d'ancienne génération… Pour offrir à vos collaborateurs, fournisseurs et sous-traitants la flexibilité de travailler sur l'appareil de leur choix, sans introduire de vulnérabilités dans votre réseau, il vous faut une solution de sécurité robuste et adaptative.

Le PKI, c'est de la flexibilité, mais c'est aussi une extrême évolutivité. Autrement dit, une infrastructure PKI peut non seulement authentifier un nombre indéfini d'appareils, indépendamment de leurs propriétaires et de leur logiciels, mais elle peut également authentifier simultanément les appareils de centaines de milliers d'utilisateurs, où qu'ils se trouvent. Pour les (500 000) utilisateurs, tout s'effectue de manière totalement transparente.

Qui dit confiance, dit fiabilité

Depuis plus d'une décennie, les solutions d'identification PKI ont permis à une seule et même entreprise d'assurer la disponibilité non-stop de ses services dans plus de 170 pays.

LE PKI, C'EST DE LA FLEXIBILITÉ, MAIS C'EST AUSSI UNE EXTRÊME ÉVOLUTIVITÉ.



Pour que la sécurité inspire confiance, elle doit d'abord se montrer fiable. À cette échelle, l'authentification SaaS (Software-as-a-Service) doit donc être suffisamment robuste pour fonctionner en tout lieu et à tout moment. Partout dans le monde, des centaines de milliers d'utilisateurs bénéficient d'un accès sécurisé au réseau IBM, 24h/24 et 7j/7, quel que soit leur appareil. Le système est si sûr que l'entreprise n'a pas à se soucier d'une éventuelle vulnérabilité, et si transparent que les utilisateurs ne le remarquent même pas.

Déploiement : planétaire

Le leader historique des équipements et logiciels informatiques pilote ses opérations depuis des milliers de bureaux dans le monde

Principale mission : la flexibilité

Dans un contexte opérationnel critique, l'infrastructure PKI permet d'authentifier, de sécuriser et d'identifier un demi-million d'utilisateurs répartis dans le monde entier.

ÉTUDE DE CAS N° 5

SANTÉ

Une solution de confiance lorsque des vies sont en jeu

Pour la plupart d'entre nous, un objet connecté n'est qu'un simple bonus : une connexion Bluetooth qui nous permet de vérifier la température et l'humidité d'une terrasse, une connexion Wi-Fi entre un iPad dans la cuisine et une smart TV dans le salon pour reprendre un épisode là où nous l'avions laissé au moment de servir le dîner… La plupart du temps, être connecté est plus un désir qu'un besoin. Mais pour certaines personnes, être connecté n'est pas qu'un avantage pratique. C'est une question de vie ou de mort.

Il y a quelques années, de nouveaux pacemakers dit « intelligents » sont apparus sur le marché. Connecté via Bluetooth à un moniteur externe et à une application installée sur le smartphone du patient, ce pacemaker peut non seulement fournir les signaux électriques nécessaires au maintien de la fréquence cardiaque du porteur, mais également expliquer son mode de fonctionnement au patient et au médecin. Le pacemaker fonctionne-t-il comme prévu ? Quelle est la durée de vie de la batterie ?

Pour obtenir ce genre de données, le patient devait autrefois se rendre à l'hôpital, voire subir une intervention chirurgicale pour détecter ou corriger les anomalies. Désormais, il est possible de surveiller, d'enregistrer et de communiquer toutes ces données automatiquement et en continu.

Les pacemakers connectés ne sont pas une simple commodité. Sans eux des milliers de personnes ne seraient pas actuellement en vie. Mais comme dans toute connexion, il existe des risques d'interférence. À l'image de n'importe quel appareil IoT, un pacemaker connecté exige un chiffrement sécurisé de bout en bout.

Une question vitale au sens propre

En août 2017, un titre inhabituel[8] fait la une des journaux – inhabituel, du moins, pour toute personne peu versée dans les subtilités de l'IoT. L'agence américaine des produits alimentaires et médicamenteux (Food and Drug Administration, FDA) rappelait un certain nombre de pacemakers en raison d'une menace de cybersécurité. Dans ce qui ressemblait à un récit de plus sur les risques de compromission sur Internet, la FDA avertissait que certains pacemakers pouvaient « être vulnérables aux intrusions et aux exploits de cybersécurité ».

UN HACKER POUVAIT-IL VRAIMENT S'INTRODUIRE DANS LE PACEMAKER D'UN PATIENT ET PERTURBER SON FONCTIONNEMENT, VOIRE L'ARRÊTER COMPLÈTEMENT ? RÉPONSE : OUI.

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

Une idée plutôt étrange qui s'apparentait plus au scénario d'un film de science-fiction qu'à un danger réel. Un hacker pouvait-il vraiment s'introduire dans le pacemaker d'un patient et perturber son fonctionnement, voire l'arrêter complètement ? Réponse : oui.

L'invention de nouveaux appareils médicaux interconnectés (lits intelligents, glucomètres, etc.) a certes eu des retombées extraordinaires en termes de qualité des soins aux patients. Seule ombre au tableau, les inquiétudes se multipliaient concernant la protection des données des patients et les possibles compromissions de ces appareils.

Et pour cause : des hackers avaient trouvé un moyen d'accéder aux pacemakers. Certes, les communications entre le pacemaker et le moniteur étaient chiffrées, mais le moniteur lui-même n'était pas sécurisé. Ayant réussi à accéder au moniteur, ces criminels étaient capables d'envoyer des commandes répétées au pacemaker, réduisant ainsi la durée de vie de la batterie. Pire, ils étaient parvenus à transmettre une commande demandant au pacemaker d'envoyer une décharge électrique au patient. Pour protéger aussi bien les appareils que les patients, de nombreux fabricants se sont tournés vers les solutions PKI.

Dans le domaine médical, l'avantage du PKI ne tient pas seulement à sa longue histoire dans le chiffrement fort, mais aussi à son processus d'identification intégré.

UNE SOLUTION DE SÉCURITÉ GARANTE DE L'INTÉGRITÉ DE L'APPAREIL ET DES DONNÉES DU PATIENT, ET SUFFISAMMENT FIABLE POUR ÊTRE DÉPLOYÉE LORSQUE DES VIES SONT EN JEU.

Les appareils médicaux deviendront plus compacts et plus intelligents, tandis que l'infrastructure PKI continuera d'agir inlassablement en coulisses pour protéger les données des patients – un enjeu vital au propre comme au figuré.

Concrètement, une solution PKI facilite la sécurisation des données des appareils tout en authentifiant ces derniers par le biais d'un identifiant chiffré. Cela signifie qu'un appareil peut être sécurisé pendant sa fabrication, sécurité dont bénéficient ensuite l'hôpital et le patient en bout de chaîne. L'usage de l'appareil évolue au cours de son cycle de vie ? Les personnels en charge de la sécurité changent ? Aucun souci, la protection reste la même à tout moment.

Vers des appareils médicaux encore plus intelligents

Des projets de R&D d'appareils encore plus miniaturisés et plus sophistiqués ont récemment obtenus de nouveaux financements et ont reçu l'aval de diverses agences de santé. Les pacemakers sans fil sont aujourd'hui utilisés à travers le monde. Suffisamment petits pour être insérés via un cathéter fémoral et implantés directement dans le cœur, ils éliminent le besoin de recourir à une chirurgie plus invasive ou à des fils électriques susceptibles de s'user à mesure que le tissu cardiaque se contracte au fil de millions ou de milliards de pulsations.

Les pacemakers de nouvelle génération seront sans fils et plus intelligents. Connectés à de petits défibrillateurs, ils surveilleront non seulement le niveau d'intégrité de l'appareil, mais également la santé du cœur du patient. Via une connexion Bluetooth, ils pourront ainsi ordonner au défibrillateur d'envoyer une décharge en cas de défaillance cardiaque du porteur. Ils transmettront les données au cardiologue et seront capables d'effectuer des ajustements en temps réel, sans intervention chirurgicale, pour renforcer automatiquement la santé cardiaque du patient sans que celui-ci ne se rende compte de quoi que ce soit.

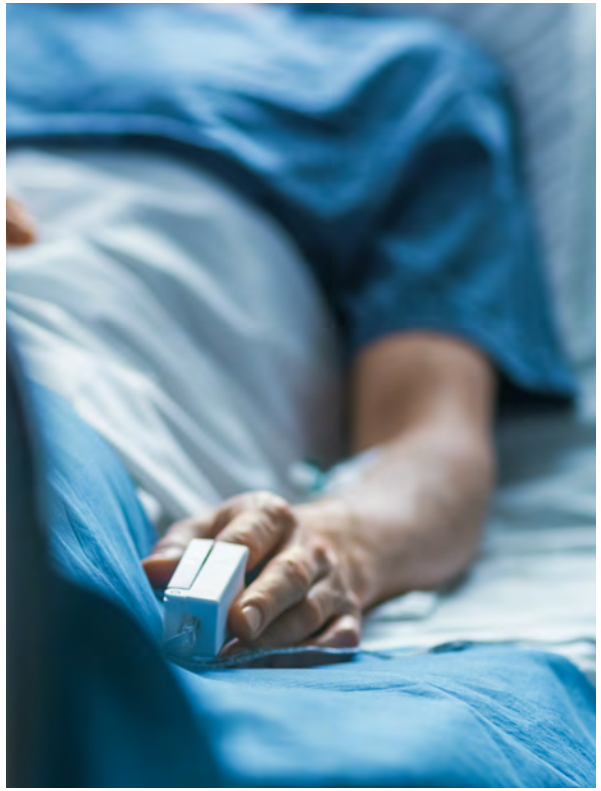
Aujourd'hui, des milliers de personnes vivent l'esprit tranquille, sachant qu'un système de surveillance simple et sécurisé veille au grain pour assurer le bon fonctionnement de leur pacemaker et les alerter en cas de problème. À court terme, les technologies cardiovasculaires sont appelées à faire de nouveaux progrès considérables, offrant des données de meilleure qualité à plus de patients (et leurs médecins) et une assistance immédiate sans opération ni consultation. Les appareils médicaux deviendront plus compacts et plus intelligents, tandis que l'infrastructure PKI continuera d'agir inlassablement en coulisses pour protéger les données des patients – un enjeu vital au propre comme au figuré.

Déploiement : international

Des millions de personnes et des milliers d'hôpitaux et d'établissements de santé soumis à des normes et protocoles d'implémentation très variés.

Principale mission : la fiabilité

Une solution de sécurité garante de l'intégrité de l'appareil et des données du patient, et suffisamment fiable pour être déployée lorsque des vies sont en jeu.



CHAPITRE 3

MÉCONNAÎTRE LE DANGER, C'EST S'Y EXPOSER

Depuis des décennies, les infrastructures PKI ont su se montrer dignes de la confiance placée en elles. Mais cette confiance est avant tout une question d'expertise. Après tout, les vulnérabilités d'une solution PKI mal déployée peuvent présenter un risque aussi important qu'un système non sécurisé.

Les infrastructures PKI existent depuis si longtemps que les ingénieurs et les informaticiens ont largement eu le temps d'étudier leur fonctionnement en situation réelle. Si certains projets de déploiement intelligents et innovants ont connu un réel succès, certaines autres tentatives ont également échoué en raison d'erreurs de conception ou d'une mauvaise gestion ayant conduit à des défaillances dans ce qui est autrement un système presque parfait.

Chaque déploiement de solution PKI offre l'opportunité d'en étudier le fonctionnement, en particulier lorsque ce déploiement s'effectue dans un nouvel environnement ou est lié à une nouvelle technologie. Et chaque fois que les choses se passent bien, les ingénieurs PKI en tirent des leçons précieuses sur la manière la plus efficace et la plus sûre d'utiliser la technologie.

Ce que les experts peuvent nous apprendre

Protection adéquate des clés

L'efficacité d'une solution PKI ne vaut que par la clé privée utilisée pour signer la chaîne de certificats. Il existe en général une clé pour l'Autorité de certification (AC) racine et une pour l'Autorité de certification émettrice. Une création ou un stockage non sécurisé de l'une des clés, ou des deux, affecte donc la fiabilité des certificats PKI émis. C'est le cas parfois en entreprise, par exemple lorsqu'un informaticien crée des clés en texte clair sur un serveur qu'il gère à l'aide d'un logiciel téléchargé depuis Internet, puis transfère ces clés à l'AC pour en faire une sauvegarde sur le réseau. Dans ce cas de figure, le système PKI est extrêmement vulnérable, car les clés – qui n'ont jamais été protégées – peuvent être facilement volées. Seule une protection adéquate garantit la fiabilité de toute la hiérarchie PKI.

Statut des certificats

Un système PKI doit permettre à un appareil ou un navigateur de déterminer si un certificat donné est toujours valide et utilisable. Or, lorsque ce système n'est pas correctement déployé, les informations nécessaires à la révocation sont souvent absentes de la hiérarchie, voire totalement inexistantes. Dans certains cas, le système ne gère pas correctement les demandes alors que les informations sont pourtant présentes et exactes. Quoi qu'il en soit et quelle qu'en soit la cause, le résultat est le même : le système n'est pas fiable.

Mauvaise configuration

Hormis la bonne configuration des systèmes, les certificats ou les chaînes de certificats nécessitent souvent des configurations spécifiques des systèmes PKI pour protéger les logiciels et le matériel. Dans le cas de déploiements « maison », il est fréquent de tomber sur des solutions qui permettent de résoudre un problème donné, mais exposent le certificat à des risques de contournement, d'usurpation d'identité ou d'utilisation abusive.

DEPUIS DES DÉCENNIES, LES INFRASTRUCTURES PKI ONT SU SE MONTRER DIGNES DE LA CONFIANCE PLACÉE EN ELLES. MAIS CETTE CONFIANCE EST AVANT TOUT UNE QUESTION D'EXPERTISE.

Chiffrement PKI : quatre erreurs de configuration à éviter

Ne pas planifier les futures itérations

Lorsqu'un responsable de la sécurité met en place des solutions PKI développées en interne, il ne tient souvent pas compte des changements qui se produisent au fil du temps. Une solution PKI incapable de s'adapter à l'évolution des organisations (structure, objectifs, produits, équipes, etc.) ou de prendre en charge de nouveaux déploiements, devient rapidement obsolète. Pire, elle constitue en soi une menace à part entière.

Tenter de gérer un écosystème PKI en interne

La simplicité des infrastructures PKI peut être trompeuse. Un système PKI est flexible, évolutif, rapide et fiable, mais si et seulement s'il est correctement intégré et déployé. Or, les solutions développées en interne finissent souvent par se transformer en véritables usines à gaz. Sans une installation réalisée par des experts et une gestion opérationnelle efficace, il devient difficile d'assurer le suivi des systèmes PKI, de mesurer leur niveau d'intégrité et de détecter 'les éventuelles défaillances ou lacunes qu'ils présentent. Une infrastructure PKI managée (externalisée) et des plateformes centralisées permettent de résoudre ces problèmes. Elles éliminent le besoin d'un suivi permanent et dissipent toute inquiétude relative aux violations de sécurité, aux clés errantes ou aux erreurs des utilisateurs.

Développer un écosystème PKI sans tenir compte de la conformité

L'un des grands avantages des systèmes PKI réside dans la flexibilité des options de déploiement. Il existe plusieurs modèles allant des environnements sur site aux déploiements 100 % cloud. Non seulement il est essentiel de déterminer l'option la mieux adaptée à tous les besoins (métiers, utilisateurs, sécurité; etc.), mais aussi de savoir quelle option garantit une sécurité conforme aux réglementations locales, nationales ou transnationales en vigueur. Il est également important de comprendre comment la solution PKI s'intègre dans la stratégie de sécurité globale d'une organisation et d'un secteur.

Ne pas se préparer à la révolution PQC

L'informatique post-quantique (PQC) est en train de passer de la science-fiction à la réalité. Mais malgré ses avantages, l'informatique quantique apporte avec elle son lot de dangers. Certes, la capacité réelle des ordinateurs quantiques à casser des codes mathématiquement réputés inviolables reste encore inconnue. Néanmoins, certains professionnels de la sécurité commettent l'erreur d'attendre l'arrivée de l'informatique quantique pour préparer leur environnement aux menaces potentielles. Or, il existe déjà des solutions posant les bases de la sécurité des systèmes dans le monde de la cryptographie post-quantique. Et les experts en sécurité insistent sur l'importance d'étudier la question et de tester d'ores et déjà les systèmes appelés à protéger nos ressources dans cette nouvelle ère.

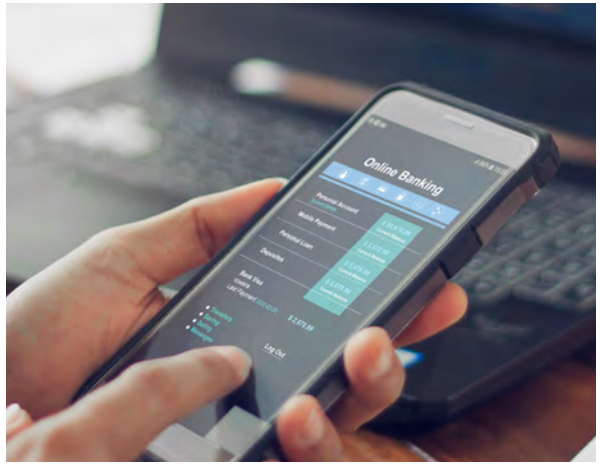
PKI : UNE MISE AU POINT S'IMPOSE.

Comment une technologie réputée fiable depuis des décennies peut-elle se réinventer ? La réponse ne réside pas tant dans le changement de la technologie elle-même que par une grande inventivité dans la manière d'utiliser cette technologie.

Qu'on se le dise, le PKI est et reste sûr. Il n'a cessé de prouver sa fiabilité en matière de sécurité et d'identification depuis l'époque de Netscape et des modems à 33,6 kbit/s. Hormis quelques mises à jour de protocoles et modifications mineures – pour rester en phase avec certaines évolutions dans l'informatique –, la technologie PKI d'aujourd'hui n'est pas foncièrement différente de celle d'hier.

En 1996, les pionniers de son implémentation voulaient protéger les résultats de recherche sur Excite et effectuer des achats en toute sécurité sur eBay. D'une certaine manière, un grand nombre de personnes l'abordent encore dans ce sens aujourd'hui. Cependant, beaucoup ne réalisent pas que les infrastructures PKI modernes permettent également d'éviter des accidents de trains et de protéger les personnes contre le vol de leurs données personnelles stockées sur leur smartwatch. Et oui, le PKI continue aussi de chiffrer les transactions sur eBay.

L'infrastructure PKI a su évoluer au rythme des technologies et des besoins de sécurité partout dans le monde – à la maison comme dans les infrastructures étatiques les plus critiques, en passant par tous les secteurs d'activité possibles et imaginables. En fin de compte, le rôle des solutions PKI sur les balises de secours d'urgence n'est peut-être pas moins important que le fait que chaque jour, elles veillent à ce que des millions de personnes puissent effectuer des transactions bancaires en ligne sans qu'aucun numéro de carte ne tombe entre de mauvaises mains. Dans un cas comme dans l'autre, l'importance de cette confiance ne peut être sous-estimée. Une infrastructure PKI est l'alliance parfaite entre une technologie éprouvée et une solution de sécurité et d'identification de ce que nous inventons aujourd'hui et imaginerons pour demain. Peu importe ce que le futur nous réserve, la technologie PKI continuera de s'imposer comme le choix de la confiance, de la flexibilité et de la fiabilité.



L'INFRASTRUCTURE PKI A SU ÉVOLUER AU RYTHME DES TECHNOLOGIES ET DES BESOINS DE SÉCURITÉ PARTOUT DANS LE MONDE.

Vous avez connaissance de cas d'usage innovants de l'infrastructure PKI ? Nous aimerions les mettre en valeur. Vous souhaitez en savoir plus sur les solutions DigiCert PKI ? Nous sommes à votre disposition.
PKI_Info@digicert.com

À propos de DigiCert

Chez DigiCert, nous œuvrons sans relâche pour incarner un objectif commun : a better way.

Plus qu'un simple slogan, cette quête perpétuelle d'un meilleur moyen de sécuriser Internet est profondément ancrée dans notre ADN. C'est pourquoi nos certificats TLS/SSL ont su gagner la confiance de 89 % des entreprises du Fortune 500, 97 des 100 plus grandes banques mondiales et 81 % des sites d'e-commerce dans le monde entier. C'est aussi pour cela que notre support et nos services atteignent les taux de satisfaction client les plus élevés du marché. Et c'est enfin pourquoi nous révolutionnons une nouvelle fois l'univers du PKI avec la plateforme DigiCert ONE et des outils de gestion conçus pour aider les entreprises et collectivités à protéger les identités, accès, serveurs, réseaux, e-mails, codes, signatures, documents et appareils IoT. En somme, DigiCert s'impose comme le dénominateur hors du commun dans les technologies SSL, IoT, PKI et tout ce que l'avenir nous réserve.