



Contact médias :

Ken Kadet, VP, Public Relations
952-937-1154 | ken.kadet@entrust.com

La transformation digitale et l'évolution de l'organisation du travail stimulent la demande d'infrastructures à clés publiques (PKI) et de certificats numériques, selon l'édition 2021 de l'étude mondiale sur les tendances des PKI et de l'IoT signée Entrust

Le manque de pilotage et le déficit de ressources et de qualifications continuent à mettre les déploiements PKI à rude épreuve.

MINNEAPOLIS (États-Unis), le 10 novembre 2021 – Sous l'effet des changements organisationnels, l'infrastructure à clés publiques (PKI) et les certificats numériques n'ont jamais eu autant le vent en poupe en entreprise, alors que jamais encore n'avait été observée une telle pénurie de qualifications en gestion de PKI, fait valoir une étude du Ponemon Institute, parrainée par [Entrust](#), leader dans la fourniture de solutions fiabilisant les identités, les paiements et la protection des données. L'édition [2021 de son étude mondiale sur les tendances des PKI et de l'IoT](#) révèle également que les professionnels de l'IT continuent à voir un manque de clarté dans le pilotage ainsi que dans le déficit de ressources et de qualifications. Les principales difficultés restent inhérentes au déploiement et à la gestion de l'infrastructure à clés publiques.

Au cœur de la quasi-totalité des infrastructures IT, le modèle PKI sécurise les initiatives digitales stratégiques, telles que le cloud, le déploiement d'appareils mobiles, les identités et l'Internet des objets (IoT). À ce titre, l'infrastructure PKI joue un rôle déterminant dans l'accélération de la transformation digitale que ces technologies accompagnent, phénomène mis en lumière avec la pandémie mondiale et ses répercussions sur les méthodes de travail.

Facteurs accélérant ou contrariant l'adoption de la PKI

S'agissant des principales tendances accélérant le déploiement d'applications via la PKI, l'Internet des objets (IoT) demeure, à 47 %, celle enregistrant la plus forte croissance, suivie par les services dans le cloud, cités par 44 % des professionnels interrogés, et les mobiles grand public, qui occupent la troisième place du classement à 40 %.

Le principal obstacle entravant le déploiement et la gestion de la PKI est le manque de clarté dans le pilotage – cité par 71 % des professionnels interrogés. Le fait que ces derniers soulèvent cette difficulté majeure depuis cinq ans prouve qu'il s'agit là d'un réel domaine de préoccupation pour nombre d'entreprises.

Les déficits de ressources et de qualifications se classent en deuxième et troisième positions à 51 % et 46 %. De même, la non prise en charge des nouvelles applications par les PKI en place (55 %) et les difficultés de recrutement (46 %) constituent les principaux obstacles à l'utilisation d'une PKI.

Les domaines qui devraient être les plus exposés aux changements et aux incertitudes sont les nouvelles applications, comme l'Internet des objets (IoT) – dans la ligne de mire de 41 % des professionnels interrogés. Les deuxième et troisième domaines les plus cités sont les obligations extérieures et normes (37 %) et les évolutions dans les technologies PKI (27 %).

« Pendant les années durant lesquelles cette étude a été réalisée, l'écart entre la faveur croissante dont jouit l'adoption d'infrastructures à clés publiques et les obstacles freinant cette dernière s'est manifestement creusé », précise Larry Ponemon, président-fondateur du Ponemon Institute. *« D'où le double risque d'aggraver le casse-tête auquel se heurtent d'ores et déjà les entreprises et de susciter des failles dans leurs démarches de sécurité. Sachant que le télétravail, le cloud et l'IoT ne font qu'accentuer davantage la distribution des environnements, il est évident qu'il existe un besoin immédiat, dans nombre d'entreprises, de bénéficier de davantage de visibilité, d'automatisation et de contrôle centralisé. »*

Montée en puissance des identités machines

S'agissant des identifiants d'authentification PKI, les certificats TLS/SSL pour les sites web et services orientés grand public constituent le scénario d'utilisation le plus souvent cité (81 % des professionnels interrogés). Viennent ensuite, en deuxième position, les réseaux privés et applications VPN (67 %, contre 60 % en 2020) et, en troisième position, la sécurité des e-mails (55 %, contre 51 % en 2020), supplantant respectivement à ces mêmes places les applications cloud public et l'authentification des utilisateurs en entreprise. Cette évolution met en évidence le recentrage de priorités qui s'est opéré au profit de la sécurisation des collaborateurs en télétravail et des charges de travail distribuées.

L'étude révèle également que le nombre moyen de certificats émis ou acquis par les entreprises poursuit sa progression, passant de 56 192 en 2020 à 58 639 cette année, soit une hausse de 4,3 % sur un an (et de 50 % depuis 2019). Si le nombre d'identités humaines sécurisées demeure relativement uniforme ces dernières années, il existe aujourd'hui davantage d'identités machines (appareils et workflows) que d'identités humaines. Cette progression des identités machines est essentiellement constituée du recours croissant à l'IoT, aux services cloud et aux nouvelles applications.

Quel que soit le motif de cette progression, plus le nombre de certificats à gérer par une entreprise est élevé, plus leur gestion correcte s'avère essentielle. Alors qu'un professionnel interrogé sur cinq (20 %) précise utiliser une liste manuelle de révocation de certificats et qu'ils sont près d'un tiers (32 %) à admettre ne faire appel à aucune technique de ce type, ces entreprises risquent d'être vulnérables aux attaques. Elles s'exposent ainsi à des pannes de leurs systèmes stratégiques ainsi qu'aux interruptions d'activité et aux coûts qui en découlent.

« LaPKI n'a jamais été autant convoitée – que ce soit en raison des contraintes exercées depuis un an pour sécuriser une organisation en télétravail ou au format hybride ou de la croissance continue de l'IoT et des services dans le cloud », affirme John Metzger, vice-président du marketing produits et de la sécurité digitale chez Entrust. « Dans le même temps, les qualifications et les ressources indispensables au déploiement et à la gestion d'une infrastructure PKI continuent à manquer – et ce problème est aggravé par l'absence de pilotage organisationnel clair sur les déploiements PKI. Pour faire face à cette complexité, les entreprises ont d'abord besoin d'une stratégie, puis de produits à l'appui de cette transformation. Concrètement, il leur faut un partenaire comme Entrust qui possède les capacités technologiques mais aussi les acquis et l'expertise pour accompagner leur réussite dans cet environnement. »

Informations complémentaires

Page de destination : [Édition 2021 de l'étude mondiale sur les tendances de l'infrastructure PKI et de l'IoT](#)

Blogue : [Votre infrastructure PKI est-elle prête à exploiter le potentiel d'un univers connecté ?](#)

Méthodologie utilisée pour l'édition 2021 de l'étude mondiale sur les tendances de l'infrastructure PKI et de l'IoT

L'édition 2021 de l'étude mondiale annuelle sur les tendances de l'infrastructure PKI et de l'IoT, réalisée par le Ponemon Institute pour le compte d'Entrust, s'appuie sur les données recueillies auprès de plus de 2 500 professionnels de la sécurité IT dans 17 pays/régions : Allemagne, Asie du Sud-Est, Australie, Brésil, Corée du Sud, Espagne, États-Unis, Fédération de Russie, France, Hong Kong, Japon, Mexique, Moyen-Orient (professionnels basés en Arabie saoudite et aux Émirats arabes unis), Pays-Bas, Royaume-Uni, Suède et Taïwan.

À propos d'Entrust Corporation

Entrust sécurise un monde en mouvement en fiabilisant les identités, les paiements et la protection des données. Aujourd'hui plus que jamais, chacun entend vivre des expériences fluides et sécurisées, qu'il s'agisse d'effectuer des achats, de traverser des frontières, d'accéder à des services d'administration en ligne ou de se connecter à un réseau d'entreprise. Entrust propose une gamme inégalée de solutions de sécurité numérique et d'émission de titres sécurisés qui s'inscrivent au cœur même de toutes ces interactions. Avec nos plus de 2500 collaborateurs, notre réseau mondial de partenaires et des clients dans plus de 150 pays, il n'est guère étonnant que les organisations les plus dignes de confiance dans le monde nous accordent la leur. Pour de plus amples informations, consultez le site www.entrust.com.

###