



Rapport de recherche mondial sur les infrastructures à clés publiques (PKI) 2026

La PKI sous pression: le point de bascule pour la modernisation

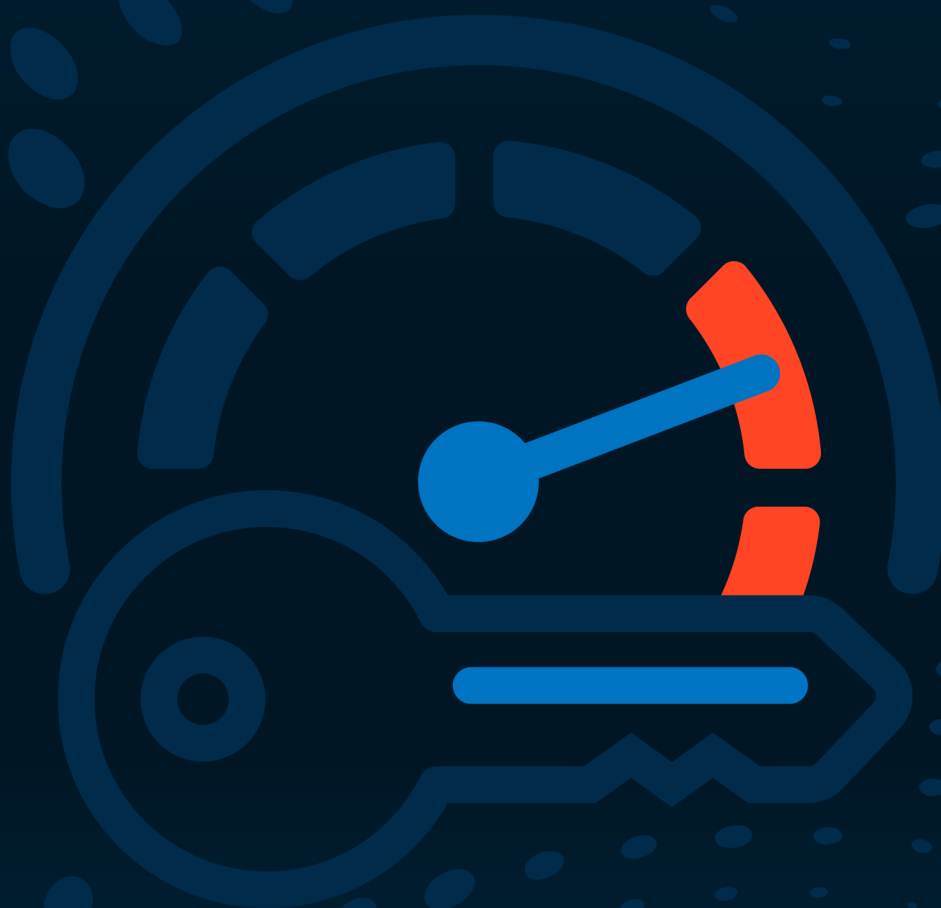


Table des matières

Préface de Lakshmi Hanspal, responsable de la confiance chez DigiCert	3
Résumé exécutif	4
Le défi: une PKI sous pression	5
Visibilité et risque	7
Complexité et maturité	9
IA et quantique	14
La solution: moderniser l'PKI	16
Méthodologie	17
Auteurs et contributeurs	18

Avant-propos



Lakshmi Hanspal

Responsable de la confiance,
DigiCert

La modernisation des PKI et la préparation à l'ère post-quantique ne sont plus des problématiques futuristes. Elles font désormais partie des réalités opérationnelles d'aujourd'hui.

Les responsables de la sécurité et des infrastructures doivent faire face à la convergence de plusieurs tendances majeures. Les organisations gèrent toujours plus d'identités machines, davantage de systèmes connectés, font face à une incertitude croissante liée à l'IA, et doivent s'accommoder de délais de plus en plus courts pour agir avant que les vulnérabilités cryptographiques ne deviennent de véritables risques pour l'entreprise.

Tout cela engendre des défis croissants en matière de complexité, alors même que les interruptions de service liées aux certificats et les défaillances de confiance numérique deviennent une source de plus en plus fréquente de perturbations pour les entreprises. L'agilité cryptographique n'est plus simplement souhaitable : elle devient rapidement indispensable aux opérations quotidiennes, à tous les niveaux de l'organisation.

Afin de comprendre où en sont les organisations, nous avons interrogé plus de 400 décideurs seniors dans les domaines de l'IT et de la sécurité à travers le monde, notamment des RSSI, des DSI ainsi que des responsables de la cybersécurité, des opérations IT, de la gouvernance, des risques et de la conformité (GRC), et des équipes produits.

Leurs réponses sont à la fois éclairantes et préoccupantes. La plupart des organisations ont conscience des enjeux. Mais elles sont beaucoup moins nombreuses à avoir transformé cette prise de conscience en actions concrètes.

Chez DigiCert, nous ne nous sommes pas contentés d'étudier cette problématique : nous l'avons vécue. À mesure que nos propres environnements se développaient, nous avons été confrontés aux mêmes réalités. Nos équipes disposaient d'une visibilité de plus en plus limitée sur les actifs cryptographiques, devaient composer avec une gestion fragmentée voire silotée des certificats et subissaient la pression très concrète de devoir moderniser l'infrastructure sans perturber les activités qui en dépendent. La préparation au post-quantique a ajouté un degré d'urgence que nous ne pouvions ignorer.

Nous sommes donc devenus notre propre « Customer Zero ».

Nous avons inventorié nos actifs cryptographiques, identifié les certificats non gérés, automatisé la gestion de leur cycle de vie et commencé à renforcer nos systèmes critiques afin de les préparer à la cryptographie post-quantique. Cette démarche était nécessaire et nous a permis d'acquérir une compréhension directe et concrète des défis auxquels les organisations seront confrontées à chaque étape de cette transition.

Voici ce dont je suis convaincu : vous n'avez pas besoin d'un budget parfait, d'une feuille de route irréprochable ou d'une transformation globale menée en une seule fois pour réaliser de véritables progrès. Ce dont vous avez besoin, c'est d'un point de départ clair, d'une visibilité suffisante et de la volonté de franchir l'étape suivante.

Ce rapport vous apporte les données, les points de comparaison et une vision sans détour de la situation actuelle du secteur. Je vous invite à vous en servir pour engager la discussion, construire votre argumentaire et passer à l'action.

Les organisations qui agissent dès maintenant seront les mieux placées pour relever les défis d'aujourd'hui tout en s'adaptant au paysage cryptographique de demain, en constante évolution.

*Lakshmi
Hanspal*

Résumé exécutif

Cette étude montre que les entreprises ne se contentent plus de prendre conscience des défis liés à la PKI : elles commencent désormais à agir pour renforcer leur résilience opérationnelle.

La PKI gagne en importance au moment même où sa gestion devient plus complexe. L'écart entre l'importance stratégique de la PKI et les capacités opérationnelles des organisations est désormais suffisamment marqué pour nécessiter l'attention des dirigeants. Les risques sont bien compris ; en revanche, de nombreuses organisations doivent encore mettre en place la visibilité, la gouvernance et l'automatisation nécessaires pour gérer la PKI comme une composante structurante de l'entreprise, plutôt que comme un ensemble de solutions ponctuelles.



Les risques liés à la PKI sont bien compris, mais encore insuffisamment maîtrisés.

Adam Strange, analyste principal, sécurité des données, Omdia.

Les trois grands défis de la PKI aujourd'hui

1

La visibilité conditionne directement l'exposition au risque.

Le manque de visibilité sur l'ensemble du parc de certificats constitue le principal défi auquel les entreprises sont confrontées. Seules 34 % des organisations déclarent disposer d'un inventaire complet et à jour de tous leurs certificats numériques.

Le lien entre visibilité et risque est clair : 73 % des organisations se disent très ou extrêmement préoccupées par les interruptions de service provoquées par l'expiration de certificats.

2

La complexité et le niveau de maturité de la PKI freinent la capacité à répondre aux besoins croissants de l'entreprise.

74 % des organisations s'inquiètent de la prolifération des certificats et 52 % prévoient d'augmenter leurs investissements dans la PKI au cours des trois prochaines années.

Pourtant, même si les professionnels de l'IT et de la sécurité reconnaissent les risques et la nécessité de moderniser la PKI, beaucoup peinent encore à porter les discussions sur les ressources et les risques jusqu'aux décideurs.

3

S'adapter à l'évolution rapide de l'IA et à la montée de la menace quantique exige agilité et anticipation.

Plus de 73 % des organisations estiment que la PKI jouera un rôle essentiel pour établir la confiance dans les cas d'usage liés à l'IA.

La préparation à l'ère quantique reste en retard : seuls 22 % des systèmes cryptographiques ont été entièrement évalués afin d'identifier d'éventuelles vulnérabilités face aux futures attaques quantiques.

La modernisation de la PKI apporte des réponses concrètes à ces défis.

La nécessité opérationnelle de moderniser la PKI est de plus en plus évidente, mais de nombreuses organisations n'en sont encore qu'aux premières étapes. Comme cette transformation peut être complexe, la plupart adoptent une approche progressive. Les organisations les plus avancées constatent que la réussite passe par la réduction des processus manuels, l'amélioration de la visibilité et la mise à disposition des compétences et du soutien opérationnel nécessaires.

L'impact de la modernisation de la PKI

Les organisations ayant modernisé leur PKI signalent une réduction de 60 % des interruptions de service.



Introduction

La PKI sous pression

La PKI est sous pression, car le contexte opérationnel qui a façonné les pratiques d'hier n'est plus adapté aux réalités d'aujourd'hui.

Le volume de certificats augmente, les identités non humaines se multiplient, la durée de validité des certificats se raccourcit et toujours plus de systèmes dépendent de la confiance cryptographique. Parallèlement, les exigences réglementaires et sectorielles intègrent de plus en plus la PKI dans leur périmètre, renforçant la responsabilité des dirigeants en matière de disponibilité, de résilience et de gouvernance de l'IA.

Cette convergence fait évoluer la PKI d'une infrastructure de fond vers une capacité stratégique, dont la mise en œuvre, la supervision et la gouvernance relèvent pleinement des directions IT et sécurité.

Comment utiliser ce rapport

Les données de ce rapport portent sur la manière dont les organisations pilotent les opérations PKI au quotidien. En interrogeant les décideurs seniors responsables de leur mise en œuvre, nous dressons un état des lieux de la PKI aujourd'hui et des évolutions nécessaires pour qu'elle reste adaptée aux besoins de demain.

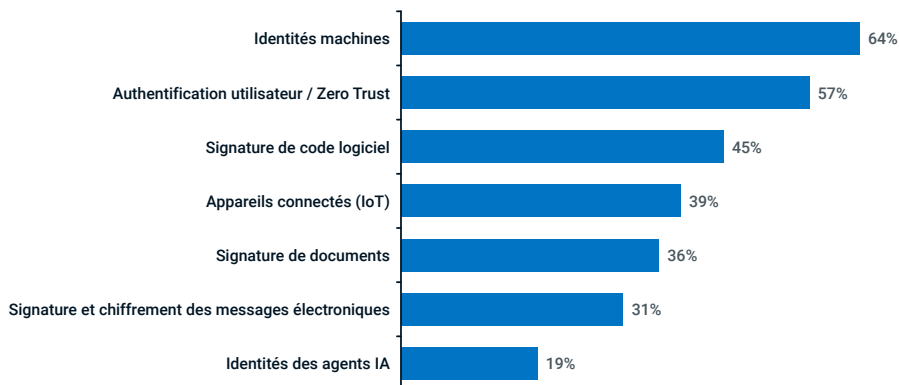
Les résultats qui suivent vous permettront de situer vos opérations PKI, de comparer votre organisation aux tendances observées et de disposer de données utiles pour nourrir votre planification, en interne comme auprès des décideurs.

Comprendre la PKI d'entreprise aujourd'hui

Avant d'aborder la PKI sous l'angle des trois grands défis identifiés, examinons d'abord la place qu'elle occupe aujourd'hui dans les organisations. Les données montrent que la PKI s'étend désormais bien au-delà des certificats web publics. Les identités machines, l'authentification des utilisateurs et les initiatives Zero Trust constituent des composantes majeures de la PKI pour plus de la moitié des répondants, avec également une présence importante dans d'autres cas d'usage non web, comme la signature de code, l'Internet des objets (IoT) et les contenus.

Ces résultats expliquent pourquoi les organisations sont particulièrement préoccupées par les interruptions de service : la PKI assure le chiffrement, l'identité, l'authentification et de nombreux autres mécanismes de confiance pour un large éventail d'infrastructures critiques, bien au-delà des seuls serveurs web accessibles au public.

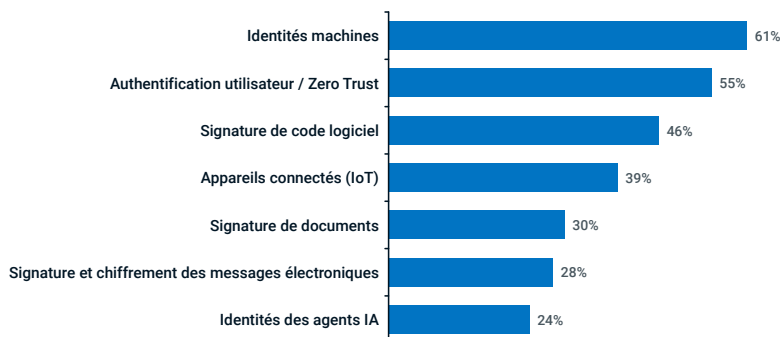
Parmi les éléments suivants, lesquels sont couverts par votre infrastructure PKI actuelle?



Priorités de modernisation de la PKI

Sans surprise, les usages actuels de la PKI sont étroitement liés aux priorités de modernisation. Près des trois quarts des répondants se disent très préoccupés par les interruptions dues à l'expiration des certificats et par leur prolifération. Les professionnels connaissent les conséquences d'une défaillance et structurent leurs efforts de modernisation autour des domaines où les besoins sont les plus pressants et les risques les plus élevés.

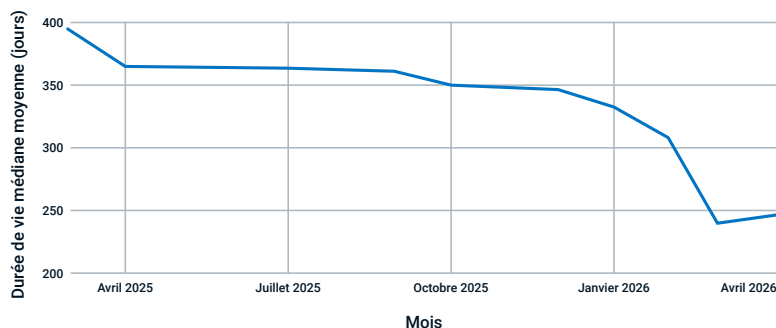
Quels sont les domaines prioritaires pour la modernisation de votre PKI au sein de votre organisation?



La réduction de la durée de validité des certificats accentue la pression

Alors que la complexité et le nombre de connexions, d'identités et de cas d'usage augmentent, la durée de validité des certificats publics diminue. Le secteur se dirige vers une durée de validité maximale de 47 jours pour les certificats TLS publics en mars 2029. Les équipes qui dépendent encore d'installations manuelles, de responsabilités mal définies ou de feuilles de calcul comme système de référence disposent donc d'une marge de manœuvre toujours plus réduite. Dans de nombreuses organisations, la PKI est devenue un écosystème qui se fragmente plus vite que les équipes ne peuvent l'intégrer et le gouverner.

Durée de vie médiane mensuelle des certificats publics (2025-2026)



L'IA et l'informatique quantique ajoutent un niveau de complexité supplémentaire.

L'IA accroît les besoins en matière d'identité, d'intégrité, de provenance et d'application des politiques pour les contenus, les modèles et les agents. Dans le même temps, la transition vers une cryptographie résistante à l'informatique quantique renforce les exigences de visibilité et d'agilité dans l'ensemble de l'environnement. Ensemble, ces évolutions montrent que la modernisation de la PKI constitue une réponse naturelle à des enjeux de confiance devenus urgents.

À retenir

La pression qui s'exerce sur la PKI ne provient pas d'une seule source. Elle résulte de la combinaison de plusieurs tendances : croissance des identités machines, réduction de la durée de validité des certificats, besoins croissants de gouvernance de l'IA et préparation à l'ère quantique. Ces évolutions convergent au même moment, notamment alors que la prévision de Gartner concernant le Q-Day¹ coïncide avec l'entrée en vigueur de la durée de validité de 47 jours pour les certificats en 2029.

¹ Résumé Gartner Insights : Comment atténuer les risques liés à la cryptographie posés par l'informatique quantique

Visibilité et risque

Plus la visibilité augmente, plus le risque diminue.

Seul un inventaire complet du déploiement et de l'état de chaque certificat dans l'entreprise permet de disposer des informations nécessaires pour éviter les zones d'ombre, les interruptions de service et les défaillances.

La visibilité contribue à prévenir les interruptions de service et les attaques.

L'étude met en évidence un constat essentiel : une organisation ne peut pas gérer efficacement les risques liés aux certificats sans disposer d'une visibilité suffisante. Seules 34 % des organisations déclarent avoir un inventaire complet et à jour de tous leurs certificats numériques. Autrement dit, deux organisations sur trois ne disposent que d'un inventaire partiel, n'en ont aucun ou ne connaissent pas précisément leur environnement de certificats. Or, la plupart des entreprises en gèrent des milliers. Lorsqu'un seul certificat expiré peut rendre indisponible une application métier entière, l'absence d'inventaire complet crée un niveau de risque élevé.

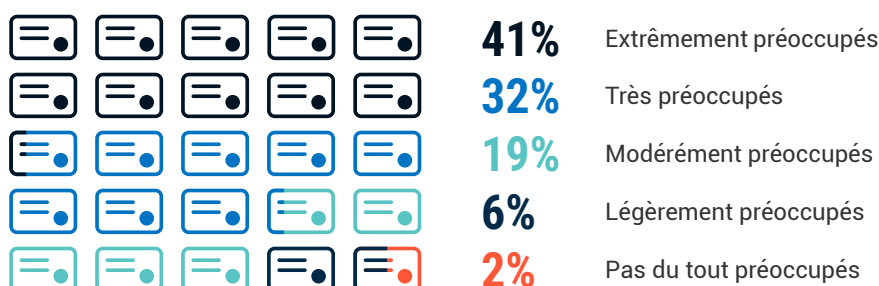
Comment votre organisation recense-t-elle et suit-elle les certificats numériques actuellement utilisés?



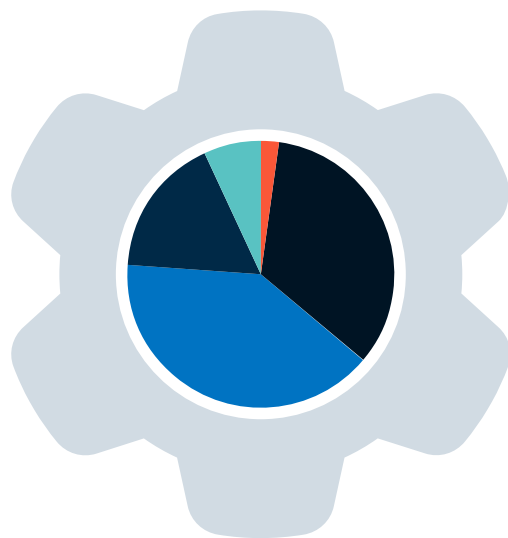
Cette préoccupation est également présente au niveau de la direction. Près des trois quarts des répondants se disent très ou extrêmement préoccupés par les interruptions dues à l'expiration des certificats, et une proportion presque identique exprime le même niveau d'inquiétude face à leur prolifération. Ces résultats illustrent une tension bien connue : les organisations comprennent les conséquences d'une défaillance de certificat, mais beaucoup ne disposent pas encore de la visibilité nécessaire pour les prévenir de manière systématique.

Par ailleurs, environ la moitié des répondants citent des solutions cloisonnées difficiles à gérer, tandis que 47 % évoquent un suivi sur tableur, source d'erreurs. Le manque de visibilité ne tient donc pas uniquement à une découverte incomplète : il résulte aussi d'outils, de responsabilités et de processus fragmentés.

Dans quelle mesure êtes-vous préoccupé par le risque de pannes/interruptions de service dues à l'expiration des certificats?



Dans quelle mesure êtes-vous préoccupé par la prolifération des certificats au sein de votre organisation à mesure que le nombre de systèmes/identités augmente?



40% Extrêmement préoccupés

34% Très préoccupés

17% Modérément préoccupés

6% Légèrement préoccupés

2% Pas du tout préoccupés

4,1 milliards

de certificats publics délivrés en 2025

Cela représente une hausse de 55 % par rapport à l'année précédente: 2,6 milliards de certificats avaient été émis dans le monde en 2024, d'après les journaux publics de transparence. Le rythme d'émission des certificats internes est encore plus élevé.



Les bons outils et processus améliorent la visibilité tout en réduisant les risques.

Malgré la diversité des approches de modernisation, les participants à l'enquête expriment clairement leur volonté d'améliorer leur PKI. Un meilleur suivi et un contrôle renforcé des certificats, une visibilité centralisée, un gain de temps et une réduction des interruptions de service contribuent à simplifier la gestion et à réduire les risques. La visibilité centralisée et l'adoption d'une approche unifiée s'imposent ainsi comme des priorités majeures pour les organisations confrontées à la complexité de leur PKI.

C'est pourquoi la découverte doit constituer la première étape de toute démarche de modernisation. Un inventaire fiable permet de passer des suppositions aux faits. Il aide les équipes à attribuer clairement les responsabilités, à identifier les dépendances liées aux renouvellements, à prioriser l'automatisation et à repérer les domaines où l'agilité cryptographique sera la plus difficile à atteindre. Sans cette visibilité, tous les autres efforts de modernisation reposent sur des informations partielles.

À retenir

La visibilité permet de mieux maîtriser les risques d'interruption liés aux certificats et constitue le socle de la modernisation de la PKI.

Complexité et maturité

La complexité et le manque de maturité accentuent les problèmes de visibilité et les risques.

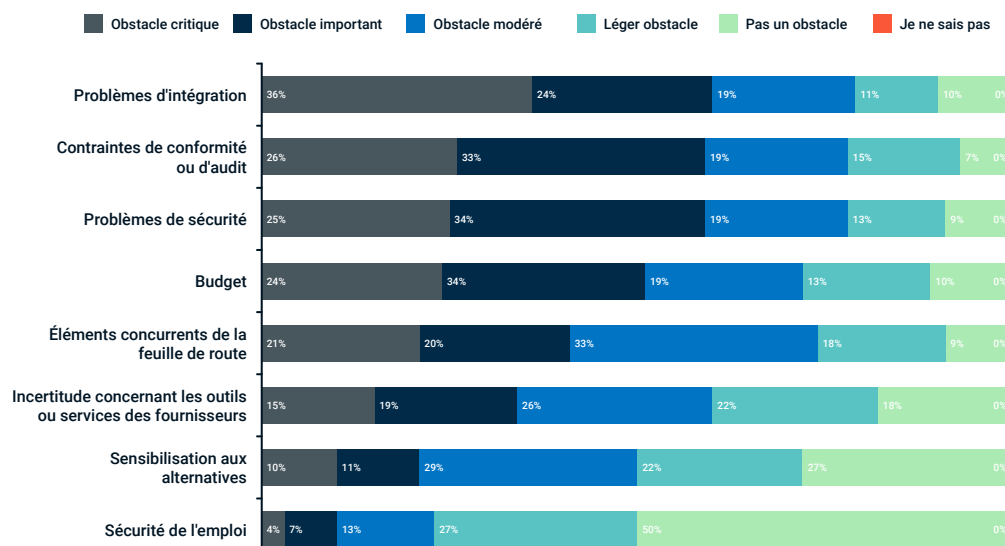
La fragmentation des environnements PKI et de leur gestion rend de plus en plus difficile la maîtrise de la prolifération des certificats.

La complexité est à la fois structurelle et technique

La complexité est l'une des principales causes du manque persistant de visibilité. La PKI est devenue structurellement complexe, et pas uniquement sur le plan technique. Le problème ne tient pas seulement à une intégration difficile ou à un workflow lourd : la confiance numérique s'est étendue aux PKI publiques et privées, aux services cloud, aux autorités de certification traditionnelles, aux identités machines, à la signature de code, aux appareils connectés et aux plateformes spécialisées, plus vite que la plupart des organisations n'ont pu les intégrer et les gouverner.

Les répondants font état d'obstacles de nature très diverse. Les problèmes d'intégration figurent parmi les principaux freins au progrès opérationnel, mais les professionnels citent également des enjeux de sécurité et de conformité, de budget, de planification et d'autres facteurs. Les organisations ne font donc pas face à un obstacle unique : la mise en œuvre et l'exploitation d'une PKI modernisée dépendent d'un ensemble complexe de facteurs architecturaux, procéduraux et organisationnels.

Dans quelle mesure les éléments suivants constituent-ils un obstacle à l'adoption par votre organisation d'une gestion automatisée des certificats?



Quels défis avez-vous rencontrés, ou prévoyez-vous de rencontrer, lors de la mise en œuvre de la modernisation de votre PKI?

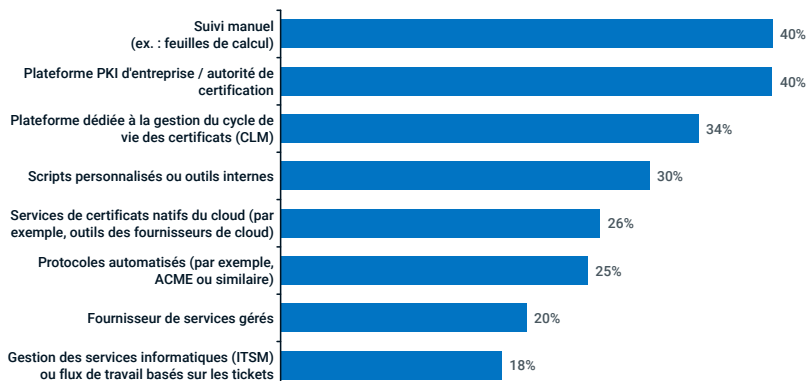


Plusieurs méthodes de gestion des certificats ne répondent plus aux besoins des entreprises.

De nombreuses entreprises ne disposent pas d'un modèle unifié de gestion des certificats. Elles utilisent plusieurs méthodes en parallèle : le suivi manuel coexiste souvent avec une PKI d'entreprise (autorité de certification privée), une plateforme de gestion du cycle de vie des certificats, des scripts personnalisés ou encore des workflows ITSM.

En moyenne, les entreprises utilisent simultanément deux à trois méthodes différentes. Beaucoup se trouvent donc dans une phase de transition, passant d'une gestion sans automatisation à une automatisation partielle, puis complète. Dans la pratique, une automatisation partielle peut couvrir le renouvellement du certificat sans automatiser son installation. Même si cela représente un progrès par rapport à une gestion entièrement manuelle, le risque d'interruption reste élevé en l'absence d'automatisation de bout en bout.

Quelles méthodes/plateformes votre organisation utilise-t-elle actuellement pour la gestion des certificats?



Les méthodes manuelles ne permettent pas de maîtriser la prolifération des certificats, en particulier lorsqu'elles reposent sur des tableurs.

Depuis des décennies, les tableurs servent à suivre les inventaires et l'état des certificats. Ils sont pratiques, familiers et constituent souvent le moyen le plus rapide de démarrer. Le problème est qu'on leur demande aujourd'hui d'assurer une fonction pour laquelle ils n'ont jamais été conçus. À mesure que le volume de certificats augmente et que les délais de renouvellement se raccourcissent, les tableurs cessent d'être un simple outil de gestion et deviennent un facteur de risque.

Avant l'apparition d'outils d'automatisation fiables, les tableurs étaient indispensables. Aujourd'hui, des plateformes CLM matures, des protocoles standards d'interopérabilité, des contrôles pilotés par des politiques et l'installation automatisée permettent de réduire considérablement la charge liée aux feuilles de calcul et aux autres processus manuels. La clé réside dans l'ordre des priorités : rationaliser, intégrer et automatiser d'abord les cas d'usage à plus forte valeur, plutôt que de chercher à regrouper immédiatement l'ensemble de l'écosystème PKI de l'entreprise sous une seule plateforme d'automatisation.

À retenir

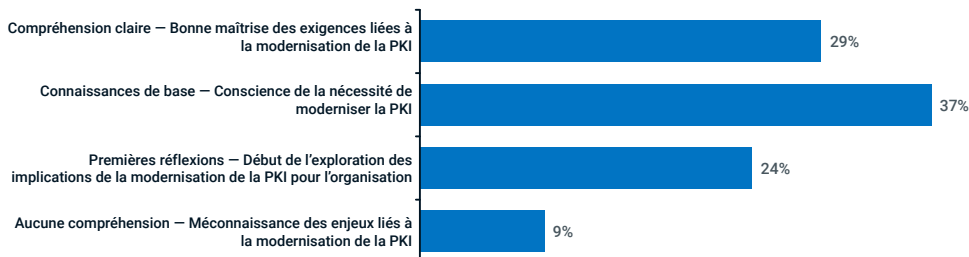
La complexité est réelle, mais elle peut être maîtrisée. Elle montre surtout que la PKI a besoin d'un modèle opérationnel cohérent, reposant sur une consolidation progressive, des intégrations fiables et une automatisation appliquée en priorité là où les risques sont les plus élevés.

La maturité passe par l'adoption des bonnes pratiques PKI.

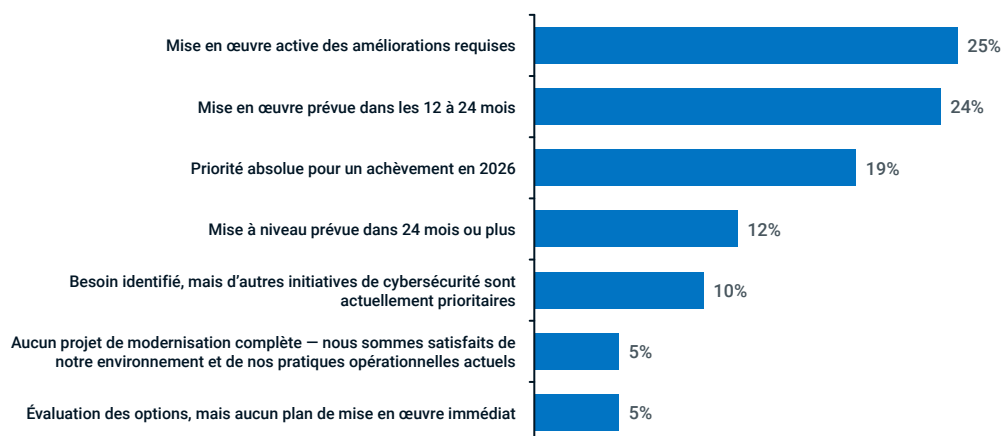
Une PKI atteint un niveau de maturité lorsque les bonnes intentions se traduisent par un modèle opérationnel capable d'accompagner la croissance de l'entreprise en toute sécurité. Cela suppose de mettre en place la visibilité, l'attribution claire des responsabilités, la gouvernance et des processus reproductibles nécessaires pour faire fonctionner la PKI comme un système maîtrisé. À ce stade, les efforts de modernisation sont engagés, mais restent encore inégaux : la prise de conscience, l'urgence et la mise en œuvre n'avancent pas au même rythme.

Ce décalage ressort clairement de l'enquête. Près de trois répondants sur dix déclarent que leur organisation comprend clairement les enjeux de la modernisation de la PKI, et un sur quatre indique déjà mettre en œuvre les améliorations nécessaires. Parallèlement, environ 80 % agissent déjà ou prévoient de le faire dans un délai d'un à trois ans. La volonté est largement présente, même si le niveau de mise en œuvre varie encore fortement.

Face au raccourcissement de la durée de validité des certificats et à l'arrivée imminente de la cryptographie post-quantique, les organisations doivent mettre à jour leurs infrastructures PKI. Comment votre organisation comprend-elle la modernisation de la PKI?

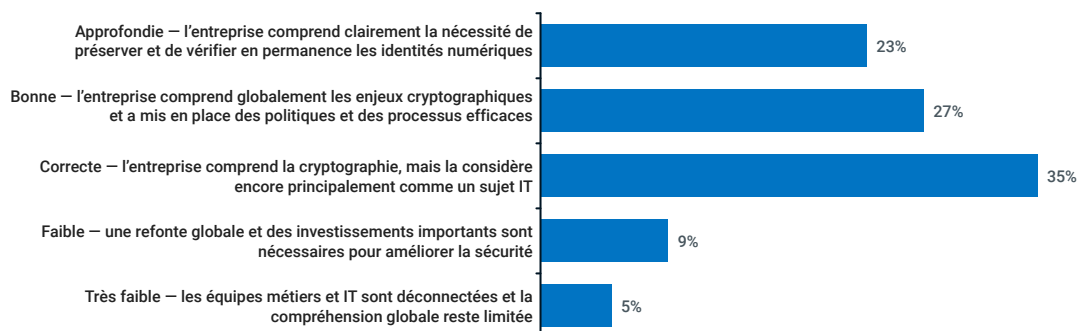


Quels sont les projets de votre organisation pour moderniser entièrement son infrastructure PKI?



Les échanges au sein des organisations montrent également des signes d'amélioration. Un peu plus de la moitié des répondants estiment que leur entreprise possède une compréhension approfondie ou satisfaisante de l'identité numérique et de l'intégrité cryptographique. 35 % supplémentaires indiquent que leur organisation comprend la cryptographie, mais continue de la considérer principalement comme un sujet IT. En d'autres termes, la PKI gagne en visibilité auprès des dirigeants, mais de nombreuses organisations doivent encore transformer cette prise de conscience en gouvernance et en discipline opérationnelle.

Selon vous, quelle est la perception générale au sein de l'entreprise quant à l'importance cruciale d'une PKI efficace et moderne?

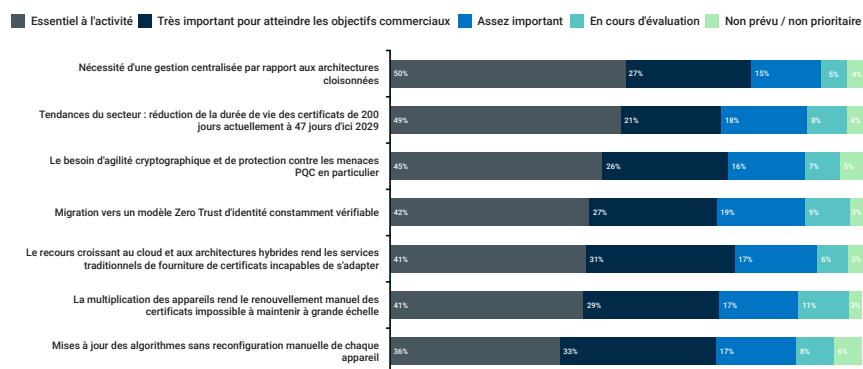


Les organisations les plus matures privilégient la centralisation

Les environnements cloisonnés compliquent le maintien d'une visibilité complète, la maîtrise des risques liés à la prolifération des certificats et la gestion de l'ensemble du parc. Les organisations les plus matures privilégient donc une gestion centralisée de la PKI : 76 % la considèrent comme essentielle ou très importante pour leur activité.

Au-delà de la gestion unifiée, la réduction de la durée de validité des certificats et la préparation aux menaces post-quantiques dessinent les contours d'un modèle opérationnel mature : centraliser les éléments critiques de la PKI, automatiser les tâches répétitives et concevoir des processus capables d'évoluer, plutôt que de considérer la PKI comme un environnement statique.

Quelle importance votre organisation accorde-t-elle aux facteurs susceptibles de motiver la modernisation de son environnement PKI?



Des résultats améliorés pour les organisations ayant modernisé leur PKI

Les résultats de l'enquête montrent des améliorations significatives après la modernisation de la PKI. Parmi les répondants concernés, 64 % déclarent bénéficier d'une gestion automatisée du cycle de vie, 60 % constatent une réduction des interruptions de service, 44 % soulignent une meilleure prise en charge de la conformité réglementaire et 43 % indiquent avoir gagné en visibilité et en contrôle. Lorsqu'elle est bien menée, la modernisation réduit les interruptions, allège la charge administrative et simplifie la conformité.

La maturité d'une PKI ne se mesure ni au nombre d'autorités de certification déployées, ni au nombre d'outils achetés. Elle se mesure à la capacité de l'organisation à répondre de façon fiable à quelques questions opérationnelles essentielles : quels actifs possédons-nous ? Qui en est responsable ? Quand doivent-ils être renouvelés ? Quels services en dépendent ? Quelles politiques s'appliquent ? Et pouvons-nous effectuer des changements sans interruption ?

À retenir

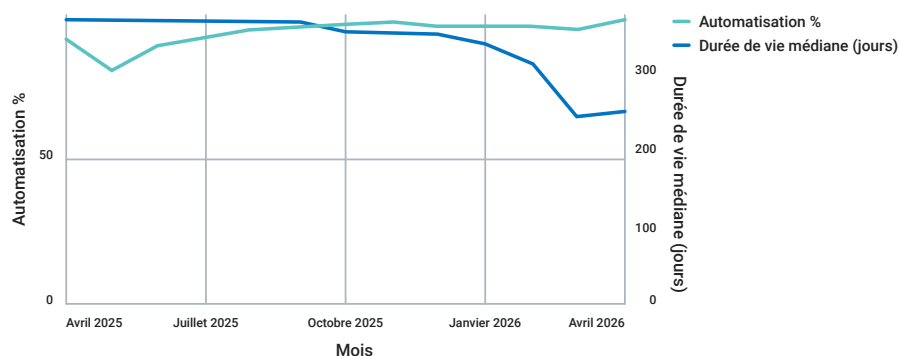
Les organisations prennent conscience du problème et commencent à identifier les actions nécessaires. Les plus avancées dans leur démarche de modernisation en constatent déjà les bénéfices.

47

Durée de validité de 47 jours et automatisation

Les données de gestion des certificats des clients DigiCert ONE montrent qu'ils ont commencé à réduire la durée de validité de leurs certificats TLS publics depuis l'approbation, par le CA/B Forum, d'une réduction progressive à 47 jours. Cette évolution n'augmente pas nécessairement le nombre de certificats qu'une organisation doit gérer ; elle augmente en revanche la fréquence à laquelle les équipes de sécurité doivent exécuter les tâches liées à leur cycle de vie.

Pourcentage d'automatisation en fonction de la durée de vie médiane des certificats publics



IA et quantique

IA et informatique quantique: accélération et changement de paradigme

Ces technologies émergentes représentent l'un des plus grands défis auxquels la PKI ait été confrontée depuis des décennies, et potentiellement l'une des transformations les plus profondes de son histoire.

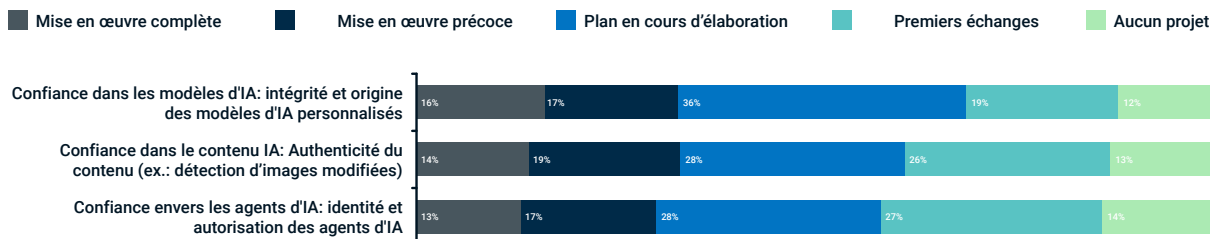
La confiance dans les contenus, les modèles et les agents d'IA nécessite une approche PKI adaptée.

L'IA renforce les exigences de confiance numérique en obligeant les organisations à répondre, à la vitesse des machines, à des questions plus complexes sur l'identité, la provenance et les autorisations. À mesure que les entreprises déploient des agents autonomes, des modèles et des contenus générés par l'IA, elles ont besoin de mécanismes plus robustes pour prouver ce qui est authentique, digne de confiance et autorisé à agir. La PKI répond déjà à ce type d'enjeux ; l'IA ne fait que les rendre plus visibles et plus urgents.

L'enquête montre que les dirigeants perçoivent déjà le lien étroit entre les enjeux liés à l'IA et la PKI. Près des trois quarts des répondants estiment que la PKI jouera un rôle majeur dans les usages de l'IA.

La préparation reste toutefois insuffisante. Même si les organisations reconnaissent de plus en plus le rôle de la PKI dans la sécurité et la gouvernance de l'IA, la plupart n'en sont encore qu'aux premières étapes de planification et de mise en œuvre. Le modèle dominant n'est donc pas encore celui de processus matures et généralisés, mais plutôt un mélange d'exploration, de planification et de premiers projets.

Comment décririez-vous le mieux votre niveau actuel de planification concernant ces aspects spécifiques de la confiance en l'IA ?

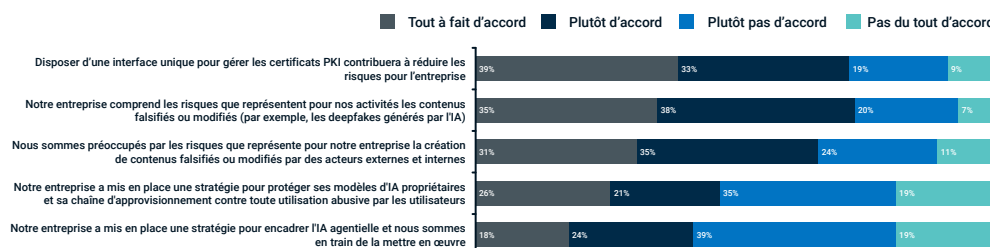


Passer de la sensibilisation aux risques à une stratégie opérationnelle de confiance pour l'IA

C'est au niveau de la gouvernance que ce manque de préparation apparaît le plus clairement. La majorité des répondants ne considèrent pas que leur entreprise dispose déjà d'une stratégie pour encadrer et déployer l'IA agentielle. Plus de la moitié estiment également ne pas avoir de stratégie suffisamment établie pour protéger leurs modèles d'IA propriétaires et sécuriser la chaîne d'approvisionnement des modèles externes utilisés. Dans le même temps, 73 % affirment que leur entreprise comprend les risques liés aux contenus falsifiés ou altérés, 66 % restent préoccupés malgré les mesures prises et 72 % considèrent qu'une visibilité centralisée sur la gestion des certificats PKI sera essentielle à l'ère de l'IA.

C'est pourquoi l'IA doit être considérée comme un moteur de modernisation de la PKI, et non comme un programme de confiance distinct. Les organisations qui ne sont pas en mesure de visualiser et de contrôler aujourd'hui leur utilisation des certificats auront demain davantage de difficultés à établir la confiance dans les agents, les modèles et les contenus d'IA.

Dans quelle mesure êtes-vous d'accord avec les affirmations suivantes?



À retenir

La confiance dans l'IA ne constitue pas une discipline distincte de la modernisation de la PKI. Elle met au contraire en évidence la nécessité de renforcer dès aujourd'hui la gouvernance de la confiance numérique.

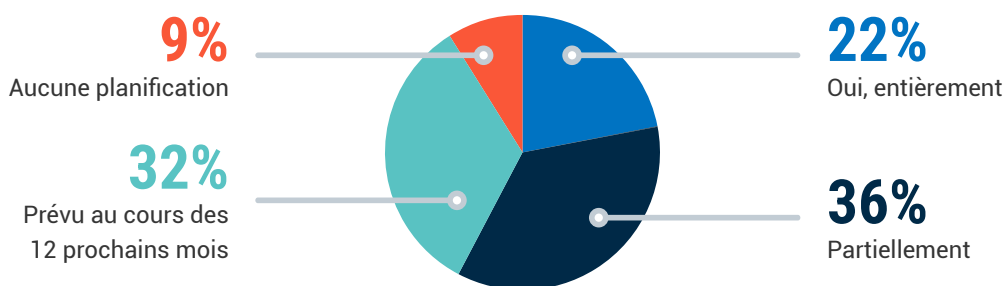
L'ère quantique approche. La préparation demande du temps.

Si l'IA constitue le défi immédiat en matière de confiance, l'informatique quantique arrive juste derrière. La transition vers la cryptographie post-quantique ne se résumera ni à une mise à jour de routine ni à une opération ponctuelle. Les organisations devront savoir où la cryptographie est utilisée, quels systèmes en dépendent, comment ces dépendances s'articulent et comment mener la transition en limitant au maximum les perturbations.

Les résultats de l'enquête montrent à la fois une prise de conscience réelle et un travail encore inachevé. Seuls 22 % des répondants déclarent avoir entièrement évalué leurs bibliothèques et systèmes cryptographiques afin d'identifier les vulnérabilités potentielles face aux futures attaques quantiques. 36 % indiquent l'avoir fait partiellement et 32 % prévoient de le faire au cours des 12 prochains mois. La préparation complète reste donc rare, mais la majorité des organisations avancent dans la bonne direction.

Cette tendance se retrouve dans les facteurs de modernisation cités par les répondants. Plus de 71 % considèrent que l'agilité cryptographique et la protection contre les menaces quantiques sont essentielles ou très importantes pour l'entreprise. Les dirigeants ont donc compris l'enjeu stratégique de la préparation à l'ère quantique, même si les travaux de découverte et de migration restent encore à un stade précoce.

Votre organisation a-t-elle évalué les vulnérabilités des bibliothèques et systèmes cryptographiques dans le contexte de futures attaques quantiques?



L'essentiel est que la préparation à l'ère quantique repose sur les mêmes fondations opérationnelles que celles abordées dans ce rapport. Une organisation ne peut pas devenir crypto-agile si elle ignore où sont déployés ses certificats, ses clés, ses algorithmes et ses bibliothèques cryptographiques. Elle ne peut pas non plus planifier une transition coordonnée si les responsabilités sont fragmentées ou si les processus de cycle de vie restent manuels. La préparation à l'ère quantique commence donc bien avant le déploiement d'un nouvel algorithme.

À retenir

La préparation à l'ère post-quantique ne doit pas être considérée comme une initiative distincte. L'inventaire des certificats et l'automatisation du cycle de vie nécessaires aux autres initiatives contribuent directement à l'agilité indispensable pour migrer vers la cryptographie post-quantique.

Modernisation de la PKI

La modernisation de la PKI répond aux enjeux de visibilité, de complexité, de maturité, d'IA et de préparation à l'ère quantique.

Le principal enseignement de cette étude n'est pas que les organisations échouent à mettre en œuvre leur PKI. C'est plutôt que les approches encore utilisées par beaucoup d'entre elles ne sont plus adaptées à l'ampleur prise par la PKI. Le problème est plus facile à maîtriser qu'il n'y paraît : les dirigeants reconnaissent la nécessité de moderniser, des budgets sont prévus et la plupart des organisations ont déjà l'intention d'agir. L'enjeu consiste désormais à transformer cette dynamique en un contrôle opérationnel reproductible.

Pour les responsables IT et sécurité, cela signifie considérer la modernisation de la PKI comme une capacité essentielle. La PKI influe directement sur la disponibilité, l'efficacité opérationnelle, la gouvernance de l'IA et l'agilité cryptographique. Les organisations qui modernisent efficacement leur PKI ne se contentent pas de réduire les interruptions liées aux certificats ou d'améliorer leur efficacité : elles mettent en place un socle de confiance intelligent et évolutif pour accompagner la croissance des identités machines, l'adoption de l'IA et la transition vers l'ère quantique.

La modernisation de la PKI peut sembler être un chantier de grande ampleur — et elle l'est. Mais elle n'a rien d'abstrait. Commencez là où la valeur opérationnelle est immédiate et où l'argument économique est le plus simple à démontrer.

Mettre en place la découverte et l'inventaire

Réduire les risques liés au manque de visibilité

Constituez un inventaire fiable des certificats et des actifs cryptographiques associés dans les environnements publics et privés. Ajoutez-y ensuite le contexte nécessaire, notamment la responsabilité et l'impact métier, afin de transformer les données brutes en informations exploitables. C'est le socle de tout ce qui suit. La découverte permet aux équipes de passer de « nous pensons » à « nous savons ».

Automatiser les certificats critiques

Comblent les lacunes et réduire les fragilités pour mieux maîtriser la complexité et gagner en maturité

Les certificats TLS/SSL publics constituent le cas d'usage de modernisation le plus universel, car toutes les organisations exposées à Internet sont concernées par la réduction de leur durée de validité. Cette tendance ne fera que s'accroître. Automatiser l'émission et l'installation des certificats TLS publics est donc l'un des moyens les plus rapides de réduire les risques d'interruption tout en mettant en place des processus de cycle de vie reproductibles. Cette démarche aide également les équipes à construire les modèles opérationnels nécessaires pour étendre ensuite l'automatisation à la PKI interne, à la signature de code, à l'identité des appareils et à d'autres domaines de confiance.

Standardiser la PKI interne

Réduire la fragmentation et se préparer aux futures évolutions cryptographiques

C'est souvent dans les environnements PKI internes que la complexité s'accumule le plus vite et que les pratiques obsolètes persistent le plus longtemps. À mesure que le volume de certificats augmente et que les exigences cryptographiques évoluent, les pratiques incohérentes accroissent les risques opérationnels et rendent plus difficile la coordination des changements.

Les organisations devraient mettre en place une gouvernance centralisée fondée sur des politiques clairement définies pour leurs environnements PKI internes. Ces politiques peuvent préciser les autorités de certification approuvées, la criticité et la responsabilité métier, les standards de configuration des certificats et des données cryptographiques, ainsi que les exigences de conformité. Des politiques cohérentes améliorent la visibilité, réduisent les frictions opérationnelles, simplifient les efforts de conformité et créent une base plus solide pour des initiatives futures comme la gouvernance de l'IA et la cryptographie post-quantique.

Ces politiques permettent également de consolider les autorités de certification inutiles ou redondantes, de mettre hors service les plateformes héritées et de placer les environnements PKI internes cloisonnés sous un modèle de gouvernance plus cohérent. Les violations de politique présentant le plus fort impact doivent être corrigées en priorité. L'objectif n'est pas de tout reconstruire en une seule fois, mais de réduire systématiquement les risques liés aux usages actuels et émergents de la PKI.

Méthodologie

Ce rapport s'appuie sur une étude primaire menée de façon indépendante par Omdia en avril 2026. L'enquête a porté sur l'évolution de la PKI, les facteurs de modernisation, les défis opérationnels et les perspectives d'avenir.

L'étude a interrogé 423 décideurs de haut niveau, notamment des RSSI, des DSI et des responsables IT et sécurité en charge de la cybersécurité, de la PKI et de l'infrastructure numérique. Les répondants représentaient les fonctions Produits et R&D, Opérations IT et techniques, Cybersécurité, ainsi que Gouvernance, Risques et Conformité.

Les répondants travaillaient au sein d'organisations situées en Amérique du Nord, dans la région EMEA et en Asie-Pacifique, et représentaient 11 secteurs d'activité.



Toutes les organisations participantes comptaient au moins 1 000 employés

39%

comptaient entre 1 000 et 4 999 employés

24%

comptaient entre 5 000 et 9 999 employés

37%

comptaient 10 000 employés ou plus

Les questions de l'enquête visaient à mesurer les réalités opérationnelles et les priorités stratégiques liées à la modernisation de la PKI, à la confiance numérique et à la préparation cryptographique. L'analyse et les conclusions reposent sur les données collectées, la méthodologie de recherche d'Omdia et un ensemble de données propriétaire. Certaines questions autorisaient plusieurs réponses ; les totaux peuvent donc dépasser 100 %.

L'analyse complémentaire s'appuie sur les données issues des activités d'autorité de certification publique et de PKI gérées par DigiCert entre janvier 2025 et mars 2026. Elle comprend des statistiques agrégées provenant d'un échantillon de 757 entreprises clientes. Les données relatives aux autorités de certification publiques proviennent des journaux de transparence des certificats.

Auteurs et contributeurs

Omdia Consulting

Omdia est un acteur de référence dans les domaines des données, de la recherche et du conseil. L'entreprise accompagne les fournisseurs de services numériques, les sociétés technologiques et les décideurs afin de les aider à réussir dans une économie numérique interconnectée. Grâce à son réseau mondial d'analystes, Omdia fournit des analyses expertes et une vision stratégique des secteurs des technologies, des télécommunications et des médias. La combinaison de données fiables, d'analyses de marché et d'expertise sectorielle permet d'éclairer la prise de décision. Omdia fait partie d'Informa TechTarget, au sein du groupe Informa coté à la Bourse de Londres.

Commencez dès maintenant votre transition vers une PKI moderne.



À propos de DigiCert

DigiCert est un leader mondial de la confiance intelligente. Nous protégeons le monde numérique en garantissant la sécurité, la confidentialité et l'authenticité de chaque interaction. Notre plateforme DigiCert ONE, basée sur l'IA, unifie la gestion du cycle de vie de la PKI, du DNS et des certificats afin de sécuriser les infrastructures, les logiciels, les appareils, les messages, ainsi que les contenus, agents et modèles d'IA. Découvrez pourquoi plus de 125 000 organisations, dont 90 % des entreprises du classement Fortune 500, font confiance à DigiCert pour faire face aux menaces actuelles et se préparer à un avenir résilient face aux risques quantiques sur www.digicert.com/fr