EVERTRUST

WHITE PAPER | 2025

LA SOUVERAINETÉ NUMÉRIQUE

Qu’est ce que c’est et comment l’intégrer dans son infrastructure de confiance ?

Souveraineté

PKI

Autonomie Européenne

CLM

www.evertrust.fr

CONTEXTE ET ENJEUX DE LA SOUVERAINTÉ NUMÉRIQUE

Depuis plus d'une décennie, la souveraineté numérique s'est imposée comme un enjeu central du débat public et stratégique en France et en Europe.

Née d'une prise de conscience face à la domination des géants technologiques américains puis chinois, et catalysée par des révélations majeures telles que l'affaire Snowden ou le scandale Cambridge Analytica, la question de l'autonomie stratégique numérique ne cesse de gagner en importance dans les sphères politiques, industrielles et économiques.

Plus récemment, des incidents concrets – comme la suspension de l'accès à la messagerie professionnelle du procureur de la Cour pénale internationale **à la suite d'une décision politique extraterritoriale** – ont illustré la capacité de certains fournisseurs à agir directement sur la continuité d'activité d'institutions européennes majeures.

Ces épisodes, loin d'être des signaux d'alarme, servent aujourd'hui de catalyseurs pour accélérer la réflexion stratégique et l'action collective autour de l'autonomie numérique.

En effet, ce «simple clic» actionné depuis Washington a agi comme un électrochoc sur le continent : il a accéléré les débats politiques et les initiatives législatives visant à renforcer l'indépendance numérique.

Aux Pays-Bas, où siège la CPI, des parlementaires ont exigé que 30% des services cloud utilisés par l'État soient européens ou nationaux d'ici 2029.

30%

Services cloud européens requis aux Pays-Bas d'ici 2029

∞

Opportunités pour renforcer l'autonomie européenne

SOUVERAINETÉ : UN CONCEPT PLURIEL, DES DÉFINITIONS CONTRASTÉES

Il est essentiel de souligner que la notion de souveraineté numérique européenne ne fait pas l'objet d'une définition unique et universellement partagée.

Selon les institutions, les experts ou les acteurs économiques, la souveraineté numérique recouvre des réalités et des priorités différentes, souvent façonnées par le contexte politique, technologique ou géopolitique du moment

Pour la Commission Européenne

La souveraineté numérique européenne, c'est la capacité de l'Europe à agir librement et de manière autonome dans l'espace numérique, à maîtriser ses infrastructures, ses technologies et ses données, tout en protégeant ses citoyens et ses entreprises des dépendances vis-à-vis d'acteurs extra-européens.

La souveraineté numérique est considérée comme un outil stratégique pour garantir la sécurité, la prospérité et la capacité d'innovation de l'UE

Pour l'ANSSI en France

La souveraineté numérique est la capacité à maîtriser, protéger et gouverner ses actifs numériques essentiels, en s'assurant qu'ils ne puissent être compromis ou contrôlés par des intérêts extérieurs.

Dans ses guides et référentiels (comme SecNumCloud), l'agence recommande explicitement de privilégier des solutions permettant de garder la main sur les données, les clés cryptographiques et les systèmes essentiels.

L'OBJECTIF RESTE COMMUN : UN ARSENAL RÉGLEMENTAIRE EN PLEINE CONSOLIDATION

L'Europe a mis en place un cadre réglementaire robuste et des programmes ambitieux pour accompagner cette dynamique de souveraineté numérique.
Cette chronologie illustre l'accélération des initiatives européennes ces dernières années :

RGS (2010)

Il vise à garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité des échanges électroniques, notamment pour les services publics.

eIDAS (2016)

Il vise à faciliter la reconnaissance mutuelle des moyens d'identification et à renforcer la sécurité et la fiabilité des transactions électroniques dans l'Union européenne.

RGPD (2018)

Il encadre le traitement des données personnelles sur le territoire de l'UE et impose des obligations strictes en matière de transparence, sécurité et consentement.

NIS 2 (2024)

Élargit les obligations de cybersécurité à de nouveaux secteurs critiques (santé, transport, énergie)

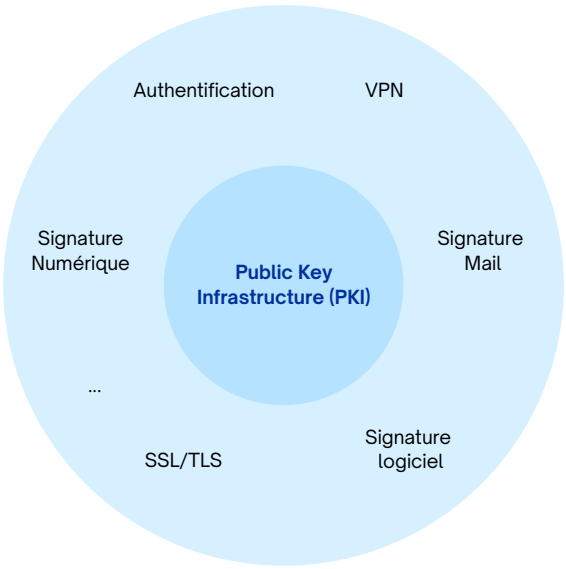
DORA (2025)

Renforce la résilience opérationnelle numérique du secteur financier avec des exigences strictes de continuité et de contrôle des tiers fournisseurs de services technologiques

Cyber Resilience Act (en cours)

Impose des standards de sécurité pour tous les produits connectés mis sur le marché européen.

LA PKI : COEUR DE LA CONFIANCE NUMÉRIQUE



Dans cette perspective, la question de la maîtrise des infrastructures de confiance prend une dimension particulièrement concrète. Si la souveraineté numérique est souvent évoquée à travers les réglementations, les politiques industrielles ou la localisation des données, elle se joue aussi, au quotidien, dans la gestion des éléments les plus sensibles: les clés cryptographiques et les identités numériques.

Or, confier la gestion de ses clés ou de ses certificats à un acteur extérieur – en particulier à un fournisseur soumis à une législation extraterritoriale comme le Cloud Act américain – revient à déléguer une part essentielle de sa souveraineté.

Même si les données sont hébergées en Europe, la juridiction qui s'applique au fournisseur peut permettre à une autorité étrangère d'exiger l'accès aux clés ou aux identités, sans que l'organisation puisse s'y opposer.

Ce paradoxe est au cœur des enjeux actuels: Peut-on réellement garantir la confidentialité, l'intégrité et la continuité de ses services lorsque les clés de ses infrastructures critiques sont potentiellement accessibles à des tiers non européens ?

C'est toute la différence entre une infrastructure de confiance maîtrisée – PKI et gestion du cycle de vie des certificats (CLM) opérées en souveraineté – et une solution externalisée hors du périmètre européen. Ce choix impacte directement la capacité à contrôler :

- L'accès et la gestion des clés privées,
- La révocation ou le renouvellement des certificats,
- L'auditabilité et la traçabilité des opérations sensibles

COMMENT CHOISIR UN FOURNISSEUR DE PKI SOUVERAIN ?

Le choix d'un fournisseur PKI souverain est un enjeu stratégique pour toute organisation soucieuse de maîtriser sa chaîne de confiance numérique, de répondre aux exigences réglementaires et de limiter les risques liés à l'extraterritorialité.

> Les recommandations des autorités publiques, les études sectorielles et les retours d'expérience convergent sur plusieurs critères essentiels pour évaluer et sélectionner un fournisseur PKI en toute confiance.

Maîtrise juridique & localisation

Plusieurs rapports institutionnels (Sénat français, Commission européenne, ANSSI) insistent sur la nécessité de privilégier des fournisseurs dont l'hébergement, les opérations et la gouvernance sont localisés dans l'Union européenne.

Cette approche garantit que la gestion des clés privées reste encadrée par le droit européen, réduisant l'exposition aux lois extraterritoriales.

eIDAS · RGPD · NIS 2 · UE

Sécurité technique & robustesse

Les fournisseurs européens reconnus intègrent les standards de sécurité les plus exigeants : HSM certifiés, gestion automatisée du cycle de vie des certificats, segmentation des environnements, et audits réguliers.

Les architectures hybrides et modulaires sont désormais considérées comme des bonnes pratiques.

SecNumCloud · NIS2 · ISO 27001

Conformité & certifications

Le fournisseur doit démontrer sa conformité aux exigences européennes (RGPD, eIDAS, NIS2, RGS) et disposer de certifications reconnues qui attestent de la qualité des processus de gestion, de la sécurité des infrastructures et de la capacité à répondre aux audits et contrôles.

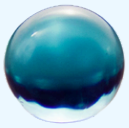
ANSSI · ISO 27001 · SecNumCloud

Flexibilité d'intégration

Le fournisseur PKI doit proposer des solutions modulaires, compatibles avec les systèmes d'information existants (annuaire LDAP, Active Directory, systèmes de gestion des identités) et capables de s'adapter à des cas d'usage variés (authentification, signature électronique, chiffrement)

API · CLM & PKI

Transparence & auditabilité



Le fournisseur doit offrir un accès clair aux journaux d'activité, permettre des audits réguliers indépendants et fournir une documentation exhaustive.

Les acteurs européens investissent aussi dans l'innovation, notamment autour du PKI as a Service, de la gestion automatisée des identités et des signatures électroniques qualifiées, renforçant ainsi la confiance des clients.

PKI as a Service · Audit trail

Accompagnement & partenariat

Le choix d'un fournisseur PKI est aussi une relation à long terme.

Un accompagnement personnalisé, une expertise technique accessible et un support réactif sont des facteurs clés pour réussir le déploiement et la gestion quotidienne de la PKI.

Expertise · Proximité · UE

À PROPOS

EVERTRUST est une société Européenne qui développe des solutions de gestion des certificats numériques et d'infrastructure à clés publiques (PKI) pour les entreprises et organisations mondiales.

Fondée en 2017, l'entreprise propose une gamme d’outils couvrant l'ensemble du cycle de vie des certificats numériques : gestion automatisée des certificats publics et privés, autorité de certification privée haute performance, autorité de validation (OCSP) et autorité d'horodatage (TSA).

Basée en France, EVERTRUST est certifiée ISO 27001 et membre d'Hexatrust, du PKI Consortium et de la Microsoft Intelligent Security Association (MISA).

EVERTRUST se positionne aujourd’hui comme un acteur européen indépendant répondant aux enjeux croissants de souveraineté numérique.

+20%

des grands groupes français accompagnés

+30M

certificats gérés via nos solutions

+500K

identités machines gérées via nos solutions

EVERTRUST

Reprenez le contrôle de votre confiance numérique avec une PKI 100% souveraine

Je contacte EVERTRUST