Certificats du .fr : la dépendance que l'État n'achète pas

Neuf ans après sa précédente édition, l'observatoire de la résilience de l'Internet français, conduit par l'ANSSI et l'Afnic, établit que les sites en .fr chiffrent leurs échanges, dans leur immense majorité, sous la garantie d'autorités de certification américaines, et qu'une seule organisation en signe les trois quarts. Cette situation relève de la dépendance au sens de Jeffrey Pfeffer et Gerald Salancik : le contrôle qu'exerce sur une organisation celui qui détient une ressource dont elle ne peut se passer. C'est la plus complète de toutes celles que le débat sur la souveraineté numérique recense, et la seule qui ne passe par aucun marché. Personne ne l'achète, donc aucun levier d'achat ne la gouverne.

Par Alexandre Berge · 21 novembre 2026 · 17 min de lecture · Chronique

Trois émetteurs garantissent le chiffrement de presque tout le .fr

L'édition 2026 du rapport « Résilience de l'Internet français » a été présentée le 2 novembre 2026 au Campus Cyber, à La Défense, lors de la journée du conseil scientifique de l'Afnic, par François Contat pour l'ANSSI et Marc van der Wal pour l'Afnic. La précédente livraison, consacrée à l'année 2016, avait été mise en ligne le 29 septembre 2017. Entre les deux, l'observatoire créé en 2011 sous l'égide de l'agence nationale de cybersécurité est resté silencieux. Il revient avec un périmètre élargi à l'authentification du courrier électronique et avec un indicateur qui n'existait pas sous cette forme : la répartition des certificats web selon le pays de l'autorité qui les émet.

Le dispositif de mesure est simple dans son principe. Un robot d'indexation développé par l'Afnic interroge le port 443 (celui des échanges web chiffrés) de chaque nom de domaine du registre, préfixé de « www » si nécessaire, et relève le certificat présenté. Au 10 juin 2026, les échanges ont pu être collectés pour 2 963 264 zones (une zone correspond ici à un nom de domaine délégué sous .fr), dont 95 % présentaient un certificat valide. La partie technique du bilan est flatteuse : 94 % des serveurs négocient la version la plus récente du protocole TLS (Transport Layer Security, la couche qui chiffre la communication entre un site et son visiteur), et la confidentialité persistante est presque généralisée.

Le chiffre qui change la lecture vient ensuite. Selon le rapport, 90,31 % des certificats relevés ont été émis par des autorités de certification (les organismes qui attestent qu'une clé de

chiffrement appartient bien au site qui la présente) établies aux États-Unis. Une seule organisation, Let's Encrypt, en émet 75,13 %. Trois émetteurs en couvrent plus de 91 %. Les autorités françaises ne concernent que 1,59 % des zones étudiées, et près de 99 % de cette part revient à un seul acteur, le registraire Gandi. Le même rapport relève une concentration voisine dans un autre étage de l'infrastructure : 79,73 % des zones déléguées sous .fr ont tous leurs serveurs de noms dans un seul système autonome (un réseau administré par un même opérateur, au sens du routage), contre 83 % en 2016. La dispersion progresse, mais à un rythme que le rapport lui-même qualifie de très lent.

> **Qui signe le web français en 2026**
>
> Le tableau des organisations émettrices publié par l'observatoire place Let's Encrypt (États-Unis) à 75,13 %, Google Trust Services (États-Unis) à 10,89 %, Sectigo (Royaume-Uni) à 6,56 %, DigiCert (États-Unis) à 1,65 %, Gandi (France) à 1,58 %, GoDaddy (États-Unis) à 1,53 % et Amazon (États-Unis) à 0,96 %. Le premier émetteur établi dans l'Union après la France est GlobalSign (Belgique), à 0,63 %. Additionnées, les lignes du tableau par pays qui correspondent à des États membres de l'Union (France, Belgique, Autriche, Pays-Bas, Grèce, Pologne, Lettonie, Irlande) totalisent environ 3,07 % des domaines mesurés. Le reste du continent européen se résume pour l'essentiel au Royaume-Uni, à 6,59 %.

La conclusion du rapport ne cache pas la portée de ces chiffres. Elle note que l'adoption massive de TLS 1.3 est tempérée par la concentration des certificats auprès d'autorités américaines, et invite les acteurs, au nom de l'évolution du contexte international, à identifier leurs dépendances géographiques et à chercher à les réduire. Le constat est donc posé par l'institution elle-même. Ce qui reste à établir, c'est la nature exacte de cette dépendance, et la raison pour laquelle aucun des instruments que l'État mobilise ailleurs ne s'y applique.

Une ressource vitale, concentrée et soumise à la discrétion d'autrui

> **La dépendance envers les ressources (Pfeffer et Salancik, 1978)**
>
> Dans *The External Control of Organizations: A Resource Dependence Perspective* (Harper & Row, 1978, réédité par Stanford Business Books en 2003), Jeffrey Pfeffer et Gerald R. Salancik soutiennent que le comportement d'une organisation s'explique moins par ses objectifs propres que par les acteurs extérieurs qui contrôlent les ressources dont elle a besoin. La *dépendance* d'une organisation envers une autre tient à trois facteurs : l'importance de la ressource pour son fonctionnement et sa survie, la latitude dont dispose le détenteur pour en décider l'allocation et l'usage, et la concentration de son contrôle, c'est-à-dire la rareté des sources de substitution. Le pouvoir du détenteur est l'envers de cette dépendance. Les organisations dépendantes cherchent à la gérer en s'adaptant, en négociant, en s'alliant, ou en agissant sur leur environnement par le droit et l'action politique.

Le cadre de Pfeffer et Salancik a l'intérêt de ne pas confondre dépendance et dépense. Une ressource peut peser très peu dans les comptes et commander pourtant toute l'activité. Les trois facteurs s'appliquent ici sans forçage.

L'importance de la ressource ne fait pas débat. Le rapport rappelle que la validité du certificat présenté par le serveur est au cœur de la sécurité du protocole : sans elle, le navigateur ne peut établir que le site interrogé est bien celui qu'il prétend être. Pour un téléservice public, une banque ou une mutuelle, un certificat expiré ou révoqué ne dégrade pas le service, il l'interrompt aux yeux de l'usager. Le certificat pèse très peu dans les échanges et conditionne pourtant tout le reste : c'est le cas que la théorie isole lorsqu'elle sépare le poids d'une ressource dans les comptes de son caractère critique.

La concentration est mesurée par le rapport lui-même, et elle atteint un niveau rare pour une ressource d'infrastructure. Elle se comprend au regard de la nature de l'offre dominante. Let's Encrypt est le service de l'Internet Security Research Group, une organisation à but non lucratif constituée en Californie, qui délivre gratuitement des certificats émis de façon automatisée. Son rapport annuel 2025 fait état de 762 millions de sites desservis, contre 492 millions un an plus tôt, et de fréquemment plus de huit millions de certificats émis par jour. Le service est financé par des entreprises sponsors, des subventions et des dons. La gratuité et l'automatisation ont accompagné la généralisation du chiffrement que mesure l'observatoire. Elles ont aussi installé un émetteur dominant que nul contrat ne relie à ceux qui en dépendent.

La discrétion, enfin, se lit dans le calendrier des règles. L'Internet Security Research Group fixe seul la durée de vie de ses certificats : son rapport annonce un profil ramené par défaut à 45 jours à compter du 13 mai 2026, un passage du profil classique à 64 jours le 10 février 2027, puis une configuration finale à 45 jours le 16 février 2028. Ces décisions s'inscrivent dans un mouvement plus large. Le 11 avril 2025, le CA/Browser Forum (l'instance où autorités de certification et éditeurs de navigateurs fixent les exigences de base des certificats web) a adopté le scrutin SC-081, proposé par Apple, qui réduit la durée maximale de validité de 398 à 47 jours entre mars 2026 et mars 2029. Les quatre « consommateurs de certificats » appelés à voter, Apple, Google, Microsoft et Mozilla, ont tous voté pour, de même que vingt-cinq émetteurs, parmi lesquels les français Certigna et Certinomis. Le forum ne compte que ces deux collèges : aucun gestionnaire de site, public ou privé, n'y vote. Chacun devra pourtant renouveler ses certificats plusieurs fois par an, et donc automatiser une opération qui était annuelle.

Les trois conditions d'une dépendance forte sont ainsi réunies. Le cas présente en outre une particularité que le cadre de 1978 aide à voir. Dans la relation classique entre une organisation et son fournisseur, le prix est le lieu où la dépendance se négocie : le contrat, la clause de réversibilité, la mise en concurrence sont les contrepoids ordinaires du client. Une ressource gratuite supprime ce lieu. Le gestionnaire du site n'est pas un client dont la défection inquiète, il est un bénéficiaire, et sa seule option est de partir.

Le certificat se remplace, la confiance ne se négocie pas

Cette option existe, et le rapport la recommande. Pour TLS, l'observatoire conseille « de ne pas dépendre d'une seule autorité de certification » et de prévoir des procédures de remplacement rapide des certificats. Le conseil suppose que la ressource est substituable, et il a raison sur ce point précis : d'autres émetteurs délivrent des certificats techniquement équivalents, et le changement d'émetteur est une opération ordinaire pour un service qui l'a préparée.

Mais l'émission n'est pas la ressource décisive. Le rapport décrit lui-même le mécanisme qui la rend utile : le certificat présenté par un serveur n'est valide que s'il forme une chaîne de signatures remontant à une racine de confiance, et pour les navigateurs web ces racines correspondent généralement à un registre public, tel que le magasin de certificats maintenu par Mozilla pour Firefox, d'autres applications s'en remettant à celui du système d'exploitation. Un émetteur, quel que soit son pays, n'existe pour le visiteur que s'il figure dans ces magasins. Leur composition et leurs règles d'admission relèvent de quelques éditeurs, les mêmes qui ont voté seuls, côté consommateurs, la réduction des durées de validité.

La dépendance se dédouble donc. Celle qui porte sur l'émetteur, mesurée par l'observatoire, est forte mais réductible par la diversification. Celle qui porte sur la confiance, que l'observatoire décrit sans la mesurer, est d'une autre nature : elle ne se réduit pas en changeant d'émetteur, puisque tout émetteur de remplacement doit lui-même être admis par les mêmes programmes. Dans les termes de Pfeffer et Salancik, la concentration du contrôle n'est pas au niveau du fournisseur de certificats, elle est au niveau de ceux qui décident quels fournisseurs comptent.

La mesure par pays de l'émetteur comporte d'ailleurs une limite qui va dans le même sens. Elle classe un certificat selon l'autorité qui l'a signé en dernier, pas selon la racine dont cette autorité tient sa propre validité. En mai 2020, une page d'incident publiée par Gandi montrait que son autorité émettrice, « Gandi Standard SSL CA 2 », était rattachée à la racine « USERTrust RSA Certification Authority », que Sectigo présente comme l'une de ses racines. Rien dans le tableau de 2026 ne permet de savoir à quelle racine se rattachent aujourd'hui les 1,58 % attribués au registraire français. La part nationale mesurée est donc un plafond plutôt qu'un plancher.

Décembre 2013 : une racine d'État découvre qu'elle est invitée

Un précédent français montre ce que signifie concrètement cette seconde dépendance. Le 7 décembre 2013, Adam Langley, ingénieur sécurité de Google, publie sur le blog de sécurité de l'entreprise le récit d'une découverte faite le 3 décembre au soir : des certificats non autorisés pour plusieurs domaines de Google, émis par une autorité intermédiaire rattachée à l'ANSSI. Selon ce billet, l'agence a établi que le certificat intermédiaire avait été installé dans un équipement commercial, sur un réseau privé, pour inspecter du trafic chiffré, en violation de

ses procédures. L'avis de sécurité publié ensuite par Mozilla précise que le certificat intermédiaire avait été émis par une autorité subordonnée de l'ANSSI, agence gouvernementale membre du programme de racines de Mozilla, et installé sur un équipement de surveillance réseau capable d'intercepter le trafic de domaines que son titulaire ne détenait pas.

La réponse est venue des éditeurs, et chacun l'a fixée seul. Google met à jour immédiatement les données de révocation de Chrome pour bloquer l'autorité intermédiaire, puis annonce, dans une mise à jour du 12 décembre, que la racine de l'ANSSI sera restreinte dans une version ultérieure de Chrome aux domaines de premier niveau français : .fr, .gp, .gf, .mq, .re, .yt, .pm, .bl, .mf, .wf, .pf, .nc et .tf. Le 9 décembre, Kathleen Wilson, responsable du module des certificats d'autorité chez Mozilla, annonce la révocation de la confiance accordée au certificat intermédiaire dans Firefox 26 et Firefox ESR 24, et renvoie toute autre mesure visant cette autorité au forum public de la politique de sécurité de Mozilla. L'avis MFSA 2013-117, daté du 10 décembre, enregistre la correction dans Firefox, Thunderbird et SeaMonkey.

La faute, en l'occurrence, était française, et la réaction des éditeurs relevait de leur rôle de gardiens de la confiance. C'est précisément ce qui rend le précédent instructif : il ne met en cause aucun abus, il montre une architecture. Pour une infrastructure de confiance opérée par l'État, l'étendue de la validité a été redéfinie en quelques jours par une entreprise privée étrangère, selon une procédure qu'elle maîtrisait seule, sans autre recours que la discussion publique ouverte par Mozilla. Le périmètre dans lequel la racine de l'État français restait reconnue par Chrome a été tracé par Google. L'épisode illustre exactement la discrétion sur l'allocation que décrivent Pfeffer et Salancik : le détenteur de la ressource ne se contente pas de la fournir ou de la retirer, il en fixe les conditions d'usage. Treize ans plus tard, la question n'est plus seulement celle des racines publiques. Elle concerne les trois quarts des sites du .fr, qui reposent sur un émetteur et des programmes de confiance sur lesquels aucune autorité française n'a de prise contractuelle.

Bruxelles a choisi la voie politique, l'observatoire en reste à l'hygiène

Le cadre de 1978 distingue deux familles de réponses à une dépendance. Les premières sont individuelles : s'adapter, diversifier ses sources, négocier. Les secondes sont politiques : modifier l'environnement lui-même par le droit. L'Union européenne a emprunté la seconde voie. Le règlement (UE) 2024/1183 du 11 avril 2024, qui révise le cadre eIDAS, dispose dans son article 45 que les certificats qualifiés d'authentification de site internet, délivrés par des prestataires qualifiés européens, « sont reconnus par les fournisseurs de navigateurs internet ». Son article 45 bis encadre les mesures conservatoires que les navigateurs peuvent encore prendre contre ces certificats : elles ne sont admises qu'en cas de préoccupations étayées touchant la sécurité ou l'intégrité, doivent être notifiées par écrit à la Commission, à l'organe de contrôle, au titulaire et au prestataire, et l'organe de contrôle peut en demander la

levée après enquête.

Le texte codifie ainsi la situation de décembre 2013. La sanction unilatérale d'un éditeur devient une mesure motivée, notifiée et contestable devant une autorité publique. C'est la stratégie que Pfeffer et Salancik prêtent aux organisations qui ne peuvent réduire leur dépendance par le marché : obtenir de la puissance publique qu'elle contraigne le détenteur de la ressource. Mais le considérant 65 du même règlement précise que l'utilisation de ces certificats par les sites internet devrait être volontaire. Le droit européen garantit la reconnaissance d'une ressource européenne, il n'organise pas son emploi. Avec environ 3 % des domaines .fr mesurés servis par des émetteurs établis dans l'Union, l'instrument existe sans que la demande se soit déplacée.

Le rapport de l'observatoire ne fait pas le lien. Ses recommandations, regroupées par protocole, sont adressées aux opérateurs de réseaux, aux gestionnaires de zones DNS et aux responsables de services de messagerie et de sites web. Pour le routage, il conseille de diversifier les liens de transit, notamment avec des opérateurs européens. Pour les certificats, il conseille de ne pas dépendre d'une seule autorité, sans qualifier l'alternative. Dans le texte du rapport, les certificats qualifiés du règlement eIDAS ne sont pas mentionnés, et aucune recommandation ne s'adresse à un acheteur ou à une administration en tant que telle. La concentration est décrite comme une affaire de bonne pratique d'ingénierie, à corriger site par site.

C'est l'angle mort. Le débat français sur la souveraineté numérique s'est construit autour d'objets qui s'achètent : les offres d'informatique en nuage, soumises à qualification, les suites bureautiques, dont les marchés sont désormais contrôlés, les logiciels, dont la commission d'enquête parlementaire sur les dépendances numériques a proposé de rendre le libre obligatoire dans la commande publique (comme l'a analysé la chronique du 4 septembre 2026 consacrée au rapport n° 3054). Ces instruments ont un point commun : ils agissent au moment de l'achat. La couche de confiance du web n'a pas de moment d'achat. Un certificat gratuit, émis automatiquement par un serveur, ne laisse de trace dans aucun marché public, aucune ligne budgétaire, aucun avis de la direction interministérielle du numérique. La dépendance la plus complète que mesure le rapport est ainsi celle qui échappe le plus complètement aux leviers que l'État s'est donnés. Dans le cadre de Pfeffer et Salancik, une telle situation ne laisse au dépendant que la voie politique : là où aucune transaction n'offre de prise, la réduction de la dépendance devient une question d'organisation collective plutôt que de vigilance individuelle.

Ce que mesurera la prochaine édition

Le titre de cette chronique tenait en une proposition : la dépendance des sites français envers les autorités de certification américaines est celle que l'État n'achète pas. L'analyse en a précisé les deux étages. Le premier, la concentration des émetteurs, est spectaculaire mais

réductible, et le rapport en propose le remède. Le second, la maîtrise des programmes de confiance des navigateurs, est moins visible et ne se réduit ni par l'achat ni par la diversification, seulement par le droit, comme l'Union l'a tenté et comme l'épisode de 2013 en avait montré l'enjeu. Entre les deux, la gratuité joue un rôle paradoxal : elle a rendu le chiffrement universel en supprimant le lieu où une dépendance se négocie d'ordinaire.

L'hypothèse que cette lecture permet de formuler est vérifiable sans information interne. Tant que la diversification des autorités de certification reste une recommandation adressée aux gestionnaires de sites, sans traduction dans les règles que l'État s'applique à ses propres services en ligne ni dans les recommandations de l'observatoire, la structure mesurée en 2026 ne bougera pas de manière significative. Deux indicateurs permettront de le constater. Le premier est le tableau « Code pays de l'émetteur » de la prochaine édition du rapport : si celle-ci paraît d'ici le 31 décembre 2028, la part cumulée des émetteurs établis dans l'Union devrait y rester inférieure à 5 % des domaines mesurés, et celle de Let's Encrypt supérieure à 70 %. Le second est le texte des recommandations de cette même édition : l'hypothèse sera infirmée si elles mentionnent les certificats qualifiés de l'article 45 du règlement eIDAS ou s'adressent explicitement aux administrations. Si aucune nouvelle édition n'a paru à cette date, le constat sera d'une autre nature, mais il dira la même chose : une dépendance mesurée une fois par décennie n'est pas encore devenue un objet de gouvernement.

Note méthodologique

Les chiffres proviennent du rapport « Résilience de l'Internet français » 2026 (Afnic et ANSSI). Le texte du rapport parle de part « des certificats » quand ses tableaux sont exprimés en « pourcentage de domaines » : l'auteur a retenu la lecture par domaines mesurés, seule compatible avec les tableaux, et a calculé lui-même la part cumulée des émetteurs établis dans l'Union à partir du tableau par pays. Les sources publiques divergent sur la date de publication (présentation publique le 2 novembre 2026, publication datée du 3 novembre par la presse spécialisée, annonce sur le site de l'Afnic datée du 17 novembre) : la date de présentation a été retenue. Les affirmations d'absence relatives aux recommandations sont bornées au texte intégral du rapport. Le choix de distinguer dépendance envers l'émetteur et dépendance envers les programmes de confiance relève de l'interprétation de l'auteur. Recherche de sources, croisement des données et structuration du raisonnement s'appuient sur une assistance par intelligence artificielle. Le choix de l'angle et du cadre théorique, la vérification des sources, les arbitrages et l'établissement du texte final relèvent de l'auteur.

Sources

Sources primaires institutionnelles

- Afnic et ANSSI, « Résilience de l'Internet français », édition 2026, rapport de l'Observatoire de la résilience de l'Internet français, annoncé le 17 novembre 2026. https://www.afnic.fr/

wp-media/uploads/2026/11/Rapport-2026-de-lObservatoire-de-la-resilience-de-linternet-francais.pdf

- Afnic, « L'ANSSI et l'Afnic publient le rapport 2026 de l'Observatoire de la Résilience de l'Internet », 17 novembre 2026. https://www.afnic.fr/observatoire-ressources/actualites/lanssi-et-lafnic-publient-le-rapport-2026-de-lobservatoire-de-la-resilience-de-linternet/
- Afnic, « JCSA26 : Journée du Conseil scientifique de l'Afnic 2026 », programme de la journée du 2 novembre 2026, page consultée le 17 novembre 2026. https://www.afnic.fr/observatoire-ressources/agenda/jcsa26-journee-du-conseil-scientifique-de-lafnic-2026/
- Afnic, « Rapport 2016 de l'Observatoire de la résilience de l'Internet français », 29 septembre 2017. https://www.afnic.fr/observatoire-ressources/actualites/rapport-2016-de-lobservatoire-de-la-resilience-de-linternet-francais/
- ANSSI, « Observatoire de la résilience de l'Internet français », page de l'observatoire, consultée le 17 novembre 2026. https://cyber.gouv.fr/nous-connaitre/ecosysteme/recherche-anssi/observatoire-de-la-resilience-de-linternet-francais/

Textes normatifs et règles du secteur

- Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique, Journal officiel de l'Union européenne, L, 30 avril 2024 (considérant 65, articles 45 et 45 bis). https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1183
- CA/Browser Forum, « Ballot SC081v3: Introduce Schedule of Reducing Validity and Data Reuse Periods », résultats du vote clos le 11 avril 2025. https://cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-reducing-validity-and-data-reuse-periods/
- Internet Security Research Group, « 2025 Annual Report », document consulté le 17 novembre 2026. https://www.abetterinternet.org/documents/2025-ISRG-Annual-Report.pdf

Parallèle historique

- Adam Langley (Google), « Further improving digital certificate security », Google Online Security Blog, 7 décembre 2013 (mise à jour du 12 décembre 2013). https://security.googleblog.com/2013/12/further-improving-digital-certificate.html
- Kathleen Wilson (Mozilla), « Revoking Trust in one ANSSI Certificate », Mozilla Security Blog, 9 décembre 2013. https://blog.mozilla.org/security/2013/12/09/revoking-trust-in-one-anssi-certificate/
- Mozilla, « Mozilla Foundation Security Advisory 2013-117: Mis-issued ANSSI/DCSSI

certificate », 10 décembre 2013. https://www.mozilla.org/en-CA/security/advisories/mfsa2013-117/

- Gandi, « Sectigo AddTrust External CA Root Expiring May 30, 2020 », rapport d'incident, 29 mai 2020. https://status.gandi.net/incidents/026k81gp3vmk
- Sectigo, « Sectigo Chain Hierarchy and Intermediate Roots », base de connaissances, page consultée le 17 novembre 2026. https://www.sectigo.com/knowledge-base/detail/Sectigo-Chain-Hierarchy-and-Intermediate-Roots/kA01N000000rgSZ

Chroniques liées

- ElegArtech, « Souveraineté numérique : le rapport n° 3054 fait de l'open source une obligation, et chiffre la dépendance que dix ans de discours n'avaient pas nommée », 4 septembre 2026. https://elegartech.fr/articles/souverainete-numerique-le-rapport-n-3054-fait-de-l-open-source-une-obligation-et-chiffre-la-dependance-que-dix-ans-de-discours-n-avaient-pas-nommee

Cadre théorique

- Jeffrey Pfeffer et Gerald R. Salancik, *The External Control of Organizations: A Resource Dependence Perspective*, New York, Harper & Row, 1978, réédition Stanford, Stanford Business Books, 2003.