Certification et registars

Certification

Les échanges sur Internet sont sécurisés à l'aide du chiffrement : HTTPS, VPN, SSH, etc.

Cette sécurité repose sur des certificats. Un certificat comprend :

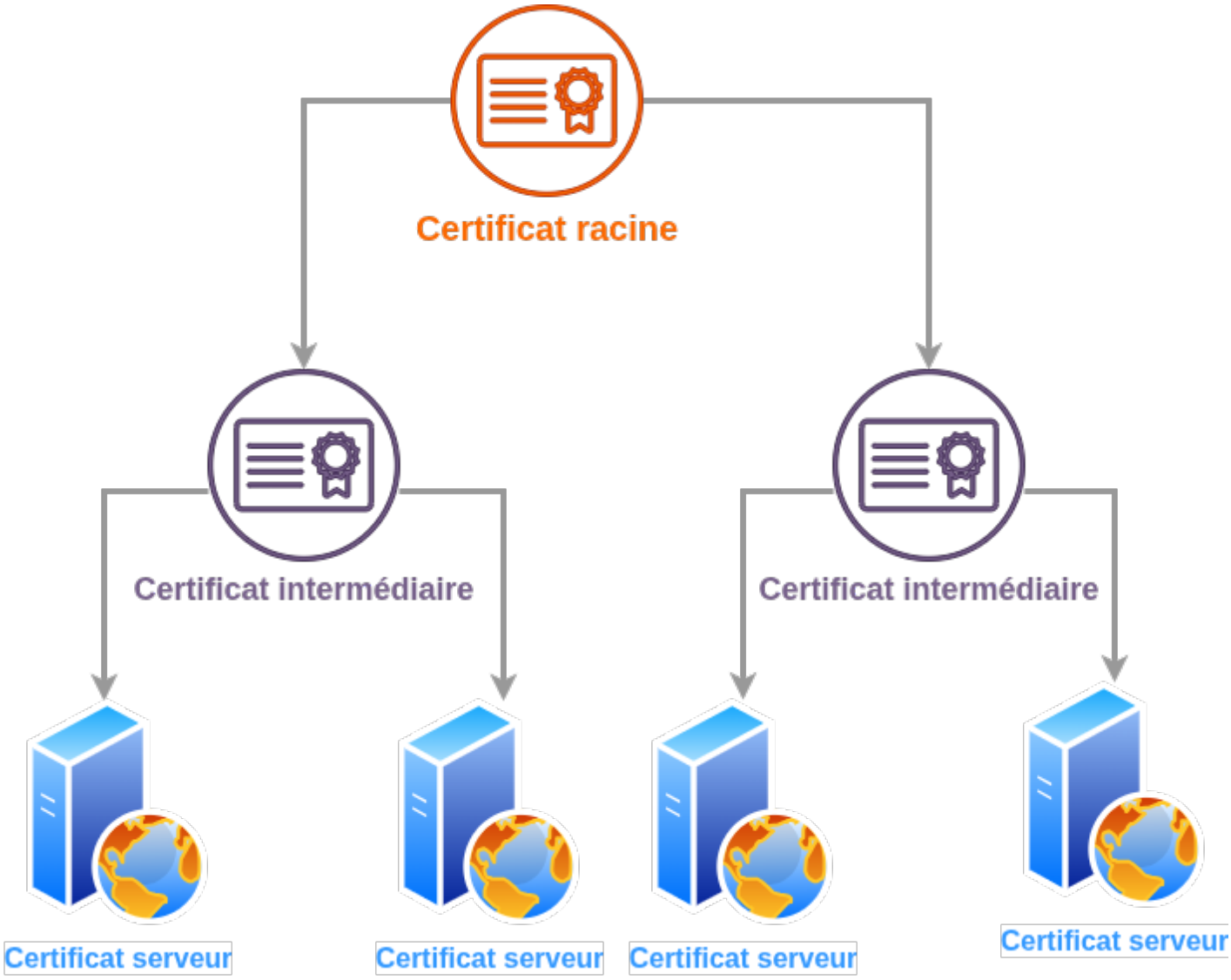
- Le nom de domaine
- La clé publique du serveur
- Sa période de validité
- La signature d'une autorité de certification (CA)

> La signature de l'autorité de certification est cruciale : elle prouve que le certificat provient d'une entité de confiance reconnue par les navigateurs.

Chaîne de délégation

La confiance dans un certificat repose sur une chaîne de certification.

Celle-ci commence par une autorité racine, dont le certificat est auto-signé et intégré dans les systèmes d'exploitation et navigateurs. Cette autorité racine délègue ensuite la signature des certificats à des autorités intermédiaires, qui émettent les certificats utilisés par les sites web.



Ce modèle permet de limiter les risques : en cas de compromission d'une autorité intermédiaire, il est possible de la révoquer sans affecter l'ensemble de l'écosystème.

La création ou le renouvellement d'un certificat racine est une opération hautement sensible qui nécessite des conditions de sécurité physique et logique très strictes. Généralement, les clés cryptographiques sont transportées de manière sécurisée et générées dans un environnement fermé, blindé et isolé du réseau.
Plusieurs témoins sont présents tout au long du processus afin de garantir la traçabilité et la transparence des opérations.

> Ce niveau de précaution est indispensable car la compromission d'une autorité racine mettrait en danger la confiance de l'ensemble des connexions sécurisées sur Internet.

Voir article dédié chez Cloudflare :

https://www.cloudflare.com/fr-fr/learning/dns/dnssec/root-signing-ceremony/

Letsencrypt

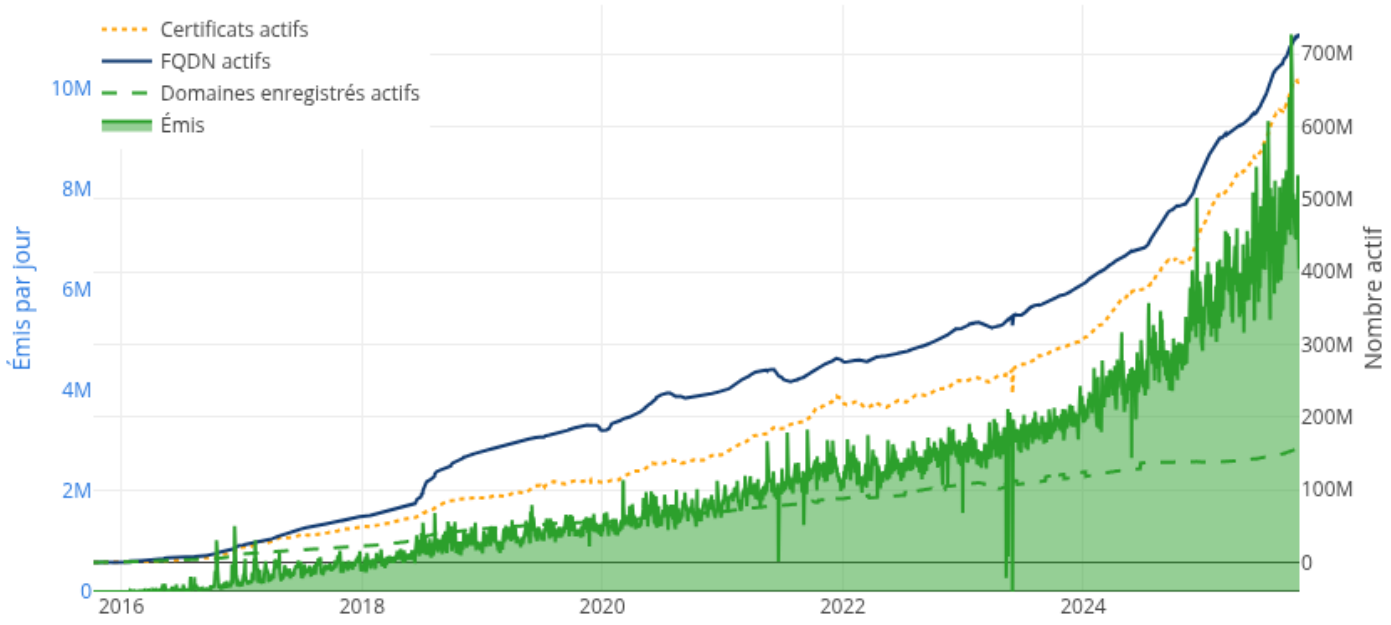
Lancée en 2015 par l'**Internet Security Research Group,** Let's Encrypt est une autorité de certification gratuite, automatisée et ouverte.

Son objectif est de démocratiser l'usage du HTTPS en **supprimant les barrières techniques et financières**.

Les certificats émis par Let's Encrypt sont reconnus par les navigateurs, car l'autorité est signée par une chaîne de confiance incluant l'autorité racine ISRG Root X1.

La popularité de Letsencrypt est incontestable.

https://letsencrypt.org/fr/stats-dashboard/



Registars français

Registar	Volumétrie
OVHCloud	~ 5 millions de domaines
LWS	~ 800k domaines
Gandi	~2,5 millions de domaines (2019)

Registar	Volumétrie
Netim	-
Scaleway (Illiad)	-
O2switch	~ 500k domaines
Ikoula	-

Revision #13
Created 2 October 2025 21:17:40 by Thibaud FRICHET
Updated 21 October 2025 20:30:35 by Thibaud FRICHET