Table des matières

Ajouter les certificats X.509 manquants

Les autorités de certification fonctionnent sur un mode arborescent. Pour pouvoir vérifier un certificat, il faut que le magasin contienne la chaîne complète certificat racine et certificats intermédiaires éventuels. Le Cnam utilise le service TCS pour les signer les certificats des serveurs publics.

Depuis le mois de janvier 2025, le fournisseur de TCS est Harica. Ses certificats racine sont généralement déjà préinstallés :

- HARICA TLS ECC Root CA 2021
- HARICA TLS RSA Root CA 2021

Pour TCS, ajouter :

- GEANT TLS ECC 1
- GEANT TLS RSA 1

sur Linux

Sur Debian et Ubuntu :

- s'assurer que le paquetage `ca-certificates` est installé et à jour
- déposer les fichiers dans `/usr/local/share/ca-certificates` et lancer la commande `update-ca-certificates(8)` (avec l'identité de `root`).

Sur les systèmes basés sur Red Hat :

- s'assurer que le paquetage `ca-certificates` est installé et à jour
- déposer les fichiers dans `/etc/pki/ca-trust/source/anchors` et lancer la commande `update-ca-trust(8)` (avec l'identité de `root`).

sur macOS

Ouvrir l'application « Trousseau d'accès » (dans `/System/Applications/Utilities`, `Keychain.app`) depuis un compte d'administration. Importer dans le trousseau « Système » les certificats.

sur Windows

🔧 Fix Me!

Les deux certificats racine ECC sont assemblés dans le fichier harica_chain.pem (par exemple pour eduroam).