Migration des certificats sur la PNCN

Remplacement des certificats RACINE AGRIATES par ceux de la Plateforme National de Confiance Numérique

Fabrice Barconnière

Pôle de Compétences Logiciels Libres

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'ÉDUCATION NATIONALE,
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE

EOLE

Migration des certificats sur PNCN

Déroulement de la présentation.

- Comment faire
- Démonstration
- Procédure de renouvellement (Toulouse)
- Questions/Réponses

Migration des certificats sur PNCN

- Micros coupés durant la présentation.
- Chat : https://webchat.freenode.net
  - Canal #eolevisio
  - Cocher « je ne suis pas un robot »

Migration des certificats sur PNCN

But :

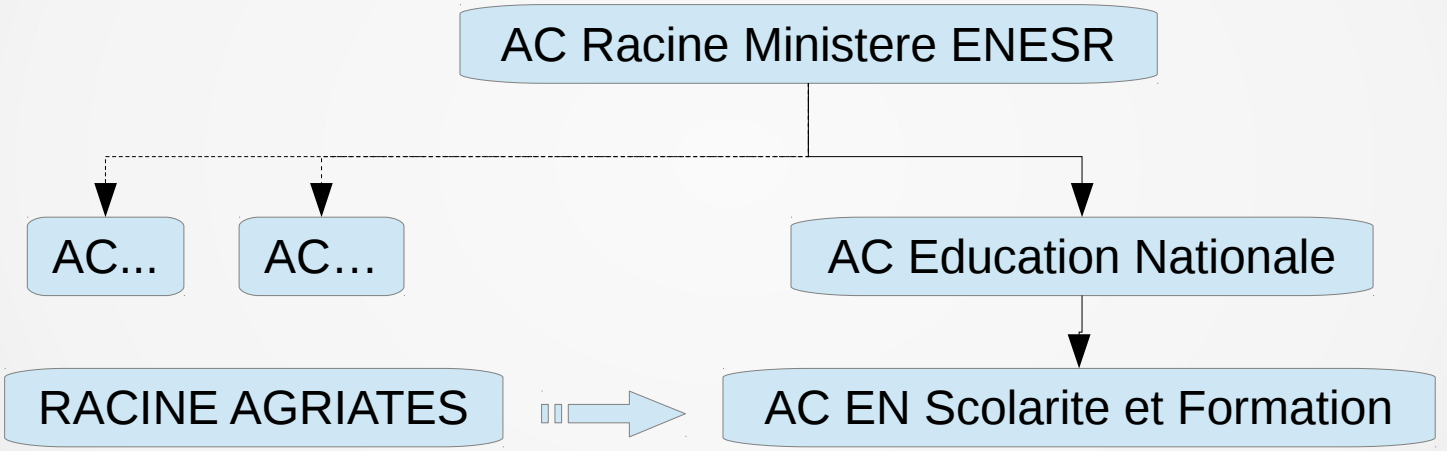
- Mise en conformité selon les préconisations de l'ANSSI
- Utiliser des certificats sha2

Prérequis :

- Sphynx 2.4.2 (2.5.2 bientôt stable)
- Amon 2.4.0 minimum (2.5 recommandé)

Paramétrage du serveur Sphynx

Le serveur doit être paramétré pour être conforme à l'IGC PNCN.



Lancer **gen_config** pour vérifier et adapter la configuration.

Paramétrage du serveur Sphynx

Onglet Vpn-pki

- **Utiliser la PKI PNCN** : **oui**
- **Localité (L=)** : renseigner une **ville**
- **Nom de l'organisation (O=)** : **Education Nationale**
- **Nom de l'unité de l'organisation (OU=)**, 2 valeurs :
  - **0002 110043015** et **Academie de ....**
- **URL des listes de révocation de certificats (sinon rien)**
  - optionnel, listes présentes dans chaque certificat

Paramétrage du serveur Sphynx

Paramétrage du serveur Sphynx

Lancer **reconfigure** pour prendre en compte ces modifications.

Cela permet de :

- générer une configuration openssl conforme pour les requêtes de certificats auprès de la PNCN
- configurer ARV pour forcer un suffixe DNS au CN du certificat lors de la génération d'une requête

Mise à niveau des serveurs EOLE

Le serveur Sphynx doit être en version 2.4.2 minimum.

Le serveur Sphynx doit être mis à niveau avant les Amon.

Les serveurs Amon doivent être en version 2.4.x minimum.

- Plusieurs situations possibles
- Plusieurs scénarios possibles

Mise à niveau des serveurs EOLE

- Vous disposez d'un Sphynx version 2.2 ou moins :
  - Réinstallation du serveur Sphynx

- Vous disposez d'un Sphynx 2.3, 2.4.0 ou 2.4.1, 3 choix :
  - Réinstallation du serveur Sphynx
  - Migration du serveur existant
  - Sauvegarde + réinstallation + restauration

Mise à niveau des serveurs EOLE

- Vous disposez de serveurs Amon version 2.2 ou moins :
  - Réinstallation du serveur au moment du passage à la PNCN
- Vous disposez de serveurs Amon 2.3, 2 choix :
  - Réinstallation du serveur
  - Migration du serveur existant

Mise à niveau des serveurs EOLE

Durées des migrations (procédure **Upgrade-Auto**) :

- Amon/Sphynx 2.3 vers Amon/Sphynx 2.4.2 : 1 heure
- Amon/Sphynx 2.4.x vers Amon/Sphynx 2.4.2 : 5 à 10 minutes

Durées des installations :

- Compter 1 heure environ
- Pour Amon, penser à sauvegarder les logs

Mise à niveau des serveurs EOLE

Opérations post-migration :

- **reboot**
- **gen_config** avec connexion Zéphir (adapter la configuration sur Sphynx)
- **instance**
- Régénérer la configuration IPsec :
  - Pour Sphynx : se connecter sur ARV et cliquer sur **Appliquer**
  - Pour Amon : lancer **active_rvp init** (un redémarrage de bastion peut-être nécessaire la première fois)

Prise en compte de la PNCN

Dans ARV, un modèle de lien associé à l'autorité de certification **AC EN Scolarite et Formation** doit exister.

Sur une primo installation d'un serveur Sphynx 2.4.2 :

- enregistrer le serveur sur Zéphir
- lancer le script **init_sphynx** pour créer le modèle de lien

Prise en compte de la PNCN

Sur un serveur Sphynx déjà en production, encore configuré pour **RACINE AGRIATES** (migration ou réinstallation) :

- configurer le serveur pour utiliser la PNCN
- lancer le script **init_pncn** pour :
  - cloner les modèles de liens existants associés à l'AC **RACINE AGRIATES**
  - associer **AC EN Scolarite et Formation** à ces modèles clonés
  - renommer les modèles de liens existants associés à l'AC **RACINE AGRIATES** en les préfixant par **OLD_PKI_**

Prise en compte de la PNCN

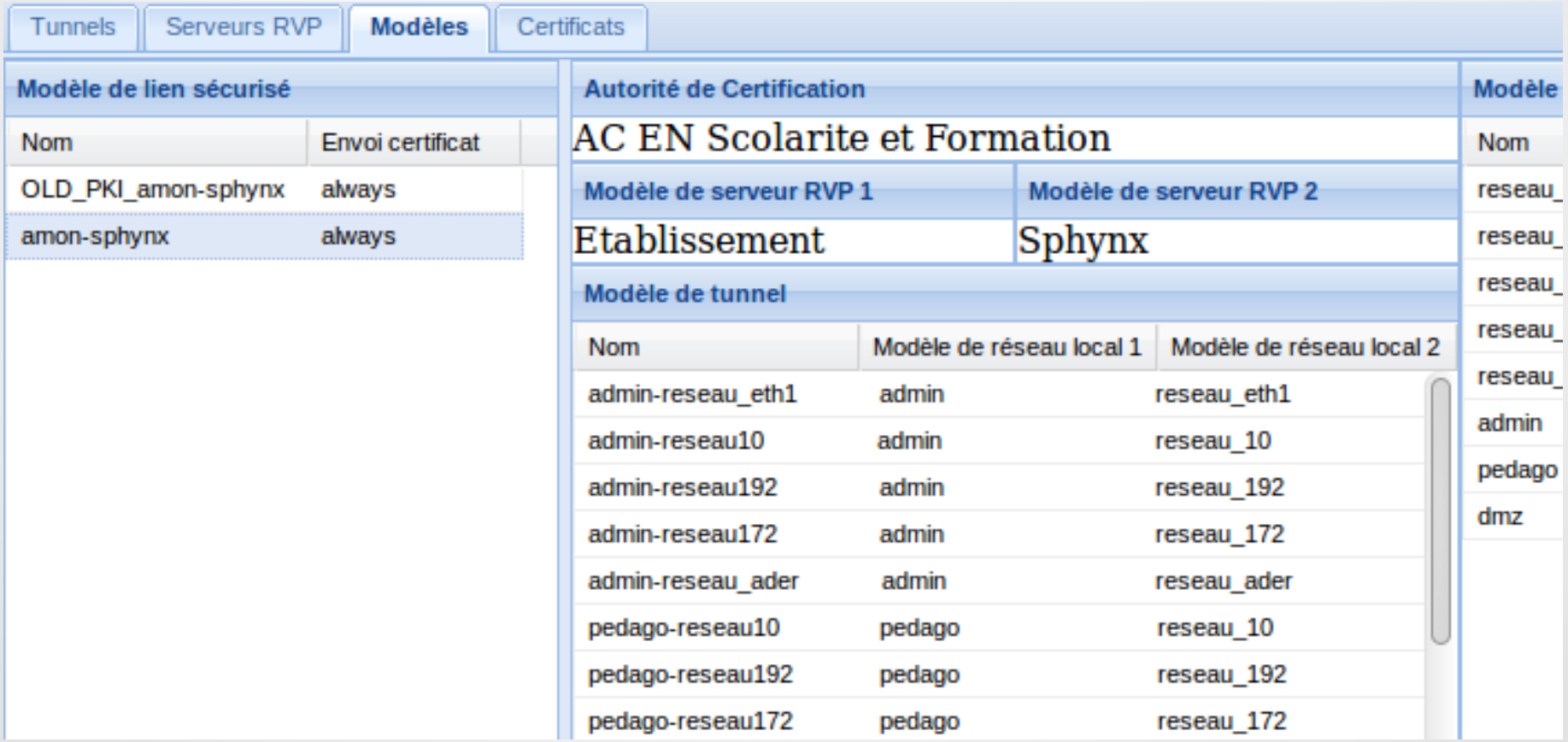
On pourra ainsi utiliser les deux PKI simultanément et procéder à une migration progressive.

Sphynx peut avoir des connexions VPN basées sur **RACINE AGRIATES** et **AC EN Scolarite et Formation**.

Plus possible d'effectuer des requêtes RACINE AGRIATES

Prise en compte de la PNCN

- Modèles de connexion



Importer les certificats PNCN en PKCS12

L'importation de fichiers pkcs12 n'est pas prévue dans ARV.

- Ce format inclus la chaîne de certification jusqu'au certificat final ainsi que la clé privée.

ARV peut importer les certificats et les clés privées mais dans des fichiers séparés.

- Il va falloir transformer ce fichier pksc12 en deux fichiers que ARV pourra importer.

Importer les certificats PNCN en PKCS12

Script de conversion disponible en téléchargement :

https://dev-eole.ac-dijon.fr/attachments/download/1550/split_pkcs12

Sphynx 2.4.2 : Passage à l'IGC PNCN

DEMO

Sphynx 2.4.2 : Passage à l'IGC PNCN

Démonstration pour une Sphynx en production :

- Connexion ARV mode « **RACINE AGRIATES** » :
  - montrer le modèle de lien
- Adapter la configuration de Sphynx
- Lancer le script **init_pncn**
- Connexion ARV mode « **PNCN »** :
  - montrer les modèles de lien
  - passer une connexion en **PNCN**
  - Activer le VPN sur Amon

Sphynx 2.4.2 : Passage à l'IGC PNCN

Procédure de renouvellement

DEMANDE DE CERTIFICAT SHA2
SCOLARITÉ ET FORMATION

- Directement sur l'Entité d'Enregistrement de la PNCN, par dépôt d'un p10
  - cf. Documentation : Certificat Scolarité et Formation

- Par demande auprès du pôle et génération automatique à partir des anciens certificats AGRIATES

  - Récupération des certificats SHA1
  - Génération d'un fichier CSV pilote par académie
  - Génération des p12 Scolarité et Formation
  - Envoi des mots de passe associés

DÉTAILS DU BATCH

- Envoi à chaque ISR d'académie d'un fichier pilote CSV pour

  - Suppression éventuelle de certificats à ne pas reconduire
  - Modification des « CN » si besoin, ne pas saisir de FQDN dans ce fichier
  - Modification du mail de contact si non renseigné ce sera isr@ac-academie.fr
  - Pas de caractères * dans les champs DNS (ou Subject Alternative Name)
  - Saisie de la ville, si aucune saisie, elle sera identique à la valeur « academie » de chacun des domaines ac-academie.fr
  - Modification éventuelle du pays (pour les TOM)

- Retour des CSV au pôle cf. Contacts diapo suivante
- Génération des p12 et mots de passe en fonction des retours
- Chaque p12 est envoyé au mail de contact du CSV précédemment rempli
- L'ensemble des mots de passe d'une académie sera envoyé à l'ISR correspondant quelque soit le mail de contact saisi dans le CSV isr@ac-academie.fr
- Ce mail sera chiffré avec la clé publique du certificat PNCN de chaque ISR
- Une documentation spécifique pour le déchiffrement sera mise à disposition sur le site du pôle

CONTACTS PNCN

- Documentations
  - Site du pôle PNCN
- Privilégier le mail
  - Support-pncn@education.gouv.fr et laurent.ruffie@ac-toulouse.fr
- Laurent Ruffié sera votre principal interlocuteur
  - Tel : 05.36.25.83.13

Licence

Cette présentation est mise à disposition sous licence Creative Commons by-nc-sa 2.0-fr

Attribution	Partage dans les mêmes conditions
Pas d'utilisation commerciale	France

Vous pouvez obtenir une copie de la licence :

- Par internet : https://creativecommons.org/licenses/by-nc-sa/2.0/fr/
- Par courrier postal : Creative Commons, 444 Castro Street, Suite 900 Mountain View, California, 94041, USA