Morgan Bissey

Table des matières

Table des matières 1
Présentation 1
1) Qu'est-ce que RADIUS ? 1
2) Fonctionnement 2
3) Recommandation de l'ANSSI 2
4) Protocole d'authentification 3
Procédure 4
1) Installation de l'autorité de certification 4
2) Installation du serveur NPS 10
3) Configuration du serveur NPS 10
Axes d'amélioration, mise en place de l'EAP-TLS 17
1) Certificat et auto-inscription, authentification EAP-TLS 17
a) Modification de la stratégie réseau sur le serveur NPS 17
b) Création des modèles pour l'auto-inscription 18
c) GPO pour les certificats 22
d) GPO pour le point d'accès Wifi 28

Présentation

1) Qu'est-ce que RADIUS ?

Développé 1991 pour devenir la norme de l'IETF, le protocole RADIUS (Remote Authentication Dial-In User Service) est un protocole réseau qui autorise et authentifie les utilisateurs qui accèdent à un réseau distant.

Le protocole fournit une gestion centralisée de l'authentification, de l'autorisation et de la comptabilité (protocole AAA) pour les utilisateurs se connectant à un réseau, empêchant les utilisateurs non autorisés d'accéder au réseau.

Il fonctionne sur un modèle client-serveur, où le serveur RADIUS gère les informations d'authentification, les autorisations et la comptabilisation, tandis que les clients RADIUS ou serveurs d'accès réseau (NAS) fournissent l'accès au réseau et envoient une

demande au serveur RADIUS. Son fonctionnement se rapproche du protocole LDAP (Lightweight Directory Access Protocol). Le protocole fonctionne sur les ports 1812 et 1813.

2) Fonctionnement

- Le processus commence lorsque l'utilisateur tente de se connecter au réseau via un client RADIUS/NAS. (La borne Wi-Fi ici)
- Ensuite, le client RADIUS/NAS envoie une requête d'accès au serveur RADIUS, incluant les identifiants de l'utilisateur qu'il vient de récupérer. Le serveur vérifie les identifiants à partir de sa base de données. En fonction de la vérification, le serveur envoie un message d'acceptation, de rejet, ou de contestation au client RADIUS/NAS.
- Le client RADIUS/NAS applique les attributs d'autorisation fournis par le serveur à la session de l'utilisateur. Des informations de comptabilité sont envoyées au serveur RADIUS pendant la session de l'utilisateur.

Bien que RADIUS soit largement utilisé, il présente des préoccupations de sécurité.

Il est possible d'atténuer ces préoccupations en implémentant des mesures de sécurité supplémentaires et en envisageant des protocoles AAA alternatifs (TACACS+) pour les environnements nécessitant une sécurité plus avancée. TACACS+ est l'abréviation de Terminal Access Controller Access-Control System Plus. L'avantage de ce protocole est que toutes les informations d'authentification, d'autorisation et de comptabilité sont chiffrées.

3) Recommandation de l'ANSSI

L'ANSSI indique qu'il est important de s'assurer que toute information sensible ou secrète échangée durant l'authentification (mot de passe, clé de session...) ne puisse pas être récupérée par un attaquant, au moyen d'une écoute passive ou d'une attaque active (attaque de l'homme du milieu par exemple).

Les méthodes d'authentification EAP-TLS, EAP-TTLS et EAP-PEAP dans ses dernières versions peuvent respecter les recommandations. En revanche, les méthodes d'authentification non encapsulées telles que EAP-MSCHAPv2 et EAPMD5 ne respectent pas cette recommandation

Recommandations :

- Utilisation d'une couche cryptographique standard ;
- Authentification mutuelle entre le supplicant et le serveur;

- Masquage de l'identité du supplicant durant la phase d'authentification, si le contexte le justifie.
- Utiliser une version de TLS récente et une suite cryptographique robuste.

Plusieurs modifications sont nécessaires pour garantir la disponibilité, l'intégrité et la confidentialité du SI. (Affectation de VLAN, ACL, cloisonnement des flux, supervision, blocage des adresses MAC inconnues)
En cas de perte ou de vol, modifier le mot de passe de l'utilisateur compromis est une solution pour se protéger.

4) **Protocole** d'authentification

Avec le protocole RADIUS est associé avec le protocole Extended Authentication Protocol qui sert pour le transport des données nécessaire à l'authentification. Le déploiement de l'IEEE 802.1X fournit une couche de sécurité pour l'utilisation des réseaux câblés et sans fil.

Ce protocole est extensible, car on peut définir de nouvelles méthodes d'authentifications, il est indépendant de la méthode utilisée :

- EAP-MD5 : Authentification avec un mot de passe
- EAP-TLS : Authentification avec un certificat électronique
- EAP-TTLS : Authentification avec n'importe quelle méthode d'authentification, au sein d'un tunnel TLS
- EAP-PEAP : Authentification avec n'importe quelle méthode d'authentification EAP, au sein d'un tunnel TLS
- EAP-TLS (Transport Layer Security) : Comme d'autres protocoles (SMTPTLS, IMAP-TLS, HTTPS, etc.), EAP s'appuie sur TLS pour proposer une authentification sécurisée. Cette méthode s'appuie sur les certificats électroniques. Ainsi, chaque partie (serveur et client) doit posséder un certificat pour prouver son identité.
- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) : Authentification Microsoft avec Hash du mot de passe. MS-CHAP v2 ajoute une authentification mutuelle client/serveur permettant de vérifier leur identité respective.

Nous avons donc décidé pour ASSURMER de mettre en place une connexion au Wi-Fi avec une authentification PEAP utilisant les identifiants AD avec un certificat émis par

l'autorité de certification d'ASSURMER qui permettra de vérifier l'identité du serveur NPS.

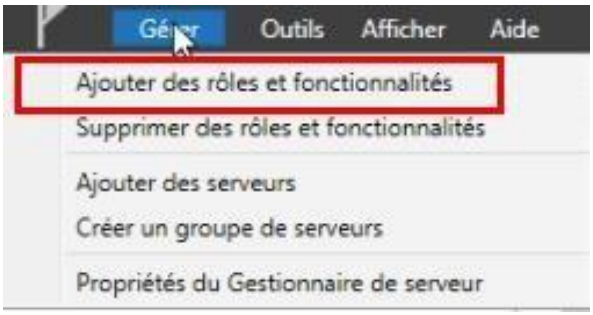
La mise en place de l'EAP-TLS fera l'objet d'un axe d'amélioration car les tests que nous avons réalisés n'ont pas tous été fructueux. Elle est considérée comme étant plus sécurisée, car c'est une méthode d'authentification mutuelle ou le client et serveur se prouvent respectivement leur identité. La méthode PEAP ne permet que de vérifier celle du serveur, permettant à n'importe quel client de se connecter, ouvrant donc une porte d'accès pour un attaquant. Cette méthode nécessite en plus de déployer un certificat client/ordinateur.

Procédure

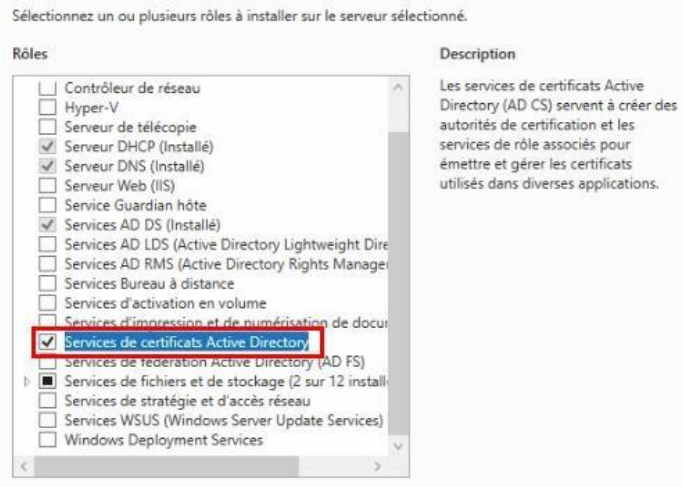
1) Installation de l'autorité de certification

ADCS va permettre de générer un certificat qui permettra aux clients de vérifier l'identité du serveur NPS. En cas de mise en place de l'EAP-TLS, il permettra de déployer un certificat sur les clients sans fil également.

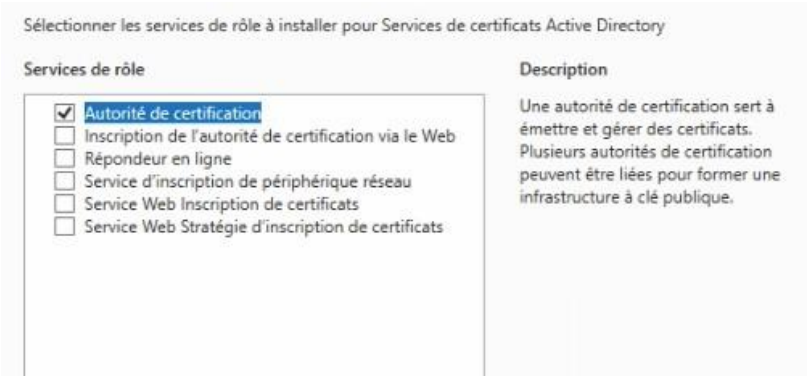
- Sur le DC01, cliquer sur « Gérer » puis « Ajouter des rôles et fonctionnalités ».



- Sélectionner « Services de certificats Active Directory ».

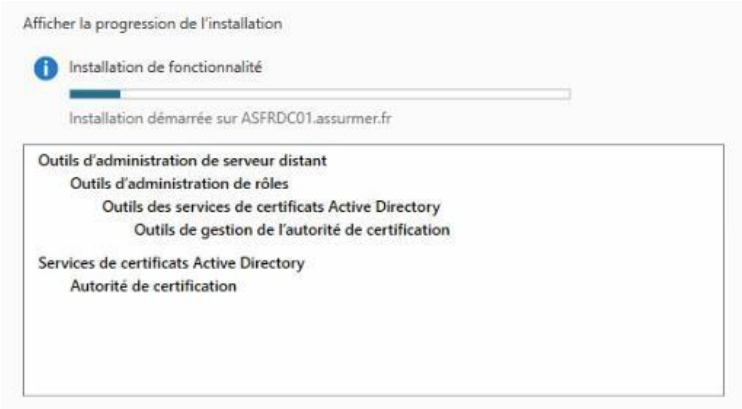


- Dans les « Services de rôles », cocher uniquement « Autorité de certification ».

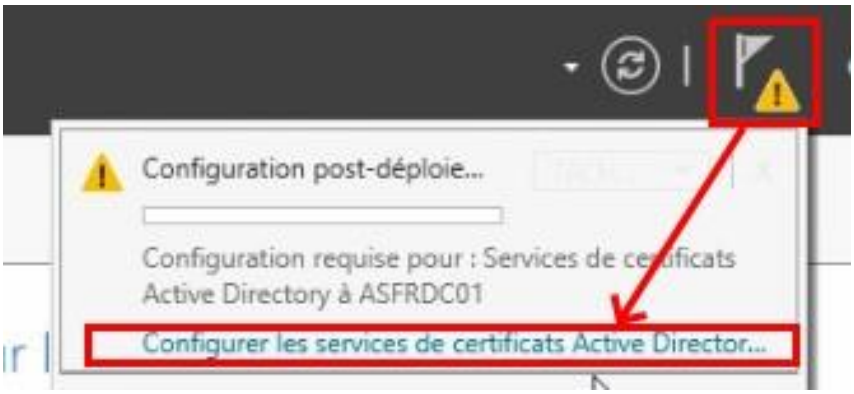

Sélectionner les services de rôle à installer pour Services de certificats Active Directory
Services de rôle
Autorité de certification
Inscription de l'autorité de certification via le Web
Répondeur en ligne
Service d'inscription de périphérique réseau
Service Web Inscription de certificats
Service Web Stratégie d'inscription de certificats
Description
Une autorité de certification sert à émettre et gérer des certificats. Plusieurs autorités de certification peuvent être liées pour former une infrastructure à clé publique.

-

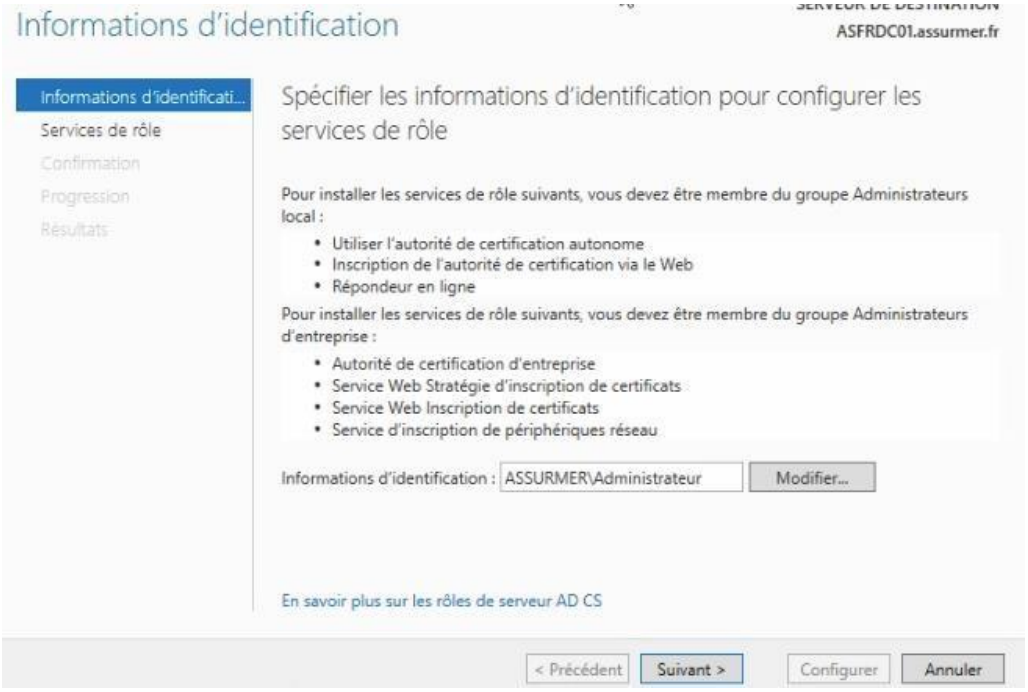
Lancer l'installation.



- Lancer la configuration post-déploiement en cliquant sur le drapeau.



- Dans « Informations d'identification », laisser par défaut.



-

Pour le « service de rôle », laisser par défaut.

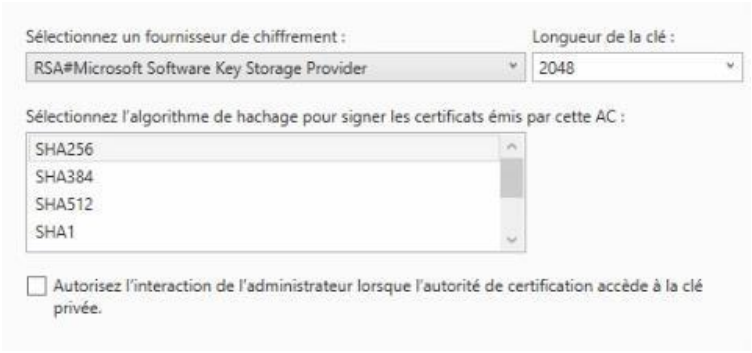
- Sélectionner « Autorité de certification de l'entreprise » dans le type d'installation de l'AC.

- Sélectionner « Autorité de certification racine » dans le type de l'AC.

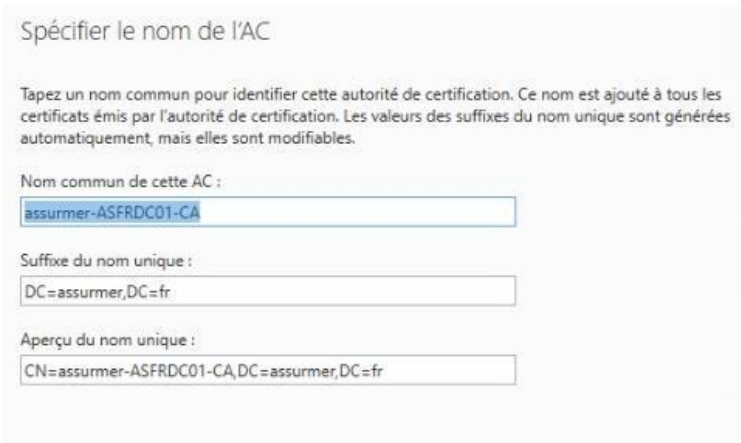
- Choisir « Créer un clé privée ».

-

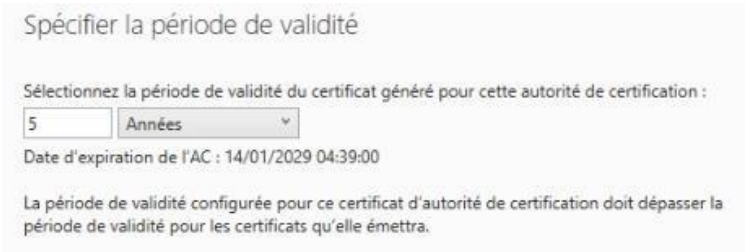
Pour le chiffrement, laisser les paramètres par défaut.



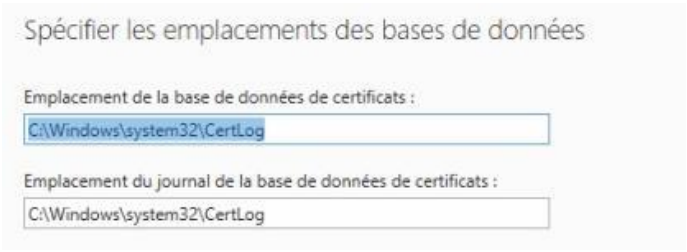
- Pour le nom de l'AC, laisser les paramètres par défaut.



- Pour la période de validité, laisser les paramètres par défaut.



- Pour l'emplacement de la base de données, laisser les paramètres par défaut.



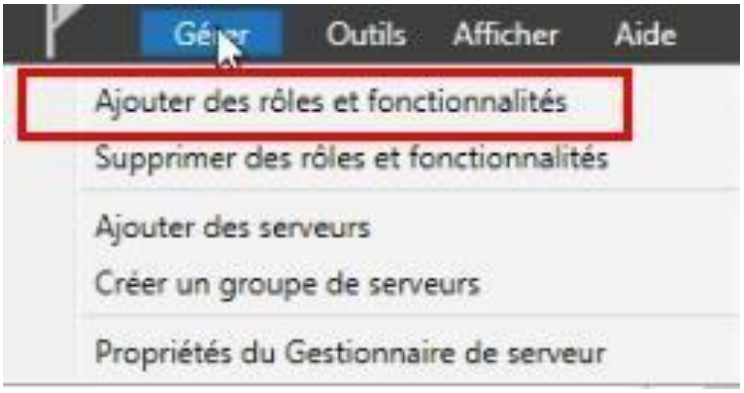
-

- Finaliser la configuration. L'ADCS est prêt.

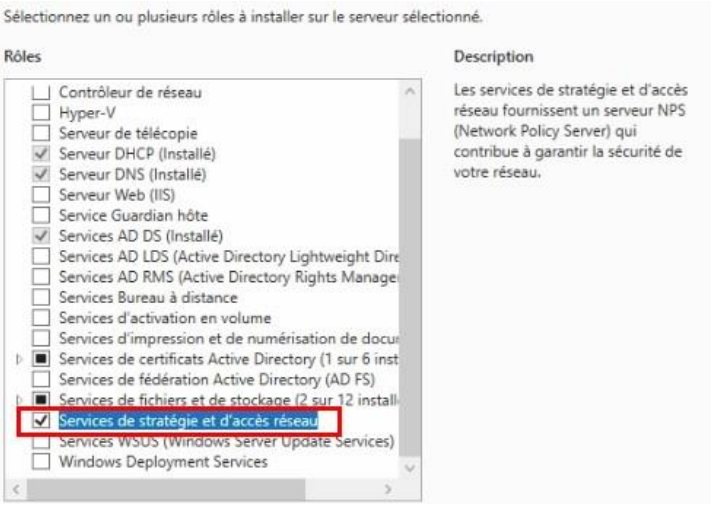
2) Installation du serveur NPS

Le serveur NPS (RADIUS Windows) servira de contrôleur LAN sans fil et permettra de mettre en place le protocole PEAP avec MS-CHAPv2 et EAP-TLS pour l'authentification.

- Sur le DC01, cliquer sur « Gérer » puis « Ajouter des rôles et fonctionnalités ».



- Sélectionner « Services de stratégie et d'accès réseau ».



- Terminer l'installation du service.

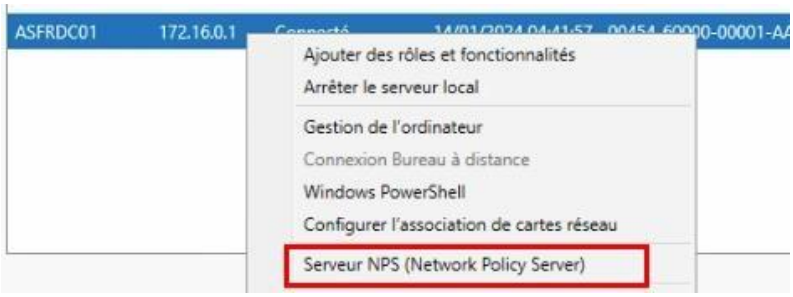
3) Configuration du serveur NPS

Nous allons maintenant configurer la console NPS pour ajouter le client RADIUS et la stratégie de connexion sans fil.

- Cliquer sur « Services de stratégie et d'accès réseau ».

-

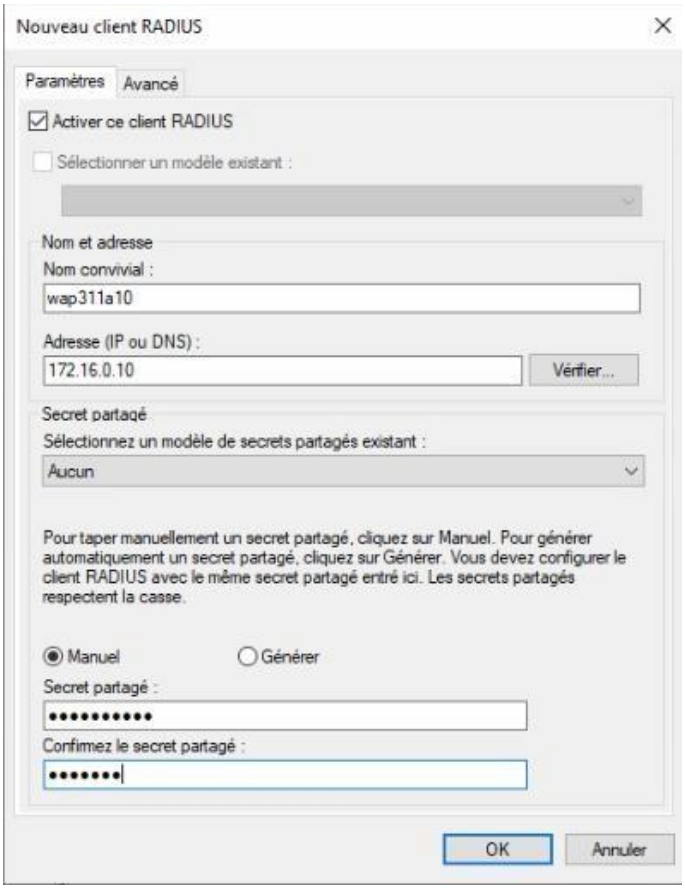
- Sur le serveur, faire clic droit puis cliquer sur « Serveur NPS (Network Policy Server) ».



- Faire clic droit sur « NPS (Local) puis cliquer sur « Inscrire un serveur dans Active Directory » afin de récupérer les informations de l'Active Directory.

- Sur « Client RADIUS », faire clic droit puis « Nouveau ».

Ajouter les informations de la borne Wifi et la clé précédemment définie dans « Secret partagé ».



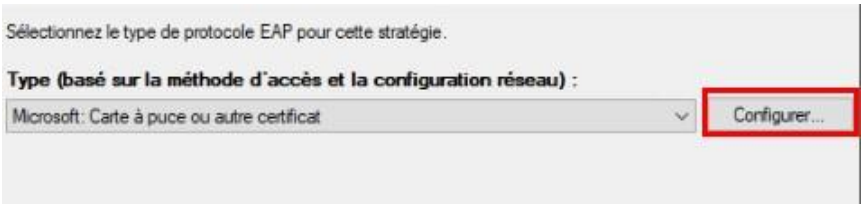
- Sur « NPS (Local) », dans l'onglet « Configuration standard », choisir le scénario « Serveur RADIUS pour les connexions… » puis cliquer sur « Configurer 802.1X ».

-

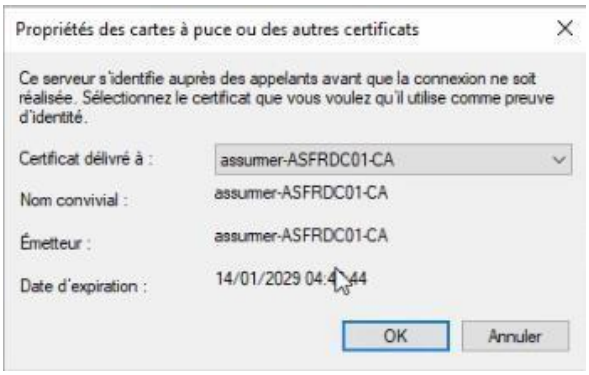
Pour le « Type de connexions », cocher « Connexions sans fil sécurisées ». Donner un nom.

- Ajouter le client RADIUS.

- Pour le protocole EAP, laisser « Carte à puce ou autre certificat ». Cliquer sur configurer.

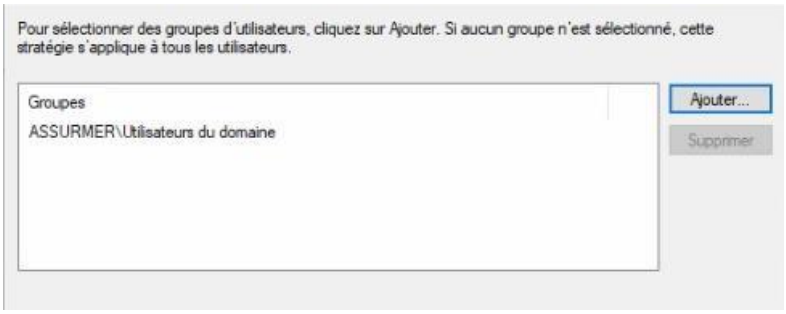


- Choisir l'ADCS pour le certificat.

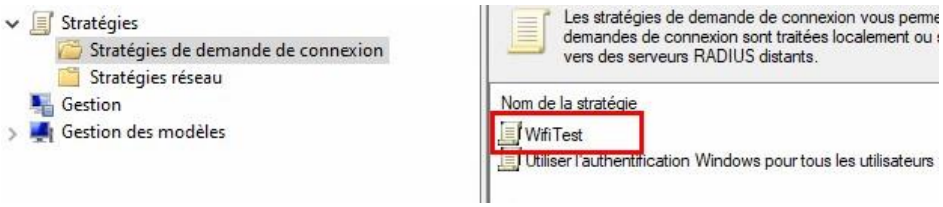


-

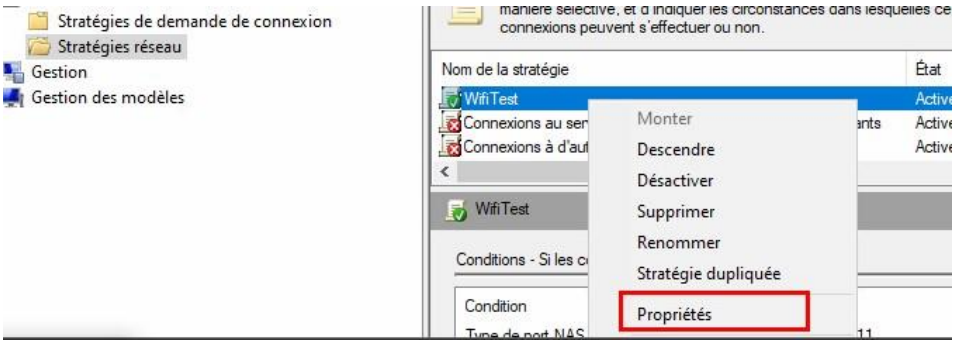
Pour les groupes d'utilisateurs, ajouter les utilisateurs du domaine.



- Cliquer sur « Terminer ».
- La stratégie apparaît alors dans « Stratégies de demande de connexion » et « Stratégies réseau ».

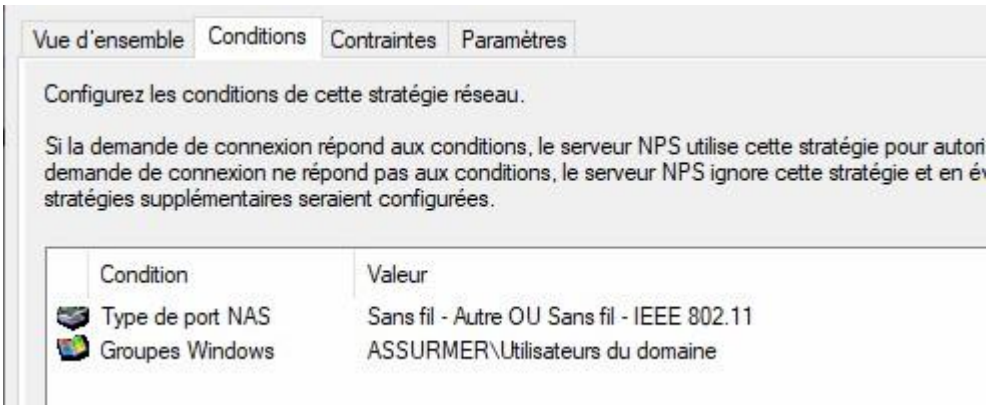


- Cliquer sur « Stratégies réseau ». Puis ouvrir les propriétés de « WifiTest ».

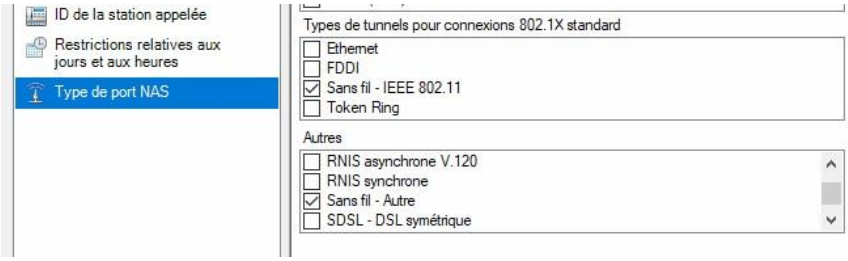


- Dans « Vue d'ensemble », laisser les paramètres par défaut.
- Dans « Conditions », on peut voir que seuls les utilisateurs du domaine et les appareils sans fil sont concernées.

-

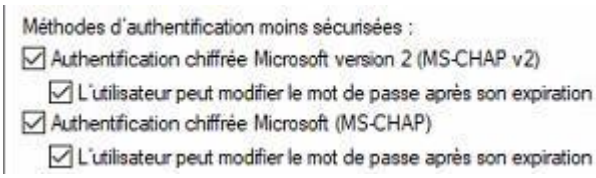


Dans « Contraintes », sur « Type de port NAS », cocher « Sans fil – Autre » et « Sans fil – IEEE 802.11 »



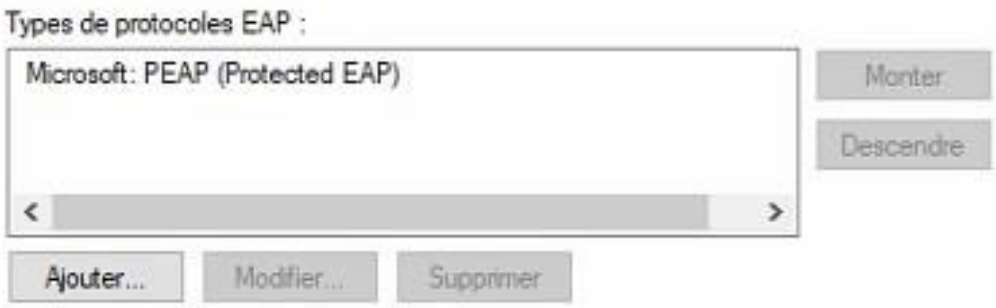
- Il est possible de mettre des restrictions relatives aux jours et aux heures, des délais d'inactivité et d'expiration.

- Dans « Méthodes d'authentification », activer le MS-CHAP v2 et le MSCHAP. Ces options permettent la connexion avec le compte AD.

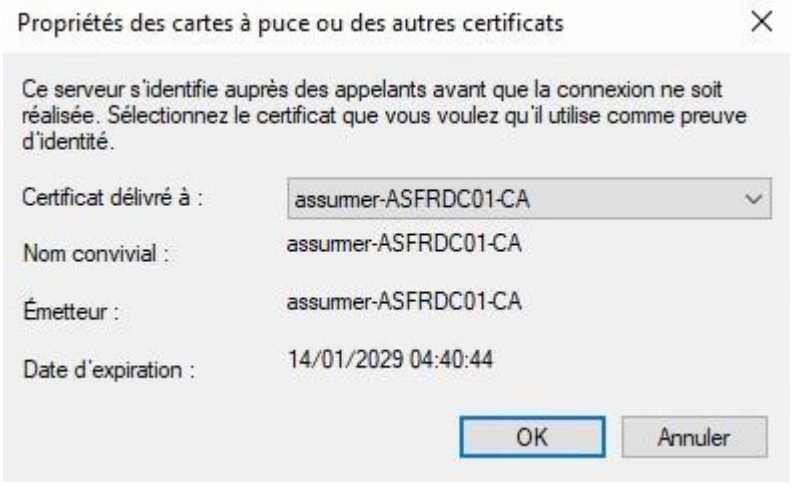


- Supprimer « Microsoft : Carte à puce ou autre certificat » et mettre « Microsoft PEAP » à la place. Puis « Modifier ».

-



Choisir le certificat de l'ADCS.



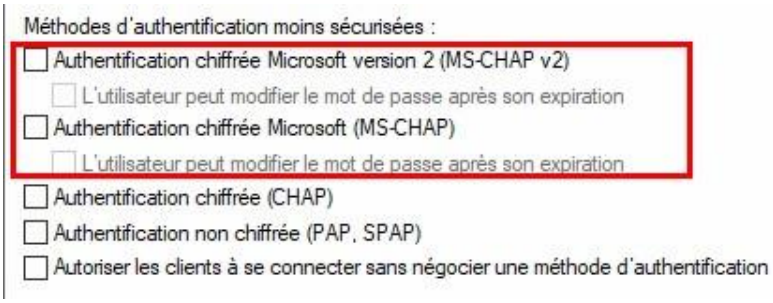
Axes d'amélioration, mise en place de l'EAP-TLS

1) Certificat et auto-inscription, authentification EAP-TLS

L'inscription automatique de certificat permet de générer des certificats utilisateurs ou ordinateurs dans le magasin personnel du demandeur sans qu'une personne n'en fasse spécifiquement une demande. Il est possible de l'automatiser pour la déployer sur l'ensemble des postes pour pouvoir utiliser l'EAP-TLS.

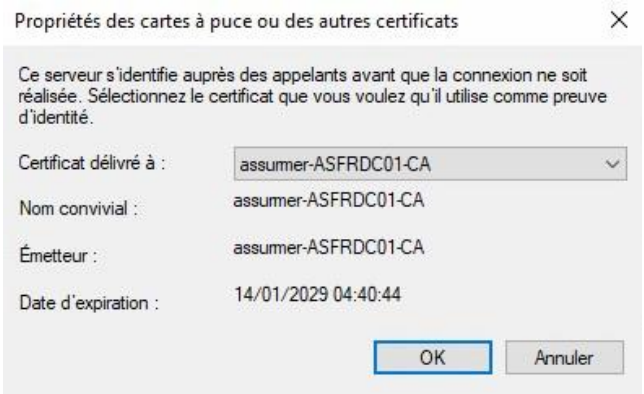
a) Modification de la stratégie réseau sur le serveur NPS

- Dans « Méthodes d'authentification », désactiver le MS-CHAP v2 et le MS-CHAP. Ces options permettent la connexion PEAP avec le compte AD, or nous allons mettre en place une connexion par certificat.



- Cliquer sur « Microsoft : Carte à puce ou autre certificat ». Puis « Modifier ».

- Choisir le certificat de l'ADCS.

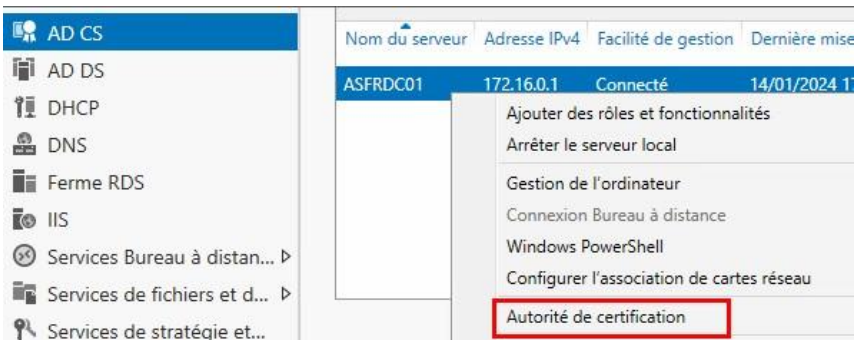


b) Création des modèles pour l'auto-inscription

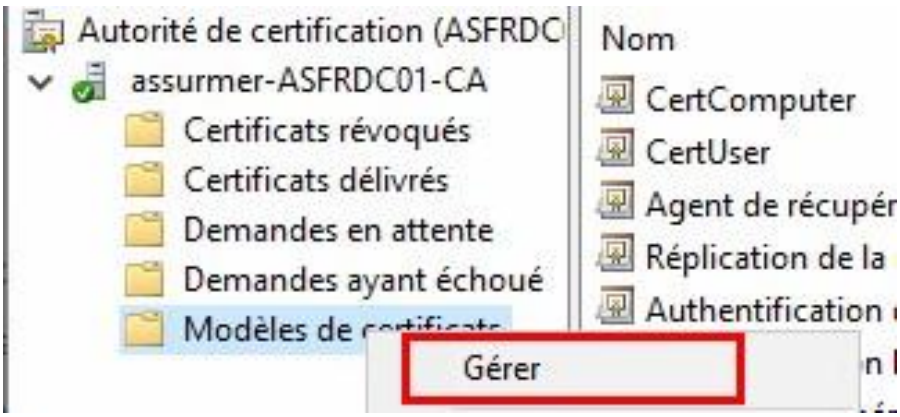
Nous allons d'abord créer un modèle d'inscription.

- Cliquer sur AD CS.

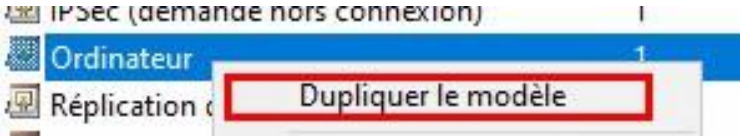
- Faire clic droit puis « Autorité de certification ».



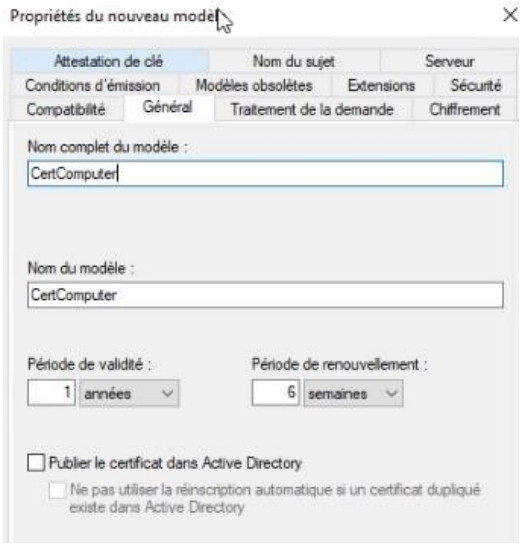
- Cliquer sur « Modèles de certificats » puis « Gérer ».



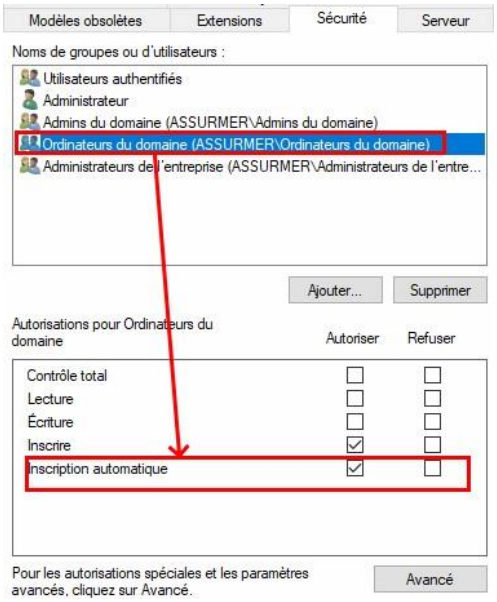
- Sur le modèle « Ordinateur », faire une duplication.



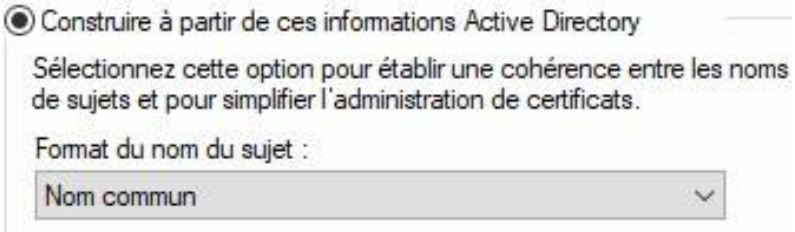
- Dans l'onglet « Général », ajouter un nom.



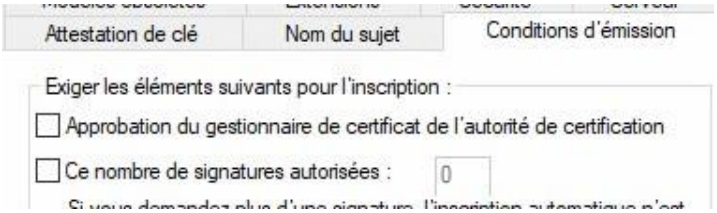
- Dans l'onglet « Sécurité », cliquer sur « Ordinateurs du domaine » puis cocher « Inscription automatique ».



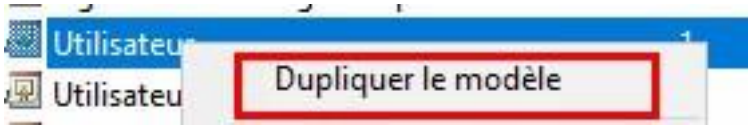
- Dans l'onglet « Nom du sujet », dans le format de nom, mettre « Nom commun ».



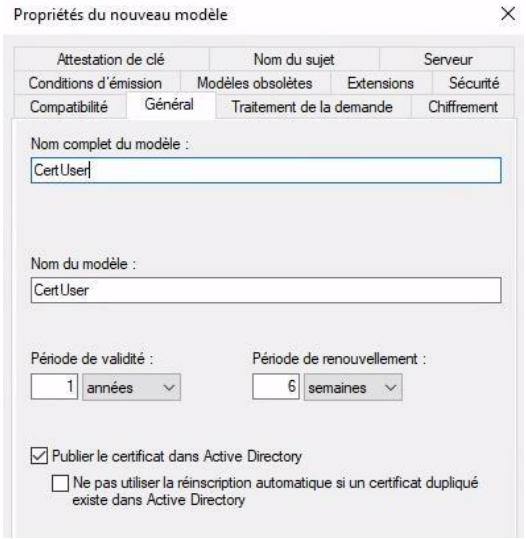
Dans l'onglet « Condition d'émission », vérifier que « L'approbation du gestionnaire de certificat de l'autorité de certification » n'est pas cochée pour pouvoir générer automatiquement.



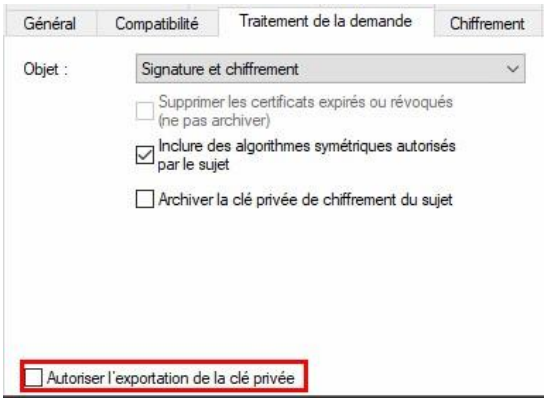
- Sur le modèle « Utilisateur », faire une duplication.



- Dans l'onglet « Général », ajouter un nom.

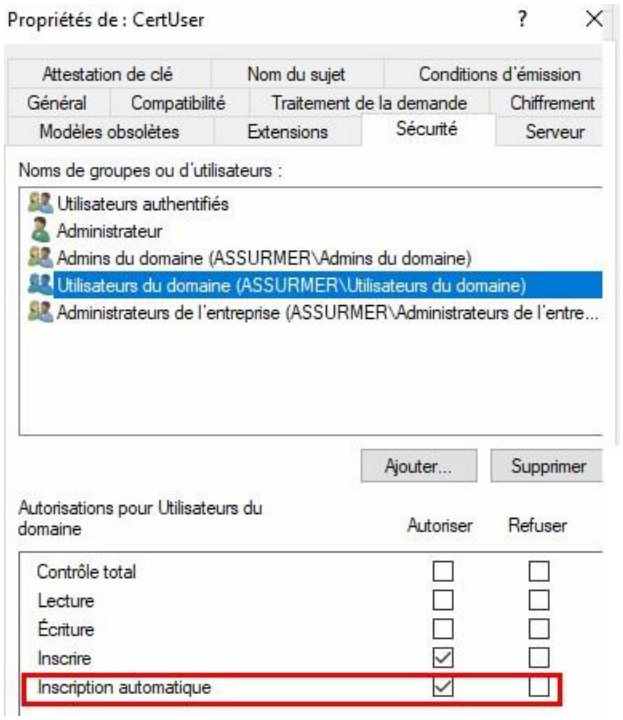


- Dans l'onglet « Traitement de la demande », décocher « Autoriser l'exportation de la clé privée ».

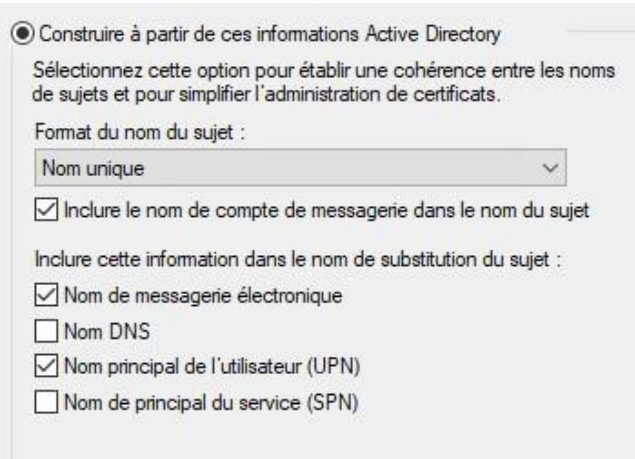


-

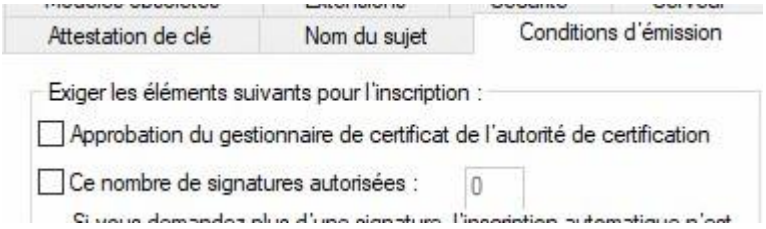
- Dans l'onglet « Sécurité », cliquer sur « Utilisateurs du domaine » puis cocher « Inscription automatique ».



- Dans l'onglet « Nom du sujet », laisser par défaut

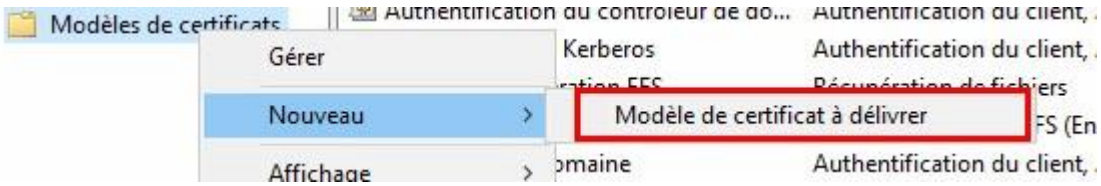


- Dans l'onglet « Condition d'émission », vérifier que « L'approbation du gestionnaire de certificat de l'autorité de certification » n'est pas cochée.

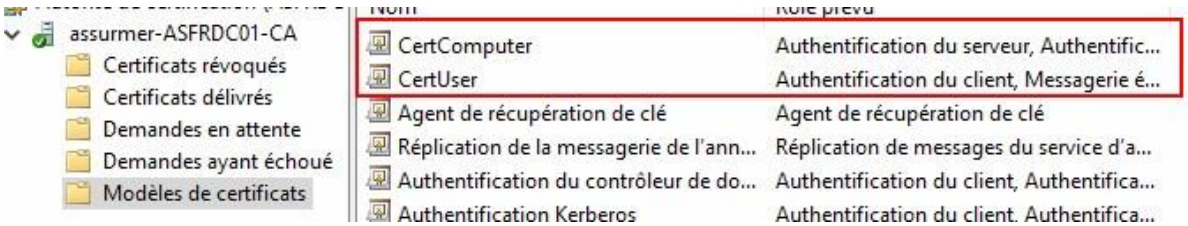


Nos modèles sont prêts

- Faire clic droit sur « Modèle de certificats » puis « Nouveau » puis « Modèles de certificats à délivrer ».



- Ajouter les 2 modèles.



/!\ Pour les certificats utilisateurs, il est nécessaire d'ajouter une adresse de messagerie sur les comptes utilisateurs. Sinon le certificat ne sera jamais inscrit pour les utilisateurs.

c) GPO pour les certificats

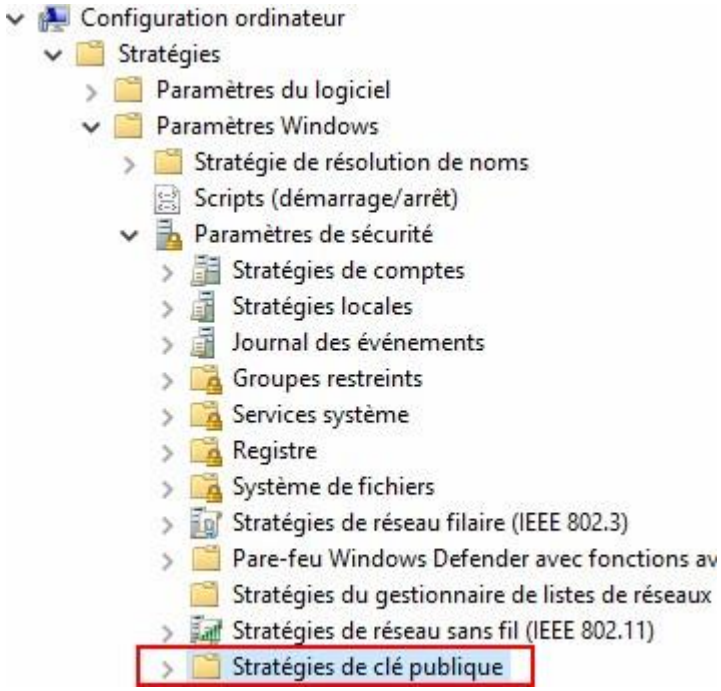
Afin de déployer les certificats, il est nécessaire de faire une GPO.

- Ouvrir le gestionnaire des stratégies de groupe.

- Sur l'OU qui contient les ordinateurs, créer une GPO « CertWifiCpt » qui servira à délivrer le certificat machine.

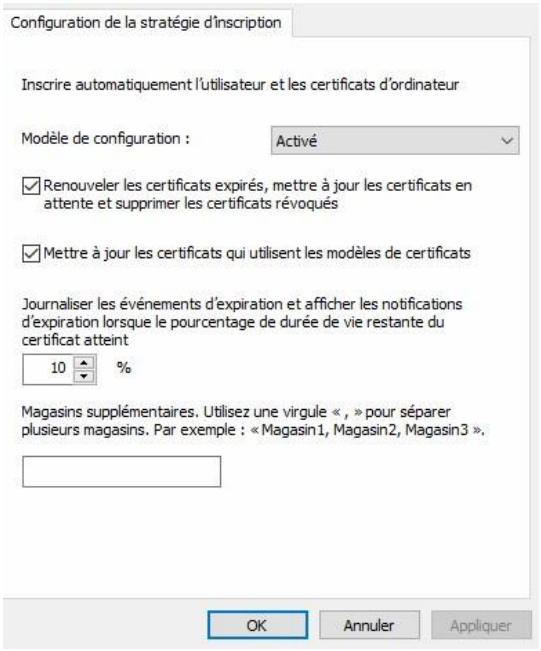
-

- Cliquer sur Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies de clé publique.

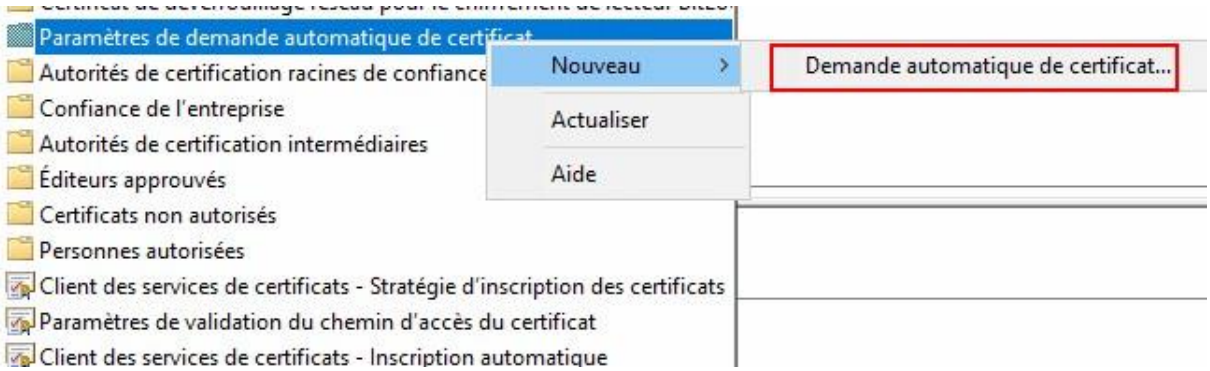


Faire clic droit sur « Client des services de certificats – Inscription automatique » puis « Propriétés ».

- Mettre en « Activé ». Cocher le paramètre « Renouveler … » et « Mettre à jour ».

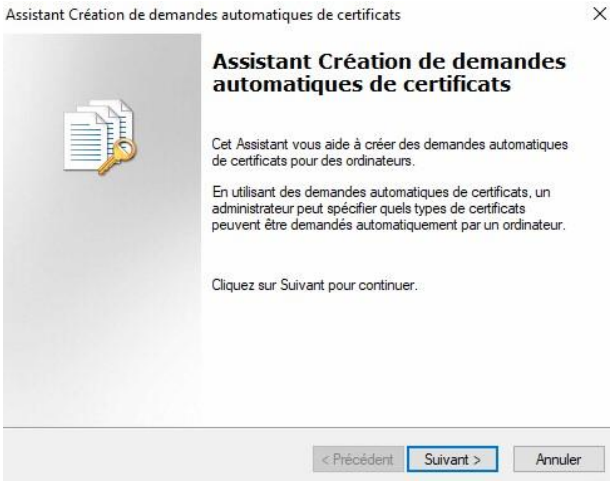


- Faire clic droit sur « paramètres de demande automatique de certificat » puis « Nouveau » puis « Demande automatique de certificat … ».

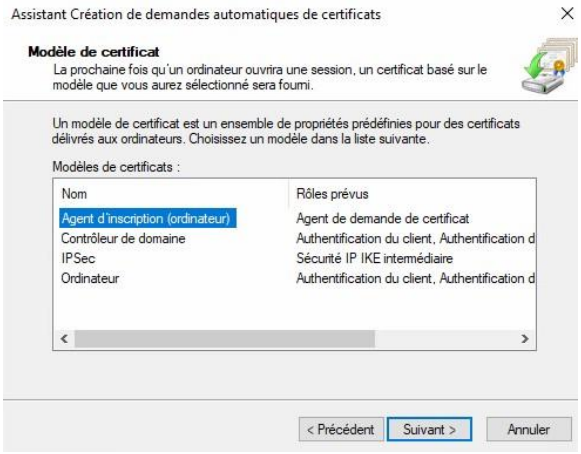


-

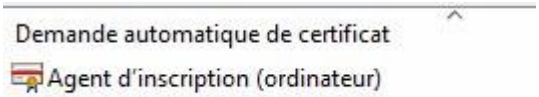
Cliquer sur « Suivant ».



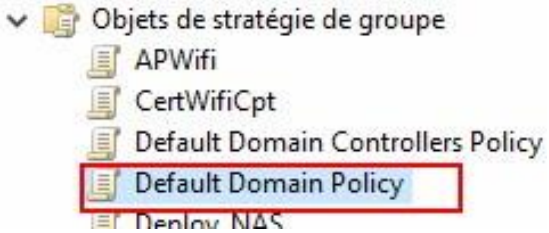
- Le modèle certificat est affiché. Cliquer sur « Suivant » puis « Terminer ».



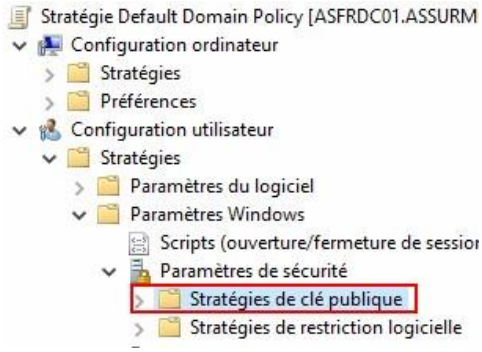
- L'agent d'inscription s'affiche ensuite dans le conteneur.



- Sur l'OU « Objets de stratégie de groupe », modifier « Default Domain Policy » pour délivrer les certificats utilisateurs.

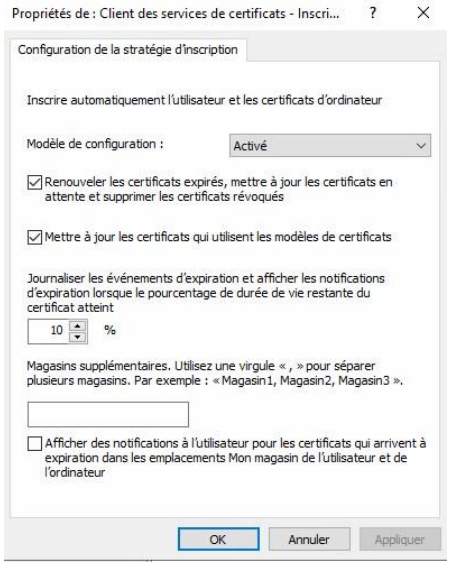


Cliquer sur Configuration utilisateur/ Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies de clé publique.



- Faire clic droit sur « Client des services de certificats – Inscription automatique » puis « Propriétés ».

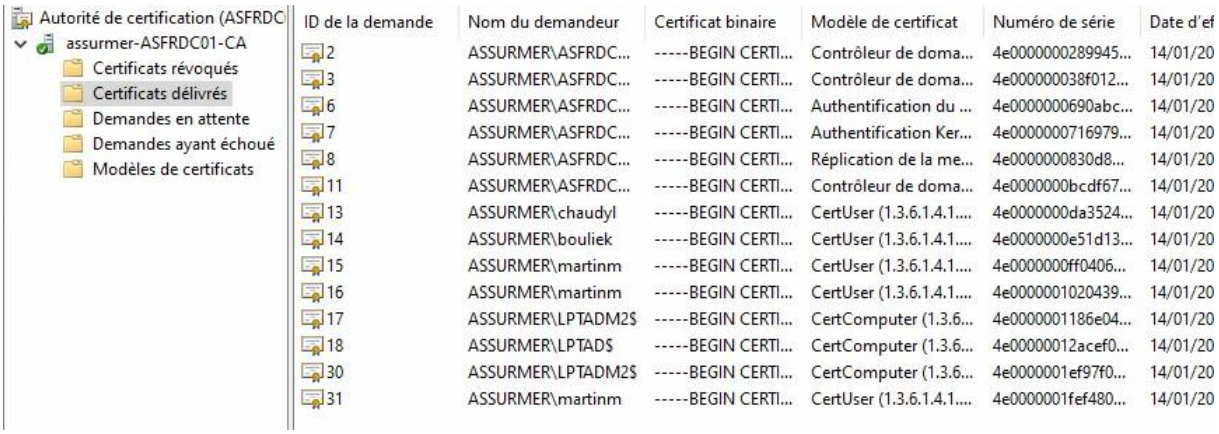
- Mettre en « Activé ». Cocher le paramètre « Renouveler … » et « Mettre à jour ». Il y a une option en plus pour notifier mais non utilisé dans notre cas.



Les GPO pour délivrer les certificats et inscrire automatiquement les ordinateurs et utilisateurs sont désormais configurés.

Dans l'autorité de certification, les certificats délivrés apparaissent :

-



ID de la demande	Nom du demandeur	Certificat binaire	Modèle de certificat	Numéro de série	Date d'ef
2	ASSURMER\ASFRDC...	-----BEGIN CERTI...	Contrôleur de doma...	4e0000000289945...	14/01/20
3	ASSURMER\ASFRDC...	-----BEGIN CERTI...	Contrôleur de doma...	4e000000038f012...	14/01/20
6	ASSURMER\ASFRDC...	-----BEGIN CERTI...	Authentification du ...	4e0000000690abc...	14/01/20
7	ASSURMER\ASFRDC...	-----BEGIN CERTI...	Authentification Ker...	4e0000000716979...	14/01/20
8	ASSURMER\ASFRDC...	-----BEGIN CERTI...	Réplication de la me...	4e0000000830d8...	14/01/20
11	ASSURMER\ASFRDC...	-----BEGIN CERTI...	Contrôleur de doma...	4e0000000bcdf67...	14/01/20
13	ASSURMER\chaudyl	-----BEGIN CERTI...	CertUser (1.3.6.1.4.1....	4e0000000da3524...	14/01/20
14	ASSURMER\bouliek	-----BEGIN CERTI...	CertUser (1.3.6.1.4.1....	4e0000000e51d13...	14/01/20
15	ASSURMER\martinm	-----BEGIN CERTI...	CertUser (1.3.6.1.4.1....	4e0000000ff0406...	14/01/20
16	ASSURMER\martinm	-----BEGIN CERTI...	CertUser (1.3.6.1.4.1....	4e0000001020439...	14/01/20
17	ASSURMER\LPTADM2$	-----BEGIN CERTI...	CertComputer (1.3.6...	4e0000001186e04...	14/01/20
18	ASSURMER\LPTAD$	-----BEGIN CERTI...	CertComputer (1.3.6...	4e00000012acef0...	14/01/20
30	ASSURMER\LPTADM2$	-----BEGIN CERTI...	CertComputer (1.3.6...	4e0000001ef97f0...	14/01/20
31	ASSURMER\martinm	-----BEGIN CERTI...	CertUser (1.3.6.1.4.1....	4e0000001fef480...	14/01/20

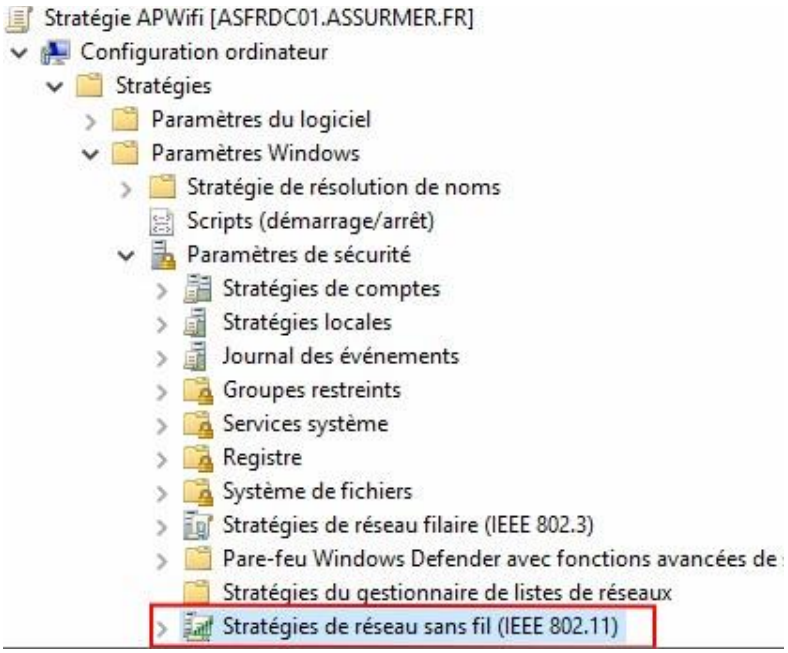
d) GPO pour le point d'accès Wifi

Nous allons déployer un réseau WiFi par GPO de manière qu'il soit connu automatiquement par les machines de du parc informatique et intégré à l'Active Directory.

- Ouvrir le gestionnaire des stratégies de groupe.

- Sur l'OU qui contient les ordinateurs, créer une GPO « APWifi » qui servira à déployer automatiquement le SSID.

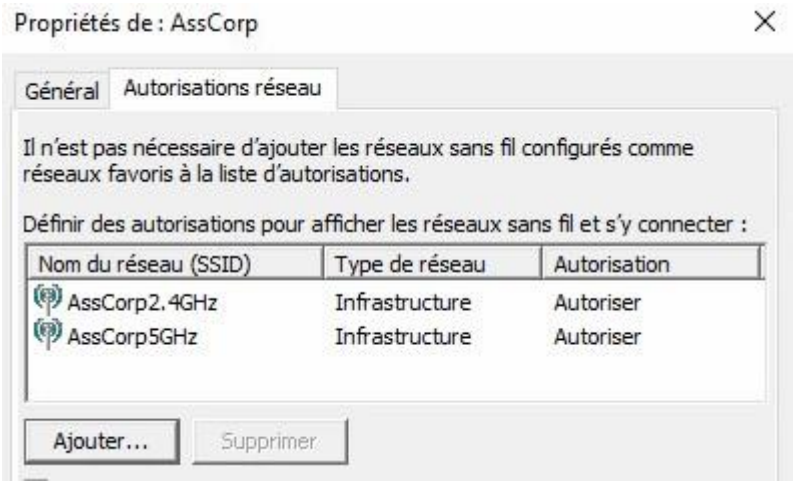
- Cliquer sur Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies de réseau sans fil (IEEE802.11).



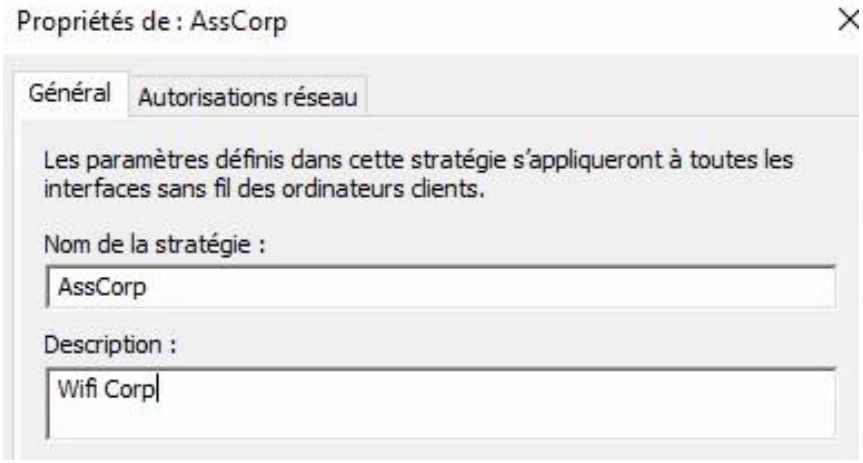
- Faire clic droit puis cliquer sur « créer une stratégie Vista and Later Releases ».

-

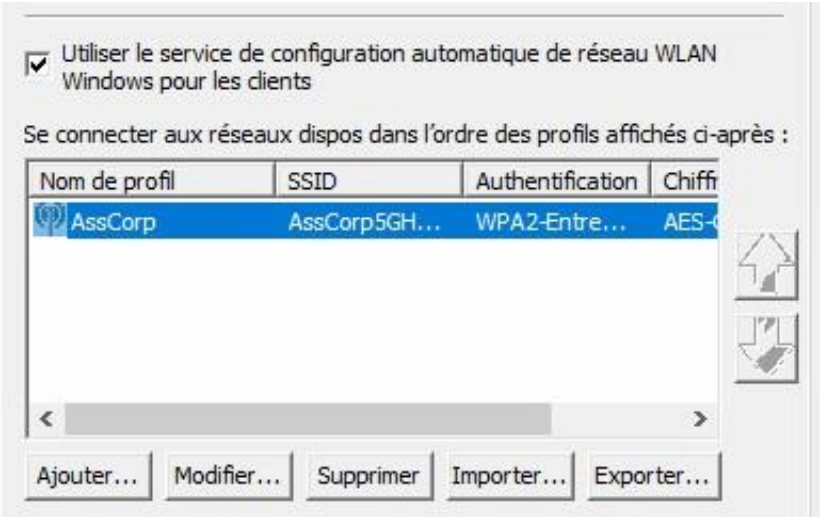
Dans « Autorisations réseau », autoriser les 2 SSID configurés sur la borne.



- Dans « Général », ajouter un nom à la stratégie et une description.

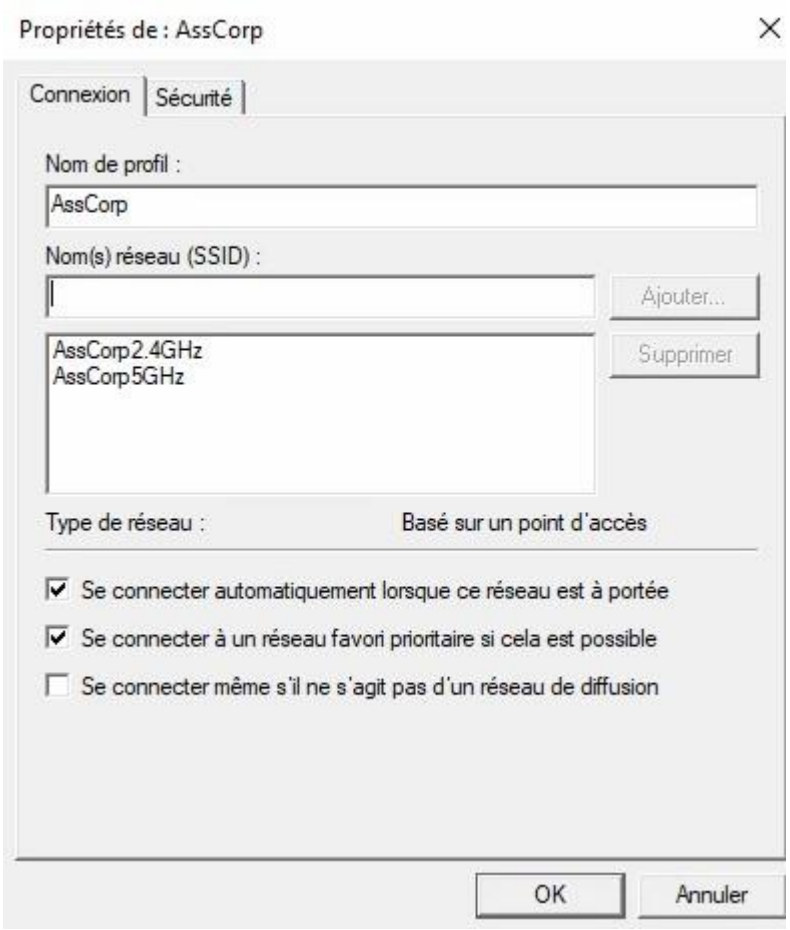


- Ajouter ensuite un profil.

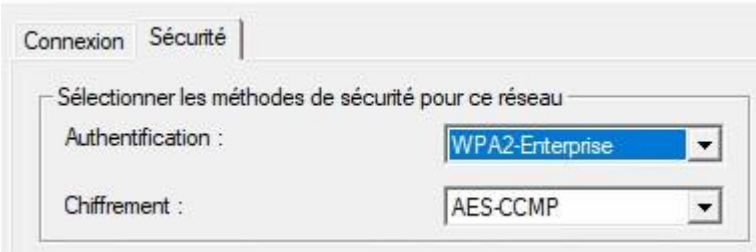


-

Renseigner le nom de profil, les SSID.



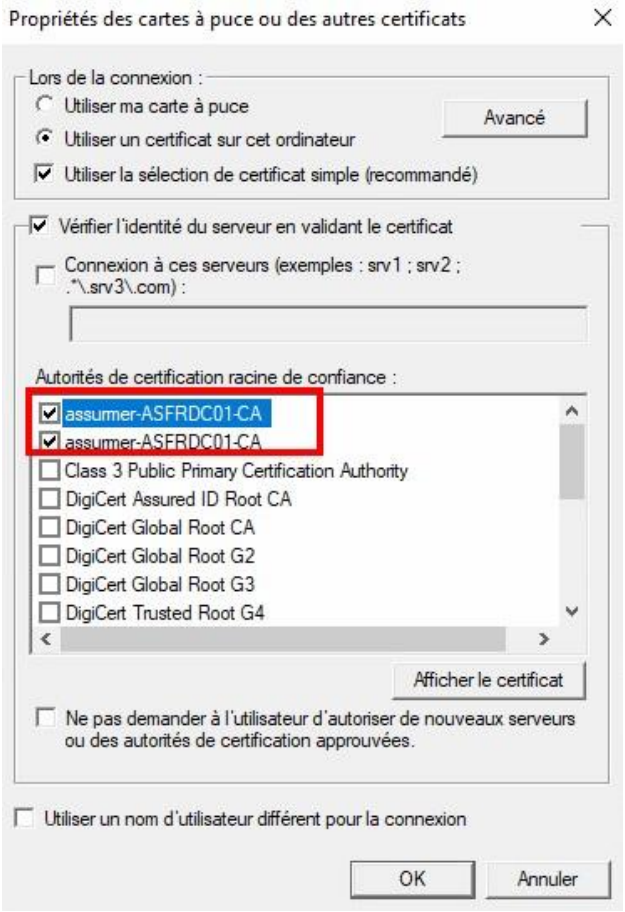
- Dans « Sécurité », laisser l'authentification et le chiffrement par défaut.



- Sur la méthode d'authentification réseau, mettre « Microsoft : Carte à puce ou autre certificat » puis cliquer sur « Propriétés ».

En « Autorités de certification de racine de confiance », cocher l'ADCS.

-



- Dans « Avancé », cocher « Emetteur du certificat » et cocher les ADCS également.

- Le point d'accès est prêt.