Atelier : Installer une autorité de certification

1. Objectif

La société Corp souhaite implémenter certaines fonctionnalités de sécurité nécessitant des certificats. Afin d'éviter des dépenses importantes d'achat de certificats, les administrateurs de la société ont décidé de déployer une autorité de certification entreprise en interne. Cette autorité émettrice fournira les certificats nécessaires aux utilisateurs et ordinateurs de l'Active Directory.

Dans cet atelier pratique, nous allons installer et configurer cette autorité de certification racine entreprise émettrice.

Cette autorité de certification étant réutilisée dans les ateliers des chapitres suivants, une sauvegarde complète de la plateforme (points de contrôle) sera effectuée en fin d'atelier.

Les ordinateurs virtuels utilisés dans cet atelier sont les suivants :

- S1 : contrôleur de domaine
- S2 : autorité de certification racine entreprise (CorpRootCa)
- W10 : client Active Directory

2. Installer le rôle

Ouvrez la console de gestion Gestionnaire de serveur, développez le menu **Gérer** et sélectionnez le menu **Ajouter des rôles et fonctionnalités**.

Dans la fenêtre Avant de commencer de l'assistant cliquez sur le bouton **Suivant**.

Dans l'assistant Ajout de rôles et de fonctionnalités, dans la fenêtre Sélectionner le type d'installation, sélectionnez **Installation basée sur un rôle ou une fonctionnalité** et cliquez sur le bouton **Suivant**.

Dans la fenêtre Sélectionner le serveur de destination, sélectionnez Sélectionner un serveur du pool de serveurs et sélectionnez le serveur **s2.corp.lan**.

Dans la fenêtre Sélectionner des rôles de serveurs, cochez **Services de certificats Active Directory**.

Dans la fenêtre Assistant Ajout de rôles et de fonctionnalités, cliquez sur le bouton **Ajouter des fonctionnalités**.

Dans la fenêtre Sélectionner des fonctionnalités, cliquez sur le bouton **Suivant**.

Lisez la description de l'écran Services de certificats Active Directory et cliquez sur le bouton **Suivant**.

Dans la fenêtre Sélectionner des services de rôles, sélectionnez **Autorité de certification** puis cliquez sur le bouton **Suivant**.

Dans la fenêtre Confirmer les sélections d'installation, validez les éléments qui seront installés puis cliquez sur le bouton **Installer**.

Attendez que l'installation soit complète puis cliquez sur le bouton **Fermer**.

3. Configurer le rôle

Cliquez sur l'icône de notification (le point d'exclamation dans un triangle jaune à gauche du menu **Gérer**).

L'icône de notification indique que des tâches supplémentaires doivent être exécutées (**Configurer les services de certificats Active Directory**).

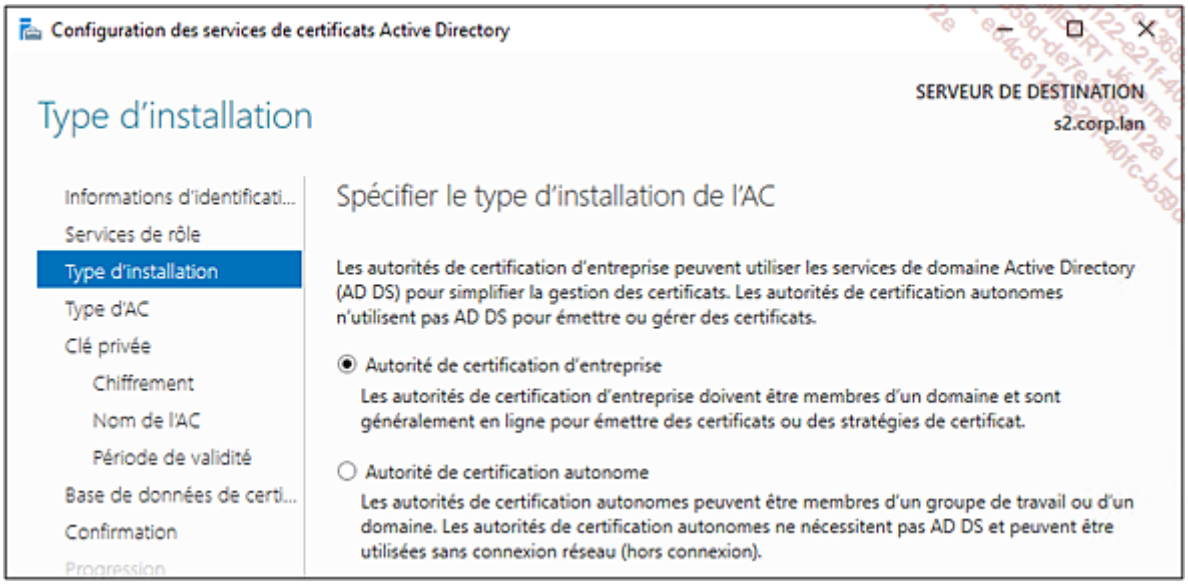
Si l'icône de notification n'apparaît pas, assurez-vous que l'installation est bien complète puis rafraîchissez la console du gestionnaire de serveur en cliquant sur l'icône **Actualiser tableau de bord** (les doubles flèches arrondies à gauche du menu **Gérer**).

Sélectionnez **Configurer les services de certificats Active Directory sur le serveur de destination**.

Dans l'assistant Configuration des services de certificats Active Directory, sur l'écran Informations d'identification validez que les informations d'identification sont **CORP\Admin** (sinon modifiez-les à l'aide du bouton **Modifier**) puis cliquez sur le bouton **Suivant**.

Dans la fenêtre Services de rôle, cochez le service de rôle **Autorité de certification** puis cliquez sur le bouton **Suivant**.

Dans la fenêtre Type d'installation, sélectionnez **Autorité de certification d'entreprise** puis cliquez sur le bouton **Suivant**.

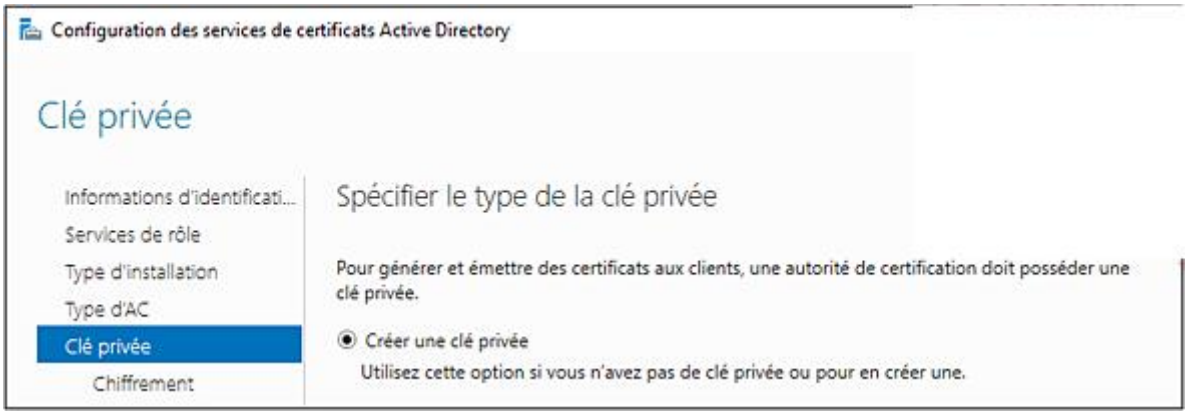


Les autorités de certification d'entreprise bénéficient de nombreux avantages grâce à une intégration à l'Active Directory.

Dans la fenêtre Type d'autorité de certification, sélectionnez **Autorité de certification racine** puis cliquez sur le bouton **Suivant**.

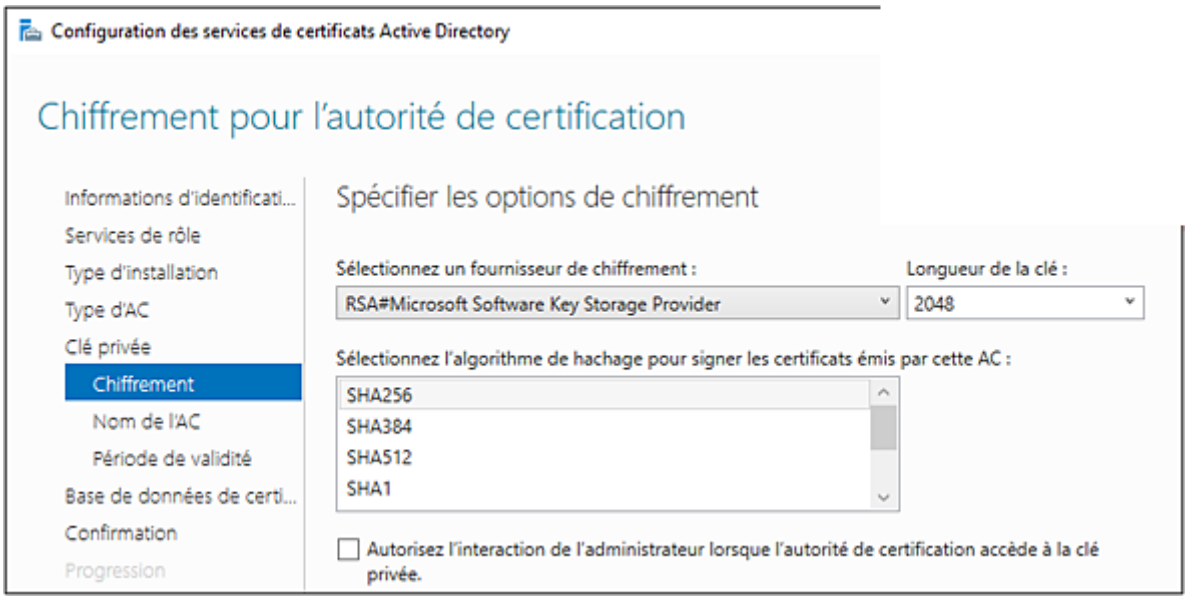
La première autorité de certification installée est obligatoirement une autorité de certification à la racine de l'arborescence de notre hiérarchie de PKI.

Dans la fenêtre Spécifier le type de la clé privée, sélectionnez **Créer une clé privée** puis cliquez sur le bouton **Suivant**.



L'autorité obtient à l'installation un certificat d'autorité de certification autosigné avec une clé privée et une clé publique.

Dans la fenêtre Chiffrement pour l'autorité de certification, validez que le fournisseur de chiffrement est **RSA#Microsoft Software Key Storage Provider**, que la longueur de la clé est **2048** et que l'algorithme de hachage est **SHA256** puis cliquez sur le bouton **Suivant**.



Le fournisseur de chiffrement de Microsoft convient par défaut. La longueur des clés privée/publique de l'autorité peut être augmentée jusqu'à 2048 si la sécurité l'exige. L'algorithme de Hachage est celui utilisé pour les opérations de signature et d'intégrité (SHA256 est le choix valide actuellement, SHA1 est déprécié).

Dans la fenêtre Nom de l'autorité de certification, dans la zone **Nom commun** de cette AC saisissez **CorpRootCA** puis cliquez sur le bouton **Suivant**.

Dans la fenêtre Période de validité, dans la zone **Sélectionner la période de validité** du certificat généré pour cette autorité de certification saisissez **15** puis cliquez sur le bouton **Suivant**.

Dans la fenêtre Base de données de l'autorité de certification, laissez les emplacements par défaut pour la base de données de certificats et le journal de la base de données (C:\Windows\system32\Certlog) et cliquez sur le bouton **Suivant**.

Dans la fenêtre Confirmation validez les éléments qui seront installés puis cliquez sur le bouton **Configurer**.

Dans la fenêtre Résultat, validez que la configuration a réussi puis cliquez sur le bouton **Fermer**.

4. Valider l'installation

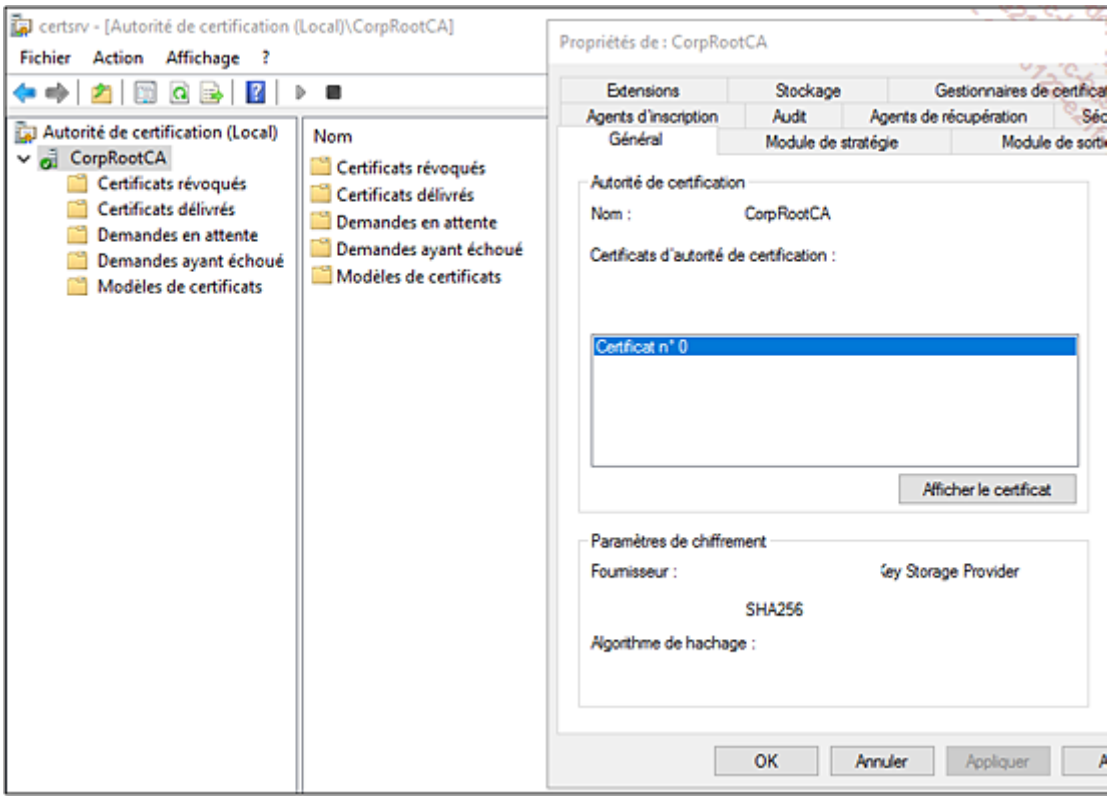
Dans la console de gestion Gestionnaire de serveur, développez le menu **Outils** et sélectionnez **Autorité de certification**.

La console de gestion Autorité de certification s'ouvre.

Faites un clic droit sur l'icône de la console sur la barre de tâches et sélectionnez le menu **Épingler à la barre des tâches**.

Épingler la console à la barre de tâches évite les recherches dans le menu Outils du Gestionnaire de serveur.

Dans la console Autorité de certification, faites un clic droit sur **CorpRooCA** et sélectionnez le menu **Propriétés**.

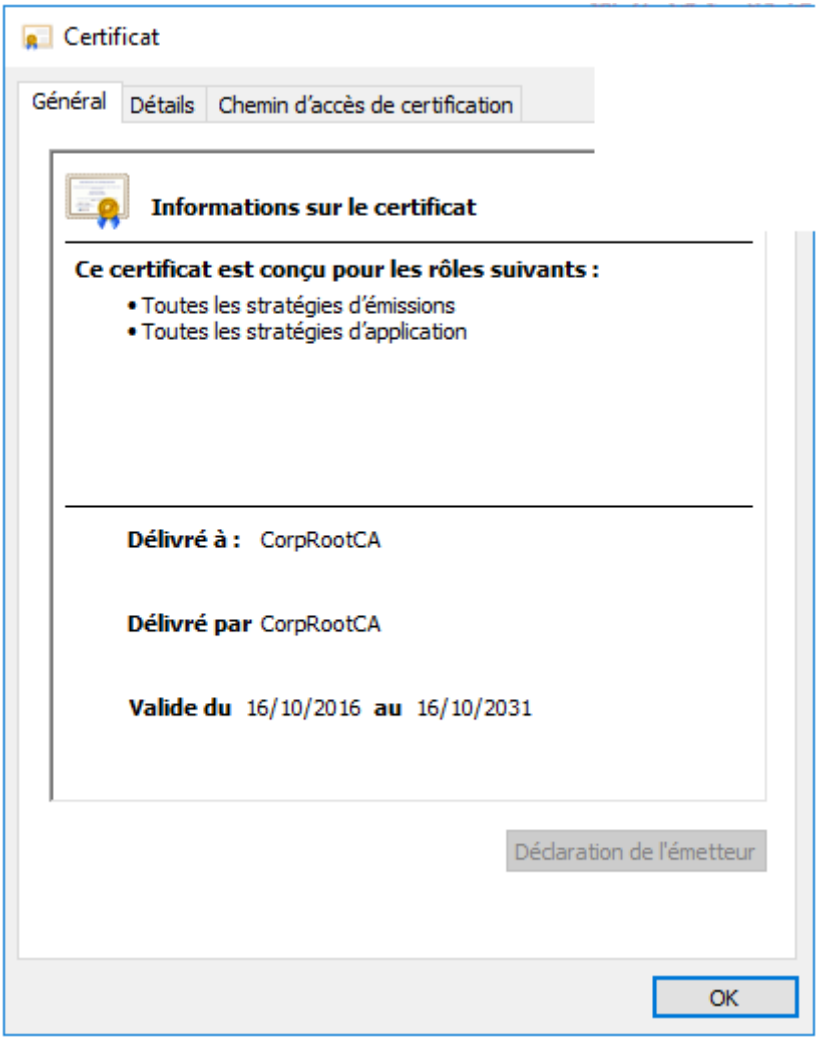


Malgré un bug d'affichage dans la console, on peut ici valider le fournisseur de chiffrement (RSA#Microsoft Software Key Storage Provider) et l'algorithme de hachage (SHA256) sélectionnés lors de la configuration de l'autorité de certification.

Cliquez sur le bouton **Afficher le certificat**.

Le certificat de l'autorité de certification s'affiche.

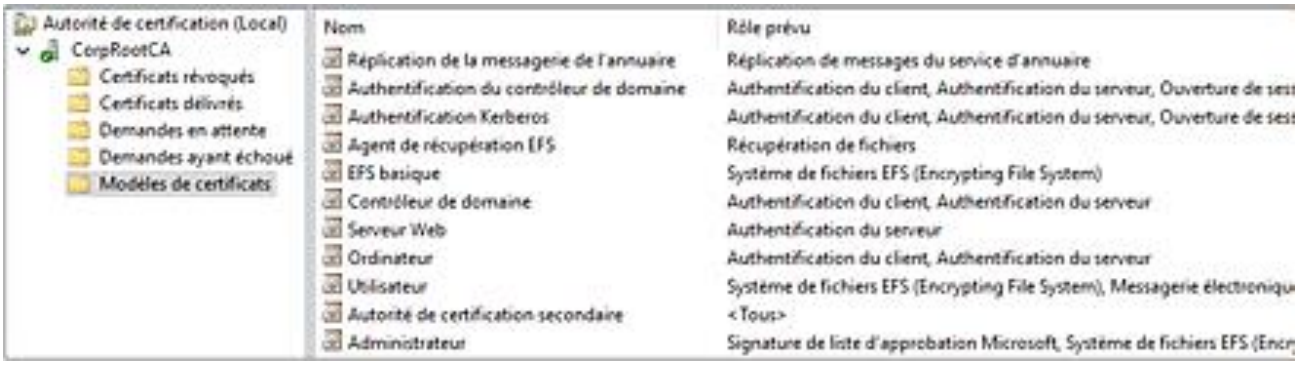
Validez qu'il est autosigné (champs **Délivré à CorpRootCA**, **Délivré par CorpRootCA**) et que sa durée de vie est bien de 15 ans.



Le certificat autosigné de l'autorité dispose de tous les rôles.

Cliquez deux fois sur le bouton **OK** pour fermer les propriétés de l'autorité de certification.

Développez **CorpRootCA** et sélectionnez le conteneur **Modèles de certificats** et examinez la liste des modèles de certificats prêts à être délivrés.



Plusieurs modèles de certificats sont disponibles par défaut pour l'inscription.

Publier une première liste de révocation

Faites un clic droit sur le dossier **Certificats révoqués** puis sélectionnez les menus **Toutes les tâches/Publier**.

Dans la fenêtre Publier la liste de révocation des certificats, sélectionnez **Nouvelle liste de révocation des certificats** puis cliquez sur le bouton **OK**.

Une nouvelle liste de révocation complète des certificats doit être publiée immédiatement.

5. Inscrire un certificat

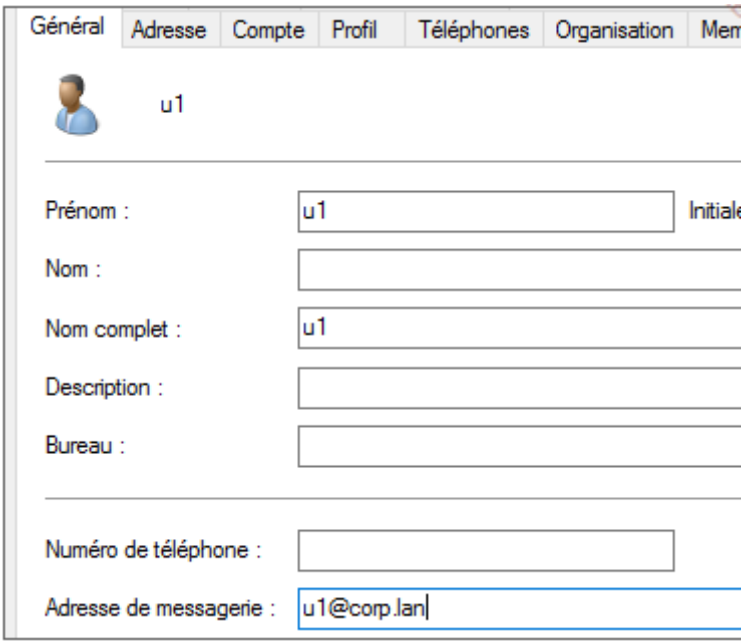
Modifier l'adresse de messagerie du compte utilisateur u1

Ouvrez la console de gestion Utilisateurs et ordinateurs Active Directory.

Développez **corp.lan\test**.

Faites un clic droit sur l'utilisateur u1 et sélectionnez le menu **Propriétés**.

Saisissez **u1@corp.lan** dans la zone **Adresse de messagerie**.



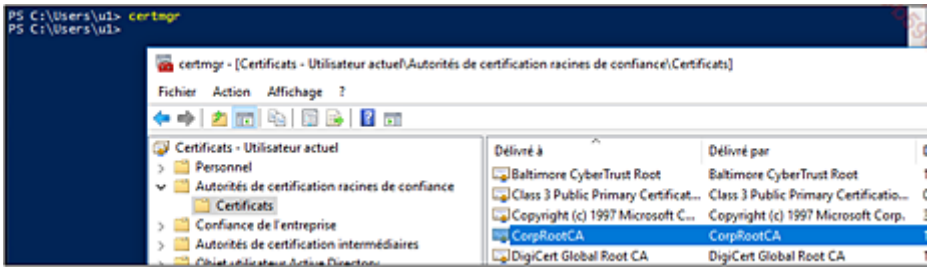
Le modèle de certificat Utilisateur requiert une adresse de messagerie pour composer le champ **Nom** du sujet (voir chapitre Gestion automatisée des certificats).

Cliquez sur le bouton **OK**.

Valider la présence du certificat de l'autorité de certification côté client

Ouvrez une invite de commande PowerShell et exécutez la commande **`certmgr.msc`**.

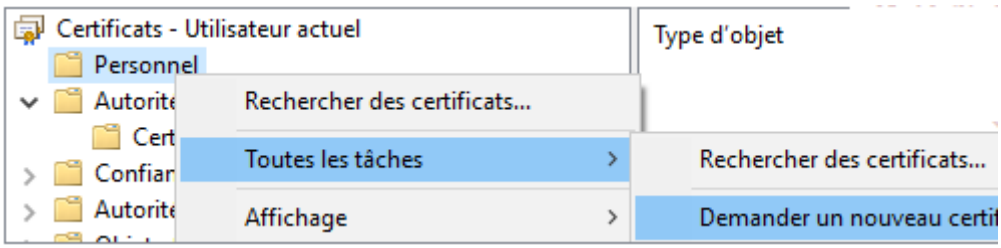
Développez Certificats/Utilisateur/Autorités de certifications de racines de confiance/Certificats et validez la présence du certificat de l'autorité de certification CorpRootCA.



Si le certificat de l'autorité de certification CorpRootCA n'apparaît pas, exécutez la commande **`certutil -pulse`** ou redémarrez l'ordinateur et vérifiez à nouveau la présence du certificat.

Demander un certificat

Dans la console Certificats/Utilisateur Actuel, faites un clic droit sur le dossier **Personnel** et sélectionnez les menus **Toutes les taches/Demander un nouveau certificat**.



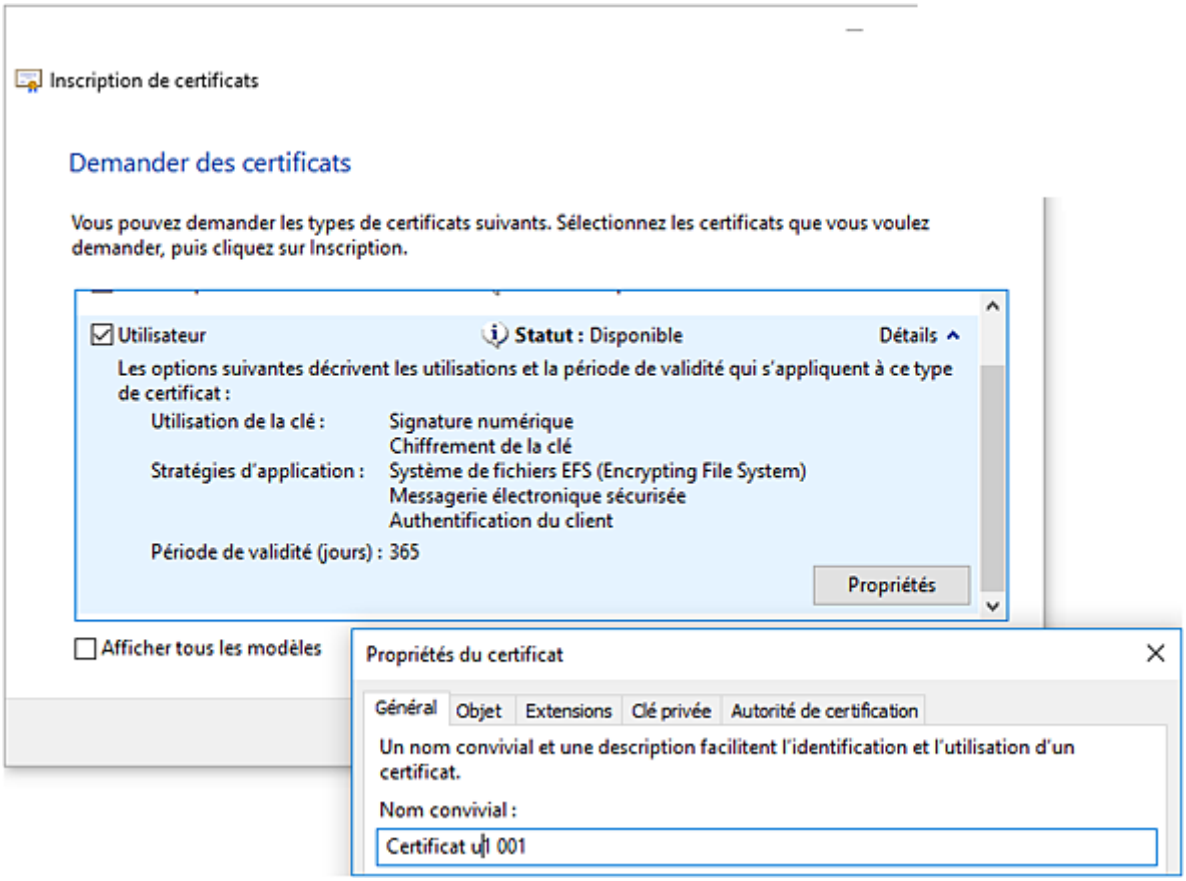
Exécution de l'assistant de demande de certificats.

Dans l'assistant Inscription de certificats, dans la fenêtre Avant de commencer, lisez les recommandations puis cliquez sur le bouton **Suivant**.

Dans la fenêtre Sélectionner la stratégie d'inscription de certificat, validez que la sélection par défaut est bien **Stratégie d'inscription à Active Directory** puis cliquez sur le bouton **Suivant**.

Dans la fenêtre Demander des certificats, cochez le modèle **Utilisateur**.

Cliquez sur l'icône flèche vers le bas à droite du menu **Détails** pour le développer, cliquez sur le bouton **Propriétés** et dans la zone **Nom convivial** de l'onglet **Général**, saisissez **Certificat u1 001**.



Détails du modèle Utilisateur et ajout d'un nom convivial (Certificat u1 001) à la demande de certificat de u1.

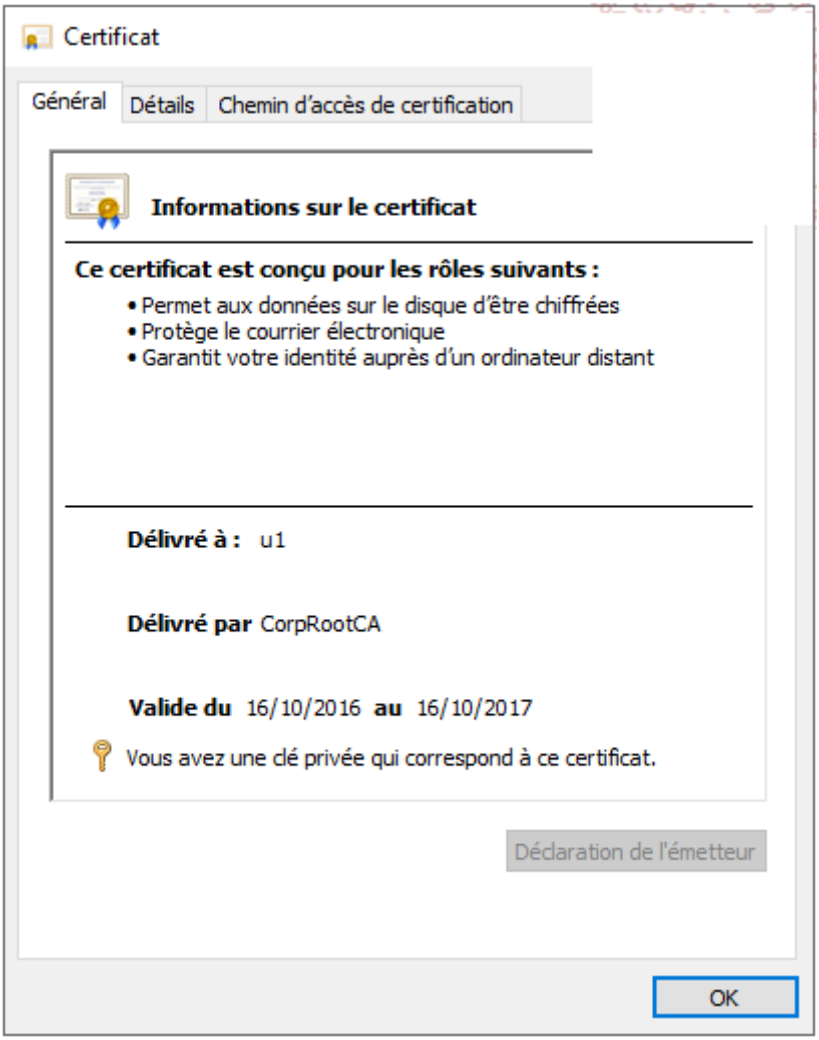
Cliquez sur les boutons **OK** et **Inscription**.

Validez l'inscription du certificat.

Valider les informations du certificat

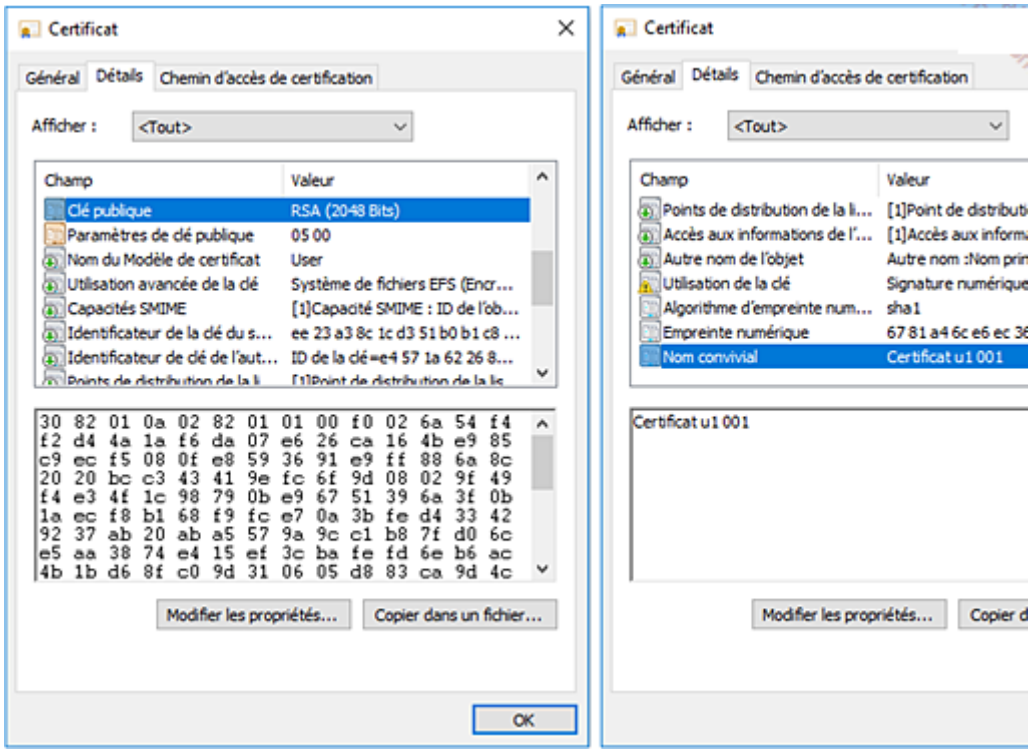
Dans la console Certificats/Utilisateur actuel, développez les dossiers Personnel/Certificats puis double cliquez sur le certificat obtenu (dans la zone de droite de la console).

Dans l'onglet **Général**, validez que le certificat est délivré à u1 par l'autorité de certification CorpRootCA.



Le certificat est bien délivré à U1 par CorpRootCA pour une durée de vie d'une année. Une clé privée est associée à ce certificat.

Sélectionnez l'onglet **Détails** et validez la présence des champs **Clé publique** et **Nom convivial**.



Les propriétés du certificat permettent de visualiser, entre autres, la valeur de la clé publique et le nom convivial.

Sélectionnez l'onglet **Chemin d'accès de certification** et validez que le certificat est bien délivré par l'autorité de certification CorpRootCA.

6. Créer un point de contrôle

> L'environnement de test, incluant une autorité de certification racine entreprise, est maintenant opérationnel. Nous allons effectuer plusieurs points de contrôle pour le sauvegarder. Si nécessaire, nous pourrons ainsi, très facilement, restaurer cet environnement.

Dans la barre de menu de l'ordinateur virtuel s1, cliquez sur le bouton **Point de contrôle**, dans la zone **Nom du point de contrôle**, saisissez **Autorité de certification CorpRootCA** puis cliquez sur le bouton **Oui**.

Répétez cette manipulation pour créer un point de contrôle avec un nom identique (Autorité de certification CorpRootCA) sur tous les autres ordinateurs virtuels de cet atelier.

Ouvrez le gestionnaire Hyper-V, pour chaque ordinateur virtuel, sélectionnez l'ordinateur virtuel dans la partie centrale et vérifiez, dans la zone **Points de contrôle**, la présence du point de contrôle créé.