



service de maintenance informatique
des lycées pour l'e-éducation

Manuel d'Exploitation

ALCASAR : extrait pour les utilisateurs



Client :	Région Occitanie
Référence :	2018_SMILE_MEX_093
Version :	V1R0
Date :	03/08/2018
Niveau :	Utilisateur du Wifi IoRdi

1 Paramétrage des équipements utilisateurs

1.1 Paramètres réseau

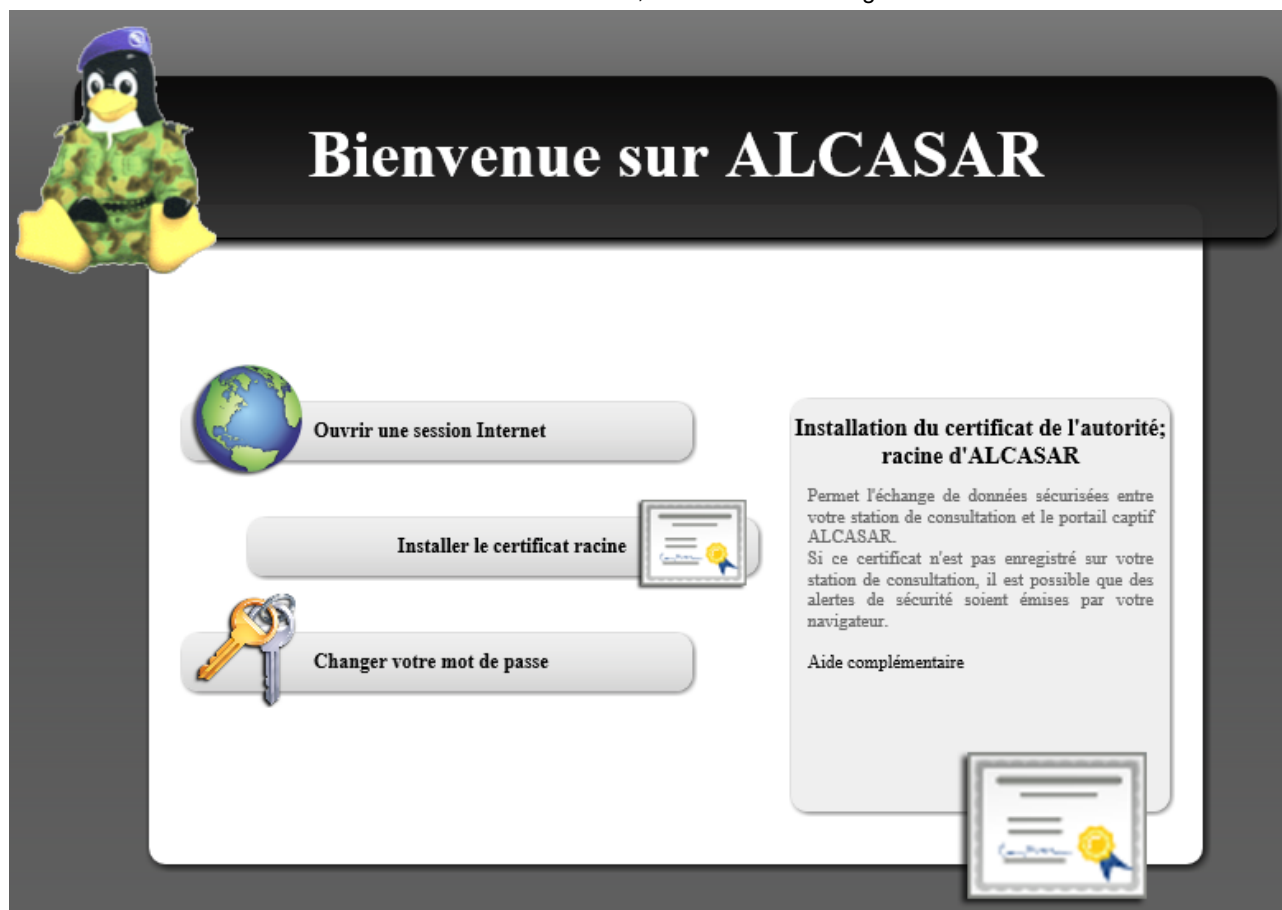
Le mode DHCP doit être activé sur les équipements des utilisateurs. Ces équipements ne nécessitent qu'un simple navigateur acceptant le langage « JavaScript ».

Pour être intercepté facilement par ALCASAR, il est conseillé de configurer la page de démarrage par défaut de ce navigateur sur un site WEB non chiffré (en HTTP) ou d'utiliser la page d'accueil d'ALCASAR : <http://alcasar-0312289v.localdomain/>.

Les paramètres de proxy ne doivent pas être activés.

1.2 Mire d'authentification

Lors d'une tentative d'accès à Internet sans être authentifié, l'utilisateur est redirigé vers l'écran suivant.



Après avoir cliqué sur « Ouvrir une session Internet », l'utilisateur est invité à s'authentifier via la page suivante :

'Lycée XXX - YYY'

Contrôle d'accès



La Région
Occitanie
Pyrénées - Méditerranée

Identifiant

Mot de passe

Authentification

Sécurité des Systèmes d'Information

- Ce contrôle a été mis en place pour assurer réglementairement la traçabilité, l'imputabilité et la non-répudiation des connexions.
- Les données enregistrées ne pourront être exploitées que par une autorité judiciaire dans le cadre d'une enquête.
- Votre activité sur le réseau est enregistrée conformément au respect de la vie privée.
- Ces données seront automatiquement supprimées au bout d'un an.
- Cliquez [ici](#) pour changer votre mot de passe ou pour intégrer le certificat de sécurité à votre navigateur



ATTENTION !

ALCASAR est sensible à la casse de l'identifiant (majuscules et minuscules sont prises en compte)

1.3 Ajout d'un favori / marque-page (bookmark)

Dans votre navigateur, il peut être pratique d'ajouter un favori pointant vers la page d'accueil d'ALCASAR (<http://alcasar-0312289v.localdomain>) afin de changer facilement votre mot de passe, de vous connecter/déconnecter ou d'intégrer le certificat de l'Autorité de Certification.

1.4 Intégration du certificat de l'Autorité de Certification d'ALCASAR

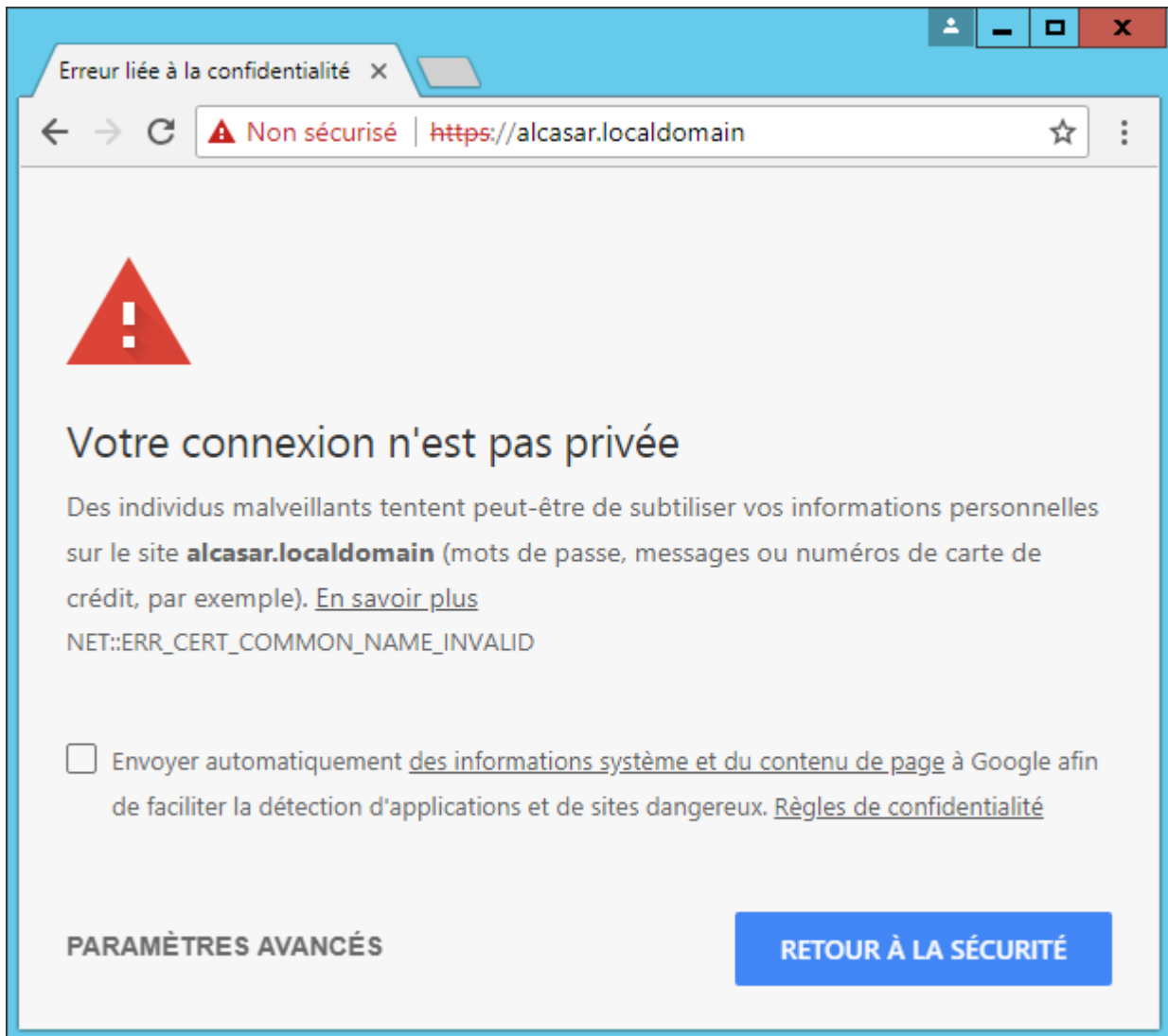
Certaines communications effectuées entre les équipements de consultation et ALCASAR sont chiffrées au moyen du protocole SSL (Secure Socket Layer).

Ce chiffrement exploite deux certificats créés lors de l'installation : le certificat d'ALCASAR et le certificat d'une Autorité de Certification locale (A.C.).

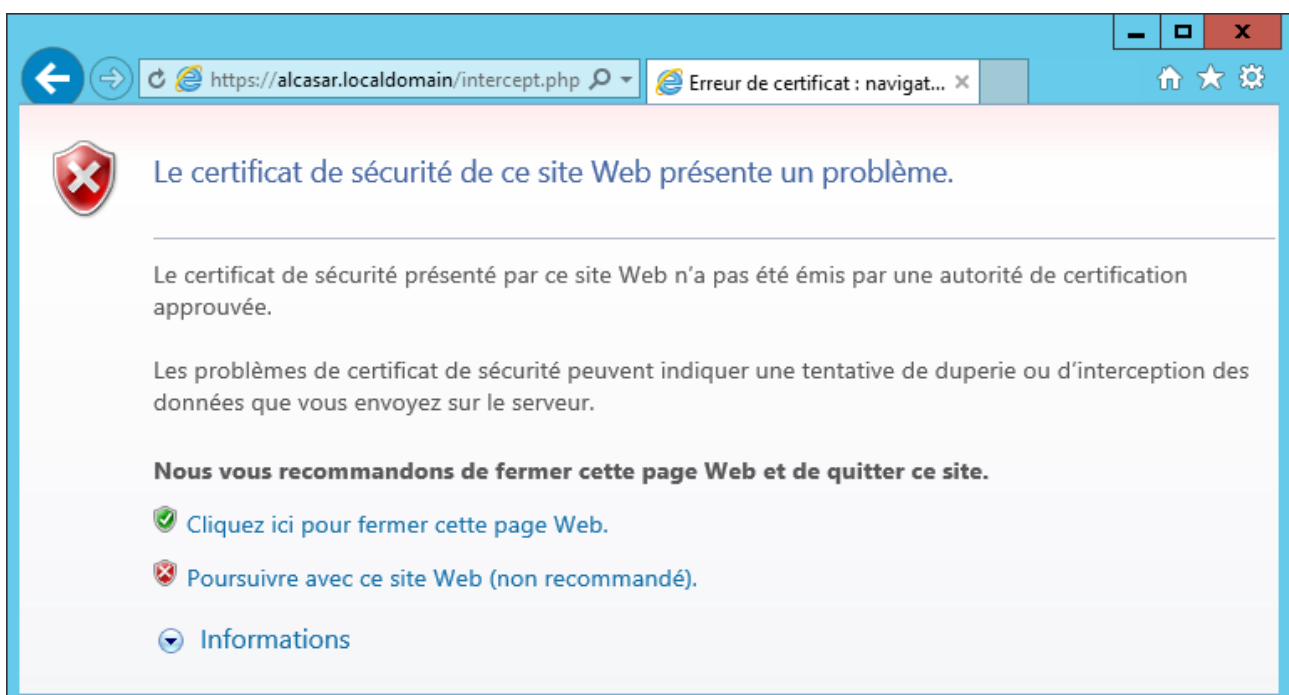
Par défaut, les navigateurs WEB situés sur le réseau de consultation ne connaissent pas cette autorité.

Ils présentent donc les fenêtres d'alerte suivantes lorsqu'ils communiquent pour la première fois avec ALCASAR.

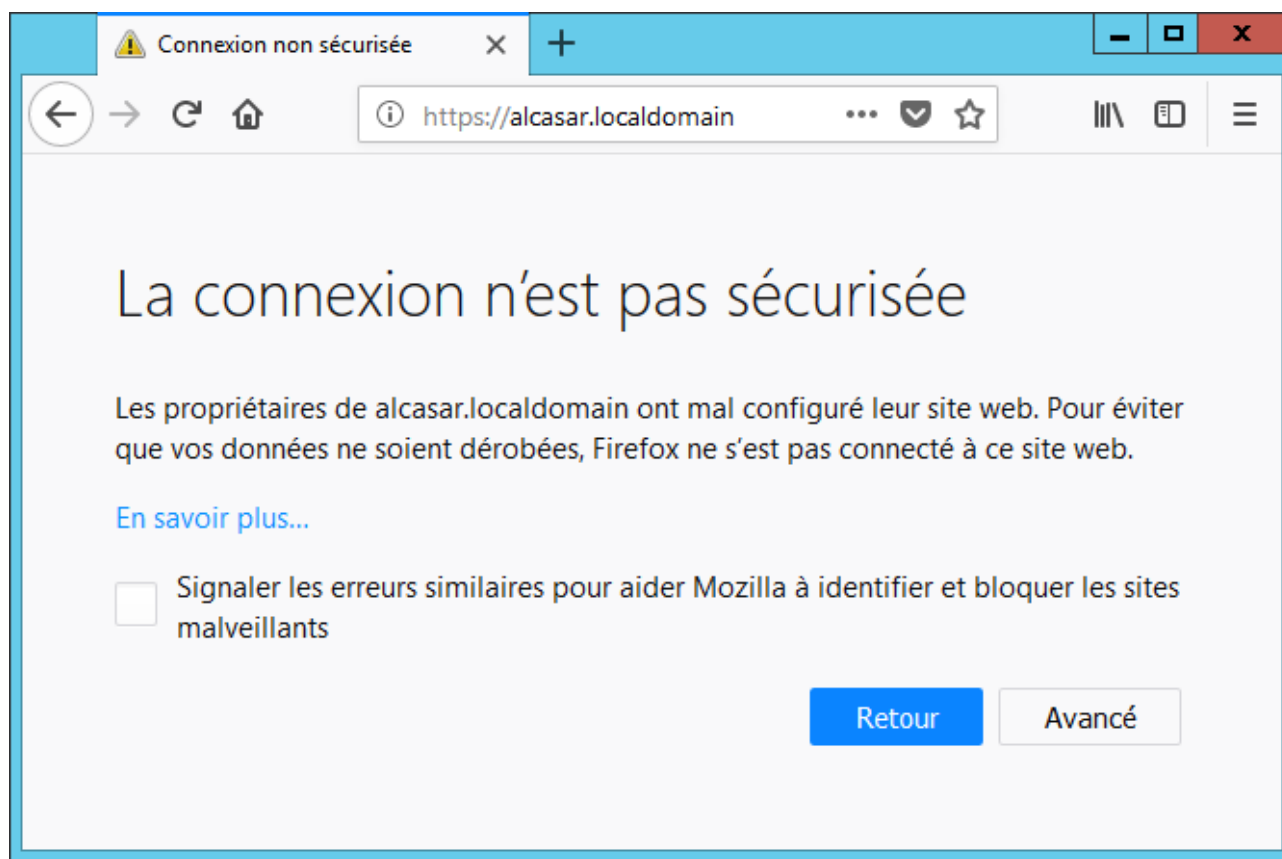
Pour Chrome :



Pour Internet Explorer :

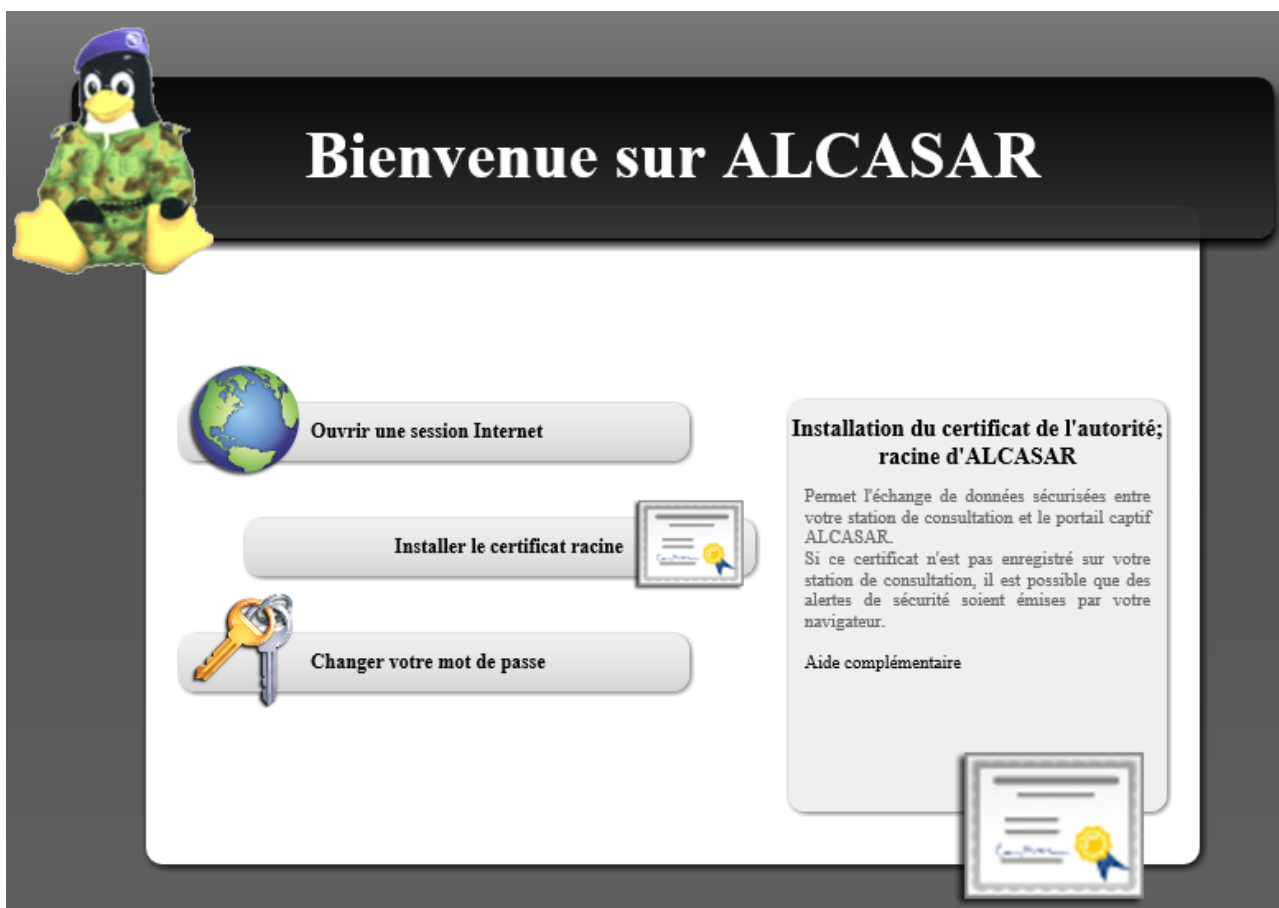


Pour Firefox :



Bien qu'il soit possible de poursuivre la navigation, il est intéressant d'installer le certificat de l'A.C. dans les navigateurs afin qu'ils ne présentent plus ces fenêtres d'alerte

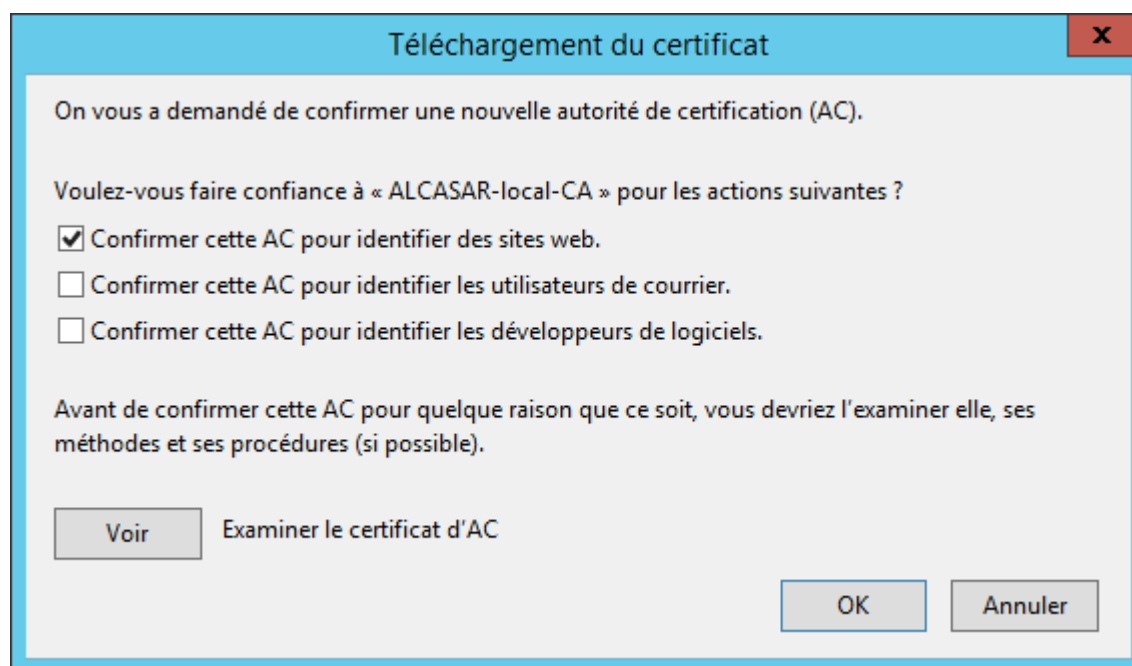
Pour cela, cliquez sur la zone « Installer le certificat racine » de la page d'accueil d'ALCASAR.



Pour chaque navigateur, l'installation est la suivante :

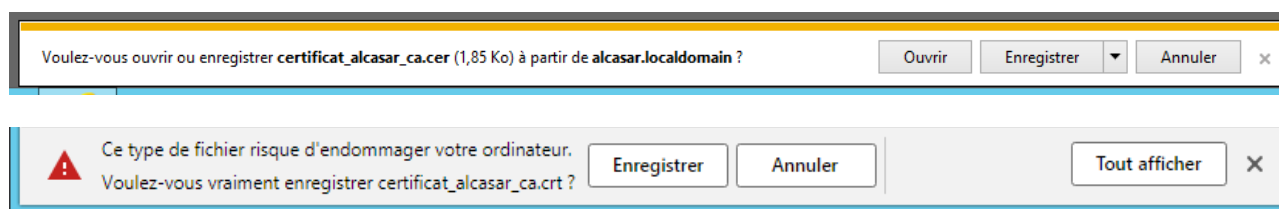
Pour Firefox :

Sélectionnez « Confirmer cette AC pour identifier des sites WEB ».



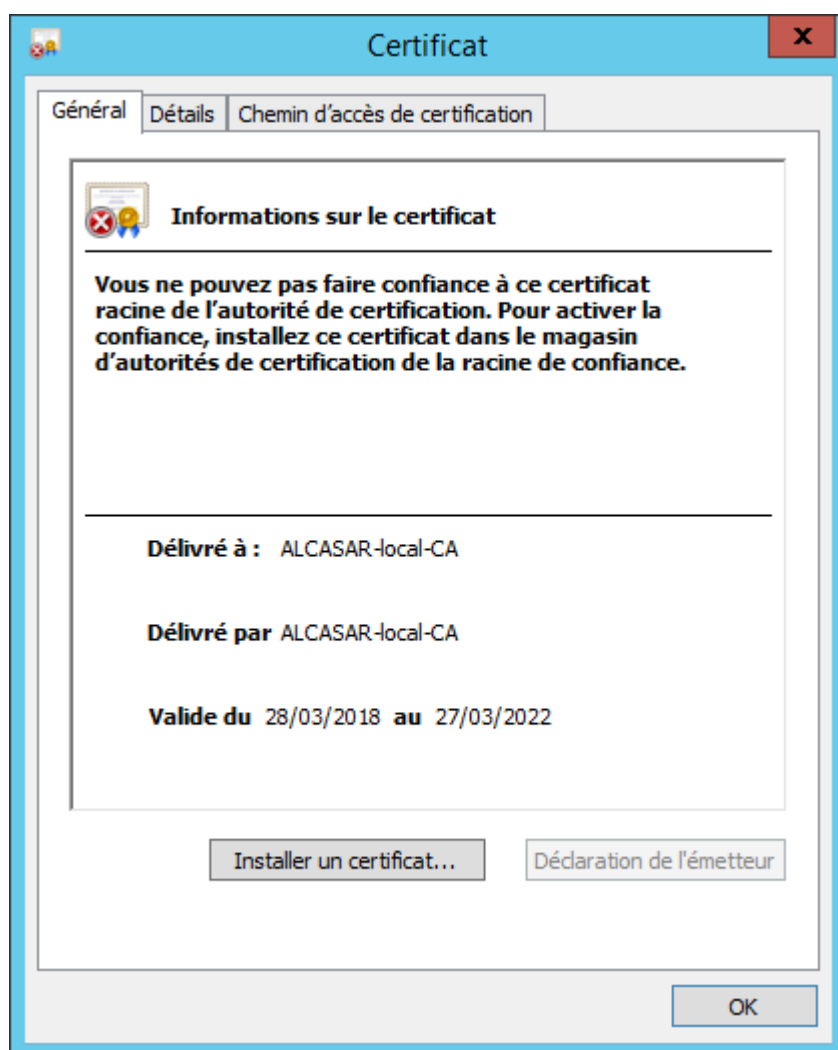
Pour Internet Explorer et Chrome :

Enregistrer le fichier « certificat_alcasa_ca.cer » sur l'ordinateur client.

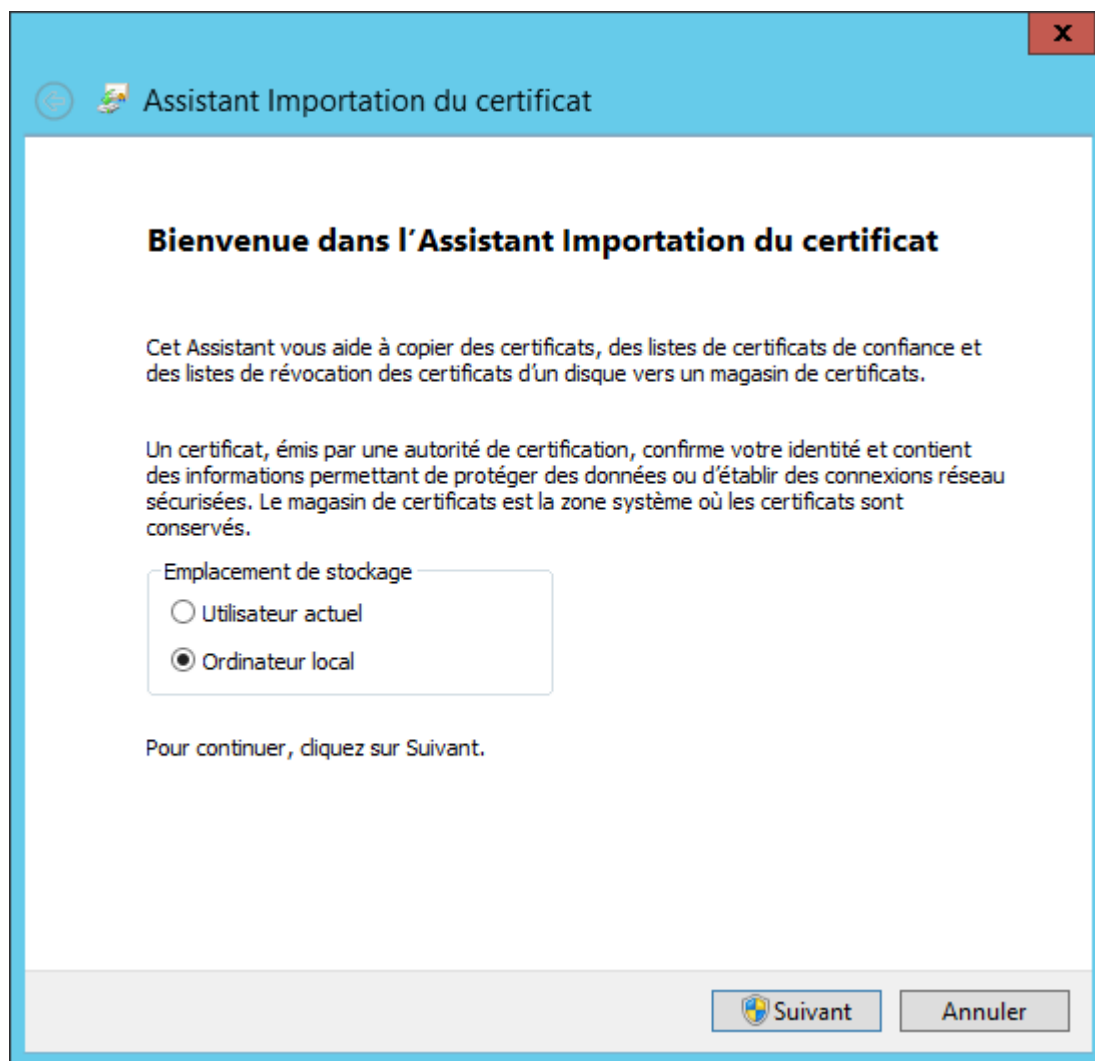


Aller dans l'emplacement où a été enregistré le fichier, faire un clic droit sur celui-ci et choisir « Ouvrir avec » puis « Extension noyau de chiffrement »

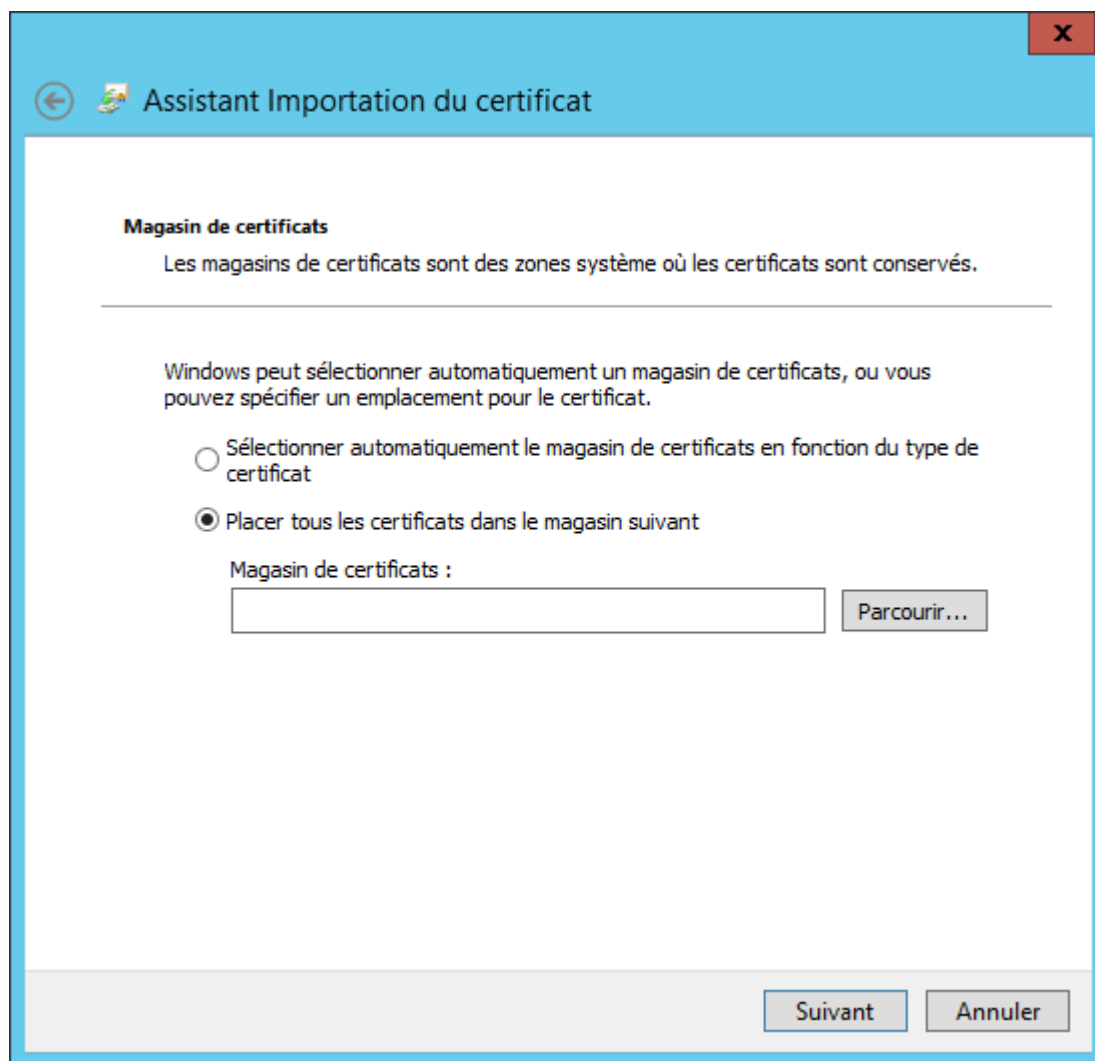
Dans la nouvelle fenêtre, cliquer sur « Installer un certificat... »



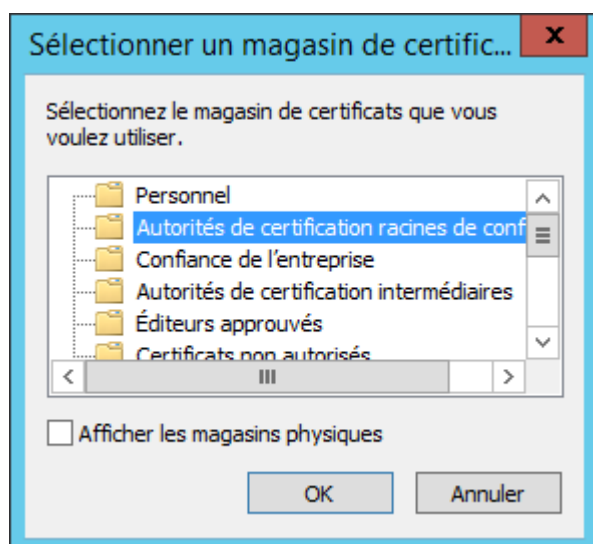
Choisir « Ordinateur local »



Choisir « Placer tous les certificats dans le magasin suivant » puis sur « Parcourir »



Choisir « Autorités de certification racines de confiance »



Valider jusqu'à avoir le message « L'importation a réussi. »