cirb.brussels
IT is for you

Fidus
services integrator
cirb-cibg

DOCUMENTATION - CERTIFICAT CLIENT

FIDUS

Table des matières

1. INTRODUCTION

1.1. RÔLE DU CERTIFICAT CLIENT FIDUS

Le certificat client FIDUS permet à FIDUS d'identifier l'institution cliente lors des requêtes à FIDUS. Par cette identification, FIDUS peut vérifier les droits d'accès aux différents services FIDUS.

Il y a un certificat par environnement FIDUS : TEST, STAGING et PRODUCTION. Ainsi, FIDUS peut également organiser la ségrégation entre environnement.

Il peut également y avoir plusieurs certificats par institution cliente. Une institution peut ainsi organiser la ségrégation au niveau de ses applications si nécessaire. Ceci est une possibilité mais pas une obligation.

Dans le certificat, l'Organization Unit (OU) fourni l'identifiant FIDUS de l'institution cliente. Si plusieurs certificats sont émis par le même client, il est important que cet identifiant (et donc le OU) soit le même pour tous les certificats. Il doit aussi être le même dans les trois environnements.

2. OBTENIR UN CERTIFICAT

Le certificat du client est fourni au client par le CIRB sur base d'un Certificate Signing Request (CSR) créé par le client.

Vous trouverez comment créer techniquement le CSR dans le document:

Documentation – Création de CSR FIDUS

Lors de la constitution du CSR, vous serez amené à protéger le certificat avec un mot de passe. Le certificat avec le mot de passe constitue la clé privée. Le certificat seul constitue la clé publique.

Conservez toujours ce mot de passe de manière sécurisée !
Ne l'envoyez jamais par mail, même à FIDUS ou au CIRB !
Ce mot de passe servira aussi lors du renouvellement des certificats

Ne le perdez pas(1) !

(1) En cas de perte, il faudra recommencer toute la procédure !

3. DESCRIPTION DU CSR

Un CSR est composé de plusieurs champs :

Common Name (CN)
Organization Unit (OU)
Organization (O)
Locality (L)
State/Region (SR)
Country (C)

3.1. COMMON NAME (CN)

3.1.1. Explications CN

FIDUS utilise ce champ pour identifier l'environnement FIDUS concerné et qu'il s'agit bien d'une certificat émis pour des appels à FIDUS.

Pour ce faire, le CN devra toujours être de la forme :

CN = application-test.fidus.brussels → pour l'environnement de test
CN = application-sta.fidus.brussels → pour l'environnement de staging
CN = application-prod.fidus.brussels → pour l'environnement de production

Attention, les parties en rouge ne peuvent pas être changées.

Application peut prendre toute valeur choisie par le client : par exemples un nom d'application, un nom de service ou encore un nom général

3.1.2. Exemples CN

CN = impala-test.fidus.brussels

CN = RH-sta.fidus.brussels

CN = lez-prod.fidus.brussels

3.2. ORGANIZATION UNIT (OU)

3.2.1. Explications OU

FIDUS utilise ce champ pour identifier l'institution cliente.

Pour ce faire, le OU devra toujours être de la forme :

OU = identifiant de l'institution

L' identifiant de l'institution peut prendre toutes les valeurs choisies par le client en respectant certaines règles :

- L'identifiant doit être unique pour l'institution. En effet, si deux identifiants différents sont utilisés pour la même institution, il faudra multiplier les configurations dans la banque de règle FIDUS. De même, des appels à FIDUS seront répertoriés comme deux institutions différentes (statistiques, reporting, audit logs, recherche d'incident, etc …)

- L'identifiant doit permettre de comprendre à la lecture, de quelle institution il s'agit. Les abréviations sont permises quand elle sont utilisées dans le langage courant et quelles sont non ambiguës. Cet identifiant sera utilisé dans les logs (et donc visible par le citoyen) ou dans les statistiques par exemple.

- L'identifiant doit donc être univoque. Une institution ne peut pas utiliser un identifiant déjà attribué à une autre institution.

L'équipe FIDUS peut vous aider dans le choix de cet identifiant.

Si votre institution change de nom, il faudra penser à terme à changer votre certificat.

3.2.2. Exemples OU

OU = SLRB

OU = Bruxelles Environnement

OU = COCOF[(1)]

(1) COCOF n'est plus une abréviation officielle (SPRBF) mais est encore largement utilisé.

3.3. ORGANIZATION (O)

3.3.1. Explications O

Ce champ est utilisé par l'Autorité Certificative (CA) pour identifier l'organisme émetteur de la demande de certificat. Pour les clients FIDUS, cet organisme est le CIRB.

Le O ne peut donc pas être modifié.

O = Centre d'Informatique pour la région Bruxelloise

3.4. LOCALITY, STATE/REGION, COUNTRY (L, S, C)

3.4.1. Explications L, SR et C

Ces champs sont utilisés par l'Autorité Certificative (CA) pour identifier la division administrative et le pays de l'émetteur de la demande de certificat.

Ces trois champs sont fixes et ne peuvent être modifiés.

L = Brussels
S = Brussels Region
C = BE

3.5. EXEMPLES COMPLETS

3.5.1. Exemple de certificat de test

CN = invoicing-test.fidus.brussels
OU = Bruxelles Environnement
O = Centre d'Informatique pour la Region Bruxelloise
L = Brussels
S = Brussels Region
C = BE

3.5.2. Exemple de certificat de staging

CN = invoicing-sta.fidus.brussels
OU = Bruxelles Environnement
O = Centre d'Informatique pour la Region Bruxelloise
L = Brussels
S = Brussels Region
C = BE

3.5.3. Exemple de certificat de production

CN = invoicing-prod.fidus.brussels
OU = Bruxelles Environnement
O = Centre d'Informatique pour la Region Bruxelloise
L = Brussels
S = Brussels Region
C = BE

4. PROCÉDURE D'OBTENTION DU CERTIFICAT

1- Constituer le CSR comme expliqué précédemment
2- Remplir le « Formulaire de demande de Certificat FIDUS »
3- Envoyer le « Formulaire de demande de Certificat FIDUS » à dlegrelle@cirb.brussels pour validation du CSR
4- Après validation du CSR, la demande sera transmise par l'équipe FIDUS à l'équipe sécurité du CIRB qui fera la demande de certification à Digicert
5- Dès réception du certificat, il vous sera retourné pour installation sur vos serveurs

5. FAQ

5.1. COMMENT CRÉER UN CSR ?

Toutes les explications se trouvent dans ce document et dans le document « Documentation – Création de CSR FIDUS ».

5.2. COMMENT VÉRIFIER LE CONTENU D'UN CSR ?

Copier la clé avec les balises

-----BEGIN NEW CERTIFICATE REQUEST----- et

-----END NEW CERTIFICATE REQUEST-----

Aller sur https://ssltools.digicert.com/checker/views/csrCheck.jsp

Collez la clé et ses balises dans le champ approprié

Cliquez sur le bouton Check CSR

Vérifier que tous les champs correspondent aux règles expliquées dans ce document

Faites particulièrement attention :

- aux accents/caractères spéciaux
- au contenu des champs CN, OU et O
- à l'algorithme de signature qui doit être SHA256
- à l'algorithme de clé qui doit être RSA
- à la taille de la clé qui doit être supérieure à 2048

5.3. QUELLES SONT LES ERREURS LES PLUS FRÉQUENTES LORS DE LA CRÉATION D'UN CSR ?

5.3.1. Inverser le contenu du O et du OU

Certains outils de création n'utilisent pas la même nomenclature.
Par exemple : département pour Organization Unit.

5.3.2. L'organisation doit toujours être le CIRB

Et plus précisément Centre d'Informatique pour la Region Bruxelloise

5.3.3. Le OU doit toujours être l'identifiant de votre institution

N'hésitez pas à demander conseil à l'équipe FIDUS

5.3.4. Le CN ne peut pas être dans votre domaine

Il doit être dans le domaine fidus.brussels

5.3.5. Je n'ai pas le password pour installer le certificat dans mon keystore

Demander à la personne qui a créer le CSR initial

5.3.6. Je ne sais pas qui a créé le CSR

L'équipe FIDUS peut, peut-être, vous renseigner sur la personne qui a fait la demande de certificat

5.3.7. Le mot de passe est définitivement perdu

Il faut refaire la procédure complète avec un nouveau CSR

5.4. QUAND DOIT-ON RENOUVELER LE CERTIFICAT ?

Les certificats sont faits pour une durée de deux ans. Deux mois avant leur expiration, le CIRB renouvelle automatiquement le certificat et vous le fourni (à la personne de contact).

Il vous suffit d'installer le certificat avec le mot de passe initial.

Si vous n'avez plus ce mot de passe, reportez-vous à la question précédente.

5.5. J'AI UN FOURNISSEUR QUI DÉVELOPPE MON APPLICATION. PEUT-IL UTILISER MES CERTIFICATS ?

NON. Il doit faire une demande au nom de sa société.
Il recevra un certificat de test et un autre de staging. Il ne recevra jamais de certificat de production.

5.6. J'AI UN CONSULTANT QUI TRAVAIL SUR L'APPLICATION, PEUT-IL UTILISER MES CERTIFICATS ?

OUI. Mais il le fera sous votre responsabilité.

5.7. PUIS-JE UTILISER LE MÊME CERTIFICAT POUR PLUSIEURS APPLICATION DE MON ORGANISATION ?

OUI.

5.8. PUIS-JE UTILISER LE MÊME CERTIFICAT POUR UNE MÊME APPLICATION, DÉVELOPPÉE POUR PLUSIEURS ORGANISATIONS DIFFÉRENTES?

Exceptionnellement, c'est possible mais pas conseiller.
Dans ce cas, il faudra gérer un LegalContext, différent pour chaque organisation, lors des appels à FIDUS.