cirb.brussels
IT is for you

Fidus
services integrator
cirb-cibg

DOCUMENTATION – CRÉATION DE CSR

FIDUS

Table des matières

1. INTRODUCTION

1.1. INFORMATION PRÉALABLE

Pour bien comprendre la manière dont le CSR doit être construit, il faut lire **impérativement** et **préalablement** la

Documentation – Certificat Client FIDUS

1.2. A PROPOS DE CETTE DOCUMENTATION

Cette documentation est une documentation technique destinée à un lecteur possédant un minimum de connaissances informatiques et plus spécialement de connaissances sur le fonctionnement des certificats.

Il existe de nombreux outils permettant de créer des certificats. Cette documentation se base sur l'outil **keytool et OpenSSL**. Nous ne pouvons pas faire une documentation pour tous les outils existants sur le marché.

Le lecteur devra faire les liens et les adaptations nécessaires à l'utilisation d'autres outils. La littérature abondante disponible sur Internet permettra de répondre aux interrogations éventuelles du lecteurs sur le sujet.

Enfin, cette documentation utilise des exemples pour illustrer le processus. Il est important de lire préalablement la

Documentation – Certificat Client FIDUS

Pour comprendre ce qui doit être changé et ce qui doit obligatoirement être conserver dans les exemples. Les parties qui doivent être adaptée à la situation du client seront reprises en **vert** dans ce document.

2. ETAPES SUCCESSIVES

La génération d'un certificat FIDUS et son utilisation dans vos applications seront réalisés suivant les étapes :

	Etapes	Documentations / Formulaires
1	Génération d'un Certificate Signing Request (CSR)	Documentation – Certificat Client FIDUS Documentation – Création de CSR FIDUS
2	Envoi d'une demande de certificat FIDUS	Formulaire de demande de certificat FIDUS
3	Installation d'un certificat FIDUS	Documentation – Création de CSR FIDUS
4	Utilisation du certificat dans vos applications	Documentation – Certificat Client FIDUS
5	Renouvellement d'un certificat FIDUS	Documentation – Certificat Client FIDUS Documentation – Création de CSR FIDUS

3. GÉNÉRATION D'UN CERTIFICAT X509

Un certificat x509 est composé d'une clé publique et d'une clé privée. Lors de la création du certificat, vous devez fournir un certain nombre de champs :

Champ		Usage
Common Name	CN	CN= ***application cliente***-{test, sta, prod}.fidus.brussels
Organization Unit	OU	OU= ***organisation cliente***
Organization	O	O= Centre d'Informatique pour la Région Bruxelloise
Locality	L	L= Brussels
State/Region	S	S= Brussels Region
Country	C	C= BE

Exemple d'un certificat de **production** :

CN= **impala**-prod.fidus.brussels
OU= **SPRB-GOB**
O= Centre d'informatique pour le Région Bruxelloise
L= Brussels
S= Brussels Region
C= BE

4. UTILISATION DE KEYTOOL

4.1. CRÉATION D'UN KEYSTORE

Pour créer un keystore contenant une paire de clés publique/privée vous aurez besoin de deux mots de passe. Un pour le keystore et un pour la clé privée.

Conservez précieusement ces deux mots de passe. Leur perte ou leur diffusion impliquera la réalisation d'une nouvelle procédure complète de demande de certificat. Ne les transmettez jamais par e-mail. Ne les diffusez jamais à des personnes non habilitées de votre organisation. Ne les transmettez jamais à des personnes en dehors de votre organisation.

	**Gardez le fichier contenant la clé privée (.key / .jks) en sécurité** **Ne l'envoyez pas avec la demande** **Ne l'envoyez jamais par e-mail non protégée**

Generate using keytool
Keytool -genkeypair -alias "**impala-prod**" -keyalg RSA -keysize 2048 -keystore **monkeystore_prod.jks** -dname "CN=**impala**-prod.fidus.brussels, OU=**SPRB-GOB**, O=Centre d'informatique pour la Région Bruxelloise, L=Brussels, S=Brussels Region, C=BE"

4.2. GÉNÉRATION D'UN CSR AVEC KEYTOOL

Pour générer une demande de certificat à partir d'une paire de clés (voir ci-dessus), copiez et adaptez la commande suivante :

Generate using keytool
keytool -certreq -alias "**impala-prod**" -file **impala-prod**.csr -keystore **monkeystore_prod**.jks

4.3. INSTALLATION DU CERTIFICAT SIGNÉ AVEC KEYTOOL

Le CSR sera utilisé pour remplir le

Formulaire de demande de certificat FIDUS

Envoyez ce CSR à dlegrelle@cirb.brussels
En retour, vous recevrez une clé publique certifiée par DIGICERT.

Pour l'installer dans un keystore vous devez utiliser la commande suivante :

Generate using keytool
keytool -importcert -alias "**impala-prod**" -file **impala-prod**.csr -keystore **monkeystore_prod**.jks

5. UTILISATION DE OPENSSL

5.1. GÉNÉRATION D'UN CSR AVEC OPENSSL

Vous devez avoir accès à une machine sur laquelle OpenSSL est installé.
Si votre application utilise des fichiers « server.key » et « server.crt », cette méthode est recommandée.

5.1.1. A partir d'une clé privée existante

Tapez sur une ligne la commande suivant, en effectuant les substitutions nécessaires (voir ci-dessous) :

Generate using openssl

```
openssl req
  -new
  -key impala.key
  -out impala.csr
  -subj"/CN=impala-prod.fidus.brussels/OU=SPRB-GOB/
O= Centre d'Informatique pour la Région Bruxelloise
/L=Brussels/ST=Brussels Region/C=BE"
```

5.1.2. Sans clé privée existante

Tapez sur une ligne la commande suivant, en effectuant les substitutions nécessaires (voir ci-dessous) :

Generate using openssl

```
openssl req
  -new
  -newkey rsa:2048
  -keyout impala.key
  -out impala.csr
  -subj"/CN=impala-prod.fidus.brussels/OU=SPRB-GOB/
O= Centre d'Informatique pour la Région Bruxelloise
/L=Brussels/ST=Brussels Region/C=BE"
```

5.2. INSTALLATION DU CERTIFICAT SIGNÉ AVEC OPENSSL

Le CSR sera utilisé pour remplir le

Formulaire de demande de certificat FIDUS

Envoyez ce CSR à dlegrelle@cirb.brussels
En retour, vous recevrez une clé publique certifiée par DIGICERT.

Pour l'installer dans un keystore vous devez utiliser la commande suivante :

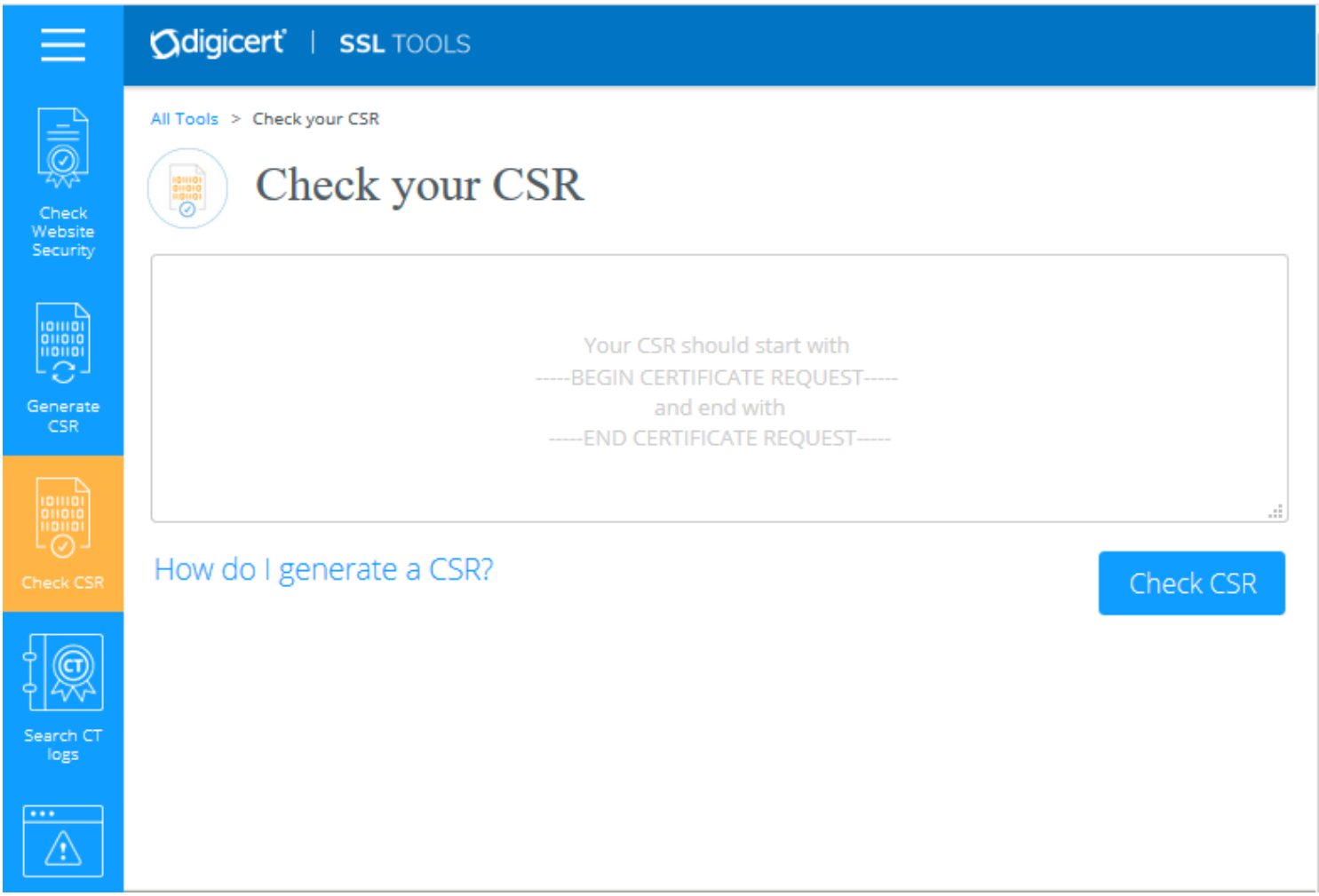
Generate using openssl

```
openssl
    pkcs12
    -export
    -chain
    -CAfile impala.crt
    -in domain.crt
    -inkey priv.keystore
    -out <certificate>.keystore
    -name ssl
    -passout pass:<password>
```

6. VÉRIFICATION DE VOTRE CERTIFICAT

Vous pouvez vérifier que votre certificat contient bien les champs attendus par FIDUS à l'adresse : https://ssltools.digicert.com/checker/views/csrCheck.jsp

Copiez la clé avec les balises et placez la dans l'encadré



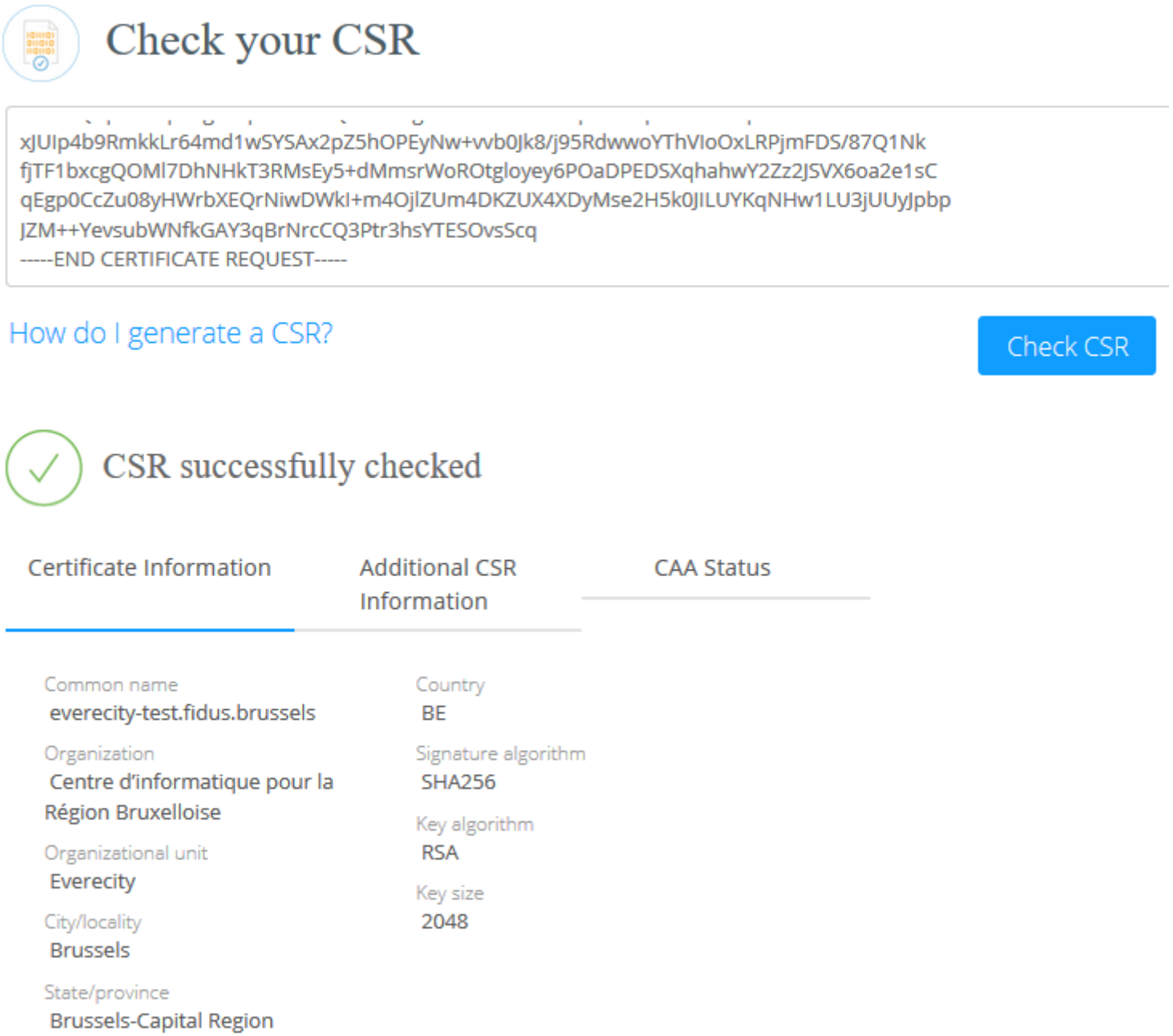
Cliquez sur le bouton Check CSR

Vérifier que tous les champs correspondent aux règles expliquées dans la

Documentation – Certificat Client FIDUS

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



7. RENOUVELEMENT DU CERTIFICATE

Le certificat est valable pour une durée limitée. Celle-ci est actuellement de deux ans.

Vous recevrez automatiquement un nouveau certificat avant la date d'expiration du certificat qui va arriver à expiration. Vous devrez installer ce nouveau certificat en suivant les instructions du point 4.4 précédent pour keytool ou du point 5.2 précédent pour openssl.

Attention, vous aurez besoin du mot de passe de la clé privée

	**Gardez en sécurité le mot de passe de la clé privée.** **Si vous l'oubliez, vous ne pourrez pas utiliser le certificat généré.**