GUIDE ÉLÉMENTAIRE DU SSL

Travailler en toute sécurité dans un monde numérique

certificat.fr

16 - 11 - 2020 V1.7.1

Que trouverez-vous dans notre guide ?

"SSL est la technologie de sécurité standard pour établir un lien crypté entre un serveur web et un navigateur. Ce lien garantit que toutes les données transmises entre le serveur web et le navigateur restent privées."

Introduction

Le guide élémentaire du SSL est une introduction aux certificats SSL/TLS. Nous présentons les différents types, méthodes de validation, prix et marques, mais aussi les différents formats de fichiers de certificats et la facilité avec laquelle la gestion des certificats peut être effectuée. Sans avoir à tenir vous-même des listes Excel, vous pouvez stocker toutes vos notes sur une seule plateforme et garder le contrôle de vos certificats SSL grâce au rapport de gestion standard inclus.

Le fonctionnement d’un certificat

SSL / TLS assure le cryptage, l’intégrité et l’authentification des données.
Cela signifie que lorsque vous utilisez SSL / TLS, vous pouvez avoir confiance :

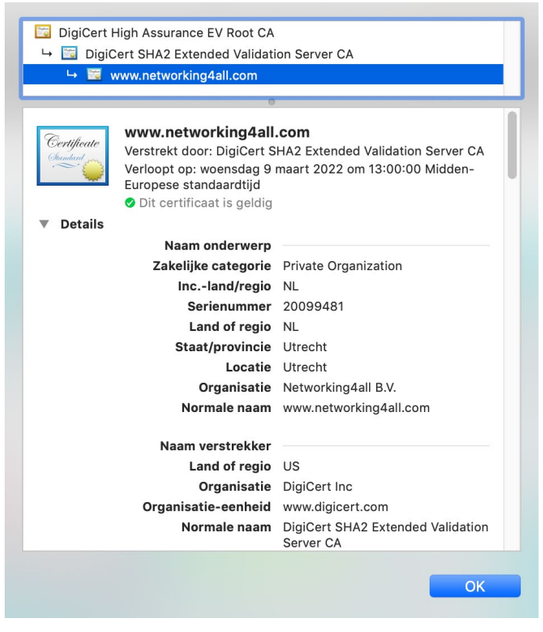
- Personne n’a lu votre message
- Personne n’a modifié votre message
- Que vous communiquez avec le bon serveur

Chiffrement
Si un message est envoyé sur Internet, par exemple un formulaire web, il est envoyé non crypté par défaut. Partout où passe le message, on pourrait lire ces données, comme on envoie une carte postale. Les certificats SSL sont conçus pour crypter ces données. Considérez que c’est une lettre entourée d’une enveloppe. Ces données cryptées ne peuvent être déchiffrées que par la partie qui possède la bonne clé. Le message envoyé peut bien sûr toujours être intercepté, mais comme les données sont cryptées, on ne peut rien en faire.

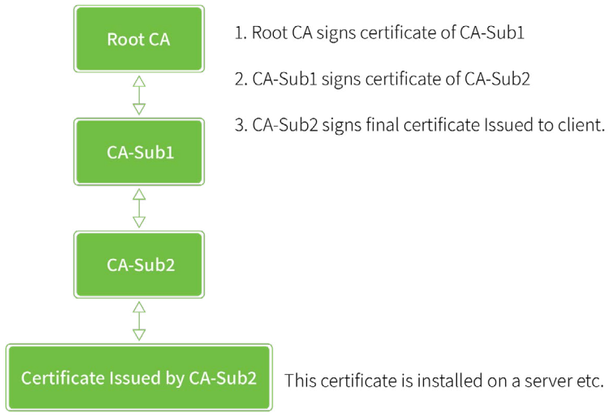
Les données sont cryptées selon un certain algorithme de chiffrement. L’algorithme transforme les données en un texte chiffré illisible. Avec les certificats SSL, nous utilisons un chiffrement asymétrique. La cryptographie asymétrique utilise deux clés distinctes : une clé est utilisée pour chiffrer ou signer l’information, c’est la “clé publique”. La deuxième clé est utilisée pour décrypter à nouveau les informations, c’est la “clé privée”.

La clé privée se trouve sur votre serveur et reste toujours sous votre contrôle. Nous vous fournissons la clé publique avec laquelle les tiers peuvent crypter leurs messages. Après installation du certificat SSL sur votre serveur web, le chiffrement et déchiffrement seront effectués de manière entièrement automatique par votre serveur web et le visiteur.

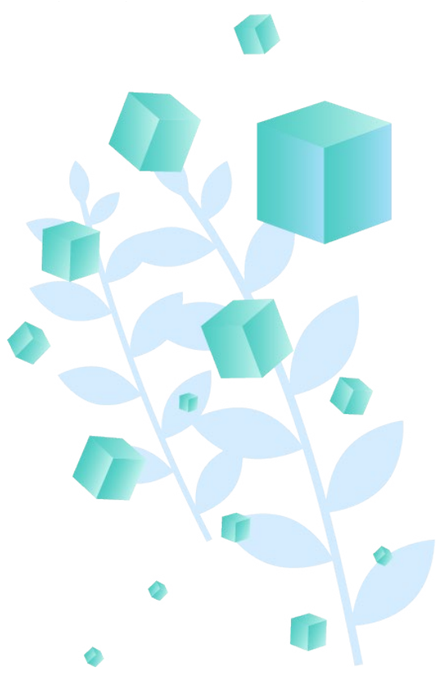
Identification
Le fonctionnement de base d’un certificat SSL est le cryptage. En plus de cela, il peut remplir une autre fonction, à savoir l’identification. Comment savoir si le certificat SSL a été délivré à la bonne entité ? Imaginez un site web frauduleux qui ressemble beaucoup à votre site web au niveau de son nom de domaine. Parfois, ce n’est qu’un caractère différent de l’original. En ajoutant les coordonnées de votre entreprise dans le certificat SSL, tout le monde peut voir que le certificat SSL est valable pour votre entreprise et votre nom de domaine et il est certain que les données arrivent au bon destinataire.



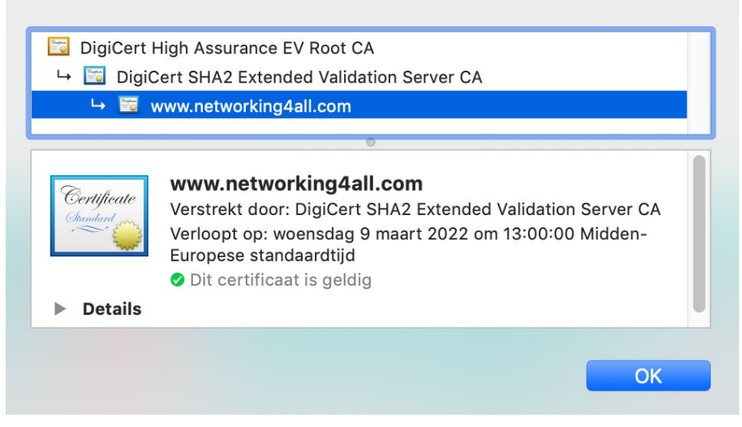
CA chain



Votre navigateur contient un certain nombre de certificats racine, y compris ceux que nous émettons. Le CA-Sub1 est donc automatiquement approuvé par le navigateur. Dans cet exemple, sous CA-Sub2, vous verrez le certificat final, celui de votre site Web. On voit souvent un sous CA, mais parfois aussi plusieurs. Il est donc important que l’autorité de certification racine soit approuvée par défaut sur votre ordinateur portable ou professionnel. En raison du fonctionnement de la chaîne, le certificat SSL émetteur sera également automatiquement approuvé par chaque navigateur. Par exemple, si un intermédiaire (CA-sub) est manquant, le certificat SSL ne sera pas approuvé. Vérifiez donc toujours votre installation SSL avec un vérificateur SSL tel que https://www.certificat.fr/quickscan pour vous assurer que votre configuration SSL est optimale.

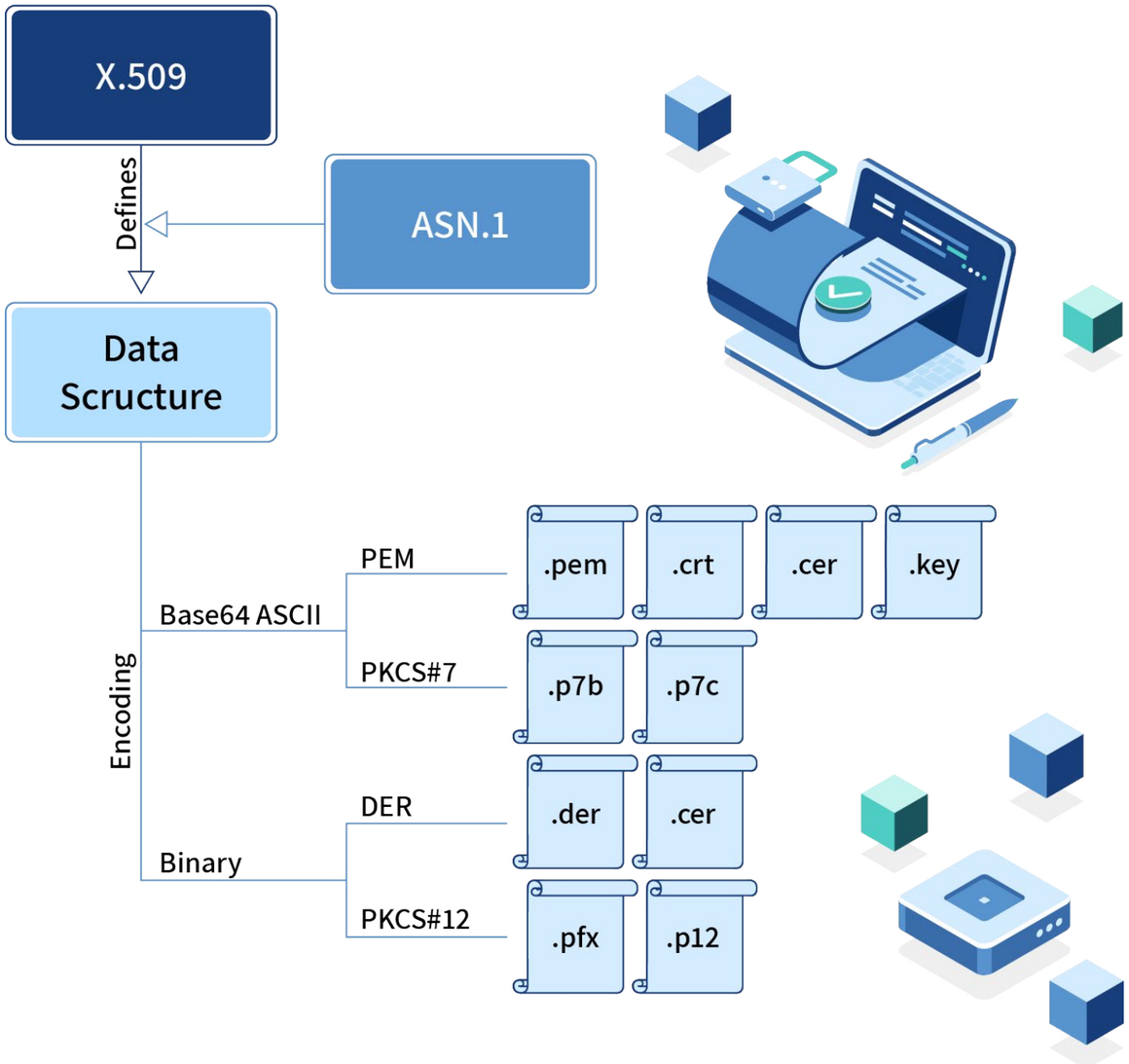


Ci-dessous notre certificat SSL. Le certificat racine est Digicert, l’intermédiaire Digicert Extended Validation et le dernier le certificat SSL du site www.networking4all.com



Les formats d'un certificat SSL

Un certificat SSL est un certificat X.509. X.509 est une norme qui définit la structure du certificat. Il détermine les champs de données qui doivent être inclus dans le certificat SSL. X.509 utilise un langage formel appelé Abstract Syntax Notation One pour exprimer la structure des données du certificat. Il existe différents types d'extensions de fichier liées aux certificats SSL. Voici une explication des types les plus courants.



***.pem (Privacy enhanced Electronic Mail) & *.cer (Canonical Encoding Rules)**
La plupart des AC délivrent leurs certificats dans le format de fichier PEM ou CER. Ces certificats contiennent les données suivantes :

Reconnaissable par	:	"––BEGIN CERTIFICATE––" et "––END CERTIFICATE––"
Certificat	:	Oui
Certificat racine	:	Non
Certificat intermédiaire	:	Non
Clé publique	:	Oui
Clé privée	:	Non
Chiffrement	:	Base64 (chaque chaîne comporte 64 caractères)
Serveurs Web	:	IIS et APACHE

***.der (Distinguished Encoding Rules)**
Contient le certificat X.509 sous forme binaire, il a le même contenu, les différentes extensions sont uniquement pour la convenance de l'utilisateur. Certains systèmes demandent un .der, d'autres un .pem. Ces certificats sont principalement utilisés sur des serveurs web basés sur Java.

Reconnaissable par	:	"––BEGIN CERTIFICATE––" et "––END CERTIFICATE––"
Certificat	:	Oui
Certificat racine	:	Non
Certificat intermédiaire	:	Non
Clé publique	:	Oui
Clé privée	:	Non
Chiffrement	:	Binaire

***.pfx ou *.p12 (Personal Information Exchange Format)**
Ces fichiers contiennent une chaîne de certification complète, y compris les clés privées et publiques. Habituellement, ces fichiers sont générés sous forme de fichier de sauvegarde sur un serveur afin de pouvoir être importés ultérieurement en une seule opération. Cela peut être utile si, par exemple, vous souhaitez installer un certificat wildcard sur plusieurs serveurs. Comme ces fichiers contiennent également la clé privée, ils doivent être munis d'un mot de passe.

Certificat	:	Oui
Certificats racine	:	Oui
Certificats intermédiaire	:	Oui
Clé publique	:	Oui
Clé privée	:	Oui
Chiffrement	:	Binaire

***.p7b OU *.p7c (Cryptographic Message Syntax Standard)**
Ce type de fichiers est idéal pour importer et obtenir une chaîne de certification complète. Ces fichiers sont souvent utilisés par des serveurs et des pare-feux. Les certificats *.p7b et *.p7c sont la contrepartie des certificats *.pfx et *.p12, à l'exception du fait que le fichier *.p7b ne contient jamais la clé privée.

Reconnaissable par	:	"—–BEGIN PKCS7—–" et "—–END PKCS7—–—"
Certificat	:	Oui
Certificats racine	:	Oui
Certificats intermédiaire	:	Oui
Clé publique	:	Oui
Clé privée	:	Non
Chiffrement	:	Base64 (chaque chaîne comporte 64 caractères)

***.csr (Certificate Signing Request) OU *.p10**
Une demande de signature de certificat est presque toujours générée dans un fichier *.csr. Le fichier *.csr est soumis à l'AC et constitue la première partie de l'ensemble du certificat.

Reconnaissable par	:	"—– BEGIN NEW CERTIFICATE REQUEST —–" et "—– END NEW CERTIFICATE REQUEST —–"
Certificat	:	Non
Certificats racine	:	Non
Certificats intermédiaire	:	Non
Clé publique	:	Oui
Clé privée	:	Non
Chiffrement	:	Base64 (chaque chaîne comporte 64 caractères)

***.key (Private Key)**
Le fichier *.key est la sauvegarde de la clé privée et ne contient que la clé privée. Sur les systèmes Windows, la clé privée ne peut pas être exportée à partir d'un certificat. Cependant, avec OpenSSL (implémentation open source du protocole SSL/TLS), il est possible d'exporter la clé privée. La clé privée est créée selon le même processus que le *.csr.

Reconnaissable par	:	"—– BEGIN RSA PRIVATE KEY —–" et "—– END RSA PRIVATE KEY —–"
Certificat	:	Non
Certificats racine	:	Non
Certificats intermédiaire	:	Non
Clé publique	:	Non
Clé privée	:	Oui
Chiffrement	:	Base64 (chaque chaîne comporte 64 caractères)

Convertir un certificat au format PFX (PKCS #12)

Pour convertir le fichier d'un certificat (.pem / .crt / .cer) en un fichier .pfx, nous avons besoin de plusieurs choses.

1. La clé privée associée au certificat
2. Le certificat lui-même
3. Eventuellement un certificat intermédiaire ou racine de l'AC
4. OpenSSL

La conversion d'un certificat avec clé privée en PFX (PKCS #12)
peut être faite avec la commande OpenSSL suivante.

openssl pkcs12 -in certificat-ssl.cer -certfile cert-intermediaire.cer -certfile cert-racine.cer -inkey cle-privee.key -export -out certificat-ssl.pfx

OpenSSL vous demande d'entrer un mot de passe pour protéger votre clé privée. Conservez ce mot de passe dans un endroit sûr.

Les certificats SSL pluriannuels

Il est possible de commander des certificats SSL pluriannuels sur la base d'un abonnement de 1 à 6 ans. Cela s'applique uniquement aux certificats SSL des serveurs web, et non aux certificats de signature. Les certificats SSL pluriannuels sont disponibles pour les marques Digicert, Geotrust, Thawte et Networking4all.

Comment fonctionnent les certificats SSL pluriannuels ?
Les certificats SSL pluriannuels sont disponibles pour 2, 3, 4, 5 ou 6 ans. Si vous commandez ou renouvelez un certificat d'une durée de 2 ans ou plus, vous les utiliserez alors.
Cela signifie que vous achetez le SSL pour la période sélectionnée, avec un réémission du certificat une fois par an. Voir "Réémission annuelle du certificat" ci-après.

Réémission annuelle du certificat
Le processus est très simple, il s'agit en fait d'une réémission où le nouveau certificat a, à la fois une nouvelle date de début et de fin. Pour une réémission, il vous suffit de nous fournir un CSR et de passer par les étapes de validation. La réémission est possible dans un délai de 30 jours avant la date d'expiration du certificat.

Exemple:
Vous achetez un abonnement SSL d'une durée de 3 ans le 1er septembre 2020. Vous ne serez facturé qu'une seule fois et ne procéderez qu'à une seule configuration. A partir du 1er août 2021, vous-même ou votre équipe technique pourrez demander une réémission via le site web ou l'API en nous fournissant un nouveau CSR. Dès que la validation du domaine sera terminée, vous recevrez un nouveau certificat valable jusqu'au 1er septembre 2022. Il sera nécessaire de réinstaller le certificat sur le serveur.

Les certificats SSL DV, OV et EV

Les certificats SSL peuvent être divisés selon 3 validations différentes:
- Validation de Domaine
- Validation d'Organisation
- Validation Étendue

Certificats à Validation de Domaine (DV)
A utiliser pour : des sites web non publics

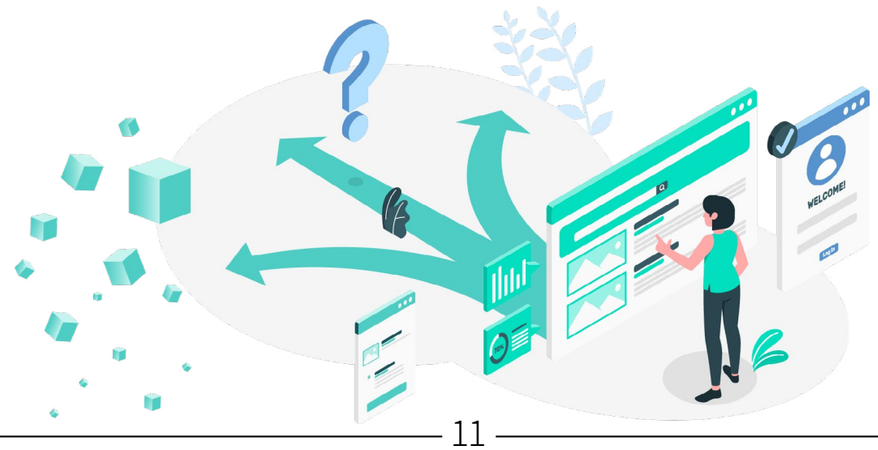
Dans le cas d'un certificat DV, aucune information sur l'entreprise n'est incluse dans le certificat et l'existence de l'organisme demandeur n'est pas vérifiée. Les certificats validés par domaine sont généralement délivrés sous 15 minutes après avoir approuvé l'accès au domaine par une validation par EMAIL, FICHIER ou DNS.

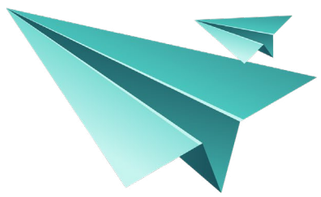
Certificats à Validation d'Organisation (OV)
À utiliser pour : des sites web publics sans but commercial ni entité gouvernementale

Dans le cas d'un certificat d'organisation, les coordonnées de l'entreprise sont incluses dans le certificat et l'existence de l'organisme demandeur est vérifiée. Il est également vérifié si la personne de contact travaille et a connaissance de la demande de SSL. En raison de cette validation étendue, les certificats OV donnent plus de confiance aux personnes avec lesquelles vous communiquez au moment où vous laissez vos coordonnées sur un certain site web. Les certificats validés par l'organisation sont généralement délivrés sous deux jours.

Certificats à Validation Étendue (EV)
A utiliser pour : des sites web commerciaux, e-commerce, institutions bancaires et gouvernementales.

Un certificat à Validation Étendue est l'un des processus de validation les plus étendus. Ce processus est comparable à celui d'un certificat OV, mais les données de l'organisation sont comparées dans plusieurs sources et un contrat EV est signé (numériquement). Les données organisationnelles d'un certificat EV peuvent être récupérées en 1 clic dans le navigateur (en fonction du navigateur). Le temps d'émission moyen de ce type de certificat est de 6 jours.





Les types de certificats SSL

Différents types de certificats SSL sont utilisés dans le cadre de chaque validation.

	Certificats DV	Certificats OV	Certificats EV
Un domaine	✓	✓	✓
SAN	✓	✓	✓
Wildcard	✓	✓	✗
Wildcard SAN	✓	✓	✗

Unité (1 domaine)
Une URL basée sur un domaine peut être incluse dans le certificat.
Par exemple : www.certificat.fr

SAN (Multi-domaines)
Plusieurs URL peuvent être incluses dans le certificat. Selon la marque, il peut s'agir uniquement de sous-domaines ou d'un mélange de sous-domaines et de domaines différents.
Par exemple : www.certificat.fr | api.certificat.fr | www.networking4all.com

Wildcard
Avec un certificat wildcard, vous pouvez sécuriser un nombre illimité de sous-domaines sur un même domaine racine.
Par exemple : *.certificat.fr

Wildcard SAN
Un certificat SAN wildcard vous permet d'ajouter plusieurs wildcard, sous-domaines et domaines différents dans un seul certificat.
Par exemple : *.certificat.fr | *.networking4all.com | www.ssl.nu

Les méthodes de validation SSL

Avant d'émettre le certificat SSL, un processus de validation est effectué.
Chaque type de certificat, DV, OV ou EV, a son propre processus de validation.

DV

Validation de Domaine
- Contrôle du domaine
- Contrôle CAA
- Délivrance sous 15 minutes

OV

Validation d'Organisation
- Contrôle du domaine
- Contrôle de l'organisation par plusieures sources
- Validation par téléphone
- Contrôle CAA
- Délivrance sous 2 jours

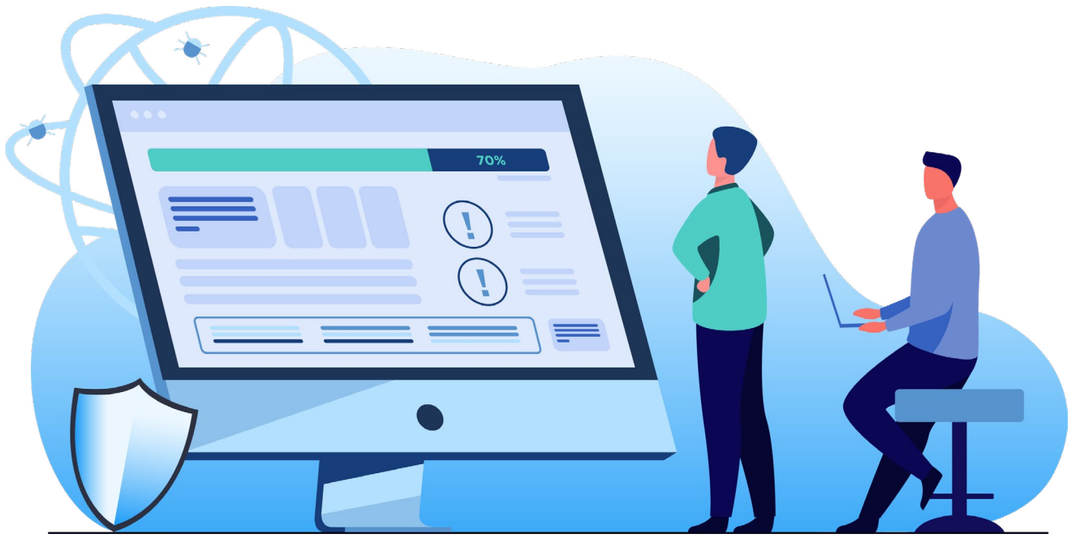
EV

Validation Étendue (EV)
- Contrôle du domaine
- Contrôle de l'organisation par le biais de diverses sources légales
- Vérification téléphonique avec le demandeur du certificat
- Signature digitale du contrat
- Contrôle CAA
- Délivrance sous 6 jours

Contrôle du domaine (DV, OV, EV)
Le contrôle de validation du domaine. Cela peut être fait de la manière suivante :

Option 1 - Par mail d'approbation
Un email d'approbation ne peut être envoyé qu'aux adresses email de domaine standard telles que admin, administrator, webmaster, hostmaster, postmaster@nomdedomaine.extension ou à l'adresse électronique enregistrée dans le Whois. L'adresse email du whois ne peut être utilisée par l´AC que si elle est visible dans le Whois

Adresse email 1 admin
Adresse email 2 administrator
Adresse email 3 webmaster
Adresse email 4 hostmaster
Adresse email 5 postmaster
Adresse email Whois 1 (si visible)
Adresse email Whois 2 (si visible)



Option 2 - Par entrée TXT/DNS
Si vous n'avez pas d'adresse électronique disponible ou si vous trouvez simplement plus facile de valider via un enregistrement TXT dans le DNS, cela est également possible. Vous pouvez nous solliciter pour obtenir le code de valeur aléatoire et le mettre en place. Il sera nécessaire de le laisser installé jusqu'à ce que le certificat soit délivré.

Option 3 - Par fichier d'authentification HTTP
Avec l'approbation par fichier HTTP, un fichier TXT peut être installé à un emplacement prédéfini contenant un code de valeur aléatoire que vous pourrez obtenir par nos services et mettre en place. Ne retirez pas le code avant émission du certificat.

Contrôle de validation à la Chambre de Commerce (OV, EV)
L'existence de l'organisation est vérifiée (nom selon les données du CSR) dans une des sources fiables telles que la Chambre de Commerce. Pour d'autres sources autorisées, veuillez nous contacter.

Vérification téléphonique auprès du demandeur du certificat (OV, EV)
L'Autorité de Certification (AC) prend contact par téléphone avec le demandeur du certificat selon une source générale, telle que Pages Jaunes.fr par exemple.
Contactez-nous pour plus d'informations sur d'autres sources autorisées.

Signature (digitale) du contrat EV
Pour terminer, au cours du processus de validation EV, un contrat EV doit être signé concernant l'accord avec l'autorité de certification et la confirmation des détails de l'organisation et de l'employé candidat au sein de la même organisation.

Contrôle CAA
Avant de pouvoir émettre un certificat, l'Autorité de Certification doit contrôler les enregistrements de ressource CAA (Autorisation des Autorités de Certification).

Cette mesure de sécurité permet aux propriétaires d'un nom de domaine de préciser dans leur DNS (Domain Name System) les autorités de certification (AC) qui sont autorisées à émettre des certificats pour leur nom de domaine.
Une AC est obligée de contrôler la ressource CAA depuis septembre 2017.

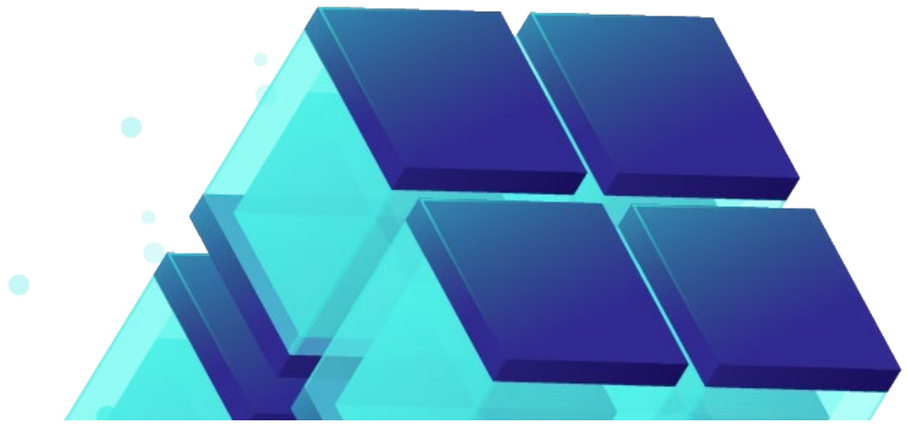
Si une AC reçoit une commande de certificat pour un nom de domaine avec un enregistrement CAA et qu'elle ne fait pas partie des émetteurs autorisés, elle ne sera pas autorisée à émettre le certificat pour ce domaine ou tout sous-domaine.
Si un enregistrement CAA d'une autre AC a été ajouté au domaine, alors un enregistrement CAA supplémentaire doit être ajouté auprès de l'AC, à la suite du certificat demandé, ou tous les enregistrements CAA sur le domaine devront être supprimés.

Le code CAA pour Networking4all (certificat OV) et GlobalSign :
CAA 0 issue ''globalsign.com''

Le code CAA pour Networking4all EV, Digicert, Geotrust, et Thawte :
CAA 0 issue ''digicert.com''

Pour les certificats Wildcard, il est nécessaire d'enregistrer 2 codes CAA :
CAA 0 issue wild ''globalsign.com''
CAA 0 issue ''globalsign.com''
CAA 0 issue wild ''digicert.com''
CAA 0 issue ''digicert.com''

Délivrance
Le processus de validation du certificat est vérifié par un second agent, après quoi, le certificat peut être délivré. Il est alors envoyé par mail dans un fichier zip à l'adresse électronique de la personne de contact chargée de la commande initiale.



Le profil de validation SSL

Avec les commandes de Networking4all, Digicert, Thawte et Geotrust OV et EV, le profil du domaine et de l'organisation peut être réutilisé pendant 1 an, à condition que les nouvelles commandes (ou les renouvellements) correspondent au profil.

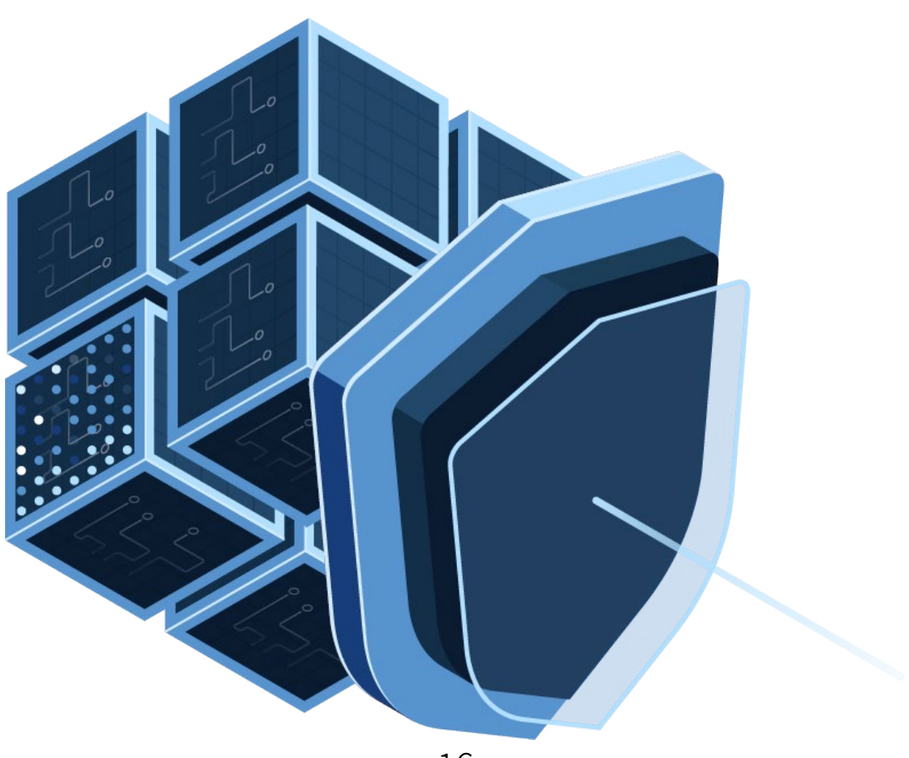
Par exemple:

Profil de l'organisation:
Networking4all BV
Weg der Verenigde Naties 1
3527KT Utrecht
Pays-Bas

Profil du domaine:
www.certificat.fr

Si vous renouvelez le certificat dans un délai d'un an ou si vous passez une nouvelle commande avec les mêmes coordonnées (y compris la même personne de contact), le certificat sera délivré plus rapidement en raison de la réutilisation des profils sauvegardés.

Globalsign offre le certificat ´´Ready SSL´´ adapté pour les certificats OV et EV, une solution similaire, alors que Networking4all, Digicert, Thawte et Geotrust utilisent la validation de profil par défaut, ce qui n'est pas le cas avec Globalsign. Il s'agit d'un service personnalisé, à commander séparément.



Les certificats SSL Networking4all

Networking4All/Certificat.fr a plus de 20 ans d'expérience dans le domaine des certificats SSL et de la gestion de portefeuille SSL. En tant que partenaire Platinum Elite de Digicert, après de nombreuses années de coopération, une ligne de marque blanche SSL de premier plan a été établie, basée sur la racine Digicert. Racine très solide et depuis longtemps attestée. Ceci en association avec les avantages de Networking4All/Certificat.fr tels qu'un service et support rapides et flexibles.

Les certificats SSL Networking4ALL

- ✓ **Un service de qualité de Networking4all/Certificat.fr**
- ✓ **Délivré sur la racine fiable de Digicert**
- ✓ **Domaine sans www délivré gratuitement**
- ✓ **Garantie SSL**
- ✓ **Intermédiaire marque blanche, possibilité de vendre des certificats sous votre propre nom**
- ✓ **Priorité validation et support**
- ✓ **Prix adaptés**
- ✓ **Paiement différé**
- ✓ **Validation du profil**
- ✓ **Rapports sur la sécurité et la gestion des certificats SSL**

Les certificats à Validation de Domaine
Networking4all Basic SSL DV
Networking4all Basic SSL DV Plus
Networking4all Basic SSL DV SAN
Networking4all Basic SSL DV Wildcard
Networking4all Basic SSL DV Wildcard SAN

Les certificats à Validation d'Organisation
Networking4all Business SSL OV
Networking4all Business SSL OV SAN
Networking4all Business SSL OV Wildcard (SAN)

Les certificats à Validation Étendue
Networking4all Business SSL EV
Networking4all Business SSL EV SAN

SSL Garantie
La garantie SSL est le montant de garantie maximal que l'autorité de certification peut verser à l'utilisateur si le certificat est émis à un tiers non autorisé et seulement si l'utilisateur a subi un préjudice financier.

Les marques SSL

Networking4all/Certificat.fr a depuis plus de 15 ans une coopération très étroite avec les marques SSL suivantes :

DigiCert
DigiCert est une société de sécurité américaine spécialisée dans les certificats SSL. En 2017, DigiCert est devenu propriétaire du groupe Symantec ; les marques SSL Symantec, Thawte, GeoTrust sont désormais sous la bannière de DigiCert. Networking4all a, ces dernières années, beaucoup travaillé en collaboration avec DigiCert pour commercialiser leur marque au sein du Benelux. Notre coopération nous a donc valu le statut de Partenaire Elite Platine.

Certificats Digicert Basic SSL

- ✓ Données organisationnelles dans le certificat
- ✓ Validation de l'organisation et du demandeur, délivrance 1-2 jours
- ✓ Améliore votre référencement dans Google
- ✓ Sous-domaine sans www gratuit inclus, si demande du nom de domaine principal placée avec www
- ✓ Garantie SSL Digicert Basic 1.000.000 $

Certificats Digicert Business Secure Site SSL
La ligne Digicert Secure Site présente les avantages supplémentaires suivants par rapport à la ligne Basic SSL :

- ✓ Les utilisateurs Secure Site SSL ont la priorité en terme de support et de validation
- ✓ Possibilité pour les utilisateurs Secure Site d'utiliser le sceau Norton Secured Seal pour votre site internet. L'un des logos les plus reconnus en ligne en matière de sécurité/confiance
- ✓ Secure Site OV offre une garantie SSL supérieure de 1 750 000 $
- ✓ Les utilisateurs de certificats Secure Site OV ont accès à une vérification de logiciels malveillants grâce à plus de 70 scanners antivirus et à des services de liste noire d'URL/domaines pour une vérification rapide des logiciels malveillants

Certificats Digicert Secure Site Pro SSL
La ligne Digicert Secure Site Pro présente les avantages supplémentaires suivants par rapport à la ligne Digicert Business Secure Site :

- ✓ Secure Site Pro OV offre une garantie SSL de 2.000.000 $
- ✓ Contrôle cloud CT Logs
- ✓ Cryptographie Post-Quantique de nouvelle génération (Post-Quantum Crypto-Ready)

Thawte
Thawte tient ses origines d'Afrique du Sud. En 2010, Symantec de Verisign a acquis la marque et aujourd'hui, Thawte fait partie de l'AC Digicert.

Les certificats à Validation de Domaine
Thawte SSL123
Thawte SSL123 SAN
Thawte SSL123 Wildcard

Les certificats à Validation d'Organisation
Thawte SSL Web Server
Thawte SSL Web Server SAN
Thawte SSL Web Server Wildcard

Les certificats à Validation Étendue
Thawte SSL Web Server EV
Thawte SSL Web Server EV SAN
Thawte SSL Web Server EV Wildcard

Geotrust
Geotrust est un fournisseur de certificats numériques fondé en 2001. GeoTrust a été repris par Symantec de Verisign en 2010 et fait maintenant partie de l'AC Digicert.

Les certificats à Validation de Domaine
Geotrust Quickssl Premium
Geotrust Quickssl Premium SAN
Geotrust Quickssl Premium Wildcard

Les certificats à Validation d'Organisation
Geotrust TruebusinessID
Geotrust TruebusinessID Multi-domain
Geotrust TruebusinessID Wildcard

Les certificats à Validation Étendue
Geotrust TruebusinessID with EV
Geotrust TruebusinessID Multi-domain with EV

GlobalSign
GlobalSign a été créé en Belgique en 1996. Après quoi, elle a été rachetée par sa société mère japonaise GMO Cloud. Grâce à cette origine intercontinentale, GlobalSign est devenu leader du marché SSL en Europe et au Japon. Certificat.fr/Networking4all a, ces dernières années, beaucoup travaillé avec GlobalSign pour commercialiser leur marque au sein du Benelux. Notre coopération nous a donc valu le statut de Preferred Partner.

Les certificats à Validation de Domaine
Globalsign DomainSSL
Globalsign DomainSSL SAN
Globalsign DomainSSL Wildcard

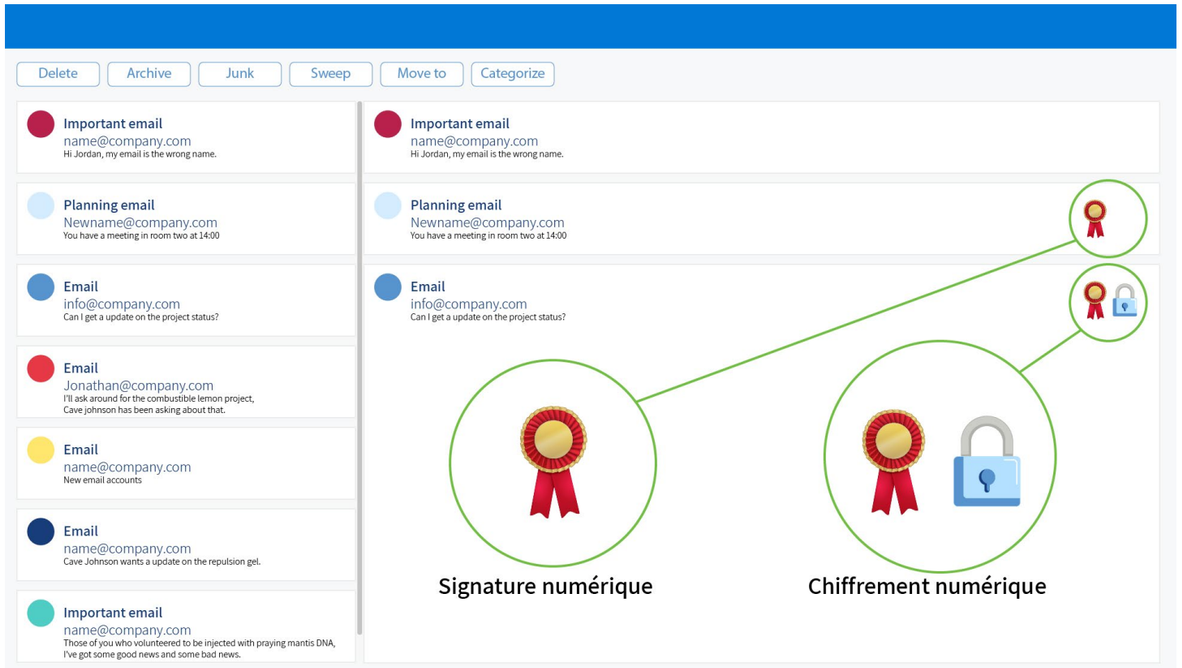
Organisatie gevalideerde SSL certificaten
Globalsign OrganizationSSL
Globalsign OrganizationSSL SAN
Globalsign OrganizationSSL Wildcard

Les certificats à Validation d'Organisation
Globalsign ExtendedSSL
Globalsign ExtendedSSL SAN

Les certificats pour signature de mail ou identité digitale

Les certificats client, également appelés certificats d'identification personnelle, sont utilisés pour vérifier l'identité d'une personne. Avec un certificat d'identification personnelle, vous pouvez :

- ✓ Accédez à des applications, des sites web et des interfaces spécifiques, mais aussi à des équipements tels que les ordinateurs portables et les téléphones mobiles.
  Également appelée authentification du client.
- ✓ Signature numérique de mail : elle confirme l'identité de l'auteur et empêche toute altération non autorisée, garantit au destinataire que le courrier électronique provient de vous et non d'un usurpateur, et empêche que le contenu du mail soit modifié dans cet intervalle.
- ✓ Chiffrer numériquement les courriers électroniques: permet de protéger la confidentialité du message et d'éviter que des données sensibles ne tombent entre de mauvaises mains. Avec le cryptage S/MIME, seul le destinataire a accès au contenu du courriel.
- ✓ Signer des fichiers Office



Les certificats pour signature de document

Avec les certificats de signature de documents, les personnes, les équipes/services et les organisations peuvent ajouter une signature électronique, numérique, à un document dans différents formats de fichiers pour prouver leur identité. La signature numérique est un hachage crypté de votre message qui ne peut être décrypté que par une personne possédant une copie de votre clé publique. Le destinataire peut facilement vérifier l'expéditeur en inspectant le certificat. Le PDF est de loin la plateforme la plus utilisée, le destinataire n'ayant besoin que d'Adobe Reader.

Caractéristiques d'un certificat pour signature de document

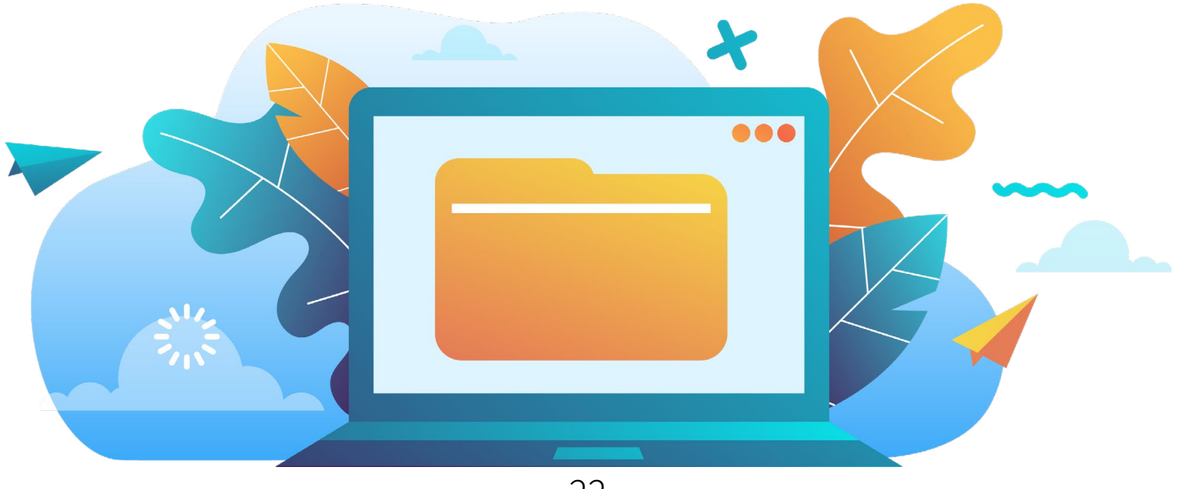
- Certitude quant à l'identité de l'expéditeur du document
- Certitude quant au contenu inchangé du document
- La signature numérique est juridiquement valable
- Grâce à l'horodatage, la signature apposée reste vérifiable et valable à long terme

Horodatage

Un horodatage garantit que les signatures apposées ne prennent pas fin après l'expiration du certificat de signature de document. En horodatant, la signature apposée reste vérifiable et valide à long terme.

Plateformes compatibles:

- Adobe
- Microsoft Office
- Apache OpenOffice
- LibreOffice



Les certificats pour signature de code

Dans la signature de code, une signature numérique est ajoutée aux logiciels/applications. Ils sont utilisés par les développeurs de logiciels pour signer numériquement des applications, des programmes et des logiciels. Il est clair pour l'utilisateur final que le logiciel/l'application provient d'un fournisseur de logiciels agréé et n'a pas été modifié par un tiers depuis la publication. La signature comprend le nom de l'entreprise et un horodatage.
En outre, les certificats de signature de code garantissent que les utilisateurs ne reçoivent aucun message d'avertissement lors de l'installation et/ou du démarrage.

Horodatage

Un horodatage garantit que les signatures définies n'expirent pas après que le certificat de signature de code soit arrivé à terme. En horodatant, la signature apposée reste vérifiable et valide à long terme.

Pourquoi signer un code ?

Protéger l'intégrité et la réputation de votre code.
Les signatures numériques contiennent la preuve de l'intégrité du contenu, de sorte que, votre code ne peut être modifié et distribué avec des modifications non approuvées. Si le hachage utilisé pour signer l'application correspond au hachage d'une application téléchargée, l'intégrité du code est donc intacte. Si le hachage utilisé ne correspond pas, alors, les utilisateurs recevront un avertissement de sécurité ou bien le code ne pourra pas être téléchargé.

Offrir à ses clients une expérience fiable et sécurisée.
En signant votre code, vous vous assurez qu'il n'a pas été falsifié et qu'il provient de vous. En signant avec un certificat de signature de code, cela montre que vous bénéficiez de la confiance d'une tierce partie, en l'occurrence l'autorité de certification, dans le domaine de la sécurité de la signature de code et contribue à une expérience fiable et sécurisée pour vous et vos clients.

	Code Signing	Code Signing EV
Signatures illimitées	✓	✓
Suppression de l'avertissement de sécurité "éditeur non identifié"	✓	✓
Contrôle étendu de l'organisation	✗	✓
Analyse de bonne réputation immédiate avec Microsoft Smartscreen	✗	✓
Horodatage	✓	✓
Jeton USB token requis	✗	✓

A propos de Networking4all / Certificat.fr

Fondée en 2000, nous travaillons depuis 2002 depuis une plateforme en ligne, développée par nos soins, pour la gestion des certificats SSL. Nous sommes le partenaire privilégié de GlobalSign (Preferred Partner) et le partenaire Platinum Elite de Digicert. Cela implique que nous disposons de connexions directes facilitant la communication de part et d'autre. Nous nous concentrons notamment sur les Pays-Bas, la France et la Belgique, mais sommes aussi fournisseur de nombreuses grandes entreprises internationales dans le monde entier. Depuis 2012, nous disposons de notre propre certificat intermédiaire sous la racine Digicert, de manière à avoir le plus de moyens possibles de contrôle. En 2019, nous avons modernisé l'ensemble de notre plateforme de gestion et sommes en mesure de compter parmi nos clients la quasi-totalité des grandes banques, des assureurs, des e-commerces, des municipalités et des sociétés de sécurité aux Pays-Bas. Notre équipe de développement travaille quotidiennement à l'amélioration et à la création de nouvelles fonctionnalités pour faciliter au maximum la gestion de vos certificats SSL.

Les avantages Networking4all / Certificat.fr, le portail de gestion SSL

Notre objectif : vous décharger et réduire vos coûts. Nous proposons différentes marques et solutions, à partir d'un portail complet. En outre, nous disposons de gestionnaires de comptes et de spécialistes de la sécurité prêts à vous fournir des conseils clairs et directs. Grâce à notre portail développé par nos soins et récompensé par un prix, vous pouvez gagner du temps, réduire les risques et réagir directement à toute vulnérabilité.

Certifié ISO 9001 et ISO 27001
La certification ISO 9001 est une norme mondialement reconnue pour la gestion de la qualité. Elle comprend des procédures selon lesquelles nous travaillons en permanence pour accroître la satisfaction de nos clients. Avec la certification ISO 27001, nous démontrons à quel point la sécurité de l'information est importante pour nous. Ces processus sont contrôlés, enregistrés, surveillés et améliorés en permanence. Ces certifications ISO sont évaluées et délivrées chaque année par le KIWA, un institut d'audit réputé internationalement.

Un portail récompensé
Notre système de gestion refondu pour les certificats SSL a remporté le prix international de l'innovation décerné par Digicert lors de son lancement en 2019. Depuis le menu principal, vous pouvez directement gérer vos certificats SSL tels que les demandes, les réémissions, la gestion, les alertes, les contacts, l'authentification 2FA, etc. Mais aussi un bon aperçu de vos commandes, devis, pdf, factures, etc.

Garantie de qualité
Nous nous efforçons toujours de trouver une solution adaptée aux besoins de nos clients. Si vous avez choisi un certificat SSL non adapté ou saisi un nom de domaine erroné, aucun problème. Vous serez toujours remboursé dans les 30 jours suivants la date de délivrance du certificat.

Elite Platinum Partner de DigiCert et Preferred Partner de GlobalSign
Pour Digicert, nous sommes l'un des rares partenaires Elite Platinum et partenaire privilégié (Preferred Partner) de GlobalSign. C'est pourquoi, nous avons une communication directe en ce qui concerne la validation et les éventuelles requêtes ; nous développons aussi de nouveaux produits en coopération avec les principales AC telles que Digicert et Globalsign que nous pouvons faire délivrer dans des délais optimaux.

20 ans d'expérience du marché SSL
Networking4all/Certificat.fr a plus de 20 ans d'expérience sur le marché du SSL. C'est pourquoi notre entreprise dispose de vastes connaissances dans ce domaine et de solides connexions avec les grandes entreprises d'audit.

Conditions et mode de règlement
Nous disposons d'un large éventail de modes de paiement. Par exemple, il est possible de régler par paiement différé ou via Paypal, par carte bancaire ou vous pouvez encore commander à partir d'un compte de dépôt. Il est également possible de demander un devis au préalable. Vous travaillez avec un délai de paiement à 14, 30 ou 60 jours ? Vous pouvez coordonner vos souhaits avec notre service administratif et/ou commercial.

Alertes SSL
Grâce à notre système de suivi, des alertes vous seront envoyées suffisamment tôt pour que vos certificats SSL n'arrivent pas à expiration. Il vous sera également possible de personnaliser les rappels par certificat (nombre de rappels, nombre de jours avant expiration, destinataires).
Ces alertes seront envoyées 30 jours avant la date d'expiration par mail à la personne de contact, en charge de la commande. Vous pouvez ajouter vous-même des rappels ou des personnes à un certificat SSL.

Notifications
Vous pouvez apposer des notes dans chacune de vos commandes SSL afin de faciliter leur gestion. Cette option est idéale pour laisser des remarques à vos collègues, pour noter les numéros de vos commandes, serveurs, projets, migrations, et bien plus.

Aperçu de tous vos certificats
Si vous désirez un aperçu complet de tous vos certificats SSL, y compris ceux que vous n'avez pas (encore) commandé chez nous, c'est possible. Il suffit de spécifier le site internet ou d'importer le certificat dans l'aperçu SSL. Ils s´exécuteront alors directement avec les contrôles de tous vos autres certificats. Vous recevrez pour ce faire un message d'alerte d'expiration.

Sites et comptes
Créez un compte pour chacun des consultants ou employés autorisés à soumettre des demandes pour savoir exactement qui a demandé quel certificat. Si vous avez plusieurs entreprises ou plusieurs sites d'où vous travaillez, il est facile de tout gérer dans un seul compte.

Support et assistance technique
Notre équipe SSL dédiée se tient à votre disposition pour répondre à toutes vos questions sur les issues techniques et de validation. Si vous avez besoin d'aide pour choisir le produit le plus approprié, n'hésitez pas à nous contacter pour obtenir des conseils personnalisés, notre équipe sera heureuse de vous aider.

Propre équipe de validation
Nous disposons de notre propre équipe dédiée à la validation des certificats. Vos commandes seront immédiatement traitées par nos spécialistes. En cas d'anomalie, vous serez directement contacté par nos services, ce qui vous fera gagner un temps précieux.

Validation unique
Nous vérifions chaque certificat SSL contenant des informations sur l'organisation. Si vous disposez de plusieurs certificats SSL pour un nom de domaine, cela peut prendre un certain temps. Nous créons alors un profil pour ces noms de domaines afin qu'une seule validation soit effectuée. Ce dernier sera valable pendant une période d'un an. Les certificats OV et EV seront par la suite délivrés plus rapidement grâce au profil préalablement enregistré.

Outils
Votre certificat SSL est-il correctement installé ? Cela semble être le cas même quand il manque un intermédiaire. Cependant, votre système le reconnaît et ne rapporte pas d'erreur. Pour une meilleure sécurité, utilisez notre vérificateur SSL pour toujours vérifier votre installation.

Enregistrement (vérification)
Toute opération est stockée dans l'historique d'un certificat SSL. Cela vous permet de suivre en temps réel le statut d'une commande. Vous pourrez voir également vos actions ou celles de vos employés. De cette façon, cela vous aidera à savoir exactement qui a présenté une demande et qui est en charge du suivi du dossier.

Réductions et responsable commercial
Á partir de 10 certificats SSL, nous vous proposons le service d'un/d'une responsable commercial(e) dédié(e). Ce dernier/cette dernière vous apportera des conseils personnalisés. De plus, avec elle ou lui, vous déterminerez ensemble dans quelle échelle de remise vous vous trouvez, de sorte que, en plus des avantages liés à la plateforme de gestion de vos certificats SSL, un gain tarifaire pourra toujours être accordé.

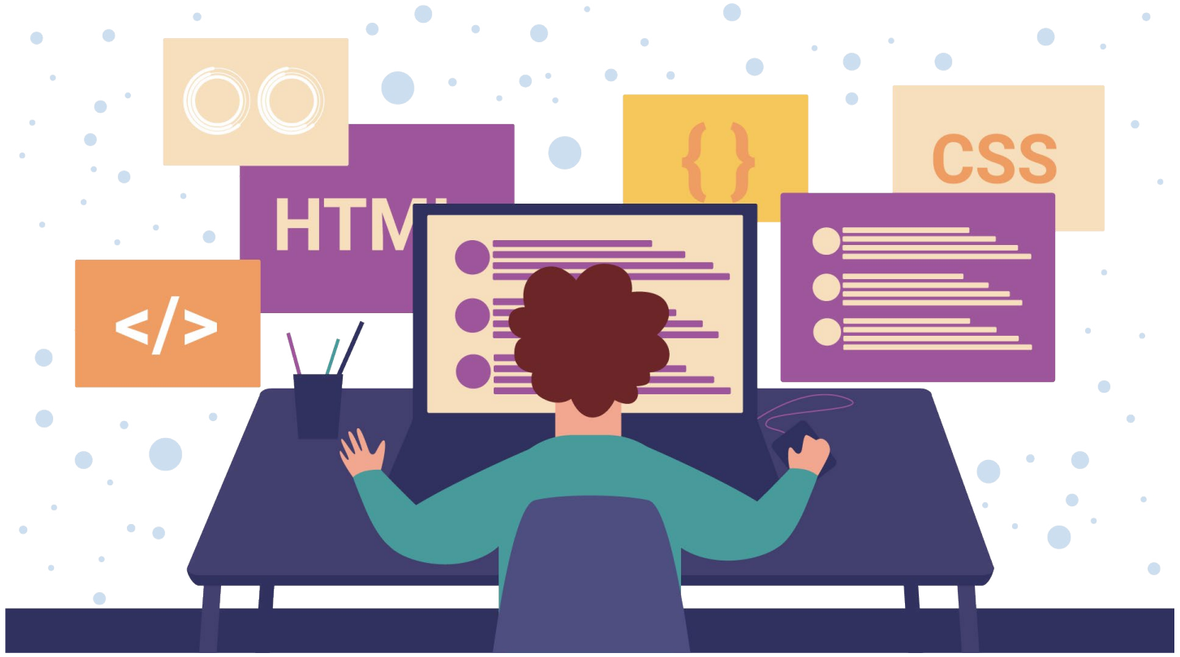
API
Nous mettons à votre disposition une Interface de Programmation d'Application (API) vous permettant d'automatiser certaines fonctions. Êtes-vous hébergeur, dont le besoin est de soumettre et de faire valider automatiquement des certificats SSL ? Êtes-vous éditeur de logiciels CMS ou d'autres plateformes nécessitant une connexion SSL, veuillez nous contacter pour discuter des possibilités.

API SOAP / API REST

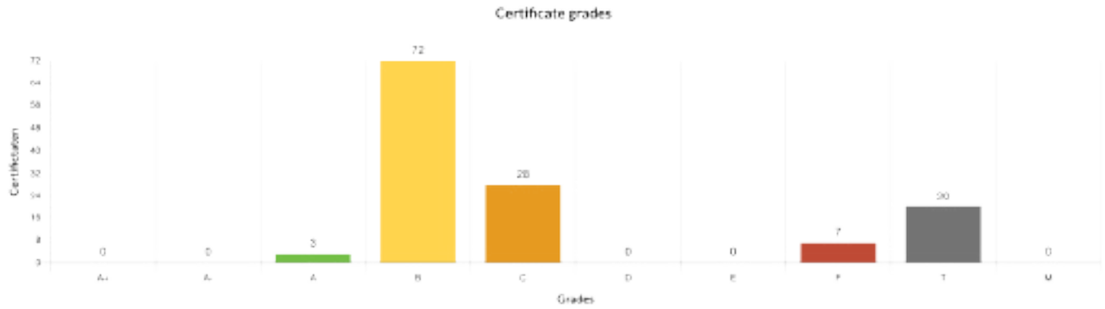
Networking4all offre à ses partenaires une API (Application Programming Interface) SOAP (Simple Object Access Protocol) et une API REST (Representational State Transfer) pour la gestion en temps réel des transactions et des produits, et les commandes de certificats SSL. Les clients API peuvent, entre autres, exécuter les commandes suivantes : créer de nouvelles connexions, en modifier, demander des informations sur ces dernières, et commander ou remplacer des certificats SSL.

Rapport sur la gestion d'installation de vos certificats SSL

Vous souhaitez également connaître le statut de tous les certificats SSL délivrés et installés : par un tiers au sein de votre organisation ou par un consultant externe. Par le biais de l'outil SSL Labs, vous pourrez consulter manuellement les scores d´installation par certificat SSL, de A à F. Bien sûr, idéalement, vous souhaitez rester dans la zone verte A. Toutefois, un certificat SSL peut passer de A à B si de nouvelles failles sont détectées. Dans ce cas, le certificat SSL peut contenir de nouvelles vulnérabilités, il doit être remplacé, mais cela se fait généralement dans la configuration du serveur. Vérifier tout vous-même à chaque fois prend beaucoup de temps et n'est pas toujours précis et immédiat. C'est pourquoi, avec SSL Labs, vous avez la possibilité à tout moment d'obtenir un aperçu actualisé de l'état de santé de vos certificats SSL et pourrez être informé de tout changement inattendu. Vous garderez donc toujours le contrôle. Pour plus d'informations, contactez notre équipe commerciale et/ou support.



Rapport d´installation SSL



À propos de ce rapport

Ce rapport SSL est basé sur une analyse approfondie des configurations des certificats SSL que vous avez achetés (ceux qui sont accessibles au public). Il est souvent surprenant de constater le peu d'attention accordée à la manière dont le SSL est configuré. Le SSL est relativement facile à utiliser, mais il présente aussi des inconvénients. Ce rapport vise à établir une méthodologie d'évaluation simple pour les gestionnaires et les administrateurs, après quoi, ces derniers peuvent modifier et optimiser la configuration du serveur web sans avoir à être des experts en la matière. En scannant régulièrement l'ensemble du portefeuille et en envoyant des mises à jour lorsque des changements surviennent, vous êtes toujours "aux commandes".

évaluation d´installation de vos certificats

A	mail.Angelica.nl	A	G.Washington.nl	A	JohnLaurens.mail.io
B	Samuel-Seabury.nl	B	Eliza-H.eu	B	George-Eacker.com
B	James-Madison.com	C	Marquis.de.Lafayette.fr	C	Charles-Lee.du
F	Peggy_Schuyler.eu	F	John-Adums.com	F	www.Aaron.burr
T	www.A.Ham.be	F	www.Philip-Hamiton.be	F	Maria-Reynolds.be
T	Hercules-Mulligan.be	T	Thomas-Jefferson.com	T	King-George-3th.eu

Notre clientèle

Depuis l'existence de Networking4all/Certificat.fr, nous avons pu constituer une clientèle de plus de 3.500 clients dans divers secteurs d'activité, chacun ayant ses propres spécificités et besoins.

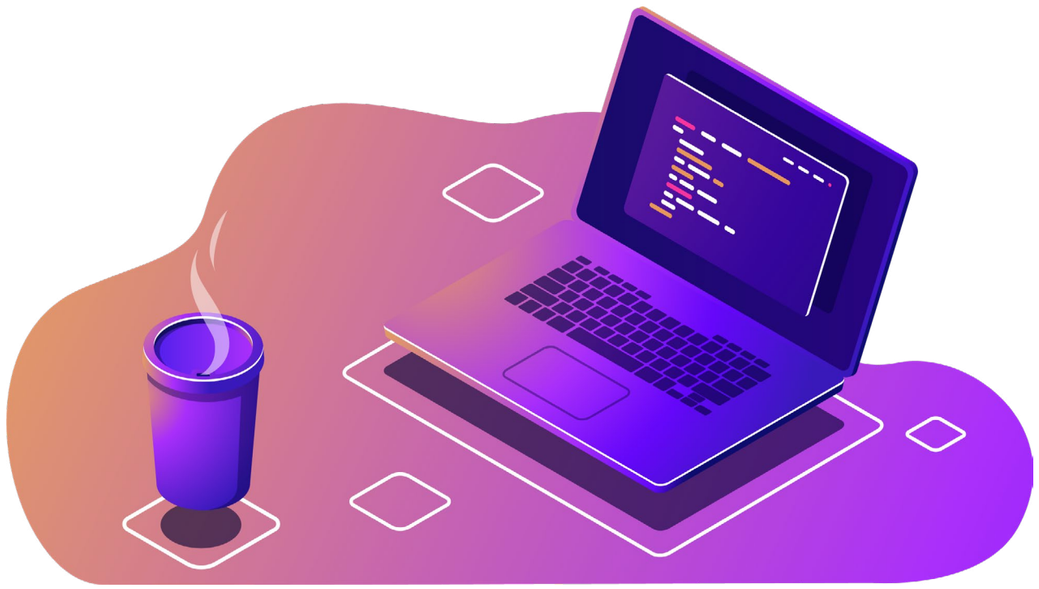
Nous fournissons des produits et des services à de petites ou grandes entreprises dans les domaines du commerce de gros, des services aux entreprises, de l'informatique, de la santé, de l'éducation et des administrations publiques. Nous nous engageons à rendre l'internet plus sûr et à améliorer votre sécurité.

Nos partenaires

La collaboration est importante au sein de chaque industrie. Cela nous permet de partager facilement et d'innover plus rapidement et plus efficacement au sein du marché de la sécurité informatique.

digicert®

GlobalSign®
GMO INTERNET GROUP



Liste de prix SSL

Consulter notre site internet pour les prix en vigueur.

Liste de prix DV	1 an	2 ans	3 ans	4 ans	5 ans	6 ans
Networking4all Basic SSL DV	30,- €	57,- €	84,- €	111,- €	138,- €	165,- €
Networking4all Basic SSL DV Plus	129,- €	245,- €	361,- €	477,- €	593,- €	709,50 €
Networking4all Basic SSL DV SAN	99,- €	179,- €	277,- €	366,- €	455,- €	544,50 €
Networking4all Basic SSL DV Wildcard	158,- €	300,- €	442,- €	585,- €	727,- €	869,- €
Networking4all Basic SSL DV Wildcard SAN	158,- €	276,50 €	442,- €	585,- €	727,- €	869,- €
GeoTrust QuickSSL Premium	79,- €	138,25 €	221,- €	292,- €	363,- €	434,50 €
GeoTrust QuickSSL® Premium SAN	109,- €	190,75 €	305,- €	403,- €	501,- €	599,50 €
GeoTrust QuickSSL Premium Wildcard	245,- €	428,75 €	686,- €	906,50 €	1.127,- €	1.347,50 €
GlobalSign DomainSSL	119,- €	-	-	-	-	-
GlobalSign DomainSSL SAN	144,- €	-	-	-	-	-
GlobalSign DomainSSL Wildcard	449,- €	-	-	-	-	-
Thawte SSL123	39, €	68,25 €	109, €	144, €	179, €	214,50 €
Thawte SSL123 San	69,- €	131,- €	193,- €	255,- €	317,- €	379,50 €
Thawte SSL123 Wildcard	299,- €	523,25 €	837,- €	1.106,- €	1.375,- €	1.644,50 €
Trust Provider DomainSSL	9,- €	15,75 €	25,- €	33,- €	41,- €	49,50 €
Trust Provider DomainSSL Wildcard	69,- €	120,75 €	193,- €	255,- €	317,- €	379,50 €
RapidSSL	11,- €	20,90 €	31,- €	41,- €	51,- €	60,50 €
RapidSSL Wildcard	115,- €	219,- €	322,- €	425,50 €	529,- €	632,50 €
AlphaSSL	29,- €	-	-	-	-	-
AlphaSSL Wildcard	69,- €	-	-	-	-	-

Les certificats SSL Networking4ALL

- ✓ **Un service de qualité de Networking4all/Certificat.fr**
- ✓ **Délivré sur la racine fiable de Digicert**
- ✓ **Domaine sans www délivré gratuitement**
- ✓ **Garantie SSL**
- ✓ **Intermédiaire marque blanche, possibilité de vendre des certificats sous votre propre nom**
- ✓ **Priorité validation et support**
- ✓ **Prix adaptés**
- ✓ **Paiement différé**
- ✓ **Validation du profil**
- ✓ **Rapports sur la sécurité et la gestion des certificats SSL**

Liste de prix OV	1 an	2 ans	3 ans	4 ans	5 ans	6 ans
Networking4all Business SSL OV	89,- €	169,- €	249,- €	329,- €	409,- €	489,50 €
Networking4all Business SSL OV SAN	149,- €	279,- €	417,- €	551,- €	685,- €	819,50 €
Networking4all Business SSL OV Wildcard	279,- €	499,- €	781,- €	1.032,- €	1.283,- €	1.534,50 €
GeoTrust True BusinessID	99,- €	173,25 €	277,- €	366,- €	455,- €	544,50 €
GeoTrust True BusinessID Multi-Domain	199,- €	348,25 €	557,- €	736,- €	915,- €	1.094,50 €
GeoTrust True BusinessID Wildcard	299,- €	523,25 €	837,- €	1.106,- €	1.375,- €	1.644,50 €
GlobalSign OrganizationSSL	169,- €	-	-	-	-	-
GlobalSign OrganizationSSL SAN	204,- €	-	-	-	-	-
GlobalSign OrganizationSSL Wildcard	599,- €	-	-	-	-	-
Digicert Basic SSL	169, €	295,- €	473,- €	625,- €	777,- €	929,50 €
Digicert Basic Multi-Domain SSL	299,- €	515,- €	837,- €	1.106,- €	1.375,- €	1.644,50 €
Digicert Basic Wildcard SSL	599,- €	975,- €	1.565,- €	2.068,- €	2.571,- €	3.074,50 €
Digicert Business Secure Site SSL	279,- €	489,- €	767,- €	976,50 €	1.185,- €	1.395,- €
Digicert Business Secure Site Multi-Domain SSL	699,- €	1.229,- €	1.922,- €	2.446,- €	2.971,- €	3.495,- €
Digicert Business Secure Site Wildcard SSL	1.999,- €	3.498,25 €	5.497,- €	6.996,50 €	8.495,- €	9.995,- €
Digicert Secure Site Pro SSL	659,- €	1.154,- €	1.812,- €	2.306,50 €	2.801,- €	3.295,- €
Digicert Secure Site Pro Multi-Domain SSL SSL	1.299,- €	2.274,- €	3.572,- €	4.546,50 €	5.521,- €	6.495,- €
Thawte SSL Web Server	99,- €	173,25 €	277,- €	366,- €	455,- €	544,50 €
Thawte SSL Web Server SAN	169,- €	295,75 €	473,- €	625,- €	777,- €	929,50 €
Thawte SSL Web Server Wildcard	309,- €	540,75 €	865,- €	1.143,- €	1.421,- €	1.699,50 €

Liste de prix EV	1 an	2 ans	3 ans	4 ans	5 ans	6 ans
Networking4all Business SSL EV	129,- €	229,- €	361,- €	477,- €	593,- €	709,50 €
Networking4all Business SSL EV SAN	309,- €	559,- €	865,- €	1.143,- €	1.421,- €	1.699,50 €
GeoTrust True BusinessID with EV	139,- €	243,25 €	389,- €	514,- €	639,- €	764,50 €
GeoTrust True BusinessID Multi-Domain with EV	329,- €	575,75 €	921,- €	1.217,- €	1.513,- €	1.809,50 €
GlobalSign ExtendedSSL	395,- €	-	-	-	-	-
GlobalSign ExtendedSSL SAN	499,- €	-	-	-	-	-
Digicert Basic EV SSL	269,- €	469,- €	753,- €	995,- €	1.237,- €	1.479,50 €
Digicert Basic EV Multi-Domain SSL	449,- €	775,- €	1.257,- €	1.661,- €	2.065,- €	2.469,50 €
Digicert Business Secure Site EV SSL	659,- €	1.154,- €	1.812,- €	2.306,50 €	2.801,- €	3.295,- €
Digicert Business Secure Site EV Multi-Domain SSL	1.299,- €	2.273,25 €	3.572,- €	4.546,50 €	5.521,- €	6.495,- €
Digicert Secure Site Pro EV SSL	1.049,- €	1.836,- €	2.885,- €	3.671,50 €	4.458,- €	5.245,- €
Digicert Secure Site Pro EV Multi-Domain SSL	2.039,- €	3.568,25 €	5.607,- €	7.136,50 €	8.666,- €	10.195,- €
Thawte SSL Web Server EV	209,- €	365,75 €	585,- €	773,- €	961,- €	1.149,50 €
Thawte SSL Web Server EV SAN	359,- €	628,25 €	1.005,- €	1.328,- €	1.651,- €	1.974,50 €

Contact

Vous souhaitez en savoir plus sur nos produits et services ou échanger avec l'un de nos spécialistes?
N´hésitez à nous contacter. Nous sommes à votre service!

Certificat.fr
57, rue d'Amsterdam
75008 Paris

Adresse postale Pays-Bas
PO Box 15320
1001 MH Amsterdam

+33 (0) 1 86 26 26 34
info@certificat.fr
www.certificat.fr