



Logius  
Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties

## DigiD SSL

Versie 2.1.1

Datum 16 augustus 2010  
Status Definitief

## Colofon

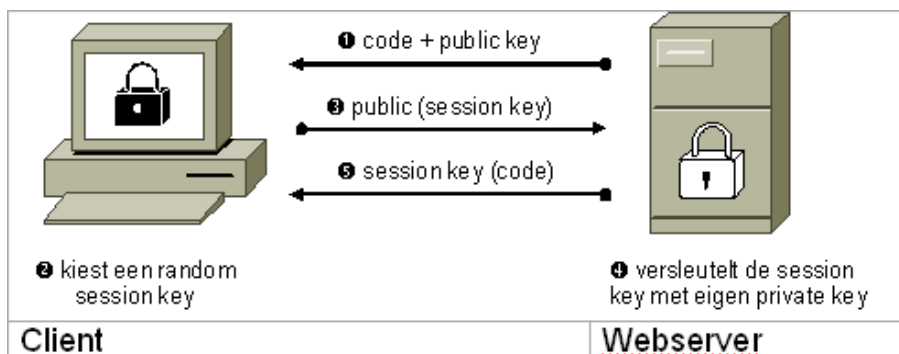
Projectnaam	DigiD
Versienummer	2.1.1
Organisatie	Logius Postbus 96810 2509 JE Den Haag <a href="mailto:servicecentrum@logius.nl">servicecentrum@logius.nl</a>

## Inhoud

<b>Colofon</b> .....	2
<b>Inhoud</b> .....	3
<b>Inleiding</b> .....	4
1.1 <i>De werking van SSL</i> .....	4
<b>2 Services certificaat (SSL)</b> .....	6
2.1 <i>Verkrijgen van een services certificaat (SSL)</i> .....	6
2.2 <i>Algemene beschrijving werking two-sided SSL</i> .....	8
2.3 <i>Vorbereidingen benodigd voor toegang tot DigiD     webservices</i> .....	8
2.3.1 <i>Procedure bij vermoeden van compromittering.</i> .....	9

## Inleiding

Secure Socket Layer (SSL) is gebaseerd op PKI en gebruikt twee sleutels. Elke computer/server wordt uitgerust met een dergelijk sleutelpaar, die uniek is per computer. De ene sleutel is publiekelijk beschikbaar en kan worden gebruikt voor het controleren van berichten afkomstig van de computer die beschikt over het sleutelpaar. Ook kan deze sleutel berichten versleutelen die zijn gericht aan deze computer. De andere sleutel blijft geheim en wordt gebruikt om berichten te ondertekenen en versleutelde berichten te ontsleutelen.



**Figuur 1: Publiek sleutelsysteem**

### 1.1

#### **De werking van SSL**

De webserver stuurt de publieke sleutel (public key)<sup>1</sup>, samen met een door de webserver willekeurig gekozen code. Zodra de client de publieke sleutel ontvangt, bepaalt de client een sessiesleutel (session key).

De client versleutelt de sessiesleutel met de publieke sleutel. De versleutelde sessiesleutel wordt door de client teruggestuurd naar de webserver. Deze ontsleutelt de sessiesleutel, zodat de sessiesleutel overblijft.

Zodra de webserver de sessiesleutel heeft vastgesteld, wordt de willekeurige code opnieuw verstuurd naar de client, maar nu versleuteld met de sessiesleutel. Op deze wijze weet de client dat hij nog steeds communiceert met dezelfde webserver en dat er sprake is van een beveiligde verbinding.

De essentie van SSL is dus dat de webserver een code stuurt naar de client met een sleutel, die de client zelf heeft vastgesteld. Wilt u meer weten over het SSL-protocol? Kijk dan op [http://en.wikipedia.org/wiki/Secure\\_Sockets\\_Layer](http://en.wikipedia.org/wiki/Secure_Sockets_Layer).

SSL is standaard ingebouwd in elke browser. Een gebruiker hoeft geen extra software te installeren. Een webpagina met SSL-beveiliging is gemakkelijk herkenbaar. Zo heeft bijvoorbeeld Microsoft Internet Explorer

<sup>1</sup> Met de client wordt de computer bedoeld, die de webserver benadert. Dit kan de web browser van de gebruiker zijn, maar ook de server van de DigiD authenticatiedienst.

een klein icoon in de vorm van een slotje in de rechterbenedenhoek staan wanneer de verbinding gebruik maakt van SSL-beveiliging.

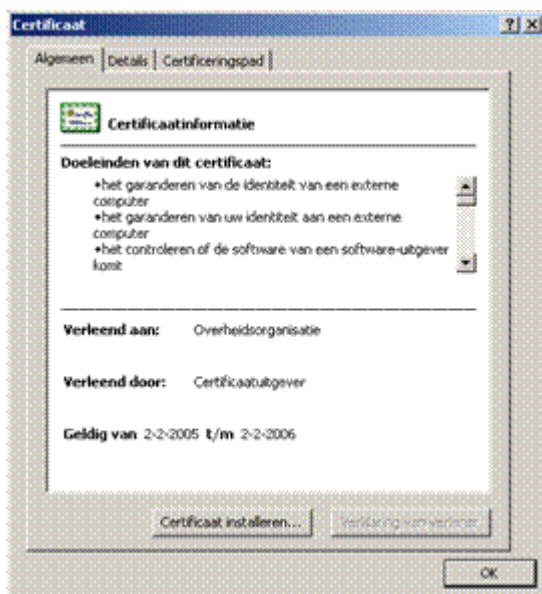
Daarnaast hebben beveiligde webpagina's "https://" in hun URL staan in plaats van het gebruikelijke "http://". De browser herkent dit en start een SSL-verbinding.

## 2 Services certificaat (SSL)

Een services certificaat (SSL) is ook wel bekend als SSL server certificaat of als SSL certificaat. Het certificaat bevat informatie over de eigenaar en naam van de computer en maakt het mogelijk om een beveiligde verbinding tussen uw webdienst en de gebruiker op te zetten. Het services certificaat (SSL) maakt het mogelijk voor de gebruiker om te controleren wie de eigenaar is van de computer en daarmee de identiteit van de webdienst te valideren.

Met behulp van uw services certificaat (SSL) is de bezoeker van uw webdienst er zeker van dat hij op uw website is gekomen, en dat de door hem ingevoerde gegevens niet door derden kunnen worden afgeluisterd. U heeft een dergelijk certificaat nodig om een beveiligde verbinding te kunnen opbouwen met de bezoeker van uw webdienst. DigiD vereist dat dit services certificaat (SSL) conform PKIoverheid is.

U kunt een certificaat bekijken door het te downloaden en te openen. Hieronder ziet u een voorbeeld van een dergelijk certificaat.



**Figuur 2: services certificaat (SSL)**

DigiD beschikt zelf ook over een services certificaat (SSL); u kunt het als volgt downloaden (deze beschrijving is gebaseerd op de Internet Explorer browser, andere browsers werken min of meer op dezelfde wijze):

Surf naar <https://applicaties.digid.nl/>

Dubbelklik op het sleuteltje op de taakbalk.

### 2.1 Verkrijgen van een services certificaat (SSL)

De afnemer die zijn webdienst op DigiD wil aansluiten, is zelf verantwoordelijk voor het verkrijgen van een services certificaat (SSL) conform PKIoverheid.

Een services certificaat (SSL) wordt uitgereikt door een certificaatdienstverlener binnen het hiërarchisch model van PKIoverheid, een vertrouwde instantie die publieke sleutels certificeert, certificaten publiceert en certificaten intrekt.

DigiD gebruikt voor haar SSL-verbindingen services certificaat (SSL) uitgegeven binnen de PKI voor de overheid. Op [www.pkioverheid.nl](http://www.pkioverheid.nl) vindt u alle toegetreden certificaatdienstverleners en meer informatie over de services certificaten (SSL).

Om een services certificaat (SSL) aan te schaffen dient u contact op te nemen met één van deze certificaatdienstverleners. Vermeld bij het aanvragen expliciet dat u wilt beschikken over een services certificaat (SSL) binnen de PKI voor de overheid.

De onderstaande tekst bevat technische informatie voor het aanvragen en installeren van een service certificaat (SSL).

Voor het aanvragen van uw services certificaat (SSL) is het nodig om een Certificate Signing Request (CSR) aan te maken. De wijze waarop een CSR wordt aangemaakt is afhankelijk van de software die u op uw webserver gebruikt. Raadpleeg de handleiding van uw webserver software. Uw hostingpartij kan u daarbij helpen.

Voor het maken van een beveiligde website met behulp van een SSL server certificaat heeft u naast het certificaat het volgende nodig: een website op een eigen webserver of bij een hosting provider, bereikbaar via SSL (dit is meestal poort 443), een IP-adres welke alleen voor uw website wordt gebruikt. Het is niet mogelijk om Virtual Hosts te gebruiken, wat bij normale niet-beveiligde verbindingen wel gebruikelijk is.

N.B. Het Common Name-veld in de CSR moet de Fully Qualified Domain Name (FQDN) zijn of het webadres waarmee klanten verbinding moeten maken via SSL. Bijvoorbeeld, een SSL server certificaat dat is uitgegeven voor gemeente.nl, zal niet geldig zijn voor secure.gemeente.nl. Als het webadres dat voor SSL gebruikt moet worden secure.gemeente.nl is, zorgt u er dan voor dat u als Common Name secure.gemeente.nl in het CSR invult.

N.B. Voor DigiD dient er gebruik te worden gemaakt van een 1024-bits services certificaat (SSL) met minimaal 128-bits lijn-encryptie sterkte. Zorg dus dat de aanvraag is gebaseerd op een 1024-bits sleutel.

N.B. Een services certificaat (SSL) heeft een beperkte geldigheidsduur, over het algemeen drie jaar. U dient ervoor te zorgen dat het services certificaat (SSL) geldig blijft. Vóór het verstrijken van de geldigheidsduur van uw certificaat, dient u deze te verlengen. Installeren van webdienst services certificaat (SSL)  
U dient uw Services Certificaat (SSL) op uw webserver te installeren. Zorgt u ervoor dat bij het opbouwen van de SSL-verbinding alle certificaten in de certificatenhiërarchie beschikbaar worden gesteld. Raadpleeg hiervoor de handleiding van uw webserver software.

## 2.2 Algemene beschrijving werking two-sided SSL

Secure Sockets Layer (SSL) is een encryptieprotocol dat communicatie op het internet beveiligt. Met SSL kan de identiteit van een server worden gecontroleerd. Bijvoorbeeld of er wel contact met de echte DigiD server wordt gemaakt. Door gebruik te maken van een public key infrastructure (PKI) kan ook de identiteit van de client<sup>2</sup> worden bepaald. Er is dan sprake van dubbelzijdig SSL.

PKI werkt met zogenaamde publieke certificaten (public keys). Deze certificaten worden door een Certificate Server Provider (CSP) na strenge controle uitgegeven waarbij de naam van het systeem of de organisatie leesbaar in het certificaat wordt opgenomen als Distinguished Name (DN). Met een two-sided SSL-certificaat kunnen systemen of organisaties hun identiteit aantonen mits zij beschikken over de bijpassende geheime cryptografische sleutel (private key). Bij SSL kan een client de naam van de server controleren. Bij dubbelzijdig SSL zal vervolgens de server om het certificaat van de client vragen en op basis daarvan besluiten om de client wel of geen toegang te verlenen.

CSP : Certificate service provider, een partij die certificaten uitgeeft.

DN : Distinguished Name, de naam waarmee het certificaat geïdentificeerd wordt.<sup>3</sup>

CSR : Een Certificate Signing Request is een publieke sleutel (public key) van uw server welke wordt gebruikt bij het aanvragen van een certificaat.

FQDN : Fully qualified domain name: volledig gekwalificeerde domeinnaam. Wordt ook wel fully qualified hostname (FQHN) genoemd

## 2.3 Voorbereidingen benodigd voor toegang tot DigiD webservices

Om toegang te krijgen tot de beschermde resources, zoals hierboven genoemd moeten de volgende zaken geregeld zijn:

### De afnemer

- De afnemer moet voor zijn aansluiting een server certificaat aanvragen. De eisen aan dit certificaat zijn:
  - Dit certificaat moet ondertekend zijn door PKIoverheid CSP.
  - Het certificaat moet verplicht een Subject.Serial bevatten dat of door de CSP wordt gegenereerd of door de aanvragende partij wordt ingevuld met het CSR ofwel Certificate Signing Request nummer.
  - In het certificaat moet in het Subject onder de CN de Fully Qualified Domain Name van de server worden opgenomen die middels de DNS herleidbaar is.
- De afnemer moet het verkregen server certificaat in zijn keystore opnemen.

---

<sup>2</sup> Met client wordt hier de rol in het communicatieprotocol bedoeld, zoals in client-server. Zowel de client als de server kunnen een computersysteem zijn, die verwarrend voor het begrip van SSL, vaak als sersersysteem of server worden aangeduid.

<sup>3</sup> Het is niet helemaal juist om te zeggen dat de DN een certificaat identificeert, er kunnen meerdere versies van het certificaat bestaan met dezelfde Distinguished Name. Bijvoorbeeld als het certificaat verlopen is, of eventueel is ingetrokken. De CSP die ondertekend kant echter maar één instantie die bij de DN hoort, en in dat licht is de DN identificerend (voor de instantie of organisatie).

- De afnemer moet alleen zijn certificaat, dus zonder zijn private key, als een Base64 Encoded bestand met .CER<sup>4</sup> extensie na overleg met Logius opsturen.
- De afnemer moet het CSP certificaat en de bijbehorende keten van vertrouwen (trust chain) opnemen in zijn truststore.

### 2.3.1 *Procedure bij vermoeden van compromittering.*

Een certificaat, of beter gezegd de private key, van een afnemer kan gecompromitteerd raken. De volgende instructie dient dan gevolg te worden:

- Afnemer meldt na constatering of een vermoeden van compromittering direct aan Logius en de CSP aan dat zijn certificaat niet meer betrouwbaar is.
- Logius neemt in overleg met de afnemer de vervolgstappen.

---

<sup>4</sup> In een .CER bestand kan naast het certificaat niet ook nog de bijbehorende private key worden opgeslagen, zoals in andere formaten vaak wel kan. Dit voorkomt dus beveiligingsproblemen met de uitwisseling van het certificaat.