

# SSL Encryptie

## *Informatie*

### **Niveau's van SSL Encryptie**

De SSL Encryptie is op te splitsen in ruwweg twee niveau's. Het lage beveiligingsniveau maakt gebruik van 40 of 56 bits SSL Encryptie. Het hoge beveiligingsniveau maakt gebruik van 128 of 256 bits SSL Encryptie. Certificaten die CS Net uitgeeft zijn altijd geschikt voor minimaal 128 bits SSL Encryptie. Of in de praktijk dit ook gerealiseerd wordt is mede afhankelijk van de gebruikte webserver software en het besturingssysteem van de webserver alsook de webbrowser van de bezoeker van de website.

### **40 bits SSL Encryptie**

De eenvoudigste SSL Encryptie die gebruikt wordt is de 40 bit encryptie. Alleen de oudste webbrowsers zijn nog slechts geschikt voor 40 bits SSL Encryptie. Deze webbrowsers kwamen op de markt toen 40 bit encryptie nog niet gekraakt kon worden.

Browsers die tot deze categorie behoren zijn onder andere Microsoft Internet Explorer versie ouder dan versie 3.02 en Netscape versie voor versie 4.02. Een gebruiker die met zo'n oude webbrowser zal altijd een 40 bits SSL encryptie gebruiken, ongeacht de zwaarte van het SSL certificaat.

### **128 bits en 256 bits SSL Encryptie**

128 bits SSL Encryptie is ten opzichte van 40 bits SSL Encryptie vele malen veiliger. Het verschil zit in het aantal verschillende mogelijke encryptiesleutels dat bij gebruik van 128 bits sleutels,  $2^{88}$  maal groter is dan bij gebruik van 40 bits sleutels. Waar een hacker met kennis van zaken en de juiste apparatuur en software voor 40 bits SSL Encryptie tegenwoordig slechts enkele minuten nodig heeft om de gebruikte encryptiesleutel te kraken, is dezelfde hacker voor een 128 bits SSL Encryptie jaren bezig.

Of 128 bits SSL Encryptie daadwerkelijk gebruikt wordt hangt af van de webbrowser van de bezoeker van de website, maar ook van de webserver software en het besturingssysteem waaronder de webserver draait. Daarnaast dient het servercertificaat van de webserver Server Gated Cryptography (SGC) te ondersteunen.

Microsoft Internet Explorer vanaf versie 3.02 maar niet nieuwer van versie 5.5, en Netscape vanaf 4.02 tot versie 4.72 ondersteunen 128 bits SSL Encryptie mits de webserver uitgerust is met een SGC SSL certificaat en het besturingssysteem dit ondersteunt.<sup>1</sup>

Nieuwere versies van Internet Explorer vanaf versie 5.5, Netscape vanaf versie 4.72 en andere moderne webbrowsers zoals Firefox, Opera, Safari, etc. ondersteunen 128 bits SSL en zelfs 256 bits SSL. Overigens is voor 256 bits SSL encryptie ook vereist dat de webserver dit ook ondersteunt. Apache webserver ondersteunt deze mogelijkheid vanaf versie 2.1.3.

---

<sup>1</sup> Exportrestricties van de Verenigde Staten verbieden export van software die 128 bits SSL Encryptie ondersteunt, uitgezonderd voor gebruik door lokale overheden en financiële instellingen. Vandaar dat Internationale versies van o.a. Internet Explorer en Netscape nog lange tijd alleen 40 bits SSL Encryptie ondersteunden.