

SSL certificaten

Wat zijn validatiemethodes, welke zijn er; DV, OV en EV?

Er zijn drie methodes om de entiteit van een website vast te stellen. Dit zijn DV, OV en EV. Wat betekent: Domein Validatie (DV), Organisatie Validatie (OV), Extended Validatie (EV). Iedere validatiemethode heeft zijn eigen plus- en minpunten. Het is natuurlijk belangrijk om te weten welk type voor u het beste is.

Domeinnaam validatie (DV)

Voordelen

U kunt met dit type SSL Certificaat een publiekelijk of intern ip-adres beveiligen. Wij adviseren u altijd, indien mogelijk, om een SSL Certificaat te koppelen aan een hostname, oftewel domeinnaam. Hiermee bent u flexibeler (mocht het ip-nummer wijzigen), het is makkelijker te onthouden en er is een snellere uitgifte mogelijk. Een domeinnaam kunt u binnen enkele minuten vastleggen en via het DNS beheer het ip-nummer koppelen.

Nadelen

Dit type SSL Certificaat geeft alleen een bewijs dat de website beveiligd is. Er is geen Certificaat Autoriteit die de identiteit van de eigenaar van de website bij een derde partij heeft gevalideerd.

Gebruik

Meest gebruikt voor websites waarvoor een https verbinding (beveiligde verbinding) voldoende is, webmail, intranetten, citrix secure gateway, etc. Dit SSL Certificaat is ideaal wanneer men snel een SSL Certificaat nodig heeft.

Organisatie validatie (OV)

Voordelen

Geeft eindgebruikers het bewijs dat het bedrijf/organisatie ook werkelijk eigenaar is van de website en dat deze gecontroleerd is door een Certificaat Autoriteit (CA). Naast de domeinnaam wordt dus ook het bedrijf zelf geïdentificeerd.

Nadelen

De uitgifte van dit SSL Certificaat duurt meestal 1 tot 2 werkdagen. Bij sommige SSL Certificaten wordt een gefaxt document vereist of wordt er ter validatie telefonisch contact gelegd met de eigenaar van de domeinnaam. Deze SSL Certificaten zijn door deze extra handelingen duurder dan de domeinnaam gevalideerde SSL Certificaten.

Gebruik

Meestal voor E-commerce websites. Met dit SSL Certificaat geeft men eindgebruikers te kennen, dat de identiteit van het bedrijf en de website gecontroleerd en veilig zijn. Men moet echter wel de SSL Certificaat details opvragen, wil men deze informatie inzien. Dit komt niet standaard in beeld en is niet voor alle gebruikers makkelijk te vinden.

Extended (uitgebreide) validatie (EV)

Voordelen

Activeert de 'groene balk' in de nieuwe webbrowsers zoals IE7 en Firefox en toont visueel de identiteit van de website eigenaar en de Certificaat Autoriteit. Dit SSL Certificaat geeft het hoogst mogelijke vertrouwen aan de eindgebruikers.

Nadelen

Dit SSL Certificaat is duurder dan een Domeinnaam gevalideerd of Organisatie gevalideerd SSL Certificaat als gevolg van de uitgebreide controle procedures. De uitgifte duurt dan ook vaak langer dan de OV-certificaten (meestal 1 tot 2 weken).

SSL certificaten

Gebruik

Bedrijven die duidelijk naar hun klanten willen communiceren dat hun identiteit gecontroleerd is en dat de website veilig is. Tevens voorkomt dit vrijwel de mogelijkheid om een website te kopieëren en hiermee met phishingtechnieken informatie van gebruikers te achterhalen. Dit geeft hiermee dus tevens een bescherming tegen fraude van uw merk- of bedrijfsnaam.

Unieke FAQ ID: #1024

Auteur: n/a

Laatst bijgewerkt: 2014-03-11 15:27