Aansluitvoorwaarden Kadaster Internetdiensten (Oktober 2019)

Een veilige dienstverlening

We willen als Kadaster veilig communiceren met al onze partners. Wij moeten daarbij voldoen aan de richtlijnen, zoals die zijn opgesteld door de overheid. Bij veilig communiceren hebben onze partners en leveranciers ook een zeer belangrijke rol.

Richtlijnen

De meeste Kadaster diensten worden aangeboden op basis van het TLS (Transport Layer Security)-protocol. TLS zorgt voor een veilige verbinding met een dienst waarvan je gebruik wenst te maken. Het Nationaal Cyber Security Centrum (onderdeel van het Ministerie van Justitie en Veiligheid) heeft richtlijnen opgesteld voor een veilig TLS gebruik. Binnen de NCSC richtlijnen (zie bijlage) zijn er drie mogelijke instellingen voor een beveiligingsniveau: onvoldoende, voldoende en goed. Het Kadaster streeft naar het tweede beveiligingsniveau: **voldoende.**

Impact

We ondersteunen op dit moment naast TLS1.2 ook nog TLS 1.0 en TLS1.1 toegang en vanaf 15 oktober staan we alleen het TLS1.2 gebruik toe. Analyse geeft aan dat slechts 6% van de connecties nog gebruik maakt van TLS1.0 en minder dan 1% gebruik maakt van TLS1.1. We verwachten daarmee een minimale impact van het alleen nog toestaan van TLS1.2.

We stellen u met een test-url in staat om zelf vast te stellen of uw verbinding ook na 15 oktober 2019 veilig is.

> https://tls-conformiteit10.kadaster.nl/gaa/conf10-check/
>
> **(LETOP de conformiteit10 check is met een / op het einde!)**

U, als gebruiker, moet de conformiteitstoets doen om vast te stellen dat de verbinding veilig is. Wanneer de toets correct werkt, ziet u dat direct in het scherm zoals dit hieronder is afgebeeld. Wanneer u een ander scherm dan onderstaande scherm ziet, moet u contact met ons opnemen.

Kadaster - Beveiligde verbinding geslaagd ☑

Een veilige dienstverlening

Het Kadaster ontsluit veel van zijn diensten op het internet. Dit wil het Kadaster op een zo veilig mogelijke manier doen. Om dit ook in de toekomst te kunnen blijven doen is het noodzakelijk het koppelvlak naar het internet te onderhouden en ontstane kwetsbaarheden op dit vlak zo snel mogelijk op te heffen.

Richtlijnen

De meeste Kadaster diensten worden aangeboden via 'https' (http op basis van het TLS (transport layer security) protocol). TLS zorgt voor een veilige verbinding met de dienst waarvan je gebruik wenst te maken. Het Nationaal Cyber Security Centrum (onderdeel van het Ministerie van Veiligheid en Justitie) heeft richtlijnen opgesteld voor een veilig gebruik van TLS. Dit zijn de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS). Het Kadaster conformeert zich aan de NCSC richtlijnen. Dit betekent op dit moment concreet dat er alleen gecommuniceerd kan worden op basis van TLS 1.2 (in de toekomst ook TLS1.3) en een bepaalde lijst van door NCSC voorgeschreven cipher suites.

Impact

Op dit moment is er alleen impact te verwachten voor client software die niet gebruik kan maken van TLS 1.2 of hoger en/of niet kan communiceren met een van de door NCSC voorgeschreven cipher suites.

Toekomstig onderhoud

Het Kadaster zal toekomstige aanscherping van de NCSC normen ook doorvoeren op de Kadaster communicatie endpoints waarbij er naar wordt gestreefd om deze maximaal drie maanden na aanpassing van de norm gerealiseerd te hebben.

Onderstaande Tabel geeft de door NCSC voorgeschreven ciphers weer.

De kleuren zijn een verwijzing naar de inschattingen van het NCSC over de geschiktheid van de cipher suites. De groene regels zijn het sterkst, en moeten prioriteit krijgen. Daarna de oranje.
Maar **alle cipher suites uit de tabel zijn toegestaan**. De kleuring geeft dus de prioriteit aan.

TLS 1.2 Cipher suites

Cipher Suite name	Authentication Algorithm (Au)	Key Exchange Algorithm (Kx)	Symetric Encryption Algoritm (Enc)	MAC Digest	Cipher id Value
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	RSA	ECDHE	AESGCM(256)	AEAD	0xC0,0x30
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	RSA	ECDHE	AESGCM(128)	AEAD	0xC0,0x2F
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	RSA	ECDHE	AES(256)	SHA384	0xC0,0x28
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	RSA	ECDHE	AES(128)	SHA256	0xC0,0x27

Naar verwachting eind 2019 beschikbaar:

TLS 1.3 Cipher suites

Cipher Suite name	AEAD Algorithm for record protection	Hash algorithm used with HKDF	Cipher id Value
TLS_AES_256_GCM_SHA384	AEAD_AES_256_GCM	SHA384	0x13,0x02
TLS_CHACHA20_POLY1305_SHA256	AEAD_CHACHA20_POLY1305	SHA256	0x13,0x03
TLS_AES_128_GCM_SHA256	AEAD_AES_128_GCM	SHA256	0x13,0x01
TLS_AES_128_CCM_SHA256	AEAD_AES_128_CCM	SHA256	0x13,0x04
TLS_AES_128_CCM_8_SHA256	AEAD_AES_128_CCM_8	SHA256	0x13,0x05