

TLS ZORGT VOOR VEILIGE VERBINDING MET DE GEMEENTEWEBSITE

HTTPS zorgt voor een beveiligde verbinding tussen een browser en een webserver en helpt fraude en het lekken van gegevens te voorkomen. HyperText Transfer Protocol Secure (HTTPS) is een versleutelde HTTP-verbinding beveiligd door Transport Layer Security (TLS). Heel veel (overheids)organisaties en bedrijven maken al gebruik van HTTPS, vooral als gevoelige informatie wordt uitgewisseld met de gebruikers. Bijvoorbeeld betalingsgegevens, persoonsgegevens, et cetera. Door gebruik te maken van HTTPS geven gemeenten aan, belang te hechten aan beveiliging en privacy van burgers. De implementatie van de TLS-standaard is relatief eenvoudig en levert een belangrijke bijdrage aan een veilig gebruik van uw gemeentelijke websites. De IBD adviseert dan ook om HTTPS in uw gemeente te implementeren.



Deze factsheet richt zich op het veilig verbinden met gemeentelijke websites. In deze factsheet wordt achtereenvolgens aandacht besteed aan de beveiligingsvoordelen van HTTPS voor gemeenten, de achterliggende TLS-standaard, hoe uw gemeente gebruik kan maken van HTTPS en tenslotte het IBD advies. Voor uitgebreidere en meer technische achtergrond informatie wordt verwezen naar de uitgebreide versie van deze factsheet op de website van de IBD.

Op de website internet.nl kunt u eenvoudig controleren of uw gemeentewebsite gebruik maakt van een versleutelde verbinding, zodat de verbinding tussen een browser en de gemeente-webserver niet kan worden afgeluisterd of gemanipuleerd. Tevens wordt gecontroleerd of de cryptografische instellingen van HTTPS en TLS op de gemeentewebsite voldoende sterk zijn.

Verhogen vertrouwen in gemeentelijke websites

Als op een gemeentelijke website via een contactformulier persoonsgegevens worden gevraagd, dan zorgt HTTPS ervoor dat de vertrouwelijkheid en integriteit van verzonden gegevens wordt beschermd. Ook kan de identiteit van de website-eigenaar ermee aangetoond worden.

Voldoen aan wet- en regelgeving

In sommige gevallen is het gebruik van versleutelde verbindingen verplicht. Deze verplichting kan gesteld zijn in het informatiebeveiligingsbeleid van uw gemeente, maar ook in wet- of regelgeving. De Wet bescherming persoonsgegevens (Wbp) kent een brede verplichting (art. 13) om persoonsgegevens afdoende te beveiligen. Zo wordt bij verzending van persoonsgegevens via het internet in veel gevallen een versleutelde verbinding vereist. Deze vereiste speelt vaak voor gemeenten omdat veel uitgewisselde gegevens persoonsgegevens zijn. Tevens stelt de '[Norm ICT-beveiligingsassessments DigiD](#)' van Logius dat organisaties die diensten op basis van DigiD aanbieden verplicht zijn deze diensten via HTTP met het TLS-protocol te beveiligen (HTTPS). De TLS-standaard is sinds 2013 opgenomen op de lijst met verplichte open standaarden voor de gehele publieke sector ('[pas-toe-of-leg-uit-lijst](#)') van het Forum Standaardisatie. Dit betekent dat overheden en semi-overheden TLS dienen toe te passen en alleen in geval van zwaarwegende redenen daarvan mogen afwijken. [Tevens adviseert het Nationaal Cyber Security Centrum \(NCSC\) versleutelde communicatie \(TLS\), om de betrouwbaarheid van webapplicatie gegevens te garanderen.](#)

**"BEVEILIGING DOOR TLS ZORGT
VOOR HET BEVEILIGD VERSTUREN
VAN WEBVERKEER TUSSEN EEN
BROWSER EN EEN WEBSERVER"**

WAT LEVERT HTTPS MIJN GEMEENTE OP?

HTTPS beschermt de communicatie tussen een client en een server op basis van de volgende drie fundamentele eigenschappen:

- **Vertrouwelijkheid:** De gegevens zijn tijdens het transport versleuteld en kunnen niet worden afgeluisterd en zorgt ervoor dat kwaadwillenden geen gevoelige informatie in handen kunnen krijgen.

- **Integriteit:** Er vindt een controle plaats op de integriteit van de uitgewisselde informatie zodat gemanipuleerde gegevens worden gedetecteerd en zorgt ervoor dat kwaadwillenden het verkeer tussen de browser en de website niet kunnen manipuleren.
- **Authenticatie:** De identiteit van de communicatiepartner wordt geverifieerd (authenticatie van de webserver) en zorgt ervoor dat kwaadwillenden zich niet kunnen voordoen als uw gemeente.

Wat is TLS?

Transport Layer Security (TLS) is een protocol die twee partijen/systemen, in staat stelt om via een onbetrouwbaar netwerk zoals het internet veilig gegevens uit te wisselen. Om dit te bewerkstelligen wordt tussen deze communicerende computersystemen een versleutelde verbinding opgezet. Nadat met TLS de beveiligde verbinding is opgezet kan deze verbinding gebruikt worden om op een veilige manier tussen de browser en een webserver gegevens uit te wisselen.

Op dit moment zijn verschillende versies van TLS in gebruik. Op dit moment wordt TLS versie 1.2 door de experts beschouwd als meest veilige versie. Deze versie is niet 'achterwaarts compatibel'. Ten behoeve van de interoperabiliteit dienen daarom vaak ook de minder veilige versies 1.1 en 1.0 toegepast te worden. Een client of server kan daarom meerdere versies van TLS naast elkaar ondersteunen.

Digitale certificaten

TLS maakt gebruik van digitale certificaten om zekerheid te bieden over de identiteit van de domeinnaam (bijvoorbeeld www.ibdgemeenten.nl) of de achterliggende organisatie (bijvoorbeeld IBD) voordat communicatie plaatsvindt. De gemeente dient een digitaal certificaat aan te vragen bij een certificatautoriteit (CA). [Voor specifieke gemeentelijke dienstverlening is een digitaal certificaat van PKI-overheid nodig, dit waarborgt de betrouwbaarheid van informatie-uitwisseling op basis van Nederlandse wetgeving.](#)

Hoe maak ik onze gemeentewebsite veiliger?

Hiervoor dient zowel het onderliggende TLS-protocol als het HTTPS-protocol een veilige configuratie te hebben. Zowel TLS als HTTPS zijn bepalend voor het te bereiken beveiligingsniveau. De '[ICT-beveiligingsrichtlijnen voor TLS](#)' van het NCSC kunnen gebruikt worden bij het opstellen en beoordelen van configuraties voor het TLS-protocol.

Om tot het gewenste beveiligingsniveau te komen kan het volgende stappenplan gevolgd worden:

1. Identificeer domeinen die beveiligd dienen te worden

De volgende vragen kunnen helpen om de te beveiligen domeinen te identificeren:

- Is de vertrouwelijkheid en/of integriteit van de gegevens van belang?
- Dient de bezoeker zekerheid te hebben of deze de 'officiële' gemeentelijke website bezoekt of een 'nep' website?

2. Identificeer de achterliggende systemen

Stel tevens van de achterliggende systemen vast of deze systemen in eigen beheer van uw gemeente zijn of dat deze door een externe leverancier worden beheerd.

3. Stel een passende TLS- en HTTPS-configuratie vast

Bij het inkopen of uitbesteden van ICT-systemen of -diensten kunnen gemeenten, bij het stellen van eisen aan te leveren producten en diensten, verwijzen naar de 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' van het NCSC.

4. Organiseer het certificaatbeheer

Voor het inrichten van het certificaatbeheer kunnen gemeenten gebruik maken van de factsheet '[Veilig beheer van digitale certificaten](#)' van het NCSC.

5. Test regelmatig de TLS-verbinding

Hulpmiddelen waarmee de TLS configuratie van websites kan worden gecontroleerd zijn onder andere:

- Website zelftest via Internet.nl¹
- TLS server test via [Qualys SSL Test](#)²
- TLS browser test via [Qualys SSL Test](#)

6. Optioneel: Kies een kundige implementatiebegeleider of geef opdracht aan uw hostingpartij

¹ De website Internet.nl test tegen de 'ICT-beveiligingsrichtlijnen voor TLS' van het NCSC

² De TLS server test van Qualys SSL Labs hanteert een [eigen scoringsmethode](#)

Advies IBD met betrekking tot HTTPS

De IBD geeft het advies om:

- tenminste de gemeentelijke websites die gevoelige of transactionele (persoons)gegevens verwerken en die de toegangsweg zijn tot een DigiD-login helemaal te beschermen met HTTPS. Aanvullend hierop raadt de IBD aan om alle gemeentelijke domeinen (op termijn) te beschermen met HTTPS, zodat gebruikers van de gemeentelijke websites de identiteit van de eigenaar kunnen verifiëren.
- voor het configureren van TLS en HTTPS de ICT-beveiligingsrichtlijnen en factsheets van het NCSC¹ te volgen.

¹ Zie voor meer informatie ook de factsheet '[HTTPS kan een stuk veiliger](#)' van het NCSC.

MEER INFORMATIE

MEER INFORMATIE OVER ONZE DIENSTVERLENING VINDT U IN DE ANDERE FACTSHEETS VAN DE IBD EN OP DE WEBSITE WWW.IBDGEMEENTEN.NL. HIER KUNNEN GEMEENTEN BOVENDIEN VIA DE COMMUNITY RELEVANTE INFORMATIE MET ELKAAR DELEN, VRAGEN AAN ELKAAR STELLEN EN DOCUMENTEN UITWISSELEN. DE HELPDESK VAN DE IBD IS TE BEREIKEN TIJDENS KANTOORUREN VAN 9:00 TOT 17:00 UUR OP HET NUMMER 070 373 8011 OF VIA HET E-MAILADRES INFO@IBDGEMEENTEN.NL. TIJDENS DEZE KANTOORUREN REAGEERT DE IBD BINNEN 30 MINUTEN OP EEN INCIDENTMELDING. BUITEN KANTOORUREN IS DE IBD OP HETZELFDE NUMMER BEREIKBAAR VOOR SPOEDEISENDE MELDINGEN EN ZAL DE IBD BINNEN 60 MINUTEN REAGEREN OP EEN TELEFONISCHE OPROEP.