Intakeadvies NVN-CEN/TS 18026:2024 EN

Vergadering:	Forum Standaardisatie 11 februari 2026
Agendapunt:	5B
Documentnummer:	20260211.5B
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	29 januari 2026
Versie:	1.0
Bijlagen:	Geen
Rechten:	CC0 publieke domein verklaring

1 Samenvatting en advies

De Stuurgroep Open Standaarden adviseert het Forum Standaardisatie om NVN-CEN/TS 18026:2024 EN in procedure te nemen. Wanneer het Forum Standaardisatie de standaard in procedure neemt is een volledig expertonderzoek aangewezen om de standaard te toetsen aan de criteria van het Forum Standaardisatie voor opname op de lijst van aanbevolen standaarden.

NVN-CEN/TS 18026 EN biedt overheidsorganisaties een reeks cybersecurityvereisten die zij kunnen stellen aan clouddienstverleners die clouddiensten leveren. Binnen de Europese markt sluit deze standaard aan bij het EU Cybersecurity Certification Scheme for Cloud Services (EUCS), een raamwerk voor het certificeren van de cybersecurity van clouddienstverleners. Het raamwerk voorziet in verschillende zekerheidsniveaus en maakt het mogelijk dat clouddienstverleners zich op één gekozen niveau laten certificeren. Deze certificering kan vervolgens binnen de gehele Europese Unie worden gebruikt, met als doel het vertrouwen in clouddiensten te vergroten, en de versnippering van nationale beveiligingseisen te beperken. Het EUCS is ontwikkeld op basis van de Europese Cybersecurity Act (CSA), die de juridische grondslag vormt voor Europese cybersecurityschema's voor ICT-producten en -diensten. NVN-CEN/TS 18026:2024 EN dient als de technische standaard die de specifieke beveiligingseisen definieert die nodig zijn voor certificering binnen het EUCS-raamwerk.

Tijdens een expertbijeenkomst en bij het tot stand komen van een expertadvies moet en/of kan er extra aandacht zijn voor de volgende punten:

- Welke andere standaarden een soortgelijke functionaliteit bieden en mogelijk als alternatief moeten worden overwogen voor toetsing in plaats van NVN-CEN/TS 18026:2024 EN;
- Het opstellen van het functioneel toepassingsgebied;
- Aandacht voor het draagvlak onder clouddienstproviders voor NVN-CEN/TS 18026:2024 EN, ten behoeve van het vermijden van leveranciersafhankelijkheid van grote hyperscalers;
- Aandacht voor hoe NVN-CEN/TS 18026:2024 EN bijdraagt aan meer digitale autonomie voor de overheid;
- Aandacht voor het verkennen van de toepassing van NVN-CEN/TS 18026:2024 EN bij gemeenten en waterschappen.

In de rest van dit document wordt het advies nader onderbouwd. Hoofdstuk 2 geeft een korte uitleg van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam, alsmede de vervolgstappen. Hoofdstuk 4 toetst in hoeverre de standaard voldoet aan de criteria om in behandeling genomen te worden door het Forum Standaardisatie. Hoofdstuk 5 verkent of er inhoudelijke belemmeringen bestaan die een positief expertadvies in de weg zouden kunnen staan. Tot slot wordt er in hoofdstuk 6 een praktijkvoorbeeld gegeven dat Forum Standaardisatie kan gebruiken om de maatschappelijke waarde van de standaard te communiceren.

2 Korte beschrijving van de standaard

2.1 Over de standaard

NVN-CEN/TS 18026 EN bevat een reeks cybersecurityvereisten voor clouddiensten. De standaard voorziet in drie verschillende zekerheidsniveaus, namelijk Basis, Substantieel en Hoog. Sommige eisen zijn op alle niveaus aanwezig, soms uitgebreid op hogere niveaus, terwijl enkele alleen van kracht zijn op het hoogste niveau. Er wordt een risicobeoordeling uitgevoerd om de specifieke risico's voor de clouddienst te bepalen, waarbij ook rekening wordt gehouden met de mogelijkheden van het niveau en de specifieke cyberrisico's voor de clouddienst. De risicobehandeling behelst vervolgens de selectie van passende beheersmaatregelen door de organisatie om te voldoen aan de eisen voor dat niveau.

De standaard is een recent ontwikkelde Europese norm voor de beveiliging van clouddiensten en is opgesteld door de Europese Commissie. Zij sluit inhoudelijk aan op bestaande internationale kaders voor informatiebeveiliging en cybersecurity, zoals de ISO/IEC 27000-serie, maar bevat aanvullende en specifiek op de Europese context afgestemde eisen. De standaard is afgestemd op Europese wet- en regelgeving, waaronder de Europese Cyber Security Act, en is daarmee zowel internationaal herkenbaar als Europees specifiek toepasbaar.

2.2 Waarom is deze standaard belangrijk?

Momenteel ontbreken duidelijke en uniforme overheidsvereisten op het gebied van cloudbeveiliging. Met behulp van deze standaard kan de vraag naar beveiligingseisen helder worden uitgevraagd. De standaard voorkomt versnippering van veiligheidsvoorschriften binnen de EU door één uniform beveiligingsniveau vast te leggen. Hierdoor hoeven clouddienstleveranciers zich nog maar één keer te certificeren volgens het EUCS-schema (op het gekozen niveau) om aan de cybersecurity-eisen van alle deelnemende EU-lidstaten te voldoen. Het toepassen van de standaard draagt zo bij aan betere bescherming van gegevens en systemen, waardoor overheidsorganisaties veiliger kunnen opereren. Tot slot kan het toepassen van één uniform beveiligingsniveau bijdragen aan gelijk een speelveld binnen de Europese markt. Leveranciers hebben dan te maken met uniforme veiligheidsvoorschriften waaraan ze moeten voldoen. Daarbij geldt wel dat afdoende leveranciers in staat moeten zijn daaraan te kunnen voldoen.

3 Betrokkenen en proces

Op 6 mei 2025 hebben Tom Hoogendijk en Roman Volf (Ministerie van Economische Zaken) NVN-CEN/TS 18026:2024 EN aangemeld bij Forum Standaardisatie voor toetsing voor plaatsing op de lijst van aanbevolen standaarden.

Op 30 juni 2025 heeft een intakegesprek plaatsgevonden met de indiener, procedurebegeleider InnoValor Advies en Bureau Forum Standaardisatie. Bij het online intake gesprek waren de volgende personen aanwezig:

- Tom Hoogendijk (Ministerie van Economische Zaken)
- Roman Volf (Ministerie van Economische Zaken)
- Aday Destici (InnoValor Advies)
- Claudia Vermeulen (InnoValor Advies)
- Wouter Kobes (Bureau Forum Standaardisatie)
- Joram Verspaget (Bureau Forum Standaardisatie)

In dit gesprek is verkend of NVN-CEN/TS 18026:2024 EN voldoet aan de criteria om in procedure genomen te worden. Daarnaast is vooruitgeblikt op de toetsingsprocedure. Dit intakeadvies is tot stand gekomen op basis van het intakeonderzoek.

4 Voldoet de standaard aan de criteria om in procedure genomen te worden?

NVN-CEN/TS 18026:2024 EN voldoet niet aan alle vier criteria om in behandeling genomen te worden voor plaatsing op de lijst aanbevolen standaarden. Hoe de standaard is getoetst op de vier criteria wordt hieronder toegelicht in paragrafen 4.1-4.4.

4.1 Draagt de standaard substantieel bij aan het bevorderen van de interoperabiliteit, toekomstige gegevensopslag en/of een verminderde leveranciersafhankelijkheid?

Zoals het er nu naar uitziet draagt NVN-CEN/TS 18026:2024 EN niet bij aan het bevorderen van veilige toekomstige gegevensopslag en een verminderde leveranciersafhankelijkheid. De standaard richt zich uitsluitend op clouddienstverleners. Toepassing ervan lijkt – gezien de gestelde eisen – vooral haalbaar door een beperkt aantal grote hyperscalers. Dit vergroot de afhankelijkheid van grote cloudproviders, omdat vooral zij aan de gestelde eisen van de standaard kunnen voldoen.

De standaard bevat geen specifieke bepalingen die interoperabiliteit tussen verschillende overheidsorganisaties bevorderen of die de afhankelijkheid van bepaalde leveranciers verminderen. Daarmee is het effect van de standaard op leveranciersafhankelijkheid of interoperabiliteit beperkt.

Profielen of voorbeeldimplementaties van de standaard zijn aanwezig en kunnen in overleg met de Rijksinspectie Digitale Infrastructuur (RDI) vrij worden gebruikt. De RDI fungeert als de Nederlandse National Cybersecurity Certification Authority (NCCA) vanuit de Cyber Security Act (CSA) en houdt toezicht op de implementatie van de EUCS.

4.2 Heeft de standaard een toepassing die binnen de overheid een enkele organisatie of sector overstijgt?

Ja, toepassing van de standaard overstijgt een enkele organisatie of sector, aangezien deze betrekking heeft op het gehele ICT-portfolio van de (semi-)overheid. Daarmee is de toepassing breed en kan deze in elke sector van de (semi-)overheid worden toegepast, waardoor deze een enkele organisatie of sector overstijgt.

4.3 Is de standaard niet al wettelijk verplicht?

Nee, NVN-CEN/TS 18026:2024 EN is niet wettelijk verplicht. Wel zijn er ontwikkelingen gaande die zowel overheidsorganisaties als clouddienstproviders raken.

- Overheidsorganisaties

De standaard is ontwikkeld door CEN-CENELEC (European Committee for Standardization-European Committee for Electrotechnical Standardization) in opdracht van de Europese Commissie en het is aannemelijk dat er binnen enkele jaren (>2 jaar) meer Europese kaders volgen. De NIS2-richtlijn, die wordt omgezet in nationale wetgeving via de Cyberbeveiligingswet, legt organisaties een zorgplicht op om passende technische en organisatorische maatregelen te treffen voor de beveiliging van hun netwerk- en informatiesystemen conform geldende Europese normen, waarbij deze standaard als referentiekader zou kunnen dienen.

- Clouddienstproviders

Voor clouddienstproviders is de zorgplicht niet rechtstreeks afkomstig uit NIS2-rictlijn zelf, maar wordt deze verder en concreter ingevuld via Uitvoeringsverordening EU 2024/2690. Op grond van artikel 21, lid 5, derde alinea van Richtlijn EU 2022/2555 specificeert deze verordening welke technische en organisatorische maatregelen nodig zijn voor het beheer van cyberbeveiligingsrisico's. In de verordening wordt expliciet vastgelegd dat deze maatregelen zijn gebaseerd op Europese en internationale normen en technische specificaties die relevant zijn voor de beveiliging van netwerk- en informatiesystemen. In overweging 3 van de verordening wordt specifiek verwezen naar ISO/IEC 27001, ISO/IEC 27002 en de technische specificatie CEN/TS 18026:2024. Hiermee wordt NVN-CEN/TS 18026:2024 EN erkend als relevant referentiekader voor clouddienstverleners. Hierdoor ontstaat feitelijk een directe verplichting voor clouddienstproviders.

4.4 Draagt de standaard bij aan de oplossing van een bestaand, relevant probleem?

Ja, NVN-CEN/TS 18026:2024 EN draagt bij aan de oplossing van een bestaand, relevant probleem. Er zijn nu geen duidelijke (unanieme) vereisten vanuit de overheid op het gebied van Cloudbeveiliging en middels deze standaard kunnen overheidsorganisaties hun vereisten richting leveranciers eenduidig uitvragen. Daarnaast stelt de standaard iedereen in staat om te voldoen aan de beveiligingseisen door middel van drie zekerheidsniveaus (Basis, Substantieel Hoog) waarbij duidelijke maatregelen zijn voorgeschreven voor ieder niveau. Dit creëert een gelijkwaardig speelveld op het gebied van cybersecurity.

5 Is er zicht op een positief expertadvies?

Er lijkt geen zicht op een positief expertadvies. Vastgesteld is dat NVN-CEN/TS 18026:2024 EN niet volledig voldoet aan de basiscriteria. Het belangrijkste aandachtspunt daarnaast is het draagvlak onder clouddienstproviders voor NVN-CEN/TS 18026:2024 EN, ten behoeve van het vermijden van leveranciersafhankelijkheid van een beperkt aantal grote hyperscalers.

Als het Forum Standaardisatie de standaard wel in procedure neemt, wordt een groep experts gevraagd de standaard te toetsen op de vier inhoudelijke criteria voor opname op de 'Pas toe of leg uit'-lijst of de lijst aanbevolen standaarden. Het Forum Standaardisatie neemt geen standaarden in procedure waarvan bij aanvang al vaststaat dat deze niet op een positief expertadvies kan rekenen. Daarom wordt in dit intakeadvies vooruitgeblikt op de vier inhoudelijke criteria. Dit wordt toegelicht in paragrafen 5.1-5.4.

5.1 Toegevoegde waarde

Er is sprake van een duidelijke en urgente behoefte binnen de gehele Europese Unie aan een uniform kader voor cloudbeveiliging, dat NVN-CEN/TS 18026:2024 EN biedt. Het gebruik van clouddiensten (Infrastructure as a Service (IaaS), Platform as a Service (PaaS) en Software as a Service (SaaS)) neemt zowel in de publieke als in de private sector sterk toe. Daarmee

groeit de noodzaak voor betrouwbare, consistente en breed erkende vereisten voor de beveiliging van clouddiensten. De kosten van implementatie zijn bekend en kunnen als acceptabel worden beschouwd.

NVN-CEN/TS 18026:2024 EN conflicteert niet met reeds opgenomen standaarden in Nederland, zoals opgenomen op de lijst van open standaarden van het Forum Standaardisatie. De Europese Commissie heeft opdracht gegeven voor de ontwikkeling van deze standaard en voerde vooraf onderzoek uit om aan te tonen dat het ontwikkelen van deze standaard van groot belang is. De standaard is EU-breed toepasbaar en gestoeld op internationale standaarden. De EC bevordert een spoedige ontwikkeling vanwege het belang voor clouddiensten en brede Europese toepassing.

De beveiligingsrisico's die gepaard gaan met overheidsbrede adoptie van de standaard zijn acceptabel, omdat de voorgestelde maatregelen, vergelijkbaar met ISO 27002, algemeen geaccepteerde maatregelen zijn. De standaard is relevant omdat zij bijdraagt aan het beheersen van beveiligingsrisico's, zoals onvoldoende bescherming van gegevens, inconsistent toegepaste beveiligingsmaatregelen en het ontbreken van duidelijke eisen voor clouddiensten.

De toepassing van deze standaard binnen de overheid brengt geen additionele privacyrisico's met zich mee. De bescherming van persoonsgegevens is reeds volledig geborgd door naleving van de Algemene Verordening Gegevensbescherming (AVG/GDPR).

5.2 Open standaardisatieproces

De documentatie over het ontwikkel- en beheerproces, waaronder het voorlopige specificatiedocument, notulen en de beschrijving van de besluitvormingsprocedure, is vrij beschikbaar voor de overheid en kan zonder belemmeringen via NENconnect worden ingezien. Zij stellen ook het intellectueel eigendomsrecht op de standaard royalty-free voor eenieder beschikbaar

Het besluitvormingsproces is toegankelijk voor alle belanghebbenden waaronder gebruikers, leveranciers, adviseurs en wetenschappers. Dit proces volgt de op consensus gebaseerde aanpak van CEN/CENELEC. Belanghebbenden kunnen formeel bezwaar aantekenen tegen de gevolgde procedure. Tot op heden heeft zich echter geen situatie voorgedaan waarbij formeel bezwaar is aangetekend. De standaardisatieorganisatie organiseert regelmatig overleggen met belanghebbenden over de doorontwikkeling en het beheer van NVN-CEN/TS 18026:2024 EN. Herzieningen volgen de standaardprocedure van CEN/CENELEC, waarbij de standaard elke vier à vijf jaar wordt geëvalueerd. Afhankelijk van de uitkomst kan de standaard worden ingetrokken, gewijzigd of ongewijzigd blijven. Eerdere aanpassing of intrekking is ook mogelijk, afhankelijk van de situatie. Publieke consultaties maken deel uit van het proces van de standaardisatieorganisatie voordat (een nieuwe versie van) de standaard wordt vastgesteld. De ontwikkeling en het beheer van de standaard zijn belegd bij een onafhankelijke non-profit standaardisatieorganisatie, te weten CEN/CENELEC (Informatie Normcommissieleden).

De financiering van de ontwikkeling en het onderhoud van de standaard is voor ten minste drie jaar gegarandeerd. CEN/CENELEC beschikt over gepubliceerd beleid met betrekking tot het versiebeheer van de standaard. Dit beleid is beschreven in een beheerplan (Amendments/Revisions to European Standards) en is goed vindbaar en verkrijgbaar.

Het belang van de Nederlandse overheid is in voldoende mate geborgd bij zowel de ontwikkeling als het beheer van de standaard. Nederland, vertegenwoordigd door het Ministerie van Economische Zaken (EZ), is nauw betrokken geweest bij het ontwikkelproces. Gedurende meerdere jaren heeft Nederland een actieve en leidende rol vervuld, onder andere door het leveren van de voorzitter en een lead editor, en door het voeren van het secretariaat via NEN. Tevens zijn diverse faciliterende en coördinerende taken, in opdracht van de Europese Commissie, door Nederland uitgevoerd. Deze intensieve betrokkenheid strekte zich uit over een periode van circa drie à vier jaar voor de specifieke standaardontwikkeling, en in bredere zin over ruim zeven jaar binnen het domein van Europese cybersecurity-initiatieven.

De vertegenwoordiging van belanghebbenden bij het beheer van de standaard is evenwichtig samengesteld en vormt een goede afspiegeling van zowel het werkingsgebied als het functioneel toepassingsgebied van de standaard. Deze representatie wordt bij iedere revisie opnieuw beoordeeld en, waar nodig, aangepast om blijvende aansluiting bij de belangen van alle relevante partijen te waarborgen. Het belang van de Nederlandse overheid is voldoende geborgd bij de ontwikkeling en het beheer van de standaard. NEN fungeert als toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard beschikbaar is en opgevraagd kan worden. De adoptie en implementatie van de standaard worden ondersteund door EZ en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK).

5.3 Draagvlak

Belangrijke overheidsstakeholders ondersteunen de adoptie van de standaard. Het betreft onder meer de Rijksdienst voor Digitale Infrastructuur (RDI), het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en het Ministerie van Justitie en Veiligheid (JenV). Daarnaast is de Online Trust Coalitie (OTC) betrokken, als breed gedragen publiek-private samenwerking op het gebied van clouddiensten, met een sterke vertegenwoordiging op nationaal, Europees en internationaal niveau. Deze combinatie van partijen vormt een krachtige en representatieve stem voor het Nederlandse belang in de verdere ontwikkeling en toepassing van de standaard. De eerdergenoemde overheidsorganisaties die daadwerkelijk worden geraakt door een mogelijke verplichting van de standaard staan achter het gebruik ervan.

Meerdere leveranciers bieden ondersteuning voor NVN-CEN/TS 18026:2024 EN. Op dit moment is er nog geen formeel certificeringsschema beschikbaar voor cloudserviceproviders (CSP's) op basis van NVN-CEN/TS 18026:2024 EN. De voorbereidingen voor de ontwikkeling van een dergelijk schema zijn echter gestart. De technische specificatie vormt hierbij het fundament voor een toekomstig kader voor conformiteitsbeoordeling, waarmee in de komende periode verdere uitwerking en implementatie kan plaatsvinden. De standaard is

relevant voor alle Nederlandse overheidsorganisaties die clouddiensten afnemen, zoals Saas, PaaS en IaaS.

Er zijn voldoende positieve signalen over toekomstig gebruik van de standaard. Deze blijken onder andere uit uitingen van de OTC, Dutch Cloud Community (DCC), Philips, Amazon AWS, Oracle, NEN, Eurosmart en andere diverse marktpartijen op het gebied van clouddienstverlening, met name vanwege de behoefte aan een duidelijkere vraagcirculatie en het stimuleren van innovatie.

5.4 Opname op de lijst bevordert adoptie

De indiener geeft aan dat de status van aanbevolen standaard het passende middel lijkt om de adoptie van NVN-CEN/TS 18026:2024 EN binnen de (semi)overheid te bevorderen.

De indiener geeft aan dat 'Pas toe of leg uit'-verplichting niet het passende middel is om de adoptie van NVN-CEN/TS 18026:2024 EN binnen de (semi)overheid te bevorderen. De standaard is ontwikkeld voor toepassing binnen de gehele overheid. In een latere fase kan deze verplichting mogelijk wel bijdragen aan verdere adoptie, bijvoorbeeld door uniformiteit in aanbestedingen te bevorderen en het belang om cloudbeveiliging op Europees niveau te versterken.

Gezien de toenemende dreiging op het gebied van cybersecurity blijft een toekomstige verplichtstelling mogelijk. Dit sluit aan bij signalen vanuit onder andere de OTC, overheidsaanbestedingen en relevante marktpartijen in de clouddienstverlening, die de behoefte aan duidelijke vraagarticulatie en het stimuleren van innovatie onderstrepen.

6 Praktijkvoorbeeld

Op dit moment zijn er nog geen praktijkvoorbeelden bekend van de toepassing van NVN-CEN/TS 18026:2024 EN. De Europese Commissie heeft wel de noodzaak onderzocht voor een breed Europees certificeringsschema voor clouddiensten. Dit onderzoek heeft geleid tot de ontwikkeling van de bovengenoemde standaard, die als fundament dient voor harmonisatie van beveiligingseisen binnen de EU.

Voor Nederland biedt de standaard de mogelijkheid om bestaande inspanningen op het gebied van cloudbeveiliging te versterken, versnippering van nationale benaderingen te voorkomen en de internationale positie van Nederlandse publieke en private partijen in de cloudmarkt te versterken.

Voor Europa draagt de standaard bij aan een eenduidig normenkader dat het vertrouwen in clouddiensten vergroot, de interne markt versterkt en een gelijk speelveld creëert voor aanbieders. Daarmee wordt de weerbaarheid tegen cyberdreigingen verhoogd en ontstaat een solide basis voor toekomstige wet- en regelgeving, waaronder implementaties van de NIS2-richtlijn.