



Forumbesluit NVN-CEN/TS 18026:2024 EN

Vergadering:	Forum Standaardisatie 30 september 2026
Agendapunt:	2
Documentnummer:	FS-20260930.2
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	7 september 2026
Bijlagen:	Intakeadvies NVN-CEN/TS 18026:2024 EN Expertadvies NVN-CEN/TS 18026:2024 EN Verslag reactie(s) internetconsultatie NVN-CEN/TS 18026:2024 EN
Rechten	CC0 publieke domein verklaring

1 Besluit

De Stuurgroep open standaarden adviseert het Forum Standaardisatie om te besluiten [NVN-CEN/TS 18026:2024 EN](#) aan te bevelen aan de overheid via plaatsing op de lijst Aanbevolen standaarden van het Forum Standaardisatie.

Het voorgestelde functioneel toepassingsgebied voor NVN-CEN/TS 18026:2024 EN is:

NVN-CEN/TS 18026:2024 kan worden toegepast bij de aanschaf van een ICT-dienst of ICT-product indien deze (geheel of gedeeltelijk) gebruikmaakt van cloud computing.

Toepassing vindt risicogebaseerd plaats naar eigen inzicht, waarbij het niveau 'basis' wordt gehanteerd als minimum om aan de standaard te kunnen voldoen.

Bij de status 'Aanbevolen' is NVN-CEN/TS 18026:2024 EN van toepassing bij aanschaf en doorontwikkeling van een ICT-dienst of ICT-product dat geheel of gedeeltelijk gebruikmaakt van cloud computing. Bij de aanschaf moet daarom worden vastgesteld of de betreffende ICT-dienst of het ICT-product gebruikmaakt van cloud computing. Indien dit het geval is, valt de aanschaf binnen het functioneel toepassingsgebied van de standaard en kan NVN-CEN/TS 18026:2024 EN worden toegepast.

Binnen de Europese markt sluit NVN-CEN/TS 18026:2024 EN aan bij het [EU Cybersecurity Certification Scheme for Cloud Services](#) (EUCS), een raamwerk voor het certificeren van de cybersecurity van clouddienstverleners. Omdat EUCS nog niet formeel is vastgesteld door de Europese Commissie, is plaatsing van NVN-CEN/TS 18026:2024 EN op de lijst Aanbevolen standaarden op dit moment het passende middel om de adoptie van de standaard binnen de (semi-)overheid te bevorderen. Ook (nog) zonder formele vaststelling van EUCS bevat de standaard relevante cybersecurity-vereisten die nu al bruikbaar zijn voor aanbestedingen.

Daarnaast biedt opname op de lijst Aanbevolen standaarden de mogelijkheid om bekendheid met en ervaring in de toepassing van de standaard binnen de overheid op te bouwen. Ook bieden meerdere leveranciers op dit moment nog geen aantoonbare ondersteuning voor de standaard. Er zijn echter wel positieve signalen van marktpartijen over de standaard, wat doet vermoeden dat meerdere leveranciers zich in de toekomst kunnen conformeren aan de standaard.

In dit Forumbesluit wordt de definitie van cloud computing gehanteerd zoals opgenomen in de door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) op 16 april 2026 vastgestelde [Begrippenlijst Clouddterminologie](#). Hiermee sluit dit Forumbesluit aan op het Rijkscloudbeleid en de uniforme cloudddefinities die binnen de Nederlandse overheid worden gehanteerd. De definitie luidt als volgt:

Een model dat het mogelijk maakt om plaats- en tijdsafhankelijk, op een gemakkelijke manier, op afroep, via een netwerk toegang te krijgen tot een voortdurend beschikbare gedeelde verzameling van configureerbare computing resources die snel kunnen worden geleverd en vrijgegeven met minimale inspanning of interactie met de aanbieder.

Een nadere uitwerking van deze definitie, inclusief de essentiële karakteristieken van cloud computing en de onderscheiden service- en implementatiemodellen, is te vinden in de [Begrippenlijst Clouddterminologie](#) van het OBDO.

Tevens worden voor de definities van informatiebeveiliging en cyberbeveiliging de volgende definities gehanteerd:

Informatiebeveiliging: het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie, zoals gehanteerd binnen de ISO/IEC 27000-serie en uitgewerkt in [ISO/IEC 27001](#).

Cyberbeveiliging: de bescherming van netwerk- en informatiesystemen, hun gebruikers en andere betrokkenen tegen cyberdreigingen, met als doel de vertrouwelijkheid, integriteit, beschikbaarheid en authenticiteit van gegevens en diensten te waarborgen. Deze definitie sluit aan bij de benadering uit de [Cyberbeveiligingswet \(NIS2-richtlijn\)](#).

In de rest van dit document wordt dit besluit nader onderbouwd. Hoofdstuk 2 geeft een korte uitleg van het nut en belang van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit voorstel tot stand kwam, alsmede de vervolgstappen. Hoofdstuk 4 beschrijft de resultaten

van de toetsing van de standaard op de inhoudelijke hoofdcriteria. Tot slot geeft hoofdstuk 5 aanvullende adviezen om de adoptie van de standaard te stimuleren.

2 Korte beschrijving van de standaard

2.1 Over de standaard

[NVN-CEN/TS 18026:2024 EN](#) is een recent gepubliceerde Europese norm die een reeks cybersecurityvereisten bevat voor de cyberbeveiliging van clouddiensten. De standaard is in eerste aanleg ontwikkeld door de [European Union Agency for Cybersecurity](#) (ENISA) op verzoek van de Europese Commissie onder de regels van de [Europese Cybersecurity Act](#) en vervolgens omgezet naar een Europese Norm (EN) door [CEN/CENELEC](#) als Europese standaardisatieorganisatie. De standaard sluit inhoudelijk aan op bestaande internationale kaders voor informatiebeveiliging en cybersecurity, zoals de [ISO/IEC 27000-serie](#), en bevat daarnaast eisen die zijn afgestemd op Europese wet- en regelgeving. Hierdoor is de standaard zowel internationaal herkenbaar als Europees specifiek toepasbaar.

De standaard voorziet in drie verschillende zekerheidsniveaus, namelijk: 'Basis', 'Substantieel' en 'Hoog'. Sommige eisen zijn op alle niveaus van toepassing, soms uitgebreid op hogere niveaus, terwijl enkele eisen 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 cyber risico'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.

Binnen de Europese markt sluit NVN-CEN/TS 18026:2024 EN aan bij het EUCS, een raamwerk voor het certificeren van de cybersecurity van clouddienstverleners. Ten tijde van het opstellen van dit voorstel (4 september 2026) is EUCS nog niet formeel vastgesteld door de Europese Commissie. Zodra EUCS in werking treedt en van toepassing wordt, zullen nationale certificeringsschema's naar verwachting gedurende een overgangsperiode van drie jaar worden afgebouwd. Tot die tijd blijven bestaande nationale schema's relevant voor zover deze nog van toepassing zijn en kan reeds worden verwezen naar de criteria en eisen uit EUCS. Clouddienstleveranciers hoeven zich dan 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.

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 in aanbestedingen. Daarnaast beperkt de standaard versnippering van veiligheidsvoorschriften binnen de EU door één uniform beveiligingsniveau vast te leggen. Verder draagt het toepassen van de standaard bij aan betere bescherming van gegevens en systemen, waardoor overheidsorganisaties veiliger kunnen opereren.

Tot slot kan het toepassen van één uniform beveiligingsniveau bijdragen aan een gelijk speelveld binnen de Europese markt, met kansen voor Nederlandse cloudleveranciers in die markt. Leveranciers hebben dan te maken met uniforme veiligheidsvoorschriften waaraan ze moeten voldoen. Daarbij geldt wel dat voldoende leveranciers in staat moeten zijn daaraan te voldoen.

3 Betrokkenen en proces

3.1 Gevolgde procedure

Ministerie van Economische Zaken en Klimaat (EZK) heeft NVN-CEN/TS 18026:2024 EN op 6 mei 2025 aangemeld voor plaatsing op de lijst Aanbevolen standaarden.

De procedurebegeleider InnoValor Advies heeft op 30 juni 2025 een intakegesprek gevoerd met de indiener, in aanwezigheid van Bureau Forum Standaardisatie. In dit gesprek is onderzocht of NVN-CEN/TS 18026:2024 EN voldoet aan de criteria om in procedure te worden genomen. De resultaten van het onderzoek zijn vastgelegd in het [intakeadvies](#).

Op basis van het intakeadvies heeft het Forum Standaardisatie op 11 februari 2026 besloten de standaard in procedure te nemen. Vervolgens heeft de procedurebegeleider in overleg met de indiener en Bureau Forum Standaardisatie een expertgroep samengesteld en een voorzitter aangesteld om de standaard te toetsen.

De leden van de expertgroep zijn op 11 mei 2026 bijeengekomen om de standaard te toetsen aan de criteria en geïdentificeerde aandachtspunten te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied opgesteld. De uitkomst van het expertonderzoek is vastgelegd in het [expertadvies](#).

Het Bureau Forum Standaardisatie publiceerde het expertadvies ter openbare consultatie via de website van [Internetconsultatie](#) van 19 juni 2026 tot 31 juli 2026. In de openbare consultatie zijn [drie openbare reacties](#) ontvangen. De reacties zijn aansluitend voorgelegd aan de indiener van de standaard.

Dit voorstel tot Forumbesluit is opgesteld op basis van het expertadvies, reacties uit de openbare consultatie en inzichten van de leden van het Forum Standaardisatie. Indien het Forum Standaardisatie instemt met dit voorstel, geeft het daarmee de status Aanbevolen aan deze standaard. Het OBDO wordt ter kennisname geïnformeerd over het besluit.

3.2 Resultaat van het expertonderzoek

De geconsulteerde experts adviseren om NVN-CEN/TS 18026:2024 EN aan te bevelen aan de overheid via plaatsing op de lijst Aanbevolen standaarden van het Forum Standaardisatie voor de aanschaf van een ICT-dienst of ICT-product indien deze (geheel of gedeeltelijk) gebruikmaakt van cloud computing.

NVN-CEN/TS 18026:2024 EN voldoet aan de criteria 'Toegevoegde waarde', 'Open standaardisatieproces' en 'Opname op de lijst bevordert adoptie', maar nog niet volledig aan

het criterium 'Draagvlak'. Meerdere leveranciers bieden op dit moment nog geen aantoonbare ondersteuning voor de standaard, hoewel er positieve signalen vanuit de markt zijn die erop wijzen dat meerdere leveranciers zich in de toekomst kunnen conformeren. Ook ontbreekt op dit moment nog een implementatietoets voor cybersecuritycertificering van diensten van Cloud Service Providers (CSP's) op basis van NVN-CEN/TS 18026:2024 EN. Gezien het ontwikkelstadium van EUCS en de gekozen status van Aanbevolen standaard wordt dit onvoldoende zwaarwegend geacht om aanbeveling in de weg te staan.

De standaard draagt bij aan standaardisering van processen en de manier waarop CSP's communiceren, waaronder uniformering van definities. Dit draagt tevens bij aan verhoging van het beveiligingsniveau. Vooralsnog zijn er geen profielen of voorbeeldimplementaties van de standaard beschikbaar. Naar verwachting worden deze, zodra EUCS is vastgesteld als Europese act, vanuit ENISA beschikbaar gesteld.

EZK wordt geadviseerd de promotie van de standaard te ondersteunen en verdere stappen te zetten in de adoptie ervan. Zodra de EUCS-certificering is vastgesteld, wordt geadviseerd NVN-CEN/TS 18026:2024 EN opnieuw aan te melden voor toetsing voor plaatsing op de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie. Ten slotte wordt het Forum Standaardisatie geadviseerd nader te reflecteren op de definities van autonomie, digitale soevereiniteit en leveranciersafhankelijkheid, zodat meer duidelijkheid ontstaat over de onderlinge samenhang en toepassing van deze begrippen.

3.3 Resultaat van de openbare consultatie

In de openbare consultatie zijn [drie openbare reacties](#) ontvangen. De volledige reacties zijn in het consultatieverslag bijgevoegd. De samenvattingen van de openbare reacties, evenals de reactie van indiener EZK daarop en het voorstel van de Stuurgroep open standaarden aan het Forum Standaardisatie, zijn in de volgende paragrafen opgenomen.

3.3.1 Reacties openbare consultatie

De openbare reacties onderschrijven het belang van NVN-CEN/TS 18026:2024 EN en ondersteunen plaatsing van de technische specificatie op de lijst Aanbevolen standaarden van het Forum Standaardisatie. Tegelijkertijd wordt verplichte toepassing op dit moment nog niet passend geacht. Daarbij wordt gewezen op het nog niet vastgestelde EUCS-certificeringsstelsel, de beperkte praktijkervaring met de standaard en het nog beperkte zicht op de daadwerkelijke adoptie binnen de Nederlandse overheid.

In de reacties wordt tevens aandacht gevraagd voor de representativiteit en betrokkenheid van verschillende overheidsorganisaties, waaronder waterschappen, gemeenten, provincies en uitvoeringsorganisaties. Ook wordt het belang genoemd van een praktische en toetsbare implementatie, bijvoorbeeld door middel van implementatiehandreikingen, aansluiting op bestaande normen en assurancekaders, pilots en monitoring van de effecten op onder meer leveranciersafhankelijkheid, marktdynamiek en digitale autonomie.

Verder wordt het belang van digitale autonomie, digitale soevereiniteit en het beperken van leveranciersafhankelijkheid benadrukt. Ook wordt gewezen op de aansluiting van NVN-CEN/TS 18026:2024 EN op internationaal erkende standaarden, waaronder ISO/IEC 27001, ISO/IEC 27002 en ISO/IEC 27017. Tot slot wordt in de reacties aandacht gevraagd voor de verdere ontwikkeling van EUCS, de governance en de relatie van NVN-CEN/TS 18026:2024 EN met bestaande internationale standaarden.

3.3.2 Reactie van indiener EZK op de ontvangen reacties

EZK onderschrijft het belang van een zorgvuldig en representatief adviestraject en acht het van belang dat relevante partijen die de standaard in de praktijk zullen toepassen, voldoende zijn vertegenwoordigd. De kanttekening over de vertegenwoordiging van decentrale overheden en uitvoeringsorganisaties wordt onderschreven. Ook wordt het belang van digitale autonomie, digitale soevereiniteit en het beperken van leveranciersafhankelijkheid onderschreven. NVN-CEN/TS 18026:2024 EN is echter primair gericht op cybersecurity van clouddiensten en is niet specifiek ontworpen om deze aspecten rechtstreeks te adresseren. Bij een eventuele toekomstige toetsing voor de 'Pas toe of leg uit'-lijst kunnen deze aspecten, evenals marktwerking en leveranciersafhankelijkheid, opnieuw worden onderzocht.

EZK onderschrijft ook de gekozen gefaseerde benadering. Omdat EUCS nog niet formeel is vastgesteld, een formeel certificeringsmechanisme ontbreekt en de toepassing van de standaard in de praktijk nog in ontwikkeling is, wordt NVN-CEN/TS 18026:2024 EN voorgesteld voor plaatsing op de lijst Aanbevolen standaarden en niet op de 'Pas toe of leg uit'-lijst. Praktische guidance, mappings met bestaande normen en assurancekaders, pilots en monitoring worden gezien als waardevolle aandachtspunten voor verdere adoptie en implementatie.

Tot slot wordt het belang van aansluiting bij internationaal erkende standaarden onderschreven. NVN-CEN/TS 18026:2024 EN sluit inhoudelijk aan op bestaande internationale kaders voor informatiebeveiliging en cybersecurity. Het voorstel om ISO/IEC 27017 afzonderlijk op een lijst van het Forum Standaardisatie op te nemen, valt buiten de reikwijdte van deze procedure en vereist een afzonderlijke aanmelding en toetsing. De opmerkingen over de verdere ontwikkeling en implementatie van EUCS worden voor kennisgeving aangenomen; deze toetsing ziet uitsluitend op NVN-CEN/TS 18026:2024 EN.

3.3.3 Voorstel Stuurgroep open standaarden

De reacties op de openbare consultatie hebben niet geleid tot aanpassing van het voorstel om NVN-CEN/TS 18026:2024 EN via plaatsing op de lijst Aanbevolen standaarden van het Forum Standaardisatie aan de overheid aan te bevelen.

Uit de reacties blijkt brede aandacht voor het belang van digitale autonomie, digitale soevereiniteit en leveranciersafhankelijkheid. Daarnaast wordt aandacht gevraagd voor implementatieondersteuning, assurance, adoptiebevordering en monitoring. Deze aandachtspunten zijn relevant voor de verdere toepassing en adoptie van de standaard, maar geven geen aanleiding om het voorstel aan te passen.

Ook wordt in de reacties aandacht gevraagd voor de relatie met internationaal erkende standaarden en voor de verdere ontwikkeling van EUCS. NVN-CEN/TS 18026:2024 EN bouwt voort op bestaande internationale standaarden voor informatiebeveiliging en cybersecurity, zoals de ISO/IEC 27000-serie en bevat eisen die zijn afgestemd op Europese wet- en regelgeving. De verdere ontwikkeling en het certificeringsproces van EUCS zijn op dit moment nog onvoldoende duidelijk om toepassing van de standaard binnen de (semi-)overheid via de status 'Pas toe of leg uit' verplicht te stellen.

Er is wel voldoende draagvlak om NVN-CEN/TS 18026:2024 EN de status 'Aanbevolen standaard' te geven. Deze status biedt de mogelijkheid om de bekendheid met en ervaring in het toepassen van de standaard binnen de (semi-)overheid op te bouwen en daarmee de verdere adoptie te bevorderen. De reacties op de openbare consultatie geven geen aanleiding om deze conclusie te wijzigen.

4 Toetsing op inhoudelijke criteria

Het Forum Standaardisatie hanteert vier inhoudelijke hoofdcriteria om te toetsen of een standaard in aanmerking komt voor verplichten ('Pas toe of leg uit') of aanbevelen aan de overheid.

1. Heeft de standaard toegevoegde waarde?
2. Zijn de standaard en het standaardisatieproces voldoende open?
3. Heeft de standaard voldoende draagvlak?
4. Is opname op de lijst een passend middel om de adoptie te bevorderen?

Ieder van deze hoofdcriteria heeft deelcriteria [die staan beschreven op de website van het Forum Standaardisatie](#). Dit hoofdstuk beschrijft per criterium het resultaat van de toetsing.

4.1 Toegevoegde waarde

De toetsingsprocedure wijst uit dat NVN-CEN/TS 18026:2024 EN voldoet aan het criterium 'Toegevoegde waarde'.

NVN-CEN/TS 18026:2024 EN draagt bij aan een eenduidig referentiekader voor cybersecurity van clouddiensten. Zo dient iedere Cloud Service Provider (CSP) de scope en grenzen van de aangeboden dienst te documenteren, zodat duidelijk is welke onderdelen onder de verantwoordelijkheid van de CSP vallen. Daarnaast kan de standaard indirect bijdragen aan leveranciersafhankelijkheid doordat meerdere leveranciers een gelijk referentiekader gebruiken voor het inrichten van cybersecurity. De standaard bevat echter 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.

De standaard biedt meerwaarde ten opzichte van [NEN ISO/IEC 27001](#) en [NEN-ISO/IEC 27002](#), doordat de standaard voortbouwt op bestaande normen en kaders voor informatiebeveiliging en deze verder uitwerkt met specifieke en gedetailleerde eisen voor

clouddiensten. De standaard bevat onder andere eisen die aansluiten op ISO/IEC 27001, waaronder eisen ten aanzien van een [Information Security Management System](#) (ISMS), en biedt daarmee aanvullende handvatten voor de beveiliging van cloudomgevingen.

De kosten van implementatie voor inkopende organisaties van NVN-CEN/TS 18026:2024 EN worden in algemene zin als acceptabel beschouwd. Tegelijkertijd zijn er nog geen concrete voorbeeldcases beschikbaar en zijn de totale implementatiekosten nog niet eenduidig bekend of volledig inzichtelijk. Organisaties dienen op basis van een eigen risicobeoordeling de specifieke risico's van de clouddienst te bepalen, waarbij rekening wordt gehouden met het benodigde beveiligingsniveau en de specifieke cyberrisico's van de betreffende clouddienst. Het voldoen aan hogere niveaus kan aanvullende kosten met zich meebrengen. Daarnaast bestaan er onzekerheden over de impact van de benodigde investeringen, met name voor middelgrote en kleinere cloudaanbieders.

De kosten voor het verkrijgen van het [specificatiedocument](#) worden als acceptabel beschouwd. Op dit moment geldt hiervoor een tarief van 185 euro exclusief btw. De deelname aan het [standaardisatieproces](#) via NEN brengt jaarlijkse kosten van 2.680 euro exclusief btw met zich mee voor het lidmaatschap. De overheid kan de documentatie kosteloos raadplegen via NEN Connect.

Omdat de standaard nog recent is ontwikkeld, is er nog geen uitgewerkte kwalitatieve business case beschikbaar. Tegelijkertijd neemt het gebruik van clouddiensten, zoals Infrastructure as a Service (IaaS), Platform as a Service (PaaS) en Software as a Service (SaaS), zowel in de publieke als private sector sterk toe. Daarmee groeit de behoefte aan betrouwbare, consistente en breed erkende vereisten voor de cyberbeveiliging van clouddiensten.

4.2 Open standaardisatieproces

De toetsingsprocedure wijst uit dat het beheer van NVN-CEN/TS 18026:2024 EN voldoet aan het criterium 'Open standaardisatieproces'.

Het specificatiedocument is zonder belemmeringen beschikbaar via [NEN.nl](#). Daarnaast is de documentatie over het ontwikkel- en beheerproces ([CEN/CENELEC](#)) vrij beschikbaar voor de overheid en kan deze zonder belemmeringen worden ingezien. Het [intellectueel eigendomsrecht](#) op (onderdelen van) de standaard wordt door de standaardisatieorganisatie en door partijen die bijdragen aan de ontwikkeling van de standaard onherroepelijk royalty-free voor eenieder beschikbaar gesteld.

Tevens is het [besluitvormingsproces](#) toegankelijk voor alle belanghebbenden, waaronder gebruikers, leveranciers, adviseurs en wetenschappers. De ontwikkeling en het beheer van de standaard volgen de op consensus gebaseerde aanpak van [CEN/CENELEC](#), met nationale implementatie via NEN in Nederland. Daarnaast kunnen belanghebbenden [formeel bezwaar aantekenen](#) tegen de gevolgde procedure en [openbare consultaties](#) maken onderdeel uit van het proces 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. Ook beschikt CEN/CENELEC over gepubliceerd beleid met betrekking tot het versiebeheer van de standaard en is de [beheerdocumentatie](#) goed vindbaar en verkrijgbaar.

Nederland is vertegenwoordigd door het [Ministerie van Economische Zaken en Klimaat](#) (EZK), nauw betrokken geweest bij het ontwikkelproces. De vertegenwoordiging van belanghebbenden bij het beheer van de standaard via de [NEN-normcommissie](#) evenwichtig samengesteld en vormt deze een goede afspiegeling van zowel het werkingsgebied als het functioneel toepassingsgebied van de standaard. Tot slot fungeert NEN als toegankelijk aanspreekpunt waar meer informatie over de standaard beschikbaar is en kan worden opgevraagd. De adoptie en implementatie van de standaard worden ondersteund door EZK en BZK binnen de overheid.

4.3 Draagvlak

De toetsingsprocedure wijst uit dat NVN-CEN/TS 18026:2024 EN deels voldoet aan het criterium 'Draagvlak'.

De [Rijksdienst voor Digitale Infrastructuur](#) (RDI), het [Ministerie van Binnenlandse Zaken en Koninkrijksrelaties](#) (BZK) en het [Ministerie van Justitie en Veiligheid](#) (JenV) de adoptie van de standaard. Ook is de [Online Trust Coalitie](#) (OTC) betrokken als breed gedragen publiek-private samenwerking op het gebied van clouddiensten. Tegelijkertijd is er geen inzicht in de mate waarin gemeenten, provincies, waterschappen en uitvoeringsorganisaties de adoptie van de standaard ondersteunen.

Vanuit marktpartijen zijn er positieve signalen over de standaard en de verwachting is dat meerdere leveranciers zich in de toekomst aan de standaard kunnen conformeren. Dit blijkt onder andere uit uitingen van de OTC en de Dutch Cloud Community (DCC), en vanuit organisaties zoals NEN, Eurosmart en andere marktpartijen op het gebied van clouddienstverlening. Op dit moment is echter nog niet aantoonbaar dat meerdere leveranciers ondersteuning bieden voor de standaard.

Ook zijn er signalen dat toepassing van de standaard voor het zekerheidsniveau 'Hoog', gezien de gestelde eisen, mogelijk slechts haalbaar is voor een beperkt aantal grote Cloud Service Providers. Vooralsnog is er geen implementatietoets beschikbaar voor cybersecuritycertificering van diensten van Cloud Service Providers op basis van NVN-CEN/TS 18026:2024 EN. Ook zijn er nog geen profielen of voorbeeldimplementaties van de standaard beschikbaar. De verwachting is dat deze profielen vanuit ENISA beschikbaar worden gesteld zodra de EUCS is vastgesteld als Europese act.

De standaard draagt niet direct bij aan interoperabiliteit, maar draagt wel bij aan de standaardisering van processen, definities en de manier waarop Cloud Service Providers met elkaar communiceren. Dit draagt tevens bij aan de verhoging van het beveiligingsniveau.

4.4 Opname op de lijst bevordert adoptie

De toetsingsprocedure wijst uit dat NVN-CEN/TS 18026:2024 EN voldoet aan het criterium 'Opname op de lijst bevordert adoptie'.

Het Forum Standaardisatie acht de status 'Pas toe of leg uit' op dit moment minder geschikt, omdat er nog onvoldoende duidelijkheid bestaat over de verdere ontwikkeling van en het certificeringsproces voor EUCS. Zolang hierover geen duidelijkheid bestaat, is het niet passend om de toepassing van de standaard binnen de (semi-)overheid verplicht te stellen.

Er is voldoende draagvlak voor NVN-CEN/TS 18026:2024 EN om de standaard op dit moment de status van Aanbevolen standaard te geven. Deze status biedt de mogelijkheid om binnen de (semi-)overheid bekendheid met en ervaring in de toepassing van de standaard op te bouwen en daarmee de verdere adoptie te bevorderen.

In een latere fase kan het toekennen van de status 'Pas toe of leg uit' mogelijk wel bijdragen aan verdere adoptie, bijvoorbeeld door meer uniformiteit in aanbestedingen te bevorderen en het belang van cloudb beveiliging op Europees niveau te versterken. Dit sluit aan bij signalen vanuit onder andere de OTC, overheidsaanbestedingen en relevante marktpartijen in de clouddienstverlening over de behoefte aan duidelijke vraagarticulatie en het stimuleren van innovatie.

5 Adviezen bij opname van de standaard

Het Forum Standaardisatie geeft de volgende adviezen bij plaatsing van NVN-CEN/TS 18026:2024 EN op de lijst Aanbevolen standaarden:

- Aan Ministerie van Economische Zaken en Klimaat om de promotie van de standaard te ondersteunen en verdere stappen te zetten in de adoptie ervan;
- Aan Ministerie van Economische Zaken en Klimaat om, zodra de EUCS-certificering is vastgesteld, NVN-CEN/TS 18026:2024 EN opnieuw aan te melden voor toetsing voor plaatsing op de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie.

Aanvullend neemt het Forum Standaardisatie het voorstel uit de expertsessie over om nader te reflecteren op de definities van autonomie, digitale soevereiniteit en leveranciersafhankelijkheid, zodat meer duidelijkheid ontstaat over de onderlinge samenhang en toepassing van deze begrippen.