



Justitiële Informatiedienst
Ministerie van Justitie en Veiligheid

DEPARTEMENTAAL VERTROUWELIJK

e-Evidence ETSI-API aansluitvoorwaarden

Versienummer 0.4.1

Datum	24 juni 2026
Status	concept

Colofon

Projectnaam	e-Evidence
Versienummer	0.4.1

Inleiding

Om te voldoen aan de e-Evidence verordening¹ wordt door het Ministerie van Veiligheid en Justitie in Nederland een voorziening voor dienstaanbieders ingericht. Deze voorziening maakt het mogelijk voor Nederlandse dienstaanbieders om verzoeken van buitenlandse autoriteiten te ontvangen en te beantwoorden.

Waar de insteek aanvankelijk was om deze voorziening zelf te ontwikkelen en beschikbaar te stellen wordt hier vooralsnog vanaf gezien en zal de door de Europese Commissie ontwikkelde Reference Implementation (RI) in Nederland uitgerold en beschikbaar worden gemaakt.

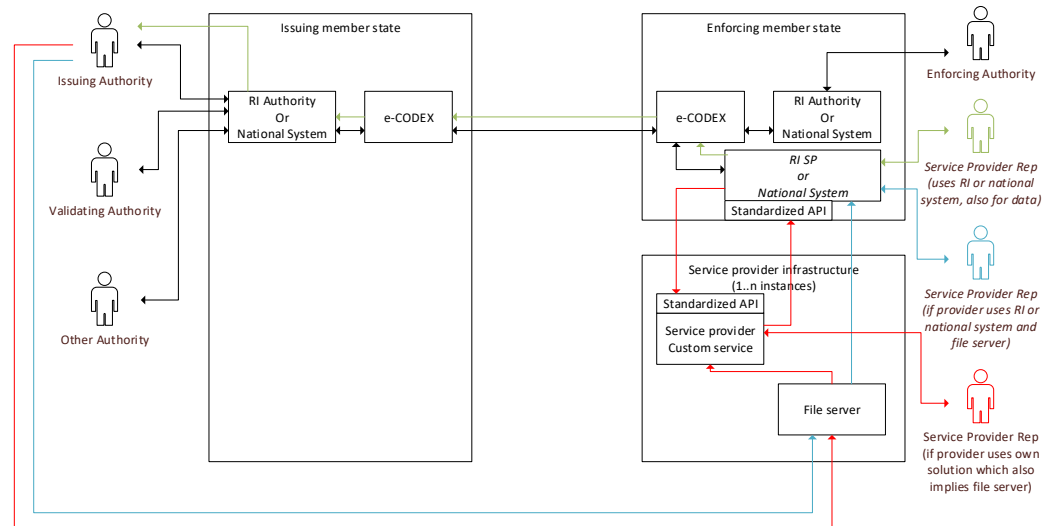
De basis interface die aan alle dienstaanbieders beschikbaar wordt gesteld is een web interface, maar voor een selecte groep aan dienstaanbieders wordt ook een API beschikbaar gemaakt. Deze API is gebaseerd op de ETSI TS 104 144 standaard, die weer gebruik maakt van de TS 103 120 standaard.

Dit document beschrijft de eisen aan en aansluitvoorwaarden die gelden voor Nederlandse dienstaanbieders in scope van de e-Evidence verordening die een geautomatiseerde koppeling middels deze API voorzien.

¹ <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32023R1543>

1 Overzicht e-Evidence

Globaal ziet het e-Evidence landschap er als volgt uit:



Dit document is van toepassing op de koppeling middels de op ETSI standaarden gebaseerde API. In de tekening zijn dit de rode lijnen.

2 Eisen

Om gebruik te kunnen maken van de ETSI API dient uw organisatie aan een aantal eisen te voldoen.

2.1 Uw organisatie valt binnen de scope van e-Evidence

Uw organisatie is aanbieder van digitale diensten binnen de Europese Unie, uw organisatie is in Nederland bij de Kamer van Koophandel geregistreerd.

2.2 Registratie bij de Europese Commissie en goedkeuring ACM

Om het voor buitenlandse autoriteiten mogelijk te maken met uw organisatie te communiceren moet u zich hebben ingeschreven bij de Europese Commissie. Dit kunt u doen middels de online formulieren te vinden op:

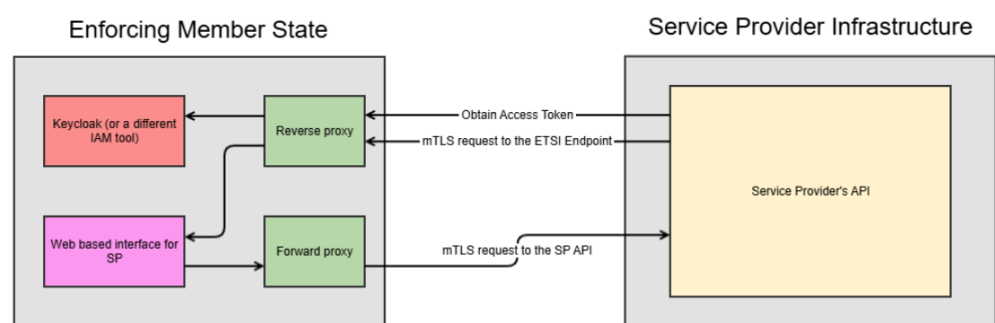
<https://webgate.ec.europa.eu/cdb-sp-reg/home>

U ontvangt t.z.t. de inloggegevens hiervoor van de Autoriteit Consument & Markt (ACM) zodra u zich daarvoor kunt inschrijven. In Nederland is de Autoriteit Consument & Markt (ACM) aangesteld als centrale autoriteit. Zij beoordelen uw registratie en keuren deze goed of af.

Voorafgaand aan deze goedkeuring, kunt u desgewenst uw systemen al (laten) aanpassen aan de ETSI API voor e-Evidence.

2.3 Ontwikkeling ETSI API aan dienstaanbiederskant

Het verkeer met de ETSI API is bidirectioneel. Dit betekent dat het niet enkel voldoende is om de op de e-Evidence dienstverlening gepubliceerde API te consumeren, zelf zult u ook een API beschikbaar moeten stellen waarop onder andere verzoeken kunnen worden afgeleverd.



Zie voor meer informatie ten aanzien van de ETSI standaarden de documentatie op de ETSI site

(https://www.etsi.org/deliver/etsi_ts/104100_104199/104144/01.04.01_60/ts_104144v010401p.pdf)².

² Huidige versie van de ETSI TS 104 144 is versie 1.4.1

3 Voorwaarden voor aansluiting

3.1 Aansluiting op JUBES

De e-Evidence voorziening voor dienstaanbieders wordt gehost op infrastructuur van het Ministerie van Veiligheid en Justitie. Om ons netwerk te beveiligen wordt voor al onze informatie-uitwisseling met externe partners gebruik gemaakt van de Justitie Berichten Service (JUBES). Dit betekent dat u, om gebruik te kunnen maken van de ETSI API eerst aangesloten moet worden op de JUBES dienstverlening.

Het aanvraagformulier hiervoor wordt op aanvraag verstrekt. Verzoeken hiertoe kunt u richten tot het Klant en Contact Centrum van de Justitiële Informatiedienst via info@justid.nl.

Aansluiting op JUBES brengt twee aanvullende voorwaarden met zich mee:

3.1.1 *Vaste IP-adressen*

De voorziening die namens u gaat communiceren met de ETSI API moet voorzien zijn van vaste IP-adressen.

3.1.2 *mTLS en certificaatgebruik*

Tevens worden alle verbindingen beveiligd met tweezijdige TLS (mutual TLS, afgekort als mTLS). Dit betekent dat uw organisatie zich op verbindingsniveau moet identificeren met een client certificaat.

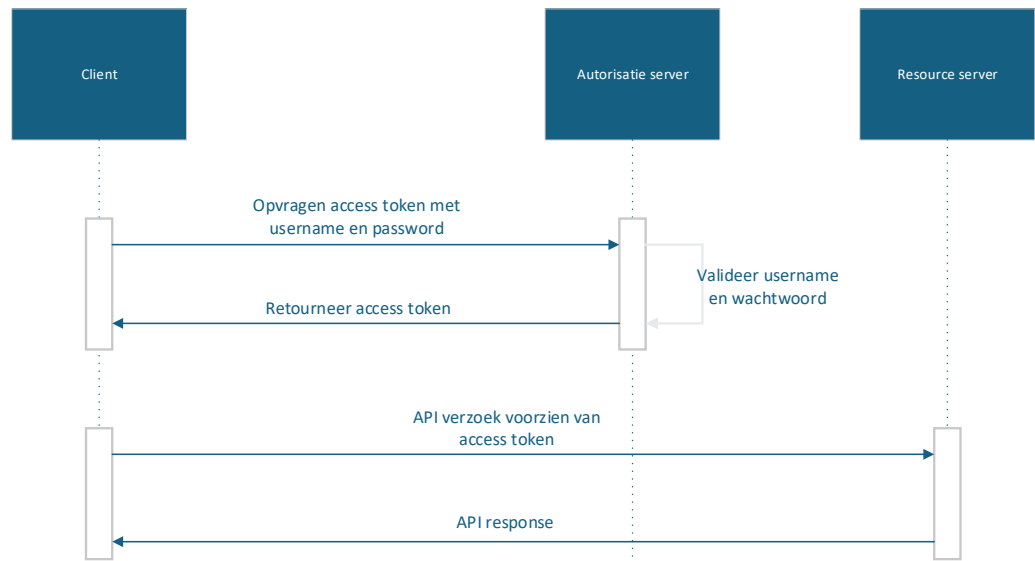
Vanwege de beperkingen die het CAB-Forum oplegt aan publiekelijk vertrouwde certificaten (die mogen de extensie voor client authentication niet langer krijgen) raden wij aan een PKIoverheid certificaat te gebruiken. Het PKIoverheid stelsel is gebaseerd op een private root van de Nederlandse overheid die niet direct gebonden is aan de beperkingen van het CAB-Forum.

Iedere partij die ingeschreven staat bij de Kamer van Koophandel kan een PKIoverheid certificaat aanschaffen.

3.2 OAUTH Password Credentials

De Reference Implementation van de Europese Commissie vereist naast mTLS ook dat er eerst een access token wordt verkregen. Dit access token wordt vervolgens in opvolgende API calls meegegeven aan de API.

Om dit te ondersteunen wordt de OAUTH Password Credentials flow gebruikt.



Hiervoor wordt per dienst aanbieder die via de API koppelt een registratie gedaan in ons IAM systeem.

De door de dienst aanbieder te gebruiken credentials worden vervolgens verstrekt.

NB. Op de koppeling vanaf de e-Evidence voorziening richting een specifieke dienst aanbieder wordt enkel gebruik gemaakt van mTLS.

4 Proces

In het kort dienen de volgende stappen doorlopen te worden:

1. Verifieer of u als dienst aanbieder onder de e-Evidenceverordening valt.
2. De aanvraag starten via een melding bij het Klant en Contact Centrum van de Justitiële Informatiedienst op info@justid.nl
3. U krijgt vervolgens het aanvraagformulier, deze vult u in en stuurt u terug
4. Na verwerking en configuratie krijgt u van ons de volgende gegevens:
 - a. Het URL van de API
 - b. Het URL van het token endpoint
 - c. De user credentials
5. Na configuratie in uw systeem wordt er een connectiviteitstest uitgevoerd