



**VOORWAARDEN VAN HET VIDEO-IDENTIFICATIEPROCES EN DE AFGIFTE
VAN KORTETERMIJNCERTIFICATEN**

QES ONCE

Enerzijds is SIGNICAT, S.L.U., (voorheen bekend als "Electronic Identification S.L."), met zetel te Avenida Ciudad de Barcelona 81, 4ª Planta, ingeschreven in het Handelsregister van Madrid op 13 maart 2013 met NIF B86681533, (hierna SIGNICAT SLU), is een Gekwalificeerde Verlener van Vertrouwsdiensten, handelend overeenkomstig de bepalingen van Verordening (EU) 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 juli 2014 betreffende elektronische identificatie en vertrouwsdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, alsmede de technische ETSI-normen die van toepassing zijn op de afgifte en het beheer van gekwalificeerde certificaten, voornamelijk EN 319 411-1 en EN 319 411-2, teneinde de naleving van de wettelijke voorschriften en de internationale erkenning van hun diensten te vergemakkelijken.

Anderzijds de ABONNEE of AANVRAGER, wiens identificatiegegevens voor de toepassing van dit contract zijn opgenomen in het gebruikte Identificatiedocument en in de video die als resultaat van het proces van video-identificatie en Certificaatafgifte wordt gegenereerd.

1. OBJECT

Het doel van dit document is de AANVRAGER/ABONNEE op een duidelijke en begrijpelijke manier te informeren over de huidige "Voorwaarden van het video-identificatieproces en de afgifte van certificaten van korte duur", en de diensten te regelen in overeenstemming met de voorwaarden in dit document, de certificatiepraktijkverklaring, de eIDAS-verordening en de lokale wetgeving die van toepassing kan zijn.

Dit voorafgaande identificatieproces is noodzakelijk om de identiteit te accrediteren van de AANVRAGER/ABONNEE, die SIGNICAT SLU verzoekt een gekwalificeerd certificaat van elektronische handtekening van natuurlijke persoon van korte duur ("Certificatiediensten") af te geven, certificaat waarvan het gebruik onderworpen is aan de voorwaarden van de hieronder beschreven Elektronische Certificatiedienst die door SIGNICAT SLU als gekwalificeerde aanbieder van vertrouwsdiensten wordt verleend.

De ABONNEE erkent en gaat ervan uit dat het lezen en aanvaarden van dit document door het aanvinken van de vakjes wordt beschouwd als een eenvoudige elektronische handtekening.

2. TOEPASSELIJKE DEFINITIES

- **CERTIFICATIE AUTORITEIT (CA)**: entiteit die zowel door de verzender als door de ontvanger van het bericht wordt vertrouwd. Dit vertrouwen van beide in een "vertrouwde derde partij" stelt elk van hen in staat op zijn beurt de door de Certificatie Autoriteit ondertekende documenten te vertrouwen, met name de documenten die elke openbare sleutel identificeren met de overeenkomstige eigenaar en die certificaten worden genoemd. Bij het verlenen van de door de ABONNEE gevraagde dienst treedt SIGNICAT SLU op als Certificatie Autoriteit die een bepaalde openbare sleutel koppelt aan een bepaalde ABONNEE door middel van de afgifte van een Certificaat.
- **REGISTRATIE AUTORITEIT (RA)**: Entiteit die, naast andere functies, de AANVRAGER van een certificaat en, in voorkomend geval, de andere omstandigheden die met het certificaat samenhangen, op unieke wijze identificeert overeenkomstig het bepaalde in punt 1.3.2. De Registratie Autoriteit verstrekt de Certificatie Autoriteit de geverifieerde gegevens van de aanvrager zodat de Certificatie Autoriteit het overeenkomstige certificaat

kan afgeven. Alle of alle eigen functies van de RA kunnen rechtstreeks door SIGNICAT SLU of door een door SIGNICAT SLU gemachtigde entiteit worden waargenomen.

- **CERTIFICAAT VOOR ELEKTRONISCHE ONDERTEKENING:** Een elektronische verklaring die de valideringsgegevens van een handtekening koppelt aan een natuurlijke persoon en ten minste de naam of het pseudoniem van die persoon bevestigt.
- **KWALIGERED CERTIFICAAT VOOR ELEKTRONISCHE ONDERTEKENING:** Een certificaat voor een elektronische handtekening dat is afgegeven door een Gekwalificeerde Verlener van Vertrouwsdiensten en voldoet aan de eisen van Bijlage I van EU-Rerodening 910/2014 van 23 juli 2014 (eIDAS- Rerodening), dat de maximale wettelijke garanties biedt op het gebied van identificatie van de ondertekenaar en zijn unieke koppeling aan de handtekening, integriteit en onweerlegbaarheid van de gegevens zoals die aan de handtekening zijn gekoppeld.
- **CERTIFICATIEPRAKTIJKVERKLARING ("CPS"):** is een door een Certificatie Autoriteit opgesteld document dat de verlening van certificeringsdiensten door die Certificatie Autoriteit in haar hoedanigheid van certificeringsdienstverlener, in dit geval SIGNICAT SLU, omvat of regelt. Het regelt onder meer het beheer van de gegevens voor het aanmaken en verifiëren van handtekeningen en van de Certificaten, de voorwaarden voor het aanvragen, afgeven, gebruiken, opschorten en beëindigen van de geldigheid van de Certificaten.
- **GEKWALIFICEERDE ELEKTRONISCHE HANDTEKENING:** een geavanceerde elektronische handtekening die is aangemaakt door een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en is gebaseerd op een gekwalificeerd certificaat voor elektronische handtekeningen. De geldigheid van de handtekening is iuris tantum omdat het een gekwalificeerde handtekening is; de bewijslast rust op de persoon die de handtekening als geldig verwerpt.
- **GEKWALIFICEERDE VERLENER VAN VERTROUWENSDIENSTEN:** een verlener van vertrouwsdiensten die een of meer gekwalificeerde vertrouwsdiensten verleent en door de toezichthoudende instantie is gekwalificeerd.
- **APPLICANT OF ABONNEE** is de geïdentificeerde natuurlijke persoon die de SIGNICAT SLU-certificatiediensten contracteert en die, voorafgaand aan de afgifte van het gekwalificeerde certificaat, het SIGNICAT SLU-video-identificatieproces heeft aangevraagd en met succes heeft afgerond.

3. VOORWAARDEN VAN HET VIDEO-IDENTIFICATIEPROCES

Het Identificatieproces van de Aanvrager van de door SIGNICAT SLU aangeboden identificatiediensten voor de afgifte van elektronische certificaten wordt uitgevoerd op een van de volgende wijzen, overeenkomstig artikel 24.1 eIDAS:

- a) in aanwezigheid van de natuurlijke persoon of een gemachtigde vertegenwoordiger van de rechtspersoon, waarvoor de Aanvrager zich moet begeven naar de kantoren van SIGNICAT SLU, Av. de la Ciudad de Barcelona, 81, 4^a Planta, 28007 Madrid, aangezien er geen gedelegeerde Registratie Autoriteiten zijn.

- b) op afstand, met behulp van elektronische identificatiemiddelen, waarvoor de aanwezigheid van de natuurlijke persoon of van een gemachtigde vertegenwoordiger van de rechtspersoon is gegarandeerd vóór de afgifte van het gekwalificeerde certificaat, en in overeenstemming met het video-identificatieproces waarnaar in dit document en de verklaring inzake Certificatiepraktijkverklaring wordt verwezen en dat toegankelijk is via de volgende link:
<https://www.signicat.com/about/qualified-certificates-for-electronic-signatures>
- c) door middel van een overeenkomstig punt a) of b) afgegeven certificaat van gekwalificeerde elektronische handtekening of een gekwalificeerd elektronisch zegel.
- d) met behulp van andere nationaal erkende identificatiemethoden die qua betrouwbaarheid gelijkwaardig zijn aan fysieke aanwezigheid. De gelijkwaardige beveiliging wordt bevestigd door een conformiteitsbeoordelingsinstantie.

3.1 BEVESTIGING VAN DE IDENTITEIT MET ELEKTRONISCHE MIDDELEN EN BESCHRIJVING VAN HET VIDEO-IDENTIFICATIEPROCES.

Het video-identificatieproces (hierna het "video-identificatieproces" of het "proces" genoemd) is een methode voor realtime, onbeheerde video-identiteitsverificatie op afstand die wordt aangeboden via de eigen suite van softwarebibliotheken, REST-toepassingsinterfaces en webapplicaties van SIGNICAT SLU (de "Applicatie"), waarmee het gehele proces van registratie van een persoon wordt geïmplementeerd, ondersteund en vastgelegd en waarmee identiteitsdocumenten op afstand kunnen worden gevalideerd door middel van video-opname. Deze video-opname en validatie van het identiteitsdocument gebeurt in real time en op geautomatiseerde wijze (ongeveer 10-20 seconden), en wordt uitgevoerd door SIGNICAT SLU via zijn gekwalificeerde menselijke Agenten die als verificatieoperatoren optreden als Registratie Autoriteit en belast zijn met de accreditatie van de identiteit.

3.1.1 Algemene informatie over het video-identificatieproces.

De AANVRAGER krijgt toegang tot de Applicatie en de interface vraagt de AANVRAGER, alvorens de handelingen ter verificatie van de identiteit te starten, dit document te lezen en ermee in te stemmen en uit vrije wil toestemming te verlenen voor de verwerking van biometrische gegevens die nodig zijn om de video-identificatie uit te voeren. Te dien einde verstrekt SIGNICAT SLU de AANVRAGER vooraf het Privacybeleid met de verwerking van persoonsgegevens die tijdens het Proces zal worden uitgevoerd overeenkomstig de bepalingen van de Regelgeving inzake Gegevensbescherming.

Indien de AANVRAGER deze toestemming niet verleent, kan het Proces niet doorgaan en moet de AANVRAGER een van de in het Eerste Deel van dit document genoemde alternatieven voor identificatie toepassen, overeenkomstig het bepaalde in artikel 24, lid 1, van de eIDAS-Verordening.

Hierna wordt het aan de AANVRAGER getoond:

- o Een viewer van het te ondertekenen contract
- o Een oproep tot actie om dit document te accepteren
- o Een downloadoptie waarmee de gebruiker het document kan opslaan.

Zodra de AANVRAGER het document niet bekijkt en geen toestemming geeft, kan het Proces niet worden voortgezet.

Tenslotte en voorafgaand aan de start van het video-identificatieproces, de ABONNEE wordt dan gevraagd om een telefoonnummer voor het verzenden van een OTP. Door middel van deze OTP geeft de ABONNEE, naast het bekrachtigen van deze Voorwaarden, toestemming voor de afgifte van het Certificaat, met inbegrip van de gegevens uit het video-identificatieproces zoals bepaald in Artikel 3.3.5 van dit document, evenals het contractuele document dat aan het begin van het proces is weergegeven en waarop de gegevens voor het aanmaken van de handtekening door SIGNICAT SLU zullen worden toegepast met als doel het genereren van een gekwalificeerde elektronische handtekening.

Na verificatie van deze OTP zal SIGNICAT SLU de gegevens voor het aanmaken van de handtekening toepassen, zoals voorzien en beschreven in Artikel 3.4.

Zodra de AANVRAGER het Proces heeft gelezen, aanvaard en vrijelijk zijn toestemming en conformiteit heeft gegeven, zal de AANVRAGER doorgaan met het uitvoeren van de Video-identificatie die nodig is voor SIGNICAT SLU om door te gaan met de afgifte van het gekwalificeerde natuurlijke persoonscertificaat.

De AANVRAGER wordt tijdens het video-identificatieproces steeds met stem en tekst begeleid en door middel van de Applicatie wordt een geautomatiseerde controle van de omgevingselementen (lichtomstandigheden, netwerk, camerakwaliteit) uitgevoerd om een optimale opname van de video-identificatie en het bewijs daarvan te verkrijgen.

In die zin zijn de stappen van het Proces voorafgaand aan de afgifte van het gekwalificeerde certificaat de volgende:

In de eerste stap van het Proces wordt de AANVRAGER vervolgens opgedragen het te gebruiken identiteitsdocument te tonen, zodat via gespecialiseerde technologie een beeldvergelijking met de originele documenten kan worden uitgevoerd om de authenticiteit van het document te controleren en gegevensextractie (OCR) van de MRZ of andere delen van het document uit te voeren.

Daarom zal de voorkant van het door de AANVRAGER tijdens het Proces gebruikte identiteitsdocument worden vastgelegd. Daartoe zal de AANVRAGER worden verzocht de voorzijde van zijn/haar document te tonen en de afbeelding in het daarvoor bestemde vakje te plaatsen.

Wanneer het vastleggen is voltooid, wordt een bericht van overeenstemming weergegeven en wordt het volgende deel van het Proces voortgezet.

De volgende stap bestaat uit het vastleggen van de achterkant van het document. De AANVRAGER wordt gevraagd de achterkant van zijn/haar document te tonen en de afbeelding in het getoonde vak te plaatsen.

Wanneer het vastleggen is voltooid, wordt een bericht van overeenstemming weergegeven en gaat het volgende deel van het Proces verder.

De biometrische gegevens van de AANVRAGER worden dan vastgelegd om een vergelijking in real

time uit te voeren met de afbeelding van het identiteitsdocument voor een gezichtsherkenningproces op basis van automatische biometrische scores. Daartoe wordt de AANVRAGER gevraagd zijn/haar gezicht te tonen en de afbeelding in het vakje op het scherm te passen.

Wanneer de biometrische gegevens zijn vastgelegd, wordt de AANVRAGER als bewijs van leven gevraagd een gezichtsbeving naar de camera te maken, en als alles correct is, wordt een bericht van overeenstemming weergegeven en gaat het volgende deel van het Proces verder.

Indien het gehele Proces succesvol is, wordt de AANVRAGER geïnformeerd dat het video-identificatieproces is voltooid en dat het tijdens het Proces gegenereerde bewijsmateriaal zal worden gecontroleerd en gevalideerd door middel van het Verificatie-instrument van de Registratie Autoriteit ter beoordeling van het Proces door een gekwalificeerd persoon die vooraf een specifieke opleiding heeft gevolgd.

Op dit punt stelt de Applicatie de video-identificatie en de tijdens de video-identificatie gegenereerde gegevens beschikbaar aan een gekwalificeerde menselijke Agent die belast is met de verificatie van de identiteit van de Procesaanvrager en verzoekt om de asynchrone beoordeling van de opgenomen video, alsmede de rest van het bewijsmateriaal en de tijdens het Proces verkregen elementen. De gemiddelde verificatietijd voor een agent bedraagt ongeveer drie minuten.

3.1.2. Beveiligingselementen van het Video-identificatieproces en validatie door Gekwalificeerde Menselijke Agenten.

Voor de asynchrone toetsing door een Gekwalificeerde Menselijke Agent is er een beveiligingsprotocol dat gebaseerd is op de beste praktijken van de EU en berust op de aan de Gekwalificeerde Menselijke Agent aangeboden tool waarin het tijdens het Proces verkregen bewijsmateriaal wordt getoond, alsmede de markeringen of meldingen van niet-verkregen bewijsmateriaal.

De opname van de video, het verzoek om verificatie van de video-identificatie en het advies van de bevoegde ambtenaar worden in de Applicatie getraceerd, en op elk spoor wordt een tijdstempel aangebracht om de consistentie en integriteit ervan te waarborgen.

Daarom waarborgt het Proces de bewakingsketen van de verificatie, van het door het Proces verzamelde bewijsmateriaal tot de sporen die de identificatie koppelen aan de Gekwalificeerde Menselijke Agent van de Registratie Autoriteit. Dit resulteert in een geverifieerde identiteit met een technische beveiliging die gelijkwaardig is aan die in de fysieke aanwezigheid van de AANVRAGER.

Zodra de identiteit positief is gevalideerd door de Gekwalificeerde Menselijke Agent, zal de identiteit van de AANVRAGER zijn geaccrediteerd en zal de AANVRAGER in staat worden gesteld verder te gaan en de elektronische SIGNICAT SLU-Certificeringsdienst te ontvangen waarmee hij verder kan gaan met het Proces van afgifte van het certificaat van gekwalificeerde natuurlijke persoon en ondertekening van de elektronische documenten.

Indien het resultaat van het Proces negatief is, kan het Proces voor de afgifte van gekwalificeerde certificaten niet worden voortgezet en moet de AANVRAGER zich fysiek naar de lokalen van de SIGNICAT SLU begeven voor een persoonlijke verificatie van zijn identiteit.

3.2 VERPLICHTINGEN VAN DE AANVRAGER MET BETREKKING TOT HET VIDEO-IDENTIFICATIEPROCES.

De AANVRAGER verbindt zich ertoe, gedurende het gehele Proces:

- Gebruik de Dienst in overeenstemming met de bepalingen van dit document, de CPS, alle toepasselijke bijzondere voorwaarden en alle andere door SIGNICAT SLU verstrekte instructies, handleidingen of procedures.
- Dat het in het proces gebruikte identiteitsdocument een authentiek, rechtsgeldig document is en dat bovendien:
 - Het is geen fotokopie of een gedrukte kaart:
 - Het is niet in digitaal formaat (mobiel, tablet of computer).
 - Het zit niet in een hoes.
 - Het is onbeschadigd en compleet, en alle veiligheidskenmerken zijn in het document aanwezig.
- Dat tijdens het Proces en het vastleggen van de video om ervoor te zorgen dat de video niet wordt afgekeurd:
 - De lichtomstandigheden in de video moeten ervoor zorgen dat het gezicht van de geïdentificeerde persoon en het document duidelijk zichtbaar zijn.
 - De video moet een constante stroom hebben, zonder onderbrekingen of vertragingen.
 - Een levende persoon moet zich legitimeren.
 - Indien een andere persoon dan de te identificeren persoon het gehele Proces uitvoert, wordt de identificatie verworpen.
 - Indien iemand anders op de video aanwezig is, maar de persoon duidelijk niet dwingt zich te laten identificeren, kan de identificatie geldig zijn, alsook indien een bepaalde persoon een gehandicapte persoon helpt bij het maken van de identificatie.
 - Alle delen van het document moeten duidelijk zichtbaar zijn: voorkant, achterkant en gezicht van de persoon.
 - De ABONNEE mag niet slapen of tekenen vertonen die erop wijzen dat hij onder invloed van drugs of alcohol is.

3.3 AFGIFTE, LEVERING EN AANVAARDING VAN HET CERTIFICAAT

3.3.1 Certificaataanvraag en sleutelgeneratie door SIGNICAT SLU namens de ABONNEE.

Zodra het Proces van Video-identificatie is voltooid, machtigt de ABONNEE SIGNICAT SLU om namens hem de publieke en private sleutels te genereren en te beheren die SIGNICAT SLU in staat stellen over te gaan tot de afgifte van het gekwalificeerde certificaat voor natuurlijke personen op korte termijn en om namens hem de elektronische documenten te ondertekenen die hem via SIGNICAT SLU of derden van publieke of private aard waarmee SIGNICAT SLU bepaalde contractuele overeenkomsten heeft gesloten, ter beschikking worden gesteld.

3.3.2 Waarheidsgetrouwe informatie

De ABONNEE is er verantwoordelijk voor dat alle informatie die aan SIGNICAT SLU wordt verstrekt, hetzij rechtstreeks, hetzij via het identiteitsdocument dat tijdens het Proces van Video-identificatie en certificaatafgifte wordt gebruikt, juist en volledig is voor het doel van het certificaat, en dat deze te allen tijde wordt bijgewerkt, waarvoor hij/zij garandeert een wettig en geldig identiteitsdocument te gebruiken, zonder dat dit door de ABONNEE door derden is gewijzigd en/of aangepast.

3.3.3 Afgifte van het certificaat

Voor de afgifte van het certificaat zal SIGNICAT SLU gebruik maken van de door de ABONNEE tijdens het Video-identificatieproces verstrekte gegevens van het identiteitsdocument. Deze gegevens worden door SIGNICAT SLU geëxtraheerd en rechtstreeks in het elektronische certificaat opgenomen om de identiteit van de ABONNEE daaraan te koppelen.

3.3.4 Levering van het certificaat

In het uitgifteproces is er geen specifieke levering van het kortetermijncertificaten aan de ABONNEE. SIGNICAT SLU beheert het in zijn hoedanigheid van Gekwalificeerde Verlener van Vertrouwensdiensten, zodat de ABONNEE het kan gebruiken voor de elektronische ondertekening van documenten.

3.3.5 Aanvaarding van de afgifte van het certificaat en bekrachtiging van deze Voorwaarden.

Door zijn telefoonnummer in te voeren en de OTP te valideren overeenkomstig Artikel 3.1.1 geeft de ABONNEE toestemming voor de afgifte van het certificaat, met inbegrip van de gegevens die uit het Video-identificatieproces zijn gehaald, en bekrachtigt hij deze Voorwaarden.

3.4 SERVERGEBASEERDE HANDTEKENINGENDIENST

Zodra het identificatieproces is voltooid en de identiteit is gevalideerd door de verificatie agent, zal de identiteit van de ondertekenaar worden gegarandeerd en zal SIGNICAT SLU, als Gekwalificeerde Verlener van Vertrouwensdiensten, een aanvraag indienen voor het document dat aan het begin van het proces is geaccepteerd door de Abonnee (in overeenstemming met Artikel 3.1.1) de gegevens voor het aanmaken van de handtekening van de Gebruiker/Abonnee op het document dat wordt weergegeven en geaccepteerd door de introductie van het OTP, waardoor de exclusieve controle ervan wordt gegarandeerd.

SIGNICAT SLU verleent de ABONNEE, op niet-exclusieve en niet-overdraagbare basis, een licentie om kopieën van de software van het beveiligde cryptografische apparaat van SIGNICAT SLU te gebruiken voor de werking van het handtekeningapparaat, indien van toepassing, alsmede voor de productie van de elektronische handtekening, het certificaat en andere cryptografische diensten door de ondertekenaars.

De ABONNEE mag kopieën van de software maken voor uitsluitend archief- of back-updoeleinden.

Indien iemand anders dan SIGNICAT SLU wijzigingen aanbrengt in de geleverde software, vervallen alle garanties met betrekking tot de software onmiddellijk.

4. ALGEMENE VOORWAARDEN VAN DE VERTROUWENSDIENST

4.1 ALGEMENE VOORWAARDEN VAN DE VIDEO-IDENTIFICATIEDIENST

- Bewaartermijn van de documentatie

Alle informatie in verband met het video-identificatieproces voor de afgifte van gekwalificeerde elektronische certificaten van natuurlijke personen, met inbegrip van biometrische informatie, wordt door SIGNICAT SLU bewaard voor de duur van de contractuele relatie, zolang niet om verwijdering ervan wordt verzocht, en gedurende de verjaringstermijn van eventuele rechtsvorderingen die kunnen ontstaan of vorderingen die van officiële instanties kunnen worden ontvangen.

In dit verband bedraagt de maximale bewaartermijn van de relevante informatie in verband met het video-identificatieproces en de afgifte van gekwalificeerde certificaten, d.w.z. een kopie van de video-opname, foto's of schermafbeeldingen van de AANVRAGER en het gebruikte identiteitsdocument, het automatische resultaat van de door de SIGNICAT SLU-toepassing uitgevoerde verificatie, alsmede de beoordeling en opmerkingen van de Gekwalificeerde Menselijke Identiteit Verificatie Agenten, samen met hun besluit om de identificatie goed of af te keuren, 15 jaar vanaf het tijdstip waarop het certificaat is afgegeven, tenzij bij wet anders is bepaald. Zodra de relatie is beëindigd, worden de gegevens van de AANVRAGER naar behoren afgeschermd, overeenkomstig de bepalingen van de toepasselijke regelgeving.

Bovendien wordt gemeld dat alle bewijzen van onvolledige identificatieprocessen die niet zijn voltooid wegens verdenking van poging tot fraude, gedurende vijf jaar vanaf de uitvoering van het Proces zullen worden bewaard, met vermelding van de reden voor niet-voltooiing, overeenkomstig het daartoe vastgestelde beleid.

- Beperking van aansprakelijkheid in verband met het video-identificatieproces.

Kwaliteit van het proces: SIGNICAT SLU garandeert de goede uitvoering van de hierin beschreven Video-identificatiediensten, mits de aan de AANVRAGER ter beschikking gestelde middelen correct en overeenkomstig de instructies van SIGNICAT SLU worden gebruikt.

De toegang tot en het gebruik van de Video-identificatiediensten houdt voor SIGNICAT SLU geen verplichting in om te controleren op de afwezigheid van virussen, wormen of andere schadelijke computerelementen. Het is aan de AANVRAGER, als gebruiker, om in ieder geval te beschikken over adequate hulpmiddelen voor het opsporen en desinfecteren van schadelijke computerprogramma's. SIGNICAT SLU is niet verantwoordelijk voor eventuele schade die tijdens het Video Identificatie Proces aan de computerapparatuur van de AANVRAGER of van derden wordt toegebracht.

Beschikbaarheid van het proces: De werking van het Video-ID-proces kan afhangen van de juiste configuratie van de apparatuur van waaruit de gebruiker toegang krijgt tot het video-identificatieproces en dit initieert, zodat de gebruiker de aangeboden aanwijzingen moet volgen en in alle gevallen te allen tijde moet beschikken over de gespecificeerde hardware- en softwarevereisten.

Evenzo moet voor het video-identificatieproces een Internettoegangslijn beschikbaar zijn. De werking van het video-identificatieproces kan afhangen van de adequate kwaliteit en snelheid van

de verbinding via welke de AANVRAGER toegang krijgt tot de toepassing, en derhalve is de AANVRAGER als enige verantwoordelijk voor de terbeschikkingstelling van telecommunicatielijnen, Internetabbonementen of -verbindingen of andere technische middelen die nodig zijn voor de toegang tot en het gebruik van zijn gegevens.

SIGNICAT SLU is niet aansprakelijk voor schade die voortvloeit uit of verband houdt met de niet-uitvoering of gebrekkige uitvoering van de verplichtingen waarvoor de AANVRAGER verantwoordelijk is, noch voor het onjuiste gebruik van de Procesresultaten en -sleutels, noch voor enige indirecte schade die kan voortvloeien uit het gebruik van het Proces of de door SIGNICAT SLU verstrekte informatie.

SIGNICAT SLU is niet aansprakelijk voor eventuele onjuistheden in de identificatie van de AANVRAGER die voortvloeien uit de door de AANVRAGER tijdens het Proces verstrekte informatie.

SIGNICAT SLU is niet aansprakelijk voor de juiste werking met applicaties die niet zijn goedgekeurd, en voor schade veroorzaakt door de onmogelijkheid van gebruik met dergelijke applicaties door de AANVRAGER.

4.2 ALGEMENE VOORWAARDEN VOOR ELEKTRONISCHE CERTIFICERINGSDIENSTEN.

- Wettelijk kader voor dienstverlening

De certificeringsdiensten worden technisch en operationeel geregeld door de SIGNICAT SLU Certificatiepraktijkverklaring en het Certificeringsbeleid, en de latere bijwerkingen daarvan, alsmede door de aanvullende documentatie die aan de ABONNEE wordt verstrekt.

Deze algemene Voorwaarden, de Certificatiepraktijkverklaring en de Certificeringsbeleid, indien van toepassing op het afgegeven certificaat, vormen het juridisch kader dat de relatie tussen SIGNICAT SLU en de ABONNEE regelt, zowel intern als tegenover derden, onverminderd de bepalingen van de geldende wetgeving.

Dit document bevat de meest relevante elementen en vereisten van de rechten en verplichtingen van de partijen.

De Certificatiepraktijkverklaring (CPS) en de toepasselijke specifieke Certificeringsbeleid (CP) zijn door middel van verwijzing in dit document opgenomen. De laatste bijgewerkte versie van de CPS zal te allen tijde gratis toegankelijk zijn in de volgende talen via de onderstaande link:

Spaans: <https://www.signicat.com/es/acerca-de/certificados-cualificados-para-firma-electronica>

Engels: <https://www.signicat.com/about/qualified-certificates-for-electronic-signatures>

In geval van tegenstrijdigheid prevaleert de betekenis van de in deze document opgenomen termen boven die welke in het CPS zijn opgenomen.

- Duur van het contract

Deze Overeenkomst is van kracht op de uitgifte- en vervaldata zoals vermeld in het door de ABONNEE bij SIGNICAT SLU aangevraagde en gecontracteerde Gekwalificeerd Individueel Certificaat.

- Verplichtingen tot correct gebruik

De ABONNEE dient de door SIGNICAT SLU aangeboden certificatedienst uitsluitend te gebruiken voor de in de CPS toegestane toepassingen, die de ABONNEE kent en aanvaardt door ze te lezen en te aanvaarden door middel van de keuzevakjes die in het proces zijn opgenomen.

De ABONNEE verbindt zich ertoe de digitale certificatedienst en elk ander door SIGNICAT SLU geleverd technisch element en de certificaten te gebruiken in overeenstemming met deze Voorwaarden, de DPC en de PC's die van toepassing kunnen zijn, de bijzondere Voorwaarden die van toepassing kunnen zijn en alle andere instructies, handleidingen of procedures die door SIGNICAT SLU aan de ABONNEE worden verstrekt en in overeenstemming met de bepalingen van de toepasselijke wetgeving.

Het contract van de Certificatedienst met SIGNICAT SLU staat alleen het gebruik van het certificaat toe in het kader van de activiteit van de ABONNEE, overeenkomstig het doel van het gevraagde type certificaat, namelijk het gekwalificeerd certificaat van elektronische handtekening van een natuurlijke persoon van korte duur. Zodra het certificaat is afgegeven, mag de ABONNEE het certificaat niet voor commerciële doeleinden gebruiken, tenzij uitdrukkelijk overeengekomen tussen de partijen. Onder commercieel gebruik van het certificaat wordt verstaan elke handeling waarbij de ABONNEE buiten deze overeenkomst om, al dan niet tegen betaling, aan derden diensten aanbiedt waarvoor het afgegeven certificaat moet worden gebruikt.

- **Verboden transacties**

De door SIGNICAT SLU geleverde digitale certificatediensten zijn niet ontworpen of bedoeld voor gebruik of wederverkoop als controleapparatuur voor gevaarlijke situaties, of voor toepassingen die faalveilige prestaties vereisen, zoals de werking van nucleaire faciliteiten, navigatie- of communicatiesystemen in de lucht, luchtverkeerscontrolesystemen of wapencontrolesystemen, waarbij een fout rechtstreeks de dood, lichamelijk letsel of ernstige milieuschade kan veroorzaken.

- **SIGNICAT SLU-verplichtingen en verantwoordelijkheden**

a) Met betrekking tot de dienstverlening van de registratieautoriteit.

SIGNICAT SLU verbindt zich ertoe de certificaatgegevens en de latere afgifte ervan aan het ABONNEE te registreren en daartoe de controles uit te voeren die zij nodig acht met betrekking tot de identiteit en andere persoonlijke en aanvullende gegevens van de ABONNEES en, in voorkomend geval, van de ondertekenaars.

Deze controles omvatten de door de ABONNEE verstrekte bewijsstukken en, indien SIGNICAT SLU dit nodig acht, alle andere door de ABONNEE verstrekte relevante documenten en informatie.

Indien SIGNICAT SLU fouten ontdekt in de gegevens die in de certificaten moeten worden opgenomen of die deze gegevens rechtvaardigen, kan zij vóór de afgifte van het certificaat de wijzigingen aanbrengen die zij nodig acht of het afgifteproces opschorten en het desbetreffende incident met de ABONNEE afhandelen.

Indien SIGNICAT SLU de gegevens corrigeert zonder eerst het desbetreffende incident met de ABONNEE af te handelen, stelt zij de ABONNEE in kennis van de uiteindelijk gecertificeerde gegevens.

SIGNICAT SLU behoudt zich het recht voor het certificaat niet af te geven wanneer de verstrekte bewijsstukken onvoldoende zijn voor de correcte identificatie en authenticatie van de ABONNEE, of wanneer het aan de afgifte van het certificaat voorafgaande Video-identificatieproces niet door SIGNICAT SLU als geldig is bevestigd.

De bovenstaande verplichtingen worden opgeschort in gevallen waarin de ABONNEE optreedt als registratieautoriteit en beschikt over de technische elementen voor het genereren van sleutels en de afgifte van certificaten.

b) Met betrekking tot het verlenen van de digitale certificatedienst.

SIGNICAT SLU verbindt zich ertoe te voldoen aan de verplichtingen van Wet 6/2020, van 11 november, die bepaalde aspecten van elektronische vertrouwensdiensten regelt, en met name om:

- a) Certificaten afgeven, beheren, opschorten en intrekken, overeenkomstig de door de ABONNEE verstrekte instructies, in de gevallen en om de redenen als omschreven in de SIGNICAT SLU CPS.
- b) De diensten uitvoeren met de passende technische en materiële middelen en met personeel dat voldoet aan de kwalificatie- en ervaringsvoorwaarden die in het CPS.
- c) Voldoen aan de kwaliteitsniveaus van de dienstverlening, overeenkomstig de bepalingen van de CPS, wat de technische, operationele en veiligheidsaspecten betreft.
- d) De status van de certificaten meedelen aan derden die daarom verzoeken, overeenkomstig de bepalingen van de CPS voor de verschillende certificaatverificatiediensten.
- e) Kwaliteit van het Proces: SIGNICAT SLU garandeert de goede uitvoering van de in dit document beschreven Certificatiediensten op voorwaarde dat de aan de ABONNEE ter beschikking gestelde middelen correct en overeenkomstig de instructies van SIGNICAT SLU worden gebruikt.

De toegang tot en het gebruik van de Certificatiediensten houdt voor SIGNICAT SLU geen enkele verplichting in om te controleren op de afwezigheid van virussen, wormen of andere schadelijke computerelementen. Het is in elk geval de verantwoordelijkheid van de ABONNEE, als gebruiker, om te zorgen voor de beschikbaarheid van geschikte instrumenten voor het opsporen en desinfecteren van schadelijke computerprogramma's. SIGNICAT SLU is niet aansprakelijk voor schade die tijdens het Video Identificatie Proces aan de computerapparatuur van de ABONNEE of derden wordt toegebracht.

- f) Beschikbaarheid van het Proces: de werking van het Certificatie Proces kan afhangen van de juiste configuratie van de apparatuur van waaruit de gebruiker toegang krijgt tot het Video- identificatieproces en dit initieert, zodat de gebruiker de aangeboden aanwijzingen moet volgen en in ieder geval steeds moet beschikken over de gespecificeerde

hardware- en softwarevereisten.

Evenzo moet voor het Video-identificatieproces een Internetverbinding beschikbaar zijn. De werking van het Video-identificatieproces kan afhangen van de adequate kwaliteit en snelheid van de verbinding via welke de ABONNEE toegang krijgt tot de applicatie, zodat hij als enige verantwoordelijk is voor de terbeschikkingstelling van telecommunicatielijnen, Internetabbonnementen of -verbindingen of andere technische middelen die nodig zijn voor de toegang tot en het gebruik van zijn gegevens.

- **Als een Certificatiedienstverlener.**

SIGNICAT SLU moet:

a) Waarheidsgetrouwe informatie publiceren overeenkomstig Wet 6/2020 van 11 november tot regeling van bepaalde aspecten van elektronische vertrouwensdiensten en Verordening (EU) 910/2014.

b) Niet zelf of via een derde de gegevens voor het aanmaken van handtekeningen opslaan of kopiëren, behalve in het geval van beheer ervan namens de houder met het oog op de toepassing van de particuliere sleutels voor het aanmaken van handtekeningen, zoals aangegeven door de ABONNEE via het OTP-systeem dat SIGNICAT SLU aan de ABONNEE ter beschikking stelt voor het ondertekenen van elektronische documenten. In dat geval gebruiken zij betrouwbare systemen en producten, met inbegrip van veilige elektronische communicatiekanalen, en worden passende technische en organisatorische procedures en mechanismen toegepast om ervoor te zorgen dat de omgeving betrouwbaar is en onder de exclusieve controle van de certificaathouder wordt gebruikt. Voorts beveiligen en beschermen zij de gegevens voor het aanmaken van handtekeningen tegen wijziging, vernietiging of ongeoorloofde toegang en waarborgen zij de permanente beschikbaarheid ervan.

c) Een publiek toegankelijke zoekdienst hebben over de geldigheids- of intrekingsstatus van afgegeven certificaten.

d) Voldoen aan de volgende aanvullende verplichtingen:

1. De termijn gedurende welke zij de informatie betreffende de verleende diensten overeenkomstig Artikel 24, lid 2, onder h), van Verordening (EU) 910/2014 moeten bewaren, bedraagt 15 jaar na het verstrijken van het certificaat of de beëindiging van de verleende dienst. In geval van afgifte van gekwalificeerde certificaten voor elektronische verzegeling of authenticatie van Websites aan rechtspersonen, leggen verleners van vertrouwensdiensten ook de informatie vast aan de hand waarvan de identiteit van de natuurlijke persoon aan wie voornoemde certificaten zijn afgegeven, kan worden vastgesteld, ter identificatie in gerechtelijke of administratieve procedures.

2. Een verzekering tegen wettelijke aansprakelijkheid afsluiten voor een minimumbedrag van 1.500.000 euro, behalve als de dienstverrichter tot de overheidssector behoort. Indien hij meer dan één van de in Verordening (EU) 910/2014 bedoelde gekwalificeerde diensten verricht, komt daar voor elk soort dienst nog eens 500.000 euro bij. Voornoemde garantie kan geheel of gedeeltelijk worden vervangen door een garantie in de vorm van een bankgarantie of een borgtochtverzekering, zodat de som van de verzekerde bedragen in overeenstemming is met het bepaalde in het vorige lid. De in de twee voorgaande leden vastgestelde bedragen en middelen van verzekering en waarborg kunnen bij koninklijk besluit worden gewijzigd.

3. In geval van beëindiging van zijn activiteit als Gekwalificeerde Verlener van Vertrouwensdiensten stelt hij de cliënten voor wie hij zijn diensten verricht en de toezichthoudende instantie daarvan ten minste twee maanden vóór de daadwerkelijke beëindiging van de activiteit in kennis op een wijze die een doeltreffende afgifte en ontvangst mogelijk maakt. Het plan voor de beëindiging van de dienstverrichter kan inhouden dat de cliënten, zodra is vastgesteld dat de cliënten zich niet verzetten, worden overgedragen aan een andere gekwalificeerde dienstverrichter, die de informatie over de tot dan toe verrichte diensten mag behouden. Hij stelt het controleorgaan tevens in kennis van alle andere relevante omstandigheden die de voortzetting van zijn activiteit kunnen verhinderen. Met name stelt zij, zodra zij daarvan kennis heeft, de toezichthoudende instantie in kennis van de opening van een insolventieprocedure tegen haar.

4. Het conformiteitsbeoordelingsverslag toezenden aan het Ministerie van Economische Zaken en Digitale Transformatie onder de voorwaarden van Artikel 20, lid 1, van Verordening (EU) nr. 910/2014. Niet-nakoming van deze verplichting heeft tot gevolg dat de kwalificatie van de dienstverlener en de door hem verleende dienst worden ingetrokken en dat hij van de in Artikel 22 van voornoemde Verordening bedoelde vertrouwenslijst wordt geschrapt, nadat de dienstverlener is verzocht de voornoemde niet-nakoming te beëindigen.

e) SIGNICAT SLU aanvaardt alle aansprakelijkheid jegens derden voor de handelingen van personen of andere aanbieders aan wie zij de uitvoering van een of meer van de functies die nodig zijn voor het verlenen van elektronische vertrouwensdiensten, met inbegrip van handelingen ter verificatie van de identiteit voorafgaand aan de afgifte van een gekwalificeerd certificaat, delegeert.

- **GARANTIES VOOR CERTIFICERINGSDIENSTEN**

SIGNICAT SLU-garantie door de digitale certificeringsdiensten.

SIGNICAT SLU garandeert dat de particuliere sleutel van de Certificatie Autoriteit die voor de afgifte van certificaten wordt gebruikt, niet gecompromitteerd is, tenzij zij anders heeft meegedeeld via het certificeringsregister, overeenkomstig de CPS.

SIGNICAT SLU garandeert de ABONNEE bij de afgifte van het certificaat alleen dat:

- a) In voorkomend geval worden de certificaten gekwalificeerd onder de voorwaarden van Wet 6/2020 van 11 november, die bepaalde aspecten van elektronische vertrouwensdiensten regelt.
- b) SIGNICAT SLU heeft geen valse of misleidende verklaringen opgesteld of ingevoerd in de certificaatinformatie, noch heeft zij nagelaten de door de ABONNEE verstrekte en geverifieerde noodzakelijke informatie op te nemen.
- c) Alle certificaten voldoen aan de formele en inhoudelijke eisen van de CPS en het PC van de SIGNICAT SLU.
- d) SIGNICAT SLU heeft de in de CPS beschreven procedures nageleefd.

SIGNICAT SLU neemt redelijke maatregelen om ervoor te zorgen dat elk product dat bij de levering van zijn diensten wordt geleverd, vrij is van computervirussen, worms en andere illegale code, en verbindt zich ertoe ABONNEE in kennis te stellen van eventuele virussen, worms of andere illegale code die achteraf in een product worden ontdekt.

- **UITSLUITINGEN VAN DE GARANTIE**

SIGNICAT SLU staat niet in voor de software die door de certificaat ABONNEE of ondertekenaar, of enige andere persoon, wordt gebruikt om een digitale handtekening of een door SIGNICAT SLU afgegeven digitaal certificaat te genereren, te verifiëren of anderszins te gebruiken, tenzij SIGNICAT SLU schriftelijk het tegendeel verklaart.

- **BEPERKINGEN VAN AANSPRAKELIJKHEID ALS VERTROUWDE ELEKTRONISCHE DIENSTVERLENERS.**

SIGNICAT SLU is, mits binnen de grenzen van het toepasselijke recht, niet aansprakelijk voor schade veroorzaakt aan de persoon aan wie zij haar diensten heeft verleend of aan derden te goeder trouw, indien deze laatste in een van de gevallen waarin Verordening (EU) 910/2014 voorziet of in het volgende:

- a) Het niet verstrekken aan de verlener van de vertrouwensdienst van waarheidsgetrouwe, volledige en nauwkeurige informatie voor het verlenen van de vertrouwensdienst, met name over de gegevens die in het elektronische certificaat moeten worden opgenomen of die nodig zijn voor de afgifte ervan of voor de beëindiging of opschorting van de geldigheid ervan, wanneer de onnauwkeurigheid ervan niet met de nodige zorgvuldigheid door de dienstverlener kon worden ontdekt.

- b) Verzuim om SIGNICAT SLU onverwijld in kennis te stellen van elke wijziging in de omstandigheden die van invloed zijn op de verlening van de vertrouwensdienst, met name die welke in het elektronische certificaat zijn vermeld.
- c) Nalatigheid bij het bewaren van uw handtekening, zegel of authenticatiegegevens van de Website, bij het waarborgen van de vertrouwelijkheid ervan en bij het beschermen van de toegang tot of de bekendmaking van deze gegevens of, in voorkomend geval, van de middelen die toegang verlenen tot deze gegevens.
- d) Geen opschorting of intrekking van het elektronische certificaat te vragen in geval van twijfel over de handhaving van de vertrouwelijkheid van de gegevens voor het aanmaken van de handtekening, het zegel of de authenticatie van de Website of, in voorkomend geval, van de middelen die daartoe toegang geven.
- e) Gebruik de gegevens voor het aanmaken van handtekeningen, zegels of Websiteverificatie wanneer de geldigheidsduur van het elektronische certificaat is verstreken of de aanbieder van de vertrouwensdienst u op de hoogte stelt van het verstrijken of opschorten van de geldigheid ervan.

SIGNICAT SLU is evenmin aansprakelijk voor schade indien de ontvanger onzorgvuldig handelt.

De ontvanger wordt geacht nalatig te zijn wanneer hij geen rekening houdt met de opschorting of het verlies van de geldigheid van het elektronische certificaat, of wanneer hij de elektronische handtekening of het elektronische zegel niet verifieert.

SIGNICAT SLU is niet aansprakelijk voor schade in geval van onjuistheid van de gegevens in het elektronisch certificaat indien deze zijn geaccrediteerd door een openbaar of officieel document, geregistreerd in een openbaar register indien dit vereist is.

- **AANSPRAKELIJKHEID VAN DE ABONNEE**

De ABONNEE is jegens eenieder aansprakelijk voor elke inbreuk op zijn verplichtingen, en met name voor de activiteit van identificatie of, in voorkomend geval, registratieautoriteit, uit hoofde van deze Voorwaarden.

De ABONNEE is verantwoordelijk voor alle elektronische communicatie die is geauthenticeerd door middel van een digitale handtekening die met zijn/haar particuliere sleutel is gegenereerd, wanneer het certificaat geldig is geverifieerd door middel van de door SIGNICAT SLU vastgestelde mechanismen en voorwaarden.

Zolang de in Artikel 5 van dit document vastgelegde kennisgeving niet is overgelegd, komt de verantwoordelijkheid die kan voortvloeien uit het ongeoorloofde en/of oneigenlijke gebruik van de certificaten in elk geval toe aan de ABONNEE.

- **GESCHIKTHEID VAN PRODUCTEN DIE GEBRUIK MAKEN VAN IDENTIFICATIE, ELEKTRONISCHE HANDTEKENING OF ENCRYPTIE**

SIGNICAT SLU is niet verantwoordelijk voor de geschiktheid van op de markt beschikbare producten en diensten met betrekking tot digitale certificering, identificatie, elektronische handtekening of encryptie die worden gebruikt in computerapplicaties van Abonnee, behalve wanneer deze door SIGNICAT SLU worden geleverd. In dat geval zijn de partijen onderworpen aan de desbetreffende gebruiksvoorwaarden.

- **EIGENDOM VAN CERTIFICATEN EN ONDERTEKENINGSAPPARAAT**

De geleverde certificaten en ondertekeningsapparaat blijven eigendom van de ABONNEE.

- **RESOLUTIE**

De resolutie vindt plaats in de volgende gevallen:

- a) Bij schending door de andere partij van een van haar verplichtingen, indien deze schending niet is opgeheven:
- b) Binnen dertig dagen na ontvangst van de kennisgeving door de partij die niet in gebreke is gebleven.
- c) Onmiddellijk, indien niet-naleving de veiligheid van de diensten in gevaar brengt.
- d) Wegens het samenvallen van elke andere reden voor vervroegde beëindiging die in de geldende wetgeving en met name in de geldende wetgeving inzake elektronische handtekening en digitale certificering is vastgesteld.

- **VERTROUWELIJKHEIDSBELEID**

SIGNICAT SLU kan geen vertrouwelijke informatie over certificaten vrijgeven en kan niet worden gedwongen deze vrij te geven zonder een specifiek voorafgaand verzoek van:

- a) De persoon ten aanzien van wie het SIGNICAT SLU een geheimhoudingsplicht heeft, of
- b) Een gerechtelijk bevel, een administratief bevel of elk ander bevel waarin de geldende wetgeving voorziet.

De ABONNEE aanvaardt evenwel dat bepaalde gegevens, zowel persoonlijke als andere, die bij de aanvraag van certificaten worden verstrekt, worden opgenomen in hun certificaten en in het mechanisme voor de controle van de status van de certificaten, en dat deze gegevens niet vertrouwelijk zullen worden behandeld, zoals de wet voorschrijft.

- **TERUGBETALINGSBELEID**

SIGNICAT SLU vergoedt in geen geval de kosten van de certificeringsdienst.

- **BEWAARTERMIJN VAN DE INFORMATIE**

Alle informatie in verband met het Proces van afgifte van gekwalificeerde elektronische certificaten voor natuurlijke personen, met inbegrip van het door de ABONNEE naar behoren geformaliseerde contract, de tijdens het afgifteproces gegenereerde logboeken, worden door SIGNICAT SLU bewaard voor de duur van de contractuele relatie, zolang niet om verwijdering daarvan wordt verzocht, en gedurende de verjaringstermijn van eventuele rechtsvorderingen of vorderingen die van officiële instanties kunnen worden ontvangen.

In dit verband is de maximale bewaartermijn van de relevante informatie in verband met het video-identificatieproces van afgifte van gekwalificeerde certificaten 15 jaar vanaf het tijdstip van afgifte van het certificaat, tenzij bij wet anders is bepaald. Na beëindiging van de relatie worden de gegevens van de ABONNEE naar behoren afgeschermd, overeenkomstig de bepalingen van de toepasselijke regelgeving.

5. GEMEENSCHAPPELIJKE BEPALINGEN

5.1 PLAATS VAN UITVOERING VAN DE ACTIVITEIT

De plaats van uitvoering van de verplichtingen van SIGNICAT SLU met betrekking tot digitale certificatediensten en, in voorkomend geval, licenties voor het gebruik van software, is de vestigingsplaats van SIGNICAT SLU.

5.2 SCHEIDBAARHEID VAN DE VOORWAARDEN.

De clausules van dit document staan los van elkaar en daarom blijven, indien een clausule ongeldig of onuitvoerbaar wordt geacht, de overige clausules van kracht en uitvoerbaar, tenzij de partijen uitdrukkelijk anders zijn overeengekomen.

5.3 TOEPASSELIJK RECHT EN BEVOEGDE JURISDICTIE.

De betrekkingen met SIGNICAT SLU worden beheerst door de bepalingen van Verordening (EU) 910/2014 eIDAS, door de Spaanse wetgeving, en in het bijzonder door alle bepalingen die voortvloeien uit haar nalevingsbeleid.

De bevoegde rechtsmacht is die van Wet 1/2000, van 7 januari, betreffende de Burgerlijke Rechtsvordering, behalve wanneer de ABONNEE als consument wordt beschouwd, in welk geval SIGNICAT SLU zich onderwerpt aan de rechtsmacht die hem wettelijk toekomt.