



**ALGEMENE VOORWAARDEN VAN HET VIDEO-
IDENTIFICATIEPROCES EN DE UITGIFTE VAN CERTIFICATEN VAN
KORTE DUUR**

QES ONCE

Dit is een Nederlandse vertaling van de Engelse versie van de algemene voorwaarden van het video-identificatieproces en de uitgifte van certificaten van korte duur QES ONCE, die hier te vinden is: <https://www.signicat.com/about/english>. Deze algemene voorwaarden QES ONCE zijn uitsluitend voor het gemak van ABONNEES of AANVRAGERS vertaald en hebben geen juridische waarde. De Engelse versie is te allen tijde bindend en prevaleert boven de Nederlandse vertaling.

Eerzijds **SIGNICAT, S.L.U.** (voorheen bekend als „Electronic Identification S.L.”), met statutair adres te Avenida Ciudad de Barcelona 81, 4ª Planta, ingeschreven in het openbaar handelsregister op 13 maart 2013, met identificatienummer B-86681533 (hierna „SIGNICAT SLU” genoemd), is een gekwalificeerde verlener van vertrouwensdiensten die handelt overeenkomstig de bepalingen van Verordening (EU) nr. 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, alsmede de technische normen van ETSI die van toepassing zijn op de uitgifte en het beheer van gekwalificeerde certificaten, voornamelijk EN 319 411-1 en EN 319 411-2, om de naleving van wettelijke vereisten en de internationale erkenning van haar diensten te vergemakkelijken.

Anderzijds de **ABONNEE of AANVRAGER**, wiens identificatiegegevens voor de toepassing van deze Overeenkomst zijn opgenomen in het gebruikte identiteitsdocument en in de video die is gegenereerd als resultaat van het proces van video-identificatie en uitgifte van het certificaat.

1. VOORWERP

Dit document heeft tot doel de Aanvrager/Abonnee op duidelijke en begrijpelijke wijze te informeren over de huidige „Algemene voorwaarden van het video-identificatieproces en de uitgifte van certificaten van korte duur”, en de diensten te regelen overeenkomstig de bepalingen van dit document, de Certification Practice Statement (CPS), de eIDAS-verordening en de eventueel toepasselijke lokale regelgeving.

Dit voorafgaande identificatieproces is noodzakelijk om de identiteit aan te tonen van de Aanvrager/Abonnee, die SIGNICAT SLU verzoekt om een gekwalificeerd certificaat voor elektronische handtekeningen van een natuurlijke persoon van korte duur uit te geven („Certificeringsdiensten”), een certificaat dat onderworpen is aan de hieronder beschreven voorwaarden van de elektronische certificeringsdienst die SIGNICAT SLU als gekwalificeerde verlener van vertrouwensdiensten verleent.

Het gekwalificeerde elektronische certificaat dat op grond van deze Algemene voorwaarden wordt uitgegeven, beantwoordt aan het volgende certificeringsprofiel:

- Gekwalificeerd certificaat voor natuurlijke personen in de CLOUD met QSCD, met OID 1.3.6.1.4.1.55193.1.1.2. Dit is een gekwalificeerd certificaat dat wordt uitgegeven voor gekwalificeerde elektronische handtekeningen en de authenticatie daarvan, overeenkomstig het certificeringsbeleid QCP-n-qscd, met OID 0.4.0.194112.1.2. Dit certificaat wordt uitgegeven in een gecentraliseerd QSCD en is een gekwalificeerd certificaat overeenkomstig de bepalingen van artikel 28 van Verordening (EU) nr. 910/2014.

Het werkt met gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen (QSCD) overeenkomstig de artikelen 29 en 51 van Verordening (EU) nr. 910/2014 en voldoet aan de bepalingen van de technische normen van het Europees Instituut voor telecommunicatienormen, aangeduid met referentienummer ETSI EN 319 411-2. Het QSCD bestaat met name uit de hardwarebeveiligingsmodule nShield Solo XC v12.60.15 en de Entrust Signature Activation Module (SAM), versie 1.1.1, beide gecertificeerd volgens Common Criteria EAL4+ en gekwalificeerd als gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen.

Het waarborgt de identiteit van de ondertekenaar en zijn band met de abonnee van de elektronische vertrouwensdienst, doordat het de aanmaak mogelijk maakt van de „gekwalficeerde elektronische handtekening”, dat wil zeggen de geavanceerde handtekening die gebaseerd is op een gekwalificeerd certificaat en is aangemaakt met een gekwalificeerd middel, en daarmee voor alle rechtsgevolgen en doeleinden gelijkgesteld is aan een handgeschreven handtekening, zonder dat aan andere aanvullende voorwaarden hoeft te worden voldaan.

De ABONNEE erkent en aanvaardt dat het lezen en aanvaarden van dit document door het aanvinken van de selectievakjes wordt beschouwd als een gewone elektronische handtekening.

2. TOEPASSELIJKE DEFINITIES

- **CERTIFICERINGSAUTORITEIT (CA):** vertrouwde entiteit van de afzender en de ontvanger van het bericht. Dit vertrouwen van beiden in een „vertrouwde derde” stelt elk van hen in staat op zijn beurt te vertrouwen op de documenten die door de Certificeringsautoriteit zijn ondertekend, in het bijzonder de documenten die elke publieke sleutel aan de bijbehorende eigenaar koppelen en die certificaten worden genoemd. Bij het verlenen van de door de Abonnee aangevraagde Dienst treedt SIGNICAT SLU op als Certificeringsautoriteit die door de uitgifte van een Certificaat een bepaalde publieke sleutel aan een bepaalde Abonnee koppelt.
- **REGISTRATIEAUTORITEIT (RA):** entiteit die onder meer de aanvrager van een certificaat en, in voorkomend geval, de overige met het certificaat verbonden omstandigheden op eenduidige wijze identificeert overeenkomstig de bepalingen van afdeling 1.3.2. De Registratieautoriteit verstrekt de Certificeringsautoriteit de geverifieerde gegevens van de aanvrager, zodat de Certificeringsautoriteit het bijbehorende certificaat kan uitgeven. Alle of een deel van de eigen taken van de RA kunnen rechtstreeks door SIGNICAT SLU of door een door SIGNICAT SLU gemachtigde entiteit worden uitgevoerd.
- **CERTIFICAAT VOOR ELEKTRONISCHE HANDTEKENINGEN:** elektronische verklaring die validatiegegevens voor elektronische handtekeningen aan een natuurlijke persoon koppelt en ten minste de naam of het pseudoniem van die persoon bevestigt.
- **GEKWALIFICEERD CERTIFICAAT VOOR ELEKTRONISCHE HANDTEKENINGEN:** certificaat voor elektronische handtekeningen dat is uitgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage I bij Verordening (EU) nr. 910/2014 van 23 juli 2014 (eIDAS-verordening), en dat de hoogste juridische waarborgen biedt wat betreft de identificatie van de ondertekenaar en de eenduidige koppeling ervan aan de handtekening, alsmede de integriteit en onweerlegbaarheid van de aan de handtekening gekoppelde gegevens.
- **CERTIFICATION PRACTICE STATEMENT („CPS”):** document dat is opgesteld door een Certificeringsautoriteit en dat de verlening van certificeringsdiensten door die Certificeringsautoriteit 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, alsmede de

voorwaarden voor de aanvraag, uitgifte, het gebruik, de opschorting en de beëindiging van de geldigheid van de Certificaten.

- **GEKWALIFICEERDE ELEKTRONISCHE HANDTEKENING:** geavanceerde elektronische handtekening die is aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en die gebaseerd is op een gekwalificeerd certificaat voor elektronische handtekeningen. Omdat het een gekwalificeerde handtekening betreft, geldt een weerlegbaar vermoeden (iuris tantum) van geldigheid; de bewijslast rust op degene die de geldigheid van de handtekening betwist.
- **GEKWALIFICEERDE VERLENER VAN VERTROUWENSDIENSTEN:** verlener van vertrouwensdiensten die een of meer gekwalificeerde vertrouwensdiensten verleent en aan wie door het toezichthoudende orgaan de gekwalificeerde status is verleend.
- **ABONNEE OF AANVRAGER:** de in de koptekst geïdentificeerde natuurlijke persoon die de certificeringsdiensten van SIGNICAT SLU afneemt en die vóór de uitgifte van het gekwalificeerde certificaat het video-identificatieproces van SIGNICAT SLU heeft aangevraagd en met succes heeft doorlopen.

3. ALGEMENE VOORWAARDEN VAN HET VIDEO-IDENTIFICATIEPROCES

Het identificatieproces van de Aanvrager voor de identificatiediensten die SIGNICAT SLU verleent met het oog op de uitgifte van elektronische certificaten, wordt overeenkomstig artikel 24, lid 1, van de eIDAS-verordening op een van de volgende manieren uitgevoerd:

- 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 aan de Av. de la Ciudad de Barcelona, 81, 4, 28007 Madrid, aangezien er geen gedelegeerde Registratieautoriteiten zijn;
- b) op afstand, met gebruikmaking van elektronische identificatiemiddelen, waarbij de aanwezigheid van de natuurlijke persoon of van een gemachtigde vertegenwoordiger van de rechtspersoon vóór de uitgifte van het gekwalificeerde certificaat is gewaarborgd, en overeenkomstig het video-identificatieproces dat in dit document en in de Certification Practice Statement wordt beschreven, toegankelijk via de volgende link: <https://www.signicat.com/about/qualified-certificates-for-electronic-signatures>;
- c) door middel van een gekwalificeerd certificaat voor elektronische handtekeningen of een gekwalificeerd elektronisch zegel dat is uitgegeven overeenkomstig punt a) of b);
- d) met behulp van andere op nationaal niveau erkende identificatiemethoden die qua betrouwbaarheid een met fysieke aanwezigheid gelijkwaardige zekerheid bieden. De gelijkwaardige zekerheid wordt bevestigd door een conformiteitsbeoordelingsorgaan.

3.1. VALIDATIE VAN DE IDENTITEIT LANGS ELEKTRONISCHE WEG EN BESCHRIJVING VAN HET VIDEO-IDENTIFICATIEPROCES

Het video-identificatieproces (hierna het „Video-identificatieproces” of het „Proces”) is een methode voor onbegeleide identiteitsverificatie op afstand via video in realtime, die wordt geleverd via de eigen suite van softwarebibliotheken, REST-applicatie-interfaces en webapplicaties van SIGNICAT SLU (de „Applicatie”), die het volledige registratieproces van een persoon uitvoert, ondersteunt en vastlegt en het mogelijk maakt identiteitsdocumenten op afstand te valideren via een video-opname. Deze video legt het identiteitsdocument vast en valideert het in realtime en op geautomatiseerde wijze (ongeveer 10-20 seconden), wat door SIGNICAT SLU wordt uitgevoerd via haar gekwalificeerde menselijke agenten die, als verificatiemedewerkers optredend als Registratieautoriteit, belast zijn met het vaststellen van de identiteit.

3.1.1. Algemene informatie over het Video-identificatieproces

De Aanvrager opent de Applicatie en de interface en wordt, voordat de handelingen ter verificatie van de identiteit worden gestart, verzocht dit document te lezen en ermee in te stemmen en vrijelijk toestemming te geven voor de verwerking van de biometrische gegevens die nodig zijn om de video-identificatie uit te voeren. Daartoe verstrekt SIGNICAT SLU de aanvrager vooraf het Privacybeleid, waarin de verwerking van persoonsgegevens wordt beschreven die tijdens het Proces zal plaatsvinden overeenkomstig de bepalingen van de regelgeving inzake gegevensbescherming.

Indien de Aanvrager deze toestemming niet geeft, kan het Proces niet worden voortgezet en moet de Aanvrager gebruikmaken van een van de alternatieve identificatiemethoden die zijn vermeld in clausule 1 van dit document, overeenkomstig de bepalingen van artikel 24, lid 1, van de eIDAS-verordening.

Zodra de Aanvrager het privacybeleid heeft gelezen en vrijelijk toestemming heeft gegeven, wordt het proces voortgezet.

De Aanvrager wordt tijdens het Video-identificatieproces te allen tijde door spraak en tekst begeleid en via de Applicatie wordt een geautomatiseerde controle van de omgevingsfactoren (lichtomstandigheden, netwerk, camerakwaliteit) uitgevoerd om een optimale opname van de video-identificatie en het bijbehorende bewijsmateriaal te verkrijgen. In dit verband zijn de stappen van het proces vóór de uitgifte van het gekwalificeerde certificaat als volgt:

In de eerste stap van het Proces wordt de Aanvrager gevraagd het te gebruiken identiteitsdocument te tonen om met behulp van patroonherkenningstechnologie een beeldvergelijking met de originele documenten uit te voeren, de echtheid van het document te verifiëren en de gegevens (OCR) uit de MRZ of andere delen van het document te extraheren, met de mogelijkheid de gegevens in realtime op te vragen.

Daarom wordt de voorzijde van het identiteitsdocument dat de Aanvrager tijdens het Proces gebruikt, vastgelegd. Hiertoe wordt de Aanvrager gevraagd de voorzijde van zijn/haar document te tonen en het beeld in het weergegeven kader te plaatsen.

Wanneer de opname is voltooid, verschijnt een bevestigingsbericht en gaat het Proces verder met de volgende stap.

De volgende stap bestaat uit het vastleggen van de achterzijde van het document. De Aanvrager wordt gevraagd de achterzijde van zijn/haar document te tonen en het beeld in het weergegeven kader te plaatsen.

Wanneer de opname is voltooid, verschijnt een bevestigingsbericht en gaat het proces verder met de volgende stap.

Vervolgens worden de biometrische gegevens van de Aanvrager vastgelegd om in realtime een vergelijking te maken met de afbeelding op het identiteitsdocument, in een gezichtsherkenningproces op basis van automatische biometrische scoring. Hiertoe wordt de Aanvrager gevraagd zijn/haar gezicht te tonen en het beeld in het op het scherm weergegeven kader te plaatsen.

Nadat de biometrische gegevens zijn vastgelegd, wordt de Aanvrager als levensechtheidscontrole gevraagd een gezichtsbeweging voor de camera te maken; als alles correct is, verschijnt een bericht van overeenstemming en gaat het proces verder met de volgende stap.

Als het volledige Proces succesvol is verlopen, wordt de Aanvrager meegedeeld dat het Video-identificatieproces is voltooid en dat het tijdens het Proces gegenereerde bewijsmateriaal zal worden gecontroleerd en gevalideerd met behulp van de verificatietool van de Registratieautoriteit, voor beoordeling van het Proces door een gekwalificeerde persoon die daarvoor vooraf een specifieke opleiding heeft gevolgd.

Op dat moment maakt de Applicatie verbinding met een gekwalificeerde menselijke agent die belast is met de verificatie van de identiteit van de Aanvrager van het Proces, en verzoekt zij om de asynchrone beoordeling van de opgenomen video en van het overige tijdens het Proces verkregen bewijsmateriaal en de overige elementen. De gemiddelde verificatietijd per agent bedraagt ongeveer drie minuten.

Vervolgens wordt de gebruiker om een telefoonnummer gevraagd om hem/haar een OTP te kunnen sturen. Door middel van deze OTP bekrachtigt de gebruiker deze Algemene voorwaarden en geeft hij/zij bovendien toestemming voor de uitgifte van het Certificaat, met daarin de gegevens die uit het video-identificatieproces zijn gehaald zoals bepaald in clausule 3.3.5 van dit document.

3.1.2. Beveiligingselementen van het Video-identificatieproces en validatie door een gekwalificeerde menselijke agent

Voor de asynchrone beoordeling door een gekwalificeerde menselijke agent bestaat een beveiligingsprotocol op basis van goede praktijken van de EU, ondersteund door de tool die de gekwalificeerde menselijke agent ter beschikking wordt gesteld, waarin het tijdens het Proces verkregen bewijsmateriaal wordt getoond, evenals de signaleringen of meldingen van het niet-verkregen bewijsmateriaal.

De opname van de video, het verzoek om verificatie van de video-identificatie en het oordeel van de gekwalificeerde agent worden in de Applicatie vastgelegd, en op elke vastlegging wordt een tijdstempel aangebracht om de samenhang en integriteit ervan te waarborgen.

Het Proces waarborgt daarmee de bewijsketen van de verificatie, van het door het Proces verzamelde bewijsmateriaal tot de vastleggingen die de identificatie koppelen aan de gekwalificeerde menselijke agent van de Registratieautoriteit. Het resultaat is aldus een geverifieerde identiteit met een technische zekerheid die gelijkwaardig is aan die van een verificatie in fysieke aanwezigheid van de Aanvrager.

Zodra de identiteit door de gekwalificeerde menselijke agent positief is gevalideerd, is de identiteit van de Aanvrager vastgesteld en kan de Aanvrager doorgaan met het ontvangen van de certificeringsdienst van SIGNICAT SLU, waarmee hij/zij het proces van uitgifte van het gekwalificeerde certificaat voor natuurlijke personen en de ondertekening van de elektronische documenten kan voortzetten.

Indien het resultaat van het Proces negatief is, kan het Proces voor de uitgifte van gekwalificeerde certificaten niet worden voortgezet en moet de Aanvrager zich fysiek naar de vestiging van SIGNICAT SLU begeven om zijn/haar identiteit persoonlijk te laten verifiëren.

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

De ABONNEE verbindt zich er gedurende het Proces toe:

- De Dienst te gebruiken overeenkomstig de bepalingen van dit document, de CPS, de eventueel toepasselijke bijzondere voorwaarden en alle andere instructies, handleidingen of procedures die door SIGNICAT SLU worden verstrekt.
- Ervoor te zorgen dat het tijdens het Proces gebruikte document een authentiek, rechtsgeldig document is en dat het bovendien:
 - geen fotokopie of afgedrukte kaart is;
 - niet in digitale vorm is (mobiele telefoon, tablet of computer);
 - zich niet in een hoesje bevindt;
 - niet beschadigd en volledig is, waarbij alle beveiligingselementen in het document aanwezig zijn.
- Ervoor te zorgen dat tijdens het Proces en de video-opname, ter voorkoming van afwijzing:
 - de lichtomstandigheden in de video het mogelijk maken het gezicht van de geïdentificeerde persoon en het document duidelijk te zien;
 - de videostream constant is, zonder onderbrekingen of vertragingen;
 - een levende persoon het identiteitsbewijs toont;
 - indien een andere persoon dan de te identificeren persoon het volledige Proces uitvoert, de identificatie als niet authentiek wordt afgewezen;
 - indien iemand anders in de video aanwezig is maar de te identificeren persoon duidelijk niet onder druk zet, de identificatie geldig kan zijn, bijvoorbeeld wanneer iemand een persoon met een handicap helpt bij de identificatie;

- alle onderdelen van de opnamen van het document, voorzijde, achterzijde en gezicht van de persoon, duidelijk zichtbaar zijn;
- de ABONNEE niet slaapt en geen tekenen vertoont die kunnen worden uitgelegd als onder invloed zijn van drugs of alcohol.

3.3. UITGIFTE, LEVERING EN AANVAARDING VAN HET CERTIFICAAT

3.3.1. CERTIFICAATAANVRAAG EN SLEUTELGENERATIE DOOR SIGNICAT SLU NAMENS DE ABONNEE

Na voltooiing van het Video-identificatieproces machtigt de ABONNEE SIGNICAT SLU om namens hem/haar de publieke en private sleutels te genereren en te beheren, zodat SIGNICAT SLU het gekwalificeerde certificaat van korte duur voor natuurlijke personen kan uitgeven en namens hem/haar de elektronische documenten kan ondertekenen die beschikbaar worden gesteld via SIGNICAT SLU of via publiek- of privaatrechtelijke derden met wie SIGNICAT SLU bepaalde contractuele afspraken heeft.

3.3.2. JUISTHEID VAN DE INFORMATIE

De ABONNEE is ervoor verantwoordelijk dat alle informatie die rechtstreeks of via het tijdens het uitgifteproces van het certificaat gebruikte identiteitsdocument aan SIGNICAT SLU wordt verstrekt, juist, volledig voor het doel van het certificaat en te allen tijde actueel is; daartoe garandeert hij/zij een wettig en geldig identiteitsdocument te gebruiken dat niet door de ABONNEE of door derden is vervalst en/of gewijzigd.

3.3.3. UITGIFTE VAN HET CERTIFICAAT

Voor de uitgifte van het certificaat gebruikt SIGNICAT SLU de gegevens van het identiteitsdocument dat de ABONNEE tijdens het video-identificatieproces heeft verstrekt. Deze informatie wordt door SIGNICAT SLU geëxtraheerd en rechtstreeks in het elektronische certificaat opgenomen om de identiteit van de ABONNEE aan het elektronische certificaat te koppelen.

3.3.4. LEVERING VAN HET CERTIFICAAT

Bij het uitgifteproces van het certificaat van korte duur vindt geen specifieke levering van het certificaat aan de ABONNEE plaats. SIGNICAT SLU beheert het in haar hoedanigheid van gekwalificeerde verlener van vertrouwensdiensten, zodat de ABONNEE het kan gebruiken voor de elektronische ondertekening van documenten.

3.3.5. AANVAARDING VAN DE UITGIFTE VAN HET CERTIFICAAT EN BEKRACHTIGING VAN DEZE ALGEMENE VOORWAARDEN.

Door zijn/haar telefoonnummer in te voeren en de OTP te valideren zoals bepaald in clause 3.1.1, geeft de ABONNEE toestemming voor de uitgifte van het certificaat, met daarin de gegevens die uit het video-identificatieproces zijn gehaald, en bekrachtigt hij/zij deze Algemene voorwaarden.

3.4. DIENST VOOR ONDERTEKENING OP DE SERVER

Zodra het identificatieproces is voltooid, de OTP is ingevoerd en de identiteit door de verificatiemedewerker is gevalideerd, is de identiteit van de ondertekenaar gewaarborgd en worden de volgende documenten duidelijk aan de ABONNEE getoond om tot de elektronische ondertekening over te gaan:

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

Om het proces voort te zetten, moet de ABONNEE het document bekijken en aanvaarden; anders moet de ABONNEE worden meegedeeld dat het proces niet kan worden voortgezet.

Voor de aanvaarding van het document wordt de ABONNEE meegedeeld dat er een tweede sms wordt verzonden met een nieuwe OTP (6 cijfers) die nodig is om de ondertekening te voltooien, waarmee de ABONNEE SIGNICAT SLU als gekwalificeerde verlener van vertrouwensdiensten machtigt om de gegevens voor het aanmaken van de handtekening van de Abonnee toe te passen, waarbij de uitsluitende controle daarover wordt gewaarborgd.

De Applicatie verifieert deze informatie en gaat, indien deze juist is, over tot de uitgifte van het certificaat en de ondertekening van het document. Het certificaat is 1 dag geldig en wordt uitsluitend gebruikt om het aanvaarde document te ondertekenen.

SIGNICAT SLU verleent de ABONNEE op niet-exclusieve en niet-overdraagbare basis een licentie voor het gebruik van kopieën van de software voor het beveiligde cryptografische middel van SIGNICAT SLU voor de werking van het ondertekeningsmiddel, indien van toepassing, alsmede voor de productie van de elektronische handtekening, het certificaat en de overige cryptografische diensten door de ondertekenaars.

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

Indien iemand anders dan SIGNICAT SLU wijzigingen aanbrengt in de verstrekte 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 informatie

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

De maximale bewaartermijn van de relevante informatie met betrekking tot het proces van video-identificatie en uitgifte van gekwalificeerde certificaten, d.w.z. een kopie van de video-opname, foto's of schermabeeldingen van de Aanvrager en het gebruikte identiteitsdocument, het automatische resultaat van de door de Applicatie van SIGNICAT SLU uitgevoerde verificatie, alsmede de beoordeling en opmerkingen van de gekwalificeerde menselijke identiteitsverificatieagenten, samen met hun besluit tot goedkeuring of afwijzing van de identificatie, bedraagt 15 jaar na de intrekking of het verstrijken van het certificaat, tenzij wettelijk anders bepaald. Na beëindiging van de contractuele relatie worden de gegevens van de ABONNEE naar behoren geblokkeerd, overeenkomstig de bepalingen van de toepasselijke regelgeving.

Daarnaast wordt meegedeeld dat al het bewijsmateriaal van onvolledige identificatieprocessen die wegens een vermoeden van poging tot fraude niet zijn voltooid, gedurende 5 jaar na de uitvoering van het Proces wordt bewaard, met vermelding van de reden van niet-voltooiing, overeenkomstig het daartoe vastgestelde beleid.

- **Beperking van aansprakelijkheid met betrekking tot het video-identificatieproces**

Kwaliteit van het Proces: SIGNICAT SLU garandeert de goede werking van de in dit document beschreven video-identificatiediensten, mits de aan de ABONNEE ter beschikking gestelde middelen correct en overeenkomstig de instructies van SIGNICAT SLU worden gebruikt.

Toegang tot en gebruik van de video-identificatiediensten houden voor SIGNICAT SLU geen verplichting in om te controleren of er geen virussen, worms of andere schadelijke computerelementen aanwezig zijn. Het is de verantwoordelijkheid van de ABONNEE als gebruiker om te allen tijde over passende middelen te beschikken voor de detectie en verwijdering van schadelijke computerprogramma's. SIGNICAT SLU kan niet aansprakelijk worden gesteld voor schade aan de computerapparatuur van de ABONNEE of van derden tijdens het Video-identificatieproces.

Beschikbaarheid van het Proces: de werking van het Video-identificatieproces kan afhangen van een correcte configuratie van de apparatuur waarmee de gebruiker het video-identificatieproces opent en start; de gebruiker moet daarom de verstrekte instructies volgen en in ieder geval te allen tijde voldoen aan de gespecificeerde software- en hardwarevereisten.

Evenzo moet voor de uitvoering van het video-identificatieproces een internetverbinding beschikbaar zijn. De werking van het video-identificatieproces kan afhangen van de toereikende kwaliteit en snelheid van de verbinding waarmee de ABONNEE de applicatie opent; hij/zij is als enige verantwoordelijk voor het voorzien in telecommunicatielijnen, internetabonnementen of -verbindingen of andere technische middelen die nodig zijn om toegang te krijgen tot zijn/haar gegevens en deze te gebruiken.

SIGNICAT SLU is niet aansprakelijk voor schade die voortvloeit uit of verband houdt met de niet-nakoming of gebrekkige nakoming van de verplichtingen die onder de verantwoordelijkheid van de ABONNEE vallen, noch voor het onjuiste gebruik van de resultaten van het Proces en de sleutels, noch voor indirecte schade die kan voortvloeien uit het gebruik van het Proces of van de door SIGNICAT SLU verstrekte informatie.

SIGNICAT SLU is niet aansprakelijk voor onjuistheden in de identificatie van de ABONNEE die het gevolg zijn van informatie die de ABONNEE tijdens het Proces heeft verstrekt.

SIGNICAT SLU is niet aansprakelijk voor de correcte werking met niet-goedgekeurde applicaties, noch voor schade die ontstaat doordat de ABONNEE deze applicaties niet kan gebruiken.

4.2. ALGEMENE VOORWAARDEN VAN DE VIDEO-IDENTIFICATIEDIENST

Juridisch kader voor de verlening van de dienst

De certificeringsdiensten van SIGNICAT SLU worden technisch en operationeel geregeld door de Certification Practice Statement en het certificeringsbeleid (Certification Policies) van SIGNICAT SLU en de latere bijwerkingen daarvan, alsmede door de aanvullende documentatie die aan de ABONNEE wordt verstrekt en waarvan hij/zij verklaart op het moment van ondertekening van dit Contract kennis te hebben genomen. Deze algemene voorwaarden, de Certification Practice Statement en het certificeringsbeleid, voor zover van toepassing op het uitgegeven certificaat, vormen derhalve het juridische kader dat de relatie tussen SIGNICAT SLU en de ABONNEE regelt, zowel onderling als ten aanzien van derden, onverminderd de bepalingen van de geldende wetgeving.

Dit document bevat derhalve de belangrijkste aspecten en vereisten van de rechten en verplichtingen van de partijen.

De toepasselijke Certification Practice Statement (CPS) en het specifieke certificeringsbeleid (CP) zijn door verwijzing in dit document opgenomen. De meest recente versie van de CPS is te allen tijde kosteloos beschikbaar 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 tegenstrijdigheden prevaleert de betekenis van de termen in dit document boven hetgeen in de CPS is bepaald.

Looptijd van het contract

Deze Overeenkomst is geldig gedurende de periode tussen de datum van uitgifte en de vervaldatum die zijn vermeld in het gekwalificeerde certificaat voor natuurlijke personen dat de Abonnee bij SIGNICAT SLU heeft aangevraagd en afgenomen.

Verplichtingen inzake correct gebruik

De ABONNEE mag de door SIGNICAT SLU verleende certificeringsdienst uitsluitend gebruiken voor de in de CPS toegestane doeleinden, die de ABONNEE kent en aanvaardt doordat hij/zij het document heeft gelezen en de in het proces opgenomen selectievakjes heeft aangevinkt.

De ABONNEE is verplicht de digitale certificeringsdienst en alle andere door SIGNICAT SLU geleverde technische elementen, alsmede de certificaten, te gebruiken overeenkomstig deze algemene voorwaarden, de CPS en de eventueel toepasselijke CP's, de in voorkomend geval in de handleiding vermelde bijzondere voorwaarden en alle andere instructies of procedures die SIGNICAT SLU aan de ABONNEE verstrekt, en met inachtneming van alle geldende wettelijke bepalingen.

Het afnemen van de certificeringsdienst bij SIGNICAT SLU staat het gebruik van het Certificaat uitsluitend toe binnen het kader van de officiële activiteit van de ABONNEE, overeenkomstig het doel van het aangevraagde type certificaat, d.w.z. het gekwalificeerde certificaat voor elektronische handtekeningen van een natuurlijke persoon van korte duur. Nadat het certificaat is uitgegeven, mag de ABONNEE het certificaat, tenzij uitdrukkelijk anders overeengekomen tussen de partijen, niet voor commerciële doeleinden gebruiken. Onder commercieel gebruik van het certificaat wordt verstaan elke handeling waarmee de ABONNEE buiten dit contract, tegen betaling of kosteloos, diensten aan derden aanbiedt waarvoor het gebruik van het uitgegeven certificaat vereist is.

Verboden transacties

De door SIGNICAT SLU verleende digitale certificeringsdiensten zijn niet ontworpen of toegestaan om te worden gebruikt of doorverkocht als apparatuur voor het beheersen van gevaarlijke situaties, of voor toepassingen die foutloos handelen vereisen, zoals de exploitatie van nucleaire installaties, navigatie- of luchtvaartcommunicatiesystemen, luchtverkeersleidingssystemen of wapenbeheersingssystemen, waarbij een fout rechtstreeks de dood tot gevolg kan hebben of lichamelijk letsel of ernstige milieuschade kan veroorzaken.

Verplichtingen en verantwoordelijkheden van SIGNICAT SLU

a. Met betrekking tot de verlening van de dienst als registratieautoriteit

SIGNICAT SLU verbindt zich ertoe de gegevens van het certificaat te registreren en het certificaat vervolgens aan de ABONNEE uit te geven, waarvoor zij de controles moet uitvoeren die zij noodzakelijk acht met betrekking tot de identiteit en de overige persoonlijke en aanvullende gegevens van de ABONNEES en, in voorkomend geval, van de ondertekenaars zelf.

Deze verificaties moeten betrekking hebben op de bewijsstukken die de ABONNEE via de aanvrager heeft verstrekt en, indien SIGNICAT SLU dit noodzakelijk acht, op alle andere relevante documenten en informatie die door de ABONNEE zijn verstrekt.

Indien SIGNICAT SLU fouten ontdekt in de gegevens die in de certificaten moeten worden opgenomen of die deze gegevens onderbouwen, kan zij vóór de uitgifte van het certificaat de wijzigingen aanbrengen die zij noodzakelijk acht, of het uitgifteproces opschorten en het betreffende incident met de ABONNEE afhandelen.

Indien SIGNICAT SLU de gegevens corrigeert zonder het betreffende incident vooraf met de ABONNEE te hebben afgehandeld, moet zij de uiteindelijk gecertificeerde gegevens aan de ABONNEE meedelen.

SIGNICAT SLU behoudt zich het recht voor het certificaat niet uit te geven wanneer de verstrekte bewijsstukken onvoldoende zijn voor de correcte identificatie en authenticatie van de ABONNEE, of wanneer het vóór de uitgifte van het certificaat uitgevoerde video-identificatieproces niet door SIGNICAT SLU als geldig is bevestigd.

Bovenstaande verplichtingen worden opgeschort indien de ABONNEE optreedt als registratieautoriteit en beschikt over de technische elementen voor het genereren van sleutels, het uitgeven van certificaten en het registreren van ondertekeningsmiddelen van ondernemingen.

b. Met betrekking tot de verlening van de digitale certificeringsdienst

SIGNICAT SLU verbindt zich ertoe de verplichtingen na te komen die zijn vastgelegd in Wet 6/2020 van 11 november, die bepaalde aspecten van elektronische vertrouwensdiensten regelt, en met name:

- a) Certificaten uit te geven, te leveren, te beheren, op te schorten, in te trekken en te vernieuwen overeenkomstig de instructies van de ABONNEE, in de gevallen en om de redenen die zijn beschreven in de CPS van SIGNICAT SLU.
- b) De diensten uit te voeren met de passende technische en materiële middelen en met personeel dat voldoet aan de in de CPS vastgelegde voorwaarden inzake kwalificatie en relevante ervaring.
- c) De serviceniveaus na te leven, overeenkomstig het bepaalde in de CPS, op technisch, operationeel en beveiligingsgebied.
- d) De status van de certificaten mee te delen aan derden die daarom verzoeken, overeenkomstig het bepaalde in de CPS voor de verschillende diensten voor verificatie van certificaten.
- e) Kwaliteit van het Proces: SIGNICAT SLU garandeert de goede werking van de in dit document beschreven certificeringsdiensten, mits de aan de ABONNEE ter beschikking gestelde middelen correct en overeenkomstig de instructies van SIGNICAT SLU worden gebruikt.

Toegang tot en gebruik van de certificeringsdiensten houden voor SIGNICAT SLU geen verplichting in om te controleren of er geen virussen, wormen of andere schadelijke computerelementen aanwezig zijn. Het is de verantwoordelijkheid van de ABONNEE als gebruiker om te allen tijde over passende middelen te beschikken voor de detectie en verwijdering van schadelijke computerprogramma's. SIGNICAT SLU kan niet aansprakelijk worden gesteld voor schade aan de computerapparatuur van de ABONNEE of van derden tijdens het Video-identificatieproces.

- f) Beschikbaarheid van het Proces: de werking van het certificeringsproces kan afhangen van een correcte configuratie van de apparatuur waarmee de gebruiker het video-identificatieproces opent en start; de gebruiker moet daarom de verstrekte instructies volgen en in ieder geval te allen tijde voldoen aan de gespecificeerde software- en hardwarevereisten.

Evenzo moet voor de uitvoering van het video-identificatieproces een internetverbinding beschikbaar zijn. De werking van het video-identificatieproces kan afhangen van de toereikende kwaliteit en snelheid van de verbinding waarmee de ABONNEE de applicatie opent; hij/zij is als enige verantwoordelijk voor het voorzien in telecommunicatielijnen, internetabonnementen of -verbindingen of andere technische middelen die nodig zijn om toegang te krijgen tot zijn/haar gegevens en deze te gebruiken.

- **Als verlener van certificeringsdiensten**

SIGNICAT SLU zal:

- a) Waarheidsgetrouwe informatie publiceren overeenkomstig Wet 6/2020 van 11 november, die bepaalde aspecten van elektronische vertrouwensdiensten regelt, en Verordening (EU) nr. 910/2014.
- b) De gegevens voor het aanmaken van handtekeningen, zegels of websiteauthenticatie van de natuurlijke of rechtspersoon aan wie zij haar diensten heeft verleend, niet zelf of via derden opslaan of kopiëren, behalve in het geval van het beheer daarvan namens de houder met het oog op de toepassing van de private sleutels voor het aanmaken van handtekeningen, zoals aangegeven door de ABONNEE via het OTP-systeem dat SIGNICAT SLU de ABONNEE ter beschikking stelt voor de ondertekening van elektronische documenten. In dat geval worden betrouwbare systemen en producten gebruikt, met inbegrip van beveiligde elektronische communicatiekanalen, en worden passende technische en organisatorische procedures en mechanismen toegepast om te waarborgen dat de omgeving betrouwbaar is en onder de uitsluitende controle van de houder van het certificaat wordt gebruikt. Bovendien moeten de gegevens voor het aanmaken van handtekeningen, zegels of websiteauthenticatie worden beveiligd en beschermd tegen elke wijziging, vernietiging of onbevoegde toegang, en moet de voortdurende beschikbaarheid ervan worden gewaarborgd.
- c) Een voor het publiek toegankelijke raadplegingsdienst aanbieden over de geldigheids- of intrekingsstatus van de uitgegeven certificaten.
- d) De volgende aanvullende verplichtingen nakomen:
 - 1. De termijn gedurende welke de informatie over de verleende diensten moet worden bewaard overeenkomstig artikel 24, lid 2, onder h), van Verordening (EU) nr. 910/2014, bedraagt 15 jaar na het verstrijken van het certificaat of het einde van de verleende dienst. Indien gekwalificeerde certificaten voor elektronische zegels of websiteauthenticatie aan rechtspersonen worden uitgegeven, registreren de verleners van vertrouwensdiensten ook de informatie aan de hand waarvan de identiteit kan worden vastgesteld van de natuurlijke persoon aan wie die certificaten zijn geleverd, met het oog op diens identificatie in gerechtelijke of administratieve procedures.
 - 2. Een aansprakelijkheidsverzekering afsluiten voor een minimumbedrag van 1.500.000 euro, tenzij de verlener tot de publieke sector behoort. Indien meer dan één van de in Verordening (EU) nr. 910/2014 bedoelde gekwalificeerde diensten wordt verleend, wordt voor elk extra type dienst 500.000 euro toegevoegd. Deze zekerheid kan geheel of gedeeltelijk worden vervangen door een bankgarantie of een borgtochtverzekering, zodat de som van de verzekerde bedragen in overeenstemming is met het bepaalde in de vorige alinea. De bedragen en de in de twee voorgaande alinea's vastgestelde verzekerings- en zekerheidsmiddelen kunnen bij koninklijk besluit worden gewijzigd.
 - 3. In geval van beëindiging van haar activiteit als gekwalificeerde verlener van vertrouwensdiensten de klanten aan wie zij de diensten verleent en het toezichthoudende orgaan ten minste twee maanden vóór de daadwerkelijke beëindiging van de activiteit daarvan in kennis stellen, langs een weg die, waar mogelijk, de daadwerkelijke bezorging en ontvangst aantoont. Het beëindigingsplan van de dienstverlener kan voorzien in de overdracht van klanten, nadat is vastgesteld dat er geen bezwaar bestaat, aan een andere gekwalificeerde verlener, die alle informatie over de tot dan toe verleende diensten kan bewaren. Evenzo stelt zij het toezichthoudende orgaan in

kennis van elke andere relevante omstandigheid die de voortzetting van haar activiteiten kan verhinderen. Zij moet met name melding maken van de opening van een insolventieprocedure tegen haar zodra zij daarvan kennis krijgt.

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 leidt, nadat de dienstverlener is verzocht de genoemde inbreuk te beëindigen, tot intrekking van de gekwalificeerde status van de verlener en van de door hem verleende dienst en tot verwijdering ervan van de vertrouwenslijst bedoeld in artikel 22 van de genoemde verordening.
- e) SIGNICAT SLU aanvaardt jegens derden de volledige verantwoordelijkheid voor de handelingen van de personen of andere dienstverleners aan wie zij de uitvoering van alle of een deel van de voor de verlening van elektronische vertrouwensdiensten noodzakelijke taken delegeert, met inbegrip van de handelingen ter verificatie van de identiteit voorafgaand aan de uitgifte van een gekwalificeerd certificaat.

GARANTIES VOOR CERTIFICERINGSDIENSTEN

Garantie van SIGNICAT SLU voor digitale certificeringsdiensten

SIGNICAT SLU garandeert dat de private sleutel van de certificeringsautoriteit die wordt gebruikt om certificaten uit te geven, niet is gecompromitteerd, tenzij anders meegedeeld via het certificeringsregister, overeenkomstig de CPS.

SIGNICAT SLU garandeert de ABONNEE, op het moment van uitgifte van het certificaat, uitsluitend dat:

- a) de certificaten, in voorkomend geval, gekwalificeerd zijn en functioneren in een beveiligd middel voor het aanmaken van handtekeningen, onder de voorwaarden van Wet 6/2020 van 11 november, die bepaalde aspecten van elektronische vertrouwensdiensten regelt;
- b) SIGNICAT SLU geen valse of onjuiste verklaringen heeft veroorzaakt of opgenomen in de informatie in een certificaat, en evenmin heeft nagelaten noodzakelijke, door de ABONNEE verstrekte en geverifieerde informatie op te nemen;
- c) alle certificaten voldoen aan de vorm- en inhoudsvereisten die zijn vastgelegd in de CPS en het CP van SIGNICAT SLU;
- d) SIGNICAT SLU de in de CPS beschreven procedures heeft nageleefd.

SIGNICAT SLU betracht redelijke zorgvuldigheid om te waarborgen dat elk product dat zij in het kader van haar diensten levert, vrij is van computervirussen, wormen en andere illegale code, en is verplicht de ABONNEE in kennis te stellen van elk virus, elke worm of andere illegale code die later in een product wordt ontdekt.

UITSLUITING VAN GARANTIES

SIGNICAT SLU geeft geen garantie voor software die door de ABONNEE van het certificaat, de ondertekenaar of een andere persoon wordt gebruikt om een door SIGNICAT SLU uitgegeven digitale

handtekening of digitaal certificaat aan te maken, te verifiëren of anderszins te gebruiken, tenzij er een schriftelijke verklaring van SIGNICAT SLU is die het tegendeel bepaalt.

BEPERKINGEN VAN AANSPRAKELIJKHEID ALS VERLENER VAN ELEKTRONISCHE VERTROUWENSDIENSTEN.

SIGNICAT SLU is, voor zover dit binnen de grenzen van het toepasselijke recht valt, niet aansprakelijk voor schade en verliezen die zijn veroorzaakt aan de persoon aan wie zij haar diensten heeft verleend of aan derden te goeder trouw, indien deze zich voordoen in een van de gevallen bedoeld in Verordening (EU) nr. 910/2014 of in de volgende gevallen:

- a) Het niet verstrekken aan de verlener van vertrouwensdiensten van waarheidsgetrouwe, volledige en juiste informatie voor de verlening van de vertrouwensdienst, met name over de gegevens die in het elektronische certificaat moeten worden opgenomen of die nodig zijn voor de uitgifte ervan of voor het vervallen of de opschorting van de geldigheid ervan, voor zover de onjuistheid daarvan niet door de dienstverlener, handelend met de vereiste zorgvuldigheid, is ontdekt.
- b) Het niet zonder onnodige vertraging aan SIGNICAT SLU meedelen 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 weergegeven.
- c) Nalatigheid bij het bewaren van de gegevens voor handtekeningen, zegels of websiteauthenticatie, bij het waarborgen van de vertrouwelijkheid ervan en bij de bescherming tegen elke toegang daartoe of openbaarmaking daarvan of, in voorkomend geval, van de middelen die daartoe toegang geven.
- d) Het niet verzoeken om opschorting of intrekking van het elektronische certificaat bij twijfel over het behoud van de vertrouwelijkheid van de gegevens voor handtekeningen, zegels of websiteauthenticatie of, in voorkomend geval, van de middelen die daartoe toegang geven.
- e) Het gebruiken van de gegevens voor het aanmaken van handtekeningen, zegels of websiteauthenticatie nadat de geldigheidsduur van het elektronische certificaat is verstreken, of nadat de verlener van vertrouwensdiensten u in kennis heeft gesteld van het vervallen of de opschorting van de geldigheid ervan.

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

De ontvanger wordt geacht nalatig te handelen wanneer hij geen rekening houdt met de opschorting of het verlies van 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 elektronische certificaat indien deze zijn aangetoond door middel van een openbaar of officieel document, of zijn ingeschreven in een openbaar register indien dat vereist is.

AANSPRAKELIJKHEID VAN DE ABONNEE

De ABONNEE is jegens eenieder aansprakelijk voor de niet-nakoming van zijn/haar verplichtingen, met name met betrekking tot de identificatieactiviteit of, in voorkomend geval, de activiteit als registratieautoriteit, overeenkomstig deze algemene voorwaarden.

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

Zolang de in clausule 5 van dit document bedoelde kennisgeving niet heeft plaatsgevonden, berust elke aansprakelijkheid die kan voortvloeien uit het onbevoegde en/of oneigenlijke gebruik van de certificaten bij de ABONNEE.

GESCHIKTHEID VAN PRODUCTEN DIE GEBRUIKMAKEN VAN IDENTIFICATIE, ELEKTRONISCHE HANDTEKENING OF VERSLEUTELING

SIGNICAT SLU is niet aansprakelijk voor de geschiktheid van de op de markt beschikbare producten en diensten op het gebied van digitale certificering, identificatie, elektronische handtekening of versleuteling die in de computertoepassingen van de ABONNEE worden gebruikt, behalve wanneer SIGNICAT SLU deze levert. In dat geval zijn de partijen onderworpen aan de betreffende gebruiksvoorwaarden.

EIGENDOM VAN CERTIFICATEN EN ONDERTEKENINGSMIDDEL

De geleverde certificaten en ondertekeningsmiddelen blijven eigendom van de ABONNEE.

BEËINDIGING

Beëindiging vindt plaats in de volgende gevallen:

- a) Wegens een tekortkoming van de andere partij in de nakoming van een van haar verplichtingen, indien deze inbreuk niet is verholpen;
- b) binnen dertig dagen na ontvangst van de kennisgeving van de partij die haar verplichtingen niet heeft geschonden;
- c) onmiddellijk, indien de inbreuk de veiligheid van de diensten in gevaar brengt.
- d) Wegens het zich voordoen van een andere grond voor vroegtijdige beëindiging die is vastgelegd in de geldende wetgeving en, in het bijzonder, in de geldende wetgeving inzake elektronische handtekeningen en digitale certificering.

VERTROUWELIJKHEIDSBELEID

SIGNICAT SLU mag geen vertrouwelijke informatie over certificaten openbaar maken en kan daartoe niet worden gedwongen zonder een specifiek voorafgaand verzoek van:

- a) de persoon ten aanzien van wie SIGNICAT SLU verplicht is de informatie vertrouwelijk te houden, of
- b) een gerechtelijk, administratief of ander bevel dat op grond van de geldende wetgeving is voorzien.

De ABONNEE aanvaardt echter dat bepaalde informatie, al dan niet persoonlijk, die in de certificaataanvraag is verstrekt, wordt opgenomen in zijn/haar certificaten en in het mechanisme voor verificatie van de certificaatstatus, en dat deze informatie op grond van een wettelijk voorschrift niet als vertrouwelijk wordt beschouwd.

TERUGBETALINGSBELEID

SIGNICAT SLU betaalt de kosten van de certificeringsdienst in geen geval terug.

BEWAARTERMIJN VAN DE INFORMATIE

Alle informatie met betrekking tot het Proces van uitgifte van gekwalificeerde elektronische certificaten voor natuurlijke personen, met inbegrip van het door de ABONNEE naar behoren ondertekende contract en de tijdens de gehele uitgifte gegenereerde logbestanden, wordt door SIGNICAT SLU bewaard gedurende de looptijd van de contractuele relatie, zolang niet om verwijdering ervan wordt verzocht, en gedurende de verjaringstermijn van eventuele rechtsvorderingen of claims die van officiële instanties kunnen worden ontvangen.

In dit verband bedraagt de maximale bewaartermijn van de relevante informatie met betrekking tot het proces van video-identificatie en uitgifte van gekwalificeerde certificaten 15 jaar na de intrekking of het verstrijken van het certificaat, tenzij wettelijk anders bepaald. Na beëindiging van de contractuele relatie worden de gegevens van de ABONNEE naar behoren geblokkeerd, overeenkomstig de bepalingen van de toepasselijke regelgeving.

5. ALGEMENE BEPALINGEN

5.1. PLAATS VAN UITOEFENING VAN DE ACTIVITEIT

De plaats van nakoming van de verplichtingen van SIGNICAT SLU met betrekking tot digitale certificeringsdiensten en, in voorkomend geval, softwaregebruikslicenties, is het vestigingsadres van SIGNICAT SLU.

5.2. SCHEIDBAARHEID VAN DE ALGEMENE VOORWAARDEN.

De clausules van dit document zijn onafhankelijk van elkaar; indien een clausule ongeldig of niet-afdwingbaar wordt geacht, blijven de overige clausules daarom van toepassing, tenzij de partijen uitdrukkelijk anders zijn overeengekomen.

5.3. TOEPASSELIJKE REGELGEVING EN BEVOEGDE RECHTER.

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

De bevoegde rechter is de rechter die is aangewezen in Wet 1/2000 van 7 januari inzake burgerlijke rechtsvordering, behalve wanneer de ABONNEE als consument wordt aangemerkt; in dat geval onderwerpt SIGNICAT SLU zich aan de rechter die wettelijk bevoegd is.