VILLKOR FÖR VIDEOIDENTIFIERINGSPROCESSEN OCH UTFÄRDANDE AV KORTFRISTIGA CERTIFIKAT

QES ONCE DEFERRED

Detta är en svensk översättning av den engelska versionen av villkoren för videoidentifieringsprocessen och utfärdande av kortfristiga certifikat QES ONCE DEFERRED, som finns på https://www.signicat.com/about/english. Dessa villkor för QES ONCE DEFERRED har översatts endast för att underlätta för TECKNARE eller ANSÖKARE och har inget juridiskt värde. Den engelska versionen ska alltid vara bindande och ha företräde framför den svenska översättningen.

Å ena sidan SIGNICAT, S.L.U. (Tidigare kallad Electronic Identification, S.L.), med säte på Avenida Ciudad de Barcelona 81, 4ª Planta, registrerat i handelsregistret i Madrid den 13 mars 2013 med Org.nr. B86681533 (nedan kallat SIGNICAT SLU), är en kvalificerad tillhandahållare av betrodda tjänster som agerar i enlighet med bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, samt de tekniska standarder från ETSI som är tillämpliga på utfärdande och hantering av kvalificerade certifikat, huvudsakligen EN 319 411-1 och EN 319 411-2, i syfte att underlätta efterlevnaden av rättsliga krav och internationellt erkännande av sina tjänster.

Å **andra sidan**, **TECKNAREN eller ANSÖKAREN**, vars identifieringsuppgifter för detta avtal finns i den Identifieringshandling som används och i den video som genereras som ett resultat av processen för Videoidentifiering och utfärdande av certifikat.

1. SYFTE:

Syftet med detta dokument är att på ett klart och begripligt sätt informera sökanden/tecknaren om de nuvarande*"Villkoren för fjärridentifieringsprocessen med hjälp av oassisterad video och villkoren för den elektroniska certifieringstjänsten för utfärdande av korttidscertifikat*", och att reglera tjänsterna i enlighet med de villkor som anges i detta dokument, Deklaration om certifieringspraxis, eIDASförordningen och lokala lagar som kan gälla.

Denna föregående identifieringsprocess är nödvändig för att ackreditera identiteten hos sökanden/prenumeranten, som begär att SIGNICAT SLU ska utfärda ett kvalificerat certifikat för elektronisk signatur för fysisk person med kort tidsfrist ("Certifieringstjänster"), certifikat vars användning är föremål för villkoren för den elektroniska certifieringstjänsten som tillhandahålls av SIGNICAT SLU som en kvalificerad leverantör av betrodda tjänster som beskrivs nedan.

Det kvalificerade elektroniska certifikat som utfärdas under dessa Villkor och bestämmelser motsvarar följande certifieringsprofil:

- Kvalificerat certifikat för fysisk person i MOLNET (CLOUD) med QSCD med OID 1.3.6.1.4.1.55193.1.1.2. Detta är ett kvalificerat certifikat, utfärdat för ändamålen kvalificerade elektroniska signaturer och deras autentisering, i enlighet med certifieringspolicyn QCP-n-qscd, med OID 0.4.0.194112.1.2. Detta certifikat utfärdas i en centraliserad QSCD och består av ett kvalificerat certifikat i enlighet med bestämmelserna i artikel 28 i förordning (EU) nr 910/2014.

Det drivs med hjälp av kvalificerade enheter för skapande av elektroniska signaturer (QSCD) i enlighet med artiklarna 29 och 51 i förordning (EU) nr 910/2014 och uppfyller bestämmelserna i de tekniska föreskrifterna från Europeiska institutet för telekommunikationsstandarder, identifierade med referensnumret ETSI EN 319 411-2. Särskilt är denna QSCD en nShield Solo XC Hardware Security Module v12.60.15 och Entrust Signature Activation Module (SAM), version 1.1.1, båda certifierade i enlighet med Common Criteria EAL4+ och kvalificerade som kvalificerade enheter för skapande av elektroniska signaturer. Den garanterar undertecknarens identitet och dennes koppling till abonnenten av den elektroniska betrodda tjänsten, genom att tillåta generering av den "kvalificerade elektroniska signaturen", det vill säga den avancerade signaturen baserad på ett kvalificerat certifikat som har skapats

med hjälp av en kvalificerad enhet, vilket därmed likställer den med den handskrivna signaturen för rättsliga effekter och syften, utan behov av att uppfylla några andra ytterligare krav.

Abonnenten bekräftar och antar att läsning och godkännande av detta dokument genom att kryssa i kryssrutorna ska betraktas som en enkel elektronisk signatur.

2. TILLÄMPLIGA DEFINITIONER

- **CERTIFIERINGSMYNDIGHET (AC):** Betrodd enhet för avsändaren och mottagaren av meddelandet. Detta förtroende för en "betrodd tredje part" gör det möjligt för båda att i sin tur lita på de dokument som undertecknats av certifieringsmyndigheten, i synnerhet de dokument som identifierar varje offentlig nyckel med dess motsvarande ägare och som kallas certifikat. Vid tillhandahållandet av den Tjänst som Abonnenten efterfrågar kommer SIGNICAT SLU att agera som Certifikatutfärdare och knyta en viss publik nyckel till en viss Abonnent genom utfärdande av ett Certifikat.

- **REGISTRERINGSMYNDIGHET (RA**): En enhet som, bland andra funktioner, unikt identifierar den som ansöker om ett certifikat och, i tillämpliga fall, de andra omständigheter som är förknippade med certifikatet i enlighet med avsnitt 1.3.2. Registreringsmyndigheter för SIGNICAT SLU SCP. Registreringsmyndigheten förser certifikatutfärdaren med verifierade uppgifter om den sökande, så att certifikatutfärdaren kan utfärda motsvarande certifikat. Alla eller några av RA:s egna funktioner får övertas antingen direkt av SIGNICAT SLU eller av en enhet som bemyndigats av SIGNICAT SLU.

- **CERTIFIKAT FÖR ELEKTRONISK SIGNATUR**: En elektronisk deklaration som kopplar valideringsdata för en signatur till en fysisk person och bekräftar åtminstone namnet eller pseudonymen för den personen.

- **KVALIFICERAT CERTIFIKAT FÖR ELEKTRONISK SIGNATUR**: Ett certifikat för elektronisk signatur som har utfärdats av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller de krav som anges i bilaga I till EU-förordning 910/2014 av den 23 juli 2014 (eIDAS-förordningen), som ger maximala rättsliga garantier när det gäller identifiering av undertecknaren och dess koppling till signaturen på ett unikt sätt, integritet och oavvislighet för uppgifterna eftersom de är kopplade till signaturen.

- **DEKLARATION OM CERTIFIERINGSPRAXIS ("CPS"):** är ett dokument upprättat av en certifieringsutfärdare som anger eller reglerar tillhandahållandet av certifieringstjänster av denna certifieringsutfärdare i sin egenskap av tillhandahållare av certifieringstjänster, i detta fall SIGNICAT SLU. Den reglerar bland annat hanteringen av uppgifter för skapande och verifiering av signaturer och av certifikaten, de villkor som gäller för begäran, utfärdande, användning, upphävande och avslutande av certifikatens giltighet.

- **KVALIFICERAD ELEKTRONISK SIGNATUR**: en avancerad elektronisk signatur som skapas av en kvalificerad enhet för skapande av elektroniska signaturer och som är baserad på ett kvalificerat

certifikat för elektroniska signaturer. Giltigheten av signaturen är iuris tantum eftersom det är en kvalificerad signatur, bevisbördan ligger på personen som avvisar signaturen som giltig.

- **KVALIFICERAD TILLHANDAHÅLLARE AV BETRODDA TJÄNSTER**: en tillhandahållare av betrodda tjänster som tillhandahåller en eller flera kvalificerade betrodda tjänster och som har beviljats kvalificering av tillsynsorganet.

- **ANSÖKARE ELLER TECKNARE** är den identifierade fysiska person som beställer SIGNICAT SLUcertifieringstjänster och som, före utfärdandet av det kvalificerade certifikatet, ansökte om och framgångsrikt slutförde SIGNICAT SLU Video Identification Process.

3. VILLKOR OCH BESTÄMMELSER FÖR VIDEOIDENTIFIERINGSPROCESSEN

Identifieringsprocessen för sökanden av de identifieringstjänster som tillhandahålls av SIGNICAT SLU för utfärdande av elektroniska certifikat ska utföras på ett av följande sätt, i enlighet med artikel 24.1 i eIDAS:

a) i närvaro av den fysiska personen eller en behörig företrädare för den juridiska personen, för vilket ändamål sökanden måste gå till SIGNICAT SLU:s kontor på Av. de la Ciudad de Barcelona, 81, 4ª Planta, 28007 Madrid, eftersom det inte finns några delegerade registreringsmyndigheter.

b) på distans, med hjälp av elektroniska identifieringsmedel, för vilka den fysiska personens närvaro eller en behörig företrädare för den juridiska personen har garanterats före utfärdandet av det kvalificerade certifikatet, och i enlighet med den videoidentifieringsprocess som avses i detta dokument och i uttalandet om certifieringspraxis, tillgängligt via följande länk: https://www.signicat.com/about/qualified-certificates-for-electronic-signatures

c) med hjälp av ett kvalificerat certifikat för elektronisk signatur eller en kvalificerad elektronisk stämpel som utfärdats i enlighet med led a eller b.

d) använda andra nationellt erkända identifieringsmetoder som ger likvärdig säkerhet i fråga om tillförlitlighet som fysisk närvaro. Likvärdig säkerhet ska bekräftas av ett organ för bedömning av överensstämmelse.

3.1 VALIDERING AV IDENTITET PÅ ELEKTRONISK VÄG OCH BESKRIVNING AV VIDEOIDENTIFIERINGSPROCESSEN.

Videoidentifieringsprocessen (nedan "Videoidentifieringsprocessen" eller "Processen") är en metod för obemannad identitetsverifiering i realtid via video på distans som tillhandahålls genom en uppsättning programvarubibliotek, RESTful Application Interface och webbapplikationer, ägda av SIGNICAT SLU ("Applikationen"), som implementerar, stöder och registrerar hela processen för att registrera en person och möjliggör validering av identitetshandlingar på distans med hjälp av videoinspelning. Denna video fångar och validerar identitetshandlingen i realtid och på ett automatiserat sätt (cirka 10-20 sekunder),

och utförs av SIGNICAT SLU genom dess kvalificerade mänskliga agenter som, som verifieringsoperatörer, fungerar som registreringsmyndighet och ansvarar för att ackreditera identiteten.

3.1.1 Allmän information om videoidentifieringsprocessen.

Sökanden öppnar Applikationen och innan åtgärderna för att verifiera identiteten påbörjas ber gränssnittet Sökanden att läsa och godkänna detta dokument och att fritt ge sitt samtycke till behandlingen av biometriska data som krävs för att utföra videoidentifieringen. För detta ändamål har SIGNICAT SLU tidigare försett sökanden med den Integritetspolicy som innehåller den behandling av personuppgifter som kommer att utföras under Processen i enlighet med bestämmelserna i Dataskyddsförordningen.

Om Sökanden inte lämnar detta samtycke kan Processen inte fortsätta och Sökanden måste använda sig av något av de alternativ för identifiering som anges i punkt 1 i detta dokument i enlighet med bestämmelserna i artikel 24.1 i eIDAS-förordningen.

Den kommer sedan att visas för den sökande:

- En förhandsgranskning av det avtal som skall undertecknas
- Uppmaning till handling för godkännande av detta dokument
- Ett nedladdningsalternativ som gör det möjligt för användaren att spara dokumentet

Om den Sökande inte tar del av dokumentet och lämnar detta samtycke kan Processen inte fortsätta.

Slutligen, innan videoidentifieringsprocessen påbörjas, kommer användaren att ombes ange ett telefonnummer för att kunna skicka en OTP.

Med hjälp av denna OTP kommer användaren, utöver att ratificera dessa villkor, att godkänna utfärdandet av certifikatet, inklusive de uppgifter som hämtats från videoidentifieringsprocessen enligt punkt 3.3.5 i detta dokument, samt det avtalsdokument som har visats i början av processen och på vilket signaturskapningsdata kommer att tillämpas av SIGNICAT SLU i syfte att generera en kvalificerad elektronisk signatur.

Efter verifiering av denna OTP kommer SIGNICAT SLU att tillämpa signaturskapande data, enligt vad som förutses och beskrivs i klausul 3.4.

När den Sökande har läst, accepterat och samtyckt till Processen, kommer han/hon att utföra den Videoidentifiering som krävs för att SIGNICAT SLU ska kunna utfärda certifikatet för kvalificerad fysisk person.

Sökanden vägleds hela tiden av röst och text under videoidentifieringsprocessen och med hjälp av Applikationen utförs en automatiserad kontroll av miljöelementen (ljusförhållanden, nätverk, kamerakvalitet) för att få en optimal inspelning av Videoidentifieringen och dess bevis.

I denna mening är stegen i processen före utfärdandet av det kvalificerade certifikatet följande:

Det första steget i processen innebär att den sökande visar upp den identitetshandling som ska användas för att utföra en bildjämförelse med originalhandlingarna med hjälp av specialiserad teknik för att kontrollera handlingens äkthet och utföra datautvinning (OCR) av MRZ eller andra delar av handlingen och möjligheten att ringa in referenserna i realtid.

Därför kommer framsidan av den identitetshandling som den Sökande använder under Processen att registreras. För att göra detta ombeds den sökande att visa framsidan av sitt dokument och passa in bilden i den ruta som visas.

När registreringen är klar visas ett meddelande om överensstämmelse och nästa del av processen fortsätter.

Nästa steg är att ta fram baksidan av dokumentet. Den sökande ombeds att visa baksidan av sitt dokument och passa in bilden i den ruta som visas.

När registreringen är klar visas ett meddelande om överensstämmelse och nästa del av processen fortsätter.

Sökandens biometriska data registreras sedan för att i realtid jämföras med bilden på ID-kortet för en ansiktsigenkänningsprocess baserad på automatisk biometrisk poängsättning. För att göra detta ombeds den sökande att visa sitt ansikte och passa in bilden i rutan som visas på skärmen.

När de biometriska uppgifterna har samlats in ombeds den sökande att göra en ansiktsrörelse mot kameran som bevis på att han eller hon lever, och om allt är korrekt visas ett meddelande om överensstämmelse och nästa del av processen fortsätter.

Om hela Processen är framgångsrik informeras Sökanden om att videoidentifieringsprocessen har slutförts och att de bevis som genererats under Processen kommer att kontrolleras och valideras med hjälp av Registreringsmyndighetens verifieringsverktyg för granskning av Processen av en kvalificerad människa som tidigare utbildats genom en specifik utbildning.

Vid denna tidpunkt gör Applikationen videoidentifieringen och de data som genererats under videoidentifieringen tillgängliga för en kvalificerad mänsklig Agent som ansvarar för att verifiera identiteten hos Processförfrågan och begär asynkron granskning av den inspelade videon, liksom resten av de bevis och element som erhållits under Processen. Den genomsnittliga verifieringstiden för en agent är vanligtvis cirka tre minuter.

3.1.2. Säkerhetselement i videoidentifieringsprocessen och validering av kvalificerad mänsklig agent.

För den asynkrona granskningen av ett kvalificerat mänskligt ombud finns det ett säkerhetsprotokoll baserat på EU:s bästa praxis som bygger på det verktyg som erbjuds det kvalificerade mänskliga ombudet

där de bevis som erhållits under processen visas, liksom flaggor eller meddelanden om de som inte erhållits.

Inspelningen av videon, begäran om verifiering av videoidentifieringen samt den kvalificerade tjänstemannens yttrande spåras inom applikationen och en tidsstämpel tillämpas på varje spår för att säkerställa dess konsekvens och integritet.

Processen säkerställer därför kontrollkedjan för verifieringen från de bevis som samlas in genom processen till de spår som kopplar identifieringen till registreringsmyndighetens kvalificerade mänskliga ombud. Detta resulterar i en verifierad identitet med teknisk säkerhet som är likvärdig med den som utförs i den Sökandes fysiska närvaro.

När identiteten har validerats positivt av den kvalificerade mänskliga agenten har sökandens identitet ackrediterats och sökanden kommer att kunna fortsätta och ta emot den elektroniska certifieringstjänsten SIGNICAT SLU som gör det möjligt för honom/henne att fortsätta med processen att utfärda certifikatet för kvalificerad fysisk person och underteckna de elektroniska dokumenten.

Om resultatet av Processen är negativt kommer det inte att vara möjligt att fortsätta med Processen för utfärdande av kvalificerade certifikat, och Sökanden måste fysiskt gå till SIGNICAT SLU-lokalerna för att genomföra en personlig verifiering av sin identitet.

3.2 SÖKANDENS SKYLDIGHETER I SAMBAND MED VIDEOIDENTIFIERINGSPROCESSEN.

Sökanden åtar sig under hela Processen att:

- Använda Tjänsten i enlighet med bestämmelserna i detta dokument, CPS, eventuella tillämpliga särskilda villkor och eventuella andra instruktioner, manualer eller förfaranden som tillhandahålls av SIGNICAT SLU.

- Att den identitetshandling som används i Processen är en autentisk, juridiskt giltig handling och att, dessutom:

    - Det är inte en fotokopia eller ett tryckt kort:
    - Det är inte i digitalt format (mobil, surfplatta eller dator).
    - Det är inte inuti ett lock.
    - Det är oskadat och komplett, och alla säkerhetsdetaljer finns i dokumentet.

- Detta under processen och inspelningen av videon för att säkerställa att videon inte avvisas:

    - Ljusförhållandena i videon bör göra det möjligt att tydligt se den identifierade personens ansikte och handlingen.
    - Videon ska ha ett konstant flöde, utan avbrott eller fördröjningar.
    - En levande person måste visa legitimation.
    - Om en annan person än den person som ska identifieras utför hela Processen,

kommer identifieringen att avvisas.

- Om någon annan är närvarande i videon, men uppenbarligen inte tvingar personen att identifieras, kan identifieringen vara giltig, liksom om en viss person hjälper en funktionshindrad person att göra identifieringen.
- Det måste vara möjligt att tydligt visualisera alla delar av dokumentfångsten, framsidan, baksidan och personens ansikte.
- Den sökande får inte sova eller visa tecken som kan tolkas som att han eller hon är påverkad av droger eller alkohol

3.3 UTFÄRDANDE, LEVERANS OCH GODKÄNNANDE AV CERTIFIKATET

3.3.1 Certifikatansökan och nyckelgenerering av SIGNICAT SLU på uppdrag av Abonnenten.

När Videoidentifieringsprocessen har slutförts, bemyndigar Prenumeranten SIGNICAT SLU att för deras räkning generera och hantera de offentliga och privata nycklar som gör det möjligt för SIGNICAT SLU att fortsätta med utfärdandet av det kvalificerade kortfristiga fysiska personcertifikatet och att för deras räkning underteckna de elektroniska dokument som, i början av processen, har gjorts tillgängliga för dem genom SIGNICAT SLU eller tredje parter av offentlig eller privat karaktär med vilka SIGNICAT SLU har vissa avtalsöverenskommelser.

3.3.2 Informationens trovärdighet

Abonnenten ansvarar för att all information som lämnas till SIGNICAT SLU antingen direkt eller genom den identitetshandling som används under videoidentifieringen och certifikatutfärdandeprocessen är korrekt, fullständig för certifikatets syfte och att den alltid är uppdaterad, för vilken han/hon garanterar att använda en juridisk och giltig identitetshandling, utan att den har ändrats och/eller modifierats av Abonnenten av tredje part.

3.3.3 Utfärdande av certifikatet

För utfärdandet av certifikatet kommer SIGNICAT SLU att använda de uppgifter om identitetshandlingar som sökanden/abonnenten har lämnat under videoidentifieringsprocessen. Dessa uppgifter kommer att extraheras av SIGNICAT SLU och direkt införlivas i det elektroniska certifikatet i syfte att koppla din identitet till det.

3.3.4 Tilldelning av certifikatet

Vid utfärdandet sker ingen specifik leverans av certifikatet till prenumeranten. SIGNICAT SLU kommer att hantera det i sin egenskap av Qualified Trust Service Provider, så att prenumeranten kan använda det för elektronisk underskrift av dokument.

3.3.5 Godkännande av utfärdandet av certifikatet och ratificering av dessa villkor.

Genom att ange sitt telefonnummer och validera OTP i enlighet med punkt 3.1.1 accepterar sökanden/prenumeranten utfärdandet av certifikatet, inklusive de uppgifter som extraherats från videoidentifieringsprocessen.

3.4 SERVERBASERAD SIGNATURTJÄNST

När identifieringsprocessen har slutförts och identiteten har validerats av verifieringsagenten kommer undertecknarens identitet att garanteras och SIGNICAT SLU, som en kvalificerad leverantör av betrodda tjänster, kommer att tillämpa användarens/abonnentens signaturskapande data på dokumentet som visas och accepteras genom införandet av OTP på det dokument som accepteras i början av processen av abonnenten (i enlighet med klausul 3.1.1), vilket garanterar dess exklusiva kontroll.

SIGNICAT SLU ger prenumeranten, på en icke-exklusiv och icke-överförbar basis, en licens att använda kopior av SIGNICAT SLU:s programvara för säkra kryptografiska enheter för driften av signaturenheten i tillämpliga fall, samt för produktion av den elektroniska signaturen, certifikat och andra kryptografiska tjänster av undertecknarna.

Prenumeranten får göra kopior av programvaran endast för arkivering eller säkerhetskopiering.

Om någon annan än SIGNICAT SLU gör ändringar i den levererade programvaran upphör alla garantier med avseende på programvaran omedelbart att gälla.

4. ALLMÄNNA VILLKOR FÖR FÖRTROENDETJÄNSTEN

4.1 ALLMÄNNA VILLKOR FÖR VIDEOIDENTIFIERINGSTJÄNSTEN

– Förvaringsperiod för dokumentation

All information i samband med videoidentifieringsprocessen för utfärdande av kvalificerade elektroniska certifikat för fysiska personer, inklusive biometrisk information, kommer att lagras av SIGNICAT SLU under hela avtalsförhållandet, så länge radering inte begärs, och under preskriptionstiden för eventuella rättsliga åtgärder som kan uppstå, eller krav som kan mottas från officiella organ.

I detta avseende ska den maximala lagringsperioden för relevant information i samband med videoidentifieringsprocessen och utfärdandet av kvalificerade certifikat, dvs. en kopia av videoinspelningen, foton eller skärmdumpar av sökanden och den identitetshandling som används, det automatiska resultatet av den verifiering som utförs av SIGNICAT SLU-applikationen, samt den bedömning och de observationer som görs av de kvalificerade personkontrollanterna, tillsammans med deras beslut att godkänna eller avslå identifieringen, vara 15 år från återkallelse eller utgång av certifikatets giltighet, om inte annat föreskrivs i lag. När förhållandet har upphört kommer den sökandes uppgifter att blockeras i enlighet med bestämmelserna i tillämpliga förordningar.

Dessutom rapporteras att alla bevis på ofullständiga identifieringsprocesser som inte har slutförts på grund av misstanke om försök till bedrägeri kommer att bevaras under en period av 5 år från det att processen slutfördes, med angivande av skälet till att processen inte slutfördes, i enlighet med den policy som fastställts för detta ändamål.

– **Begränsning av ansvar i samband med videoidentifieringsprocessen.**

Processens kvalitet: SIGNICAT SLU garanterar att de Videoidentifieringstjänster som beskrivs häri utförs korrekt under förutsättning att de medel som görs tillgängliga för Sökanden används korrekt och i enlighet med SIGNICAT SLU:s instruktioner.

Åtkomst till och användning av Videoidentifieringstjänsterna innebär inte någon skyldighet för SIGNICAT SLU att kontrollera frånvaron av virus, maskar eller andra skadliga datorelement. Det är under alla omständigheter upp till Sökanden, som användare, att ha tillgång till lämpliga verktyg för att upptäcka och desinficera skadlig programvara. SIGNICAT SLU ansvarar inte för eventuella skador på Sökandens eller tredje parts datorutrustning som orsakas under Videoidentifieringsprocessen.

Processens tillgänglighet: Videoidentifieringsprocessens funktion kan bero på korrekt konfiguration av den utrustning från vilken användaren får tillgång till och startar videoidentifieringsprocessen, så användaren måste följa de anvisningar som ges och under alla omständigheter ha de krav på maskinvara och programvara som anges vid varje tidpunkt.

För att kunna genomföra videoidentifieringsprocessen måste det finnas tillgång till en Internetanslutning. Videoidentifieringsprocessens funktion kan bero på kvaliteten och hastigheten på den anslutning genom vilken den sökande får tillgång till applikationen, och därför ska den sökande vara ensam ansvarig för tillhandahållandet av telekommunikationslinjer, internetabonnemang eller anslutningar eller andra tekniska medel som är nödvändiga för att han/hon ska få tillgång till och använda sina uppgifter.

SIGNICAT SLU ska inte vara ansvarigt för skador som uppstår till följd av eller i samband med underlåtenhet eller bristfälligt utförande av de skyldigheter som den sökande ansvarar för, inte heller för felaktig användning av processresultaten och nycklarna, eller för någon indirekt skada som kan uppstå till följd av användningen av processen eller den information som tillhandahålls av SIGNICAT SLU.

SIGNICAT SLU ska inte hållas ansvarigt för eventuella felaktigheter i Sökandens identifiering till följd av den information som Sökanden lämnat under Processen.

SIGNICAT SLU ansvarar inte för korrekt användning med applikationer som inte är godkända, och för skador som orsakas av att det är omöjligt för den sökande att använda sådana applikationer.

4.2 ALLMÄNNA VILLKOR FÖR ELEKTRONISKA CERTIFIKATTJÄNSTER FÖR KORTTIDSCERTIFIKAT.

– **Rättslig ram för tillhandahållande av tjänster**

Certifieringstjänsterna regleras tekniskt och operativt av SIGNICAT SLU Certification Practices Statement och Certification Policies, och av deras efterföljande uppdateringar, samt av den kompletterande dokumentation som tillhandahålls prenumeranten.

Dessa allmänna villkor, Certification Practices Statement och Certification Policies, om tillämpligt för det

utfärdade certifikatet, utgör den rättsliga ram som kommer att reglera förhållandet mellan SIGNICAT SLU och TECKNAREN, både internt och gentemot tredje part, utan att det påverkar bestämmelserna i gällande lagstiftning.

Detta dokument utgör de mest relevanta delarna och kraven för parternas rättigheter och skyldigheter.

Certification Practice Statement (CPS) och tillämpliga specifika Certification Policies (CP) är införlivade i detta dokument genom hänvisning. Den senast uppdaterade versionen av PSC kommer att finnas tillgänglig när som helst och kostnadsfritt på följande språk via den länk som anges nedan:

- **Spanska:** https://www.signicat.com/es/acerca-de/certificados-cualificados-para-firmaelectronica
- **Engelska:** https://www.signicat.com/about/qualified-certificates-for-electronic-signatures

I händelse av inkonsekvens ska innebörden av de villkor som anges i detta avtal ha företräde framför vad som anges i PSC.

- **Avtalets tidsfrist**

Detta Avtal träder i kraft på de utfärdande- och förfallodagar som anges i det Kvalificerade Personcertifikat som Abonnenten har begärt och tecknat hos SIGNICAT SLU.

- **Skyldigheter för korrekt användning**

Abonnenten måste använda den certifieringstjänst som tillhandahålls av SIGNICAT SLU uteslutande för de användningsområden som tillåts i CPS, som är kända och accepterade av abonnenten genom att läsa och acceptera dem med hjälp av de valrutor som ingår i processen.

ABONNENTEN förbinder sig att använda den digitala certifikattjänsten och alla andra tekniska element som levereras av SIGNICAT SLU och certifikaten i enlighet med dessa villkor, GCP och de CP som kan vara tillämpliga, de särskilda villkor som kan vara tillämpliga och alla andra instruktioner, manualer eller förfaranden som SIGNICAT SLU tillhandahåller ABONNENTEN och i enlighet med bestämmelserna i tillämplig lagstiftning.

Upphandlingen av certifikattjänsten med SIGNICAT SLU tillåter endast användning av certifikatet inom ramen för abonnentens verksamhet, i enlighet med syftet med den typ av certifikat som begärts, dvs. det kvalificerade certifikatet för elektronisk signatur för en fysisk person med kort varaktighet. När certifikatet har utfärdats får abonnenten inte använda certifikatet för kommersiella ändamål, såvida inte parterna särskilt har kommit överens om detta. Med kommersiell användning av certifikatet avses varje åtgärd genom vilken abonnenten erbjuder tjänster till tredje part utanför detta avtal, mot en avgift eller kostnadsfritt, som kräver användning av det utfärdade certifikatet.

- **Förbjudna transaktioner**

De digitala certifieringstjänster som tillhandahålls av SIGNICAT SLU är inte utformade eller avsedda för användning eller återförsäljning som utrustning för kontroll av farliga situationer, eller för användning som kräver felsäker prestanda, såsom drift av kärnkraftsanläggningar, flygburna navigations- eller kommunikationssystem, flygtrafikledningssystem eller vapenledningssystem, där ett fel direkt kan orsaka dödsfall, fysisk skada eller allvarlig miljöskada.

– **Skyldigheter och ansvarsområden för SIGNICAT SLU**

a) I samband med tillhandahållandet av Registration Authority Service.

SIGNICAT SLU åtar sig att registrera certifikatuppgifterna och dess efterföljande utfärdande till TECKNARENTECKNAREN, för vilket ändamål det måste utföra de kontroller som det anser nödvändiga avseende TECKNARENS identitet och andra personliga och kompletterande uppgifter och, i förekommande fall, av undertecknarna.

Dessa kontroller måste omfatta den skriftliga motivering som tillhandahålls av Abonnenten, och om SIGNICAT SLU anser det nödvändigt, alla andra relevanta dokument och information som tillhandahålls av Abonnenten.

Om SIGNICAT SLU upptäcker fel i de uppgifter som ska ingå i certifikaten eller som motiverar dessa uppgifter, kan SIGNICAT SLU göra de ändringar som anses nödvändiga innan certifikatet utfärdas eller avbryta utfärdandeprocessen och hantera motsvarande incident med TECKNARENN.

Om SIGNICAT SLU korrigerar uppgifterna utan att först hantera motsvarande incident med abonnenten, ska SIGNICAT SLU meddela abonnenten om de uppgifter som slutligen certifierats.

SIGNICAT SLU förbehåller sig rätten att inte utfärda certifikatet när den tillhandahållna dokumentationen inte är tillräcklig för korrekt identifiering och autentisering av prenumeranten, eller när den videoidentifieringsprocess som utförts före utfärdandet av certifikatet inte har bekräftats som giltig av SIGNICAT SLU.

Ovanstående skyldigheter skall inte gälla om abonnenten fungerar som registreringsmyndighet och har de tekniska komponenter som krävs för att generera nycklar och utfärda certifikat.

b) I förhållande till tillhandahållandet av Certifieringstjänsten.

SIGNICAT SLU åtar sig att uppfylla de skyldigheter som anges i lag 6/2020 av den 11 november, som reglerar vissa aspekter av elektroniska förtroendetjänster, och i synnerhet att:

a) Utfärda, administrera, tillfälligt upphäva och återkalla certifikat, i enlighet med de instruktioner som lämnats av TECKNAREN, i de fall och av de skäl som beskrivs i SIGNICAT SLU CPS.

b) Utföra tjänsterna med lämpliga tekniska och materiella resurser och med personal som uppfyller de krav på kvalifikationer och erfarenhet som anges i SCP.

c) Uppfylla kvalitetsnivåerna för tjänsterna, i enlighet med bestämmelserna i PSC, när det gäller tekniska, operativa och säkerhetsmässiga aspekter.
d) Meddela status för certifikaten till tredje parter som begär det, i enlighet med bestämmelserna i CPS för de olika tjänsterna för verifiering av certifikat.

e) *Processens kvalitet:* SIGNICAT SLU garanterar att de Certifieringstjänster som beskrivs i detta dokument utförs korrekt under förutsättning att de medel som görs tillgängliga för Prenumeranten används på lämpligt sätt och i enlighet med SIGNICAT SLU:s anvisningar.

Tillgång till och användning av certifieringstjänsterna innebär inte någon skyldighet för SIGNICAT SLU att kontrollera frånvaron av virus, maskar eller något annat skadligt datorelement. Det är under alla omständigheter prenumerantens ansvar som användare att se till att det finns lämpliga verktyg för att upptäcka och desinficera skadliga datorprogram. SIGNICAT SLU ansvarar inte för eventuella skador på Abonnentens eller tredje parts datorutrustning som uppkommer under Videoidentifieringsprocessen.

f) Processens tillgänglighet: Certifieringsprocessens funktion kan bero på korrekt konfiguration av den utrustning från vilken användaren får tillgång till och inleder videoidentifieringsprocessen, varför användaren måste följa de anvisningar som ges och i alla händelser alltid ha de hårdvaru- och programvarukrav som anges.

För att kunna genomföra certifieringsprocessen måste det också finnas tillgång till en Internetanslutning. Processens funktion kan bero på lämplig kvalitet och hastighet på den anslutning genom vilken prenumeranten får tillgång till applikationen, varför prenumeranten är ensam ansvarig för tillhandahållandet av telekommunikationslinjer, internetabonnemang eller anslutningar eller andra tekniska medel som är nödvändiga för att han/hon ska få tillgång till och använda sina uppgifter.

– **Som leverantör av certifieringstjänster.**

SIGNICAT SLU skall:

a) Offentliggöra sanningsenlig information i enlighet med lag 6/2020 av den 11 november, som reglerar vissa aspekter av elektroniska betrodda tjänster och förordning (EU) 910/2014.

b) Att inte lagra eller kopiera, själv eller genom en tredje part, signaturskapande data, utom i fallet med dess hantering på innehavarens vägnar i syfte att tillämpa de privata signaturskapande nycklarna, som anges av TECKNAREN genom OTPsystemet som SIGNICAT SLU gör tillgängligt för TECKNAREN för undertecknande av elektroniska dokument. I detta fall ska de använda betrodda

system och produkter, inklusive säkra elektroniska kommunikationskanaler, och lämpliga tekniska och organisatoriska förfaranden och mekanismer ska genomföras för att säkerställa att miljön är betrodd och används under certifikatinnehavarens exklusiva kontroll.

Dessutom ska de säkra och skydda signaturframställningsdata mot ändring, förstörelse eller obehörig åtkomst och säkerställa dess fortsatta tillgänglighet.

c) Ha en allmänt tillgänglig tjänst för att söka information om giltigheten eller återkallandet av utfärdade certifikat.

d) Fullgöra följande ytterligare skyldigheter:

1. Den tidsperiod under vilken de ska bevara informationen om de tjänster som tillhandahålls i enlighet med artikel 24.2 h i förordning (EU) nr 910/2014 ska vara 15 år från det att certifikatet löper ut eller den tillhandahållna tjänsten upphör att gälla. Vid utfärdande av kvalificerade certifikat för autentisering av elektroniska sigill eller webbplatser till juridiska personer ska tillhandahållare av betrodda tjänster också registrera information som gör det möjligt att fastställa identiteten hos den fysiska person till vilken sådana certifikat har utfärdats, i syfte att identifiera personen i rättsliga eller administrativa förfaranden.

2. 1 500 000, såvida inte leverantören tillhör den offentliga sektorn. Om företaget tillhandahåller mer än en kvalificerad tjänst enligt förordning (EU) nr 910/2014 ska ytterligare 500 000 euro läggas till för varje typ av tjänst. Denna garanti får helt eller delvis ersättas av en garanti i form av en bankgaranti eller en borgensförsäkring, på ett sådant sätt att summan av de försäkrade beloppen överensstämmer med bestämmelserna i föregående stycke. De belopp och metoder för försäkring och garanti som fastställs i de två föregående punkterna får ändras genom kungligt dekret.

3. Om företaget upphör med sin verksamhet som kvalificerad tillhandahållare av betrodda tjänster ska det underrätta de kunder till vilka det tillhandahåller sina tjänster och tillsynsorganet minst två månader före det faktiska upphörandet av verksamheten, på ett sätt som bevisar effektiv leverans och mottagande när så är möjligt. Planen för uppsägning av tjänsteleverantören kan omfatta överföring av kunder, när det har fastställts att de inte har invänt, till en annan kvalificerad tjänsteleverantör, som får behålla informationen om de tjänster som tillhandahålls fram till dess. Den ska också informera tillsynsorganet om alla andra relevanta omständigheter som kan hindra den från att fortsätta sin verksamhet. I synnerhet måste den, så snart den får kännedom om det, meddela att ett insolvensförfarande har inletts mot den.

4. Skicka rapporten om bedömning av överensstämmelse till ministeriet för ekonomi och digital omvandling på de villkor som anges i artikel 20.1 i förordning (EU) nr 910/2014. Underlåtenhet att uppfylla denna skyldighet kommer att leda till att tjänsteleverantörens kvalifikationer och den tjänst han tillhandahåller återkallas och att han stryks från den tillförlitliga förteckning

som avses i artikel 22 i ovannämnda förordning, efter det att tjänsteleverantören har uppmanats att upphöra med denna bristande efterlevnad.

e) SIGNICAT SLU skall ta på sig allt ansvar gentemot tredje man för handlingar av personer eller andra leverantörer till vilka de delegerar utförandet av någon eller några av de funktioner som är nödvändiga för tillhandahållandet av elektroniska betrodda tjänster, inklusive åtgärder för identitetskontroll före utfärdandet av ett kvalificerat certifikat.

– **GARANTIER FÖR CERTIFIERINGSTJÄNSTER**

SIGNICAT SLU-försäkring av de elektroniska certifieringstjänsterna.

SIGNICAT SLU garanterar att certifikatutfärdarens privata nyckel som används för att utfärda certifikat inte har äventyrats, såvida den inte har meddelat något annat via certifikatregistret, i enlighet med CPS.

SIGNICAT SLU garanterar endast TECKNARENN, vid tidpunkten för utfärdandet av certifikatet, att:

a) I tillämpliga fall är certifikaten kvalificerade enligt villkoren i lag 6/2020 av den 11 november, som reglerar vissa aspekter av elektroniska förtroendetjänster.

b) SIGNICAT SLU har inte skapat eller infört falska eller vilseledande uppgifter i någon certifikatinformation och har inte heller underlåtit att inkludera nödvändig information som tillhandahållits och verifierats av TECKNAREN.

c) Alla certifikat uppfyller de formella och innehållsmässiga kraven i CPS och PC i SIGNICAT SLU.

d) SIGNICAT SLU har följt de förfaranden som beskrivs i PSC.

SIGNICAT SLU använder rimlig omsorg för att säkerställa att varje produkt som levereras i tillhandahållandet av sina tjänster är fri från datavirus, maskar och annan olaglig kod, och åtar sig att meddela Prenumeranten om eventuella virus, maskar eller annan olaglig kod som senare upptäcks i någon produkt.

– **UNDANTAG FRÅN GARANTIN**

SIGNICAT SLU garanterar inte någon programvara som används av Certifikatutfärdaren eller Undertecknaren, eller någon annan person, för att generera, verifiera eller på annat sätt använda en digital signatur eller ett digitalt certifikat som utfärdats av SIGNICAT SLU, såvida det inte finns ett skriftligt uttalande från SIGNICAT SLU om motsatsen.

– **ANSVARSBEGRÄNSNINGAR FÖR LEVERANTÖRER AV BETRODDA ELEKTRONISKA TJÄNSTER.**

SIGNICAT SLU ska, förutsatt att det sker inom de gränser som fastställs i tillämplig lag, inte hållas ansvarigt för skador som orsakats den person till vilken det har tillhandahållit sina tjänster eller till tredje part i god tro, om den senare drabbas i något av de fall som anges i förordning (EU) 910/2014 eller i följande:

a) Underlåtenhet att förse tillhandahållaren av betrodda tjänster med sanningsenlig, fullständig och korrekt information för tillhandahållandet av den betrodda tjänsten, särskilt om de uppgifter som måste ingå i det elektroniska certifikatet eller som är nödvändiga för dess utfärdande eller för att dess giltighet ska upphöra eller tillfälligt upphävas, när tjänsteleverantören inte kunde upptäcka felaktigheten genom att vidta tillbörlig aktsamhet.

b) Underlåtenhet att utan onödigt dröjsmål underrätta SIGNICAT SLU om alla förändringar i de omständigheter som påverkar tillhandahållandet av betrodda tjänster, särskilt de som återspeglas i det elektroniska certifikatet.

c) Försumlighet när det gäller att bevara din signatur, ditt sigill eller dina autentiseringsuppgifter för webbplatsen, att säkerställa deras konfidentialitet och att skydda eventuell åtkomst till eller röjande av dem eller, i tillämpliga fall, av de medel som ger åtkomst till dem.

d) Att inte begära upphävande eller återkallande av det elektroniska certifikatet i händelse av tvivel om upprätthållandet av sekretessen för dess signaturskapande, försegling eller webbplatsautentiseringsdata eller, i tillämpliga fall, av de medel som ger tillgång till dem.

e) Använd signaturframställnings-, förseglings- eller webbplatsautentiseringsdata när giltighetstiden för det elektroniska certifikatet har löpt ut eller om tillhandahållaren av betrodda tjänster meddelar dig om att giltighetstiden har löpt ut eller upphävts.

SIGNICAT SLU ska inte heller vara skadeståndsskyldig om mottagaren agerar oaktsamt.

Mottagaren skall anses vara försumlig om han/hon underlåter att ta hänsyn till att det elektroniska certifikatets giltighet har upphävts eller förlorats, eller om han/hon underlåter att kontrollera den elektroniska signaturen eller det elektroniska sigillet.

SIGNICAT SLU ska inte vara skadeståndsskyldigt vid felaktighet i de uppgifter som ingår i det elektroniska certifikatet om dessa har styrkts genom en offentlig eller officiell handling, registrerats i ett offentligt register om detta krävs.

- **<u>TECKNARENS ANSVAR</u>**

Abonnenten ska vara ansvarig gentemot varje person för brott mot sina skyldigheter, och i synnerhet för identifiering eller, i förekommande fall, registrering av myndighet, enligt villkoren i dessa villkor.

Abonnenten är ansvarig för all elektronisk kommunikation som autentiserats med hjälp av en digital signatur som genererats med hans / hennes privata nyckel, när certifikatet har verifierats giltigt med hjälp av de mekanismer och villkor som fastställts av SIGNICAT SLU.

Så länge som den fastställda delgivningen av detta dokument inte äger rum, är det under alla omständigheter SUBSCRIBENTEN som bär det ansvar som kan uppstå till följd av obehörig och/eller felaktig användning av certifikaten.

– **LÄMPLIGHETEN HOS PRODUKTER SOM ANVÄNDER IDENTIFIERING, ELEKTRONISK SIGNATUR ELLER KRYPTERING**

SIGNICAT SLU ansvarar inte för lämpligheten av produkter och tjänster relaterade till digital certifiering, identifiering, elektronisk signatur eller kryptering som finns på marknaden och som används i prenumerantens datorapplikationer, förutom när de tillhandahålls av SIGNICAT SLU. I detta fall ska parterna vara bundna av de relevanta användarvillkoren.

– **ÄGANDERÄTT TILL CERTIFIKAT**

De levererade certifikaten förblir prenumerantens egendom.

– **UPPSÄGNING**

Avveckling ska ske i följande fall:

a) För den andra partens åsidosättande av någon av sina skyldigheter, om detta åsidosättande inte har rättats till:

b) Inom trettio dagar från mottagandet av underrättelsen från den part som inte har underlåtit att uppfylla sina skyldigheter.

c) Omedelbart, om bristande efterlevnad äventyrar tjänsternas säkerhet.

d) På grund av sammanträffande av någon annan orsak till förtida uppsägning som fastställs i gällande lagstiftning och särskilt i gällande lagstiftning om elektronisk signatur och digital certifiering.

– **INTEGRITETSPOLICY**

SIGNICAT SLU kan inte avslöja och kan inte tvingas att avslöja någon konfidentiell information om certifikat utan en specifik föregående begäran från:

a) Den person i förhållande till vilken SIGNICAT SLU har en skyldighet att hålla information konfidentiell, eller

b) Ett domstolsbeslut, ett administrativt beslut eller något annat beslut som föreskrivs i gällande lagstiftning.

Abonnenten accepterar dock att viss information, personlig och annan, som tillhandahålls i ansökan om certifikat, kommer att ingå i deras certifikat och i mekanismen för kontroll av certifikatens status, och att ovannämnda information inte kommer att hållas konfidentiell, enligt vad som krävs i lag.

– **ÅTERBETALNINGSPOLICY**

SIGNICAT SLU kommer inte att ersätta kostnaden för certifieringstjänsten i något fall.

– **INFORMATIONENS LAGRINGSTID**

All information i samband med processen för utfärdande av kvalificerade elektroniska certifikat för fysiska personer, inklusive det avtal som vederbörligen formaliserats av prenumeranten, de loggar som genereras under hela utfärdandet, kommer att lagras av SIGNICAT SLU under avtalsförhållandet, så länge radering inte begärs, och under preskriptionstiden för eventuella rättsliga åtgärder som kan uppstå, eller krav som kan tas emot från officiella organ.

I detta avseende ska den maximala perioden för bevarande av relevant information i samband med förfarandet för utfärdande av kvalificerade certifikat vara 15 år från återkallelse eller utgång av certifikatets giltighet, om inte annat föreskrivs i lag. När förhållandet har upphört kommer abonnentens uppgifter att blockeras i enlighet med bestämmelserna i tillämpliga förordningar.

5. ORDINARIE GEMENSAMMA

5.1. PLATS DÄR VERKSAMHETEN UTFÖRS

Platsen för fullgörande av SIGNICAT SLU:s skyldigheter avseende digitala certifieringstjänster och, i förekommande fall, licenser för användning av programvara, är SIGNICAT SLU:s hemvist.

5.2. SKILJBARHET AV VILLKOR OCH BESTÄMMELSER.

Klausulerna i detta dokument är oberoende av varandra, varför, om någon klausul anses ogiltig eller ogenomförbar, de återstående klausulerna ska fortsätta att gälla och genomdrivas, om inte annat uttryckligen överenskommits mellan parterna.

5.3. TILLÄMPLIG LAG OCH BEHÖRIG JURISDIKTION.

Förbindelserna med SIGNICAT SLU ska styras av bestämmelserna i förordning (EU) 910/2014 eIDAS, av spansk lag, och i synnerhet av alla de bestämmelser som följer av SIGNICAT SLU:s efterlevnadspolicy.

Den behöriga jurisdiktionen är den som anges i lag 1/2000 av den 7 januari om civilprocess , utom när sökanden betraktas som en konsument, i vilket fall SIGNICAT SLU kommer att underkasta sig den jurisdiktion som juridiskt motsvarar den.