Allgemeine Nutzungsbedingungen der CA YOUSIGN SAS - QUALIFIED SIGNATURE CA

v1.2.5 | Verteilung: C1 - Öffentlich

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

VERSIONSHISTORIE			
Version	**Gegenstand der Änderung**	**Datum**	**Autor**
1.2.5	Änderung der Firmenbezeichnung von Yousign zu Youtrust (Abschnitt Allgemeine Darstellung und gesamtes Dokument); Neugestaltung des Registrierungsablaufs des Inhabers (Abschnitt Zertifikatstypen, Validierungsverfahren und Nutzungsbeschränkungen); Streichung der Dienste **[Persönliche Identifizierung vor Ort]**: OID 1.2.250.1.302.1.11.1.0 und **[Ferngestützte Identifizierung]**: OID: 1.2.250.1.302.1.15.1.0; Verallgemeinerung der Terminologie "PVID" zu einer anbieterübergreifenden Formulierung; Änderung der Adresse des Gesellschaftssitzes (Abschnitt Kontaktstelle).	2. Juli 2026	Tony DUFOUR
1.2.4	Änderung der Gültigkeitsdauer der Inhaberzertifikate auf 60 Minuten (vorher 15 Minuten).	23. Jan. 2024	Tony DUFOUR
1.2.3	Änderung des Layouts	3. Okt. 2023	Sid Ahmed Remmide
1.2.2	Vervollständigung der Akronyme und Ergänzung der Übersetzungen, soweit zutreffend (Abschnitt Akronyme) Aktualisierung der Postanschrift (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Kontaktstelle) Ersetzung des Begriffs „Kunde“ durch „Inhaber“ (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Zertifikatstypen, Validierungsverfahren und Nutzungsbeschränkungen)	9. Mai 2023	Adrien Van Den Branden Tony Belot

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	Ergänzung eines Verweises auf die Zertifizierungsrichtlinie, in der das Sperrverfahren beschrieben wird, und Streichung der damit redundanten Informationen (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Zertifikatstypen, Validierungsverfahren und Nutzungsbeschränkungen) Ergänzung von Pflichten des Inhabers hinsichtlich der Aufbewahrung und der Weitergabe des privaten Authentifizierungsschlüssels (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Pflichten der Inhaber) Ergänzung der Links zu den CRLs von `YOUSIGN SAS - QUALIFIED SIGNATURE CA` (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Überprüfung des Zertifikatsstatus) Klarstellung zur Grenze der Freistellung von Schadensersatz (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Haftungsbeschränkung) Umbenennung des Unterabschnitts (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Vertraulichkeit) Streichung des lokalen Verweises auf die geltenden Gesetze und Vorschriften (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Vertraulichkeit) Ersetzung der zuständigen Gerichte von Caen durch die Gerichte von Paris (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Anwendbares Recht und Streitbeilegung) Überprüfung des Inhalts des Unterabschnitts und Ergänzung eines Verweises auf die Online-Datenschutzrichtlinie (Abschnitt		

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	Allgemeine Nutzungsbedingungen, Unterabschnitt Verwaltung personenbezogener Daten) Geringfügige Korrekturen von Schreib- und Formulierungsfehlern		
1.2.1	Streichung des qualifizierten Feldes `esi4-qcStatement-5` aus dem Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Audit und Zertifizierung	27. Jan. 2023	Sid Ahmed Remmide
1.2.0	Ergänzung einer Bestimmung zur Annahme dieser ANB durch die Unterzeichner als Voraussetzung für den Erhalt eines Zertifikats (Abschnitt Allgemeine Darstellung) Verweis auf die verschiedenen Zertifizierungsrichtlinien nach OID (Abschnitt Dokumentidentifikation) Ergänzung des Begriffs QSCD (Abschnitt Akronyme) Aktualisierung der Postanschrift des Unternehmens Yousign (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Kontaktstelle) Ergänzung der qualifizierten Zertifikate für die qualifizierte elektronische Signatur des Typs QCP-n-qscd mit der OID 1.2.250.1.302.1.16.1.0 (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitte Zertifikatstypen, Validierungsverfahren und Nutzungsbeschränkungen und Anwendbare Vereinbarungen und Zertifizierungspraktiken) Ergänzung der Pflicht des Inhabers, ein Authentifizierungsmittel zu registrieren, im Fall der OID 1.2.250.1.302.1.11.1.0 (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Zertifikatstypen, Validierungsverfahren und Nutzungsbeschränkungen)	4. Jan. 2023	Tony Belot

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	Ergänzung des Attributs UID in den DNs im Fall der OID 1.2.250.1.302.1.16.1.0 (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Zertifikatstypen, Validierungsverfahren und Nutzungsbeschränkungen) Änderung der Komponente, die für den Vergleich des von der RA übermittelten Namens und Vornamens zuständig ist (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Zertifikatstypen, Validierungsverfahren und Nutzungsbeschränkungen) Klarstellung der Aufbewahrungsdauer der Registrierungsunterlagen der Inhaber (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Nutzungsbeschränkungen) Ergänzung der Pflichten der Inhaber für die OIDs 1.2.250.1.302.1.15.1.0 und 1.2.250.1.302.1.16.1.0 (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Pflichten der Inhaber) Ergänzung der anwendbaren Dokumente im Zusammenhang mit dem PVID (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Anwendbare Vereinbarungen und Zertifizierungspraktiken) Ergänzung der für das Remote QSCD und für das PVID geltenden Qualifizierungen und Zertifizierungen (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Audit und Zertifizierung) Ergänzung der Zertifikatsstufen und der zusätzlichen qualifizierten Felder (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Audit und Zertifizierung) Korrektur von Tippfehlern in den zusätzlichen qualifizierten Feldern		

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	(Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Audit und Zertifizierung)		
1.1.1	Ergänzung der Veröffentlichungsadressen für die Sperrinformationen der CA, zum Beispiel im Fall ihrer Kompromittierung (Abschnitt Überprüfung des Zertifikatsstatus)	28. Juli 2022	Tony Belot
1.1.0	Änderung des Layouts Ergänzung der ferngestützten Identifizierung Aktualisierung der Klausel "Verwaltung personenbezogener Daten" hinsichtlich der Rechte des Inhabers Zertifikatsprüfung ergänzt im Zusammenhang mit der eIDAS Trusted List Aktualisierung und Vervollständigung der Pflichten des Inhabers Korrektur der Veröffentlichungs-URLs der CRLs Klarstellung der Kontaktdaten für die Übermittlung von Sperranträgen	27. Mai 2022	Tony Belot
1.0.4	Aktualisierung der Akronyme Änderung der Kontakt-E-Mail-Adresse der Zertifizierungsstelle Aktualisierung der Klausel "Haftungsbeschränkung" Ergänzung der Klauseln "Verwaltung personenbezogener Daten" und "Sprache"	21. Dez. 2020	yves.rocha@yousign.com
1.0.3	Aktualisierung von Überprüfung des Zertifikatsstatus. Klarstellung zur OCSP-Antwort.	22. Sep. 2020	Kévin Dubourg
1.0.2	Änderung des Layouts	18. Aug. 2020	Florent Eudeline
1.0.1	Aktualisierung der Verantwortlichkeiten des Inhabers und Ergänzung eines	2. Nov. 2018	Antoine Louiset

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	Signaturtests bei der Registrierung des Inhabers		
1.0.0	Erstellung des Dokuments	25. Sep. 2018	Antoine Louiset

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

Inhaltsverzeichnis

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

1. Einleitung

1.1. Allgemeine Darstellung

Das Unternehmen Youtrust ist ein Anbieter von elektronischen Zertifizierungsdiensten (ECSP), der seinen Kunden und für den eigenen Gebrauch Dienste bereitstellt, die elektronische Zertifikate und insbesondere eine elektronische Signatur umfassen.

In diesem Rahmen bildet dieses Dokument die Allgemeinen Nutzungsbedingungen für die von der Zertifizierungsstelle „YOUSIGN SAS - QUALIFIED SIGNATURE CA“ ausgestellten Zertifikate. Dieses Dokument stellt die Modalitäten der Zertifikatsverwaltung sowie die Verpflichtungen und Pflichten der verschiedenen Parteien dar.

Der Zertifikatsinhaber nimmt diese Allgemeinen Nutzungsbedingungen in der Phase der Zertifikatsanforderung ausdrücklich an. Andernfalls kann ihm von der Zertifizierungsstelle „YOUSIGN SAS - QUALIFIED SIGNATURE CA“ kein Zertifikat ausgestellt werden.

Das Unternehmen Youtrust trug bis zum 01.07.2026 den Namen Yousign; zu diesem Datum wurde seine Firmenbezeichnung im Handels- und Gesellschaftsregister (RCS) ohne Änderung der SIREN-Nummer geändert. Daher tragen die Zertifizierungsstellen den Namen Yousign und behalten eine zutreffende Kennung der juristischen Person Youtrust.

1.2. Dokumentidentifikation

Diese „Allgemeinen Nutzungsbedingungen“ beziehen sich auf die CA „YOUSIGN SAS - QUALIFIED SIGNATURE CA“, die Zertifikate gemäß ihrer Zertifizierungsrichtlinie ausstellt.

Die Zertifikatsprofile werden durch ihre jeweiligen OIDs identifiziert:

- **[Qualifizierte Signatur]** : OID 1.2.250.1.302.1.16.1.0

Weitere, deutlichere Elemente (Name, Versionsnummer, Aktualisierungsdatum) ermöglichen ebenfalls seine Identifizierung.

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

1.3. Akronyme

Akronym	Bedeutung	Übersetzung
CA	Certification Authority	-
RA	Registration Authority	-
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information	Französische Nationalagentur für die Sicherheit von Informationssystemen
ANB	Allgemeine Nutzungsbedingungen	-
DN	Distinguished Name	Eindeutiger Name
CPS	Certification Practice Statement	Erklärung zu den Zertifizierungspraktiken
DPO	Data Protection Officer (Datenschutzbeauftragter)	-
eIDAS	electronic IDentification, Authentication and trust Services	Elektronische Identifizierung und Vertrauensdienste
PKI	Public Key Infrastructure	Public-Key-Infrastruktur
ARL	Authority Revocation List	Sperrliste der CA-Zertifikate
CRL	Certificate Revocation List	Zertifikatssperrliste
OCSP	Online Certificate Status Protocol	Online-Protokoll zur Abfrage des Zertifikatsstatus
OID	Object Identifier	Objektkennung
CP	Certificate Policy	Zertifizierungsrichtlinie
PVID	Prestataire de Vérification d'Identité à Distance	Anbieter für die Fernidentitätsprüfung
QCP-n	Policy for EU qualified certificate issued to a natural person (Richtlinie für an eine natürliche Person ausgestellte qualifizierte EU-Zertifikate)	-

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

Akronym	Bedeutung	Übersetzung
QSCD	Qualified Signature Creation Device	Qualifizierte elektronische Signaturerstellungseinheit

2. Allgemeine Nutzungsbedingungen

Diese ANB beruhen auf der in Anhang A der Norm EN 319 411-1 (Version 1.3.1) vorgesehenen Vorlage.

Kontaktstelle	Youtrust Verwaltung der CA Yousign 36 rue de Saint Petersbourg 75008 Paris authority@yousign.com
Zertifikatstypen, Validierungsverfahren und Nutzungsbeschränkungen	Die von diesen ANB erfassten Zertifikate werden von der folgenden Zertifizierungsstellen-Kette ausgestellt: ● Wurzel-CA: „YOUSIGN SAS - ROOT2 CA“ ○ Ausstellende CA: „YOUSIGN SAS - QUALIFIED SIGNATURE CA“ Die CA stellt flüchtige qualifizierte Zertifikate aus, die gemäß dem Verfahren für die ferngestützte qualifizierte elektronische Signatur oder die fortgeschrittene elektronische Signatur im Sinne der eIDAS-Verordnung verwendet werden. Die qualifizierten Zertifikate für die ferngestützte qualifizierte elektronische Signatur werden nach einer erstmaligen ferngestützten Identitätsprüfung ausgestellt. Der private Schlüssel des Inhabers wird in einer qualifizierten Fernsignaturerstellungseinheit (Remote QSCD) erzeugt und verwendet. Der Inhaber kann ein starkes Authentifizierungsmittel registrieren, das den Anforderungen an elektronische Identifizierungsmittel des Sicherheitsniveaus „substanziell“ entspricht und den Erhalt neuer Zertifikate für die ferngestützte qualifizierte elektronische Signatur ermöglicht. Diese Zertifikate tragen die OID 1.2.250.1.302.1.16.1.0; sofern Regeln speziell für diesen Zertifikatstyp gelten, werden sie in diesem Dokument durch den Hinweis **[Qualifizierte Signatur]**.

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

Die Zertifikate dürfen ausschließlich im Rahmen des von Youtrust angebotenen Signaturdienstes verwendet werden, um ein Dokument oder eine Nachricht in allen Bereichen zu signieren, in denen eine Signatur zum Nachweis der Gültigkeit oder als Beweismittel erforderlich ist, und insbesondere:

- elektronische Signatur durch einen Inhaber und anschließende Überprüfung dieser Signatur durch eine Verwaltung oder ein Unternehmen auf elektronischem Weg;
- elektronische Signatur durch einen Inhaber und anschließende Überprüfung dieser Signatur durch eine natürliche Person.

Eine solche elektronische Signatur belegt neben der Authentizität und der Integrität der so signierten Daten die Willenserklärung des Unterzeichners in Bezug auf den Inhalt dieser Daten. Die qualifizierte elektronische Signatur gilt zudem als vertrauenswürdig und ist nach der eIDAS-Verordnung einer handschriftlichen Unterschrift gleichgestellt.

Der Inhaber ist eine natürliche Person.

Die DNs sind wie folgt aufgebaut:

Attribut	**Beschreibung**	**Vorhandensein**
CN	commonName: Name und Vorname des Inhabers	Ja
SN	surname: Name des Inhabers	Ja
GN	givenName: Vorname des Inhabers	Ja
OI	organizationIdentifier: Kennung der Einheit, mit der der Inhaber verbunden ist, nach der eIDAS-Syntax: NTRFR-<SIREN-Nummer>	Nur bei Verbindung mit einer juristischen Person
OU	organizationUnit: Kennung der Einheit, mit der der Inhaber	

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	verbunden ist, nach der RGS-Syntax: 0002 <SIREN-Nummer>	
O	organizationName: Name der Einheit, mit der der Inhaber verbunden ist	
C	countryName: Land der Registrierungsstelle von Youtrust, immer gleich FR (Frankreich)	Ja
SerialNumber	serialNumber: Datum und Uhrzeit des Beginns der Zertifikatserzeugung.	Ja
UID	userIdentifier: Transaktionskennung des Unterzeichners in der Infrastruktur von Youtrust.	Nur [Qualifizierte Signatur]

Die von der CA „YOUSIGN SAS - QUALIFIED SIGNATURE CA“ ausgestellten Testzertifikate sind unmittelbar durch das Hinzufügen des Präfixes „TEST – “ im Wert des Attributs CN erkennbar, zum Beispiel:
CN = TEST – Jean DUPONT,...

Abgesehen von dieser Besonderheit folgen die von der CA „YOUSIGN SAS - QUALIFIED SIGNATURE CA“ ausgestellten Testzertifikate denselben Verfahren wie die Zertifikate des regulären Produktivbetriebs.

Der Einsatz eines qualifizierten Zertifikats erfordert ein Verfahren zur Überprüfung der Identität des Inhabers.

1. **Fall der Validierung mit einem physischen Identitätsdokument**

Die erstmalige Validierung der Identität des Inhabers erfolgt auf der Website der RA im Rahmen einer ferngestützten Identifizierung. Das ferngestützte Prüfverfahren umfasst die folgenden Schritte:

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	• der Inhaber verbindet sich über einen an seine E-Mail-Adresse übermittelten eindeutigen Link mit der Website der RA und muss sicherstellen, dass er über ein Smartphone mit Kamera verfügt;
	• die RA zeigt dem Inhaber die für seine Zertifikatsanforderung verwendeten Identitätsangaben an:
	  ○ Name und Vorname;
	  ○ E-Mail-Adresse;
	• der Inhaber bestätigt, die geltenden Allgemeinen Nutzungsbedingungen zur Kenntnis genommen zu haben, und erklärt sich bereit, sie ohne Vorbehalt zu unterzeichnen;
	• der Inhaber bestätigt die Richtigkeit der dargestellten Angaben und willigt ein, das auf dieser Grundlage erstellte Zertifikatsantragsformular zu unterzeichnen;
	• befindet sich der Inhaber nicht auf einem mobilen Gerät, wird er aufgefordert, seine Identifizierung auf einem mobilen Gerät (mit Kamera) fortzusetzen, über einen zu scannenden QR-Code oder über den Empfang einer SMS;
	• die ferngestützte Identitätsprüfung wird von einem zertifizierten PVID-Dienstleister durchgeführt (mit einer Validierung durch einen menschlichen Bearbeiter) und umfasst die folgenden Schritte:
	  ○ der Inhaber nimmt die ANB und die Datenschutzrichtlinie des PVID-Dienstes an und willigt in die Verarbeitung seiner biometrischen Daten ein, damit das PVID seine Identität feststellen kann;

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	○ der Inhaber stellt sicher, dass er über ein Smartphone verfügt, das die vom PVID dargelegten Anforderungen erfüllt; ○ der Inhaber legt der Kamera ein gültiges amtliches Identitätsdokument aus den folgenden Nachweisen vor: ○ den Personalausweis; ○ den Reisepass; ○ den Aufenthaltstitel; und folgt den vom PVID nacheinander erteilten Anweisungen; ○ das PVID prüft die Gültigkeit und die Echtheit des vorgelegten Dokuments und entnimmt ihm die Identitätsangaben des Inhabers; ○ das PVID fordert den Inhaber auf, sein Gesicht der Kamera zu zeigen und die ihm dynamisch erteilten Anweisungen zu befolgen; ○ der Inhaber folgt den vom PVID nacheinander erteilten Anweisungen; ○ das PVID stellt sicher, dass das Gesicht des Inhabers mit dem Foto auf dem Identitätsdokument übereinstimmt; ○ das PVID übermittelt das Ergebnis der Identitätsprüfung an die RA. Das endgültige Ergebnis des PVID wird asynchron übermittelt, nachdem die Elemente von einem menschlichen Bearbeiter geprüft wurden.

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	2. Fall der Validierung einer Identität mithilfe eines elektronischen Identifizierungsmittels
	
	Die erstmalige Validierung der Identität des Inhabers erfolgt auf der Website oder in der mobilen Anwendung des Anbieters des elektronischen Identifizierungsmittels. Das ferngestützte Prüfverfahren umfasst die folgenden Schritte:
	• der Inhaber muss vorab über ein von der RA unterstütztes und aktives elektronisches Identifizierungsmittel verfügen;
	• der Inhaber verbindet sich über einen an seine E-Mail-Adresse übermittelten eindeutigen Link mit der Website der RA;
	• die RA zeigt dem Inhaber die für seine Zertifikatsanforderung verwendeten Identitätsangaben an:
	  ○ Name und Vorname;
	  ○ E-Mail-Adresse;
	• der Inhaber bestätigt, die geltenden Allgemeinen Nutzungsbedingungen zur Kenntnis genommen zu haben, und erklärt sich bereit, sie ohne Vorbehalt zu unterzeichnen;
	• der Inhaber bestätigt die Richtigkeit der dargestellten Angaben und willigt ein, das auf dieser Grundlage erstellte Zertifikatsantragsformular zu unterzeichnen;
	• der Inhaber wird zu einer Webseite oder einer Anwendung des Anbieters des elektronischen Identifizierungsmittels weitergeleitet;
	• der Inhaber muss sich beim Anbieter des elektronischen Identifizierungsmittels authentifizieren;

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	• der Anbieter des elektronischen Identifizierungsmittels übermittelt das Ergebnis der Identitätsprüfung an die RA. Die RA archiviert sodann das unterzeichnete Zertifikatsantragsformular, die unterzeichneten ANB sowie die Nachweise der Identitätsprüfung des Inhabers. Im Anschluss an diese erstmalige Identitätsprüfung kann der Inhaber ein Authentifizierungsmittel registrieren, das ihm ermöglicht, später neue qualifizierte Zertifikate für die qualifizierte Signatur zu erhalten, ohne die erstmalige Identitätsprüfung zu wiederholen. Fehlt ein solches Mittel, muss der Unterzeichner bei seiner nächsten qualifizierten elektronischen Signatur eine neue erstmalige Identitätsprüfung durchführen. Die im flüchtigen Zertifikat, das bei jeder Signatur erzeugt wird, enthaltenen Identitätsangaben sind diejenigen, die durch die ferngestützte Identifizierung validiert wurden. Diese Angaben bleiben für eine Dauer von höchstens 3 Jahren gültig, bevor der Inhaber die Identitätsangaben erneut validieren lassen muss; diese Dauer ist entsprechend dem Ablaufdatum des Identitätsdokuments oder des bei der Ausgabe des Authentifizierungsmittels vorgelegten elektronischen Identifizierungsmittels zu verkürzen. Es liegt in der Verantwortung des Inhabers, eine Aktualisierung der Identitätsangaben zu verlangen, wenn diese vor Ablauf der Dauer von 3 Jahren nicht mehr aktuell sind. Der Inhaber muss in den folgenden Fällen einen Antrag auf Sperrung seines Authentifizierungsmittels stellen: • sein privater Schlüssel steht im Verdacht, kompromittiert zu sein, ist kompromittiert oder ist verloren gegangen (gegebenenfalls samt der zugehörigen Aktivierungsdaten); • sein Authentifizierungsmittel zur Autorisierung einer Signaturtransaktion wurde kompromittiert oder steht im Verdacht, kompromittiert zu sein. Ein Sperrantrag gewährleistet dem Inhaber, dass mit seinem aktuellen Authentifizierungsmittel keine neue Signatur mehr zugelassen wird.

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

Nutzungsbeschränkungen	Die ausgestellten Zertifikate sind ausschließlich für Signaturtransaktionen verwendbar, die von der Infrastruktur von Youtrust abgewickelt werden. Die Zertifikate der Inhaber haben eine Gültigkeitsdauer von 120 Minuten. Die entsprechenden privaten Schlüssel haben eine Lebensdauer, die der Dauer des Signaturvorgangs entspricht. Youtrust bewahrt die Registrierungsunterlagen der Inhaber 10 Jahre lang auf (20 Jahre für Zertifikate, die im Rahmen eines von einem in Italien niedergelassenen Kunden von Youtrust angestoßenen elektronischen Signaturvorgangs ausgestellt wurden). Youtrust bewahrt die Protokolle und Aufzeichnungen zur Ausstellung und Verwendung der privaten Schlüssel der Inhaber 17 Jahre lang auf.
Pflichten der Inhaber	Der Inhaber berücksichtigt die folgenden Anforderungen: ● sich zu verpflichten, im Registrierungsverfahren aktuelle und gültige Identitätsangaben bereitzustellen; ● die Pflichten in Bezug auf den Dienst der ferngestützten Identitätsprüfung einzuhalten, die vom Anbieter der ferngestützten Identitätsprüfung auferlegt werden; ● das von der CA ausgestellte Zertifikat stillschweigend anzunehmen, indem er die Erstellung der Signatur bestätigt, nach Validierung des Antragsformulars und Annahme der ANB; ● die Aufbewahrung der Informationen der Registrierungsunterlagen und der Verwaltung seiner Signaturschlüssel durch die CA zu akzeptieren; ● sich zu verpflichten, das von der RA ursprünglich registrierte starke Authentifizierungsmittel zu verwenden; ● das Signaturzertifikat unter Beachtung der vorgesehenen Nutzungsbeschränkungen einzusetzen; ● um die ausschließliche Kontrolle über seinen privaten Signaturschlüssel zu gewährleisten, und im Fall der Registrierung eines Authentifizierungsmittels muss der Inhaber: ○ eine robuste Authentifizierung auf seinem Telefon einrichten (PIN-Code oder Passwort, mit Begrenzung der Anzahl der Entsperrversuche); ○ sein Telefon niemals verleihen, auch nicht an eine Vertrauensperson; ○ im Fall von Verlust oder Diebstahl die vom Telefonanbieter empfohlenen Maßnahmen anwenden (zum Beispiel Fernlöschung) und die

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	Identität durch Kontaktaufnahme mit Youtrust sperren lassen; ○ im Fall der endgültigen Weitergabe des Telefons an einen Dritten (Verkauf, Übertragung usw.) die vom Telefonanbieter empfohlenen Maßnahmen zu dessen Zurücksetzung anwenden und Youtrust zur Sperrung der Identität kontaktieren; ○ sein Telefon aktuell halten, indem er die von seinem Hersteller und vom Anbieter des Betriebssystems bereitgestellten Software-Aktualisierungen installiert; ○ auf dem Telefon nur Anwendungen installieren, die in den offiziellen Stores des Betriebssystems veröffentlicht sind, potenziell gefährliche Anwendungen (einschließlich Jailbreak-Werkzeuge) vermeiden und die installierten Anwendungen aktuell halten; ○ seinen privaten Authentifizierungsschlüssel und alle weiteren Informationen zu seiner Identität auf seinem Telefon vertraulich aufbewahren; ○ seinen privaten Authentifizierungsschlüssel oder alle weiteren Informationen zu seiner Identität nicht auf einem anderen Telefon oder Gerät weitergeben, selbst wenn dieses andere Telefon oder Gerät dem Inhaber oder einer anderen Person, einschließlich einer Vertrauensperson, gehören sollte. Jede nach einer Authentifizierung auf dem Telefon erstellte Signatur gilt als vom Inhaber geleistet, der dieses Telefon registriert hat; der Grundsatz der Nichtabstreitbarkeit erlaubt es dem Inhaber nicht, die Unterzeichnung zu bestreiten. ● sich zu verpflichten, die CA zu benachrichtigen, wenn einer der folgenden Sperrgründe vorliegt: ○ die in seinem Zertifikat enthaltenen Angaben stimmen nicht mehr mit der Identität oder der im Zertifikat vorgesehenen Verwendung überein, und dies vor dem regulären Ablauf des Zertifikats; ○ in seinen Registrierungsunterlagen wurde ein Fehler (absichtlich oder nicht) festgestellt; ○ der private Schlüssel des Inhabers steht im Verdacht, kompromittiert zu sein, ist kompromittiert oder ist verloren gegangen

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	(gegebenenfalls samt der zugehörigen Aktivierungsdaten); ○ sein Authentifizierungsmittel zur Autorisierung einer Signaturtransaktion wurde kompromittiert oder steht im Verdacht, kompromittiert zu sein; ● sich zu verpflichten, den Status des ausgestellten Signaturzertifikats über die von der CA veröffentlichten CRLs und den eingerichteten OCSP-Dienst zu überprüfen; ● das Signaturzertifikat unter den in der CP vorgesehenen und in diesen ANB übernommenen Nutzungsbedingungen zu verwenden.
Pflichten der CA	Youtrust ist verantwortlich für: ● die Validierung und die Veröffentlichung der CP, der CPS und der ANB der CA; ● die Konformität der ausgestellten Zertifikate mit der CP; ● die Einhaltung aller Sicherheitsgrundsätze durch die verschiedenen Komponenten und die zugehörigen Kontrollen; ● im Fall eines schwerwiegenden Vorfalls (zum Beispiel Verlust, Verdacht der Kompromittierung, Kompromittierung oder Diebstahl des privaten Schlüssels zur Zertifikatsverwaltung) die Meldung des Vorfalls an die ANSSI (supervision-eIDAS@ssi.gouv.fr). Youtrust haftet für alle schädigenden Folgen, die aus der eigenen Nichteinhaltung dieses Dokuments entstehen. Sofern nicht nachgewiesen wird, dass Youtrust kein vorsätzliches Verschulden und keine Fahrlässigkeit begangen hat, haftet Youtrust für jeden Schaden, der einer natürlichen oder juristischen Person entsteht, die sich in vertretbarer Weise auf die ausgestellten Zertifikate verlässt, in jedem der folgenden Fälle: ● die im Zertifikat enthaltenen Angaben entsprechen nicht den bei der Registrierung bereitgestellten Angaben; ● bei der Ausstellung des Zertifikats wurde nicht überprüft, ob der Inhaber den entsprechenden privaten Schlüssel besitzt; ● die CA hat die Sperrung eines Zertifikats nicht erfassen lassen und diese Information nicht im Einklang mit ihren Verpflichtungen veröffentlicht. Youtrust haftet nicht für Schäden, die durch eine Verwendung des Zertifikats entstehen, die die für seine Nutzung

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	festgelegten Grenzen überschreitet. Bei Einstellung der Tätigkeit der CA werden die ausgestellten und noch innerhalb ihrer Gültigkeitsdauer befindlichen Zertifikate gesperrt. Schließlich haftet Youtrust im Fall eines Verschuldens oder einer Fahrlässigkeit bei den Vorsichtsmaßnahmen, die hinsichtlich der Vertraulichkeit der ihr von den Inhabern anvertrauten personenbezogenen Daten zu treffen sind.
Überprüfung des Zertifikatsstatus	Der Nutzer eines Zertifikats ist verpflichtet, den Status der Zertifikate zu überprüfen, einschließlich derjenigen der entsprechenden Vertrauenskette. Die CA stellt den Nutzern eine aktuelle CRL zur Verfügung, die im Internet unter folgender Adresse veröffentlicht wird: • http://crl.yousign.fr/crl/yousignsasqualifsignca.crl • http://crl2.yousign.fr/crl/yousignsasqualifsignca.crl • http://crl3.yousign.fr/crl/yousignsasqualifsignca.crl Youtrust betreibt zudem einen OCSP-Dienst, der unter folgender Adresse erreichbar ist: http://ocsp.yousign.fr. Diese Informationen sind sieben Tage in der Woche, vierundzwanzig Stunden am Tag verfügbar, mit einer Verfügbarkeit von 99,7 % über einen Monat. Die CRL enthält die Erweiterung „ExpiredCertsOnCRL“ und bewahrt die Seriennummern aller gesperrten Zertifikate auf, auch derjenigen, die abgelaufen sind. Der OCSP-Dienst setzt die Erweiterung „archive cutoff“ gemäß RFC 6960 um, mit einem Datum, das dem Beginn der Gültigkeit des CA-Zertifikats entspricht, und hält den Sperrstatus des Zertifikats auch nach dessen Ablauf verfügbar. Enthält die OCSP-Anfrage eine Abfrage zu einer Seriennummer, die nicht von der CA ausgestellt wurde, so setzt der OCSP-Server in die entsprechende Antwort den Status „unknown“. Enthält die OCSP-Anfrage eine Abfrage zu einer von der CA ausgestellten Seriennummer, so entspricht die OCSP-Antwort den IETF-Standards RFC 6960.

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	Die von der CA ausgestellten Zertifikate sind qualifizierte Zertifikate im Sinne der eIDAS-Verordnung. Dies ist auf Grundlage der von der ANSSI veröffentlichten Vertrauensliste (Trusted List) unter https://www.ssi.gouv.fr/eidas/TL-FR.xml zu überprüfen. Diese Liste muss insbesondere das Zertifikat der CA und deren Qualifizierungsstatus enthalten. Im Fall der Sperrung der CA, zum Beispiel infolge einer Kompromittierung ihres privaten Schlüssels, wird die Sperrinformation in einer ARL veröffentlicht, die unter folgender Adresse verfügbar ist: ● http://crl.yousign.fr/crl/yousignsasroot2ca.crl ● http://crl2.yousign.fr/crl/yousignsasroot2ca.crl ● http://crl3.yousign.fr/crl/yousignsasroot2ca.crl Im Fall des Betriebsendes der CA erzeugt Youtrust: ● eine letzte CRL, deren Ablaufdatum auf den Wert 99991231235959Z gesetzt wird; ● eine letzte OCSP-Antwort wird für jedes ausgestellte Zertifikat vorab erzeugt und enthält ein Ende-der-Gültigkeit-Datum, das auf den Wert 99991231235959Z gesetzt wird. Stellt Youtrust die Tätigkeit der CA ein, so verpflichtet sich das Unternehmen, die CRLs und die vorab erzeugten OCSP-Antworten verfügbar zu halten.
Haftungsbeschränkung	Youtrust kann nicht für eine unbefugte oder nicht konforme Verwendung der Authentifizierungsdaten, der Zertifikate, der CRLs sowie sonstiger bereitgestellter Ausrüstung oder Software haftbar gemacht werden. Youtrust lehnt jede Haftung für Schäden ab, die aus Fehlern oder Unrichtigkeiten der in den Zertifikaten enthaltenen Angaben entstehen, wenn diese Fehler oder Unrichtigkeiten unmittelbar auf die Fehlerhaftigkeit der vom Inhaber mitgeteilten Angaben zurückzuführen sind. In jedem Fall und im streng nach anwendbarem Recht zulässigen Umfang ist Youtrust nicht zur Zahlung von Schadensersatz gleich welcher Art verpflichtet, sei er unmittelbar, materiell, wirtschaftlich, finanziell oder immateriell, der sich aus der Durchführung dieser Bedingungen ergibt.

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

Anwendbare Vereinbarungen und Zertifizierungspraktiken	Die Zertifizierungsrichtlinien, in denen die Anforderungen beschrieben werden, die die CA einzuhalten beabsichtigt, sind unter folgender Adresse veröffentlicht: https://yousign.fr/fr/public/document, Die Dienstrichtlinie und die Nutzungsbedingungen des Dienstes der ferngestützten Identitätsprüfung des Partners von Youtrust sind anwendbar.
Vertraulichkeit	Als vertraulich gelten mindestens die folgenden Informationen: • die internen Verfahren der CA; • die privaten Schlüssel der CA, der Komponenten und der Zertifikatsinhaber; • die den privaten Schlüsseln der CA und der Inhaber zugeordneten Aktivierungsdaten; • alle Geheimnisse der PKI; • die Ereignisprotokolle der PKI-Komponenten; • die Registrierungsunterlagen der Inhaber; • die Sperrgründe, sofern der Inhaber nicht ausdrücklich zustimmt. Youtrust wendet Sicherheitsverfahren an, um die Vertraulichkeit dieser Informationen zu gewährleisten. Youtrust verpflichtet sich, die geltenden Gesetze und Vorschriften einzuhalten.
Versicherungspolitik	Youtrust bestätigt, Inhaberin einer Versicherungspolice zu sein, die ihre Berufshaftpflicht abdeckt. Sie verpflichtet sich, diese Versicherungspolice für die gesamte Dauer ihrer Berufstätigkeit in Kraft zu halten.
Sprache	Diese ANB wurden in mehreren Sprachen erstellt, darunter Französisch. Auslegungssprache ist im Fall eines Widerspruchs oder einer Streitigkeit über die Bedeutung eines Begriffs oder einer Bestimmung die französische Sprache.
Anwendbares Recht und Streitbeilegung	Diese ANB unterliegen französischem Recht und werden nach französischem Recht ausgelegt. Im Fall einer Streitigkeit zwischen den Parteien, die sich aus der Auslegung, der Anwendung und/oder der Durchführung des Vertrags ergibt, und in Ermangelung einer gütlichen Einigung zwischen den vorgenannten Parteien wird die

Dieses Dokument ist ausschließliches Eigentum von Youtrust.

	ausschließliche Zuständigkeit den Gerichten von Paris zugewiesen.
Verwaltung personenbezogener Daten	Youtrust verpflichtet sich, die geltenden Gesetze und Vorschriften zur Verwaltung personenbezogener Daten einzuhalten, insbesondere die Europäische Verordnung Nr. 2016/679 vom 27. April 2016, die sogenannte „Datenschutz-Grundverordnung“ (DSGVO). Der Inhaber wird darauf hingewiesen, dass die Ausstellung elektronischer Zertifikate und die Durchführung des elektronischen Signaturvorgangs die Verarbeitung personenbezogener Daten durch Youtrust erfordern. Der Inhaber wird gebeten, die Datenschutzrichtlinie zu konsultieren, um weitere Informationen darüber zu erhalten, wie seine personenbezogenen Daten verarbeitet werden und wie er seine Rechte ausüben kann.
Audit und Zertifizierung	Das von Youtrust für die CA und die fortgeschrittene elektronische Signatur verwendete kryptografische Modul ist von der ANSSI qualifiziert. Die Einheit zur Erstellung qualifizierter elektronischer Signaturen ist eine qualifizierte Fernsignaturerstellungseinheit („Remote QSCD“), die nach der eIDAS-Verordnung qualifiziert ist. Der Dienst der ferngestützten Identitätsprüfung ist von der ANSSI auf dem Sicherheitsniveau „substanziell“ oder „hoch“ zertifiziert. Die Zertifikate entsprechen der Norm ETSI 319 411-2 und sind im Sinne der eIDAS-Verordnung von der ANSSI qualifiziert. Die Zertifikate haben die Stufe QCP-n-qscd. Die Zertifikate enthalten die folgenden qualifizierten Felder: • esi4-qcStatement-4 = id-etsi-qcs-QcSSCD • esi4-qcStatement-1 = id-etsi-qcs-QcCompliance • esi4-qcStatement-6 = id-etsi-qct-esign

Dieses Dokument ist ausschließliches Eigentum von Youtrust.