Allgemeine Nutzungsbedingungen der von der CA YOUSIGN SAS – SIGN3 CA ausgestellten Serversiegel-Zertifikate

v1.0.2 | Verteilung: C1 – Öffentlich

VERSIONSHISTORIE			
Version	**Gegenstand der Änderung**	**Datum**	**Autor**
1.0.2	Ergänzung der PKI Disclosure Statements (Abschnitt Allgemeine Darstellung) Ergänzung der OID für qualifizierte Siegel (Abschnitt Dokumentidentifikation) Aktualisierung der Definition des Zertifikatsnehmers (Abschnitt Definitionen) Ergänzung eines Absatzes zu den Pflichten der CA (Abschnitt Pflichten der CA) Ergänzung der Auswahlkriterien für kryptografische Module für die OID für qualifizierte Siegel (Abschnitt Audits und anwendbare Referenzen)	14. Mai 2025	Tony BELOT Tony DUFOUR
1.0.1	Änderungen der Pflichten zur Überprüfung der Zertifikate durch die Nutzer (Abschnitte Pflichten der Subjekteinheit und des gesetzlichen Vertreters und Pflichten des Zertifikatsnehmers und des RCC)	28. Juni 2024	Jean VERRONS
1.0.0	Ergänzung der Definition des Begriffs „Zertifikatsnehmer“ (Abschnitt Definitionen) Einführung des Begriffs „Subjekteinheit“ und des möglichen Unterschieds zwischen dieser Einheit und dem Zertifikatsnehmer (Abschnitte Definitionen, Art der ausgestellten Zertifikate, Modalitäten des Erhalts, Nutzungsbeschränkungen, Pflichten der Subjekteinheit und des gesetzlichen Vertreters, Pflichten des Zertifikatsnehmers und des RCC und Pflichten zur Überprüfung der Zertifikate durch die Nutzer)	13. Juli 2023	Tony Belot

VERSIONSHISTORIE			
Version	**Gegenstand der Änderung**	**Datum**	**Autor**
	Ersetzung des Begriffs „Inhaber“ durch präzisere Begriffe, die entweder den Zertifikatsnehmer oder seinen gesetzlichen Vertreter oder die Subjekteinheit oder den RCC bezeichnen (Abschnitte Modalitäten des Erhalts, Pflichten der Subjekteinheit und des gesetzlichen Vertreters und Pflichten des Zertifikatsnehmers und des RCC) Klarstellung der Verantwortlichkeiten des Zertifikatsnehmers (und seines RCC) und der Subjekteinheit (und ihres gesetzlichen Vertreters) sowie ihrer Beziehungen (Abschnitte Allgemeine Darstellung, Pflichten der Subjekteinheit und des gesetzlichen Vertreters, Pflichten des Zertifikatsnehmers und des RCC, Haftungsbeschränkung, Verwaltung personenbezogener Daten und Beweisvereinbarung) Aktualisierung der Links zur öffentlichen Dokumentation (Abschnitte Art der ausgestellten Zertifikate und Referenzdokumente) Abstimmung des Zwecks der Zertifikate zwischen den ANB und der CP (Abschnitt Zweck der Zertifikate) Verlagerung der Modalitäten für Verwaltung, Speicherung, Schutz und Besitznachweis des privaten Schlüssels in die CP (Abschnitt Modalitäten des Erhalts) Änderung des Begriffs „Server“ zu „Anwendungsdienst“ (Abschnitt Pflichten des Zertifikatsnehmers und des RCC)		

VERSIONSHISTORIE			
Version	**Gegenstand der Änderung**	**Datum**	**Autor**
	Verlagerung der URLs zu den CRLs und zur ARL in die CP (Abschnitte Pflichten zur Überprüfung der Zertifikate durch die Nutzer und Überprüfung des Zertifikatsstatus) Geringfügige syntaktische und formale Korrekturen		
0.0.1	Erstellung des Dokuments, erzeugt aus den Allgemeinen Nutzungsbedingungen der CA - YOUSIGN SAS - SIGN2 CA für Siegelzertifikate, Version 1.0.1, mit den folgenden Änderungen: • Änderung der Verweise auf die CA Sign2 zu Sign3, Aktualisierung der OID und der CRL-Adressen • Vervollständigung der Akronyme und Ergänzung der Übersetzungen, soweit zutreffend (Abschnitt Akronyme) • Ergänzung eines Abschnitts für die Definitionen (Abschnitt Definitionen) • Klarstellung zur Identifikation des Dokuments (Abschnitt Dokumentidentifikation) • Ergänzung der anwendbaren ETSI-Norm und der Zertifikatsstufe (Abschnitt Dokumentidentifikation) • Aktualisierung der Kontaktadresse der CA (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Kontakt der Zertifizierungsstelle) • Streichung des Beispiels der Verwendung der Zertifikate für eine einfache elektronische Signatur einer natürlichen Person (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Zweck der Zertifikate)	23. Juni 2023	Tony Belot

VERSIONSHISTORIE			
Version	**Gegenstand der Änderung**	**Datum**	**Autor**
	• Klarstellung und Vereinfachung der Rollen des RCC und des gesetzlichen Vertreters, Verlagerung des Inhalts der Registrierungsunterlagen und der zulässigen Nachweise in die CP (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Modalitäten des Erhalts) • Ergänzung der systematischen Übermittlung des Zertifikats an den Inhaber nach dessen Erzeugung und Streichung der Möglichkeit späterer Anfragen (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Modalitäten des Erhalts) • Klarstellung der Modalitäten für Speicherung, Verwendung und Schutz der privaten Schlüssel (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Modalitäten des Erhalts) • Streichung der Sperrkanäle per Post und Telefon, Verlagerung der Einzelheiten des Sperrverfahrens in die CP (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Modalitäten der Sperrung) • Klarstellung des zur Verwendung des Zertifikats berechtigten Dienstes (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Nutzungsbeschränkungen) • Verstärkung der Pflichten des Inhabers und Klarstellung der für die Erneuerung der Zertifikate		

VERSIONSHISTORIE			
Version	**Gegenstand der Änderung**	**Datum**	**Autor**
	erforderlichen Vorlaufzeit (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Pflichten der Inhaber) • Klarstellung zur Grenze der Freistellung von Schadensersatz (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Haftungsbeschränkung) • Streichung des Unterabschnitts zu den Entschädigungsbedingungen (Abschnitt Allgemeine Nutzungsbedingungen) • Streichung des Verweises auf die CPS (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitte Referenzdokumente und Audits und anwendbare Referenzen) • Aktualisierung des zuständigen Gerichts von Caen nach Paris (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Anwendbares Recht und Streitbeilegung) • Überprüfung des Inhalts des Unterabschnitts und Ergänzung eines Verweises auf die Online-Datenschutzrichtlinie (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Verwaltung personenbezogener Daten) • Streichung der Konformitätsprüfung und Klarstellung zum regelmäßig durchgeführten Audit (Abschnitt Allgemeine Nutzungsbedingungen, Unterabschnitt Audits und anwendbare Referenzen)		

VERSIONSHISTORIE			
Version	**Gegenstand der Änderung**	**Datum**	**Autor**
	• Verschiedene Änderungen zur Erleichterung der Lesbarkeit des Dokuments		

Inhaltsverzeichnis

1. Einleitung

1.1. Allgemeine Darstellung

Dieses Dokument legt die ANB der von der Zertifizierungsstelle ausgestellten Serversiegel-Zertifikate fest `YOUSIGN SAS - SIGN3 CA`.

Diese ANB werden vom Zertifikatsnehmer und von der Subjekteinheit im Rahmen des Antragsverfahrens angenommen. Dieses Dokument stellt die Modalitäten der Zertifikatsverwaltung sowie die Verpflichtungen und Pflichten der verschiedenen Parteien dar.

Dieses Dokument entspricht der Vorlage der PKI Disclosure Statements im Sinne der Norm EN 319 411-1.

1.2. Dokumentidentifikation

Dieses Dokument wird durch seinen Titel und seine Versionsnummer bezeichnet. Diese Nummer kann sich unabhängig von den Änderungen der OID der Zertifizierungsrichtlinie weiterentwickeln.

Diese Fassung der ANB gilt für die folgenden OIDs:

- `1.2.250.1.302.1.18.1.0` für Zertifikate der Stufe LCP der Norm ETSI 319 411-1, die im Rahmen von Serversiegel-Zertifikaten verwendet werden, die für eine juristische Person ausgestellt werden;
- `1.2.250.1.302.1.24.1.0` für qualifizierte Zertifikate der Stufe QCP-l der Norm ETSI 319 411-2, die im Rahmen von Serversiegel-Zertifikaten verwendet werden, die für die juristische Person Yousign SAS ausgestellt werden.

Elemente, die für eine bestimmte Richtlinie spezifisch sind, wird die OID dieser Richtlinie in eckigen Klammern vorangestellt. Es können mehrere OIDs angegeben werden; in diesem Fall werden sie hintereinander aufgeführt. Gilt ein Element für alle in diesem

Dokument beschriebenen OIDs, so wird entweder das Tag `[alle OIDs]` verwendet, oder es wird kein Tag angegeben.

1.3. Akronyme

Akronym	Bedeutung	Übersetzung
CA	Certification Authority	-
RA	Registration Authority	-
ANB	Allgemeine Nutzungsbedingungen	-
DN	Distinguished Name	Eindeutiger Name
CPS	Certification Practice Statement	Erklärung zu den Zertifizierungspraktiken
DPO	Data Protection Officer	Datenschutzbeauftragter
PKI	Public Key Infrastructure	Public-Key-Infrastruktur
ARL	Authority Revocation List	Sperrliste der CA-Zertifikate
LCP	Lightweight Certificate Policy	Vereinfachte Zertifikatsrichtlinie
CRL	Certificate Revocation List	Zertifikatssperrliste
OCSP	Online Certificate Status Protocol	Online-Protokoll zur Abfrage des Zertifikatsstatus
OID	Object Identifier	Objektkennung
CP	Certificate Policy	Zertifizierungsrichtlinie
RCC	Responsable du Certificat de Cachet	Verantwortlicher für das Siegelzertifikat
URL	Uniform Resource Locator	Einheitlicher Ressourcenzeiger

1.4. Definitionen

Begriff	Bedeutung
Zertifikatsnehmer	`[1.2.250.1.302.1.18.1.0]` Der Zertifikatsnehmer ist eine juristische Person, die

Begriff	Bedeutung
	Kundin des Unternehmens Yousign ist. Zwischen dem Zertifikatsnehmer und dem Unternehmen Yousign besteht ein Vertragsverhältnis. [1.2.250.1.302.1.24.1.0] Der Zertifikatsnehmer ist die juristische Person Yousign SAS.
Subjekteinheit	Die Subjekteinheit ist die juristische Person, für die das Zertifikat ausgestellt wurde. Diese juristische Person wird durch einen gesetzlichen Vertreter vertreten, der von der RA registriert wurde. Der DN des Zertifikats ermöglicht die Identifizierung dieser Einheit.
Responsable du Certificat de Cachet	Der RCC ist die natürliche Person, die für den Schutz der Aktivierungsdaten des privaten Schlüssels verantwortlich ist, der dem Zertifikat der Subjekteinheit entspricht. Der RCC ist standardmäßig ein gesetzlicher Vertreter der Subjekteinheit. Alternativ kann er eine von einem gesetzlichen Vertreter der Subjekteinheit benannte Person sein. In letzterem Fall kann der RCC der Subjekteinheit hierarchisch zugeordnet sein oder einer anderen Einheit zugeordnet sein, mit der ein Vertrags- oder Regulierungsverhältnis besteht. Der RCC kann sich während der Gültigkeitsdauer des Zertifikats ändern (Austritt des RCC aus der Einheit, Änderung der Zuordnung und der Verantwortlichkeiten innerhalb der Einheit usw.), ohne dass die Gültigkeit des Zertifikats in Frage gestellt wird.
Nutzer	Ein Nutzer ist eine natürliche oder juristische Person, die Zugang zu einer signierten Datei hat, deren Signatur mit dem privaten Schlüssel eines von der unter diese ANB fallenden CA ausgestellten Zertifikats erzeugt wurde. Es ist anzumerken, dass zwischen dem Unternehmen Yousign und einem Nutzer kein unmittelbares Verhältnis besteht.

2. Allgemeine Nutzungsbedingungen

Kontakt der Zertifizierungsstelle	Yousign SAS Verwaltung der CA Yousign 507, rue de Suède et de Norvège 14000 Caen authority@yousign.com
Art der ausgestellten Zertifikate	Die ANB gelten für die im Abschnitt angegebenen Zertifikate Dokumentidentifikation. Die Zertifikate werden einem RCC ausgestellt, der ein formeller Vertreter des Zertifikatsnehmers des Yousign-Dienstes ist und der mit der Verwaltung und dem Einsatz dieser Zertifikate beauftragt ist. Die von der CA ausgestellten Zertifikate sind Serversiegel-Zertifikate, die im Namen einer im Zertifikat bezeichneten Subjekteinheit ausgestellt werden. Die Zertifikate werden über die folgende Zertifizierungskette ausgestellt: • Wurzel-CA: `YOUSIGN SAS - ROOT2 CA` • Ausstellende CA: `YOUSIGN SAS - SIGN3 CA` Die Zertifikate der Zertifizierungskette sind unter der folgenden Adresse verfügbar https://yousign.com/fr-fr/documentation-technique-des-certifications.
Zweck der Zertifikate	Die von der CA ausgestellten Zertifikate sind Serversiegel-Zertifikate, die es ermöglichen, die Authentizität und die Integrität der Daten zu gewährleisten.
Modalitäten des Erhalts	Der RCC muss einen formellen Antrag an die RA senden. Die Registrierungsunterlagen sind in der CP beschrieben. Das erzeugte Zertifikat wird dem RCC nach seiner Erzeugung übermittelt und bleibt anschließend in jedem signierten Dokument zugänglich. Der Besitz des privaten Schlüssels ist gemäß der in der CP beschriebenen Methode nachzuweisen.

Modalitäten der Erneuerung	Das Erneuerungsverfahren entspricht einem neuen Zertifikatsantrag.
Modalitäten der Sperrung	Der Antrag auf Sperrung eines Zertifikats ist per E-Mail an die im Abschnitt „Kontakt der Zertifizierungsstelle“ angegebene Adresse zu stellen. Ein Sperrantragsformular ist vom Antragsteller auszufüllen und zu unterzeichnen. Das Verfahren zur Bearbeitung des Sperrantrags ist in der CP dokumentiert.
Nutzungsbeschränkungen	Die Verwendung eines privaten Serverschlüssels und des zugehörigen Zertifikats ist strikt dem in den Registrierungsunterlagen festgelegten Siegelerstellungsdienst vorbehalten. Die Zertifikate haben eine Gültigkeitsdauer von drei (3) Jahren. Die entsprechenden privaten Schlüssel werden nach Ablauf dieses Zeitraums ohne Möglichkeit der Wiederherstellung vernichtet. Yousign bewahrt die Protokolle und Aufzeichnungen zur Ausstellung und Verwendung der den Zertifikaten zugeordneten privaten Schlüssel siebzehn (17) Jahre lang auf.

Pflichten der CA	`[alle OIDs]`
	Die CA ist verantwortlich für:
	• die Validierung und die Veröffentlichung der CP und dieser ANB der CA;
	• die Konformität mit der CP und mit diesen ANB.
	
	`[1.2.250.1.302.1.24.1.0]`
	Die CA ist verantwortlich für:
	• im Fall eines schwerwiegenden Vorfalls (zum Beispiel Verlust, Kompromittierung oder Diebstahl des privaten Schlüssels der Zertifikate) die Meldung des Vorfalls an die ANSSI innerhalb von 24 Stunden.

Pflichten der Subjekteinheit und des gesetzlichen Vertreters	Die Subjekteinheit, vertreten durch ihren gesetzlichen Vertreter, berücksichtigt die folgenden Anforderungen: • ein Vertrags-, Hierarchie- oder Regulierungsverhältnis mit dem Zertifikatsnehmer haben; • sich verpflichten, die in den Registrierungsunterlagen verlangten Informationen und Nachweise aktuell und gültig bereitzustellen; • prüfen, dass der Inhalt des ausgestellten Zertifikats richtig ist;

	• das Zertifikat ausschließlich unter den in der CP vorgesehenen und in diesen ANB übernommenen Nutzungsbedingungen einsetzen und dabei die Nutzungsbeschränkungen beachten; • einwilligen, dass jede erfolgreiche Authentifizierung beim elektronischen Siegeldienst als mit Zustimmung des RCC und der Subjekteinheit erfolgt gilt; • sich verpflichten, die CA ohne unangemessene Verzögerung zu benachrichtigen, wenn einer der folgenden Sperrgründe vorliegt: o in den Registrierungsunterlagen oder im Zertifikat wurde ein Fehler (absichtlich oder nicht) festgestellt; o die im Zertifikat enthaltenen Angaben stimmen nicht mehr mit der Identität oder der im Zertifikat vorgesehenen Verwendung überein, und dies vor dem regulären Ablauf des Zertifikats; o die Aktivierungsdaten stehen im Verdacht, kompromittiert zu sein, sind kompromittiert, verloren, gestohlen oder gesperrt. • es unterlassen, das Zertifikat zu verwenden, sobald die Aktivierungsdaten, der private Schlüssel oder die CA im Verdacht stehen, kompromittiert zu sein, kompromittiert, verloren, gestohlen oder gesperrt sind; • sich verpflichten, den Status des ausgestellten Zertifikats über die von der CA veröffentlichten CRLs zu überprüfen; • in die Aufbewahrung der Informationen der Registrierungsunterlagen sowie der Verwaltung der Schlüssel und des Zertifikats durch die RA und die CA einwilligen.
Pflichten des Zertifikatsnehmers und des RCC	Der Zertifikatsnehmer, vertreten durch den RCC, berücksichtigt die folgenden Anforderungen: • ein Vertrags-, Hierarchie- oder Regulierungsverhältnis mit der Subjekteinheit haben; • sich verpflichten, vor jedem Zertifikatsantrag die formelle Zustimmung eines gesetzlichen Vertreters der Subjekteinheit einzuholen; • sich verpflichten, die in den Registrierungsunterlagen verlangten Informationen und Nachweise aktuell und gültig bereitzustellen; • prüfen, dass der Inhalt des ausgestellten Zertifikats richtig ist;

	• das von der CA ausgestellte Zertifikat mit dessen Übergabe durch die RA stillschweigend annehmen; • die Vertraulichkeit der Aktivierungselemente gewährleisten, die es dem Anwendungsdienst ermöglichen, auf den elektronischen Siegeldienst zuzugreifen; • einwilligen, dass jede erfolgreiche Authentifizierung beim elektronischen Siegeldienst als mit Zustimmung des RCC und der Subjekteinheit erfolgt gilt; • das Zertifikat nur mit Zustimmung der Subjekteinheit, in dem mit der Subjekteinheit vereinbarten Rahmen und innerhalb der in den ANB vorgesehenen Nutzungsbeschränkungen verwenden; • sich verpflichten, die CA ohne unangemessene Verzögerung zu benachrichtigen, wenn einer der folgenden Sperrgründe vorliegt: o in den Registrierungsunterlagen oder im Zertifikat wurde ein Fehler (absichtlich oder nicht) festgestellt; o die im Zertifikat enthaltenen Angaben stimmen nicht mehr mit der Identität oder der im Zertifikat vorgesehenen Verwendung überein, und dies vor dem regulären Ablauf des Zertifikats; o die Aktivierungsdaten stehen im Verdacht, kompromittiert zu sein, sind kompromittiert, verloren, gestohlen oder gesperrt. • es unterlassen, das Zertifikat zu verwenden, sobald die Aktivierungsdaten, der private Schlüssel oder die CA im Verdacht stehen, kompromittiert zu sein, kompromittiert, verloren, gestohlen oder gesperrt sind; • sich verpflichten, die RA vor jeder Ungültigmachung der Rolle des bekannten RCC zu benachrichtigen; • sich verpflichten, den Status des ausgestellten Zertifikats über die von der CA veröffentlichten CRLs zu überprüfen; • die Erneuerung des Zertifikats mindestens drei (3) Monate vor dessen Ablauf beantragen; • in die Aufbewahrung der Informationen der Registrierungsunterlagen sowie der Verwaltung der Schlüssel und des Zertifikats durch die RA und die CA einwilligen.
Pflichten zur Überprüfung der	Die Nutzer der Zertifikate müssen: • die Verwendung, für die ein Zertifikat ausgestellt wurde, prüfen und beachten;

Zertifikate durch die Nutzer	• für jedes Zertifikat der Zertifizierungskette, vom Zertifikat der Subjekteinheit bis zur CA YOUSIGN SAS – ROOT2 CA, die digitale Signatur der das betreffende Zertifikat ausstellenden CA verifizieren und die Gültigkeit dieses Zertifikats überprüfen (Gültigkeitsdaten, Sperrstatus); • die in der CP dargelegten Pflichten der Zertifikatsnutzer prüfen und beachten. Die CRLs werden unter den in den Zertifikaten angegebenen und in der CP wiedergegebenen URLs veröffentlicht.
Überprüfung des Zertifikatsstatus	Im Fall der Sperrung der CA, zum Beispiel infolge einer Kompromittierung ihres privaten Schlüssels, wird die Sperrinformation in einer ARL bereitgestellt, die unter den in den Zertifikaten angegebenen und in der CP wiedergegebenen URLs veröffentlicht wird.
Haftungsbeschränkung	Yousign kann nicht für eine unbefugte oder nicht konforme Verwendung der Authentifizierungsdaten, der Zertifikate, der CRLs sowie sonstiger bereitgestellter Ausrüstung oder Software haftbar gemacht werden. Yousign 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 Zertifikatsnehmer oder von der Subjekteinheit mitgeteilten Angaben zurückzuführen sind. In jedem Fall und im streng nach anwendbarem Recht zulässigen Umfang ist Yousign 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.
Referenzdokumente	Die Zertifizierungsrichtlinie der CA YOUSIGN SAS - SIGN3 CA für Serversiegel ist unter der folgenden Adresse zugänglich: https://yousign.com/fr-fr/documentation-technique-des-certifications.
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 ausschließliche Zuständigkeit den Gerichten von Paris zugewiesen.
Verwaltung personenbezogener Daten	Yousign 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 Zertifikatsnehmer und die Subjekteinheit werden darauf hingewiesen, dass die Ausstellung elektronischer Zertifikate die Verarbeitung personenbezogener Daten durch Yousign erfordert. Sie werden gebeten, die Datenschutzrichtlinie zu konsultieren, um weitere Informationen darüber zu erhalten, wie ihre personenbezogenen Daten verarbeitet werden und wie sie ihre Rechte ausüben können.

Audits und anwendbare Referenzen	`[alle OIDs]`
	Yousign richtet einen technischen Lenkungsausschuss von Yousign ein.
	
	Ein technisches Sicherheitsaudit wird mindestens jährlich durchgeführt. Die Audits werden intern durch Personal von Yousign oder in Form einer Dienstleistung durch auf die Sicherheit von Informationssystemen spezialisierte Akteure mit anerkannter Fachkompetenz im Bereich der Sicherheit von Informationssystemen durchgeführt.
	
	`[1.2.250.1.302.1.24.1.0]`
	Das von Yousign verwendete kryptografische Modul ist von der ANSSI qualifiziert.
	
	Die Zertifikate entsprechen der Norm ETSI 319 411-2 auf der Stufe QCP-l und sind im Sinne der eIDAS-Verordnung von der ANSSI qualifiziert.

Beweisvereinbarung	Für jedes angebrachte elektronische Siegel akzeptieren Yousign, der Zertifikatsnehmer und die Subjekteinheit, dass die Elemente, die in Folgendem enthalten sind: ● den Registrierungsunterlagen, wie zum Beispiel: ○ die Identifikationselemente des Zertifikatsnehmers und seines RCC; ○ die Identifikationselemente der Subjekteinheit und ihres gesetzlichen Vertreters; ○ die bereitgestellten Nachweise; ● den Nachweisunterlagen, wie zum Beispiel: ○ die Verfahren, die zum Anbringen des elektronischen Siegels auf den Dokumenten verwendet werden (zum Beispiel das Authentifizierungsverfahren); ○ das elektronische Siegelzertifikat; ○ die Zeitstempelelemente; ○ eine Gesamtheit von IT-Aufzeichnungen; vor Gericht zulässig sind und Beweis für die Daten und Elemente erbringen, die sie enthalten, sowie für die Authentifizierungsverfahren, die sie zum Ausdruck bringen. Die Registrierungsunterlagen und die Nachweisunterlagen werden von Yousign archiviert und mit einem Zeitstempel versehen.