

# PDS

## PKI Disclosure Statement

### Fortgeschrittene elektronische Signatur (AdES)

DOKUMENTBEZEICHNUNG	ICERT-INDI-PDSFEA (DEU)
VERSION	1.1
DATUM	12.05.2023



# INHALT

1. Einführung .....	3
2. Kontakte .....	3
3. Art der Zertifikate, Validierung und Verwendung .....	4
4. Zuverlässigkeitsgrenzen.....	4
5. Pflichten des Zertifikatsinhabers.....	5
6. Pflichten der Antragsteller, die keine Zertifikatsinhaber sind .....	6
7. Gültigkeitsstatus der Zertifikate.....	8
8. Beschränkte Garantie und fehlende/beschränkte Haftung .....	8
9. Geltende Verträge, Richtlinien und Beschreibungen der Zertifizierungspraxis (CPS) .....	9
10. Datenschutzbestimmungen .....	9
11. Erstattungspolitik.....	9
12. Anwendbares Recht betreffend Beschwerden und Beilegung von Streitigkeiten .....	10
13. Archive, Lizenzen und Marken, Audits.....	11

## 1. Einführung

Das vorliegende PKI-Disclosure-Statement (PDS) erfüllt die Veröffentlichungspflicht laut Norm ETSI EN 319 411-1 im Hinblick auf den von InfoCert S.p.A. (nachfolgend „**InfoCert**“ oder „**TSP**“) angebotenen Zertifizierungsdienst, und soll die erforderlichen technischen Informationen für die Antragsteller zur Nutzung des Dienstes bereitstellen.

Die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG wird im Folgenden als „**eIDAS-Verordnung**“ bezeichnet.

Das vorliegende Dokument ergänzt die Allgemeinen Geschäftsbedingungen und gilt als wesentlicher Bestandteil der Vertragsunterlagen von InfoCert.

Die Veröffentlichung dieses PDS ersetzt nicht die Veröffentlichung der Beschreibung der Zertifizierungspraxis (CPS), die detailliertere Informationen enthält und auf der InfoCert-Website unter folgendem Link verfügbar ist:

<https://www.firma.infocert.it/documentation/>.

## 2. Kontakte

InfoCert S.p.A. – USt-IdNr. 07945211006  
Qualifizierter Vertrauensdiensteanbieter  
Piazza Sallustio, 9  
00187 Rom, Italien

Geschäftsstellen  
Piazza Luigi da Porto 3  
35131 Padua, Italien

Telefon: +39 06 836691 – Fax: +39 06 23328861

Call Center Digitale Signaturen: siehe <https://help.infocert.it/contatti/> Web:  
<http://www.firma.infocert.it/> E-Mail:

firma.digitale@legalmail.it

Der **Widerruf** eines digitalen Signaturzertifikats kann anhand des entsprechenden, auf der InfoCert-Website veröffentlichten Formulars beantragt werden, das per zertifizierte E-Mail (PEC), per Einschreiben oder Fax zusammen mit einer Fotokopie eines gültigen Personaldokuments zu übermitteln ist. Der Widerruf kann auch bei der zuständigen Registrierungsstelle laut den in den Allgemeinen Geschäftsbedingungen angegebenen Verfahren beantragt werden. InfoCert behält sich das Recht vor, zusätzliche Überprüfungen der Identität des Antragstellers durchzuführen.

Die **Aussetzung** eines digitalen Signaturzertifikats kann direkt online auf der Website von InfoCert unter Verwendung des bei der Registrierung zugeteilten Geheimcodes beantragt werden.

### 3. Art der Zertifikate, Validierung und Verwendung

InfoCert stellt Signaturzertifikate im Sinne der Norm **ETSI EN 319 411-1** und anderer damit verbundener Normen aus, die Privatunternehmen, öffentlichen Einrichtungen, Freiberuflern, Einzelpersonen usw. zu den auf der Website des TSP oder von anderen Registrierungsstellen (RA) veröffentlichten Bedingungen angeboten werden.

Einzelheiten, Richtlinien, Verwendungsbeschränkungen und Spezifikationen zu Algorithmen und Schlüsseln sind in den Beschreibungen der Zertifizierungspraxis enthalten, die unter dem Link <https://www.firma.infocert.it/documentation> eingesehen werden können.

Das asymmetrische Zertifizierungsschlüsselpaar kann je nach Zertifikatsrichtlinie durch eine Verschlüsselungshardwareeinheit erstellt werden.

### 4. Zuverlässigkeitsgrenzen

InfoCert stellt als TSP **Zertifikate** zur fortgeschrittenen elektronischen Signatur **für natürliche Personen** aus.

Die Gültigkeitsdauer jedes Zertifikats ist im Zertifikat selbst angegeben (mindestens eine Stunde; höchstens drei Jahre und drei Monate).

Es ist untersagt, das Zertifikat außerhalb der im CPS und in den Verträgen angegebenen Grenzen und Definitionen und jedenfalls unter Verletzung der im Zertifikat angegebenen Nutzungs- und Wertgrenzen (*Schlüsselerwendung, erweiterte Schlüsselerwendung, Nutzerhinweis*) zu verwenden.

Ereignisprotokolle im Zusammenhang mit der Ausstellung von Zertifikaten werden gemäß der TSP-Datenschutzpolitik mindestens 20 (zwanzig) Jahre im Datenspeichersystem von InfoCert aufbewahrt.

## 5. Pflichten des Zertifikatsinhabers

Der **Zertifikatsinhaber** hat die Pflicht, sich an die Klauseln des CPS und der Allgemeinen Geschäftsbedingungen zu halten. Dies umfasst im Besonderen:

- das Lesen und das Verständnis der Vertragsunterlagen und aller zusätzlichen Informationsunterlagen.
- die Einhaltung der vom Vertrauensdiensteanbieter festgelegten und im CPS beschriebenen Identifizierungsverfahren.
- die Erteilung aller für die Identifizierung erforderlichen Angaben und, falls verlangt, die Ergänzung durch die entsprechenden Unterlagen.
- die ausschließliche Nutzung des zugewiesenen Schlüsselpaars für die Zwecke und die Art, wie im CPS erlaubt.
- die Akzeptierung der Vertragsbestimmungen zur Erbringung des Dienstes, wie in den vom TSP vorbereiteten analogen oder elektronischen Formularen aufgeführt, durch Unterzeichnung des Antrags auf Registrierung und Zertifizierung.
- die unverzügliche Benachrichtigung des TSP oder der Registrierungsstelle während der Gültigkeit und bis zum Ablaufdatum des Zertifikats, wenn folgende Umstände eintreten:

- Verlust, Diebstahl oder Beschädigung der Signatureinheit des Zertifikatsinhabers;
  - Verlust der alleinigen Kontrolle über den privaten Schlüssel des Zertifikatsinhabers, beispielsweise infolge der Kompromittierung der Aktivierungsdaten (z. B. PIN) der Signatureinheit;
  - ungenaue oder nicht mehr gültige Angaben im Zertifikat des Zertifikatsinhabers.
- die Geheimhaltung der für die Nutzung von Signatureinheiten oder -diensten erforderlichen Anmeldeinformationen, indem diese Dritten weder mitgeteilt noch zugänglich gemacht werden und die alleinige Kontrolle über sie behalten wird.
- die unverzügliche und endgültige Nichtverwendung des kompromittierten Schlüssels, es sei denn, er dient der Entschlüsselung des gegenständlichen Schlüssels.
- das Sicherstellen, dass der Zertifikatsinhaber den privaten Schlüssel nicht weiter verwendet, wenn der Antragsteller über den Widerruf des Zertifikats des Betroffenen oder eine Kompromittierung des TSP informiert wurde.

Die Verantwortung für die Beschaffung und Nutzung einer Internetverbindung und aller erforderlichen Instrumente (Hard- und Software) liegt beim Antragsteller.

## 6. Pflichten der Antragsteller, die keine Zertifikatsinhaber sind

**Antragsteller**, die keine **Zertifikatsinhaber** sind, haben die Pflicht, sich an die Klauseln des CPS und der Allgemeinen Geschäftsbedingungen zu halten. Dies umfasst im Besonderen:

- das Lesen und das Verständnis der Vertragsunterlagen und aller zusätzlichen Informationsunterlagen.
- die Einhaltung der vom TSP festgelegten Identifizierungsverfahren.
- die Erteilung aller für die Identifizierung erforderlichen Angaben und, falls verlangt, die Ergänzung durch die entsprechenden Unterlagen.

- die Akzeptierung der Vertragsbestimmungen zur Erbringung des Dienstes, wie in den vom TSP vorbereiteten analogen oder elektronischen Formularen aufgeführt, durch Unterzeichnung des Antrags auf Registrierung und Zertifizierung.
- die Festlegung und entsprechende Mitteilung an den TSP über die zur Übermittlung der Dokumente genutzte Informationstechnologie, die dem Fernsignaturverfahren und der Aktivierung der Signaturschlüssel durch den Zertifikatsinhaber unterzogen werden.
- die Übernahme der Kosten für den Fernsignaturdienst und Angabe des Zertifikatsinhabers, für den die Zertifikate bestimmt sind, anhand von besonderen Urkunden und Verfahren.
- die Angabe der bevorzugten Art des Authentifizierungssystems zur Aktivierung des Fernsignaturverfahrens.
- die Unterzeichnung des entsprechenden vom TSP bereitgestellten Formulars für den Antrag auf Widerruf/Aussetzung des Zertifikats im Falle einer diesbezüglichen Entscheidung durch den Zertifikatsinhaber.
- die Information des Zertifikatsinhabers über die auf dem Zertifikat beruhenden Pflichten, die Erteilung korrekter und wahrheitsgemäßer Angaben zur Identität des Zertifikatsinhabers und die Einhaltung der Verfahren und Hinweise des TSP und/oder der Registrierungsstelle.
- die Erteilung der folgenden Angaben an den TSP, wenn der Zertifikatsinhaber eine juristische Person ist:
  - Nachname und Vorname des Antragstellers;
  - Steueridentifikationsnummer oder vergleichbarer Code oder Nummer zur Identifizierung des Antragstellers;
  - Angaben zum Personaldokument, das zur Identifizierung des Antragstellers vorgelegt wird, d. h. Art, Nummer, ausstellende Behörde und Ausstellungsdatum;
  - E-Mail-Adresse für Mitteilungen vom TSP an den Antragsteller;
    - Name des Zertifikatsinhabers als juristische Person
    - USt-IdNr. oder Nationales Handelsregister.
- die Einreichung eines speziellen, vom Antragsteller unterzeichneten Antrags im PKCS #10-Format, wenn Schlüssel durch eine Einheit des Zertifikatsinhabers

generiert werden. Wird die Signatureinheit nicht vom TSP zur Verfügung gestellt, hat der Antragsteller sicherzustellen, dass die Einheit den geltenden Vorschriften entspricht, indem er entsprechende Unterlagen vorlegt und sich regelmäßigen Prüfungen durch den TSP unterzieht.

## 7. Gültigkeitsstatus der Zertifikate

Alle Parteien, die sich auf die in den Zertifikaten enthaltenen Informationen verlassen, müssen prüfen, ob die Zertifikate nicht ausgesetzt oder widerrufen wurden.

Informationen über den Status von Zertifikaten sind in der Liste der widerrufenen Zertifikate (CRL) zu finden, die von der Zertifizierungsstelle (CA) unter der im Zertifikat angegebenen URL oder durch den OCSP-Dienst veröffentlicht wird.

## 8. Beschränkte Garantie und fehlende/beschränkte Haftung

Die Zertifikate werden laut diesem Dokument und den Allgemeinen Geschäftsbedingungen ausgestellt. Alle notwendigen technischen Details sind im CPS festgelegt.

InfoCert haftet für direkte oder indirekte Schäden, die einer natürlichen oder juristischen Person entstehen, infolge der Nichterfüllung der Pflichten laut Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014, ob durch Vorsatz, Fahrlässigkeit oder infolge des Versäumnisses durch InfoCert, alle geeigneten Maßnahmen zur Vermeidung solcher Schäden zu ergreifen.

In einer wie hier oben beschriebenen Situation hat der Antragsteller oder der Zertifikatsinhaber Anspruch auf Entschädigung des Schadens, der ihm als direkte Folge des oben genannten vorsätzlichen oder fahrlässigen Verhaltens entstanden ist, wobei die Höchstbeträge laut Art. 3 Abs. 7 der Verordnung im Anhang des AgID-Beschlusses Nr. 185/2017 für jeden einzelnen Schaden und jedes Jahr auf keinen Fall überschritten werden dürfen.



Schäden, die auf einer unsachgemäßen Nutzung des Zertifizierungsdienstes oder auf dem Telekommunikationsnetz beruhen, sind nicht erstattungsfähig. Dies gilt auch im Falle eines Zufallsereignisses, höherer Gewalt oder für Ursachen, die InfoCert nicht zu verantworten hat.

## 9. Geltende Verträge, Richtlinien und Beschreibungen der Zertifizierungspraxis (CPS)

Die für den TSP-Service geltenden Verträge und Bedingungen sind genauso wie die Beschreibungen der Zertifizierungspraxis auf der Website von InfoCert unter <https://firma.infocert.it/documentation> veröffentlicht.

## 10. Datenschutzbestimmungen

Sofern nicht ausdrücklich anderes vereinbart, gelten Informationen über den Zertifikatsinhaber und den Antragsteller, von denen der TSP im Rahmen der üblichen Tätigkeiten Kenntnis erlangt, als vertraulich, und dürfen nicht veröffentlicht werden, es sei denn, sie sind ausdrücklich für die Öffentlichkeit bestimmt: *öffentlicher Schlüssel, Zertifikat (falls vom Zertifikatsinhaber beantragt), Angaben zum Widerruf oder zur Aussetzung des Zertifikats.*

InfoCert verarbeitet personenbezogene Daten gemäß dem italienischen gesetzvertretenden Dekret Nr. 196 vom 30. Juni 2003 und der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DSGVO), die seit dem 25. Mai 2018 in vollem Umfang rechtskräftig ist.

## 11. Erstattungspolitik

Zur Ausübung eines etwaigen Vertragsrücktritts muss der Zertifikatsinhaber den TSP vor Ablauf der Rücktrittsfrist mittels ausdrücklicher Erklärung per zertifizierte E-Mail (PEC) an [richieste.rimborso@legalmail.it](mailto:richieste.rimborso@legalmail.it) oder per Einschreiben mit Rückschein an InfoCert S.p.A. – Direzione Generale e Amministrativa – Via Marco e Marcelliano 45, 00147 Rom,

informieren. Der Einfachheit halber kann hierzu das auf der Website bereitgestellte Kündigungsformular verwendet werden, das auf der Website von InfoCert unter folgendem Link zur Verfügung steht: <https://www.InfoCert.it/pdf/Modulo-di-recesso-tipo.pdf>.

Der Zertifikatsinhaber und/oder der Antragsteller trägt/tragen die Kosten für eine eventuelle Rücksendung der Signatureinheit, während der TSP bereits geleistete Zahlungen ordnungsgemäß erstattet. Die gegenständliche Erstattung wird auf das für die ursprüngliche Transaktion verwendete Girokonto überwiesen, es sei denn, der Zertifikatsinhaber hat ausdrücklich eine andere Bankverbindung für die Zahlung angegeben; in jedem Fall wird die Zahlung ohne Kosten für den Zertifikatsinhaber angewiesen und geleistet.

## 12. Anwendbares Recht betreffend Beschwerden und Beilegung von Streitigkeiten

Die Erbringung von Zertifizierungs- und Zeitstempeldiensten wird durch das geltende italienische Gesetz geregelt. Für Sachverhalte, die in diesem Dokument nicht ausdrücklich behandelt werden, wird auf das italienische Zivilgesetzbuch und andere anwendbare Gesetze verwiesen.

Für jede Streitigkeit, die sich aus der Auslegung und Erfüllung des vorliegenden Vertrags ergibt, oder damit zusammenhängt, ist ausschließlich das Gericht Rom zuständig, sofern in den Allgemeinen Geschäftsbedingungen des vorliegenden Vertrags nicht anders festgelegt.

Ist der Kunde ein Verbraucher, so unterliegt jede Streitigkeit im Zusammenhang mit dem von ihm geschlossenen Vertrag zwingend der Zuständigkeit des Gerichts seines Wohnorts oder Wohnsitzes.

### 13. Archive, Lizenzen und Marken, Audits

Obwohl der TSP die Verwendung eingetragener Marken nicht prüft, kann er die Ausstellung eines Zertifikats verweigern oder im Falle einer Streitigkeit den Widerruf eines bestehenden Zertifikats verlangen.

Die Konformitätsbewertung im Rahmen der Verordnung (EU) Nr. 910/2014 vom 23.07.2014 wurde laut den Normen ETSI EN 319 401 und ETSI EN 319 411-1 von CSQA Certificazioni S.r.l. unter Verwendung des eIDAS-Bewertungsverfahrens, definiert von ACCREDIA im Rahmen der Normen ETSI EN 319 403 und ISO/IEC 17065:2012, durchgeführt.

Die Vertrauensliste der italienischen Zertifizierungsstellen ist unter folgendem Link zu finden: <https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/IT>.