

[CQINFO] Information on the use of qualified electronic signatures and seals according to Article 24 eIDAS Regulation

Author: Daniel Zens

Version 5.0/ 9th June, 2022

OID-Number/Nummer: 1.2.40.0.36.1.2.5.1

Publication: <https://service.globaltrust.eu/static/general-en.pdf>

Policy Online: <https://www.globaltrust.eu/certificate-policy.html>

Contact: <https://www.globaltrust.eu/impressum.html>

Limits: <https://globaltrust.eu/limitations>

Suspension/ Revocation: <https://www.globaltrust.eu/revocation.html>

© e-commerce monitoring GmbH 2022

Editorial note: This document has been provided with a signature. The date of signature can deviate from the date of the start of the validity of this document for different legal and organisational reasons. The signature does not give information about the start of the validity of the document, but confirms the integrity of the content.

Redaktioneller Hinweis: Das vorliegende Dokument ist mit einer Signatur versehen. Das Datum der Signatur kann aus verschiedenen rechtlichen und organisatorischen Gründen vom Datum des Gültigkeitsbeginns des Dokuments abweichen. Die Signatur gibt keine Auskunft über den Gültigkeitsbeginn des Dokuments, sondern bestätigt nur die Unversehrtheit des Inhalts.

Copyright note: The document is subject to copyright and is only made available in the context of certification services. An additional application, full or partial transmission to a third party or the publication of the document by a third party requires the prior consent of the author(s) and the CA

Urheberrechtshinweis: Das Dokument unterliegt dem Urheberrecht und wird nur im Rahmen der Zertifizierungsdienste zur Verfügung gestellt. Eine darüber hinausgehende Verwendung, eine vollständige oder auszugsweise Übermittlung an Dritte oder die Veröffentlichung des Dokuments durch Dritte bedarf der vorherigen Zustimmung des Autors/der Autoren und des Vertrauensdiensteanbieters.

1. BEFORE YOU START

Qualified electronic signature is information society's central technology to conclude legally valid agreements. You should therefore be particularly careful with the resources and information provided. Your qualified signature is comparable to cash, so keep all information about it in a comparable way.

Smartcard, password (in the case of a card-based qualified signature) or user ID, transport PIN, activation PIN, mobile phone and confirmation code (in the case of a cloud-based qualified signature) describe the identity of the signatory and allow the holder to conclude legally binding contracts on behalf of the signatory .

The signature must therefore take all reasonable measures to prevent the theft of the information and objects and thus an identity theft or to make it more difficult that the identity theft is unlikely.

This includes, in particular, the careful storage of all physical components, the choice of sufficiently complex passwords and PINs, the confidentiality of all personal information, the avoidance of computer functions that save confidential information, such as autocomplete functions, password storage in text files, writing down passwords and the like.

2. INTRODUCTION

This information relates to all products of e-commerce monitoring gmbh that are intended to issue qualified certificates for electronic signatures and electronic seals. The information is aimed at certificate applicants, signatories and other third parties, provided they have a legal interest in GLOBALTRUST products.

Qualified certificates are offered under the names GLOBALTRUST QUALIFIED and TRUST2GO® (without the name affix "AATL ADVANCED"). All other services, in particular qualified time stamping services, qualified certificates for website authentication and other non-qualified services, are not the subject of this document.

Further information can be requested at the trust service provider (VDA) e commerce monitoring GmbH or on <https://globaltrust.eu/en/certificate-policy-2/>.

3. CONTACT INFORMATION

Company name: e-commerce monitoring GmbH
Headquarters: A-1160 Vienna, Redtenbachergasse 20
Office address: A-1020 Vienna, Handelskai 388 Top 621 (entrance Wehlstraße 299)
UID: ATU54992708
Commercial court Vienna FN 224536a company with limited liability
Managing Director: Dr. Hans G. Zeger
Website: <https://globaltrust.eu>
Email address: info@globaltrust.eu
Tel +43/01/5320944
Fax +43/01/5320974

A standby hotline for revocations will be announced to the signatory in the course of processing the application.

4. *EIDAS CONFORMITY ASSESSMENT*

The operator is registered as a qualified certification service provider in accordance with eIDAS and the Austrian Trust Service Act in the trust list of the European Union. The operation takes place under the supervision of the Telekom-Control-Commission / RTR GmbH. The VDA is subject to an annual conformity assessment by accredited bodies. The certification service is operated in ISO-27001-certified data centers.

Conformity assessment certificates and other certifications are published on the operator's website.

5. *APPLICABLE LAW*

All certification services described in this document are provided in accordance with the Austrian Signature and Trust Services Act¹, including the Signature and Trust Services Regulation and the EU regulation on electronic identification and trust services² (eIDAS). The technical implementation takes place in accordance with ETSI standard ETSI EN 319 401³, ETSI EN 319 411-1⁴, ETSI EN 319 411-2⁵, the extensions for the issue of qualified certificates in accordance with ETSI EN 319 412⁶ or comparable equivalent standards. Furthermore, the requirements ETSI TS 119 421 on remote signatures and EN 419221 on the operation of server-based signature services are applied.

The contractual relationship between the VDA and the applicant includes:

- the order
- this document
- the [GCP] GLOBALTRUST Certificate Policy (public, OID number: 1.2.40.0.36.1.1.8.1, <https://www.globaltrust.eu/static/globaltrust-certificate-policy.pdf>)
- the [GCPS] GLOBALTRUST Certificate Practice Statement (public, OID number: 1.2.40.0.36.1.2.3.1, <https://www.globaltrust.eu/static/globaltrust-certificate-practice-statement.pdf>)
- the [GCSP] GLOBALTRUST Certificate Security Policy (non public)
- Other economic conditions not regulated by the provisions of the certification services, in particular conditions and payment modalities, can be found in the general terms and conditions of the VDA (<https://e-monitoring.at/static/terms.pdf>).

6. *SUBSCRIBER IDENTIFICATION*

Qualified certificates for electronic signatures are issued only to clearly identified natural persons. Qualified certificates for electronic seals are issued only to verified organizations, with an authorized signatory natural person identified as the responsible party.

¹ Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG) BGBl. I Nr. 50/2016 siehe <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009585>

² 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, siehe <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0910>

³ EN 319 401 General Policy Requirements for Trust Service Providers http://www.etsi.org/deliver/etsi_en/319400_319499/319401/

⁴ EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1 General Requirements http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/

⁵ EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/

⁶ ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles Part 1-5, <https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx>

Identity verification of natural persons can be performed by personal presence by presentation of suitable official personal documents or by remote procedures such as, in particular, postal or video based procedures.

If third parties are involved in the identification process, the requirements applicable to the respective certification service are contractually transferred in full to the third party. In any case, the responsibility for the proper provision of the certification services remains with the VDA.

7. LEGAL EFFECTS OF THE SIGNATURE MECHANISMS

Qualified electronic Signature

According to eIDAS Art 24 para 2:

A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.

For Austria according to § 4 Abs. 1 Signatur- und Vertrauensdienstegesetz (SVG)

(1) Eine qualifizierte elektronische Signatur erfüllt das rechtliche Erfordernis der Schriftlichkeit im Sinne des § 886 ABGB. Andere gesetzliche Formerfordernisse, insbesondere solche, die die Beziehung eines Notars oder eines Rechtsanwalts vorsehen, sowie vertragliche Vereinbarungen über die Form bleiben unberührt.

(2) Letztwillige Verfügungen können in elektronischer Form nicht wirksam errichtet werden. Folgende Willenserklärungen können nur dann in elektronischer Form wirksam abgefasst werden, wenn das Dokument über die Erklärung die Conformity assessment eines Notars oder eines Rechtsanwalts enthält, dass er den Signator über die Rechtsfolgen seiner Signatur aufgeklärt hat:

1. Willenserklärungen des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind;

2. eine Bürgschaftserklärung (§ 1346 Abs. 2 ABGB), die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit abgegeben wird.

(3) Bei Rechtsgeschäften zwischen Unternehmern und Verbrauchern sind Vertragsbestimmungen, nach denen eine qualifizierte elektronische Signatur nicht das rechtliche Erfordernis der Schriftlichkeit erfüllt, für Anzeigen oder Erklärungen, die vom Verbraucher dem Unternehmer oder einem Dritten abgegeben werden, nicht verbindlich, es sei denn, der Unternehmer beweist, dass die Vertragsbestimmungen im Einzelnen ausgehandelt worden sind oder mit dem Verbraucher eine andere vergleichbar einfach verwendbare Art der elektronischen Authentifizierung vereinbart wurde.

For other countries please refer to national commercial laws.

Among EU member states, the signature must be recognized in accordance with eIDAS.

Qualifiziertes electronic seal

According to eIDAS Art 35

[CQINFO] Information on the use of qualified electronic signatures and seals according to Article 24 eIDAS Regulation 1

1. An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.
2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.
3. A qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States.

.8. SUBSCRIBER OBLIGATIONS

Subscriber obligations include:

- ☒ Input of complete and correct information in compliance with the requirements of this policy, especially during the registration procedure.
- ☒ Insofar as a mobile telephone number is required for the use of the private key, the signatory shall use a telephone number at his sole disposal.
- ☒ Verify that all information in the certificate is correct directly after successful delivery
- ☒ Assigning a password/PIN that differs from the transport lock password/PIN.
- ☒ Retain the private key to a hardware unit to which the subscriber has sole access
- ☒ The signatory shall keep all components, information and procedures given to him for the use of the private key under his sole control and protect them from access by unauthorized third parties.
- ☒ The application of appropriate caution to prevent unauthorized use of the private key.
- ☒ Use appropriate caution to prevent the unauthorized use of the private key.
- ☒ Destroy invalid keys. This also applies for keys saved on signature creation devices. An appropriate method of destruction includes returning the signature creation device to the operator with a request to destroy the invalid key.
- ☒ The key pair may only be used for the generation of electronic signatures. All further limitations on the administration of keys of which the subscriber is informed should likewise be observed.
- ☒ The certificate may only be used for electronic signatures that have been generated with the QSCD or QRSCD corresponding to the certificate.

Inform the operator immediately if one or more of the following circumstances arise:

- ☒ The transport-protection (e.g. the TransportPIN) for the signature creation device is not usable,
- ☒ The private key or its activation data has been lost,
- ☒ The mobile phone has been stolen or otherwise got lost, in case a mobile phone is required as a signature activation component
- ☒ The private key of the subscriber or its activation data may have been compromised
- ☒ Sole control over the private key has been lost,
- ☒ The information in the certificate is incorrect or has changed

The signatory acknowledges:

- ☒ In case the signatory loses his password, there is no possibility for reconstruction at the CA and therefore a chargeable new key generation and certificate issuance must take place.
- ☒ Five password misentries lead to account ban that only will be reversed in case the signatory can credibly assert that he caused the misentries himself

9. SIGNATURE PRODUCTS AND PROCEDURES

For the creation and verification of qualified electronic signatures and seals, the operator either recommends special products and procedures or provides them. The signatory is obliged to use only recommended or provided products and procedures, taking into account any conditions of use. The enumeration is of demonstrative character, further products will be published continuously on the website of the operator (<https://globaltrust.eu/geeignete-signaturerstellungseinheiten/>).

Suitable signature creation devices for the TRUST2GO® qualified mobile signature

Product: TRUST2GO

Type: remote-QSCD-Gesamtssystem

Conformity Assessment Body: A-SIT (AT)

Conformity Assessment Report: AIT VIG A-SIT-VIG-20-105 (<https://www.a-sit.at/downloads/1909>)

Ausgestellt: 12.07.2022

Certification: § 7 ABS. 1 SVG IVM ART. 30 ABS. 3 LIT. B EIDAS-VO

Signature suite:

RSASSA-PKCS1-v1_5 according to PKCS#1 v2.2 (RFC 8017) with key lengths 2048, 3072 or 4096 Bit,

RSASSA-PSS according to PKCS#1 v2.2 (RFC 8017) with key lengths 2048, 3072 or 4096 Bit

ECDSA according to FIPS PUB 186-4 and the NIST29-curves P-256, P-384 or P-521 with parameters p, q length 256, 384 or 512 Bit,

Hash functions

SHA31-256, SHA-384 and SHA-512 according to ISO32/IEC33 10118-3 / FIPS 180-4

Suitable signature creation devices for qualified signatures:

Product: Atos CardOS v5.3

Type: Smartcard

Conformity Assessment Body: A-SIT (AT)

Conformity Assessment Report: A-SIT-1.108 Sichere Signaturerstellungseinheit CardOS V5.3 QES, V1.0

(http://www.a-sit.at/de/bestaetigungsstelle/bescheinigungen_sigg/veroeffentlichungen.php)

Published: 08.08.2014

Certification: Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5

Signature suite:

- ECDSA12 according to ANSI X 9.62 or ISO/IEC 15946-2 with lengths of the parameters p, q of 256 or 384 bits. The curves P-256 or P-384 according to FIPS PUB 186-4 as well as brainpoolP256r1 or brainpoolP384r1 according to RFC 5639 are supported.

Hash function: SHA-2

Suitable card readers

A Conformity assessment is not mandatory for the operation of a card reader according to the Austrian signature regulations, but can be helpful for the selection of reliable devices. On request, GLOBALTRUST will test desired card readers and issue a Conformity assessment under which conditions they are suitable for GLOBALTRUST smart cards.

Basically, all card readers that support ISO 7816 are suitable for the use of GLOBALTRUST smart cards.

Suitable signature software

GLOBALTRUST QUALIFIED

e-commerce monitoring GmbH, 1160 Wien, Redtenbacherg. 20

Geschäftsadresse: A-1020 Wien, Handelskai 388 (Eingang Wehlstr. 299/6/EG/621) <http://www.globaltrust.eu>

Gerichtsstand Wien

Information gemäß DSGVO <http://e-monitoring.at/dsgvo.html>

info@e-monitoring.at

☎ +43/01/5320944, Fax +43/1/5320974

UID: ATU54992708 HG Wien FN 224536 a

[text.29683nbnr]

Trust, we verify!

The specification of a format for data to be signed must be generally available and must ensure that the signed data can be represented without doubt and with the same result both during signature creation and signature verification. If dynamic changes can be encoded in a format, those elements that can cause dynamic changes must not be used.

Product: e-Sign Agent

Document formats: pdf

Signatur formats: Adobe (pdf)

Hints: free software provided by GLOBALTRUST

Download Windows: <https://service.globaltrust.eu/static/eSignAgent.msi>

Documentation: <https://service.globaltrust.eu/static/trust2go-benutzer.pdf>

10. REVOCATION, SUSPENSION AND CERTIFICATE PROBLEM REPORT

The operator provides the following:

(a.) Suspension

The validity of a certificate is temporarily suspended, can be triggered manually or automatically and is valid for a maximum of 10 days

(b.) Revocation

Leads to premature invalidation of a certificate. Re-activation is excluded.

The fact of revocation or revocation of a certificate is publicly available. The use of the directory and revocation service is free of charge and anonymous.

Electronic signatures issued before revocation or suspension remain valid.

Requests for revocation should be submitted as soon as possible via <https://www.globaltrust.eu/revocation.html>. Alternatively, revocations may also be requested by email to revocation@globaltrust.eu or by telephone. In any case, sufficient authorization for revocation must be proven, for example by online authentication.

Revocation reasons include:

- The subscriber requests it
- The original certificate request was not duly mandated
- the private Key has been compromise or does not any longer comply with technical standards
- Components, information or procedures fort he private Key usage have been compromised
- certificate abuse
- The signatory is no longer legally permitted to use a designation in the certificate
- The operator becomes aware of a significant change to the information recorded in the certificate.-

Circumstances arise that make the technical content or format of the certificate an unacceptable security risk.

(c.) Deactivation

At the request of the signatory or by the operator, instead of a block or revocation, only a deactivation of the 2nd authentication procedure can be performed, if the private key is not compromised, but there are other concerns in the signature process (loss of the cell phone,...).

(d.) Certificate Problem Report

In the event of any certificate-related problems, for example if misuse is suspected, anyone involved can contact the operator at abuse@globaltrust.eu or by telephone.

11. LIABILITY

The operator has a liability insurance with an insurance company with sufficient solvency that meets the legal requirements.

The operator does not provide insurance for end users, the warranty extends to the features warranted in the GLOBALTRUST Certificate Policy. This does not affect or limit warranties based on statutory requirements.

The operator complies with all requirements according to the applicable Austrian and European data protection regulations. Unless otherwise regulated, the provisions of the Austrian Data Protection Act as amended from time to time shall apply on the basis of the European Union Data Protection Directive EC/46/95 or any successor regulation of the European Union.

The operator shall comply with all necessary information, clarification and consent obligations of the applicable data protection provisions.

The operator is responsible:

- for observing this policy in its own realm of responsibility, in particular for the measures contained within for the prompt publication of suspension and revocation lists and for the maintenance of suspension and revocation standards named in this policy.
- for informing applicants, subscribers and users of signatures, certificates and public keys of their obligations to observe the policy. It is proved that this has been communicated if the certificates issued by the operator contain clear reference to the location of documentation for the applicable policy.
- for ensuring that the applicant data contained in a certificate is verified at the time that the certificate is issued and that the data does not differ from the data in registries used for verification or from documents submitted. Verification measures are documented in this policy. The registries used for verification depend on the kind of applicant and can include technically or regionally different sources. Which sources are used for which applicant is documented in detail in the operator's internal process documentation.
- for following up on evidence that a registration office or other persons or organisations authorised by the operator have established a deficiency in verification of identity and ensuring that certificates are not issued without sufficient identification of the subscriber and that certificates are immediately revoked if there is reason to doubt that an identity verification has not been conducted properly.
- that a qualified certificate for electronic signatures matches the signature creation data in a qualified signature creation device, if this has been issued by the operator. Otherwise that the subscriber was in the possession of the QSCD at the time that the qualified certificate for electronic signatures was issued.

The operator guarantees indemnities for proven damages for which it is responsible.

12. *USEFUL LINKS*

1. Imprint

- <https://globaltrust.eu/imprint>

2. Legal repository

- <https://globaltrust.eu/en/certificate-policy-2/>

3. Suitable signature Products (including qualified signature creation devices)

- <https://globaltrust.eu/geeignete-signaturerstellungseinheiten/>

4. Limits

- <https://globaltrust.eu/limitation>

5. Directory

- <https://www.globaltrust.eu/directory.html>

6. Revocation, Suspension

- <https://www.globaltrust.eu/revocation.html>