GLOBALTRUST

powered by e-commerce monitoring gmbh

[CQINFO-WEB-EN] Information on the use of qualified server certificates GLOBALTRUST SERVER QUALIFIED according to Article 24 eIDAS Regulation

Author: Daniel Zens

Version 1.0a/ 6th February, 2024

OID-Number/Nummer: OID-Nummer: 1.2.40.0.36.1.2.5.1

Publication: https://service.globaltrust.eu/static/general-web-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

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 Vertrauensdienstanbieters.

1. GENERAL

This preliminary information is intended for certificate applicants, signers and other third parties who have a legal interest in the GLOBALTRUST certificate products.

This document can be accessed at https://www.globaltrust.eu/static/general-web-en.pdf and is provided with a qualified electronic signature according to eIDAS-VO.

Further information can be requested at the Trust Service Provider (TSP) e commerce monitoring GmbH or retrieved online at https://globaltrust.eu/en/certificate-policy-2/

2. VALIDITY OF THIS DOCUMENT

Editorial Deadline: 6th February, 2024
Shortcut: [CQINFO-WEB-EN]
Titel: Information on the use of qualified server certificates GLOBALTRUST SERVER QUALIFIED
Fehler! Verweisquelle konnte nicht gefunden werden.
OID-Number: 1.2.40.0.36.1.2.6.1
Contact for general questions about certificates and electronic signatures: info@globaltrust.eu
Information on GLOBALTRUST- certificate products: http://www.globaltrust.eu

3. REFERENCES

In connection with this document, reference is made to the following documents in their respective valid versions:

[GCP] GLOBALTRUST Certificate Policy (public, OID-Number: 1.2.40.0.36.1.1.8.1, http://www.globaltrust.eu/static/globaltrust-certificate-policy.pdf)

[GCPS] GLOBALTRUST Certificate Practice Statement (public, OID-Number: 1.2.40.0.36.1.2.3.1, http://www.globaltrust.eu/static/globaltrust-certificate-practice.pdf)

[eIDAS-VO] REGULATION (EU) Nr. 910/2014 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing the directive 1999/93/EG, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&rid=1

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

[CABROWSER-EV] CA/Browser-Forum Guidelines For The Issuance And Management Of Extended Validation Certificates, https://cabforum.org/extended-validation/

4. USED DEFINITIONS

In connection with this information, the following terms are used in accordance with the GLOBALTRUST Certificate Policy:

Excerpt from the [GCP] GLOBALTRUST Certificate Policy section "1.6 Definitions and Abbreviations"

Electronic signature
Data in electronic form according to EU signature regulation [eIDAS-VO], which is attached or logically linked to electronic data and authenticates it.

Advanced electronic signature
An electronic signature that fulfils the following criteria:
a) it is assigned exclusively to the subscriber;
b) it enables the identification of the subscriber;
c) it is created by means that the subscriber can keep under their sole control;
d) it is linked to the data to which it refers in such a way that later changes to the data can be recognised.

Qualified electronic signature
An electronic signature that fulfils the following criteria:
- all criteria of an advanced electronic signature,
- that is based upon a qualified certificate and
- has been created by a qualified signature-creation device (QSCD).

Certificate
An electronic attestation that assigns signature verification data to a subscriber and confirms the identity of that signatory, the legal entity he represents, or a system controlled by him or his legal entity.

Qualified certificate for electronic signatures
A certificate for the creation of electronic signatures that it is issued with the latest technology and fulfils, in particular, the requirements in [eIDAS-VO] Appendix I and is provided by a Certification Service Provider (CA) that fulfils the requirements in [eIDAS-VO].
The content follows [ETSI EN 319 412]. The validity period of the qualified certificate for electronic signatures is limited to 5 years by law and can be shortened by the CA for legal or other important reasons at any time.**Qualified server certificate**
A certificate for website authentication that it is issued with the latest technology and fulfils, in particular, the requirements in [eIDAS-VO] Appendix IV as well as [CABROWSER-EV] and is provided by a Certification Service Provider (CA) that fulfils the requirements in [eIDAS-VO].
The content follows [ETSI EN 319 412] as well as [CABROWSER-EV] The validity period of the qualified server certificate is limited to 825 days by law and can be shortened by the CA for legal or other important reasons at any time. Qualified server certificates issued on or after 1st September 2020 will have a validity period no greater than 397 days..

Qualified certificate

The certificate can be issued either as a qualified certificate for electronic signatures or as a qualified server certificate and contains a reference to the certificate policy under which the certificate has been issued and which clearly identifies it as a qualified certificate.

The subject is encoded according to UTF-8 if it contains umlauts or special characters. PrintableString can be used if it does not contain umlauts or special characters.

The subject can contain the following inputs: countryName (mandatory), localityName (mandatory), stateOrProvinceName (optional), organizationName (if the certificate is being issued for an organisation), organizationalUnitName (optional), commonName or pseudonym or givenName (it is mandatory to fill in one), title (optional), serialNumber (mandatory), businessCategory (mandatory in case of qualified server certificates), jurisdictionLocalityName and/or jurisdictionStateOrProvinceName and/or jurisdictionCountryName (only in case of qualified server certificates, usage according to [CABROWSER-EV]) Each field can only be used for those inputs which are defined according to the applicable standards and norms.

Further information in the certificate:

- X509v3 Key Usage: critical Digital Signature, nonRepudiation and Key Encipherment (in case of qualified server certificates)
- X509v3 Extended Key Usage: mandatory at least one entry, e.g. TLS Web Server Authentication and/or TLS Web Client Authentication AnyExtendedKeyUsage is not used.
- CA Issuers - URI:http://service.globaltrust.eu/static/globaltrust-NN-**-der.cer
- X509v3 CRL Distribution Points: Full Name: URI:http://service.globaltrust.eu/static/globaltrust-NN-**.crl
- OCA - URI:http://OCA-NN-**.globaltrust.eu
- X509v3 Certificate Policies: Policy: 1.2.40.0.36.1.1.##.1
- CPS: http://www.globaltrust.eu/certificate-policy.htm Policy:
- X509v3 Certificate Policies: Policy: 1.2.40.0.36.1.1.##.1

• 0.4.0.1456.1.1 (qualified certificates for electronic signatures issued before 15.12.2021)
• 0.4.0.194112.1.2 (qualified certificates for electronic signatures issued on or after 15.12.2021)
• 0.4.0.194112.1.3 (qualified certificates for electronic seals)
• 0.4.0.19431.1.1.3 (qualified remote signatures)
• 0.4.0.194112.1.4 (qualifizierte server certificates) and 2.23.140.1.1 (qualified server certificates, if also EV compliant)

- 1.2.40.0.36.4.1.3: [Serial number of the signature-creation device as ASN1 OCTET STRING]
- qcStatements:
- id-etsi-qcs-QcCompliance (OID 0.4.0.1862.1.1),
- id-etsi-qcs-QcLimitValue: QcEuLimitValue (OID 0.4.0.1862.1.2) (optional)
- id-etsi-qcs-QcRetentionPeriod: QcEuRetentionPeriod (OID 0.4.0.1862.1.3) (optional)
- id-etsi-qcs-QcSSCD (OID 0.4.0.1862.1.4)
- id-etsi-qcs-QcType (OID 0.4.0.1862.1.6)
- id-etsi-qct-esign (OID 0.4.0.1862.1.6.1)
- id-etsi-qct-eseal (OID 0.4.0.1862.1.6.2)
- id-etsi-qct-web (OID 0.4.0.1862.1.6.3)
- Administration attribute "Verwaltungseigenschaft" (OID 1.2.40.0.10.1.1.1): Administration identifier (optional)
- Operator attribute "Dienstleistereigenschaft" (OID 1.2.40.0.10.1.1.2): NULL (optional)
- Official attribute "Organwaltereigenschaft" (OID 1.2.40.0.10.3.4): Administration identifier (optional)
- Attribute of signature for electronic authority (OID 1.2.40.0.10.1.7.2): NULL (optional)

- further OID inputs if they are in accordance with the conditions for qualified certificates (optional)

SIGNATURE ALGORITHM USED: SHA2 (SHA256WITHRSAENCRYPTION OR HIGHER)5. OPERATINIONAL CONTROLS OF THE TSP

The certification activities of the TSP are subject to the supervision of the Austrian Supervisory Body Telekom-Control-Commission (TKK) and RTR-GmbH, both A-1060 Vienna, Mariahilfer Strasse 77-79. Contact details for the supervisory body can be found at https://signatur.rtr.at/

The TSP's activity was accredited on June 29, 2015 according to TKK decision A 4/2014-36. Since July 1, 2016, the activity has been carried out in accordance with the eIDAS regulation.

Information on the TSP and it's certification services can be found at the supervisory body at https://www2.rtr.at/de/vd/Zertifizierungsdiensteanbieterdetails?anbieter=ecm.

The certification services are provided on the basis of the following documents in the currently valid version:

- [GCPS] GLOBALTRUST Certificate Practice Statement (public, OID-Nummer: 1.2.40.0.36.1.2.3.1, http://www.globaltrust.eu/static/globaltrust-certificate-practice.pdf)
- [GCP] GLOBALTRUST Certificate Policy (public, OID-Number: 1.2.40.0.36.1.1.8.1, http://www.globaltrust.eu/static/globaltrust-certificate-policy.pdf)
- [GCSP] GLOBALTRUST Certificate Security Policy (non public)

Other economic conditions that are 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 TSP (https://e-monitoring.at/static/terms.pdf).

6. SECURITY CONCEPT

The security concept of the TSP is fully described in the [GCP] GLOBALTRUST Certificate Policy.

1. GENERAL SECURITY INFORMATION

Excerpt of the [GCP] GLOBALTRUST Certificate Policy Section "6. TECHNICAL SECURITY CONTROLS ":

The operational infrastructure of the operator is checked and adjusted to changed requirements regularly. Changes that affect the extent to which security is achieved must be approved by the certification committee as per the role concept (⇨ GLOBALTRUST Certificate Security Policy). In the event of a change of the GLOBALTRUST Certificate Security Policy, the responsible regulatory authorities are informed.

Technical operations are conducted in the offices of the operator or a sufficiently qualified contractor. Current contractors are fully documented and can be disclosed to the regulatory authority at any time. All contractors are bound to protect data security in accordance with this policy, [DSGVO], signature requirements and other relevant legal requirements and technical standards, as it concerns the activity assigned to them.

The operator uses signature and cryptographic keys to perform certification services and internal (administrative) business processes where technically possible, technically necessary for security and economically acceptable.

2. *SPECIFIC SECURITY INFORMATION*

Excerpt from [GCP] GLOBALTRUST Certificate Policy Section "5. 5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS ":

The CA is responsible for the organisation and documentation of all processes in the context of certification services (including time stamp services). This also applies to services outsourced to a contracted partner. The documentation formats used are a part of the GLOBALTRUST Certificate Security Policy. The documentation method used is internally documented.
The tasks and assigned responsibilities of the contracted partner are clearly regulated. In addition, controls are established to check that activities are performed properly.
The certification service includes the technical (automated) permanent availability of the revocation list. This also applies to the automated acceptance of revocation requests.
The availability of central certification services

- *distribution of CA certificates*
- *suspension and revocation management and*
- *distribution of revocation statuses*

uses redundant system components and is subject to continual supervision. The availability target of the central certification services is 99.9% in a month. Availability is measured and recorded by the operational monitoring. The records are kept for at least a year and register the start and end points of failures. If the availability target has not been reached in a particular month, additional organisational and technical measures are deployed to improve availability.

All operational procedures are documented and are subject to this GLOBALTRUST Certificate Policy, the GLOBALTRUST Certificate Security Policy and the applicable GLOBALTRUST Certificate Practice Statement.

The certification services are conducted only in appropriate premises. The details are as set out in the GLOBALTRUST Certificate Security Policy.

It is ensured that access to the premises in which functions critical to security are performed is restricted and that the risk of physical damage to facilities is minimised.
In particular, the following security measures apply:

1. *Access to devices upon which certification and revocation services are performed is restricted to authorised personnel only. The systems that issue certificates are physically protected from the threat of environmental disasters.*
2. *Security measures are taken to prevent the loss, damage or compromising of facilities and interruption of operations.*

Power and air conditioning are available in sufficient quantity

The location of components critical to certification is selected so that water damage is unlikely.
Sufficient precautions are made to protect against fire.
Media is stored securely away from components critical to certification

Certification services (particularly application, issuance, processing and revocation of certificates) are performed under a strict separation of administrative and technical operations.
Organisational measures for secure management are of central importance to the operator.
Particularly in the event of failure or unforeseen events ("stress" situations), appropriate strategies

and general measures should cover instances that could not fully be defined as business processes beforehand.

Main general measures include:
a) four-eyes principle for critical processes
b) motivated employees
c) clear and distinct distribution of responsibilities
d) comprehensive documentation of operational events
e) cooperative exchange of information in the context of an institutionalised certification committee

All administrative business processes relevant to certification are documented in an internal content management and monitoring system. These processes are described, administered and used in internal documentation.

The role concept, role description and role responsibilities are defined in the [GCSP] GLOBALTRUST Certificate Security Policy. *Changes in the distribution of roles are to be carried out so that all the activities necessary in this practice statement and in the certificate policies can be fulfilled and a satisfactory replacement provided.*

Critical processes are subject to the four-eyes principle. The persons involved are documented.

All employees engaged in certification services have the necessary expertise, in particular employees who administer the orders of signature products, supervise technical operations and conduct development of certification products.

The management of the CA can task suitable authorised persons or suitable contractors according to the role concept in this policy (GLOBALTRUST Certificate Security Policy) for the purpose of performing certification services. These persons or contractors plan and implement all operative measures including the establishment of necessary documentation, certification guidelines and operational premises.

The following events are subject to special documentation:
- Exceptional situations in operation (inc. maintenance, system failures,...) are documented by the monitoring system and additional comments and explanations can be added if required. The monitoring data is regularly signed and archived.
- All relevant events that occur in the course of certificate issuance are logged, in particular all events that concern the life cycle of issued certificates and cross-certificates.
- All events that concern applications for new certificates, applications for the renewal of certificates and the approval of applications are documented.

The compromising of a CA key is considered a worst-case scenario. A compromise is the transfer of the CA private key to third parties in a form that makes use / exploitation possible.
In this event, the CA immediately briefs and informs the regulatory authority, the subscribers, persons who rely on the certification services, and if necessary other certification service providers and organisations with whom the CA has relevant agreements (such as software- and browser vendors), that the revocation and certificate information can no longer be seen as reliable. If necessary, the public is informed via the website https://www.globaltrust.eu/

Certificates and revocation lists will immediately be marked as no longer valid. The subscriber will be issued with a new certificate with the aid of a newly generated secure CA key.

The operator has taken precautions in case of the failure of individual operational components. Certification services will then be in failure operation (partial functionality is available) instead of normal operation (full functionality is available). Details are described in the GLOBALTRUST Certificate Security Policy.

The transition from normal operation ("primary") to failure operation ("disaster recovery") is mostly automatic and takes five minutes including delays. The maximum permitted outage that still allows an automated transition from normal operation to failure operation is described in the internal GLOBALTRUST Certificate Security Policy as a worst-case scenario. Additional failures require manual intervention by authorised staff. The response time for manual intervention is a maximum of 24 hours, but a response is made within the time requirements of the regulatory authority at least.
Where alternative services or systems are used, these comply with the same security requirements as the main system.
The transition from normal operation to failure operation and other failure procedures are tested at regular intervals to an extent that is reasonable and economically acceptable.

There is a risk analysis for all central components of certification operations, which is described in the GLOBALTRUST Certificate Security Policy. In this risk analysis, the procedures for restoring normal operation after resources have been compromised are also described.

7. PROPERTIES OF QUALIFIED SERVER CERTIFICATES

The TSP offers qualified server certificates in the variant defined in the [eIDAS-VO].

Qualified certificates are only issued to clearly identified persons.
The identity check can be carried out by the personal presence of the applicant and the submission of suitable official personal documents. It can also be done remotely by sending clearly legible copies of suitable official personal documents in advance. In the second case, instead of the identity check, the first step is a plausibility check on the submitted documents. The identity check is carried out when the documents for the qualified certificate are handed over by appropriately authorized persons or in the course of an alternative identification method certificated as aequivalent to the physical presence..

Excerpt of the eIDAS Section 3
"certificate for website authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;"
"qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;"
Excerpt of the [CABROWSER-EV]:
"[EV Certificates] Identify the legal entity that controls a Web site: Provide a reasonable assurance to the user of an Internet browser that the Web site the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information; and
Enable encrypted communications with a Web site: Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet

between the user of an Internet browser and a Web site […] Make it more difficult to mount phishing and other online identity fraud attacks using Certificates; Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users[…]"

8. SIGNATOR'S OBLIGATIONS

Excerpt from the [GCP] GLOBALTRUST Certificate Policy section "4.5.1 Subscriber private key and certificate usage

The subscriber is obligated to:

1. input complete and correct information in compliance with the requirements of this policy, especially during the registration procedure.

2. verify that all information in the certificate is correct directly after successful delivery

3. retain the private key to a hardware unit to which the subscriber has sole access (for example, encrypted storage of a private key using a password, signature PIN or passphrase, special signature creation devices that prevent or essentially complicate the reading of a private key). For simple signatures, for example GLOBALTRUST CLIENT, limitations on access and organisational measures that limit access to the computer that contains the key and the certificate are also understood to be sufficient security measures for the purpose of this policy.

3a. In the case of private key management by the operator or a third party on behalf of the signatory in the context of server-based signature services, the signatory shall keep all components, information and procedures for the use of the private key under its sole control and protect them from access by unauthorised third parties.

3b. 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.

3c. retain the private key to a hardware unit to which the only duly mandated representatives of the subscriber (creator of a seal) have access. For example, encrypted storage of a private key using a password, signature PIN or passphrase, special seal creation devices that prevent or essentially complicate the reading of a private key. For simple seals, for example GLOBALTRUST CLIENT, limitations on access and organisational measures that limit access to the computer that contains the key and the certificate are also understood to be sufficient security measures for the purpose of this policy.

3d. In the case of private key management by the operator or a third party on behalf of the subscriber in the context of server-based signature services, the signatory shall keep all components, information and procedures for the use of the private key under their control and protect them from access by unauthorised third parties.

3e. Insofar as a mobile telephone number is required for the use of the private key, the creator of a seal shall use a telephone number that only can be used by duly mandated representatives..

3f. 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.

4. in the case of self-generation of a private key, appropriate secure procedures should be applied to ensure a sufficient quality of randomness in the generation of keys. In particular, these are hardware components explicitly intended for this purpose, such as HSM modules, or software components, which allow their user to increase the quality of randomness through system events (in particular the entry of files with random numbers, the performance of movements of the mouse or keystrokes during key generation). The CA reserves the right to require full disclosure of information on the key generation procedure from the subscriber and to reject a certification application if

concerns arise over the quality of randomness of the key. Inappropriate key procedures are detailed on the website of the operator and may not be used.

5. use appropriate caution to prevent the unauthorised use of the private key.

6. use server certificates exclusively on devices that are accessible from the addresses listed in the certificate (for X.509v3 in the subjectAltName extension).

7. inform the operator immediately if one or more of the following circumstances arise before the validity of the certificate has expired:

- 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 private key of the subscriber or its activation data may have been compromised,

- The mobile phone has been stolen or otherwise got lost, in case a mobile phone is required as a signature activation component

- exclusive control over the private key has been lost,

- the information in the certificate is incorrect or has changed,

8. completely remove the key from operation immediately as soon as the subscriber becomes aware that it has been compromised.

9. completely remove the keyfrom operation if informed by the operator that the CA key has been compromised.

10. the secure safekeeping of the key remains the sole responsibility of the subscriber.

11. 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.

12. The subscriber should inform the user of signed data of his obligations for the purpose of this policy in a suitable way. He may not conclude agreements or provide explanations to a third party that contradict this policy, the applicable standards, the valid juridical, in particular legal, conditions, or the GLOBALTRUST Certificate Practice Statement.

13. The following limitations apply to the issuance of qualified certificates for electronic signatures:

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.

14. In the event that the CA key or subscriber key has been compromised, the subscriber should follow the instructions of the CA within 48 hours. This time span is shortened if specific security risks are expected. In this event, the subscriber will be informed of the shortened reaction time by telephone, email or other suitable means.

15. The subscriber accepts that the CA can revoke a certificate in the event of a violation of the conditions of this policy, other agreements concluded with the subscriber, or the use of the certificate for criminal or fraudulent activities. Compensation will not be paid for a certificate revoked on these grounds or for resulting damages.

16. The signatory accepts that:

- In case the signatory looses 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. *LIABILITY OF THE TSP*

Excerpt from the [GCP] GLOBALTRUST Certificate Policy section "9. 9. OTHER BUSINESS AND LEGAL MATTERS ":

The CA has arranged indemnity insurance with an insurance company of sufficient solvency that complies with legal requirements and if applicable with [CABROWSER-EV] and [WEBTRUST-EV]. The insurance arranged is documented internally.

The CA does not provide insurance for end users. The warranty covers the features promised in the GLOBALTRUST Certificate Policy. This does not affect or restrict warranties based on legal regulations.
The CA fulfils all requirements as per the applicable Austrian and European data protection laws. If not otherwise regulated, the regulations of the Austrian data protection law applies in its current version on the basis of the data protection guidelines of the General Data Protection Regulation 2016/679 of the European Union or successor regulation of the European Union

The CA 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 CA 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 CA internal process documentation.*
- *for following up on evidence that a registration office or other persons or organisations authorised by the CA 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 signature creation device, if this has been issued by the CA. Otherwise that the subscriber was in the possession of the SSCD at the time that the qualified certificate for electronic signatures was issued.*

This responsibility applies similarly for all certificates that have been issued using enduser-sub-certificates.

Software producers that distribute the root certificates of the CA are not responsible for the content of the certificates. They are held harmless by the CA where this is legally permitted and does not affect procedures for which the software producer is responsible. The software producer is responsible for ensuring that validity status is displayed correctly in the certificates of the CA.

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

10. CONDITIONS OF USE OF CERTIFICATES

Excerpt from the [GCP] GLOBALTRUST Certificate Policy section 4.5.2

Legitimate uses are derived from the certificate's contents, the GLOBALTRUST Certificate Policy and the applicable GLOBALTRUST Certificate Practice Statement.

With regard to signature-creation devices, there are no obligatory technical guidelines for advanced signatures. The subscriber is free to use the signature-creation device at his discretion, but must ensure sole personal control of the signatures assigned to him as is legally compulsory.
Binding transactions with a value over 100 000 EUR require a qualified certificate for electronic signatures.
If it is not possible to verify the certificate of an electronic signature, it is the sole responsibility of the relying party whether or not they recognise the validity of the signature. The CA holds no responsibility in this regard.
It is permissible to announce limitations on the use or validity of the certificate on the website or in otherwise published conditions (in particular notice of the maximum transaction value for which the signature can be validly issued). The responsibility of the CA is also limited in line with the given limitations and maximum amounts.
Additional limitations can also arise from the type of certificate issued and its usage.
The subscriber is required to use the Key Pair only in accordance with this Policy and to use only the key generation algorithms and parameters described in this Policy.

11. USEFUL LINKS

1. Impressum / General legal information about the TSP (including reports of abuse)
   - http://www.globaltrust.eu/impressum.html
   - http://www.globaltrust.eu/abuse.html

2. Public overview of the applicable policies
   - http://www.globaltrust.eu/certificate-policy.html

3. Product overview (incl. products suitable for qualified certificates, time accuracy of the time stamp services)
   - http://www.globaltrust.eu/produkte.html

4. Limits/specifications when using/issuing certificates
   - http://www.globaltrust.eu/limitation.html

5. Directory service
   - http://www.globaltrust.eu/directory.html

6. Blocking and revocation
   - http://www.globaltrust.eu/revocation.html

7. Third Party Recognition of Root CA
   - http://www.globaltrust.eu/thirdparty.html

8. Reports on the availability of the certification services (including time stamp services)

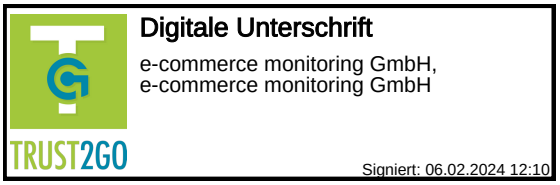
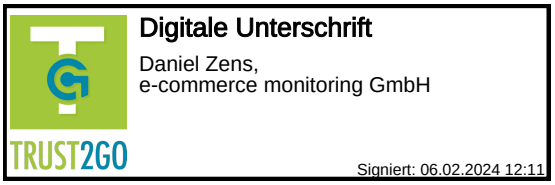
- http://www.globaltrust.eu/auditreport.html

9. Online-Support

- http://www.globaltrust.eu/support.html

10. Certification partner

- http://www.globaltrust.eu/partner.html

11. News

- http://www.globaltrust.eu/news.html