

Policy for the Qualified Timestamping Service of the BEV

Version 1.4
20. February 2009

1 Document Information

1.1 Purpose and Validity

This document contains the Policy for the Qualified Timestamping Service of the BEV. It is published by the BEV and announced according to § 6 Abs. 2 SigG to the Telekom-Control-Kommission as the supervisory authority for electronic signatures.

1.2 Document History

| VERSION | DATE | REASON FOR CHANGE IN THIS DOCUMENT |
|---------|------------|--|
| 1.0 | 30.11.2006 | Version to announce the start of the service to the TKK |
| 1.1 | 16.12.2007 | Changes on the website under point 3.1 on www.bev.gv.at |
| 1.2 | 13.07.2007 | Note under 3.4 that MD5, SHA-1 are not used due to security concerns and, furthermore, according to recommendation 2048-bit encryption is used |
| 1.3 | 03.04.2008 | Change of BEV's telephone and fax number under point 3.1 to Tel. +43(0)1-211 10-0, Fax +43(0)1-211 10-2199 |
| 1.4 | 20.02.2009 | Adjustment of the document due to the amendment of the Signaturgesetz BGBl I Nr. 8/2008 and BGBl I Nr. 59/2008 plus the Signaturverordnung BGBl II Nr. 3/2008 and the Verordnung des Bundesamtes für Eich- und Vermessungswesen über die Darstellungsverfahren der gesetzlichen Maßeinheiten für die Zeit und Frequenz, Amtsblatt für das Eichwesen Nr. 3-4/2008, page 4. Change of contact information. Change of „Bundesministerium für Wirtschaft und Arbeit“ to “Bundesministerium für Wirtschaft, Familie und Jugend“ |

2 Content

| | | |
|----------|--|-----------|
| 1 | Document Information | 2 |
| 1.1 | Purpose and Validity | 2 |
| 1.2 | Document History | 2 |
| 2 | Content | 3 |
| 3 | Introduction | 4 |
| 3.1 | Bundesamt für Eich- und Vermessungswesen (BEV, Austrian Federal Office of Metrology and Surveying) | 4 |
| 3.2 | Identification | 4 |
| 3.3 | Area of Application of the Qualified Timestamping Service | 4 |
| 3.4 | Algorithms and Formats Used for the Qualified Timestamping Service | 4 |
| 3.5 | Expected Service Life of the Timestamp | 5 |
| 3.6 | Accuracy of the Timestamp | 5 |
| 3.7 | Terms of Use | 5 |
| 3.8 | Obligations of the BEV as Provider of the Qualified Timestamping Service | 5 |
| 3.9 | Obligations of the Users of the Timestamping Service | 6 |
| 3.10 | Obligations of those Trusting in the Timestamp | 6 |
| 3.11 | Information on the Verification of Timestamps | 6 |
| 3.12 | Archiving Period of the Log Information | 7 |
| 3.13 | Applicable Legal Provisions | 7 |
| 3.14 | Limitations of Liability | 7 |
| 3.15 | Settlement of Disputes | 8 |
| 3.16 | Declaration of Conformity | 8 |
| 4 | Key Management | 9 |
| 4.1 | Generating the Keys for the Timestamping Service | 9 |
| 4.2 | Protection of the Private Key | 9 |
| 4.3 | Distribution of the Public Keys | 9 |
| 4.4 | Rekeying | 10 |
| 4.5 | End of the Life Cycle of the Private Keys | 10 |
| 4.6 | Life Cycle of the Signature Creation Devices | 10 |
| 5 | Timestamping | 11 |
| 5.1 | Timestamps | 11 |
| 5.2 | Time Accuracy | 11 |
| 6 | Management and Operations | 12 |
| 6.1 | Security Management | 12 |
| 6.2 | Security-Relevant Facilities | 12 |
| 6.3 | Personnel Security | 13 |
| 6.4 | Physical Security | 14 |
| 6.5 | Organisational Security Measures | 15 |
| 6.6 | Access Protection | 15 |
| 6.7 | Trusted Systems | 16 |
| 6.8 | Disasters and Compromise | 16 |
| 6.9 | Cessation of Services | 17 |
| 6.10 | Compliance with Legal Requirements | 17 |
| 6.11 | Recording and Archiving | 18 |
| 7 | Appendix | 18 |
| 7.1 | Definitions and Abbreviations | 18 |

3 Introduction

3.1 Bundesamt für Eich- und Vermessungswesen (BEV, Austrian Federal Office of Metrology and Surveying)

The Bundesamt für Eich- und Vermessungswesen (BEV) is a subordinate authority of the Federal Ministry of Economy, Family and Youth. One of the tasks of the BEV is the maintenance of several atomic clocks. These atomic clocks are part of the worldwide network of time emitters from which all official time data in the member states of the International Meter Convention are derived.

This document describes the Qualified Timestamping Service (QZSD) operated by the BEV. A timestamping service is a service, by which any electronic document can be furnished with tamper-proof time data. A “qualified timestamping service” is a timestamping service that fulfils the respective high standards of the Austrian Signaturgesetz.

Contact information: Bundesamt für Eich- und Vermessungswesen, Physikalisch-technischer Prüfdienst (PTP), Arltgasse 35, 1160 Vienna, Tel. +43 1 211 10-6327, Fax + 43 1 211 10-6000, <http://www.bev.gv.at>, e-mail: ptp@bev.gv.at.

All relevant information concerning the Qualified Timestamping Service of the BEV, especially the up-to-date version of this Policy as well as the fees and conditions for using this service are published on www.bev.gv.at.

3.2 Identification

This policy contains all information necessary for a „Timestamp Policy“ according to Standard ETSI TS 102 023. Such documents are identified by an ASN.1 Object Identifier (OID), which is also indicated on the issued timestamp itself, to show the conformity of the issued timestamp with this standard. The OID of this Policy is: 1.2.40.0.10.1.8.1.

3.3 Area of Application of the Qualified Timestamping Service

The Qualified Timestamping Service of the BEV is offered publicly, provided that the conditions given under 3.7 are met; and it can be used for any purpose that makes it necessary to furnish an electronic document with tamper-proof time data from an independent, reliable body.

3.4 Algorithms and Formats Used for the Qualified Timestamping Service

The hash values of the documents to be timestamped which are transmitted to the Qualified Timestamping Service can be created with the algorithms SHA-1, RIPEMD-160, SHA-256, SHA-384 or SHA-512. Those are the cryptographic hash functions which are recommended by the Austrian bodies (Rundfunk und Telekom Regulierungs-GmbH and A-SIT) that were entrusted to execute the Austrian Signaturgesetz.

To calculate the hash value of the timestamp itself the algorithm SHA-256 is used. RSA is used as signature algorithm, the key length of all key pairs used for the Qualified Timestamping Service is 2048 bit, as advised by the standard.

The hash function MD5 is not supported. As the hash function MD5 never fulfilled the requirements of the Austrian Signaturverordnung and as experts doubt the collision resistance of SHA-1, these deviations from the standard seem to be necessary from the point of view of the RTR-GmbH as well.

The issued timestamp as well as the communication between the clients and the servers of the Qualified Timestamping Service meet the Standard RFC 3161.

3.5 Expected Service Life of the Timestamp

Due to technical progress cryptographic processes get weaker in the course of time. The processing power of computers increases exponentially as time elapses, thus ever longer cryptographic codes can be cracked by processing power. It will not be possible to crack the methods chosen by the BEV (RSA with 2048 Bit, SHA-256) for decades even with major financial efforts using the presently available methods and allowing for increasing processing power. Besides of the processing power also the scientific level of knowledge increases. Progress in cryptography might dramatically decrease the effort necessary to crack an algorithm. Other than the processing power, whose future development can be assessed quite easily by looking at the exponential increase during the last decades, scientific progress is more difficult to predict. The authorities responsible for the electronic signature thus usually just give recommendations for a few years (in Austria and Germany usually six years). The algorithms RSA 2048 Bit and SHA-256 are mentioned in this recommendation without restrictions until the respective expiration of the recommendation.

The BEV follows these recommendations: it can be assumed that the timestamps created by the Qualified Timestamping Service of the BEV cannot be forged for a period of at least six years even by making extraordinary financial efforts. The BEV will watch the relevant development and if need be exchange the algorithms used in accordance with the status of current research; up-date the Policy and put the information on the website.

3.6 Accuracy of the Timestamp

The security measures described in this document guarantee that no timestamp issued by the Qualified Timestamping Service of the BEV deviates by more than one second from the Coordinated Universal Time (UTC).

3.7 Terms of Use

The BEV reserves the right to offer the Qualified Timestamping Service free of charge to any user or to conclude service level agreements with certain users or user groups. As far as the service is offered free of charge and for any user, this is done for test purposes; any guarantee or liability is excluded. Insofar as the service is provided within the frame of service level agreements, the use depends on the particular service level agreements.

The Qualified Timestamping Service can be used to put a timestamp on any document. To create a timestamp, only a hash value but not the whole document is sent to the BEV. Thus the responsibility for the content of the document and for the correct calculation of the hash value rests solely with the user of the service.

For obligations of the users of the Qualified Timestamping Service please see 3.9, for obligations of those trusting in the timestamp please see 3.10 and 3.11, rules for liability see 3.14.

3.8 Obligations of the BEV as Provider of the Qualified Timestamping Service

The BEV as provider of a Qualified Timestamping Service has the duty to fulfil all relevant requirements in accordance with the Austrian Signaturgesetz and the Austrian Signaturverordnung. Under § 10 SigG one has to use technical components and procedures which secure the accuracy and authenticity of the time specification. § 18 SigG and § 6 SigV 2008 make demands concerning the applicable signature creation devices, and in particular the fulfilment of these requirements has to be verified by a confirmation body.

Furthermore the BEV commits to complying with the Standards ETSI TS 102 023 on which the Policy is based. Additional detailed requirements are derived from this European Standard, amongst others the accuracy of one second (see above 3.6).

3.9 Obligations of the Users of the Timestamping Service

The timestamping service meets the Standard RFC 3161. The timestamp server accepts requests that are formatted in accordance with this standard and answers with timestamps according to this standard or with an error message. The user is responsible for the correct calculation of the hash value of the document that is to be timestamped and that the applied hash function is correctly denominated in the timestamp request. The timestamping service does only accept the hash functions laid down under point 3.4 and thus verifies if the length of the transmitted hash value corresponds to the identifier of the hash function used by the user. As the document to be timestamped is not presented itself, the timestamping service cannot verify the correct calculation of the hash value by the user's software.

Please be aware of the fact that the BEV can rekey the used key pair of the timestamping service anytime (see below 4.4) and that the user cannot assume that a timestamp request is processed by a certain server due to the redundancies of the system. Therefore users of the certification service should use software that is not affected by rekeying.

Furthermore the users are obliged to comply with the terms of use mentioned under 3.7 and the concluded service level agreements.

3.10 Obligations of those Trusting in the Timestamp

Who wants to put his/her trust in the security value of the timestamp created by the Qualified Timestamping Service of the BEV, has to take into account the following information on the verification of timestamps and on liability.

3.11 Information on the Verification of Timestamps

The Qualified Timestamping Service meets the Standard RFC 3161. The algorithms mentioned above under 3.4 are used (RSA with 2048 Bit, SHA-256) for the signatures of the timestamps, the signatures are based on certificates in accordance with Standard X.509. To verify the validity of timestamps, software complying with these standards has to be used.

In order to make sure that the certificate on which the signature of the timestamps is based really is BEV's certificate, we advise to check the certificate chain right to the topmost certificate of the Austrian supervisory authority for electronic signatures, which keeps the directory of all Austrian certification service providers. The present top certificate of the Austrian supervisory authority is a self-signed certificate called „Telekom-Control-Kommission Top 1“, it will be valid until 13.09.2010 and is clearly recognisable by the SHA-1-fingerprint „91 49 29 ee c7 a0 21 b5 da 49 1a 35 a5 98 4c 2c f2 5b c7 55“. Information about possible changes referring to this are published by the Austrian supervisory authority in accordance with its security and certification concept on the website <http://www.signatur.rtr.at>, where the top certificate of the supervisory authority can be retrieved. All certificates relevant for the verification of the timestamp are also published on the website of the BEV.

All certificates in the certificate chain between the certificates of BEV's Qualified Timestamping Service and the top certificate of the supervisory authority include references to the corresponding revocation lists. In order to verify the authenticity and validity of a timestamp, one has to use software that can verify such certification chains and the corresponding revocation lists. Please be aware that many standard software products verify signatures and timestamps only at the present point in time and therefore send an error message if one of the verified certificates is already expired or has been revoked in the meantime. Especially with regard to the verification of timestamps that were issued several years ago, such error messages can be misleading. Therefore we advise to use software which is able to verify the certificate chain at the historic point in time when the timestamp was generated. At this point in time all certificates used at that time right to the top certificate of the supervisory authority must have been valid and not have been revoked. A later expiry of the validity period of a certificate or a later revocation of a certificate does not invalidate the issued timestamp. The security value of a timestamp decreases only due to

technical progress (see 3.5 above), but not because of the expiry of the validity or the revocation of one of the used certificates.

In case the Qualified Timestamping Service is used to determine the chronological order of documents (e.g. if applications are handled in the order of arrival) we recommend to use the distinctive serial number as measure and not the time of the timestamp. As the time specification does not include split seconds, several timestamps can show the same time. Furthermore, according to the principle of load balance the timestamps are created by at least two different timestamp servers, whose clocks can differ by split seconds. On the other hand, the serial numbers for all timestamps come from the same database system and therefore are a reliable source of information on the order of the issued timestamps.

3.12 Archiving Period of the Log Information

Every single timestamp creation is entered in a log file, it consists amongst others of the serial number of the timestamp, the time specification and the hash value of the timestamped document (but not the document itself), (see 6.11 below). This log information is archived for at least 3 years. During this period the BEV grants persons who claim legal interest (e.g. because a case is pending concerning a timestamped document) upon application access to the relevant entry in the log file.

Furthermore please see the information concerning liability under 3.14.

3.13 Applicable Legal Provisions

The BEV is a subordinate authority of the Federal Ministry of Economy, Family and Youth and has its head office in Vienna. It is subject to Austrian Law and the court of jurisdiction is in Vienna (unless special regulations apply).

According to § 3 Z 5 of the Verordnung of the Bundesamtes für Eich- und Vermessungswesen über die Darstellungsverfahren der gesetzlichen Maßeinheiten für die Zeit und Frequenz, Amtsblatt für das Eichwesen Nr. 3-4/2008 (Ordinance of the BEV on the Presentation Methods for Time and Frequency, Gazette for Metrology, no 3-4/2008), the BEV has to provide a Qualified Timestamping Service for public distribution.

In particular the Signaturgesetz (see §§ 10 and 18 SigG) and the Signaturverordnung 2008 (see §§ 11 and 12 SigV 2008) are relevant for the Qualified Timestamping Service.

As a provider of a Qualified Timestamping Service the BEV is subject to the supervision of the Telekom-Control-Kommission as supervisory authority for electronic signatures (§ 13 SigG). The provision of the timestamping service is announced in accordance with § 6 Abs 2 SigG to the supervisory authority; this policy and any changes are submitted to the supervisory authority. The supervisory authority publishes on its website <http://www.signatur.rtr.at> a directory of the Austrian certification service providers (abbreviated "ZDA" according to the Austrian Signaturgesetz), as well as information about the services provided by the ZDA (certification service providers).

3.14 Limitations of Liability

The Qualified Timestamping Service is subject to the Austrian civil law as far as indemnity provisions are concerned. § 23 SigG includes a special provision concerning the liability of the ZDA that issue qualified certificates or vouch for certificates of a ZDA from a Third country (§ 23 Abs. 1 SigG). The BEV does neither issue qualified certificates nor does it provide products, with the help of which persons can create qualified electronic signatures on their own behalf. But in accordance with §§ 10 and 18 SigG the BEV is obliged to use signature creation devices for its Qualified Timestamping Service that were certified under § 18 Abs. 5 SigG by a confirmation body.

As provider of a Qualified Timestamping Service the BEV does not know the timestamped documents. The Qualified Timestamping Service does merely receive the hash value of these documents, which does not give any information about the content of the document. Therefore the

BEV is by no means liable for the content of any document that bears a timestamp. In this context the BEV is only liable for the observance of the Policy. Essentially this means that incoming timestamp requests are checked for formal correctness; that the included hash value receives an exact time specification and that a timestamp meeting the Standard RFC 3161 is created and that technical components and procedures which comply with the requirements of the relevant legal provisions and of this Policy are used in the process.

The BEV does not guarantee a certain service life of the created timestamp. As stated under 3.5 it is to be expected that the timestamp is long-term tamper-proof. In this process the BEV follows the status of research and the recommendations of Austrian and foreign authorities for electronic signatures. However, it is not possible to completely rule out that startling scientific progress makes a technology that to date seemed to be long-term secure suddenly appear to be less secure. Everybody who has to rely on the security of technology has to bear that risk. In this regard, the BEV assumes no liability.

The Qualified Timestamping Service of the BEV is offered on at least two independent servers in two different locations. The components employed perform redundantly. Therefore the availability of the timestamping service is very high. However, the guarantee for the availability as well as the guarantee for the interoperability between the software used on the clients and on the timestamp servers is only warranted within the frame of service level agreements. For persons and institutions that have no such explicit agreement with the BEV, no availability whatsoever is guaranteed. The BEV can also allow persons and institutions – possibly also the general public – the free of charge use of the Qualified Timestamping Service for test purposes without signing a service level agreement. In this regard the BEV assumes no liability: Nor does the BEV assume liability for the interoperability and it reserves the right to restrict or block the access to the timestamping service at any time – without giving reasons or prior notice.

Liability for slight negligence (barring personal injury) is excluded.

3.15 Settlement of Disputes

The BEV will endeavour to find a solution to satisfy the users in case of complaints.

In accordance with § 15 Abs. 4 SigG customers or interest groups can submit disputes or complaints which have not been satisfactorily settled with a certification service provider, to the Rundfunk und Telekom Regulierungs-GmbH (<http://www.rtr.at>) for settlement. The jurisdiction of the ordinary courts remains untouched. The BEV will contribute to such arbitration processes in accordance with the rules of procedure issued by the RTR-GmbH and support an amicable solution.

3.16 Declaration of Conformity

This Policy is geared to the requirements and the structure of the Standard ETSI TS 102 023 v1.2.1 (2003-01) „Policy requirements for time-stamping authorities“. This European standard was also published as RFC 3628. The BEV fulfils all requirements of this standard.

In accordance with § 6 Abs. 4 SigG the BEV shall comply with the Policy presented to the supervisory authority when taking up the service as well as during operations. The BEV is under the supervision of the Telekom-Control-Kommission as supervisory authority for electronic signatures, which in particular refers to the compliance with the security and certification concept in accordance with § 13 Abs. 2 Z 1 SigG.

4 Key Management

4.1 Generating the Keys for the Timestamping Service

All key pairs of the Qualified Timestamping Service of the BEV are generated in a secured environment (see below 6.4) by two persons adhering to the four-eyes principle, who were entrusted with the role of key officers (see below 6.3). Exactly one key pair is generated for each server. All generated key pairs are consecutively numbered, starting with 01, i.e. at the start of the service the keys no. 01 and 02 are used.

The keys are generated in a secure signature creation device, which is either certified according to FIPS 140-1 (or FIPS 140-2) level 3 or higher or certified according to the Common Criteria Protection Profile EAL 4 (e.g. CWA 14169, CWA 14167-2, CWA 14167-4) or comparable security criteria (e.g. according to ITSEC). Fulfilment of security requirements according to § 18 Abs. 5 Signaturgesetz and § 6 Signaturverordnung has to be evaluated by a confirmation body. During key generation, the operational conditions have to be kept as per confirmation of the confirmation body (§ 6 Abs. 4 Signaturverordnung 2008) and the technical-organisational security measures under § 6 Abs. 3 Signaturverordnung 2008.

The keys are created in such a way and the signature creation device is configured in such a way that it is impossible to export the keys from the signature creation device. Further security requirements for the trusted systems for key generation are specified below under 4.6.

RSA is the algorithm used for all key pairs of the Qualified Timestamping Service; the key length is 2048 bits. When selecting more detailed parameters of key generation, the requirements of the annex of the Signaturverordnung 2008 as well as the recommendations from international standards (e.g. ETSI TS 102 176) as well as the recommendations of the authorities competent for electronic signatures are met.

4.2 Protection of the Private Key

The private keys of the Qualified Timestamping Service are stored in the secure signature creation device where they were created (see above 4.1). They never leave that device. The signature creation device is configured in such a way that the private keys cannot be exported (see below 4.6). Thus, there is no backup of the private keys. If a key is lost due to a defect of a signature creation device, then a new key pair will be generated (see above 4.1):

The private keys of the Qualified Timestamping Service are used exclusively to sign qualified timestamps within this service.

4.3 Distribution of the Public Keys

A certificate in X.509 format is issued for the public keys of BEV's Qualified Timestamping Service. The keys are named in such a manner that the BEV as timestamp provider, the name of the service and the consecutive number of the key pair are referred to, e.g. „C=AT, O=Bundesamt für Eich- und Vermessungswesen, CN=Sicherer Zeitstempeldienst-01“.

The certificates of the Qualified Timestamping Service as well as all the certificates which are on top in the certification hierarchy right to a self-signed root certificate are published on BEV's website.

In this process the BEV will preferentially use certificates which are issued according to § 13 Abs. 3 Signaturgesetz by the supervisory authority for electronic signatures, the Telekom-Control-Kommission. Thus the timestamps right to the topmost certificate can be verified in the supervisory authority's directory (see above 3.11). However, the BEV reserves the right to use other certificates instead (e.g. self-issued certificates or certificates issued by another certification service provider). In this case appropriate information on the certificate hierarchy and on the verification of the certificate chain is published. At any rate, great care is taken to ensure that the policy upon which

the issued certificates are based guarantees a comparable security level to this Policy of the Qualified Timestamping Service.

4.4 Rekeying

At all events rekeying shall be performed if the applied algorithm (RSA), the key length used (2048 bits) or the algorithm in the certificates issued for the key are no longer considered to be sufficiently secure (see above 3.5). Only certificates whose algorithms are considered to be sufficiently secure over the full validity period are used for the Qualified Timestamping Service.

In the event of a compromise rekeying is performed as well (see below 6.8).

In addition, the BEV can rekey at any point in time, e.g. if a server or a signature creation device is to be replaced.

The pending expiry date of the certificate issued for a key of the Qualified Timestamping Service does not affect the further use of the key. As far as the applied algorithm and key length are considered to be still sufficiently secure, it shall be made sure that a new certificate is issued (which has the same content in the subject field) before the certificate expires.

4.5 End of the Life Cycle of the Private Keys

The BEV ensures that a key which was put out of operation according to the information above under 4.4. can no longer be used.

It is ensured organisationally that in the cases described under 4.4 rekeying is performed. Furthermore it is ensured technically that the software of the Qualified Timestamping Service no longer creates timestamps if the certificate upon which the timestamp is based expires.

Only one copy of each private key exists in the secure signature creation device where it was created. If a key is taken out of operation, two persons in the trusted roles of key officers adhering to the four-eyes principle shall delete it permanently by using the delete function of that signature creation device.

4.6 Life Cycle of the Signature Creation Devices

The secure signature creation devices used for the Qualified Timestamping Service are protected during their whole life cycle. In particular this means:

Before a signature creation device is put into operation, checks shall be made according to the device documentation and the self-test function to confirm if it is an original device and was not manipulated during shipping.

The measures described in chapter 6 ensure that the signature creation device cannot be changed during the total time of operation. The signature creation device has an evaluated tamper detection mechanism, which detects any manipulation attempts and thereby automatically and permanently deletes all stored keys. Furthermore the signature creation device is configured in such a way as to prevent any download of new firmware and any change of security-relevant settings in the configuration without permanently deleting the stored keys.

The start-up of the signature creation devices, the key generation plus putting the keys or the whole device out of operation shall be performed exclusively by two persons adhering to the four-eyes principle, who were entrusted with the role of key officers. All processes in this context are recorded.

The proper functioning of the signature creation devices is constantly checked by unit self tests. Organisational measures ensure that error messages are identified and dealt with accordingly.

Before a signature creation device is put out of operation all keys stored there are deleted permanently by using the delete function. If this is not possible due to a defect of the device, the device is destroyed by other means in such a way as to delete the keys permanently.

5 Timestamping

5.1 Timestamps

The BEV ensures that all timestamps are issued in a secure way and give the accurate time. The timestamps issued comply with the Standard RFC 3161 according to the profile specified in the Standard ETSI TS 101 861 (with the exception that the timestamp uses the hash value SHA-256, since doubts were cast on the long-term security of SHA-1). In accordance with RFC 3161 the timestamps contain in particular:

- the ASN.1 Object Identifier of this Policy (see above 3.2),
- a unique identifier, represented by a consecutively assigned serial number,
- the time specification, which the time emitter UTC(BEV) transmits directly (see 5.2),
- this time specification may deviate by a maximum of one second from UTC, and this maximum deviation is also specified in the timestamp (if the server detects an error which might cause the timestamp to deviate by more than one second from UTC, no timestamp is issued),
- the hash value of the document to be timestamped,
- information on the country (C=AT), on the name of the timestamping service provider (O=Bundesamt für Eich- und Vermessungswesen), and on the server which created the timestamp. The latter is identified by the consecutive number of the key pair which is used (CN=Sicherer Zeitstempeldienst-xx).

All timestamps are signed with a key, which is provided exclusively for this purpose.

5.2 Time Accuracy

The time signal used for the timestamping service comes directly from the atomic clocks, which the BEV itself operates. These are part of the international network of atomic clocks, which is managed by the International Bureau of Weights and Measures (BIPM) set up by the Metre Convention.

The BEV operates three atomic clocks, which are synchronised among themselves and with the other atomic clocks in the network of the BIPM. Two of these atomic clocks are each connected to an NTP server in the same room. Via VPN tunnel the time signal is transmitted from the NTP servers to both timestamp servers in BEV's two data centres.

A GPS receiver, housed in another of BEV's buildings, serves as a further time source. Likewise, the time signal is transmitted from the GPS receiver using NTP via VPN tunnel to both timestamp servers.

Beyond that, both timestamp servers obtain time signals via NTP from selected NTP servers on the Internet.

On both timestamp servers an NTP server is installed, which uses the time signals thus received to synchronise the system clock. The NTP server is configured in such a way as to give first priority to the NTP servers of the atomic clocks and will resort to the other time signals only if the time signal of the atomic clocks fails.

The security measures implemented by the BEV (see chapter 6), in particular the VPN tunnels used, prevent manipulation of the time emitters and manipulation of the time signal on its way from the time emitters to the qualified timestamp servers.

Moreover, security measures were implemented in order to identify errors which would disconnect the time emitters and the timestamp servers. If there is a risk of the server's time deviating by more than one second from UTC, the relevant timestamp server will disconnect until the bug is fixed.

The components employed also guarantee a correct handling of leap seconds. Due to BEV's activities when operating the UTC(BEV) time emitters within the scope of the BIPM, the BEV records the times when leap seconds are inserted or removed.

If an incident happens which gives ground for the assumption that timestamps deviating by more than one second from UTC were issued, the users of the timestamping service and the persons trusting the timestamping service are informed (see below 6.8).

6 Management and Operations

6.1 Security Management

The BEV makes sure that all administrative and organisational measures are taken which guarantee a security level adequate to the Qualified Timestamping Service and correspond to the state of the art.

The BEV bears the overall responsibility for the performance of the Qualified Timestamping Service and for the compliance with this Policy, irrespective whether the required activities are carried out by the BEV itself or are sourced out to a contractor. If activities are sourced out to an external contractor, these activities are defined clearly and appropriate contracts ensure that the requirements of this Policy are fulfilled.

Among the outsourced activities are in particular inspection rounds made by an external security company plus the services of the contracted data centre. In this context, the operator of the data centre only houses the servers, connects to the Internet and manages the access. BEV's servers are located each in a separate lockable area, which is allocated exclusively to the BEV. Access to this area is only permitted to those personnel of the BEV, whose names were given the operator of the data centre (see below 6.4).

The head of the BEV is responsible for security management, in particular for further development of this Policy and quality assurance. The head of the BEV decides on amendments of this Policy.

All security measures and standard procedures are recorded in writing, kept up-to-date and implemented in the corresponding organisational units (see 6.3).

The personnel (see 6.3) and the contractors involved in the activities of the Qualified Timestamping Service are provided with the respective current versions of this Policy and the internal security guidelines and the operating manuals and they are committed to observe this Policy in the respective current version.

6.2 Security-Relevant Facilities

The following facilities are required for the provision of the Qualified Timestamping Service. By means of the measures described in chapter 6 the BEV provides for an adequate protection of these security-relevant facilities.

- In one of BEV's buildings („Building E“), in a room secured by access control (see below 6.4) three atomic clocks are located, two of which are used for the timestamping service, furthermore, two NTP servers, plus the required network infrastructure in this and other rooms.
- In another of BEV's buildings („Building A“) a GPS receiver is located, as well as an NTP server and the network infrastructure. The GPS antenna is installed on the roof of the building.
- In two other buildings the data centres of BEV's service provider are located. The BEV has rented a separate lockable area in both of these data centres. Several different servers of the

BEV are housed there, in particular the two servers of the Qualified Timestamping Service. Depending on the selected product, the secure signature creation devices are either within the servers (e.g. PCI cards) or they are protected by mechanical measures (lockable container) against unauthorised removal and unauthorised disconnection from the server. In addition, the database servers running BEV's database system are located in the data centres. This database system is used to archive the log files of the Qualified Timestamping Service and to assign the timestamps unambiguous serial numbers in a strictly ascending order.

- The mentioned buildings are redundantly connected by BEV-operated networks on leased dark fibres. In particular, each of the two data centres is connected to Building A as well as to Building E by two dark fibres each run on a different route.

The servers of the Qualified Timestamping Service including the connected secure signature creation devices shall only be used for the purposes of the Qualified Timestamping Service.

All other components as well as all relevant rooms are used for other activities of the BEV as well, which however are not incompatible with the activities of the Qualified Timestamping Service:

- The atomic clocks and the NTP servers in Building E serve various activities requiring precise time specifications. All of these activities have in common the precision of the time signal and the reliability of the overall system. Therefore, all relevant components are designed redundantly. Accuracy, authenticity and reliability are among the main tasks of the personnel in charge of the atomic clocks and the NTP servers.
- The GPS receiver is exclusively used for the purposes of the Qualified Timestamping Service.
- The network infrastructure connecting the buildings is used for various tasks of the BEV. Hence for the purpose of the Qualified Timestamping Service, VPN tunnels are created between the rooms housing the time emitters and their NTP servers and both of the data centres.
- In both of the data centres numerous servers of the BEV are located, which perform various tasks. In particular, the database and the storage area network plus the backup system are used for various purposes of the BEV. Therefore, the security-relevant main tasks of the timestamping service (verification of accuracy and possible failure of the time signal, security of the private key, verification of the incoming timestamp requests and issuing the timestamps) are exclusively installed on the timestamp servers and the directly connected secure signature creation devices. The Qualified Timestamping Service uses the database exclusively to manage the timestamp serial numbers and to store log files.

6.3 Personnel Security

All activities in connection with the Qualified Timestamping Service of the BEV shall be performed only by persons who are explicitly entrusted with one of the roles described below.

Since the security-relevant main tasks are performed on the timestamp servers and the linked secure signature creation devices, a separate role, the key officer, was specified to manage these servers.

- A *key officer* is responsible for the secure configuration of the timestamp servers and the secure signature creation devices. Regarding any measure taken on the secure signature creation devices themselves (configuration, key generation, deleting keys, see chapter 4) the four-eyes principle is applied, any other measure on the servers can be taken by one key officer alone. The head of the BEV appoints four persons as key officers, choosing two persons from the staff responsible for IT security and two persons from the staff responsible for server operation. The latter are responsible for routine server maintenance (in particular: installing security patches, verifying error messages, troubleshooting, supervising external maintenance personnel). Activities which fall under the four-eyes principle may be performed by any two of the four key officers.

This Policy does not specify separate roles for the other tasks, which are performed by the personnel of the different departments of the BEV within their respective fields of activities. In particular these are:

1) Employees who are responsible for maintaining the atomic clocks and the NTP servers in Building E. Supervising the accuracy of the atomic clocks and NTP servers is among the employees' main tasks.

2) The Department Information Technology is responsible for

- Network operations;
- Server operation (two of the employees engaged there are entrusted with the role of key officer, see above);
- Technical applications management (one of the employees engaged there is entrusted with the project management of the Qualified Timestamping Service);
- Storage area network operation, data backup and maintenance of the databases;
- The protection of the IT infrastructure and the access from the outside (two of these security officers are entrusted with the role of key officers, see above);
- Monitoring of servers and applications and generating operating status reports.

Only persons who are reliable and have the required expert knowledge and the required experience and qualification necessary to perform the tasks in accordance with the roles are employed.

6.4 Physical Security

All components except the time emitters (including the NTP servers) are located in the two data centres (in particular the timestamp servers, the secure signature creation devices, the database and the storage area network). The operator of the contracted data centre protects the data centres against unauthorised access. In both data centres the BEV has rented separate lockable areas, which may be accessed only by BEV's named personnel. Identity verification and access control are carried out by the operator of the contracted data centre. All servers as well as the switches for the network connections between BEV's various locations are located within the locked area.

Beyond that, the timestamp servers as well as the secure signature creation devices are locked in such a way that hardware changes cannot be made by all authorized personnel, but only by those persons who are entrusted with the role of key officer. Particular care is taken to ensure that the secure signature creation devices cannot be removed and/or disconnected from the server (e.g. by using PCI cards as secure signature creation devices or by locking server and signature creation device in a common container).

The operator of the data centre takes security measures against unauthorised access, burglary and theft, for fire protection, against power failure and water ingress. Moreover, due to the redundant distribution to two data centres further precautions against power failure and Internet disconnection and against disasters are taken.

The atomic clocks and their NTP servers are located in a locked room, which can be accessed only by personnel of the responsible department and the authorised security personnel. The room is secured by a fireproof door. There are no workstations in that room, the room is locked and is entered on the occasion of regular work at the systems. The department responsible for facility management has custody over the keys.

The GPS receiver and the NTP server are located in a locked LAN rack in a locked room. Only staffs of the responsible department and authorised security personnel have access to the room, only staffs of the departments responsible for network engineering and GPS and time receiver

maintenance have access to the rack. The keys for the room are managed by the Facility Management Department; the keys for the rack are managed by the Network Engineering Department.

6.5 Organisational Security Measures

Ongoing security monitoring of the timestamp servers and of the applied technologies and algorithms are among the tasks of the key officers. In particular after discovery of security leaks they have to install security patches. On becoming aware of circumstances due to which one of the used algorithms no longer seems to be secure in the long run, the appropriate actions shall be taken to modify the algorithms used (see above 3.5). If it seems that a compromise occurred or that timestamps were issued which differ by more than one second from UTC, the actions described below under 6.8 shall be taken.

The BEV has implemented a three-tier antivirus programme which filters viruses at the Internet gateway, on the file server and on the clients. By installing only selected and virus checked software, the timestamp servers and the database servers are additionally protected against viruses.

Data carriers are protected against damage, theft, and unauthorised access. The data of the Qualified Timestamping Service (log files) are transferred to BEV's general database system. If hard disk drives need to be replaced in the timestamp servers, attention will be paid that the data, in particular passwords and private keys (e.g. for the software to access the secure signature creation device and in order to manage the VPN tunnels), are deleted or changed. The private keys to sign the timestamps are in separate signature creation devices anyway (see chapter 4).

All tasks associated with the Qualified Timestamping Service are compiled in clear working process descriptions, in particular the server configuration of the timestamping service and the secure signature creation devices and error handling. The responsible departments involved in the Qualified Timestamping Service (in particular the departments responsible for the time emitters and for network security) have incorporated the various tasks required for the Qualified Timestamping Service in their respective internal documentation.

In the course of server and application monitoring and generating operating status reports, attention is paid that the capacity of the servers and signature creation devices (in particular the achievable amount of timestamps per minute) as well as the capacity of the database is sufficiently dimensioned. In case of planning a system expansion, the staff member responsible for the project management of the Qualified Timestamping Service will be informed and be responsible for planning and project management of the system expansion.

Should possible errors occur, process descriptions for error handling are compiled. Among these errors are in particular the drop-out of a time signal provided by the timestamp servers, error messages relating to the plausibility of the time signals, server failure, error messages from the secure signature creation device's self-tests, database access errors etc. As to problems concerning the database, the storage area network or the network, the already existing procedures for error handling are followed.

The timestamp servers and the secure signature creation devices are used exclusively for the Qualified Timestamping Service. For these components special security measures are taken, which are described in this Policy and in the security concept for BEV's Qualified Timestamping Service. The atomic clocks and their NTP servers, the network, the database, the storage area network and the backup system are shared by multiple applications of the BEV.

6.6 Access Protection

BEV's internal network is protected by firewalls against unauthorised external access. The security-relevant network components are within BEV's sphere and are monitored by staff of the Department Information Technology. The connection between the NTP servers in Building E and

the timestamp servers in the two data centres, and moreover, the connection between the GPS receiver in Building A and the timestamp servers are protected by a VPN tunnel.

All the systems used, in particular the timestamp servers, the secure signature creation devices, the NTP servers and the database require a personal or role-based login (as a rule with username and password). In the event of staff change all the passwords known to the leaving employee are changed. In particular, a login with username and password is required for any administrative access to one of the servers of the timestamping service and for any activity at one of the secure signature creation devices.

The personnel is responsible for their respective actions. Any security-relevant event is recorded or entered in the automated event logs (see below 6.11).

6.7 Trusted Systems

With regard to the security of the timestamping service, the following systems are of special importance:

- Time emitters (atomic clocks and GPS receivers)
- NTP servers
- Timestamp servers
- Secure signature creation devices
- Network components, firewall clusters
- Database server, storage area network, backup systems

All devices carry the risk of failure and consequently of availability impairment. Therefore all mentioned systems are designed redundantly (except for the GPS receiver, which however is only used as a backup time emitter in case of disconnection from the atomic clocks).

Furthermore all devices bear the risk of impairing the integrity, e.g. by bugs, viruses, etc. In order to minimise this risk, changes have to be checked for potential security problems before implementation. As to the timestamp servers, this task falls in the key officers' sphere of activity, all other systems fall in the sphere of activity of the respective departments in charge. On the mentioned servers only the software required on the respective server is installed. On the timestamp servers only the software required for the timestamping service may be installed. On the secure signature creation devices only the software which is included in the expertise or the certificate of the confirmation body may be used, and it must be configured in such a way that ex post software change is impossible without permanently deleting the stored keys.

As to the secure signature creation device, in particular the risk of the private key leaving or being read out of the signature creation device must be minimised. Therefore exclusively such technical components are used which were checked according to the criteria mentioned above under 4.1, by a confirmation body. Moreover the devices are configured in such a way that key export is impossible.

As to the database, the storage area network and the backup system, breach of trust must be prevented. This is ensured by access control.

6.8 Disasters and Compromise

The duplicate execution of all important components takes precaution against disaster. If one of the two data centres fails, both the Qualified Timestamping Service and the log file database will continue running unaffected in the other data centre. In case of loss of connection to the atomic clocks in Building E the time signal can be obtained by a GPS receiver in Building A. Since all components of the Qualified Timestamping Service plus the underlying infrastructure (network infrastructure, time emitters ...) are carefully documented, even in case of a total breakdown the service can be recovered.

In case a private key is lost (e.g. due to loss of a signature creation device), a new key pair is generated (see above 4.4). There is no backup of the private keys (see above 4.2).

If it is detected that incorrect timestamps were issued (in particular timestamps deviating by more than one second from UTC), the public trusting the timestamps is informed.

If the security requirements of this Policy are severely affected (compromised), the issuance of timestamps is stopped immediately. Depending on the severity of the incident, the public is informed.

If there is legitimate concern that a private key of the timestamping service has been stolen or cracked, issuing timestamps with that key is stopped immediately and the certificate issued for that key is revoked. In such a case the public is informed at all events.

As to the mentioned information measures, the exact extent of information is balanced in accordance to the severity of the case and the effects on the use of the Qualified Timestamping Service known to the BEV. At any rate the BEV shall inform the known users, as far as their e-mail addresses have been announced. The information shall in particular contain a statement about the effects of the incident on the long-term security of the issued timestamp.

6.9 Cessation of Services

The BEV reserves the possibility of discontinuing the Qualified Timestamping Service any time without giving reasons. Notwithstanding the BEV can conclude service level agreements with specific users, thereby ensuring a defined availability over a fixed period. There is no obligation or liability to continue performing the service beyond the contractual obligation.

The revocation of all certificates of the timestamp servers still valid is initiated when the service is discontinued. All private keys are permanently deleted (see above 4.5). Should the BEV have issued proprietary certificates for the timestamp servers, the appropriate security and certification concept would have stipulated how long the revocation lists for the qualified certificates must be available online (by all means at least until the validity period of the respective certificates expires). The documentation of issuing, suspending and revoking a qualified certificate by the BEV is archived for at least 30 years as from the expiry date stated in the certificate. If the BEV discontinues certification service providing, this documentation shall be submitted to the supervisory authority or to another certification service provider who was entrusted with the continuation.

All known users of the Qualified Timestamping Service are informed about the cessation of the services. In addition, the BEV will publish on its website the cessation of the services and will make the information required for the long-term verification of timestamps available until at least three years after cessation of the service.

The documentation of the Qualified Timestamping Service is archived beyond the cessation of the service (see below 6.11).

6.10 Compliance with Legal Requirements

The BEV is a subordinate authority of the Federal Ministry of Economy, Family and Youth, and has its head office in Vienna. Hence it is subject to Austrian jurisdiction and the court of jurisdiction is in Vienna (unless special regulations apply).

As provider of a qualified certification service the BEV is obliged to observe in particular the Signaturgesetz and the Signaturverordnung 2008 as well as the Datenschutzgesetz 2000, each as amended from time to time. The Qualified Timestamping Service and all its changes are announced to the Telekom-Control-Kommission as the supervisory authority for electronic signatures and are subject to its supervision.

Personal data are managed in the log files as well as in the process of user administration and possible invoicing. These are protected by state of the art data protection measures.

6.11 Recording and Archiving

The relevant staff members record and archive cumulatively the following processes:

- Setting up the timestamp servers, installing software, changing the installed software. The time when the changes became effective should be recorded as exactly as possible.
- Any non-automated action at the secure signature creation devices, in particular initialising, configuring and generating key pairs as well as deleting keys and putting the devices out of operation. Furthermore the life cycle of the certificates issued for these keys is documented (information on issuance of the certificates as well as on a possible revocation) and the certificates are archived.

These records are filed in the general records of the BEV and be stored for an indefinite period of time.

The database system automatically generates log entries about the following processes. These log files are stored for at least three years:

- Start and stop of the timestamp software
- Error messages of the timestamp servers, in particular error messages relating to time synchronisation
- Log entries about every single created timestamp, which contain amongst others the serial number, the exact point in time and the hash value of the timestamped document.

BEV's records as well as the applied database system and BEV's backup strategy protect the recorded data efficiently against ex post changes, data loss and unauthorised data access.

Information on recorded log data is given only within the frame of the law, in particular the Datenschutzgesetz 2000. In particular information on log data of a specific timestamp will be given only if legal interest is claimed, for instance due to the fact that a timestamped document is the subject of an action (see above 3.12).

7 Appendix

7.1 Definitions and Abbreviations

| Term/Abbreviation | Definition, Description |
|-------------------------|--|
| A-SIT | Secure Information Technology Center - Austria (Zentrum für sichere Informationstechnologie – Austria) http://www.a-sit.at |
| ASN.1 | Abstract Syntax Notation 1. Amongst others, X.509 certificates are encoded in this notation. |
| Supervisory authority | In Austria, the Telekom-Control-Kommission is entrusted with the tasks of a supervisory authority for electronic signatures. |
| BEV | Federal Office of Metrology and Surveying (Bundesamt für Eich- und Vermessungswesen) |
| BIPM | Bureau International des Poids et Mesures |
| C | Country, State, e.g.: C=AT in the Distinguished Name of a certificate |
| CN | Common Name, e.g.: CN= first name, surname in the Distinguished Name of a certificate |
| Common Criteria | Common criteria for the examination and evaluation of the security of information technology |
| CWA | CEN Workshop Agreement, a standard of the standards organisation CEN |
| Distinguished Name | The structured spelling of names, used amongst others in certificates and timestamps, e.g. the form C=AT, O=Name of the organisation, CN=first name surname |
| Authentic, authenticity | An electronic signature is authentic if it comes from that party who is |

| | |
|---------------------------|--|
| | shown as signer |
| ETSI | European Telecommunications Standards Institute |
| FIPS | Federal Information Processing Standard |
| GPS | Global Positioning System, a satellite network which was developed to determine the exact position, but also can be used as a time emitter. |
| Valid, validity | Certificates have a validity period. A certificate loses its validity either by expiry or by revocation. An electronic signature is valid if it is created within the validity period of the certificate it is based on. The verification of the signature validity is an important step in the process of verifying the authenticity. |
| hash function, hash value | A hash function is a mathematical function which enables any document to be represented by a value of specific length (e.g. 256 bit), the hash value. A hash function is required to be irreversible (i.e. no conclusions about the document can be drawn from the hash value), and that in practice it is impossible that two documents have an identical hash value. Examples for hash functions are SHA-256 and RIPEMD-160. |
| ITSEC | Criteria for the evaluation of the security of information technology |
| LAN | Local Area Network |
| NTP | Network Time Protocol, the most widespread protocol to synchronise clocks via the Internet. |
| O | Organisation, e.g.: O=company name in the Distinguished Name of a certificate |
| OID | Object Identifier. Is used in the ASN.1 Notation to name any content, e.g. as a reference to the policy, based upon which a timestamp or a certificate was issued. |
| PCI | Peripheral Component Interconnect |
| Policy | Here: rules and standards describing a timestamping service (or any other certification service), which the provider commits to observe. Mostly the policy is published and an OID in the issued timestamps (and certificates) refers to the relevant policy. |
| QZSD | Qualified Timestamping Service |
| RFC | Request for Comments, a document in which a standard for the Internet was set |
| RIPEMD-160 | RACE Integrity Primitives Evaluation Message Digest, a hash function |
| RSA | The most widespread asymmetric cryptographic function to generate electronic signatures, named after the initials of the developers, Rivest, Shamir and Adleman. |
| RTR-GmbH | Rundfunk und Telekom Regulierungs-GmbH, the operative unit of the Telekom-Control-Kommission as supervisory authority for electronic signatures |
| Key | The information which is used in a cryptographic process to encrypt or decrypt (or to generate or verify) signatures. In an asymmetric cryptographic process every user uses a key pair. The private key can be used to generate signatures, the public key to verify these signatures. |
| SHA | Secure Hash Algorithm, a family of hash functions. The most widespread hash function SHA-1 (160 bit) is increasingly considered to be no longer secure enough, which is why SHA-256, SHA-384 and SHA-512 (256, 384 or 512 bit) are used. |
| Signature, electronic | Electronic data which are added to an electronic document and which certify the signer's identity, i.e. the generator of the signature. |

| | |
|--|---|
| Federal Electronic Signature Law (Signaturgesetz, SigG) | Federal Electronic Signature Law - Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG), BGBl. I Nr. 190/1999 in der geltenden Fassung) |
| Federal Signature Ordinance (Signaturverordnung 2008, SigV 2008) | Ordinance of the Federal Chancellor on Electronic Signatures - Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008), BGBl. II Nr. 3/2008 in der geltenden Fassung |
| TKK | Telekom-Control-Kommission, the Austrian supervisory authority for electronic signatures. RTR-GmbH acts as the operative unit of the TKK. |
| TS | Technical Standard, e.g. z. B. ETSI TS 102 023 |
| UTC | Coordinated Universal Time. Central European Time differs from UTC by one hour, Central European Summer Time by two hours. UTC is based on atomic clocks, all seconds are of equal length. In order to compensate irregularities in Earth's rotation, sometimes leap seconds are inserted or deducted. By contrast Universal Time (UT) is based on Earth's rotation. The seconds of UT have slightly differing lengths. |
| UTC(BEV) | The form of UTC represented by BEV's atomic clocks. |
| VPN | Virtual Private Network |
| Revocation, revocation list | Certificates can be revoked, and consequently their validity expires before the end of the validity period stated in the certificate. As a rule a certification service publishes information about revoked certificates in the form of a revocation list, a list of all revoked certificates. |
| Root certificate | The topmost certificate in a hierarchy of certificates. A root certificate is self-signed, hence it is based on itself and not on another certificate. |
| X.509 | The most widespread standard to encode certificates. X.509 uses ASN.1 as notation. |
| ZDA | Certification Service Provider |
| Timestamping Service | A service which adds a timestamp to documents, i.e. a time specification and a signature, which comprise the document (or rather its hash value) and the time specification. A timestamp certifies that the document already existed at a given point in time and was not changed thereafter. |
| Timestamping Service, Qualified | A Qualified Timestamping Service is a timestamping service which fulfils defined high requirements of the Signaturgesetz and the Signaturverordnung 2008, as described in this document. |
| Certificate | An electronic certification which allocates a specific key pair (and therefore all signatures or timestamps generated with the private key of that key pair) to a specific person. |