WISeKey Time Stamping Authority

OISTE WISeKey TSA Policy Statement

Date:	May 8th 2012
Version:	1.2
Status:	Ready to Review

Trademark and Copyright notices

Contact Information

OISTE / WISeKey Policy Approval Authority
29, route de Pré-Bois
Case postale 853
CH-1215 Geneva 15
Switzerland

cps@wisekey.com

Version Control

Issue date	Version	Name	Comment
May 8th 2012	1.2	WISeKey SA	Compliance Review

Table of Contents

1. Introduction

1.1. Scope

This document describes WISeKey time stamp service policy, defining general rules that shall be followed by the WISeKey time stamping service. Time stamps issued in accordance with this policy may be used to protect long-term electronic signatures of a given datum.

A digital time stamp proves the existence of a digital datum at a specific time. A time stamped datum cannot be altered unnoticed.

To time stamp a datum, it can be sent to WISeKey time stamping service. An object consisting of a hash of the datum and actual time is then created and electronically signed by the WISeKey time stamping service, thus protecting its integrity.

1.2. About WISeKey

WISeKey SA is a “Société Anonyme” under Swiss law with headquarters in Geneva, Switzerland and subsidiaries and affiliates in different regions and countries worldwide. The company manages the WISeKey Certification Authority Services (WCAS), including the OISTE WISeKey Global Root CA, which is maintained off-line in a high-security facility in Switzerland. WISeKey has located its headquarters in Switzerland and is simultaneously establishing affiliates in regions and countries worldwide. This enables, on the one hand, the traditional Swiss neutrality and high quality infrastructures and services and, on the other hand, the local capacity to establish infrastructures in each country and region adapted to the local needs, regulations and policies. This results in a series of links between entities that conform a chain of trust running throughout its infrastructures worldwide.

WISeKey’s main objective is the deployment of a global trusted community based upon a public key infrastructure using best-in-class technological platforms leveraging its own Private infrastructures as well as Public infrastructures.

Since WISeKey’s creation, it has had a global outlook, which allowed it to provide solutions to clients such as international organizations, multi-nationals and governments. Its successes include providing the front line security for the world’s first binding government Internet voting system and assisting the International Telecommunication Union to deploy their Electronic Commerce project.

WISeKey is an essential enabler of the ongoing transition from the traditional paper-based communications to the fully digitized communications by providing the necessary security and trust conveyance required by even the most demanding users whilst simultaneously accommodating the needs of the most inexpert users. For further information, please visit www.wisekey.com.

2. References

[1]	ETSI TS 102 023 V1.2.1 (2003-01), Policy Requirements for time-stamping authorities
[2]	ETSI TS 101 861 V1.3.1 (2006-01), Time stamping profile
[3]	IETF RFC 3126, Electronic Signature Formats for long term electronic signatures, September 2001.
[4]	FIPS PUB 140-1, Security Requirements for Cryptographic Modules
[6]	ETSI TS 102 176-1 V2.0.0 (2007-11), Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
[8]	IEFT RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), August 2001
[9]	IEFT RFC 2246, The TLS Protocol, Version 1.0, January 1999
[10]	IEFT RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, June 1999
[11]	Oiste Wisekey Root Certification Practice Statement, Version 1.02
[13]	ETSI TS 101 456 V1.4.3 (2007-05): Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates
[14]	IEFT RFC 3280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile
[15]	CWA 14167-1, Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

Table 1: References

3. Abbreviations

CPS	Certification Practice Statement
CP	Certification Policy
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
NTP	Network Time Protocol
OID	Object Identifier
RDN	Relative Distiguished Name
RFC	Request For Comments
RSA	Rivest Shamir Adleman Algorithm
TSA	Time-Stamping Authority
TSP	Time-Stamping Policy
SHA	Secure Hash Algorithm
TSU	Time-Stamping Unit
TSP	Time-Stamping Policy
TST	Time-Stamping Token
UTC	Coordinated Universal Time
UTC(k)	time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns (see ITU-R Recommendation TF.536-1).
WCAS	WISeKey Certification Authority Services
WPAA	WISeKey Policy Approval Authority

table 2:Abbreviations

4. Definitions

4.1. Time Stamping Unit (TSU)

A time stamping unit is a set of hardware and software which is managed as a unit and has a single time-stamping signing key active at a time[2]

4.2. Relying Party

Recipient of a time-stamp token who relies on that time-stamp token.[8]

4.3. Subscriber

Entity requiring the services provided by a TSA and which has explicitly or implicitly agreed to its terms and conditions. [8]

4.4. time-stamp policy:

Named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements

4.5. Time-stamp Token (TST)

Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time. [8]

4.6. Time Stamping Authority (TSA)

Authority which issues time-stamp tokens. The time stamping authority is trusted by the subscribers and relaying parties to issue time stamp tokens. The TSA has the responsibility for the operation of one or more TSU's that sign TST's.

4.7. TSA Disclosure statement

Set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements

4.8. TSA practice statement

Statement of the practices that a TSA employs in issuing time-stamp tokens

4.9. TSA system

Composition of IT products and components organized to support the provision of time-stamping services time-stamping unit: set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time

4.10. Coordinated Universal Time (UTC)

Time scale based on the second as defined in ITU-R Recommendation TF.460-5

5. Time-Stamp Policy

5.1. Identification

This TSA policy statement is referred to as the ‘OISTE WISeKey TSA Policy Statement’. The primary source of the current version of the TSA policy statement and other important WISeKey documents is http://www.WISeKey.com/repository/.

5.2. Overview

This section explains the relative roles of Time-stamp policy and TSA practice statement.

The TSA Policy is a set of rules used to issue and manage TST’s and to regulate the security level for the TSA. The TST’s are in line with ETSI TS 102.203.

The private keys used for signing and the TSU are in line with ETSI TS 101.861 and RFC 3161. The profile of the basic fields of the certificates used are described in table 3:Basic TSA certificate fields

Version	Version 3	Critical
Serial Number	Unique value for all certificate issued by certification authorities within WISeKey	-
Signature Algorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	-
Issuer (DN)	Common name (CN) = [CN] Organization (O) = [O] Country (CH) = [CH]	-
Not Before	Date of issuance	-
Not After	Not after the expiry date of the WISeKey Issuing CA	-
Subject	In accordance with [14].	-
Key Size	2048 bits	-
Signature	Certificate signature generated and encoded according to [14]	-
Key Usage	Digital Signature, Non-repudiation	Y
Extended Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)	Y
Basic Constraints	End-Entity, Path Length Constraint=0	
CRL Distribution Point	Extension marked non-critical. Fullname: <resent>	
Authority Information Access	Access Method : On-Line Certificate Status Protocol (OID 1.3.6.1.5.5.7.48.1) Alternative Name: <present>	

table 3:Basic TSA certificate fields

5.3. Identification

The OID identifying Time Stamp service certificates issued by WISeKey is 2.16.756.5.14.4.7.1.

5.4. User Community and Applicability

WISeKey does not restrict the applicability of its time stamps. They may be used as well for closed user group as for public time stamping services.

The WISeKey TSP is aimed to meet the requirements specified in [1]

5.5. Conformance

WISeKey TSA uses the OIDs described in chapter 5.3: Identification of the time stamping policy.

WISeKey meets its obligations as defined in chapter 6.1: TSA Obligations

6. Obligations and Liabilities

6.1. TSA Obligations

6.1.1. General

This chapter lists all obligations, liabilities, guarantees and responsibilities of the WISeKey TSA, its subscribers and relying parties.

WISeKey is party to mutual agreements and obligations between the TSA, subscribers and relying parties.

WISeKey guarantees that all requirements described in chapter 7: Requirements on TSA Practices are met.

6.1.2. TSA obligations towards Subscribers

WISeKey provides permanent access to the time stamping service except

- During service and maintenance intervals. Maintenance windows will be announced on WISeKey's website.
- When a third party service is not available, e.g. a reliable time source
- When events that cannot be influenced by WISeKey hinder the service (force majeure, war, strike etc.)

Moreover, WISeKey shall

- Ensure that their activity is legal, in particular that they do not violate intellectual property and licenses.
- Ensure that only correct time stamps are issued
- Ensure that their equipment for the TSS meets the requirements described in [15]
- Ensure that they meet the requirements outlined in Chapter 5: Time-Stamp Policy

6.2. Subscriber Obligations

The subscriber shall verify that the time-stamp token has been signed correctly and that the digital certificate used to sign the time stamp token has not been compromised.

Additional requirements can be included in contractual agreements between the TSA and the subscriber.

6.3. Relying Party Obligations

The relying party relying on a time-stamp token must verify that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp has not been compromised until the time of the verification.

During the TSU's certificate validity period, the validity of the signing key can be checked using current revocation status for the TSU's certificate. If the time of verification exceeds the end of the validity period of the corresponding certificate, they must verify that the cryptographic procedures (hash function, signing algorithm) and the key size used are still considered secure

They must also take into account any limitations on the usage of the time-stamp indicated by the time-stamp policy

6.4. Financial Liability

WISeKey shall not be liable for matters that lie outside its sphere influence and responsibility

WISeKey undertakes to operate the WISeKey TSA in accordance with the WISeKey TSP, the OISTE-WISEKEY CPS [11], and the terms of service level agreements with the Subscriber. WISeKey makes no express or implied representations or warranties relating to the availability or accuracy of the time-stamping service.

WISeKey bears specific liability for damage to Subscribers and Relying Parties in relationship to valid qualified digital certificates relied upon in accordance with specific national laws and regulations. These liabilities are described in section 2.3: Financial Responsibility of the OISTE-WISEKEY CPS [11].

7. Requirements on TSA Practices

WISeKey implements controls allowing provision of non-repudiation services in accordance with the regulations of this policy.

7.1. Practice and Disclosure Statements

7.1.1. TSA Practice Statement

WISeKey ensures the reliability necessary for providing time-stamping services. The OISTE-WISEKEY CPS [11] defines how WISeKey meets these requirements.

WISeKey undertakes comprehensive audits of internal operations and may submit to periodic third party audits. For details on security audit procedures refer to chapter 3.4. Security Audit procedures of [11]

The WPAA is responsible for setting certification practices and certificate policy direction overall for the PKI. For details on Change procedures refer to chapter 6.1. Specification change procedures of [11]

This WISeKey TSA Policy Statement and the OISTE-WISEKEY CPS [11] can be found in the WISeKey repository at http://www.wisekey.com/repository.

7.1.2. TSA Disclosure Statement

This WISeKey TSA Policy Statement and the OISTE-WISEKEY CPS [11] can be found in the WISeKey repository at http://www.wisekey.com/repository.

Contact information can be found at the beginning of this document.

The accuracy of time in the time-stamp token is defined in chapter 7.3.2: Clock Synchronization with UTC.

For subscriber obligations, refer to chapter 6.3: Relying Party Obligations

For relying party's obligations, refer to chapter 6.3: Relying Party Obligations

For limitations of liability, refer to chapter 6.4: Financial Liability

The period of time during which TSA event logs are retained is specified in chapter 7.4.10: Compliance with legal requirements

The cryptographic algorithms and key lengths used by the WISeKey TSA comply with ETSI TS 101.861 and are currently:

- Hash: SHA-1 or MD5
- Signature: sha1WithRSAEncryption, 2048 bit key

7.2. Key management life cycle

7.2.1. TSA key generation

The WISeKey TSA ensures that any cryptographic keys are generated in under controlled circumstances. The generation of the TSU's signing key(s) are undertaken in a physically secured environment as described in chapter 7.4.4: Physical and Environmental Security by personnel in trusted roles as described in chapter 7.4.3: Personal Security under, at least, dual control. The personnel authorized to carry out this function are limited to those assigned to the specific roles under WISeKey’s role concept.

Key pairs for the WISeKey TSA are generated in software certified to meet the requirements of FIPS 140-2 level 1 or higher.

Algorithms and key size are described in chapter 7.1: Practice and Disclosure Statements

7.2.2. TSU Private Key Protection

The WISeKey TSA ensures that TSU private keys remain confidential and maintain their integrity.

In particular:

- The TSU private signing key are held and used within a cryptographic module software container which meets the requirements identified in FIPS PUB 140-2 level 1 or higher

- If TSU private keys are backed up, they are copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment as described in chapter 7.4.4: Physical and Environmental Security. The personnel authorized to carry out this function is limited to those requiring to do so under the TSA's practices.

- Any backup copies of the TSU private signing keys are protected to ensure its confidentiality.

7.2.3. TSU public key Distribution

The WISeKey TSA ensures that the integrity and authenticity of the TSU signature verification (public) keys and any associated parameters are maintained during its distribution to relying parties.

WISeKey TSA key are signed by the OISTE WISeKey Root PKI

The certificate hash (thumbprint) and the certificates of the OISTE WISeKey Root PKI are available on the WISeKey Web site (www.wisekey.com/repository/).

7.2.4. TSU Rekey

The life-time of WISeKey TSU's certificate is not longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose.

TSA rekey procedure is executed upon expiry of validity period of certificate of TSA.

7.2.5. End of TSU key life cycle

The WISeKey TSA ensures that TSU private signing keys are not used beyond the end of their life cycle.

The TSU private signing keys, or any key part, including any copies are destroyed such that the private keys cannot be retrieved. The TST generation system rejects any attempt to issue TSTs if the signing private key has expired.

Operational or technical procedures are in place to ensure that a new key is put in place when a TSU's key has expired.

7.3. Time Stamping

7.3.1. Time Stamping Token (TST)

The WISeKey TSA ensures that time-stamp tokens are issued securely and include the correct time.

In particular:

- The time-stamp token includes an identifier for the time-stamp policy.
- Each time-stamp token has a unique identifier.
- The time values the TSU uses in the time-stamp token is traceable to at least one of the real time values distributed by a UTC(k) laboratory.
- The time included in the time-stamp token is synchronized with UTC within the accuracy defined in this policy
- The time-stamp token includes a representation (e.g. hash value) of the datum being time-stamped as provided by the requestor.
- The time-stamp token is signed using a key generated exclusively for this purpose.
- The time-stamp token includes an identifier for the country in which the TSA is established, and an identifier for the WISeKey TSA.

7.3.2. Clock Synchronization with UTC

The WISeKey TSA provides time with ±1 second of a trusted UTC(k) time source. The WISeKey TSUs have technical measures in place to ensure that their time is synchronized with UTC within the declared accuracy. The TSTs used by the WISeKey TSA include date and time values that are time traceable to the real UTC time value, provided by WISeKey's internal NTP server, which is synced via GPS satellite, and radio reference sources.

TSU clocks are periodically recalibrated against the reference UTC time source.

7.4. TSA Management and Operation

7.4.1. Security Management

The WISeKey TSA retains responsibility for all aspects of the provision of time-stamping services within the scope of this time-stamp policy.

7.4.2. Asset classification and management

The WISeKey TSA maintains an inventory of all assets and a classification for the protection requirements to those assets consistent with the risk analysis.

7.4.3. Personal Security

All WISeKey staff involved in the operation of the WISeKey TSA is subjected to background checks and vetting. Character references are thoroughly investigated for all operational personnel.

All operation of the WISeKey TSA is under the direct responsibility of WISeKey Executive Officers.

Personnel involved in the control and operation of the WISeKey TSA shall be sufficiently trained to comply with the functions allocated to their role and shall be provided with ongoing training to ensure the appropriate levels of awareness of the security policies and procedures.

7.4.4. Physical and Environmental Security

The hardware and software used for the WISeKey TSA is maintained in a high security facility with comprehensive perimeter security and enforced internal access controls.

Sophisticated intruder detection systems are deployed to notify security personnel of any violation of access controls.

No member of the staff is allowed to gain physical access or operate any component of the WISeKey TSA without the presence of other designated members of staff who have the skills required to confirm that no unauthorized or inappropriate actions are conducted.

Procedures are defined and documented for all operations upon the WISeKey TSA.

Operating procedures are regularly reviewed in the light of new operational requirements.

7.4.5. Operations management

The WISeKey TSA ensures that the WISeKey TSA system components are secure and correctly operated, with minimal risk of failure:

In particular:

- The integrity of TSA system components and information is protected against viruses, malicious and unauthorized software.
- Incident reporting and response procedures are employed in such a way that damage from security incidents and malfunctions is minimized.
- Media used within the WISeKey TSA trustworthy systems are securely handled to protect media from damage, theft, unauthorized access and obsolescence.
- Procedures are established and implemented for all trusted and administrative roles that impact on the provision of time-stamping services.

Media handling and security

- All media are handled securely in accordance with requirements of the information classification scheme (see chapter 7.4.2:Asset classification and management). Media containing sensitive data is securely disposed of when no longer required.

System Planning

- Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

Incident reporting and response

- The WISeKey TSA acts in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security.

Operations procedures and responsibilities

- WISeKey TSA security operations are separated from other operations.

These operations are managed by WISeKey TSA trusted personnel, but, may actually be performed by, non-specialist, operational personnel (under supervision), as defined within the appropriate security policy, and, roles and responsibility documents.

7.4.6. System Access Management

The WISeKey TSA ensures that TSA system access is limited to properly authorized individuals.

In particular:

- Controls are implemented to protect the WISeKey TSA's internal network domains from unauthorized access including access by subscribers and third parties.

- The WISeKey TSA ensures effective administration of users (this includes operators, administrators and auditors) and access to maintain system security, including user account management, auditing and timely modification or removal of access.
- The WISeKey TSA ensures that access to information and application system functions is restricted in accordance with the access control policy and that the TSA system provides sufficient computer security controls for the separation of trusted roles identified in TSA's practices, including the separation of security administrator and operation functions. Particularly, use of system utility programs is restricted and tightly controlled.
- WISeKey TSA personnel is properly identified and authenticated before using critical applications related to time-stamping.
- WISeKey TSA personnel is accountable for their activities.
- The WISeKey TSA ensures that local network components are kept in a physically secure environment and that their configurations are periodically audited for compliance with the requirements specified by the TSA.
- Continuous monitoring and alarm facilities are provided to enable the TSA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

7.4.7. Trustworthy Systems Deployment and Maintenance

The generation of the keys in WISeKey TSA is always performed in trusted environment described in Chapter 7.2.1: TSA key generation

7.4.8. TSA Key Revelation

In the event of compromise of a TSU private key, WISeKey will follow the procedures outlined in chapter 3.7.: Compromise and Disaster Recovery of the OISTE-WISEKEY CPS [11]. This includes revoking the certificate. The TSU will not issue time-stamps if its private key is not valid.

7.4.9. TSA Termination

7.4.10. Compliance with legal requirements

WISeKey operates out of Switzerland and its certification services are therefore governed and construed in accordance with Swiss laws. The certification services provided under the authority of third parties may be subject to the laws of other jurisdictions as is indicated in their CPS and/or Certificate Policy.

7.4.11. TSA Event Journal

WISeKey maintains records of relevant information concerning the operation of the WISeKey TSA.

No personal data relating to Subscribers is transmitted between jurisdictions.

Records concerning the operation of time-stamping services are available at the request of Subscribers or if required by court order or other legal requirement. The WISeKey TSA maintains records, including precise time, of:

• Time-stamp requests and created time-stamps

• Events related to TSA administration.

7.5. Organisational Scheme

WISeKey security precautions fulfil the standards of several chapter 2: References of this document. Many important policy and practice documents for the WISeKey PKI are available at http://www.wisekey.com/repository/. Other internal procedural documents may be provided only under strictly controlled conditions.

WISeKey operates out of Switzerland and its certification services are therefore governed and construed in accordance with Swiss laws. The certification services provided under the authority of third parties may be subject to the laws of other jurisdictions as is indicated in their CPS and/or Certificate Policy.