# CERTIFYID - PRIVACY POLICY

## Version 1.0
## Effective Date: 1st December 2005

**Important Note for Relying Parties**
Reliance on a certificate or certificate revocation list issued by the OISTE WISeKey Root PKI that issued the certificate you are relying on requires agreeing to the terms of the Relying Party Agreement and assessing whether such reliance is reasonable. In order to do so, it is essential to read and understand the provisions of this document, the OISTE WISeKey Root PKI CPS (all of which are available at **http://www.wisekey.com/repository**).

# 1. Introduction

The OISTE WISeKey Root PKI provides root certification services in accordance with the OISTE WISeKey Root PKI CPS. In the provision of such certification services, WISeKey has a Policy Approval Authority in charge of creating, maintaining and managing the policies and practices that are followed by them including this Privacy Policy.

## *1.1. Purpose*

This Privacy Policy describes the practices and policies followed by WISeKey and any third parties providing services within the OISTE WISeKey Root PKI (herein "authorized third parties"), with regard to the processing of the personal data provided by Applicants and Certificate Subscribers to which they provide certification services. For the purposes of this document, "processing" refers to how personal data is:

- collected
- retained
- used
- disclosed
- destroyed

All personal data processing undertaken by either WISeKey or authorized third parties is based on the distinction between "Identification Information" and "Summary Information" provided in the OISTE WISeKey Root PKI CPS (see section 2.2 below).

The statements made in this document are consistent with the obligations set out in the contractual framework for the WISeKey PKI.

## *1.2. Publication and Revision*

This privacy policy is freely available on the WISeKey Web site
at **http://www.wisekey.com/repository** and paper copies of this document are available on request, subject to an administration fee.
This document is reviewed periodically by the WISeKey Policy Approval Authority and updated where necessary to reflect changes to operational practices, personal data collected and relevant legislation.

## *1.3. Gaining Access to Your Personal Data*

WISeKey and any authorized third parties will, upon request, provide a data subject (an individual about whom information is held) with:

- A statement of the WISeKey policy on the collection and management of personal information (this policy).
- A description of what personal data is held about them by WISeKey or the authorized third party.
- A description of the purposes for which the data is held.
- A copy of all personal data held, whether it has been obtained directly from the data subject or from a third party.

Personal data will not be disclosed if doing so would compromise the security of the service being provided to the certificate Subscriber, (e.g. disclosure of a revocation passphrase). However, approved policies dealing with certificates and cryptographic keys used exclusively for confidentiality purposes may provide for the disclosure of passphrases and private cryptographic keys.

Requests for access to personal data processed by WISeKey or authorized third parties must be made in writing to the address provided in section 1.4 below and include the following certificate information:

- Full distinguished name of the data subject, including their common name, organisational unit, organisation name and country code, where applicable; and
- Serial number of the certificate issued and date of expiry, suspension or revocation.

Requests for access to personal data processed by authorized third parties must be made in writing to the address provided by them upon provision of certification services and shall include the same information described above.

In both cases, a fee may be charged for the granting of access to personal data, which in no case shall be greater than €20.00.

## *1.4. Point of Contact at Certification Service Provider*

Initial contact for access to personal data should be established with the entity that processed the data. In the case of authorized third parties, upon processing a certificate application the address is provided to the Applicant or Subscriber.

In the case of WISeKey, initial contact should be established with:

**WISeKey SA**
**29 Route de Pré-Bois**
**PO Box 885**
**Geneva 15, CH-1215**
**Switzerland**
**Email : cps@wisekey.com**
**Tel: + 41 22 594 3000**
**Fax: +41 22 594 3001**

# 2. Collection of Personal Information

## *2.1. Purpose of Collection*

WISeKey and authorized third parties collect and store personal data only for the following purposes:

- Proving an individual's identity before a digital certificate is issued to them.
- Publishing information in a digital certificate about an individual for access by a community of people who may rely on the certificate.
- Archival of information to support subsequent confirmation of certificate and digital signature validity.
- Undertaking administration of operations, such as communicating with certificate subscribers and billing for services.

## *2.2. Information to be Collected*

The information collected will be limited to that needed to satisfy the OISTE WISeKey Root PKI CPS. Data subjects will be informed with regard to:

- What information is being collected
- ☐Why it is required
- What purpose it will be used for
- To whom it will be disclosed

Information will only be obtained from third parties with the knowledge and consent of the data subject. In all cases, the following distinction shall apply for the processing of personal data:

### 2.2.1. **Summary Information**

The basic information required for the production of a public key certificate, for the verification of a digital signature, for the validation of a certificate's status as well as the information produced as a result of such verification and validation.

### 2.2.2. **Identification Information**

This information includes all data obtained or presented to positively identify an entity and provide the certification services requested by it, excluding Summary Information. A Certificate Subscriber authorizes WISeKey and any authorized third party to publicly disclose, in the manner it deems appropriate for the provision of their certification services, the *Summary Information* as transcribed in the certificate issued. *Identification Information* will be securely processed in accordance with this Privacy Policy.

Information about race, ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sexual orientation will not be collected and personality profiles (as defined in Swiss Data Protection legislation) will not be

established except when specifically required to satisfy the requirements of a particular Policy, or of local legislation.

## *2.3. Accuracy of Information*

### 2.3.1. **Data Subject Duties**

It is a data subject's responsibility to ensure that any information they provide to a WISeKey or an authorized third party is accurate. If this information subsequently changes, it is the data subject's obligation to inform them promptly. If the data subject becomes aware of any inaccuracies in the personal data held about them, it is its responsibility to advise the entity that processed its personal data.

### 2.3.2. **Certification Service Provider Duties**

WISeKey or the corresponding authorized third party will take reasonable steps at the time of collection to ensure that the personal data it collects that is required to be verified comes from an authentic source.

# 3. Storage of Identification Information

All Identification Information shall be archived by the entity that directly provides the certification services to a Subscriber (i.e. WISeKey or an authorized third party).
Such storage shall be undertaken for a period of 10 years from the certificate expiry date. Identification Information is retained for this period to provide evidence in the event of a challenge on the validity of a certificate or a digital signature. Such period may be extended with regard to specific records and information upon request by the data subject of special archiving services. In all cases, the records may be archived in paper or electronic form.