



## WISeKey Public Key Infrastructure

White Paper on the Deployment of  
Affiliate Registration Organisations  
(Bronze Service Provider)

Version 1.0  
August 2001

**World Internet  
Security Key**

---

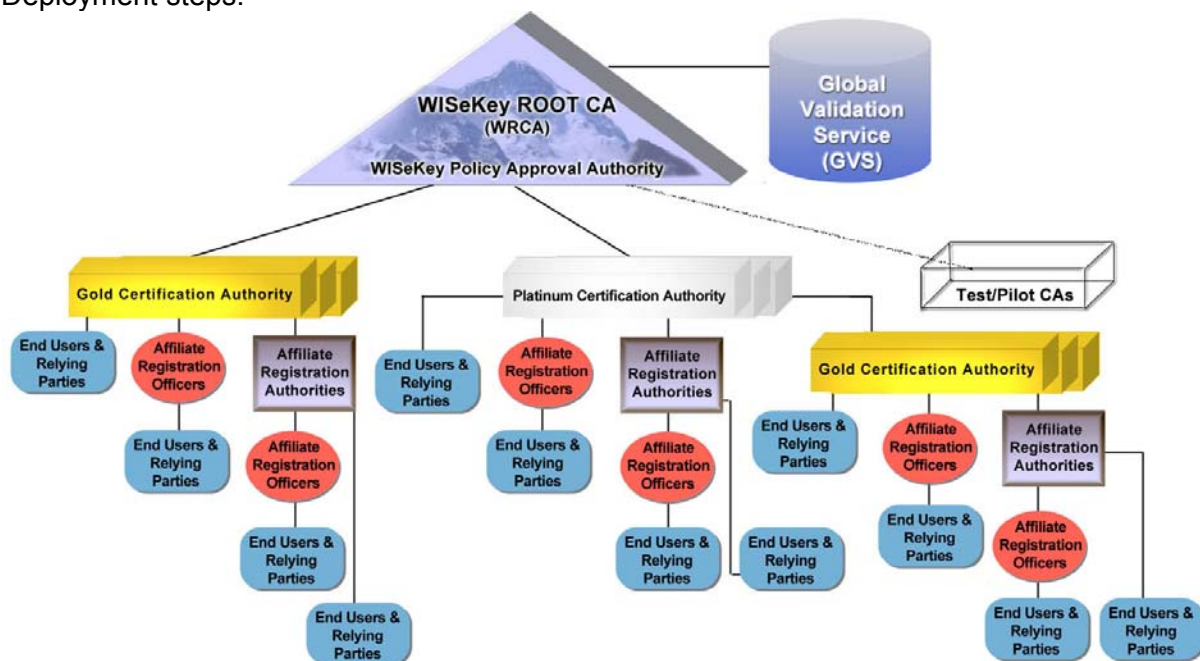
*WIS@key*

## Introduction

Within the framework of the ITU-WISeKey-WTC Geneva Partnership Agreement, WISeKey is assisting the ITU in expanding the Electronic Commerce for Developing Countries (EC-DC) project in more than 100 developing countries. This framework will soon enable developing and least developed countries to acquire and use secure e-services solutions through non-exclusive partnerships with the industry as described in this document. As part of this cooperation, a Registration Authority deployment in over 100 developing and least developed countries worldwide has become a reality. In May 2001, the ITU and WISeKey launched a secure Portal including a secure B2B e-marketplace based on PKI and announced a technology neutral approach for the deployment of this global PKI.

Under this cooperation, participating countries will benefit from first-class security and trust services for e-transactions under affordable conditions by pooling and sharing available resources. In addition to the potential economic advantages, the project is creating an environment to stimulate investments & development of the ICT infrastructure, providing an easy start-up solution to entrepreneurs and bridging the digital divide.

This document allows you to understand the various levels of participation within the WISeKey PKI infrastructure; the functions of an Affiliate Registration Authorities; the content of the package; the requirements to operate an Affiliate Registration Authorities; and the Deployment steps.



### Hierarchy of the WISeKey Public Key Infrastructure

There are four levels of infrastructure available under the WISeKey Public Key Infrastructure (PKI), they are the Bronze, Silver, Gold and Platinum levels. Both the Bronze (Affiliate Registration Organisations) and Silver (Affiliate Registration Authorities) levels provide Registration Authority services which include face to face identification of certificate applicants and input of authentication data to enable the Gold and Platinum levels – the actual Certification Authorities – to generate, suspend, revoke and, in general, manage the

life-cycle of digital certificates. The following diagram illustrates the WISeKey PKI infrastructure and the corresponding levels and possible links between them.

The differences between Affiliate Registration Organisations and Affiliate Registration Authorities are primarily their position within the WISeKey PKI and the infrastructure required to operate them. Affiliate Registration Organisations provide the Registration functions for End Users as they identify certificate applicants, process certificate issuance, suspension, and revocation requests as well as maintain an archive of their provision of such certification services. Because of the basic infrastructure they are required to maintain, they have less autonomy than Affiliate Registration Authorities for localising and tailoring their certification services to specific needs.

The functional advantage of the Affiliate Registration Authority is that an organisation can manage its certification services at a central location, with many Affiliate Registration Organisations in different geographical locations providing certification services. For example, where the cost of an Affiliate Certification Authority are not justified, an Affiliate Registration Authority can be established at the national level having offices in several cities and towns, each of which are connected to the PKI as Affiliate Registration Organisations.

In addition, Affiliate Registration Authorities can:

- Determine which certificate policies they will support from those available from their super ordinate Affiliate Certification Authority that issued its ARA certificate;
- Customize the Affiliate Registration Organisation user interface to their local needs, e.g. local language support, localised presentation format etc.;
- Negotiate with their Affiliate Certification Authority, that issued their ARA certificate, to have Certificate Policies adopted to local requirements;
- Use a dedicated infrastructure for the provision of certification services requested by its Affiliate Registration Organisations and End Users.

WISeKey Affiliate Certification Authorities (Platinum or Gold level) are organizations that have many members (certificate holders) and are widely recognized in their community as a Trusted Third Party. The level of investment and technical staffing required for Affiliate Certification Authorities is significantly different to the Affiliate Registration Organisation and Affiliate Registration Authority levels. Typically Affiliate Certification Authorities are either specifically set-up as a separate organisation, or as a department or subsidiary of an organisation. Normally, the decision to become an Affiliate Certification Authority is based upon the organisations internal need for such an infrastructure, their capacity to make the necessary investment and their ability to mass-market certification services. An Affiliate Certification Authority can brand its certification services and develop its own Certificate Policies and procedures, according to the requirements and needs of its market.

The present document focuses on the Affiliate Registration Organisations (ARO's) and therefore covers issues of relevance for the establishment and operation of an Affiliate Registration Organisation, namely: Affiliate Registration Organisation Functions, Bronze Service Provider Package Description, Requirements to operate an Affiliate Registration Organisation and Deployment Steps.

## **I. Affiliate Registration Organisation Functions**

ARO's perform a series of functions which allow the decentralisation and outsourcing of several activities required for the provision of certification services. In performing such functions, ARO's are required to comply with:

- the Certification Practice Statement of the Affiliate Certification Authority it is subordinated to;
- the Certificate Policy corresponding to the certificates it processes (e.g. Identity Certificates, Confidentiality Certificates, etc.) and the Privacy Policy
- the ARO Administrator Guide; and
- the ACA - ARO Agreement

The essential functions ARO's perform include:

- Identification of End Users
- Secure Cryptographic Key Pair Generation
- Requesting the issuance, renewal, suspension and revocation of certificates
- Maintaining archives of their operations, including the documentation presented by certificate applicants.
- Local training on information security and the use of public key certificates.
- Distribution of certificates, PIN letters and key pair storage devices to their customers.
- Additional Revenue Generating Services

### **a) Identification of End Users**


One of the fundamental activities undertaken by AROs for the provision of certification services is the identification of the entity to which a certificate will be issued, be it an individual or a legal entity (i.e. company or other institution). Due to the ease of deployment and low cost of Affiliate Registration Organisation systems, they are ideal candidates to either directly perform the identification of certificate applicants or know what local entities can securely provide such identification services (e.g. notaries, chambers of commerce, and trade registries).

The Affiliate Registration Organisation can develop its own business plan to determine whether identification should be done directly by itself, or through a reliable outsourced entity that complies with the high-security identification procedures required in the WISeKey PKI and described in the CPS and Certificate Policy of the relevant Affiliate Certification Authority.

In some cases, the Affiliate Registration Organisation can be installed within an institution or a company in order to provide certification services for the employees of such an institution or company. The identification procedure may therefore be done internally as the records of each employee are already maintained and easily accessible.

In all cases, ARO's are required to maintain an archive of all documentation used in the identification procedure (regardless of whether it is outsourced or not) as explained in the "Maintaining Archives" section below.

### b) Secure Cryptographic Key Pair Generation

 Most End Users do not have the capacity or knowledge to generate the cryptographic key pairs required for the issuance of a certificate. It is therefore necessary to provide them with a mechanism by which they can obtain cryptographic key pairs in a sufficiently secure manner by using appropriate algorithms and guaranteeing that a copy of such key pair is not held by anybody else.

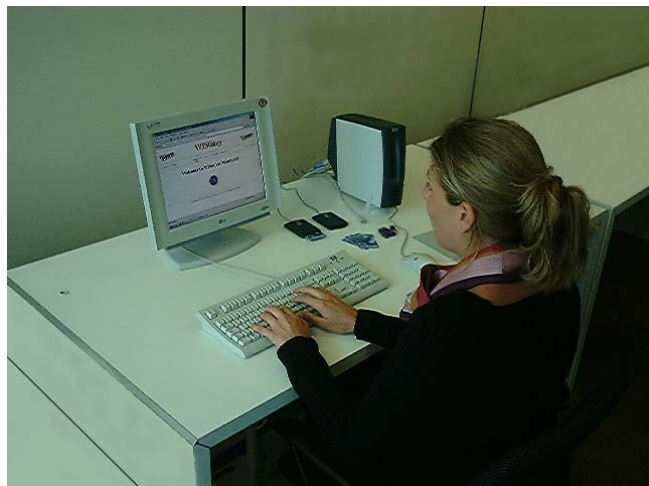
Affiliate Registration Organisations have the capacity of generating cryptographic key pairs in a way that complies with international standards and provides the aforementioned guarantee. Where an ARO cannot provide this service, the Affiliate Certification Authority or Affiliate Registration Authority would do so on its behalf and deliver it directly to the End User or to the ARO.

The ARO system includes a standard implementation for high security key pair generation services. This is based on the capabilities of dedicated USB token and smart card products to generate key pairs on the hardware itself. At no moment is the private key ever outside the hardware in which it is generated (USB token or smart card) and it is protected in such a manner that there is no way to recover, backup or archive the private key.

### c) Requesting the issuance, renewal, suspension and revocation of certificates

Affiliate Registration Organisations play a crucial role in the WISeKey Public Key Infrastructure as they constitute the "tentacles" that give local access and support to End Users. Consequently, End Users become THEIR CLIENTS, which represents an opportunity to offer other goods and services.

In doing so, they provide End Users with the possibility of locally sending the certificate requests for high-security certificates (which are more secure than certificates downloaded from a Web Site). ARO also provides a location that End Users can contact or visit to request the suspension or the revocation of their certificates in the event that, for example, they lose their private key. It is important to note that under no circumstances can the private key be recovered if the USB token or smart card are lost, destroyed or damaged. In such cases, a new key pair must be generated and a new certificate issued.



**Registration Officer working place**

#### d) Maintaining Archives

Affiliate Registration Organisations maintain archives of their operations in accordance with the Privacy Policy of the ACA under which it operates. This includes all of the physical documentation presented by certificate applicants during the certificate application process. These archives constitute an essential part of providing certification services because, in the event that the validity of a certificate or a digital signature is doubted, the procedure undertaken by the ARO and the documents archived will be the proof that the certificate issuance process was done appropriately and is therefore reliable as proof of identity and other aspects provided by the technology and the applicable law (e.g. integrity, legal validity, etc.).



Cabinet for archiving

#### e) Distribution of certificates, PIN letters and key pair storage devices to their customers



If the ARO decides to provide a full certificate processing center, they will have the capacity to locally manage the distribution of certificates, cryptographic key tokens and the PIN letters for the tokens. Depending on the implementation required by the ARO, this might include printing of smart cards (e.g. with the ARO logo, the client's picture and/or the client's logo).

#### f) Local training on information security and the use of public key certificates

Many ARO clients will require training on the problems that arise with regard to information security, on the use of certificates and other related areas. This may constitute an additional source of revenue for ARO's and hence improve its business model.

#### g) Additional Revenue Generating Services

As it is well-known, certificates are a tool that can be used for many purposes, in much the same way that a manual signature and identity documents have been for many centuries. WISeKey is constantly seeking applications in which the End Users can actively use their certificates. In order to satisfy the needs of their clients, the ARO's may have a wide variety of applications and online services which their customers may be able to access upon payment of a subscription fee and purchasing a WISeKey certificate. In such cases, the ARO could generate additional revenue from the sale of subscription to such applications or online services.

## II. Bronze Service Provider Package Description

### Pre-configured and tested Registration Authority PC including

#### System

- Windows 2000 based system including
- Ethernet LAN adapter and modem
- Keyboard and mouse
- 15" LCD monitor
- Smart card reader for serial port
- Smart card reader for USB port
- Administrator smart card



#### Software

- Unicert Web RAO application software
- Driver software for USB token and smart cards
- Microsoft Internet Explorer (128bit)
- Acrobat Reader



#### Plus :

- First year subscription to 300 standard certificates
- Legal, operational and technical documentation
- Directory and validation services via WISeKey's Ecommerce PKI CA
- Training for Registration Authority Officers (BSP Users) in Geneva, CH
- Support via email
- Independent audit (excluding costs of travel and expenses)
- Hardware and software maintenance
- Order processing for smart cards, smart card readers and tokens

#### Not included: (customer is responsible for these items)

- On-site installation of the BSP system
- Connection to the Internet or other communication facilities
- Communication costs

#### NOTE:

The BSP System is strictly dedicated for the purpose of registering WISeKey certificate subscribers and may not be used for any other application or purpose outside the scope defined by the Affiliate Registration Organisation Agreement.

Delivery of the WISeKey Bronze Service Provider is subject to export authorisation for the restricted products included in the package.

WISeKey may make changes to these specifications at any time.

### **III. Requirements to operate an Affiliate Registration Organisation**

#### **a) Physical Infrastructure**

- On-site Software archives
- On-site and Off-site secure archives for physical documents.
- Area with restricted access (room with reasonably secure locking mechanism accessible only by persons authorised to work in the ARO service)
- Secure compartment or safe (with a reasonably secure locking mechanism accessible only by the person(s) who are authorised to operate the system) in which to store the operator smart card while the ARO system is not in use

#### **b) Technological Services**

- 220 V 50 Hz power supply
- Local computer support services which can serve the needs to maintain the systems
- Internet Service Provider connectivity at a speed of at least 33.6 Kbps or direct LAN connection to the Internet

#### **c) Staff**

- At least 2 staff appropriately trained with the ability to perform checks and to process End User applications (previous experience in establishing company registers or working in building up trade registers is a bonus).
- Staff should not have any criminal convictions (recent police records are required as proof of this).

#### **d) Documents**

The following documents needs to be presented during the Request Phase described in section IV:

- Copy of its statutes or by-laws duly registered in the Registry of Commerce together with the physical address of the Affiliate Registration Organisation and the name of the officer of the organisation responsible for its operation. For entities which are not registered in the trade registry are also acceptable (e.g. official documents of public entities, notaries, etc.)

- The names together with an extract from the Police Records for every person whose work will be related to the ARO operation (including the sensitive functions such as identity verification).
- A signed declaration from the organisation certifying the existence in the organisation's offices of premises where access is restricted only to authorised personnel and a description of such premises and the access control mechanisms available (e.g lock and key, smart card access, or biometrics, etc.).
- A description of the market for digital certificates that the applicant could foreseeable penetrate.
- Signing of a Bilateral Non-Disclosure Agreement.
- A description of the Internet access service used by the applicant.

#### **e) Operational Requirements**

- First level Support for End-User – the Applicant needs to ensure that it is able to provide first level support for its End-User. This first level support should include answering general PKI questions, as well as solving hardware and software problems related to the usage of certificates.
- Suspension and Revocation Service - the Applicant needs to be able to provide a suspension and revocation service according to the Ecommerce PKI CPS. He should be able to execute a revocation or suspension request triggered by an End-User via phone, fax or email within 12 hours or contact the WISeKey Suspension and Revocation Service within 2 hours.
- Sale of Accessories – the Applicant should be prepared to offer basic equipment, like card reader, USB extensions, etc., to End-Users.

## IV. Deployment Steps

### a) Request Phase

The first step in establishing an Affiliate Registration Organisation requires the interested organisation to demonstrate its capacity to perform ARO functions and meet the requirements as described in section II. This is essential as failure to exercise the functions appropriately can incur legal liability for the organisation. After sending an official request by using the *ARO Request Form* an organization needs to submit all required documents. After WISeKey has examined those documents with the result that the Applicant is compliant to the requirements the next phase will begin.

### b) Contract Phase

A chain of contracts supports the WISeKey PKI hierarchy, which includes a contract between Affiliate Registration Organisations and the Affiliate Certification Authority that issued its certificate or the Affiliate Registration Authority it is subordinated to. The second phase in deployment is thus the establishment of a contractual relationship between the Affiliate Registration Organisation and the relevant entity. This contract allocates the rights and obligations of the parties in the operation of their respective PKI entities, which in the case of Affiliate Registration Organisations, include the following:

- The existence of no *de legge* or *de facto* conflicts or incompatibilities in the nature of the organisation that will be implementing and providing of certification services.
- Compliance with standards no lower than those required by the traditional law (where it allows such certification methods to meet formal or evidentiary requirements) or with electronic commerce and electronic signature legislation (under discussion or enacted).
- Respect of statutory or contractual privacy and data protection rights of its clients and compliance with the corresponding obligations arising from the Affiliate Certification Authority's Certification Practice Statement and Privacy Policy.
- Compliance with any applicable consumer protection legislation as well as any other relevant law.
- Attainment of the necessary authorisations for the importation, use, sale and provision of cryptographic goods and services of the quality and security levels imposed by statutory or contractual requirements.

Insurance (where available) covering among other things:

- The erroneous or omitted identification of a certificate applicant.
- Damages incurred as a result of claims based on the Registration Authority's activities, loss of information caused by system malfunction or misuse.
- Loss, theft, modification or unauthorized access to the Registration Authority's private cryptographic key or other information stored in its secured systems.
- Loss, damage to or theft of the ARO system.

Performance of Affiliate Registration Organisation functions as described in section I.

Infrastructure and procedural security to maintain a high level of security of the hardware, software, cryptographic keys, activation data (e.g. passwords) and the records of the Affiliate Registration Organisation activities.

### **c) Delivery, Training and Audit Phase**

Once the basic requirements are met and the contract is signed, payment of 50% of the ARO system costs is required to be made by the Applicant. After receiving this payment, the ARO System shall be delivered to Applicant. WISeKey or the Affiliate Certification Authority provides a system that includes the hardware and software specified in the section II of this document, providing full ARO functionality.

After system delivery, a one-day training workshop held in Geneva (or at Applicant's offices – travel and accommodation expenses paid by Applicant) is held, were the Applicant considers it is prepared to commence operations, an audit is undertaken to ensure compliance and capability to comply with the requirements. The training workshop is available for 2 Applicant representatives (conducted in Geneva, Switzerland) and focuses on:

- ARO implementation, operation and maintenance, designed for the applicant organisations' technical staff that will operate the system.
- Strategy, legal and technology issues related to secure electronic transactions designed for applicant organisations' management and/or sales staff.

Some modifications on the End User Agreement and other documentation may be required in the Applicant's jurisdiction (e.g. adjustments to comply with local law, translation to local language, drafting of a customised Certificate Policy). The costs of the modifications will be paid by the Applicant.

### **d) Activation Phase**

The successful completion of the audit will be followed by the activation of the ARO at the CA level, after which the ARO is able to issue certificates. Within a period of 15 days following activation, the Applicant is required to pay the remaining 50% of the ARO System invoice.

The audit costs, travel and accommodation expenses as well as any taxes and transactions costs are paid by ARO in accordance with the invoice and expense reports presented by the auditor and relevant WISeKey staff.