



Citizen ID

Product Sheet Citizen ID

OpenTrust

24/10/2013

Product Sheet



1 INTRODUCTION

This document summarizes the product overview of Citizen ID (Sequoia) PKI suite from OpenTrust, previously named Keynectis.

Citizen ID is the new branding name of the certified product previously called “Sequoia” and referenced as such by French ANSSI. For the sake of coherence, the denomination “Citizen ID (Sequoia)” is constantly used hereunder.

2 PRODUCT OVERVIEW

Citizen ID (Sequoia)® v2 is a complete product suite for secure electronic Identity Management for governments, administrations, industry, and end users. It covers all needs for protection of electronic information and sensitive data.

Citizen ID (Sequoia)® V2 is available in two modes:

On premises Mode: Software solution installed a license on premises. Adapted to all customer requirements, Citizen ID (Sequoia)® enables clients to manage themselves their Public Key Infrastructure and allows implementing a large variety of business cases.

SaaS Mode (Software as a Service): Service managed on a multi-tenant platform, hosted in OpenTrust’s high-secure data center. Based on its expertise as Certified Trust Service Provider (French label “PSCE/PSCO”), OpenTrust assures highest requirements in terms of high availability and security for the benefit of its customers.

Citizen ID (Sequoia)® suite contains three software components:

Keyseed (version 2.6.2):

Offline software module in charge of CA lifecycle management, connected to a Hardware Security Module (HSM). This module enables in particular, CA key pair generation, CA certificate signature, Authority Revocation Lists (ARL) Signature, import and export of secret keys.

Trust.Center (version 2.3.5):

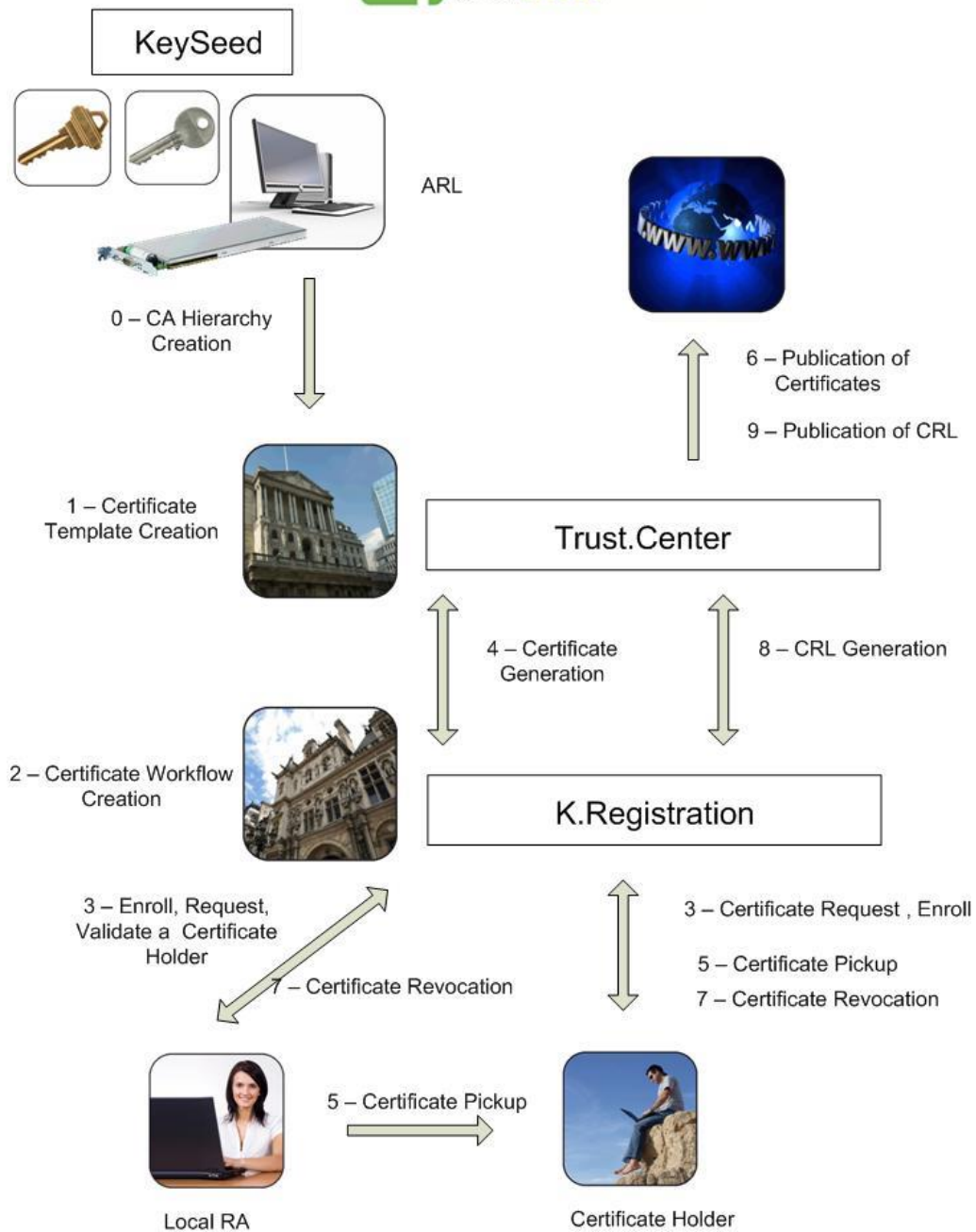
Software module in charge of end user certificate life cycle management, i.e certificate template definition, certificate and certificate revocation lists (CRL) generation.

K.Registration (version 2.6.7):

Software module in charge of end user certificate lifecycle management workflows (enrollment, validation, issuance, pickup, revocation, renewal)



Citizen ID (Sequoia) OPENTRUST



These modules can be used in combination to implement a complete PKI. It is also possible to use them independently. Following configurations are possible:

- KeySeed® only
- Trust.Center® only
- Trust.Center® in combination with KeySeed®
- Trust.Center® in combination with K.Registration® and KeySeed®



3 SECURITY FEATURES

3.1 Security Certification

Citizen ID (Sequoia) has been certified Common Criteria EAL4+ by the French ANSSI.

The certificate is available on http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/p_19_Sequoia_v2.html

3.2 Security Services

Citizen ID (Sequoia) allows to set up the following services for certificate management and associated revocation lists :

- Enrolment Service ;
- Certificate Request Service ;
- Certificate Generation Service ;
- Certificate Pick Up Service ;
- Revokation Service ;
- Publication Service ;
- Service for creation and management of trusted roles (admin, operator, auditor)
- Journal & Audit Services.

3.3 Security Target

The underlying Target of Evaluation (TOE) has been published by ANSSI.



4 TECHNICAL FEATURES

4.1 Performances

The solution allows to produce a very big number of certificates per day.

Citizen ID (Sequoia) is able to reach highest throughput with figures surpassing several Million certificates per day and depending only on hardware infrastructure (number of servers, high availability configuration, load balancers)

4.2 Operational Environnement

4.2.1 Hardware and Operating System Requirements

Component	Equipment	Operating System
Keyseed®	PC / Workstation	Windows 2000 (Windows XP SP 3 recommended) Linux Ubuntu 10.04 or Redhat 5 with pdf reader
K.Registration® and Trust.Center®	Server Solaris v240 / T200 or Server HP ProLiant DL380 G5 / DL360 G6	Solaris 10 or Linux Redhat ES5

4.2.2 Required Software Components

Component Citizen ID (Sequoia)	Software	Recommended Version
K.Registration® Web Server	Apache	httpd-2.2.3-22.el5
	mod_ssl	mod_ssl-2.2.3-22.el5
	mod_jk (plug-in Apache / Jboss)	ks-mod_jk22-1.2.28-FCS
K.Registration® Application Server and RA Proxy Server and Trust.Center® : Application Server and Crypto Server	Java JDK	jdk-1.5.0_11-fcs crypto librairies Citizen ID (Sequoia) Sequoia.Security version 2.4.0 and bouncycastle (Java) version 1.43



(HSS)		
K.Registration® and Trust.Center® Data Base Server	Oracle, including Command Line Interface sqlplus for execution of sql script during installation	11g
Trust.Center® Web Server	Apache	httpd-2.2.3-22.el5
	mod_ssl	mod_ssl-2.2.3-22.el5
	openSSL	0.9.8l
	mod_jk (plug-in Apache / Jboss)	ks-mod_jk22-1.2.28-FCS

4.2.3 Workstation - TOE actor

The required work stations for TOE actors are specified as follows:

- Operator Workstation:
 - o Hardware : PC type workstation ;
 - o Software : Operating System Microsoft (Windows 2000, recommended XP Professionnel Version 2002 Service Pack 3), Web browser (Internet Explorer 7.0 upwards or Mozilla Firefox 3.6 upwards) ;
- System Engineer Workstation:
 - o Hardware : PC type workstation ;
 - o Software : Operating System Microsoft (Windows 2000, recommended XP Professionnel Version 2002 Service Pack 3), Web browser (Internet Explorer 7.0 upwards or Mozilla Firefox 3.6 upwards) ;
 - o

4.2.4 Certificate Holder PC

The PC requirements are as follows :

- Hardware : Regular Personal Computer ;
- Software :
 - o Web browser and email client : Lotus Notes Compatible PKCS#11 version 6.5 upwards, Mozilla for version 1.0 upwards, Outlook 2000 for versions Outlook 2000, 2002 and 2003, Outlook Express versions 5 upwards ;
 - o Operating System : Windows 2000, XP (Service Pack 3) and Vista.

4.2.5 Smart Cards

Following smart cards are supported :

- GemXPRESSO (TP IS v2) Gemalto ;
- Ypsid card sscd (Sagem Orga) ;
- TPC IMCY (Axalto) ;
- ActivCard (ActivIdentity) ;
- AuthentIC V4 (Oberthur) ;
- ID One Cosmo (Oberthur) ;
- Instant EID IP2 Setec ;

4.2.6 HSM

Following Hardware Security Modules are supported :



- Trustway ;
- Luna SA, CA, SP et XP ;
- Thales NCipher NShield
- Cryptographic module ANSSI (IGC/A) only with component KeySeed®.

5 CONTACTS

Sales Contact: M. Sylvain David – Key Account Manager +33 1 55 64 22 06 / +33 6 60 21 15 70
sylvain.david@opentrust.com

Technical Contact: M. Régis Ktorza – Pre Sales Engineer +33 1 55 64 22 24 / +33 6 42 61 37 78
regis.ktorza@opentrust.com