

WISeKey CertifyID Registration Manager Administration Portal User Guide

Date: October 2008
Version: 1.10.0
Authors: WISeKey SA

TABLE OF CONTENTS

1 ABOUT THIS MANUAL.....	4
COPYRIGHT	4
PRE-REQUISITES	4
DOCUMENT CONVENTIONS.....	4
TERMINOLOGIES USED IN THE DOCUMENT	5
SERVER-SIDE HARDWARE REQUIREMENTS	6
SERVER-SIDE SOFTWARE REQUIREMENTS	6
BROWSER CLIENT COMPATIBILITY	6
2 ABOUT CERTIFYID REGISTRATION MANAGER ADMINISTRATION PORTAL.....	7
INTRODUCTION	7
USER INTERFACE FRAMEWORK	9
FRAMEWORK WIZARDS.....	9
USER INTERFACE NOTATION	9
END ENTITY MANAGEMENT MODULE	10
2.1.1 USER RESOURCE MANAGEMENT MODULE	10
2.1.2 COMPANY RESOURCE MANAGEMENT MODULE	19
SECURITY MANAGEMENT MODULE	23
2.1.3 LOG MANAGEMENT MODULE	24
PKI MANAGEMENT MODULE.....	25
2.1.4 REQUEST MANAGEMENT MODULE	25
2.1.5 CERTIFICATE MANAGEMENT MODULE	28
USER AND ADMIN NOTIFICATIONS:.....	32

1 About this Manual

This guide helps the Administrators / Users to create/manage/remove entities like user, company, group, role, Certification Authority, Certificate Template, certificate, requests.

Copyright

No part of the contents of this document may be reproduced or distributed in any form or by any means without the prior written permission of WIS@key SA.



is a registered trademark of WIS@key SA.



is a registered trademark of WIS@key SA.

Microsoft, MS are registered trademarks, and Windows is a trademark of Microsoft Corporation.

Published in Geneva, Switzerland, by WIS@key SA.
Copyright © 2008 WIS@key SA.
All Rights Reserved.

Pre-requisites

This guide assumes that the reader/user is familiar with general public key infrastructure (PKI) process and the terminologies used in it. In addition the user should be conversant with Windows 2003 Server administration, Certificate Authority services, SQL server and its use.

Document Conventions

This User Guide uses the following conventions:

- **NOTE** means *reader take note*. Notes contain helpful suggestions.
- **IMPORTANT** means the reader must follow the instructions strictly.
- Descriptions for significant fields are available.

Terminologies Used in the Document

The following table lists the meaning of key terms used in this User Guide.

Term	Description
Certificate Signing Request (CSR)	CSR is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate
Secure Sockets Layer (SSL)	SSL is a cryptographic protocol that provides secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers.
Group	Group is a special resource that defines the access to other resources using the group-resource membership. All resources should be linked to at least one group
User's Active Group	User's active group is the one which is active at the time of user creation. This can be changed by administrator later
Target Role	Every group should be targeted to at least one role of the logged-in user. Target Role - Group association defines the operation permission of the users associated to the role
Certificate	A Digital Certificate issued by a Certification Authority.
Certification Authority (CA)	A CA is an entity that is trusted to issue and manage certificates. A CA is part of a Public Key Infrastructure, which is typically used to provide the underlying security services that are part of the security solution for conducting business on the Internet, ensuring that electronic transactions are conducted with confidentiality, data integrity, proper user authentication, and protection against repudiation.
Database	A set of relative information created, stored, or manipulated by a computerized management information system.
Digital Certificate	A Digital Certificate is a digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. A digital certificate is a data structure used in public key system to bind a particular, authenticated individual to a particular private key.
Revocation	To change the status of a valid or suspended certificate to 'Revoked' from a specified time and forward.
Uniform Resource Locator (URL)	Also a synonym for Uniform Resource Identifier (URI), a URL is a string of characters that is used to identify or name a resource. URLs are mainly used to enable interaction with resources on a network, such as the World Wide Web (WWW), via specific protocols.

Server-side Hardware Requirements

Hardware	Description
Hard Disk Space	100 MB of free hard disk space on webserver plus on Database server ~1 MB per 20 users.

Server-side Software Requirements

Software	Description
Operating System	Windows Server 2003 or Windows Server 2008
RDBMS	SQL Server 2005
MCSA Web Service	1.2.0029 or higher
CertifyID Policy Module	1.2.25.0 or higher

Browser Client Compatibility

Software	Description
Operating Systems	Windows (XP, Vista, Server, ME, 98), Linux, Unix , Mac, or any system running one of the browser versions below
Web Browsers fully supported	Internet Explorer 5, 6, 7 Mozilla Firefox 1.5, 2, 3
Web Browsers working but not actively supported	Internet Explorer 8 beta Safari 2, 3, 4 Opera 8, 9

2 About CertifyID Registration Manager Administration Portal

Introduction

The administration portal helps user to define, manage and monitor all the components of the certification services infrastructure. This is also used by Registration Officers to manage the identity lifecycle of the user community. Access to this portal is highly secured. Users can login to this portal with certificates, using SSL with certificate authentication. This portal enables the creation and management of different eID templates, and policies, for flexibility in different scenarios.

The portal currently supports languages English, Spanish, French and German. URA Administrator can switch to any of the available languages of his/her preference. This can be achieved by selecting the list available in top right and above the upper banner menu.

The core function can be grouped into three main modules:

- End-Entity Management Module
- Security Management Module
- PKI Management Module

These main modules are accessible through the upper banner menu panel

WIS@key CertifyID

Logged on user and user's active group.
ADMIN@ROOT GROUP

Languages supported
English

Home | End Entity Management | Security Management | PKI Management | Logout

URA ADMIN PORTAL

Upper banner Menu

Side banner Menu

End Entity Management

- Manage users
- Manage companies

Security Management

- Manage roles
- Manage the access control list
- Manage operations and actions

PKI Management

- Manage certificate authorities
- Manage certificate templates
- Manage certificate requests (create, submit, defer, deny)
- Manage certificates (approve, issue, suspend, revoke)

Figure 1: Certify ID Registration Manager Administration Portal in English



Figure 2.1: Certify ID Registration Manager Administration Portal in Spanish



Figure 2.2: Certify ID Registration Manager Administration Portal in German



Figure 2.3: Certify ID Registration Manager Administration Portal in French

User Interface Framework

Framework wizards







Users, Companies, Certificate Templates, etc are considered resources of the system, and they are all managed in a consistent user interface framework including the operations below:

- Create
- Edit
- Save
- Approve
- Suspend
- Deny
- Remove
- Search

The usage of the operations is described in individual sections of this document.

User Interface Notation

System includes some notation below :

-  : View the detail of a system resource such as a user, a company or a certificate, etc
-  : Add a user into a group or add a certificate template into a role, etc
-  : Remove or select to edit a user from a group or a certificate template from a role, etc.
-  : Remove a user from a group or remove a certificate template from a role, etc.
-  : Turn back the previous screen including a resource listing page or a framework wizard step.
-  Each of the main modules contains one or several resource modules and each resource module comprised of following pages:
 - Browse/Search Page
 - View Page
 - Create Page

The resource modules are accessible through side banner menu panel once a main module was selected.

End Entity Management Module

The End-Entity management module has following resource modules:

- User Management
- Company Management

Main Functionalities of End Entity management:

- Browse the user database and filter by user status.
- Approve, deny, reject or defer user registrations.
- Create, manage and edit user and company profiles.

2.1.1 User Resource Management Module

The user management page summarize the possible operations can be effected on user resources.

The screenshot displays the WISEkey CertifyID Admin@Root Group user management interface. The page title is "LIST OF ALL USERS". The interface includes a "Create New User" button, a search bar, and a "View results from all sub groups" checkbox. The table below shows the list of users:

ID	Name	Last Name	Email	Login Title	Group	Status	Display
5	Guest	User1	guest1@wisekey.com	guest1	Root Group	Active	→
3	John	Smith	jsmith@wisekey.com	jsmith	Sub Group	Active	→
2	John	doe	jdoe@wisekey.com	jdoe	Root Group	Active	→
1	WISEkey Admin		admin@wisekey.com	administrator	Root Group	Active	→

Page 1 of 1

Figure 3: User Management

As shown in Figure 3, user management page allows creation of a new user, searching an existing user or browse users belongs to the active group.

2.1.1.1 Create new user

The creation of a new user is through a web wizard as shown in the Figure 4. The use of the wizard simplifies entry of the data. User can skip optional steps in the wizard. Mandatory fields in each wizard page are displayed with a red asterisks (*).

USER REGISTRATION PROCESS WIZARD (STEP 1 OF 3)
Please fill in basic user information

User Basic Information	
Title	<input type="text"/>
First Name *	<input type="text"/>
Middle Name	<input type="text"/>
Last Name *	<input type="text"/>
Email	<input type="text"/>
Mobile	<input type="text"/>
UID	<input type="text"/>
Preferred Language	English
Login Title	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Role *	Administrator

USER REGISTRATION PROCESS WIZARD (STEP 2 OF 3)
Please fill in basic user information

Address	
Address Line 1	<input type="text"/>
Address Line 2	<input type="text"/>
Address Line 3	<input type="text"/>
Zip	<input type="text"/>
City	<input type="text"/>
State	<input type="text"/>
Country	Select
Phone	<input type="text"/>
Fax	<input type="text"/>

USER REGISTRATION PROCESS WIZARD (STEP 3 OF 3)
Please fill in basic user information

Use existing company information with company ID
 Edit the company information page

Company Information	
CompanyID / Name	<input type="text"/> <input type="button" value="Load Company"/>
Company Name	<input type="text"/>
Position	<input type="text"/>
Department	<input type="text"/>

Figure 4: Creation of a new user

During the entry of data, the user is instructed to fill in the mandatory information and also to provide correct details. For example, email address like joe@wisekey.ch. An in-correct detail stops the user from proceeding to further steps.

USER REGISTRATION PROCESS WIZARD (STEP 1 OF 3)
Please fill in basic user information

User Basic Information	
Title	<input type="text"/>
First Name *	<input type="text"/>
Middle Name	<input type="text"/>
Last Name *	<input type="text"/>
Email	<input type="text"/>
Mobile	<input type="text"/>
UID	<input type="text"/>
Preferred Language	English
Login Title	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Role *	<input type="text"/>

Please fix the following errors:

- First Name is mandatory
- Last Name is mandatory
- Role is mandatory

Figure 5: Mandatory fields are highlighted

And the optional information like user address, user company information can be entered or not, by selecting appropriated options in the wizard.

The image shows two screenshots of the 'USER REGISTRATION PROCESS WIZARD'. The left screenshot is 'STEP 2 OF 3' and contains a form titled 'Please fill in basic user information' with fields for Address Line 1, 2, and 3, Zip, City, State, Country (a dropdown menu), Phone, and Fax. The right screenshot is 'STEP 3 OF 3' and contains a form titled 'Please fill in basic user information' with radio buttons for 'Use existing company information with company ID' and 'Edit the company information page'. Below these are fields for CompanyID / Name (with a 'Load Company' button), Company Name (a dropdown menu), Position, and Department.

Figure 6: User creation optional information

A new user can be created in the application by clicking “Finish” button at any step in the wizard. After successful creation of user account the page is redirected to user view page.

2.1.1.2 Search a user

The search user page part of user management page helps in searching existing user from user database who belongs (linked) to the current active group. In addition, there is option to fetch users from the user’s current active group and its subgroups.

The screenshot shows a search form with a checked checkbox labeled 'View results from all sub groups', a dropdown menu currently set to 'All', a text input field for the search term, and a 'Search' button.

Figure 7: Search user

The search form fetches users based on the search filters available for user. The following are the filters available for user search

1. User ID
2. First Name
3. Middle Name
4. Last Name
5. Title
6. Mobile
7. E-Mail

Once the search button is hit, the result will be display as shown in Figure 8.

The screenshot shows the search results page. At the top, the search form is shown with 'View results from all sub groups' checked, 'First Name' selected in the dropdown, and 'John' entered in the search field. Below the form are three status filter buttons: 'All', 'Active', and 'Suspended'. The main content is a table with the following data:

ID	Name	Last Name	Email	Login	Title	Group	Status	Display
3	John	Smith	jsmith@wisekey.com	jsmith		Sub Group	Active	→
2	John	doe	jdoe@wisekey.com	jdoe		Root Group	Active	→

Below the table, it says 'Page 1 of 1'.

Figure 8: Search results set

The filtered user details can be viewed by clicking the “→” from the results.

2.1.1.3 Browse user database

Browse user database page allows viewing all users linked to the current active group or all users linked to the current active group and its sub groups based on their status and updating the user status using the button available at bottom of the page.

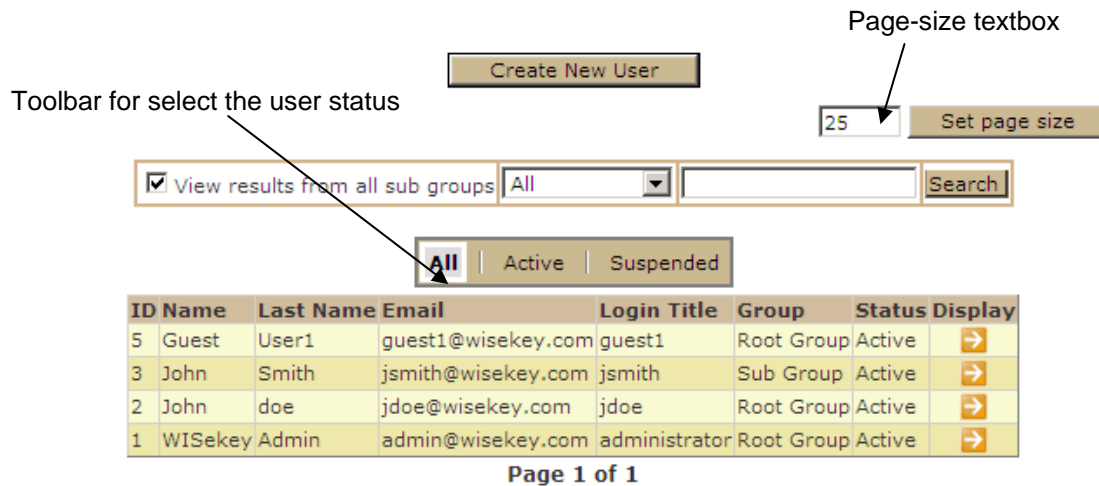


Figure 9: Browsing the User database

The user details can be filtered using their statuses as shown in Figure 9 by selecting the available statuses. Paging option is customized to list only “n” number of users based on the value defined in the page-size textbox.

User statuses and list of actions that can be taken:

- **All:** display all users details linked to the active group irrespective of status.
 - No action
- **Active:** display all users details linked to the active group whose account is approved.
 - Suspend
- **Suspended:** display all users details linked to the active group whose account is suspended.
 - Approve, Remove

The status of user can be changed by taking appropriate actions (using the available buttons) after the choosing the checkbox.

2.1.1.4 View User information

The user related information is regrouped in this page as follows:

- **User:** user’s basic information such as user names, email, phone number.
- **Address:** user’s address information.
- **Company:** user’s company name, user department and job title.
- **Request:** user’s certificate requests list.
- **Certificate:** user’s certificate list.
- **Authentication:** user’s login, password information.
- **Role:** user’s role/privilege information.
- **Group:** user’s group membership information.

User information is accessible through the application toolbar as shown in Figure 10.

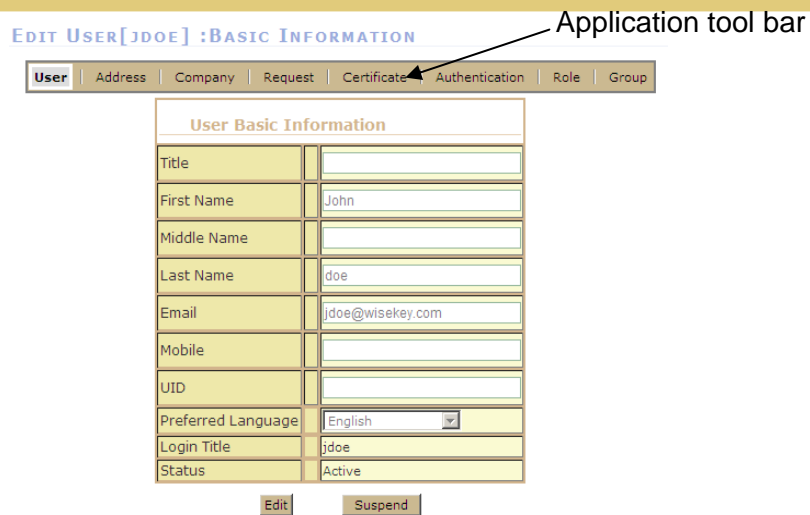


Figure 10: User basic information (View Mode)

The user information can be modified after creation by clicking the Edit button. The operation changes the view mode to edit mode.



Figure 11: User Basic Information (Edit Mode)

In Edit mode, there are two buttons “Cancel” and “Save”. “Cancel” button allows switching to View mode without making any changes to the information in data base and “Save” button allows updating the modified data in to database.

User has an option to set his/her preferred language for his session. The change in preferred language helps user to view the portal in his/her preferred language.

If user deletes the user, he/she has an opportunity for restoring the details. Choosing remove user does not provide the option of restoration of details.

User Address Information

The user address is optional information, as specified in user creation section. The user address information can be empty when user is created without address. This information can be updated later by editing the address fields.

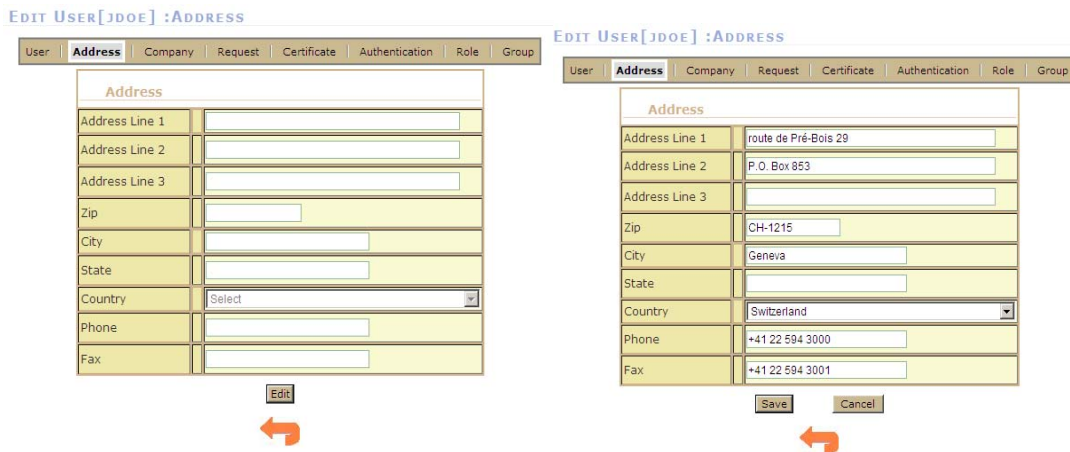


Figure 12: User Address Information

User Company Information

Same as the address, the user company is an optional information. In Edit mode, company, Job title and department should be provided to associate user to the company.

Prerequisites:

1. Company(CA) should have been created – Refer Company creation for more details

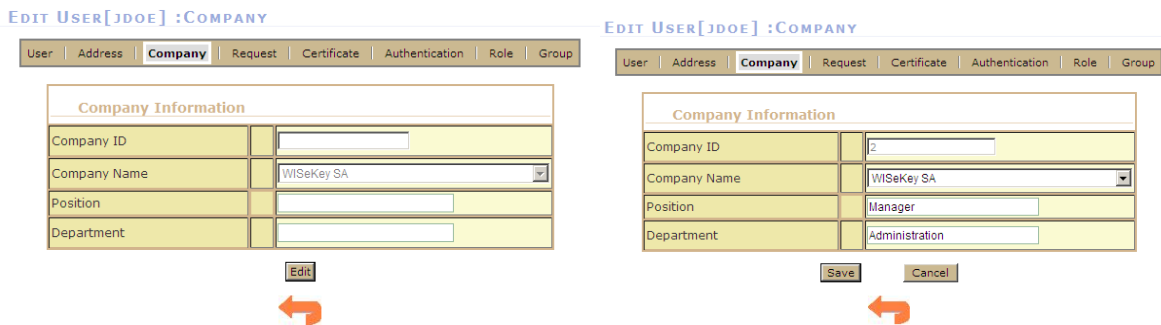


Figure 13: User Company Information

User Request Information

The user request panel allows creating new request for the user. The certificate request can be generated directly through the web enrollment or by uploading the offline pre-generated certificate request. In addition, the user's all requests are listed as shown in Figure 14.

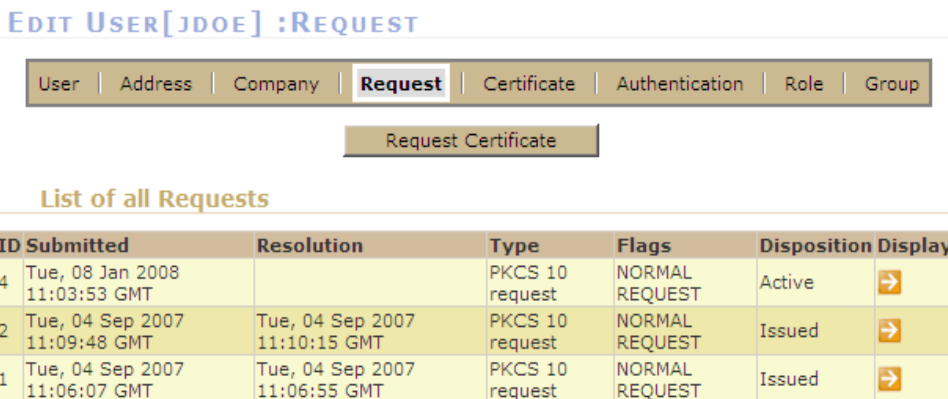


Figure 14: User Request

Enroll Certificate Request

This page will be available when at-least one of the users' active roles is associated with a certificate template. User can reach this page by clicking "Online Web Enrollment" button available.

Prerequisites:

1. Certification Authority(CA) should have been created – Refer CA creation for more details
2. Certificate Template(CT) should have been created and associated with available CA – Refer Certificate Template creation, Certificate Template -CA association and Subject field creation
3. Role should have been created and associated with available template. Refer Role creation and Role-Template association.

EDIT USER[JDoe] :REQUEST

User | Address | Company | **Request** | Certificate | Authentication | Role | Group

Request Certificate

List of all Requests

ID	Submitted	Resolution	Type	Flags	Disposition	Display
4	Tue, 08 Jan 2008 11:03:53 GMT		PKCS 10 request	NORMAL REQUEST	Active	➔
2	Tue, 04 Sep 2007 11:09:48 GMT	Tue, 04 Sep 2007 11:10:15 GMT	PKCS 10 request	NORMAL REQUEST	Issued	➔
1	Tue, 04 Sep 2007 11:06:07 GMT	Tue, 04 Sep 2007 11:06:55 GMT	PKCS 10 request	NORMAL REQUEST	Issued	➔

➔

There is no Certificate Template available for the selected User

Figure 14.1: Online Web Enrollment (no template is associated to user role).

Certificate web enrollment sections:

- **Certificate Template:** Certificate template used to generate the request. Only the templates associated to the current users role are listed. Selected template identifies the type of web-enrollment that is whether online or offline.
- **User information:** User name of the user on behalf of whom the request information is submitted.
- **Subject [Identifying Information]:** This section may be different from the Figure shown in 14.2, as the subject fields of a template are defined with any subject identifier of users' choice.
- **Subject Alternative Name Information:** This section may be different the Figure shown in 14.2, as the subject fields of a template are defined with any subject alternative name identifier of users' choice.
- **Key Options:** specify the key specification like key size, CSP.

Certificate Template	
Certificate Template Name	Administrator
CERTIFICATE WEB ENROLLMENT	
User Information	
First Name	John
Last Name	Doe
Subject	
Common Name	John Doe *
Organization	WISekey
Subject Alternative Name Information	
Key Options	
Cryptographic Service Provider	
	Microsoft Enhanced Cryptographic Provider v1.0
Key Size	1024
Mark keys as exportable	<input checked="" type="checkbox"/>
Protected private key	<input type="checkbox"/>
SMIME Capability	<input type="checkbox"/>
Generate	

Figure 14.2: Web enrollment for certificate request generation

Submit Certificate Request

Certificate request can be also uploaded offline. By selecting a template that supports offline certificate request upload, user can navigate to the offline certificate upload page.

The Figure-15 shows the uploading offline certificate request page. Request can be uploaded from a file or directly copied to textbox in base 64 format. The “upload” button parses the certificate request and display the subject information. Then by clicking “Save” button, the request could save to database. A offline certificate request should be approved by an administrator.

Figure 15: Uploading offline certificate request

Enroll Certificate Request Using Existing Public Key

After online request generation and upload of existing request, there is a third possibility, which is to use the public key of an existing request but all other information such as key usages, extension, and subjects will be added separately. When a certificate template using this option is chosen, there is an option “Using Existing Public Key” to determine whether a public key from an existing web page is used for the certificate request (see Figure 16). If this option is not active, a new keypair will be generated on submission of the form.

Figure 16: Using existing public key

Issue Certificate

The Figure 17 shows the certificate install page. This page will be displayed after the certificate request is made, and allows us to download, install or view detail of the certificate.

[Home](#) [End Entity Management](#) [Security Management](#) [PKI Management](#) [Logout](#)

Your certificate (ID:148) has been issued successfully

[Certificate details](#) [Download](#) [Install](#)



Figure 17: Uploading offline certificate request

Email Verification

For the certificate templates that require email verification, then users must use the verification url (including RequestId and verification code) sent to the users to finish request submission process. Certificate will be issued once the email has been verified.

User Certificate Information

All users' certificates were listed as shown in Figure 18.

EDIT USER [JDOE] : CERTIFICATE

User | Address | Company | Request | **Certificate** | Authentication | Role | Group

List of all Certificates

ID	Subject	Effective	Expiration	Serial Number	Disposition	Display
3	CommonName=John Doe Organization=WISekey	Wed, 05 Sep 2007 10:10:58 GMT	Fri, 05 Sep 2008 10:20:58 GMT	617F71AB000000000000C	Active	



Figure 18: User Certificate

User Authentication Information

User authentication panel specifies the user credential for access the Administration portal. Currently two authentication types are available

- Form based Password/login Authentication
- Active directory authentication

When "Form Authentication" is selected from the Authentication type drop down list, user login ID will be displayed. This field by default filled with the user's email ID but if the user wish to change this information, then this could be changed to his/her convenience.

Figure 19: Form Authentication

The password can be reset by filling Password and Confirm password as shown in Figure 19 and both of these fields should contain same value.

Same as "Form Authentication", the "Window authentication" display windows authentication information. In order to authenticate a user against an active directory, the user need to specify their login in correct format as specified in Figure 20.

Figure 20: Windows authentication

User Role Information

The user can have one or more roles to access the administration portal. This panel displays all assigned roles of the user and the available roles that can be associated to the user.

Prerequisites:

1. Role should have been created – Refer Role creation for more details





Figure 21: User Role information

A role can be removed from user assigned role list by clicking the (X).

A new role can be assigned to user by clicking the “Add” button after selecting a role from the list of available role as shown in Figure 21.

User Group-Membership Information:

User by default will be linked to a group which is an active group at the time of user creation. This can be edited later by administrator. User will be logged on to the system using any active group that’s linked his user account. If a user is linked to more than one group then the user information will be shared among the linked groups.

A group link can be added by clicking  after selecting it. A user link can be added by clicking  after selecting any linked group. However, a logged in user cannot remove a link from his/her active group. Also a user needs to be linked to at least one group.

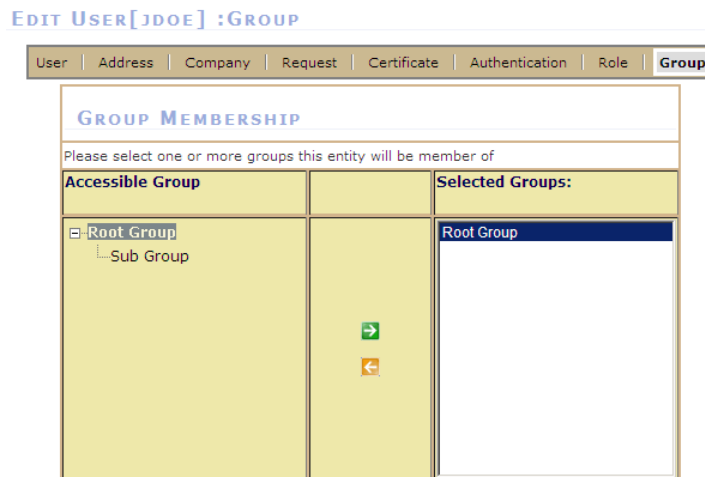


Figure 22: User-Group membership

2.1.2 Company Resource Management Module

The company management page summarize the possible operations can be effected on company resources.

- Browse companies
- View company
- Create company

2.1.2.1 Create new company

The creation of a new company consists of filling the mandatory company information like company name and address information like Address line, City and country.

CREATE NEW COMPANIES

Company | Employees | Dedicated Certification Authority | Group

Company Information

Company Name *

Address

Address Line 1

Address Line 2

Address Line 3

Zip

City

State

Country

Phone

Fax

Processing status

Status

Figure 23: Creation of a new Company

2.1.2.2 Browse Company database

Browse company database page allows viewing all companies linked to the current active group or all companies linked to the current active group and its sub groups based on their status.

LIST OF ALL COMPANIES

Create New Company

View results from all sub groups

10

ID	Name	Status	Display
2	WISeKey SA	Active	<input type="button" value="→"/>
1	WISeKey SA	Active	<input type="button" value="→"/>

Page 1 of 1

Figure 24: Browsing the company database

The company details can be filtered using their statuses as shown in Figure 24 by selecting the available statuses. Paging option is customized to list only “n” number of companies based on the value defined in the page-size textbox.

Company statuses and list of actions that can be taken:

- **All:** display all companies details linked to the active group irrespective of status.
 - No action
- **Active:** display all companies details linked to the active group whose status is approved.
 - Suspend
- **Suspended:** display all companies details linked to the active group whose status is suspended.
 - Approved, Remove

The status of a company can be changed by taking appropriate actions (using the available buttons) after the choosing the checkbox.

2.1.2.3 View Company information

Application tool bar

EDIT COMPANY [WISEKey SA] : BASIC INFORMATION

Company		Employees	Dedicated Certification Authority	Group
Company Information				
Company Name	WISEKey SA			
Address				
Address Line 1	route de Pré-Bois 29			
Address Line 2	P.O. Box 853			
Address Line 3				
Zip	CH-1215			
City	Geneva			
State				
Country	Switzerland			
Phone	+41 22 594 3000			
Fax	+41 22 594 3001			
Processing status				
Status	Active			
<input type="button" value="Edit"/>		<input type="button" value="Suspend"/>		



Figure 25: Company Basic Information (View Mode)

The company related information is regrouped in this page as follows:

- **Company:** company's basic information such name, address and status.
- **Employees:** company's employees' information.
- **Dedicated Certification authority:** company's dedicated certification authorities' information.
- **Group:** Company's group membership information

Company information is accessible through the application tool as shown in Figure 25.

In Edit mode, there are two buttons "Cancel" and "Save". "Cancel" button allows switching to View mode without making any changes to the information in data base and "Save" button allows updating the modified data in to database.

If user deletes the company, he/she has an opportunity for restoring the details. Choosing Remove Company does not provide the option of restoration of details.

Company Employees Information

The company employees' information panel displays the all users associated to this company with their position and their department as shown in Figure 26.

EDIT COMPANY[WISEKEY SA] :EMPLOYEES

Company | **Employees** | Dedicated Certification Authority | Group

Current Company Users

ID	First Name	Last Name	Email	Position	Department
X 2	John	Doe	jdoe@wisekey.com	Manager	Development

Page 1 of 1

User Search Criteria

And [v] Email [v] contains [v] []

And [v] Last Name [v] contains [v] []

And [v] User ID [v] is [v] []

Search



Figure 26: Company Employees Information

A user can be removed from a company by clicking the (X).

A new user can be assigned to company by clicking the “Add user” button after selecting a user from the list of available user as shown in Figure 27.

EDIT COMPANY[WISEKEY SA] :EMPLOYEES

Company | **Employees** | Dedicated Certification Authority | Group

Current Company Users

ID	First Name	Last Name	Email	Position	Department
X 2	John	Doe	jdoe@wisekey.com	Manager	Development

Page 1 of 1

User Search Criteria

And [v] First Name [v] contains [v] W []

And [v] Last Name [v] contains [v] []

And [v] User ID [v] is [v] []

Search

ID	First Name	Last Name	Email	Position	Department	
1	Wisekey	Administrator	admin@wisekey.com			Add User



Figure 27: Add a user as company employees

Company Dedicated Certification Authorities

The company may or may not dedicated certificate authorities. This panel displays all dedicated certificate authorities of the company.

Prerequisites:

1. Certification Authority(CA) should have been created – Refer CA creation for more details

EDIT COMPANY[WISEKEY SA] :DEDICATED CERTIFICATION AUTHORITY

Company | Employees | **Dedicated Certification Authority** | Group

Add/ Remove a certification authority dedicated to this company.

Current certification authorities dedicated to company

Please select a dedicated certification authority for this company

Certification Authority	Root CA
Description	
Add	



Figure 28: Company dedicated Certification Authorities

An existing certification authority can be removed from the company by clicking the (X).

A new certificate authority can be dedicated to this company by clicking the “Add” button after selecting a certification authority from the list and filling the description as shown in Figure 28.

Company Group-Membership Information

Company by default will be linked to a group which is an active group at the time of company creation. This can be edited later by the administrator. If a company is linked to more than one group then the company information will be shared among the linked groups.

A link can be added by clicking “➔”, after selecting any available group. The company group link can be removed by clicking “➡” after selecting any linked group. Any company needs to be linked to at least one group.

EDIT COMPANY[WISEKEY SA] :GROUP

Company | Employees | Dedicated Certification Authority | **Group**

GROUP MEMBERSHIP

Please select one or more groups this entity will be member of

Accessible Group		Selected Groups:
<ul style="list-style-type: none"> [-] Root Group <ul style="list-style-type: none"> [-] Sub Group 	<p>➔</p> <p>➡</p>	<ul style="list-style-type: none"> Root Group



Figure 29: Company-Group membership

Security Management Module

The security management module has following resource modules:

- Group Resource module
- Role Resource module
- Operation Resource module
- Access Control List Resource module

- Log Resource module

Main Functionalities of Security Entity management:

- Create and edit groups, link groups to resource
- Create and edit user roles, assign users to roles, target roles to groups
- Define role ACLs

2.1.3 Log Management Module

The log management helps in tracking the operations performed on resources.

2.1.3.1 Search Log Message

User can locate a log message by specifying any of the details or by providing all the details.

1. Resource type
2. Operation type
3. Start Date
4. End Date

Figure 46: Search Log Message

2.1.3.2 Browse Log Message database

Browse log message page display the all log message, using the navigation bar a specific log message list can be reached easily. Paging option is customized to list only “n” number of log message based on the value defined in the page-size textbox

LIST OF ALL LOG MESSAGES

Search Log Message

View results from all sub groups

10 Set page size

ID	Resource Type	Operation Type	Operator ID	Resource ID	Log Date	Display
728	Operation	List	1		4/3/2008 2:56:46 PM	→
727	Operation	Modify	1	401	4/3/2008 2:52:58 PM	→
726	Operation	View	1	401	4/3/2008 2:51:07 PM	→
725	Operation	List	1		4/3/2008 2:51:03 PM	→
724	Operation	List	1		4/3/2008 2:51:00 PM	→
723	Operation	List	1		4/3/2008 2:49:54 PM	→
722	Role	List	1		4/3/2008 2:49:42 PM	→
721	Role	List	1		4/3/2008 2:49:41 PM	→
720	Group	List	1		4/3/2008 2:49:39 PM	→
719	Group	View	1	1	4/3/2008 2:49:36 PM	→

Page 1 of 63
|< >|

Figure 47: Browsing the log message database

PKI Management Module

The PKI management module has following resource modules:

- Certification Authority Resource module
- Certificate Template Resource module
- Request Resource module
- Certificate Resource module

Main Functionalities of PKI management

- Add, manage, and edit certification authorities.
- Define, create, or modify certificate templates.
- Browse for pending, approved, deferred, denied, submitted, or rejected certificate request.
- Browse the certificates database by certificate status i.e. issued, revoked, suspended or all.

2.1.4 Request Management Module

The Request management page summarize the possible operations can be effected on Request resource.

2.1.4.1 Search Request Database

The search user page part of PKI management page helps in searching existing certificate request belongs to logged on user.

The search form fetches certificate request based on the search filters available for certificate filters. The following are the filters available for request search

1. Request ID
2. Request DN
3. Country
4. Organization
5. Organization Unit
6. Common Name
7. Email

Once the search button is hit, the result will be display as shown in Figure 64.

<input checked="" type="checkbox"/> Show activated users' Requests only	<input checked="" type="checkbox"/> View results from all sub groups	Request ID	5	Search									
<table border="1"> <tr> <td>All</td> <td>Active</td> <td>Suspended</td> <td>Marked for submission</td> <td>Submitted to CA</td> <td>Failed</td> <td>Denied</td> <td>Issued</td> <td>Failed</td> </tr> </table>					All	Active	Suspended	Marked for submission	Submitted to CA	Failed	Denied	Issued	Failed
All	Active	Suspended	Marked for submission	Submitted to CA	Failed	Denied	Issued	Failed					
ID	Request DN	Submitted	Resolution	Status	Valid	Display							
5	CommonName=John Smith EMail=jsmith@wisekey.com	Thu, 11 Sep 2008 10:49:39 GMT		Active	Yes								

Page 1 of 1

Figure 64: search Request

The filtered request details can be viewed by clicking the “” from the results

2.1.4.2 Browse request database

Browse request database page allows viewing all request belongs to logged on user based on their status and updating the request status using the button available at bottom of the page.

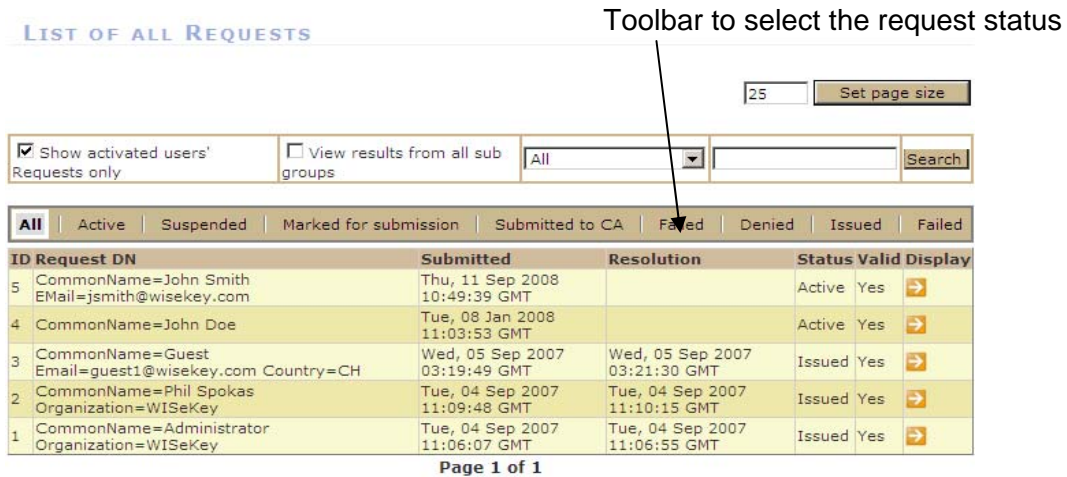


Figure 65: Browsing the request database

The request status can be selected using the toolbar, as shown in Figure 65. In order to navigate easily the request list were displayed using the paging. The following request statuses are used to display the user's certificate

Request statuses and list of actions that can be taken:

- **All:** display all request details of logged on user.
 - No action
- **Suspended:** display all request details of logged on user whose status is suspended.
 - Approve, Remove
- **Denied:** display all request details of logged on user whose status is revoked.
 - Remove
- **Marked For Submission:** display all request details which are awaiting active CA for submission of logged on user.
 - Submit, Suspend, Deny
- **Submitted To CA:** display all request details which is submitted to CA and the CA whose policy is configured to issue certificate after administrator approval of logged on user.
 - Submit
- **Issued:** display all request details of logged on user for those certificate is issued by CA server. No action can be performed on Issued requests.
- **Failed:** display all request details of all of logged on user for those certificate issuance is failed by CA server.
 - Remove

The status of request can be changed by taking appropriate actions (using the available buttons) after the choosing the checkbox.

Request issued/failed is the last stage in certificate request processes.

2.1.4.3 View Request information

The request related information is regrouped in this page as follows:

- **Request Details:** Request details like RequestID, Request Type, flag,
- **Request Subject information:** Display the subjects information
- **Request Subject Alternative Name:** Display the subject alternative name information.
- **Request Attribute information:** Displays the request attribute information.
- **Parsed Request** Allows to display the ASN1 parsed result.
- **Base 64 Request:** display the base 64 request.
- **Issue the Certificate Request**

Request Details

Remote Host IP in request details page gives the IP address of the user who generated the CSR. Contract details would be available only if the template uses contract.

Request Details	
Request ID	5
Request Type	PKCS 10 request
Request Flag	NORMAL REQUEST
Request Disposition	Active
Submit Date	Thu, 11 Sep 2008 10:49:39 GMT
Resolution Date	
Certificate Template	Browser Client
CSP	Microsoft Enhanced Cryptographic Provider v1.0
Require x approvals	1
Missing Approvals	1
Remote Host IP	127.0.0.1
User ID	3
Contract	contracttemplate.rtf <input type="button" value="Contract"/>

Figure 66.1: request details (View Mode)

Request Subject/Subject Alternative Name information

Request Subject Information	
Identifier	Value
Common Name	= John Smith

Subject Alternative Information	
Identifier	Value
User Principal Name (UPN)	= john.smith@contoso.com

Figure 66.2: Request Subject Information

Request Attribute Information

Request Attribute Information	
Key Usage (Critical)	
Digital Signature	
Non-Repudiation	
Key Encipherment	
Data Encipherment	
Extended Key Usage (Not Critical)	
Client Authentication	
Identifier	Value
SMIME	= No
PKCS10KeyOnly	= Yes

Figure 66.3: Request Subject Information

Parsed Request

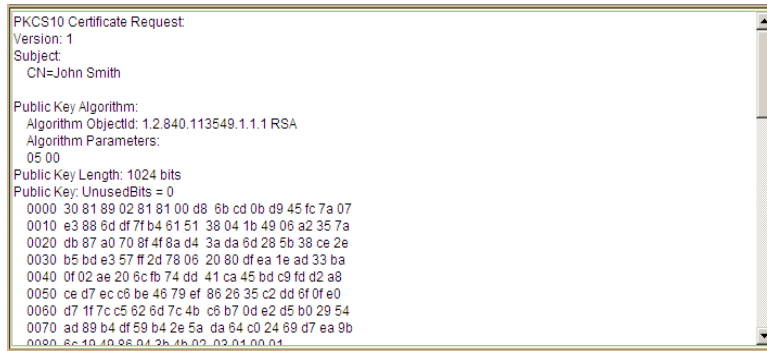


Figure 66.4: ASN1 parsed request

Base 64 Request

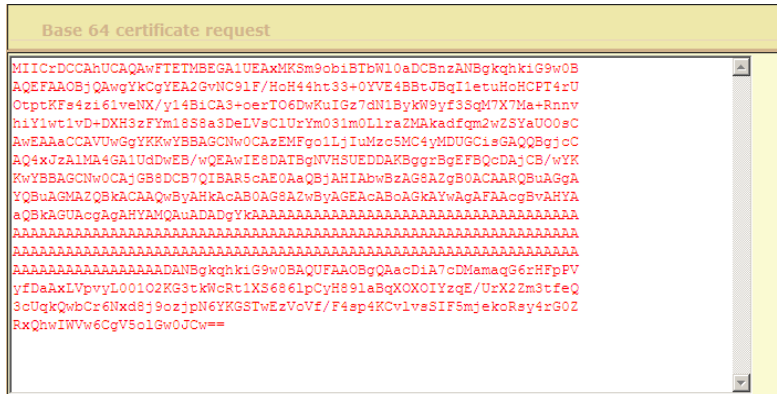


Figure 66.5: Base 64 Request

Issue Certificate Request

When certificate request is approved, then issuing certificate request panel appears as shown in Figure 66.6. After selecting a certification authority and then by submitting request using the “Submit” button, the certificate will be issued. On the last approval (which is configured in template to have one or more approvals) when the CA is active and the CA server is configured to issue certificate automatically the certificate will be issued by the CA server.



Figure 66.6: Issuing a certificate request panel

2.1.5 Certificate Management Module

The Certificate management page summarizes the possible operations that can be effected on certificate resource.

2.1.5.1 Search Certificate Database

The search certificate page part of PKI management page helps in searching existing certificate belongs to logged in user

The search form fetches certificate request based on the search filters available for certificate filters. The following are the filters available for request search

1. Certificate ID
2. Request ID
3. Country
4. Organization
5. Organization Unit
6. Common Name
7. Title

8. First Name
9. Last Name
10. Domain Component
11. Email
12. Serial Number

LIST OF ALL CERTIFICATES

25 Set page size

Show activated users' Certificates only
 View results from all sub groups

Certificate ID
3
Search

All |
 Active |
 Suspended |
 Revoked

ID	Request ID	Subject	Effective	Expiration	Serial Number	Status	Display
3	3	CommonName=John Doe Organization=WISeKey	Wed, 05 Sep 2007 10:10:58 GMT	Fri, 05 Sep 2008 10:20:58 GMT	617F71AB000000000000C	Active	➔

Page 1 of 1

Figure 67: search certificate

The filtered certificate details can be viewed by clicking the “➔” from the results

2.1.5.2 Browse certificate database

Browse certificate database page allows viewing all certificates belongs to logged on user based on their status and updating the certificates status using the button available at bottom of the page.

LIST OF ALL CERTIFICATES

25 Set page size

Show activated users' Certificates only
 View results from all sub groups

All

Search

All |
 Active |
 Suspended |
 Revoked

ID	Request ID	Subject	Effective	Expiration	Serial Number	Status	Display
3	3	CommonName=John Doe Organization=WISeKey	Wed, 05 Sep 2007 10:10:58 GMT	Fri, 05 Sep 2008 10:20:58 GMT	617F71AB000000000000C	Active	➔
2	2	CommonName=Phil Spokas Organization=WiseKey	Tue, 04 Sep 2007 18:00:15 GMT	Thu, 04 Sep 2008 18:10:15 GMT	6137F6F70000000000006	Active	➔
1	1	CommonName=Administrator Organization=WISeKey	Tue, 04 Sep 2007 17:56:54 GMT	Thu, 04 Sep 2008 18:06:54 GMT	6134E8400000000000005	Revoked	➔

Page 1 of 1

Figure 68: Browsing the certificate database

The certificate status can be selected using the toolbar, as shown in Figure 68. In order to navigate easily the certificate list were displayed using the paging. The following certificate statuses are used to display the user's request database

Certificate statuses and list of actions that can be taken:

- **All:** display all certificate details of logged in user irrespective of status.
 - No action
- **Activated:** display all certificate details of logged in user whose status is active.
 - Suspend, Revoke
- **Suspended:** display all certificate details of logged in user whose status is suspended.

- Approve, Remove, Revoke
- **Revoked:** display all certificate details of logged in user whose status is revoked.
 - Remove

Revoking a Certificate:

When you revoke a certificate the certificate will be revoked from CA server and which could not be activated later. While revoking a certificate you should provide the reason and comment for revocation. Revocation wo not delete the certificate details from database.

The screenshot shows a web browser window titled "CertifyID Registered User Site -- Webpage Dialog". It contains a form with a "Revocation Reason" dropdown menu currently set to "Unspecified". Below this is a large, empty text area labeled "Revocation Comment". At the bottom of the form is a "Submit" button.

Figure 69: Revoking certificate

Removing certificate:

When you remove a certificate the certificate will be revoked from CA server and which cannot be activated later. While removing a certificate you should provide the reason for revocation. Remove delete the certificate and associated resources from database. Removing a revoked certificate will not pop-up the revocation reason which uses the earlier reason of revocation.

The screenshot shows a web browser window titled "CertifyID RA -- Webpage Dialog". It displays a warning message: "This action will definitely remove the certificate from the database and revoke it. Please choose a revocation reason". Below the message is a "Revocation Reason" dropdown menu set to "Unspecified". At the bottom is a "Submit" button.

Figure 70: Removing certificate

2.1.5.3 View Certificate information

The request related information is regrouped in this page as follows:

- **Identifying Information:** Certificate ID, Request ID and status.
- **Certificate details:** Display the issuer, serial number, issued date, expiring date and certificate template.
- **Parsed Certificate Information:** Allows to display the ASN1 parsed result of certificate.
- **Install:** allows installing the certificate in client machine.
- **Download:** allows downloading the certificate in Base 64 or Binary format.
- **Renew Certificate:** renew certificate allows user to renew an existing certificate which may be revoked/suspended/expired/active.

CERTIFICATE DETAILS	
Identifying Information	
Certificate ID	4
Request ID	5 <input type="button" value="Request details"/>
Status	Active
Certificate Details	
Issuer	CN=egl-Kaladhar-3134, DC=data, DC=net
Serial Number	1195776000000000024F
Valid From	Fri, 12 Sep 2008 06:36:03 GMT
Valid Until	Sat, 12 Sep 2009 06:36:03 GMT
Certificate Template	Browser Client
Certificate Subject Information	
Identifier	Value
Common Name	= Wisekey Administrator
Organization	= WISEKey
Email	= admin@wisekey.com
Subject Alternative Information	
Identifier	Value
Email	= admin@wisekey.com
Detailed content of the certificate	
<input type="button" value="Display"/>	
<input type="button" value="Install"/> <input type="button" value="Suspend"/> <input type="button" value="Revoke"/>	
<input type="button" value="Download"/> Base-64 encoded X.509(.CER) <input type="button" value="v"/>	
<input type="button" value="Renew Certificate"/>	

Figure 71: Certificate Details Information

Certificate Details

The certificate details page allows user to view the certificate details, status and download or install the certificate as shown in Figure 71.

CERTIFICATE DETAILS	
Identifying Information	
Certificate ID	4
Request ID	5 <input type="button" value="Request details"/>
Status	Active
Certificate Details	
Issuer	CN=egl-Kaladhar-3134, DC=data, DC=net
Serial Number	1195776000000000024F
Valid From	Fri, 12 Sep 2008 06:36:03 GMT
Valid Until	Sat, 12 Sep 2009 06:36:03 GMT
Certificate Template	Browser Client

Figure 71.1: Certificate details (View Mode)

Certificate Subject/Subject Alternative Information

Certificate Subject Information	
Identifier	Value
Common Name	= Wisekey Administrator
Organization	= WISEKey
Email	= admin@wisekey.com
Subject Alternative Information	
Identifier	Value
Email	= admin@wisekey.com

Figure 71.2: Certificate Subject Information

Parsed Certificate

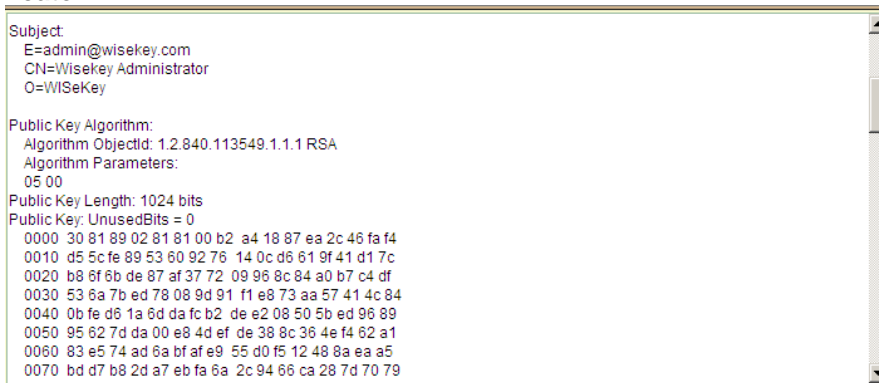


Figure 71.3: ASN1 parsed certificate

Install:

The install button will redirect to another page, during the install a security alert will be displayed as shown in the Figure below: This will install the certificate in client machine.

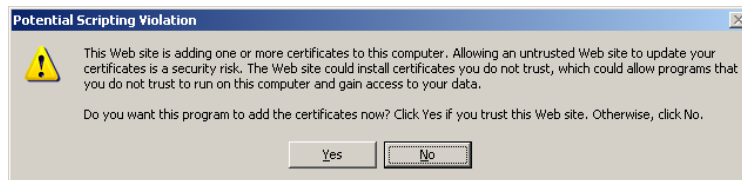


Figure 71.4: Security Alert during certification installation

Download:

Certificate for the moment can be downloaded in following format:

- base 64 encoded certificate
- binary encoded certificate

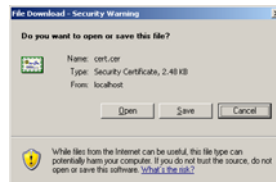


Figure 71.5 Download Certificate

User and Admin Notifications:

Notification details associated to operations and events is defined in database table notification. It can be configured to enable/disable notifications to users and administrators.

URA is having two types of Administrators

1. Host Administrator – Administrator for the site. Host Administrator’s email id is configured in registry using the key OperatorNotificationEmail under HKLM\SOFTWARE\WISEKEY\CID\Admin
2. Group Administrator – Administrator for a group. Group administrators email addresses were configured in the group’s notification list. It’s recommended to configure one or several group administrators for all your groups

Host Admin Notifications:

Host Admin notifications can be enabled/disabled using the flag “IsHostAdminNotify”

Group Admin Notifications:

Group Admin notification can be enabled/disabled using the flag "IsGroupAdminNotify". If a Group Administrator is an existing URA user then group administrator would be notified in his/her preferred language.

User Notifications:

User Notifications can be enabled/disabled using the flag "IsUserNotify". Users will be notified in their preferred language which is set during user creation/user update.

The following table gives NotificationID details for different event/operation.

Notification ID	Operation/Event Description	User may be notified
1	When a Request is Generated	X
2	When a Request is Denied	X
3	When a Certificate is Created	X
4	When a Certificate is Approved	X
5	When a Certificate is Suspended	X
6	When a Certificate is Revoked	X
7	When a Role is Created	
8	When a Role is Approved	
9	When a Role is Suspended	
11	When a Role is Removed	
12	When a User is Created	X
13	When a User is Approved	X
14	When a User is Suspended	X
16	When a User is Removed	X
17	When a Group is Created	
18	When a Group is Approved	
19	When a Group is Suspended	
21	When a Group is Removed	
22	When a Company is Created	
23	When a Company is Approved	
24	When a Company is Suspended	
26	When a Company is Removed	
27	When a CA is Created	
28	When a CA is Approved	
29	When a CA is Suspended	
31	When a CA is Removed	
32	When a Certificate Template is Created	
33	When a Certificate Template is Approved	
34	When a Certificate Template is Suspended	
36	When a Certificate Template is Removed	
37	When a Request is Removed	X
38	When a Certificate is Removed	X
100	When a Certificate is Installed	X
101	When a Certificate is Downloaded	X
102	When a Certificate is Expired	X
103	When a Group's user/certificate limit is reached	
104	When a Group is nearing user/certificate limit	
105	When a group's validity date is reached	

106	When a group is nearing its validity date	
-----	---	--

NOTE:

1. When a user has to be notified about any event/operation then user details should contains user's email address.
2. When a Host Administrator has to be notified about any event/operation then registry key "OperatorNotificationEmail" should be configured with host administrator's email ID under HKLM\SOFTWARE\WISKEY\CID\Admin.
3. When a Group Administrator has to be notified then group needs to be configured with one or more valid email IDs.