Title:

2X Digi-Sign
ARP Instructions

Document Type: Digi-Sign Affiliate, Reseller & Partner [ARP] Network
Reviewed: Marketing Department
FileTracker: M:\ARP\ARP Program\ARP Program Overview
Copyright: Copyright © 2010, Digi-Sign, The Certificate Corporation

Table of Contents

 © Digi-Sign, The Certificate Corportation, Copyright 2010

Introduction

Your customers are using Secure Socket Layer [SSL] certificates for secure connections to the login page. They're also entering usernames and passwords over this secure connection (that uses the https:// protocol), to gain access to the system. So every system requires an SSL certificate.

Username and password (something the user knows) access is not considered to be secure. It is too easy to copy, share, steal and/or compromise. Two factor authentication (something you know combined with something you have) is considered secure. And with each user possessing a Digi-Access™ certificate, your customers' security can be significantly improved.

In co-operation with 2X, Digi-Sign has two solutions that address your needs, and those of you customers, with ease. Namely:

- Digi-SSL™ Service – for issuing and managing SSL certificates
- Digi-Access™ Service – for two factor authentication

As a 2X Partner, your company is already an approved member of the Digi-Sign ARP Network where these two specialised systems have been customised for your customers. In reading this manual you will learn:

- How to get your own Digi-SSL™ Service system
- How to implement Digi-Access for your customers
- How billing, invoicing and commission rebates work
- How to access the ARP Extranet & the benefits to your organisation

The remainder of this document covers all aspects of the 2X Digi-Sign programme and includes all the necessary information you need including:

- Product Offerings
- Sales Information
- Technical Instructions
- Billing & Accounting

Any enquiries about this document and other requests for any other information should be directed to the distributor or country agent for 2X.

© Digi-Sign, The Certificate Corportation, Copyright 2010

1 Digi-SSL Service™

Let's start with the simplest of requirements: SSL. Whether you have 5 or 5,000 2X systems in operation, every year you need to issue a new SSL certificate in order to maintain the system's security. So how do you:

- Remember when each SSL certificate needs to be replaced?
- Place orders quickly and easily and get your SSL order completed?
- Ensure that you bill each customer for their SSL?

The answer is simple: you use the Digi-SSL™ Service system to do all of this for you.

1.1 How to get your Digi-SSL™ Service system

All 2X Partners are already approved members of the Digi-Sign ARP Network, so there's no paperwork, credit check or contract to sign. So to activate your Digi-SSL™ Service system, all you need to do is order your system online using this URL:

https://www.digi-sign.com/order/arp/digi-ssl/

The order will be completed within 48 hours and with this powerful system you can order and manage your SSL certificates with ease.

1.2 Digi-SSL™ certificate prices

2X has negotiated the following retail prices for Digi-SSL™ certificates. Your 2X Partner discount applies to these retail prices (see sub section 6.1 for commission rebates):

2X Digi-SSL™ Xs	Disc.	Unit Cost	Total
1		€ 177.--	€ 177.--
2	5%	€ 167.--	€ 334.--
3	5%	€ 157.--	€ 471.--
4+	P.O.A. Contact Digi-Sign Sales		

Standard SSL certificate

2X Digi-SSL™ Xg	Disc.	Unit Cost	Total
1		€ 467.--	€ 467.--
2	5%	€ 447.--	€ 894.--
3	5%	€ 437.--	€ 1,311.--
4+	P.O.A. Contact Digi-Sign Sales		

SAN, Unified Communications or Wildcard SSL certificate

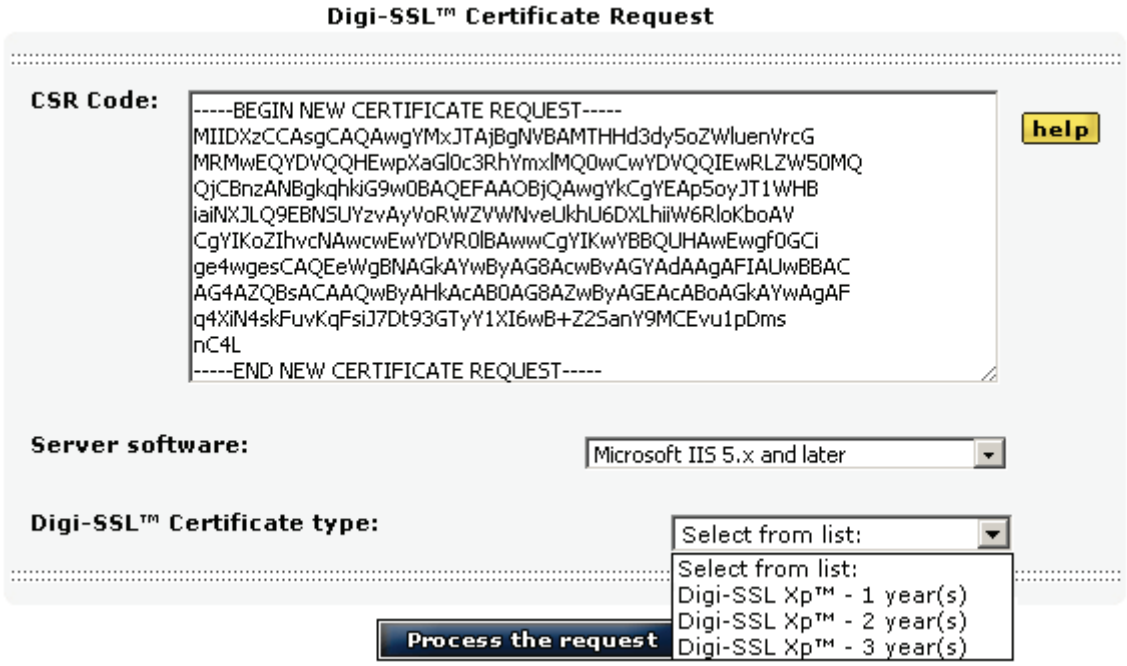
1.3 How to get your Digi-SSL™ certificates

1. Generate the Certificate Signing Request [CSR] on the 2X IIS Server. For instructions on how to generate the CSR, use the online support page using this URL:

© Digi-Sign, The Certificate Corportation, Copyright 2010

http://www.digi-sign.com/support/digi-ssl/microsoft-iis56

2. Login in to your 2X Digi-SSL™ Service system and paste the CSR into the field on this form, then select 'Microsoft IIS5.x and later' and choose either 1, 2 or 3 year(s) before using the 'Process the Request' button.



3. After a few minutes, the new Digi-SSL™ certificate will be emailed to you, ready for installation on the 2X server. For instructions on how to install the certificate, use the online support page using this URL:

http://www.digi-sign.com/support/digi-ssl/install-certificate/microsoft-iis56

© Digi-Sign, The Certificate Corportation, Copyright 2010

2 Digi-Access™ two factor authentication

The incentive for using two factor authentication is underpinned by the extensive media coverage on matters relating to online security. Username and password access can no longer be considered as adequate security. As stated, it is too easy to copy, share, steal and/or compromise.

The two factor authentication offered by Digi-Access™ increases your customers' security and reflects well on your organisation as one the takes security seriously. Certificates expire annually (if they are not revoked by the customer in the interim) and must be renewed.

To implement Digi-Access™ for your customer, you must follow these steps exactly as documented below:

2.1 Gain access to the ARP Extranet
2.3 Order the Digi-Access™ system for your customer
3 Install the Error 403 pages on the IIS server
4 Configure the 2X server
5 Issue Digi-Access™ certificates to the end users
16 Issue your commission rebate invoice

2.1 How to access the ARP Extranet

If you have already completed Section 1 above, then go to sub section 2.2.1 below.

All 2X Partners are already approved members of the Digi-Sign ARP Network, so there's no paperwork, credit check or contract to sign. The ARP Network is managed through an Extranet and to gain access to the ARP Extranet, you must have a Digi-Access™ certificate. You will need to request your own personal Digi-Access™ certificate by:

http://www.digi-sign.com/arp/2x/complete+program#join

The order will be completed within 48 hours and you are notified by email to activate your Digi-Access™ certificate before logging into the ARP Extranet.

2.2 Digi-Access™ certificate prices

2X Digi-Access™ Users	Disc.	Unit Cost	Total
1		€ 27.00	€ 27.--
10	5%	€ 25.65	€ 257.--
25	5%	€ 24.37	€ 609.--
50	5%	€ 23.15	€ 1,157.--
100	5%	€ 21.99	€ 2,199.--
250	5%	€ 20.89	€ 5,223.--
500	5%	€ 19.85	€ 9,924.--
1,000	5%	€ 18.86	€ 18,885.--
2,500	5%	€ 17.91	€ 44,781.--

© Digi-Sign, The Certificate Corportation, Copyright 2010

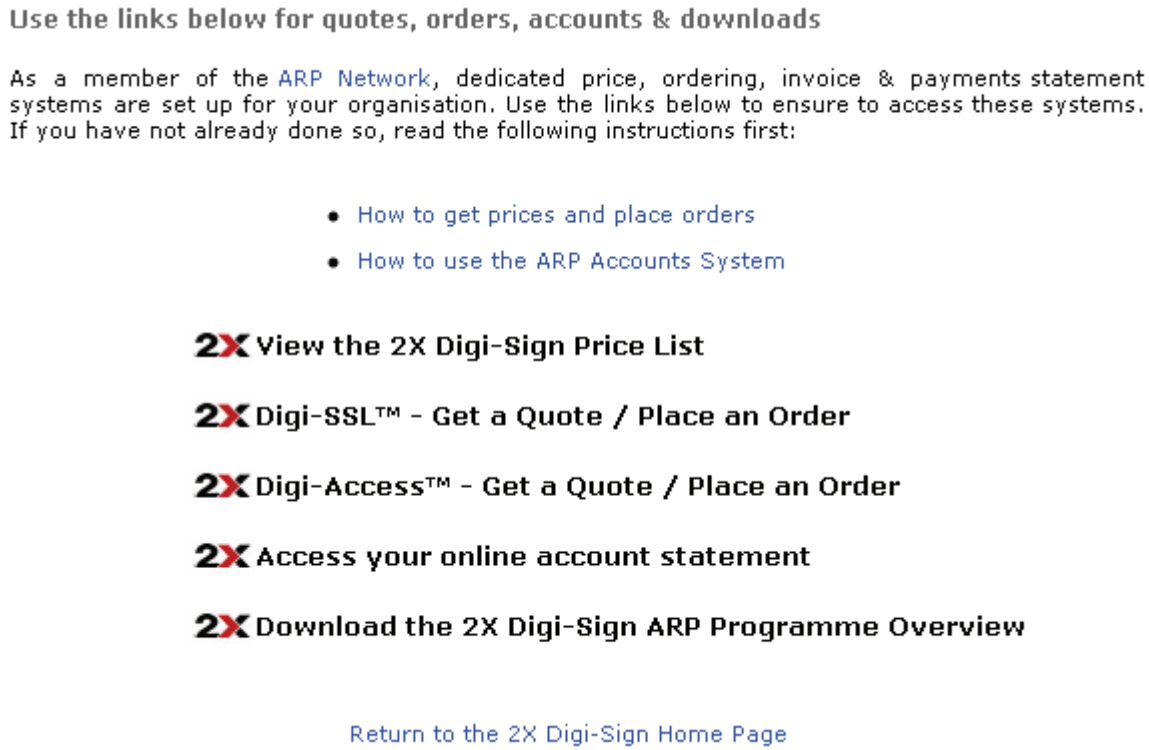
5,000	5%	€ 17.02	€ 85,084.--
10,000	5%	€ 16.17	€ 161,659.--
10,000+	P.O.A. Contact Digi-Sign Sales		

2.2.1 Logging into the ARP Extranet

The ARP Extranet is located at this URL:

https://arp.digi-sign.com/2x/

Once you are logged in you will see the following service links:



2.3 How to order a Digi-Access™ system

If you have not already done so, complete sub section 2.1 before proceeding further. The dedicated quotations and ordering system is set up for use by all 2X Partners. Read the sections below to ensure that you get the right price and to ensure that your orders are processed without delay:

2.3.1 Step-by-step ordering instructions

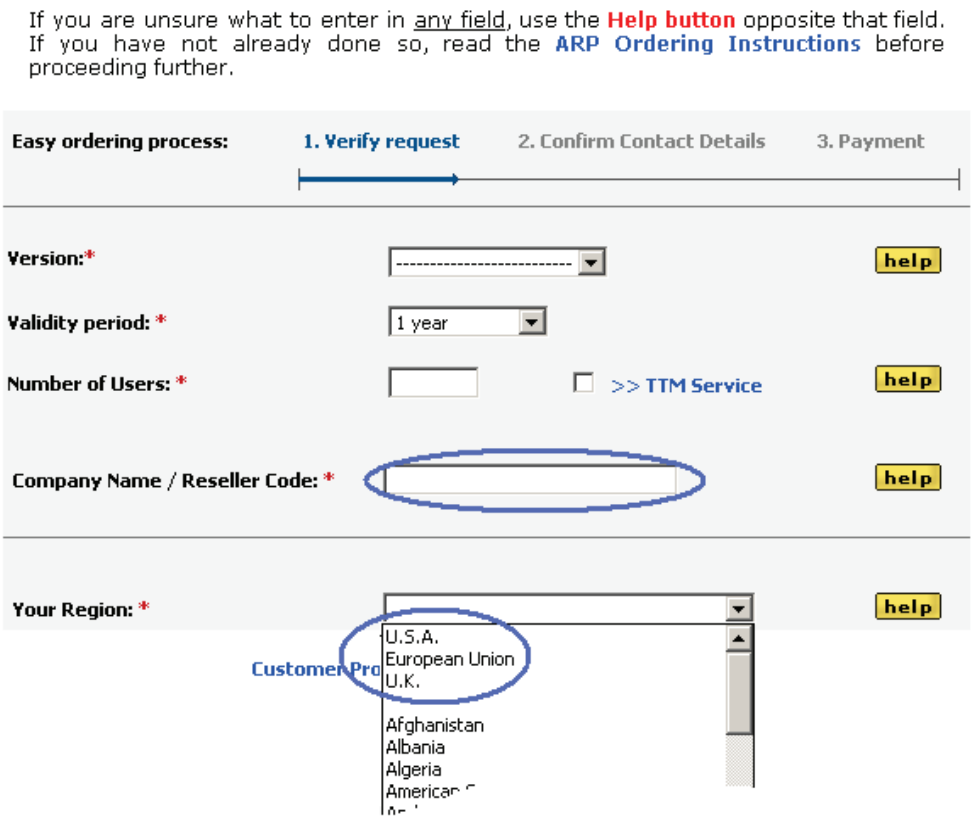
2.3.1.1	*Every field must be completed correctly*	The ordering system information must be completed correctly because this information is used to technically configure the system you are ordering. In particular, you should understand the difference between you, the person placing the order and

 © Digi-Sign, The Certificate Corportation, Copyright 2010

your customer, for whom the system will be activated

2.3.1.2 *Name/Code &* ***Region***

On this first page of the ordering form, all fields have a Help button to assist you in completing this form correctly. Pay careful attention to the 'Company Name / Reseller Code:' (credits you for the sale) and 'Your Region:' (**dictates the currency of invoices and payments**) fields



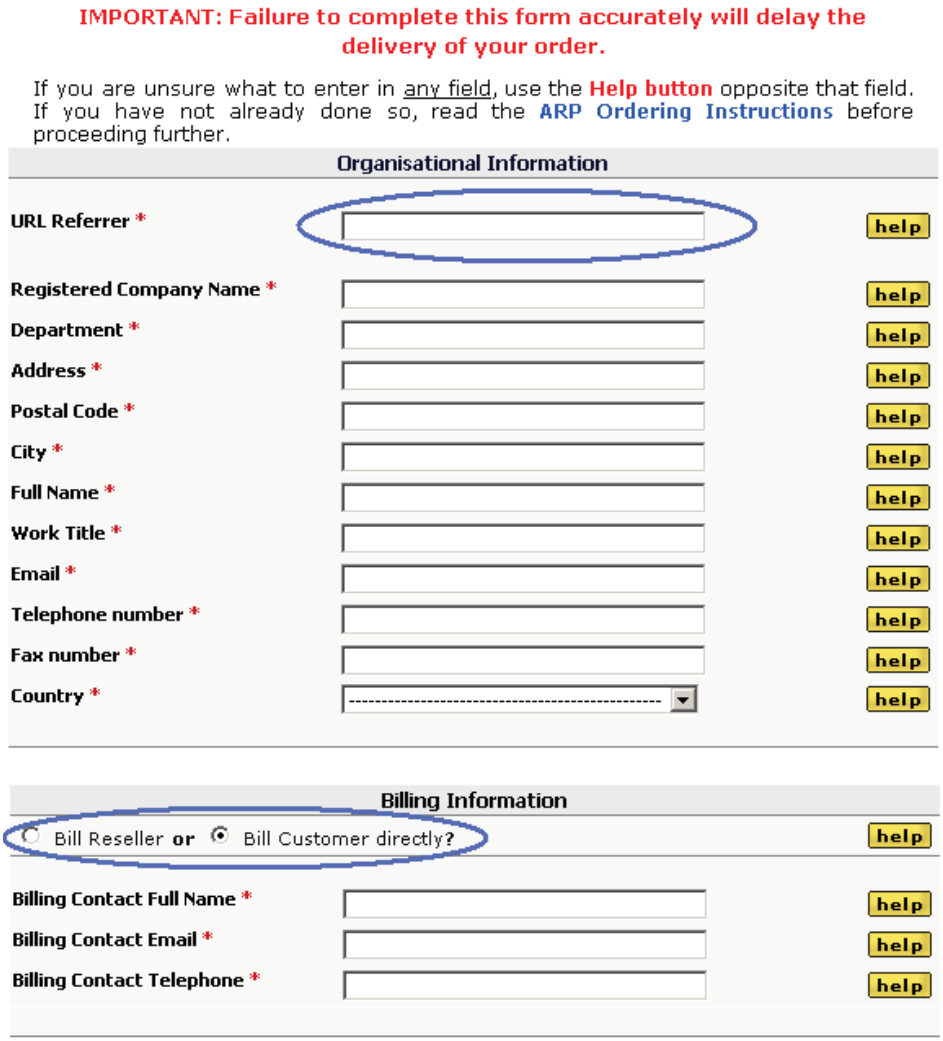
2.3.1.3 *Confirm Order*

After the above form is submitted, the cost of the order is displayed. This is the **customer's purchase price** and should not be confused with the price that you will pay as the 2X Partner. Your discount is subtracted from this price

2.3.1.4 *Order Details*

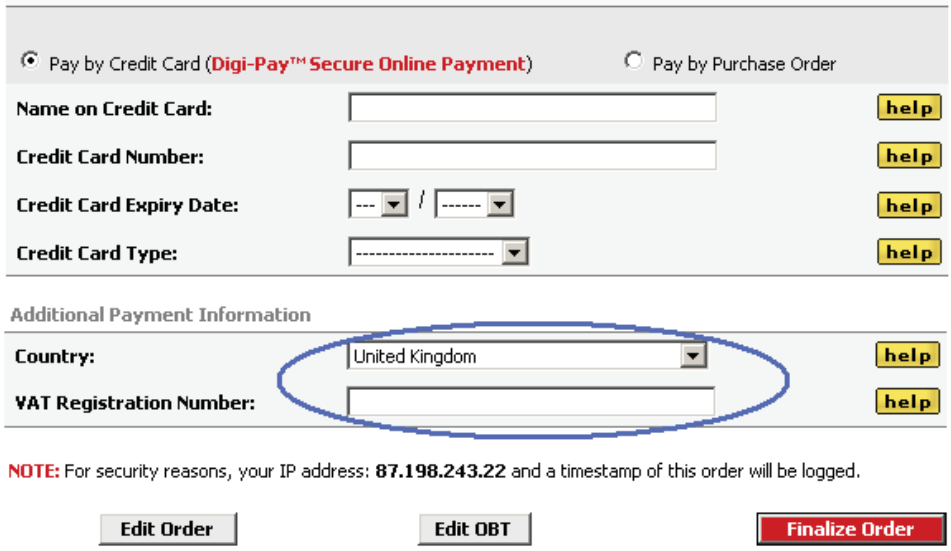
The information on this form is very important both technically and commercially, so complete this form carefully. Pay careful attention to the 'URL Referrer' (specific technical information) and 'Billing Information' (dictates the details of the invoice that will be issued) fields

© Digi-Sign, The Certificate Corportation, Copyright 2010



2.3.1.5 *Payment method to complete*

The information on this form is important both commercially and for tax reasons. Pay careful attention to the 'Country' (tax information that dictates whether the invoice will have sales tax/VAT applied) field



© Digi-Sign, The Certificate Corportation, Copyright 2010

3 Installing the Error 403 Pages

The 2X Application Server runs on a Microsoft® IIS server where there are specific default error pages designed to work with Digi-Access™ certificates. To enhance the user experience you should replace these default error pages with the customised Digi-Access™ error 403 pages.

The default 403 error pages that relate to the use of Digi-Access™ are stored in the C:\WINDOWS\help\iisHelp\common\ folder. The 2X Application Server Administrator should download the Digi-Access™ error 403 pages using this URL:

https://www.digi-sign.com/downloads/download.php?id=digi-access-403

Place the pages in the downloaded .ZIP in a new folder, for example:

C:\WINDOWS\help\iisHelp\digi-access\

Test that the server is correctly configured to display these new error pages before restarting the server to complete the setup procedure.

© Digi-Sign, The Certificate Corportation, Copyright 2010

4 Configure the 2X server

For every 2X Digi-Access™ customer, a unique Digi-Access™ Registration Authority [RA] is activated so that the customer can manage the end users Digi-Access™ certificates. Once the order (see sub section 2.3) for your customer has been approved, the Digi-Access™ RA is activated and you are notified automatically.

Enabling Digi-Access™ client certificates for two factor authentication will take 30 minutes (or less) following these simple steps:

1. Download and save these two certificates:

    a. Digi-Sign Root CA
    b. Digi-Sign CA Digi-Access™ Xs

    Using this URL:

    https://www.digi-sign.com/downloads/download.php?id=digi-access-cas

2. On the server, click the Start button, select Run and type MMC, before clicking the 'OK' button.

3. You should now be in the Microsoft Management Console and should follow these steps:

    a. Click File and select Add/Remove Snap-in

    b. Select Add, select Certificates from the Add Standalone Snap-in box and click Add

    c. Select Computer Account, then Local Computer and click Finish

    d. Close the Add Standalone Snap-in box and click OK in the Add/Remove Snap-in

    e. Return to the Microsoft Management Console

4. Now all you need to do is import the Digi-Access™ Root certificate, following these steps:

    a. Right click the Trusted Root Certification Authorities, select All Tasks, and then select Import

    b. After clicking Next > you should browse to the Digi-Sign Root CA

© Digi-Sign, The Certificate Corportation, Copyright 2010

c. Ensure that the Digi-Sign Root CA certificate appears under Trusted Root Certification Authorities

d. Then click Next > and then Finish

5. Then import the Digi-Access™ intermediate CA certificate, as follows:

   a. Right click the Intermediate Certification Authorities, select All Tasks, and then select Import

   b. After clicking Next > you should browse to the Digi-Sign CA Digi-Access Xs

   c. Ensure that the Digi-Sign CA Digi-Access Xs appears under Intermediate Certification Authorities

   d. Then click Next > and then Finish

   e. Restart the IISAdmin service, or reboot the computer to complete the installation

6. Go to Windows Administrative Tools and open the properties window for the website that you have enabled SSL on. Open the Directory Security by right clicking on the Directory Security tab and then follow these steps:

   a. Click Edit in the Anonymous access and authentication control section. The Authentication Methods window will appear

   b. Make sure that all options (check boxes) in this section are disabled, including the Anonymous Access, Basic Authentication, Digest Authentication and Integrated Windows Authentication

   c. Click OK to apply changes

   d. Click Edit in Secure communications section and the Secure Communications window will appear

   e. Ensure that both the 'Require secure channel (SSL)' option and the 'Require 128-bit encryption' option are enabled

   f. Then ensure that the 'Enable client certificate mapping' option is enabled and that the 'Ensure that Enable certificate trust list' option is enabled

   g. Move to the 'Under Current CTL' and click New, followed by Next > and a Certificate Trust List Wizard window will appear

© Digi-Sign, The Certificate Corportation, Copyright 2010

h. Browse for the Digi-Sign_Root_CA.cer Certificate file and click Open, followed by Next>

i. In the Friendly Name field enter: Digi-Access

j. In the Description field enter: Digi-Access Two Factor Client Authentication

k. Click Next > and then Finish

l. You should now see your Certificate Trust List [CTL] List on the Secure Communications window

m. Click OK and then OK again

7. Start Internet Services Manager, or open the MMC that contains the IIS snap-in.

a. Right-click the Web site for which you want to configure authentication (for example, Default Web Site), and then click Properties

b. Click the Directory Security tab, and then under Secure communications, click Edit

c. Click to select the Enable client certificate mapping check box, and then click Edit

d. Click the Many-to-1 tab, and then click Add

e. In the General dialog box, type 'Digi-Access' as the name for the rule, and then Next

f. In the Rules dialog box, click New

g. In the Edit Rule Element dialog box that appears, configure the settings that you want for the rule

h. There are two fields from client certificates that can be used as criteria for many-to-one rules:

- * Issuer - This field specifies information about the Certification Authority [CA] that issued the Digi-Access™ certificate

- * Subject - This field specifies information about the entity to whom the Digi-Access™ certificate was issued

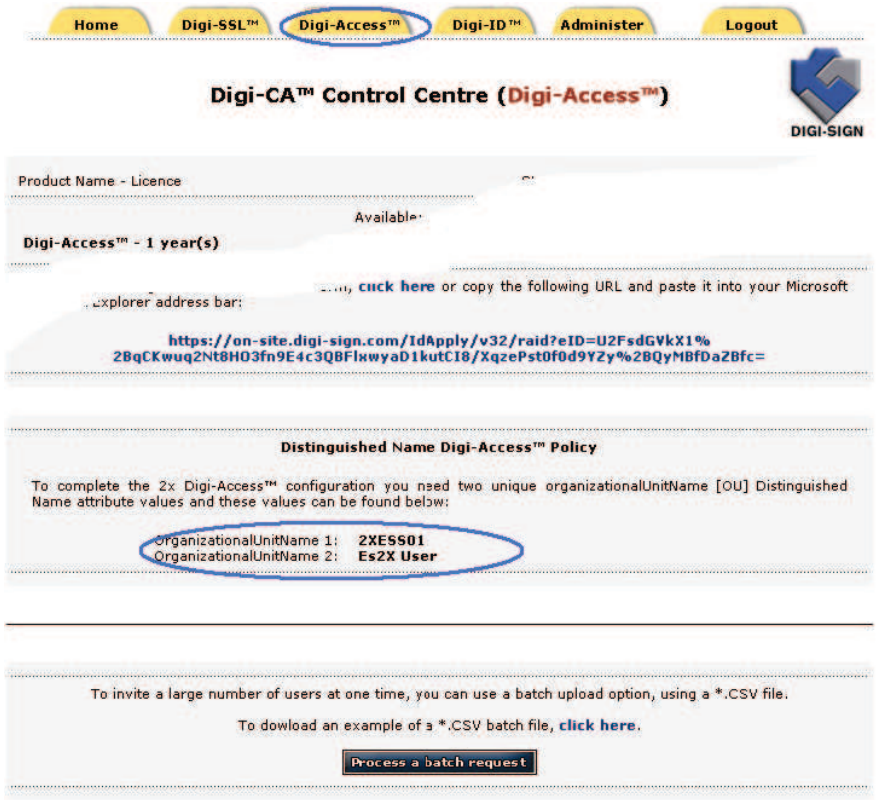
i. Each of these fields can contain common LDAP sub fields for example:

 © Digi-Sign, The Certificate Corportation, Copyright 2010

- CN = commonName (for example, "Bob Smith")
- OU = organizationalUnitName (for example, "Sales")
- OU = organizationalUnitName (for example, "2xacme")
- OU = organizationalUnitName (for example, "2x10003")
- O = organizationName (for example, "Acme, Inc.")
- L = localityName (for example, "Dublin")
- S = stateOrProvinceName (for example, "Dublin")
- C = countryName (for example, "IE")

8. To complete the 2X Application Server configuration you require the two unique organizationalUnitName [OU] codes. These are provided automatically in the Digi-Access™ tab of the Digi-CA™ Control Centre (Digi-Access™).

9. To complete the 2X Application Server configuration you require the two unique organizationalUnitName [OU] codes. These are provided automatically in the Digi-Access™ tab of the Digi-CA™ Control Centre (Digi-Access™):



10. To create a mapping, you create a rule based on a field/subfield pair for a specific value. For example, you could create a rule that matched the Subject's O subfield with 'Acme' to allow access to all clients with certificates that were issued for the

 © Digi-Sign, The Certificate Corportation, Copyright 2010

Acme organization. This effectively eliminates client connections from any clients that are not part of the Acme organization. When finished creating the rule settings, click OK, and then click Next

IMPORTANT NOTE:- In addition to the above parameters you enter, two additional rule sets will be generated by the Registration Authority [RA] that will be used to distribute the end users' Digi-Access™ certificates. These two rule sets are based on Organizational Unit Name [OU] fields and will be 'silently' pre-appended to each Digi-Access™ Certificate issued by the Digi-Access™ CA.

These OU field values distinguish end users as belonging to your specific user domain. You must obtain these values from Digi-Access™ RA Certificate Management Console where these two rule sets can be found in the Certificate Manager's 'Distinguished Name' policy configuration.

11. In the Mapping dialog box, click Accept this certificate for Logon Authentication, and then in the Account box, type, or click Browse to browse to the Windows user account that you want to map. Type the password of the user account in the Password box.

12. Click OK three times, and then quit Internet Services Manager, or close the IIS snap-in.

 © Digi-Sign, The Certificate Corportation, Copyright 2010

5 Issuing Digi-Access™ Certificates

The Digi-CA™ Certificate Authority [CA] system activates a dedicated Registration Authority [RA], that issues the Digi-Access™ end user certificates for your customer. The RA can issue thousands of certificates every hour. This 'endless' capacity means that getting Digi-Access™ certificates to the end users can occur as quickly as required.

5.1 Overview of the issuing process

Issuing the Digi-Access™ certificates is either a one or two stage process. Either the user receives an email inviting them to apply for their certificate, or they are referred from an existing online site/system to the Certificate Request form (e.g. a link on one of the Error 403 web pages – see section 3).

However the user is prompted to get their certificate, in the first stage, the Digi-CA™ Inviting 'action' requires the end user 'reaction' (completing an application form). In the second stage, the Digi-CA™ Approving 'action' requires the end user 'reaction' (activating the certificate) and this completes the process. It is best understood as follows:

- Inviting each end user to complete the online Certificate Enrolment form
    - Completing the enrolment form by the end user
- Approving each correctly completed enrolment and issuing the approval notice
    - Activating the certificate by the end user

5.2 Issuing process options

How the Digi-Access™ certificates are issued is set by the 'Enrolment Policy'. The options within the Enrolment Policy are designed to be very flexible. They can be customised to meet almost any requirement with many different settings and combinations. The three basic options are:

- Manual
    - Inviting and approving requiring manual input from the Administrator
- Automated
    - Inviting and approving are completely automated
- Combination
    - Inviting and approving may require some manual input from the Administrator

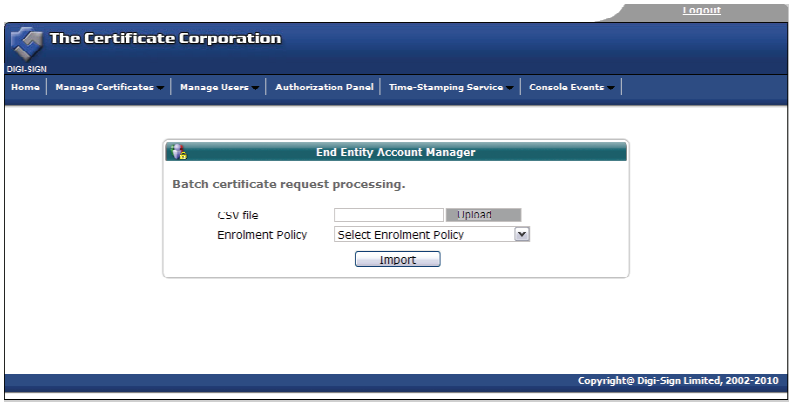
 © Digi-Sign, The Certificate Corportation, Copyright 2010

5.3 Sample issuing process

As stated, because the Enrolment Policy is very flexible, there are many different ways to invite and approve end users' certificates. The following is a sample issuing process only. You may wish to include other options, as required.

5.3.1 Stage 1 'Digi-CA™ Action' - Inviting Certificate Applications

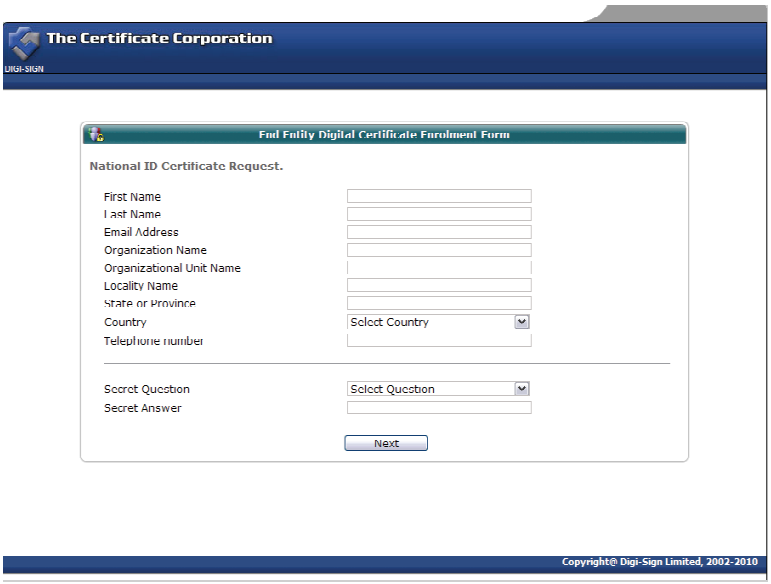
Using the Digi-CA™ RA Management Console interface the Administrator uploads a .CSV batch file inviting as many users as required.



5.3.1.1 Stage 1 'User Reaction' - Completing Enrolment Form

The Digi-CA™ system sends an email to each end user with a unique link to the Digi-Access™ certificate enrolment form. Using the link provided in the email, the end user then completes the Digi-Access™ certificate enrolment form.

Note:- this is the default Digi-Access™ End Entity Digital Certificate Enrolment Form. This form uses basic HTML programming that can be altered to match your specific design requirements.



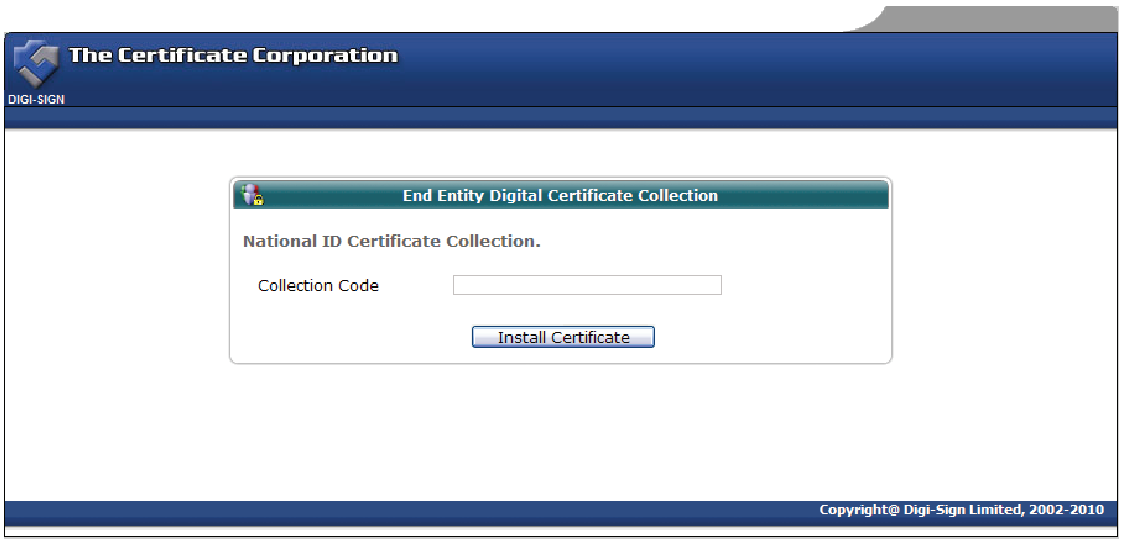
 © Digi-Sign, The Certificate Corportation, Copyright 2010

5.3.2 Stage 2 'Digi-CA™ Action' - Approving Enrolment Applications

Once the end user completes all the fields and submits the enrolment form to the Digi-CA™ system, the Administrator is notified. The Administrator then approves each end user application using the Digi-Access™ certificate Authorization Panel.

5.3.2.1 Stage Two 'User Reaction' - Activating the Certificate

Assuming the Administrator approves the application, the Digi-CA™ system sends a new email to the end user advising them that their application has been approved. Using the link provided in the email, the end user then activates the Digi-Access™ certificate and this completes the issuing process.



 © Digi-Sign, The Certificate Corportation, Copyright 2010

6 Terms of Supply & Commission Rebates

The following is important information relating to terms of supply, payments and commission rebates.

6.1 Claiming your commission rebate

6.1.1	*Customer pays Digi-Sign directly*	Payment for Digi-Sign services is made directly by the customer to Digi-Sign in full and according to the official 2X Digi-Sign price list.
6.1.2	***You invoice for commission***	At the end of each month, it is your responsibility to invoice Digi-Sign for the commission(s) due from the previous month. This is done by accessing the ARP Extranet and using the Accounting instructions located at this URL: **http://www.digi-sign.com/arp/accounts**
6.1.3	***PDF invoices only***	All invoices should be sent in .PDF format to: **arp-accounts@digi-sign.com**
6.1.4	*Payment is by EFT*	Payment will only be made by electronic funds transfer, so ensure you provide full banking details.
6.1.5	*30 Days*	Settlement of invoices is 30 days, end of month.
6.1.6	***No invoice** in 90 days. **No payment***	Failure to issue your commission invoice within **90 days** of the service being delivered to your customer will result in the commission for that sale being **cancelled, without exception**.

6.2 Terms of Supply

6.2.1	*Electronic invoices & reminders*	Digi-Sign does not operate a manual debtors reminder service. Invoices are issued electronically by email. Reminder emails are sent periodically to advise your customers of outstanding accounts.
6.2.2	***Paid on time***	Payment of all outstanding amounts on, or before, their due date, as clearly marked on every invoice, is required.
6.2.3	***Or service disconnected***	Failure to pay outstanding amounts owing on invoices, on or before their due date may result in service to your customers being disconnected and/or discontinued **without warning**.

 © Digi-Sign, The Certificate Corportation, Copyright 2010