# Dematerialized Securities System -Guidelines for client workstation setup

Version 1.0

10/03/2016

# Contents

1.	Requirements	3
1.1	Java Runtime Environment (JRE)	4
1.2	Browsers	5
1.3	Certificates	5
1.4	Adobe PDF Reader – Browser Plug-in	7
Арре	endix A - Installing ATHEX Certificates on Internet Explorer	8
Арр	endix B - Installing ATHEX Certificates on Firefox	26
Арр	endix C – Code Signing Certificates	41

### 1. Requirements

As a consequence of upgrading the DSS application in the new web-based environment (Oracle Forms 11gR2), user's access to the application is changing as well. The user interface is supported by means of a Java applet, which is accessible from a browser of the client workstation. Therefore, some configuration actions need to be performed on the workstation that is hosting the client application.

Prerequisites for supporting the application can be summarized in the following:

- Installing the Java Runtime Environment (JRE), a program that allows Java applications to be executed by a host computer.
- Installing one of the supported browsers.
- Installing the ATHEX certificates.
- Installing the Adobe PDF Reader and browser plug-in.

### 1.1 Java Runtime Environment (JRE)

According to the Oracle guidelines<sup>1</sup>, for the supported setup of a client workstation that supports Forms 11gR2 applications, the minimum JRE edition that is applicable is version 1.6.0\_10.

For installing the latest JRE edition, visit the Java <u>download</u> page and select the JRE Download option.



<sup>&</sup>lt;sup>1</sup> http://www.oracle.com/technetwork/developer-tools/forms/oracle-forms-11gr2certmatrix-519680.xls

### 1.2 Browsers

The following browsers support the client application:

- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Firefox 3.6
- Firefox 5
- Safari 5

### 1.3 Certificates

The use of certificates<sup>2</sup>, regarding the DSS application, spans over three layers of certification:

- Certification of the executable code, as well as the vendor of this code.
- Certification of the web server hosting the application (server authentication).
- Certification of the user of the application (client authentication), in cases where this is applicable.

Detailed instructions in order to install certificates for Internet Explorer are provided <u>Appendix A</u> and for Firefox in <u>Appendix B</u> of this document.

#### Certification of the executable code

The application's executable code is provided by two vendors, namely Oracle and ATHEXGroup, and is digitally signed certificates which are issued by VeriSign and Symantec

- http://ocsp.verisign.com
- http://s2.symcb.com
- http://sv.symcd.com
- http://sf.symcd.com
- http://ocsp.athexgroup.gr
- http://www.helex.gr

<sup>&</sup>lt;sup>2</sup> For the well-functioning of certificates, communication between the client workstation and the certificate's vendor needs to be established, in order to confirm the non-revocation of a certificate by its issuer (certificate revocation list). As an indication, in the current implementation, the client workstation needs to have internet access to the following resources:

http://ocsp.geotrust.com

http://gtssl-ocsp.geotrust.com

http://crl.geotrust.com

respectively. <u>Appendix C</u> describes the process for permanently accepting the two certificates used by software vendors.

#### Certification of the web server (server authentication)

Communication between the client workstation and the DSS application incorporates the use of the Secure Sockets Layer (SSL) protocol, allowing the server's identity certification by the client workstation. In order to avoid security warning messages regarding the server's validity, it is required to install the Primary certification authority certificate (ROOT CA), as well as the Underlying Certificate Authority (Athex SSL Certificates CA), which can be retrieved from the following link <u>http://www.helex.gr/en/web/guest/digital-certificates-pki-regulations</u>.

#### Certification of the user of the application (client authentication) through ATHEXNet

In case the application is accessed from workstations within the closed proprietary network administered by ATHEXGroup (ATHEXNet)<sup>3</sup> or through the attached intranet network of the participant, it is not required to install a certificate that validates the identity of the user (client authentication).

#### Certification of the user of the application (client authentication) through the Internet

In case the application is accessed from the Internet, client authentication is mandatory, combined with the use of a secondary access password. Certificates for the intended users are issued by the Digital Certificates Division of ATHEXGroup, upon user request. The certificate provided to the user, needs to be installed in the browser that will access the application, under the personal certificates group.

<sup>&</sup>lt;sup>3</sup> For the same reason as mentioned in the previous footnote, workstations connecting through ATHEXNet, need to configure their browsers in order to use the proxy athexsquid.athexnet.gr for connecting to non-local addresses. This proxy provides access to the aforementioned web resources. During proxy configuration, the DSS application url's need to be excluded explicitly.

### 1.4 Adobe PDF Reader – Browser Plug-in

For the correct display of Oracle Reports generated by the DSS application in PDF format, the following components must be installed:

- Adobe Reader application, for reports saved locally in the client workstation (<u>https://get.adobe.com/reader/</u>).
- The appropriate Adobe PDF plugin for the browser, in order to support reports displayed through browser tabs (<u>https://helpx.adobe.com/acrobat/using/display-pdf-in-browser.html</u>).

# Appendix A - Installing ATHEX Certificates on Internet Explorer

#### Installing ATHEX Certificates for server authentication

Below, are the steps required for installing the different types of certificates on Internet Explorer:

• From the Internet Explorer menu select: "Tools" -> "Internet Options".

Internet Options
General Security Privacy Content Connections Programs Advanced
Home page To create home page tabs, type each address on its own line.
about:blank
Use current Use default Use new tab
Startup
Tabs Change how webpages are displayed in tabs. Tabs
Browsing history
Delete temporary files, history, cookies, saved passwords, and web form information.
Delete browsing history on exit
Delete Settings
Appearance Colors Languages Fonts Accessibility
OK Cancel Apply

• Select the "Content" tab, click "Certificates".

Internet Options				l	? ×
General Security	Privacy	Content	Connections	Programs	Advanced
Certificates	ertificates	for encrypt	ed connections	and identifi	cation.
Clear SSL	state	Certif	ficates	Publishe	ers
AutoComplete -					
AutoC on we for yo	omplete st bpages an u.	tores previo d suggests	matches	Setting	gs
Feeds and Web S	lices —				
Feeds conter read in progra	and Web In trom we Internet ams.	Slices provi bsites that Explorer ar	de updated can be nd other	Setting	<u>gs</u>
Some settir	<u>ngs</u> are ma	naged by y	our system ad	ministrator.	
		ОК	Ca	ancel	Apply

• Select the "Trusted Root Certification Authorities" tab, click "Import".

Certificates			- 11	×
Intended purpose:	<all></all>			•
Intermediate Certifica	tion Authorities	Frusted Root Certification A	uthorities Tr	usted Publ
Issued To		Issued By	Expiratio	Friendly 1
VeriSign Trust Na VeriSign Commen VeriSign Class 3 UTN-USERFirst-C UTN-USERFirst-F Thawte Timestan thawte Primary B Thawte Premium	etwork rcial Software P Public Primary Dbject Hardware mping CA Root CA Server CA	VeriSign Trust Network VeriSign Commercial S VeriSign Class 3 Public UTN-USERFirst-Object UTN-USERFirst-Hardw Thawte Timestamping thawte Primary Root CA Thawte Premium Serv	2/8/2028 8/1/2004 17/7/2036 9/7/2019 9/7/2019 1/1/2021 17/7/2036 1/1/2021	VeriSign VeriSign USERTru: USERTru: Thawte T thawte thawte
Import Exp	oort Ren urposes	nove	ſ	Advanced
Learn more about <u>certi</u>	ficates			Close

• The helper program "Certificate Import Wizard" appears. Click "Next".

Certificate Import Wizard	×
Certificate Import Wizard	Xelcome to the Certificate Import Wizard           This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.           A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.           To continue, click Next.
	< Back Next > Cancel

• Click "Browse" and locate the certificate "ATHEX Root CA.cer" from the directory where it is saved. Click "Next".

File to Import		
Specify the file you want to import.		
File name:		
C:\ATHEXCertificates\ATHEX Root CA.	cer	Browse
Note: More than one certificate can be	stored in a single file in	the following formats:
Personal Information Exchange-PKC	S #12 (.PFX,.P12)	
Cryptographic Message Syntax Stan	dard-PKCS #7 Certifica	ates (.P7B)
Microsoft Serialized Certificate Store (.SST)		
earn more about <u>certificate file formats</u>		

• Select "Place all certificates in the following store" with the "Certificate store" option set to "Trusted Root Certification Authorities". Click "Next".

ificate Im	oort Wizard
Certificate	Store
Certific	ate stores are system areas where certificates are kept.
Windo the ce	ws can automatically select a certificate store, or you can specify a location for rtificate.
$\bigcirc$	Automatically select the certificate store based on the type of certificate
۲	Place all certificates in the following store
	Certificate store:
	Trusted Root Certification Authorities Browse
.earn more	about <u>certificate stores</u>

• In the summary tab, click "Finish".

Certificate Import Wizard		×
	Completing the Certifi Wizard	icate Import
	The certificate will be imported afte	r you dick Finish.
	You have specified the following se	ttings:
	Certificate Store Selected by Use Content File Name	Trusted Root Certifica Certificate C:\ATHEXCertificates'
	< Back	Finish Cancel

• Select the "Intermediate Certification Authorities" tab, click "Import".

Certificates			- 11	×
Intended purpose:	<all></all>			•
Intermediate Certificat	tion Authorities	Trusted Root Certification A	uthorities Tr	usted Publ
Issued To		Issued By	Expiratio	Friendly 1
www.verisign.co	om/CPS Incorp A - G3 ws Hardware C omain Validatio ertification Aut dinate CA	Class 3 Public Primary thawte Primary Root CA Root Agency Microsoft Root Authority localhost COMODO RSA Certific AddTrust External CA ATHEX General Certifi	25/10/2016 31/10/2023 1/1/2040 31/12/2002 12/4/2016 12/2/2029 30/5/2020 23/5/2022	<none> </none>
Import Exp Certificate intended pu Server Authentication 2.16.840.1.113733.1	oort Rer urposes , Client Authentica .8.1	nove ation, 2.16.840.1.113730.4	.1,	Advanced
Learn more about <u>certi</u>	ficates			Close

• The helper program "Certificate Import Wizard" appears. Click "Next".

Certificate Import Wizard	×
Certificate Import Wizard	Xelcome to the Certificate Import Wizard           This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.           A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.           To continue, click Next.
	< Back Next > Cancel

• Click "Browse" and locate the certificate "ATHEXSSLCertificates.cer" from the directory where it is saved. Click "Next".

File to Import			
Specify the file	you want to import.		
File name:			
C:\ATHEXCerti	ificates\ATHEXSSLCertif	icates.cer	Browse
Note: More tha	n one certificate can be	stored in a single file in th	e following formats:
Personal Info	ormation Exchange- PKC	CS #12 (.PFX,.P12)	
Cryptograph	ic Message Syntax Star	ndard- PKCS #7 Certificate	es (.P7B)
Microsoft Ser	rialized Certificate Store	e (.SST)	
Learn more about <u>ce</u>	rtificate file formats		

• Select "Place all certificates in the following store" with the "Certificate store" option set to "Intermediate Certification Authorities". Click Next.

ificate Imp	ort Wizard
Certificate S	tore
Certifica	ite stores are system areas where certificates are kept.
Window the cert	s can automatically select a certificate store, or you can specify a location for ificate.
© A	utomatically select the certificate store based on the type of certificate
P	lace all certificates in the following store
c	Certificate store:
[	Intermediate Certification Authorities Browse
earn more a	about certificate stores
	< Back Next > Cancel

• In the summary tab, click "Finish".

Certificate Import Wizard		×		
	Completing the Certificate Import Wizard The certificate will be imported after you click Finish.			
	You have specified the following set	ttings:		
	Certificate Store Selected by User	Certificate		
	File Name	C: \ATHEXCertificates		
	< III	Þ		
	< Back F	-inish Cancel		

### Installing ATHEX Certificates for client authentication

• Select the "Personal" tab, click "Import".

Certificates		( ) (	-	and in the second	×
Intended purp	ose: </th <th>All&gt;</th> <th></th> <th></th> <th>•</th>	All>			•
Personal Of	ther People	Intermediate Certification	Authorities T	rusted Root Certificatio	on 🔸 🕨
Issued To		Issued By	Expiratio	. Friendly Name	
Import	Export	Remove		Adva	anced
Certificate in	tended purp	oses			
				View	
Learn more ab	oout <u>certifica</u>	tes		Cl	ose

• The helper program "Certificate Import Wizard" appears. Click "Next".

Certificate Import Wizard	×		
Certificate Import Wizard	Welcome to the Certificate Import Wizard         This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.         A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.		
	To continue, click Next.		
	< Back Next > Cancel		

• Click "Browse" and locate the user certificate issued by ATHEXGroup (file having ".p12" extension) from the directory where it is saved. Click "Next".

File to	Import
S	pecify the file you want to import.
Fi	le name:
	C:\ATHEXCertificates\client_certificate.p12 Browse
N	ote: More than one certificate can be stored in a single file in the following formats:
	Personal Information Exchange- PKCS #12 (.PFX,.P12)
	Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
	Microsoft Serialized Certificate Store (.SST)
Learn	more about <u>certificate file formats</u>
	< Back Next > Cano

• Enter the provided password for this certificate. Click "Next".

tificate Import Wizard	
Password	
To maintain security, the private key was protected with a password.	
Type the password for the private key.	
Password:	
•••••	
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.	
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.	
Include all extended properties.	
Learn more about protecting private keys	
< Back Next > Ca	ancel

• Select "Place all certificates in the following store" with the "Certificate store" option set to "Personal". Click "Next".

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
$\bigcirc$ Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Personal Browse
Learn more about <u>certificate stores</u>
< Back Next > Cancel

• In the summary tab, click "Finish".

Certificate Import Wizard		×		
	Completing the Certificate Import Wizard The certificate will be imported after you click Finish.			
	You have specified the following : Certificate Store Selected by Us Content File Name	settings: ser Personal PFX C:\ATHEXCertificates'		
	< <u> </u>	4		
	< Back	Finish Cancel		

### Appendix B - Installing ATHEX Certificates on Firefox

#### **Installing ATHEX Certificates for server authentication**

Below, are the steps required for installing the different types of certificates on Firefox:

 From the Firefox menu select: "Options" -> "Advanced" -> "Certificates". Click "View Certificates".



• The "Certificate Manager" appears. Select "Authorities" tab, click "Import".

ur Certificates People Servers Authorities	Others	
You have certificates on file that identify thes	e certificate authorities:	
Certificate Name	Security Device	
AC Camerfirma S.A.	Puiltin Object Taken	
Global Chambersign Root - 2008	Builtin Object Token	
AC Camerfirma SA CIF A82743287		
Chambers of Commerce Root	Builtin Object Token	
Global Chambersign Root	Builtin Object Token	
ACCV		
ACCVRAIZ1	Builtin Object Token	
View Edit Trust Import	Export Delete or Distrust	
		011

• Locate the certificate "ATHEX Root CA.cer" from the directory where it is saved. Click "Open". The "Downloading Certificate" dialog appears. Select option "Trust this CA to identify websites". Click "OK" in order to import the certificate.

Downloading Certificate	x
You have been asked to trust a new Certificate Authority (CA).	
Do you want to trust "ATHEX Root CA" for the following purposes?	
Trust this CA to identify websites.	
Trust this CA to identify email users.	
Trust this CA to identify software developers.	
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).	
View Examine CA certificate	
OK Cancel	

 For Firefox, it is required that the "ATHEX Root CA" certificate is also imported through Java's Control Panel. On Windows, select "Start"->"Control Panel".



• Select "Java". The "Java Control Panel" appears. Select tab "Security".

🛓 Java Control Panel	
General Update Java Security Advanced	
Enable Java content in the browser	
Security level for applications not on the Exception Site list	
🔘 Very High	
Only Java applications identified by a certificate from a trusted authority are a and only if the certificate can be verified as not revoked.	allowed to run,
e High	
Java applications identified by a certificate from a trusted authority are allowe the revocation status of the certificate cannot be verified.	d to run, even if
Excention Site List	
Applications launched from the sites listed below will be allowed to run after the	appropriate security
prompts. Click Edit Site List	
to add items to this list.	lit Site List
View the active Deployment Rule Set	
Restore Security Prompts Manag	ge Certificates
ОК Са	ncel Apply

• Click "Manage Certificates". The "Certificates" window appears. In the "Certificate type" option, select "Secure Site CA" from the drop-down list.

Certificates	23	
Certificate type: Secure Site CA	•	
Issued To	Issued By	
	•	
	-	
Import	Remove Details	
	Close	

• Click "Import". Locate the certificate "ATHEX Root CA.cer" from the directory where it is saved. Click "Open". On success, the certificate is shown in tab "Secure Site CA".

Cert	ficates		X
Ce	rtificate type: Secure Site CA		•
	Issued To	Issued By	
	ATHEX Root CA	ATHEX Root CA	
			Ŧ
L	Import Export	Remove Details	
			Close

### Installing ATHEX Certificates for client authentication

• In the "Certificate Manager" select "Your Certificates" tab, click "Import".

	rom these organizations i	that identify you:		
Certificate Name	Security Device	Serial Number	Expires On	Ε.
4				

• Locate the user certificate issued by ATHEXGroup (file having ".p12" extension) from the directory where it is saved. Click "Open". Enter the provided password for this certificate. Click "OK".

-				_
Certificate Name	Security Device	Serial Number	Expires On	E.,
Password Required			×	
Please er	nter the password that v	vas used to encrypt th	is certificate backup:	
	ner the passifiera that i	ius useu to energipt in	is certificate backapt	
				I
	ОК	Cancel		I
	ОК	Cancel		

• For Firefox, it is required that the client certificate is also imported through Java's Control Panel. This will also create a Java personal keystore, if there isn't one already in the workstation.

On Windows, select "Start"->"Control Panel".



• Select "Java". The "Java Control Panel" appears. Select tab "Security".

🛓 Java Control Panel				
General Update Java Security Advanced				
Enable Java content in the browser				
Security level for applications not on the Exception Site list				
🔘 Very High				
Only Java applications identified by a certificate from a trusted authority are a and only if the certificate can be verified as not revoked.	allowed to run,			
e High				
Java applications identified by a certificate from a trusted authority are allowe the revocation status of the certificate cannot be verified.	d to run, even if			
Excention Site List				
Applications launched from the sites listed below will be allowed to run after the	appropriate security			
prompts. Click Edit Site List				
to add items to this list.	lit Site List			
View the active Deployment Rule Set				
Restore Security Prompts Manag	ge Certificates			
ОК Са	ncel Apply			

• Click "Manage Certificates". The "Certificates" window appears. In the "Certificate type" option, select "Client Authentication" from the drop-down list.

Certificates	a set or the location like its	×
Certificate type: Client Authent User System	ication	<b>•</b>
Issued To	Issued By	
		<b>^</b>
		· · · ·
Impo	rt Export Remove Details	
		Close

• Click "Import". Locate the user certificate issued by ATHEXGroup (file having ".p12" extension) from the directory where it is saved. Click "Open". Enter the provided password for this certificate. Click "OK".

Authentication Required				
Enter password to access file:				
Password:				
	OK Cancel			

• If a personal Java keystore already exists, the password for the existing keystore is required. If a personal Java keystore doesn't exist, Java will ask for a password in order to create a new keystore. Be sure to take a note of the keystore password, as it will be required for subsequent use. This password is not to be confused with the client's certificate password used in the previous step.

Authentication Required
Enter a password to access your personal keystore:
Password:
OK Cancel

• On success, the certificate is shown in tab "Client Authentication".

Certi	ficates	In additions of a field capter like in	×
Ce	rtificate type:	Client Authentication	•
	Issued To	Issued By	
		ATHEX General Certificates CA	· · · ·
			-
		Import Export Remove Details	
			Close

### Appendix C - Code Signing Certificates

When the application is executed for the first time, the Java Runtime will issue warnings about the acceptance of the publishers of the code. Two dialogs will be presented, one regarding code that is signed by Oracle and another one regarding code that is signed by ATHEXGroup.

It is advised to select option "Do not show this again for apps from the publisher and location above" and click "Run". Certificates for both publishers will be automatically imported in the trusted certificates store of Java.

× Do you want to run this application?						
6	4	Name:	OracleForms			
	<u>ڪ</u>	Publisher:	Oracle America, Inc.			
		Location:	http://dssmock.athexnet.gr			
This app informa	This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above.					
🗸 Do n	ot show this a	again for apps	from the publisher and location a	bove		
Í	More Inform	ation		Run Cancel		



After acceptance, the two certificates will be imported in the Java Control Panel, under the Trusted Certificates category.

Cer	tificates		23
	ertificate type: Trusted Certificates		•
	System		
	Issued To	Issued By	
	HELLENIC EXCHANGES - ATHENS STOCK EXCH	Symantec Class 3 SHA256 Code Signing CA	<b>^</b>
	Oracle America, Inc.	VeriSign Class 3 Code Signing 2010 CA	
			-
	Import Export	Remove Details	
			Close