



Ascertia Limited  
40 Occam Road  
Surrey Research Park  
Guildford  
Surrey  
GU2 7YG

Tel: +44 1483 685500  
Fax: +44 1483 573704

[www.ascertia.com](http://www.ascertia.com)

# ARP Lite User Guide

---

Document Version: 4.1.0.2

Document Issued: July 2007

©Copyright Ascertia Ltd, 2007

This document contains commercial-in-confidence material. It must not be disclosed to any third party without the written authority of Ascertia Limited.

---

Commercial-in-Confidence

# Contents

<b>1</b>	<b>Scope</b> .....	3
<b>2</b>	<b>Introduction</b> .....	5
2.1	Overview .....	5
<b>3</b>	<b>Configurations and Settings</b> .....	6
3.1	ARP Lite User Interface .....	6
<b>4</b>	<b>ARP Lite System Tray Menu</b> .....	20
<b>5</b>	<b>ARP Lite Messages</b> .....	21
5.1	Pop-Up Messages .....	21
<b>6</b>	<b>How to Enable ARP in Windows Applications</b> .....	24
<b>7</b>	<b>Appendix</b> .....	25
7.1	General Error messages .....	25
7.2	General tab messages .....	25
7.3	Applicability tab messages .....	25
7.4	Alert Settings tab messages .....	26
<b>8</b>	<b>Frequently Asked Questions</b> .....	27
8.1	I have a signed email in Outlook Express and Outlook 2000 but ARP is not invoked?27	
8.2	I have a signed email, where the certificate has a valid CDP extension but ARP is still not invoked? .....	27
8.3	I am setting the Responder URL and Port but ARP seems not connecting to the Responder?.....	28
8.4	I am trying to connect to an SSL based server but I am getting Error in Connection messages? .....	28
8.5	I have configured ARP to check the revocation status of OCSP responder's certificates, but ARP does not do this, why?.....	29
8.6	ARP keeps my PFX file password saved, is it saved encrypted?.....	29
8.7	I am trying to uninstall ARP but am unable to?.....	29
8.8	I am using a proxy server to connect to an OCSP responder. I have configured proxy correctly. I am not able to connect to the OCSP responder on local intranet if proxy server is down? 30	
8.9	I have configured ARP to sign OCSP request and have selected a Personal Information Exchange (pfx/pkcs#12) file in ARP, but the request generated is not being signed?30	
8.10	Can more than 1 Revocation Provider be used simultaneously? .....	31
8.11	ARP seems to be called when opening 3rd party applications i.e. ACDSee or Network Neighborhood why? .....	31
8.12	How Outlook Express 5.0/6.0, Outlook 2000/2002 and IE respond when ARP shows the results?.....	32
8.13	On some Smart cards PIN is asked every time OCSP Request is about to be signed whereas in some, PIN is asked only once why?.....	62
8.14	After installing ARP my MSN Messenger has stopped working why?.....	62
<b>9</b>	<b>Troubleshooting:</b> .....	64

# 1 Scope

This manual describes how to configure and use Advanced Revocation Provider (ARP) Lite on a Windows® operating system.

## 1.1 Intended Readership

This guide is intended for ARP administrators/users that are responsible for configuring and using ARP.

## 1.2 Document Layout

This manual is divided into the following chapters:

Chapter 1:	Provides this introduction to the document
Chapter 2:	Introduces ARP Lite concepts and architecture
Chapter 3:	Describes how to configure ARP Lite
Chapter 4:	Explains ARP System Tray messages and icons
Chapter 5:	Describes how to configure ARP trust anchors using Internet Explorer
Chapter 6:	Describes how to view historical transactions conducted through ARP

## 1.3 Conventions

The following typographical conventions are used in this guide to help locate and identify information:

**Bold text** identifies menu names, menu options, items you can click on the screen, file names, folder names, and keyboard keys.

Courier font identifies code and text that appears on the command line.

**Bold courier** identifies commands that you are required to type in.

## 1.4 Technical Support

If technical support is required, Ascertia has a dedicated support team providing debugging assistance, integration assistance and general customer support. Ascertia Support can be accessed in the following ways:

Support Email:	support@ascertia.com
Support MSN Messenger:	support@ascertia.com

In addition to the free support service described above, Ascertia provides formal support agreements with all product sales. Please contact [sales@ascertia.com](mailto:sales@ascertia.com) for more details.

A Product Support Questionnaire should be completed to provide Ascertia Support with further information about your system environment. When requesting help it is always important to confirm:

- Network Environment
- System Platform details
- Advanced Revocation Provider version number
- The specific issue seen and the relevant steps taken to reproduce it.
- Database version and patch level
- The product log files

## 2 Introduction

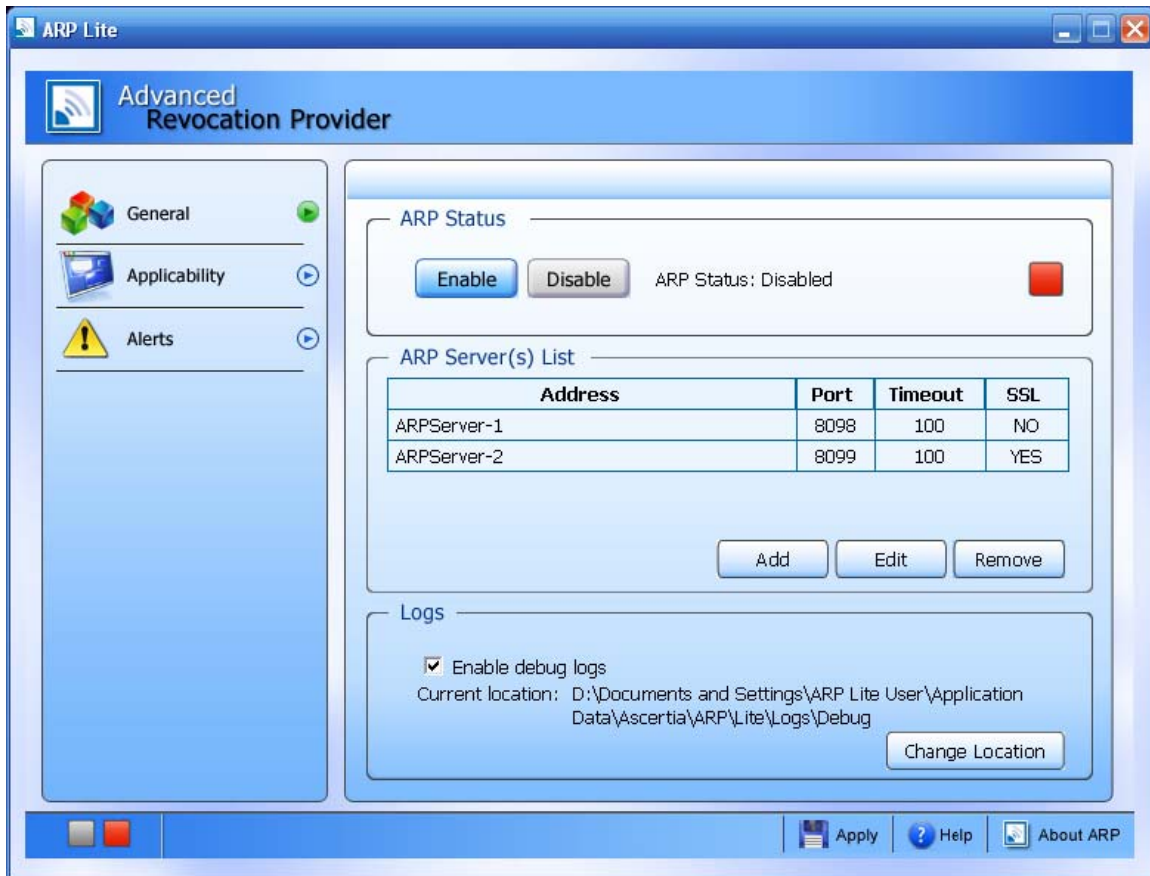
### 2.1 Overview

Ascertia Advanced Revocation Provider (ARP) is a powerful and flexible solution for checking the revocation status of digital certificate(s) using either Online Certificate Status Protocol (OCSP) or traditional Certificate Revocation Lists (CRLs). It is able to switch between these modes based on the configured validation policy and can also utilize cached CRLs and OCSP responses to meet high performance requirements.

## 3 Configurations and Settings

### 3.1 ARP Lite User Interface

This section explains the ARP Lite GUI. Once you have successfully installed ARP Lite, by double-clicking on the **ARP Lite** shortcut on the desktop will show the following screen:



The main window consists of three sections:

**Application Banner Bar:** At the top of the window the Application Banner Bar shows the application logo and name.

**Tab Items Section:** On the left hand side of the main window is the Tab Items Section. You can click different tab Items to set their respective configurations.

**Configuration Pane:** Configuration Pane is where the tab Items are populated and you can set their respective configuration settings.

**Status Bar:** Status Bar shows the status of the ARP Lite i.e. is it currently running or stopped. The Status bar also contains the following toolbar options:

- **Apply:** applies the new settings you have just made.
- **Help:** opens up the Help guide.

- **About ARP:** Opens up an **About ARP Lite** dialogue box that gives the information about the product's version and copyright information. This information should be supplied to Ascertia Support Team when requesting help.

### 3.1.1 General Pane

This section explains the ARP Lite General pane.

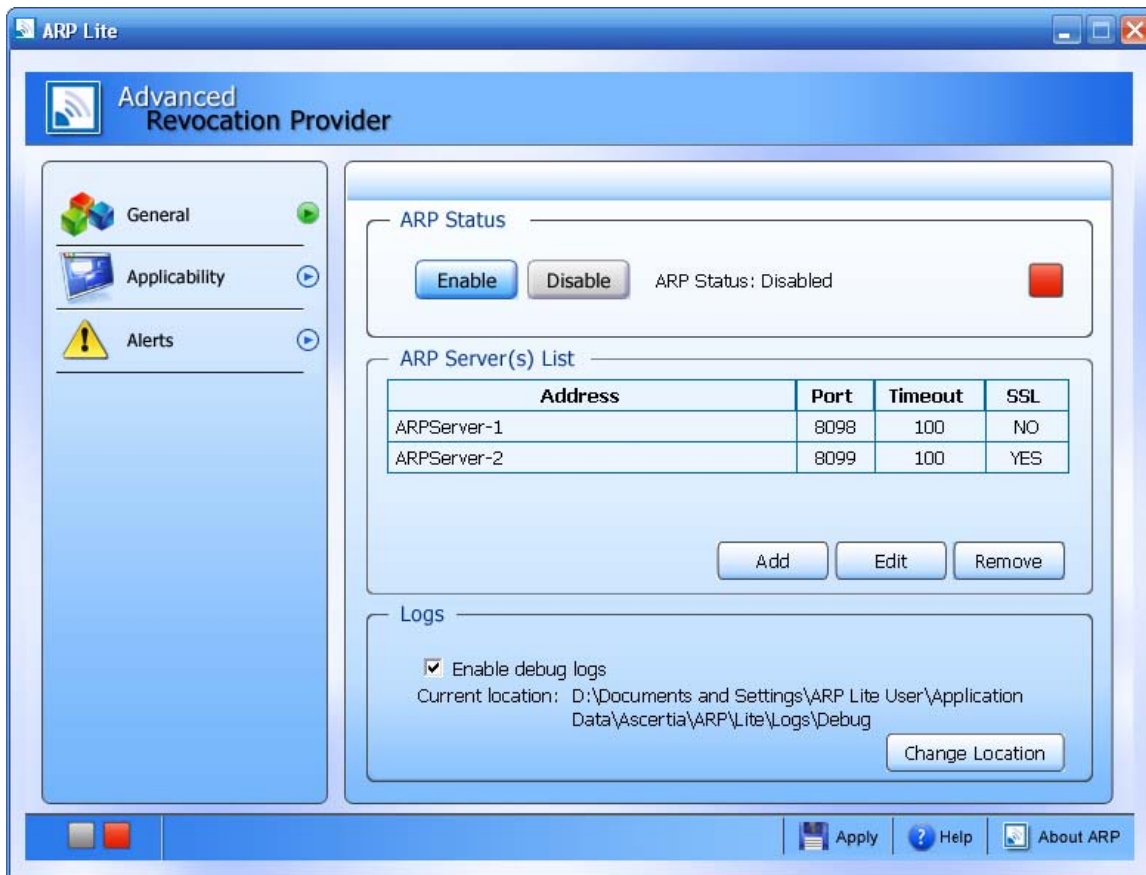
The General pane is where you make the most important settings for the ARP Lite e.g.:

- Enable/Disable ARP Lite
- Configure ARP Server to connect with, for revocation checking
- Configure debug logs

Whenever you open ARP Lite, by default the General Tab is shown. Also by default ARP is enabled, this means ARP will be invoked whenever a Microsoft® CAPI enabled application processes a certificate revocation.

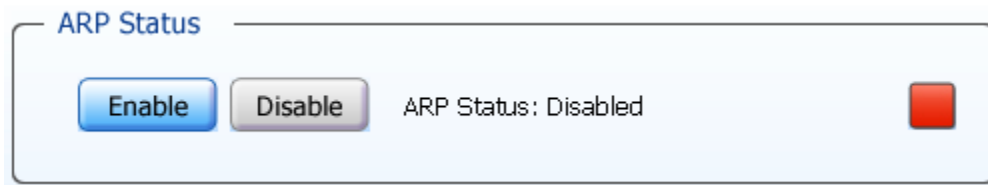


You can only configure the ARP Lite once it's stopped (otherwise all the settings are grayed out). See below to learn how to disable ARP Lite. In order for the settings to take affect you need to enable ARP Lite.

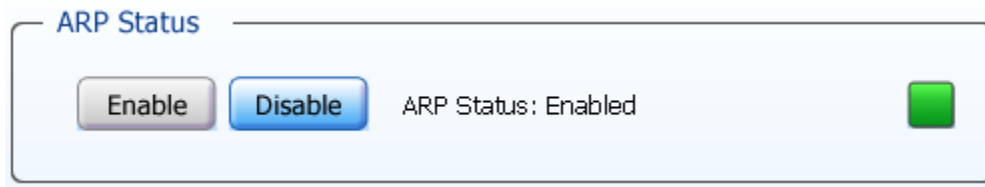


### 3.1.2 Enable/Disable ARP Lite

You can disable the ARP Lite by using the **Disable** button. This will stop the ARP Lite service and enable the **Enable** button (i.e. ARP Lite is disabled currently but it can be switched on). ARP Lite cannot process any request when it is disabled:

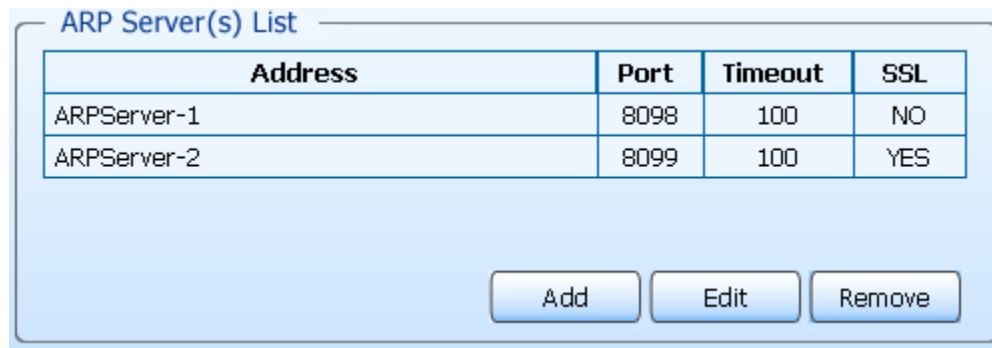


To enable ARP Lite simply click **Enable** button. This will enable ARP Lite and show the following (i.e. **Disable** button is now enabled allowing you to disable it when needed):

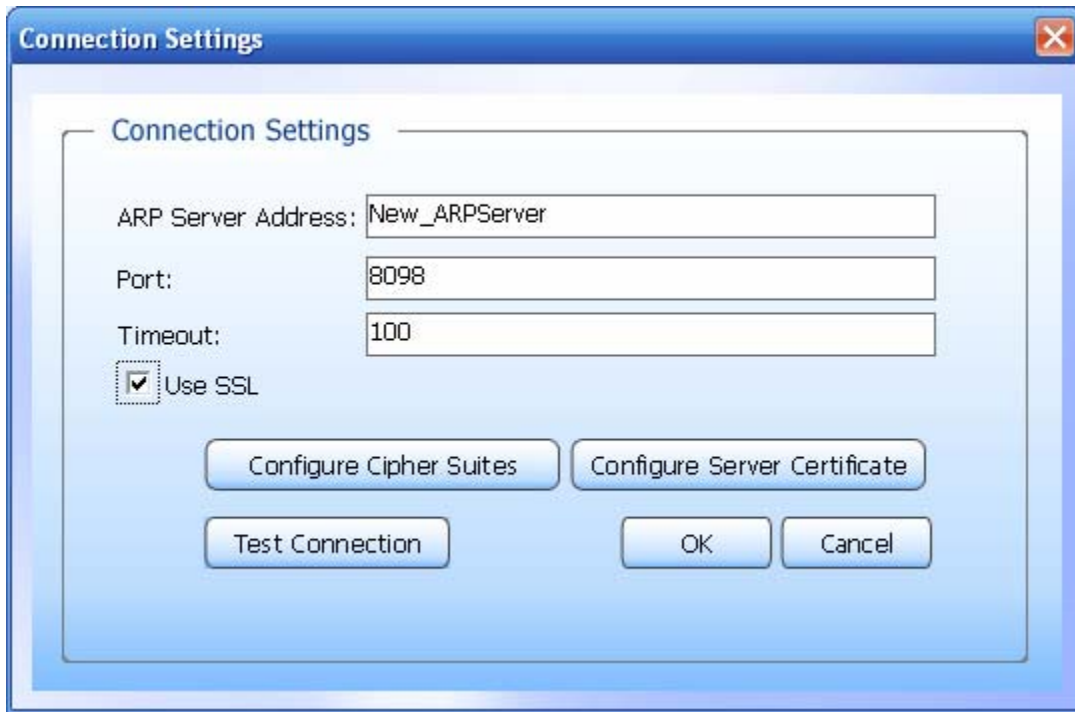


### 3.1.3 Configure ARP Server in order to connect it with ARP Enterprise Edition for revocation checking

This allows you to configure ARP Server from which ARP Lite can connect with ARP Enterprise Edition to get revocation status of the requested certificate.



Press the **Add** button to add new ARP Server:




In connection settings you can configure new ARP Server:

**ARP Server address:** In ARP Server Address you specify the address of the ARP Server to which you send Revocation Requests.

**Port:** The Port no. you set is the one at which ARP Lite will listen and communicate with the ARP Server.

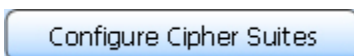
**Timeout:** Timeout you set is the time that ARP Lite will wait for ARP Server to send response to the Revocation Request and if it fails to receive in the specified time then it will disconnect from the ARP Server and will send connection error reply.

	<p>Note: If you specify 0 sec for the Timeout this means that the ARP Lite will wait for the ARP Server Response for an unlimited period of time i.e. till the time it receives the response it will be in wait state.</p>
---	--

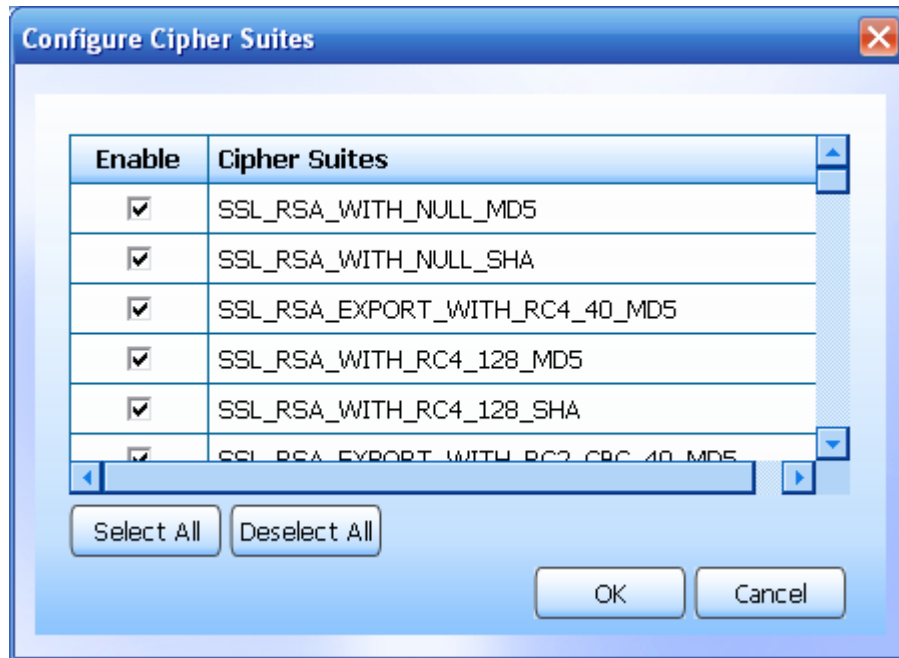
You also have the option to set Secure Socket Layer SSL settings.

**Use SSL:** When you checked the checkbox for Use SSL, Configure Cipher Suites and Configure Server Certificate buttons will be enabled; otherwise they will remain disabled.

**Configure Cipher Suites:** To select the cipher suite press the Configure Cipher Suites Button.

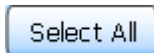


This will open the Configure Cipher Suites window.

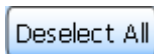


On the Configure Cipher Suites window you have the buttons to Select All or Deselect All cipher suites.

You can select any or all the cipher suites. When you click **Select All** Button it will select or enable all the Cipher suites that are available or listed.



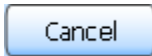
Similarly, when you click **Deselect All** Button it will deselect all or any selected cipher suite.



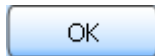
If you have checked the **Use SSL** checkbox and you press "**Deselect All**" button and press the Ok button Message screen will be shown on the user screen.




If you do not want to apply the changes or selected cipher just press the Cancel button on the Configure Cipher Suites window.



The Configure Cipher Suites window will be closed with out applying changes. Press Ok Button to apply the changes and close the window.

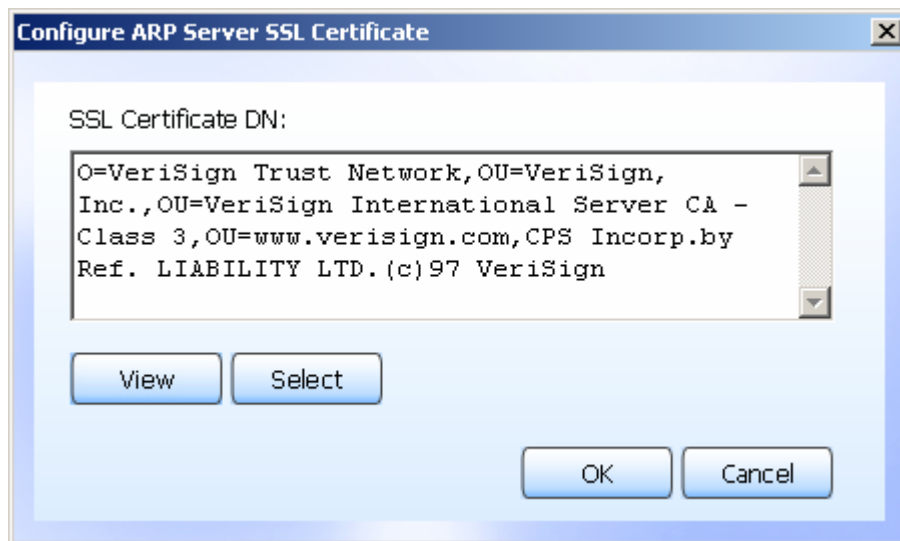


	<p>Note: You need to select the same Cipher Suites on the ARP Lite as you have selected for the ARP Server for the successful communication between ARP Lite and ARP Server.</p>
---	--

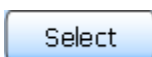
**Configure Server Certificate:** To configure server certificate click the Configure Server Certificate Button.



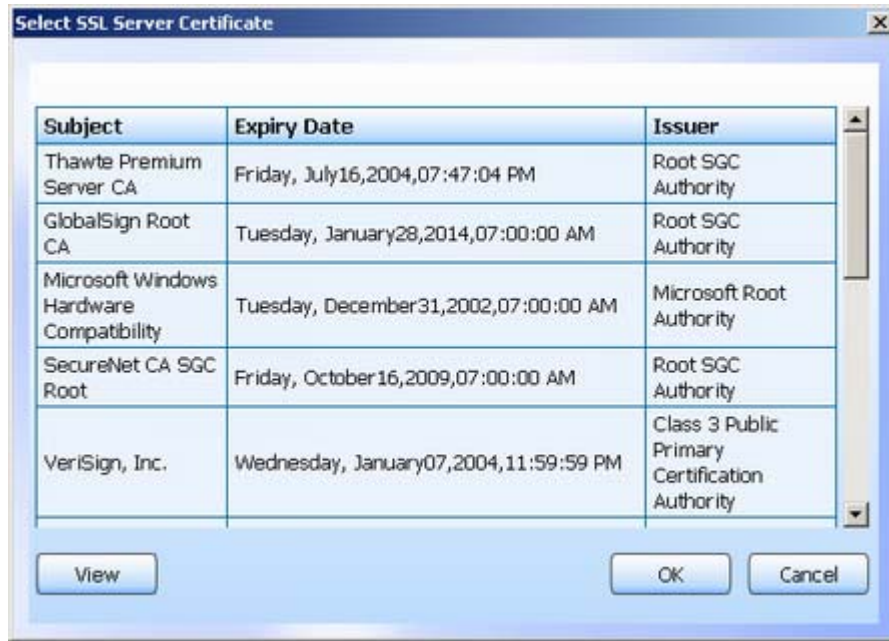
This will open up the Configure ARP Server SSL Certificate window.



To select ARP Server Certificate for SSL mode you can press the Select Button.



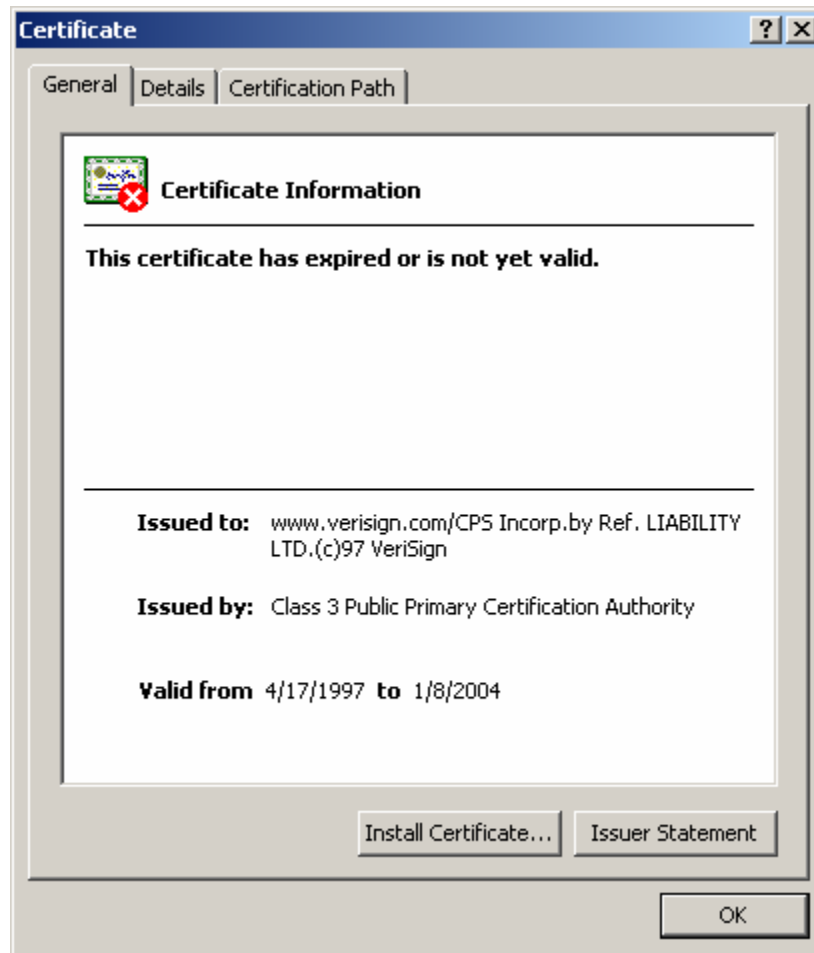
This will open up Select SSL Server Certificate viewer.



The Select SSL Server Certificate viewer is synchronized with Windows Key store and contains only certificates having Extended Key Usage Extension. You can select the required certificate and can view its detailed information by clicking the View button.



This will open Certificate Viewer.



You can view the complete information of selected certificate i.e. the information about the CA of the certificate, about the validity period and the complete Certificate Path.

The selected certificate will be shown in the SSL Certificate DN list box in the Configure ARP Server SSL Certificate window. You can also see the details of the certificate by pressing the view button available on the Configure ARP Server SSL Certificate window.

Test Connection: The selected configurations can be tested by using the Test Connection Button.

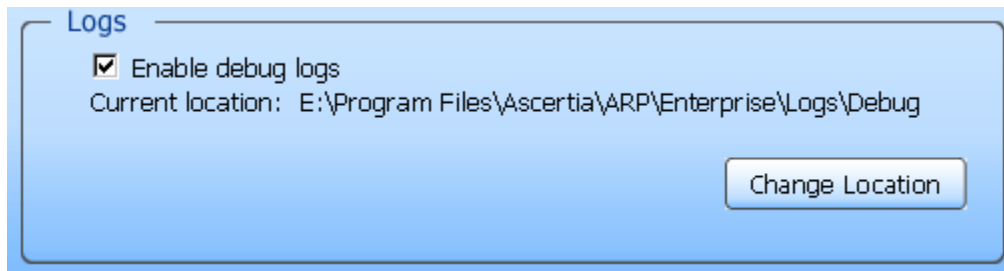


Test Connection Button will open a Test Connection window that shows the status bar indicating the connection to the server.



### 3.1.4 Configure Debug Logs

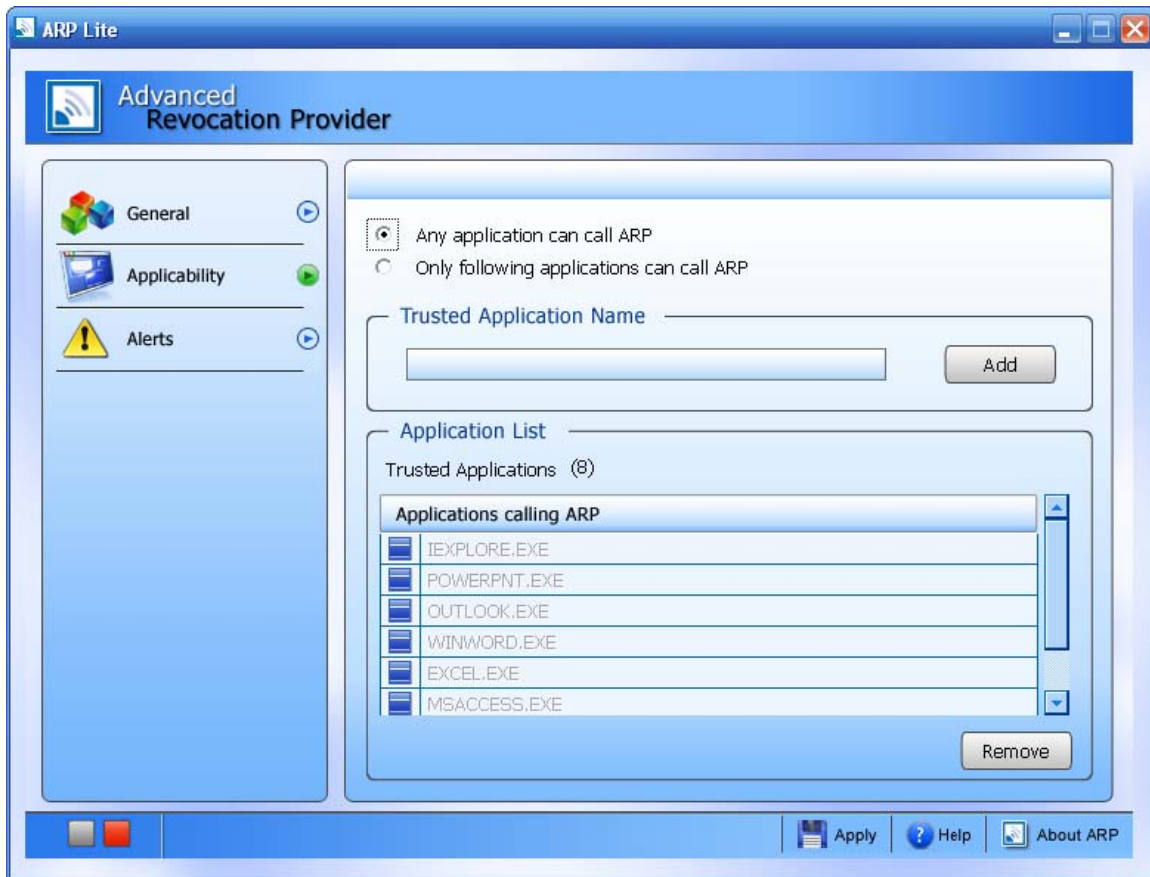
You can enable debug logs that shall be maintained on physical drive.



Clicking on **Change Location** button allows you to change the debug logs location when required.

## 3.2 Applicability Pane

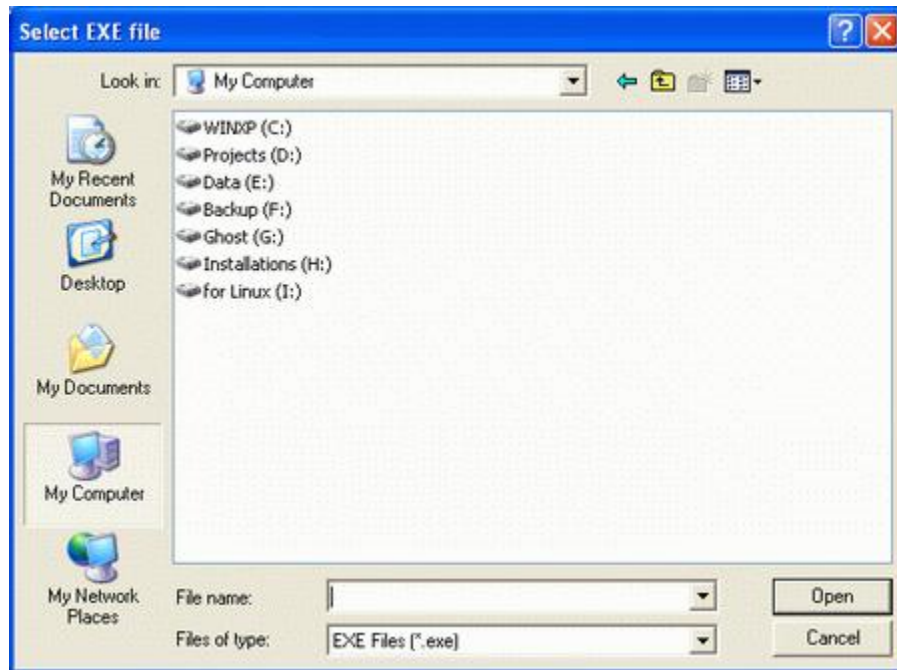
ARP Lite can be called by any application installed on your machine or by only specified applications.



**Any Application can call ARP:** Select the radio button **Any application can call ARP** if you want ARP Lite to be called by any application. In this case list of trusted application in **Application List** section will be disabled. The user cannot add any application or remove any application from the list, since all applications are allowed.

**Only Following Application can call ARP:** Select the radio button **Only following Application can call ARP** if you want to restrict the use of ARP to only certain applications. Selecting this option will enable the list of trusted applications in **Application List** section.

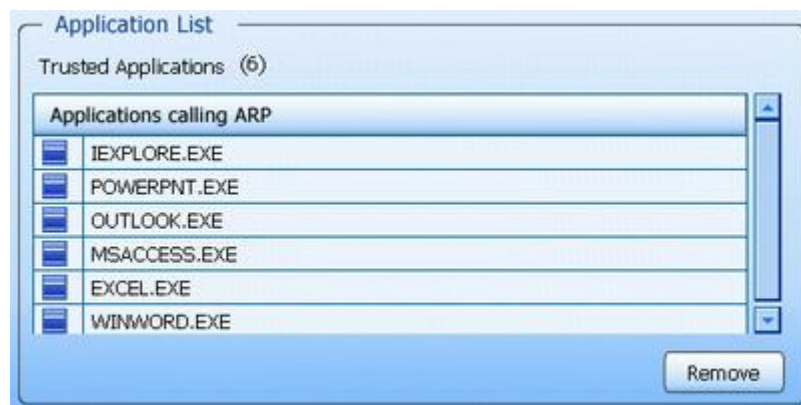
You can add the application(s) by pressing **Add** button. This will open up a dialog box **Select EXE file** as follows:



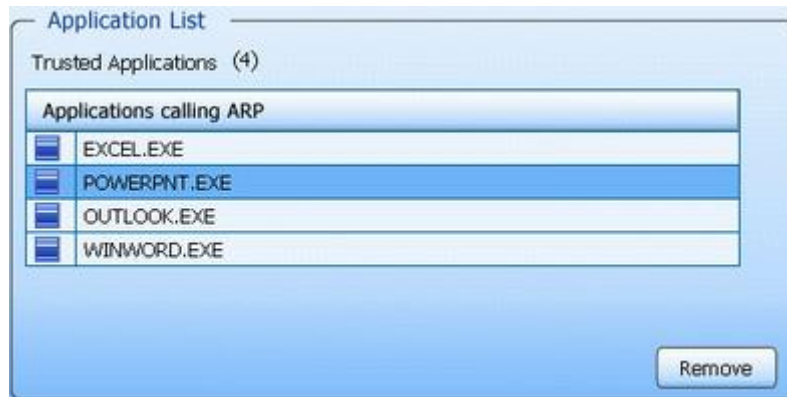
You can select the application that you want to specify in the Trusted Applications List.



The application will be added in the Applications List as shown:



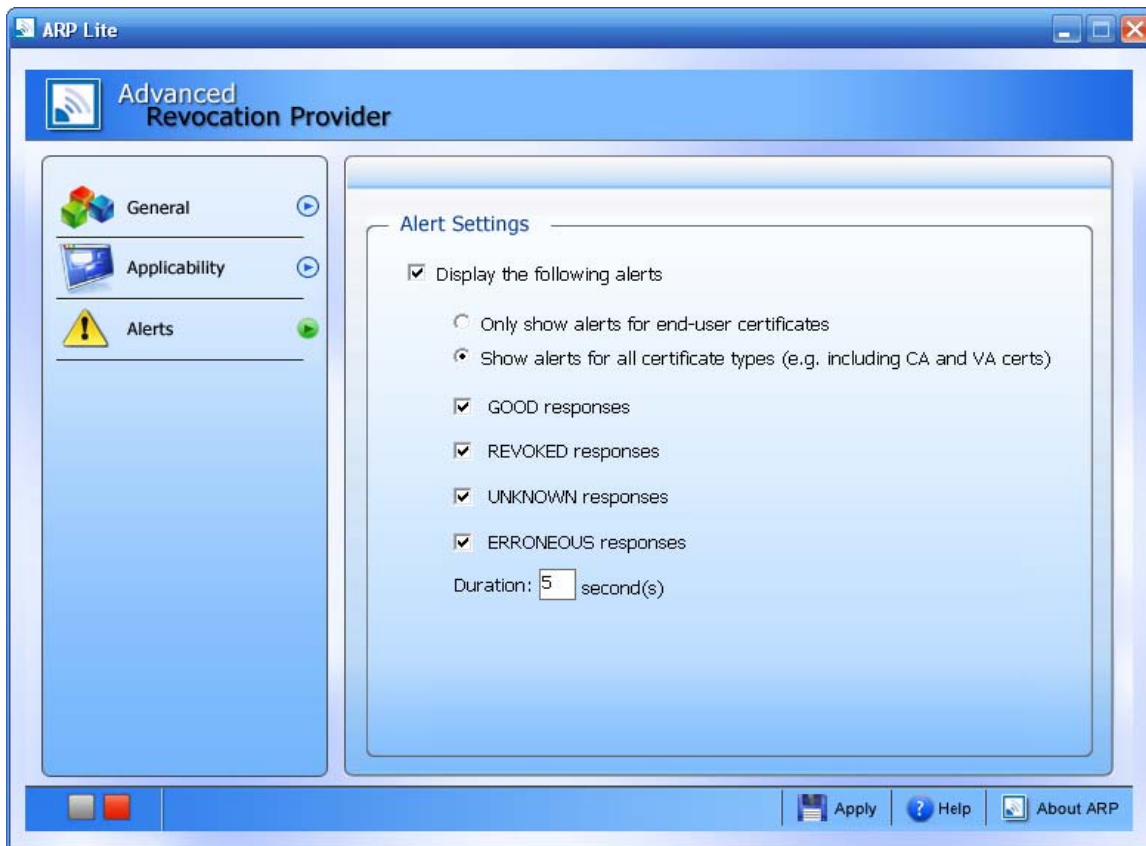
Similarly, you can also remove the name of any application that you do not want to call ARP Lite with the help of **Remove** button. Select the row that contains the name of the application in the **Applications List** and click the button **Remove**. The application will be removed from Trusted Applications List.



Like other settings, you can only set **Applicability** tab Configurations and Settings when ARP Lite is disabled.

### 3.3 Alerts Settings Pane

In Alerts settings following options can be configured:



### 3.3.1 ARP Alert Configuration

**ARP Alert Configuration:** To display different alerts on the ARP Lite machine select the checkbox against the **Display Alerts**. This will allow you to further select the different alerts that will automatically pop up on your screen. You can select all or any one of the available alerts in the **ARP Alert Configuration** section. It is recommended that the user may uncheck the option **GOOD responses** so that the user is notified only in cases other than Good responses.

**Only show alerts for end-user certificates** – If this option is checked then ARP Lite will show alerts only for end user certificates.

**Show alerts for all certificate types** – if this option is checked then ARP Lite will show alerts for all certificates i.e. End Entity, CA, and Root CA's.

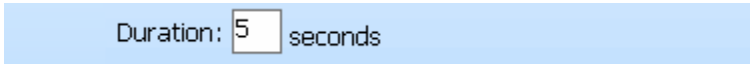
**GOOD responses** – If this option is marked then the alerts for good responses will be displayed.

**REVOKED responses** – If this option is marked then the alerts for revoked responses will be displayed.

**UNKNOWN responses** – If this option is marked then the alerts for unknown responses will be displayed.

**ERRONEOUS responses** – If this option is marked then the alerts for erroneous responses will be displayed.

**Alert Display Duration:** You can set the time duration for which a pop-up message will be displayed on your screen.

A screenshot of a configuration window showing the alert display duration. The text "Duration:" is followed by a small input box containing the number "5", and then the word "seconds".

Duration: 5 seconds

You may select not to display alerts and in that case alert settings would be grayed out and will remain disabled.

**Alert Settings**

Display the following alerts

- Only show alerts for end-user certificates
- Show alerts for all certificate types (e.g. including CA and VA certs)

GOOD responses

REVOKED responses

UNKNOWN responses

ERRONEOUS responses

Duration:  second(s)

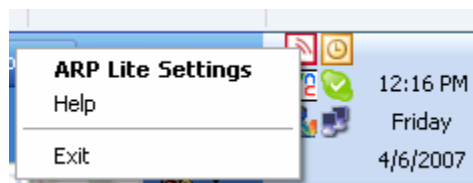
## 4 ARP Lite System Tray Menu

When ARP Lite is started, the ARP icon is shown in the system tray:



The color of the ARP icon shows its status i.e. if the color of the ARP icon is **Red** this means that ARP is Disabled and if the ARP system tray icon is in **Green** color this shows that ARP is Enabled.

By right clicking on the ARP icon in the system tray, it will display the following options



**ARP Lite Settings:** Opens up the ARP Lite Setting pane.

**Help:** Opens up the ARP Lite User Guide.

**Exit:** Exits the ARP Lite application.

## 5 ARP Lite Messages

### 5.1 Pop-Up Messages

Whenever ARP Lite processes a certificate status request, an animated ARP icon is shown in the system tray as shown below:



Once the certificate status information is determined a pop-up window is shown in the system tray:



The results in the pop-up window are as follows:

Pop-up Message Window	Detail
<b>Trust Status</b>	Specifies whether you can trust the certificate or not, i.e. the overall result. At the top of the window the Trust Status of the certificate will be shown as: <b>Trusted</b> and a <b>Green Tick mark</b> will be shown, or <b>Not Trusted</b> and a <b>Red Cross</b> will be shown. Note the Trust Status of a certificate will depend on its revocation status but also on whether the revocation status service provider can be trusted (e.g. the signature on the OCSP response is valid, the response is not expired or replayed and the responder's certificate is itself not revoked). The level of verification performed on the OCSP response message and on the responder's certificate is dependent on the configured policy. CRLs will also have a similar set of checks.
<b>Target Certificate Name</b>	This is the common name of the certificate subject taken from the target certificate. It is shown right after the Trust Status.
<b>Revocation Status</b>	Revocation status can has three values: <b>"Good"</b> symbolized with a <b>Green Tick Mark</b> (this is the result if the OCSP responder returned a "Good" response or if the certificate was not contained in the relevant CRL) <b>"Revoked"</b> symbolized with a <b>Red Cross</b> (this is the result if the OCSP responder returned a "Revoked" response or if the

certificate was contained in the relevant CRL)  
"Unknown" symbolized with a **Yellow Question Mark** (this is the result if the certificate status cannot be determined by any of the configured mechanisms)

You can also close the pop up window by clicking the cross (X) button on top-right corner of the window. By default the pop up window will disappear after the time interval specified in **Alert Settings Pane** → **Alert Display Duration**.

Example for Good and Trusted Status:



In this example the Trust Status is **Trusted** shown with a **Green Tick Mark**, the common name in the certificate is **Andy Amos**, the Revocation Status is **Good** symbolized with a **Green Tick Mark** and no **Revocation Reason** is given as the Revocation Status is Good. When a certificate Revocation result is Good and Trusted the text is shown with green color.

Example for Revoked and Not Trusted Status:



In this example the Trust Status is **Not Trusted** shown with a **Red Cross**, the common name in the certificate is **Andy Amos**, the Revocation Status is **Revoked** symbolized with a **Red Cross**. When a certificate Revocation result is Revoked and Not Trusted the text is shown with red color.

Example for Unknown Status:



In this example the Trust Status is **Not Trusted** shown with a **Red Cross**, the common name in the certificate is **Andy Amos**, the Revocation Status is **Unknown** symbolized with a **Yellow Question Mark**. When a certificate Revocation result is Unknown and Not Trusted the text is shown with red color.

## 6 How to Enable ARP in Windows Applications

In certain Microsoft® applications certificate status checking is switched off by default, therefore you need to perform some basic configuration before certificate status checking is enabled and ARP can be invoked. Note that, in such cases when in default mode, even the basic Microsoft CRL-based revocation handler will not be invoked until you make the necessary settings. The following table highlights the settings that need to be made in various applications:

Application Name	Settings in Windows Application
Outlook Express 5.0 and above	Run the program and select <b>Tools &gt; Options &gt; Security tab &gt; Advanced</b> . In Revocation Checking section select the option <b>Only when Online</b>
Outlook 2000 with SR-1	Revocation checking enabled by default
Outlook 2002 / 2003	Revocation checking enabled by default
Word 2002 / 2003	Revocation checking enabled by default
Internet Explorer 5.0 and above	Run the program and select <b>Tools &gt; Internet Options &gt; Advanced</b> tab. In <b>Security</b> section check the following check box: <b>Check for server certificate revocation (requires restart)</b>
Microsoft Certificate Server v2.0	Revocation checking enabled by default
Microsoft CAPI Enabled	ARP Lite can be invoked by any application that is Microsoft CAPI enabled.

If you require further information, you should consult the Microsoft application help file or Ascertia [support](#). To know more about how you can enable other applications e.g. Adobe Acrobat, MSN messenger, Office applications, Windows logon, IIS please read the ARP test drive pages on the Ascertia website <http://www.ascertia.com>

## 7 Appendix

Following is the list of messages which ARP Lite will generate in case a problem arises.

### 7.1 General Error messages

Message No.	Reason	Error Message String
Msg001	If Evaluation Key File is missing	Invalid EKF File- Bad path or file does not exist.
Msg002	If Branding file is missing.	The Branding file is missing.
Msg003	If ARP Lite General Pane registry settings are missing	Settings have been corrupted. Please contact administrator or re-installing the application may fix the problem.
Msg004	If ARP Lite Applicability Pane registry settings are missing	Settings have been corrupted. Please contact administrator or re-installing the application may fix the problem.
Msg005	If ARP Lite Alerts Settings Pane registry settings are missing	Settings have been corrupted. Please contact administrator or re-installing the application may fix the problem.
Msg006	If evaluation period has expired.	License Expired

### 7.2 General tab messages

Message No	Reason	Error Message String
Msg001	If no row is selected.	Please select some row to move up.
Msg002	If no row is selected.	Please select some row to move down.

### 7.3 Applicability tab messages

Message No	Reason	Error Message String
Msg001	If no row is selected	Please select a row from the table to remove.
Msg002	Confirmation in case an application is intended to be deleted	Do you want to remove the selected application?

Msg003	If you have reached the maximum application limit.	You have reached the maximum application limit. You can not add more than 20 applications.
Msg004	If there are no rows in the table.	There is no row in the table to remove.

## 7.4 Alert Settings tab messages

Message No	Reason	Error Message String
Msg001	If invalid value is entered in "Alert Display Duration"	Please enter a valid value for "Alert Display Duration" e.g. 5. Valid field range : 0 to 60

## 8 Frequently Asked Questions

If you want to have more information regarding ARP or facing a problem running ARP then have a look at following ARP Frequently Asked Questions. For more information, visit [www.ascertia.com](http://www.ascertia.com).

### 8.1 I have a signed email in Outlook Express and Outlook 2000 but ARP is not invoked?

Invocation of ARP is based upon the parent application i.e. Outlook Express, Internet Explorer etc. Note that in Outlook Express it is necessary that the signed emails certificate contains a [CDP](#) extension otherwise ARP will not be launched. In case of Outlook 2000/2002 this is not necessary. Also ensure that ARP is enabled. In Outlook Express you also have to enable revocation checking in order for ARP to be called, see below:



### 8.2 I have a signed email, where the certificate has a valid CDP extension but ARP is still not invoked?

Try re-starting your application. If this does not work, try re-starting your machine.

### 8.3 I am setting the Responder URL and Port but ARP seems not connecting to the Responder?

Make sure the Responder is running at a given address and you have typed in the correct URL i.e. [www.globaltrustfinder.com](http://www.globaltrustfinder.com), <http://ocsp.globaltrustfinder.com>, 196.168.0.6, or machine name (e.g. testing-4). Also make sure you are running the correct communication protocol, i.e. if server is listening on [SSL](#) then ARP should use SSL and vice versa. Do also check if you have configured your proxy settings correctly.

Before using ARP you should also consider the following points:

- 1) If the [OCSP](#) responder is running locally then you should not use a proxy, i.e. un-check *connect using a proxy server* because if proxy is down then ARP will not be able to connect to the OCSP Responder.
- 2) If you are behind proxy and you need to connect to an OCSP responder running online (on the Internet), you should enter the Proxy Server Address and port number
- 3) If you are using an online OCSP responder as well as a local OCSP Responder, and if you do not want to go through a Proxy for local OCSP responder traffic then uncheck *By pass Proxy for local (intranet) address*. If this is enabled it will only slow things down as requests will be sent to Proxy machine then routed to the target OCSP Responder

### 8.4 I am trying to connect to an SSL based server but I am getting Error in Connection messages?

Make sure an SSL based server is running where you are sending the OCSP Requests. SSL communication with an OCSP responder depends on whether or not you have specified a full address for the OCSP responder (including HTTP/HTTPS part) and whether or not the setting for SSL within ARP is enabled. There are various scenarios:

- 1) If the OCSP responder URL contains [www.globaltrustfinder.com](http://www.globaltrustfinder.com) OR <http://ocsp.globaltrustfinder.com>, OR just a machine name (e.g. ocsp-test3) then the OCSP Requests will be sent as plain (without SSL)
- 2) If the OCSP responder URL contains HTTPS in the URL (e.g. [www.globaltrustfinder.com](https://www.globaltrustfinder.com) OR <https://ocsp-test3>) then OCSP Requests will be sent using SSL
- 3) If the OCSP responder URL contains no HTTP (e.g. ocsp-test3 or [www.globaltrustfinder.com](http://www.globaltrustfinder.com)) but the *Use SSL* is checked within ARP then OCSP Requests will be sent using SSL pipe
- 4) If the OCSP responder URL contains no HTTP (e.g. ocsp-test3 or [www.globaltrustfinder.com](http://www.globaltrustfinder.com)) but the *Use SSL* is not checked within ARP then OCSP Requests will be sent as plain (without SSL)

The following table illustrates all the different scenarios:

	SSL Setting in ARP	
	SSL not enabled	SSL Enabled

<b>OCSP responder Address</b>	<b>Specifies HTTP</b>	Not SSL	Not SSL
	<b>Specifies HTTPS</b>	SSL	SSL
	<b>Does not specify either</b>	Not SSL	SSL

## 8.5 I have configured ARP to check the revocation status of OCSP responder's certificates, but ARP does not do this, why?

ARP may not be checking the OCSP responder certificate status due to one of the following reasons:

- 1) The OCSP responders' certificates contain a noCheck extension or this certificate is present in your trust anchor list
- 2) ARP has either failed to verify the signature on the OCSP message correctly. In such case ARP will not go for revocation status check of Responders certificate. The reason being, if the response cannot be trusted in the first place, what is the point of checking the status of the responders certificate?

## 8.6 ARP keeps my PFX file password saved, is it saved encrypted?

Yes, ARP encrypts the PFX file password before saving it on the permanent storage. Your PFX password will not be visible in plain form.

## 8.7 I am trying to uninstall ARP but am unable to?

Make sure any Microsoft application, which uses ARP, is not currently running. It is necessary to close such applications (e.g. Internet Explorer, Outlook Express or Outlook 2000/2002 etc.), as they will have loaded ARP. Closing these applications will unload ARP and it can now be uninstalled afterwards.

If a Crypto application e.g. Outlook Express etc is using ARP and you try to uninstall ARP following dialog is shown:



Make sure you close all applications, which are using ARP before uninstallation and click *Retry* to resume the uninstallation. If this message is still shown, click *Don't display this message again* and click *Reboot* button. Such dlls will be removed on your reboot. It is a **MUST** to reboot after such operation.

## 8.8 I am using a proxy server to connect to an OCSP responder. I have configured proxy correctly. I am not able to connect to the OCSP responder on local intranet if proxy server is down?

When using proxy server, it is highly recommended that you check the *By pass proxy server for local (intranet) addresses* checkbox. So ARP will not go to proxy server while communicating with the local address(es). In that case, even if the proxy server is down, ARP can still connect to intranet address(es). It is also worth noting that ARP considers addresses as local ones, if and only if, the address does NOT contain a dot/period in its name (e.g. responder-machine1).

## 8.9 I have configured ARP to sign OCSP request and have selected a Personal Information Exchange (pfx/pkcs#12) file in ARP, but the request generated is not being signed?

There could be one of the following reasons for not signing:

- 1) The signing certificate might have expired. ARP currently DOES NOT give you a warning if your signing certificate is expired, but if the signing certificate has expired then ARP will not be able to sign the OCSP request.
- 2) Make sure the pfx/ [pkcs](#) #12 file is present where it was selected and you have sufficient privileges to access the file. If file is present on a network path or removable media, then make sure that the network path still exists and the removable media is present when trying to generate an OCSP request. Also ARP does not make a copy of your Personal Information Exchange (pfx/pkcs#12) file for security reasons.

## 8.10 Can more than 1 Revocation Provider be used simultaneously?

Yes, MS Crypto Application use CRL based revocation by default. On Installing ARP the CRL based revocation can be removed. If you do not remove this then it will be called depending upon the response from ARP. Calling of CRL based revocation is depending upon the Crypto Application.

ARP shows certificate status as	CRL based Revocation called
Good	No
Revoke	No
Unknown Signature Required Connection Failure Try Later	Yes

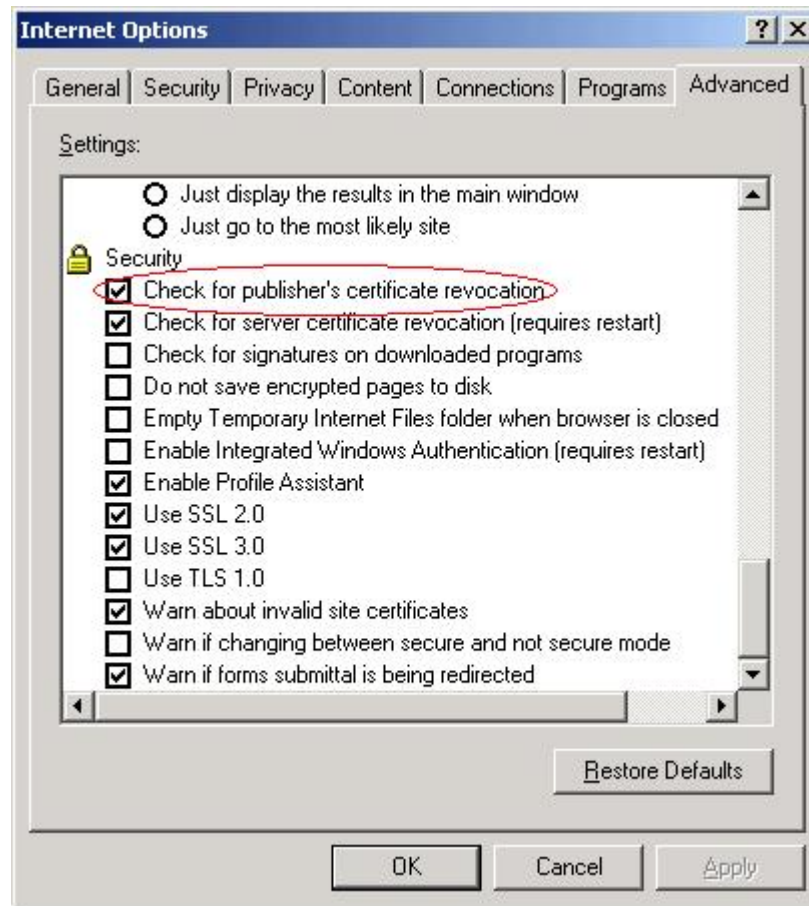
To date we have tested the above functionality on following applications:

- 1) Outlook Express 5.0/6.0
- 2) Outlook 2000 SR-1
- 3) Outlook 2002

As an example if ARP returns unknown and the default CRL based revocation provider returns revoked then the calling application will get a result of revoked for the certificate.

## 8.11 ARP seems to be called when opening 3rd party applications i.e. ACDSee or Network Neighborhood why?

ARP Revocation Provider is a DLL, which can be called by Microsoft or Third Party crypto applications. There might be a number of other applications, which might call ARP for checking revocation of certificates. To remove this feature open IE, and from the Internet Options uncheck the option Check for publisher's certificate revocation as below:



## 8.12 How Outlook Express 5.0/6.0, Outlook 2000/2002 and IE respond when ARP shows the results?

Good question! Well all of the above applications have slightly different ways of showing the response when ARP hands control back to the calling application.

Wherever possible you should rely on the results window of ARP. This provides the most accurate, clear and detailed results possible.

Microsoft applications do not distinguish between certificate status of good or unknown, this is mainly because they were built with CRLs in mind. This is a good reason on why you should instead rely on the results provided through the ARP window.

There are a number of different cases, which need to be considered:

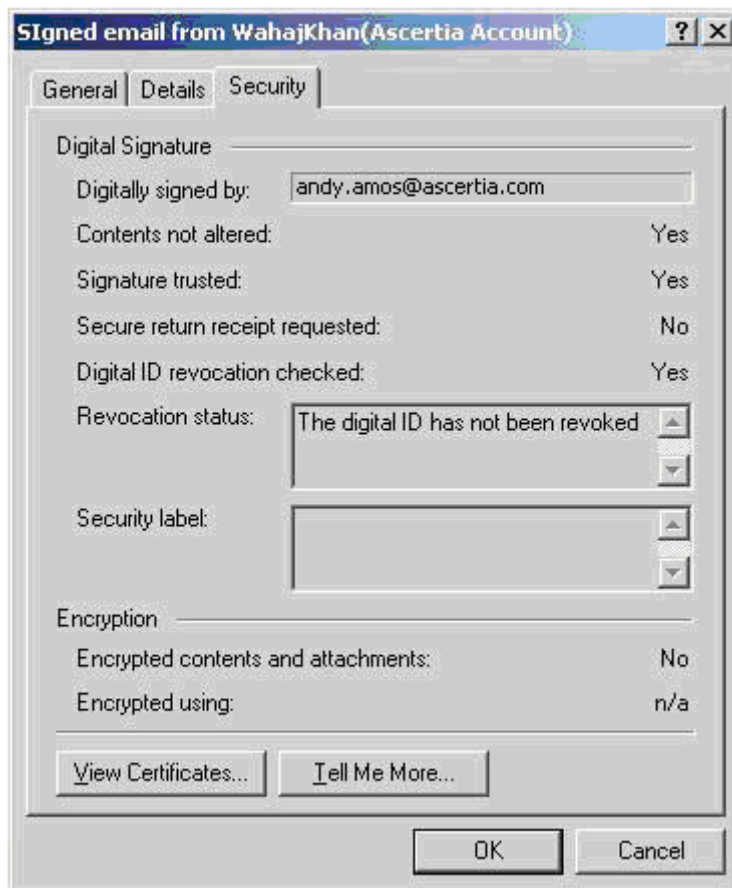
- Case 1:** ARP Result Window: Trusted, Certificate Status: good
- Case 2:** ARP Result Window: Not Trusted, Certificate Status: good  
(Not Trusted may have been returned because some other check failed e.g.

- Replay Check failed)
- Case 3:** ARP Result Window: Not Trusted, Certificate Status: unknown
- Case 4:** ARP Result Window: Not Trusted, ARP unable to connect to OCSP Responder
- Case 5:** ARP Result Window: Not Trusted, Lite is not authorized to use OCSP Responder
- Case 6:** ARP Result Window: Not Trusted, Certificate Status: revoked

The following are the details of how each application behaves in the above cases:

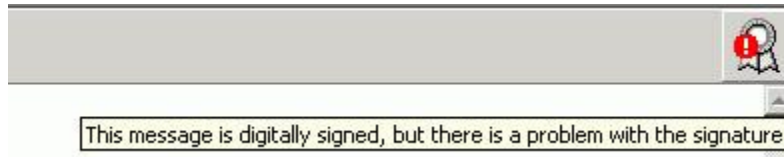
**Outlook Express 5.0**

If ARP results window shows the overall result as Trusted this means that the certificate status is good and all other checks performed have passed successfully. On opening such windows the following dialog is shown:

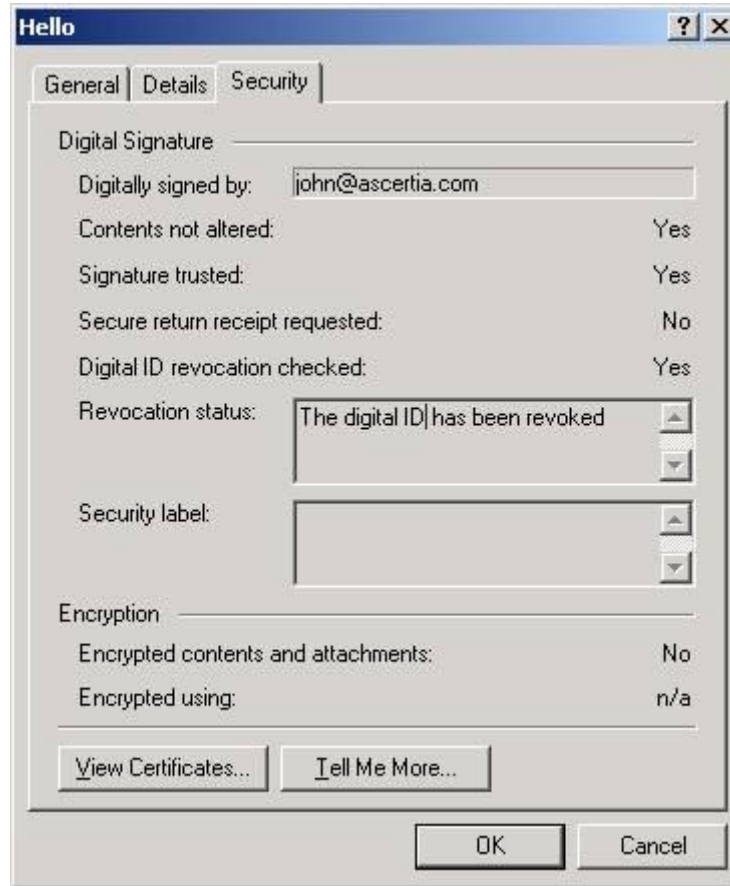


If ARP is unable to connect to OCSP responder or there is a problem in the OCSP Request, Outlook Express will still show the above dialog (case 2-5).

For case 6, on clicking a signed email having a revoked certificate, the following pre-view window is shown (assuming the preview pane is enabled):

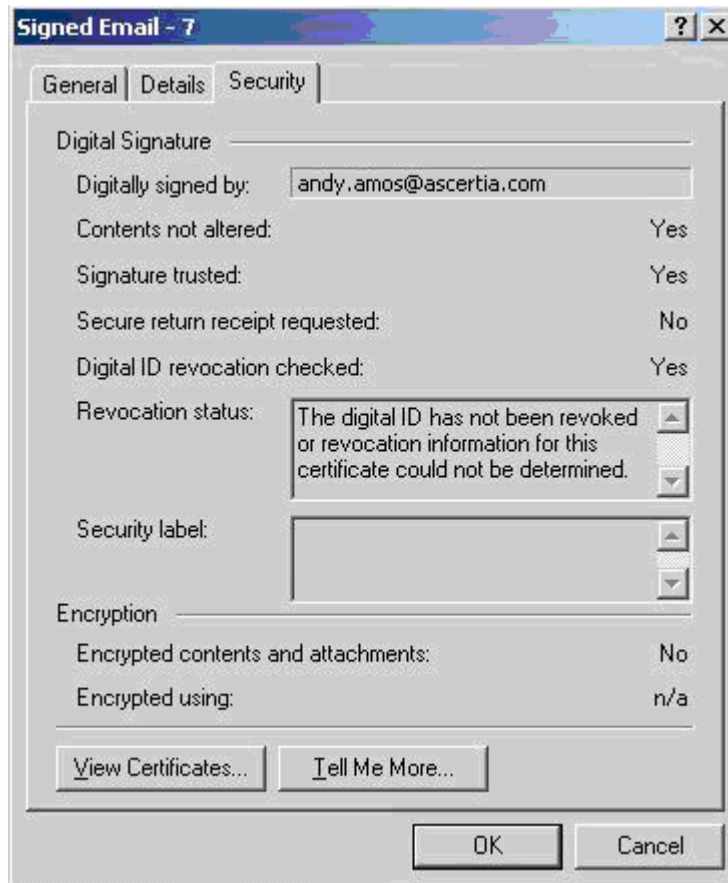


If the certificate status is revoked then on opening the email, following dialog is shown:



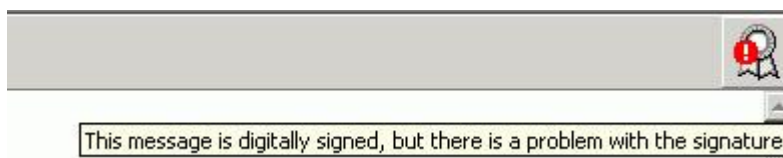
**Outlook Express 6.0**

For Case 1 the following dialog is shown in Outlook Express 6.0:

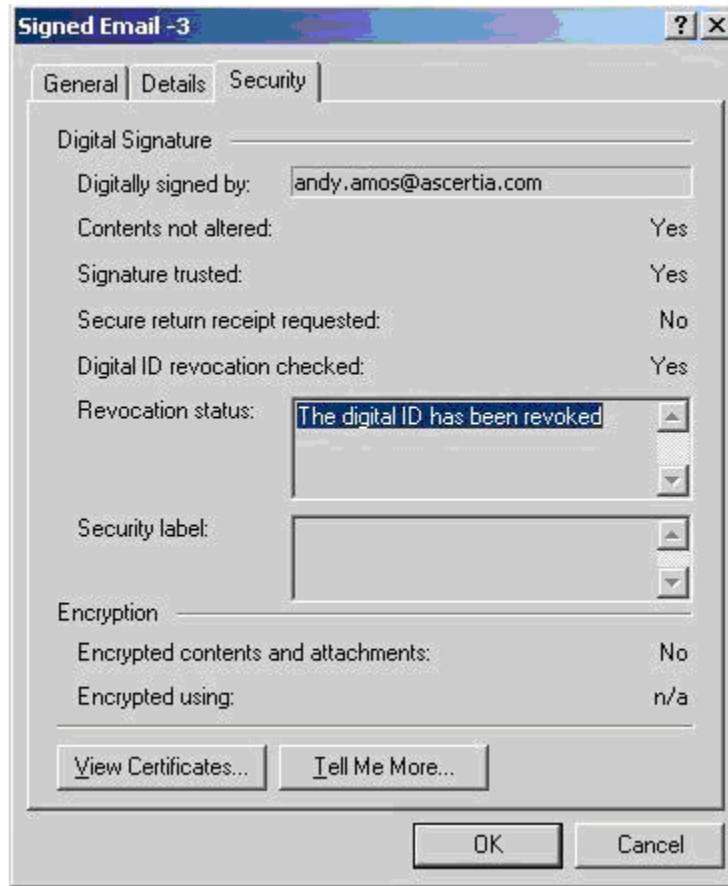


If ARP is unable to connect to OCSP responder or there is a problem in the OCSP Request, Outlook Express will still show the above dialog (case 2-5).

For case 6, on clicking a signed email having a revoked certificate, the following pre-view window is shown (assuming the preview pane is enabled):



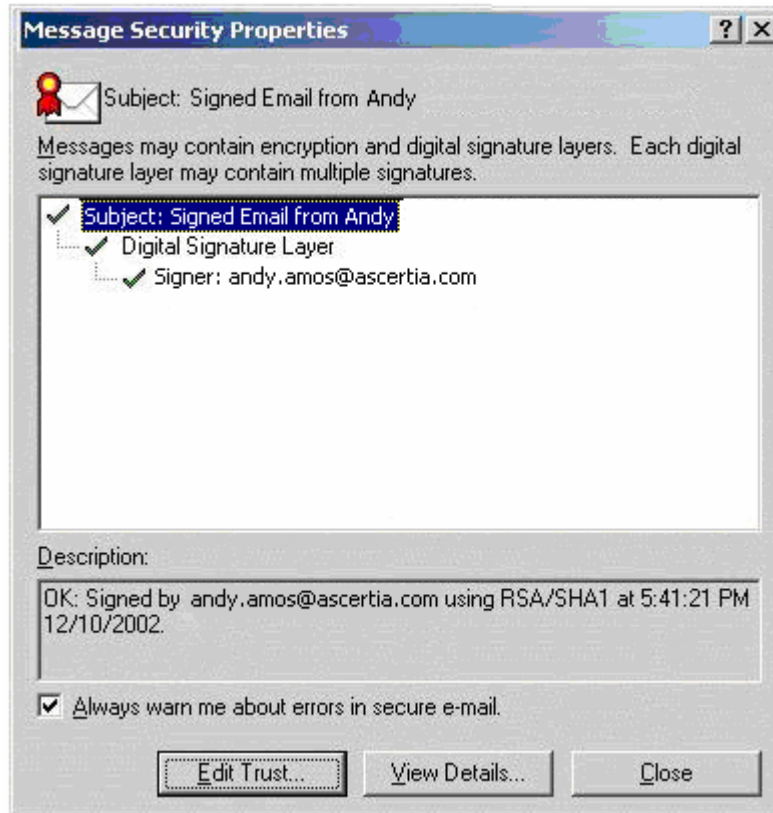
If the certificate status is revoked then on opening the email, the following dialog is shown:



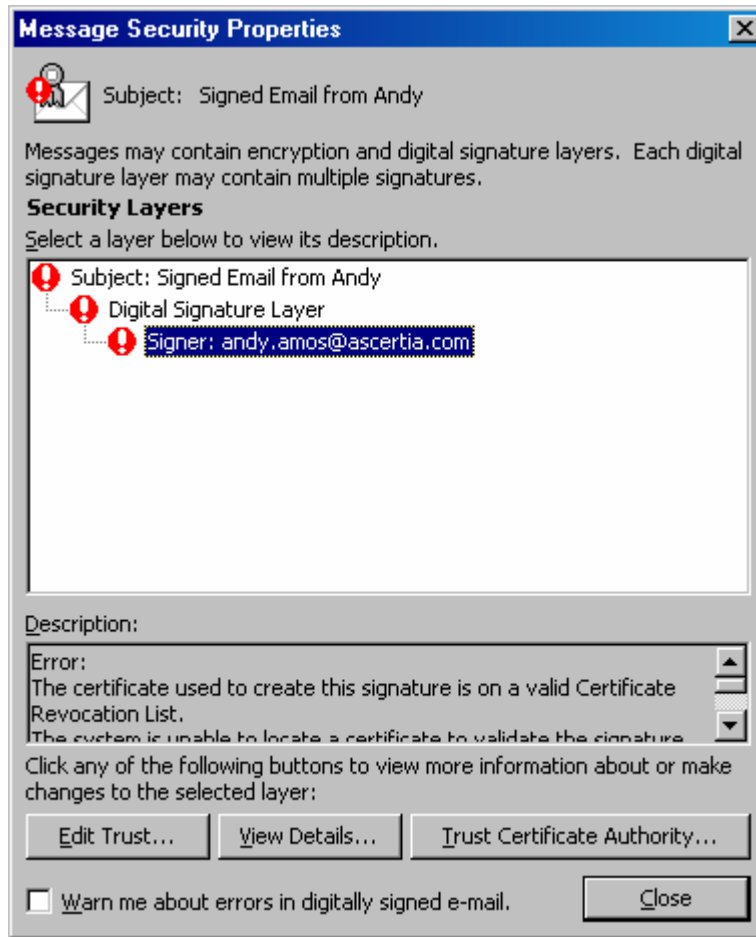
**Outlook 2000**  
**Outlook 2000 build 3821 (Updated after installing SR-1)**

Certificate Status: Good or Unknown:

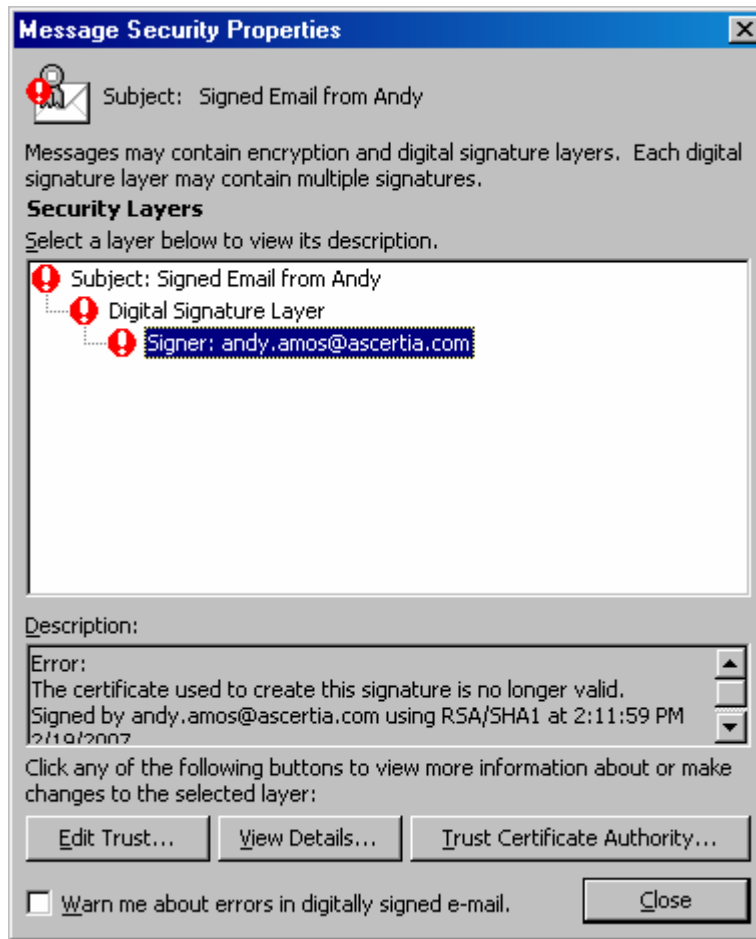
Also in case ARP is unable to connect to Responder then still the following dialog is shown:



Certificate Status: Revoked



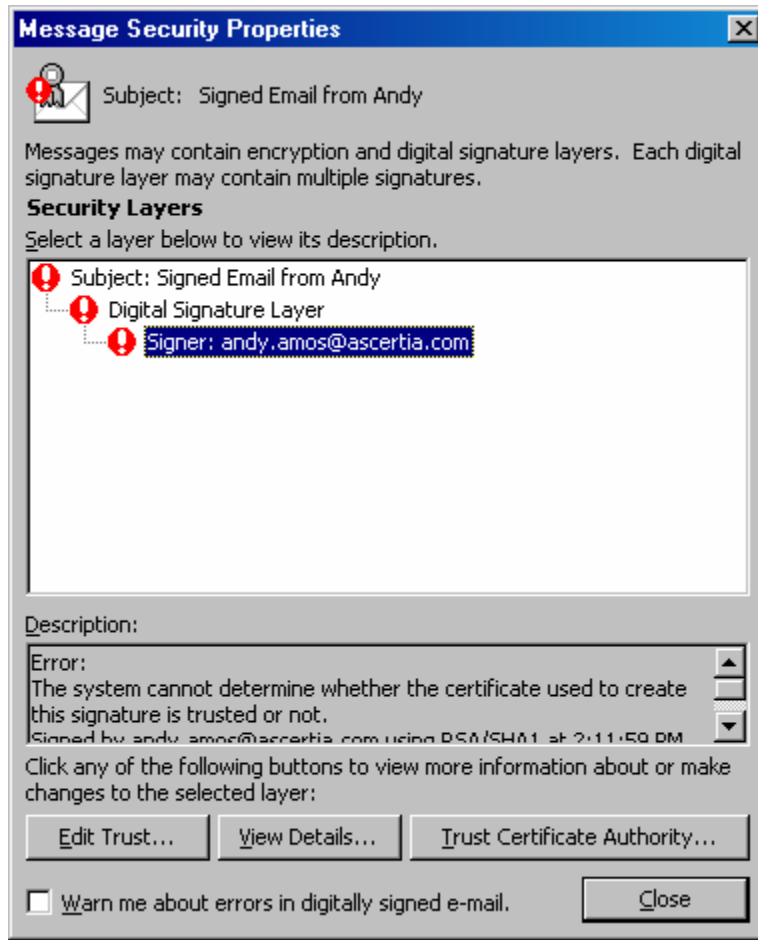
Certificate is Expired



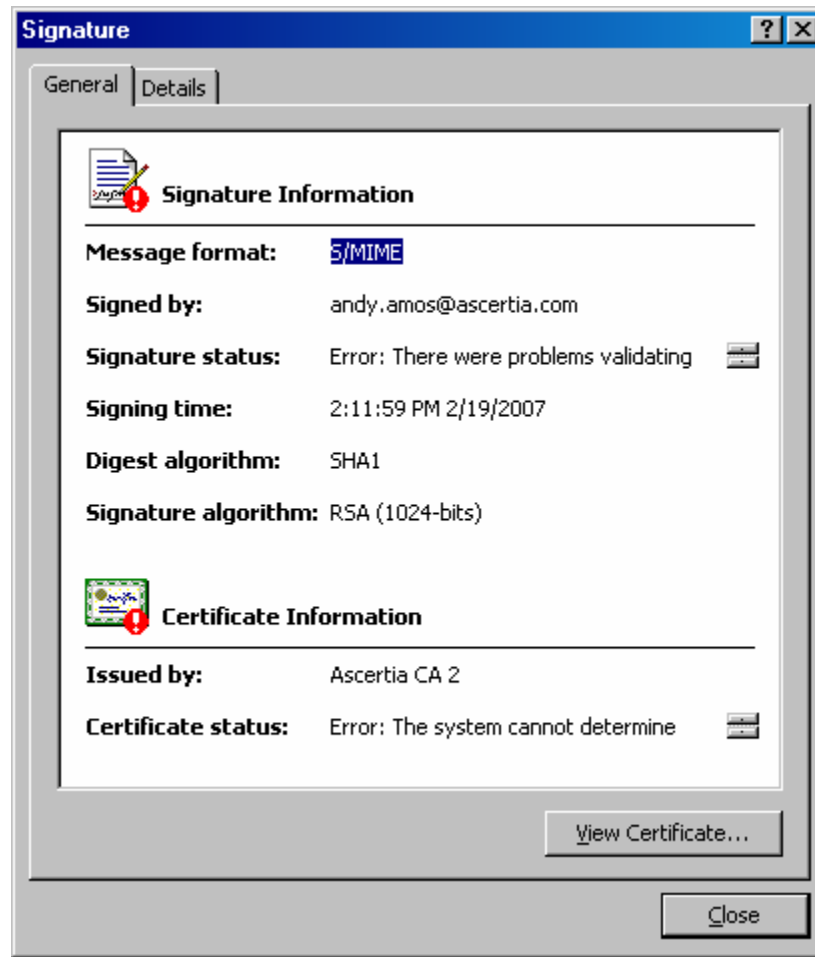
**Outlook 2000 build 5414 (Updated after installing SR-1, SP2 and Email-Security Update)**

Certificate Status: Good but Issuer certificate of target is not explicitly trusted

Also in case ARP is unable to connect to Responder then still the following dialog is shown

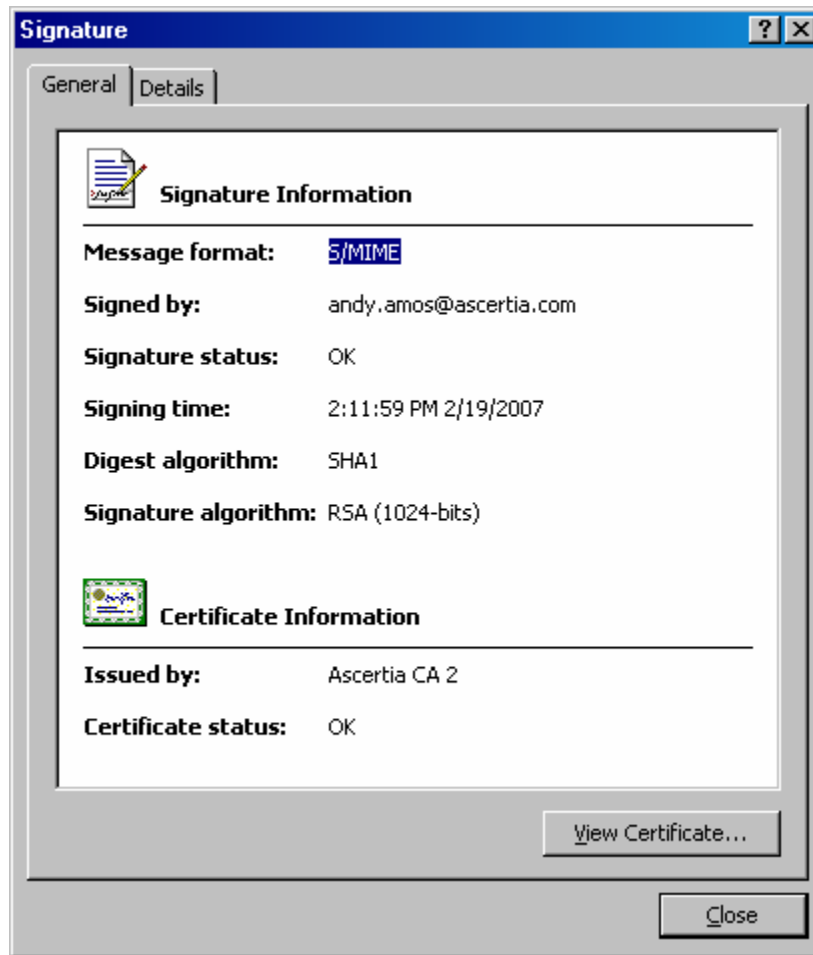


If message is viewed and is clicked following window is shown:

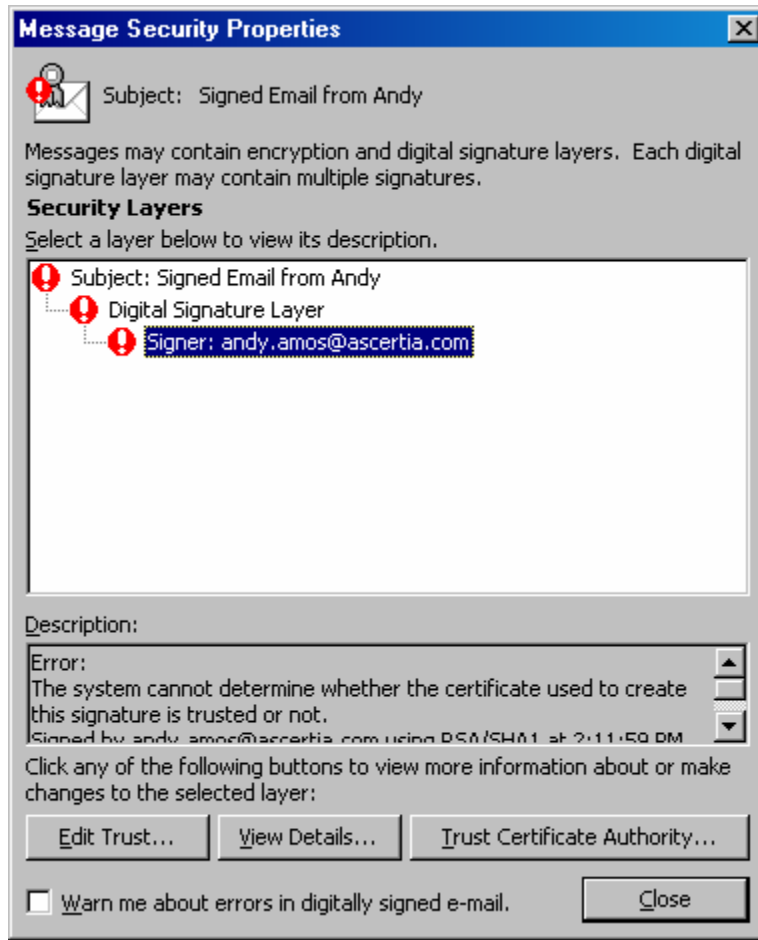


Certificate Status: Good but Issuer certificate of target is explicitly Trusted

Also incase ARP is unable to connect to Responder and Issuer certificate of target is explicitly trusted then still the following dialog is shown

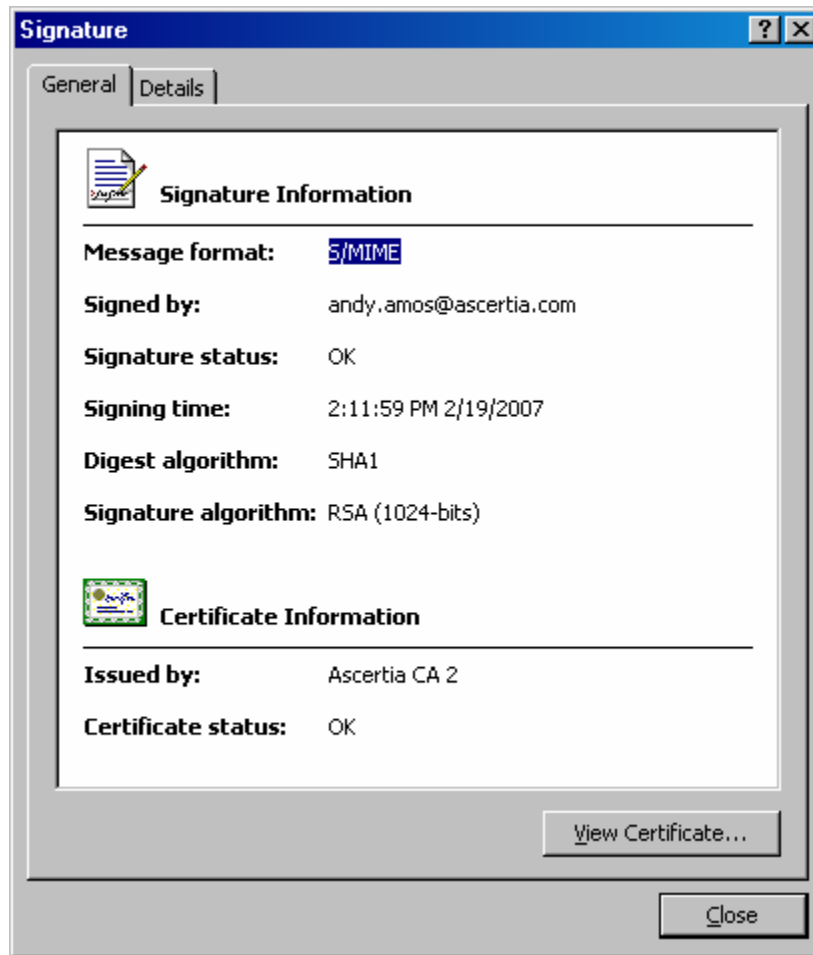


Certificate Status: Unknown but Issuer certificate of target is not explicitly trusted

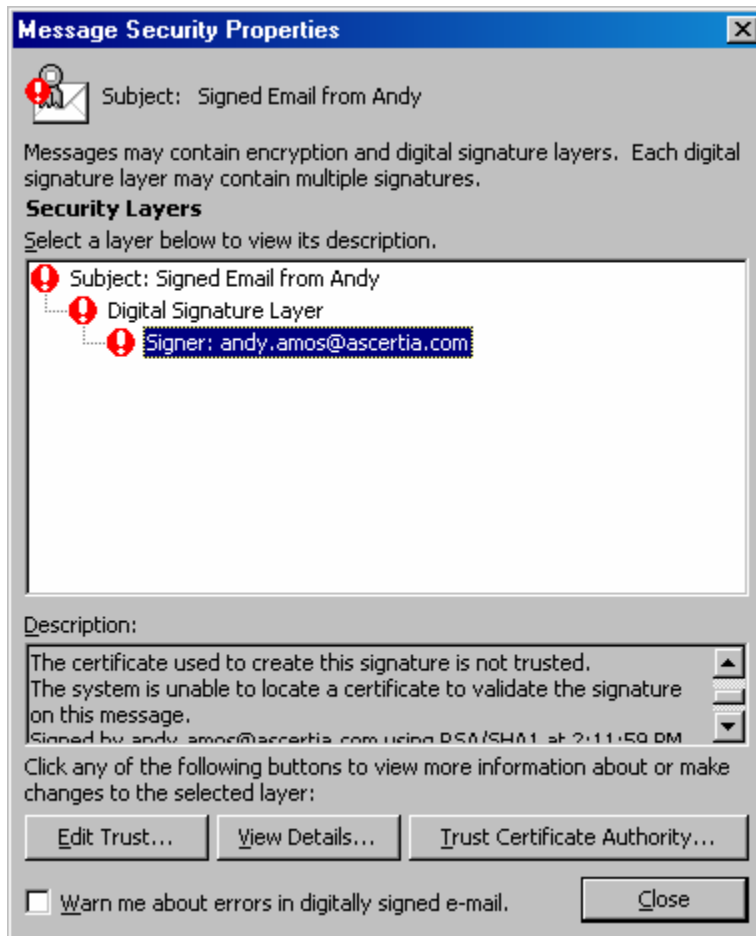


Certificate Status: Unknown but Issuer certificate of target is explicitly trusted

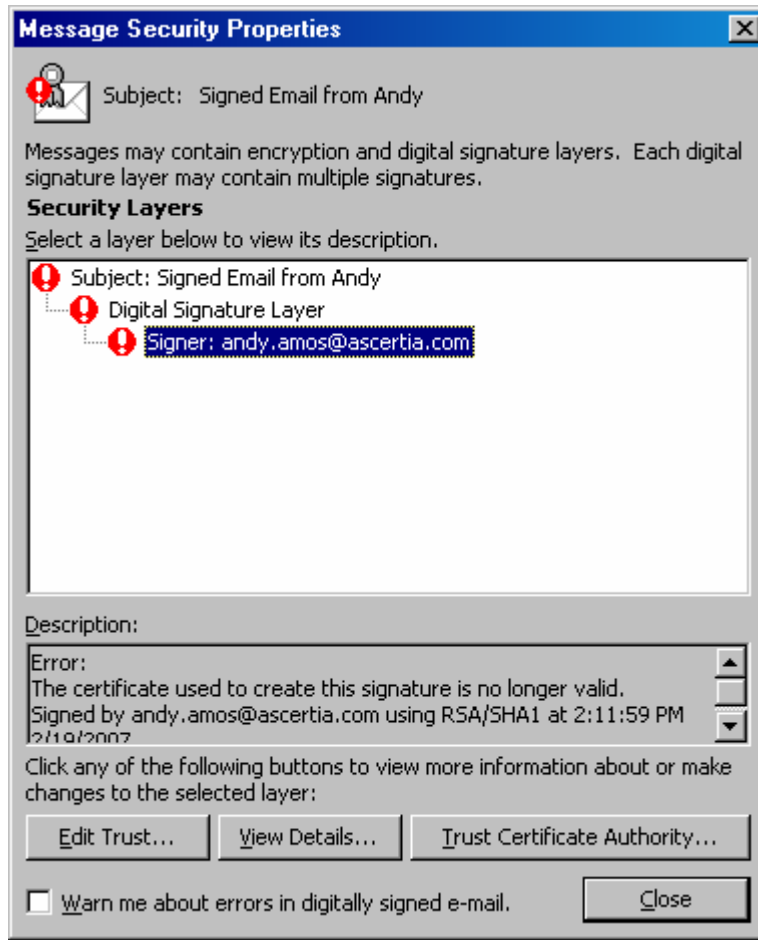
Also incase ARP is unable to connect to Responder and Issuer certificate of target is explicitly trusted then still the following dialog is shown



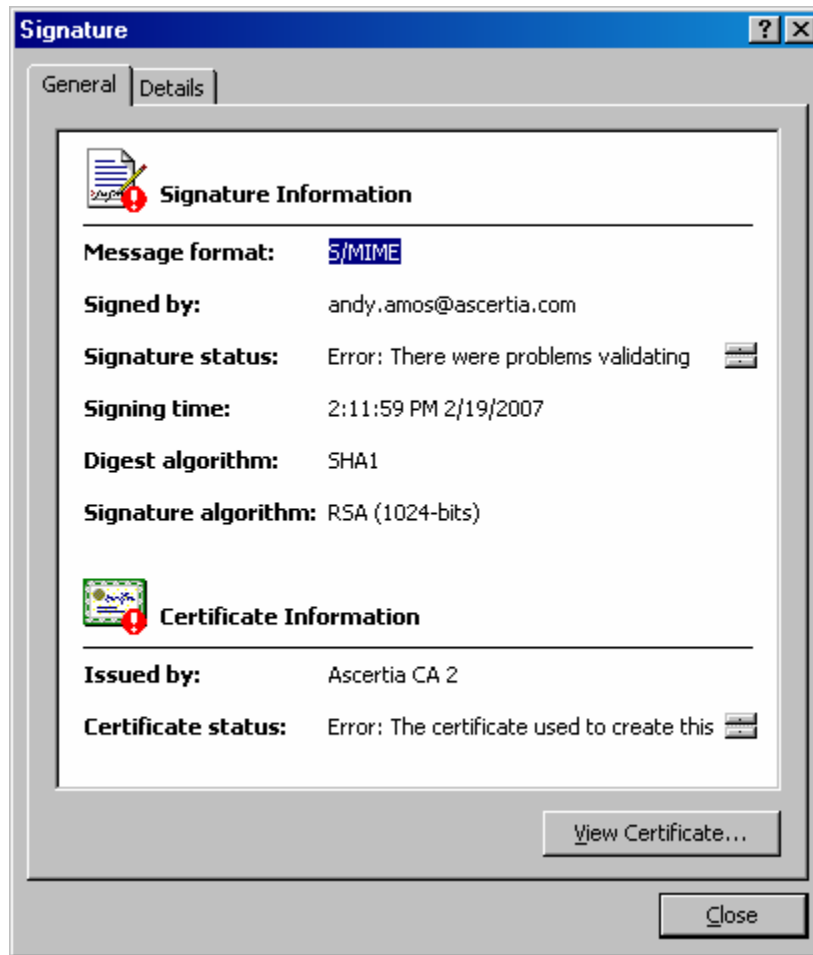
Certificate Status: Revoked whether Issuer certificate of target is explicitly trusted or not



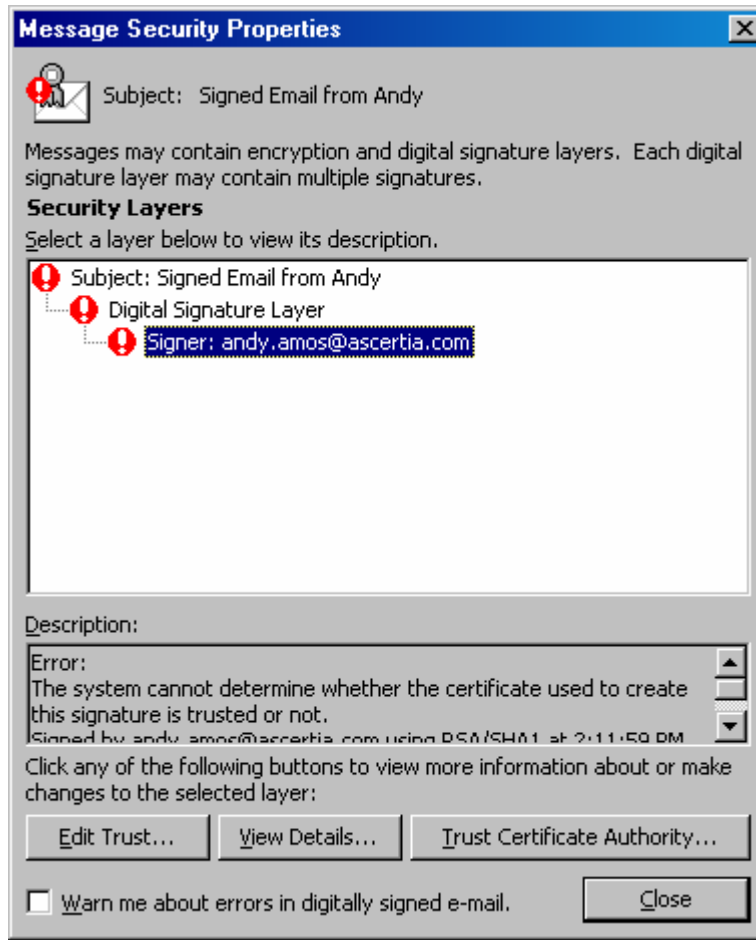
Certificate Status: Expired whether Issuer certificate of target is explicitly trusted or not



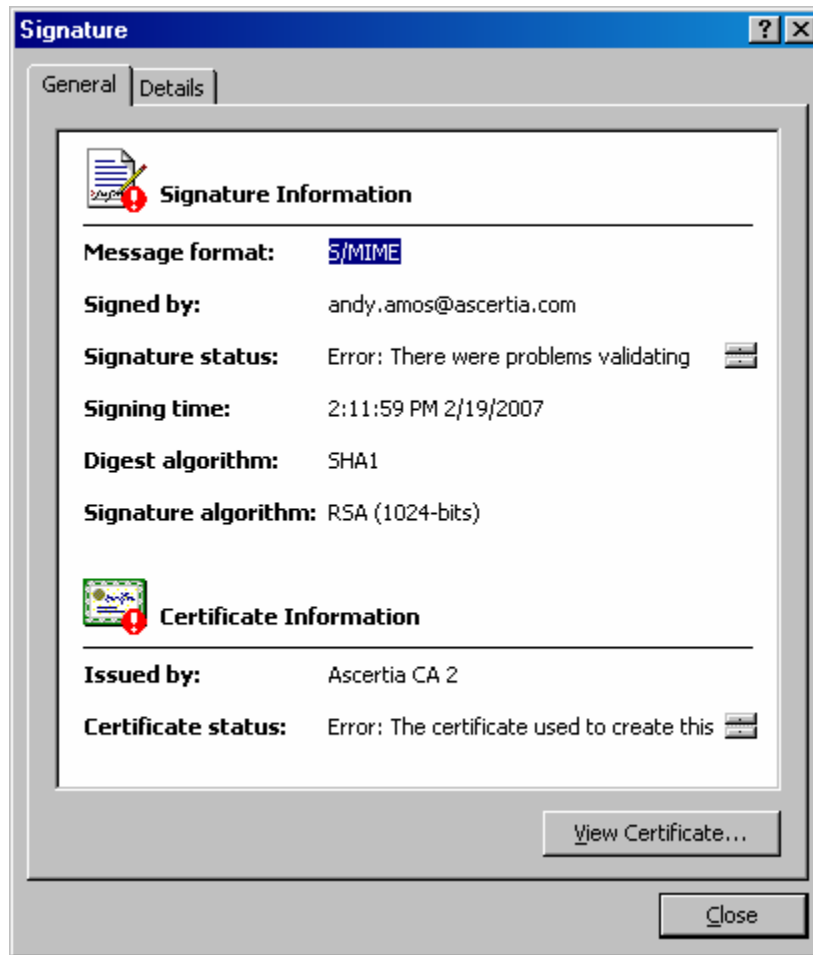
If message is viewed and is clicked following window is shown:



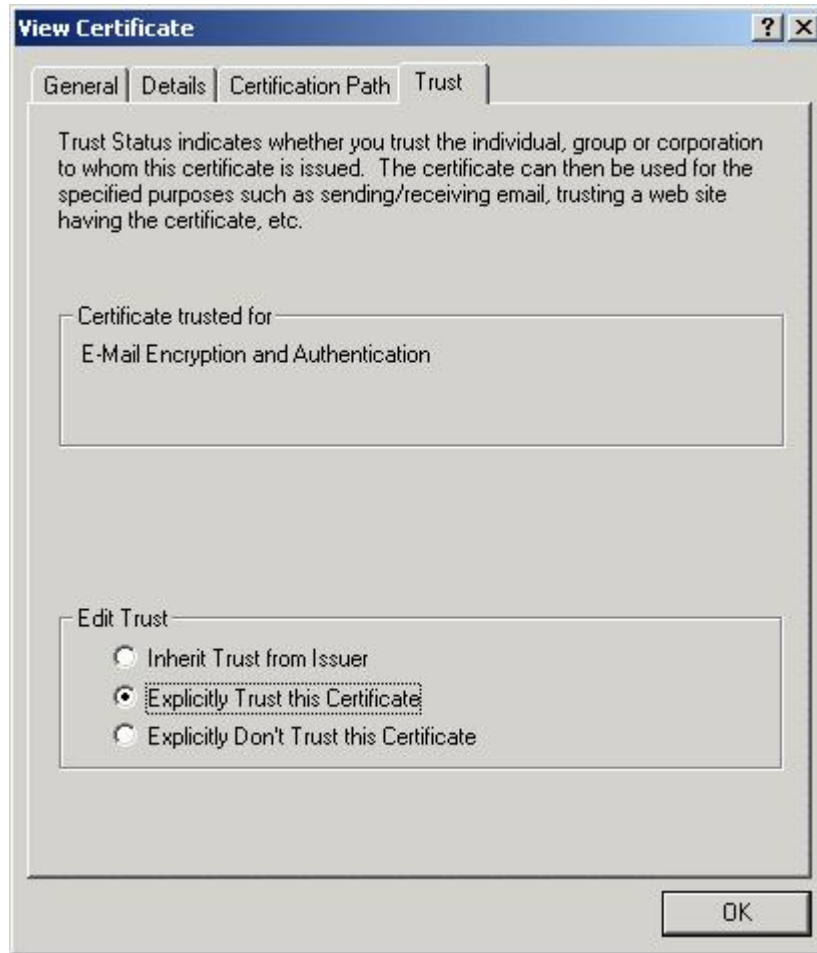
If some how the email do not contain a valid certificate i.e.



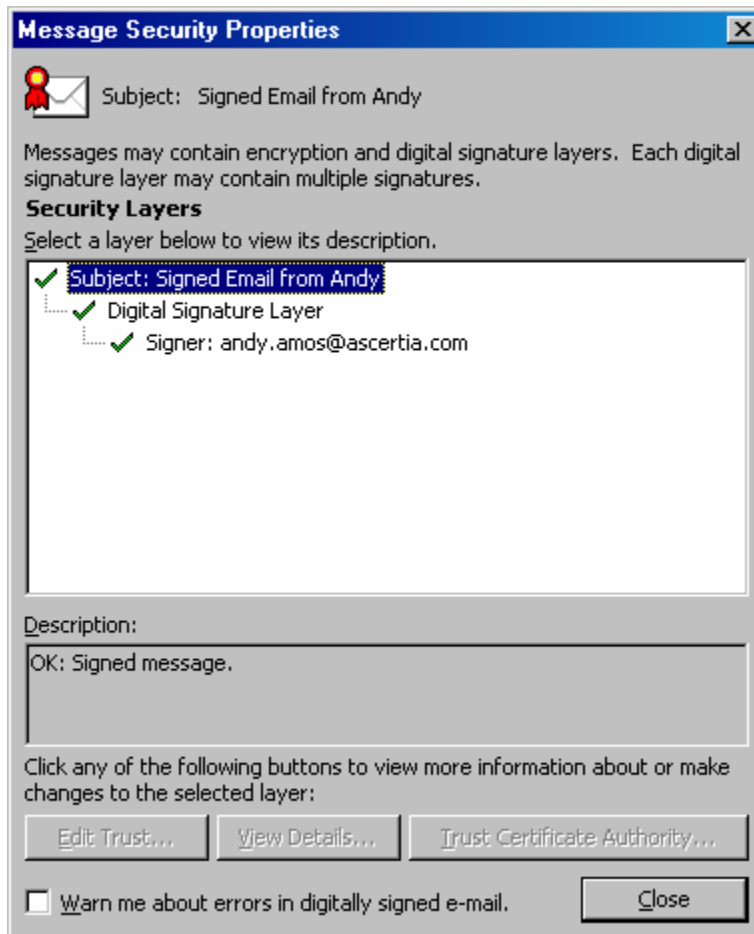
If message is viewed and is clicked following window is shown:



If a certificate is trusted explicitly by clicking Edit Trust button provided the certificate is not expired or revoked:

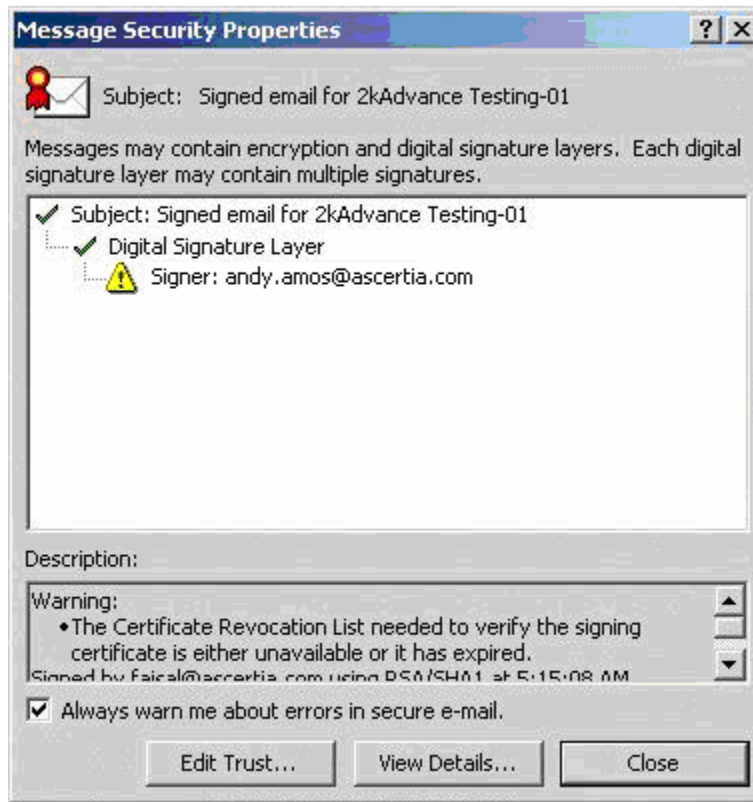


Then following dialog is shown:



**Outlook 2002**  
**Installed from Office 2002**  
 Certificate Status: Good or unknown


Also in case ARP is unable to connect to Responder then still the following dialog is shown:



If Signer certificate is explicitly trusted than the exclamation mark is removed

Certificate Status: Revoked

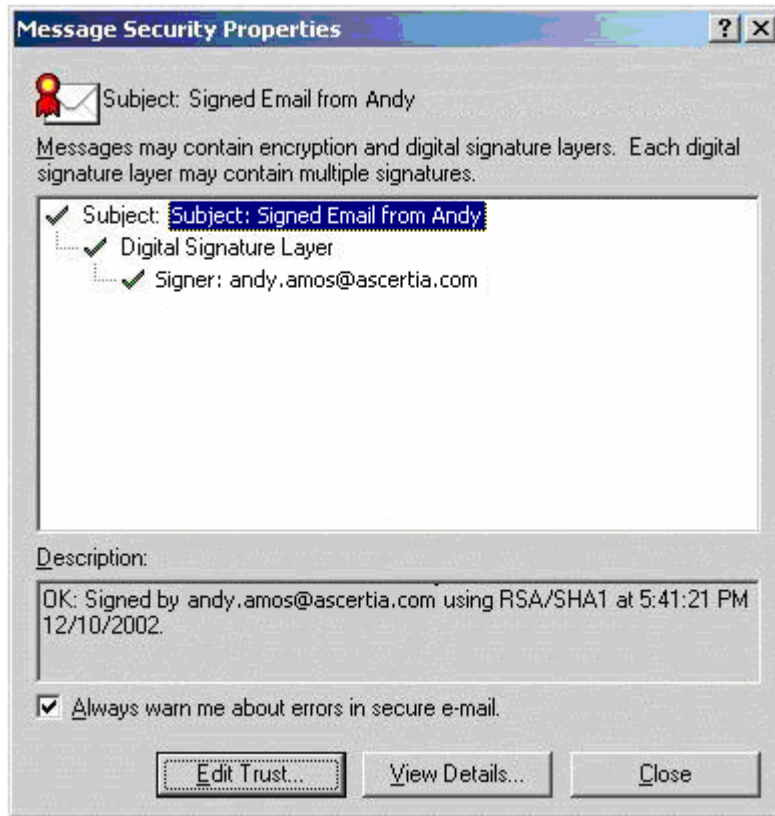


	<p>Explicit trust of Issuer certificate means the Issuer certificate is in Certificate store of IE where explicit trust of Signer means clicking Edit Trust button and clicking Explicitly Trust this certificate. Almost in all cases the Issuer certificate should be trusted in IE Certificate store other wise following message will appear "The system cannot determine whether the certificate used to create the signature is trusted or not" <b>OR</b> "Certificate not Trusted"</p>
---	---

**Outlook 2002 build 10.2627.2627 Installed from Office XP**

Certificate Status: Good or unknown

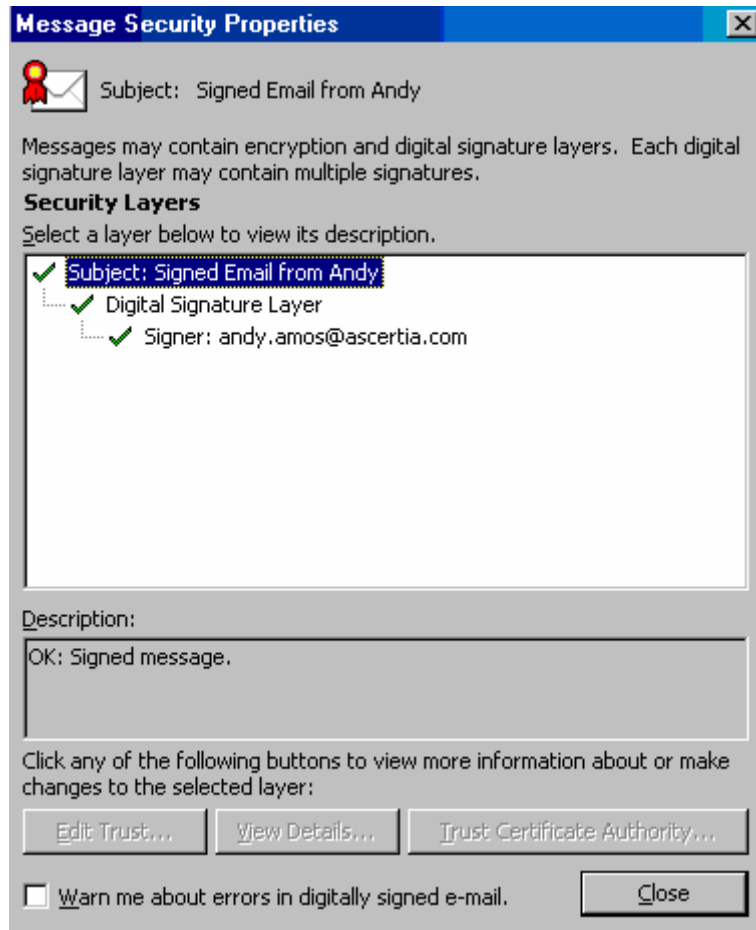
Note that in versions of Outlook 2000 or Outlook 2002 we get an exclamation mark with Signer certificate.



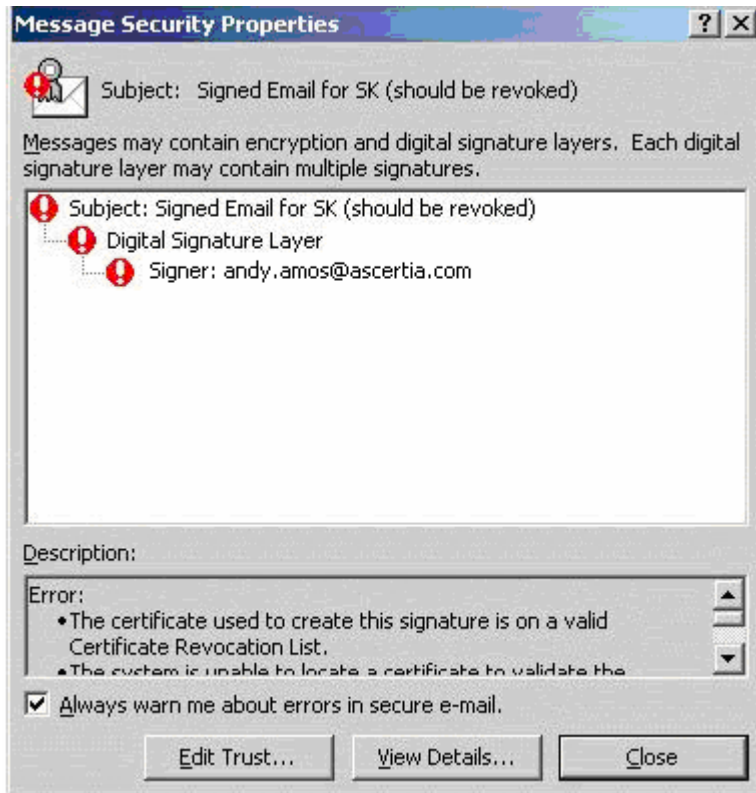
There is a known issue that in case ARP is unable to connect to Responder then one of the following dialogs is shown:



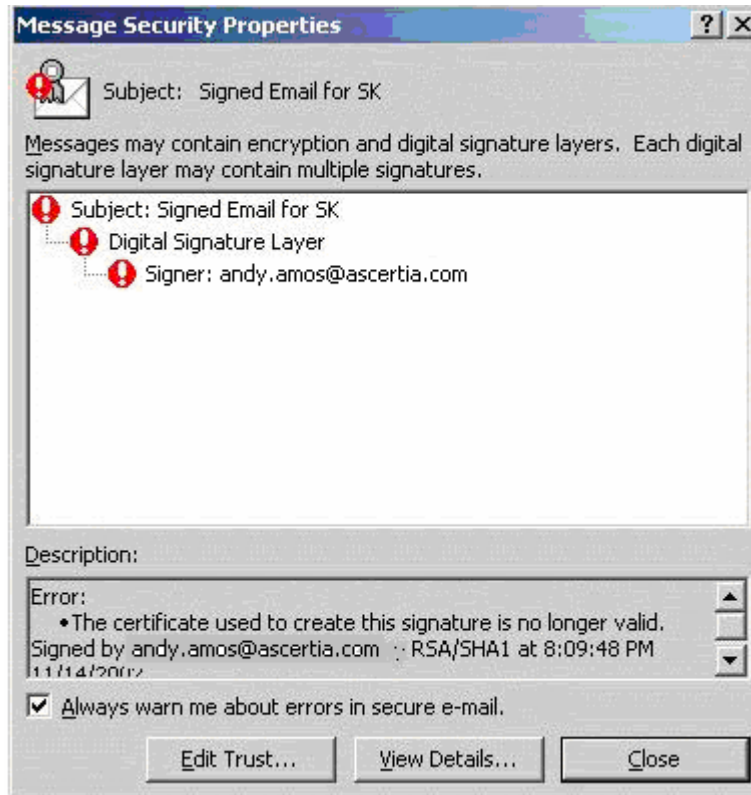
OR



Certificate Status: revoked



Certificate Status: Expired



**Outlook 2002 build 10.2627.3311 Installed from Office XP**

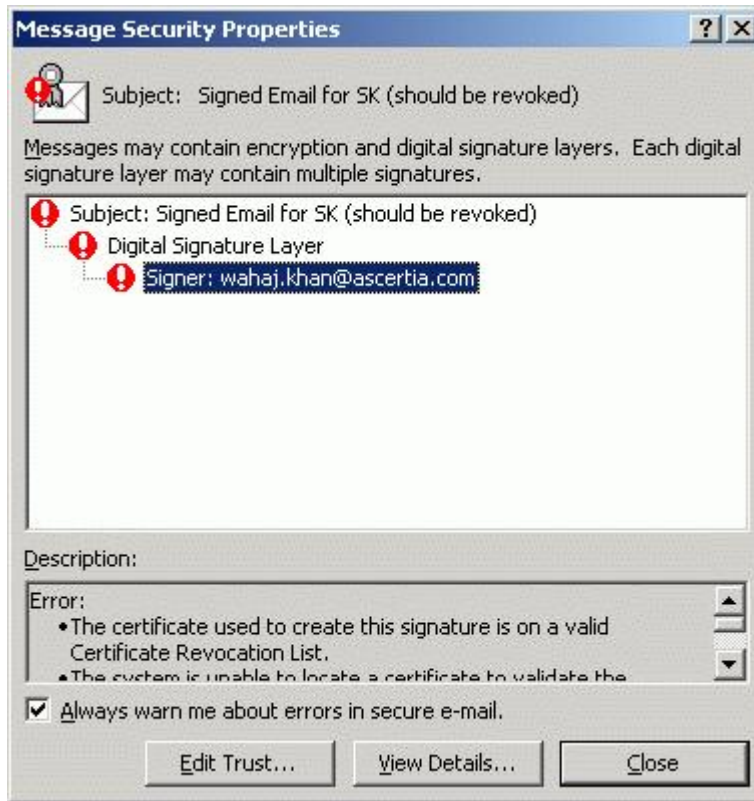
Certificate Status: Good or unknown

Also in case ARP is unable to connect to Responder then still the following dialog is shown:



If Signer certificate is explicitly trusted than the exclamation mark is removed

Certificate Status: Revoked



Certificate Status: Expired



**Internet Explorer 5.0/6.0**

For case1 as certificate status is good, IE will not show any further dialog and will simply open the relevant website.

In cases 2-5 as the revocation information is not known, IE will show the following dialog and only if the user selects “Yes” then IE will open the relevant website.



For case 6, if ARP returns revoked as the certificate status then the following dialog is shown:



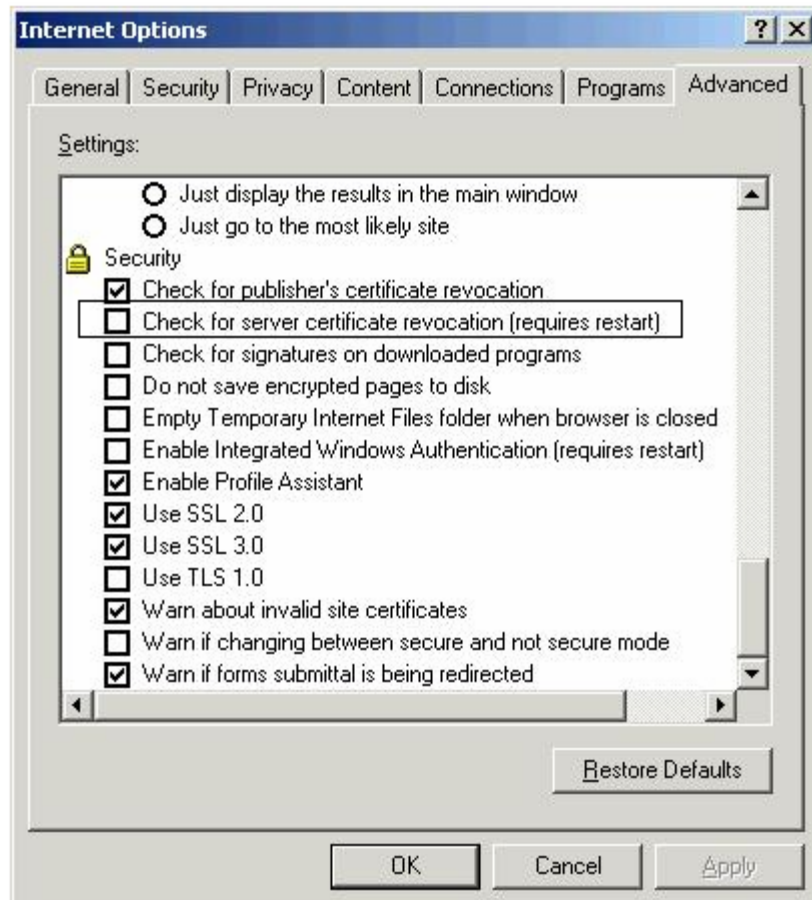
In any Crypto Application if revocation status of a signing certificate is good or unknown etc and is not revoked then clicking once will launch ARP. On clicking the same email again, the Crypto Application will not call ARP as the previous status was not revoked. The Crypto Application stores the certificate status and calls ARP on the basis of it. If the certificate status is revoked, ARP will be invoked by calling application every time email is clicked or opened. To launch ARP again from the email having certificate status good or unknown, try opening some other email and then open the concerned email.

### **8.13 On some Smart cards PIN is asked every time OCSP Request is about to be signed whereas in some, PIN is asked only once why?**

This is because of some setting inside the Smart cards e.g. Gemplus Smart Cards ask for PIN every time the private key is accessed for signing, Rainbow USB does not ask for a PIN at all whereas Oberthur one only asks for PIN once. Consult your Smart card vendor for more information on this.

### **8.14 After installing ARP my MSN Messenger has stopped working why?**

MSN messenger along with other Microsoft applications use the default revocation provider installed on the system. During login messenger checks the validity of the server certificate. If messenger application is not added in the ARP's Applicability section then messenger won't run. Alternatively you can turn off the revocation checking by un-checking the option Check for server certificate revocation (requires restart) option using the setting as shown below.



## 9 Troubleshooting:

Follow the instruction below to resolve the problems

<b>Problem No</b>	<b>Problem Description</b>	<b>Solution</b>
Prb001	If the text on the ARP Lite Setting user interface is not shown properly i.e. the font size of the text has increased, decreased or hidden.	Open Internet Explorer, go to the View → Text Size and select Medium and restart ARP Lite.

For further problems and clarifications contact Ascertia [Technical Support](#).