How to check for proxy server man-in-the-middle actions

As part of a customer's (or customer organization's) information security posture, there could be applications acting as a proxy server when the customer attempts to communicate with the internet.

One function of these proxy servers might be to perform a "man-in-the-middle" action with PKI certificates. When a website presents a certificate to the customer's browser (i.e. any URL that starts "https://..."), the proxy intercepts the in-bound PKI certificate from the website and creates a 'facsimile' certificate that it sends to the customer's browser. Since the customer browser will already have been configured to accept these certificates, the customer may not even be aware of this.

Then when the customer has to send their WidePoint issued PKI certificate back to the website (to log-on, renew, or test their certificate) the proxy intercepts the out-bound PKI certificate from the user (customer) and creates a 'facsimile' certificate that it sends to the target website. So the website does not receive the certificate that WidePoint issued; it receives a certificate issued by the proxy server. The website will not have been configured to accept the proxy-issued certificate and the customer will receive a failure message of some kind.

These applications (an outright proxy server or a web security application on the customer's computer) should be able to be configured so that when the customer goes to particular websites the proxy does not interfere with the certificates. Some applications known to do this are Windows Defender, ESET, AVG, Avast!, BitDefender, Fiddler, BrowserSafeGuard, Rockettab, Kaspersky! Web/Mail Shield, etc. Every application seems to have a different name for this 'feature' and a different way to configure the application. The configuration change may need to be done by the customer's IT support staff. When they update their configuration, recommend they configure these URLs:

- https://*.orc.com
- https://*.widepoint.com
- https://*.mil
- https://*.gov

Below is an example of configuration for one such application (Kaspersky):

```
Perform the following steps to upgrade to the latest release of Kaspersky Total Security:
a) Exit Kaspersky: right-click on the Kaspersky K icon in the lower right corner of your screen (the system
tray). Select 'Exit' from the list that appears.
b) Download and install Kaspersky using this link
After the file is downloaded, double click the file to start the installation, and follow the on screen
prompts.

To add a website to the trusted URLs (or Trusted Web Pages) list:
Open Kaspersky.
Click on 'Settings'.
Click on 'Protection' on the left.
Click on 'Web Ant-Virus' on the right.
Click on 'Advanced Settings'.
Click on 'Configure trusted web pages' (or possibly Trusted URLs).
Click on the 'Add' button.
Enter the web address in the same format as shown: https://*.example.com/*
Select 'Active'.
Click on the 'Add' button.
If needed, repeat the process for additional sites.
Close the 'Trusted web pages' window.
```

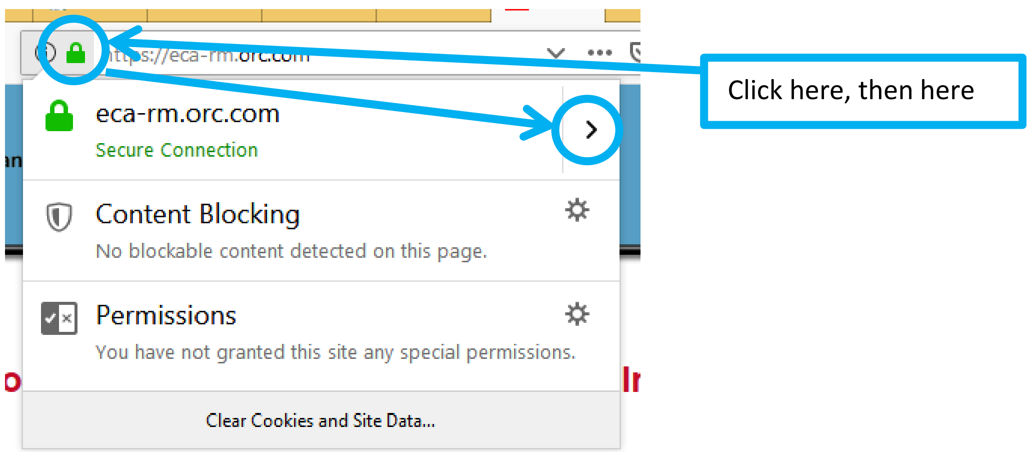
Click the Back arrow in the upper left three times to return to the main window.
Retry the web site. If it does not work, close all open web browsers and reopen the site.

If at any point you need live assistance with following the steps, please visit the following link for support options http://support.kaspersky.com/us/b2c#region

Best regards,
Technical Support | Kaspersky Lab

To check for this, have the customer look for evidence of a proxy server man-in-the-middle action. For example when pointed at our server (https://eca-rm.orc.com/) the browser will present a padlock icon click the padlock icon to examine the certificate. At the URL above, the certificate should say that it was issued by ORC ECA 6. If it says anything else, then there is an application in the customer's environment that is interfering with certificate information and could be preventing installation.

Example: Firefox

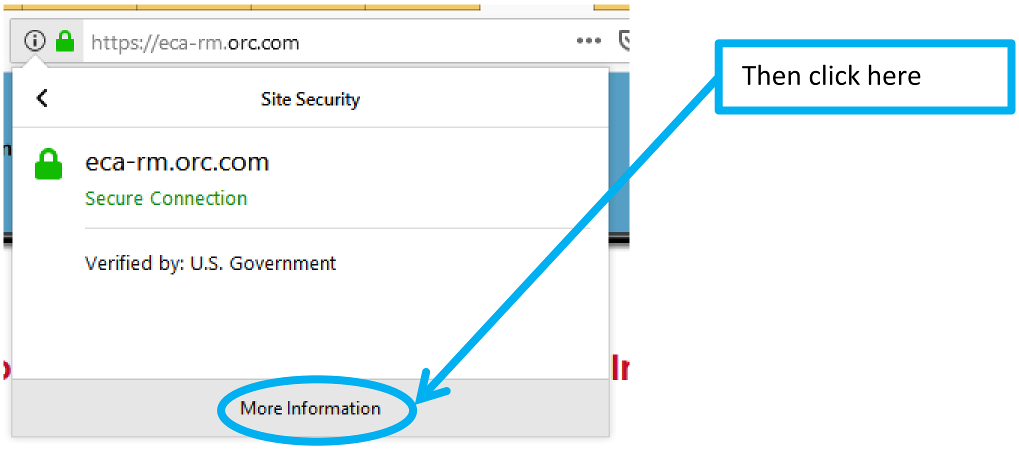


eca-rm.orc.com
Secure Connection

Content Blocking
No blockable content detected on this page.

Permissions
You have not granted this site any special permissions.

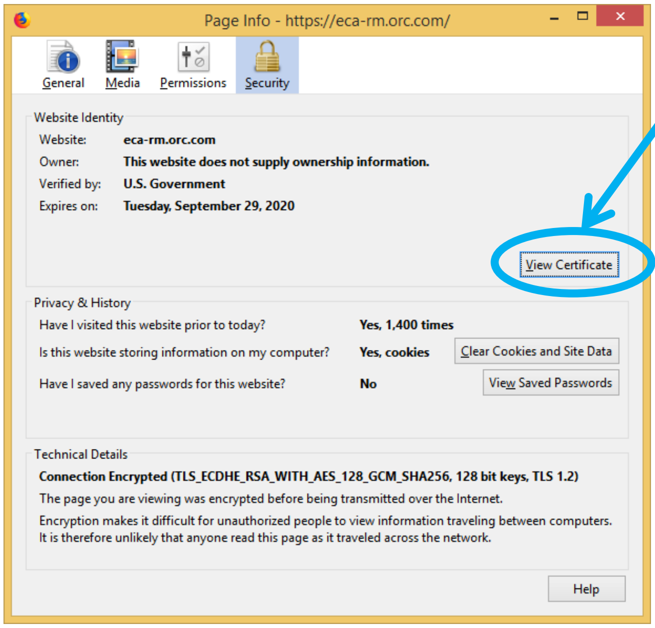
Click here, then here



eca-rm.orc.com
Secure Connection

Verified by: U.S. Government

Then click here



Website Identity

Website: eca-rm.orc.com
Owner: This website does not supply ownership information.
Verified by: U.S. Government
Expires on: Tuesday, September 29, 2020

Privacy & History

Have I visited this website prior to today?	Yes, 1,400 times	
Is this website storing information on my computer?	Yes, cookies	Clear Cookies and Site Data
Have I saved any passwords for this website?	No	View Saved Passwords

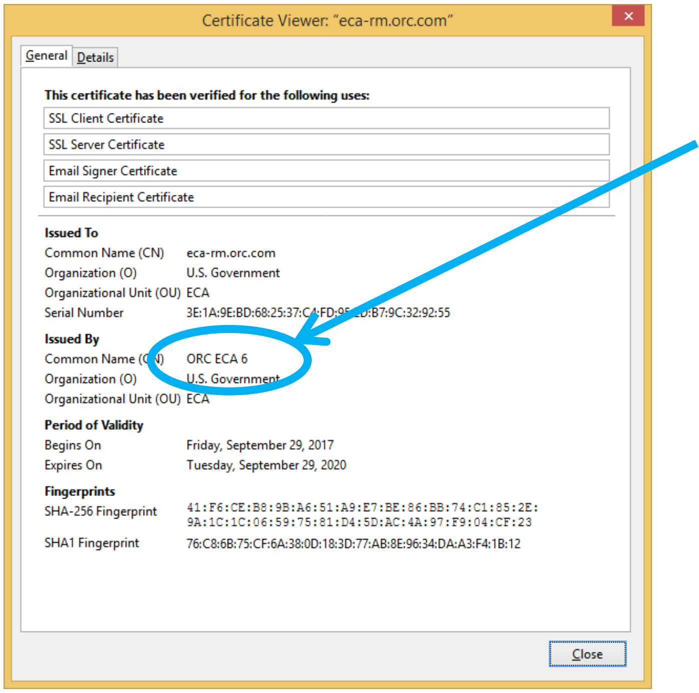
Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Then click here



This certificate has been verified for the following uses:

SSL Client Certificate
SSL Server Certificate
Email Signer Certificate
Email Recipient Certificate

Issued To

Common Name (CN) eca-rm.orc.com
Organization (O) U.S. Government
Organizational Unit (OU) ECA
Serial Number 3E:1A:9E:BD:68:25:37:C4:FD:95:[illegible]D:B7:9C:32:92:55

Issued By

Common Name (CN) ORC ECA 6
Organization (O) U.S. Government
Organizational Unit (OU) ECA

Period of Validity

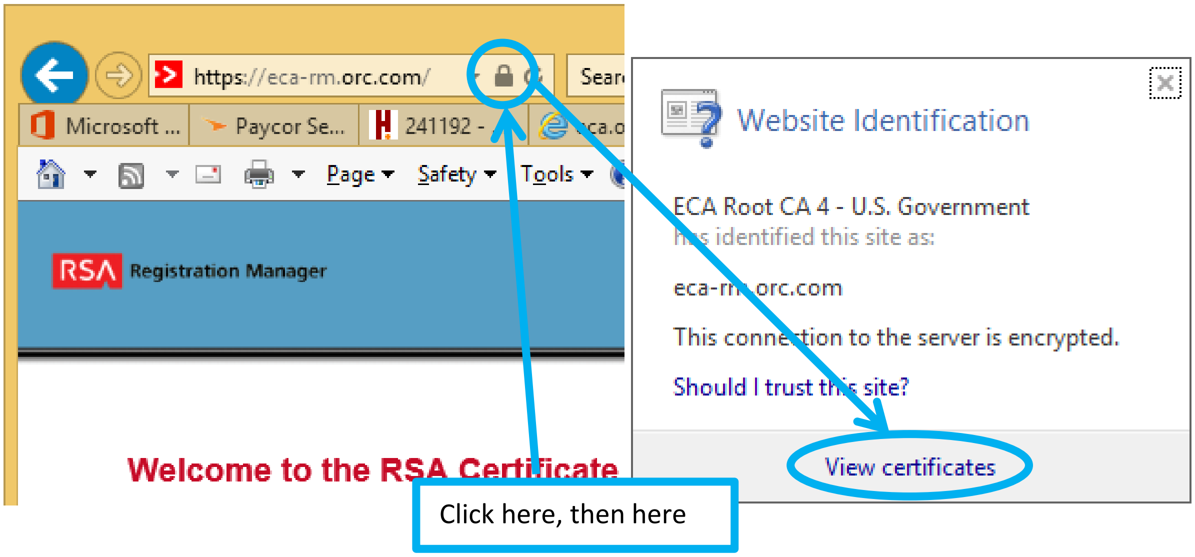
Begins On Friday, September 29, 2017
Expires On Tuesday, September 29, 2020

Fingerprints

SHA-256 Fingerprint 41:F6:CE:B8:9B:A6:51:A9:E7:BE:86:BB:74:C1:85:2E:9A:1C:1C:06:59:75:81:D4:5D:AC:4A:97:F9:04:CF:23
SHA1 Fingerprint 76:C8:6B:75:CF:6A:38:0D:18:3D:77:AB:8E:96:34:DA:A3:F4:1B:12

If this says anything other than "ORC ECA 6", the customer has an application acting as a proxy server and performing "man-in-the-middle" actions on certificates

Example: Internet Explorer



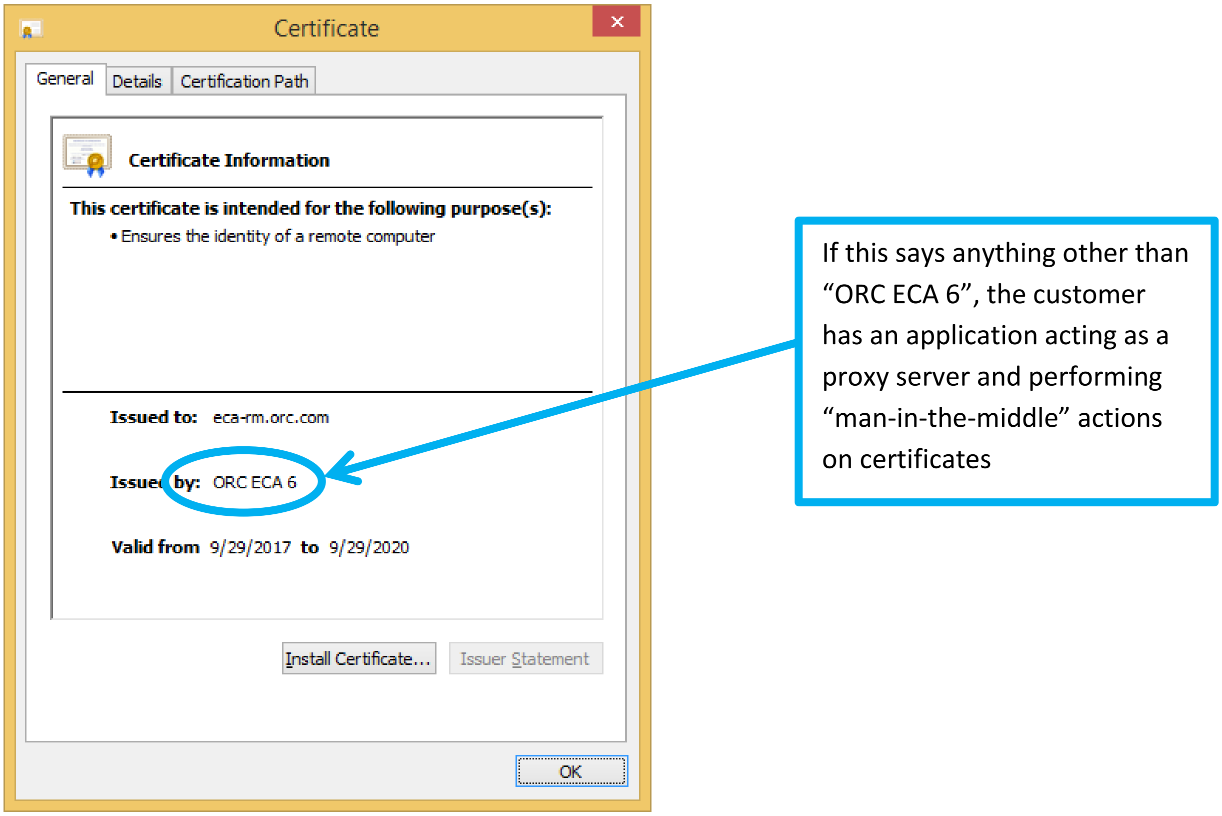
Welcome to the RSA Certificate

ECA Root CA 4 - U.S. Government has identified this site as:

eca-rm.orc.com

This connection to the server is encrypted.

Click here, then here



This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

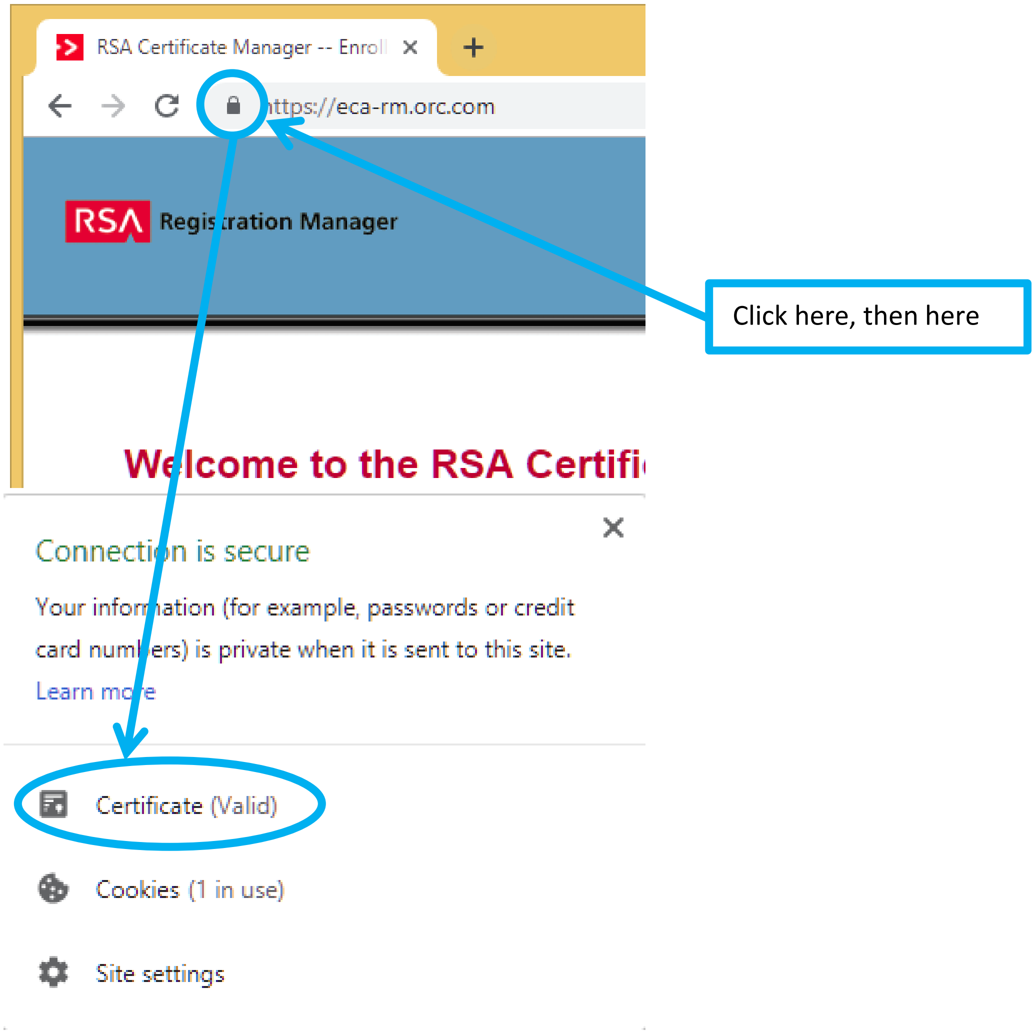
Issued to: eca-rm.orc.com

Issued by: ORC ECA 6

Valid from 9/29/2017 **to** 9/29/2020

If this says anything other than "ORC ECA 6", the customer has an application acting as a proxy server and performing "man-in-the-middle" actions on certificates

Example: Chrome

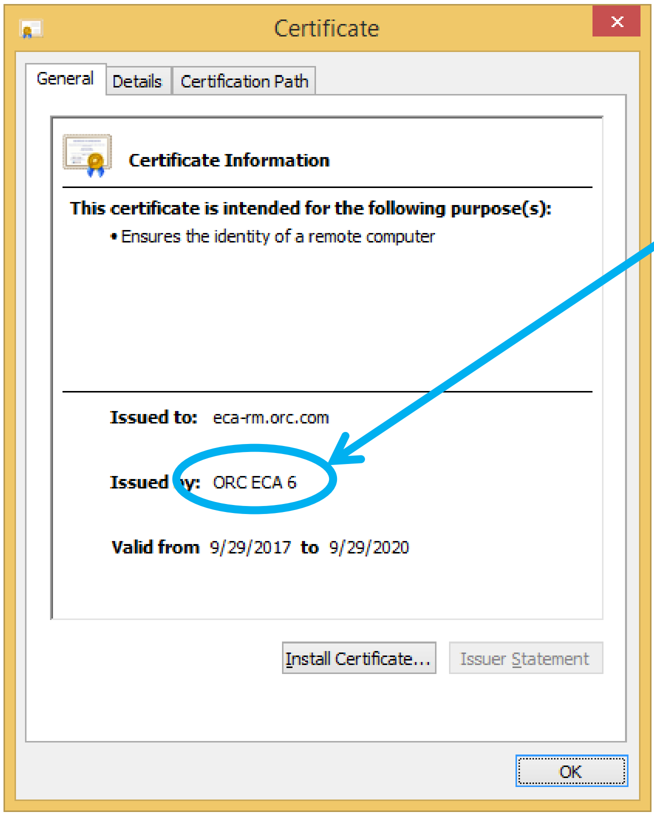


Welcome to the RSA Certifi

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

Click here, then here



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

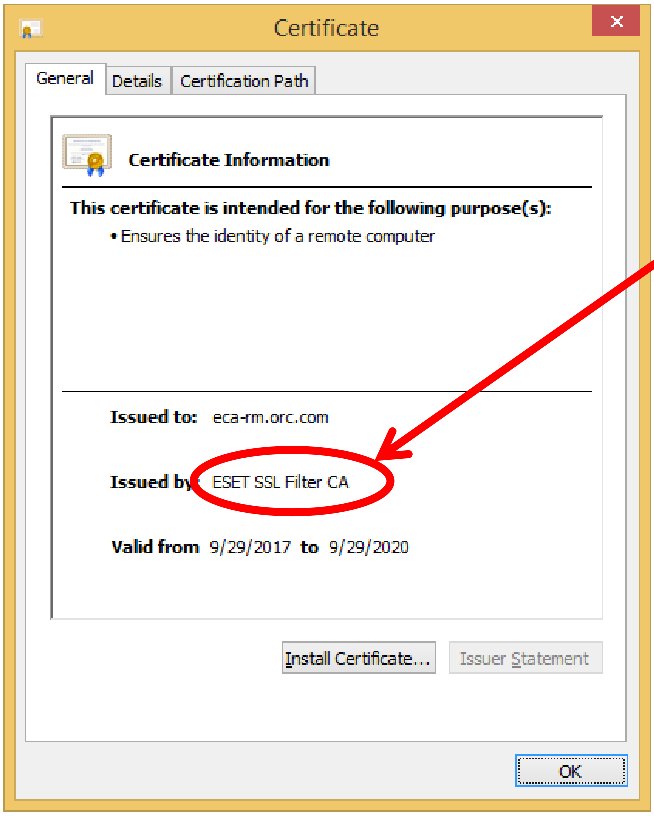
Issued to: eca-rm.orc.com

Issued by: ORC ECA 6

Valid from 9/29/2017 **to** 9/29/2020

If this says anything other than "ORC ECA 6", the customer has an application acting as a proxy server and performing "man-in-the-middle" actions on certificates

Example of "man-in-the-middle" below



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: eca-rm.orc.com

Issued by: ESET SSL Filter CA

Valid from 9/29/2017 **to** 9/29/2020

The issuer of the true certificate is "ORC ECA 6". With ESET's "SSL/TLS Protocol filtering" enabled, ESET performs man-in-the-middle actions. This can prevent a successful log-on, certificate test, certificate renewal, or certificate installation.