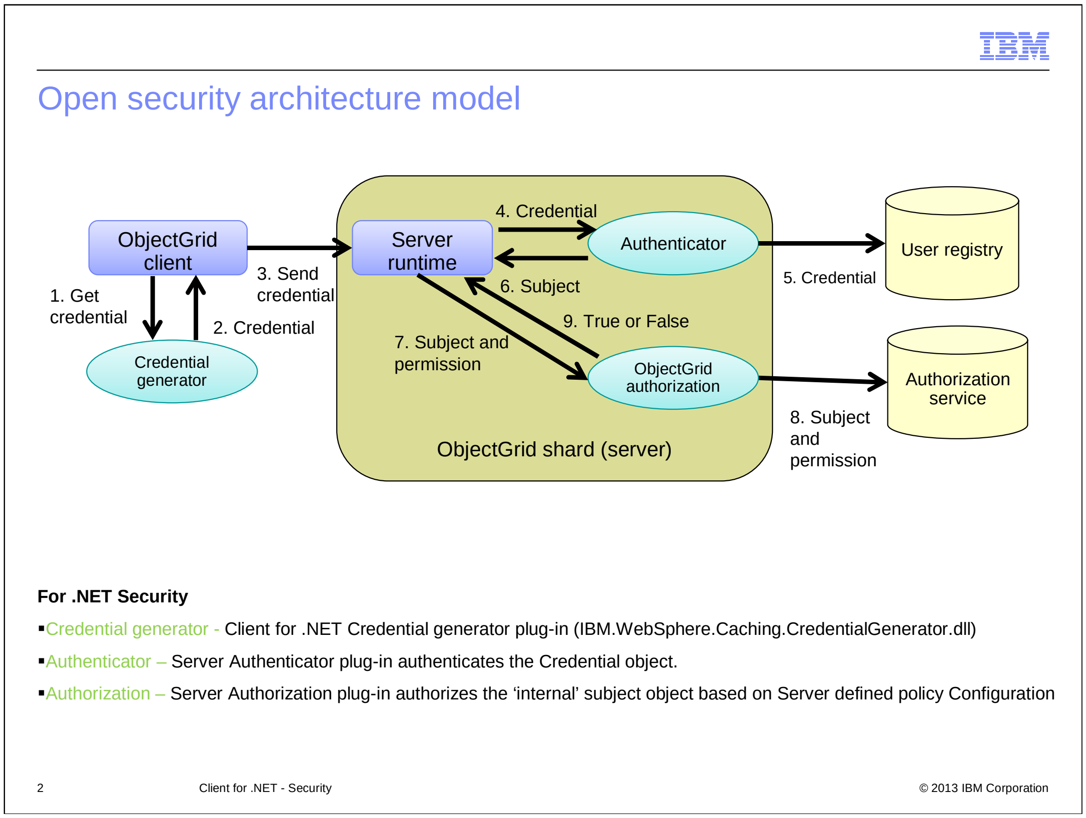
IBM WebSphere Extreme Scale V8.6

Client for .NET - Security

This presentation describes the security features and configuring security in the WebSphere® eXtreme Scale for .NET client.



Open security architecture model

ObjectGrid client

1. Get credential

Credential generator

2. Credential

3. Send credential

Server runtime

4. Credential

Authenticator

5. Credential

User registry

6. Subject

7. Subject and permission

ObjectGrid authorization

8. Subject and permission

Authorization service

9. True or False

ObjectGrid shard (server)

For .NET Security

- Credential generator - Client for .NET Credential generator plug-in (IBM.WebSphere.Caching.CredentialGenerator.dll)
- Authenticator – Server Authenticator plug-in authenticates the Credential object.
- Authorization – Server Authorization plug-in authorizes the ‘internal’ subject object based on Server defined policy Configuration

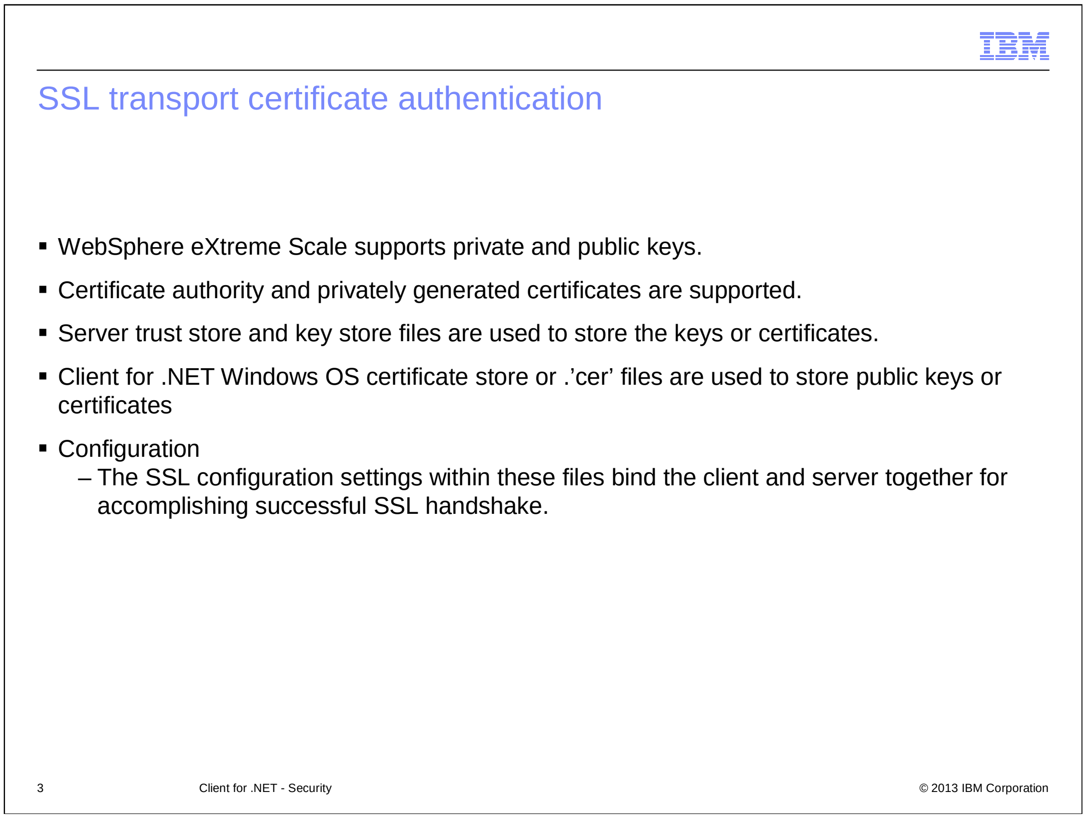
2 Client for .NET - Security © 2013 IBM Corporation

WebSphere eXtreme Scale for .NET Client provides several mechanisms to secure access to the data stored in the grid. First, the transport encryption can be configured with either SSL or TLS to ensure grid data is never sent in the clear. Second, the grid supports client authentication to restrict data access based on client credentials, and finally, the grid supports client authorization to restrict specific data operations based on configurable user permissions. Since all security is disabled by default, manual configuration of WebSphere eXtreme Scale is required to enable security. When configuring WebSphere eXtreme Scale for .NET Client 8.6 security, the following security configuration restrictions apply: When transport encryption is enabled, grid authentication must also be enabled. When grid authorization is enabled, grid authentication must also be enabled.

WebSphere eXtreme Scale supports an open security architecture model that allows you to write user-created plug-ins on both the client and the server side for client credential generation and server authentication and authorization. The .NET client ships with a user password credential generator plug-in. The WebSphere eXtreme Scale server ships with the corresponding credential authentication and authorization plug-ins.

In the diagram at step 1, the client for .NET plug-in generates a user password ‘credential object’ that is passed at step 3 from the ObjectGrid client to the ObjectGrid server. The ‘credential object’ is interpreted on the server side by the matching server plug-in interface implementation that consists of the authenticator and the ObjectGrid authorization. Additionally, the ObjectGrid shard plug-ins can access an external user registry – like LDAP - and authorization services – like JAAS - for authentication and authorization.

The client and server plug-ins are defined and bound together by the Client.Net.Properties and server's security.xml and objectgrid.xml configuration settings. The Client.Net.Properties file controls which client credential generator implementation plug-in is used. The server's security.xml defines the authenticator plug-in that is used to authenticate the delivered credential object, and the server's objectgrid.xml file defines the authorization plug-in that is used to authorize client access to grid data.



SSL transport certificate authentication

- WebSphere eXtreme Scale supports private and public keys.
- Certificate authority and privately generated certificates are supported.
- Server trust store and key store files are used to store the keys or certificates.
- Client for .NET Windows OS certificate store or .’cer’ files are used to store public keys or certificates
- Configuration
  - The SSL configuration settings within these files bind the client and server together for accomplishing successful SSL handshake.

3 Client for .NET - Security © 2013 IBM Corporation

WebSphere eXtreme Scale supports traditional private and public key exchange. The SSL authentication performed by the .NET client is asymmetrical. The client authenticates the server but the server does not authenticate the client during the SSL authentication handshake.

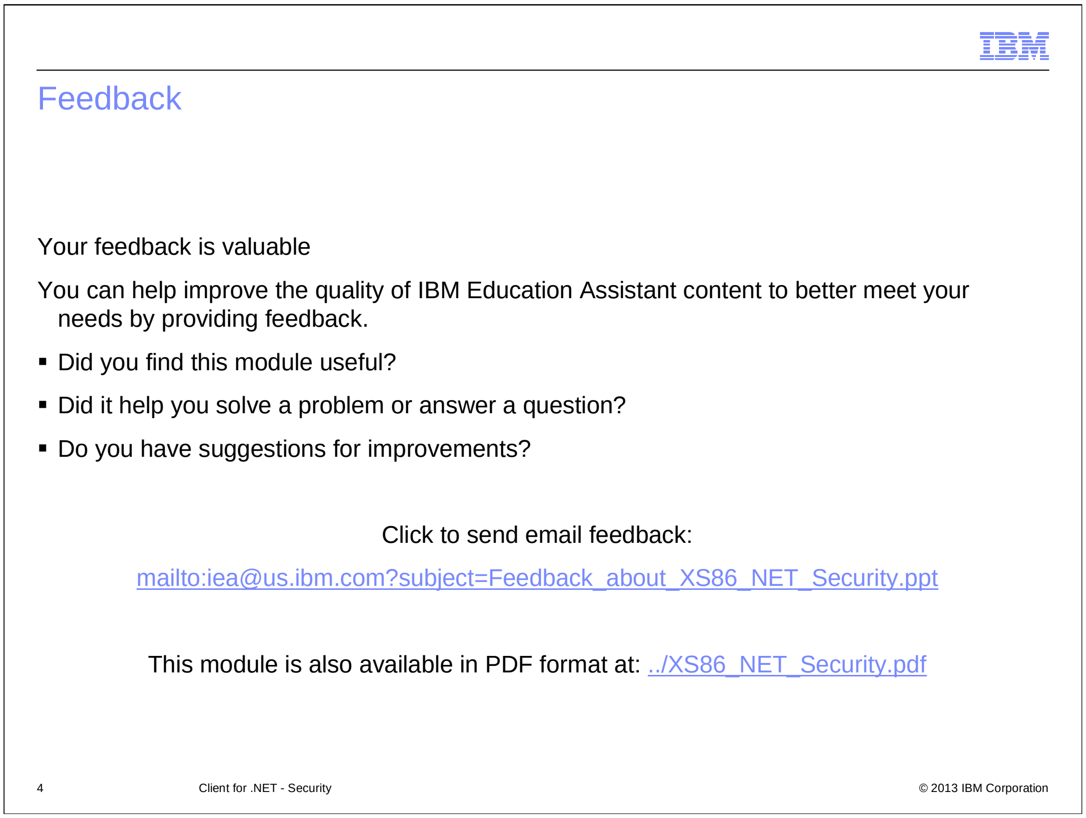
Private keys are generated by the user and stored on the WebSphere eXtreme Scale servers. Public keys, extracted from the server private keys, are stored on the client. A single server private key can be used on each server with its extracted public key stored on each of the WebSphere eXtreme Scale clients. To prevent having the same private key shared across all WebSphere eXtreme Scale servers certificate authority or privately generated certificates can be used as these are also supported for WebSphere eXtreme scale server client SSL authentication. Alternatively, each server can have its own private key with an extracted public key from each server. All of the extracted server public keys will then need to be added to each client for .NET Windows OS certificate store not using a single ‘.cer’ file.

Certificate authority and privately generated certificates are supported.

Server trust Store/Key store files are used to store the private keys or certificates on the server for use by SSL authentication. The Java keytool utility can be used to generate public/private key pairs, keystores and truststores. WebSphere eXtreme Scale documentation provides tutorials for generating these items.

The client for .NET Windows certificate store or .cer files are used to store public keys or certificates. The .cer file, as configured within the Client.Net.Properties settings, is used to point to a single certificate. Alternatively, single or multiple .cer files can be stored in the Windows certificate store using the Windows certmgr.msc tool. When using the Windows certmgr.msc tool, the keys or certificates should be added to the ‘trusted root certification authority’ logical store certificate store level.

The SSL configuration settings within these files ‘bind’ the client and server together for accomplishing successful SSL handshake. Configuring SSL for the .NET client is controlled by the settings in the Client.Net.Properties file. Configuring SSL for the WebSphere eXtreme Scale server is controlled by the settings in the containerServer.props file for ObjectGrid shard servers, and in the catalogServer.props file for eXtreme Scale catalog servers.



Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

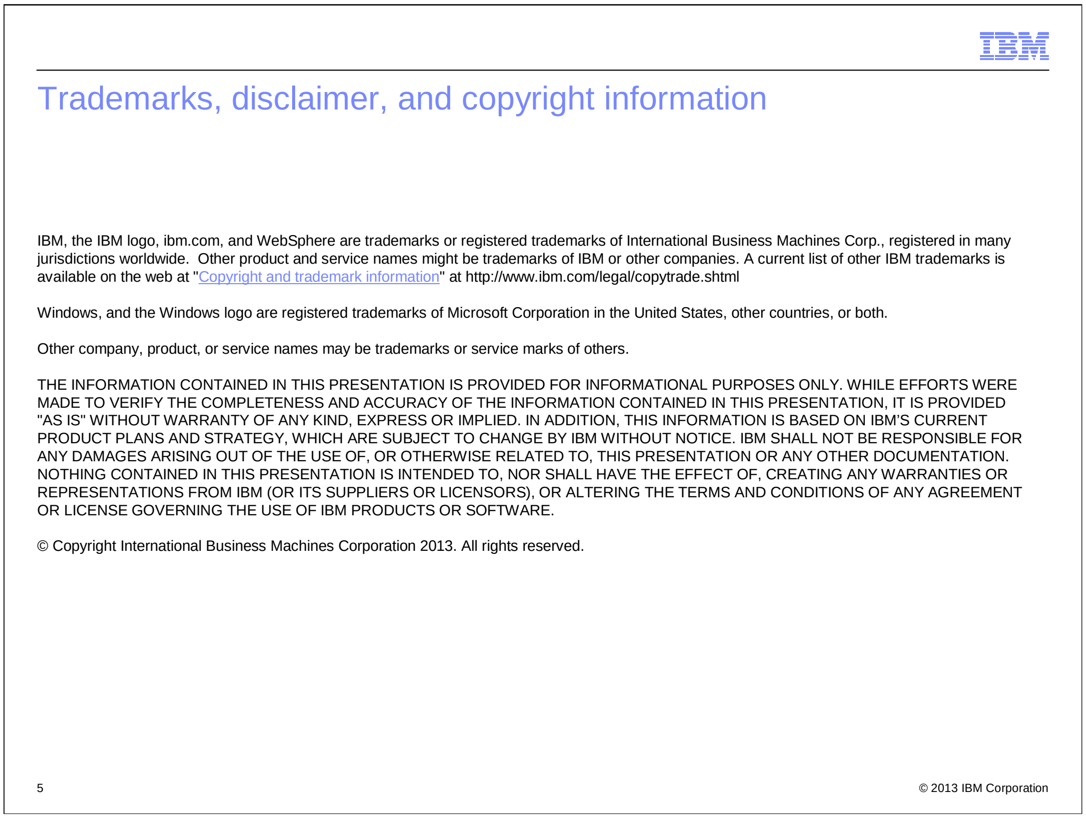
- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_XS86_NET_Security.ppt

This module is also available in PDF format at: ../XS86_NET_Security.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

Windows, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.