Orbacus Version 4.3.5

FSSL for Orbacus Guide

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

http://www.microfocus.com

2016-09-27

Contents

Preface

The Orbacus Library

The Orbacus documentation library consists of the following books:

- Orbacus Guide
- FSSL for Orbacus Guide (this book)
- JThreads/C++ Guide
- Orbacus Notify Guide

Orbacus Guide

This manual describes how Orbacus implements the CORBA standard, and describes how to develop and maintain code that uses the Orbacus ORB. This is the primary developer’s guide and reference for Orbacus.

FSSL for Orbacus Guide

This manual describes the FSSL plug-in, which enables secure communications using the Orbacus ORB in both Java and C++.

JThreads/C++ Guide

This manual describes JThreads/C++, which is a high-level thread abstraction library that gives C++ programmers the look and feel of Java threads.

Orbacus Notify Guide

This manual describes Orbacus Notify, an implementation of the Object Management Group’s Notification Service specification.

Audience

Manuals in the Orbacus library are written for intermediate to advanced level programmers who are:

- Experienced with Java or C++ programming
- Familiar with the CORBA standard and its specifications

These manuals do not teach the CORBA specification or CORBA programming in general, which are prerequisite skills. These manuals concentrate on how Orbacus implements the CORBA standard.

Document Conventions

Typographical conventions

This book uses the following typographical conventions:

`Fixed width`	Fixed width (Courier font) in normal text represents portions of code and literal names of items such as classes, functions, variables, and data structures. For example, text might refer to the `IT_Bus::AnyType` class. Constant width paragraphs represent code examples or information a system displays on the screen. For example: `#include <stdio.h>`
`Fixed width italic`	Fixed width italic words or characters in code and commands represent variable values you must supply, such as arguments to commands or path names for your particular system. For example: `% cd /users/`*`YourUserName`*
Italic	Italic words in normal text represent *emphasis* and introduce *new terms*.
Bold	Bold words in normal text represent graphical user interface components such as menu commands and dialog boxes. For example: the **User Preferences** dialog.

Keying Conventions

This book uses the following keying conventions:

No prompt	When a command’s format is the same for multiple platforms, the command prompt is not shown.
`%`	A percent sign represents the UNIX command shell prompt for a command that does not require root privileges.
`#`	A number sign represents the UNIX command shell prompt for a command that requires root privileges.
`>`	The notation > represents the MS-DOS or Windows command prompt.

`. . .`
`.`
`.`
`.`
	Horizontal or vertical ellipses in format and syntax descriptions indicate that material has been eliminated to simplify a discussion.

`[]`	Brackets enclose optional items in format and syntax descriptions.
{ }	Braces enclose a list from which you must choose an item in format and syntax descriptions.
|	In format and syntax descriptions, a vertical bar separates items in a list of choices enclosed in { } (braces). In graphical user interface descriptions, a vertical bar separates menu commands (for example, select **File**|**Open**).

Contacting Micro Focus

Our Web site gives up-to-date details of contact numbers and addresses.

Further Information and Product Support

Additional technical information or advice is available from several sources.

The product support pages contain a considerable amount of additional information, such as:

- The *Product Updates* section of the Micro Focus SupportLine Web site, where you can download fixes and documentation updates.
- The *Examples and Utilities* section of the Micro Focus SupportLine Web site, including demos and additional product documentation.

To connect, enter http://www.microfocus.com in your browser to go to the Micro Focus home page, then click *Support*.

Note:

Some information may be available only to customers who have maintenance agreements.

If you obtained this product directly from Micro Focus, contact us as described on the Micro Focus Web site, http://www.microfocus.com. If you obtained the product from another source, such as an authorized distributor, contact them for help first. If they are unable to help, contact us.

Also, visit:

- The Micro Focus Community Web site, where you can browse the Knowledge Base, read articles and blogs, find demonstration programs and examples, and discuss this product with other users and Micro Focus specialists.

- The Micro Focus YouTube channel for videos related to your product.

Information We Need

However you contact us, please try to include the information below, if you have it. The more information you can give, the better Micro Focus SupportLine can help you. But if you don't know all the answers, or you think some are irrelevant to your problem, please give whatever information you have.

- The name and version number of all products that you think might be causing a problem.
- Your computer make and model.
- Your operating system version number and details of any networking software you are using.
- The amount of memory in your computer.
- The relevant page reference or section in the documentation.
- Your serial number. You can find this by either logging into your order via the Electronic Product Distribution email or via the invoice with the order.

Contact information

Our Web site gives up-to-date details of contact numbers and addresses.

Additional technical information or advice is available from several sources.

The product support pages contain considerable additional information, including the *Product Updates* section of the Micro Focus SupportLine Web site, where you can download fixes and documentation updates. To connect, enter http://www.microfocus.com in your browser to go to the Micro Focus home page, then click *Support*.

If you are a Micro Focus SupportLine customer, please see your SupportLine Handbook for contact information. You can download it from our Web site or order it in printed form from your sales representative. Support from Micro Focus may be available only to customers who have maintenance agreements.

You may want to check in particular:

> https://supportline.microfocus.com/productdoc.aspx. (documentation updates and PDFs)

To subscribe to Micro Focus electronic newsletters, use the online form at:

> http://www.microfocus.com/Resources/Newsletters/infocus/newsletter-subscription.asp

CHAPTER 1

Using FSSL for Orbacus

This chapter describes the FSSL plug-in, which enables secure communications using the Orbacus ORB in both Java and C++.

In this chapter

This chapter contains the following sections:

What is SSL?

Overview

The Secure Sockets Layer (SSL) protocol, developed by Netscape Communications Corporation, provides communications privacy over a network. It is designed to prevent eavesdropping, tampering, and message forgery. The FSSL plug-in enables secure communications using the Orbacus ORB in both Java and C++. The plug-in supports SSLv3, TLSv1, TLSv1.1, TLSv1.2.

How does it work?

SSL uses symmetric cryptography for data communication (for example, DES). In symmetric cryptography, both parties use the same key to encrypt and decrypt data. This is different than asymmetric cryptography, in which different keys are used for encryption and decryption. The advantage of using symmetric cryptography for securing message traffic is that it operates much faster than asymmetric cryptography, thereby minimizing the overhead incurred by the use of a secure communication protocol.

Asymmetric cryptography, also known as public key cryptography (for example, RSA or DSS), is still used in the SSL protocol for authentication and key exchange. Using public key cryptography, each party has an associated public and private key. Data encrypted with the public key can only be decrypted with the private key, and vice versa. This allows a party to prove its identity by encrypting the data with its private key. As no other party has access to the private key, the data must have been sent by the true party.

Each peer is authenticated using an X.509 certificate [4]. Generally, a certificate will contain the user's name and public key and is signed by a trustworthy entity, the so-called Certificate Authority (CA).

Usually a chain of X.509 certificates are presented. The certificate at the head of the chain is the peer's certificate. Each certificate is signed by the next certificate in the chain. The certificate at the end of the chain is self-signed, and is generally the certificate of the Certificate Authority itself.

A certificate has an associated private key and passphrase. Without the private key is it not possible to use a certificate to prove identity. The passphrase protects the private key and is used to decrypt the private key at runtime.

Given a certificate, there must be some logic to determine whether this certificate is trusted. This is typically done against some certificate authority. A certificate authority is an organization that is responsible for issuing certificates to individuals. The choice of trusted certificate authorities is something that is best left up to the application. For instance, a company may issue certificates to all of their employees and only trust one certificate authority certificate.

The generation and signing of certificates is beyond the scope of this document. For both the C++ and Java plug-ins please see [5].

The SSL protocol ensures that the connection between communicating parties is reliable. The integrity of the message data is verified using a keyed Message Authentication Code (MAC). The sender of a message uses a secure, one-way hash function (for example, SHA, MD5) to compute a unique MAC for the message. The receiver uses the same function to compute its own MAC, and then compares what it computed against the MAC computed by the sender. This means that corrupted or deliberately changed messages can be detected because the two MACs will not match.

Cipher suites

A cipher suite [1] defines: The public key algorithm used for peer authentication and key exchange. The symmetric algorithm used for data encryption. The secure hash function for MAC computation. During the initial handshake, the client offers its set of supported cipher suites in its preferred order. The server responds by selecting one of the suites, or raising a handshake failure if they have none in common.

The following table summarizes the algorithms used by each cipher suite for key exchange, symmetric cryptography, and MAC calculation.

Table 1: *Supported Cipher Suites*

Name	Key Alg	Symmetric Alg	MAC Calc	Notes
FSSL_RSA_EXPORT_WITH_NULL_MD5	RSA	None	MD5	
FSSL_RSA_EXPORT_WITH_NULL_SHA	RSA	None	SHA	
FSSL_RSA_EXPORT_WITH_RC4_40_MD5	RSA	RC4 (40 bits)	MD5	FSSL C++: OpenSSL no longer supports this cipher suite. FSSL Java: Must use TLSv1
FSSL_RSA_WITH_RC4_128_MD5	RSA	RC4 (128 bits)	MD5	
FSSL_RSA_WITH_RC4_128_SHA	RSA	RC4 (128 bits)	SHA	
FSSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5	RSA	RC2 (40 bits)	MD5	FSSL C++: OpenSSL no longer supports this cipher suite. FSSL Java: Must use TLSv1
FSSL_RSA_WITH_IDEA_CBC_SHA	RSA	IDEA (128 bits)	SHA	FSSL Java: JSSE does not support this cipher suite.
FSSL_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA	DES (40 bits)	SHA	FSSL C++: OpenSSL no longer supports this cipher suite. FSSL Java: Must use TLSv1

Table 1: *Supported Cipher Suites*

Name	Key Alg	Symmetric Alg	MAC Calc	Notes
FSSL_RSA_WITH_DES_CBC_SHA	RSA	DES (56 bits)	SHA	FSSL C++: OpenSSL no longer supports this cipher suite. FSSL Java: Must use TLSv1
FSSL_RSA_WITH_3DES_EDE_CBC_SHA	RSA	DES (168 bits)	SHA	
FSSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA	DES (40 bits)	SHA	FSSL C++: OpenSSL no longer supports this cipher suite. FSSL Java: Must use TLSv1
FSSL_DHE_RSA_WITH_DES_CBC_SHA	RSA	DES (56 bits)	SHA	FSSL C++: OpenSSL no longer supports this cipher suite. FSSL Java: Must use TLSv1
FSSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	RSA	DES (168 bits)	SHA	FSSL Java: Must use TLSv1
FSSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	DSS	DES (40 bits)	SHA	FSSL C++: OpenSSL no longer supports this cipher suite. FSSL Java: Must use TLSv1

Table 1: *Supported Cipher Suites*

Name	Key Alg	Symmetric Alg	MAC Calc	Notes
FSSL_DHE_DSS_WITH_DES_CBC_SHA	DSS	DES (56 bits)	SHA	FSSL C++: OpenSSL no longer supports this cipher suite. FSSL Java: Must use TLSv1
FSSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	DSS	DES (168 bits)	SHA	
FSSL_DH_anon_EXPORT_WITH_RC4_40_MD5	ADH	RC4 (40 bits)	MD5	FSSL C++: OpenSSL no longer supports this cipher suite. FSSL Java: Must use TLSv1
FSSL_DH_anon_WITH_RC4_128_MD5	ADH	RC4 (128 bits)	MD5	
FSSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	ADH	DES (40 bits)	SHA	FSSL C++: OpenSSL no longer supports this cipher suite. FSSL Java: Must use TLSv1
FSSL_DH_anon_WITH_DES_CBC_SHA	ADH	DES (56 bits)	SHA	
FSSL_DH_anon_WITH_3DES_EDE_CBC_SHA	ADH	DES (168 bits)	SHA	
FSSL_RSA_WITH_AES_128_GCM_SHA256	RSA	AESGCM(128)	SHA256	FSSL Java: Available in Java 8 Must use TLSv1.2
FSSL_RSA_WITH_AES_128_CBC_SHA256	RSA	AES(128)	SHA256	

Table 1: *Supported Cipher Suites*

Name	Key Alg	Symmetric Alg	MAC Calc	Notes
FSSL_RSA_WITH_AES_128_CBC_SHA	RSA	AES(128)	SHA	
FSSL_RSA_WITH_AES_256_GCM_SHA384	RSA	AESGCM(256)	SHA256	FSSL Java: Available in Java 8 Must use TLSV1.2 JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_ RSA_WITH_AES_256_CBC_SHA256	RSA	AES(256)	SHA256	FSSL Java: JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_RSA_WITH_AES_256_CBC_SHA	RSA	AES(256)	SHA	FSSL Java: JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_DHE_DSS_WITH_AES_128_GCM_SHA256	DH	AESGCM(128)	SHA256	FSSL Java: Available in Java 8 Must use TLSV1.2
FSSL_DHE_DSS_WITH_AES_128_CBC_SHA256	DH	AES(128)	SHA256	FSSL Java: Must use TLSV1.2
FSSL_DHE_DSS_WITH_AES_128_CBC_SHA	DH	AES(128)	SHA	

Table 1: *Supported Cipher Suites*

Name	Key Alg	Symmetric Alg	MAC Calc	Notes
FSSL_DHE_DSS_WITH_AES_256_GCM_SHA384	DH	AESGCM(256)	SHA384	FSSL Java: Available in Java 8 Must use TLSV1.2 JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_DHE_DSS_WITH_AES_256_CBC_SHA256	DH	AES(256)	SHA256	FSSL Java: Must use TLSV1.2 JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_DHE_DSS_WITH_AES_256_CBC_SHA	DH	AES(256)	SHA	FSSL Java: JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_DHE_RSA_WITH_AES_128_GCM_SHA256	DH	AESGCM(128)	SHA256	FSSL Java: Available in Java 8 Must use TLSV1.2
FSSL_DHE_RSA_WITH_AES_128_CBC_SHA256	DH	AES(128)	SHA256	FSSL Java: Must use TLSV1.2

Table 1: *Supported Cipher Suites*

Name	Key Alg	Symmetric Alg	MAC Calc	Notes
FSSL_DHE_RSA_WITH_AES_128_CBC_SHA	DH	AES(128)	SHA256	
FSSL_DHE_RSA_WITH_AES_256_GCM_SHA384	DH	AESGCM(256)	SHA384	FSSL Java: Available in Java 8 Must use TLSV1.2 JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_DHE_RSA_WITH_AES_256_CBC_SHA256	DH	AES(256)	SHA256	FSSL Java: Must use TLSV1.2 JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_DHE_RSA_WITH_AES_256_CBC_SHA	DH	AES(256)	SHA	FSSL Java: Must use TLSV1.2 JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH	AESGCM(128)	SHA256	FSSL Java: Available in Java 8 Must use TLSV1.2

Table 1: *Supported Cipher Suites*

Name	Key Alg	Symmetric Alg	MAC Calc	Notes
FSSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDH	AES(128)	SHA256	FSSL Java: Must use TLSV1.2
FSSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDH	AES(128)	SHA	
FSSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH	AESGCM(256)	SHA384	FSSL Java: Available in Java 8 Must use TLSV1.2 JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDH	AES(256)	SHA384	FSSL Java: Must use TLSV1.2 JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDH	AES(256)	SHA	FSSL Java: JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDH	3DES(168)	SHA	
FSSL_ECDHE_ECDSA_WITH_RC4_128_SHA	ECDH	RC4(128)	SHA	

Table 1: *Supported Cipher Suites*

Name	Key Alg	Symmetric Alg	MAC Calc	Notes
FSSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH	AESGCM(128)	SHA256	FSSL Java: JSSE does not support this cipher suite
FSSL_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH	AES(128)	SHA256	FSSL Java: Available in Java 8 Must use TLSV1.2
FSSL_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH	AES(128)	SHA	
FSSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH	AESGCM(256)	SHA384	FSSL Java: JSSE does not support this cipher suite
FSSL_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH	AES(256)	SHA384	FSSL Java: Available in Java 8 Must use TLSV1.2 JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH	AES(256)	SHA	FSSL Java: JCE Unlimited Strength Jurisdiction Policy Files required
FSSL_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDH	3DES(168)	SHA	

Table 1: *Supported Cipher Suites*

Name	Key Alg	Symmetric Alg	MAC Calc	Notes
FSSL_ECDHE_RSA_WITH_RC4_128_SHA	ECDH	RC4(128)	SHA	

Note: Java support for cipher suites depends on the settings in Java's `java.security` file. Review, and if necessary update, this file in order to ensure that it supports the cipher suites you want to use. Later versions of Java can be more restrictive in the algorithms allowed.

Installation

Plug-in installation

The FSSL plug-in is an implementation of the Orbacus Open Communications Interface (OCI) and is installed at runtime through configuration. For more general information on Orbacus configuration and the OCI please see the *Orbacus Guide*.

Client installation

The client side FSSL plug-in is installed as follows:

```
ooc.oci.client=fssliop [--seed FILE] [--backend IMPL]
    [--trace N] [--secure_protocol PROTOCOL LIST]
```

The following options are supported:

`--seed FILE`	FSSL for C++ only. If specified, FSSL will use the contents of the file filename as random data to seed the OpenSSL (PRNG) Psuedo Random Number Generator. This may be necessary if the operating system doesn't have its own random data generator. (usually `/dev/random`) If no random data generator is found, and this property is not specified, FSSL will use a generic seeding algorithm.
`--backend IMPL`	FSSL for Java only. The Java version supports multiple third-party SSL toolkits which are identified to the plug-in during installation. Support for different third party SSL toolkits is provided through multiple back-end libraries where each library includes an implementation of the FSSLImpl interface. The `--backend` option accepts the name of the class implementing the FSSLImpl interface. By default the JSSE toolkit is used. Please see Appendix B for information on the supported SSL toolkits and the related back-end library. In this manual we will assume that the JSSE toolkit is being used.

`--secure_protocol PROTOCOL LIST`	Sets the protocols used for secure connections. Valid values are:
	SSLv3
	TLSv1
	TLSv1.1
	TLSv1.2
	A single protocol can be specified as follows:
	`ooc.oci.client=fssliop --secure_protocol "TLSv1.2"`
	A list of protocols can also be specified:
	`ooc.oci.client=fssliop --secure_protocol "TLSv1,TLSv1.1,TLSv1.2"`
	If no protocols are specified, then TLSv1, TLSv1.1, and TLSv1.2 are supported.

`--trace N`	Sets the level of diagnostic output generated by the plug-in itself, and vendor-specific information from the underlying SSL toolkit. The default value is 0.

Server installation

The server side FSSL plug-in is installed as shown below:

```
ooc.oci.server=fssliop
```

Note that FSSL servers must also install the client side plug-in.

Endpoint Configuration

Options

The configuration options for an FSSL endpoint are shown below:

```
fssliop [--backlog N] [--bind ADDR] [--host ADDR[,ADDR,...]]
    [--numeric] [--port N]
```

The following options are supported:

`--backlog N`	Specifies the length of the queue for incoming connection requests. Note that the operating system may override this setting if the value exceeds the maximum allowed.
`--bind ADDR`	Specifies the hostname or dotted decimal address of the network interface on which to bind the socket. If not specified, the POA Manager will bind its socket to all available network interfaces. This property is useful in situations where a host has several network interfaces, but the POA Manager should only listen for connections on a particular interface.
`--host ADDR[,ADDR,...]`	Specifies a list of one or more hostnames and/or dotted decimal addresses representing the addresses that should be advertised in IORs.
`--numeric`	If set, and if --host is not specified, then the canonical dotted decimal address is advertised in IORs. The default behavior is to use the canonical hostname, if possible.
`--port N`	Specifies the port number on which to bind the socket. If no port is specified the operating system selects an unused port automatically.

Command-Line Options

The FSSL plug-in defines the following command line options for both the C++ and the Java version of the plug-in:

`-FSSLbacklog N`	Equivalent to the --backlog endpoint option.
`-FSSLbind ADDR`	Equivalent to the --bind endpoint option.
`-FSSLhost ADDR[,ADDR,...]`	Equivalent to the --host endpoint option.
`-FSSLnumeric`	Equivalent to the --numeric endpoint option.
`-FSSLport N`	Equivalent to the --port endpoint option.

Static Linking

When statically linking a C++ application an explicit reference must be made to the FSSL plug-in in order to include the plug-in's modules. Shown below is the technique used by the sample programs in the fssl/demo subdirectory. Note that the code below is enclosed in guard macros that are only activated when statically linking. These macros are appropriate for both Unix and Windows. First, extra include files are necessary:

```
#if !defined(HAVE_SHARED) && !defined(FSSL_DLL)
#include <OB/OCI_init.h>
#include <FSSL/OCI_FSSLIOP_init.h>
#endif
Next, the plug-in must be registered prior to calling ORB_init():
#if !defined(HAVE_SHARED) && !defined(FSSL_DLL)
//
// When linking statically, we need to explicitly register the
// plug-in prior to ORB initialization
//
OCI::register_plugin("fssliop", OCI_init_fssliop);
#endif
```

URL Support

The FSSL plug-in supports corbaloc URLs with the following protocol syntax:

```
corbaloc:fssliop:host:port/object-key
```

The components of the URL are as follows:

`fssliop`	This selects the FSSL plug-in.
`host`	The hostname or IP address of the server.
`port`	The port on which the server is listening.
`object-key`	A stringified object key.

Contexts

What is a context?

A context comprises four pieces of information: identity, trust decision, a set of cipher suites, and a secure protocol. This information is necessary to establish an SSL connection from a client to a server and to allow a server to accept new SSL connections from clients. For anonymous communications only the set of cipher suites is necessary.

If a context is created and no secure protocol is specified, then all supported TLS protocols are permitted. Supported protocols are TLSv1, TLSv1.1, and TLSv1.2. The secure protocol can be specified for anonymous communications.

The protocol can be supplied in two ways:

- During configuration. See the description of the `--secure_protocol` option in the "Client installation" section.
- When creating the context programmatically. See the section "Protocols" below.

Context creation

Contexts are managed via a context manager. A reference to the context manager is obtained by resolving the FSSLContextManager initial reference. To create a new context `FSSL::Manager::create_context` is called. This returns the ID of the newly created context.

```
// C++
FSSL::ContextID id = fsslManager -> create_context(
myChain, myKey, myPassPhrase, myDecider, myCiphers);
```

```
// Java
int id = fsslManager.create_context(
myChain, myKey, myPassPhrase, myDecider, myCiphers);
```

Contexts can also be created using a PKCS12 certificate file which contains a certificate chain and private key(s). To create a new context from a PKCS12 file, `FSSL::Manager::create_pkcs12_context` is called.

```
// C++
FSSL::ContextID id = fsslManager -> create_pkcs12_context(
        pkcs12_certificate, myPassPhrase, myDecider, myCiphers);
```

```
// Java
int id = fsslManager.create_pkcs12_context(pkcs12_certificate,
             myPassPhrase, myDecider, myCiphers);
```

To destroy a context call `FSSL::Manager::destroy_context`. Applications should be careful not to destroy contexts that are currently in use.

```
// C++
fsslManager -> destroy_context(id);
```

```
// Java
fsslManager.destroy_context(id);
```

Certificates

New X.509 certificates are created using the operation `FSSL::Manager::create_certificate`. An octet sequence containing a DER-encoded certificate should be passed as an argument.

```
// C++
FSSL::Certificate_var myCertificate =
fsslManager -> create_certificate(data);
```

```
// Java++
com.ooc.FSSL.Certificate myCertificate =
 fsslManager.create_certificate(data);
```

Since reading certificate data from a file is a typical use-case a helper method `FSSL::load_file` is provided. This takes a file name as the argument and returns an octet sequence.

```
// C++
FSSL::OctetSeq_var data = FSSL::load_file("mycert.der");
```

```
// Java
byte[] data = com.ooc.FSSL.FSSL.load_file("mycert.der");
```

Handling certificate data from a PKCS12 certificate file differs from DER certificate files. Data from the PKCS12 files is loaded directly into an octet sequence using FSSL::load_file and passed as a parameter to `FSSL::Manager::create_pkcs12_context`.

```
// C++
FSSL::OctetSeq_var pkcs12_data = FSSL::load_file("cert.p12");
FSSL::ContextID id = fsslManager -> create_pkcs12_context(
     pkcs12_data, myPassPhrase, myDecider, myCiphers);
```

```
// Java
byte[] pkcs12_data = com.ooc.FSSL.FSSL.load_file("cert.p12");
int id = fsslManager.create_pkcs12_context(pkcs12_data,
           myPassPhrase, myDecider, myCiphers);
```

Passphrase

The passphrase is an octet sequence. Again a typical use-case is that the passphrase is a string, therefore a helper method `FSSL_string_to_PassPhrase` is provided.

```
// C++
FSSL::PassPhrase_var myPassphrase =
   FSSL::string_to_PassPhrase("foobar");
```

```
// Java
byte[] myPassphrase =
   com.ooc.FSSL.FSSL.string_to_PassPhrase("foobar");
```

Cipher suites

The context creation method is passed a sequence of cipher suite identifiers. A common use-case is to allow all non-anonymous ciphers. Therefore a helper method `FSSL::get_non_export_ciphers()` is provided.

```
// C++
FSSL::CipherSeq_var ciphers = FSSL::get_non_export_ciphers();
```

```
// Java
int[] ciphers = com.ooc.FSSL.FSSL.get_non_export_ciphers();
```

The following other helper methods are also provided:

- `FSSL::get_export_ciphers()` returns a sequence of all export RSA cipher suites (ciphers using keys that are less than 56 bits)
- `FSSL::get_RSA_ciphers()` returns a sequence of all RSA cipher suites

- `FSSL::get_DSS_ciphers()` returns a sequence of all DSS cipher suites
- `FSSL_get_ADH_ciphers()` returns a sequence of all ADH cipher suites.

If none of these helper methods supplies the desired functionality it is possible to manually construct a sequence of the cipher suites as follows:

```
// C++
FSSL::CipherSeq ciphers(2);
ciphers.length(2);
ciphers[0] = FSSL::RSA_WITH_RC4_128_MD5;
ciphers[1] = FSSL::RSA_WITH_RC4_128_SHA;
```

```
// Java
com.ooc.FSSL.Cipher[] ciphers =
{
    com.ooc.FSSL.Cipher.RSA_WITH_RC4_128_MD5.value,
    com.ooc.FSSL.Cipher.RSA_WITH_RC4_128_SHA.value,
};
```

Trust decision

The application itself must be responsible for a determination of whether a certificate chain is trusted or not. To do this the application should provide an implementation of the TrustDecider interface.

```
interface TrustDecider
{
boolean is_trusted(in CertificateSeq chain);
};
```

The is_trusted method is called when each new connection is established or accepted. The trust decider can assume that the provided certificate chain is valid and good. That means that each certificate in the chain is signed by the next certificate and the last is self signed. If true is returned then the chain is trusted, and the connection may continue. If false is returned then the connection is rejected.

This example trust decider only trusts those certificates directly signed by some mythical certificate authority CA-X.

```
// C++
class MyTrustDecider : public FSSL::TrustDecider
{
//
// CA-X certificate
//
FSSL::Certificate_var cert_;

public:
MyTrustDecider(FSSL::Manager_ptr fsslManager)
{
    FSSL::OctetSeq_var data = FSSL::load_file("cax.der");
    cert_ = fsslManager -> create_certificate(data);
}

virtual CORBA::Boolean
is_trusted(const FSSL::CertificateSeq& chain)
{
    if(chain.length() == 2)
    return chain[1] -> is_signed_by(cert_);
    return false;
}
};
```

```
// Java
final class MyTrustDecider extends com.ooc.CORBA.LocalObject
implements com.ooc.FSSL.TrustDecider
{
//
// CA-X certificate
//
com.ooc.FSSL.Certificate cert_;

MyTrustDecider(com.ooc.FSSL.Manager fsslManager)
{
    cert_ = fsslManager.create_creatificate(
    com.ooc.FSSL.FSSL.load_file("cax.der"));
}

public bool
is_trusted(com.ooc.FSSL.Certificate[] chain)
{
    if(chain.length == 2)
    return chain[i].is_signed_by(cert_);
    return false;
}
}
```

Protocols

Secure protocols can be set when creating a context programmatically. Call the appropriate `FSSL::Manager2::create_context`:

```
// C++
FSSL::ContextID id = fsslManager.create_context_with_protocols(
myChain, myKey, myPassPhrase, myDecider, myCiphers, myProtocols);

FSSL::ContextID id = fsslManager.create_pkcs12_context_with_protocols(
pkcs12_certificate, myPassPhrase, myDecider, myCiphers, myProtocols);

FSSL::ContextID id = fsslManager.create_anon_context_with_protocols(
myCiphers, myProtocols);
```

```
// Java
int id = fsslManager.create_context_with_protocols(
myChain, myKey, myPassPhrase, myDecider, myCiphers, myProtocols);

int id =
   fsslManager.create_pkcs12_context_with_protocols(pkcs12_certificate,
myPassPhrase, myDecider, myCiphers, myProtocols);

int id = fsslManager.create_anon_context_with_protocols(myCiphers,
   myProtocols);
```

Each of these methods is passed a sequence of protocol identifiers. A common use case is to allow all the "TLS" protocols (TLSv1, TLSv1.1, and TLSv1.2), and a helper method `FSSL::getTLSProtocols()` is provided to do this.

```
// C++
FSSL::SecureProtocolSeq_var myProtocols = FSSL::getTLSProtocols();
```

```
// Java
int[] myProtocols = com.ooc.FSSL.FSSL.getTLSProtocols();
```

Other helper methods available are:

- `FSSL::getSSLV3_protocol()` returns the SSLv3 protocol.
- `FSSL::getTLSV1_protocol()` returns the TLSv1 protocol.
- `FSSL::getTLSV1_1_protocol()` returns the TLSv1.1 protocol.
- `FSSL::getTLSV1_2_protocol()` returns the TLSv1.2 protocol.

If none of these helper methods supplies the desired functionality it is possible to manually construct a sequence of the protocols as follows:

```
// C++
FSSL::SecureProtocolSeq myProtocols(2);
myProtocols.length(2);
myProtocols[0] = FSSL::TLSV1;
myProtocols[1] = FSSL::TLSV1_2;
```

```
// Java
int myProtocols[] =
{
    com.ooc.FSSL.TLSV1.value,
    com.ooc.FSSL.TLSV1_2.value
};
```

CHAPTER 2

Extending the Hello World Application

In order to demonstrate how to use the FSSL plug-in, the standard Hello World application included with Orbacus in the subdirectory demo/hello will be modified. The complete source code for this example is included with the FSSL distribution in the directory fssl/demo/hello.

In this chapter

This chapter contains the following sections:

Server Side Usage

Setting identity

A server application must provide its identity using a context.

```
// C++
//
// Create the servers certificate chain
//
FSSL::Certificate_var serverCert =
   fsslManager -> create_certificate(
FSSL::OctetSeq_var(FSSL::load_file("server.der")));
FSSL::Certificate_var caCert =
   fsslManager -> create_certificate(
FSSL::OctetSeq_var(FSSL::load_file("ca.der")));

FSSL::CertificateSeq chain;
chain.length(2);
chain[0] = serverCert;
chain[1] = caCert;

//
// Create the server context
//
FSSL::ContextID id = fsslManager -> create_context(
   chain,
   FSSL::OctetSeq_var(FSSL::load_file("server.key")),
   FSSL::PassPhrase_var(FSSL::string_to_PassPhrase("blahblah")),
   FSSL::TrustDecider_var(new TrustDecider_impl(caCert)),
   FSSL::CipherSeq_var(FSSL::get_RSA_ciphers()));
```

```
// Java

//
// Create the servers certificate chain
//
com.ooc.FSSL.Certificate serverCert =
    fsslManager.create_certificate(
        com.ooc.FSSL.FSSL.load_file("server.der"));
com.ooc.FSSL.Certificate caCert =
    fsslManager.create_certificate(
com.ooc.FSSL.FSSL.load_file("ca.der"));

com.ooc.FSSL.Certificate[] chain =
    new com.ooc.FSSL.Certificate[2];
chain[0] = serverCert;
chain[1] = caCert;

//
// Create the server context
//
int id = fsslManager.create_context(
    chain,
    com.ooc.FSSL.FSSL.load_file("server.key"),
    com.ooc.FSSL.FSSL.string_to_PassPhrase("blahblah"),
    new ServerTrustDecider(caCert),
    com.ooc.FSSL.FSSL.get_RSA_ciphers());
```

This example defines the certificate chain for the server. The server's X.509 certificate will be obtained from the file server.der. This certificate is authenticated by the certificate in the file ca.der. The private key of the server's certificate is contained in the file server.key and is decrypted using the passphrase foobar. In a real application it wouldn't be prudent to store the certificate's passphrase in plain text. Typically the pass-phrase should be requested from the user.

Once a context has been created, the next step is to call FSSL::create_poa_manager to initialize the server side of the FSSL connection. You can configure the RootPOA's POAManager simply by creating a POAManager name 'RootPOAManager'. Keep in mind that this step must be done prior to resolving the 'RootPOA' initial reference, otherwise the RootPOAManager will have already been created with the default configuration. The third and fourth arguments to FSSL::create_poa_manager are the reference to the FSSL::Manager and a ContextID which should be associated with the POAManager to be created. The associated ContextID identifies the SSL identity the server will use when establishing connections.

```
// C++
PortableServer::POAManager_var poaManager =
FSSL::create_poa_manager(
"RootPOAManager", orb, fsslManager, id, props);
```

```
// Java
org.omg.PortableServer.POAManager poaManager =
com.ooc.FSSL.FSSL.create_poa_manager(
"RootPOAManager", orb, fsslManager, id, props);
```

Determining peer identity

The FSSL::Current interface can be used if the server needs to determine the identity of the peer that invoked the current operation.

First a reference to the FSSL::Current object must be retrieved.

```
// C++
FSSL::Current_var fsslCurrent =
FSSL::Current::_narrow(CORBA::Object_var(
    orb -> resolve_initial_references("FSSLCurrent")));
```

```
// Java
com.ooc.FSSL.Current fsslCurrent =
com.ooc.FSSL.CurrentHelper.narrow(
    orb.resolve_initial_references("FSSLCurrent"));
```

Now the FSSL::Current:get_peer_certificate_chain can be used to determine the identity of the caller:

```
// C++
FSSL::CertificateSeq_var chain =
    fsslCurrent -> get_peer_certificate_chain();
```

```
// Java
com.ooc.FSSL.X509Certificate[] chain =
    fsslCurrent.getPeerCertificateChain();
```

The negotiated cipher can also be determined using the `FSSL::Current` object.

```
// C++
FSSL::Cipher cipher = fsslCurrent -> get_peer_cipher();
```

```
// Java
com.ooc.FSSL.Cipher cipher = fsslCurrent.get_peer_cipher();
```

If this method is called outside of the context of a server method invocation a `FSSL::Current::NoContext` exception is raised. If the current connection is not an SSL connection then a `FSSL::Current::NoPeer` exception is raised.

The negotiated secure protocol can be determined using the `FSSL::Current2` object.

Get the `FSSL::Current2` as follows:

```
// C++
FSSL::Current2_var fsslCurrent =
FSSL::Current2::_narrow(CORBA::Object_var(
orb -> resolve_initial_references("FSSLCurrent")));
```

```
// Java
com.ooc.FSSL.Current2 fsslCurrent =
   com.ooc.FSSL.Current2Helper.narrow(
    orb.resolve_initial_references("FSSLCurrent")
);
```

Obtain the negotiated secure protocol as follows:

```
// C++
CORBA::String_var protocol =
  FSSL::Protocol_to_string(fsslCurrent_ -> get_peer_protocol());
```

```
// Java
String protocol = com.ooc.FSSL.FSSL.Protocol_to_string(
    current_.get_peer_protocol()
);
```

If this method is called outside of the context of a server method invocation a `FSSL::Current::NoContext` exception is raised. If the current connection is not an SSL connection then a `FSSL::Current::NoPeer` exception is raised.

Client Side Usage

Setting identity

First a context must be created, as in the server case. Next a context policy must be created with the context id. Policies are a standard CORBA mechanism for controlling operational behavior, and are considered to be immutable objects. That is, once they have been created, they may not be changed. The set of policies associated with an object reference are also considered to be immutable.

```
// C++
CORBA::Policy_var contextPolicy = fsslManager ->
   create_context_policy(id);
```

```
// Java
org.omg.CORBA.Policy contextPolicy =
   fsslManager.create_context_policy(id);
```

The CORBA standard provides three methods to associate policies with object references.

ORB level policies

The ORB level policies are managed using the ORB Policy Manager, which is resolved through the initial reference ORBPolicyManager.

```
// C++
CORBA::PolicyManager_var policyManager =
    CORBA::PolicyManager::_narrow(CORBA::Object_var(
    orb -> resolve_initial_references("ORBPolicyManager")));
```

```
// Java
org.omg.CORBA.PolicyManager policyManager =
    org.omg.CORBA.PolicyManagerHelper.narrow(
    orb.resolve_initial_references("ORBPolicyManager"));
```

Through this interface the current set of ORB level policies can be examined and changed. The set of ORB level policies will be associated with every new object reference that is created by that ORB.

Therefore, to associate a context policy with every object reference created by the ORB, the policy should be set on the ORB Policy Manager.

```
// C++
CORBA::PolicyList pl(1);
pl.length(1);
pl[0] = contextPolicy;
policyManger -> add_policy_overrides(pl);
```

```
// Java
org.omg.CORBA.Policy[] pl = new org.omg.CORBA.Policy[1];
pl[0] = contextPolicy;
policyManager.add_policy_overrides(pl);
```

Object level policies

Once object references have been created it is possible to create, a new object reference with a different set of associated policies by calling set_policy_overrides on the object reference. (In Java, set_policy_overrides is not actually called on the object, but on a delegate created from the object.)

```
// C++
CORBA::PolicyList pl(1);
pl.length(1);
pl[0] = contextPolicy;
CORBA::Object_var obj =
    myObj -> _set_policy_overrides(pl, CORBA::ADD_OVERRIDE);
```

```
// Java
org.omg.CORBA.Policy[] pl = new org.omg.CORBA.Policy[1];
pl[0] = contextPolicy;
com.ooc.CORBA.Delegate delegate = (com.ooc.CORBA.Delegate)
    ((org.omg.CORBA.portable.ObjectImpl)myObj)._get_delegate();
org.omg.CORBA.Object obj = delegate.set_policy_overrides(
pl, org.omg.CORBA.SetOverrideType.ADD_OVERRIDE);
```

Once set_policy_overrides has been called, the returned object reference will have a new set of associated policies. Note that the original object reference is not affected.

Thread level policies

A thread of execution in the application may have an associated set of policies. For the purposes of the SSL plug-in the context policy is not considered to be a thread level policy.

Full example

The following is the full example:

```
// C++
//
// Create the clients certificate chain
//
FSSL::Certificate_var clientCert =
   fsslManager -> create_certificate(
FSSL::OctetSeq_var(FSSL::load_file("client.der")));
FSSL::Certificate_var caCert =
   fsslManager -> create_certificate(
       FSSL::OctetSeq_var(FSSL::load_file("ca.der")));

FSSL::CertificateSeq chain;
chain.length(2);
chain[0] = clientCert;
chain[1] = caCert;

//
// Create the client context
//
FSSL::ContextID id = fsslManager -> create_context(
   chain,
   FSSL::OctetSeq_var(FSSL::load_file("client.key")),
   FSSL::PassPhrase_var(FSSL::string_to_PassPhrase("blahblah")),
   FSSL::TrustDecider_var(new TrustDecider_impl(caCert)),
   FSSL::CipherSeq_var(FSSL::get_RSA_ciphers()));
CORBA::PolicyManager_var policyManager =
    CORBA::PolicyManager::_narrow(CORBA::Object_var(
    orb -> resolve_initial_references("ORBPolicyManager")));
CORBA::PolicyList pl(1);
pl.length(1);
pl[0] = fsslManager -> create_context_policy(id);
policymanger -> add_policy_overrides(pl);
```

```
// Java
//
// Create the client certificate chain
//
com.ooc.FSSL.Certificate clientCert =
    fsslManager.create_certificate(
        com.ooc.FSSL.FSSL.load_file("client.der"));
com.ooc.FSSL.Certificate caCert =
    fsslManager.create_certificate(
        com.ooc.FSSL.FSSL.load_file("ca.der"));

com.ooc.FSSL.Certificate[] chain =
    new com.ooc.FSSL.Certificate[2];
chain[0] = clientCert;
chain[1] = caCert;

//
// Create the client context
//
int id = fsslManager.create_context(
    chain,
    com.ooc.FSSL.FSSL.load_file("client.key"),
    com.ooc.FSSL.FSSL.string_to_PassPhrase("blahblah"),
    new ClientTrustDecider(caCert),
    com.ooc.FSSL.FSSL.get_RSA_ciphers());
org.omg.CORBA.PolicyManager policyManager =
    org.omg.CORBA.PolicyManagerHelper.narrow(
    orb.resolve_initial_references("ORBPolicyManager"));
org.omg.CORBA.Policy[] pl = new org.omg.CORBA.Policy[1];
pl[0] = fsslManager.create_context_policy(id);
policyManager.add_policy_overrides(pl);
```

Determining Peer Identity

Before the client can determine the identity of the peer it must first get the OCI::FSSLIOP::TransportInfo. The client accomplishes this by calling _non_existent() on the object reference to force the connection and then narrowing the OCI::TransportInfo.

```
// C++
OCI::FSSLIOP::TransportInfo_var fssliopInfo;
if(!obj -> _non_existent())
{
OCI::TransportInfo_var info obj -> _get_oci_transport_info();
fssliopInfo = OCI::FSSLIOP::TransportInfo::_narrow(info);
}
```

```
// Java
com.ooc.OCI.FSSLIOP.TransportInfo fssliopInfo = null;
if(!obj._non_existent())
{
org.omg.CORBA.portable.ObjectImpl objImpl =
(org.omg.CORBA.portable.ObjectImpl)obj;
com.ooc.CORBA.Delegate objDelegate =
(com.ooc.CORBA.Delegate)objImpl._get_delegate();

com.ooc.OCI.TransportInfo info =
objDelegate.get_oci_transport_info();
fssliopInfo =
   com.ooc.OCI.FSSLIOP.TransportInfoHelper.narrow(info);
}
```

Once a reference to the FSSLIOP transport information is acquired, OCI::FSSLIOP::TransportInfo::certificate_chain can be used to determine the identity of the caller:

```
// C++
FSSL::CertificateSeq_var chain =
fssliopInfo -> certificate_chain();
```

```
// Java
com.ooc.FSSL.Certificate[] chain =
fssliopInfo.certificate_chain();
```

The negotiated cipher can be determined using the OCI::FSSLIOP::TransportInfo::negotiated_cipher.

```
// C++
FSSL::Cipher cipher = fssliopInfo -> negotiated_cipher();
```

```
// Java
com.ooc.FSSL.Cipher cipher = fssliopInfo.negotiated_cipher();
```

The negotiated secure protocol can be determined using the `OCI::FSSLIOP::TransportInfo2::negotiated_protocol`.

Get the `OCI::FSSLIOP::TransportInfo2` as follows:

```
// C++
OCI::FSSLIOP::TransportInfo2_var fssliopInfo;
if(!obj -> _non_existent())
{
OCI::TransportInfo_var info obj -> _get_oci_transport_info();
fssliopInfo = OCI::FSSLIOP::TransportInfo2::_narrow(info);
}
```

```
// Java
com.ooc.OCI.FSSLIOP.TransportInfo2 fssliopInfo = null;
if(!obj._non_existent())
{
    org.omg.CORBA.portable.ObjectImpl objImpl =
        (org.omg.CORBA.portable.ObjectImpl)obj;
    com.ooc.CORBA.Delegate objDelegate =
        (com.ooc.CORBA.Delegate)objImpl._get_delegate();

    com.ooc.OCI.TransportInfo info =
        objDelegate.get_oci_transport_info();
    fssliopInfo =
   com.ooc.OCI.FSSLIOP.TransportInfo2Helper.narrow(info);
}
```

Obtain the negotiated secure protocol as follows:

```
// C++
CORBA::String_var protocol =
        FSSL::Protocol_to_string(fssliopInfo ->
   negotiated_protocol());
```

```
// Java
String protocol = com.ooc.FSSL.FSSL.Protocol_to_string(
                      fssliopInfo.negotiated_protocol()
                      )
```

Preventing Connections to Secure/Insecure Servers

In developing your applications you may want to restrict the servers to which your proxy will connect. For instance, you may want to connect only with secure servers, or alternatively only with insecure servers.

To do this, a ProtocolPolicy policy must be used. The ProtocolPolicy is used to restrict the protocol that will be used to establish communications. By default, after initializing the FSSL plug-in, a protocol policy with a value of OCI::FSSLIOP::PLUGIN_ID is set as an ORB level policy. Therefore, only secure connections will be established unless this is overridden. To allow an object reference to use IIOP the protocol policy can be overridden on the reference as follows:

```
// C++
CORBA::Any any;
any <<= OCI::IIOP::PLUGIN_ID;
CORBA::PolicyList pl(1);
pl.length(1);
pl[0] = orb -> create_policy(OB::PROTOCOL_POLICY_ID, any);
CORBA::Object_var myObj = obj -> _set_policy_overrides(
    pl, CORBA::ADD_OVERRIDE);
```

```
// Java
org.omg.CORBA.Any any = orb_.create_any();
   any.insert_ulong(com.ooc.OCI.IIOP.PLUGIN_ID.value);
org.omg.CORBA.Policy[] pl = new org.omg.CORBA.Policy[1];
pl[0] = orb.create_policy(
    com.ooc.OB.PROTOCOL_POLICY_ID.value, any);
com.ooc.CORBA.Delegate delegate = (com.ooc.CORBA.Delegate)
    ((org.omg.CORBA.portable.ObjectImpl)myObj)._get_delegate();
org.omg.CORBA.Object obj = delegate.set_policy_overrides(
    myObj, pl, org.omg.CORBA.SetOverrideType.ADD_OVERRIDE);
```

If it is necessary to revert to a secure transport again for establishing further connections (for instance: case of a client creating successive connections to secure and insecure servers), simply reapply the OCI::FSSLIOP::PLUGIN_ID protocol policy as needed.

Complete Example

Certificates

First the certificates must be created for both the client and the server. For a real world application the certificates will most likely be provided by an actual certificate authority. However, for the purposes of this demo we'll generate the certificates by hand.

OpenSSL

Use the `openssl` command to create the certificate authority, client and server certificates. The command will require an OpenSSL configuration file named `openssl.cnf`. This can be obtained from the OpenSSL install area created when OpenSSL was built and installed. The commands below may require slight modifications, depending on the contens of the `openssl.cnf` file.

Create the certificate authority "ca.der" as follows:

```
openssl genrsa -des3 -out ca_key.pem 2048  [passphrase:  blahblah]

openssl req -new -x509 -days 3650 -set_serial 0 -key ca_key.pem -out
   cacert.pem -subj "/C=CA/ST=Newfoundland/L=St John's/O=IONA
   Technologies/OU=Team Orbacus/CN=FSSL demo
   CA/emailAddress=fssldemo@orbacus.com"

openssl x509 -outform der -in cacert.pem -out ca.der
```

Create the client certificate "client.der" and private key "client.key" as follows:

```
openssl genrsa -des3 -out client.key.pem 2048  [passphrase:  blahblah]

openssl req -new -subj "/C=CA/ST=Newfoundland/L=St John's/O=IONA
   Technologies/OU=Team Orbacus/CN=FSSL demo
   Client/emailAddress=fssldemo@orbacus.com" -out client.csr -key
   client.key.pem

openssl x509 -req -in client.csr -days 3650 -set_serial 1 -out
   client_cert.pem -CAkey ca_key.pem -CA cacert.pem -sha256
   -extensions usr_cert -extfile openssl.cnf

openssl x509 -outform der -in client_cert.pem -out client.der

openssl pkcs8 -outform DER -inform PEM -in client.key.pem -out
   client.key -topk8     [passphrase:  blahblah]
```

Create the server certificate "server.der" and private key "server.key" as follows:

```
openssl genrsa -des3 -out server.key.pem 2048  [passphrase:  blahblah]

openssl req -new -subj "/C=CA/ST=Newfoundland/L=St John's/O=IONA
   Technologies/OU=Team Orbacus/CN=FSSL demo
   Server/emailAddress=fssldemo@orbacus.com" -out server.csr -key
   server.key.pem

openssl x509 -req -in server.csr -days 3650 -set_serial 2 -out
   server_cert.pem -CAkey ca_key.pem -CA cacert.pem -sha256
   -extensions usr_cert -extfile
   /users/devp/johnd/openssl_conf/openssl.cnf

openssl x509 -outform der -in server_cert.pem -out server.der

openssl pkcs8 -outform DER -inform PEM -in server.key.pem -out
   server.key -topk8    [passphrase:  blahblah]
```

Client Side

main

First initialize the ORB.

```
// C++
int
main(int argc, char* argv[], char*[])
{
    int status = EXIT_SUCCESS;
    CORBA::ORB_var orb;

    try
    {
#if !defined(HAVE_SHARED) && !defined(FSSL_DLL)
     //
     // When linking statically, we need to explicitly register the
     // plug-in prior to ORB initialization
     //
     OCI::register_plugin("fssliop", OCI_init_fssliop);
#endif

        orb = CORBA::ORB_init(argc, argv);
        status = run(orb, argc, argv);
    }
    catch(const CORBA::Exception& ex)
    {
        cerr << ex << endl;
        status = EXIT_FAILURE;
    }

    if(!CORBA::is_nil(orb))
    {
        try
        {
            orb -> destroy();
        }
        catch(const CORBA::Exception& ex)
           cerr << ex << endl;
           status = EXIT_FAILURE;
        }
    }

    return status;
}
```

```
// Java

public static void
main(String args[])
{
       int status = 0;
       org.omg.CORBA.ORB orb = null;

       java.util.Properties props = System.getProperties();
       props.put("org.omg.CORBA.ORBClass", "com.ooc.CORBA.ORB");
       props.put("org.omg.CORBA.ORBSingletonClass",
                  "com.ooc.CORBA.ORBSingleton");

        try
        {
            orb = org.omg.CORBA.ORB.init(args, props);
            status = run(orb, args);
        }
        catch(Exception ex)
        {
            ex.printStackTrace();
            status = 1;
        }

        if(orb != null)
        {
            try
            {
                orb.destroy();
            }
            catch(Exception ex)
            {
                ex.printStackTrace();
                status = 1;
            }
        }

        System.exit(status);
    }
```

run

Next obtain a reference to the FSSL Context Manager.

```
// C++
int
run(CORBA::ORB_ptr orb, int argc, char* argv[])
{
    //
    // Initialize the FSSL plug-in.
    //
    cout << "Please wait..." << endl;
    CORBA::Object_var fsslManagerObj =
       orb -> resolve_initial_references("FSSLContextManager");
   FSSL::Manager_var fsslManager = FSSL::Manager::_narrow(fsslManagerObj);
```

```
// Java

static int
run(org.omg.CORBA.ORB orb, String[] args)
throws org.omg.CORBA.UserException
{
//
    // Obtain the ORB's property set
    //
    java.util.Properties props =
   ((com.ooc.CORBA.ORB)orb).properties();

    //
    // Resolve the FSSL Context Manager
    //
    com.ooc.FSSL.Manager fsslManager =
    com.ooc.FSSL.ManagerHelper.narrow(
    orb.resolve_initial_references("FSSLContextManager"));
```

Next the client's certificate chain must be constructed.

```
// C++

    //
    // Create the clients certificate chain
    //
    FSSL::Certificate_var clientCert =
    fsslManager -> create_certificate(
        FSSL::OctetSeq_var(FSSL::load_file("client.der")));
    FSSL::Certificate_var caCert =
    fsslManager -> create_certificate(
    FSSL::OctetSeq_var(FSSL::load_file("ca.der")));

FSSL::CertificateSeq chain;
chain.length(2);
chain[0] = clientCert;
chain[1] = caCert;
```

```
// Java
    //
    // Create the client certificate chain
    //
    com.ooc.FSSL.Certificate clientCert =
    fsslManager.create_certificate(
        com.ooc.FSSL.FSSL.load_file("client.der"));
    com.ooc.FSSL.Certificate caCert =
    fsslManager.create_certificate(
        com.ooc.FSSL.FSSL.load_file("ca.der"));

    com.ooc.FSSL.Certificate[] chain =
    new com.ooc.FSSL.Certificate[2];
    chain[0] = clientCert;
    chain[1] = caCert;
```

Once that has been done a context must be created. For this demo all RSA ciphers can be used. The implementation of the TrustDecider will come a little later.

```
// C++

//
// Create the client context
//
FSSL::ContextID id = fsslManager -> create_context(
chain,
FSSL::OctetSeq_var(FSSL::load_file("client.key")),
FSSL::PassPhrase_var(FSSL::string_to_PassPhrase("blahblah")),
FSSL::TrustDecider_var(new TrustDecider_impl(caCert)),
FSSL::CipherSeq_var(FSSL::get_RSA_ciphers()));
```

```
// Java

    //
    // Create the client context
    //
    int id = fsslManager.create_context(
    chain,
    com.ooc.FSSL.FSSL.load_file("client.key"),
    com.ooc.FSSL.FSSL.string_to_PassPhrase("blahblah"),
    new ClientTrustDecider(caCert),
    com.ooc.FSSL.FSSL.get_RSA_ciphers());
```

After that the context should be set as the default context for all object references.

```
// C++

//
// Set this as the default context for all object references
//
fsslManager -> set_context(id);
```

```
// Java

    //
    // Set this as the default context for all object references
    //
    fsslManager.set_context(id);
```

After this has been done the remainder of run will be the same as the original demo.

```
// C++

//
// Get "hello" object
//
CORBA::Object_var obj = orb ->
   string_to_object("relfile:/Hello.ref");
if(CORBA::is_nil(obj))
{
cerr << argv[0] << ": cannot read IOR from Hello.ref" << endl;
    return EXIT_FAILURE;
}

Hello_var hello = Hello::_narrow(obj);
assert(!CORBA::is_nil(hello));

//
// Main loop
//
cout << "Enter 'h' for hello or 'x' for exit:\n";
char c;
do
{
    cout << "> ";
    cin >> c;
    if(c == 'h')
    hello -> say_hello();
}
while(cin.good() && c != 'x');

return EXIT_SUCCESS;
}
```

```
// Java
//
// Get "hello" object
//
org.omg.CORBA.Object obj = orb.string_to_object("relfile:/Hello.ref");
if(obj == null)
        {
     System.err.println("hello.Client: cannot read IOR from Hello.ref");
     return 1;
}
Hello hello = HelloHelper.narrow(obj);
//
// Java is slow so we force the client to perform the handshake immediately.
//
System.out.println("Please wait...");
obj._non_existent();

//
// Main loop
//
System.out.println("Enter 'h' for hello or 'x' for exit:");

int c;

try
{
    String input;
    java.io.DataInputStream dataIn =
         new java.io.DataInputStream(System.in);
    java.io.BufferedReader in = new java.io.BufferedReader(
         new java.io.InputStreamReader(dataIn));
    do
    {
        System.out.print("> ");
        input = in.readLine();

        if(input.equals("h"))
            hello.say_hello();
    }
    while(!input.equals("x"));
}
catch(java.io.IOException ex)
{
    System.err.println("Can't read from `" + ex.getMessage() + "'");
    return 1;
        }
return 0;
}
```

Trust decider

The TrustDecider implementation for the demo will be extremely simple. It will trust only those certificates directly signed by the provided CA. To implement the TrustDecider the class FSSL_TrustDecider must be implemented. In addition on the client side only the server will be trusted.

```
// C++

class TrustDecider_impl : public FSSL::TrustDecider
```

```
// Java

class ClientTrustDecider extends com.ooc.CORBA.LocalObject
    implements com.ooc.FSSL.TrustDecider
```

Next the private members and constructor.

```
// C++

    FSSL::Certificate_var ca_;

public:

    TrustDecider_impl(FSSL::Certificate_var ca)
    : ca_(FSSL::Certificate::_duplicate(ca))
    {
    }
```

```
// Java

    private com.ooc.FSSL.Certificate ca_;

    ClientTrustDecider(com.ooc.FSSL.Certificate ca)
    {
    ca_ = ca;
    }
```

Next, is_trusted must be implemented.

```
// C++

virtual CORBA::Boolean
is_trusted(const FSSL::CertificateSeq& chain)
```

```
// Java

public boolean
is_trusted(com.ooc.FSSL.Certificate[] chain)
```

This method should ensure that the CA in the certificate chain is the CA provided by the constructor. To do that it should be verified that the CA has signed the last certificate in the chain (since CA certificates are self signed), and that the subject distinguished names are the same. In addition the common name portion of the server side certificate will be examined to ensure that only the server is accepted. Note that for a real world example more than just the common name should be validated, since it's possible that the common name is the same for two certificates.

```
// C++

CORBA::String_var serverDN = chain[0] -> subject_DN();
if(strstr(serverDN, "CN=FSSL demo Server") == 0)
    return false;
if(chain.length() == 2 && chain[1] -> is_signed_by(ca_))
{
    CORBA::String_var dn1 = chain[1] -> subject_DN();
    CORBA::String_var dn2 = ca_ -> subject_DN();
    if(strcmp(dn1, dn2) == 0)
    return true;
}
return false;
```

```
// Java

String serverDN = chain[0].subject_DN();
if(serverDN.indexOf("CN=FSSL demo Server") == -1)
return false;

if(chain.length == 2 && chain[1].is_signed_by(ca_))
{
String dn1 = chain[1].subject_DN();
String dn2 = ca_.subject_DN();
if(dn1.equals(dn2))
return true;
}
return false;
```

Server Side

main

First initialize the ORB.

```
// C++
int
main(int argc, char* argv[], char*[])
{
    int status = EXIT_SUCCESS;
    CORBA::ORB_var orb;

    try
    {
#if !defined(HAVE_SHARED) && !defined(FSSL_DLL)
   //
   // When linking statically, we need to explicitly register the
   // plug-in prior to ORB initialization
   //
   OCI::register_plugin("fssliop", OCI_init_fssliop);
#endif

      orb = CORBA::ORB_init(argc, argv);
      status = run(orb, argc, argv);
    }
    catch(const CORBA::Exception& ex)
    {
        cerr << ex << endl;
status = EXIT_FAILURE;
    }

    if(!CORBA::is_nil(orb))
    {
        try
        {
             orb -> destroy();
        }
        catch(const CORBA::Exception& ex)
        {
            cerr << ex << endl;
            status = EXIT_FAILURE;
        }
    }

    return status;
}
```

```
// Java

public static void
main(String args[])
{
int status = 0;
org.omg.CORBA.ORB orb = null;

java.util.Properties props = System.getProperties();
    props.put("org.omg.CORBA.ORBClass", "com.ooc.CORBA.ORB");
    props.put("org.omg.CORBA.ORBSingletonClass",
      "com.ooc.CORBA.ORB");

    try
    {
    orb = org.omg.CORBA.ORB.init(args, props);
status = run(orb, args);
}
catch(Exception ex)
{
ex.printStackTrace();
status = 1;
}

if(orb != null)
{
try
{
((com.ooc.CORBA.ORB)orb).destroy();
}
catch(Exception ex)
{
ex.printStackTrace();
status = 1;
}
}

System.exit(status);
}
```

run

Next obtain a reference to the FSSL Context Manager.

```
// C++

int
run(CORBA::ORB_ptr orb, int argc, char* argv[])
{
    OBCORBA::ORB_var oborb = OBCORBA::ORB::_narrow(orb);

    //
    // Obtain the ORB's property set
    //
    OB::Properties_var props = oborb -> properties();

    //
    // Resolve the FSSL Context Manager
    //
    CORBA::Object_var fsslManagerObj =
    orb -> resolve_initial_references("FSSLContextManager");
    FSSL::Manager_var fsslManager =
   FSSL::Manager::_narrow(fsslManagerObj);
```

```
// Java

static int
run(org.omg.CORBA.ORB orb, String[] args)
throws org.omg.CORBA.UserException
{
//
    // Obtain the ORB's property set
    //
    java.util.Properties props =
   ((com.ooc.CORBA.ORB)orb).properties();

    //
    // Resolve the FSSL Context Manager
    //
    com.ooc.FSSL.Manager fsslManager =
    com.ooc.FSSL.ManagerHelper.narrow(
    orb.resolve_initial_references("FSSLContextManager"));
```

Next the certificate chain for the server must be created. This is exactly the same procedure as for the client.

```
// C++

    //
    // Create the servers certificate chain
    //
    FSSL::Certificate_var serverCert =
    fsslManager -> create_certificate(
        FSSL::OctetSeq_var(FSSL::load_file("server.der")));
    FSSL::Certificate_var caCert =
    fsslManager -> create_certificate(
    FSSL::OctetSeq_var(FSSL::load_file("ca.der")));

FSSL::CertificateSeq chain;
chain.length(2);
chain[0] = serverCert;
chain[1] = caCert;
```

```
// Java

    //
    // Create the server certificate chain
    //
    com.ooc.FSSL.Certificate serverCert =
    fsslManager.create_certificate(
        com.ooc.FSSL.FSSL.load_file("server.der"));
    com.ooc.FSSL.Certificate caCert =
    fsslManager.create_certificate(
        com.ooc.FSSL.FSSL.load_file("ca.der"));

    com.ooc.FSSL.Certificate[] chain =
    new com.ooc.FSSL.Certificate[2];
    chain[0] = serverCert;
    chain[1] = caCert;
```

Once that has been done a context must be created. For this demo all RSA ciphers can be used. The implementation of the TrustDecider will come a little later.

```
// C++

//
// Create the server context
//
FSSL::ContextID id = fsslManager -> create_context(
chain,
FSSL::OctetSeq_var(FSSL::load_file("server.key")),
FSSL::PassPhrase_var(FSSL::string_to_PassPhrase("blahblah")),
FSSL::TrustDecider_var(new TrustDecider_impl(caCert)),
FSSL::CipherSeq_var(FSSL::get_RSA_ciphers()));
```

```
// Java

    //
    // Create the server context
    //
    int id = fsslManager.create_context(
    chain,
    com.ooc.FSSL.FSSL.load_file("server.key"),
    com.ooc.FSSL.FSSL.string_to_PassPhrase("blahblah"),
    new ClientTrustDecider(caCert),
    com.ooc.FSSL.FSSL.get_RSA_ciphers());
```

Once the SSL context has been created, the POAManager can be initialized and the boot manager resolved.

```
// C++

//
// Create the POA Manager
//
PortableServer::POAManager_var poaManager =
        FSSL::create_poa_manager(
            "RootPOAManager", orb, fsslManager, id, props);

//
// Create implementation object
//
Hello_impl* helloImpl = new Hello_impl();
Hello_var hello = helloImpl -> _this();

//
// Save reference
//
CORBA::String_var s = orb -> object_to_string(hello);

const char* refFile = "Hello.ref";
ofstream out(refFile);
if(out.fail())
{
    cerr << argv[0] << ": can't open `" << refFile << "': "
         << strerror(errno) << endl;
    return EXIT_FAILURE;
}

out << s << endl;
out.close();

//
// Register Hello object with the BootManager
//

// Resolve BootManager
CORBA::Object_var bmgrObj =
        orb -> resolve_initial_references("BootManager");
OB::BootManager_var bootManager = OB::BootManager::_narrow(bmgrObj);
```

```
// Create the object id
PortableServer::ObjectId_var hello_objId =
      PortableServer::string_to_ObjectId("Hello");

// Create the new binding
bootManager -> add_binding(hello_objId, hello);

//
// Run implementation
//
cout << "Server is ready." << endl;
poaManager -> activate();
orb -> run();

return EXIT_SUCCESS;
}
```

```
// Java
//
// Create the POA Manager
//
org.omg.PortableServer.POAManager poaManager =
    com.ooc.FSSL.FSSL.create_poa_manager(
        "RootPOAManager", orb, fsslManager, id, props);
//
// Create implementation object
//
Hello_impl helloImpl = new Hello_impl();
Hello hello = helloImpl._this(orb);

//
// Add reference to boot manager
//
try
{
    byte[] oid = ("Hello").getBytes();
    com.ooc.OB.BootManager bootManager =
       com.ooc.OB.BootManagerHelper.narrow(
          orb.resolve_initial_references("BootManager"));
    bootManager.add_binding(oid, hello);

catch(org.omg.CORBA.ORBPackage.InvalidName ex)

    throw new RuntimeException();
}
catch(com.ooc.OB.BootManagerPackage.AlreadyExists ex)
{
    throw new RuntimeException();
}

//
// Save reference
//
try
{
   String ref = orb.object_to_string(hello);
   String refFile = "Hello.ref";
   java.io.FileOutputStream file =
        new java.io.FileOutputStream(refFile);
   java.io.PrintWriter out = new java.io.PrintWriter(file);
   out.println(ref);
   out.flush();
   file.close();
}
```

```
catch(java.io.IOException ex)
{
   System.err.println("hello.Server: can't write to `" +
                   ex.getMessage() + "'");
   return 1;
        }

//
// Run implementation
//
System.out.println("Server is ready.");
poaManager.activate();
orb.run();

return 0;
}
```

Trust decider

The trust decider for the server is slightly different in that the distinguished name of the client is not validated since the server accepts connections from any client validated by the CA.

```
// C++

if(chain.length() == 2 && chain[1] -> is_signed_by(ca_))
{
    CORBA_String_var dn1 = chain[1] -> subject_DN();
    CORBA_String_var dn2 = ca_ -> subject_DN();
    if(strcmp(dn1, dn2) == 0)
    return true;
}
return false;
```

```
// Java

if(chain.length == 2 && chain[1].is_signed_by(ca_))
{
String dn1 = chain[1].subject_DN();
String dn2 = ca_.subject_DN();
if(dn1.equals(dn2))
return true;
}
return false;
```

APPENDIX A

FSSL Definitions

ADH
The anonymous Diffie-Hellman public-key algorithm, see [9].

ASN.1
Abstract Syntax Notation One, see [14].

DER
Distinguished Encoding Rules for ASN.1, see [4].

DES
Data Encryption Standard, see [12].

DSS
The Digital Signature Standard, see [11]

IDEA
International Data Encryption Algorithm, see [11].

MD5
RSA Data Security, Inc.'s MD5 message-digest algorithm, see [8].

PEM
Internet Privacy-Enhanced Mail, see [14]-[17].

PKCS#8
Private-Key Information Syntax Standard, see [18].

RC2, RC4

Rivest's Ciphers, variable-key-size encryption algorithms, see [11].

RSA

The RSA public-key cryptosystem, see [3].

SHA

Secure Hash Algorithm, see [7].

APPENDIX B

Toolkits Supported by FSSL

Supported toolkits

FSSL for C++ requires a third-party toolkit to operate correctly. FSSL for Java uses JSSE, supplied with the JDK.

DISCLAIMER: Micro Focus does not assume any responsibility for the purchase or licensing of any third-party product that is required to work with a particular version of the SSL plug-in. Any licensing issues that arise as a result of the use of any third party product is the sole responsibility of the purchaser.

OpenSSL

FSSL for C++ requires OpenSSL 1.0.2j. This is a public domain implementation of the Secure Sockets Layer version 3.0. Please see http://www.openssl.org for more information on this product.

JSSE

FSSL for Java supports the JSSE toolkit. JSSE is available from Oracle and is bundled with JDK 1.4 and above. Please see `http://www.oracle.com/technetwork/java/index.html` for more information on this product.

APPENDIX C

FSSL Reference

This appendix documents the FSSL interfaces.

In this appendix

This appendix contains the following sections:

Module CORBA

Interface index

Current

Provides information on the current connection.

Policy

Provides information on the current policy.

Aliases

PolicyList

```
typedef sequence<Policy> PolicyList;
```

PolicyType

```
typedef unsigned long PolicyType;
```

PolicyTypeSeq

```
typedef sequence<PolicyType> PolicyTypeSeq;
```

Module FSSL

Overview

The FSSL plug-in interfaces. This module allows for the configuration of the Secure Sockets Layer OCI plug-in.

Interface index

Certificate

X509 Certificate Interface

ContextPolicy

Context Policy Interface

Current

Provides information on the current connection.

Current2

Extends the Current interface to provide information on the secure protocol used.

Manager

Manager Interface

Manager2

Extends the Manager interface to allow the creation of contexts where the secure protocols to be used are specified.

TrustDecider

TrustDecider Interface allows users to provide custom certificate chain trust algorithms

Constants

BAD_CIPHER

```
const Cipher BAD_CIPHER = 0;
```

Identifies an invalid cipher

BAD_SECURE_PROTOCOL

```
const SecureProtocol BAD_SECURE_PROTOCOL = 0;
```

Identifies an invalid secure protocol

CONTEXT_POLICY

```
const CORBA::PolicyType CONTEXT_POLICY = 100;
```

Identifies the ContextPolicy.

DHE_DSS_EXPORT_WITH_DES40_CBC_SHA

```
const Cipher DHE_DSS_EXPORT_WITH_DES40_CBC_SHA = 14;
```

Key Exchange Algorithm DHE_DSS

Symmetric Encryption Algorithm DES(40)

MAC Encoding SHA

DHE_DSS_WITH_3DES_EDE_CBC_SHA

```
const Cipher DHE_DSS_WITH_3DES_EDE_CBC_SHA = 16;
```

Key Exchange Algorithm DHE_DSS

Symmetric Encryption Algorithm DES(168)

MAC Encoding SHA

DHE_DSS_WITH_DES_CBC_SHA

```
const Cipher DHE_DSS_WITH_DES_CBC_SHA = 15;
```

Key Exchange Algorithm DHE_DSS

Symmetric Encryption Algorithm DES(56)

MAC Encoding SHA

DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

```
const Cipher DHE_RSA_EXPORT_WITH_DES40_CBC_SHA = 11;
```

Key Exchange Algorithm DHE_RSA

MAC Encoding SHA

DHE_RSA_WITH_3DES_EDE_CBC_SHA

```
const Cipher DHE_RSA_WITH_3DES_EDE_CBC_SHA = 13;
```

Key Exchange Algorithm DHE_RSA

Symmetric Encryption Algorithm DES(168)

MAC Encoding SHA

DHE_RSA_WITH_DES_CBC_SHA

```
const Cipher DHE_RSA_WITH_DES_CBC_SHA = 12;
```

Key Exchange Algorithm DHE_RSA

Symmetric Encryption Algorithm DES(56)

MAC Encoding SHA

DH_anon_EXPORT_WITH_DES40_CBC_SHA

```
const Cipher DH_anon_EXPORT_WITH_DES40_CBC_SHA = 19;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm DES(40)

MAC Encoding SHA

DH_anon_EXPORT_WITH_RC4_40_MD5

```
const Cipher DH_anon_EXPORT_WITH_RC4_40_MD5 = 17;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm RC4(40)

MAC Encoding MD5

DH_anon_WITH_3DES_EDE_CBC_SHA

```
const Cipher DH_anon_WITH_3DES_EDE_CBC_SHA = 21;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm DES(168)

MAC Encoding SHA

DH_anon_WITH_DES_CBC_SHA

```
const Cipher DH_anon_WITH_DES_CBC_SHA = 20;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm DES(56)

MAC Encoding SHA

DH_anon_WITH_RC4_128_MD5

```
const Cipher DH_anon_WITH_RC4_128_MD5 = 18;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm RC4(128)

MAC Encoding MD5

RSA_EXPORT_WITH_DES40_CBC_SHA

```
const Cipher RSA_EXPORT_WITH_DES40_CBC_SHA = 8;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm DES(40)

MAC Encoding SHA

RSA_EXPORT_WITH_NULL_MD5

```
const Cipher RSA_EXPORT_WITH_NULL_MD5 = 1;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm NULL

MAC Encoding MD5

RSA_EXPORT_WITH_NULL_SHA

```
const Cipher RSA_EXPORT_WITH_NULL_SHA = 2;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm NULL

MAC Encoding MD5

RSA_EXPORT_WITH_RC2_CBC_40_MD5

```
const Cipher RSA_EXPORT_WITH_RC2_CBC_40_MD5 = 6;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm RC2(40)

MAC Encoding MD5

RSA_EXPORT_WITH_RC4_40_MD5

```
const Cipher RSA_EXPORT_WITH_RC4_40_MD5 = 3;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm RC4(40)

MAC Encoding MD5

RSA_WITH_3DES_EDE_CBC_SHA

```
const Cipher RSA_WITH_3DES_EDE_CBC_SHA = 10;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm DEC(168)

MAC Encoding SHA

RSA_WITH_DES_CBC_SHA

```
const Cipher RSA_WITH_DES_CBC_SHA = 9;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm DEC(56)

MAC Encoding SHA

RSA_WITH_IDEA_CBC_SHA

```
const Cipher RSA_WITH_IDEA_CBC_SHA = 7;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm IDEA(128)

MAC Encoding SHA

RSA_WITH_RC4_128_MD5

```
const Cipher RSA_WITH_RC4_128_MD5 = 4;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm RC4(128)

MAC Encoding MD5

RSA_WITH_RC4_128_SHA

```
const Cipher RSA_WITH_RC4_128_SHA = 5;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm RC4(128)

MAC Encoding SHA

RSA_WITH_AES_128_GCM_SHA256

```
const Cipher RSA_WITH_AES_128_GCM_SHA256 = 22;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm AESGCM(128)

MAC Encoding SHA256

RSA_WITH_AES_128_CBC_SHA256

```
const Cipher RSA_WITH_AES_128_CBC_SHA256 = 23;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm AES(128)

MAC Encoding SHA256

RSA_WITH_AES_128_CBC_SHA

```
const Cipher RSA_WITH_AES_128_CBC_SHA = 24;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm AES(128)

MAC Encoding SHA

RSA_WITH_AES_256_GCM_SHA384

```
const Cipher RSA_WITH_AES_256_GCM_SHA384 = 25;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm AESGCM(256)

MAC Encoding SHA384

RSA_WITH_AES_256_CBC_SHA256

```
const Cipher RSA_WITH_AES_256_CBC_SHA256 = 26;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm AES(256)

MAC Encoding SHA256

RSA_WITH_AES_256_CBC_SHA

```
const Cipher RSA_WITH_AES_256_CBC_SHA = 27;
```

Key Exchange Algorithm RSA

Symmetric Encryption Algorithm AES(256)

MAC Encoding SHA

DHE_DSS_WITH_AES_128_GCM_SHA256

```
const Cipher DHE_DSS_WITH_AES_128_GCM_SHA256 = 28;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm AESGCM(128)

MAC Encoding SHA256

DHE_DSS_WITH_AES_128_CBC_SHA256

```
const Cipher DHE_DSS_WITH_AES_128_CBC_SHA256 = 29;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm AES(128)

MAC Encoding SHA256

DHE_DSS_WITH_AES_128_CBC_SHA

```
const Cipher DHE_DSS_WITH_AES_128_CBC_SHA = 30;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm AES(128)

MAC Encoding SHA

DHE_DSS_WITH_AES_256_GCM_SHA384

```
const Cipher DHE_DSS_WITH_AES_256_GCM_SHA384 = 31;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm AESGCM(256)

MAC Encoding SHA384

DHE_DSS_WITH_AES_256_CBC_SHA256

```
const Cipher DHE_DSS_WITH_AES_256_CBC_SHA256 = 32;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm AES(256)

MAC Encoding SHA256

DHE_DSS_WITH_AES_256_CBC_SHA

```
const Cipher DHE_DSS_WITH_AES_256_CBC_SHA = 33;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm AES(256)

MAC Encoding SHA

DHE_RSA_WITH_AES_128_GCM_SHA256

```
const Cipher DHE_RSA_WITH_AES_128_GCM_SHA256 = 34;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm AESGCM(128)

MAC Encoding SHA256

DHE_RSA_WITH_AES_128_CBC_SHA256

```
const Cipher DHE_RSA_WITH_AES_128_CBC_SHA256 = 35;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm AES(128)

MAC Encoding SHA256

DHE_RSA_WITH_AES_128_CBC_SHA

```
const Cipher DHE_RSA_WITH_AES_128_CBC_SHA = 36;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm AES(128)

MAC Encoding SHA

DHE_RSA_WITH_AES_256_GCM_SHA384

```
const Cipher DHE_RSA_WITH_AES_256_GCM_SHA384 = 37;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm AESGCM(256)

MAC Encoding SHA384

DHE_RSA_WITH_AES_256_CBC_SHA256

```
const Cipher DHE_RSA_WITH_AES_256_CBC_SHA256 = 38;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm AES(256)

MAC Encoding SHA256

DHE_RSA_WITH_AES_256_CBC_SHA

```
const Cipher DHE_RSA_WITH_AES_256_CBC_SHA = 39;
```

Key Exchange Algorithm DH

Symmetric Encryption Algorithm AES(256)

MAC Encoding SHA

ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

```
const Cipher ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 = 40;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm AESGCM(128)

MAC Encoding SHA256

ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

```
const Cipher ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 = 41;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm AES(128)

MAC Encoding SHA256

ECDHE_ECDSA_WITH_AES_128_CBC_SHA

```
const Cipher ECDHE_ECDSA_WITH_AES_128_CBC_SHA = 42;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm AES(128)

MAC Encoding SHA

ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

```
const Cipher ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 = 43;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm AESGCM(256)

MAC Encoding SHA384

ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

```
const Cipher ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 = 44;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm AES(256)

MAC Encoding SHA384

ECDHE_ECDSA_WITH_AES_256_CBC_SHA

```
const Cipher ECDHE_ECDSA_WITH_AES_256_CBC_SHA = 45;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm AES(256)

MAC Encoding SHA

ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA

```
const Cipher ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA = 46;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm 3DES(168)

MAC Encoding SHA

ECDHE_ECDSA_WITH_RC4_128_SHA

```
const Cipher ECDHE_ECDSA_WITH_RC4_128_SHA = 47;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm RC4(128)

MAC Encoding SHA

ECDHE_RSA_WITH_AES_128_GCM_SHA256

```
const Cipher ECDHE_RSA_WITH_AES_128_GCM_SHA256 = 48;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm AESGCM(128)

MAC Encoding SHA256

ECDHE_RSA_WITH_AES_128_CBC_SHA256

```
const Cipher ECDHE_RSA_WITH_AES_128_CBC_SHA256 = 49;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm AES(128)

MAC Encoding SHA256

ECDHE_RSA_WITH_AES_128_CBC_SHA

```
const Cipher ECDHE_RSA_WITH_AES_128_CBC_SHA = 50;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm AES(128)

MAC Encoding SHA

ECDHE_RSA_WITH_AES_256_GCM_SHA384

```
const Cipher ECDHE_RSA_WITH_AES_256_GCM_SHA384 = 51;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm AESGCM(256)

MAC Encoding SHA384

ECDHE_RSA_WITH_AES_256_CBC_SHA384

```
const Cipher ECDHE_RSA_WITH_AES_256_CBC_SHA384 = 52;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm AES(256)

MAC Encoding SHA384

ECDHE_RSA_WITH_AES_256_CBC_SHA

```
const Cipher ECDHE_RSA_WITH_AES_256_CBC_SHA = 53;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm AES(256)

MAC Encoding SHA

ECDHE_RSA_WITH_3DES_EDE_CBC_SHA

```
const Cipher ECDHE_RSA_WITH_3DES_EDE_CBC_SHA = 54;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm 3DES(168)

MAC Encoding SHA

ECDHE_RSA_WITH_RC4_128_SHA

```
const Cipher ECDHE_RSA_WITH_RC4_128_SHA = 55;
```

Key Exchange Algorithm ECDH

Symmetric Encryption Algorithm RC4(128)

MAC Encoding SHA

SSLV3

```
const SecureProtocol SSLV3   = 1;
```

Identifies secure protocol SSLv3.

TLSV1

```
const SecureProtocol TLSV1   = 2;
```

Identifies secure protocol TLSv1.

TLSV1_1

```
const SecureProtocol TLSV1_1 = 3;
```

Identifies secure protocol TLSv1.1

TLSV1_2

```
const SecureProtocol TLSV1_2 = 4;
```

Identifies secure protocol TLSV1.2

BAD_SECURE_PROTOCOL

```
const SecureProtocol BAD_SECURE_PROTOCOL = 0;
```

Identifies an invalid protocol

Aliases

CertificateSeq

```
typedef sequence<Certificate> CertificateSeq;
```

Alias for an X509 Certificate Chain

Cipher

```
typedef unsigned long Cipher;
```

An alias for a cipher suite

CipherSeq

```
typedef sequence<Cipher> CipherSeq;
```

Alias for a sequence of Ciphers

ContextID

```
typedef unsigned long ContextID;
```

Alias for Context ID.

OctetSeq

```
typedef sequence<octet> OctetSeq;
```

Alias for sequences of octets

PassPhrase

```
typedef sequence<octet> PassPhrase;
```

Alias for a PassPhrase

PrivateKey

```
typedef sequence<octet> PrivateKey;
```

Alias for a PrivateKey

SecureProtocol

```
typedef unsigned long SecureProtocol;
```

Alias for a secure protocol.

SecureProtocolSeq

```
typedef sequence<SecureProtocol> SecureProtocolSeq;
```

Alias for a sequence of SecureProtocols.

Module IOP

Constants

CodeSets

```
const ServiceId CodeSets = 1;
```

TAG_INTERNET_IOP

```
const ProfileId TAG_INTERNET_IOP = 0;
```

TAG_MULTIPLE_COMPONENTS

```
const ProfileId TAG_MULTIPLE_COMPONENTS = 1;
```

TransactionService

```
const ServiceId TransactionService = 0;
```

Structs

IOR

```
struct IOR
{
    string type_id;
    sequence<TaggedProfile> profiles;
};
```

ServiceContext

```
struct ServiceContext
{
    ServiceId context_id;
    sequence<octet> context_data;
};
```

TaggedComponent

```
struct TaggedComponent
{
    ComponentId tag;
    sequence<octet> component_data;
};
```

TaggedProfile

```
struct TaggedProfile
{
    ProfileId tag;
    sequence<octet> profile_data;
};
```

Aliases

ComponentId

```
typedef unsigned long ComponentId;
```

MultipleComponentProfile

```
typedef sequence<TaggedComponent> MultipleComponentProfile;
```

ProfileId

```
typedef unsigned long ProfileId;
```

ServiceContextList

```
typedef sequence<ServiceContext> ServiceContextList;
```

ServiceId

```
typedef unsigned long ServiceId;
```

Module OB

Interface index

ConnectionReusePolicy

The connection reuse policy.

ProtocolPolicy

The protocol policy.

ReconnectPolicy

The reconnect policy.

TimeoutPolicy

The timeout policy.

Constants

CONNECTION_REUSE_POLICY

```
const CORBA::PolicyType CONNECTION_REUSE_POLICY = 3;
```

This policy type identifies the connection reuse policy.

PROTOCOL_POLICY

```
const CORBA::PolicyType PROTOCOL_POLICY = 2;
```

This policy type identifies the protocol policy.

RECONNECT_POLICY

```
const CORBA::PolicyType RECONNECT_POLICY = 4;
```

This policy type identifies the reconnect policy.

TIMEOUT_POLICY

```
const CORBA::PolicyType TIMEOUT_POLICY = 5;
```

This policy type identifies the timeout policy.

FSSL Bibliography

[1] The SSL Protocol, Version 3.0, Transport Layer Security Working Group.

[2] ANSI X3.106, American National Standard for Information Systems-Data Link Encryption, American National Standards Institute, 1983.

[3] R. Rivest, A. Shamir, and L. M. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, v. 21, n. 2, Feb 1978, pp. 120-126.

[4] CCITT. Recommendation X.509: The Directory - Authentication Framework. 1988.

[5] SSLeay and SSLapps FAQ, T. J. Hudson, E. A. Young.

[6] iSaSiLk 2.0 User Manual, Institute for Applied Information Processing and Communications, Graz University of Technology, 1998.

[7] NIST FIPS PUB 180-1, Secure Hash Standard, National Institute of Standards and Technology, U.S. Department of Commerce, DRAFT, 31 May 1994.

[8] R. Rivest. RFC 1321: The MD5 Message Digest Algorithm, April 1992.

[9] W. Diffie and M. E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, V.IT-22, n. 6, Jun 1977, pp. 74-84.

[10] Marc Laukien, Uwe Seimet, Matthew Newhook, and Mark Spruiell, ORBacus For C++ and Java, Object Oriented Concepts, Inc.

[11] Bruce Schneier, Applied Cryptography, John Wiley & Sons, Inc.

[12] PUB 46-1 National Bureau of Standards. FIPS PUB 46-1: Data Encryption Standard. January 1988.

[13] CCITT. Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1). 1988.

[14] RFC 1421 Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures," RFC 1421 February 1993.

[15] RFC 1422 Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate- Based Key Management," RFC 1422, February 1993.

[16] RFC 1423 Balenson, D., "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers," RFC 1423, February 1993.

[17] RFC 1424 Kaliski, B., "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services," RFC 1424, February 1993.

[18] PKCS #8: Private-Key Information Syntax Standard, An RSA Laboratories Technical Note, Version 1.2, Revised November 1, 1993.