Java(TM) Cryptography Extension Policy Files

for the Java(TM) Platform, Standard Edition Runtime Environment

README

------------------------------------------------------------------------

Import and export control rules on cryptographic software vary from

country to country. The Java Cryptography Extension (JCE) architecture

allows flexible cryptographic key strength to be configured via the

jurisdiction policy files which are referenced by the "crypto.policy"

security property in the <java-home>/conf/security/java.security file.

By default, Java provides two different sets of cryptographic policy

files:

unlimited: These policy files contain no restrictions on cryptographic

strengths or algorithms

limited: These policy files contain more restricted cryptographic

strengths

These files reside in <java-home>/conf/security/policy in the "unlimited"

or "limited" subdirectories respectively.

Each subdirectory contains a complete policy configuration,

and subdirectories can be added/edited/removed to reflect your

import or export control product requirements.

Within a subdirectory, the effective policy is the combined minimum

permissions of the grant statements in the file(s) matching the filename

pattern "default\_\*.policy". At least one grant is required. For example:

limited = Export (all) + Import (limited) = Limited

unlimited = Export (all) + Import (all) = Unlimited

The effective exemption policy is the combined minimum permissions

of the grant statements in the file(s) matching the filename pattern

"exempt\_\*.policy". Exemption grants are optional. For example:

limited = grants exemption permissions, by which the

effective policy can be circumvented.

e.g. KeyRecovery/KeyEscrow/KeyWeakening.

Please see the Java Cryptography Architecture (JCA) documentation for

additional information on these files and formats.

YOU ARE ADVISED TO CONSULT YOUR EXPORT/IMPORT CONTROL COUNSEL OR ATTORNEY

TO DETERMINE THE EXACT REQUIREMENTS.

Please note that the JCE for Java SE, including the JCE framework,

cryptographic policy files, and standard JCE providers provided with

the Java SE, have been reviewed and approved for export as mass market

encryption item by the US Bureau of Industry and Security.