Name

Key Management Console

Version

1.00

Synopsis

The Key Management Console (KMConsole) is the user interface for remote interaction with a Nanometrics system for the purpose of creating and manipulating DSA encryption keys.

Description

The following commands are supported by the Key Management Console:

1. generateKeyPair - This command generates a new DSA key pair on the security token using

specified DSA parameters and a unique key ID. The key ID can be specified by the user or automatically generated.

2. getPublicKey - This command retrieves the DSA public key value along with its parameters for the specified key ID.

3. changeKeyID - This command changes the key ID used to identify a specified key pair.

This allows the IDC to change the keyID for a keypair after it has been generated (e.g. to correspond to the serial number of a security certificate issued for

the public key).

4. getKeyList - This command retrieves the list of all key IDs currently defined.

5. setActiveKey - This command sets the key to be used for data authentication.

6. deleteKeyPair - This command deletes the specified key pair.

0. Exit - Exits the Key Management System.

Installation

See the Acquisition SUN Workstation Installation Guide. Copy all files in bin directory to /nmx/bin and all files in user to /nmx/user.

Environment

KMConsole is a Java Program and should be run with Java 1.2.2 or higher on Windows or Solaris.

Operation

KMConsole is invoked with the following syntax from a command line window under Solaris or Windows platforms.

KMConsole <destinationHost><destinationPort><modelName><SerialNumber>

The first two parameters are the IPAddress and UDP port of the network edge instrument and the latter two parameters are the instrument's model name and serial number. The IP address can be specified as a host name or in dotted notation and the UDP port and serial number must be specified in decimal. The network edge instrument refers to the closest instrument to the workstation running KMConsole. For example, if a Europa is sending serial data to the workstation via an RM-4, then the RM-4 IPAddress would be given. The model name still refers to the unit being managed; in our example, this is Europa. The model names must be one of the following: Lynx, Cygnus, Europa, or Janus.

Once invoked the command line menu will run and a command can be selected by typing its corresponding number followed by the enter key.

The user may be required to enter 3 types of inputs.

1. **Key Id** - This must be an integer from 0 - 4294967295 (unsigned 4 byte Integer value).

2. **DSA Parameters File** - The program accepts both Windows and Unix path names. The file specified must adhere to the Java Properties file syntax and contain the P, Q, and G DSA parameters. The parameters are hex representations of Big Integers and can be up to a maximum size of 256, 40, and 256 hex characters respectively for P, Q, and G. An example DSA Parameters File is included in this release. Note that the parameter identifiers in the file are case sensitive.

3. **Dest. Key Info File** - This is the destination file that the key and its parameters will be written to. The program accepts both Windows and Unix path names. A Sample output file is also included with this release.

The user may exit from a currently active command and go back to the Key Management Menu by simply pressing the Enter key with no input.

The user may exit the Key Management Console itself via the “exit” command from the main screen of the Key Management Menu.

This document information

G:\Manuals & graphics\Manuals\ReferenceManual\PCSoftware\KMConsole\1.00\KMConsole.lwp
Date created: 10/1/2002
Date last revised: 9/30/2002