SafeGuard CryptoServer

Utimaco CryptoServer CSP
and
Utimaco CryptoServer Key Storage Provider

Office Aachen
Germanusstrasse 4
D-52080 Aachen

Phone: ++49 241-1696-200

Telefax: ++49 241-1696-222

Internet: www.utimaco.de

E-Mail: info.sp@utimaco.de

Document-Number: 2008-0002

Document-Version: 1.3.0

Date: 06.03.2009

State of Release:

Author: Dipl.-Ing. Sven Kaltschmidt

Project ID:

Table of Contents

1 Introduction 1
2 Key Storage 2
3 Supported Algorithms 3
4 Authentication 4
5 Key Access Restriction 5
6 Backup / Restore of Keys 6
7 Installation / Prerequisites 7
8 Configuration 8
9 References 11

1 Introduction

This document describes the *Utimaco CryptoServer CSP and CNG provider* for Utimaco Safeware's hardware security module *CryptoServer*

CSP (Cryptographic Service Provider) is a general purpose cryptography standard developed by Microsoft. At the top side it defines an cryptographic interface to be used by applications (CryptoAPI), on the bottom side it defines an interface to be used by manufacturers in order to integrate their cryptographic hardware. With this concept the application must not know about specific drivers to access cryptographic hardware directly.

CNG (*Crypto Next Generation*) is a new cryptographic interface, which has been introduced on Vista and Windows Server 2008. It offers updated cryptographic algorithms and is intended as long term replacement of CSP. For now CSP is still supported on Vista and Windows Server 2008.

The *Utimaco CryptoServer CSP implements full RSA provider functionality.* To use this interface the firmware module CXI (cxi.mtc) must be loaded into the CryptoServer and the Utimaco Safeware's CSP library (cs2csp.dll) must be installed and registered on the host computer.

The *Utimaco CryptoServer Key Storage Provider* implements a CNG key storage interface. To use this interface the firmware module CXI (cxi.mtc) must be loaded into the CryptoServer and the Utimaco Safeware's CNG library (cs2cng.dll) must be installed and registered on the host computer.

Please refer to Microsoft's MSDN web pages for a detailed specification of the CSP / CNG functionality.

2 Key Storage

Cryptographic keys - regardless whether they are generated or imported - can be stored either internally on the CryptoServer or externally on the host computer. In this way different requirements can be fulfilled:

1. **Internal key storage**

   Keys are stored within the tamper protected area of the CryptoServer and automatically deleted in case of any physical or logical attack, which has been detected by the CryptoServer's sensory. The number of keys, which can be stored inside of the CryptoServer, depends on the keys size and the number and size of key properties and is only limited by the CryptoServer's storage capacity. Typical values are for example:

   - RSA, 1024 Bit ~ 5000 keys
   - ECDSA, NIST-P256 ~ 14000 keys

   This variant offers the highest security level.

2. **External key storage**

   Keys are stored within a special directory on the disk drive of the host computer. Each key is stored as a separate key blob file (*.kb), which is encrypted (AES 256 Bit) and signed with the CryptoServer's *Master Box Key* (MBK). As the MBK never leaves the CryptoServer keys are protected nearly as secure as if stored internally. On demand a key is automatically loaded into the CryptoServer in order to perform a cryptographic operation. The number of keys, which can be stored externally is only limited by the capacity of the disk drive.

   As the CryptoServer remains completely stateless fault tolerance is provided in this case if multiple CryptoServer containing the same Master Box Key are used. In error cases (e.g. lost network connection to the primary server), the provider automatically switches to another CryptoServer. Except from a possible delay the application doesn't recognize this operation.

   This variant offers the highest level of flexibility.

3 Supported Algorithms

The *Utimaco CryptoServer CSP* supports the following key algorithms:

Algoritm	***Key Sizes / Curves***
DES	56, 112 and 168 bit
AES	128, 192 and 256 bit
RSA	512 – 16384 bit (delta = 8bit)

The *Utimaco CryptoServer Key Storage Provider* supports the following key algorithms:

Algoritm	***Key Sizes / Curves***
DES	56, 112 and 168 bit
AES	128, 192 and 256 bit
RSA	512 – 16384 bit (delta = 1bit)
ECDSA	NIST-P256, NIST-P384, NIST-P521
ECDH	NIST-P256, NIST-P384, NIST-P521

The following hash algorithms are supported by both interfaces:

- SHA1
- RMD160
- SHA224
- SHA256
- MD5
- SHA384
- SHA512

4 Authentication

Before usage a mutual authentication is performed between host and CryptoServer by performing the following steps:

1. Creation of a secure messaging session between host and CryptoServer:
   - Host and CryptoServer exchange a session key (AES, 256 bit) by using the Diffie-Hellman key exchange mechanism.
   - Every subsequent communication is encrypted with this session key.

2. Authentication to the CryptoServer:
   - The host request a challenge value from the CryptoServer.
   - The host calculates a hash over user name, password and the challenge value and transmits the hash value to the CryptoServer.
   - The CryptoServer recalculates the hash value and grants access, if both hash values match.

3. Authentication to the host
   - The host creates a challenge value and transmits it to the CryptoServer
   - The CryptoServer signs the challenge value with its authentication key (ECDSA, NIST-P256) and returns the signature.
   - The host verifies the signature with the public part of the CryptoServer's authentication key.

Once configured on the host the above steps are automatically performed each time a connection to a CryptoServer is established. Additional authentication steps requesting user interaction is not necessary in order to operate unattended applications or services (e.g. a CA).

5 Key Access Restriction

In addition to the authentication described in the previous chapter, access to keys can be restricted for certain users in order to use the Utimaco CryptoServer Key Storage Provider in a multi-client environment.

Therefore every key is unambiguously assigned to a key group, which has to be given on key creation or import (an empty key group is only a special case, but no exception).

Key access for a certain user can be restricted by the CryptoServer's system administrator by adding the attribute 'CNG_GROUP=<pattern>' to the user account. If a user account doesn't contain this attribute no restriction will be applied. The pattern may contain wild cards to reflect graded access rights.

The following examples demonstrate the usage of user attributes:

CNG_GROUP=	***Description***
Test-CA01	the user is allowed to access the key group 'Test-CA01'
Test-CA02	the user is allowed to access the key group 'Test-CA02'
Test-CA0?	the user is allowed to access every key group named 'Test-CA0x' (e.g. Test-CA01 and Test-CA02)
Test-CA*	the user is allowed to access every key group beginning 'Test-CA'
-CA	the user is allowed to access every key group containing the pattern '-CA' in the middle

6 Backup / Restore of Keys

Even if keys are internally stored on the CryptoServer they can be backup up in a external key backup file (*.kbk). Key backup files are encrypted and signed with the CryptoServer's Master Box Key.

The syntax of the *cngtool* command line tool is as follows:

cngtool Name=<keyname> Spec=<keyspec> BackupKey[=<filename>]

Execute cngtool ListKeys to determine the parameters for <keyname> and <keyspec>. A specific file name can optionally be given as parameter, if none is given the file name is constructed according to the scheme: '<keyname>_<keyspec>.kbk'.

A key backup file can be restored to any CryptoServer, which contains the appropriate Master Box Key. In this way multiple CryptoServer can be synchronized (e.g. in order to contain the same CA's signature key).

The syntax of the *cngtool* command line tool is as follows:

cngtool RestoreKey=<filename>

If keys are stored externally, keys can be backed up or restored alternatively by either copying the complete key directory or single key blob files.

7 Installation / Prerequisites

In order to properly operate the *Utimaco CryptoServer CSP* and the *Utimaco CryptoServer Key Storage Provider* the following requirements must be met:

1. One or more CryptoServer must be available – either local (PCI) or remote (LAN).

2. The firmware module CXI has to be running on the CryptoServer.

   Therefore the firmware module package 'cxi_x.x.x.x.mpkg' has to be loaded into the CryptoServer (see [CS2ADMIN]).

3. The host software must be installed.

   Usually the installation program on the product CD automatically copies the files and registers the provider. Alternatively this can be done manually by simply copying the three files to the 'system32' directory:

   - cs2cng.dll
   - cs2cng.cpl
   - cngtool.exe
   - cs2csp.dll
   - csptool.exe

   The provider libraries must have been registered.

   Usually the installation program on the product CD automatically registers the provider. Alternatively this can be done manually by doing the following steps:

   - CSP

     Create the following registry key:

     [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\...

     …Provider\Utimaco CryptoServer CSP]

     Create the following values:

     - "Image Path"="cs2csp.dll"
     - "SigInFile"=dword:00000000
     - "Type"=dword:00000001

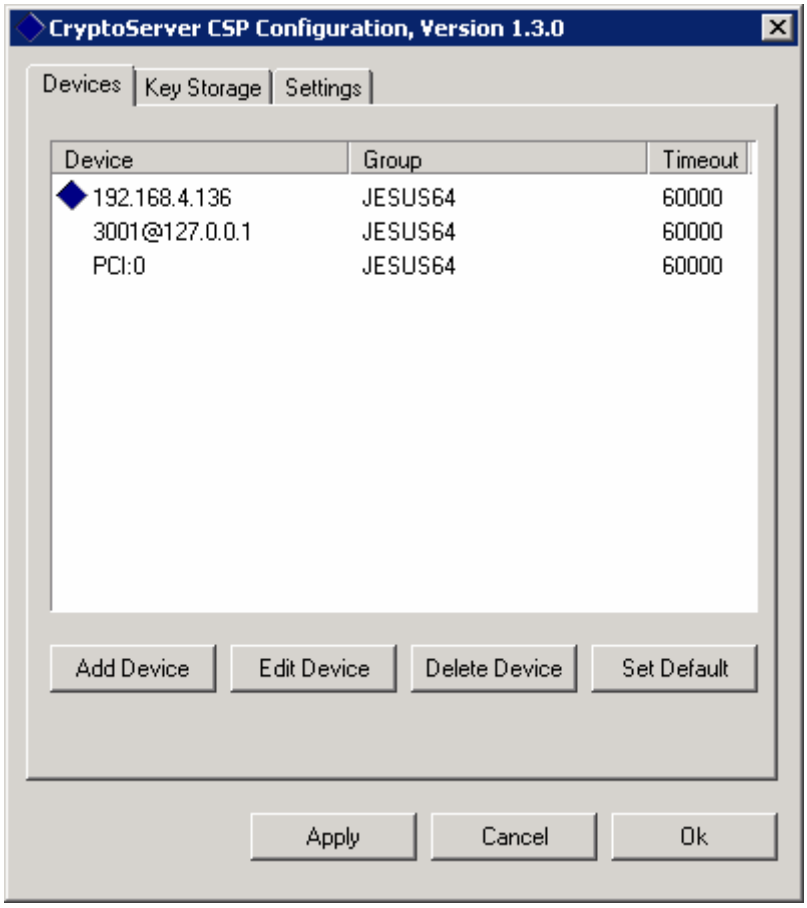
   - CNG

     Execute *cngtool RegisterProvider*

4. One or more CryptoServer must have been configured with the control panel applet (check with *cngtool ProviderInfo*).

8 Configuration

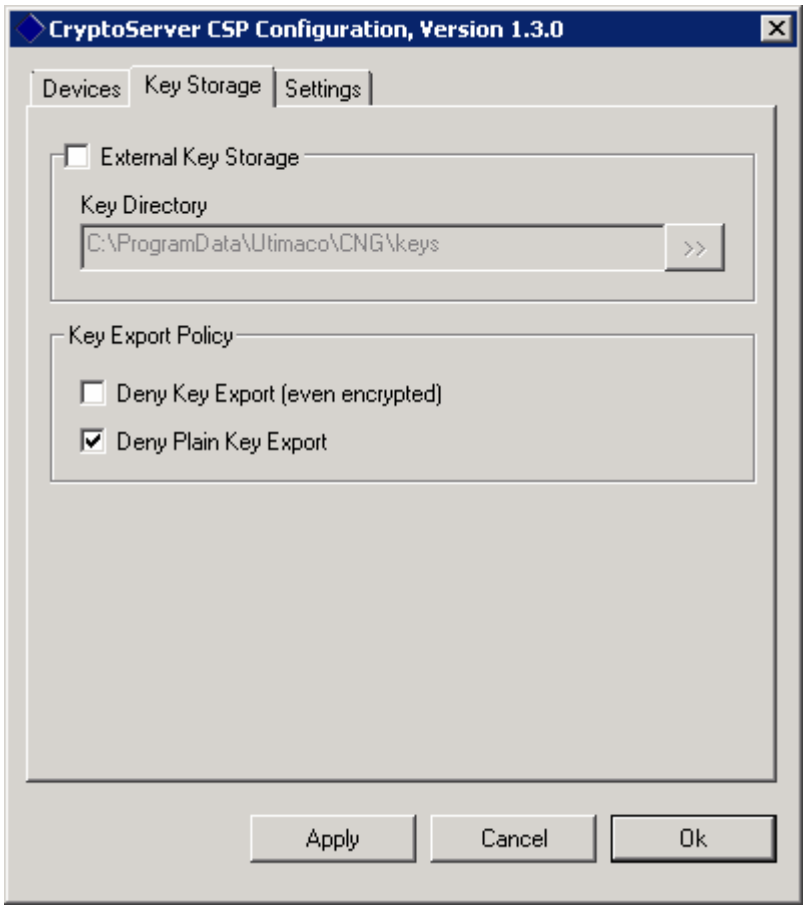
The *Utimaco CryptoServer Key Storage Provider* can easily be configured by using the control panel applet.



On the 'Devices' tab a list of already created CryptoServer is shown. This can be either a local CryptoServer PCI-card or a CryptoServer LAN (via TCP). The blue rhombus marks the default device, which will be used (exclusively in case of internal key storage or preferred in case of external key storage).

The addition of a new device has to be authenticated by the CryptoServer's system administrator or another user with appropriate rights.

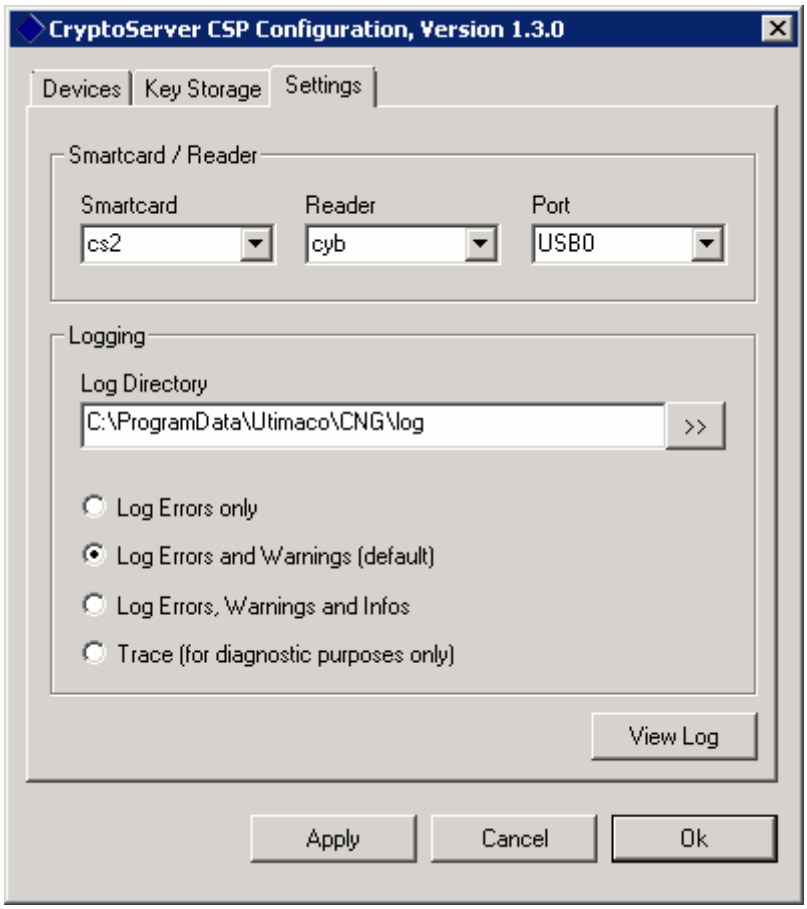
A click on the 'Apply'-button writes all configuration data to the registry but doesn't close the dialog, the 'OK'-button does the same but closes the dialog, the 'Cancel'-button closes the dialog without saving modifications.



On the 'Key Storage' tab the key storage location and the key policy can be defined.

On selection of external key storage the keys are stored locally as key files (encrypted with the CryptoServer's Master Box Key). A specific key directory may be chosen (default is '%AllUserProfile%\Utimaco\CNG\keys'). If external key storage is deselected, keys are stored internally on the CryptoServer.

The key export property of keys being created or imported can be restricted by a global policy. Basically the key export property is set on generation or import of keys according to the parameters given by the application (e.g. Microsoft CA). If key export is restricted by the given policy, the application parameters ('allow key export', 'allow plain key export') are overwritten respectively.



If smartcards should be used as authentication device the smartcard reader has to be specified. Currently the following reader are supported:

Specifier	***Model / Vendor***	***Type***
cyb	cyberJack / ReinerSCT	seriell / USB
cp8	XiMax / Xiring	seriell
acr	ACR80 / Advanced Card Systems	seriell
pcsc	any reader supporting PCSC	seriell / USB

Depending on the reader's connection type a dedicated port (e.g. COM3) or the position within an enumeration (e.g. USB:0) have to be chosen.

The Utimaco CryptoServer Key Storage Provides writes the log file 'cs2cng.log' to the specified directory (default is '%AllUserProfile%\Utimaco\CNG\log'). The files automatically rotates, if the maximum file size of 8 Mbytes has been reached. In this case the current log file is renamed to 'cs2cng.log.bak' and a new, empty log file is created. In dependence of the chosen log level errors, warnings and informational messages are written to the log file. It is recommended to set the log level to 'errors and warnings' and increase it only in case of errors.

9 References

Ref.	Title/Company	Doc.-No.
[CS2ADMIN]	CryptoServer – Administration Guide / Utimaco Safeware AG	2002-0021
[CS2Install-Manual]	CryptoServer – Installation Manual / Utimaco Safeware AG	2003-0007
[CS2MBK]	CryptoServer – Master Box Key Management – User Manual / Utimaco Safeware AG	
[CNG]	Cryptography API: Next Generation – Microsoft 2007 http://msdn2.microsoft.com/en-us/library/aa376210(VS.85).aspx	