

HOBLink Certificate Generator – the Ideal Addition to

This document contains information pertaining to the current release of the HOBLink Certificate Generator.

Overview

The HOBLink Certificate Generator is a tool for creating a Public Key Infrastructure (PKI). It is particularly indispensable if a Certification Authority (CA) is to be created and different certificates must be generated for a large number of users.

The HOBLink Certificate Generator includes the Security Manager from the HOBLink Secure software packages, expanding on the Manager with functions for automatically generating certificates. It is recommended that you familiarize yourself first with the Security Manager before you use the Certificate Generator.



When Do I Need the HOBLink Certificate Generator?

The HOBLink Certificate Generator is a must if...

- You need to create a complete PKI with your own CA (e.g., in order to remain independent from external vendors or to save on costs.)
- A large number of users need separate certificates (e.g., if client authentication is necessary).
- You need to generate certificates automatically.
- You would like to import user data from other applications.
- The employees managing the certificates have little background knowledge and therefore need a tool that is easy to use.



Product Description

Why Do I Need an Addition to HOBLink Security Manager?

It is also possible, of course, to build a PKI with the HOBLink Security Manager alone. The amount of work required to do this with the HOBLink Security Manager, however, is considerable. The HOBLink Certificate Generator is the program that greatly simplifies the task for you.

Calculating certificates consumes a significant amount of computing time. Although a standard 500-MHz Pentium processor requires only about a minute; multiply this by several thousand users, however, and the generating of certificates becomes a huge undertaking. From this perspective, creating every single certificate manually is an impossibility and a tool for the automatic generation of certificates can be seen as a necessity. This is exactly the purpose that the HOBLink Certificate Generator fulfills.

The Purpose Determines the Product

The HOBLink Certificate Generator is an independent product and must be purchased separately. The evaluation version (“try-out license”) is limited to the generation of five certificates.

A customer who needs only a few certificates for evaluating HOBLink Secure can generate these easily with the “Auto Wizard” function of the HOBLink Security Manager. Also, anyone who later wishes to protect only a few connections with HOBLink Secure should use HOBLink Security Manager. When, however, hundreds of users need individual certificates, the advantages offered by HOBLink Certificate Generator become indispensable.

As a rule, generating certificates is a one-time process executed when the administrator is setting up the PKI for the intended users. This procedure must normally be repeated only after the expiration of the certificates.

Product Features

Simply put, the HOBLink Certificate Generator takes a data source containing extensive user lists and, at the end of the process, generates certificates assigned to specific users. It checks the lists for inconsistencies, converts these into a readable internal format, generates the corresponding certificates in sequential order and saves these in separate directories.

The HOBLink Certificate Generator is (like the HOBLink Security Manager) a Java application. It requires a computer with JVM, version 1.1.7 or higher. A relatively high-performance CPU (at least Pentium 200 MHz or equivalent) is definitely recommended.

Working with the HOBLink Certificate Generator

1. As with all security measures, the first step is a risk analysis leading to the definition of a security philosophy. This determines how the PKI will be set up, which algorithms will be used, etc. Anyone who needs assistance with this task can obtain this from HOB as a chargeable service.
2. The security administrator responsible for implementing the security philosophy first creates the configuration file and certificate database for the server as well as the corresponding files for the “standard client” using the HOBLink Security Manager. After he has tested this he knows that his files meet the necessary requirements and allow for a secure connection.
3. As a rule, all of the pre-settings for all further user certificates are known at this point. In the next step, the administrator creates a list of all users who are to receive certificates. This list must conform to a certain format (tab-separated text) that is supported by all databases or spreadsheet programs.
4. Actually, the list corresponds to a table with pre-defined columns. Certain column information is mandatory, e.g., that for the unambiguous designation of the user (“Common Name”), or more generally, of the client. Entering other column information is optional.
5. These columns can also be used for pre-determined settings. If individual differences for certain users are planned, these can be entered in the list. In this case, these specific entries will overwrite the general pre-settings.

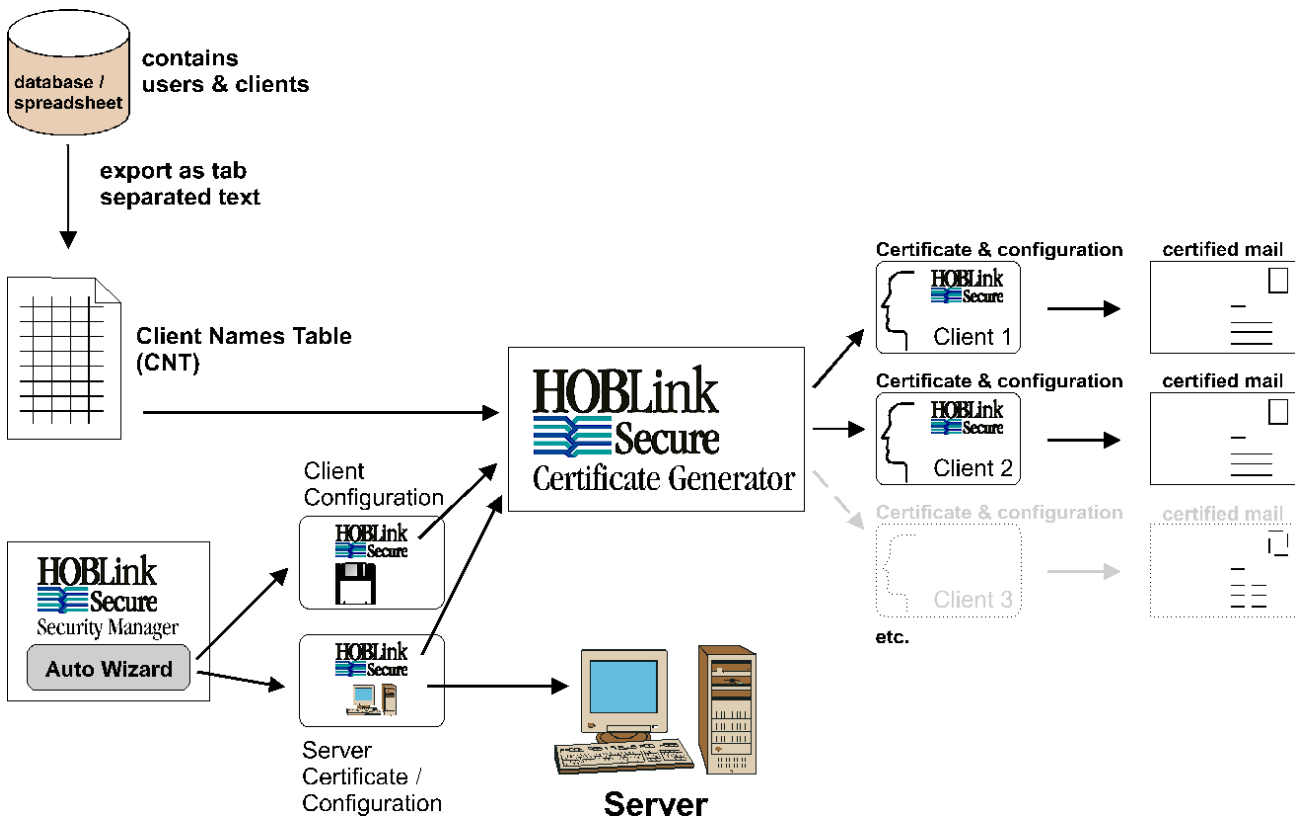
- Based on the previously created files for the server and the standard client (as “template”), the HOBLINK Certificate Generator processes the list according to the pre-settings, generates the certificate and configuration files and saves them in a clear directory structure. A log file protocols all procedures and registers possible errors and events. The security administrator checks the protocol and makes any necessary corrections. This might involve modifying certain entries and generating the affected certificates again. (An example would be when two different clients/users were mistakenly assigned the same “common name”.)

Using the Generated Certificates

The last step is copying the files for each client on a separate storage medium such as a diskette or a smart card. A tool included with HOBLINK Secure prepares each diskette so that the recipient can copy the files to his/her computer with a single mouse click. The files are then ready for use with HOBLINK Secure in combination with HOBLINK J-Term (a 3270/5250/VT525 emulation) or HOBLINK JWT (for access to Windows Terminal Server).

The storage media are then delivered to the users via a secure method, e.g. via registered mail. Each user also receives his password by separate mail allowing him to use the files. If the letter is lost or unauthorized use is suspected, the security administrator can enter the certificate concerned in a certificate revocation list.

The following illustration provides an overview of the tasks of the HOBLINK Certificate Generator:



Summary

The HOBLINK Certificate Generator is necessary for anyone who does not just need to create a few certificates occasionally, but rather wants to set up a PKI for an extensive number of users. The combination of HOBLINK Security Manager and HOBLINK Certificate Generator offers him a maximum of flexibility and ease-of-use in managing certificates. This makes setting up a CA for many users more practical and results in reduced costs as opposed to the work-intensive, manual generation of certificates or using the costly services of an external certification authority.



Technical Background and Terminology

What is a PKI?

Almost all cryptographic standards today such as SSL, TLS and IPsec for encrypting data communication and authenticating the sender and recipient are based on asymmetrical algorithms such as RSA (Rivest-Shamir-Adleman) or DH (Diffie-Hellmann). They work with private and public keys that compliment one another and are assigned to an identity (person, organization, computer, etc.) in pairs. The private key is known only to its owner, whereas the public key is generally available. The purpose of a PKI is the creation and distribution of the public key.

What are certificates?

Public keys are distributed in the form of certificates. The certificate contains the public key and names the corresponding identity. To protect the certificate from being forged, a type of check sum is calculated and it contains the digital signature of a higher authority. To check the signature of the next higher authority, you need its public key (the signature itself is made with the private key, which is known only to this institution).

What is a root certificate?

At this point, one truth becomes obvious: if I don't trust anyone, then I can't communicate safely over external channels. Therefore, at the end of this chain there must be an absolute trustworthy authority – one whom both sender and recipient trust. In our case, that is a CA (Certification Authority) that publishes a root certificate. The CA confirms its own identity in this root certificate, i.e. that it is who it claims to be. The communication partners must have this root certificate prior to communication in order to verify other certificates (e.g. from other business partners) which are derived from it. The job to be completed, then, is to generate root certificates, derive other certificates from these and then distribute them. In classic data communications with clients and servers, only a few server certificates are typically needed, whereas thousands of client certificates may be required.