

bbp development	Version: 2.4
User Manual for IBASEC 3.x	Datum: 30.04.2007

## 9.4 Case 11: Connect a new HSM with "Premium Rollout"

### Description:

The SafeNet Hardware Security Module (LunaSP HSM) comes from your supplier in an "ibasec specific state", ready to connect to your server. The HSM is individually prepared according to your HSM order.

### Prerequisite:

LunaSP HSM in "Premium Rollout" state

ready and running IBASEC server version 3. x

ibasec Main menu (GUI) running with administrator privileges

Instructions from "Premium Rollout"

### Reference:

IBASEC Server Release 3.x, Installation Guide (Solaris 8 und 9 or Wondows)

Compare with Case 13: Change parameters

Compare with Case 14: Replace HSM

Compare with Case 15: Change passwords

### Physical connection of the HSM:

Your Ibasec server has two ethernet ports. With the first port (e.g. eth0) the ibasec server is connected to your bank application servers. At the second port (e.g. eth1) a save private LAN is connected. The HSMs are operating in this protected private LAN. The default ip address class of the private LAN is 192.9.200.x. These should be non-public ip addresses. The new HSM has a unique ip address (e.g. 192.9.200.31) according to your order.

Connect the new HSM to the private LAN. Use the RJ45 plug at the rear of your HSM that is marked with "1". It's a 10/100Mbit Fast Ethernet Plug-and-Pay Adapter. the second RJ45 plug marked with "2" is not used.

It is recommended that your private LAN connection between ibasec server and the HSM(s) is straight forward without any delaying routers.

Connect the HSM to the 220V power. In case of a power loss of less then 20 minutes, the HSM could reboot automatically (without manual interference). An UPS (uninterruptible power supply) could provide you more operational security.

Switch on your HSM with the main power switch at the rear of the HSM

The second power switch at the rear of your HSM does a proper shut down or cold boot of the HSM.

Let the powered HSM two minutes to boot properly. The K5 HSM indicates the ready state on a small LCD display on the front panel.

The IT expert might check the proper connection of the HSM with a ping from the Ibasec server:  
ping 192.9.200.31

### Connect a Pin Entry Device (PED) to your HSM:

The Ibasec specific HSM uses the "Trusted Path Authentication", e.g. authorisation is managed by a PED and iKeys (PED Keys).

Connect the PED with the adequate cable to the plug in front of the HSM: The PED is powered by this data cable and shows readiness on its LCD display:

bbp development	Version: 2.4
User Manual for IBASEC 3.x	Datum: 30.04.2007

```

SCP mode...

Awaiting command...

. < . EXIT   . > . LOG

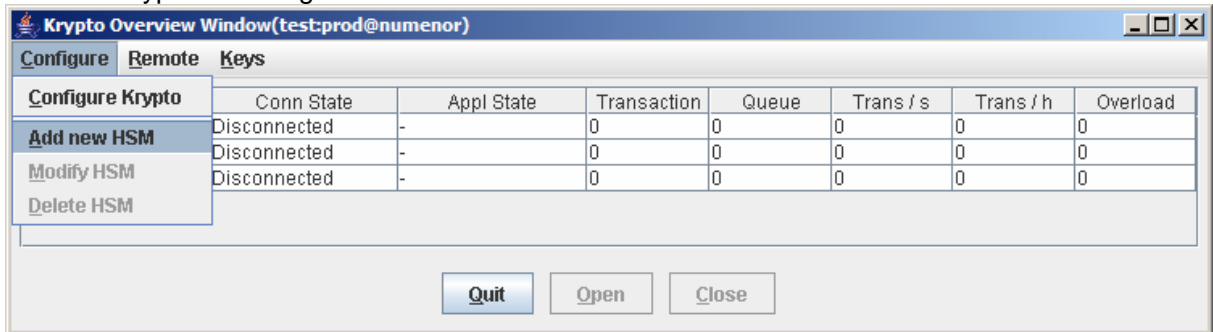
```

After the physical connection of a new HSM, it has to be registered with the Ibasec server, e.g. a new HSM has to be added to the HSM list and its parameters have to be set. The following window shows the default setting of these parameters. Compare also with Case 13: "Change or set parameters" and Case 14: "Replace HSM".

Menu → Krypto



Menu → Krypto → Configure



The screenshot of this example shows that already three other HSMs are registered with the Ibasec server. Before you add the first HSM to the list, you should select "Configure Krypto" and check for the right ip-address of your installation in the private LAN environment.

bbp development	Version: 2.4
User Manual for IBASEC 3.x	Datum: 30.04.2007

Menu → Krypto → Configure → Add new HSM

**HSM** (name), **Unit Number**, **IP Address** and **Description** belong together and depend of course from the ordered ip address of your HSM. The **Unit Number** and therefore the last octet of the ip address is **limited to < 100**.

**SubnetMask** depends on your HSM private LAN

**Max. Password Entries:** the Ibasec - HSM dialog is password protected. Too many consecutive wrong passwords should lock the connection. The limit is set here.

**Autostart:** after a successful installation and opening of a HSM the Autostart flag could be checked to enabling an automatic opening after a Ibasec server start.

**Comm Timeout:** 6 secs

**Poll Interval:** 30 secs

**Selected Applications:** select your applications (NKAPP is not available)

The **Mode Setting** is always "Unattended". The Office Mode, as known from Ibasec 2.x with Gretacoders, is no more available with the Luna SP HSMs



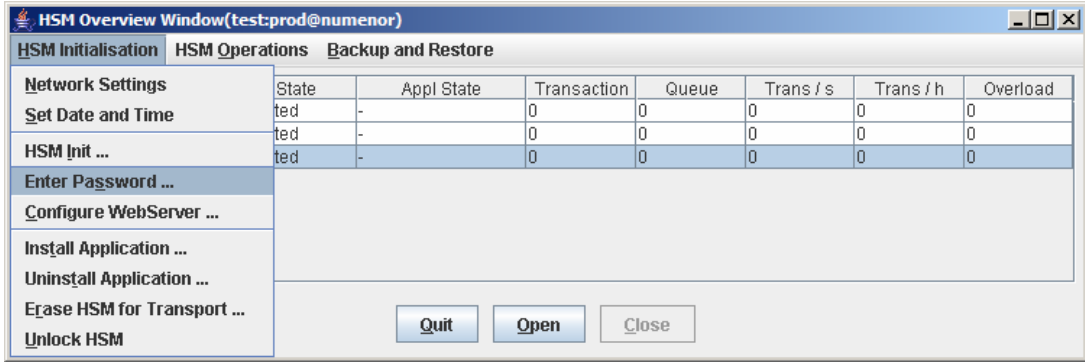
The supplier of your HSM has setup the parameters and secrets of the HSM. If you would like to change the secrets you should apply either "Change and set Passwords" (Case 15) or completely "Reinitialize the HSM" (Case 14). **But first finish the HSM connection with the supplied secrets.**

### Change the Admin and the Partition Password according to your PIN letter (Premium Rollout):

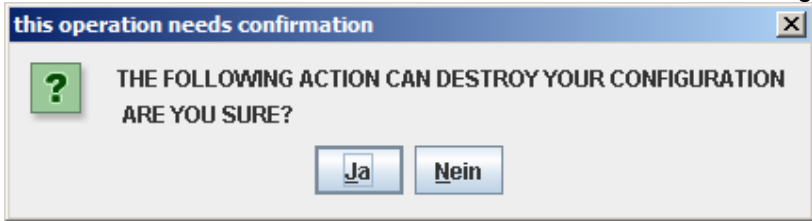
The Admin Password gives you and the Ibasec server ssh-access to the HSM. The Ibasec server has to know this password. So we have to save it with the Ibasec server. The partition password is an important secret to control the access to the key partition of the HSM (the save storage of all your public and private keys). The Ibasec server has to know this password. So we have to save it with the Ibasec server

bbp development	Version: 2.4
User Manual for IBASEC 3.x	Datum: 30.04.2007

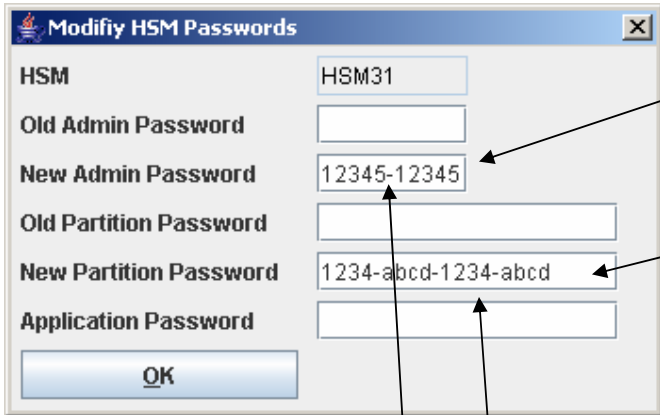
Menu → HSM



mark the HSM and then select "Enter Password" and the following warning will show up:



Menu → HSM → HSM Initialization → Enter Password...



**New Admin Password:**  
This is the new Admin Password from the **PIN letter** that comes from the HSM supplier (Premium Rollout).

**New Partition Password:**  
This is the new Partition Password from the PIN letter that comes from the HSM supplier (Premium Rollout).

Press <OK> to save passwords

**Extract from PIN\_Letter:**

HSM-Serial #	012345	
Admin-Password	12345-12345	See Note #1 on next page
Partitions-Password	1234-abcd-1234-abcd	
IP Address	192.9.200.31	

Application-Password It can be set individually without knowing the old Application-Password.

- iKeys for PED
- iKeys have no PIN. Just press the <Enter> button on the PED if you were asked to enter a PIN.
  - All iKeys of a specific color (i.e blue, black and red) are identical and may be used irrespective of HSM's.

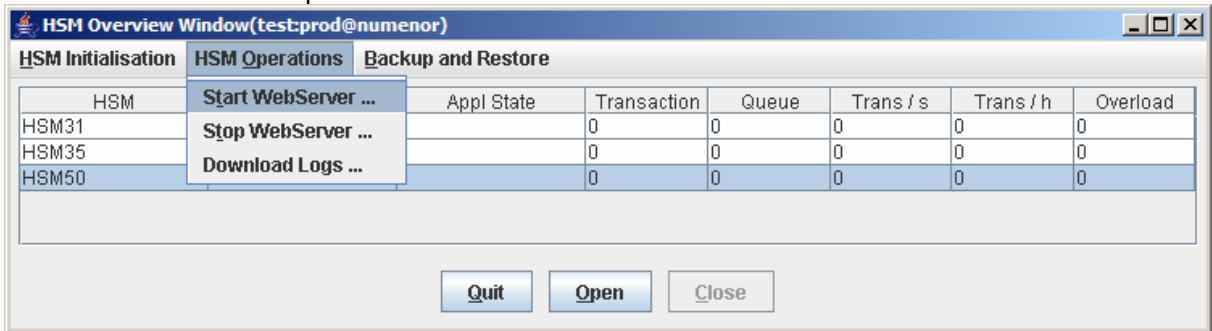
bbp development	Version: 2.4
User Manual for IBASEC 3.x	Datum: 30.04.2007

To save the passwords from the PIN letter the "Old Admin Password" field and the "Old Partition Password" field remains empty. This is not a password change. This information is needed by the Ibasec server to communicate with the HSM.

Now your HSM is ready to operate with the Ibasec server version 3.x. The first time and again with each cold boot of the HSM **it is recommended to start the web server of the HSM manually**. If you open the HSM with a halted web server, the Ibasec server falls into the recovery mode and finally starts the web server itself. You could watch this actions by opening the "Audit" (see main menu).

To save time we start the web server manually:

Menu → HSM → HSM Operations → Start Web Server



The **first time start of the web server** (after a cold boot of the HSM) the black partition PED key is needed:

```
SLOT 03:
LOGIN USER/PARTITION.
Insert a User /
Partition Owner
PED Key.
Press ENTER.
```

no PED keys are needed if the HSM is not cold booted

```
SLOT 03:
LOGIN USER/PARTITION.
Enter new PED PIN:
```

enter PIN code of PED key (if any)  
"Premium Rollout" comes without PIN code.

Now you are free to open the new HSM. Remember, we have not selected the Autostart flag at the beginning. If the new HSM works properly you could set it to Autostart. Check the state of the opened HSM → Case 12

**Follow-up actions:**

- Reinitialize the HSM → Case 14
- Change and set passwords → Case 15