

SafeNet ProtectServer Integration Guide

The current guide describes the steps required to integrate the PKI with SafeNet ProtectServer HSM. It supposes one has acquired a SafeNet ProtectServer External (PSE) along with the ProtectServer Toolkit (PTK).

To install the PKI and use SafeNet ProtectServer as Hardware Security Module, one should do the following:

1. connect the HSM (and start it up if PSE)
2. install HSM middleware (PTK-C). Version 4.2.0 or more is required
3. setup HSM middleware (if it's a PSE, it just means put the correct IP in `/etc/default/et_hsm`)
4. using `gctadmin`, setup the HSM:
 1. initialize and set PIN/SOPIN for the Admin slot
 2. create a user slot, and set its PIN/SOPIN. The PIN of this slot will be asked by the PKI later.
 3. log in on admin slot, and set security mode to "Netscape" or "FIPS"
5. install the PKI: when the system requests "CryptoSystem", select "rsaps", and enter the slot (should be 0) and PIN chosen at step 5-2-
6. after the Key Ceremony, don't forget to backup the HSM