

# YubiHSM Deployment

Document Information	
Namn	YubiHSM Deployment
Version	1.0
Editor	Leif Johansson
Date	2014-11-21

## Purpose and scope

This procedure ensures that the correct YubiHSMs are made available to the KCO for deployment.

## Governing policies

This procedure is governed by the following policies:

- SUNET Key Management Policy (SUNET KMP)
- SUNET YubiHSM KMPS

## Roles

Number of Persons	Role Name	Responsibilities
1	SO	Monitor and document process.
2	NOC+KCO	Deploy YubiHSM

## Summary

This process deploys a number of YubiHSMs created by the “YubiHSM HMAC Key Generation” process. The outcome of that process should be a set of YubiHSMs in a tamper-evident bag, the serial of which is found on a flyer attached to the “YubiHSM HMAC Key Generation” process log entry in the YubiHSM binder. The purpose of the process is to authenticate the YubiHSMs by authenticating the tamper evident bag where they are stored and to turn them over to the KCO for deployment in the application server.

## Procedure Steps

Role	Description
SO	Preparation The SO opens the SAFE and extracts the YubiHSM log binder. Identify the log page matching the YubiHSM HMAC Key Generation process where the HSMs were prepared. Extract the tamper evident bag from SO personal safe storage.
Completed (yes/no)	Notes
Time &Date	Signature/Initial

Role	Description
SO+KCO+NOC	Tamper bag serial authentication The tamper bag serial is matched against the log entry serial flyer. A failure to match means that the process must be terminated and a new set of YubiHSMs must be prepared. The SO and KCO must concur.
Completed (yes/no)	Notes
Time &Date	Signature/Initial

Role	Description
SO+KCO+NOC	HSM Deployment The tamper bag is handed over to the NOC+KCO for deployment. The serial flyer on the "YubiHSM HMAC Key Generation" log entry is marked "deployed". The KCO assumes responsibility for correct deployment of the HSM in the application server.
Completed (yes/no)	Notes
Time &Date	Signature/Initial



## SUNET KMF Procedure

Role	Description
SO	End Process The SO personal safe storage is closed. The safe is closed.
Completed (yes/no)	Notes
Time &Date	Signature/Initial