SUNET KMF Security Officer

This document describes the responsibilities of the SUNET Key Management Facility (KMF) Security Officer role. The normative document for the SUNET KMF SO is the SUNET Key Management Policy. This document is descriptive (non-normative). The SUNET Key Management Facility (KMF) is a collection of policy, practices and technology for managing cryptographic keys.

The KMF SO is responsible for controlling access to cryptographic keys and appliances where keys are stored and managed. The SUNET KMF serves multiple applications including eduID, SWAMID and a small number of pro-bono projects serving the European and Global NREN community (eg Terena REEP and the GEANT FAAS). These projects and applications are all mission critical and depend on the Security Officer to perform his/her duties in a responsible and diligent manner.

Basic Rules of Behavior

Always ask “Why?”

Whenever you are asked to act in the role of SO there must be a good reason. In most cases there should be a defined and documented process for any action you are asked to take as SO. If in doubt, involve another SO in a discussion.

You are responsible for understanding what is happening

As SO you will be asked to participate in complex, multi-step procedures involving cryptographic keys. It may be tempting to assume that the other SOs understand what is happening. Don’t. Always make sure you understand enough of the process to be able to explain what you just did to somebody else.

Treat your deposit box key as you would your house keys

Your safe deposit box is used to store tokens, smartcards and other sensitive objects. Keep your key safe and with you, just as you would any other valuable key.

Record keeping is important

Don’t rely on your memory. Make notes and affix the notes to the official record of the process. Bad notes are better than no notes. Good notes are better still.