



3SKey Best Practices Guide

October, 2010

Version: v3

Table of contents

1	Preface	1
2	Roles	2
2.1.1	Role of the administrator	2
2.1.2	Role of the user	2
2.1.3	Remarks	3
3	Practical guidelines	4
3.1	Before you start using 3SKey tokens	4
3.2	Administration	4
4	Security guidelines	5
4.1	Internet access	5
4.2	Security of tokens and passwords	5
4.2.1	What the 3SKey user must do	5
4.2.2	What the 3SKey user must not do	5
4.3	General security guidelines	6
4.3.1	What the 3SKey user must do	6
4.3.2	What the 3SKey user must not do	6

1 Preface

Purpose

This document explains how to implement 3SKey in your organisation, assigning roles, setting up systems and best practices for using 3SKey.

These guidelines are not mandatory or legally binding.

Audience

This document is intended for the following audience:

- 3SKey users who require information for implementing the 3SKey solution.

The 3SKey user should also read the [3SKey service description](#) as a companion to this document before using the product.

Additional documentation available from Swift:

- [3SKey Service Description](#)
- [3SKey installation guide for eToken PRO](#)
- [3SKey installation guide for eToken NG-FLASH](#)
- *3SKey Portal Online Help*

2 Roles

Individuals using 3SKey can have two different roles, according to their level of access rights:

- Administrator
- User

2.1.1 Role of the administrator

The administrator is the person within the organisation using 3SKey who receives, prepares, distributes and maintains the tokens.

To set up 3SKey, an administrator must follow these steps:

- The administrator(s) must activate a minimum of two tokens with administrator rights. To do so, the administrator logs in to the 3SKey portal. With a token, the administrator will be able to perform the following functions:
 - Set up and maintain a user group with administrator and user tokens
 - View the tokens and status of the tokens in the user group
 - Revoke tokens of users in the group
 - Set up a user or an administrator for recovery
 - Perform all user functions
- After activation of the administrator tokens, the administrator can link additional tokens (new tokens that were never activated) to a user group. To do so, the administrator must log in to the portal, insert an unactivated 3SKey token, and link that token to the user group. The administrator will repeat this for all tokens to be linked to the user group at the time of creation. Additional tokens can be added to the group at any time.
- The administrator will distribute the 3SKey tokens to those who are responsible for signing transactions.

2.1.2 Role of the user

The user receives the token from the administrator and activates it through the 3SKey portal. After activation, the token will be ready to use for signing messages and files.

To activate the 3SKey token, the user must log in to the 3SKey portal, which will:

- Prompt the user to replace the default password with a personal password.
- Generate a personal security code that the user must safe-store
- Download a certificate and save it to the token.

Once a token has been activated by the user, the user will be able to:

- Use their certificate to sign banking transactions
- Change their personal password and generate a new security code
- Revoke his or her own certificate
- Complete a recovery of a token prepared for recovery by the administrator
- View the key information stored on the token (unique ID, validity period)
- Renew the token before expiry

2.1.3 Remarks

- Besides for user group management, the administrator can also use their administrator token to sign banking transactions as any other user.
- Corporate customers will receive inactive tokens from their bank. During initialisation, tokens can be configured as administrator tokens for the creation of a user group or be linked by an administrator as user tokens to an existing user group.
- The physical presence of the administrator's 3SKey token and the user's 3SKey token is always required when linking tokens to a user group.
- The security code is required in some exceptional situations (e.g. revocation by user, recovery when lost or stolen, forgotten password, etc.).
- The recovery function always requires (1) the administrator to prepare a new token for recovery and (2) the user to log in with the security code and then change the password.

3 Practical guidelines

3.1 Before you start using 3SKey tokens

- Identify the PCs that will be used for the 3SKey solution
- Check that the PCs have the correct operating system and service pack
- Check that the PCs have a minimum of two USB ports
- Install the required drivers and check that the prerequisites are met. The SWIFT installer will perform a pre-check before installing the 3SKey software.
- Identify the 3SKey individual(s) who will be the administrator(s). Two separate people should be appointed as administrators.
- Identify the 3SKey users that will sign transactions
- Identify the members of each user group.
- Read and follow the instructions provided in the installation guides.

3.2 Administration

As part of their responsibilities, the administrators must:

- Distribute the tokens to users
- Keep a list of unique IDs and associated users
- Ensure there is a procedure in place to revoke users who have lost their token
- Ensure there is a procedure in place to recover a unique-ID on another token
- Ensure there is a procedure for renewing user tokens before expiry date
- Ensure there are sufficient spare tokens
- Ensure that the token of a user leaving the company is revoked
- Ensure that an administrator leaving the company is replaced by a new administrator.

4 Security guidelines

4.1 Internet access

- The 3SKey user is responsible for ensuring an active, secure Internet connection and the resolution of any other problems caused by or arising during the Internet connection to the 3SKey subscriber web application.
- In particular, the 3SKey user must troubleshoot problems relating to their Internet connection, or problems with the setup of the Internet on the user's side.

4.2 Security of tokens and passwords

- The 3SKey user is fully responsible for the security of their token. In particular, it is the sole responsibility of the 3SKey user to prevent an unauthorised party from using their token and password to initiate a transaction.
- 3SKey users must take utmost care to protect their tokens physically from unauthorised borrowing, loss, and theft. They must also take all necessary measures to prevent any unauthorised disclosure of the token's password.

4.2.1 What the 3SKey user must do

In particular, 3SKey users must ensure that they abide by the following non-exhaustive list of safeguards:

- ensure that each token is linked to a single, authorised person
- store the tokens in a safe place when they are not needed
- revoke any unused, obsolete or lost tokens

4.2.2 What the 3SKey user must not do

The 3SKey user must never:

- lend the tokens to others
- leave the token inserted in the PC used for 3SKey transactions unattended
- write down any password or communicate a password to unauthorised people
- use a password that can be deduced easily
- allow anyone to watch them type in their password

4.3 General security guidelines

4.3.1 What the 3SKey user must do

The 3SKey user must protect the systems used for 3SKey and signing banking transactions in accordance with industry security practices, such as:

- Protecting the PC from unauthorised physical and network access. Use a firewall to shield the 3SKey user's PC from incoming Internet traffic and from unauthorised access over the internal network. The firewall must be both a physical barrier to protect incoming traffic, and a localPC firewall to ensure that only authorised programs communicate with the outside.
- Installing only authorised and required software on the PC
- Ensuring that all software applications that run on the PC are regularly updated and patched. This includes Windows, the Internet browser, and additional features -- plug-ins such as Shockwave, QuickTime, Realplayer, and any others.
- Restricting outgoing traffic from the PC to business-critical sites, as well as to legitimate sites required for software updates
- Using up-to-date virus scanners and malware scanners to protect the PC from threats such as viruses, worms, keyboard loggers, Trojans etc.

The 3SKey user must ensure that the system's end-users are following secure browsing practices, such as:

- Reserving certain PCs strictly for use in accessing sites and applications with a high-level of criticality such as 3SKey and other mission-critical web applications used for banking transactions, and only accessing such sites from those dedicated PCs.

The 3SKey user must implement the following management principles to alleviate risks to its system:

- Establish user-management practices to ensure that only authorised users are created and remain on the system
Because users change roles or leave the company, ensure that the customer maintains an accurate and up-to-date list of authorised users
- Establish entitlement management practices to ensure that users are granted access to 3SKey functions only on a need-to-know or need-to-have basis.

4.3.2 What the 3SKey user must not do

The 3SKey user must not:

- Browse to Internet sites that are believed to be unsafe, when using the same PC on which it accesses the 3SKey portal or the bank's web application(s)

- Click links in e-mails that appear to come from SWIFT or anyone else, even if the link seems perfectly valid from a business perspective. Such phishing attacks may lead to a rogue site that can steal information or infect the PC. If the user can confirm a business need for visiting the site, then the user should re-type the link within the browser as it was visible in the e-mail.
- Accept a pop-up that asks the user to download and install executable software