
SFE Austraclear System**Digital Certificate Implementation
Security Guidelines**

Table of Contents

1	PURPOSE	3
2	SECURITY GUIDELINES	3
2.1	Certificate backup	3
2.2	Certificate download	3
2.3	Private key export	3
2.4	Password Policy	3
2.5	User accounts.....	3
2.6	Client host security.....	3
2.7	Additional Private Key Protection.....	4
2.8	Use of smartcards.....	4
2.9	Simultaneous user logins	4

1 Purpose

The purpose of this document is to set out the Security Guidelines covering the enrolment and implementation of SFE Austraclear digital certificates by Participants.

2 Security Guidelines

2.1 Certificate backup

The SFE does not keep copies of certificates or private keys and it is important that certificates are backed up if required for key recovery and DR purposes. The process for issuance of a replacement certificate is the same as the process for the new certificates. Exported certificates need to be securely stored and handled.

2.2 Certificate download

The PC used to download the digital certificates requires Internet access. Local Power Users or Administrators group permissions are needed to download the ActiveX controls. If it is not possible to change the user permissions, the ActiveX controls can be preinstalled. In addition, the following Internet Explorer content zone settings are required:

- Active scripting: Enable
- Script ActiveX controls marked safe for scripting: Enable
- Run ActiveX controls and plug-ins: Enable

2.3 Private Key export

Private keys should be made non-exportable. To ensure compliance, the certificate download and distribution should be controlled by the Password Administrator.

2.4 Password Policy

When creating a user account in the SFE Austraclear system, unique initial passwords should be used for each user. Strong password policies need to be implemented for all passwords and should be monitored for compliance.

2.5 User accounts

Windows domain user accounts are recommended for users of the new system. If a local user account is used, the computer should be protected by the following:

- BIOS password and tamper-proof PC enclosure
- Windows SYSKEY level 2 or 3

2.6 Client host security

It is recommended that computers running the new SFE Austraclear client are hardened. Current supported Windows patches and anti-virus software with current signatures should be installed.

2.7 Additional Private Key Protection

The primary private key protection is the Windows user account password authentication. Additional Private Key Protection is used to provide additional protection for the private key which is used for user authentication in the new system. Using a soft certificate with Additional Private Key Protection set to High or Medium may present users with more than three private key password prompts which may affect client usability.

Controls that increase security of the Windows user accounts include:

- Implementing strong password policies and monitor compliance
- Prohibiting sharing of Windows and SFE Austraclear user accounts
- Using Microsoft domain user accounts
- Improving host security by using hardening, current anti-virus software and a host firewall

If the default Windows user account protection for the private key is not considered adequate, the private key can be stored on a smartcard.

2.8 Use of smartcards

Participants can implement smartcards in order to store the digital certificates and private keys. SFE has successfully tested smartcard operation in the new system, but participants should perform testing in their environment to confirm compatibility. More information about smartcard deployment in a Microsoft Windows environment can be found at:

<http://www.microsoft.com/technet/security/topics/smrtcard/default.mspx>

2.9 Simultaneous user logins

The system allows simultaneous user logins but detects the login events by the same user name.