nCIPHER

www.ncipher.com

nShield HSM family v11.72.03 Security Target

Version 1-1 • 12 August 2019

Summary of Amendments

Version 1-1 12 August 2019

Updated for re-certification of v11.72.03

Version 1-0 20 November 2015

First version for publication

Contents

1 Preface 5
1.1 Objectives of Document 5
1.2 Scope of Document 5
1.3 Intended Readership 5
1.4 Related Documents 6
1.5 Outstanding Issues 6
1.6 Glossary 7
2 ST Introduction 11
2.1 ST and TOE Reference Identification 11
2.2 TOE Description 11
3 CC Conformance 29
3.1 Conformance to Common Criteria 29
3.2 Conformance to Protection Profiles 29
4 Security Problem Definition 30
4.1 Assets and Objects 30
4.2 Subjects 30
4.3 Threats 31
4.4 Organisational Security Policies 32
4.5 Assumptions 32
5 Security Objectives 34
5.1 Security Objectives for the TOE 34
5.2 Security Objectives for the Operational Environment 35
6 IT Security Requirements 38
6.1 Conventions 38
6.2 Security Functional Requirements 38
6.3 Security Assurance Requirements 55
6.4 Security Requirements Rationale 56
7 TOE Summary Specification 67
7.1 User Roles and Authentication 67
7.2 Key Management 69
7.3 Cryptographic Services 69
7.4 User Data Protection 70
7.5 TSF Protection 70
7.6 Trusted Channels 71
7.7 Session constraints 71

Figures / Tables

Figure 1: nShield Solo+ F3 PCIe unit and nShield Connect+ unit 12
Figure 2: TOE boundary in nShield Solo configuration 13
Figure 3: TOE boundary in nShield Connect configuration 14
Figure 4: Gaining access to an SCD protected by an OCS 18
Figure 5: Gaining access to an SCD protected by a Softcard 18
Figure 6: nShield HSM states and transitions 19
Figure 7: Local Softcard Deployment Scenario 22
Figure 8: Local OCS Deployment Scenario 23
Figure 9: Remote Use Deployment Scenario 24

Table 1: TOE scope 27
Table 2: SCD/SVD Generation Table 39
Table 3: Digital Signature Generation Table 41
Table 4: Security Assurance Requirements 56
Table 5: Security Problem Definition mapping to Security Objectives 57
Table 6: Mapping of TOE Security Objectives to SFRs 62
Table 7: Dependencies rationale for SFRs 66

1 Preface

1.1 Objectives of Document

This document presents the Common Criteria (CC) Security Target (ST) for the nCipher nShield HSM family v11.72.03.

This sanitised version of the Security Target has been derived from the full version following the rules defined in [CCDB_STlite]. It contains the same information as the full version except the Summary of Amendments has been sanitised.

The product is designed and manufactured by nCipher Security Limited.

The Sponsor and Developer for the EAL4 (augmented with AVA_VAN.5) evaluation is nCipher Security Limited.

1.2 Scope of Document

The scope of the Security Target within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation [CC]. In particular, a Security Target defines the IT security requirements of an identified TOE and specifies the functional and assurance security measures offered by that TOE to meet stated requirements [CC1, Section C.1].

Security Functional Requirements (SFRs), as defined in [CC2], are the basis for the TOE IT security functional requirements expressed in this Security Target. These requirements describe the desired security behaviour expected of a TOE and are intended to meet the security objectives as stated in this Security Target. Security Functional Requirements express security requirements intended to counter threats in the assumed operating environment of the TOE, and cover any identified organisational security policies and assumptions.

The ST is based on a draft version of “Protection profiles for Secure signature creation device — Part 2: Device with key generation, prEN 14169-2:2010”; it adopts the same terminology and much of the same content but, instead of the smart card type of SSCD envisaged in that PP, this ST deals with an SSCD that is implemented as a PCIe module in a client PC or an nShield Connect+ unit (see Figure 2 and Figure 3 in section 2.2.2), and that may be provided by a trusted third party in order to hold SCD and create signatures on behalf of Signatories who may be in the same physical location as the SSCD, or who may invoke its services remotely. The TOE defined in this ST operates in a controlled environment which implements additional security objectives to protect against unauthorised access to the module. For these reasons, conformance to 14169-2:2010 is not claimed.

1.3 Intended Readership

TOE users, developers, evaluators and certifiers.

1.4 Related Documents

1.4.1 Common Criteria[1]

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017.

1.4.2 Other documentation

[CCECG] ASEC1382 nShield HSM family v11.72.03 Common Criteria Evaluated Configuration Guide, v1.3

[CCDB_STlite] CCDB-2006-04-004 – ST sanitising for publication

[Regulation] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[ETSI] ETSI TS 102 176-1 – Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, v2.1.1, July 2011

[UG] This document comes in four variants – these are equivalent in content, but deal with different client operating systems and TOE configurations:

- nShield Connect User Guide for Windows, v11.0
- nShield Connect User Guide for Unix-based OS, v11.0
- nShield Edge and nShield Solo User Guide for Windows, v11.0
- nShield Solo User Guide for Unix-based OS, v11.0

1.5 Outstanding Issues

None.

[1] For details see http://www.commoncriteriaportal.org/

1.6 Glossary

Term	Meaning
Access Token	See Logical Token.
ACS	Administrator Card Set - a set of smart cards used to control access to Security World configuration, as well as key recovery and replacement operations.
API	Application Program Interface
Application Keys	Keys protected by the TOE and made available for use by applications running on connected client hardware, under authorisation by the relevant OCS card holders for the keys. When the unit is used as an SSCD, these keys are SCD.
Assurance	Grounds for confidence that a TOE meets the SFRs [CC1].
Card	Generic term for a smart card or Softcard
CC	Common Criteria
CGA	Certificate Generating Application – a software application that, having successfully completed certain checks, certifies a public key as belonging to its owner.
CLI	Command Line Interface
CM	Configuration Management
CSP	Certification Service Provider – an entity that issues certificates or provides other services related to electronic signatures.
DSA	Digital Signature Algorithm
DTBS	Data To Be Signed – the data presented to the TOE (i.e. an SSCD) by the Signature-Creation Application, after authenticating the signer, in order to obtain a signature over that data from the TOE.
DTBS/R	Data To Be Signed or its unique Representation – either the DTBS or a unique representation of it comprising one of the following: a hash of the DTBS; an intermediate hash of the DTBS appended to the remaining part of the DTBS; the DTBS itself.
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
Hardserver	The nShield server software running on the client PC in which the TOE is installed. The hardserver controls communications between the HSM and applications running on the client PC.
HSM	Hardware Security Module

Term	Meaning
impath	An nCipher proprietary protocol between two hardserver instances, which protects the confidentiality and integrity of data transmitted, and also identifies and authenticates its end-points. (Abbreviation of *inter-module path.*)
IPC	Inter Process Communication
Key blob	A key blob is a key object with its contents encrypted. Key blobs are used for the long term storage of keys. Blobs are cryptographically secure and can be stored on a host computer's hard disk.
Logical Token	An object formed from a combination of a quorum of shares held on ACS or OCS cards, or stored in a Softcard, and which gives access to a particular key. Also referred to as an "Access Token".
MAC	Message Authentication Code
NFKM	Security World Application Programming Interface
nShield HSM	An nShield Solo+ F3 PCIe card or an nShield Connect+.
OCS	Operator Card Set – a set of smart cards that can be used to control access to SCDs within a Security World. OCS's are protected using the Security World key, and therefore they cannot be used outside the Security World.
PC	Personal Computer
PCB	Printed Circuit Board
PCIe	Peripheral Component Interconnect Express
PKI	Public Key Infrastructure
PP	Protection Profile
PSS	Probabilistic Security Scheme – a padding method used with RSA signatures.
Quorum	The number of cards in an ACS or OCS that are required to be presented in order to authorise an operation controlled by that card set. In general this number is between 1 and the total number of cards in the set, although there are various guidelines (described in nShield documentation) for deciding on appropriate values for the quorum. The evaluated configuration in this Security Target requires that the Signatory holds all the OCS cards associated with their SCD.
RAD	Reference Authentication Data – data persistently stored by the TOE for authentication of a user as authorised for a particular role. Authentication takes the form of entering the passphrase required by a card. In this case the reference authentication data is not stored, but implicit in the encrypted form of the data that the passphrase is used to decrypt.
Remote Signatory	A Signatory whose SCD and SSCD are held by a trusted third party but used remotely under the control of the Signatory, without the Signatory needing to be physically present at the place of signature creation. Typically a Remote Signatory will use a local SCA component that communicates with a remote TOE, as described in section 2.2.4.4 .
SAR	Security Assurance Requirement

Term	Meaning
SCA	Signature-Creation Application – a software application that makes use of the TOE to provide advanced electronic signatures of data defined by the application. The SCA is responsible for interacting with the signer and obtaining their authentication data before presenting the authentication data and the data to be signed (or its unique representation) to the TOE.
SCD	Signature Creation Data – the private key used for creating electronic signatures.
SCD-Provisioning	A service that provides generation and secure distribution of SCD/SVD pairs, administration of the SCD/SVD pair (including potentially support for the certification of the SVD by a CSP) and subsequent use of the SCD to create digital signatures on behalf of the user. This service may be provided by a trusted third party.
Security World	The nCipher Security World technology provides an infrastructure for secure lifecycle management of keys. A Security World consists of at least one hardware security module; some cryptographic key and certificate data encrypted by a Security World key and stored by the client PC; a set of Administrator Cards (the ACS) used to control access to Security World configuration, recovery and replacement operations; and optionally one or more sets of Operator Cards (an OCS) used to control access to SCDs.
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
Share	A number of Shares is combined to form a Logical Token that gives access to a particular key (the number of shares required is the Quorum for the key). Each Share is stored on a single ACS or OCS card.
SHS	Secure Hash Standard
Signatory	The person who creates an electronic signature using an SCD under his or her sole control. See also Remote Signatory.
Softcard	A logical token that is protected by a pass phrase. Persistently stored in the Security World. Can be used to control access to SCD.
SSCD	Secure Signature-Creation Device – a device that generates SCD/SVD pairs, uses SCD to create electronic signatures of DTBS/R supplied by an SCA, and does so in a secure manner consistent with the requirements of [Regulation]. (The TOE defined in this Security Target acts as an SSCD.)
SSL	Secure Sockets Layer
ST	Security Target
SVD	Signature Verification Data – the public key corresponding to the SCD for a signature, which can be used to verify the signature.
Target of Evaluation	A set of software, firmware and/or hardware possibly accompanied by guidance. [CC1]
TOE	Target of Evaluation

Term	Meaning
TOE Security Functionality	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs. [CC1]
TSC	TOE Scope of Control – the set of interactions that can occur with or within a TOE and are subject to the rules of the TSP (the set of rules that regulate how assets are managed, protected and distributed within a TOE).
TSF	TOE Security Functionality
VAD	Verification Authentication Data – data (generally a password or PIN) used to verify the identity of (i.e. authenticate) a Signatory before allowing use of their private key (SCD) for signing. VAD takes the form of the passphrase entered by the user.
Wrapped key	A wrapped key contains encrypted key data as a byte block (according to the selected external standard for key wrapping). A wrapped key contains a subset of the data in a key blob.

See [CC1] for other Common Criteria abbreviations and terminology. Other relevant terminology for the application domain may also be found in EN 14169-1:2010 – Protection Profiles for Secure Signature Creation Device – Part 1: Overview.

2 ST Introduction

2.1 ST and TOE Reference Identification

TOE Reference:	nShield HSM family version 11.72.03
ST Reference:	NCT2-ST-0002
ST Version:	1-1
ST Date:	12 August 2019
CC version	3.1 Release 5
Assurance Level:	EAL4 augmented with AVA_VAN.5
ST Author:	nCipher Security Limited

The TOE is the nShield HSM family release v11.72.03.

The PCIe HSM is validated for FIPS level 2 and level 3. The evaluated configuration uses only the FIPS level 2 mode.

Section 2.2.6 describes the items included in the TOE in more detail, identifying the software items (and their versions) that are included in the TOE boundary as a part of each of the family members in the table above.

2.2 TOE Description

2.2.1 nShield HSM family Product Overview

The nShield HSM family are general purpose hardware security modules (HSMs), delivering dedicated cryptographic processing and key management capabilities for application servers, SSL/TLS web servers and security appliances. The nShield HSM family enables enterprises to add hardware protection to critical systems such as public key infrastructures (PKIs), identity management systems, databases, web servers, and application servers.

The nShield HSM family makes available a variety of cryptographic operations, encompassing encryption and decryption, hashing and message authentication, digital signature generation and verification, key exchange and key agreement functions on a managed set of keys that are maintained in a secure form with access to the keys being limited to specific sets of authorised users. As well as its own nCore development API, the TOE also supports the PKCS#11 API and thus enables straightforward integration with a wide range of application environments.

Whilst the members of the nShield HSM family are general purpose HSMs, the TOE defined in this Security Target is a member of the nShield HSM family acting as a secure signature-creation device (SSCD) that also generates keys for use in signing. The Security Target therefore presents the products in an evaluated configuration that is designed to meet the

requirements of a secure signature-creation device with key generation that provides electronic signatures as defined in [Regulation].

The TOE can generate and store multiple private keys (signature-creation data, or SCD) for use in signature generation, each with a unique identifier and set of authorisation data to determine when a Signature Creation Application (SCA) is authorised to use it. The nShield HSM family also provides functionality to receive and store certificate data, but it is up to application software in the operational environment to determine whether this feature is used, and it is not included in the scope of the TOE under this Security Target.

The TOE is described in more detail in section 2.2.2, and the intended deployment scenarios for the TOE are then described in section 2.2.4

2.2.2 nShield HSM family Description

Figure 1 below shows an nShield Solo+ F3 PCIe unit and an nShield Connect+ unit. The underlying software and hardware architecture of the TOE is shown in Figure 2 and Figure 3. As explained below, the nShield Connect+ unit itself *contains* an nShield Solo+ F3 PCIe unit.

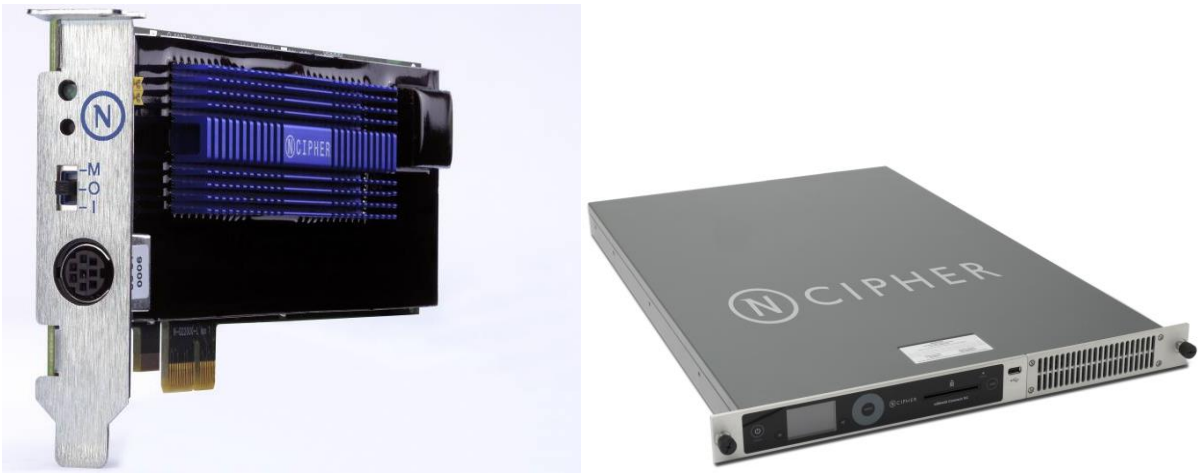

Figure 1: nShield Solo+ F3 PCIe unit and nShield Connect+ unit

The nShield Solo+ F3 PCIe unit connects directly via a serial cable to a smart card reader which is used to connect to smart cards inserted by Administrators and Signatories to authorise various operations (management operations, key generation operations or data signing operations). An nShield Connect+ unit has the smart card reader contained within its outer case.

The nShield Solo+ F3 PCIe unit can be located in either of two locations. In the first case, shown in Figure 2, the nShield Solo+ F3 is installed in a client PC in which the SCA is also running. In the second case, shown in Figure 3, the nShield Solo+ F3 PCIe unit is a component of an nShield Connect+ unit (i.e. a 19” rack-mounted hardware unit). For the nShield Connect+ case, the SCA runs in a client PC and both the nShield Connect+ unit and the client PC run instances of the nShield hardserver software, with an encrypted ‘impath’

link[2] between them. The hardserver software is called by client libraries linked into the SCA, or by invoking client utilities supplied with the nShield product.

In either case, the Security World, containing the encrypted SCD and other keys (see section 2.2.3) is stored separately in persistent storage attached to the client PC. This storage could be on a local disk, or on networked storage. The Security World data is encrypted and its plaintext content is only accessible to the nShield Solo+ F3 PCIe unit, therefore the location in which it is stored does not affect the security of the TOE. It can be located outside the TOE logical and/or physical boundaries.

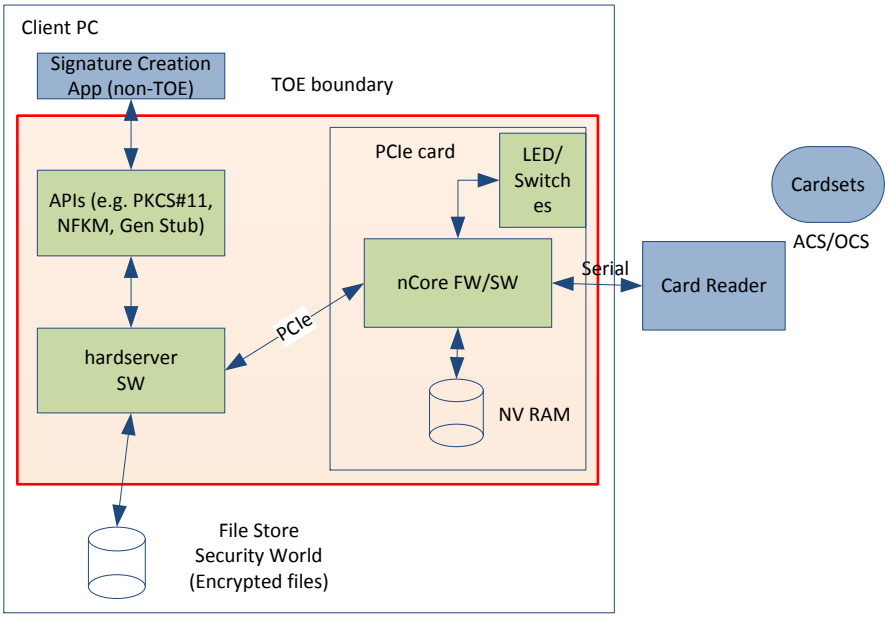

Figure 2: TOE boundary in nShield Solo configuration

[2] See Glossary and further description below.

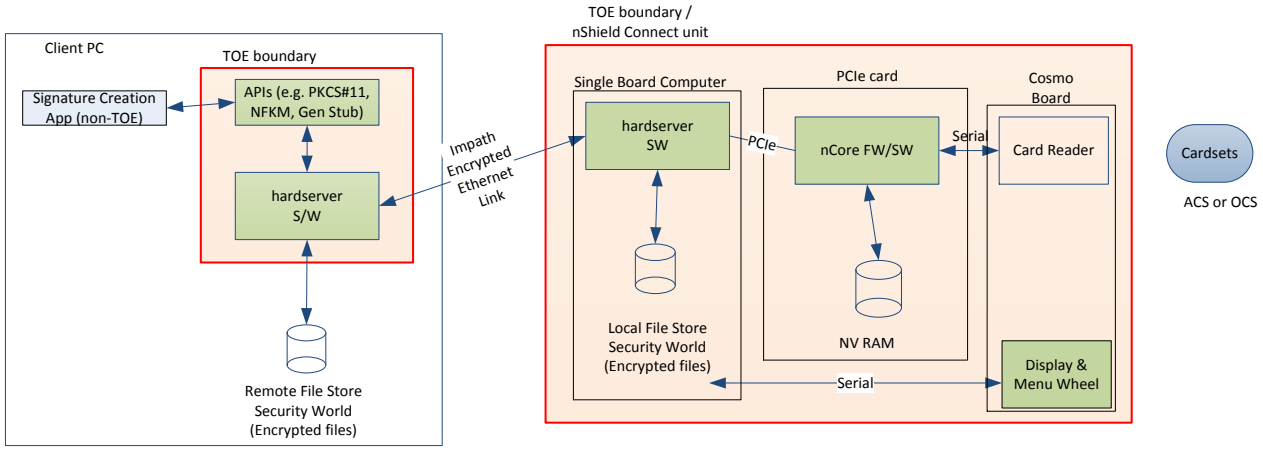

Figure 3: TOE boundary in nShield Connect configuration

In Figure 2, the client PC in which the TOE is installed runs client libraries and client utilities that call the hardserver software, which in turn communicates with the nShield Solo+ F3 PCIe unit to use its cryptographic services (provided by the nCore firmware). The hardserver maintains the Security World data (see section 2.2.3), which is held in storage connected to the client PC. Security World data is protected by the keys held in the PCIe card, and the PCIe card is the only location where unencrypted keys are held (keys used by applications are decrypted from Security World data that is passed to the PCIe card by the SCA, and the decrypted keys are held in the PCIe card while being used).

In Figure 3, both the client PC and the nShield Connect+ unit run separate instances of the same hardserver software, which enables communication between the client PC and the nShield Connect+ over a secure network. The connection between the client and the Connect is implemented by a proprietary protocol called ‘impath’, which protects the confidentiality and integrity of data. In this case the client hardserver maintains the Security World data (see section 2.2.3), which is held in storage connected to the client PC. Protection of the Security World data by keys held in the PCIe card applies in the same way as for the Client-located case described above for Figure 2. The Client PC linked to an nShield Connect+ runs client libraries and client utilities that access the Client PC hardserver, just as in Figure 2. Client utilities may also run and communicate with the hardserver on the nShield Connect+ (these all run on the nShield Connect+ motherboard, outside the PCIe card).

In both cases the smart card reader and ACS and OCS smart cards are not included in the TOE boundary as their correct operation is not required for the security of the system. No security claims are made about the reader or cards as they are required to be physically/procedurally protected by the environment.

The SCA is not part of the TOE, and is therefore treated as part of the TOE environment. Further details of the role and responsibilities of the SCA are described in the deployment scenarios in section 2.2.4. These responsibilities give rise to some of the security objectives for the environment in section 5.2.

2.2.3 TSF Keys and the Security World

The nShield HSM family protects SCDs by creating a Security World which is the infrastructure used for the secure lifecycle management of cryptographic keys. A Security World comprises:

- One or more nShield HSMs
- An Administrator Card Set (ACS) – a set of smart cards that, when combined together, give access to the TSF keys (K_{MSW} and K_{NSO}, as discussed below). The holders of these cards are Administrators. These keys are unique to a Security World, and shared by all the nShield HSMs included in that Security World.
- A repository of encrypted SCDs and associated supporting information stored by the client PC (typically using the Client PC OS's file system, but potentially in any data store or combination of stores).
- Optionally, one or more Operator Card Sets (OCSs) – a set of smart cards that, when combined together, and after submission of the correct passphrase for each inserted card, give access to one or more SCDs (each OCS gives access to a specific set of SCDs). The holders of these cards and their associated passphrases are Signatories.
- Optionally, a number of Softcards[3] stored in the repository described above – the contents of a Softcard, when combined with its correct passphrase, gives access to one or more SCDs (each Softcard gives access to a specific set of SCDs). The holders of the passphrases for Softcards are Signatories. The Security World infrastructure includes the particular ways in which keys, and hence SCD, are generated and protected by the nCore firmware using nested cryptographic structures that include K_{MSW}. This therefore limits the use of an SCD to the specific Security World in which it was created. Further details of some aspects of Security Worlds, such as the main infrastructure keys and the way in which SCD are protected, are given in later parts of this Security Target, but more details are provided in [UG].

The TOE uses two main keys to provide the protection features in this Security Target[4], and each of these is accessed by presenting an Access Token (also known in nShield terminology as a Logical Token)[5]

[3] An SCD can be protected either by an OCS or by a Softcard, but not by both. f

[4] The implementation of this abstract cryptographic architecture relies on other TSF keys which are not identified in this ST.

[5] The Access Token for a key is built by the TOE from a quorum of shares read from ACS or OCS cards, or from the share on a Softcard (depending on which of these methods was used to protect the key) – see Figure 4 and Figure 5. The mechanism for using an Access Token uses it as a key to decrypt the target key from its encrypted key blob form in the Security World. Because the Access Token is internal to the TOE and is not visible to users or applications it is not identified as a key in this external view of the TOE.

- K_{MSW} – the Security World module key

  Stored permanently in the PCIe card, with its Access Token split across the ACS cards. This key is the top-level key protecting all of the items in a Security World, except for K_{NSO}.

- K_{NSO} – the Security Officer's key

  Stored as an encrypted key blob in the Security World storage attached to the client PC, with its Access Token split across the ACS cards. This key is used to authorise certain privileged commands (because certain commands require the presentation of a "permission certificate" recording authorisation signed by K_{NSO}). It is noted that the 'Security Officer' is not a formal role defined for the TOE – it is defined only in an abstract way as a set of actions that require access to K_{NSO}. These Security Officer actions are a subset of the Administrator role identified in section 2.2.3.3 .

These keys are generated when the Security World is created on the TOE (or may be loaded as part of a Security World that is installed on the TOE). The presence of these top-level keys on the ACS cards means that the ACS cards require protection in the operational environment as sensitive items[6].

The ACS cards allow significant flexibility in the ways that administration operations can be divided between individuals. This is more fully described in [UG], but the essence of the mechanism is that the user chooses the number of ACS cards to create, and chooses how many of the complete set of cards are required to be provided in order to authorise an action (this number is referred to as the *quorum* for the card set). Each ACS card is protected by its own passphrase.

OCS cards are configured in a similar way to ACS cards: the creator of the OCS[7] chooses how many cards are in the set that protects a particular key, and then chooses how many of the set must be presented in order to authorise the use of the keys that the cards protect (the quorum for that card set).

When an SCD is created, it is stored (encrypted) in the Security World and given an identifier. To use the SCD, the SCA uses this identifier to read the encrypted key from the Security World, and passes this to the TOE as part of a request to use the SCD to create a signature. The TOE then manages the use of OCS or Softcard to access the SCD as described in section 2.2.3.1 .

2.2.3.1 Protection of SCD

The TOE protects keys (which represent SCD) by encrypting them under both Access Tokens (another form of key) and K_{MSW} and storing the resulting encrypted data in the Security World repository. Each Access Token is split into one or more Shares; the Shares are encrypted using a key derived from the passphrase and each Share is stored either on

[6] This is reflected in the application note for OE.Signatory in section 5.2.

[7] Any ACS or OCS cardholder can create a new OCS. In the context of this ST the expected process is that, where OCS rather than Softcards are used to protect SCD, then a new OCS is created to hold new SCD/SVD pairs for a new Signatory, and either the Signatory is present at the creation of the OCS, at which point they set their passphrase (VAD) for their card and generate the new SCD/SVD pair protected under the new OCS, or else that the creation of the OCS and passphrase is done by a trusted third party and the OCS and passphrase are both delivered to the Signatory using a secure delivery process (see also section 5.2.7 and section 2.2.5.1).

an OCS card or in a Softcard. For Softcard-protected SCD, a token always has exactly one Share. In the evaluated configuration, if an OCS comprises more than one card (e.g. to protect against accidental loss of a card) then all cards must be placed under the control of the Signatory.

When an application needs to use a key, it proceeds as follows (noting that the way in which the relevant user and SCD to use for a signing operation are identified is determined by the application, and is not within the scope of the TOE):

(1) The application determines (from its own database or from the Security World data) which OCS or Softcard is needed for access to the key it wishes to use.

(2) The application requests the Softcard or quorum of the relevant OCS cards associated with the SCD, which are required in order to extract the Shares to form the Access Token for the key.

(3) The Signatory enters their passphrase (and cards if using OCS), which the application collects and sends to the nShield Solo+ F3 PCIe card[8], enabling the TOE to decrypt the Shares held on the OCS or Softcard[9]. When each OCS card is inserted the TOE identifies the relevant card and returns its identity to the SCA (which can therefore display this information to the user).

(4) The passphrase(s) and data from the OCS or Softcard are combined in the nShield Solo+ F3 PCIe card to create the Access Token for this SCD (see Figure 4 and Figure 5).

(5) The application submits the encrypted key (which it may hold in its own database, or retrieve from the Security World data) to the TOE.

(6) The SCD is decrypted (using the Access Token), a handle to it is returned to the application, and the key is now available for use by that application for the remainder of the application session[10] (or until the application requests destruction of the key, or until the TOE detects that the final OCS card authorising the use of the SCD is removed from the smart card reader). In all cases keys held in TOE RAM (and plaintext keys are *only* held in TOE RAM) inside the nShield Solo+ F3 PCIe card are zeroised when deleted.

The process of using a 2-quorum of OCS cards to access an SCD (using shares 2 and 4 for the purposes of the example) is depicted in Figure 4. The process of using a Softcard to access an SCD is depicted in Figure 5.

---

[8] As in other places where the functionality of the nShield Solo+ F3 PCIe card is described, this applies whether the card is located in a client PC or an nShield Connect+ unit.

[9] This represents the checking of verification authentication data (VAD) from the user against reference authentication data (RAD).

[10] The application starts and ends sessions on the TOE using the utilities in section 2.2.6 to communicate with the hardserver and the nShield Solo+ F3 PCIe card. When the application signals the end of a session to the hardserver, the nShield Solo+ F3 PCIe card deletes the plaintext keys in memory by zeroization. The application can determine whether authentication (using an OCS or Softcard) is required on each individual use of a key or whether a successful authentication enables the key to be used an arbitrary number of times without further authentication, until the end of the session.

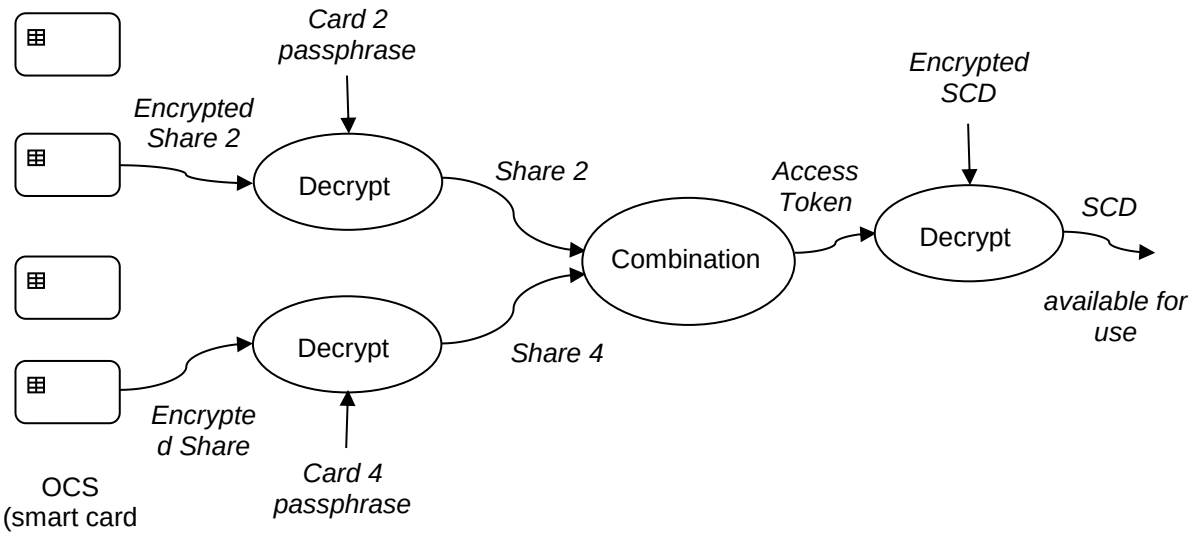

Figure 4: Gaining access to an SCD protected by an OCS

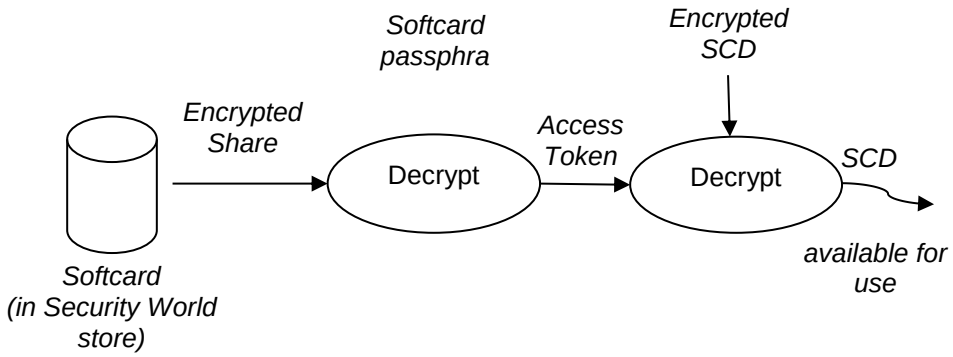

Figure 5: Gaining access to an SCD protected by a Softcard

2.2.3.2 States and Modes

The TOE implements the following state transition model.

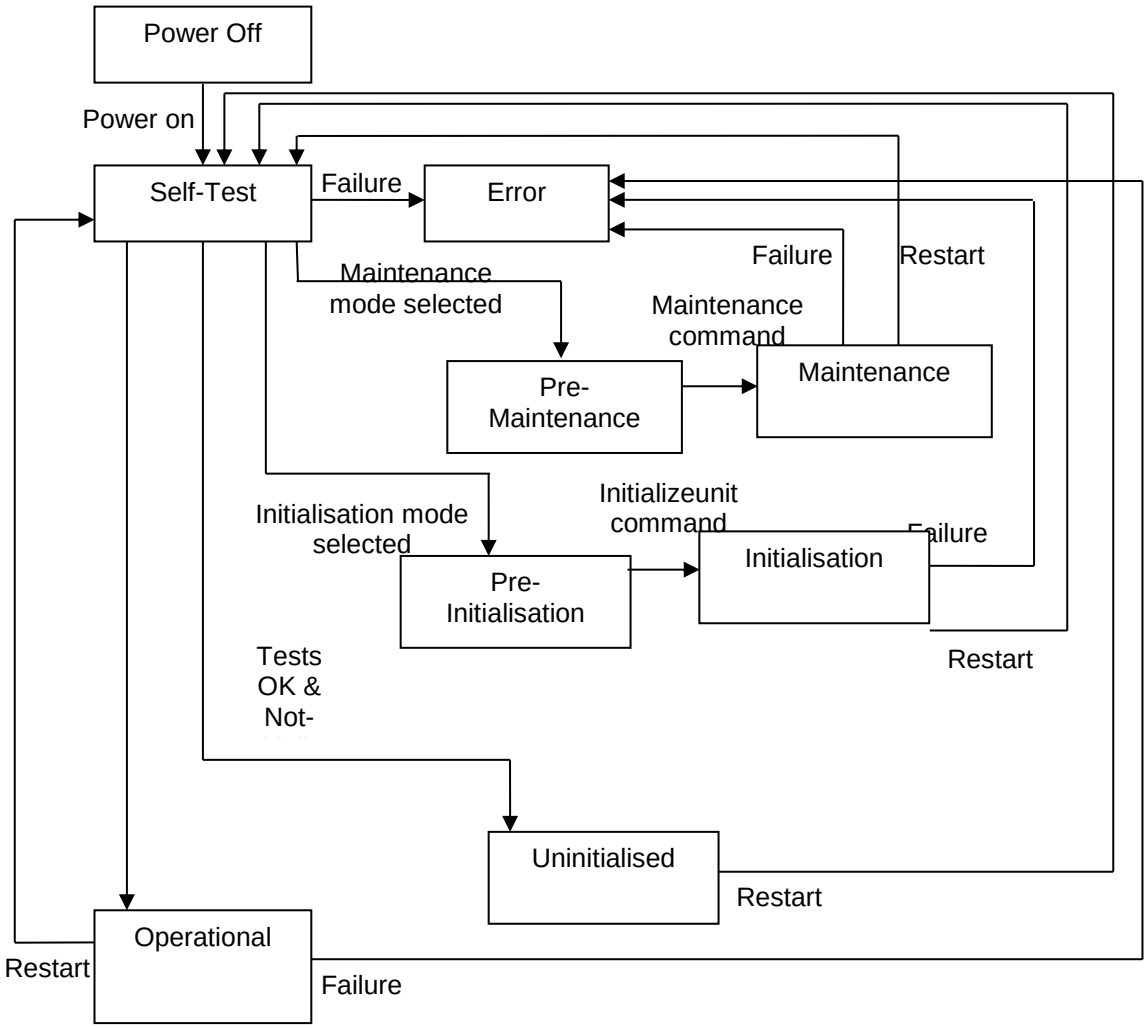

Figure 6: nShield HSM states and transitions

The TOE starts in a Power-off state[11], and on power-on enters a self-test mode that checks the hardware and cryptographic functions (the bus interface from the PCIe card and the smart card interface are inhibited in the self-test state). If any of these tests fail then the TOE enters a secure error state. If the self-tests succeed, then the TOE checks whether the Administrator has selected Pre-Maintenance mode using the mode switch on the module (see [UG, Appendix J])[12] – if so then the TOE enters the Pre-Maintenance state. After the TOE has been put into Pre-Maintenance mode, it is ready for maintenance. It enters maintenance mode when it receives a Maintenance command.

In the Maintenance state the user can restart the system or new firmware can be installed; if new firmware is installed then this operation will remove all keys and configuration data in

[11] Any other state can always return to the power-off state of course – this is not shown in Figure 6.

[12] In fact the Administrator selects the Maintenance state from the User Mode state, then restarts the nShield unit (from the CLI or by using the Clear switch on the module) which, after Self-Test, will then move to the Pre-Maintenance state.

the PCIe card and will therefore require re-initialisation of the TOE (including reinstallation of the Security World) before it can be used again. From the Maintenance state the TOE is either restarted (following user abort or successful upgrade, returning to the self-test state) or else enters the error state due to a failure. If no firmware installation was performed then when the TOE is restarted the self-test process will still recognise it as initialised.

Alternatively, if the Administrator has selected the Initialisation operation from the mode switch then the TOE enters the Pre-Initialisation state[13]. After the TOE has been put into Pre-Initialization, it is ready to be initialised. It enters Initialisation mode when it receives an initialization command. Initialising the TOE will remove all keys and configuration data in the PCIe card and will therefore require reinstallation of the Security World before it can be used again. From the Initialisation state the TOE is either restarted (returning to the self-test state in an Pre-Initialised state) or else enters the error state due to a failure. The TOE is delivered in a state where Initialisation has been completed, meaning that the TOE has generated a set of high-level keys (as in section 2.2.3), but the rest of the Security World (e.g. ACS, OCS and SCDs) has not been created.

If neither Maintenance nor Initialisation was selected then (as the last stage of the self-test) the TOE checks whether it has been initialised. If not, then it enters the Uninitialised state which can only be left either by entering the Error state (if it is sent a 'Fail' command) or by being restarted and returning to the self-test state.

Once the TOE completes a self-test and has been initialised, it enters the Operational Mode state.

2.2.3.3 Roles

The Administrator role (R.Admin) is mapped to the holders of ACS cards for the nShield HSM (cf. section 2.2.3). Administrators have access to the K_{NSO} key and therefore also fulfil the abstract role of 'Security Officer' (cf. section 2.2.3).

The Signatory role (R.Sigy) is mapped to holders of OCS cards (and their associated passphrases that enable their use) or Softcard passphrases – these are used to control access to SCDs.

2.2.3.4 Backup and Recovery of the Security World

The Security World can be backed up simply by copying the data from the store to a separate backup location. Because this data is encrypted and protected by a MAC this does not introduce confidentiality concerns (nor integrity concerns if this data were to be restored[14]). The Security World data includes the information necessary to associate SCD with its correct OCS or Softcards, and hence with the correct Signatory.

Provided that the TSF infrastructure keys (see section 2.2.3) are still present in one or more of the nShield HSMs in the Security World then the restored Security World data can be used as before. If an nShield HSM has failed and the TSF keys need to be restored then this

[13] As with Maintenance, the Administrator selects the Initialisation state from the User Mode state, then restarts the nShield Connect+ which, after Self-Test, will then move to the Pre-Initialisation state.

[14] Note that inside the Security World keys are identified by their hashes, and therefore a different key value cannot be restored to an existing Key identity.

can be done (either to the old nShield HSM or to a new nShield HSM) by using the ACS cards. Presenting a quorum of ACS cards and their associated passphrases grants the ability to recreate the keys from data present on the ACS itself, and to load them into a new nShield HSM.

The recovery process does not decrypt the Security World data or give the opportunity to change the OCS cards or Softcards associated with keys stored in the Security World)[15].

2.2.3.5 Security of the SCA-SSCD Connection

In the case of an installation of the TOE as shown in Figure 2, the DTBS/R transmitted between SCA and the SSCD is not exposed outside the physically secure environment (cf. A.Env) since it travels only inside the memory space of the client PC. In the case of an installation as shown in Figure 3, the DTBS/R travels from the hardserver on the client PC to the hardserver on the nShield Connect+ unit, and the path between the client PC and the nShield Connect+ unit is protected by an encrypted channel (the impath).

In general terms, the SCA provides the interaction with the user, generating or verifying the DTBS, obtaining the user's approval that this is the correct DTBS to sign and prompting the user for authentication data (VAD). Although the SSCD prevents access to the key material that is used to create a signature (SCD), compromise of the SCA would permit an attacker to amend a message after the user has verified it and approved the use of the SCD, or possibly to send extra messages to the SSCD after the user has loaded SCD and to have these signed without further authorisation of the SCD owner. This would enable the attacker to use the SSCD to sign messages of their own choosing.

This ST includes a security objective for the operational environment (OE.DTBS_Protect – see section 5.2.6) that is part of protecting the DTBS/R in transit from the SCA to the SSCD. This security objective relies on secure inter-process communication in the operating system. It is therefore part of the risk management for the environment to take appropriate steps to ensure that there is sufficient confidence in the operating system (relative to the risk environment). This might, for example, involve the SCA checking signatures returned to confirm that they relate to the intended DTBS/R.

As with any computing system, the SCA and SSCD platforms should implement risk-based security controls at the operating system level, such as role and identity-based access controls, logging of accountability data, and good operational security procedures (anti-virus, intrusion detection, patching, etc.).

In the specific case of the nShield Solo+ F3 TOE the hardserver in the client PC communicates with a local nShield Solo module connected to the PCIe bus in the hardware on which the Application Server (and hence the SCA) is running. The PCIe bus (which is not part of the TOE) provides error correction which protects the integrity of the DTBS/R data as it travels from the client PC memory to the nShield Solo+ F3 module installed in the client PC. However, the main protection measures in this case are the maintenance of a secure hardware and software environment (as in A.Env).

[15] Recovering a Security World is therefore distinct from recovering *individual* keys. There is a mechanism for recovering individual keys (referred to as 'Key Recovery' in [UG]), but this mechanism is disabled in the evaluated configuration (using the '-no-recovery' parameter to new-world described in [UG]).

In the nShield Connect+ case the client PC communicates with one or more nShield Connect+ units remotely over an impath connection (which is a part of the TOE). The impath connection protects the integrity of the DTBS/R data in transit from the client PC to the nShield Connect+ unit.

2.2.4 Deployment Scenarios

The nShield TOE can be flexibly deployed to meet a range of different operational scenarios. The following scenarios are covered by this Security Target. In all cases the TOE protects the SCD by encrypting it under an Access Token that is itself protected by storage in a Softcard or an OCS. The main differences are in the role and responsibilities of the SCA for collecting and delivering the authentication data that is used to recover the Access Token and hence to enable the use of the SCD on behalf of the Signatory (these responsibilities give rise to some of the security objectives for the environment in section 5.2). In all cases the SCA is also responsible for delivering the DTBS/R securely to the TOE.

2.2.4.1 Local Use

In the local use scenarios, the Signatory is physically present at the TOE, and therefore authenticates at the TOE when his or her SCD is accessed. Such scenarios would occur when, for example, an organisation deploys the TOE to manage SCD used by employees at the same physical site as the TOE, or where a person physically attends the site of a trusted third party organisation (responsible for holding encrypted SCD and operating the signature process) in order to use his or her SCD.

When a signature is to be created by the SCA, then either a Softcard or an OCS may be used to access the SCD (depending on which of these protection methods was used when the SCD was created) as described in the subsections below.

2.2.4.2 Local Softcard Use

When an SCD is required, the Encrypted Share is first retrieved from the relevant Softcard. The Softcard is retrieved from the Security World store and the Signatory enters a passphrase (via the SCA) that will enable the TOE to extract the Share and hence the Access Token as described in section 2.2.3.1 (and depicted in Figure 5). In the Softcard case only a single Share is required in order to access the SCD.

This scenario is depicted in Figure 7. The SCA selects the Softcard and SCD for the Signatory, then collects the authentication data from the Signatory and delivers it directly to the TOE via a TOE interface.

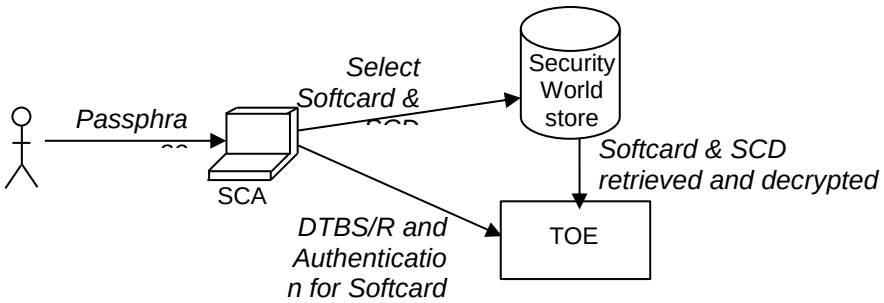

Figure 7: Local Softcard Deployment Scenario

2.2.4.3 Local OCS use

When an SCD is required, the relevant Access Token is retrieved by combining Shares from a number of OCS cards. The relevant smart cards are inserted into the smart card reader attached to the TOE and the passphrase for the card is entered by the Signatory. The insertion of cards and passphrases is then repeated until a quorum of Shares has been obtained as described in section 2.2.3.1 (and depicted in Figure 4).

This scenario is shown in Figure 8. The SCA selects the SCD for the Signatory, then collects the authentication data from the Signatory for each OCS card and delivers it directly to the TOE via a TOE interface.

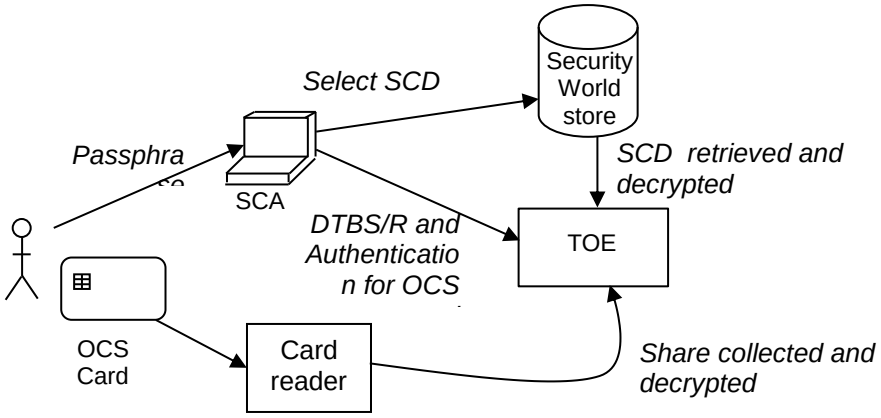

Figure 8: Local OCS Deployment Scenario

2.2.4.4 Remote Use

In remote use deployment scenarios, a trusted third party provides a signing service to a remote end user (the Remote Signatory) who does not have direct access to the TOE but needs to be able to create secure signatures. The trusted third party is thus managing the TOE on behalf of multiple Remote Signatories. Remote Signatories authenticate via the SCA, using a passphrase that protects a Softcard, which in turn protects the Signatory's SCD.

This scenario is depicted in Figure 7. As in the local Softcard scenario in section 2.2.4.2 , the SCA selects the Softcard and SCD for the Signatory, then collects the authentication data from the Signatory and delivers it to the TOE. This is used to access and use the SCD inside the TOE as described in section 2.2.3.1 . In this case the SCA is therefore responsible for protection of data transmitted across this external network environment until the data is delivered to the TOE[16]. The SCA is also responsible for protecting any other activities that it makes available and that involve sensitive data, such as passphrase change.

[16] There could also be a component of the SCA at the trusted third party site with the TOE, but this is not shown in Figure 9.

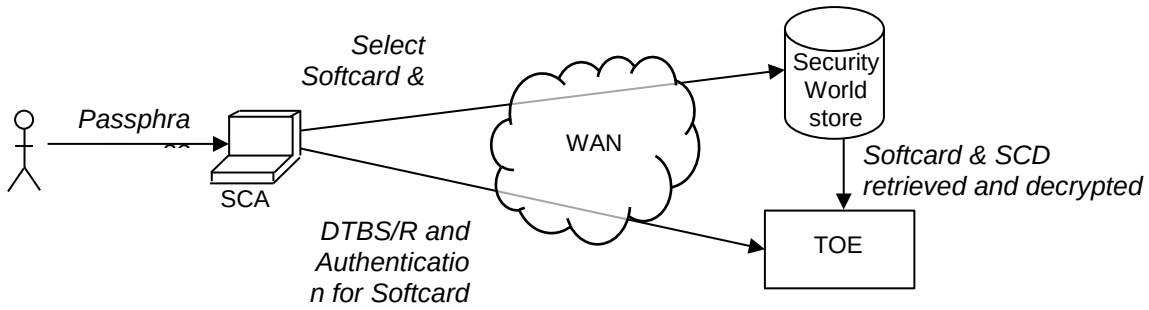

Figure 9: Remote Use Deployment Scenario

2.2.5 SSCD-Provisioning and SCD-Provisioning Lifecycle

The SSCD implemented by the TOE is made available by an organisation for use in creating SCD/SVD pairs and in creating digital signatures using an SCD that the TOE has previously generated. SSCD-Provisioning in this case therefore consists of installing the TOE in its evaluated configuration (following [CCECG]), making it available, and operating it to provide an SCD-Provisioning service.

The SCD-Provisioning lifecycle includes the creation of an SCD/SVD pair by the TOE, and the subsequent use of the SCD to create digital signatures on behalf of the Signatory using the TOE. The lifecycle comprises the following stages:

- Preparation stage
- Operational Use Stage
- Termination Stage.

The sections below describe these lifecycle stages in more detail.

2.2.5.1 Preparation Stage

The Preparation stage assumes that the TOE has been correctly installed and the Security World created (according to [CCECG]). The TOE may be located at the user's own site (in the case of an organisation that installs the TOE to produce digital signatures on its own behalf), or at the site of a trusted third party that provides digital signature services on behalf of the user or their organisation. The steps carried out by the Signatory (or in their presence) and the steps carried out on their behalf by the trusted third party may vary between different deployments.

The actions involved in creating SCD/SVD pairs are as follows:

- Creation of an OCS or Softcard.

  The OCS or Softcard that is to be used to protect the SCD is always created before the SCD/SVD pair (because creation of the OCS or Softcard includes generation of the Access Token that will be used to protect the SCD as part of the SCD/SVD pair generation step below).

  The OCS or Softcard will be associated with an individual Signatory, and therefore this step requires obtaining information on the intended recipient of the OCS or

Softcard as required by the SCD-Provisioning service provider for the preparation process and for identification as a legitimate Signatory and user of the TOE.

In cases where the Signatory is not physically present at the generation of an OCS, the SCD-Provisioning service provider must arrange for secure delivery of the OCS to the Signatory.

- Creation of the passphrase to protect an OCS card or Softcard.

  Each OCS card and each Softcard requires its own passphrase[17], which represents the VAD. The passphrase is not directly stored in the OCS or Softcard, but only when the correct passphrase is entered can the data stored in the OCS or Softcard be decrypted to a usable form (as described in section 2.2.3.1). The encrypted data in the OCS or Softcard therefore represents the RAD.

  Procedural measures must ensure that passphrases are of an appropriate strength to protect the SCD against exploitation of brute force attacks to create digital signatures on behalf of an attacker.

  In cases where the Signatory is not physically present at the generation of the passphrase, the SCD-Provisioning service provider must arrange for secure delivery of the passphrase to the Signatory.

- Generation of the SCD/SVD pair, and protection of the SCD under the relevant OCS or Softcard associated with its intended user.

  Whenever an SCD/SVD pair is generated then the TOE requires that the OCS or Softcard to protect it is identified (and the relevant passphrase(s) submitted). In cases where the Signatory is not physically present, the SCD-Provisioning service provider must employ a process that ensures the security of the passphrase when it is used to protect the new SCD[18].

- Certification of the SVD by the Certificate Generating Application (CGA) and Certification Services Provider (CSP).

  The TOE is requested (by non-TOE application software) to export the SVD for separate certification by a Certification Services Provider (CSP) via the use of a Certificate Generating Application (CGA). The format of the exported SVD will then depend on the particular certification process and its requirements (and is therefore outside the scope of this ST). If required, the external certificate can be imported into the TOE and stored in the Security World.

[17] Although the nShield product allows the creation of OCS cards and passphrases without passwords, the evaluated configuration covered by this Security Target, and established by following [CCECG] requires that passphrases are used for all OCS cards and Softcards.

[18] For example, in some deployments the passphrase might be supplied by the Signatory over a secure network connection. In other deployments the initial passphrase generated with the OCS or Softcard might be retained by the SCD-Provisioning service itself and supplied when the SCD/SVD pair is generated; the passphrase would then be securely changed and distributed to the user.

The resulting certificate provides the critical link between future digital signatures produced using the corresponding SCD and the person identified as the owner in the certificate.

Apart from providing export of the SVD, the SVD certification step is outside the scope of the TOE.

2.2.5.2 Operational Use Stage

In this lifecycle stage the TOE is available to the Signatory for creation of signatures.

Other Administrative operations that may be carried out in this stage include:

- Creation of additional SCD/SVD pairs
- Creation of additional OCS and Softcards
- OCS erasure
- Replacing the current ACS with a new ACS
- Changing the passphrase (VAD) for a smart card or Softcard. Where the ability to change the passphrase is given to remote users, then the environment is responsible for protecting the passphrase values while they are entered and transmitted to the TOE.

2.2.5.3 Termination Stage

The end of the SCD's life is reached when the user decides no longer to use that SCD, or when the user's relationship with the trusted third party who provides the signing service comes to an end. SCD can be deleted at this time (or indeed at *any* time) by deleting the data that contain the encrypted SCD in the Security World store (along with any other copies of this data that may have been made, e.g. as backups). The OCS or Softcard that protects the SCD should also be destroyed at this point.

When the entire TOE (rather than an individual SCD) reaches the end of its life, then the Administrator securely erases the relevant Security World data and top-level protection keys (see K_{MSW} and K_{NSO} in section 2.2.3).

2.2.6 Physical and Logical Scope of the TOE

The physical and logical boundaries of the TOE are shown in Figure 2 and Figure 3. The TOE therefore includes the following items:

Type	Name	Identifier	Form factor	Delivery
Hardware	nShield Solo F3 PCIe 500+	Model number NC4433E-500	PCIe board	Courier
	nShield Solo F3 PCIe 6000+	Model number	PCIe board	Courier

Type	Name	Identifier	Form factor	Delivery
		NC4433E-6K0		
	nShield Connect 500+	Model number NH2054	Network appliance	Courier
	nShield Connect 1500+	Model number NH2061	Network appliance	Courier
	nShield Connect 6000+	Model number NH2068	Network appliance	Courier
Firmware	nCore firmware	version 2.55.4	Binary image file	Shipped with the nShield Solo+ F3 or Web download
	nShield Connect firmware image	version 12.45.1	Binary image file	Shipped with the nShield Connect+ or Web download
Software	Hardserver	version 2.92.1	ISO image	Web download
	Generic stub library	version 3.30.5	ISO image	Web download
	NFKM and RQ card library	version 1.86.1	ISO image	Web download
	PKCS#11 libray	version 2.14.1	ISO image	Web download
	Client utilities nopclearfail, fwcheck, loadrom, nfloadmon, ppmk, cardpp, createocs, generatekey, new-world, racs.	version 2.54.1	ISO image	Web download
Documentation	nShield HSM family v11.72.03 Common Criteria Evaluated Configuration Guide	v1.3	pdf file	Web download

Table 1: TOE scope

2.2.7 Required non-TOE hardware and software

The following items are required in order to operate the TOE but are not part of the TOE:

- Additional utilities other than those identified as part of the TOE in section 2.2.6, encompassing:

  - General utilities (see [UG, Utilities for general operations])
  - Hardware utilities (see [UG, Hardware utilities])
  - Test utilities (see [UG, Test analysis tools] and [UG, Developer-specific utilities])
  - Security World utilities (see [UG, Security World utilities])

- Client applications

- One of the following Operating Systems:

  - Microsoft Windows Server 2012 R2
  - Microsoft Windows 7 IA-32/x64
  - Red Hat Enterprise Linux AS/ES 6 x64

- Client hardware (running client applications and client hardserver)

- Smart card reader (included in the nShield Connect+ unit; separate reader supplied with nShield Solo – part number A-018000-L (SMARTCARD READER TL ASSY))

- Smart cards for ACS and OCS (included with the nShield Solo and Connect products – part numbers AC3148T (pack of 5 smartcards) or AC3155T (pack of 10 smartcards)).

The TOE software does not place any requirements on minimum hardware beyond those required to run the relevant client operating system and applications.

3 CC Conformance

3.1 Conformance to Common Criteria

As defined by the references [CC1], [CC2] and [CC3], this TOE conforms to the requirements of Common Criteria v3.1, Revision 5. The methodology applied for the evaluation is defined in [CEM].

The TOE is Part 2 and Part 3 conformant, and meets the requirements of EAL4 augmented by AVA_VAN.5.

3.2 Conformance to Protection Profiles

This ST does not claim conformance to any PP.

4 Security Problem Definition

4.1 Assets and Objects

The assets and objects protected by the TOE are:

- SCD: the private key used to perform a digital signature operation. The confidentiality, integrity and Signatory's sole control over the use of the SCD must be maintained.
- SVD: the public key linked to the SCD and used to perform digital signature verification. The integrity of the SVD when it is exported must be maintained.
- DTBS/R: a set of data, or its representation, which the Signatory intends to sign. Their integrity and the unforgeability of the link to the Signatory provided by the digital signature must be maintained. (The DTBS/R is protected by the TOE when transmitted between the Client PC and an nShield Connect+ - see section 2.2.3.5 .)
- Signature-creation function of the TOE to create a digital signature for the DTBS/R with the SCD.

4.2 Subjects

The subjects in this ST are:

- User (S.User): an end user of the TOE who can be identified as an Administrator or a Signatory – this includes remote users (acting as Remote Signatories) who access the TOE via an SCA over a network (cf. the deployment scenarios in section 2.2.4.4). In the TOE the subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.
- Administrator (S.Admin): an S.User who is responsible for performing the TOE initialisation, TOE personalisation or other TOE administrative functions. In the TOE the subject S.Admin is acting in the role R.Admin for this user after successful authentication as Administrator.
- Signatory (S.Sigy): an S.User who has legitimate access to the TOE (either directly or as part of a remote service) and uses it on his own behalf or on behalf of the natural or legal person or entity he represents. This includes Remote Signatories who access the TOE via an SCA over a network (cf. the deployment scenarios in section 2.2.4.4) In the TOE the subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as Signatory.
- Attacker: a threat agent, in the form of a human or a process acting on their behalf, located outside the TOE. The main goal of the attacker is to access the SCD or to falsify a digital signature. An attacker has a high attack potential and knows no secrets.

4.3 Threats

The threats to the IT assets against which protection is required by the TOE or by the security environment are as follows.

4.3.1 T.SCD_Divulg: Storing, copying, and releasing of the signature-creation data

An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature-creation in the TOE.

4.3.2 T.SCD_Derive: Derive the signature-creation data

An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

4.3.3 T.Hack_Phys: Physical attacks through the TOE interfaces

An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

4.3.4 T.SVD_Forgery: Forgery of the signature verification data

An attacker presents a forged SVD to the CGA. This results in loss of SVD integrity in the certificate of the Signatory.

4.3.5 T.SigF_Misuse: Misuse of the signature creation function of the TOE

An attacker misuses the signature-creation function of the TOE to create a digital signature for data the Signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

4.3.6 T.DTBS_Forgery: Forgery of the DTBS/R

An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the Signatory intended to sign.

ST Application Note ST1

Protection of the DTBS and DTBS/R by the TOE applies only to the use of an impath between a Client PC and an nShield Connect+ - see section 2.2.3.5 .

4.3.7 T.Sig_Forgery: Forgery of the digital signature

Without use of the SCD an attacker forges data with associated digital signature and the verification of the digital signature using the SVD does not detect the forgery. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack

potential with advanced knowledge of security principles and concepts employed by the TOE.

4.4 Organisational Security Policies

4.4.1 P.CSP_QCert: Qualified certificate

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate for the SVD generated by the SSCD. The certificates contain at least the name of the Signatory and the SVD matching the SCD implemented in the TOE under sole control of the Signatory. The CSP ensures that the use of the TOE as SSCD is evident for individual signatures through the related certificate or other publicly available information.

4.4.2 P.QSign: Qualified electronic signatures

The Signatory uses a signature-creation system to sign data with an advanced electronic signature, which is a qualified electronic signature if it is based on a valid qualified certificate. The DTBS are presented to the Signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the digital signature created with an SCD implemented in the SSCD that the Signatory maintains under his sole control and that is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

4.4.3 P.Sigy_SSCD: TOE as secure signature creation device

The TOE meets the requirements for an SSCD laid down in [Regulation, Annex II] This implies that the SCD is used for digital signature creation under sole control of the Signatory and that the SCD can practically occur only once.

4.4.4 P.Sig_Non-Repud: Non-repudiation of signatures

The life cycle of the SSCD, the SCD and the SVD shall be implemented in a way that the Signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in his un-revoked certificate.

4.5 Assumptions

4.5.1 A.CGA: Trustworthy certification-generation application

The CGA protects the authenticity of the Signatory’s name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP.

4.5.2 A.SCA: Trustworthy signature-creation application

The Signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of the data the Signatory wishes to sign in a form appropriate for signing by the TOE.

4.5.3 A.Env: Protected operating environment

The TOE operates in a protected environment that limits physical access to the TOE to authorised Administrators and Signatories. The TOE software and hardware environment is maintained by Administrators in a secure state, including protection against unauthorised software and configuration changes.

4.5.4 A.REnv: Protected remote deployment

In addition to the requirements of OE.DTBS_Intend, in a remote deployment scenario the environment is responsible for ensuring that the:

- security and integrity of the components of the Remote Signatory's system are maintained entirely under the control of the user (or of a suitable organisational authority acting on the user's behalf)

- SCA preserves the confidentiality, integrity and authenticity of data transferred between the end-user and the SCA (including, for example, the confidentiality of any sensitive authentication data, and the integrity and authenticity of the DTBS/R).

5 Security Objectives

5.1 Security Objectives for the TOE

The security objectives for the TOE are as follows.

5.1.1 OT.Lifecycle_Security: Lifecycle security

The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide functionality to securely destroy the SCD.

ST Application Note ST2

The TOE provides support for protecting and using more than one SCD.

5.1.2 OT.SCD/SVD_Gen: SCD/SVD generation

The TOE provides security features to ensure that only authorised users invoke the generation of the SCD and the SVD.

5.1.3 OT.SCD_Unique: Uniqueness of the signature-creation data

The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation can practically occur only once and cannot be reconstructed from the SVD. In this context ‘practically occur once’ means that the probability of equal SCDs is negligible.

5.1.4 OT.SCD_SVD_Corresp: Correspondence between SVD and SCD

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating a digital signature creation with the SCD.

5.1.5 OT.SCD_Secrecy: Secrecy of the signature-creation data

The secrecy of an SCD (used for signature creation) is reasonably assured against attacks with a high attack potential.

5.1.6 OT.Sig_Secure: Cryptographic security of the digital signature

The TOE generates digital signatures that cannot be forged without knowledge of the SCD, through robust encryption techniques. The SCD cannot be reconstructed using the digital signatures or any other data exported from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

5.1.7 OT.Sigy_SigF: Signature creation function for the legitimate Signatory only

The TOE provides the digital signature creation function for the legitimate Signatory only and protects the SCD against attempts by other users to create a digital signature using it. The TOE shall resist attacks with high attack potential.

5.1.8 OT.DTBS_Integrity_TOE: DTBS/R integrity inside the TOE

The TOE shall not alter the DTBS/R This objective does not conflict with a signature-creation process where the TOE applies a cryptographic hash function on the DTBS/R to prepare for signature creation algorithm.

ST Application Note ST3

When DTBS/R is transmitted between hardservers in the nShield Connect+ architecture in Figure 3 then the impath shall protect the integrity of the DTBS/R.

5.1.9 OT.Tamper_ID: Tamper detection

The TOE provides system features that detect physical tampering of its components, and uses those features to limit security breaches.

5.1.10 OT.Tamper_Resistance: Tamper resistance

The TOE prevents or resists physical tampering with specified system devices and components.

5.2 Security Objectives for the Operational Environment

The objectives that are required to be met by the TOE's operational environment are as follows.

5.2.1 OE.SVD_Auth: Authenticity of the SVD

The operational environment ensures the integrity of the SVD exported by the TOE to the CGA. The CGA defines a procedure to enable it to verify the correspondence between the SCD in the SSCD of the Signatory and the SVD in the input provided to the certificate generation function of the CSP.

5.2.2 OE.CGA_QCert: Generation of qualified certificates

The CGA generates a qualified certificate that includes, inter alia

- the name or pseudonym of the Signatory
- the SVD matching the SCD stored in the TOE and controlled by the Signatory
- the advanced signature of the CSP.

The CGA confirms with the generated certificate that the SCD corresponding to the SVD is stored in an SSCD.

5.2.3 OE.SSCD_Prov_Service: Authentic SSCD provided by SSCD Provisioning Service

The SSCD Provisioning Service handles authentic devices that implement the TOE to be prepared for the legitimate user as Signatory, and personalises and provides the TOE as SSCD to the Signatory.

ST Application Note ST4

As described in 2.2.4 the TOE may be provided either locally or remotely. In either case the SSCD Provisioning Service, or equivalent entity, must:

- ensure that all OCS cards associated with an SCD are provided only to the Signatory, and that the associated passphrases (after the SCD has been issued to the Signatory) are known only by the Signatory
- ensure a Signatory's Softcard passphrase is known only by the Signatory.

5.2.4 OE.HID_VAD: Protection of the VAD

If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface.

5.2.5 OE.DTBS_Intend: SCA sends data intended to be signed

The Signatory uses a trustworthy SCA that

- generates the DTBS/R of the data that has been presented as DTBS and which the Signatory intends to sign in a form which is appropriate for signing by the TOE
- sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE
- attaches the signature produced by the TOE to the data or provides it separately.

ST Application Note ST5

Protection of the DTBS and DTBS/R by the TOE applies only to the use of an impath between a Client PC and an nShield Connect+ - see section 2.2.3.5 .

5.2.6 OE.DTBS_Protect: SCA protects the data intended to be signed

The operational environment ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE.

5.2.7 OE.Signatory: Security obligation of the Signatory

The Signatory keeps the VAD (i.e. the passphrase) associated with his or her OCS card(s) or Softcards confidential and keeps OCS card(s) under his or her control.

The Signatory also checks that:

- The OCS / Softcard and associated passphrase are generated in their presence, or

- The OCS / Softcard and associated passphrase are generated remotely and are securely delivered by their trusted third party.

5.2.8 OE.Inspect: Regular tamper inspection of the TOE

The TOE shall be inspected at regular intervals for signs of tampering to the TOE. The frequency of such inspections shall be determined by risk assessment of the tampering threat in the specific operational environment.

5.2.9 OE.Env: Protected operating environment

The TOE operates in a protected environment that limits physical and logical access to the TOE to authorised Administrators and Signatories. The TOE software and hardware environment is maintained by Administrators in a secure state, including protection against unauthorised software and configuration changes.

ST Application Note ST6

The protected environment therefore limits physical and logical access to the client PC and network to which a Connect unit is attached (cf. Figure 2 & Figure 3). All protective measures should be based on a risk management approach, following assessment of the risks in the specific operating environment in which the TOE is deployed.

5.2.10 OE.REnv: Protected remote deployment

In addition to the requirements of OE.DTBS_Intend, in a remote deployment scenario the environment is responsible for ensuring:

- that the security and integrity of the components of the Remote Signatory's system are maintained entirely under the control of the user (or of a suitable organisational authority acting on the user's behalf)
- that the SCA preserves the confidentiality, integrity and authenticity of data transferred between the end-user and the SCA (including, for example, the confidentiality of any sensitive authentication data, and the integrity and authenticity of the DTBS/R).

6 IT Security Requirements

6.1 Conventions

Footnotes are used to indicate completions made in this ST to operations in the SFRs.

The following additional conventions are used for the completion of operations:

- Refinements are denoted in one of two ways, depending on whether they add detail to an SFR ('explanatory refinements') or update the text of an SFR element ('element refinements'). Explanatory refinements follow the SFR that they update and are marked by the word "Refinement" in bold followed by bold text describing the refinement. Element refinements are indicated by bold text within an SFR element, with the original text indicated in a footnote.
- Selections and assignments made in this ST are italicised, and the original text is indicated in a footnote.

See section 1.2 for the convention on the use of Application Notes.

6.2 Security Functional Requirements

The individual security functional requirements are specified in the sections below.

6.2.1 Cryptographic Support (FCS)

FCS_CKM.1 *Cryptographic key generation*

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate an SCD/SVD pair[19] in accordance with a specified cryptographic key generation algorithm as shown in the SCD/SVD Generation Table20 and specified cryptographic key sizes as shown in the SCD/SVD Generation Table21 that meet the following: standards as shown in the SCD/SVD Generation Table22.

[19] cryptographic keys

[20] [assignment*: cryptographic key generation algorithm*]

[21] [assignment*: cryptographic key sizes*]

[22] [assignment*: list of standards*]

Key Generation Algorithm	Key Sizes	Applicable Standards
RSA – generation of probable primes	2048-bit to 16384-bit	None
DSA - generation of domain parameters and key pairs	2048-bit to 3072-bit	FIPS 186-4
ECDSA – generation of key pairs	224-bit to 521-bit	FIPS 186-4

Table 2: SCD/SVD Generation Table

ST Application Note ST7

The TOE supports generation and use of key lengths and algorithms that meet or exceed the requirements of [ETSI] and thus ensures that signatures cannot be forged, as required by [Regulation, Annex II para 1 (c)]. Namely:

- RSA keys of up to 16384 bits; ETSI recommended minimum 2048-bits
- DSA keys up to 3072-bits; ETSI recommended minimum 2048-bits
- ECDSA keys up to 521 bits; ETSI recommended minimum 224-bits.

As well as meeting the ETSI recommendations, the TOE also meets the guidelines for key sizes issued by NIST in SP800-131A.

Key generation is performed using an approved DRBG seeded from a hardware entropy source acting as a hybrid source in the terms [ETSI] document. This ensures that SCD can practically occur only once as required by [Regulation, Annexe II para 1 (b)].

The user must only use the key lengths listed in Table 2 – this is not enforced by the TOE.

FCS_CKM.4 *Cryptographic key destruction*

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroization*[23] that meets the following: *FIPS140-2*[24].

[23] [assignment*: cryptographic key destruction method*]

[24] [assignment*: list of standards*]

The key destruction covered by FCS_CKM.4 applies to plaintext keys held in TOE RAM (plaintext keys are not held anywhere other than in TOE RAM). Encrypted keys are destroyed simply by deleting the relevant Security World data (cf. section 2.2.3) and/or the OCS associated with the key (cf. section 2.2.3.1); since these items do not contain the plaintext keys they do not require any specific destruction method such as zeroization.

FCS_COP.1 *Cryptographic operation*

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform *digital signature-generation*[25] in accordance with a specified cryptographic algorithm *as shown in the Digital Signature Generation Table*[26] and cryptographic key sizes *as shown in the Digital Signature Generation Table*[27] that meet the following: *standards as shown in the Digital Signature Generation Table*[28].

Signature Generation Algorithm	Key Sizes	Padding	Hash Algorithm	Applicable Standards
RSA	2048-bit to 16384-bit	RSASSA-PKCS1-v1.5 RSASSA-PSS	SHA256 SHA384 SHA512	FIPS 186-4 ANSI X9.31 PKCS #1
DSA	2048-bit to 3072-bit	Not Applicable	SHA256 SHA384 SHA512	FIPS 186-4
ECDSA	224-bit to 521-bit	Not Applicable	SHA224 SHA256 SHA384 SHA512	FIPS 186-4 ANSI X9.62

[25] [assignment: *list of cryptographic operations*]

[26] [assignment*: cryptographic algorithm*]

[27] [assignment*: cryptographic key sizes*]

[28] [assignment: *list of standards*]

Table 3: Digital Signature Generation Table

ST Application Note ST9

The TOE supports generation and use of key lengths and algorithms that meet or exceed the requirements of [ETSI] and thus ensures that signatures cannot be forged, as required by [Regulation, Annex II para 1 (c)]. Namely:

- RSA keys of up to 16384 bits; ETSI recommended minimum 2048-bits
- DSA keys up to 3072-bits; ETSI recommended minimum 2048-bits
- ECDSA keys up to 521 bits; ETSI recommended minimum 224-bits.

The TOE offers a choice of hash functions: SHA-224, SHA-256, SHA-384 and SHA-512. Hash function is selected based on the key length.

As well as meeting the ETSI recommendations, the TOE also meets the NIST guidelines for key sizes issued in NIST SP800-131A.

The implementation of these algorithms has been validated by the NIST Cryptographic Algorithm Validation Program.

The user must only use the mechanisms identified in Table 3 – this is not enforced by the TOE.

6.2.2 User data protection (FDP)

(Note that instances of FDP_ITT.1 and FDP_IFC.1 are also introduced in section 6.2.6 to define an SFP for secure communication of DTBS/R.)

FDP_ACC.1/SCD/SVD_Generation_SFP	*Subset access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/ SCD/SVD_Generation_ SFP: The TSF shall enforce the *SCD/SVD_Generation_SFP*[29] on

(1) subjects: S.User,

(2) objects: SCD, SVD,

(3) *operations: generation of SCD/SVD pair.*[30]

FDP_ACF.1/SCD/SVD_Generation_SFP	*Security attribute based access control*

Hierarchical to: No other components.

[29] [assignment: *access control SFP*]

[30] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ SCD/SVD_Generation_ SFP	The TSF shall enforce the *SCD/SVD_Generation_SFP*[31] to objects based on the following: *the user S.User is associated with the security attribute "SCD / SVD Management"*[32].
FDP_ACF.1.2/ SCD/SVD_Generation_ SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *S.User with the security attribute "SCD / SVD Management" set to "authorised" is allowed to generate SCD/SVD pair*[33].
FDP_ACF.1.3/ SCD/SVD_Generation_ SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[34].
FDP_ACF.1.4/ SCD/SVD_Generation_ SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *S.User with the security attribute "SCD / SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair*[35].

ST Application Note ST10

The TOE allows all S.Users to generate SCD/SVD pairs, and so the security attribute "SCD / SVD Management" is implicitly set to "authorised" for all S.Users. Allocation of an SCD/SVD pair to a specific S.User (e.g. to limit the use of the SCD to the legitimate user) is achieved by protecting the SCD/SVD pair under a card allocated to the relevant S.User.

FDP_ACC.1/SVD_Transfer_SFP *Subset access control*

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control

[31] [assignment: *access control SFP*]

[32] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

[33] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[34] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

[35] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

FDP_ACC.1.1/ SVD_Transfer_SFP	The TSF shall enforce the *SVD_Transfer_SFP*[36] on *(1) subjects: S.User,* *(2) objects: SVD* *(3) operations: export*[37].

FDP_ACF.1/SVD_Transfer_SFP	*Security attribute based access control*
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/ SVD_Transfer_SFP	The TSF shall enforce the *SVD_Transfer_SFP*[38] to objects based on the following: *(1) the S.User is associated with the security attribute Role,* *(2) the SVD*[39].
FDP_ACF.1.2/ SVD_Transfer_SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *R.Sigy or R.Admin is allowed to export SVD*[40].
FDP_ACF.1.3/ SVD_Transfer_SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[41].
FDP_ACF.1.4/ SVD_Transfer_SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[42].

ST Application Note ST11

The TOE allows all S.Users to export SVD, and all R.Sigy and R.Admin are allowed to export SVD. OE.SVD_Auth and OE.CGA_QCert are relied upon to ensure the integrity and authenticity of the SVD, and its correspondence to the SCD.

---

[36] [assignment: *access control SFP*]

[37] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

[38] [assignment: *access control SFP*]

[39] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

[40] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[41] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

[42] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

FDP_ACC.1/Signature-creation_SFP	*Subset access control*

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1/ Signature-creation_SFP: The TSF shall enforce the *Signature-creation_SFP*[43] on

(1) subjects: S.User,

(2) objects: DTBS/R, SCD,

(3) *operations: signature-creation*[44].

FDP_ACF.1/Signature-creation_SFP	*Security attribute based access control*

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/ Signature-creation_SFP: The TSF shall enforce the *Signature-creation_SFP*[45] to objects based on the following:

(1) the user S.User is associated with the security attribute "Role" and

(2) *the SCD with the security attribute "SCD Operational"*[46].

FDP_ACF.1.2/ Signature-creation_SFP: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

R.Sigy is allowed to create digital signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes"[47].

FDP_ACF.1.3/ Signature-creation_SFP: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[48].

---

[43] [assignment: *access control SFP*]

[44] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

[45] [assignment: *access control SFP*]

[46] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

[47] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[48] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

FDP_ACF.1.4/ Signature-creation_SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *S.User is not allowed to create digital signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no"*[49]. *The TSF shall deny access of subject to objects created for another subject.*

ST Application Note ST12

The security attribute "SCD Operational" is interpreted as follows. It is considered set to "Yes" when the Signatory is authenticated by possession of an OCS quorum or the corresponding Softcard and knowledge of the passphrase before SCD key generation. The SCD key is protected by the OCS / Softcard, which is under the sole control of the Signatory.

FDP_RIP.1 *Subset residual information protection*

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the *de-allocation of the resource from*[50] the following objects: *SCD*[51].

FDP_SDI.2/Persistent *Stored data integrity monitoring and action*

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

FDP_SDI.2.1/ Persistent	The TSF shall monitor user data stored in containers controlled by the TSF for *integrity error*[52] on all objects, based on the following attributes: *SCD, SVD*[53].
FDP_SDI.2.2/ Persistent	Upon detection of a data integrity error, the TSF shall *(1) prohibit the use of the altered data* (2) *inform the S.Sigy about integrity error*[54].

[49] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

[50] [selection: *allocation of the resource to, deallocation of the resource from*]

[51] [assignment: *list of objects*]

[52] [assignment: *integrity errors*]

[53] [assignment: *user data attributes*]

[54] [assignment: *action to be taken*]

SCD and SVD (where persistently stored by the TOE) are protected against integrity errors as a part of the key blob format when stored in the Security World.

6.2.3 Identification and authentication (FIA)

FIA_UID.1 *Timing of identification*

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow

(1) *Self test according to FPT_TST.1*[55]

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1 *Timing of authentication*

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1 The TSF shall allow

(1) Self test according to FPT_TST.1,

(2) *Identification of the user by means of TSF required by FIA_UID.1*[56]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_AFL.1 *Authentication failure handling*

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

[55] [assignment: *list of TSF-mediated actions*]

[56] [assignment: *list of TSF-mediated actions*]

FIA_AFL.1.1	The TSF shall detect when *1*[57] unsuccessful authentication **attempt**[58] **occur**s[59] related to *consecutive failed authentication attempts*[60].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been *met*[61], the TSF shall *enforce a 4 second delay between authentication failure and the next allowed authentication attempt*[62].

ST Application Note ST14

The authentication failures limit applies to the use of ACS cards, OCS cards and Softcards.

FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet a *configurable minimum length and complexity*[63].

ST Application Note ST15

The “secrets” referred to in this SFR are the passphrases associated with cards. The TOE checks the strength of a passphrase whenever one is generated or changed.

6.2.4 Security management (FMT)

FMT_SMR.1 *Security roles*

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FMT_SMR.1.1	The TSF shall maintain the roles *R.Admin and R.Sigy*[64].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

[57] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

[58] attempts

[59] occur

[60] [assignment: *list of authentication events*]

[61] [selection: *met, surpassed*]

[62] [assignment: *list of actions*]

[63] [assignment: *a defined quality metric*]

[64] [assignment: *the authorised identified roles*]

FMT_SMF.1 *Security management functions*

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

(1) Creation and modification of RAD,

(2) Enabling the signature-creation function,

(3) Modification of the security attribute SCD/SVD management, SCD operational,

(4) *Change the default value of the security attribute SCD Identifier*[65].

ST Application Note ST16

It is noted that SCD Identifiers are always explicitly defined when the SCD is created – there is no default value for this attribute. After creation they can be changed by an Administrator or Signatory.

FMT_MOF.1 *Management of security functions behaviour*

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions.

FMT_MOF.1.1 The TSF shall restrict the ability to *enable*[66] the functions *signature-creation function*[67] to *R.Sigy*[68].

FMT_MSA.1/Admin *Management of security attributes*

Hierarchical to: No other components.

[65] [assignment: *list of management functions to be provided by the TSF*]

[66] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

[67] [assignment: *list of functions*]

[68] [assignment: *the authorised identified roles*]

Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1/Admin	The TSF shall enforce the *SCD/SVD_Generation_SFP*[69] to restrict the ability to *modify*[70] the security attributes *SCD / SVD management*[71] to *R.Admin*[72].

ST Application Note ST17

As noted for FDP_ACF.1/SCD/SVD_Generation_SFP, the TOE allows all S.Users to generate SCD/SVD pairs, and so the security attribute "SCD / SVD Management" is implicitly set to "authorised" for all S.Users and modification of the attribute is therefore not available to any user.

FMT_MSA.1/Signatory	*Management of security attributes*

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1/ Signatory	The TSF shall enforce the *Signature-creation_SFP*[73] to restrict the ability to *modify*[74] the security attributes *SCD operational*[75] to *R.Sigy*[76].

ST Application Note ST18

Refer to ST Application Note ST12

[69] [assignment: *access control SFP(s), information flow control SFP(s)*]

[70] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

[71] [assignment: *list of security attributes*]

[72] [assignment: *the authorised identified roles*]

[73] [assignment: *access control SFP(s), information flow control SFP(s)*]

[74] [selection: *change_default, query, modify, delete, [assignment: other operations]*]

[75] [assignment: *list of security attributes*]

[76] [assignment: *the authorised identified roles*]

FMT_MSA.2 *Secure security attributes*

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for *SCD / SVD Management and SCD operational*[77].

ST Application Note ST19

The TOE supports generation of SCD/SVD pairs during the operational use stage of the SSCD lifecycle, and the security attribute SCD / SVD Management always takes the implicit value “yes” for each S.Sigy and S.Admin.

FMT_MSA.3 *Static attribute initialisation*

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the *SCD/SVD_Generation_SFP, SVD_Transfer_SFP and Signature-creation_SFP*[78] to provide *restrictive*[79] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *R.Admin*[80] to specify alternative initial values to override the default values when an object or information is created.

ST Application Note ST20

The defaults are as follows:

- Role: users are always explicitly allocated a role according to the situation in which they are required to authenticate, hence no default value applies
- SCD/SVD Management: always set to “authorised” because all Administrators and Signatories can create new SCD/SVD pairs

[77] [assignment: *list of security attributes*]

[78] [assignment: *access control SFP, information flow control SFP*]

[79] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

[80] [assignment: *the authorised identified roles*]

- SCD operational: as noted for FMT_MSA.4 below, S.Admin can never create an SCD/SVD pair without authentication of the relevant S.Sigy, and therefore this attribute is always “yes”.

FMT_MSA.4 *Security attribute value inheritance*

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes:

(1) If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute “SCD operational of the SCD” shall be set to “no” as a single operation.

(2) *If S.Sigy successfully generates an SCD/SVD pair the security attribute “SCD operational of the SCD” shall be set to “yes” as a single operation.*[81]

ST Application Note ST21

The TOE enforces (1) and (2) by always requiring the Signatory authentication during the key generation process. When an SCD/SVD key pair is generated, it is assigned to a Signatory by encrypting it into a key blob under its logical token. The logical token is loaded into the TOE only after successful authentication of the Signatory by possession of an OCS quorum or Softcard and knowledge of the associated passphrase.

FMT_MTD.1/Signatory *Management of TSF data*

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/ Signatory The TSF shall restrict the ability to *modify*[82] the *RAD*[83] to *R.Sigy*[84].

[81] [assignment: *rules for setting the values of security attributes*]

[82] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]

[83] [assignment: *list of TSF data*]

[84] [assignment: *the authorised identified roles*]

6.2.5 Protection of the TSF (FPT)

FPT_FLS.1 *Failure with preservation of secure state*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

(1) *self-test according to FPT_TST fails*[85].

FPT_PHP.1 *Passive detection of physical attack*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

ST Application Note ST22

The components in the PCIe module are protected by an epoxy resin coating which provides a visual indication of tamper attempts. This requires regular visual inspection of the TOE for signs of tamper (OE.Inspect), at a frequency determined by the risk assessment of the specific operational environment.

FPT_PHP.3 *Resistance to physical attack*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist *application of values outside the specified operating conditions of the voltage supply and temperature*[86] to the *PCIe module*[87] by responding automatically such that the SFRs are always enforced.

[85] [assignment: *list of types of failures in the TSF*]

[86] [assignment: *physical tampering scenarios*]

[87] [assignment: *list of TSF devices/elements*]

FPT_TST.1 *TSF testing*

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self-tests *during initial start-up, and at the request of the authorised user*[88] to demonstrate the correct operation of *the TSF*[89].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *TSF data*[90].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of *TSF*[91].

6.2.6 DTBS/R Secure Channel (FDP)

FDP_ITT.1 *Basic internal transfer protection*

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ITT.1.1 The TSF shall enforce the *DTBS/R Integrity SFP*[92] to prevent the *modification*[93] of user data when it is transmitted between physically-separated parts of the TOE.

ST Application Note ST23

Protection of the DTBS and DTBS/R by the TOE applies only to the use of an impath between a Client PC and an nShield Connect+ - see section 2.2.3.5 . This SFR is automatically satisfied by the nShield Solo, as both instances of the hardservers are located in the same physical machine.

[88] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]*]

[89] [selection: *[assignment: parts of TSF], the TSF*]

[90] [selection: *[assignment: parts of TSF data], TSF data*]

[91] [selection: *[assignment: parts of TSF], TSF*]

[92] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[93] [selection: *disclosure, modification, loss of use*]

FDP_IFC.1/DTBSR_Integrity_SFP *Subset information flow control*

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/DTBSR_Integrity_SFP	The TSF shall enforce the *DTBS/R Integrity SFP*[94] on *DTBS/R transmitted between physically-separated hardserver instances in the Client PC and in the HSM during Signing operations*[95].

The following Security Function Policy (SFP) DTBS/R Integrity SFP is defined for FDP_IFC.1:

Data transferred between the PC client and the nShield Connect shall not be subject to unauthorised modification.

ST Application Note ST24

Protection of the DTBS and DTBS/R by the TOE applies only to the use of an impath between a Client PC and an nShield Connect+ - see section 2.2.3.5 . This SFR is automatically satisfied by the nShield Solo, as both instances of the hardservers are located in the same physical machine.

6.2.7 TOE Access (FTA)

FTA_LSA.1 Limitation on scope of selectable attributes

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_LSA.1.1	The TSF shall restrict the scope of the session security attributes *KeyID*[96], based on *IPC session*[97].

FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

[94] [assignment: *information flow control SFP*]

[95] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]

[96] [assignment: *session security attributes*]

[97] [assignment: *attributes*]

FTA_SSL.4.1	The TSF shall allow user-initiated termination of the user's own interactive session.

6.3 Security Assurance Requirements

The security assurance requirements are drawn from [CC3] and represent EAL4, with the addition of AVA_VAN.5. The assurance components are identified in the table below (with augmentations in bold).

Assurance Class	Assurance Components
Security Target (ASE)	ST introduction (ASE_INT.1)
	Conformance claims (ASE_CCL.1)
	Security problem definition (ASE_SPD.1)
	Security objectives (ASE_OBJ.2)
	Extended components definition (ASE_ECD.1)
	Derived security requirements (ASE_REQ.2)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Security architecture description (ADV_ARC.1)
	Complete functional specification (ADV_FSP.4)
	Basic modular design (ADV_TDS.3)
	Implementation representation of the TSF (ADV_IMP.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	Production support, acceptance procedures and automation (ALC_CMC.4)
	Problem tracking CM coverage (ALC_CMS.4)
	Delivery procedures (ALC_DEL.1)
	Identification of security measures (ALC_DVS.1)
	Developer defined life-cycle model (ALC_LCD.1)
	Well-defined development tools (ALC_TAT.1)
Tests (ATE)	Functional testing (ATE_FUN.1)
	Analysis of coverage (ATE_COV.2)
	Testing: basic design (ATE_DPT.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment (AVA)	**Advanced methodical vulnerability analysis (AVA_VAN.5)**

Table 4: Security Assurance Requirements

The underlying assurance level for this ST is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this ST is just such a product.

The underlying EAL4 assurance level is augmented by AVA_VAN.5 (Advanced methodical vulnerability analysis).

The TOE is intended to function in a variety of signature creation systems for qualified electronic signatures. Due to the nature of its intended application, the use of the TOE may not be directly under the control of administrators specifically trained and dedicated to the 'digital signatures' application domain. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. The component AVA_VAN.5 has the following dependencies:

- ADV_ARC.1 Architectural Design with domain separation and non-bypassability
- ADV_FSP.4 Complete functional specification
- ADV_TDS.3 Basic modular design
- ADV_IMP.1 Implementation representation of the TSF
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ATE_DPT.1 Testing: basic design.

All of these dependencies are met or exceeded in the EAL4 assurance package.

6.4 Security Requirements Rationale

6.4.1 Security Objectives Rationale

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.Inspect	OE.Env	OE.REnv
T.SCD_Divulg					x															
T.SCD_Derive		x				x														
T.Hack_Phys					x				x	x								x	x	

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.Tamper_ID	OT.Tamper_Resistance	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.Inspect	OE.Env	OE.REnv
T.SVD_Forgery				x								x								
T.SigF_Misuse	x						x	x						x	x	x	x			
T.DTBS_Forgery								x							x	x				
T.Sig_Forgery			x			x					x									
P.CSP_QCert	x			x							x									
P.QSign						x	x				x				x					
P.Sigy_SSCD	x	x	x		x	x	x	x		x			x					x		
P.Sig_Non-Repud	x		x	x	x	x	x	x	x	x	x	x	x		x	x	x	x		
A.CGA											x	x								
A.SCA															x					
A.Env																		x	x	
A.REnv																				x

Table 5: Security Problem Definition mapping to Security Objectives

T.SCD_Divulg (Storing, copying, and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in [Regulation, Annex II para 1 (a)]. This threat is countered by OT.SCD_Secrecy, which assures the secrecy of the SCD used for signature creation.

T.SCD_Derive (Derive the signature-creation data) deals with attacks on the SCD via publicly known data produced by the TOE, i.e. the SVD and the signatures created with the SCD. OT.SCD/SVD_Gen counters this threat by implementing cryptographic secure generation of the SCD/SVD pair. OT.Sig_Secure ensures cryptographic secure digital signatures.

T.Hack_Phys (Physical attacks through the TOE interfaces) deals with physical attacks exploiting physical vulnerabilities of the TOE. OT.SCD_Secrecy preserves the secrecy of the SCD. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and resisting tampering attacks on the nShield Solo+ F3 PCIe unit. OE.Inspect supports the detection and prevention (by deterrence) of tampering by requiring regular physical inspections of the TOE (for signs of damage to the epoxy resin coating, or modifications to the connection of the module to the PC). Finally, the protected environment in which the TOE is located (OE.Env) limits the exposure to physical attacks.

T.SVD_Forgery (Forgery of the signature-verification data) deals with the forgery of the SVD exported by the TOE to the CGA to generation a certificate. T.SVD_Forgery is addressed by OT.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to the CGA.

T.SigF_Misuse (Misuse of the signature-creation function of the TOE) addresses the threat of misuse of the TOE signature-creation function by users other than the Signatory to create a digital signature on data for which the Signatory has not expressed the intent to sign, as required by paragraph 1(d) of [Regulation, Annex II]. OT.Lifecycle_Security requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the Signatory. OT.Sigy_SigF ensures that the TOE provides the signature-generation function for the legitimate Signatory only. OE.DTBS_Intend ensures that the SCA sends the DTBS/R only for data the Signatory intends to sign and OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. OT.DTBS_Integrity_TOE prevents the DTBS/R from alteration when sent between physically separate parts of the TOE. If the SCA provides a human interface for user authentication, OE.HID_VAD provides confidentiality and integrity of the VAD as needed by the authentication method employed. OE.Signatory ensures that the VAD is kept confidential by the Signatory.

T.DTBS_Forgery (Forgery of the DTBS/R) addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function, such that the data does not represent the DTBS as presented to the Signatory and for which the signature has expressed its intent to sign. The operational environment addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which ensures that a trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the Signatory intends to sign in a form appropriate for signing by the TOE, and by means of OE.DTBS_Protect, which ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by ensuring the integrity of the DTBS/R when sent between physically separate parts of the TOE.

T.Sig_Forgery (Forgery of the digital signature) deals with non-detectable forgery of the digital signature. OT.Sig_Secure, OT.SCD_Unique and OE.CGA_QCert address this threat in general. OT.Sig_Secure ensures, by means of robust cryptographic techniques, that the signed data and the digital signature are securely linked together. OT.SCD_Unique ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision on a forged signature.

P.CSP_QCert (CSP generates qualified certificates) establishes that the CSP generates qualified certificates or non-qualified certificates linking the Signatory and the SVD implemented in the SSCD under sole control of this Signatory. P.CSP_QCert is addressed by

- the TOE security objective OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,

- the TOE security objective OT.SCD_SVD_Corresp, which requires the TOE to ensure the correspondence between the SVD and the SCD during their generation, and

- the security objective for the operational environment OE.CGA_QCert for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the Signatory.

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy_SigF ensures the Signatory's sole control of the SCD by requiring the TOE to provide the signature generation function for the legitimate Signatory only and to protect the SCD against the use of others. OT.Sig_Secure ensures that the TOE generates digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA_QCert addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature. The OE.DTBS_Intend ensures that the SCA provides only those DTBS to the TOE, which the Signatory intends to sign.

P.Sigy_SSCD (TOE as secure signature-creation device) requires the TOE to meet [Regulation, Annex II]. This is ensured as follows:

- OT.SCD_Unique meets paragraph 1(b) of [Regulation, Annex II], with the objective that the SCD used for signature generation can practically occur only once;

- OT.SCD_Unique, OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(a) of [Regulation, Annex II] with the objectives to ensure secrecy of the SCD. OT.Tamper_Resistance defines objectives to ensure secrecy of the SCD against physical attacks. OE.Inspect supports the detection and prevention (by deterrence) of tampering by requiring regular physical inspections of the TOE (for signs of damage to the epoxy resin coating, or modifications to the connection of the module to the PC)

- OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(c) of [Regulation, Annex II] with the objectives to ensure that the SCD cannot be derived from SVD, the digital signatures or any other data exported outside the TOE

- OT.Sigy_SigF meets the requirement in paragraph 1(d) of [Regulation, Annex II] with the objectives to ensure that the TOE provides the signature generation function for the legitimate Signatory only and protects the SCD against the use of others;

- OT.DTBS_Integrity_TOE meets the requirements in paragraph 2 of [Regulation, Annex II] with the objective that the TOE must not alter the DTBS/R[98].

[98] Paragraph 2 of [Regulation, Annex II] requires that "Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing." The TOE has no influence over whether data is presented to the signatory prior to the signature process as in the second part of this requirement. Regarding the first part of the requirement, the TOE does not itself alter the DTBS/R, and ensures the integrity of the DTBS/R when it is transmitted between a client PC and an nShield Connect+ (see section 2.2.3.5).

Paragraph 2 of [Regulation, Annex II], requires that a SSCD does not prevent the data to be signed from being presented to the Signatory prior to the signature process, and is obviously fulfilled by the method of TOE usage: the SCA will present the DTBS to the Signatory and send it to the SSCD for signing.

The usage of an SCD under sole control of the Signatory is ensured by

- OT.Lifecycle_Security requiring the TOE to detect flaws during the initialisation, personalisation and operational usage
- OT.SCD/SVD_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only
- OT.Sigy_SigF, which requires the TOE to provide the signature generation function for the legitimate Signatory only and to protect the SCD against the use of others.

OE.SSCD_Prov_Service ensures that the Signatory obtains access to a TOE sample as an authentic, initialised and personalised SSCD from a SSCD provisioning service.

P.Sig_Non-Repud (Non-repudiation of signatures) deals with the repudiation of signed data by the Signatory, even though the electronic signature is successfully verified with the SVD contained in his certificate, and the certificate is valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensure the aspects of a Signatory's sole control over, and responsibility for, the digital signatures generated with the TOE. OE.SSCD_Prov_Service ensures that the Signatory uses an authentic TOE, initialised and personalised for the Signatory. OE.CGA_QCert ensures that the certificate allows to identify the Signatory and thus to link the SVD to the Signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure authenticity of the SVD being exported by the TOE and to ensure its use under the sole control of the Signatory. OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. OT.SCD_Unique provides that the Signatory's SCD can practically occur just once.

OE.Signatory ensures that the Signatory checks that the VAD is securely transferred to his control and is always kept confidential. OT.Sigy_SigF provides that only the Signatory may use the TOE for signature creation. OE.DTBS_Intend, OE.DTBS_Protect and OT.DTBS_Integrity_TOE ensure that the TOE generates digital signatures only for a DTBS/R that the Signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may generate a valid digital signature that can be successfully verified with the corresponding SVD used for signature verification. The security objectives OT.Lifecycle_Security, OT.SCD_Secrecy, OT.Tamper_ID and OT.Tamper_Resistance protect the SCD against any compromise. OE.Inspect supports the detection and prevention (by deterrence) of tampering by requiring regular physical inspections of the TOE (for signs of damage to the epoxy resin coating, or modifications to the connection of the module to the PC).

A.CGA (Trustworthy certification-generation application) establishes the protection of the authenticity of the Signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA_QCert, which ensures the generation of qualified certificates and by OE.SVD_Auth, which ensures the protection of the integrity and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the Signatory.

A.SCA (Trustworthy signature-creation application) establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by OE.DTBS_Intend which ensures that the SCA generates the DTBS/R for the data, that has been presented to the Signatory as DTBS and which the Signatory intends to sign, in a form which is appropriate for being signed by the TOE.

A.Env (Protected operating environment) establishes that the TOE operates in a physically protected environment and that its software environment is securely maintained, and this is directly reflected in OE.Env (Protected operating environment). OE.Inspect is also related to the method of preserving physical protection, and therefore is also mapped to A.Env.

A.REnv (Protected remote deployment) establishes security requirements in the case of a deployment where the end-user is remote from the SSCD and therefore needs separate protection of the environment connecting the Remote Signatory's system and the SCA. This is addressed by OE.REnv which identifies responsibilities for the SCA and remote environment in this case.

6.4.2 Security Requirements Rationale

The mapping of TOE Security Objectives to SFRs is shown in Table 6.

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.Tamper_ID	OT.Tamper_Resistance
FCS_CKM.1	X		X	X	X					
FCS_CKM.4	X				X					
FCS_COP.1	X					X				
FDP_ACC.1/ SCD/SVD_Generation_SFP	X	X								
FDP_ACC.1/ SVD_Transfer_SFP	X									
FDP_ACC.1/Signature-creation_SFP	X						X			
FDP_ACF.1/ SCD/SVD_Generation_SFP	X	X								
FDP_ACF.1/ SVD_Transfer_SFP	X									
FDP_ACF.1/Signature-creation_SFP	X						X			
FDP_RIP.1					X		X			

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.Tamper_ID	OT.Tamper_Resistance
FDP_SDI.2/Persistent				X	X	X				
FIA_UAU.1		X					X			
FIA_UID.1		X					X			
FIA_AFL.1							X			
FIA_SOS.1							X			
FMT_MOF.1	X						X			
FMT_MSA.1/Admin	X	X								
FMT_MSA.1/Signatory	X						X			
FMT_MSA.2	X	X					X			
FMT_MSA.3	X	X					X			
FMT_MSA.4	X	X					X			
FMT_MTD.1/Signatory	X						X			
FMT_SMR.1	X						X			
FMT_SMF.1	X						X			
FPT_FLS.1					X					
FPT_PHP.1									X	
FPT_PHP.3					X					X
FPT_TST.1	X				X	X				
FDP_ITT.1							X	X		
FDP_IFC.1/ DTBSR_Integrity_SFP							X	X		
FTA_LSA.1						X	X			
FTA_SSL.4						X	X			

Table 6: Mapping of TOE Security Objectives to SFRs

OT.Lifecycle_Security (Lifecycle security) is provided by the SFR for SCD/SVD generation (FCS_CKM.1), SCD usage (FCS_COP.1) and SCD destruction (FCS_CKM.4). SCD/SVD generation is controlled by the TSF according to FDP_ACC.1/SCD/SVD_Generation_SFP and FDP_ACF.1/SCD/SVD_Generation_SFP. SVD transfer for certificate generation is controlled by the TSF according to FDP_ACC.1/SVD_Transfer_SFP and FDP_ACF.1/SVD_Transfer_SFP. SCD usage is ensured by FDP_ACC.1/Signature-

creation_SFP and FDP_ACF.1/Signature-creation_SFP, which rely on secure management according to FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/ Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Signatory, FMT_SMF.1 and FMT_SMR.1. The test function FPT_TST.1 provides failure detection throughout the lifecycle.

OT.SCD/SVD_Gen (SCD/SVD generation) ensures that generation of an SCD/SVD pair requires proper user authentication. The TSF specified by FIA_UID.1 and FIA_UAU.1 provides user identification and user authentication prior to enabling access to authorised functions. FDP_ACC.1/SCD/SVD_Generation_SFP and FDP_ACF.1/SCD/SVD_Generation_SFP provide access control for SCD/SVD generation. The security attributes of the authenticated user are provided by FMT_MSA.1/Admin, FMT_MSA.2, and FMT_MSA.3 for static attribute initialisation. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute “SCD operational” of the SCD.

OT.SCD_Unique (Uniqueness of the signature-creation data) implements the requirement of ensuring practically unique SCD as laid down in [Regulation, Annex II paragraph 1(b)], which is provided by the cryptographic algorithms specified by FCS_CKM.1.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) ensures that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so as to retain the correspondence. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by FMT_SMF.1 and by FMT_MSA.4 allow R.Admin to modify the default value of the security attribute SCD Identifier.

OT.SCD_Secrecy (Secrecy of signature-creation data) is provided cryptographic SFRs as follows. FCS_CKM.1 ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of an SCD/SVD pair prevents disclosure of the SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP_RIP.1 and FCS_CKM.4 ensure that residual SCD information is not available for unauthorised use after completion of the authorised signing session.

The security functions specified by **FDP_SDI.2/Persistent** ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational.

FPT_PHP.3 specifies additional security features of the TOE to ensure the confidentiality of the SCD.

OT.Sig_Secure (Cryptographic security of the digital signature) is provided by the cryptographic algorithms specified by FCS_COP.1, which ensures the cryptographic robustness of the signature algorithms. FDP_SDI.2/Persistent ensures the integrity of the SCD implemented by the TOE and FPT_TST.1 specifies self-tests ensuring correct signature-creation. FTA_SSL.4 and FTA_LSA.1 provide functionalities related to the session termination and scope and help in enhancing cryptographic security of the digital signature.

OT.Sigy_SigF (Signature creation function for the legitimate Signatory only) is provided by the combination of a range of SFRs as follows.

FIA_UAU.1 and FIA_UID.1 ensure that no signature generation function can be invoked before the Signatory is identified and authenticated. The security function specified by FMT_MTD.1/Signatory manages the authentication function, and FIA_AFL.1 specifies the action that restricts the ability of an attacker to apply brute force attempts to guess the passphrase. FIA_SOS.1 restricts the ability of a user to choose weak passphrases for their card. FTA_SSL.4 and FTA_LSA.1 provide functionalities related to the session termination and scope and help in assuring that signature creation function is for legitimate Signatory only.

FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature-creation process). The protection of communications between distributed parts of the TSF is covered by FDP_ITT.1 and FDP_IFC.1/DTBSR_Integrity_SFP (as discussed for OT.DTBS_Integrity_TOE).

The security functions specified by **FDP_ACC.1/Signature-creation_SFP** and **FDP_ACF.1/Signature-creation_SFP** provide access control based on the security attributes managed according to FMT_MTD.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. FMT_SMF.1 and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the Signatory. FMT_MOF.1 restricts the ability to enable the signature-creation function to the Signatory. FMT_MSA.1/Signatory restricts the ability to modify the security attribute “SCD operational” to the Signatory.

OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) ensures that the DTBS/R is not altered when it is transmitted on an impath between a Client PC and an nShield Connect+. The TOE specifies protection measures in FDP_ITT.1 (and its associated SFP in FDP_IFC.1/DTBSR_Integrity_SFP).

OT.Tamper_ID (Tamper detection) is provided by FPT_PHP.1 through passive detection of physical attacks.

OT.Tamper_Resistance (Tamper resistance) is provided by FPT_PHP.3 to resist physical attacks.

6.4.3 SFR Dependencies Rationale

Requirement	Dependencies	Fulfilled by
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1 FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 FCS_CKM.4
FDP_ACC.1/ SCD/SVD_Generation_SFP	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation_SFP
FDP_ACC.1/ Signature-creation_SFP	FDP_ACF.1	FDP_ACF.1/Signature-Creation SFP

Requirement	Dependencies	Fulfilled by
FDP_ACC.1/ SVD_Transfer_SFP	FDP_ACF.1	FDP_ACF.1/SVD_Transfer_SFP
FDP_ACF.1/ SCD/SVD_Generation_SFP	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation_SFP FMT_MSA.3
FDP_ACF.1/ Signature-creation_SFP	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signature-creation_SFP FMT_MSA.3
FDP_ACF.1/ SVD_Transfer_SFP	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/SVD_Transfer_SFP FMT_MSA.3
FDR_RIP.1	No dependencies	
FDP_SDI.2/Persistent	No dependencies	
FIA_UID.1	No dependencies	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_SOS.1	No dependencies	
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1/ Admin	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation_SFP FMT_SMR.1 FMT_SMF.1
FMT_MSA.1/ Signatory	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/Signature_Creation SFP FMT_SMR.1 FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	FDP_ACC.1/SCD/SVD_Generation_SFP, FDP_ACC.1/Signature_Creation SFP FMT_MSA.1/Admin, FMT_MSA.1/Signatory FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD/SVD_Generation_SFP, FDP_ACC.1/ Signature-creation_SFP
FMT_MTD.1/ Admin	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1

Requirement	Dependencies	Fulfilled by
FMT_MTD.1/ Signatory	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_FLS.1	No dependencies	
FPT_PHP.1	No dependencies	
FPT_PHP.3	No dependencies	
FPT_TST.1	No dependencies	
FDP_ITT.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/DTBSR_Integrity_SFP
FDP_IFC.1/ DTBSR_Integrity_SFP	FDP_IFF.1	See discussion below.
FTA_LSA.1	No dependencies	
FTA_SSL.4	No dependencies	

Table 7: Dependencies rationale for SFRs

Regarding the dependency of FDP_IFC.1/DTBSR_Integrity_SFP on FDP_IFF.1: Part 2 of the Common Criteria defines the dependency of FDP_IFC.1 (information flow control policy statement) on FDP_IFF.1 (Simple security attributes). The specification of FDP_IFF.1 would not capture the nature of the security functional requirement for the DTBS/R transmission, nor would it add any detail. As stated in the DTBS/R Integrity SFP referred to in FDP_IFC.1/DTBSR_Integrity_SFP, there are no attributes necessary (hence the transitive dependencies of FDP_IFF.1 on FMT_MSA would not add any requirements). The security functional requirement for the TOE is sufficiently described using FDP_ITT.1 and its Data Processing Policy (FDP_IFC.1).

7 TOE Summary Specification

7.1 User Roles and Authentication

7.1.1 SF.I&A – Identification and Authentication

Users are identified only in contexts where authentication is also required. In such a case the user is required to enter a smart card into the smart card reader or provide a passphrase for a Softcard, and the user is then identified by the combination of the identifier of their card and the identifier of the Share held on the card.

The TOE authenticates users in one of the following ways:

- A user authenticates as an Administrator by inserting a quorum of the smart cards from the ACS into the smart card reader, when prompted to do so (because they are attempting to perform an Administrator action). The user is then prompted to enter the passphrase for the ACS card (via the client PC for the nShield Solo+ F3, or via the front panel for the nShield Connect+). This authentication is performed locally to the TOE (the remote use scenario does not apply to Administrator authentication).

- A user (or group of users) authenticates as a Signatory (or Signatories) by inserting a quorum of the smart cards from the OCS that protects the SCD that the user wishes to use (or for the SCD/SVD pair that the user wishes to generate) into the smart card reader. The user is then prompted to enter the passphrase for the OCS card. This authentication is performed locally to the TOE (the remote use scenario does not apply to the use of OCS cards).

- A user authenticates as a Signatory by presenting the passphrase for the Softcard that protects the SCD they wish to use. This authentication can be performed either locally or remotely.

For ACS cards, OCS cards and Softcards, a passphrase is generated when the card is created, and the TOE checks at that time (or when the passphrase is changed) that the passphrase is suitably strong.

When the entered passphrase is not valid, the TOE imposes a 4 second delay between authentication failure and the next allowed authentication attempt. The enforced delay, combined with the passphrase space, means that the time required for a brute force attack on passphrases is considered to be infeasible.

The SCD/SVD key pair generation process ensures that the Signatory is authenticated before the SCD/SVD is generated and the SCD is stored securely under the protection of the TOE and the OCS / Softcard used to authenticate the Signatory. In this way, the SCD can only be used inside the TOE by presenting the OCS or Softcard and the associated passphrase to the TOE. This ensures that the SCD is never unprotected outside the TOE and is always under the sole control of the Signatory.

This Security Function implements FIA_SOS.1, FIA_UID.1, FIA_UAU.1, FIA_AFL.1, FDP_ACC.1/Signature-creation_SFP, FDP_ACF.1/Signature-creation_SFP, and FMT_SMF.1 (enabling signature-creation).

7.1.2 SF.Roles – Support for User Roles

The TOE maintains roles in the following ways:

- Administrator Role (R.Admin): this role is defined as ACS card holders and is expected to have direct access to the TOE.

- Signatory Role (R.Sigy): this role is defined as OCS card or Softcard holders. It is expected to interact with the TOE locally or remotely through a Signature Creation Application using the APIs provided by the TOE.

The role of a user is an implicit property, and is not stored as a single attribute. It is deduced from the requirements of the operation that is to be executed: Signatory commands are available to users at the command line or to applications that have identified and authenticated; Administrator commands require that the relevant Administrator(s) must identify and authenticate by presenting their card and passphrase. A user is associated with a role simply through the completion of the relevant authentication process required by a command.

Reference authentication data for ACS cards, OCS cards and Softcards is the passphrase required to access the relevant Share. The passphrase value is not directly stored by the TSF, but is required in order to decrypt the Share information. The RAD for a card is therefore created when the card is created. A cardholder can change the passphrase on their own card(s) after first supplying the current passphrase.

This Security Function implements FMT_SMR.1, and FMT_SMF.1 (creation and modification of RAD, changing SCD Identifier).

7.1.3 SF.CardSet – Card creation and SCD protection

The TOE creates Operator Card Sets (OCS) or Softcards in order to protect SCD, and to approve certain operations. An OCS consists of a set of N cards, of which any subset of K cards (known as the 'quorum' for the card set) are required to be presented in order to approve an operation – the creator of the OCS defines the values for K and N at the time the cards are generated. Cards cannot be added to an OCS after the initial generation of the set. A Softcard is a single entity (equivalent to a 1 of 1 OCS).

An OCS is created by an Administrator or Signatory and requires the environment to implement a procedure for secure delivery of the OCS to the Signatory after the cards have been used to protect the Signatory's SCD. A Softcard is generated by the TOE in response to a request from the SCA on behalf of the Signatory that will use the card to protect their SCD. If the passphrase is not set at generation time by the Signatory, then the environment is required to implement a procedure for secure delivery of the passphrase to the Signatory. During generation of the OCS or Softcard, the Signatory sets their passphrase (VAD) on each OCS card or Softcard that they will hold. The passphrase can subsequently be changed only if the current passphrase is entered, and therefore the ability to modify the passphrase is restricted to the Signatory.

The OCS or Softcard are then used to protect SCD that are generated for use by the Signatory. The SCD/SVD pair is generated as in SF.KeyGen (section 7.2.1) and the relevant OCS or Softcard is chosen to protect the newly generated SCD. The Signatory is required to enter their OCS cards or to identify the relevant Softcard, and to enter the relevant OCS or Softcard passphrase(s) during the generation process, and the resulting SCD is then

protected under the OCS or Softcard so that it can only be accessed in future when the relevant OCS or Softcard and passphrase(s) are presented.

Following SCD/SVD generation, the SVD data may be exported by either the Administrator or the Signatory, depending on procedures in the operating environment.

Ownership and presentation of the relevant cards (OCS or Softcard) therefore represents the attribute “SCD / SVD Management”, and the creation of the cards represents the setting of this attribute to “authorised”.

The SCD/SVD key pair generation process ensures that the Signatory is authenticated before the SCD/SVD is generated and the SCD is stored securely under the protection of the TOE and the OCS / Softcard used to authenticate the Signatory. This ensures that the SCD is under the sole control of the Signatory at all times and represents the setting of the attribute “SCD Operational” to “yes”.

The use of an OCS or Softcard to approve signature creation using the SCD that it protects is described under SF.I&A (section 7.1.1).

This Security Function implements FDP_ACC.1/SCD/SVD_Generation_SFP, FDP_ACF.1/SCD/SVD_Generation_SFP, FDP_ACC.1/SVD_Transfer_SFP, FDP_ACF.1/SVD_Transfer_SFP, FDP_ACC.1/Signature-creation_SFP, FDP_ACF.1/Signature-creation_SFP, FMT_SMF.1 (modification of attributes “SCD / SVD Management” & “SCD Operational”), FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, and FMT_MTD.1/Signatory.

7.2 Key Management

7.2.1 SF.KeyGen – Key Generation

The TOE generates cryptographic keys for all operations as described in the SCD/SVD Generation Table (see section 6.2.1).

This Security Function implements FCS_CKM.1.

7.2.2 SF.KeyZer – Key Destruction

The TOE destroys plaintext cryptographic keys in RAM when they are deallocated, using zeroization following the requirements of FIPS 140-2.

This Security Function implements FCS_CKM.4 and FDP_RIP.1.

7.3 Cryptographic Services

7.3.1 SF.Crypto – Cryptographic Operations

The TOE provides the cryptographic operations described in the Digital Signature Generation Table (see section 6.2.1).

This Security Function implements FCS_COP.1.

7.4 User Data Protection

7.4.1 SF.SigDataIntegrity

The TOE securely stores the SCD/SVD in external persistent storage. The key blob, which is the format used by the TOE to securely store the keys, protects the integrity and confidentiality of the keys.

This Security Function implements FDP_SDI.2/Persistent.

7.5 TSF Protection

7.5.1 SF.Phys – Physical Protection

The components in the nShield Solo+ F3 PCIe module are protected by an epoxy resin coating which provides a visual indication of tamper attempts. The TOE is designed to resist application of voltages and temperatures outside its intended operating conditions. While within the intended operating conditions the TOE operates normally and thus enforces the security functions; if a significant deviation from the intended operating conditions occurs then this is detected by the TOE and it enters an error state in which it does not perform any cryptographic operations, it does not respond on any interfaces[99] and gives a visual indication via the LED on the module until it is restarted (which causes any unencrypted SCD held in the module to be deleted, and requires re-authentication of signatories before the SCD can be used again).

This Security Function implements FPT_PHP.1, FPT_PHP.3, and FPT_FLS.1.

7.5.2 SF.Test – Self-Test

The TOE runs a suite of self-tests during start-up that include hardware self-tests, cryptographic self-tests of the cryptographic algorithms, code integrity tests, tests of the validity of the EEPROM memory in the PCIe card (which holds permanent TSF keys), and that the EEPROM contains a valid K_{NSO} (which indicates that the PCIe card has been initialised). An Administrator can initiate these tests at any other time from the CLI.

If a self-test fails then the TOE enters a secure error state in which it does not perform any cryptographic operations, and does not respond on any interfaces.

This Security Function implements FPT_TST.1 and FPT_FLS.1.

[99] If the voltage is too low then the TOE enters the Power Off state shown in Figure 6; in other cases it enters the Error state shown in Figure 6.

7.6 Trusted Channels

7.6.1 SF.Channel

In the nShield Solo+ F3 case, a secure channel exists between the hardserver and the nShield Solo+ F3 by virtue of the secure environment in which the TOE is operated. In this case the TOE also benefits from the inter-process communication and PCIe bus in the client platform (including the error-correction features of the PCIe bus) that form part of the operational environment. In the nShield Connect+ case (as in Figure 3), the TOE implements a secure channel between the hardserver in the client PC and the hardserver in the nShield Connect+ unit by means of the proprietary secure protocol called Impath. This channel provides confidentiality and integrity protection, and in particular therefore protects the DTBS/R from unauthorised modification between these parts of the TOE. Protection of communications between the SCA and the TOE is the responsibility of the environment.

This Security Function implements FDP_ITT.1 and FDP_IFC.1/DTBSR_Integrity_SFP.

7.7 Session constraints

7.7.1 SF.Session_management

It's possible to establish constraints on the session set up between the SCA and the TOE. Those constraints are related to the possibility of terminating the session when the last smart card is removed from the card reader and also to the definition of session scope based on the value of specific attributes.

This Security Function implements FTA_LSA.1 and FTA_SSL.4.

Contact Us

Web site: https://www.ncipher.com
Help Centre: https://help.ncipher.com
Email Support: support@ncipher.com

Depending on your geographic location, you can also contact us as follows:

Americas	Asia Pacific	Europe, Middle East and Africa
nCipher Security LLC Sawgrass Corporate Center, Building A 13800 Northwest 14th Street, Suite 130 Sunrise, FL 33323 USA	**nCipher Security (Hong Kong) Limited** 9/F, V-Point 18 Tang Lung Street Causeway Bay, HONG KONG	**nCipher Security Ltd** One station Square Cambridge CB1 2GA UNITED KINGDOM
Toll Free: +1 833 425 1990 Fort Lauderdale: +1 954 953 5229	Hong Kong: +852 3461 3088 Japan: +81 50 3196 4994	United Kingdom: +44 1223 723 711

www.ncipher.com

About nCipher Security

Today's fast moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency. It also multiplies the security risks. nCipher Security, a leader in the general purpose hardware security module (HSM) market, empowers world-leading organizations by delivering trust, integrity and control to their business critical information and applications.

Our cryptographic solutions secure emerging technologies – cloud, IoT, blockchain, digital payments – and help meet new compliance mandates, using the same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensuring the integrity of your data and putting you in complete control – today, tomorrow, at all times. www.ncipher.com

Search: nCipherSecurity

TRUST. INTEGRITY. CONTROL.