nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

Remote Administration

Security Whitepaper

White Paper

VERSION: 1.2

DATE: 19 MARCH 2020

Information in this document is subject to change without notice.

nCipher UK Limited makes no warranty of any kind with regard to this information, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. nCipher UK Limited shall not be liable for errors contained herein or for incidental or consequential damages concerned with the furnishing, performance or use of this material.

Contents

Introduction

Remote Administration is an extension to nCipher's Security World concept to support remote administration and authorisation of nShield Hardware Security Modules (HSMs).

Remote Administration is supported via secure remote card presentation of both Administrator and Operator card sets. Remote card presentation changes the security profile of the existing nShield product. This paper reviews the security implications due to the changes and provides recommendations for secure configuration and operation of nShield when Remote Administration functionality is enabled.

The scope of this document only covers aspects related to the introduction of Remote Administration.

For further reading on the depolyment and configuration considerations of nShield HSMs refer to the nShield Security Manual which is provided in the standard documentation set with the nShield Security World Software ISO. The reader is assumed to be familiar with the Security World architecture including Operator and Administrator card sets, nShield Solo and nShield Connect modules, hosts and applications.

Overview of Remote Administration

A physical presence is required for the majority of operations starting with the creation of the smartcards for an Administrator Card Set (ACS). Traditional Security Worlds must be created from the front panel (of an nShield Connect) or via the attached smart card reader for an embedded nShield Solo HSM. Subsequent operations require an ACS quorum to be present at the nShield Solo Card Reader or nShield Connect front panel for example when enrolling modules into a Security World and firmware upgrades. Similarly, operations requiring an Operator Card Set (OCS) require card holders to be present at the nShield HSM.

It is well understood that card holder quorums gathering in a data centre often geographically distant from their office to carry out card holder duties is expensive and inconvenient.

Remote Administration provides the capability for Administrators and Operators to present their cards remotely, thereby removing the need for being physically present at the nShield HSM. This is achieved by extending the existing Security World architecture to support a secure channel to a remote application running on a smartcard. Remote Administration enables:

- card holders to present smart cards to an HSM that is in a different location (e.g. the card holder may be in an office, while the HSM is in a datacenter)
- all smart card operations to be carried out in a different location from the HSM (apart from loading CodeSafe/SEE restricted feature certificates)
- remote creation of a Security World and associated Administrator Card Sets and Operator Cards Sets including non-persistent Operator Cards Sets
- Security World programs and utilities to be run remotely, when used in combination with a standard remote access solution
- full remote administration of Security Worlds and their HSMs including:
    - Remote mode change
    - Remote firmware upgrade of nShield Connect and nShield Solo firmware (after upgrade to v12.00)[1]
    - Module status (SOS) reporting
    - nShield Connect reboot
    - nShield Connect front panel lock out
- administration of HSMs deployed in the cloud via nShield as a Service

An overview of the system architecture for Remote Administration is shown on Figure 1 Remote Administration Architecture.

[1] Remote Administration is not required to carry out a remote firmware upgrade of an HSM however it is required (to remotely present an ACS quorum) to reload a Security World once the firmware upgrade is complete

REMOTE WORKSTATION

Prior to the introduction of Remote Administration, Administrators were able to perform limited HSM administration operations using their preferred remote access solution (e.g. Secure Shell (SSH), Remote Desktop etc). Key based operations required multi-factor authorisation via presentation of a card set quorum at the nShield HSM (see Figure 1 Remote Administration Architecture).

Note: Each card contains a fragment of a logical token. The nShield HSM reconstitutes the fragments to recreate a complete token which in turn grants access to a key.

Remote Administration requires Administrators to use their remote access solution to perform these administration operations and extends the operations that can be performed in this way. With Remote Administration, it is now possible to present a smartcard in a remote work station or laptop rather than locally at the nShield HSM. Remote Administration creates a separate secure connection from the Remote Administration smart card to the nShield HSM enabling remote card presentation.

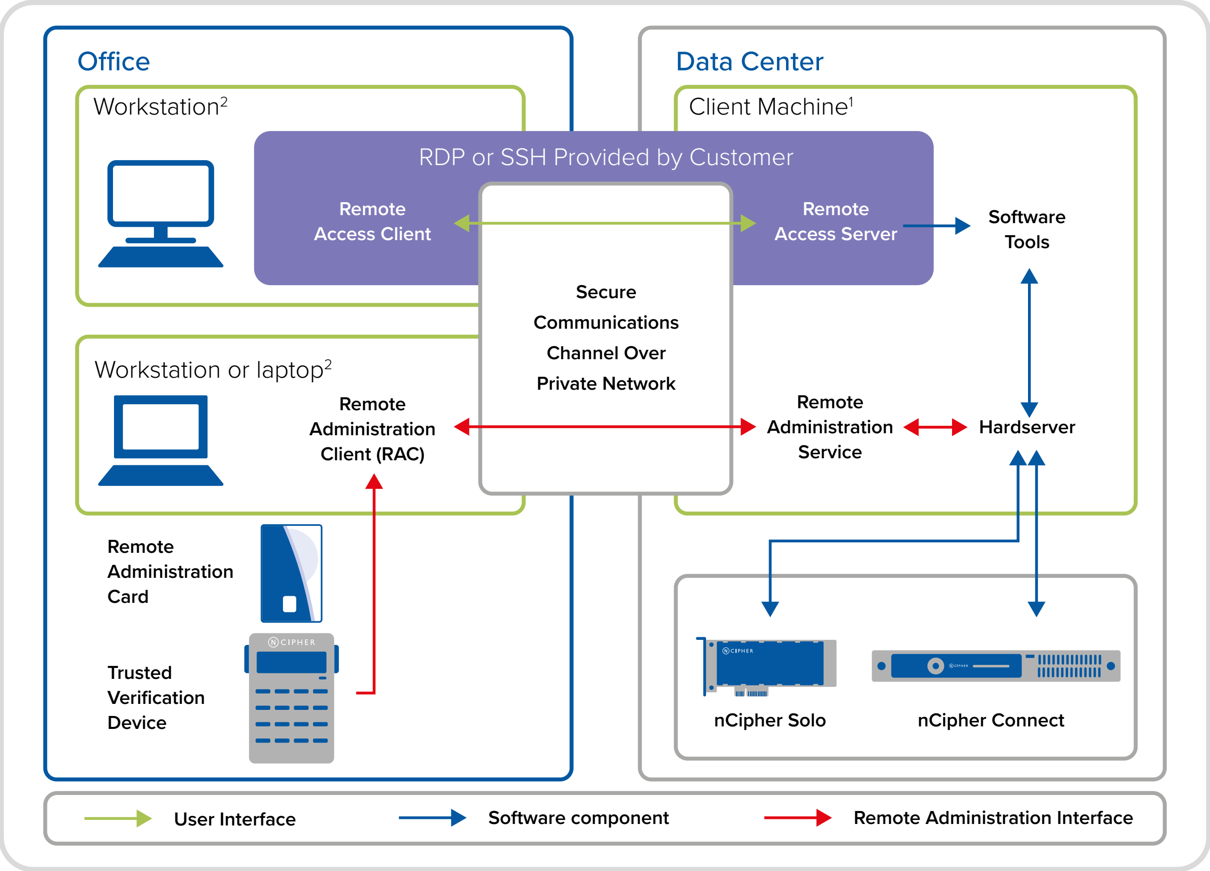
Office
Workstation2
RDP or SSH Provided by Customer
Remote Access Client
Remote Access Server
Software Tools
Secure Communications Channel Over Private Network
Workstation or laptop2
Remote Administration Client (RAC)
Remote Administration Service
Hardserver
Data Center
Client Machine1
Remote Administration Card
Trusted Verification Device
nCipher Solo
nCipher Connect
User Interface
Software component
Remote Administration Interface

Figure 1. Remote Administration Architecture

Note 1: The Remote Administration Service should be installed on a client machine of the HSMs in your Security World that you can make accessible to Remote Administration Clients. This can be on an existing RFS if it is configured as a client or another client of the HSMs.

Note 2: Note that it is possible to co-locate the Remote Access Client and Remote Administration Client (RAC) on the same workstation. In this case more stringent measures must be observed to maintain a sanitized environment, see section Client Workstation in the Deployment section.

[1] Fragmentation and reconstruction are based on the (k,n) threshold scheme as described by Shamir [13].

REMOTE ADMINISTRATION CLIENT AND SERVICE

Remote Administration smartcards require additional infrastructure to communicate with the nShield HSM. A Remote Administration Client running on the laptop or workstation, located remote from the HSM, is required to connect to a Remote Administration Service (RAS) (in the Data Center) over a standard TCP/IP connection.

REMOTE ADMINISTRATION CLIENT

The Remote Administration Client (RAC) is a non-security enforcing element that provides a bridge between the Remote Administration smart card and the back end RAS. Its function is to:

- Provide the user with a means to select the RAS they wish to connect to.
- Manage the link between the client and the selected RAS.
- Display a list of the nShield HSMs (by Electronic Serial Number, ESN) that can be connected to via the RAS.
- Permit the user to select a destination nShield HSM and manage the flow of messages between the HSM and the Remote Administration smart card.

REMOTE ADMINISTRATION SERVICE

The Remote Administration Service (RAS) is a non-security enforcing element that provides a bridge between the RAC and the back end nShield HSMs (via the hardserver). Its function is to:

- Manage connections from multiple RACs.
- Supply a list of available nShield HSMs to the connected RAC.
- Negotiate a remote slot connection to an nShield HSM via the hardserver and route messages between the RAC and destination HSM.

The RAS participates as a standard nShield client that can communicate with a hardserver over a network connection.

SMARTCARDS

Standard nCipher data smart cards which ship by default with nShield HSMs are not compatible with remote administration and must be replaced by new Remote Administration smart cards.

The Remote Administration smart cards function is to:

- Provide storage and retrieval of logical token fragments, similar to the standard nCipher data smart cards.
- Provide security mechanisms to ensure authentication and confidentiality of data transferred between itself and the nShield HSM.

The Remote Administration smart cards are FIPS 140-2 Level 3 certified supporting execution of an applet developed by nCipher.

TRUSTED VERIFICATION DEVICE

A trusted smart card reader, the nShield Trusted Verification Device (TVD), is required to prevent malware on the client machine from tampering with the selection of nShield HSM, ESN, prior to the card and HSM performing mutual authentication.

Security Properties

MULTI-FACTOR AUTHORISATION

Secret-sharing enables key fragments to be stored separately on smartcards so that `k of n' key fragments (a quorum) are required in order to load or reconstitute the key being protected [Ref 1]. This security concept is maintained with the Remote Administration feature. Attackers wishing to exploit the remote capability must therefore be capable of compromising a complete quorum to subvert access to important security-world keys.

WARRANTS

Public key certificates known as Warrants are used to authenticate the identity of cards and modules. The primary components of this public key infrastructure are given in Table 1: Warrant Keys and Parameters.

NSHIELD HSM WARRANTING

During production of nShield HSMs an elliptic curve key pair is generated within the HSM. The HSM stores the private part in secure long-term memory, and sends the public part to the nCipher warranting system. The warranting system then signs a certificate binding that public key to the HSM's serial number.

REMOTE ADMINISTRATION SMART CARD WARRANTING

A similar process to HSM warranting is followed for the Remote Administration smart cards. Signing is performed using an elliptic curve key that is itself certified by a nCipher-owned root warranting key. The warrant thus comprises a certificate chain, signed by nCipher, guaranteeing the authenticity of a key held by any card bearing the given serial number and with the given internal long-term key ($\mathbf{K}_{C\text{-}LF}$). The warranting system uses elliptic curve cryptography based on a NIST P-521 curve and signatures are ECDSA with SHA-512 hashing.

The warranting process takes place in a secure nCipher environment using nShield HSMs, with stringent auditing nCipher production environment controls surrounding use of the warranting keys.

Table 1. Warrant Keys and Parameters

Warrant Key	Parameter
$K_{W\text{-}M}$	nCipher root warranting key for modules
$K_{W\text{-}C}$	nCipher root warranting key for cards
$K_{M\text{-}LF}$	Module's internal long-term fixed (warranted) key
$K_{C\text{-}LF}$	Card's internal long-term fixed (warranted) key
ESN_{M}	nShield Module's serial number
S_{C}	Card's serial number
W_{M}	nShield Module's warrant
W_{C}	Card's warrant

The nCipher Remote Administration smart card production process writes the warrant to the card's non-volatile memory and guarantees that $\mathbf{K}_{C\text{-}LF}$ belongs to the given $\mathbf{S}_{C}$. Therefore verifying $\mathbf{S}_{C}$ would be sufficient to identify the card.

Once a card leaves production it cannot be re-warranted since the private key used to load applets onto the card is randomised immediately after loading applets during production.

The process ensures that the serial number written to a card during nCipher production is unique to the card.

SECURE CHANNEL

Remote administration of nCipher nShield HSMs requires a secure channel to be set up between an nShield HSM and a Remote Administration card, over an untrusted network. Both the nShield HSM and the Remote Administration card are cryptographically warranted during production, and it is these warrants, or trust anchors that are used to validate the identities of the card and module. The secure channel provides confidentiality, data origin authentication, message order integrity, forward secrecy, and freshness guarantees, for the protection of arbitrary data sent between the Remote Administration smart card and the nShield HSM.

The strength of the warrants allows for signature strengths of 256 bits. This level is retained throughout the protocol.

NOTATION

Notation for the various keys, messages etc. is introduced and explained in the text below. For any asymmetric private key **k**, its public part is denoted by **k'**. Signature of a message **m** by a key **k** is denoted **[m]k**, and encryption of **m** with **k** is denoted **{m}k**. Concatenation of messages **a** and **b** is written **a**||**b**, where it is assumed that **a** and **b** can be unambiguously recovered from **a**||**b**.

Table 2. Key Agreement Parameters

Warrant Key	Parameter
$K_{M\text{-}KA}$	nShield Module's ephemeral key-agreement key
$K_{C\text{-}KA}$	Remote Administration Card's ephemeral key-agreement key
Z	x co-ordinate of the ECDH derived point
V	List of protocol version numbers proposed by card
V_I	Protocol version number selected by module

PROTOCOL

The protocol consists of four phases: version negotiation; key agreement; key derivation; and the secure channel itself.

In the version negotiation phase the Remote Administration card, C, proposes a list of all of the versions it is willing to use, in preference order and the nShield module, M, responds with its selection from the list (or refuses the negotiation). The Remote Administration card then verifies that this selection is a member of the original list. Key-agreement uses a Diffie-Hellman exchange to establish a single shared secret, Z;

1. $M \rightarrow C : ESN_M \,||\, K'_{M\text{-}KA}$
2. $C \rightarrow M : S_C \,||\, K'_{C\text{-}KA} || X_C$
3. $X_C = [vi \,||\, v \,|| ESN_M \,||\, S_C \,||\, K'_{M\text{-}KA} \,||\, K'_{C\text{-}KA}]K_{C\text{-}LF}$
4. $M \rightarrow C : X_M$
5. $X_M = [vi \,||\, v \,||\, ESN_M \,||\, S_C \,||\, K'_{M\text{-}KA} \,||\, K'_{C\text{-}KA}]K_{M\text{-}LF}$
   C derives Z from $K_{C\text{-}KA}$ and $K'_{M\text{-}KA}$ and M derives *Z* from $K_{M\text{-}KA}$ and $K'_{C\text{-}KA}$
   Key-derivation establishes an AES-256 master key K from *Z*
6. K = SHA256(Z)

Four symmetric AES-256 session keys are derived using the NIST SP800-108 KDF based on CMAC in counter mode [Ref 12] to perform session based encryption and authentication in both directions. In equation 7, K_E and K_A are the encryption and authentication session keys, Mp is a padded message, IV is a random initialisation vector and T is a monotonic counter.

7. $\{T \,||\, Mp\}KE \,||\, IV \,||\, CM\ AC\ (IV \,||\, \{T \,||\, Mp\}_{KE})_{KA}$

CONFIDENTIALITY

All sensitive data are passed over the secure channel encrypted by keys derived from ephemeral keys. No sensitive data or keys are exchanged in the key-agreement phase. The use of encrypt-then-MAC ensures that there is no padding-oracle attack. The encrypt-then-mac composition is preferred since it supports confidentiality, non-malleability and integrity [Ref 9].

INTEGRITY

Any accidental or malicious modification to a message in transit will result in rejection of the message. In particular, if any message sent over the secure channel is corrupted, then the MAC validation at the receiving end will fail.

MUTUAL ENTITY AUTHENTICATION

Mutual entity authentication means that, in the current session:

- The Remote Administration card is assured that it is talking to a nCipher-warranted nShield module with the Module Electronic Serial Number, ESN that the user has confirmed.
- The nShield module is assured that it is talking to a nCipher-warranted Remote Administration smartcard with a Card Serial Number, $\mathbf{S_C}$ that appears in its Authorized Card List aka whitelist.

FORWARD SECRECY

Since the keys used to secure the communications are derived from ephemeral keys:

- Any compromise of the session keys would have no bearing on any past or future sessions.
- Compromise of $\mathbf{K_{M\text{-}LF}}$ or $\mathbf{K_{C\text{-}LF}}$ would break the security of any future sessions, but would not allow an attacker to decrypt any previous sessions from their transcripts.

FRESHNESS

Use of monotonic counters in each direction protects against replay or reordering of messages. Note that the secure channel provides inherent resistance to reflection attacks because the encryption and authentication keys are directional.

SIDE-CHANNEL RESISTANCE

Special attention is applied to implement countermeasures to side channel attacks:

- Use of ephemeral session keys that have a limit on the number of operations and time makes side channel attacks more difficult or impracticable.
- On the Remote Administration card special attention is paid to implementation of software countermeasures to fault induced attacks. The crypto library on the card has proven side channel countermeasures and the circuitry in the cards have sensors to detect attacks.

PERSISTENCE

A proprietary active and cryptographically assured mechanism is used to determine card presence.

NSHIELD TRUSTED VERIFICATION DEVICE

When setting up the secure channel between the Remote Administration card and nShield HSM module it is necessary for the user to confirm to the Remote Administration card the identity of the intended $\mathbf{ESN_M}$. In order to achieve this in a secure manner, we employ a Trusted Verification Device (TVD), instead of a standard card reader, stationed between the user's PC and the Remote Administration card. The TVD provides the essential properties of secure key entry and a secure display.

By using the TVD keypad, the Remote Administration card can be sure that the user confirmed the contents of a particular message that are securely displayed on the TVD screen.

Note: This property is achieved by using a TVD that complies with the Secoder standard. When the TVD is placed in a certain mode, messages from the keypad are prefixed with an identifier string before being forwarded to the card, while any messages coming from elsewhere having this identifier string are blocked.

The TVD prevents a compromised user PC from hijacking the key-agreement protocol and tricking the user into connecting to a module other than the one intended. In order to read any data from the secure channel the attacker must be able to read $\mathbf{K_{M\text{-}LF}}$ from a genuine module in their possession (or otherwise access the module's volatile memory during channel set-up). If the attackers can read the modules long term fixed key and then divert communications for a quorum of ACS cardholders, they can recover important security-world keys.

Correct use of the TVD protects against the re-direct attack.

AUTHORIZED CARD LIST

A Remote Administration card Authorized Card List is used to control card access to the nShield HSM as a defence-in-depth measure. The purpose of the whitelist is twofold:

- When administrator cards are first enrolled (when a Security World is first created or an Administrator Card Set is replaced), the whitelist prevents an attacker with another nCipher-issued card from masquerading as a legitimate cardholder and obtaining a share of the master secret.
- If a Remote Administration card is lost or stolen, its serial number can be removed from the whitelist, preventing the card or its credentials from being used by an attacker.

Assurance Activities

SECURE DEVELOPMENT LIFECYCLE

Remote Administration has been developed following an Agile methodology that has been tailored to incorporate best practise security activities from project outset.

Threat modelling is carried out at product feature and sprint backlog level so that security is always a consideration at the planning stage. Mitigations are defined as acceptance criteria and are tested when stories or epics complete.

INTERNAL SECURITY REVIEW AND STATIC ANALYSIS

Prior to signing the product firmware (nShield module and Remote Administration card Applets), the code is subject to an in-depth security review against a secure coding standard [Ref 2]. This is in addition to in-sprint peer code reviews conducted on a per story basis. Static code analysis runs daily as part of the Agile Continuous Integration process. The production process ensures secure loading as recommended in [Ref 6].

INDEPENDENT REVIEW

nCipher has sought to gain the highest levels of assurance through independent review. Remote Administration design and implementation has also been subject to external scrutiny, in particular any new security enforcing functionality or components have been subjected to review.

SECURE CHANNEL

The secure channel design has been reviewed by senior cryptography experts from the Royal Holloway University. Notably, the reviewers have been responsible for recent publications on attacks on SSL/TLS (Lucky13 [Ref 4] and RC4 [Ref 5]) and are therefore considered well suited to reviewing the protocol from a practical security perspective.

SECURE PROTOCOL IMPLEMENTATION REVIEW

In addition to design review, the secure channel has been further reviewed by an external Penetration Test house in order to minimise vulnerabilities arising from improper configuration or implementation defects in the code.

TVD AND SECODER PROTOCOL ASSURANCE

The Trusted Verification Device and Secoder protocol meet with the German Federal Office for Information Security (BSI) certification used in the German Banking Industry.

REMOTE ADMINISTRATION CARD APPLET VULNERABILITY ASSESSMENT

nCipher has commissioned an independent assessment of the Remote Administration smart card through a review of the source code and to check for vulnerabilities as per AVA VAN.5 (high attack potential) [Ref 3], in particular, fault and side channel analysis attacks.

SECURITY CERTIFICATION – FIPS 140-2

Both the Remote Administration card (Applet and platform) and nShield module are FIPS 140-2 Level 3 validated. All cryptographic primitives used by Remote Administration have undergone FIPS algorithm and validation testing. On the Remote Administration card, the nCipher applets and platform are included in the FIPS boundary and all software running on the nShield HSM falls within the FIPS boundary. Other components in the Remote Administration architecture are not in scope of FIPS validation since they do not implement or execute cryptographic functionality.

In addition nShield XC models are eIDAS and Common Criteria EAL4 + AVA_VAN.5 and ALC_FLR.2 certification against EN 419 221-5 Protection Profile, under the Dutch NSCIB scheme.

Managing Residual Risk

Remote Administration introduces additional complexity into a Security World deployment. This section highlights residual risks that are not completely covered by the technical solution and that may require additional operational or procedural controls. Organisations deploying Remote Administration may wish to implement additional measures based on their assessment and risk appetite.

REMOTE USE OF CARDS

Replay Attack

Sensitive messages between the card and the nShield HSM may be recorded and played back to compromise the system.

Countermeasures:

- Confidentiality and integrity of sensitive data is preserved by use of Authenticated Encryption (AE) to encrypt the APDU payloads
- Messages are uniquely identified within a session
- Directional counters used to guarantee freshness.

Residual Risk:

- Minimal.

TRAFFIC ANALYSIS

Since APDU packet headers are transmitted in clear, there is a risk that traffic analysis lets an attacker build up a picture of key sets and card-holders in place for a given organisation (where they are located and when they are used).

Countermeasure:

- Confidentiality and integrity of sensitive data is preserved by use of Authenticated Encryption (AE) to encrypt the APDU payloads
- Use of a VPN to securely tunnel data.

Residual Risk:

- There is a risk of an insider attacker (e.g. who also has corporate VPN credentials) being able to profile traffic headers and retrieval of publicly available information (the module serial number and card serial number).
- If this is a concern, customers may create a dedicated tunnel to provide access to only a closed group.

MAN IN THE MIDDLE ATTACK

A third party between the card and nShield HSM may impersonate each endpoint element, thereby enabling; re-routing of traffic to a malicious HSM or card, eavesdropping and injecting of messages into the communication path.

Countermeasures:

- Mutual authentication between card and nShield HSM based on embedded trust anchors at each end-point.
- End to end encryption (Remote Administration card to nShield HSM and vice versa) of sensitive data using ephemeral keys.
- Secure loading of the communication trust anchors (Warrants) on each of the end points.

Residual Risk:

- Manual verification of the nShield HSM identity is required at the client end. There is a risk that malware on the client workstation may interfere with the selection of the nShield HSM being connected to. Use of a TVD for HSM authentication as described in section nShield Trusted Verification Device is recommended and users may take appropriate measures to maintain secure environments as described in see section Client Workstation.
- Network components such as the proxy server that provide connectivity between the Remote Administration card and nShield HSM may be subject to availability attacks. Secure deployment options are described in chapter Deployment Considerations.
- Social Engineering attacks may be employed to persuade users to confirm the wrong **ESN_M**. Users are required to be especially vigilant in checking the numbers to be confirmed against a provided list of nShield HSM serial numbers and what is displayed on the TVD.

REMOTE CONFIGURATION

Firmware Downgrade of nShield HSM

Attackers may use the remote firmware upgrade process to downgrade the firmware to a version with known security flaws

Countermeasures:

- nShield HSMs will only permit loading of firmware that validates to a nCipher root warranting key.
- nShield HSMs do not permit loading a version of firmware with a Version Number (VSN) lower than the VSN of the firmware already on the HSM.

Residual Risk:

- None.

REMOTE ACCESS TO TOOLS

Attackers may attempt to exploit remote management capability to manage and configure the nShield HSM (e.g. set the mode switch on a nShield Solo to change its mode).

Countermeasures:

- Access to remote tools are reliant on operating system access controls and privileges

Residual Risk:

- Deploying organizations or service providers are required to configure the RAS and nShield HSM host machines so that access is limited to only those that support the business function, applying the principal of least privilege.
- Deploying organizations or service providers hosting network components will need to defend against network based threat actors. Recommended architectural and technical mitigations are described in section Secure Deployment.

REMOTE ADMINISTRATION SMART CARD AND TVD THREATS

Compromised Remote Administration Card

Attackers present a lost or stolen card remotely:

Countermeasures:

- A complete quorum would need to be compromised before important security-world keys can be derived.
- Standard smartcard protection mechanisms are used to protect logical token fragments and other Critical Security Parameters on the card from being extracted.
- Use of an Authorized Card List to prevent access by unauthorized cards.
- Logical fragments held on the card may be further protected with passphrases.

Residual Risk:

- The Remote Administration smart card sets do not mandate use of a passphrase in order to be used.
- Perform regular audit of cards and promptly remove lost or compromised cards from the whitelist as described in section Loss or Theft of as soon as they are known to be lost.
- Remote Administration cards must be regarded and treated as a sensitive asset.

COMPROMISED TVD

An attacker may attempt to re-route communications from a Remote Administration card to a malicious HSM allowing the incorrect HSM serial number (ESNM) to be confirmed using a compromised TVD.

Countermeasures:

- Signed firmware is installed on the TVD reader by the manufacturer and tamper labels applied to the enclosure.
- Remote Administration cards will only communicate with genuinely warranted nShield HSMs.

Residual Risk:

- Shim attacks that do not compromise tamper labels are still possible on the TVD devices. Close inspection of the TVD card slot to ensure that it is clear of any inserted bugging devices is recommended before use.
- TVDs must be regarded and treated as a sensitive asset and tamper labels must be inspected prior to use. It is recommended that the TVD is physically protected when not in use.

COMPROMISED AUTHORIZED CARD LIST

An attacker may attempt to perform an availability DOS attack on the system or allow the use of unauthorised cards by modifying the whitelist.

Countermeasure:

- Remote Administration cards will only communicate with genuinely warranted nShield HSMs.

Residual Risk:

- Regular inspection of the Authorized Card List is advised to ensure only valid cards are permitted.
- Regular muster of cardholders is advised to confirm that they still have the specific cards in their possession.

Deployment Considerations

This section describes best practices for secure deployment of Remote Administration components.

TRUST ARCHITECTURE

For secure deployment purposes the Remote Administration solution should be considered in the context of assets being protected and how the components that protect them are arranged architecturally. The levels of trust assumed for nShield Remote Administration are shown on Figure 2 Remote Administration architecture and levels of trust. The colours in the diagram signify the levels of trust.

- Blue elements store the most sensitive assets that require confidentiality and integrity protection (nShield HSM stores the module keys and the Remote Administration card stores logical token fragments). They are considered the most trusted since these have been designed for the purpose of storing secrets and performing cryptographic operations and are therefore subject to rigorous assurance, see chapter Security Properties.
- Orange element (the nShield Connect or nShield Solo host environment and the RAS) are less trusted but are hard for an attacker to access since they are subject to standard environmental controls and network architecture security measures in the Data Centre.
- Green elements are PCs configured and controlled by the customer to communicate with the Host. The management PC may be considered to be more trusted than the user PC. In particular, this architecture aims to ensure that an attacker cannot achieve more than denial-of-service even if she controls the user PC. Note that it is possible to co-locate the Remote Access Client and Remote Administration Client (RAC) on the same workstation. In this case more stringent measures must be observed to maintain a sanitized environment, see section Client Workstation.
- The Security Officer and Administrator/operator card holder are customer employees assumed not to be actively subverting the system.

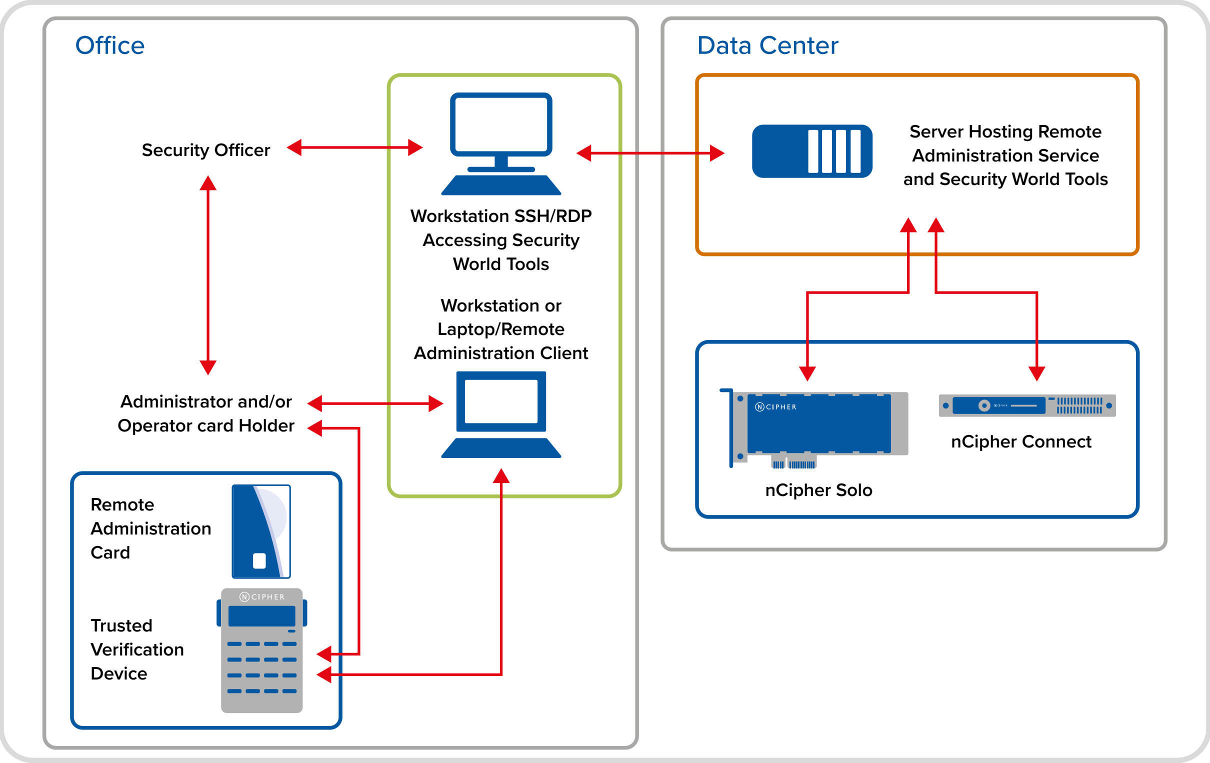
Office
Security Officer
Workstation SSH/RDP Accessing Security World Tools
Workstation or Laptop/Remote Administration Client
Administrator and/or Operator card Holder
Remote Administration Card
Trusted Verification Device
Data Center
Server Hosting Remote Administration Service and Security World Tools
nCipher Solo
nCipher Connect

Figure 2. Remote Administration architecture and levels of trust

SECURE DEPLOYMENT

The client workstation used for remote access and remote authorisation requires the network hosting the nShield HSM to be open to outside access. Opening the network to outside access presents many security risks which must be addressed through use of technological and procedural controls. It is recommended that remote access policies are implemented that follow industry best practise. To minimise the residual risk described in section Remote Use of Cards, the following general functions are recommended:

- Network architecture that protects system and resources using access control policy based on the privileges allowed for the specified user and endpoint;
- Network architecture that implements defence in depth strategy with robust protection at the network edge. The nShield HSM must be sited in a secure enclave ideally behind additional nested network firewalls and segments (zones) with monitoring and IDS both at the perimeter and internal enclaves. Refer to the nShield Security Manual for additional considerations and recommendations relating to nShield deployment and configuration. The Security Manual is included with the standard Security World Software ISO. A conceptual secure architecture for Remote Administration is shown on Figure 3 Secure Deployment Architecture
- Use of a VPN for secure tunneling of data through the public network from the client workstation to the Data Center. This in particular protects against outsider attackers wishing to profile traffic. The VPN connections are shown on Figure 4 Secure Connections Architecture.

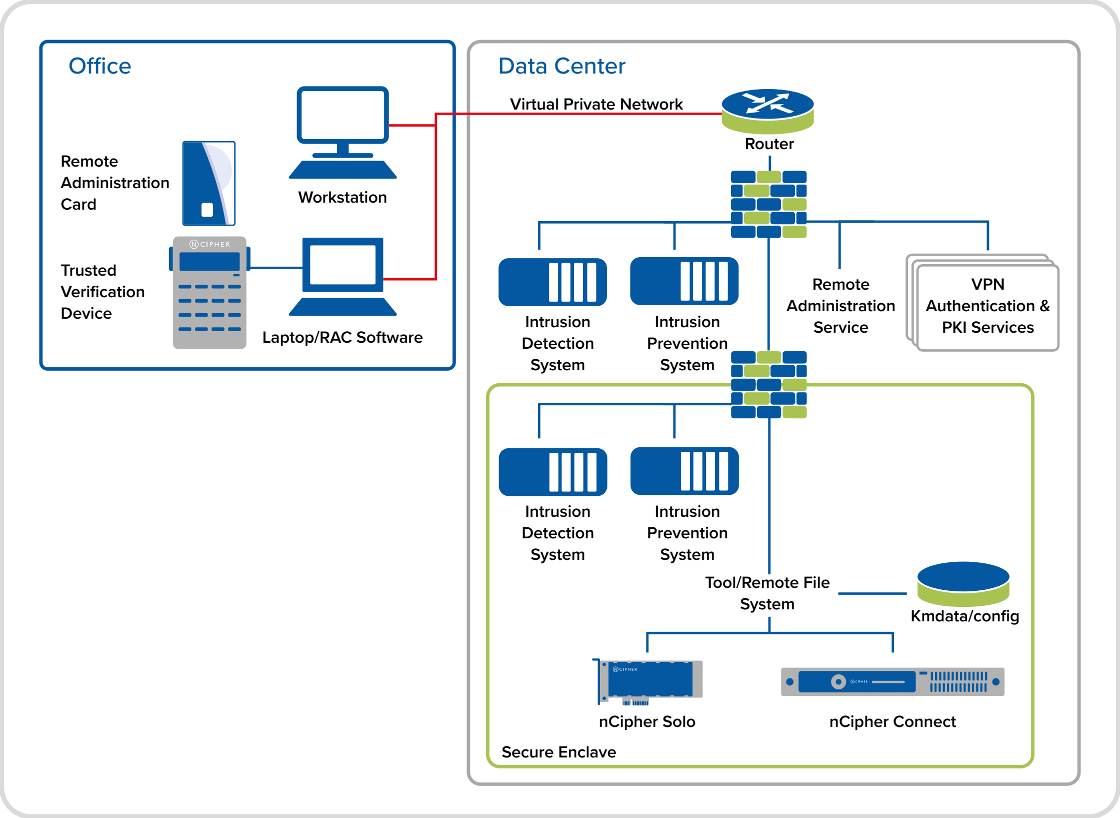
Office
Remote Administration Card
Workstation
Trusted Verification Device
Laptop/RAC Software
Data Center
Virtual Private Network
Router
Intrusion Detection System
Intrusion Prevention System
Remote Administration Service
VPN Authentication & PKI Services
Intrusion Detection System
Intrusion Prevention System
Tool/Remote File System
Kmdata/config
nCipher Solo
nCipher Connect
Secure Enclave

Figure 3. Secure Deployment Architecture

CLIENT WORKSTATION

Best practices for OS and application security controls are recommended on the client machine to minimise the residual risks identified in the section Remote Use of Cards. The following additional recommendations are specific to Remote Administration:

- Protection of the Remote Administration card: Operator and Administrator card sets must be kept securely
- TVD: The TVD must be kept safe at all times and inspected for damage to the device and tamper labels before each use
- The list of valid **ESN$_{\mathrm{Ms}}$** is provided out of band for manual verification of the nShield HSM target. This list must be kept securely and made available only to authorized card holders.

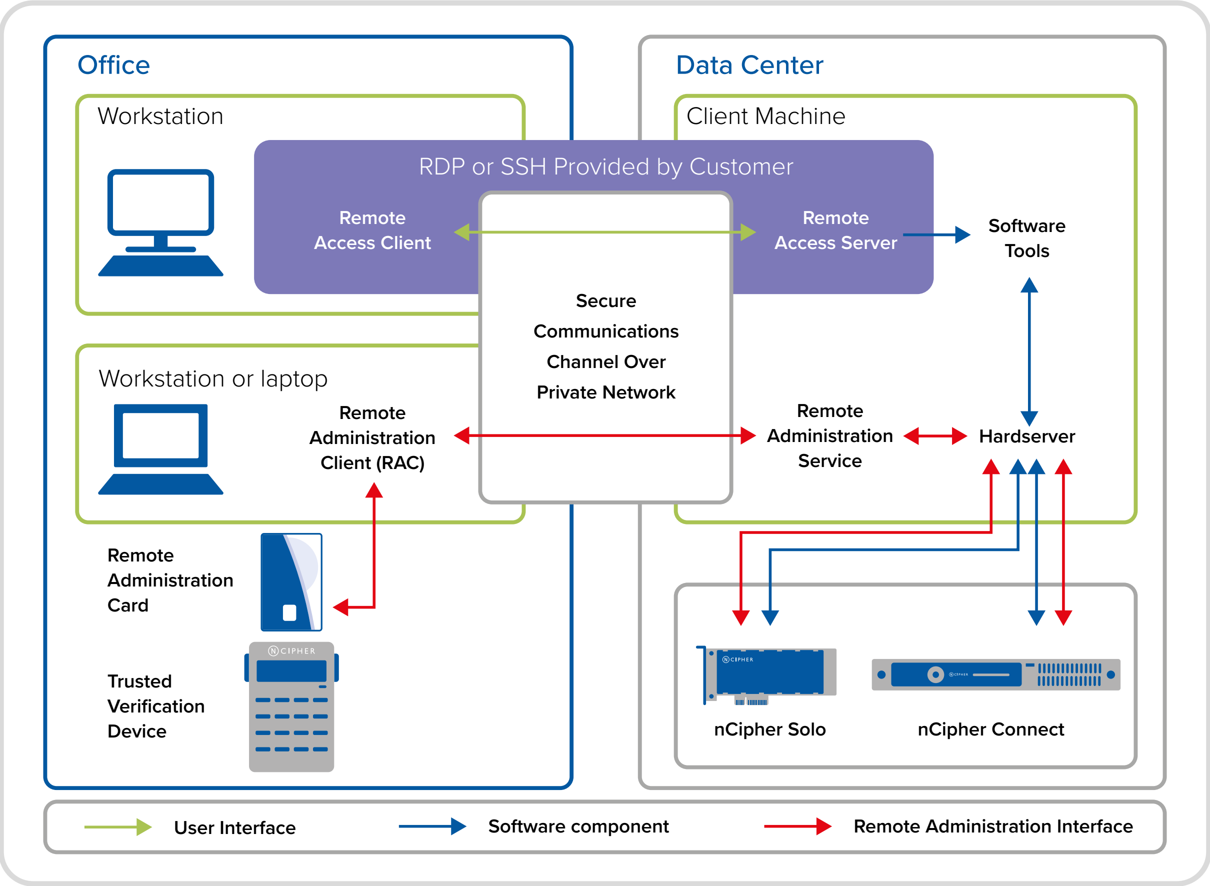
Office
Workstation
RDP or SSH Provided by Customer
Remote Access Client
Remote Access Server
Data Center
Client Machine
Software Tools
Secure Communications Channel Over Private Network
Workstation or laptop
Remote Administration Client (RAC)
Remote Administration Service
Hardserver
Remote Administration Card
Trusted Verification Device
nCipher Solo
nCipher Connect
User Interface
Software component
Remote Administration Interface

Figure 4. Secure Connections Architecture

Configuration

TURNING OFF REMOTE ADMINISTRATION

Remote Administration (remote authorisation) can be turned off by disabling the Dynamic Slot Interface used by the clients to communicate with the nShield HSMs.

Dynamic Slots are configured via the nShield Connect front panel and also in the hardserver configuration file by an appropriately authorised administrator.

REMOTE SWITCH FUNCTIONALITY

On an nShield Solo, remote access to setting the MOI switch can be deactivated by setting the physical mode override jumper on the PCIe card [Ref 8]. On an nShield Connect, remote switching functionality can be turned off by configuring the appropriate hardserver configuration file.

FIRMWARE UPDATE

If remote switching is disabled on an nShield Solo as described in section Remote Switch Functionality then it is not possible to perform a remote firmware update. On an nShield Connect remote firmware update can be disabled by a configuration setting via the front panel or by updating the relevant hardserver configuration file.

Recovery actions in event of compromise

LOSS OR THEFT OF REMOTE ADMINISTRATION CARDS

Loss or theft of the Remote Administration cards should be treated no differently from the previous non-Remote Administration cards. ACS card sets protect the Security World Root key and Security Module keys and OCS card sets protect Application keys. If OCS key recovery is enabled, the ACS protected Security Module key is also used to protect the Application keys.

- In the case of a sub-quorum loss, (k < n), of either OCS or ACS, the entire ACS/OCS card sets must be replaced and any old cards destroyed
- For full quorum loss, (k > n), the entire ACS/OCS card sets must be replaced and old cards must be destroyed. The entire security world must also be replaced. Any recovery keys must also be destroyed.

In both cases above, administrators should also strike the lost cards from the Authorized Card List (whitelist) held on the RFS fileserver and client machines [Ref 7] and [Ref 8].

TVD COMPROMISE

TVD Tamper

Inspection of the four tamper labels on the TVD device is advised before every use. The TVD is to be regarded as untrusted if there is evidence of tamper and should not be used. Users are advised to replace the TVD with another that has its labels intact. Further investigations into the impact of the tampered device may be followed in line with the deploying organisation's policy.

TVD Loss or Theft

No security impact on confidentiality and integrity of either Remote Administration card or nShield HSM held secrets. Users are advised to report the event and handle the loss as per their organisation's security procedures.

References

Warrant Key	Parameter
[Ref 1]	nCipher Security World. Available at: https://go.ncipher.com/rs/104-QOX-775/images/nCipher-Security-World-Architecture-wp.pdf
[Ref 2]	CERT Coding Standards. Available at: https://www.securecoding.cert.org/confluence/display/seccode/CERT+Coding+Standards
[Ref 3]	Common Criteria v 3.1 Release 4. Part 3: Security assurance requirements. Available at: https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf
[Ref 4]	Lucky Thirteen: Breaking the TLS and DTLS Record Protocols, Nadhem J. AlFardan and Kenneth G. Paterson, 27th February 2013. Available at: http://www.isg.rhul.ac.uk/tls/TLStiming.pdf
[Ref 5]	On the Security of RC4 in TLS and WPA. Nadhem J. AlFardan, Daniel J. Bernstein, Kenneth G. Paterson, Bertram Poettering, Jacob C.N. Schuldt. 8th July 2013. Available at: http://www.isg.rhul.ac.uk/tls/RC4biases.pdf
[Ref 6]	Smartcard Security, Information Security Bulletin, Marc Witteman, October 2003. Available at: https://www.riscure.com/archive/ISB0808MW.pdf
[Ref 7]	nShield Connect User Guide (2020). nCipher e-Security.
[Ref 8]	nShield Solo User Guide (2020). nCipher e-Security.
[Ref 9]	Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm, Mihir Bellare, Chanathip Namprempre. 14th July 2007. Available at: https://cseweb.ucsd.edu/~mihir/papers/oem.pdf
[Ref 10]	NIST Special Publication 800-56A Rev 3 (2018). Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf
[Ref 11]	FIPS PUB 186-4 (2013). Available at: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
[Ref 12]	NIST Special Publication 800-108 (2009).
[Ref 13]	“How to share a secret", Communications of the ACM 22, (11): 612–613. Shamir Adi, (1979).

NCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

ABOUT NCIPHER SECURITY

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our 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, ensure the integrity of your data and put you in complete control – today, tomorrow, always. www.ncipher.com

Search: nCipherSecurity

TRUST. INTEGRITY. CONTROL.