ARQIT NetworkSecure™ Standalone (Test Mode) Adaptor v4.0.0 Installation Guide

For integration testing with devices and applications using the ETSI 014 interface

Version	:	1.1
Classification	:	PUBLIC
Export Rating	:	NOT EXPORT CONTROLLED
Status	:	Issued
Date	:	09/07/2024

Version Control

Version	Status	Date changed	Change summary	Authored by
1.0	Issued	07/02/2024	Install guide for v3.3.0 of Standalone Adaptor	Ravi Patel
1.1	Issued	09/07/2024	Install guide for v4.0.0 of Standalone Adaptor	Ravi Patel

Contents

Introduction

Overview

The Arqit NetworkSecure Adaptor is a software application that interfaces with network devices e.g. firewalls or applications (collectively referred to ‘Devices’ in the rest of the document – that support the ETSI 014 specification for external key retrieval.

Connecting Devices to NetworkSecure Adaptors enables out-of-band symmetric keys to be requested on-demand that can be used to secure communications between Devices e.g. a point-to-point IPSec VPN link between firewalls.

Adding additional key material at both ends of the tunnel outside of the IPSec key agreement protocols (such as IKE v2 which are believed to be susceptible to retrospective attack by quantum computers) adds protection against attack by quantum computers in the future; breaking the key agreement protocol cannot reveal the additional key material ensuring data passing through the tunnel remains secure.

Purpose and scope

This document introduces the high-level architecture of Arqit’s NetworkSecure™ Adaptor configured in ‘Standalone’ or ‘Test Mode’ (shortened to **‘Standalone Adaptor’** in the document), Version 4.0.0, and describes the steps required to configure and deploy the Standalone Adaptor to provide fixed symmetric keys to Devices using the ETSI 014 interface for purposes of integration testing only.

It does not include a detailed description of the steps required to configure the Device to make key requests to the Standalone Adaptor using the ETSI REST API. It is recommended to refer to the specific Device vendor documentation for configuration instructions.

Variable Notation

In script and command line examples, variables that should be replaced are indicated by the <VariableName> notation; when replacing the variables, the <> should *not* be included.

For example, in the command line

```
sudo networksecure deploy -c <path to config.yaml>
```

the following should be entered

```
sudo networksecure deploy -c /opt/adaptor/config.yaml
```

where */opt/adaptor/config.yaml* is the example value to be used.

Further reading

The ETSI 014 specification is a comprehensive description of the interface used between the network firewall gateways (SAEs) and the Standalone Adaptor.

The Standalone Adaptors replace the KME devices shown in this specification, allowing key agreement over a classical network.

https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf

Prerequisites

Introduction

Before starting to install, please ensure the following pre-requisites are available.

Checklist

Item	Description
Secure Application Entity (SAE) licenses	A minimum of two Devices (SAEs) e.g. firewall gateways are required to make use of the Standalone Adaptor functionality and each Device must be registered with any required vendor licenses.
SAE firmware updates	Devices (SAEs) must be running firmware that generates and responds to ETSI 014 REST API calls made to Arqit's Standalone Adaptor.
Standalone Adaptor virtual machines	A dedicated VM (AWS EC2 instance or Azure Virtual Machine) is required to host each Standalone Adaptor.

Certificates	The ETSI 014 specification requires mutual TLS authentication between a network device (SAE) and its key provider (KME). Two certificates are required to enable mutual authentication between a Standalone Adaptor and its corresponding SAE e.g. firewall gateway. • The setup procedure provides the ability to generate self-signed certificates that can be used for integration testing.
Standalone Adaptor Virtual Machine image	Once you have purchased the Standalone Adaptor product, access is provided to the Standalone Adaptor Amazon Machine Image (AMI) or Azure Virtual Machine (VM) Image that can be used to create the cloud VMs required for performing ETSI 014 integration testing with Devices.

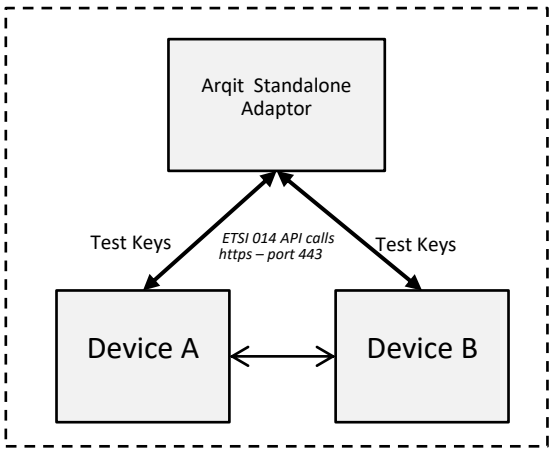
Architectural overview

The Standalone (Test mode) Adaptor is deployed for purposes of integration testing with Devices that support the ETSI 014 interface. This solution provides a quick and easy setup enabling OEM network appliance vendors or application developers to request fixed ‘dummy’ symmetric keys (256 bits) to test the ETSI 014 REST interface and related API calls.

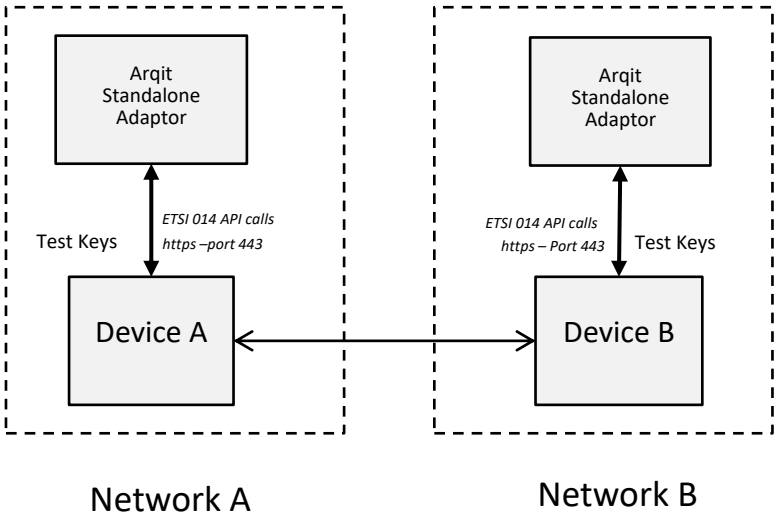
The Standalone Adaptor provides test keys and is **not suitable for production environments** that require secure i.e. quantum safe keys for enhanced security. It additionally does not provide the policy and management benefits that Arqit’s SKA-Platform™ and NetworkSecure™ Adaptor delivers.

IMPORTANT: Running in Test mode in a production environment is not supported.

The following two network deployment scenarios are supported.



Scenario 1 – Single Standalone Adaptor providing test keys to two devices locally



Scenario 2 – Two Standalone Adaptors providing test keys to connected devices

In Scenario 2, Standalone Adaptors are providing the same test key to its corresponding locally connected Device. Each Device/Standalone Adaptor pair can be located in different networks to simulate a 'real' network communication link between Devices.

NOTE:

- The test keys generated by the Standalone Adaptor(s) are based on a passphrase entered by the user at the time of deployment of the Adaptor. The same symmetric key is generated for each ETSI 'Get Key' and ETSI 'Get Key with ID' request based on the unique passphrase configured in the Standalone Adaptor.
- In both deployment scenarios, the appropriate network configuration needs to be put in place in order for both Device A and B to communicate with each other over the network to establish data communication sessions using the Standalone Adaptor test keys.

IMPORTANT – In Scenario 2, **the same passphrase** needs to be configured in each of the Standalone Adaptors to generate identical test keys.

Locating Standalone Adaptors within the network

The Standalone Adaptors do not require any internet connectivity to function, nor do the Adaptors need to communicate with each other in the deployment scenario outlined in Figure 2. They therefore can be deployed in a private network (assigned private IPv4 addresses), and in the same subnet as the locally connected Device e.g. firewall.

The Standalone Adaptor and connected Device communicate with each other over the ETSI 014 REST interface using https over port 443 (http over TLS).

Adaptor as a service

The Standalone Adaptor runs as a Linux *systemd* service. This enables the Adaptor to automatically start and run as a background service in the context of a specified user. The user must exist on the system (see how to create a User). The deployment process will create a new folder structure in the Linux file system including the `networksecure-adaptor.service` systemd service file in the following folder:

```
/etc/systemd/system/networksecure-adaptor.service
```

Adaptor folder structure

```
/opt
    /arqit
        /networksecure-adaptor
            certs/
                ...
            install/
                ...
            LICENSE
```

```
/etc
    /arqit
        /networksecure-adaptor
          config.yaml
          /examples
             example_env.conf
             example_config.yaml
/var
    /log
        /arqit
            /networksecure-adaptor
               adaptor.log
```

If the Adaptor service fails, *systemd* will attempt to restart the Adaptor three (3) times (once every 10 seconds) before generating an error message. Additionally, OS re-boots will automatically re-start the Adaptor service.

Useful systemd commands

- `sudo systemctl status networksecure-adaptor.service`
  - get status of service

- *sudo journalctl -u networksecure-adaptor.service*
  - get systemd service logs. This command enables informational messages generated by the Standalone Adaptor to be displayed in the console, including any errors that may be encountered during the normal operations of the Standalone Adaptor once it has been started by the systemd service.
- `sudo systemctl stop networksecure-adaptor.service`
  - stop the Standalone Adaptor service if running
- `sudo systemctl start networksecure-adaptor.service`
  - start the Standalone Adaptor if not already running
- `sudo systemctl restart networksecure-adaptor.service`
  - re-start the Standalone Adaptor

Systemd Security Hardening features

Systemd natively provides system hardening capabilities to enhance the security of deployed Standalone Adaptors. Arqit recommended security settings are enabled by default and outlined in Appendix A.

NOTE: systemd security hardening measures can be enabled/disabled depending on your specific system security policies and requirements. More information can be found at https://www.freedesktop.org/software/systemd/man/systemd.exec.html.

Do not modify the 'ExecStart' line in the `networksecure-adaptor.service` file.

Standalone Adaptor Setup and Configuration

This section runs through the steps to setup and configure a Standalone Adaptor.

The following sections describe the workflow.

- Setting up the Standalone Adaptor
- Device configuration
- Configuring the Standalone Adaptor
- Deploying the Standalone Adaptor
- Running the Standalone Adaptor
- Stopping the Standalone Adaptor
- Uninstall the Standalone Adaptor

It is recommended that you examine the configuration parameters (Appendix A) before beginning the setup to ensure you understand what the parameters mean and where they are located.

Pre-reading

Certificate creation and installation

The Standalone Adaptor uses self-signed certificates which are created by the Standalone Adaptor by default at the time of deployment (the parameter 'createDemoCertificates' is set to 'true' in the config.yaml file).

The internal Standalone Adaptor certificate script will create a dummy CA with CA root certificate, plus test certificates for the Standalone Adaptor and the associated Device e.g. a firewall gateway.

The SAE_ID – format for unique identifier of SAE (Device)

The ETSI 014 standard supported by the Standalone Adaptor limits the passing of a single standardised parameter (the SAE_ID of the Device at the "remote end" of the communication link e.g. a VPN tunnel) when requesting a key.

The SAE_ID for each Device must conform to the following format:

```
<Hostname>::<Adaptor FQDN>
```

where ***<Hostname>*** is the identifier for the locally connected Device:

E.g. ‘firewall-xxx’; ‘router-xxx’; ‘app-xxx’

where ***<Adaptor FQDN>*** is the Fully Qualified Domain Name of the Standalone Adaptor. (*A private IPv4 address of the Standalone Adaptor can be used here for convenience as no internet connectivity is required by the Adaptor in Test mode)*

Note: The Device Hostname and the Adaptor FQDN must not contain the character “:” (colon).

The SAE_ID should be configured to this compound value in the Device’s management console and in the Standalone Adaptor configuration.

Preparing for Standalone Adaptor Deployment

Certificate creation

The dummy certificates required for each Standalone Adaptor and connected Device are created as part of the Deployment process based on the certificate settings in the Standalone Adaptor *config.yaml* configuration file.

Create a runtime User for the Standalone Adaptor service (OPTIONAL)

The Standalone Adaptor is pre-configured with a system user '*netsecure-exec*' which has non-sudo privileges. The NetworkSecure Standalone Adaptor systemd service runs as this user on the deployed VM. This limits the attack surface and minimises the risk of an attacker who has compromised this specific user account from gaining access to root/sudo privileges. If required, another user can be created to run as the Standalone Adaptor daemon using the following command:

Steps:

1. Run the following command:

```
sudo adduser <username>
```

Device Configuration

See vendor documentation for Device specific configuration to enable key requests to be made over the network to the Standalone Adaptor using the ETSI 014 API.

Configuring the Standalone Adaptor

The Standalone Adaptor uses the config.yaml file as its source of configuration information – see Appendix A.

The following configuration parameter values in the *config.yaml* file (located at `/etc/arqit/networksecure-adaptor/config.yaml`) should be set for each specific Adaptor deployment:

- saeId: "" (SAE ID must conform to this format)
- certificates: the default values for each parameter can be used or customised if required.
- strictUuidFormatting: false (Note: if using Juniper firewalls to test the integration with the Standalone Adaptor, this value should be set to true)
- systemdServiceUser: "netsecure-exec" (runs as *netsecure-exec* by default, but it can be changed as per create a new non-privileged systemd user for Standalone Adaptor)
- isSecondary: false (this default value must not be changed)
- testMode:
    - enabled: true

i. passphrase: "" (the passphrase required for test key generation)

- qkeyMode:
  - enabled: false (this default value must not be changed)

Note: The example_config.yaml file (located at /etc/arqit/networksecure-adaptor/examples/example_config.yaml) includes the complete list of NetworkSecure configuration parameters. However the Standalone Adaptor requires only a sub-set of the parameters, as above, to be configured for each specific deployment.

Deploying the Adaptor

Once the Adaptor is configured i.e. a valid config.yaml file is available on the system, the Adaptor can be deployed to complete the installation process. If any configuration parameters in the config.yaml need to be modified **before** deployment, the config.yaml file can be modified directly to include the changes.

Steps:

1. The following command is used to deploy the Adaptor (the *config.yaml* file is stored in the default location i.e. */etc/arqit/networksecure-adaptor/config.yaml*) :

```
sudo networksecure deploy
```

Note:

- Dummy/PoC certs that are generated by the Adaptor (in the *'/opt/Arqit/networksecure-adaptor/certs'* folder) need to be uploaded to its connected Device(s) - both client.p12 and ca.crt certificates. The default caPassword, caP12Password, adaptorP12Password and clientP12Password can be changed if required in the config.yaml file, before executing the deploy command below.
- For Scenario 1 architecture, the SAE ID configured on the Adaptor is that of either Device A or Device B.
- For Scenario 2 architecture, the same passphrase needs to be entered in each of the Standalone Adaptors
- For a given passphrase, the same symmetric key (256 bits) is generated by an Adaptor for all subsequent ETSI 014 key requests it receives.
- To change the symmetric key generated by the Standalone Adaptor, the Adaptor service needs to be stopped, a different value for 'testMode:passphrase' needs to be entered and saved in the config.yaml file and the service must be re-started.
- FIPS mode is not supported for Standalone Adaptor i.e. the underling Linux OS must not be FIPS enabled.
- If the location of the config.yaml is changed after the Standalone Adaptor is deployed, the systemd service will fail to start on the next re-start or re-boot and will prevent uninstall.

Running the Standalone Adaptor

Once the Standalone Adaptor has been deployed, the *systemd* service will automatically start it.

Note: Auto-start of the Standalone Adaptor can be prevented by changing the **autoStart** parameter value to 'false' in config.yaml.

Stopping the Standalone Adaptor

Steps

1. Run the following `systemd` command:

```
sudo systemctl stop networksecure-adaptor.service
```

Uninstall the Standalone Adaptor

Steps

1. To uninstall the Standalone Adaptor, use the package manager 'remove' command:

```
sudo apt remove arqit-networksecure-adaptor
```

Upgrade Standalone Adaptor to NetworkSecure and access SKA-Platform™ features

Contact enquiries@arqit.uk and visit Arqit's website to learn more about the benefits of Arqit's SKA-Platform™ and the NetworkSecure™ Adaptor; which provides quantum safe symmetric keys over the ETSI 014 interface to protect point-to-point VPN links between network firewall gateways. An annual subscription license is required to upgrade the Standalone Adaptor to the full-featured NetworkSecure™ Adaptor and benefit from SKA_Platform™ features.

Appendix A – Configuration parameters

config.yaml

The config.yaml file (default file location *'/etc/arqit/networksecure-adaptor/config.yaml'*), documents the configuration parameters required for deploying the Standalone Adaptor.

```
---
adaptor:
  saeId: "FIXME::1.2.3.4"
  certificates:
    createDemoCertificates: true
    caFilePath: "/opt/arqit/networksecure-adaptor/certs/ca.p12"
    adaptorFilePath: "/opt/arqit/networksecure-adaptor/certs/adaptor.p12"
    caPassword: "password"
    caP12Password: "password"
    adaptorP12Password: "password"
    clientP12Password: "password"
    caCn: "arqit.network.adaptor"
    adaptorCn: "www.example.com"
    clientCn: "www.example.com"
  strictUuidFormatting: false
deployment:
  autoStart: true
  systemdServiceUser: "netsecure-exec"
  isSecondary: false
  testMode:
    enabled: true
    passphrase: "FIXME"
  qkeyMode:
    enabled: false
```

networksecure-adaptor.service (systemd config file)

This section replicates the contents of the `networksecure-adaptor.service` file which is a systemd configuration file created by the setup.sh script when deploying the adaptor. This file is created in the '*/etc/systemd/system/* ' directory.

IMPORTANT: If the location of the config.yaml is changed after the Adaptor is deployed, the systemd service will fail to start on the next re-start or re-boot.

```
[Unit]
Description=Run Arqit NetworkSecure Adaptor
After=network-online.target
StartLimitIntervalSec=60

[Service]
# DO NOT MODIFY

ExecStart=/usr/bin/bash /opt/arqit/networksecure-adaptor/install/adaptor.sh start -v $ADAPTOR_VERSION -
c $CONFIG_FILE_ABSOLUTE_PATH $TEST_MODE_FLAG $FIPS_MODE_ARG

# RESILIENCY

Type=simple
Restart=on-failure
RestartSec=10
StartLimitBurst=3

# SECURITY

# Run service as specific user
User=${SYSTEMD_SERVICE_USER}

# Prevent service from obtaining new privileges
NoNewPrivileges=yes

# Turn off physical device access
PrivateDevices=yes
DevicePolicy=closed

# Set specific system folders as read-only
ProtectSystem=yes

# Set home directory as read-only
ProtectHome=read-only

# Set Linux Control Groups as read-only
ProtectControlGroups=yes

# Deny explicit module loading
ProtectKernelModules=yes

# Set kernel variables as read-only
ProtectKernelTunables=yes

# Restrict access to Linux namespace functionality
RestrictNamespaces=yes

# Restrict access to realtime task scheduling policies
RestrictRealtime=yes

# Restrict user privilege escalation
RestrictSUIDSGID=yes

# Deny personality system call
LockPersonality=yes

# Allow adaptor service to bind to privileged ports
AmbientCapabilities=CAP_NET_BIND_SERVICE


[Install]
WantedBy=multi-user.target
```

Appendix C: Common errors

Adaptor Configuration

- Missing or Invalid parameter values in config.yaml that cause the Standalone Adaptor setup to fail.
    - saeID
    - testMode
        - passphrase

Adaptor Execution

- Missing or invalid parameter values in config.yaml that prevent starting of the Standalone Adaptor.
    - caP12Password
    - adaptorP12Password
    - caPassword
    - clientP12Password

Note: special characters in passwords should be escaped using the backslash '\' character e.g. 'pas\$345\\'