Identify - Authenticate - Anywhere

Virtual Smartcard Technical Overview

Document Control

Status	Version	Date	Owner	Description
Complete	V1.2.2	26/03/2019	Daniel Killeen	Rebranding and diagram updates
Complete	V1.2.3	14/10/2019	Krishna Kuntala	Updated references related to AWS deployment

Contents

1. Introduction

Isosec has created a new product as part of its product roadmap – Virtual Smartcard.
Virtual Smartcard is a new and highly innovative solution that addresses a number of issues with the whole lifecycle of physical smartcards within the NHS. Isosec has filed a patent application to cover key aspects of this technology in order to protect its Intellectual Property (IP). Further, specific details must be covered under a Non-Disclosure Agreement.

This document is intended to give an overview of the Virtual Smartcard solution in order to enable NHS organisations to gain an understanding and determine that Virtual Smartcard is compliant from an information governance (IG) perspective. It does this by covering a number of topics including architecture, workflow processes and the security model.
The level of detail contained in this document is aimed at being sufficient to meet this purpose whilst not revealing the key claims of the patent application.

Virtual Smartcard is offered as a cloud-based service available nationally to all NHS organisations, hosted on Amazon Web Services (AWS). For Spine ticket validations, it is dependent on AIMES who are an NHS N3 / HSCN approved cloud provider. It is suggested that readers of this document first acquaint themselves with the Virtual Smartcard marketing materials in order to gain a quick high-level view of the features of Virtual Smartcard:

To obtain a brochure or case study, please visit https://isosec.co.uk/resource-library/

2. Virtual Smartcard Technical Solution

The principle of Virtual Smartcard is to virtualise the physical NHS smartcard such that it works with and is backward compatible with existing NHS systems, applications and processes for both the management and use of smartcards. In this sense it is transparent to these systems whether a physical or virtual smartcard is used and as such both physical and virtual smartcards can coexist in the estate of an NHS organisation.

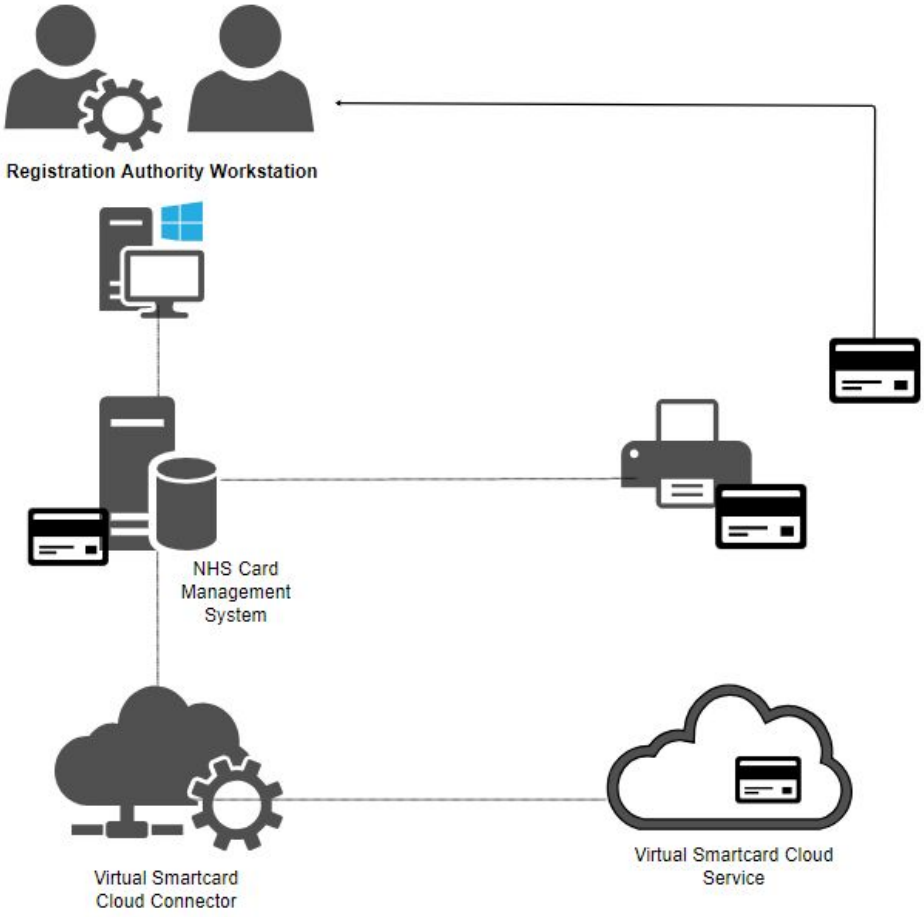
As an example, from a desktop, a user can either use their physical smartcard to authenticate using the Isosec Identity Agent or automatically authenticate with their Virtual Smartcard (linked to their AD account). A variety of 2FA methods are available for the use of Virtual Smartcard.

2.1 Virtual Smartcard Issuance

The process to issue a Virtual Smartcard is exactly the same as for a physical smartcard except for the last piece, where rather than a physical smartcard emerging from a smartcard printer, a Virtual Smartcard is created in the Virtual Smartcard cloud service where it is held securely. A Virtual Smartcard never leaves the Virtual Smartcard cloud service – it is only ever managed or used from within.

Specifically, the user must be registered in the Spine Directory Service (SDS) after having undergone all the normal rigorous eGif L3 identity verification checks required for the issuance of a physical smartcard.

This is shown as follows:



On the RA Workstation, an additional component is installed that enables the NHS Card Management System application to connect to the Virtual Smartcard cloud service. This connector essentially provides

a WINSCARD interface that the NHS Card Management uses to interact with the Virtual Smartcard service.

The RA User follows the same process for issuing a Virtual Smartcard as that of a physical card.

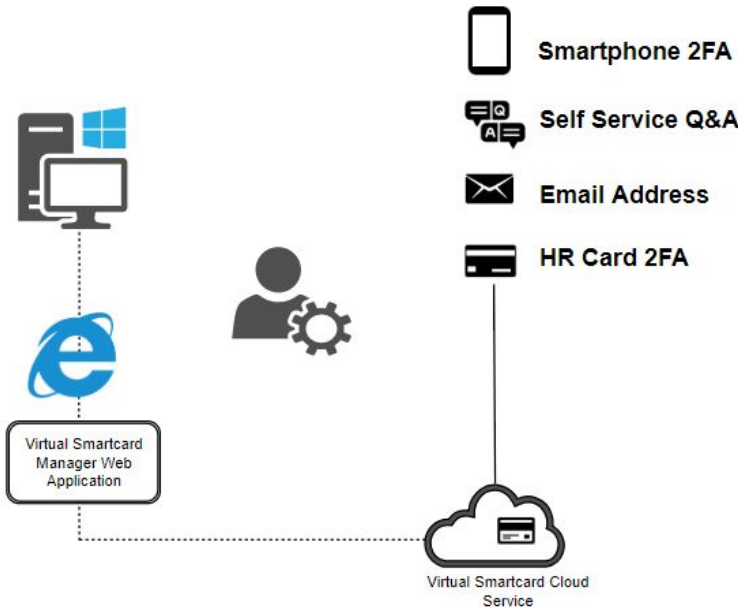
The RA process will complete as normal except it will result in a Virtual Smartcard being created in the Virtual Smartcard cloud service. This Virtual Smartcard is an analogue of the physical one, containing the equivalent smartcard keys and certificates, with the keys being encrypted using the passcode the user entered during the issuance process.

At this point there is nothing to hand to the user – to complete the issuance process, the RA User together with the user must complete the vRA Registration process, which is described in the following section.

2.2 VRA Management

Once a Virtual Smartcard has been created for the user, an RA User must complete User Enrolment using the vRA Manager (which is a web application and part of the Virtual Smartcard cloud service) before the user can use the card and optionally one of more Authentication Methods. Alternatively, the RA can partially complete the enrolment process by providing the user's email address and mobile phone number where the user completes the enrolment using self service.

Where the RA performs the enrolment with the actual user the vRA Manager is shown as follows:

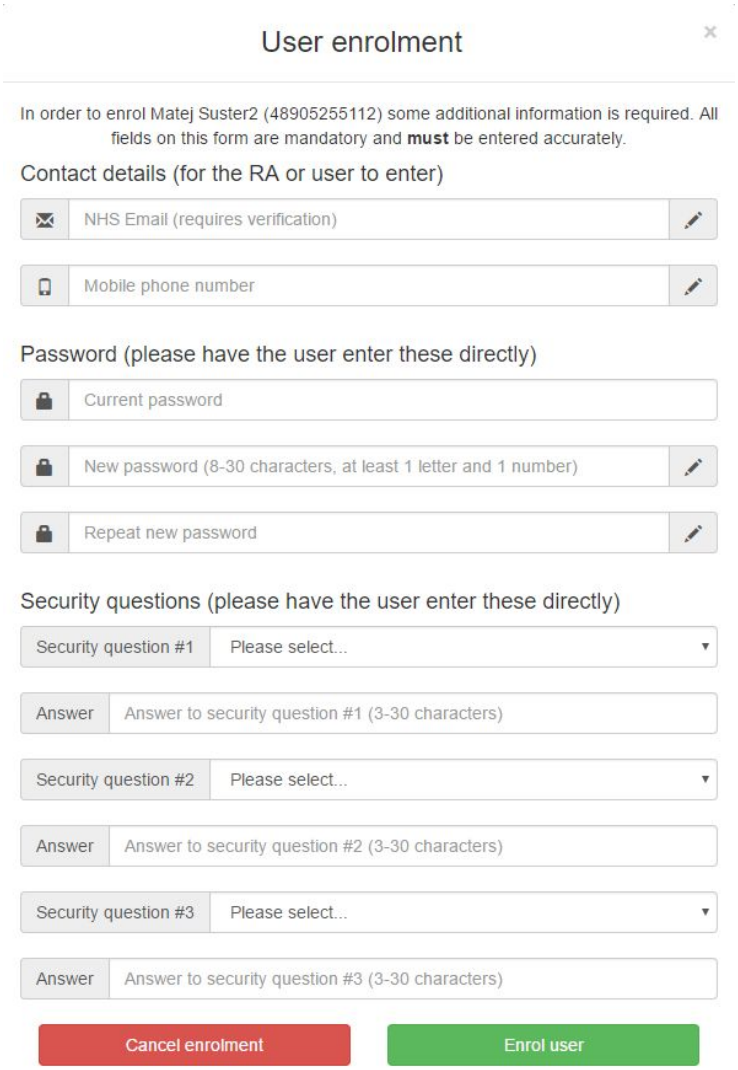


In order to use the vRA Manager, an RA User must first authenticate using the Isosec Identity Agent and be authorised as an RA (i.e. selected an RA role).

2.2.1 User Enrolment

For the Enrolment part, the RA User completes some basic contact details for the user and the user is then required to set a strong passcode, as well as three security questions and answers which are able to unlock the account via the Virtual Smartcard Self-Service Portal, should this be required.

As a minimum, the user's email address must be provided if no other associated Authentication Methods are added, in order for the user's Virtual Smartcard to be used from a generic AD account.



2.2.2 Authentication Association

For the Authentication Association, the RA User selects the user's Virtual Smartcard and then associates it with one or more of the following methods of authentication.

2.2.2.1 Authentication Association

The user's Window AD domain and account name are entered. Note, this is just simply an association - no actual connection is required between the Virtual Smartcard cloud service and the NHS organisation's AD instance.

2.2.2.2 Isosec 2F Authenticator Mobile App

The Isosec Authenticator application is available for the iOS and Android platforms, and can be downloaded from the Apple App Store / Google Play Store. Once installed, the device is associated with the user's Virtual Smartcard by scanning a QR code displayed in the vRA Manager, with the user then entering their passcode in the app.

2.2.2.3 FIDO2 Key

A FIDO2 compliant authenticator key can be registered and associated with a user's Virtual Smartcard in the vRA Manager.

2.2.2.4 MIA Mobile Platform

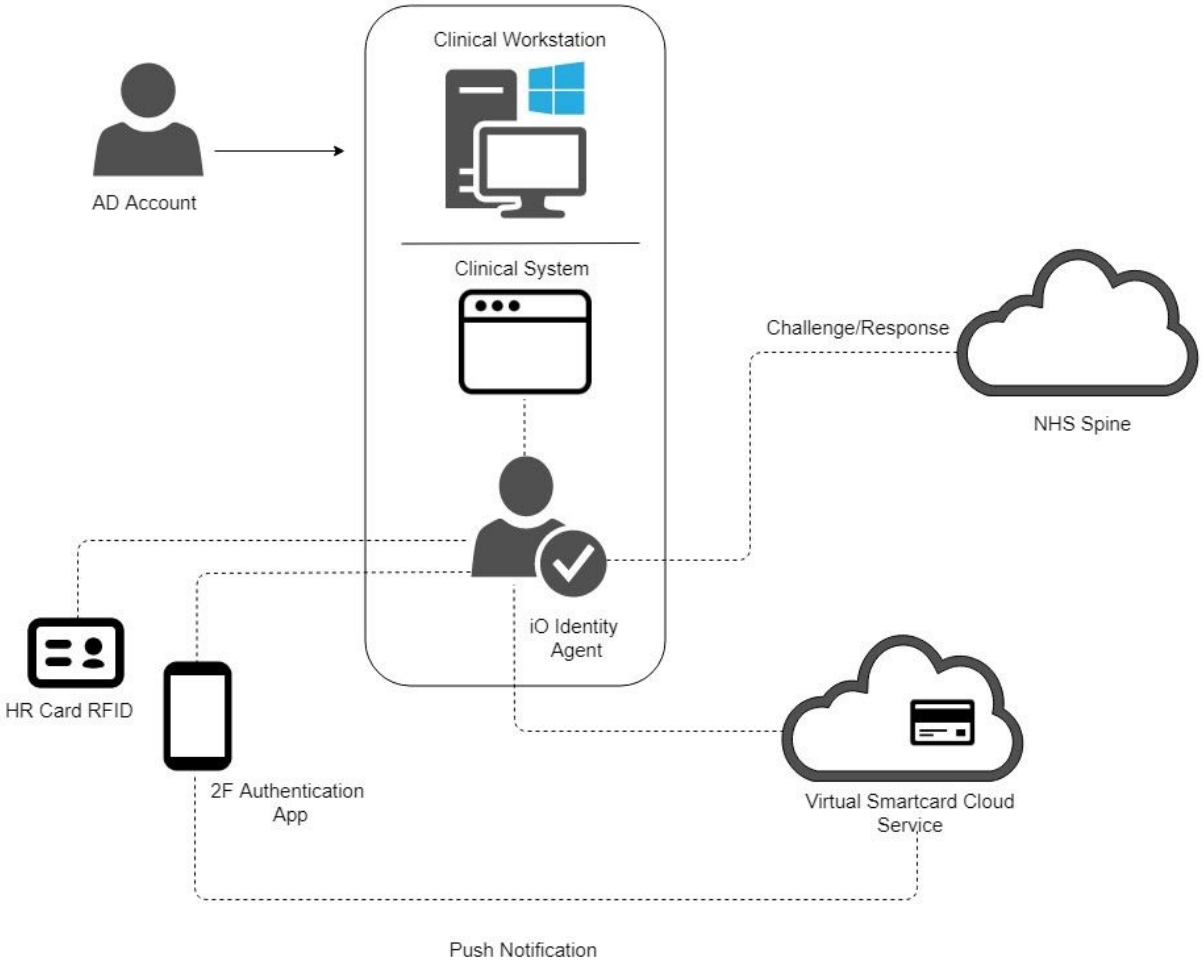
The MIA iOS, Android or Windows app can be installed from the relevant application store, and the user's device can then be associated with the user's Virtual Smartcard by scanning a QR code displayed in the vRA Manager, and the user then entering the passcode in the app.

2.2.2.5 HR Mifare Card (2F)

A contactless reader is used to scan a Mifare RFID capable card. The user's card is tapped on the RFID reader which is read by the vRA Manager and associated with the user's Virtual Smartcard.

2.3 Authentication Association

The process of authentication using the Virtual Smartcard is by design simple and easy. Diagrammatically, this is shown as follows:



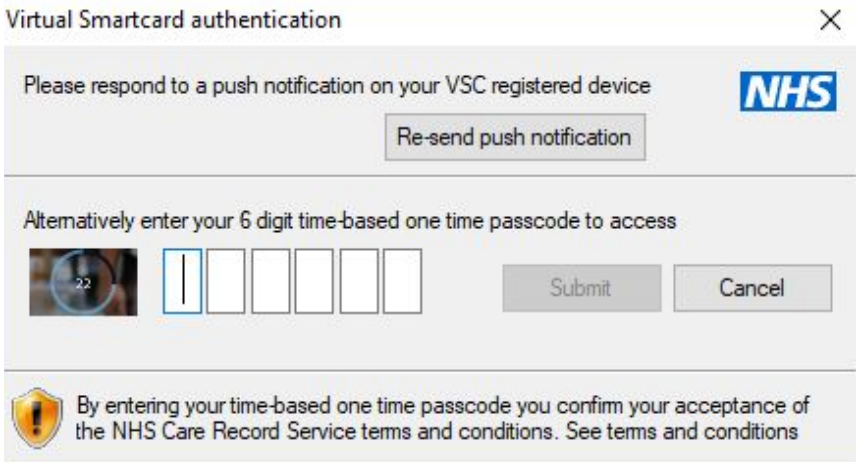
In all cases, the passcode is required to enable the user's Virtual Smartcard to be used.

The following sections describe how each of the associated Authentication Methods are used to authenticate on a Windows PC using the user's Virtual Smartcard.

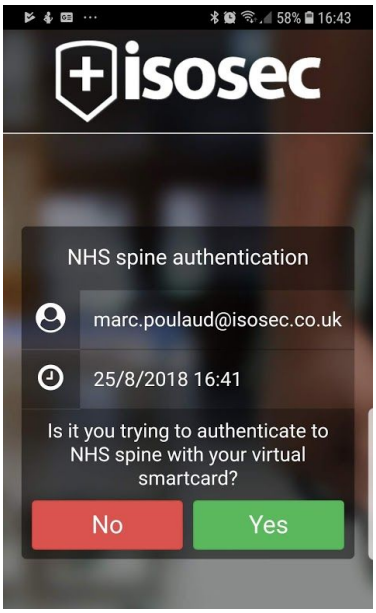
2.3.2 AD Authentication 2FA

In order to use 2F authentication the user must have the Isosec Authenticator Mobile app as an associated Authentication Method.
Once AD Authentication has completed, the user's Authenticator Mobile app will be sent a push notification (if online) or be prompted to enter a TOTP (Time-based One-Time Password) code from the app (if offline).

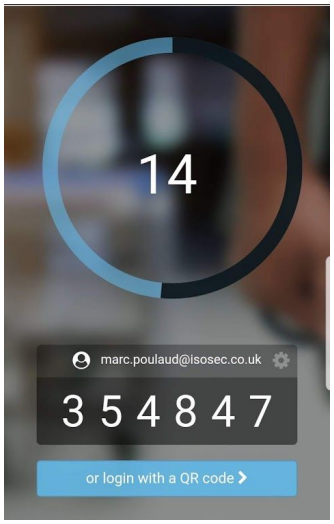
During 2F authentication, the user will see the following dialogue displayed on a Windows PC:



Simultaneously, the user's Authenticator Mobile app, the user will see the following push notification:



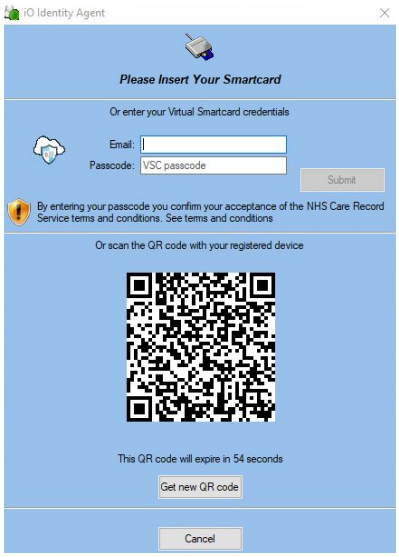
If the user's Authenticator Mobile app is offline and no push notification is received, the user will see a TOTP code which they will then be required to enter on the Windows PC:



Once the 2FA is completed, the authentication to the Spine with the user's Virtual Smartcard will complete.

2.2.3 Generic AD Authentication

In the case where users don't have named Windows AD accounts, whenever a user launches a Spine enabled application (as there is no physical card to authenticate) the following dialogue is presented to the user:



Here, the user can enter their Virtual Smartcard associated email address together with their Virtual Smartcard passcode. The user must use the Authenticator Mobile App as described in the section AD Authentication 2FA.

Alternatively, the user can simply scan the QR code using the Authenticator Mobile App and enter their passcode in the app.

2.3.4 FIDO2 Key

Once registered, iO will prompt the user to insert their FIDO2 device into the Windows PC USB port. Additionally, depending on the organisational policy, the user can also be prompted to press the activation button on the FIDO2 key and / or enter the FIDO2 key password.

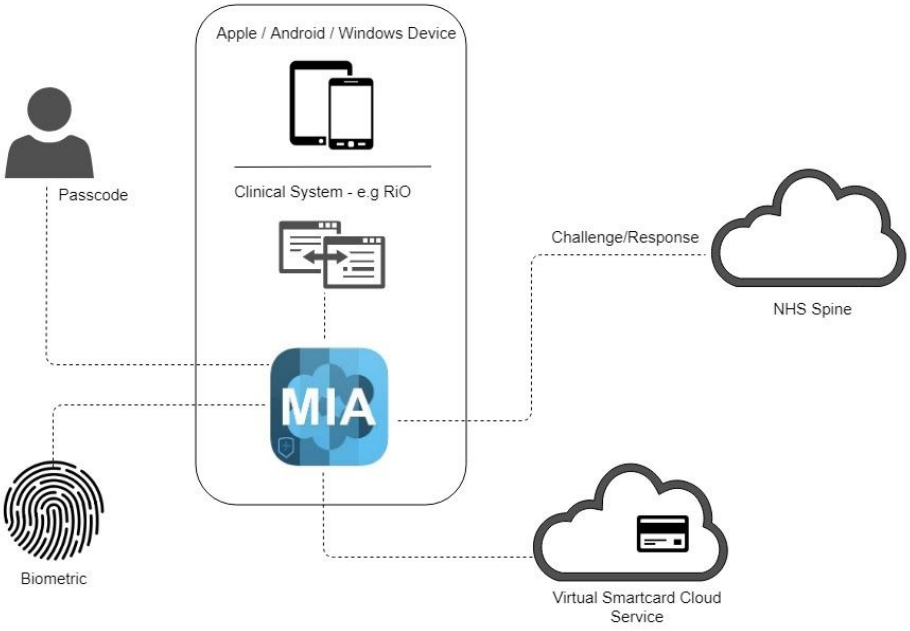
2.3.4 HR Card

When the user's Virtual Smartcard has been set up with an associated Authentication Method of their HR card, the user can simply tap their HR card on the attached RFID reader which will cause the Isosec Identity Agent to prompt the user for the Virtual Smartcard passcode. This is in much the same way as they would with their physical smartcard

Note that the card only needs to be tapped on the reader, it does not need to be in contact with the reader during the authentication process, unlike a physical smartcard.

2.4 MIA Mobile Platform

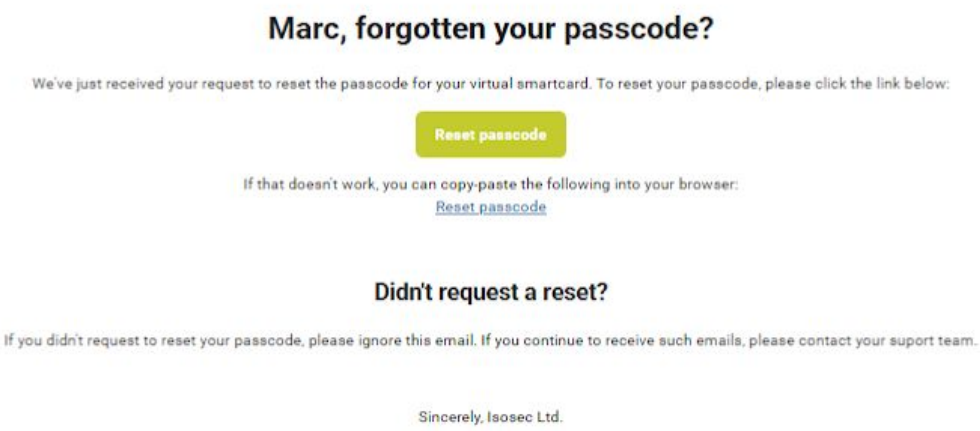
To authenticate with the MIA Mobile client, the user selects to authenticate with their Virtual Smartcard and is prompted to enter their passcode. If the device is capable of biometric authentication via fingerprint recognition, the user can use their fingerprint authentication in lieu of the passcode.



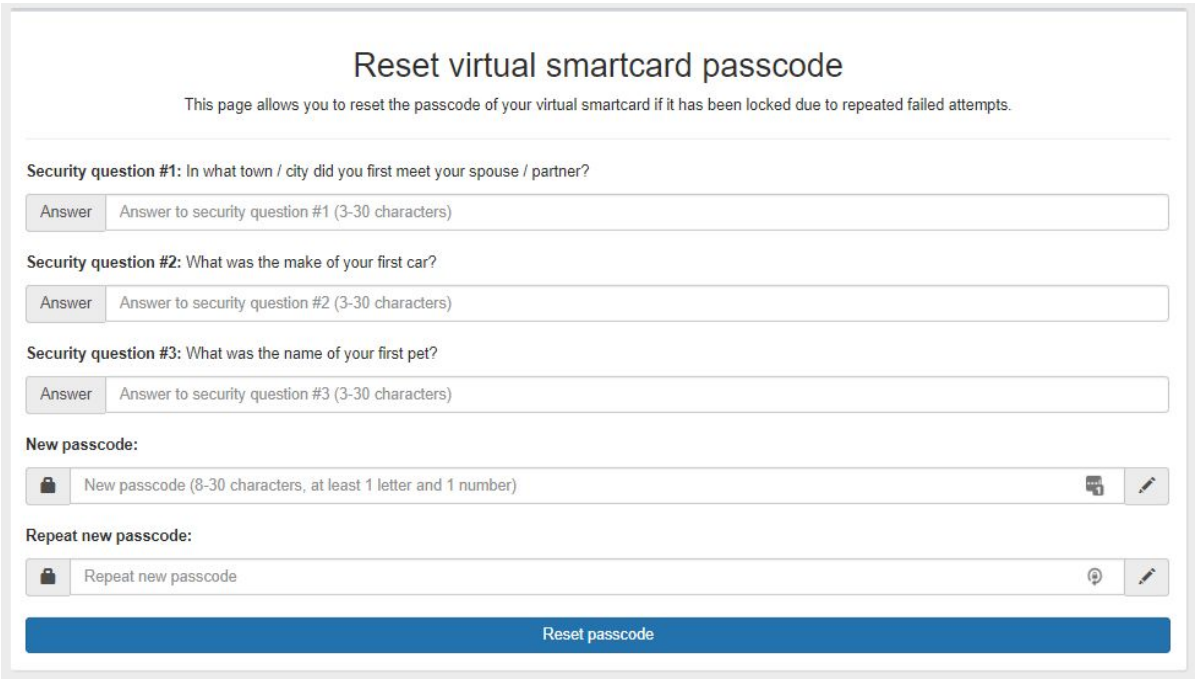
2.5 Virtual Smartcard Self-Service Portal

A user's Virtual Smartcard is protected by their passcode – if it is incorrectly entered three times the Virtual Smartcard is locked in the same way a physical card is.

To unlock the card, the user is automatically sent an email to their registered email account (specified at the user enrolment stage). This email contains a specific link to a Self-Service Portal:



When the user clicks on the link they are directed to the Self Service Portal and are required to enter correct answers to two out of three security questions (again specified at the user enrolment stage):



3. Data Model

The Virtual Smartcard service processes and stores a number of data items. All sensitive and secret information is protected as described in the security model section.

For the avoidance of doubt - no patient data is ever accessed or stored by the Virtual Smartcard cloud service.

3.1 Virtual Smartcard User Data

- Forename and Surname
- Email Address
- Contact Phone Number
- Subject Common Name (as registered in the Spine directory)
- User Certificates and Keys (Authentication and Content Commitment)
- Organisation Name

3.2 RA User Data

- Subject Common Name (as registered in the Spine directory)
- Organisation Name

3.3 Virtual Smartcard User Associated Device

- Device Name
- Platform (iOS / Android)
- Organisation Name
- Device Application (MIA, Isosec Authenticator)

3.4 User AD Data

- AD Account Domain and Name
- Organisation

3.5 Logging Data

- User or RA Identifier
- Organisation Name
- Timestamp
- Action

4. Security Model

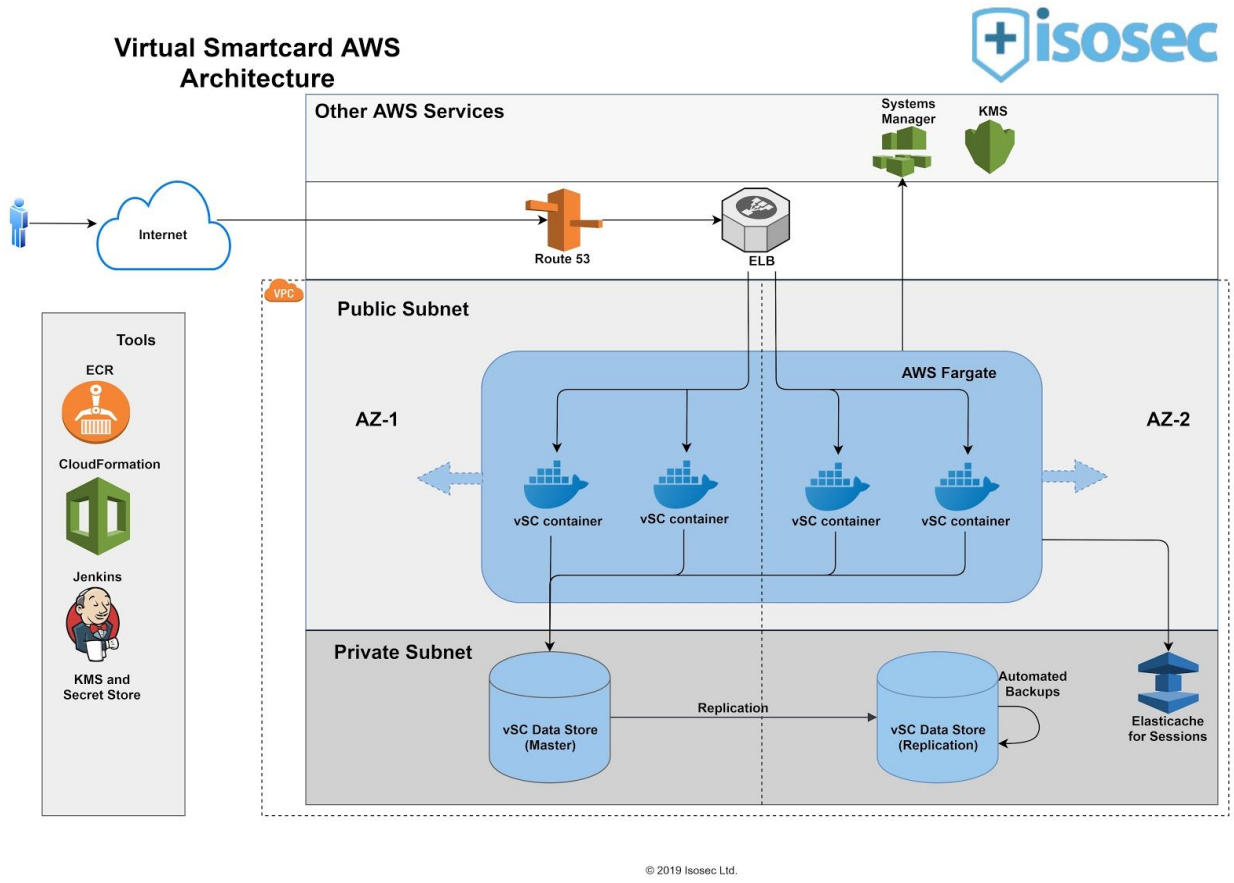
The two main security objectives are to:

1. Ensure that only the owner of the Virtual Smartcard can use it to authenticate to the Spine
2. Protect the Virtual Smartcard service (namely the Virtual Smartcard keys in the database) from an attacker.

The Virtual Smartcard security model is multi-layered and uses different protection measures to ensure the integrity of the Virtual Smartcard service, each of which are described in the following sections:

1. Amazon Web Services (AWS) Cloud Deployment
2. AIMES Cloud Provider
3. Hardened Ubuntu Host
4. Docker Containerisation
5. Database Protection
6. Virtual Smartcard User Key Encryption
7. Virtual Smartcard User Key Scope Protection
8. 2 Factor Authentication
9. Auditing
10. Virtual Smartcard Locking
11. Virtual Smartcard Unlocking
12. Data in Transit Protection
13. Secure Development Practices

4.1 Amazon Web Services (AWS) Cloud Deployment



The Virtual Smartcard service is hosted on AWS. This service allows access only to whitelisted organisations and hence blocks traffic coming from unknown hosts. It leverages different services such as AWS Fargate, RDS, Route 53, KMS, Parameter Store, Elasticache and EC2 instances for connecting to AIMES VMs for SPINE ticket validation. The secrets are protected using KMS encryption, with alerts in place for all access which provides access visibility and security for sensitive data. RDS instances are hosted inside a VPC in a private subnet hence providing access to only Fargate docker containers.

More information about AWS ISO accreditations could be found at:
https://aws.amazon.com/compliance/iso-certified/.

4.2 AIMES Cloud Provider

The Virtual Smartcard cloud service (AWS) uses the Spine ticket validation service hosted within the AIMES datacenter. The AIMES datacenter is used for providing N3/HSCN connectivity to the services hosted on AWS. AIMES are almost exclusively focused on the healthcare market, and

have obtained accreditations such as the NHS IG Toolkit and ISO27001:2013, as well as adhering to best cloud security practices.

In addition, AIMES conforms with:

- ISO27017:2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services

- ISO27018:2014 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

In addition, a 2FA secured VPN connection is required in order for Isosec to access the service.

4.3 Hardened Ubuntu Host

The Spine ticket validation service is hosted on Ubuntu 18 LTS operating systems inside of virtual machines as an immutable infrastructure platform. This has been hardened with all unnecessary account access removed .

Automatic updates are in place for security-related items relating to packages in use - Ubuntu itself, Docker, OpenSSL, PHP.

Additionally, tripwires are used within the Ubuntu system to detect access – a security notification is sent to Isosec which is logged.

4.4 Docker Containerisation

Within the AWS Fargate Cluster, Docker containerisation is used for the Virtual Smartcard service. These containers are built using an automated Jenkins pipeline and tested on multiple environments before pushing them out to any live environments.

The Virtual Smartcard service only has certain interfaces made available by Docker, with all other aspects also being inaccessible from outside of this environment.

4.5 Data Protection

The Virtual Smartcard database is deployed on an AWS RDS instance and has UK multi-AZ replication turned on for high availability. This RDS instance hosts data for all organisations, isolated inside it. This meets the functional requirement to enable a user's Virtual Smartcard to be used in different NHS organisations in much the same way a physical smartcard can.

The scope visible via the vRA Manager limits the RA to viewing only the associated Authentication Methods and details to the particular NHS organisation that both the RA and Virtual Smartcard belong to.

4.6 Virtual Smartcard User Key Protection

Each Virtual Smartcard's private key is encrypted using the user's passcode, which is an enforced strong passcode meeting a minimum quality standard. In addition, each encrypted Virtual Smartcard private key is also re-encrypted using the Virtual Smartcard service AES and RSA keys. These AES and RSA keys are split and stored in AWS Parameter Store and encrypted using KMS keys; access to KMS keys on AWS is restricted with no one person having access to all parts of the split keys.

4.7 Virtual Smartcard User Key Scope

A Virtual Smartcard private key is never in the possession of the user. Instead, it is held securely in the Virtual Smartcard database with only indirect access – the key never leaves the Virtual Smartcard service, it can only be used by the Virtual Smartcard cloud service to carry out cryptographic operations on the Virtual Smartcard service itself. All keying materials are deleted immediately and securely after use.

4.8 2F Authentication

When used with the Authenticator app and the strong passcode this provides 2F authentication.

4.9 Auditing

It is assumed that for the purposes of the wider Spine auditing that the Spine itself and Spine applications are responsible for secure audits. The reasoning behind this is that the Virtual Smartcard service has the same role and responsibility as a physical smartcard which in itself does not store any audit information, securely or otherwise.

However, audit information is held within the Virtual Smartcard service which is accessible by the RA using the vRA Manager. This audit information is held in line with the Isosec GDPR statement located at https://isosec.co.uk/data-processing/.

Each use of a Virtual Smartcard to authenticate to the Spine creates an audit message with full details of the user and the Virtual Smartcard including the success or failure (and failure reasons, such as an incorrect passcode).

4.10 Virtual Smartcard Locking

In order to decrypt the Virtual Smartcard private key, the correct strong passcode must be supplied. If the incorrect passcode is supplied three times in a row, this locks the Virtual Smartcard. This will trigger an email to be sent to the enrolled user's email account containing a single use, time-limited link which the user is required to visit in order to unlock the Virtual Smartcard.

The use of an email upon locking also serves the purpose of notifying an attempt by an unauthorised user to access the user's Virtual Smartcard.

4.11 Virtual Smartcard Unlocking

In order to unlock a locked Virtual Smartcard, the user must visit the link contained in the email. This will open a page requiring the answers to two out of three security questions which form a decryption key to recover the user's Virtual Smartcard key. A new strong passcode can then be set.

4.12 Data In Transit Protection

All data transferred between the Virtual Smartcard service and clients (such as between the Isosec Identity Agent and Virtual Smartcard Authenticator) is encrypted using a combination of RSA and AES keys. All clients encrypt data to be sent to the Virtual Smartcard service using an AES key, the AES key itself being encrypted using the Virtual Smartcard service RSA certificate. The resulting encrypted blob of data is sent to the Virtual Smartcard service using HTTPS. The Virtual Smartcard server encrypts all the data sent to the client using the provided AES key.

4.13 Secure Development Practices

Secure coding practices are used as standard throughout Isosec on all products.
This includes:

- Architect, design and development using defence in depth
- Peer review of all software designs and code

- Use of the latest development tool versions
- Use of the latest library versions (e.g. OpenSSL)
- Use of SHA256, AES256 and RSA2048 as a minimum
- Securely deleting all keying materials and sensitive data after use
- Removal of all compiler warnings