advanced

Software Powered Possibility

Service Definition

Isosec Virtual Smartcard Service

G-Cloud 13

Contact Information

We would welcome any enquiries regarding this document and its content. Please contact:

Bid Management
Sales Enablement

Email:
bidmanagementteam@oneadvanced.com

Telephone: +44(0) 330 343 4000

www.oneadvanced.com

Contents

Service Overview

1. Introduction

Virtual Smartcard is a revolutionary authentication solution that addresses a number of issues with the whole lifecycle of physical smartcards within the NHS.

In February 2021, Isosec gained accreditation from NHS Digital under the Virtual Smartcard framework - further details can be found here:

https://digital.nhs.uk/coronavirus/access-logistics-hub/coronavirus-smartcards/isosec-virtual-smartcard

The accreditation covers the use of Virtual Smartcards for the purpose of authenticating to the Spine and accessing clinical applications.

Isosec is currently undergoing a further accreditation with NHS Digital to approve the use of Virtual Smartcards for e-prescribing digital signing, with Advanced Electronic Signature (or AdES for short).

Isosec has filed a patent application to cover key aspects of its 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).

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:

- Download the Virtual Smartcard brochures, demos and case studies in our Resources Library: https://isosec.co.uk/resource-library/
- Access our Support Hub for all technical documentation, prerequisites and guides: https://help.isosec.co.uk

2. Virtual Smartcard Technical Solution

The principle of Virtual Smartcard is to virtualise the physical NHS smartcard such that it works with, and is 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 as to whether a physical or Virtual Smartcard is used. As such both physical and Virtual Smartcards can coexist in the estate of an NHS organisation. A user can have both a physical and Virtual Smartcard which use the same unique identity held within the Care Identity Service (CIS). Virtual Smartcards can be used for Spine authentication and also for e-prescribing.

2.0 iO Identity Agent

iO is a high performance Identity Agent (IA) purpose built for the NHS, which can be used with both physical and Virtual Smartcards. This simply replaces the NHS IA in environments where either physical or Virtual Smartcards are being used for both users and Registration Authorities.

As an example, from a Windows desktop, a user can either use their existing physical smartcard to authenticate using the iO Identity Agent or with their Virtual Smartcard (associated with their AD account) and the Isosec Authenticator app.

2.1 RA Issuance Components

RA issuance components are installed for a Registration Authority (RA) using the "Advanced" option on the iO Identity Agent installer. An RA is required to have the appropriate RA roles and permissions to create smartcards.

2.2 Network Requirements

To use the Virtual Smartcard service, the following URLs will need to be accessible from both the RA workstation and end user machine.

Isosec recommends whitelisting these addresses by DNS name where possible to protect against an unlikely IP address change. Further, the DNS names are protected via DNSSEC. In the case where it is not possible to use DNS names, please use the IP addresses (as a last resort).

URL	Network	Port	Protocol	Alternative IP Address
vsc.isosec.co.uk	Internet	80 & 443	HTTPS	13.248.130.26 & 76.223.5.80
audit.isosec.co.uk	Internet	80 & 443	HTTPS	3.33.254.85
ar1.isosec.co.uk	Internet	80 & 443	HTTPS	15.197.244.35
ar2.isosec.co.uk	Internet	80 & 443	HTTPS	15.197.244.35
audittest.isosec.co.uk	Internet	80 & 443	HTTPS	3.33.147.82
test-ar1.isosec.co.uk	Internet	80 & 443	HTTPS	15.197.152.12
licensing.isosec.co.uk	Internet	80 & 443	HTTPS	148.252.244.102
logging.isosec.co.uk	Internet	8, 443	HTTPS	148.252.244.102

For both the RA workstation and End-User machines, you must route the traffic to our cloud service via the N3/HSCN network and provide us with the CIDR range for the N3/HSCN network; your network provider should be able to assist you with this.

Isosec uses AWS WAF to whitelist your organisation under the provided CIDR ranges.

If the NHS organisation uses a cloud VDI desktop solution and is unable to route all the internet traffic through a N3/HSCN VPN setup, you must set up a proxy with a static IP address and route the traffic from your VDI to the Virtual Smartcard service through this proxy. This static IP address will need to be provided to Isosec so it can be whitelisted on the service.

It's key to also note that clinical End-User machines require N3/HSCN connectivity in almost all cases to be able to access clinical systems. Where user machines sit outside the NHS organisation internal network, a VPN connection is required to be able to route traffic for Spine authentication and clinical system access.

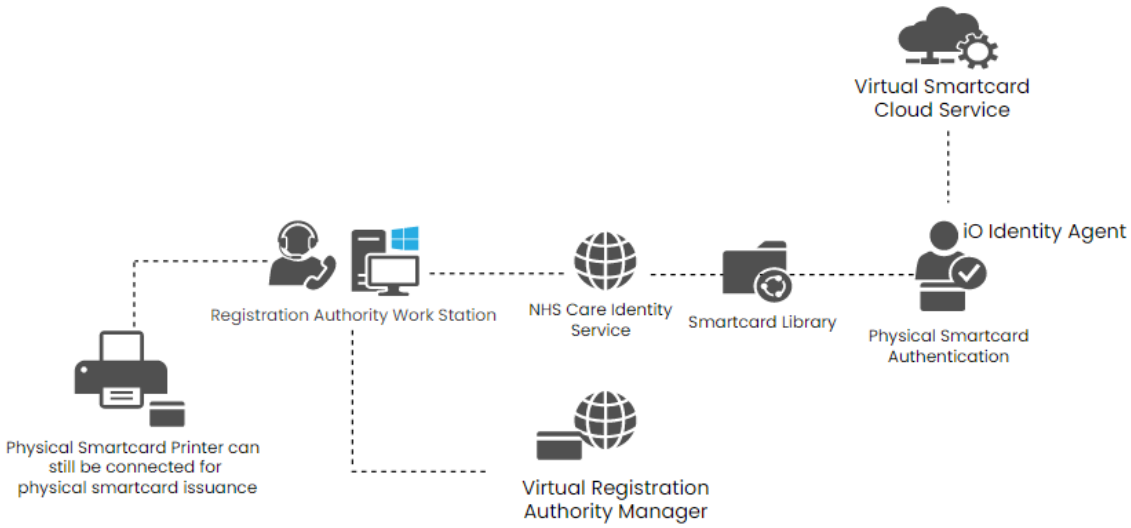
The Isosec Authenticator app simply requires public internet access - no additional network settings are required.

2.3 RA Installation Preparation

The process to issue a Virtual Smartcard is exactly the same as a physical smartcard, except for the last stages, where rather than a physical smartcard emerging from a smartcard printer, a Virtual Smartcard is created in the Virtual Smartcard cloud service and where the Virtual Smartcard keys are held and protected on a mobile device using the Isosec Authenticator app. A Virtual Smartcard never leaves the Virtual Smartcard cloud service – it is only ever managed or used from within the cloud service.

Specifically, the user must be registered in CIS 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:

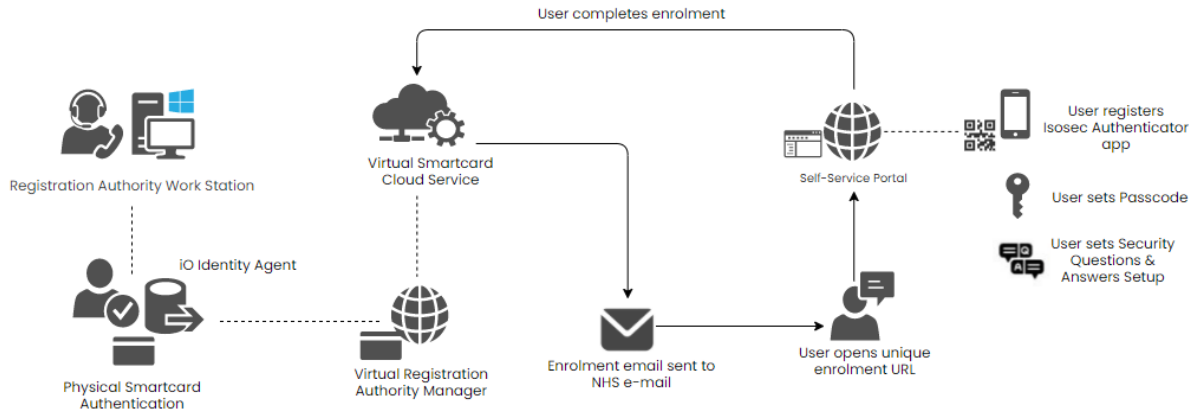


On an RA Workstation, the RA Issuance components are installed which enables the NHS CIS application to connect to the Virtual Smartcard cloud service. This essentially provides a Virtual Smartcard interface that the NHS CIS uses to interact with the Virtual Smartcard service.

2.4 VRA Management

The vRA Manager (a web application and part of the Virtual Smartcard cloud service) enables RAs to enrol and manage Virtual Smartcards. To begin the enrolment, an RA user must enter the NHS email address of the user receiving a Virtual Smartcard. This process will initiate the Self-Setup enrolment email which the user will need to complete before a Virtual Smartcard can be issued via CIS.

Overview of the Isosec VSC solution – How users are enrolled



2.4.1 User Enrolment

The user enrols for the Virtual Smartcard service using a unique Isosec Virtual Smartcard enrolment link sent to the user's registered email address. The link will redirect the user to a browser based enrolment form and instruct them to download and register the Isosec Authenticator app.

2.4.2 Device Registration

During the enrolment process, the user downloads the Isosec Authenticator mobile app (via Apple App Store or Google Play) onto their mobile device– This app is used for two factor authentication and to sign EPS prescriptions.

Using the Authenticator app, the user scans a fresh QR code generated on the browser based enrolment form to begin their device registration and sets up their Authenticator app PIN. The Authenticator PIN is later used to authorise authentication signing requests and e-prescription signing requests.

If the device being used supports biometrics (FaceID or Fingerprint) then this can be utilised as the main method to authorise authentication signing requests and e-prescription signing requests.

Once the device has been successfully registered, the user is required to return back to the browser based enrolment form to set their passcode along with three security questions and answers.

2.4.3 Passcode & Security Questions/Answers

To finalise the enrolment process, the user is required to set up the following on the browser based enrolment form.

- Strong Virtual Smartcard passcode (complexity organisation dependent)
- Three security questions & answers which can be used to unlock the account via the Self-Service Portal or Isosec Authenticator app Account Recovery, when required.

Once this process has been completed, the user's Authenticator mobile app will be sat in a "Pending Virtual Smartcard" state ready for a Virtual Smartcard to be issued by an RA.

2.5 Issuance

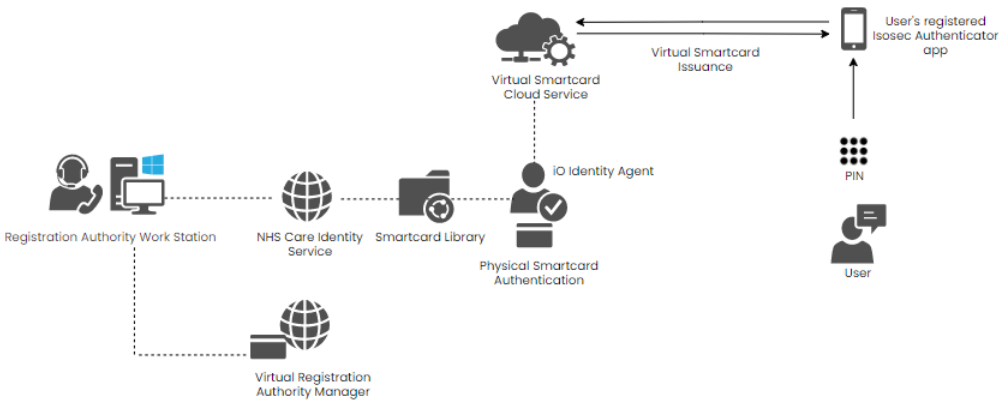
After completing enrolment, the user's account will appear in the vRA Manager with a "Ready for issuance" status. A Registration Authority (RA) locates the user to whom a Virtual Smartcard needs to be issued via Care Identity Service (CIS) and initiates the vSC issuance process.

The user to whom the Virtual Smartcard is being issued receives a push notification onto their registered device that has the Isosec Authenticator mobile app installed, and authorises the push notification requesting the VSC issuance onto their Isosec Authenticator app by supplying their Authenticator PIN within the Isosec Authenticator app.

The VSC issuance proceeds once the push notification has been accepted with a valid Authenticator app PIN and a VSC is fully issued to the user's Isosec Authenticator app. During the VSC issuance process both an authentication signing key and an e-prescription signing key are created on the user's Authenticator app.

Once a Virtual Smartcard has been created, an RA can manage the user from within the "Enrolled User" section of the vRA Manager.

Overview of the Isosec VSC solution – How users are issued a Virtual Smartcard



2.5.1 Authentication Association

For the authentication association, the RA selects the user's Virtual Smartcard and can associate it with one or more of the following methods of authentication. To note, user's can associate and manage their own devices via the Self-Service Portal.

2.5.2 AD Association

The user's Window AD domain and account name are associated within the vRA Manager. Note, this is just simply an association - no actual connection is required between the Virtual Smartcard cloud service and the NHS organisation's Active Directory or domain.

2.5.3 Isosec 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.

This device is associated with the user's Virtual Smartcard during the enrolment process by scanning a QR code and creating an authorisation PIN. Further, the Isosec Authenticator mobile app is used to authorise authentication to the Spine and sign e-prescriptions.

2.5.4 MIA (Mobile Information Access)

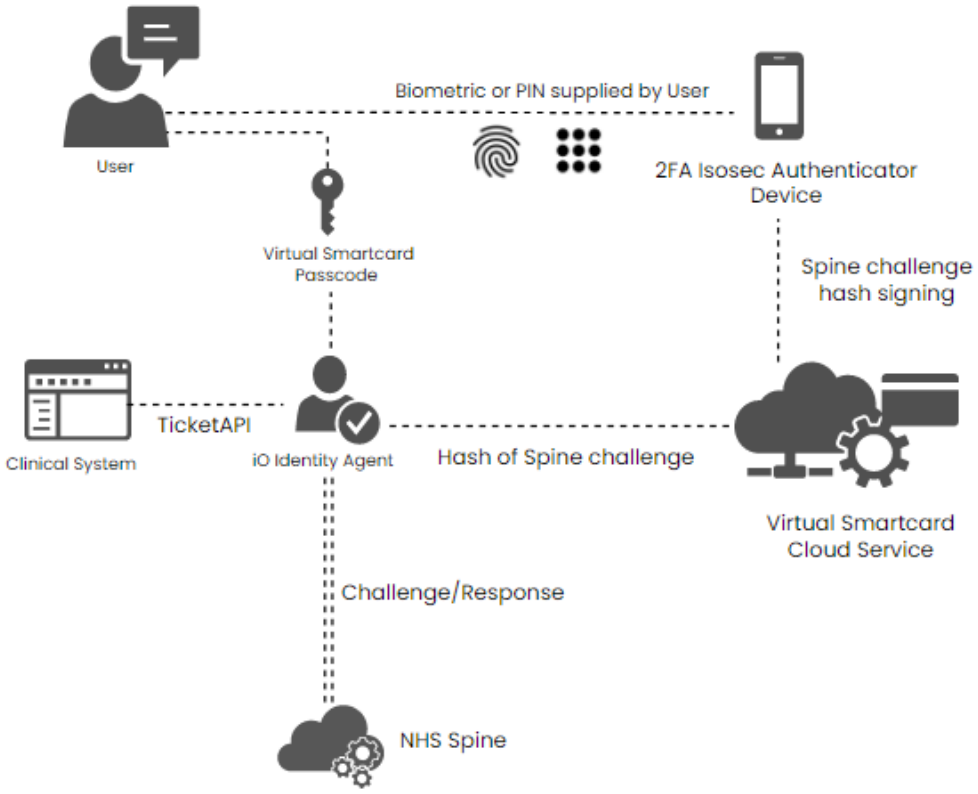
The iOS MIA app can be installed from the relevant application store, and the user's device can then be associated with their Virtual Smartcard by scanning a QR code displayed in the vRA Manager or Self-Service Portal, and the user then entering their Virtual Smartcard passcode in the app.

3. User Authentication

The user can authenticate to a desired clinical workspace on a desktop using Isosec's Identity Agent (an identity agent for windows desktops) either by providing their NHS email + Virtual Smartcard passcode, or if the user's NHS Windows account is associated with the user's Virtual Smartcard, the user will only be prompted to provide their Virtual Smartcard passcode. By providing a correct Virtual Smartcard passcode, a push notification requesting to sign an authentication challenge is automatically sent onto the user's mobile device (the user's registered device that has a VSC issued onto the Isosec Authenticator app). The user taps on the received push notification which opens the Isosec Authenticator app, and authorises the push notification by providing their Authenticator app PIN or biometry.

The process of authentication using a Virtual Smartcard is by design, simple and easy.

Overview of the Isosec VSC solution – How users authenticate with a Virtual Smartcard

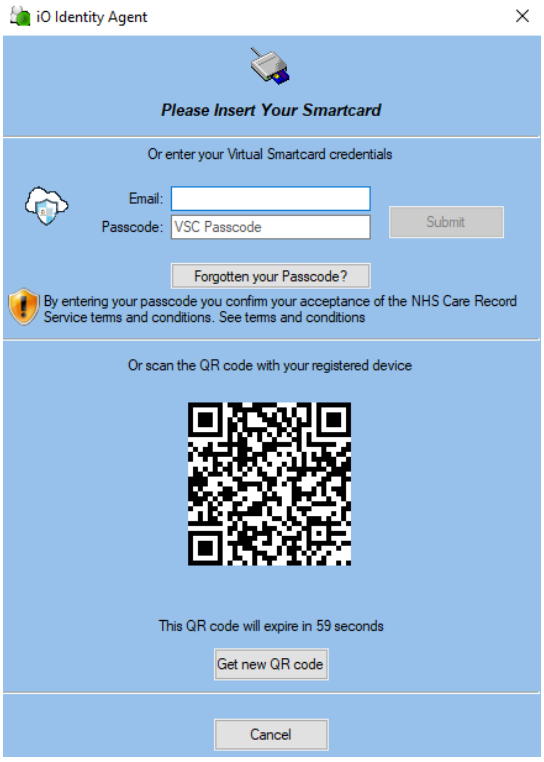


In all cases, the user is required to authorise the authentication using their Authenticator app by either entering the PIN or biometric as described above.

The following sections describe how each of the associated authentication methods are used to authenticate on a Windows PC using a Virtual Smartcard.

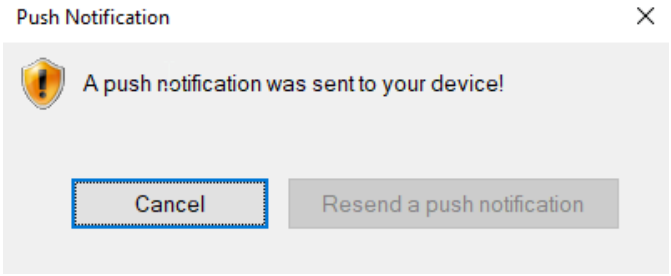
3.1 Generic Windows AD Authentication

In the case where users don't have a named Windows AD account associated with their Virtual Smartcard, whenever a user initiates authentication via the Isosec Identity Agent or launches a Spine enabled application (as there is no physical card to initiate authentication) the following dialogue is presented to the user:

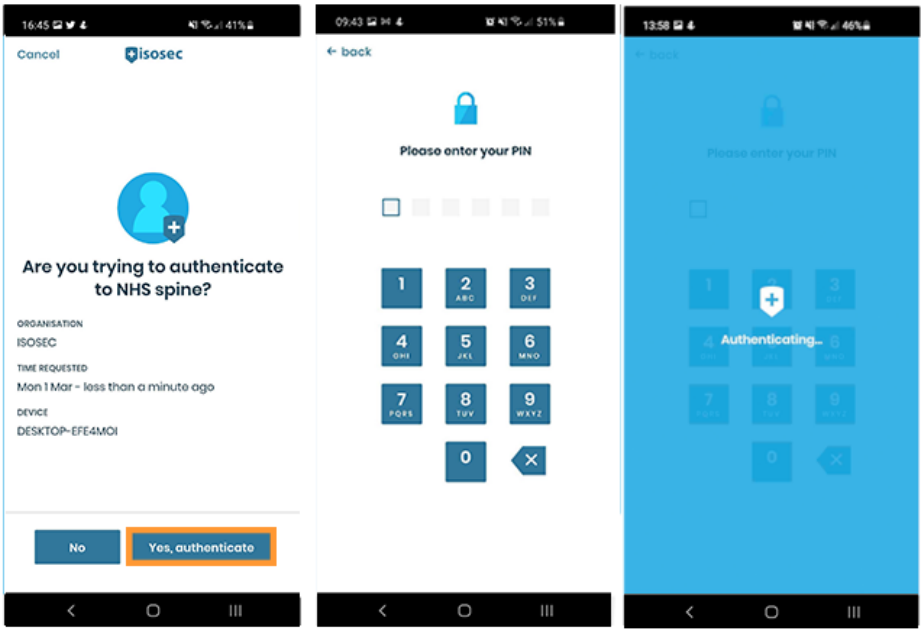


Here, the user can enter their Virtual Smartcard associated email address together with their Virtual Smartcard passcode.

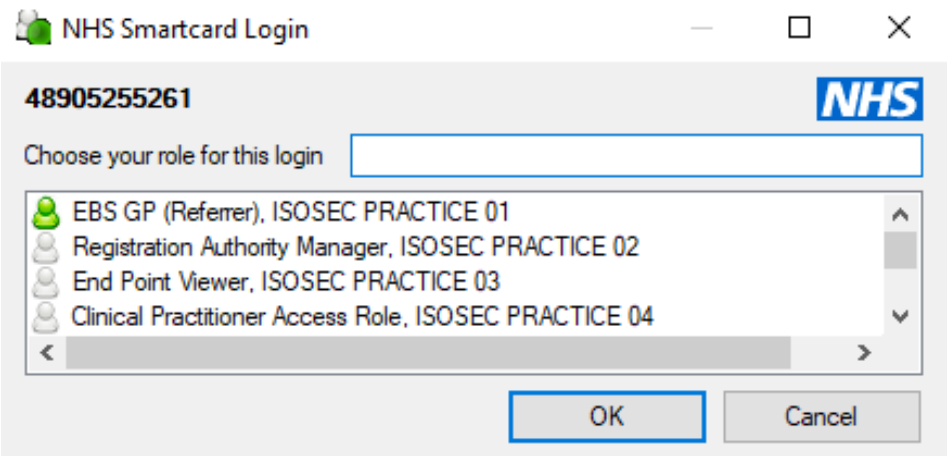
After entering the correct Virtual Smartcard passcode, the user's registered device (which has an issued VSC onto their Isosec Authenticator app) will be sent a push notification - The user will see the following dialogue displayed on a Windows PC:



Simultaneously, in the Authenticator app, the user will be presented with the following push notification and will be asked for their Authenticator app PIN or biometrics to authorise the authentication.



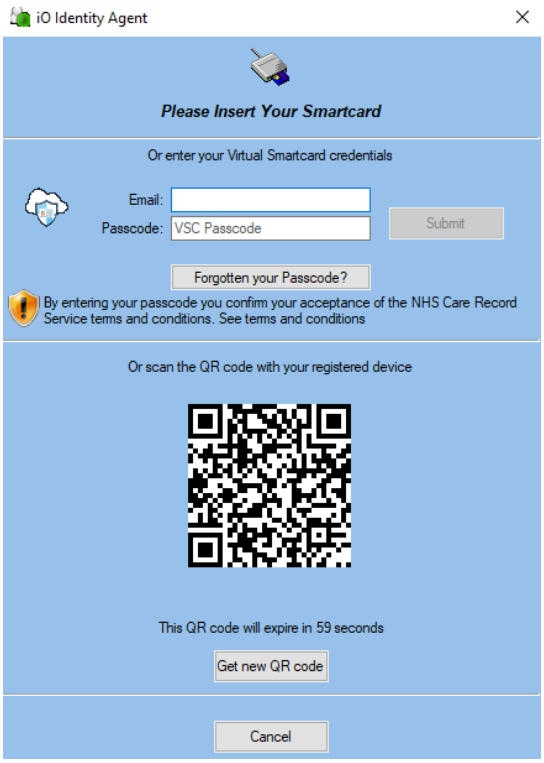
After the authorisation of the push notification on the mobile device by the user, the Spine challenge is signed by the user's authentication signing key of the Virtual Smartcard. Once complete, the Isosec Identity Agent (running on the Windows desktop) will present the user with a list of their Spine roles.



In cases where the user only has one Spine role, the Spine role is automatically selected by the Isosec Identity Agent. In case the user has multiple Spine roles, the user must select a desired Spine role and confirm the selection. In case the user has multiple Spine roles, the user must select a desired Spine role and confirm the selection.

3.2 QR Code Authentication

From the "Generic AD Windows Authentication" login window, user's are presented with a QR code authentication method as an alternative to entering their registered email address and Virtual Smartcard passcode.



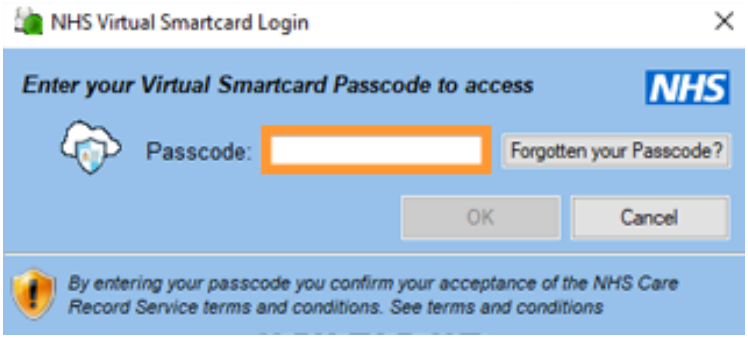
To authenticate using the QR code method, the user can simply select the “QR Code Scan” option in the Authenticator app to scan the presented QR code using their registered device's camera and when prompted, enter their Authenticator app PIN or biometrics to authorise the authentication.

Once complete, the Isosec Identity Agent (running on the Windows desktop) will present the user with a list of their Spine roles as described in Section 3.1.

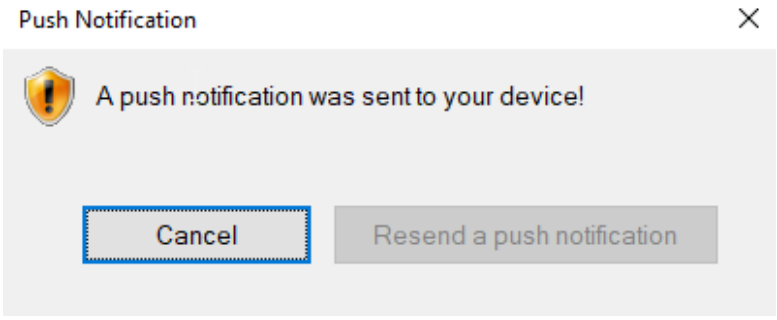
The QR code presented to the user is only valid for 60 seconds and upon expiry, the user must generate a new one using the “Get new QR code” button from the Isosec Identity Agent logon prompt.

3.3 AD Associated Virtual Smartcard

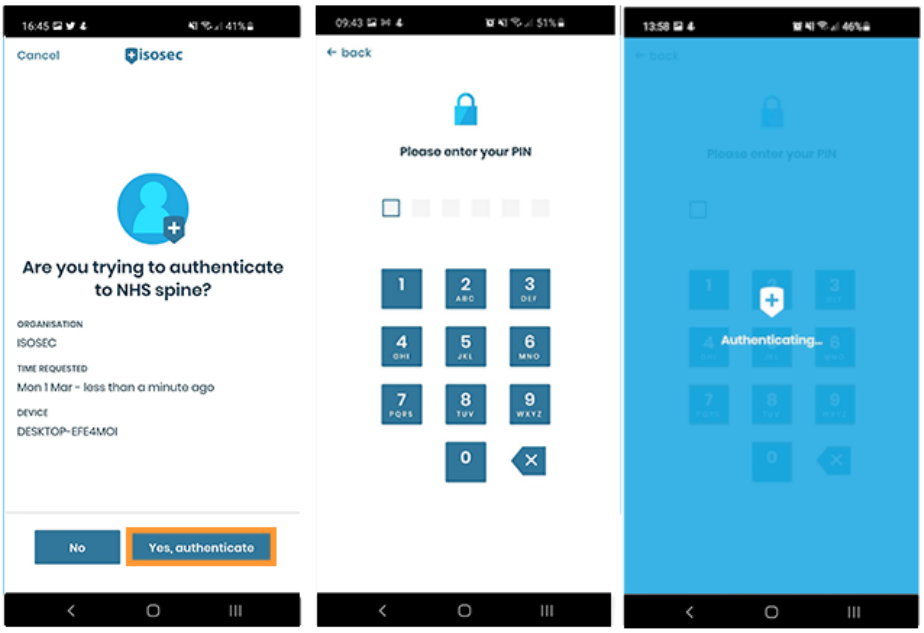
When a user’s Virtual Smartcard is associated with their AD account by a Registration Authority, the user will see the following dialogue displayed on a Windows PC when authenticating:



After entering the correct Virtual Smartcard passcode, the user's registered device that has a VSC issued onto the Isosec Authenticator app will be sent a push notification - The user will see the following dialogue displayed on a Windows PC:



Simultaneously, in the Authenticator app, the user will be presented with the following push notification and be asked for their Authenticator app PIN or biometrics to authorise the authentication.

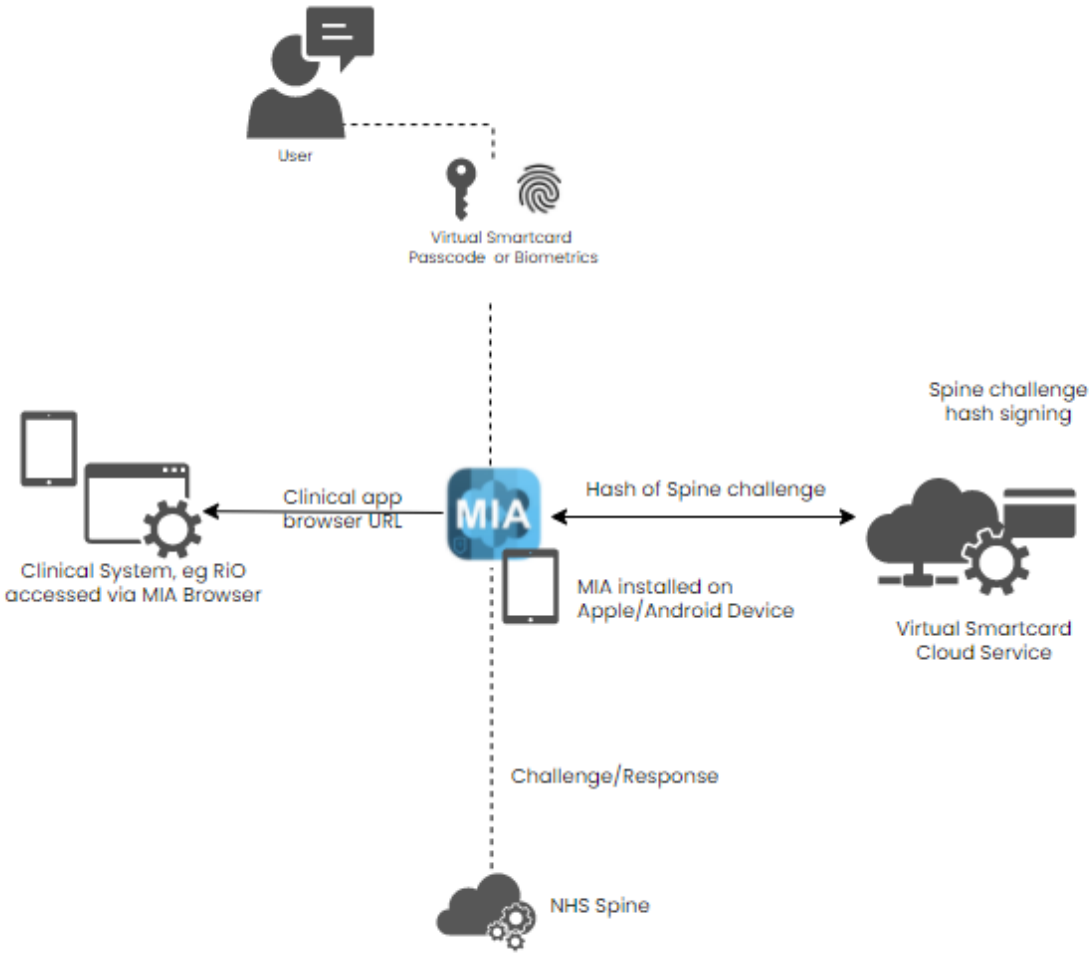


Once complete, the Isosec Identity Agent (running on the Windows desktop) will present the user with a list of their Spine roles as described in Section 3.1.

3.4 MIA (Mobile Information Access)

To authenticate in the MIA client, the user selects to authenticate with their Virtual Smartcard and is prompted to enter their passcode or biometric (if registered).

Once authenticated, the user is directed to the clinical system, such as RiO or a Portal landing page defined within the organisations MIA configuration.



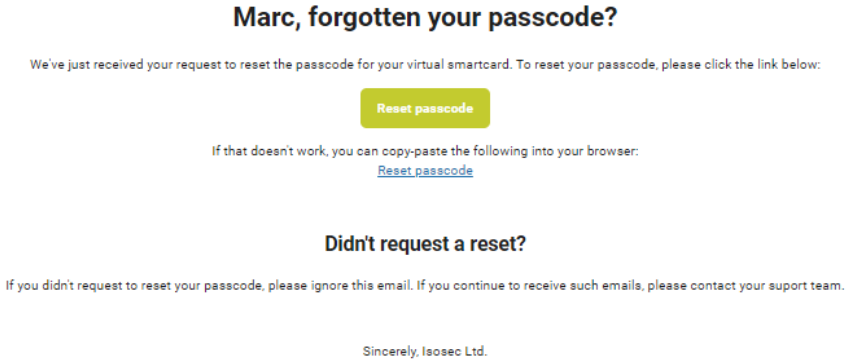
3.4 Virtual Smartcard Self-Service Portal

The Self-Service Portal can be accessed via the iO Identity Agent menu, allowing a user to manage their own Virtual Smartcard. Logging into the Self-Service Portal requires a combination of email address, passcode and a registered two-factor method such as the Authenticator mobile app or a mobile phone SMS.

3.5 Virtual Smartcard Passcode Reset

A user's Virtual Smartcard is protected by their passcode and Authenticator app PIN – if the passcode 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) which contains a unique reset link.



When the user clicks on the unique link they are directed to the Self-Service Portal and must enter correct answers to two out of three security questions (again specified at the user enrolment stage) before a new Virtual Smartcard passcode can be entered.

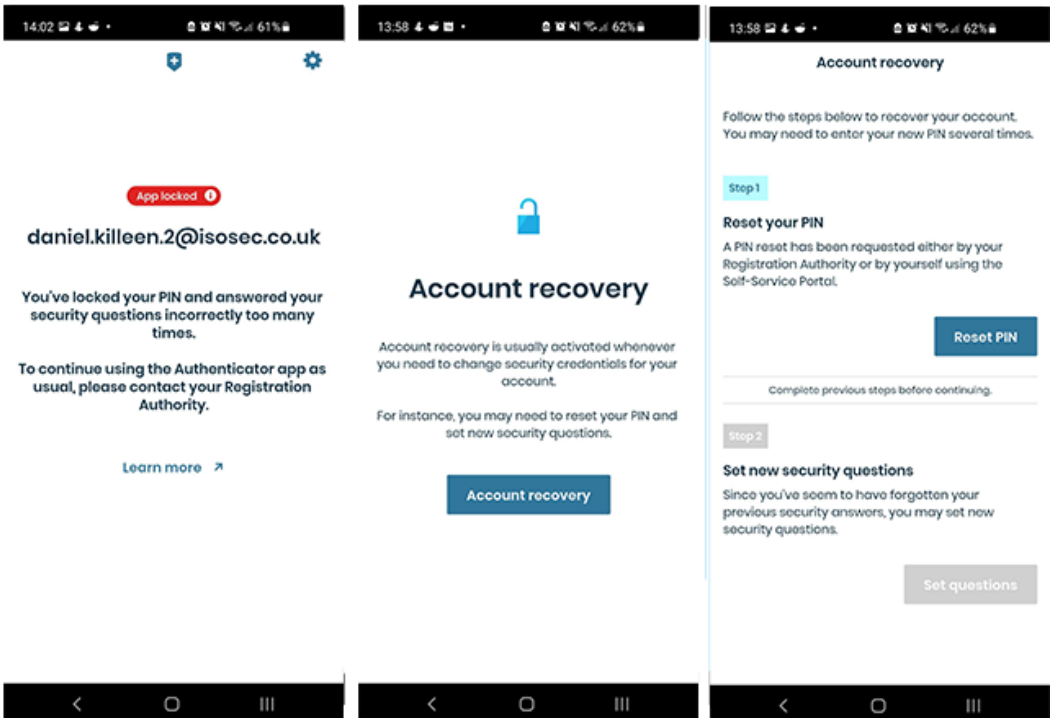
To finalise the reset, the user must accept a push notification on the Authenticator app, presenting their Authenticator app PIN or biometric to authorise the Virtual Smartcard passcode reset.

3.6 Authenticator App PIN Reset & Account Recovery

A user's Authenticator app is protected by their Authenticator app PIN and/or biometrics (if registered) – If the Authenticator app PIN is incorrectly entered five times, the Authenticator app is placed into a "PIN locked" state.

To unlock their Authenticator app PIN, the user must go through the reset process from within the app, using their three security questions and answers (created at the user enrolment stage) to set a new Authenticator app PIN and if required, re-register a biometric.

If the security questions/answers are incorrectly entered five times, the Authenticator mobile app will be placed into an “App locked” state. An RA user will need to initiate the Account Recovery process from the vRA Manager enabling the user to reset both their Authenticator app PIN and security questions and answers. Once reset, the user can once again use their Authenticator app PIN or registered biometric to authorise authentication to the Spine and sign e-prescriptions.



4. ePrescribing

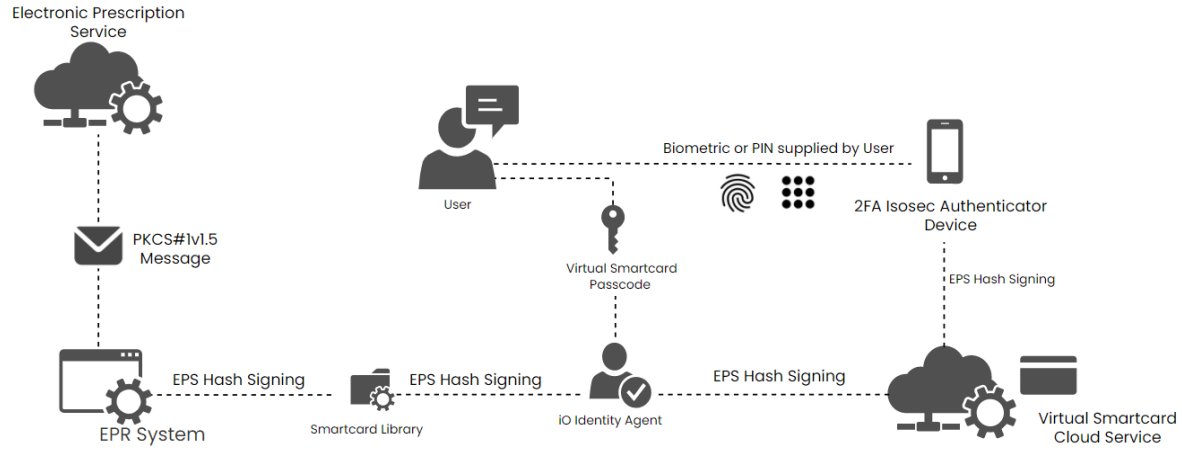
4.1 Clinical Prescribing Applications

A Virtual Smartcard can be used to sign e-prescriptions in a clinical prescribing system in a completely transparent manner. This works through the iO identity agent which presents a virtualised smartcard reader and the user’s virtualised smartcard in this reader on a Windows based machine.

From a technical perspective, a Virtual Smartcard can be presented as a Series 6 or Series 8 card and provides both a PKCS#11 and Cryptoki interface. This means that the clinical prescribing system will work as normal when signing e-prescriptions.

The user / clinician must first authenticate into a clinical workspace / IT Systems/ EPR system using their Virtual Smartcard passcode and Authenticator app. If the ePR system offers the means of prescribing, the user can prescribe medication to patients using the system itself. For issuing an e-prescription (EPS), the user must follow the steps mandated by the EPR system itself to formulate an e-prescription which can be then digitally signed

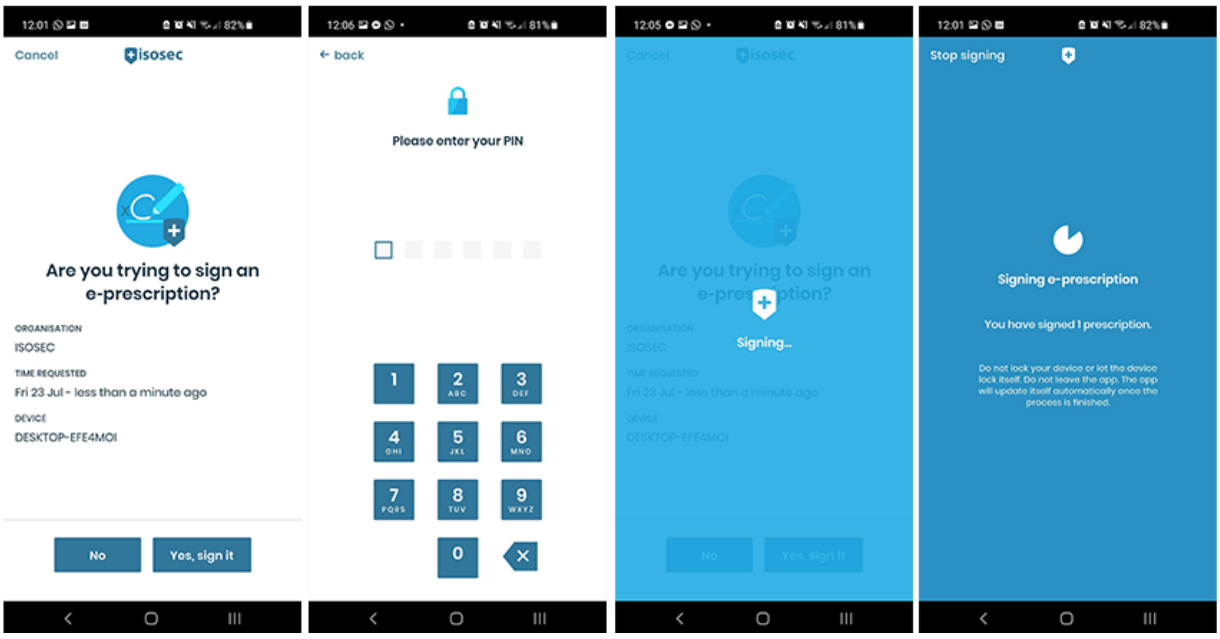
by the user's EPS signing key. Isosec's Virtual Smartcard is involved in signing the e-prescription itself, the process of issuing and signing the EPS is as follow:



4.2 Isosec Authenticator App

During the e-prescribing process, the EPR system will ask the user to Sign the e-prescription. In order to do that, the user must submit their VSC Passcode when prompted. By submitting a correct VSC passcode, a hash of the e-prescription is created and submitted by the EPR system to the smartcard library used by the EPR system, this hash is used for signing using the user's EPS signing key of the user's Virtual Smartcard.

A push notification requesting an EPS hash signing operation is automatically sent onto the user's mobile device (the device that has a VSC issued onto their Isosec Authenticator app). The user taps on the received push notification which opens the Isosec Authenticator app, and authorises the push notification by providing their Authenticator app PIN or biometry. As the e-prescription is signed, a timer will be displayed on the user's Authenticator app.



After the authorisation of the push notification on the mobile device by the user, a digital signature of the hash is created on the mobile device within the Isosec Authenticator mobile app itself, and the digital signature itself is sent back to the EPR system.

The EPR system receives the digital signature, at this point the EPR system will check the validity of the digital signature of the hash using the user's signing certificate. The EPR system uses the digital signature to formulate a PKCS#1v1.5 object representing the e-prescription itself, and submits this object to an EPS service.

The Authenticator app can also bulk sign e-prescriptions provided this functionality is available through the chosen EPR system. This means that after the user has authorised the initial e-prescription in the Authenticator app, the user will only be prompted to authorise again as part of the bulk signing in the event that:

- 250 consecutive e-prescriptions i.e. the 251st prescription
- A gap between e-prescription signing of more than 15 seconds

5. 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.

5.1 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

5.2 RA User Data

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

5.3 Virtual Smartcard User Associated Device

- Device Name
- Platform (iOS / Android)
- Organisation Name

- Device Application (MIA, Isosec Authenticator)

5.4 User AD Data

- AD Account Domain and Name
- Organisation

5.5 Logging Data

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

6. Security Model

The two main security objectives are to:

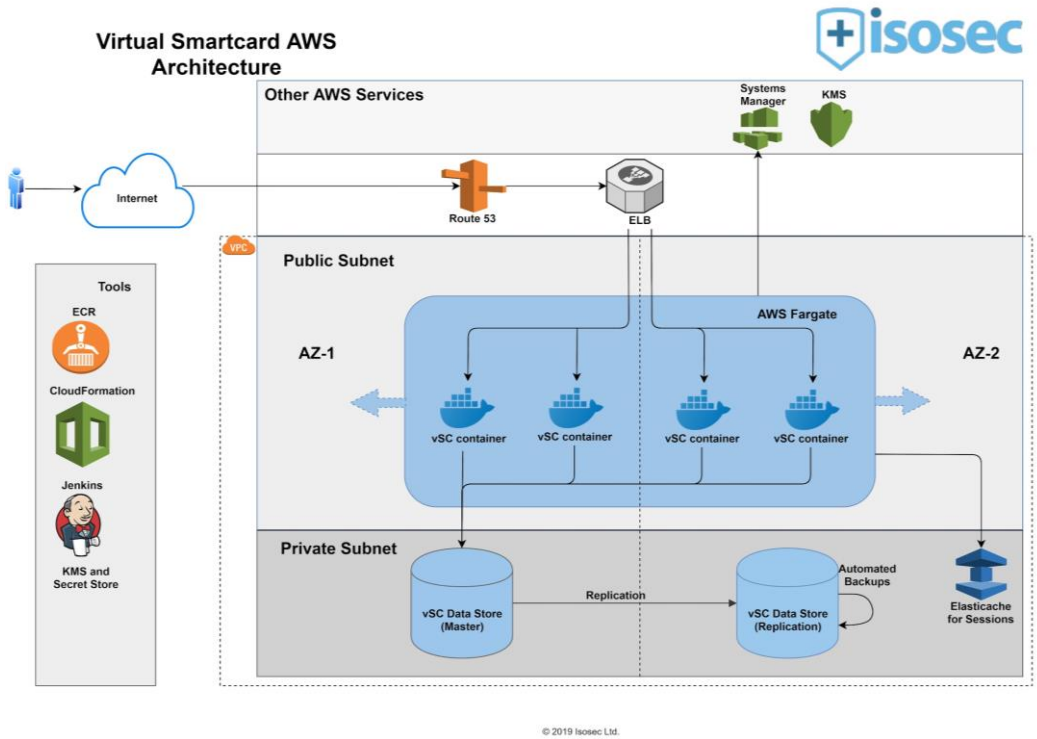
1. Ensure that the Virtual Smartcard service provides an Advanced Electronic Signature, namely the signature is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control
2. To resist and protect the Virtual Smartcard service as a whole 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.

The Virtual Smartcard security model and service has been accredited by NHS Digital (initially, on the 2nd February 2021). Details of the accreditation can be found here:

https://digital.nhs.uk/coronavirus/access-logistics-hub/coronavirus-smartcards/isosec-virtual-smartcard

6.1 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.

Two availability zones are used for redundancy hosted in the London region - no data as part of the Virtual Smartcard service is hosted outside this region i.e. UK only.

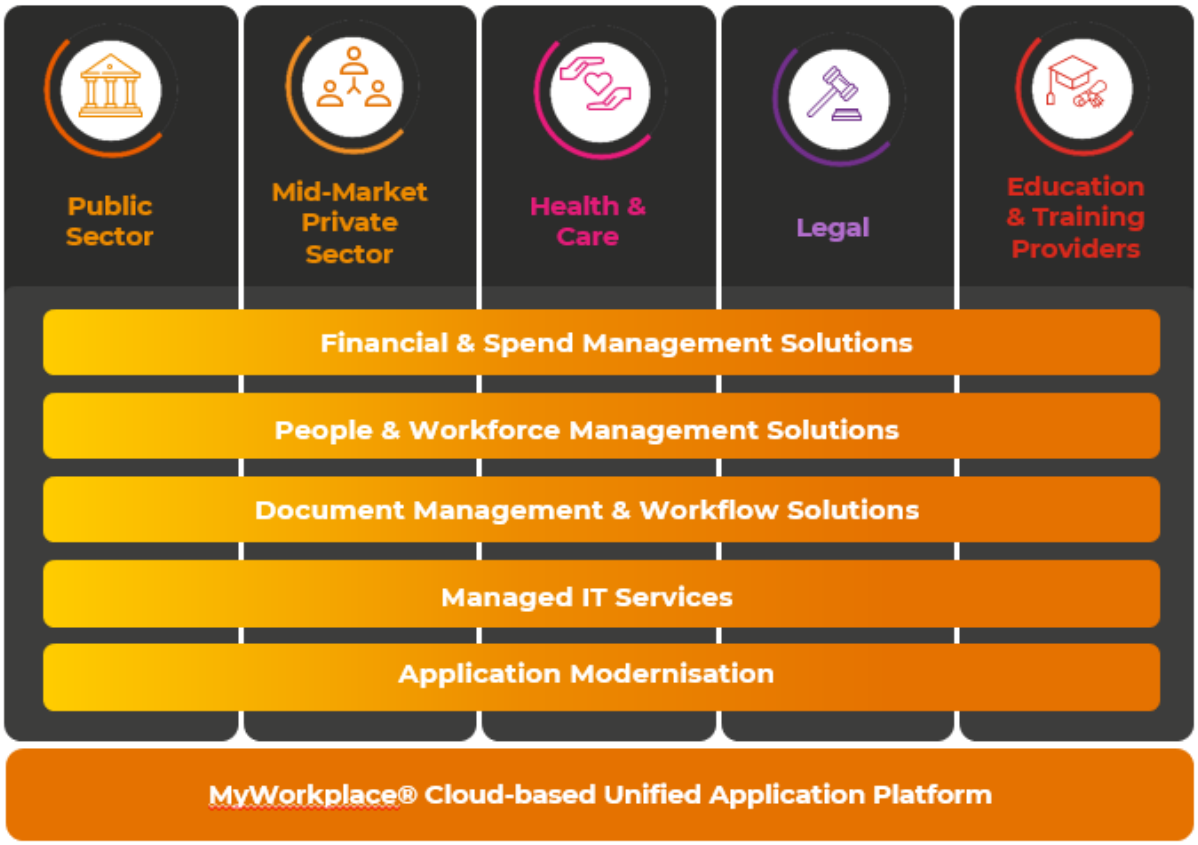
More information about AWS ISO accreditations could be found at:
https://aws.amazon.com/compliance/iso-certified/

About Advanced

Advanced at a glance

What can Advanced offer you? If we were to sum it up in one word, it would be 'possibility'. This is what we represent to our customers. It is driven by human imagination, ingenuity, and endeavour. We bring solutions and services to the table that turn possibility into reality – and the results are game-changing.

Our software and services help organisations to shine in their fields of expertise. Whether our customers are providing ground-breaking new services for clients, creating outstanding products for consumers or delivering life-altering care for patients, our software and services help them change things for the better.



We are a leading ERP Cloud provider with innovative Finance, People and Spend Management solutions. We also provide powerful horizontal solutions, such as:

- Document management, data automation and workflow software
- Specialist managed IT Services, ranging from hosting to full IT outsourcing
- Application Modernisation expertise, migrating legacy mainframe applications to open standards Cloud platforms

Our range of world-class vertical market solutions for Legal, Education, Health and Care, Charities and Membership, Sport and Field Service organisations are developed through years of experience and understanding of what is important in these sectors.

In 2021, we launched our MyWorkplace platform, the way in which all our Cloud products will be delivered going forward. This will ensure consistency of experience and will drive efficiency as all services will be accessible in one central workspace. Enabling easy access

with a single sign-on, users can quickly action their daily tasks and get data insights vital for their role. A built-in virtual assistant and task manager delivers more productivity tools.

Advanced in numbers? Well, 2021 saw Advanced grow to over £330m in revenue with in excess of 25,000 customers and 2,700 employees. Our customer retention remains above 91 per cent and our Net Promoter Score (NPS) has continued to climb since 2015.

Our solutions

We offer a wide range of solutions and services including ERP, back-office systems, sector-specific technology and IT services.

Financial management

Finance departments have had to work longer hours to meet the increased pressure of the new demands placed upon them. They are being asked to invest more time and effort to effectively plan, determine budgets and communicate performance. To make matters worse, low-quality manual and outdated finance platforms are adding to their stress and contribute to an overall feeling of burnout and inability to drive strategy.

At Advanced, we believe finance is the beating heart of any successful business. Our Advanced Financial Management suite enables finance teams to focus on strategy and performance by consolidating multiple platforms in one place, by reducing manual tasks and producing real-time business insight automatically.

- Core Financial Management
- Reporting and Dashboards
- Projects
- Inventory and Assets
- Budgets and Forecasting
- Purchasing
- Document Management
- Expenses

Spend management

We offer a suite of solutions which encompass the entire end-to-end procurement lifecycle process for organisations of all sizes and sectors. From sourcing and tender management, contract and supplier management to supplier marketplace and data automation – the suite enables businesses to drive value through effective spend management.

- Sourcing
- Procurement
- Contract & Supplier Management
- Marketplace
- Invoice Management
- Data Automation
- Spend Analytics

People management

The world of people management is undergoing a fundamental evolution. The ability of organisations to remain connected and engaged with their people will be one of the key factors determining success moving forwards.

At Advanced, we understand that your focus will be on increasing productivity and staff engagement. We also appreciate the roadblocks and headaches that outdated or rigid systems can cause. We believe that

- HR Management
- Payroll
- Rostering
- Time and Attendance
- Performance Management
- Recruitment
- Access Control

your people teams are influential, driving forces within your business. This is why we've created a range of solutions to help free your HR professionals from the burden of manual processes and administrative tasks.

Health and Care

Our portfolio of market-leading clinical solutions supports over 6,500 organisations in all areas of the health and care sector.

These innovative solutions, designed with clinical experts, are used every day by health and care professionals across the UK. They ensure patients and service users receive fast, safe and efficient care whatever the clinical or care setting: GP Practices, Hospital Trusts, out of hours or 111 service, residential home, a domiciliary service or a local authority children's services team.

- Clinical Decision Support
- Electronic Patient Records
- Online GP Consultation
- Patient Referral Management
- Urgent Care Management
- Transfer of Care
- Care Management

Legal

With flagship solutions in practice and case management (ALB and P4W), time recording (Carpe Diem), document management (NetDocuments) and legal forms, our software helps law firms, chambers and corporations become more profitable, enables their staff to be more productive and serves their customers quicker.

- Practice and Case Management
- Time Recording
- Digital Dictation
- Legal forms and documents
- Chambers Management

Education

We provide market-leading solutions for schools, colleges, universities, training providers and local authorities. Our software supports the full learner journey from enquires and applications, enrolment, timetabling and registers through to delivering apprenticeship programmes, financial management, exams and analytics.

- Management Information Systems (MIS)
- Timetabling and resource Management
- Apprenticeships and Learner Management

IT Services

- Private and Public Cloud Services

Our IT Services offering aims to help your IT department free itself from day-to-day operational activity so it can deliver strategic value back to the business. We do this by creating a scalable infrastructure that is closely aligned to your core business operations. Organisations have found that costs are typically reduced when they choose to work with us for their IT.	• Cyber Security • Managed IT Services • Digital workplace • Microsoft 365 Services
Application Modernisation Legacy technology can hold your organisation back, slow down productivity and increase your costs. The broad scope of our Application Modernisation practice means we can provide the people, products and processes to ensure that whatever your migration and modernisation goals, we can get the job done – on time and on budget.	• Automated Refactoring • Application Consolidation • Rehosting • OpenVMS • VME • Mainframe

Our customers

At Advanced, we have a customer obsession. We strive to ensure the partnerships with our customers mean they can deliver excellence for their end users. Implementing a new technology system is about more than the software alone, which is why we are dedicated to continually working with our customers to get the most out of their new investment.

Across all our markets we have over 25,000 customers and in the UK public sector alone, we work with:

- 150+ Local Authorities
- 55+ Central Government departments
- 140+ NHS organisations
- 20+ Emergency Services
- 220+ Housing Associations

Locations

As a UK organisation, Advanced operates from several large, modern office hubs with extensive facilities and an enhanced working environment for our staff. This has encouraged new talent to join us and enhanced team collaboration and expertise. With large offices in London, Birmingham, Belfast, Manchester and Newcastle, and smaller offices in other UK cities, we are physically close to most of our customers and can offer a unique and vibrant work environment in all corners of the country.

Beyond the UK, we also have offices in Dublin, Australia, the USA, India and Singapore.

Compliance and accreditation

All our services are governed by the following certifications:

- ISO 9001:2015
- ISO 27001:2013
- ISO 14001:2015
- Cyber Essentials Plus
- ISO 20000-1:2018 (Advanced Health and Care)

Security first

Advanced is Cyber Essentials Plus and ISO 27001:2013 accredited. We meet with and apply all 114 Annex A controls to our operations.

Infrastructure as a Service accreditations

The Infrastructure as a Service (IaaS) part of our solutions is accredited to hold and process information to IL2 and IL3 and is governed by ISO 9001 and ISO 27001.

The Software as a Service (SaaS) component applies to the following standards, with the target impact level we would expect the service to be able to hold and process information also shown:

- Defence, international relations, security and intelligence – no relevant standards
- Public order, public safety, and law enforcement - no relevant standards
- Trade economics and public finance
    - Impact on public finances would be targeted to BIL 1/2
    - Impact on UK trade and commerce would be targeted to BIL 1/2
- Public services
    - Inconvenience and impact on public confidence would be targeted to BIL1
    - Impact on public finances would be targeted to BIL 2
    - Locally provisioned services with no impact on health and safety would be targeted to BIL 2
- Critical national infrastructure
    - Finance would be relevant to target to BIL 1
- Impact on personal/citizens
    - Impact on the privacy of the citizen would be targeted to BIL 1
    - Utilisation of a service would also be targeted to BIL 1

Overall, our software would be targeted to BIL 1/2.

Compliance with Government ICT and information principles

Our products use a software service that has been implemented in many shared service type operations, enabling customers to use a single system across multiple organisations. The Cloud-based deployment also enables organisations to completely outsource the management of the solution. Use of common tools and platforms gives the service an 'open' approach, ideal for interoperability within organisations wishing to leverage best-of-breed systems from SMEs and beyond.

Business information is crucial to any organisation. The service provides strong management and reporting of the business history and transactional information in the service, but also supports corporate business analysis by enabling interoperability

between systems to join up disparate and discrete snapshots of information. However, access to information is always controlled, strong governance protects the business information within the service and modern secure transmission methods then protect externally interfaced data.

The service supports the seven key principles of information:

1. **Information is a valued asset –** the key analysis and reporting functions within the service enable powerful use of the information for management reporting and internal decision-making.
2. **Information is managed –** information is protected within the secure data repositories and utilised throughout its life history.
3. **Information is fit for purpose –** it is held in a way that is organised logically for the outputs needed from the system and to provide meaningful reporting.
4. **Information is standardised and linkable –** it is held only once throughout the service, it enables data to be used only once and where relationships exist, automatic links are created.
5. **Information is re-used –** it is entered only once and utilised throughout all applicable modules and reports.
6. **Public information is published –** automatic scheduling enables critical public information to be automatically published and stored, providing public access. In addition, external modules, such as the supplier self-service, allows individuals and organisations to view relevant data through a secure portal.
7. **Citizens and businesses can access information about themselves –** this is less important as citizen information is less relevant to this type of application, but where individuals interact as customers or suppliers, this is supported.

Accreditations

ISO9001:2008	Advanced is registered to the ISO 9001:2008 and TickIT Guide quality standard and our Quality Management System is published on our company Intranet. All staff must be familiar with the published Quality Procedures, and we internally audit these procedures regularly. As part of maintaining the ISO 9001 registration, we are externally audited every six months. Our external auditor is BSI. We have been registered since 1996. Our Quality Policy is an integral part of the Quality Management System.
ISO 27001:2013	Advanced is accredited to the ISO 27001:2013 standard. The certified Information Security Management System (ISMS) applies to all the Advanced Computer Software Group in managing Information Security across software and services.
ISO 14001:2015	Advanced is accredited to the ISO 14001:2015 standard. The certified Environmental Management System (EMS) specifies the requirements for an environmental management system that Advanced has used to enhance its environmental performance by managing its environmental responsibilities in a systematic manner that contributes to the environmental sustainability.
ISO 20000-1:2018	Advanced Health and Care is accredited to ISO 20000-1:2018. The certified Service Management System (SMS) assures the effective implementation, maintenance and continual improvement of service

	management. The SMS provides a consistent approach to the service lifecycle by all its service providers.
Cyber Essentials Plus	Advanced is accredited to Cyber Essentials Plus. The certification by Cyber Essentials Plus provide assurance that Advanced has met rigorous standards of the Government-backed scheme and has undergone rigorous technical assessment to demonstrate robust security controls.

Delivery and support

Delivery

Buying a solution offers a lot more than just software. With an impressive track record built up over many years, our team provides you with the services and support to implement your new system as quickly and easily as possible. We also work closely with you to encourage adoption and optimum use of the software throughout your organisation, delivering an excellent return on investment throughout the lifetime of the system. Our consultants are characterised by their professionalism, length of service and extensive knowledge of the systems they implement and support. They also have years of expertise in the sectors they operate in, and many of our consultants have backgrounds as qualified accountants, HR professionals or IT engineers, which underlines their level of skill and experience.

For implementation, Advanced will employ the use of its Professional Services Corporate Project Methodology (CPM) framework to deliver the project in a controlled and structured manner, in order to help achieve your project's outcomes.

Aligned with PRINCE 2 principles, CPM uses a partnership approach between Advanced and the customer that balances quality, time and cost. CPM supports a knowledge transfer approach using a 'train the trainer' framework, enabling customers to quickly become self-sufficient in the adoption of our enterprise software solutions.

Support

From becoming an Advanced customer, through implementation and into 'business as usual', Advanced customer support is committed to delivering an exceptional service. As your partner, the support team will continue to ensure the successful deployment and use of our solutions and services providing you with ongoing high levels of return on investment.

Our support services offer:

- General system queries and advice
- Incident submission, management and reporting
- Knowledgebase
- Product feedback
- Software maintenance and legislative updates

The Advanced customer portal provides a rich source of information and is an intuitive and responsive interface to the Advanced support team. Our support case management system, customer community, knowledgebase, ideas portal and more are all easily accessible from one single link.

You will find our support teams extremely responsive, and all customer enquiries are answered directly by our knowledgeable teams.

Feedback is important to us and whilst our customer satisfaction levels are high, we are always looking for your feedback on how we might improve our service. We continually review our practices to improve internal operations and we pride ourselves on continual improvement.

Environmental, Social and Governance (ESG) and diversity

We recognise the opportunity and responsibility we have as a business and are committed to building a better tomorrow for our employees, customers and wider community. It is hugely important to us that we play a part in leaving a positive environmental legacy. As we all witness the effects of climate change, this way of thinking has never been more important. We're investing in sustainable practices because it's the right thing to do, but also because we know our staff, customers and partners are looking for leadership and action on the issues that most affect society.

Our inaugural ESG report last year helped us on this journey, and groups all our initiatives and reporting into three focus areas:

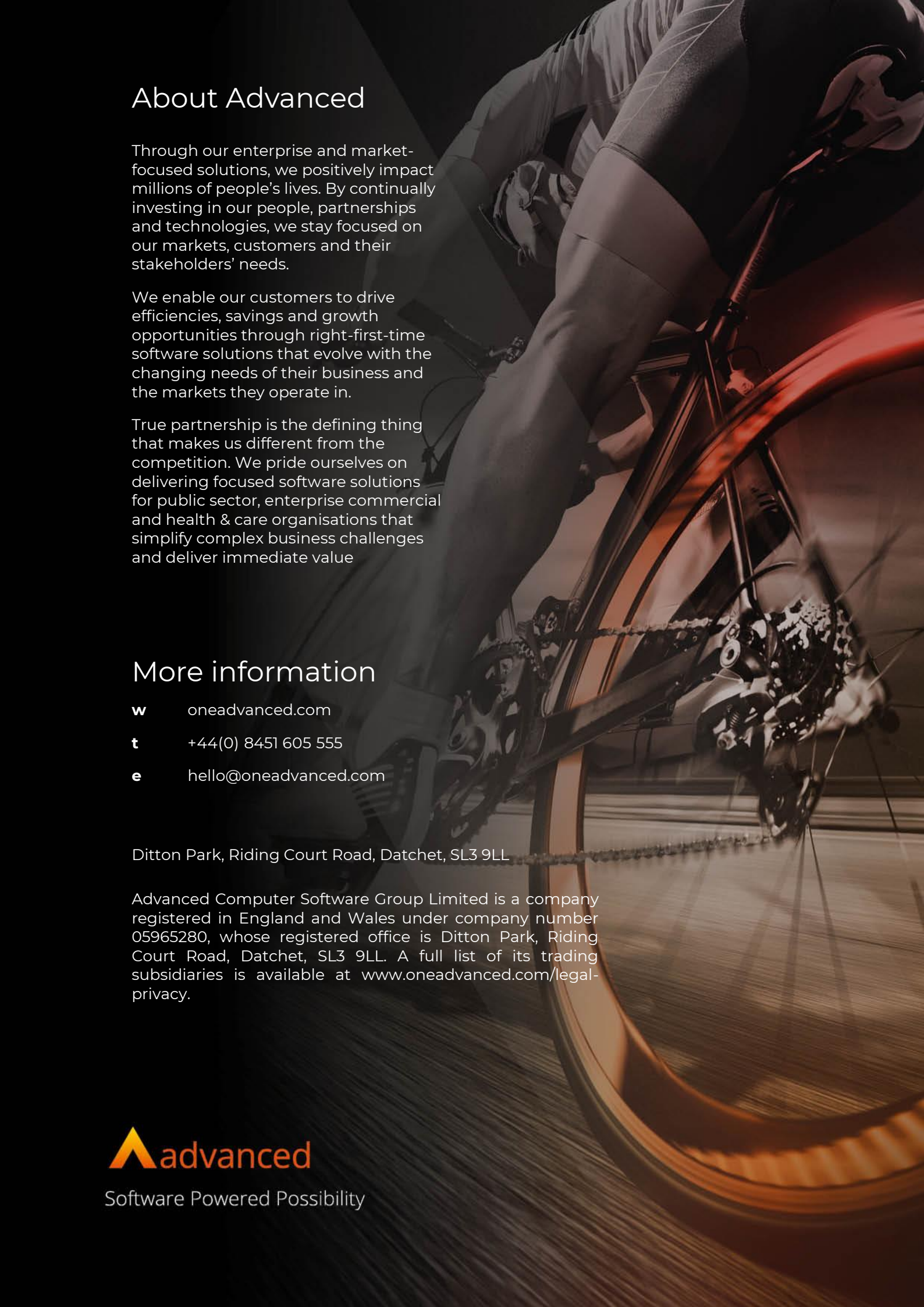
Protecting the planet
We track our total carbon impact from offices, travel and data centres and have seen an overall reduction in CO2 emissions per head of 47 per cent since 2018.

Diversity and inclusion
Cultivating a diverse workforce and inclusive culture is a priority for Advanced. One third of our Board are women and during 2020 we were recognised as one of the Top 100 Diversity Leaders in the UK by the Financial Times.

Social and community empowerment
We strive to be a responsible and contributing part of society, seeking to build strong relationships and acting as a good neighbour. Fundamental to this is making a real difference to those disadvantaged and needing support, not just in the form of monetary donations but also available time and access to opportunities. During 2021 we contributed £85,000 to recognised charities and supported countless staff-fundraising activities.

You can read more about our commitments to ESG and diversity at the below link;

https://www.oneadvanced.com/environmental-social-and-governance-strategy/



About Advanced

Through our enterprise and market-focused solutions, we positively impact millions of people's lives. By continually investing in our people, partnerships and technologies, we stay focused on our markets, customers and their stakeholders' needs.

We enable our customers to drive efficiencies, savings and growth opportunities through right-first-time software solutions that evolve with the changing needs of their business and the markets they operate in.

True partnership is the defining thing that makes us different from the competition. We pride ourselves on delivering focused software solutions for public sector, enterprise commercial and health & care organisations that simplify complex business challenges and deliver immediate value

More information

w oneadvanced.com

t +44(0) 8451 605 555

e hello@oneadvanced.com

Ditton Park, Riding Court Road, Datchet, SL3 9LL

advanced

Software Powered Possibility