System Security Plan

Coordinate My Care

1 DOCUMENT HISTORY

1.1 AMENDMENT RECORD

Date	Version	Author/Review	Brief Summary of Changes(s)
27/06/2015	Draft 0.2	Eugene Rudman	Document created
08/07/2015	Draft 0.3	Eugene Rudman	Updated based on ISC US team feedback
	1.0	Eugene Rudman	Final CMC review

1.2 REVIEW

Name	Title	Version	Date
Eugene Rudman	Manager, UK Hosted Services	0.3	28/09/2016

1.3 APPROVALS

This document must be approved by:

Name	Signature	Title	Version	Date
Eugene Rudman, ISC				
Mandy Shaw, CMC				

2 CONTENTS

3 INTRODUCTION

3.1 PURPOSE AND SCOPE OF THE DOCUMENT

The System Security Plan (SSP) details the management approaches and security controls that are in place within InterSystems (ISC) to ensure the ongoing security and availability of confidential data stored, transmitted and/or processed by the hosted Coordinate My Care (CMC) solution.

It covers the following elements of the CMC project and solution:

- ISC approach to information governance and data protection
- Security of CMC data in the interim environment
- Security of CMC data hosted in the data centre environment
- Encryption standards used by the CMC solution

4 APPROACH TO DATA PROTECTION

4.1 INTRODUCTION

ISC has strong data privacy, confidentiality and security policies that apply to all employees and their work, whether on site projects or hosted solutions.

The following approaches to data protection are captured in the ISC policies:

- All requests for access to confidential data must be approved by the requestor's line manager or project manager who can justify the business need, as well as the manager of Hosted Services. Each request includes agreement by the requestor to comply with the specific requirements relating to that asset, the type of access required, period for which access is required and business justification / the "need to know" for having such access.
- Access to confidential information is reviewed following any event which may lead to a change in access e.g. role changes. Access to confidential information assets is reviewed by the local information officer at least annually.
- No confidential information may be extracted from our hosted solution without prior written agreement from the CMC.
- No confidential information may be used for any purpose without prior written agreement from CMC.
- Access to confidential information is reviewed following any event which may lead to a change in access e.g. role changes. Access to registered confidential information assets is reviewed at least annually by the local information officer.
- Any confidential information received by ISC and/or uploaded by a customer to a system that is not on the information asset register, will be deleted.
- All confidential information, whether in transmission to/from the data centre or at rest within the data centre, must be encrypted. This also covers the temporary environment described in this document. Details of encryption used is provided in paragraph 5.
- All staff have agreed to comply with ISC security, privacy and confidentiality policies.
- All staff have to attend Data Protection Act training at least annually.
- All staff that have access to systems containing confidential data are subject to additional screening before commencement of their employment.

ISC has an active Information Governance (IG) committee which meets monthly and focuses on ensuring ISC's ongoing compliance as well as the continuous improvement of our IG processes and functions.

5 ENCRYPTION

5.1 ENCRYPTION OF DATA "IN FLIGHT"

As required by ISC policies, all confidential CMC data to be hosted in on ISC provided solution will be encrypted during transmission. This section outlines the different cases and the method of encryption that applies to each case.

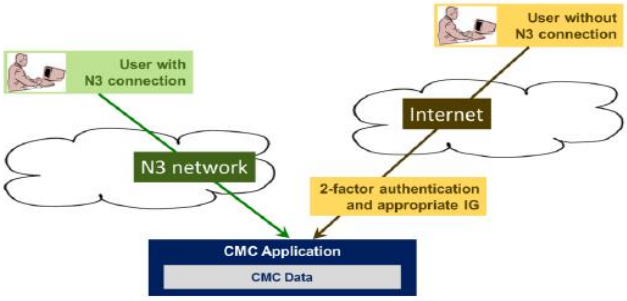


Figure 1 - End-user access to CMC solution

5.1.1 End-user access: Connections over N3

The CMC solution is a web-based application requiring the use of HTTPS and/or TLS in the case of sockets, to ensure encryption of data during transmission. This applies to both PC and mobile devices.

In the case of N3, client access does not involve the use of a VPN for further encryption. However, the N3-connected environment complies with HSCIC requirements for connection to N3 i.e. the use of physically separate firewalls i.e. Cisco 5515-X appliances for N3 connections to the CMC solution. Additionally, there will be separate web-server instances for CMC when accessed over the Internet and/or N3 so as to enforce physical segregation between N3 and Internet-facing web-servers.

5.1.2 End-user access: Connection over the Internet ("non-N3")

Where end-users access the solution over the Internet connection, separate web servers are used to meet the HSCIC security requirements. Apart from that, the same encryption applies for both PC and mobile users as in the case of N3 users i.e. HTTPS and/or TLS for sockets.

In addition, the solution will require authentication using CMC's existing Authen2cate solution. The Authen2cate service is hosted in Amsterdam and Dublin. Traffic between CMC users and Authen2cate relates to browser client certificate management only. The CMC application can be accessed over the Internet only if a valid Authen2cate certificate is in place in the user's browser. To obtain this certificate, Authen2cate is responsible for registration challenge, certificate generation, and download. Once the certificate is present in the browser, connectivity becomes available to the CMC system; all application traffic travels direct between the user device and the ISC data centre i.e. no CMC system data will flow via Authen2cate. Data stored at Authen2cate is limited to non-N3 user registration details.

5.1.3 Site to site: Connections over N3 (applicable to Royal Marsden connection)

The CMC solution requires a point to point connection between a data warehouse environment at Royal Marsden, and the CMC solution hosted in the ISC data centre. This connection uses an IPSEC VPN with AES 128-bit payload encryption. .

5.2 ENCRYPTION OF DATA "AT REST"

The CMC solution stores confidential data in the Caché database which is encrypted at disk level using AES 256-bit encryption.

The encrypted data is replicated to near-line storage at the primary and secondary data centres, where it can be used for fail-over and/or disaster recovery purposes.

6 INTERIM ENVIRONMENT

As part of the CMC project, there is a requirement to setup a temporary environment to allow work to start on the CMC solution while the main hosting data centre is being built. This section outlines the security controls in place for each of the interim environment's elements, to ensure security of data transferred to, processed and/or stored within this environment:

6.1 PHYSICAL HOSTING

Although the final data centres conform to ISO27001 standards, the interim environments will be hosted in InterSystems' Eton office which does not meet, and is not planned to meet ISO27001 standards.

The physical security mechanisms in place at the Eton office include CCTV, security pass access to the building and security pass access to the server room.

In addition to database encryption, data written to discs used by the servers will also be encrypted using software encryption on the host operating systems of the solution environments.

The virtualized CMC environments are on a separate network, distinct to InterSystems' other environments. A holding network containing a Domain Controller and Remote Desktop Services server will provide a layer of protection between the VPN and the interim environments.

Although the virtual CMC environments will be hosted on servers running other virtual machines on multiple different networks, there will be no virtual connections between these servers nor the networks, and it is accepted throughout the industry that virtual network isolation is of equivalent or greater security than isolated physical networks or VLANs.

6.2 REMOTE ACCESS

This section outlines the infrastructure and security mechanisms in place to secure data stored and processed in the Interim Environments, as well as access / transfers to and from that environment.

6.2.1 VPN

A Cisco ASA Firewall will be used to provide VPN access to the Interim Environments. This will be accessible from the Internet, and also from the N3 network.

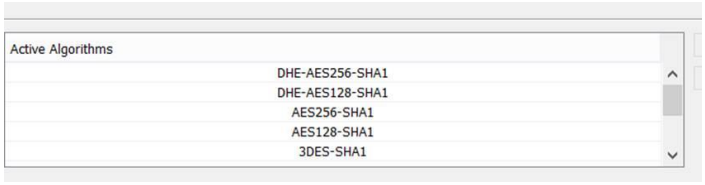
Access from the N3 network will be restricted to those with a source IP originating from the CMC site as well as other InterSystems customer sites who are using the same VPN solution to connect to their own Interim Environments. Such restrictions for the Internet connected VPN are not possible, as contractors working for those customers and/or remote InterSystems staff require connecting from different locations with no fixed IP addresses.

To enhance security, therefore, ISC uses a 2-factor authentication solution. VPN users are required to register a mobile device with our 2FA service provider, Signify. A unique, one time RSA key is generated by the device each time a user wants to log into the VPN. A separate username and password are then required to access a Remote Desktop Services (RDS) server.

The RDS Server is the only server which is reachable from the VPN. A user must first log onto to VPN, using 2-factor authentication and then to the RDS server. From there, they have to connect to the CMC environment to gain access to CMC's data.

The VPN has no direct access to the endpoint CMC environments. Other InterSystems customers do use the same VPN connection, but access a separate RDS server which is restricted to their own environments. Access control to each RDS server is controlled by Active Directory Groups on the RDS server's domain.

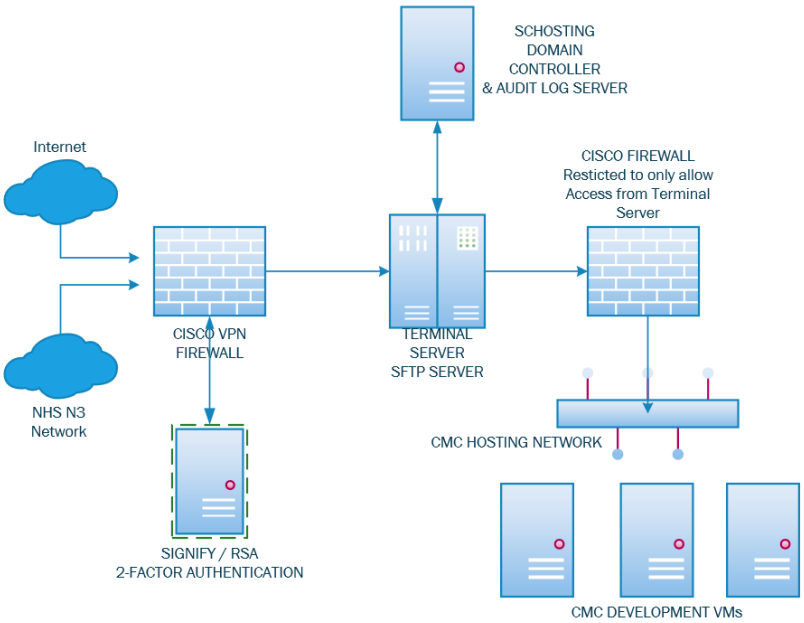
By default, the Cisco AnyConnect VPN client uses the DHE-AES256-SHA1 encryption algorithm, however if a different client is used or local restrictions mean this algorithm cannot be used then the VPN will try the following algorithms in descending order of security:



6.2.2 Remote Desktop Services

A RDS server running Windows Server 2012 has been configured for CMC. All development environments and the RDS server will be virtual. A second firewall will restrict access to the Development Environments hosted on the CMC Interim Network to traffic only from the CMC RDS server. All other traffic to/from the CMC Interim network will be blocked.

The layout will be:



Each user will have their own domain account to allow access to the RDS server. This account will also allow access to the Secure FTP server and shared folders which are also hosted on the RDS server. The RDS server and Domain Controller are encrypted using Microsoft Bitlocker.

6.2.3 Access to Development Environments

Once connected to the CMC RDS server, each user will be presented with their own Windows Desktop with all the tools they will require pre-installed. Access to each development environment within the interim Eton environments where CMC data may be stored, will be controlled via Active Directory Groups setup on the Domain Controller or via local accounts on the development environment.

Only the services required will be allowed past the firewall to the development environments. Access to any other network, including the Internet, from the RDS network and the development network will be blocked.

6.2.4 Secure File Transfer

A Secure FTP (SFTP) server will be setup on the Remote Desktop Services Server to allow customers and staff to securely transfer files to/from restricted folders on the RDS server over the VPN. Files transferred using SFTP are encrypted in transit offering a further layer of security over VPN encryption.

Once on the RDS server, files will be encrypted using Windows Bitlocker encryption which is transparent to any logged in user.

InterSystems' staff will use WinSCP to securely transfer files between the RDS server and the development environments.

6.2.5 Connecting Procedure

The procedure for clients connecting in remotely to perform data migration testing will be:

1. Connect to the interim network using Cisco AnyConnect VPN client and Signify RSA token.
2. Connect to the CMC RDS server using provided domain credentials. Each user will be presented with their own desktop which has the required tools installed.
3. From their remote desktop the users will be able to connect to the development environments via http, https and ssh. All session data will be kept inside the interim network unless it is exported via the secure FTP server.

6.2.6 Site to Site VPN Tunnel

A site to site VPN tunnel has been setup between the Royal Marsden and InterSystems Eton. This tunnel connects 1 specific server in RM directly to the CMC Hosting network where the development environments are hosted, with underlying connectivity provided using N3.

Once the main ISC hosting environment is in place, this VPN tunnel will be moved across i.e. from the ISC data centre to the Royal Marsden. Eventually there will be both live (SUTMBI02) and UAT (a repurposed SUTMBI01) links in place.

Due to limitations of the firewall equipment currently at RM, the tunnel is using AES 128bit encryption only.

6.3 LOGGING

A Syslog server will be setup on the Domain Controller to log the time and account used for VPN connections and Remote Desktop Sessions. Any file creations/modifications/deletions inside the shared folders on the RDS server will also be logged, along with any FTP activity.

6.4 BACKUP

The configuration of the interim environments in Eton will be copied to empty environments which contain no sensitive data and only the empty environments (and configuration on it) will be backed up locally.

6.5 TRANSFER TO DATA CENTRE

Once the data centre is operational, the interim environments will be transferred to the data centre. For this, one of two approved methods will be used:

- Data will be copied over an AES 128-bit encrypted VPN to Royal Marsden, from where it will be copied to the data centre using another (identically configured) VPN connection to the data centre. The underlying connection, in each case, will be N3.

- Data will be copied over an AES 256-bit encrypted VPN from within the interim environment, to the secure CMC environment in the data centre. In this case, the underlying connection will be the ISC network including any possible site to site VPN to the data centre.
  •

[Note, in the end, this was copied using a VPN from Eton to the data centre environment, over N3]

All of the data will be purged from the servers and storage in Eton, and the interim network decommissioned.

7 DATA CENTER ENVIRONMENT

7.1 PHYSICAL SECURITY

The live CMC solution will be hosted in secure racks within InterSystems' private suites / cages that are located within purpose-built data centres that are ISO 27001 compliant.

The perimeter of both data centres are secured by walls, fences and access control gates to ensure that only authorised people and/or vehicles are allowed access.

The InterSystems hosting environment is further secured through the use of security guards, man-traps, CCTV and multi-level access controls for access to the building, suites and/or cages. Access control and CCTV is monitored on a 24x7 basis.

Access to the hosting environment is restricted to authorised people with all access to the hosted environment being logged and recorded.

Access to the hosted environment is reviewed on any change that may lead to a change in privileges.

Audits of privileges are performed regularly and at a frequency no less than 6 months and/or as required for ISO 27001 compliance.

7.2 ENVIRONMENTAL CONTROLS

The hosted environment has N+1 UPS systems, N+1 generators and independent A+B power supplies. The primary data centre, additionally, has a private power sub-station.

All UPS devices are tested, and batteries replaced, regularly and at a frequency no less than recommended by the manufacturers' guidelines. Generators are tested and maintained regularly and at a frequency no less than recommended by the manufacturer's guidelines.

Both data centres have fire detection and suppression systems installed. These systems are monitored 24x7 and maintained at a frequency no less than what is recommended by the manufacturers' guidelines. In the case of our primary data centre, i.e. Telehouse in London, a dry pipe pre-action sprinkler system with centralised sensors is used. In the case of our secondary data centre, i.e. 6DG at Studley near Birmingham, a gas suppression system is used.

Cable distribution is via a raised floor with cable trays as required. In addition, leak detection is installed and monitored 24x7.

7.3 ARCHITECTURE

7.3.1 Physical architecture

The CMC solution is hosted within a wider data centre infrastructure which can be represented as follows:

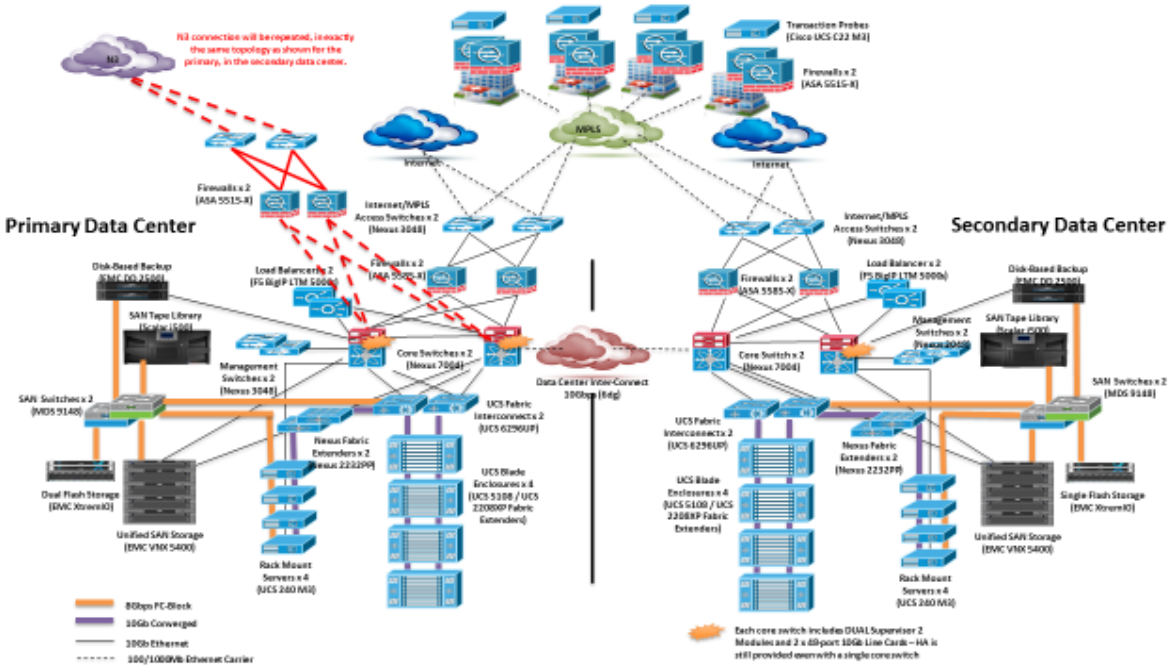


Figure 2 - Physical data center environment

Please note that not all elements are present and/or used by the CMC solution – for example, the MPLS connections and associated firewalls and probes. These are included to show the wider environment within which CMC will be hosted.

While most network pieces e.g. the Cisco ASA and F5 devices are shared, these are configured in "device context" mode which provides separate configurations for each customer. This, for example, allows customers to have the same IP address ranges without causing any issues or being able to route to each other; more importantly, it reduces the risk of a single firewall or routing configuration error causing traffic to flow between customers.

7.3.2 Logical architecture

The CMC solution is provided with a logically separate hosting environment consisting of the following:

- A dedicated, external-DMZ environment allowing access to the external-facing IP addresses of the F5 load balancers hosting the CMC solution.
- A dedicated, internal-DMZ environment hosting the web-servers associated with the CMC solution.
- A dedicated application and database environment hosting the application and associated databases.
- One or more dedicated virtual machines running on VMWare mounting dedicated storage volumes i.e. LUNs.
- A dedicated bastion host for ISC administrators responsible for managing the CMC solution / application.

Except for the bastion host, this configuration is repeated for each instance of the CMC solution e.g. "live", "test" and so on. Each network segment is protected from others, and from other customers' networks, using a pair of firewalls as detailed in paragraph 7.4 below.

7.4 FIREWALLS

The wider hosted environment is protected by dual Cisco ASA 5585-X firewalls in each data centre.

Furthermore, web servers are further protected by a layer of dual F5 load balancers in each data centre.

Lastly, connections coming over N3 are further protected using a physically separate Cisco ASA 5515-X firewalls to ensure compliance with HSCIC requirement (in addition to having separate web-server tiers for CMC connections coming over the Internet, as opposed to N3).

All firewalls and network devices are monitored on a 24x7 basis – this includes availability, performance, security and capacity. Logs are collected and stored centrally for regular review.

7.5 STORAGE AND BACKUPS

CMC's data will be stored in a dedicated database which is encrypted using AES 256-bit encryption at the disk layer, as outlined in paragraph 5.2, and stored on a logically separate storage volume.

In addition, the encrypted data is copied to a secondary site i.e. Studley which is over 100 miles away from the primary site i.e. London. Subsequently, the data is backed up to EMC data domains at both locations. These backups are almost instantly accessible and do not require the frequent testing that tapes do.

. Backup recovery is tested at a frequency of no less than once every six months.

7.6 REMOTE DATA CENTRE ACCESS

Authorised staff can connect to the CMC environment using the following steps:

- Each time the user wants to log in, a one-time RSA key is generated using software on the user's mobile device and/or token.
- The user connects to the data centre using the Cisco AnyConnect client and RSA key generated above.
- A separate username and password is then required to access a Remote Desktop Services (RDS) server, either in the management network (for systems administrators) or the client network (for application support teams).
- From there, a system and/or application administrator would be able to access the relevant service element for them to manage.

All devices, both remote and at InterSystems' office, are managed to comply with company policy which includes group policies, ongoing anti-virus updates and hard disk encryption.

In addition to access to the environment, further rules on the data centre firewalls will prevent unauthorised administrators to access the N3 connection.

7.7 EQUIPMENT AND DATA DESTRUCTION

Redundant hardware will be removed and destroyed, and media will be erased, by an accredited vendor working to BS EN 15713:2009 or later and which sets out the requirements for how media with sensitive information is collected, retained and transferred, as well as the processes and standards for destruction. A certificate of secure deletion and/or physical destruction will be issued as appropriate.

7.8 INFRASTRUCTURE PENETRATION TESTING

The infrastructure proposed for CMC has only recently been implemented and infrastructure testing has not yet been implemented. Such penetration testing will be done, and all relevant (red, amber) vulnerabilities will be remediated by an agreed date.

7.9 MONITORING

The entire solution, from networks to the CMC solution's web services and databases, will be monitored on a 24x7 basis using Nagios, vRealize and other proprietary tools designed to monitor InterSystems' products. Where incidents are detected, these are responded to on a 24x7 basis – including resolution within agreed service level targets.

Specific to security, all event logs are collected and reviewed as appropriate . .

[end of document]