

Cornwall Secure Remote Access Solution - I-chain

Introduction

I-chain has been developed to enable secure delivery of data services to locations outside of the Cornwall Health Network for all Health staff and associate partners.

The solution has been designed to accommodate users who require access to confidential clinical systems in a secure way. This has been achieved through the implementation of the 3 level security model which has a token based system supported by a directory service. This holds the authorisation and security details, down to user and/or application level.

I-chain provides, in the first instance, access to the Cornwall Intranet, email (Groupwise), e-Guide (white pages information), LMS (Learning Management System), Office Applications , Users local (H) drive held on the SAN (Central Servers), all Core applications – e.g. PAS, EROS and any other Smarterm applications. Access to other applications can be made available as required.

The solution as configured will allow users to securely access the local systems and data held within the Cornwall Health Network from any PC or Laptop device connected to the Internet.

The potential is for staff to work from home or from any premises that have Internet access, and be able to have the same level of access as if they were in the workplace. This has created great flexibility for staff, many of who are mobile across the county, and work various shift patterns.

An example of where i-chain has brought benefit is to Medical students who work within the new Knowledge Spa based in Truro. They have access to the University systems via the academic network but can now also access the hospital systems via i-chain.

It is anticipated that some 2000 users will require access within the next 2-3 years.

Technical Overview of the Cornwall Solution

To provide the necessary access to the systems a number of different components were used from multiple vendors to make up the cohesive architecture. It should be noted that although the Cornwall Solution is built around the Novell Directory service this is not a pre-requisite of the i-Chain product.

In the following illustration the connection is shown from a remote workstation.

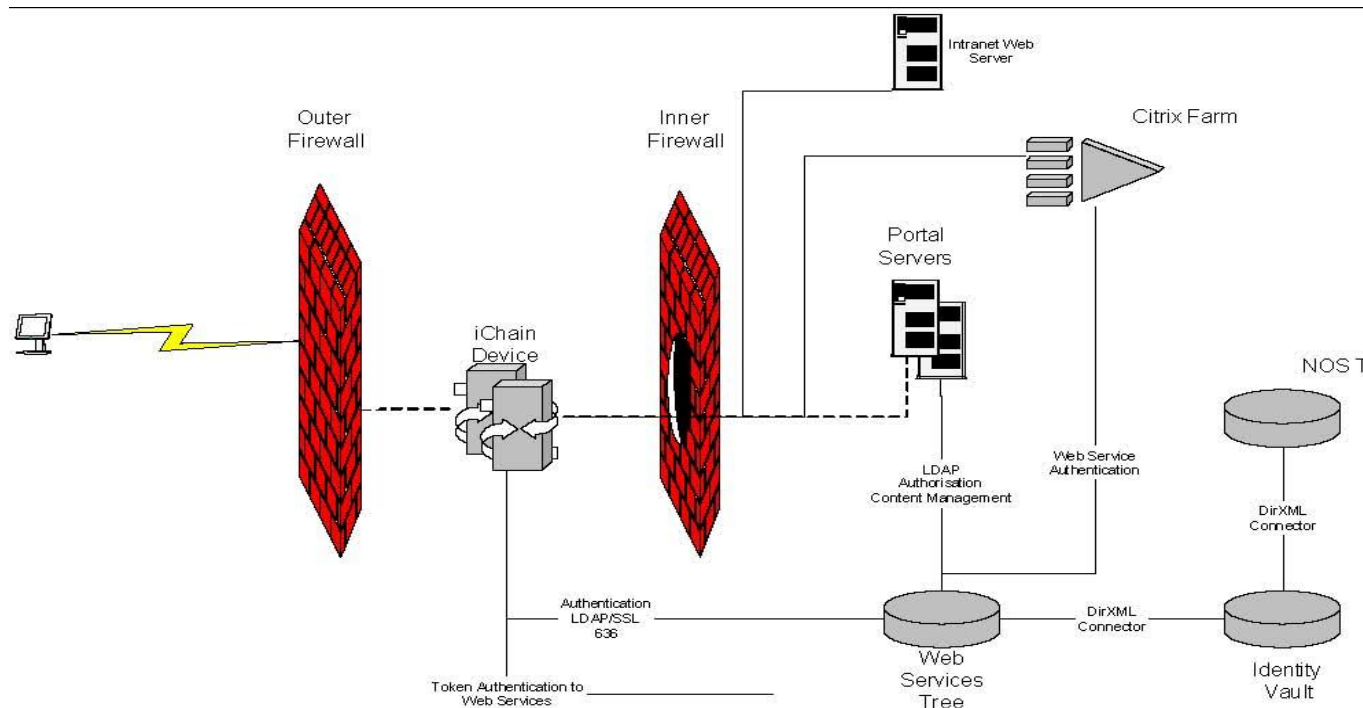


Illustration 3 Overall Architecture

The user access request is passed through the outer firewall to the i-Chain device. Here the user is authenticated against the ID and password held in the Web Services Tree. The authentication is processed using LDAPS for security.

Once authenticated the user is passed through the i-Chain device and through the inner firewall to the Portal server. Here the identity is used to present personalised content and links to the relevant applications. The content management is based on information found in the Web Services Tree.

As the user selects different applications from the portal server the URL of the new page is monitored by the i-Chain device. If a URL points at a "secure" service the i-Chain system will request the user to input a "token" value. This token, a Vasco DigiPass Go-1, will be checked against the Web Services tree to ensure secure authentication.

As a user accesses applications housed within the Citrix server farm, once authenticated, the ICA client will be launched and connected. Data between the server and the client will be encrypted using the built in Citrix 128 bit encryption.

i-Chain

The i-Chain system is used to ensure access to web services is secured against a user who exists within the directory. Each resource delivered to the remote users is identified and i-Chain is advised of the specific URL of the service. As the user accesses this service they will be prompted to authenticate before being granted access to the service. This will be verified against the web services directory and only on successful presentation of the users' credentials will access be granted.

Options exist to class users in various groups therefore providing a granular security model. For instance it is possible that as the user attempts to access services which are regarded as secure the user will be prompted for another form of authentication.

Token Authentication

Vasco tokens are directly linked to the user identity within e-Directory. The tokens themselves are small and easily carried. Full details are available from the Vasco web site at <http://www.vasco.com>.



Illustration 4Vasco DigiPass Go-1 with Novell Branding

The Vasco DigiPass Token Go-1 is a small (7cm x 4cm x 2cm) device which when opened displays a value. This should be entered into the authentication page and is verified against the directory.

Each DigiPass is identified individually and is associated with a specific user. This ensures that a user can only gain access if they have both the ID and the token.

Certificates

One of the functions of the i-Chain system is to provide secure traffic between the browser and the back end services. This is done by utilising an SSLiser built into i-Chain. This requires a PKI certificate to be available for the various services being offered.

Web Services Directory

The current directory services available within the environment are very specific to the functions that they provide. Specifically there is a hierarchical directory used for file and print access to the NetWare servers and also maintaining control of the workstation. This is known as the Network Operating System (NOS) directory.

A second directory is used for synchronisation of user information between the NOS directory and the payroll system, and also provides a feed to the NHS through and EDS system externally. This is known as the Identity Vault (IV) and can be seen as a meta-directory.

In order to provide a directory service specific to the delivery of a web oriented application a different directory was required. This will allow for the addition of the token support without affecting either the NOS or IV directories.

Users will be synchronised between the directories by using the IV directory. Information, including passwords, will be synchronised between the systems ensuring that the user only has to remember a single password for access to the LAN based services.

In a future phase the ability to recover forgotten passwords is also seen as being of benefit. This can be provided through the web services directory only. Users who have forgotten their password will be directed to a specific URL enabling them to change their password after providing specific details to the service. These details aim to ensure that only the identified user can modify their password.

Portal Service

Once the user has correctly authenticated through the i-Chain service the user will be presented with a screen providing options for accessing the back end systems and services.

This screen will also present, where possible, additional personalised content such as an overview of the users current e-mail. This can be added to by providing additional data gleaned from the Intranet or external web sites.

The portal system will be hosted within the NetWare platform as this platform has the greatest level on knowledge within the trust and as such support for the portal will be easier to maintain.

Citrix Server Farm

The Citrix farm is already in place within the trust and is linked to the NOS tree for application delivery. In order to correctly deliver the chosen applications to the user it was necessary to implement nFuse and ZEN for Desktops (ZfD) within the Citrix environment.

In essence the user should be presented with the correct set of applications based on their privileges. If a user has access privileges to the secure applications then these will be presented on one page of information. All of the users will have access to the unsecured applications and will be able to access them without additional authentication.