



## CCT MARK IA CLAIMS DOCUMENT (ICD) IBM

<b>IBM Virtual Infrastructure Access Services</b>
<b>5.5b</b>

<b>VENDOR DETAILS</b>
IBM UK Ltd
PO Box 41 North Harbour Portsmouth Hampshire PO6 3AU
Telephone Number: 0207 021 9947
Vendor Website: <a href="http://www.ibm.com/uk/">www.ibm.com/uk/</a>
Vendor Contact Email: <a href="mailto:Dave_somerville@uk.ibm.com">Dave_somerville@uk.ibm.com</a>

CCT Mark Certificate Number:	2007/06/0024
Date CCT Mark Awarded:	28 <sup>th</sup> June 2007
CCT Mark Award Expires on:	27 <sup>th</sup> June 2008
ICD Issue Date:	28 <sup>th</sup> June 2007

## Table of Contents

1	Introduction.....	3
1.1	Background .....	3
1.2	Objectives.....	3
1.3	Purpose of Document.....	3
1.4	Structure .....	3
2	Product/Service Description .....	4
2.1	Product/Service Identification .....	4
2.2	Product/Service Overview .....	5
2.2.1	Security architecture .....	7
2.2.3	Hardware requirements .....	14
2.2.4	Software requirements .....	14
2.2.5	Out of Scope .....	15
2.3	Usage assumptions .....	15
2.3.1	Assets .....	16
2.3.2	Threat scenario.....	16
2.3.2.2	Organisational security policies .....	17
2.3.2.3	Security requirements on the environment.....	18
3	Security Claims for the IS Product or IS Service .....	18
3.1	Claims Statements .....	18
3.2	Existing assurance certificates .....	20
	Annex A - Glossary of Terms .....	21
	Annex B - Marketing Statement to be used.....	23

# 1 Introduction

## 1.1 Background

This document outlines the Information Assurance (IA) claims made by IBM UK Ltd in regard to the suitability of the IBM Virtual Infrastructure Access Services product for use by the UK Public Sector for the secure connection to and management of virtualised work spaces.

## 1.2 Objectives

### 1.2.1 The objectives of this ICD are to provide:

- A description of the IBM Virtual Infrastructure Access Services product and details of its expected usage;
- Details of the IA claims made for the IBM Virtual Infrastructure Access Services product.

## 1.3 Purpose of Document

1.3.1 This document is the ICD for IBM Virtual Infrastructure Access Services product

1.3.2 This ICD is the baseline document for the CCT Mark Claims Test for the IBM Virtual Infrastructure Access Services product.

## 1.4 Structure

The structure of this ICD is as follows:

- Section 1 (this section) contains the introductory material;
- Section 2 contains the description of functionality of the IBM Virtual Infrastructure Access Services product and all the information related to the security of the IBM Virtual Infrastructure Access Services product
- Section 3 details the security functionality claims that are being made.

## 2 Product/Service Description

IBM Virtual Infrastructure Access Services is an enterprise class virtual infrastructure product.

### 2.1 Product/Service Identification

- Product name: IBM Virtual Infrastructure Access Services
- Product version: 5.5b
- Platforms:

<b>Name</b>	<b>Version</b>
Red Hat Enterprise Linux (ES)	3 Update 8
Microsoft Windows Server Standard Edition	2003
IBM Java 2 JRE	1.4.1-8
IBM Java 2 SDK	1.4.1-9
IBM HTTP Server	1.3.28
IBM MQ Series	6.0.0
IBM DB2	8.2 FP5
IBM Tivoli Directory Server (includes GSKit 7.0.1.16)	5.0 FP3
IBM WebSphere Portal Enable for Multiplatforms	5
IBM Virtual Infrastructure Access Services	5.5b

○ **Client:**

IBM provides as part of the IBM's Virtual Infrastructure Access Services product (5.5b) a client image that satisfies the following minimum specifications.

Note other Browsers and Operating systems are fully compatible with this solution and are provided here.

Operating System:

- Microsoft Windows XP SP2

Java:

- Sun Java 1.4 or higher

Browser:

- Internet Explorer 6 SP 2 (or higher)

<b>Operating System</b>	<b>Version</b>	<b>Browser</b>	<b>Version</b>
-------------------------	----------------	----------------	----------------

<b>Windows XP</b>	<b>Professional</b>	<b>Internet Explorer</b>	<b>6.0</b>
<b>Sun Java</b>	<b>J2SE v1.4.2_14.jre</b>		

## **2.2 Product Overview**

IBM Virtual Infrastructure Access Services is an enterprise class virtual infrastructure product. It provides the cross platform connection broker, security, scalability and manageability capabilities needed to simplify and centralise IT infrastructure. IBM Virtual Infrastructure Access Services is a complete desktop virtualisation product. It provides seamless, secure connectivity to all commonly-used application platforms including:

- Microsoft Terminal Server NT4, 2000 and 2003
- Web applications
- Terminal applications (3270, 5250)
- Linux applications
- Windows XP workstations.

### **Key features of IBM Virtual Infrastructure Access Services are:**

- Access from anywhere with a network connection
- Websphere Portal interface
- Multiple authentication options
- Secure access to applications and services
- Provision of legacy applications
- Centralised management of users and application entitlements
- User synchronisation with Active Directory for simplified user management
- Backend resource management and load balancing
- Extensive platform and application SSO options
- Scalable
- Wide range of deployment options

### **The basic architecture (as shown in Figure 1) consists of:**

- Client device: the user connects to IBM Virtual Infrastructure Access Services to access the backend resources and applications.
- IBM Virtual Infrastructure Access Services: the core platform that enables remote access, user personalisation and application management.
- Back-end terminal servers and existing systems and data: the resources that are being managed.

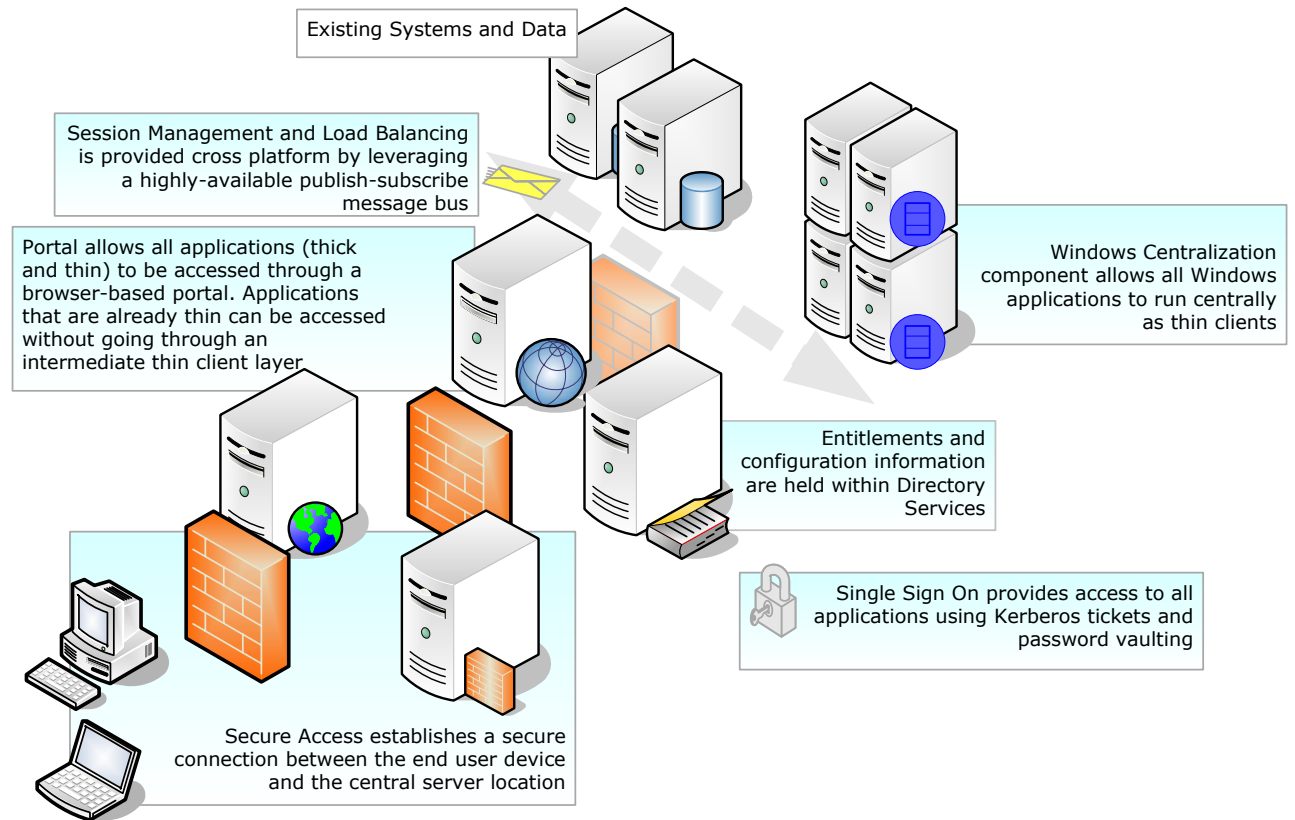


Figure 1: Overview of IBM Virtual Infrastructure Access Services

**The core IBM Virtual Infrastructure Access Services platform consists of:**

- LDAP Directory
  - IBM Tivoli Directory Server
  - Contains all the system configuration and policy settings including users, groups, applications, application assignments and servers.
  - IBM Virtual Infrastructure Access Services implements many extensions to the directory, including data referrals, data triggers and automated password encryption.
- Portal server
  - IBM WebSphere Portal Server Enable 5
  - A J2EE-based portal hosting IBM Virtual Infrastructure Access Services portlets/applications, including:
    - Authentication
    - Applications
    - Administration
    - User information
    - SSO credential management

- Web Server
  - IBM HTTP Server
  - Front end to the portal server, provides:
    - SSL termination
    - Load balancing and session affinity for portal instances.
- Tunnel Server
  - Bespoke Java-based service; the server for the secure tunnel.
  - Together with the tunnel client, this provides reliable, secure connectivity to IBM Virtual Infrastructure Access Services, including automated reconnection after client network failures.
- Agent
  - Bespoke Windows platform agent, installed on managed terminal servers and XP instances in the backend.
  - Provides load balancing, session management, application virtualisation and SSO (platform and application) services.

### **2.2.1 Security architecture**

### **2.2.2 IBM Virtual Infrastructure Access Services is designed to:**

- Provide secure access to an enterprise's applications from any network connected location, both internal to the enterprise and over the Internet;
- Allow the simple administration of users and entitled applications;
- Enable platform and application SSO.

### **Secure access**

#### **[Claim Ref VIAC01](#)**

To begin using IBM Virtual Infrastructure Access Services, the user uses a browser (see Diagram 1) to connect and authenticate over an SSL (see Diagram 2) connection with the IBM Virtual Infrastructure Access Services portal. This tunnelled connection is a standard HTTPS browser connection. IBM Virtual Infrastructure Access Services has extended WebSphere Portal Server with additional authentication methods including password, external directory (e.g. Novell eDirectory and Microsoft Active Directory) and SPNEGO.

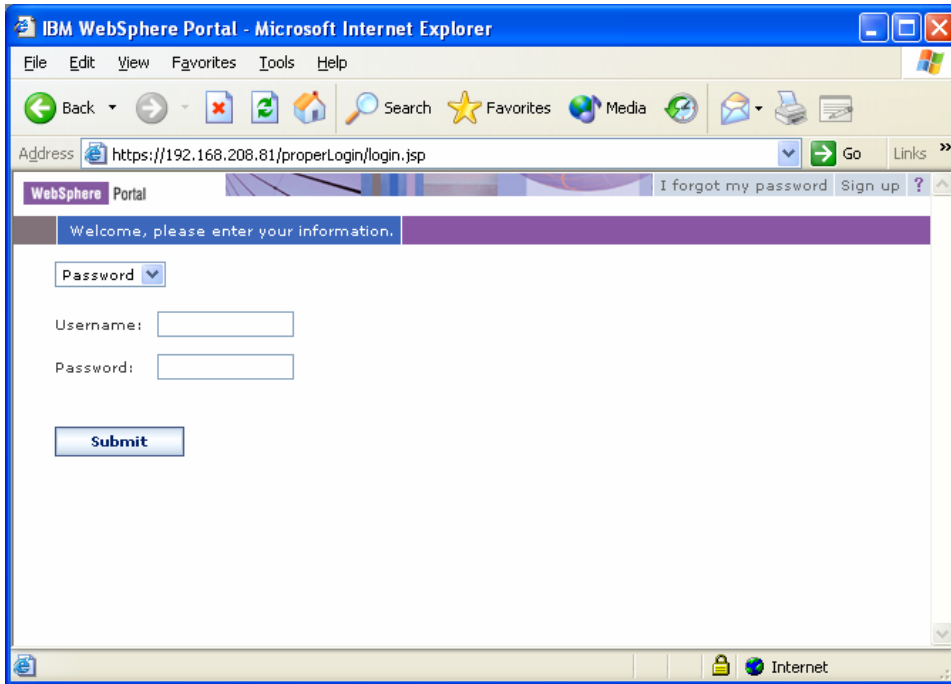


Diagram 1 – Portal Presentation for IBM Virtual Infrastructure Access Services

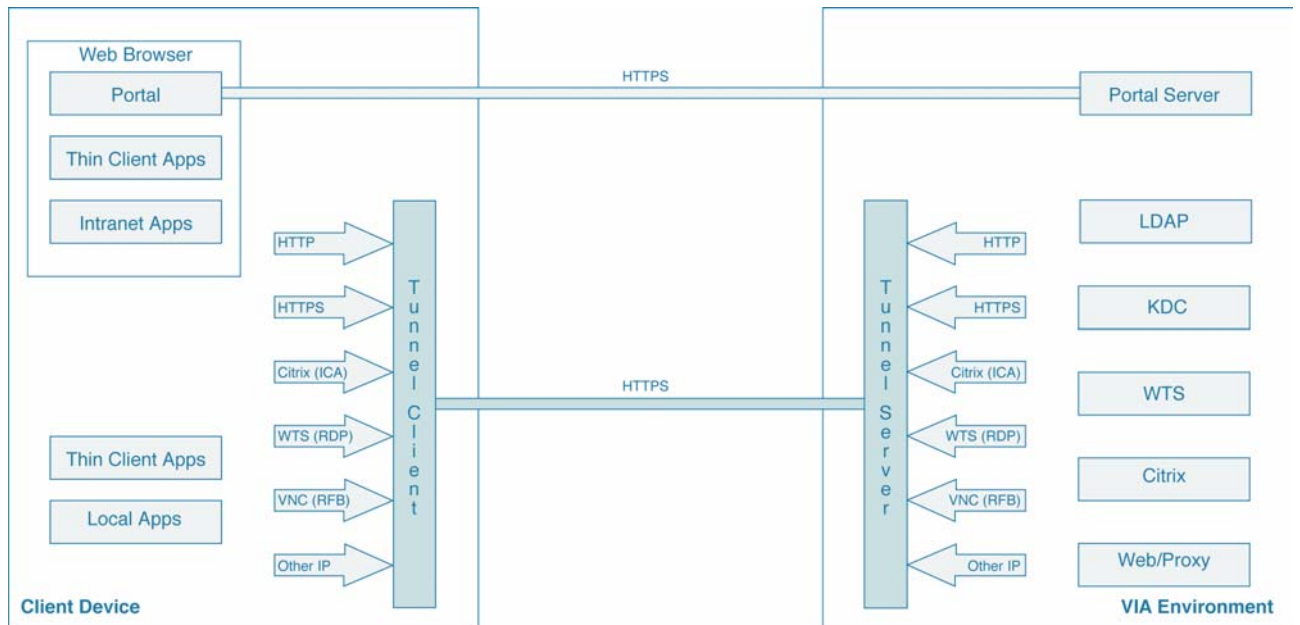


Diagram 2 - Secure Tunnel Connection

**Claim Ref VIAC04**

To connect to the IBM Virtual Infrastructure Access Services the user must supply the correct choice of credentials that are implemented within the back-end servers and that adhere to one or more of the authentication methods detailed above. Without this authentication step an unauthorised user will not be able to access the environment. Diagram 3 shows the connection process that a user’s connection would travel in order to securely connect to the back-end servers.

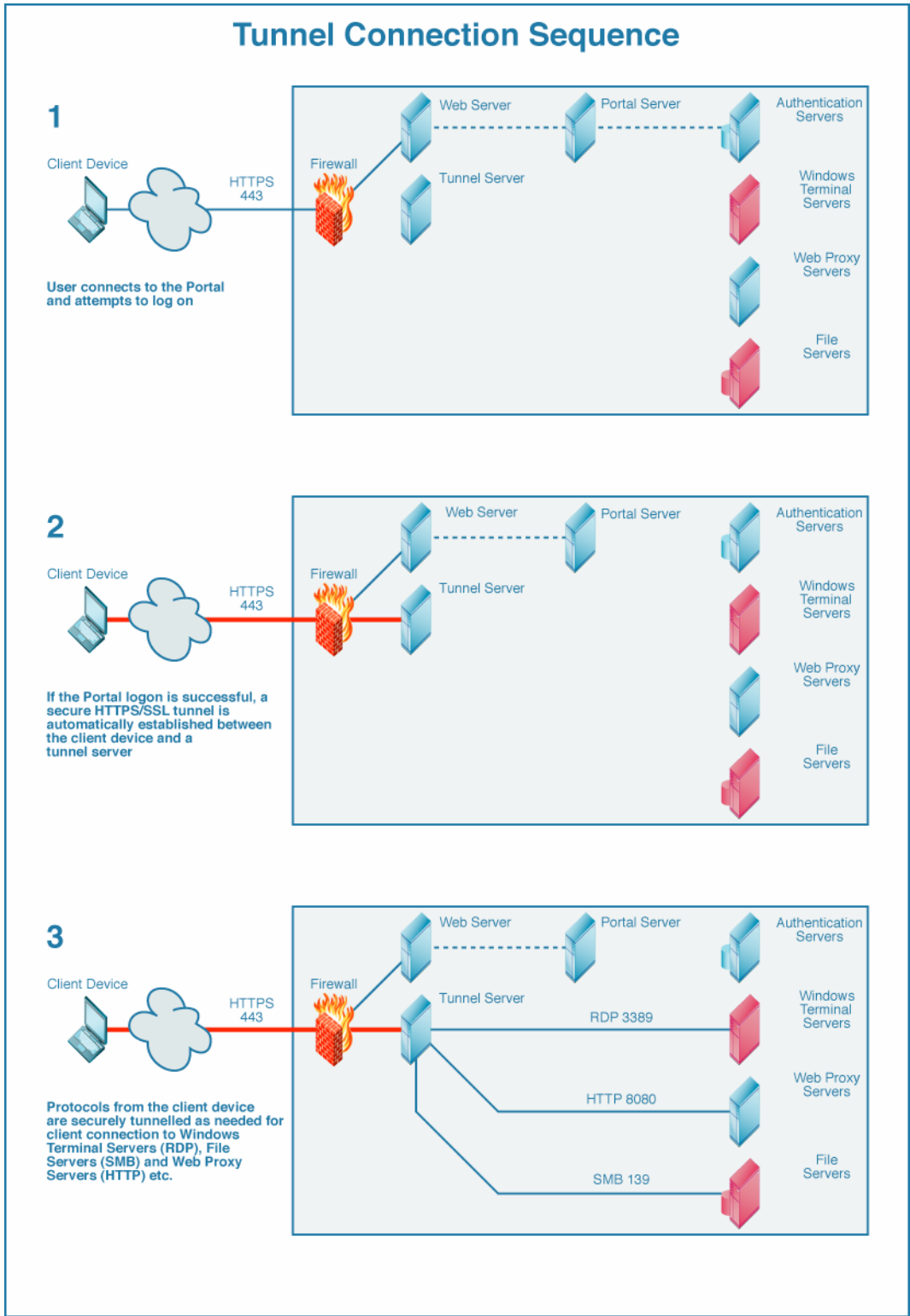


Diagram 3 – User Secure Tunnel Connection overview

**Claim Ref VIAC03**

IBM Virtual Infrastructure Access Services can be deployed in many different configurations taking into account network topology and DMZ requirements. Typically, for full Internet facing deployments, it is deployed with two access zones: Internal and Internet. These are implemented by separate sets of web and tunnel servers deployed internally and in an Internet-facing DMZ

respectively. The user is presented with a tailored set of authentication method options depending on the access zone they connect to. Usually internal access allows Active Directory password and SPNEGO authentication.

#### [Claim Ref VIAC02](#)

Once a secure portal session is established, the tunnel client is automatically downloaded and started using Java WebStart, providing the user with a secure transport for all other traffic to the IBM Virtual Infrastructure Access Services environment. The tunnel brokers connectivity between the client device and the application platforms in the enterprise. It is an SSL VPN, raising local listeners to provide tunnelled access to specific backend services. The listeners are raised dynamically as needed by IBM Virtual Infrastructure Access Services and typically only allow a single connection from the client device before being closed. This helps to ensure that only the minimum required access to the enterprise is opened up.

#### [Claim Ref VIAC07](#)

In the event of a network outage at the server end or a user initiated disconnection from the system (network cable unplugged for example) the tunnel will utilise it's re-connection feature which will poll the client device until the network connection (cable is plugged back in) is re-established and will then re-authenticate the client in the background in order to allow the user to continue to work where they left off. The tunnel re-connection feature of the solution will utilise the dynamic listeners as required in order to re-establish this connection.

#### [Claim Ref VIAC15](#)

Sessions with IBM Virtual Infrastructure Access Services have a maximum life, requiring the user to re-authenticate when the session has expired. Typically maximum session lifetime is configured as 10 hours though this may be changed by an administrator.

### **Administration**

#### [Claim Ref VIAC12](#)

IBM Virtual Infrastructure Access Services uses an LDAP directory at its heart to store policy, user, application, entitlement and server information. The standard directory service is extended with plugins enabling the following features:

- Referrals: automatic population of attribute values with data from elsewhere in the same directory, from external directories or from bespoke commands executed on the directory server itself.
- Triggers: automatic pushing of data to other records or systems when entries are modified.
- Unique number generation: allows the automatic generation of unique identifiers (e.g. when adding users).
- Password encryption: automatically encrypt designated attributes when set in plain text. The following encryption/hashing methods are

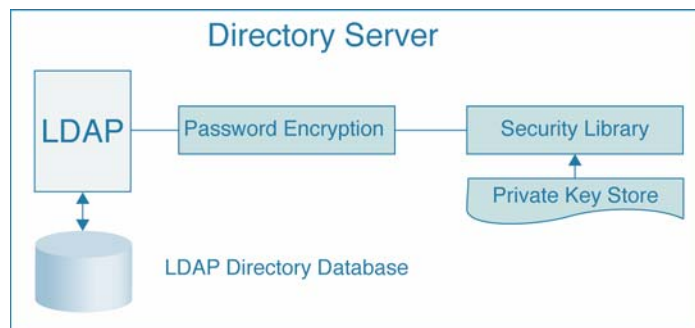
supported: MD4 (for NT passwords used by a Samba Domain Controller), SMBDES (for LAN Manager passwords used by the Samba Domain Controller), 3DES (a base-64 representation of a triple DES or AES encrypted value), DES-BASE64 (a simple DES-based password scrambling mechanism), AD-UNICODE-DES-BASE64 (a base-64 representation of a DES encrypted Active Directory unicode password).

- Extensible replication: allows data to be replicated to external directory systems (e.g. Active Directory).
- SASL binding: enabling Kerberos-based authentication with LDAP.

In the IBM Virtual Infrastructure Access Services Directory environment, user credentials such as passwords, Kerberos authKeys, Windows passwords etc. are stored in LDAP with the user's LDAP user entry. There are several encryption mechanisms that are used to protect these credentials.

The IBM Virtual Infrastructure Access Services Password Encryption plug-in integrated with the LDAP directory manages this encryption automatically for any specified LDAP attribute. When a protected attribute value such as a password is set, the encryption plug-in automatically applies the appropriate encryption before the attribute is stored in LDAP.

Diagram 4 shows the Password Encryption plugin. For 3DES triple DES and AES encryption, the plugin uses a security library to perform the encryption based on a private keystore containing encrypted private keys.



**Diagram 4: Automated Password Encryption Plugin**

### [Claim Ref VIAC11](#)

The directory data is managed by administrators using a configurable web application. Administrators authenticate as themselves to this application (and the underlying directory) and all security is delegated to the LDAP directory and its access control lists (ACLs). Cut down versions of this application can be assigned to groups such as “security administrators” for performing password resets. In this way administration can be tailored to existing processes and roles in the customer organisation.

#### [Claim Ref VIAC14](#)

When synchronised with Active Directory/eDirectory, much of the user and entitlement administration can be performed in the standard Active Directory/eDirectory user management consoles.

#### Entitlements

The IBM Virtual Infrastructure Access Services solution utilises entitlements (privilege based) controlled through the extensible LDAP schema to ensure that user access and application access is controlled securely and centrally.

#### [Claim Ref VIAC19](#)

In order to access any restricted areas with the IBM Virtual Infrastructure Access Services environment the support personnel must be members of the Administrator group. As privileged members of this group they are able to add, remove or grant usage access permissions to standard users within the environment.

Only designated root Administrators of the IBM Virtual Infrastructure Access Services are able to perform these roles.

#### [Claim Ref VIAC08 & Claim RefVIAC09](#)

Entitlements allow the IBM Virtual Infrastructure Access Services administrators to assign permissions to single users, groups of users and applications.

These entitlements also allow secure location awareness to be employed within the solution to restrict access and applications from non trusted subnets (if required) as well as providing print availability to users based on their individual or group requirements.

Control of the Entitlements database can be delegated to trusted users within an organisation to self provision applications or new users into the enterprise

#### SSO

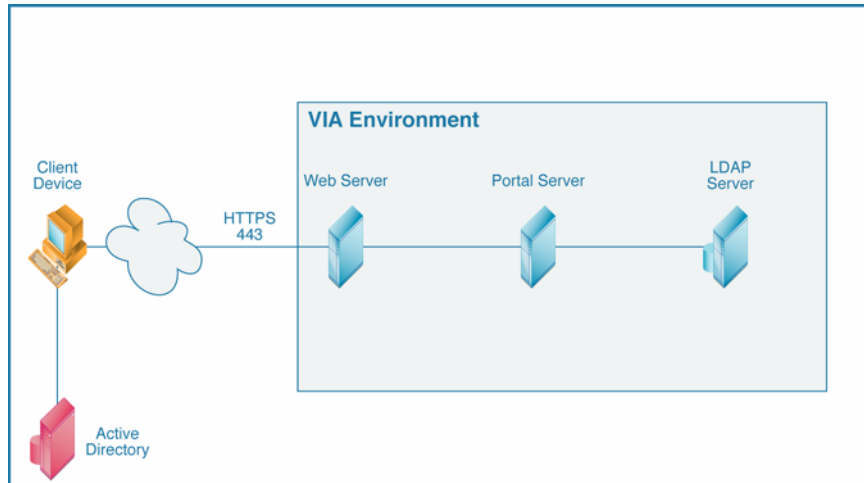
IBM Virtual Infrastructure Access Services provides several types of SSO:

- Portal session SSO, and
- Windows session and application SSO.

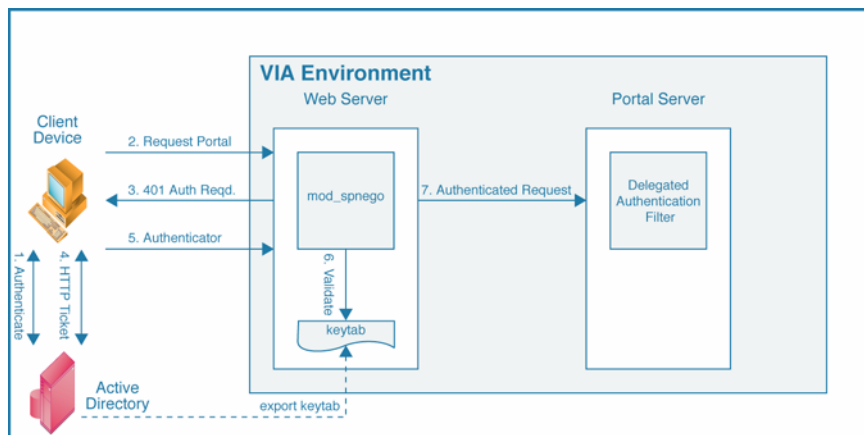
**Claim Ref VIAC16**

Portal session SSO is provided by the SPNEGO authentication extension to WebSphere Portal Server. This allows a client session that is already authenticated to a Windows Active Directory to sign into the Portal automatically using the standard Microsoft SPNEGO method.

Diagram 5 shows the process undertaken to create portal session SSO using SPNEGO. Diagram 6 shows the Portal session SSO authentication steps.



**Diagram 5 – Portal session SSO connection process**



**Diagram 6 – Portal session SSO authentication process**

**Claim Ref VIA C17 & Claim Ref VIAC18**

IBM Virtual Infrastructure Access Services also provides the ability to SSO into target desktops and hosted applications. When the user launches an application hosted on a managed terminal server (or Windows XP instance), IBM Virtual Infrastructure Access Services negotiates a new session on the server if one does not already exist. The user is automatically signed into the new session using credentials stored in LDAP. Once the new session is established (or an existing session is identified), IBM Virtual Infrastructure Access Services instructs the agent to start the required application.

An application entry in LDAP can contain SSO rules to allow the agent to identify if the application requires its own authentication. If these rules trigger

an SSO action, then credentials are fetched from LDAP and supplied to the application according to the rules.

### [Claim Ref VIAC13](#)

SSO credentials are stored in LDAP in encrypted form. Users can manage their own credentials using a portal-based application.

### 2.2.3 Hardware requirements

Any client device capable of running Java (1.3 or above) and a Web browser.

### 2.2.4 Software requirements

#### Client requirements:

- Operating System:
  - Microsoft Windows XP SP2
- Java:
  - Sun Java 1.4 or higher
- Browser:
  - Internet Explorer 6 SP 2 (or higher)

Operating System	Version	Browser	Version
Windows XP	Professional	Internet Explorer	6.0
Sun Java	J2SE v1.4.2_14.jre		

#### Server requirements:

<i>Name</i>	<i>Version</i>
Red Hat Enterprise Linux (ES)	3 Update 8
Microsoft Windows Server Standard Edition	2003
IBM Java 2 JRE	1.4.1-8
IBM Java 2 SDK	1.4.1-9
IBM HTTP Server	1.3.28
IBM MQ Series	6.0.0
IBM DB2	8.2 FP5
IBM Tivoli Directory Server (includes GSKit 7.0.1.16)	5.0 FP3
IBM WebSphere Portal Enable for Multiplatforms	5

<b>Name</b>	<b>Version</b>
IBM Virtual Infrastructure Access Services	5.5b

## **2.2.5 Out of Scope**

### **2.2.5.1**

#### **RSA SecurID Testing**

*We are not seeking testing of this area of the solution.*

#### **Client Operating Systems**

The following clients are fully compatible with IBM Virtual Infrastructure Access Services.

*We are not seeking specific testing of these clients within the solution.*

- Microsoft Windows 2000 Professional
- Microsoft Windows XPe
- Linux Clients (all versions)
- Macintosh (all versions)

#### **Java**

The following Java components are fully compatible with IBM Virtual Infrastructure Access Services.

*We are not seeking specific testing of these Java component within the solution.*

- IBM Java version 5

#### **Internet Browsers**

The following Internet Browser components are fully compatible with IBM Virtual Infrastructure Access Services.

*We are not seeking specific testing of these Internet Browsers within the solution.*

- Mozilla based browsers
- Safari

- Opera

### Client Applications

*We are not seeking testing of client specific applications.*

### Services

The scope of the claims testing is the IBM Virtual Infrastructure Access Services product infrastructure only. Due to the complex nature of the product and high skill levels required (a comprehensive understanding of general networking fundamentals, Linux, Windows, Directory Services, Terminal Services and security) to set-up, configure and run IBM Virtual Infrastructure Access Services some clients may choose to use IBM professional services for these tasks.

*We are not seeking testing of IBM Professional Services.*

## **2.3 Usage assumptions**

### **2.3.1 Assets**

IBM Virtual Infrastructure Access Services protects against the unauthorised access to, and usage of, enterprise applications.

### **2.3.2 Threat scenario**

**IBM Virtual Infrastructure Access Services is designed to counter the following threats:**

#### **[Claim Ref VIAC05](#)**

1. Unauthorised access to the application execution environment.
  - Session authentication required.

#### **[Claim Ref VIAC06](#)**

- IBM Virtual Infrastructure Access Services acts as a firewall between the client and servers. Connections through the tunnel are raised dynamically as needed by the IBM Virtual Infrastructure Access Services solution to enable application access based on user attributes/permissions policies.
2. Unwanted disclosure of authentication data (e.g. passwords).
    - Use of SSO prevents users remembering/recording multiple passwords in insecure ways.

#### **[Claim Ref VIAC10](#)**

- SSO data is stored in an encrypted form in the directory.
3. Eavesdropping on traffic between a client and the system.

- All client-to-IBM Virtual Infrastructure Access Services data is carried over SSL channels.
4. Indefinite session tailgating.
- Each IBM Virtual Infrastructure Access Services sessions has a limited lifetime.

### **2.3.2.1 Expected operational environment**

IBM Virtual Infrastructure Access Services is designed to be deployed in large enterprise environments, catering for thousands of users. It can be deployed in complex network topologies, including with multiple DMZs and internal firewalls. It integrates with existing user directory solutions for ease of administration. It can be deployed in live-live multi-site configurations for resilience.

The individual server and client OS requirements are covered elsewhere in this document, and as IBM Virtual Infrastructure Access Services sits on a dedicated platform there are few operational environment requirements. The expectation would be that the servers are installed in a data-centre environment with cooling, power and network connectivity supplied commensurate with the selected hardware platform, physical environment and expected through-put.

High-availability implementations are possible, again depending on customer requirements but are not required for the operation of IBM Virtual Infrastructure Access Services.

The IBM Virtual Infrastructure Access Services virtualisation platform gives customers the following main benefits:

- Increased business flexibility
  - Users have more flexibility since they have access to all their existing resources, whether they are inside the firewall or remote
- Increased control where it matters
  - IT has centralised control over user security, applications and data access improving compliance and reducing risk
- Lower cost
  - Simplification and centralisation of the IT infrastructure drives significant cost reductions in distributed support, hardware, software, networks and security

### **2.3.2.2 Organisational security policies**

IBM Virtual Infrastructure Access Services supports the following elements of an organisation's security policy:

- Authentication policy
  - Choice of authentication method by access zone
- Internet connectivity
  - Support for DMZ architectures
- Password policies
  - Delegated to LDAP
- Administration role division and allocation
  - Publishing applications to specific roles
  - Subset administration tools can be created
  - LDAP ACL's can control access by role
- Application availability policies
  - Publishing model of entitlements
- Software licensing policies
  - Close control over entitlements

### 2.3.2.3 Security requirements on the environment

The following are requirements for the security of the environment:

- Administration/Installation staff follow the security lock-down procedure as part of the product installation.
- Suitable firewall protection is provided around the core IBM Virtual Infrastructure Access Services product, separating it (and the protected resources) from the Internet.
- Security features of the product are not disabled.

## 3 Security Claims for the IS Product or IS Service

### 3.1 Claims Statements

Unique Reference	Claims Statements
	<b>Encryption</b>
<a href="#">VIAC01</a>	Browser to IBM Virtual Infrastructure Access Services connections is secured using SSL.
<a href="#">VIAC02</a>	Tunnelled traffic to IBM Virtual Infrastructure Access Services is secured using SSL.
	<b>Authentication</b>

<a href="#">VIAC03</a>	User authentication mechanisms supported: LDAP Password External Directory (including Active Directory) SPNEGO
<a href="#">VIAC04</a>	Unauthorised users are denied access to the Virtual Infrastructure Access Service by the authentication mechanism implemented.
	<b>Connectivity</b>
<a href="#">VIAC05</a>	By default, clients do not connect directly to backend servers. (Note: it is possible to configure IBM Virtual Infrastructure Access Services to connect directly to the backend server, bypassing the tunnel. This style of application is not covered by this claim.)
<a href="#">VIAC06</a>	The tunnel acts as a firewall between the client and the IBM Virtual Infrastructure Access Services environment. Connections through the tunnel are raised dynamically as needed by IBM Virtual Infrastructure Access Services to enable application access.
<a href="#">VIAC07</a>	Tunnel reconnection is authenticated.
	<b>Entitlements</b>
<a href="#">VIAC08</a>	Users can be members of groups.
<a href="#">VIAC09</a>	Applications are published to users and/or groups.
	<b>Directory</b>
<a href="#">VIAC10</a>	Directory access that contains user data between the client and the Virtual Infrastructure Access Services is encrypted using SSL. (Note: monitoring access is not encrypted.)
<a href="#">VIAC11</a>	Password policy (length, age) is inherited from the underlying directory.
<a href="#">VIAC12</a>	The password plugin enables auto-encryption of selected directory attributes.
<a href="#">VIAC13</a>	SSO password data is stored in encrypted form.
<a href="#">VIAC14</a>	Active Directory synchronisation allows users and groups to be managed in Active Directory.
	<b>Sessions</b>
<a href="#">VIAC15</a>	User sessions are time-limited (10 hours by default though this may be changed by an administrator). Re-authentication is needed when a session times out.
	<b>SSO</b>
<a href="#">VIAC16</a>	Portal session SSO using SPNEGO is supported.
<a href="#">VIAC17</a>	Windows Terminal Server session SSO is supported.

<a href="#"><u>VIAC18</u></a>	Windows application SSO is supported for applications running on Managed Terminal Servers.
<a href="#"><u>VIAC19</u></a>	Only Administrators of the system are able to add/remove and grant group usage privileges to users. Administrators are also able to alter password policy (length, age) in order to satisfy the security requirements of the organisation where the product is to be implemented.

### **3.2 Existing assurance certificates**

None

## Annex A - Glossary of Terms

Term	Definition
Active Directory	Microsoft's directory-based security system for managing deployments of Windows machines. Active Directory (AD) also presents an LDAP interface.
eDirectory	Novell's directory-based security system for managing deployments of Windows machines
AES	Advanced Encryption Standard; a well known and tested symmetric key encryption algorithm. Sometimes known as Rijndael.
DES	Data Encryption Standard; a well known and tested symmetric key encryption algorithm.
DMZ	De-Militarised Zone; a computer network arrangement used to provide a protection zone between two other networks. Typically used when providing services to the Internet whilst protecting the internal network of an organisation.
Firewall	Generically, system that connects two networks together whilst protecting one network from the other. This protection is provided by carefully controlling what communications are allowed between the networks. More specifically, this term usually refers to packet filtering software that controls which network packets are passed from one network to another.
HTTPS	HTTP over SSL; running HTTP traffic (standard web traffic) over an SSL connection to provide service authentication and traffic encryption.
J2EE	Java 2 Enterprise Edition; a standardised Java framework for building enterprise class Java web applications.
Java WebStart	A Java technology for the automatic downloading and execution of Java programs over a network.
LDAP	Lightweight Directory Access Protocol; a standard for accessing directory information over networks. An LDAP server stores directory data (arranged in a tree-like structure) and provides an LDAP interface to other components.
Portal	A web-based application that consolidates smaller applications (portlets) into a single, consistent view.
SPNEGO	Simple and Protected gssapi NEGOTiation mechanism; A standard for negotiating an authentication mechanism between a client and server. Used by Microsoft to negotiate Kerberos authentication from a domain-authenticated client to a network service. This is known as "Integrated Windows Authentication" by Microsoft.
SSL	Secure Sockets Layer; a standard protocol for authenticating and encrypting network traffic that

	combines public key cryptography with symmetric key cryptography. Specifically, SSL avoids the need to manage the distribution of private keys to enable high performance symmetric key cryptography. The standardised version of SSL is called TLS (Transport Layer Security).
SSL VPN	The generic term for a system that routes traffic from one location on the network to another by encapsulating it in an SSL-protected datastream. This is sometimes called SSL Tunnelling.
SSO	Single Sign-On; a technique where the computer system will automatically supply user credentials to another system so that the user does not need to enter them. Used to improve the user experience of the overall system.
Terminal server	A server used to host multiple user desktops or applications concurrently.

## **Annex B - Marketing Statement**

The IBM Virtual Infrastructure Access Services product allows authorised users to connect through any Java enabled Web browser securely over the internet to an enabled application within their enterprise. The solution combines portal, Thin client, messaging, and security technologies delivered through a single, consistent delivery framework founded upon a standard and scalable set of Internet architecture principles.

IBM Virtual Infrastructure Access Services is an effective way of delivering distributed infrastructure solutions featuring:

- Single Sign On;
- Single Logical Access point - one entry point allows greater control;
- Simplified Portal presentation

Note: The scope of the claims testing is the IBM Virtual Infrastructure Access Services product infrastructure only. Testing of client specific applications on the IBM Virtual Infrastructure Access Services infrastructure has not been undertaken.