

HL-hybris' Security Features

Author: Steve Grundy

Version: 1.1

Date: 2nd June 2008

1. Introduction

The HL-hybris system is designed to provide NHS Trusts and their Suppliers with the ability to manage catalogue and contract information.

It is recognised that this data is highly confidential and Healthlogistics.co.uk Limited operates a strict Data Security Policy [Ref: 5].

The HL-hybris system consists of an application server and a database server, hosted by an experienced and reliable Internet Service Provider (ISP) with extensive experience of supporting secure applications for banks, international businesses, the Ministry of Defence and local government.

'The implementation and hosting of the HL-hybris system conforms to the relevant requirements of the NHS Standards Enforcement in Procurement, the e-Government Interoperability Framework (e-Gif) and BS ISO/IEC 27002:2005'.

2. References

Ref: 1	NHS Information Security Management Standards Strategy and Procurement Policy	V.10 April 2004
Ref: 2	NHS Standards Enforcement in Procurement	V.10 April 2004
Ref: 3	Information Technology – Security Techniques – Code of Practice for Information Management Security	BS ISO/IEC 27002:2005
Ref: 4	e-Government Interoperability Framework (e-Gif)	Version 6.1
Ref: 5	Healthlogistics.co.uk Limited Data Security Policy	Version 1.0
Ref: 6	HL-hybris User Registration Process	Version 1.0

3. System Architecture Security Features

The security and integrity of the HL-hybris system, including all data, is maintained by a multi-layered approach.

3.1. *Hosting and Server Security*

All servers are fully managed by the hosting company, providing the following:

- All servers held in secure, temperature controlled environment
- RAID 1 configuration with mirrored hard drives
- Dedicated hardware Firewall
- 24/7 ICMP, HTTP, FTP and SMTP monitoring
- Automatically updated anti-virus software
- Weekly full backups
- Daily incremental backups
- 24 hr. helpdesk
- 2 hr hardware replacement guarantee
- Automatically updated anti-virus software
- SSH public-key cryptography for communication of all data and user authentication.

3.2. *System Security*

3.2.1 *Information Security Management*

The systems implemented by Healthlogistics.co.uk Limited, including its selected hosting supplier, allow the implementation of the facilities defined in Information Technology - Security Techniques – Code of Practice for Information Management Security [Ref: 3] and the relevant sections of the NHS Standards Enforcement in Procurement [Ref: 2].

3.2.2 *System Access*

The browser interfaces do not contravene the e-GIF policies and associated specifications for e-services access as specified in e-Gif version 6 [Ref: 4].

3.2.3 *Internet Transfer Protocols*

There is a requirement for file transfer using the FTP protocol. The implementation of FTP supports restart and recovery. There is also a requirement to use HTTP for file transfer and the system conforms to HTTP/1.1 when transferring files.

3.2.4 *Web services*

The following web services security protocols are supported:

- JAX-WS, JAX-WSA, JSR-181, and SAAJ
- SOAP 1.1, 1.2, WS-I BasicProfile, WS-Security, WS-Addressing, WS-RM and WS-Policy
- WSDL 1.1 and 2.0
- MTOM

3.3. HL-hybris Security

The HL-hybris application manages the secure access of users to any information in the database via usernames and passwords. The security model is extensive. Each individual user to the system is identified by their unique username and password, changes made in the management console can be tracked within the system. Users may be assigned to groups and therefore inherit group privileges in addition to any specifically assigned to themselves. Privileges for users can be defined for access to each individual data object, be it a single product item price or a group of products.

The system holds catalogues and contact pricing as linked but separate objects, and is able to assign secure access to price lists independently of access to shared common data.

3.4. Database security

Data used by HL-hybris, including usernames, passwords and product data is stored in the database. The database can only be accessed from the HL-hybris application using a secure username and password configured within the HL-hybris application.

3.5. Process Security

3.5.1 User Access

Access to the HL-hybris system will require user registration and approval from the Healthlogistics.co.uk Limited Directors.

The granting of access will follow the HL-hybris User Registration Process. [Ref: 6] This process requires the Directors to assess any request for access using a number of criteria:

- The user has been verified as a staff member of an HL customer
- The user has followed the correct registration procedure including his/her manager's authorisation.
- The user's actual need
- The role to be assigned to the user
- What data should be accessed by the user
- An impact assessment on existing users, including identification of risks to external parties. For example, if there is any potential impact on existing users then their approval should be sought before access is granted, and this approval recorded.

If access is granted then the user will be provided with a username and password in separate, encrypted emails (PGP). At the first logon the user will be forced to change their password, which will be stored in encrypted format in the HL-hybris database.



Passwords will have to be changed by the user every 6 months, and password strength will be enforced by the system to require a mixture of character sets and be greater than 7 characters long.

If a user fails in 3 consecutive attempts to log on within a defined period, then the username will be locked out and will require Director approval to be unlocked.

Healthlogistics.co.uk Limited also operates a strict policy of access role separation. The HL-hybris server administrator will not be given the password to the HL-hybris database where all data is stored. The Server administrator and database administration will be performed by different people.

If Healthlogistics.co.uk Limited suspects that a username is not being used by the user to whom it has been assigned then they will disable access immediately for that user, and notify the HL customer contact of the organisation this user is part of.

3.5.2 Data Access

The security system operates on the principle of segregation of duties, whereby a user or administrator can only access data they have been assigned the privileges to access, and that are needed for them to fulfil their designated role. This access is determined at user registration and approved by the Healthlogistics.co.uk Limited Directors.

The access privileges will be provided to the registered user with their log on details. The HL-hybris system will enforce these access privileges.

4. Exclusions

Healthlogistics.co.uk Limited can accept no liability for the misuse of data once it has been downloaded from the HL-hybris system using a fully authorised and approved means.