GUIDE SPECIFICATION

VERSION 1.0.2.3

Network Harbor, Inc. is the developer of the Lions Gate™ Identity Management System (IDMS). The company is a Microsoft Certified Development Partner and a Microsoft Early Innovator parent, as well as a participating member of both the National Institute of Standards and Technology, and the Armed Forces Communication and Electronics Association. Members of Network Harbor, Inc.'s executive management and development staff have over 20 years of experience in security integration development and 15 years of experience in high capability IDMS development.

The Lions Gate suite of products, to be released this year, is the product of over two years of development, testing and quality assurance. It is designed to meet the robust identity management and visitor management requirements of government including the military and is fully integrated with the PIV and CAC smart cards issued by those agencies. It leverages that card, not only for three factor authenticated logon, but for the digital signing of every transaction performed in the software. It uses FIPS compliant PKI security for information transference, and allows for a consistently pleasant and efficient ultimate end-user (cardholder) experience, as well as allowing our customers to save substantial money, and have increased flexibility and control of their physical access control infrastructure.

For additional information, contact:

Network Harbor, Inc.
5607 South Washington St.
Bartonville, IL 61607
Phone: +1 309.633.9118
Web: http://www.networkharbor.com
Email: sales@networkharbor.com

PART 1 – GENERAL

This document is intended to provide an overview of the architecture of a simplified (one facility, one PACS system), high security (multiple sub-net), Lions Gate Enterprise Suite system. It is intended to be used as a guide, and not as a rigid design specification. There are many ways to configure these systems including having all components on a single network. This simply presents a single method whereby a client might break out the Lions Gate, and PACS systems to be running on separate networks.

The most important takeaway from this document is that despite how the PACS system SDK works, all communication from the Lions Gate Secure Messaging Server (LG-ESMS-1) to the Lions Gate PACS Communication Web Service (LG-PACS-CWS-1) is done in an encrypted manner. Many PACS systems rely on a relatively unsecure, even plain text, method of SDK provisioning so this method alleviates security concerns on that front. Even if the end result is that an XML file is written to a directory, that can be (if the LG-PACS-CWS-1) done on a single machine with only the user that the service is running on having any access to the directory where the file is written.

1.01 SUMMARY

Lions Gate was designed for Enterprise, high-security, settings, and as such is designed to keep as much data flow over long transmission pipes as secure as possible. In addition, Network Harbor management has foreseen a government transition to a system of back-end attribute exchange. While this specification is not yet finalized and is under development, the Lions Gate Enterprise Secure Messaging Server will be used to enable this functionality on Network Harbor’s technology roadmap for the product. In the meantime this suite of products provides a secure, reliable, and efficient means of transferring data to and from all PACS systems connected to the Lions Gate Enterprise System.

In the example entertained below, please refer to the “Lions Gate Secure Messaging Server and PACS Connectors” graphic below for a visual representation of the setup. Again, this is shown for a high-security setup where the client wishes to split the network that supports the PACS system(s) from that supporting the Lions Gate Clients and SQL Server. Many times the client will instead operate on a much simpler scenario where all these components will reside on a single network. As such, this is not meant to display the most likely scenario, but is meant to give the client and integrator an idea of how the use of the Lions Gate Secure Messaging Server and PACS connectors gives them much more flexibility in architecture design than other solutions might offer and enables extreme security levels that are otherwise unavailable.

Note that when comparing this diagram to that done for the Lions Gate Visitor Management System, that this entire network pertains to a single facility and could all be called the Life-Safety backbone from that diagram even though here it is presented as two different networks. Both of these networks handle secure, PACS and LACS related data and as such should be secured as much as possible from intrusion, malicious software, and other attacks.

1.02 DISCUSSION

A. There are a number of scenarios where data might be exchanged between the Lions Gate Clients (LG-SC-1) and the Lions Gate Enterprise Secure Messaging Server (LG-ESMS-1) and onto one or more Lions Gate PACS Connectors (LG-PACS-CWS-1) and vice versa (communication going in the opposite director from the connector to the Lions Gate SQL Server and ultimately to the client workstation. Some of these would be:

   a. After onboarding when the new person and credential record(s) are created in the underlying PACS systems for the first time.
   b. When a cardholder or credential record is updated (name change, status change, etc.).
   c. When additional access is granted to a credential or withdrawn.
   d. When someone in the PACS system creates a new reader, access code, or time code.

B. We will now discuss each of the above so that you can see how information goes from client to PACS (in the case of a, b, and c above), or flows from the PACS back to the Lions Gate SQL Server and ultimately to the Lions Gate Client (d above).

   a. After Onboarding (from 1.02 (A) (a) above).
      i. When an onboarding application is approved in the Lions Gate Client, the personnel and credential records are added to the Lions Gate SQL Server database, and the transaction is encrypted via a randomly generated symmetric key, and then the key is asymmetrically encrypted via the public key of the Lions Gate Secure Messaging Service (which is obtained at that moment).
      ii. The SendPersonnelTransaction method of the Lions Gate Secure Messaging Service is called and the encrypted data passes through the internal firewall to the server. There the symmetric key and the symmetric key alone is unencrypted.
      iii. Each of the Lions Gate PACS Connectors are registered with the Lions Gate Secure Messaging Server (LGSMS) (in the illustrated case below only a single PACS system is shown, but there may be several), so for each of these connectors the LGSMS re-encrypts the key using the public key of the Lions Gate PACS Connector (LGPACS) being notified and calls the SendPersonnelTransaction on that server.
      iv. The LGPACS decrypts the symmetric key for the transaction and then uses that symmetric key to decrypt the transaction. It then:
         1. Determines if any active access codes or readers have been passed with the transaction pertaining to its underlying PACS system. If no such codes exist it either deletes the record (if it exists) in the PACS, or disables it (depending on Administrator settings).
         2. If there are codes or readers that pertain to that PACS system it looks to see if the personnel and credential record already exist (in this case they do not). If not (as in this case), the software provisions the PACS system with the personnel, credential, and access records. It also provisions a field in the PACS system for both the personnel and credential records

with the primary key from the Lions Gate system for easy retrieval and verification of updates).

b. Upon Update (from 1.02 (A) (b) above).

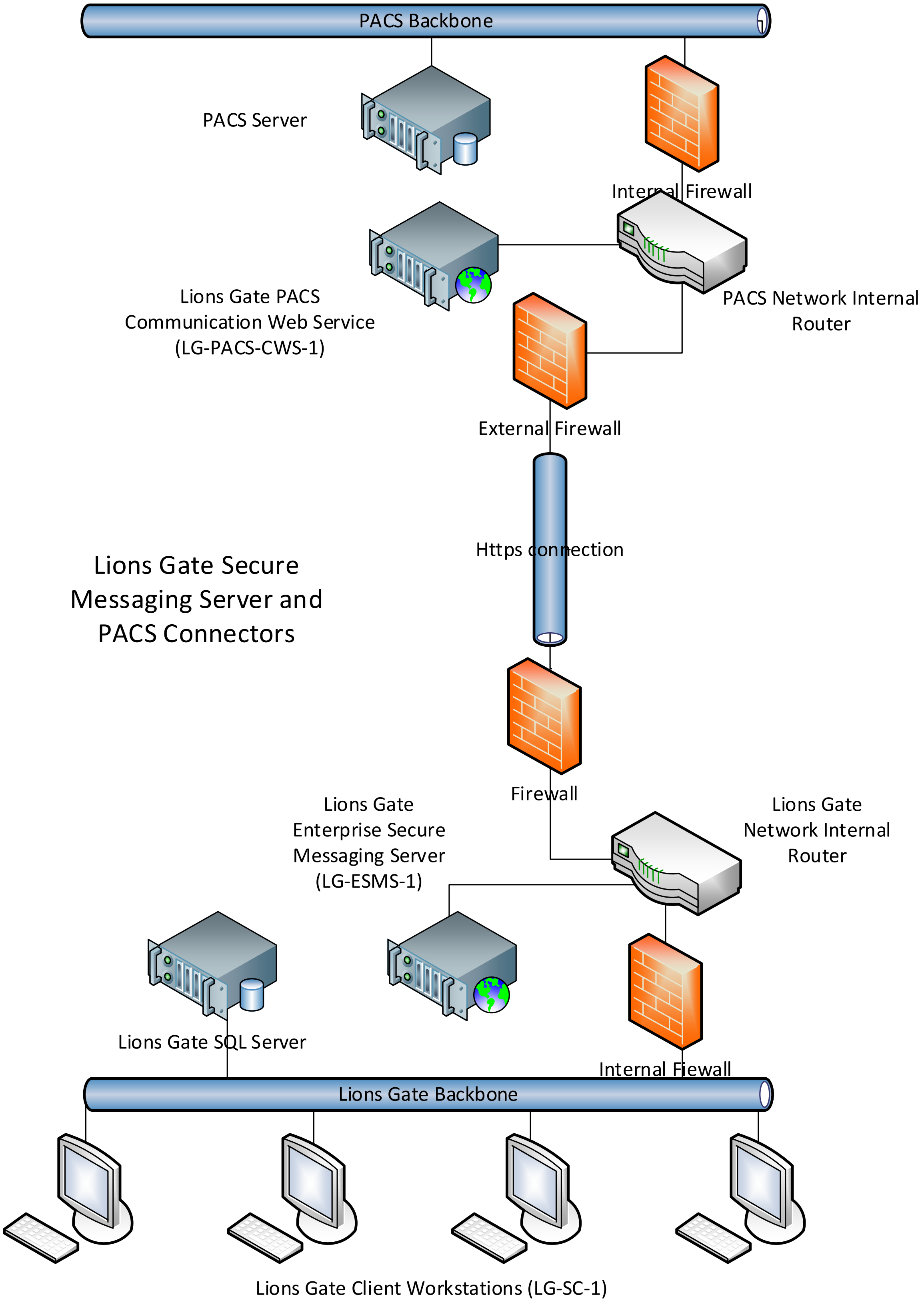
- i. This scenario works much like that in (1.02)(B)(a) above. When the personnel or credential record is updated, the transaction is encrypted just as in the above (1.02)(B)(a) scenario and the transaction passed to the LGSMS.
- ii. As in (1.02)(B)(a) above, the LGSMS decrypts the symmetric key only then encrypts it for each registered LGPACS connector and passes it to each.
- iii. As in (1.02)(B)(a) above, the LGPACS system determines if there are active access codes or readers associated with any active credentials. If there are not, the system performs the same action (deletion or disabling) if the record exists as in (1.02)(B)(a) above.
- iv. If there are active access codes or readers for an active credential the system determines if the personnel and credential record exists in the PACS. If they do not (for instance if this is the first time a code was added to an existing record for a person for this PACS), the record will be added just as in (1.02)(B)(a) above.
- v. If the records exist, they are updated to reflect the data items in the passed transaction including additions or deletions of access or change in time codes.

c. Upon a Change of Access (from 1.02 (A) (c) above).

- i. These transaction are handled exactly as in (1.02)(B)(b) above.

d. Upon creation of a new access code, reader, or time code in the PACS (from 1.02 (A) (d) above).

- i. The LGPACS windows service determines that a new access code, reader, or time code has appeared in the PACS database by periodic querying.
- ii. The LGPACS gathers the data for the new access code, reader, or time code and encrypts this as a transaction using a randomly generated symmetric key. This key is then encrypted using the LGSMS's current public key and the AddAccessCode, AddReader, or AddTimeCode function is called on the LGSMS web service as appropriate passing the encrypted transaction information and encrypted key.
- iii. The LGSMS decrypts the symmetric key and then decrypts the transaction and updates the Lions Gate SQL Server with the new access code, reader, or time code as appropriate placing them in the default access view (usually used as a holding area until an administrator can determine what access view the new access code or reader should belong to).
- iv. The code is available in the Lions Gate Client software for assignment to a record (assuming the User has appropriate access).


PACS Backbone
PACS Server
Internal Firewall
Lions Gate PACS Communication Web Service (LG-PACS-CWS-1)
PACS Network Internal Router
External Firewall
Https connection
Lions Gate Secure Messaging Server and PACS Connectors
Firewall
Lions Gate Enterprise Secure Messaging Server (LG-ESMS-1)
Lions Gate Network Internal Router
Lions Gate SQL Server
Internal Fiewall
Lions Gate Backbone
Lions Gate Client Workstations (LG-SC-1)