



Network
Harbor, inc.



Lions Gate™ Enterprise Visitor Management System

- Developed especially for government and military needs
- PIV/CAC three factor logon and integration
- Fully FIPS compliant PKI encryption

Trust, nonrepudiation and security. These are the primary needs of a secure government facility, essential to validate the presence of all persons on your grounds, guarantee them the proper protocols and access required for their roles, while maintaining the peace and protecting your property, both physical and logical.

At Network Harbor, we offer solutions that give government agencies and military facilities the tools they need to do their jobs well, while protecting our peace and their own installations, tools like our Lions Gate™ Enterprise software and its related Visitor Management System. Know everyone at your site, store every transaction they create, and make sure they have the means to do their jobs effectively and efficiently. That's why we develop the solutions that you trust.

Secure Visitor Management

Every governmental agency has visitors, and though the basics of visitor management (submission of visitor request, approval of the request, checking in for the request) are shared by everyone else who entertains visitors at their facilities, U.S. Government military and civilian agencies require a much more robust system tailored to the unique characteristics of their security needs, and utilizing and integrating their PIV and CAC smartcards with all of the security features inherent into the system. Further, this system should be integrated within their Identity Management System (IDMS) and their Physical Access Control System (PACS) so that the agencies business rules and procedures can be applied to the full population of personnel with access to agency assets.

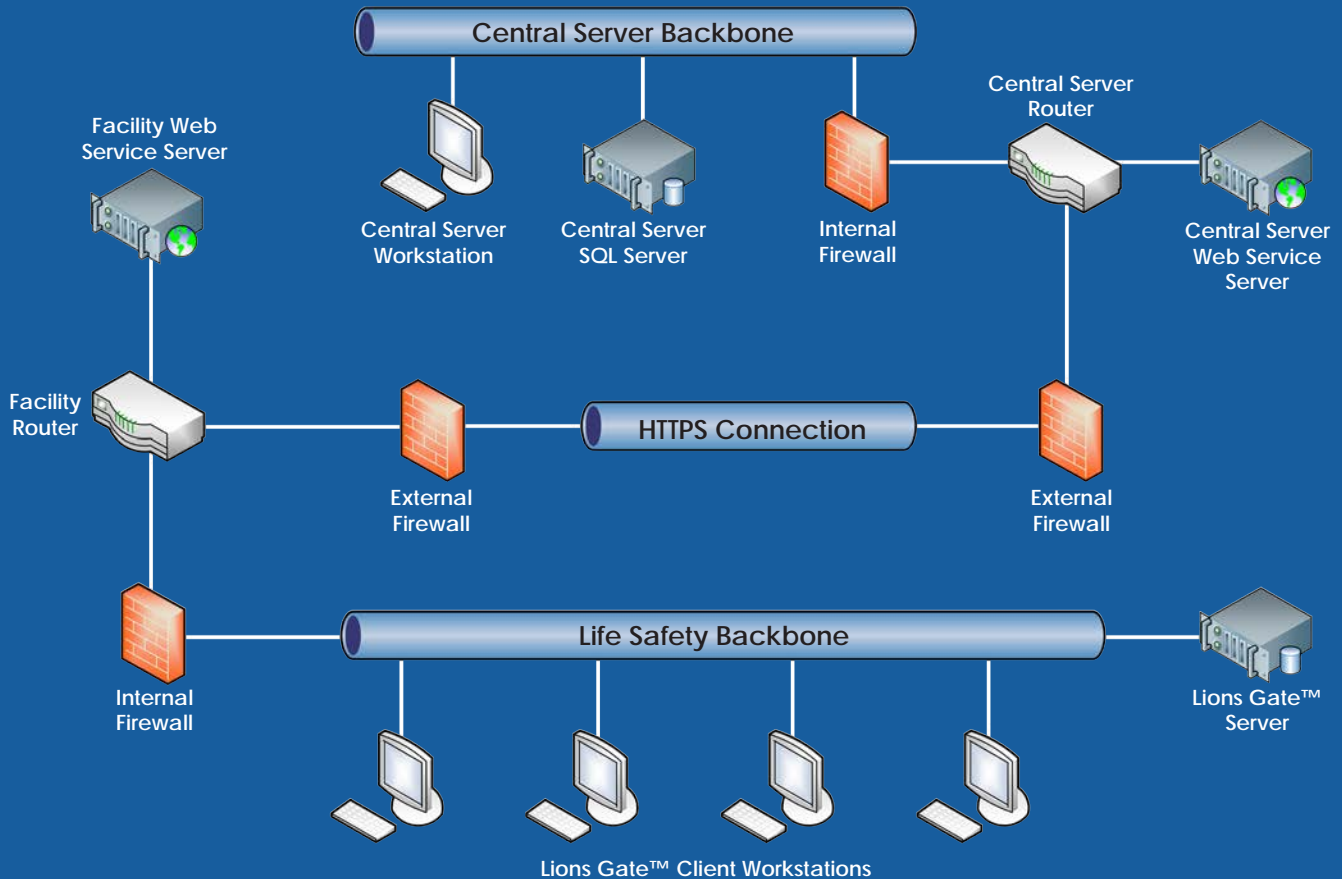
Until now, government agencies were faced with attempting to put together a system piece-meal with commercial components that were not designed from the ground up for military or agency use. These systems, lacking coherent integration with their other systems, can result in a mishmash of fragmented databases, none of which allow management to get a full picture of the personnel that have access to their facility, and none of which fully use the PIV or CAC card to provide the security that was promised with the adoption of these highly capable smart cards.

However, with the introduction of Lions Gate IDMS and its associated, and fully integrated, Visitor Management System, government agencies now have a system that is designed with the industrial strength features and security measures that these agencies need to fulfill mandated requirements. In addition to the everyday basic features of visitor management, Lions Gate™ offers a great many additional features such as listed below.

Key Features of Lions Gate™ VMS

- **Full integration with PIV and CAC cards.** Every visitor request in Lions Gate™ VMS must be initiated by a PIV or CAC cardholder (personnel without a PIV or CAC must be sponsored by someone with a PIV or CAC at the facility in question).
- **Digital certificates for every transaction.** Every transaction performed by a PIV or CAC cardholder in Lions Gate™ VMS is signed by the digital signing certificate contained on their card and this signature along with the public key is kept with the transaction for independent validation.
- **XML eSignatures captured for all users.** Legally valid eSignatures are captured for the applicant, sponsor, and approving user which contain the full XML for the application along with the signing statement. This is in addition to the digital signature created on-card by the PIV or CAC card.
- **Biometric capture of all applicants and sponsors.** Biometrics are captured for the applicant, and a biometric authentication is captured for the sponsor at the time that the sponsor approves the application as another method of assuring transaction security and non-repudiation.
- **Maintenance of clearance and access levels.** Government and military important information such as agency, rank, and security clearance and access level are captured and maintained in Lions Gate™ VMS.

Visitor Management Architecture



- **Association of credentials from legacy access control systems.** Lions Gate™ VMS allows for the association of legacy credentials with PIV or CAC cards to facilitate the continued interim use of legacy PACS systems while still allowing for the certificate revocation infrastructure security inherent in the PIV and CAC system to be used to invalidate the legacy credentials should the PIV or CAC be invalidated. This can provide significant flexibility, efficiency, and cost savings for the agency or facility involved.
- **Issuance of legacy visitor ID cards.** If a facility still uses legacy cards, the facility can allow site visitors or their sponsors (depending on how the administrator has setup the appointment) to print visitor identification cards through the Lions Gate™ Kiosk after biometric authentication has been performed.
- **Storage and reporting of complete transaction history.** Users of Lions Gate™ VMS have all of the information for a previous visitor at their fingertips for reporting and other purposes, including all of the past visits they have made, future visits scheduled, violations of security and other issues that were reported on them, contact information and all of the other pertinent information available to users within the Lions Gate™ Enterprise IDMS, the features of which are available in another brochure.

Primary Components

Below are the key components necessary to run the complete Lions Gate™ Visitor Management System. More information about each of these primary components may be available in a separate document upon request.

- **Lions Gate™ Enterprise Client** – This is the base product which provides numerous functions. More information can be found in the Lions Gate™ Enterprise Client brochure. For the purposes of the visitor application functionality, this software performs the functions of maintaining the sponsor and visitor records after onboarding, providing for business rules over the assignment of access control codes and readers, and is used as the final approval of visitor requests.
- **Lions Gate™ PIV / CAC Kiosk** – This product serves to allow sponsors to initiate, and visitors to furnish, information related to a potential visit. This product also allows visitors to check-in for an approved visit, and, if allowed, print a visitor credential (this can also be set to be performed by the sponsor, or the badges can be printed by a Lions Gate™ Enterprise Client user).
- **Lions Gate™ Central Hub** – (Enterprise Only) The Lions Gate™ Central Hub allows for the encrypted transportation of visit requests between facilities. This software also comes with configuration and management software that allows for the approval of Level II facilities created by a Level I facility. Once approved, these facilities can be visited by interested parties.
- **Lions Gate™ Local Hub** – (Enterprise Only) The Lions Gate™ Local Hub can receive visitor requests from other Level I facilities and Level II facility approvals from the central hub configuration and management software.



Contact us today to see a live demonstration of Lions Gate™ Visitor Management System or Enterprise software, to receive additional information about this unique solution, to ask about our related hardware units, to discover our many LightHouse™ services and software, or just to speak with a representative for a custom quote.



Network
Harbor, inc.



Network Harbor, Inc.

PO Box 4126

Bartonville, IL 61607

www.NetworkHarbor.com

309.633.9118

Sales@NetworkHarbor.com