

DRAFT
37-3.0-OVERVIEW-07 00-00
21 August 2000



System Overview for BROADSWORD Version 3.0



Prepared for:

497th INTELLIGENCE GROUP
INTELLIGENCE SYSTEMS DIRECTORATE (497IG/IND)
BOLLING AIR FORCE BASE
WASHINGTON, DC 20332-5000

Prepared by:

Air Force Research Laboratory, Rome Research Site
AFRL/IFED
32 Brooks Road
Rome, NY 13441-4114

JULY 2000

DRAFT

37-3.0-OVERVIEW-07 00-00

21 August 2000

EXECUTIVE SUMMARY

Broadword provides a basic data access and security infrastructure and a set of tools and services, which allow a user to search, discover and retrieve information from a collection of heterogeneous and diverse information sources (interconnected within a networked environment). To achieve this mission, Broadword provides an automated capability to support the following activities:

- a. Search, discover and retrieve information from multiple data sources, from highly structured to unstructured (free-text).
- b. Provide a unified ordering process for available information, regardless of the product format and delivery method.
- d. Apply format conversion and/or compression to retrieved information, as necessary.
- e. Meet all requirements for SCI processing as defined in DCID 6/3.

DRAFT

37-3.0-OVERVIEW-07 00-00

21 August 2000

TABLE OF CONTENTS

1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

1.1 System and Site Names

2. SYSTEM DESCRIPTION

2.1 Gatekeeper

2.1.1 User Services

2.1.2 Administration Services

2.1.3 Security Audit Review

2.2 Keymaster

2.2.1 Registering a Gatekeeper with the Keymaster

2.3 Authentication and Access Module (AAM)

2.3.1 Performing Local User Maintenance

2.3.2 Performing Regional User Maintenance

2.3.3 LDAP Replication

2.3.3.1 Registering and Updating Enterprise LDAP Servers

2.4 Trusted Transfer Agent (TTA)

2.4.1 MD5 Integrity Seals

2.4.2 Message Level and Field Level Filtering

2.4.3 Masking of Sensitive Fields for Information Passed From High to Low

2.4.4 Overall Architecture of TTA

2.4.5 Registering a TTA with a Gatekeeper

2.5 The Broadsword Client

2.5.1 General

2.5.2 Searching

2.5.2.1 Performing a Local Query

2.5.2.2 Performing a Local Product Request

2.5.2.3 Performing a Remote Query

2.5.2.4 Performing a Remote Query (to low side)/Product Requests
(from low side)

2.5.3 Administration

2.5.4 ISSO

2.6 Supported Sources

3. SYSTEM REQUIREMENTS

3.1 Hardware

3.2 Software

DRAFT

37-3.0-OVERVIEW-07 00-00

21 August 2000

1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

Information is power! Whether it is an analyst answering a question or attempting to predict the intention of an enemy or a targeteer using a product that has been created by assimilating pieces of information together from multiple disciplines, information must be made accessible regardless of where it exists.

In today's environment, the ability to gather information on a "particular item of interest," requires a user to log into each of the data sources using a unique interface for each source. Once logged in, the user must be cognizant of the interface for the source they are using to gather information. While the concept appears straightforward, it requires the user to be very knowledgeable with the various systems. In addition, it requires developers to spend an enormous amount of time and money designing/implementing these unique client interfaces for each data source. The need exists for a capability that will facilitate an efficient way of querying heterogeneous data sources within a distributed environment through a single interface. This is the mission of Broadword.

1.1 System and Site Names

Table 1.1 provides a list of sites that either already have an installed Broadword capability or will have one by the time version 3.0 becomes available. The table also provides listing of the sources that are directly connected to the system at each site. Those sites that have the first column filled in already have version 2.0 installed.

Installed	Broadword Sites	5D	A2IPB	AF Weather	AMHS	AODB	CSIL	IESS	Intelink Hydra	Intelink Meta	IPL 1.0	IPL 2.1	JIVA ISM	MIDB	MEPED	MTI	Trap/TRE	Space DB
	8 th AF, Barksdale AFB LO			√					√	√					√			
	11AF, Elmendorf AFB AK			√					√	√		√			√			
	17TRSS, Goodfellow AFB TX			√	√				√	√		√			√			
	23 rd AF, Pope AFB NC			√					√	√					√			
√	32 nd AIS, USAFE, Ramstein, Germany			√					√	√					√			
√	66 th MI, Darmstadt, Germany	√		√	√				√	√	√				√			
√	480IG, Langley AFB VA			√	√			√	√	√	√	√		√	√			
√	497IG, Bolling AFB MD			√	√				√	√					√			
√	609 th AIS, Shaw AFB SC	√		√				√	√	√					√			
√	612 th AIS, Davis Montham AFB AZ			√				√	√	√					√			
	AFSOC, Hurlburt Field FL			√					√	√					√			
	CENTCOM J-2, McDill AFB FL	√		√				√	√	√		√		√	√			
	DIA, Bolling AFB MD			√			√		√	√	√	√		√	√			
√	JAC, RAF Molesworth UK	√		√	√			√	√	√		√		√	√			
√	JFCOM, JFIC, Norfolk VA	√		√	√			√	√	√		√		√	√			
	MSIC, Huntsville AL			√					√	√					√			
	MCIA			√	√				√	√		√			√			
	NAIC, Wright Patterson AFB OH			√				√	√	√		√		√	√			
	NMIC			√	√				√	√		√			√			

DRAFT
37-3.0-OVERVIEW-07 00-00
21 August 2000

Installed	NGIC, Charlottesville VA			√	√			√	√	√	√	√		√	√			
	Broadword Sites	5D	A2IPB	AF Weather	AMHS	AODB	CSIL	IESS	Intelink Hydra	Intelink Meta	IPL 1.0	IPL 2.1	JIVA ISM	MIDB	MEPED	MTI	Trap/TRE	Space DB
	ONI, Suiteland MD			√	√			√	√	√	√	√		√	√			
	PASS-E (FITPAC), San Diego CA	√		√					√	√		√		√	√			
√	PASS-H (JICPAC), Makalapa HI	√		√	√			√	√	√		√		√	√			
	PASS-J (JDET), Yakota AB Japan	√		√					√	√		√		√	√			
	PASS-K (607 AIS), Osan AB Korea	√		√					√	√		√		√	√			
	Pentagon, Wash DC			√					√	√					√			
√	SOCOM, McDill AFB FL			√					√	√	√	√		√	√			
	SOUTHCOM, Miami FL			√	√			√	√	√		√		√	√			
√	USSPACECOM, Peterson AFB CO			√	√			√	√	√	√	√		√	√			√
	USSTRATCOM, Offut AFB NB	√		√				√	√	√		√		√	√			
√	USTRANSCOM, Scott AFB MO	√		√	√			√	√	√		√		√	√			

Table 1.1—Broadword Sites and Associated Data Sources

DRAFT

37-3.0-OVERVIEW-07 00-00

21 August 2000

2.0 SYSTEM DESCRIPTION

Broadsword implements a multi-tier architecture supporting a single, seamless interface that is secure and administratively manageable. The Broadsword architecture can be divided into five functional components. These components collectively act on behalf of all parties (the ISSO, System Administrator and user) and are tailored to meet the connectivity requirements of the site. Table 2.1 provides an overview of each component.

Functional Component	Purpose
Gatekeeper	Provides single interface to various sources for query, retrieval, and product request/delivery. It also provides a single point in which users are authenticated and all actions audited.
Keymaster	Acts as a global map manager allowing for Gatekeepers and their sources to become accessible to others who register with the same Keymaster
Access and Authentication Module (AAM)	Provides a single place where all user access and authentication information is kept. This service is bundled with the Gatekeeper (for local administration) and is accessible by authorized Keymaster administrators (for regional administration). It also supports the creation of a "yellow page" lookup of users via the use of the Lightweight Directory Access Protocol (LDAP).
Trusted Transfer Agent (TTA)	Module that allows for a Gatekeeper to communicate with an ISSE Guard. High side Gatekeepers, through the TTA and the ISSE Guard capability, can see low side sources, query them and request products to be delivered to high side users.
Broadsword Client	User interface which implements the Client/Gatekeeper API and provides ISSO, System Administrator and General Searching capabilities.

Table 2.1 – Summary of Broadsword Functional Components

2.1 Gatekeeper

The Gatekeeper component is the heart of the overall architecture. It is a robust, thin layer of software which performs a variety of internal functions, including processing users' queries; auditing; communicating with various sources; interconnecting with other Gatekeepers; maintaining system status; and collection/compilation of results. The Gatekeeper supports a single Application's Programmer's Interface (API) for developers to access the functionality

provided and to create applications. The API is based on a simple message passing mechanism and is divided into three sections: (1) User, (2) Administration and (3) ISSO. Figure 2.1, shows the overall architecture of the Gatekeeper.

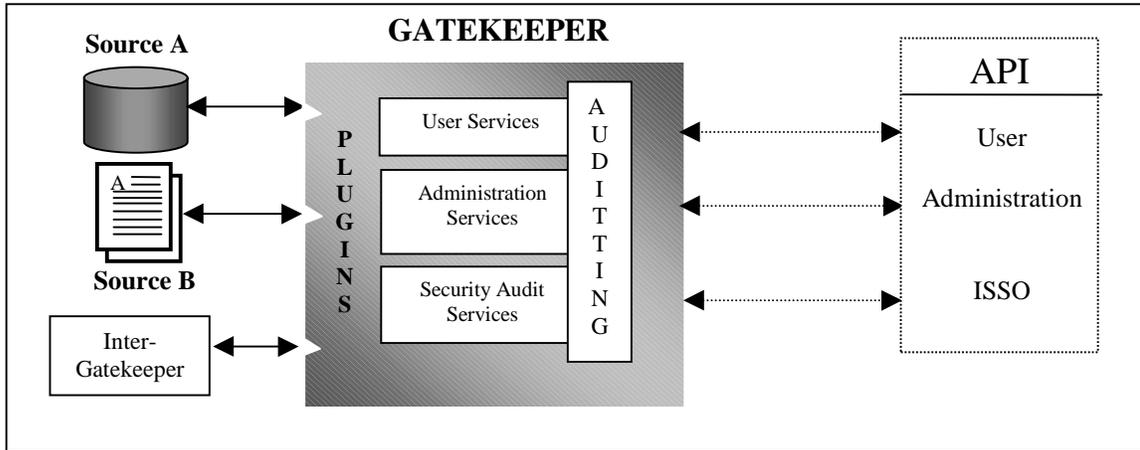


Figure 2.1 - The Overall Gatekeeper Architecture

2.1.1 User Services

The Gatekeeper provides support for the processing of user requests, collating the results, delivering products and converting/compressing supported imagery. User requests can be keyword, spatial or SQL based. The availability of request options is dependent upon the sources connected and what each source supports. Once a request has been submitted, the Gatekeeper audits the request, forwards it to all appropriate sources via plug-ins and waits for each of the sources to respond. Upon receiving the results from each of the sources, the Gatekeeper combines the results into a single response, builds an audit record and forwards the response to requester. Figure 2.2 summarizes the major functionality provided by the Gatekeeper through the User Services portion of the interface.

Some of the sources that are connected to the Gatekeeper may support the ordering and delivery of products. Products include reports from database sources, messages, documents, video clips, maps and images. Delivery mechanisms from the individual sources include: (1) tasking for non-real-time mail order delivery, (2) tasking for FTP delivery and (3) near-real-time FTP delivery.

A number of the imagery sources provide varying degrees of conversion and compression support. As a minimum, each source stores imagery using the National Imagery Transfer Format (NITF) 2.0. This standard supports many levels of compression, bit sizes and storage formats. There are a number of commercial products that can view the full range of NITF storage options. To provide for a wider range of users (those who don't have nor wish to pay for a special application), the Gatekeeper provides conversion support to TIFF 6.0 and JPEG formats.

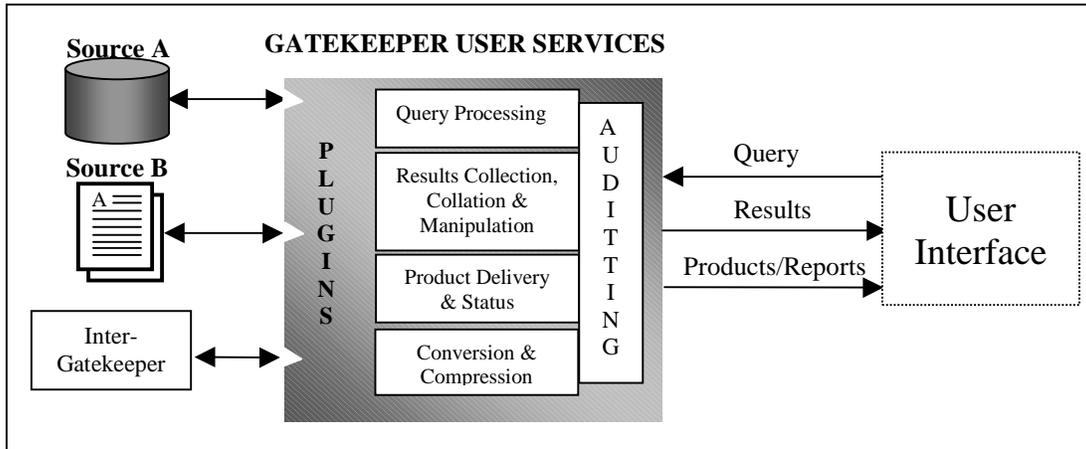


Figure 2.2 – User Services

2.1.2 Administration Services

Under Administration Services the Gatekeeper provides an interface for user maintenance, system statistics and system configuration. Access to the functionality provided by these services is limited to authorized users only. Under User/Group Maintenance, the system administrator creates and configures user accounts and groups. User accounts use one of two models. The first mode (used under Broadword version 2.0) is a combination of Sun Tools/CSE-SS and the Broadword Administrative Interface. User account creation and password maintenance is managed through CSE, while Broadword roles and source accesses are maintained through the Broadword Administration Interface. The problem identified with this approach is the fact that the System Administrator is required to go to two places to manage user accounts. To correct this situation and support the capability for regional administration, Broadword version 3.0 introduced the Access and Authentication Module (AAM). The role that AAM plays in the architecture is described in more detail in section 2.3. Each user can be assigned to one or more groups and have access to various sources. Members of groups share sources assigned to the group, privileges, and queries/results. Groups are created and configured through Group Maintenance. A user can also be assigned a default look and feel through template maintenance. Through this capability, the site can create site tailored look and feels for their users.

System Statistics provides Gatekeeper statistics, includes a listing of the the most frequently accessed products and the most frequently processed queries. In System Configuration, the system administrator configures the Gatekeeper, adds/removes backside sources, defines values for attributes and establishes connectivity with other Gatekeepers through registration with the Keymaster (described in section 2.2). Figure 2.3 summarizes the major functionality provided by the Administration Services.

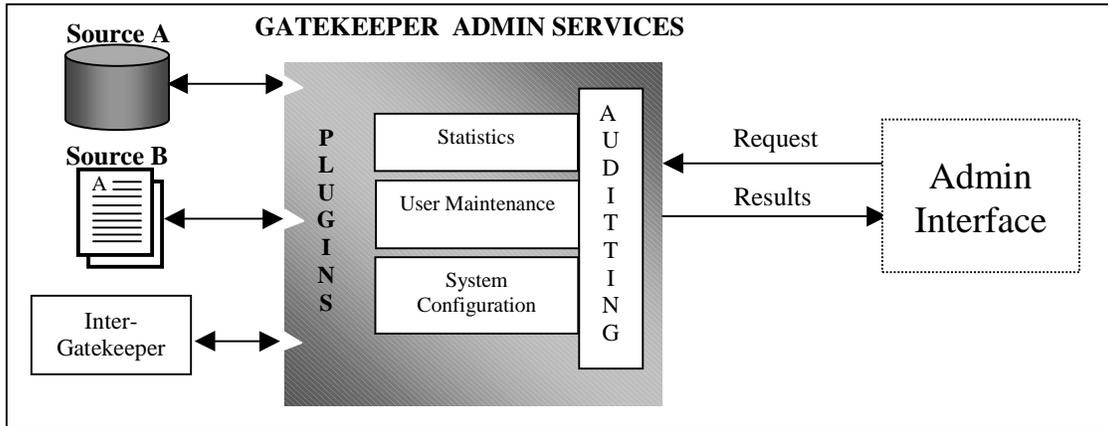


Figure 2.3 – Administration Services

2.1.3 Security Audit Review

The Security Audit Review Interface provides the ability to view, archive, and remove audit information. Those records that have been archived are also available for review. All audits are stored in a database. Broadword version 3.0 offers either Sybase or MySQL as the database engine during the installation. Security records can be filtered based on any one event, user name and/or time range. Table 2.2 provides a summary of the events that are audited by the Gatekeeper.

Gatekeeper Security Audits		
User Events:		
Catalog Request	Transfer Request	User Logged In
Query	User Change Password	User Logger Out
Administration Events:		
Accept Registration from Remote Gatekeeper	Gatekeeper Stopped	Removed Group
Added Discretionary Access Control (DAC)	Get Column Attributes	Removed Group Member
Added Group	Initiate Stream Request	Remove Source
Added Group Member	Modified Element	Remove User
Added New Source	New or Updated Gatekeeper Info	Set Source Parameter
Added User Privileges	Register Our Gatekeeper With Keymaster	Set User Discretionary Access Control (DAC)
Clear Statistics	Remove Discretionary Access Control (DAC)	Terminate Stream Request
Gatekeeper Started	Removed Remote Gatekeeper	Update Daemon Status
ISSO Events:		
Audit Dump	Get Audit Archive List	Got Audit Report
Delete Audit		

Table 2.2 Summary of Security Audits

The certifying authority uses the audit trail dumps, in conjunction with the system audit logs, to validate security auditing requirements. There are three Sybase audit log formats used within Broadword. Table 2.3a shows a sample Audit Report. This report identifies the user, the client,

DRAFT

37-3.0-OVERVIEW-07 00-00

21 August 2000

the date and time of the request, the destination address for product transfers, the type of action requested, the result of the action requested and the unique session identifier.

UserID	Client ID	Date/Time	Destination ID	Action	Result	Session Key
test01	128.132.888.888	950126 18:01		Query	Project Broadsword: 00085 Hits	5607
test01	128.132.888.888	950126 18:16		Query	Project Broadsword: 00085 Hits	5607
test01	128.132.888.888	950126 18:16	128.132.888.899	Query	Project Broadsword: 00085 Hits	5607
test01	128.132.888.888	950126 18:16	128.132.888.898	Query	Project Broadsword: 00085 Hits	5607

Table 2.3a – Sample Audit Report

Table 2.3b provides a sample Product Request Report. The Product Request Report provides information about a product transfer. In addition to the information provided on the original query, this report provides Server ID.

UserID	Client ID	Date/Time	Access ID	Server ID	Session Key
test01	128.132.999.999	950126 21:35	IPA_16193533ZNov94_061488	128.132.989.989	5607
test01	128.132.999.999	950126 21:38	IPA_16193533ZNov94_061488	128.132.989.989	5607
test01	128.132.999.999	950126 21:41	IPA_16193533ZNov94_061488	128.132.989.989	5607

Table 2.3b – Sample Product Request Audit Report

The Query Report provides information about data returned for individual hits. In addition to the information provided on the original query, this report provides the Access ID and the Server ID for the Server performing the query. Table 2.3c provides a sample of this report type.

UserID	Client ID	Date/Time	Access ID	Server ID	Session Key
test01	128.132.999.999	950126 20:33	IPA_19153415ZJan95_216672	128.132.999.888	5607
test01	128.132.999.999	950126 20:33	IPA_19153608ZJan95_213744	128.132.999.888	5607
test01	128.132.999.999	950126 20:33	IPA_19153611ZJan95_849	128.132.999.888	5607

Table 2.3c – Sample Query Response Audit Report

2.2 Keymaster

Sources at a site can be made available to other sites through the Gatekeeper to Gatekeeper connection. Gatekeepers have the ability to communicate with each other and their respective sources as long as each site has registered their Gatekeeper with a Keymaster. The Keymaster manages a list of all Gatekeepers and their sources that have registered with it. During the registration process, a Gatekeeper receives the global map. The global map identifies all other Gatekeepers and sources. Queries and product requests performed between the available Gatekeepers do not involve the Keymaster. Changes in a specific Gatekeeper's configuration are propagated up to the registered Keymaster and are then propagated back down to all other Gatekeepers.

Broadsword version 3.0 supports regional user maintenance. User accounts can be created and configured at the Keymaster for a specified registered Gatekeeper. Figure 2.4 shows the Broadsword architecture with two Gatekeepers and a Keymaster.

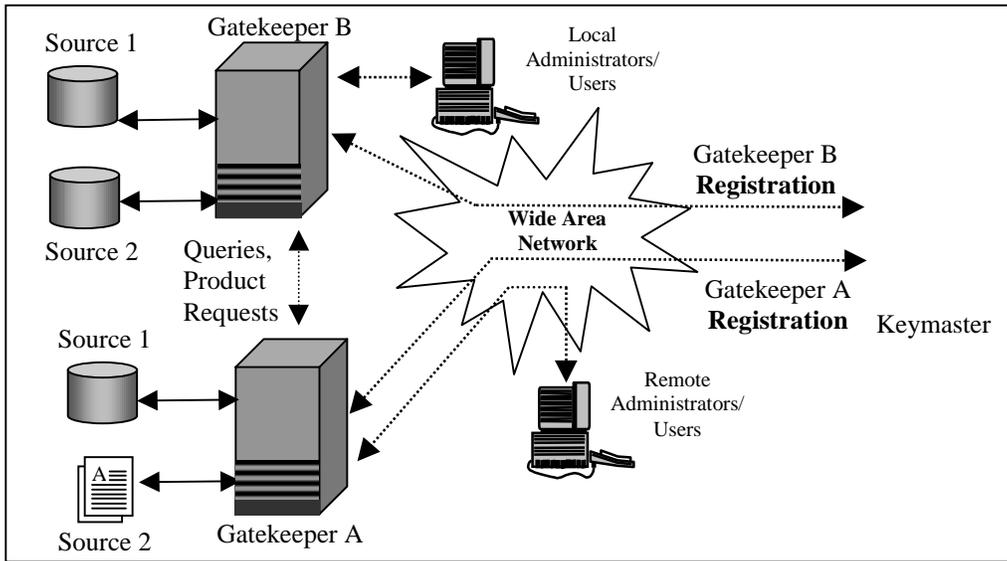


Figure 2.4 – Gatekeeper/Keymaster Architecture

The Keymaster uses a subset of the API libraries provided as part of the Gatekeeper. Specifically, it uses the login process, its associated user administration capability and ISSO functionality. Table 2.4 provides a list of auditable events within the Keymaster.

Keymaster Security Audits		
User Events:		
User Change Password	User Logged In	User Logger Out
Administration Events:		
Accept Registration From Remote Gatekeepers	Keymaster Stopped	Remove Remote Gatekeeper
Added Discretionary Access Control (DAC)	New or Updated Gatekeeper Info	Remove User Privileges
Added Group	Register Our Gatekeeper With Keymaster	Set User Discretionary Access Control (DAC)
Added Group Member	Removed Discretionary Access Control (DAC)	Set User Info
Added User Privileges	Removed Group	Update Daemon Status
Keymaster Started	Removed Group Member	
ISSO Events:		
Audit Dump	Get Audit Archive List	Got Audit Report
Delete Audit		

Table 2.4 Summary of Security Audits

2.2.1 Registering a Gatekeeper with the Keymaster

When a new Gatekeeper joins the network of Gatekeepers, it must first register itself with the “Keymaster”. The process begins when the system administrator of the new Gatekeeper calls the Keymaster Distribution Center. From the Keymaster administrator, an unique registration identifier will be generated for the new Gatekeeper. The system administrator of the new Gatekeeper will then enter this registration identifier, the port number of the Keymaster and the Keymaster’s address into the new Gatekeeper’s registration screen. At this point the new

DRAFT

37-3.0-OVERVIEW-07 00-00

21 August 2000

Gatekeeper will then generate a public/private key pair and send the Keymaster a message containing: (1) its public key, (2) the one time registration identifier and (3) a map identifying any/all sources to be made publicly available. This map, considered the local map, is generated automatically by the new Gatekeeper. It identifies which sources the system administrator has allowed to be available to other sites. This is done by setting the Publish Flag option when configuring a specific source plugin.

The Keymaster, in turn, will respond with a message containing, (1) the Gatekeeper's digital certificate (a timestamp, the Gatekeeper's identification and the Gatekeepers public key) encrypted using the Keymaster's private key, (2) a second digital certificate describing the Keymaster and (3) the world map of all other Gatekeeper's and their publicly available sources. The Keymaster will complete the registration process by updating all other Gatekeepers with the existence of the new Gatekeeper. This is accomplished by a background process, which wakes up at a designated time, looks for any changes and sends each existing Gatekeeper the new map. Before the map is actually sent, however, an identification/authentication process takes place. This process involves the Keymaster sending its digital certificate to the Gatekeeper. The Gatekeeper will decrypt the certificate and respond back to the sending party (i.e., the Keymaster) with its certificate.

Once any Gatekeeper is registered with the Keymaster and has received certificates, secure access from one Gatekeeper to another is possible. As previously stated, the advantage of this approach is that there is no need to include the Keymaster in requesting a service from one Gatekeeper by another. By avoiding the necessity to access the Keymaster for each and every request, an important potential bottleneck in the architecture has been eliminated. The only time it will be necessary for the Gatekeepers to communicate with the Keymaster is when configuration of an existing Gatekeeper changes or a public/private key is compromised. Figure 2.5 shows the relationship between the Gatekeepers and the Keymaster and identifies the components involved in the registration process of a single Gatekeeper.

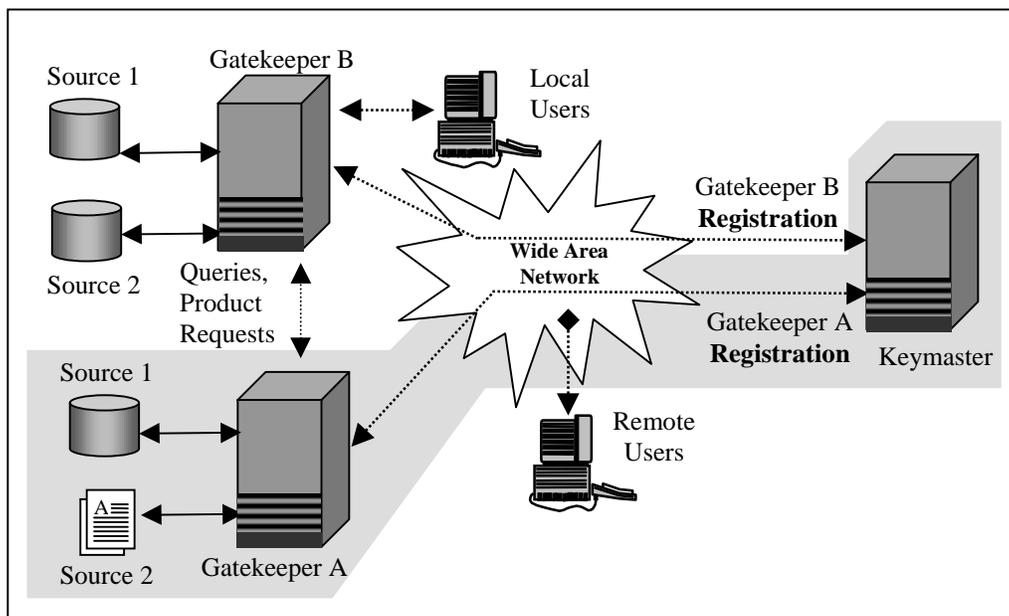


Figure 2.5 Registration Architecture

DRAFT

37-3.0-OVERVIEW-07 00-00

21 August 2000

When there is a configuration change on a single Gatekeeper, it must be propagated throughout the network. Changes are accomplished through the existing system administrator screens. When changes are made they are saved into the local configuration file. At a designated time, a background process will wake up which looks at the timestamp of the file. A newer date will indicate that a change or a number of changes have been made to the Gatekeeper's configuration and that these changes must be sent to the Keymaster. After going through the identification/authentication process between the Gatekeeper and the Keymaster as described above, the Gatekeeper sends its new configuration file up to the Keymaster. The Keymaster will acknowledge the receipt back to the Gatekeeper via a message and update its local configuration file. Again, at a designated time, the background process at the Keymaster will wake up, see that one of its Gatekeeper's configuration has changed. It must then update all Gatekeepers with this new information. This update is performed in a manner similar to that of the initial map registration.

2.3 Authentication and Access Module (AAM)

To create and configure a user within Broadword version 2.0, the administrator must first create a user account through either the SUN operating system (SUN Tools) or through CSE-SS and then use the Broadword administration tools to add privileges/sources. At best this process is disjointed and requires the administrator to know/understand multiple interfaces and applications. To alleviate this problem and to implement additional user requirements, Broadword version 3.0 has introduced the Access and Authentication Module (AAM). To support existing deployments of Broadword 2.0, version 3.0 supports and is backward compatible with the current 2.0 user maintenance infrastructure.

The overall goal of the AAM is threefold. The first is to provide the Broadword administrator a single interface to create and configure user accounts. The second goal of the AAM is to provide for regional user maintenance. Administrators are not available at all locations. There exists the requirement to create user accounts at a central location. The final goal is to automatically create a global directory service through which users can find information about other users. This capability must be compatible with the Lightweight Directory Access Protocol (LDAP) initiative being pursued by the Intelligence Community (IC) and DoD.

The trend within the IC and DoD is to use Netscape's LDAP to store all user information. The IC LDAP schema is designed as an on-line phone book or "yellow pages" directory service. It contains information describing the user, including user identification and password. It does not contain the necessary information to maintain and manage user passwords. Data such as password history, account lock/unlock, and number of invalid login attempts are a few attributes that need to be maintained in order to provide an accreditable user authentication module. The AAM provides a single interface through which all user and system access information is accessed and maintained. The AAM is accessed through the Gatekeeper Administration API. The information required is divided into three parts; user information, password management and system configuration.

By separating user information from password management, each Gatekeeper will have a pure LDAP schema as defined by the IC as well as all of the necessary information to perform a reasonable level of authentication information and password management. The list of necessary information, and the requirements that dictated this list, was derived from the password and user authentication policies provided by CSE-SS. These include:

DRAFT
 37-3.0-OVERVIEW-07 00-00
 21 August 2000

- Password Expiration
- Dictionary Attack
- Account Locking/Unlocking
- Bad Password Checking
- Password History

Table 2.5a and b provides a list of those items that are stored and in which storage mechanism.

Gatekeeper Configuration File	Data Base
Number of bad Login attempts before account locked	User Identification
Number of days before password expires	User Identification password (Encrypted using CRYPT or MD5)
Minimum password size	Space delimited list of OLD PassWorDs (Encrypted using CRYPT or MD5)
Maximum password size	Last Date/Time of Password Changed (YYYYMMDDhhmmss)
Minimum number of special characters required in a password	Account locked (Y/N)
Number of passwords saved in user's password history	Number of bad login ATTEMPTS
LDAP Host IP	
LDAP Port	
LDAP root Distinguished Name	
LDAP root password (Encrypted)	

Table 2.5a – AAM Gatekeeper/Data Base Attributes

LDAP Schema		
Mandatory Attributes:		
Citizenship	Given Name	Name
Surname		
Policy-based Attributes:		
Employee Type	Intelligence Community Email	Telephone: Unclassified Voice Phone Number
Home Organization	PKI: Certificate	
Optional Attributes:		
Company Name	Physical Address	Phone: Secure Facsimile Number
Current Organization	Physical Building Name	Phone: Secure Telephone Number
Email: Internet Address	Physical City	Phone: Unclassified Fax Phone Number
Email: Niprnet Address	Physical State or Province	Title
Email: Siprnet Address	Physical Postal Code	User Identification
Grade	Physical Country Name	Expert Country
Mailing Address	PKI: Authority Revocation List	Expert Functional Area
Telephone: DSN Voice Phone Number	PKI: CACertificate	Production Manager
Telephone: Secure Facsimile Number	PKI: Certificate Revocation List	Language Proficiency
Middle Initials	Telephone: DSN Voice Phone Number	

Table 2.5b – AAM LDAP Attributes

All users will be assigned a specific Gatekeeper through which they will log into the system and perform all requests. The local system administrator can add user accounts to the Gatekeeper. Figure 2.6 provides an overall architecture.

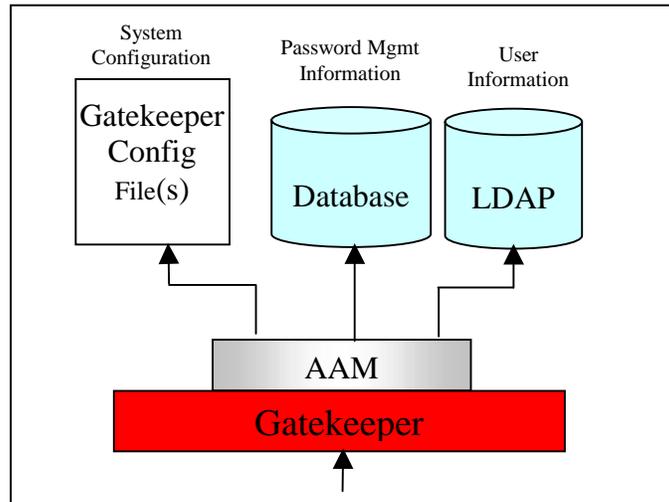


Figure 2.6 –Authentication & Access Module Architecture

The AAM also supports the ability to perform regional user maintenance. User accounts can be created/maintained remotely through the Keymaster and its interface. Keymaster administrators must be granted privilege from the local Gatekeeper administrator to allow not only the Keymaster but also the particular Keymaster administrator permission for remote access. Before the Keymaster client is permitted to access the AAM to create/modify a user account, the two components (Keymaster and Gatekeeper) must authenticate themselves. This is accomplished through the existing security authentication mechanism used between the Keymaster and registered Gatekeepers.

2.3.1 Performing Local User Maintenance

Broadword version 3.0 supports two methods for performing local user maintenance. The first method supports the way in which user access and authentication was performed in version 2.0. If the site chooses not to use the local AAM capability, they will continue to create user accounts through CSE-SS or Sun Tools and add privileges/accesses through the Broadword administration interface.

If the site chooses to use the AAM option, user maintenance is supported through a single administrator's interface. From this interface, the administrator creates user accounts and assigns groups and accesses. The information entered is stored in two different areas. General user information is stored in the Gatekeeper's LDAP while password management information is stored in a database. If the Gatekeeper's LDAP is registered with a CA, the information entered into the local LDAP may be replicated to an external LDAP using Netscape's replication server. Figure 2.8 shows where LDAP servers exist in the overall architecture and the logical connection used for updating user accounts that are generated at the Gatekeeper.

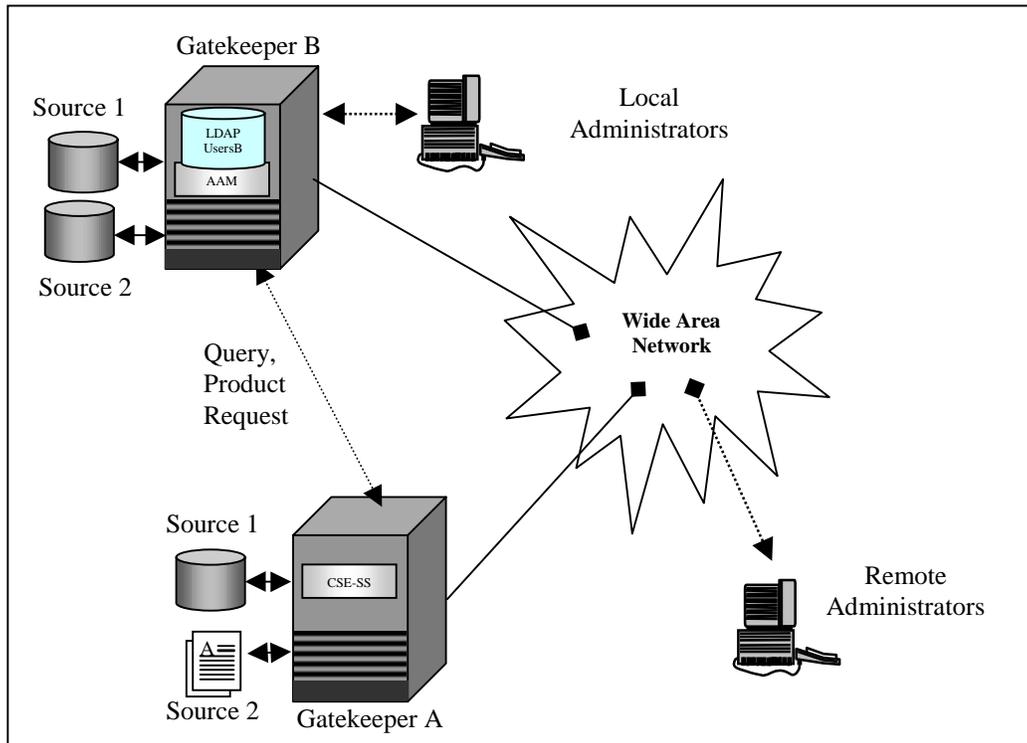


Figure 2.8 – Local User Maintenance Architecture

2.3.2 Performing Regional User Maintenance

If a Gatekeeper is registered with a Keymaster, and configured to use the AAM Gatekeeper, user accounts can be created by authorized Keymaster administrator(s). To add a user through the Keymaster, the administrator (assuming the administrator has been given the authority by the appropriate Gatekeeper Administrator) first chooses which Gatekeeper they would like to add a user account. An authentication process, similar to that used between Gatekeepers performing request, is performed before the Keymaster is allowed in. From this point on, the Keymaster interface is identical to that of the local Gatekeeper. All information is entered directly into the Gatekeeper just as if a local administrator is performing the same operations. By accessing the Gatekeeper's information directly, the configuration data is always current.

Figure 2.7 shows the components and connectivity used to support this capability. Notice here that regional user maintenance can only be performed on those Gatekeepers using the AAM who authorize Keymaster administrators to perform regional user maintenance.

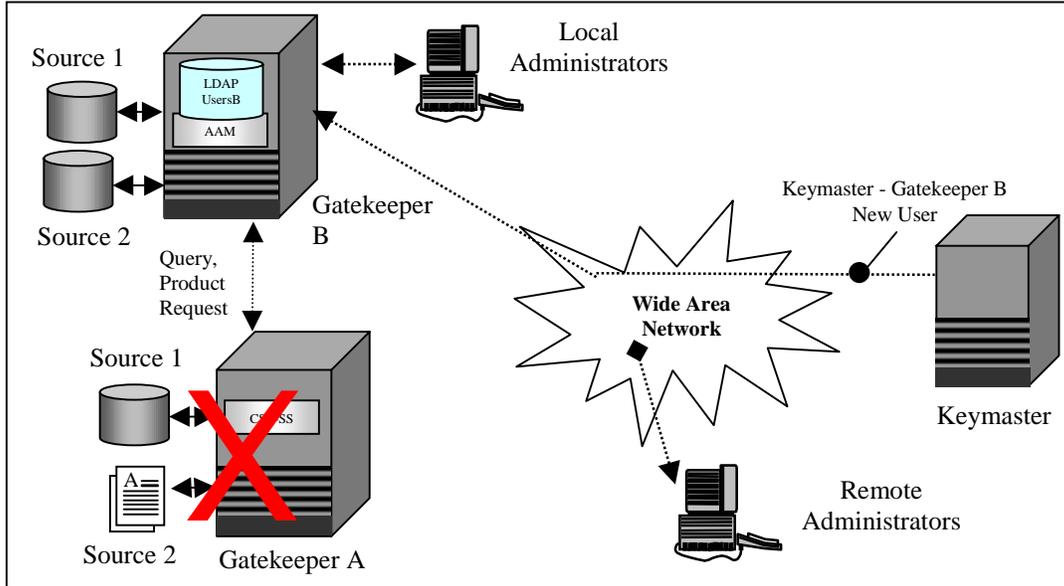


Figure 2.7 – Regional Maintenance Architecture

2.3.1 LDAP Replication

Information stored in the Gatekeeper LDAP can be replicated (via Netscape's replication service) to any other registered LDAP server. LDAP servers can exist anywhere in the network. An LDAP server may reside on the same server as that of the Keymaster or exist on one of the servers that is part of the JIVA Enterprise. Registered LDAP servers must have valid Digital Certificates and be configured to communicate through the use of Secure Sockets Layer (SSL). Digital certificates will be obtained through the Intelink System Management Center's (ISMC) Certificate Authorities. Since Broadword's LDAP servers contain only user information as designed by the IC, it is acceptable to supply this information to other registered LDAP servers. Figure 2.9 provides a high-level architecture diagram illustrating a scenario where the AAM and LDAP servers exist.

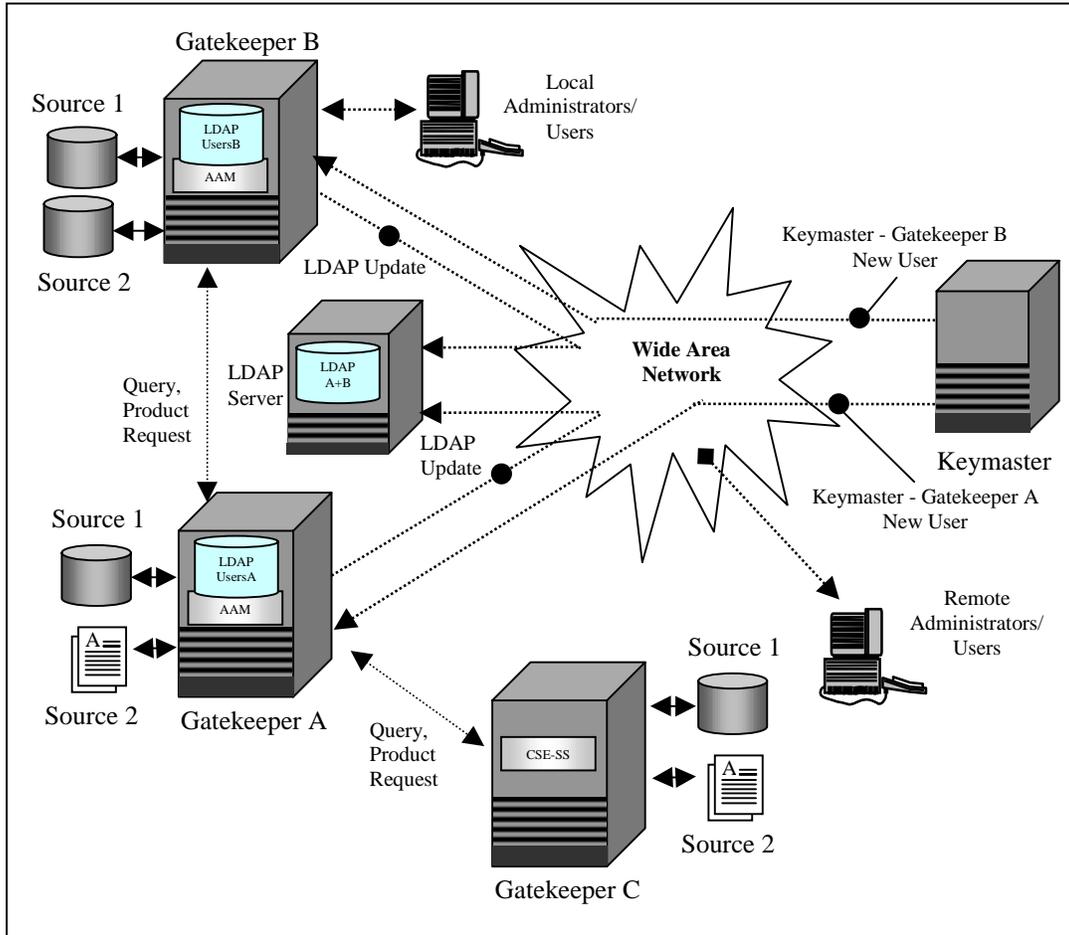


Figure 2.9 – Gatekeeper/Keymaster with LDAP Architecture

A Gatekeeper using the Broadword version 2.0 user maintenance will still be capable of registering with the Keymaster and participating with other Gatekeepers (both version 2.0 and 3.0) but will be unable to support regional user maintenance and LDAP user information.

2.3.1.1 Registering and Updating Enterprise LDAP Servers

Broadword version 3.0 implements Netscape's LDAP Server product. Each Gatekeeper, through the AAM, will be capable of obtaining a Digital Certificate from the ISMC's Certificate Authority and registering with one or many other LDAP Servers. The Gatekeeper LDAP servers will be access only and once registered with another LDAP server, be capable of replicating its information. By allowing this functionality, a global LDAP server may be automatically built and maintained. Figure 2.10 shows the architecture.

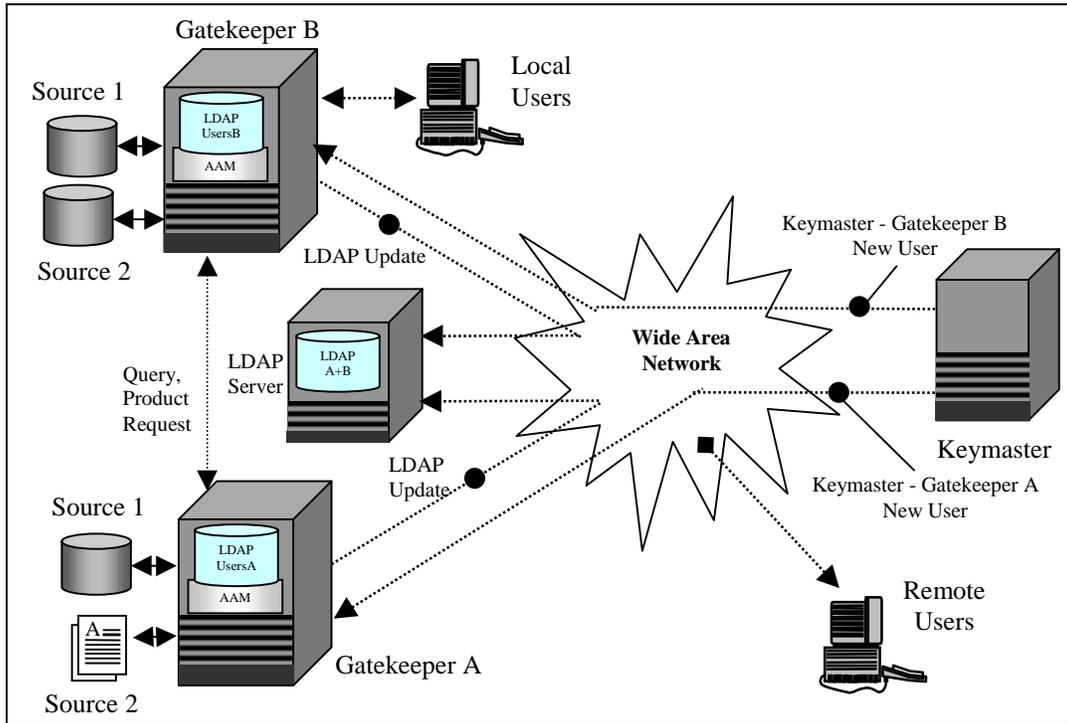


Figure 2.10 – Broadsword Architecture with LDAP

2.4 Trusted Transfer Agent (TTA)

The Gatekeeper, Keymaster and AAM, described above, provide a powerful infrastructure for the interconnection of information sources within a single Community Of Interest (COI) and a single security domain. The Trusted Transfer Agent (TTA) brings together this powerful infrastructure and the multiple security level (MSL) capability provided under the Information Support Server Environment (ISSE) Guard. TTA provides any authorized user within the Gatekeeper COI operating at the high-side security level the ability to access, query and pull information from a low-side COI.

2.4.1 MD 5 Integrity Seals

To ensure that information is not added (inadvertently or maliciously) to a TTA message once it enters the TTA processing stream, Message Digest 5 (MD5) integrity sealing is performed on all information passing from high to low and low to high through the TTA. Immediately after receiving a message from either the high side or low side Broadsword interfaces TTA assigns a Message Digest 5 (MD5) integrity seal and attaches that integrity seal in the TTA package generated. Subsequent, whenever that package is passed between TTA processes or passed through the ISSE Guard the MD5 integrity on the package is recalculated and compared with the original integrity seal to verify the seal matches. This indicates that the package has not been modified in any way (either accidentally or maliciously) since it arrived at the TTA interface. If the MD5 seal does not match at any point an error message is generated, processing of the message in question is terminated, and a system log is written indicating where the problem was detected within them TTA process flow.

DRAFT

37-3.0-OVERVIEW-07 00-00

21 August 2000

2.4.2 Message level and field level filtering

In order to ensure that high side information is not inadvertently passed through the TTA and ISSE Guard to the low side, extensive security filtering capabilities are included in the TTA Security Filtering Application (SFA) resident on the TTA High Gatekeeper platform. Since security policies change from time to time the security filters applied by the SFA are configurable by the ISSO working in concert with the TTA Administrator to enforce the appropriate security protection mechanisms. Two levels of security filtering capabilities are provided, message level filters and field level filters.

Message level filters reuse the software that performs “dirty word” filtering already accredited within ISSE Guard applications approved for the passage of formatted message traffic containing limited free text areas. Messages level filters use a “dirty word” list containing a list of words and/or phrases that are either not passable to the low side (e.g. classified code words, etc.) or strong indicators that the associated information in the message is not passable to the low side (e.g. security labels). By applying the message level filters it is determined if a message being passed through the TTA (and subsequently the ISSE Guard) from high to low contains any “dirty words”. If a message is found to contain one or more words/phrases in the dirty word list, the processing of the message is terminated. Following this, an error message describing the filter violation is generated and sent through established Broadsword mechanism back to the originating user, and a error message is generated that is written to the system/broadsword error log.

Field level filters are an additional capability added to TTA and are akin to NITF header filters already accredited within ISSE Guard applications and approved for the passage of the header portion of NITF imagery. Since the messages passing from high to low through the TTA contain formatted field-value pairs, additional filtering can be provided on a field-by-field basis. For each field within each message type, over which field level filter is needed, an entry in a file is generated describing how the information in the field is to be filtered. A variety of filter types have been created which test for a variety of conditions such as Value in Field, Value Not in Field, Value In Range etc.

2.4.3 Masking of sensitive fields for information passed from high to low

The Broadsword Inter-gatekeeper messages passed between gatekeepers of the same security level contain a variety of sensitive information describing the high side security environment. Examples include Internet Protocol (IP) addresses, user logins and passwords, platform names, etc. When passed between platforms of different security levels, as is provided by TTA, this information cannot be passed, since it would disclose potentially sensitive information about the high side to the low side domains. For this reason, The TTA Plug-in and Keymaster map Receive applications manipulate the message to ensure the proper information, necessary for TTA operation, is inserted, and that not potentially sensitive information is disclosed through the ISSE Guard to the low side security domain. The components maintain local alias tables that replace potentially sensitive information with masked out values prior to them being passed from high to low and replace those masked out values with the original value in the response messages when they arrive back to the high side components.

2.4.4 Overall Architecture of TTA

The TTA High Gatekeeper and TTA Low Gatekeeper configurations include a number of processes that must work continuously and cooperatively in order to ensure proper operation of the TTA system. If a serious error is detected in any TTA process on either the high side or the

low side platform action is taken automatically to shutdown either the high side or low side TTA processes, quickly, completely, and correctly. This ensures that no information will inadvertently pass through the TTA because processes are not working correctly, and protects against the Unix file system directories, used in various locations within the TTA system, from becoming overloaded. Once TTA is started high side and low side process controller components of TTA continuously monitor the status of all TTA high side and low side processes respectively. If one of those processes exits for any reason the process control recognizes that fact and signals all other TTA processes to gracefully exit thus bringing down the high side or low side of the TTA completely. When this event occurs, messages are written to the system log allowing the TTA administrator to determine when and why the event occurred. Figure 2.11 displays the overall Gatekeeper/TTA architecture.

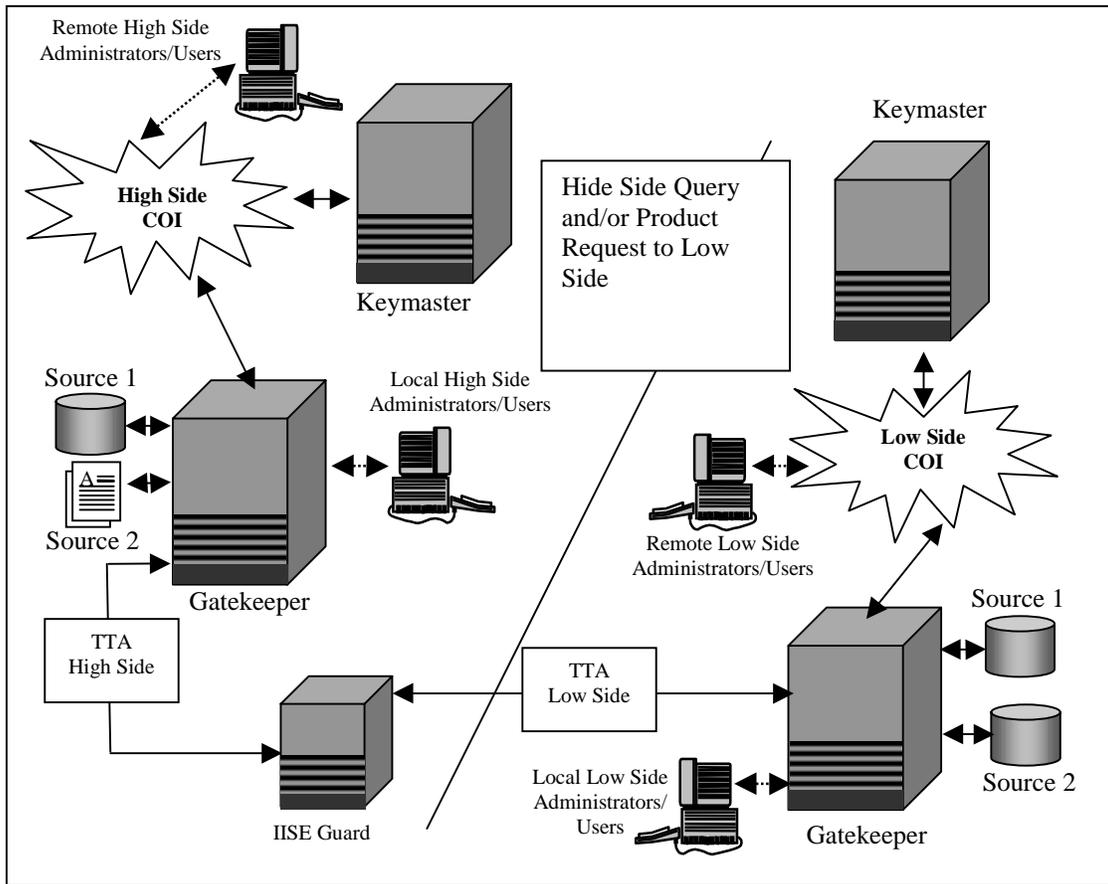


Figure 2.11 – TTA Architecture

2.4.5 Registering a TTA with a Gatekeeper

The Trusted Transfer Agent (TTA) provides the ability for two separate Gatekeeper/Keymaster infrastructures, operating at two different security levels, to communicate with each other. Specifically, in Broadword version 3.0, the TTA allows high-side users to be aware and connected to low-side sources. High-side users can query any registered source that has been published on the low-side and pull products from low to high. TTA takes advantage of the capabilities provided by the Information System Support Environment (ISSE) Guard. Before

connectivity can be established and users are allowed to query low side sources, the TTA must be registered within the two environments.

The TTA is built on top of the Gatekeeper and as such looks like a Gatekeeper in the infrastructure. The registration process begins with the low-side TTA registering with the low-side Keymaster. By registering with the low-side Keymaster, the TTA receives the global map of all Gatekeepers and sources that are available on the low side. It also will receive any updates and is a valid participant in the community established by the Keymaster. After receiving the global map, the TTA sends it to the ISSE Guard, which in turn sends it to the high-side TTA. At this point, the high-side TTA registers itself with the high-side Keymaster, supplying the low-side global map and limiting connectivity to only one specific Gatekeeper through the Gatekeeper's Discretionary Access capability. The Gatekeeper now has the knowledge of the low side sources. Figure 2.12 identifies the components used to establish connectivity.

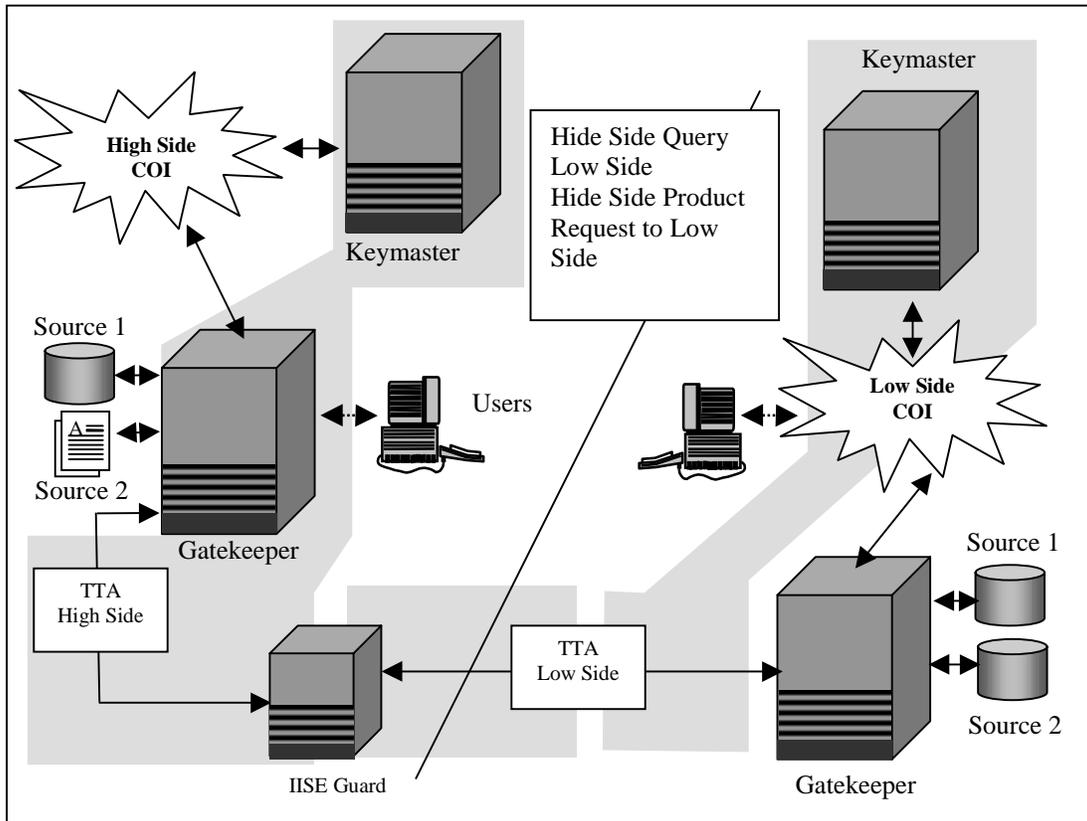


Figure 2.12 – TTA Registration Process

2.5 The Broadword Client

Broadword provides a User Interface to access the Gatekeeper and local data sources. It is Web-based and supports multiple roles. Roles are assigned on an individual user basis and can include one or more functions: searching, administration and ISSO.

The user will log into the system from the main screen. Based on the user's login, the main screen will be tailored to what roles that have been assigned by the site System Administrator. The

following paragraphs provide an overview of the functionality supported through the client interface. Figure 2.13 shows the overall User Interface Architecture.

2.5.1 General

The Preferences section allows the user to set up their default values and is split into six separate pages: (1) General Registration & Default First Page; (2) Information Support; (3) Delivery Options; (4) What and Where to Search and Search Utilities; (5) Attribute Configuration and (6) Remote Access. Users are able to define what their Search Tools page looks like, which data sources to search, and their preferred search mechanism. The Feedback page allows the user to provide on-line suggestions and comments about the interface. This form is pre-filled with information provided on the Preferences page. The Support page provides a listing of points of contact for requirements, help desk, site system administration, site ISSO and site Intelink officer. The About page provides the version number of the system, and whom the current copy is registered to. These capabilities are provided to all users regardless of their roles.

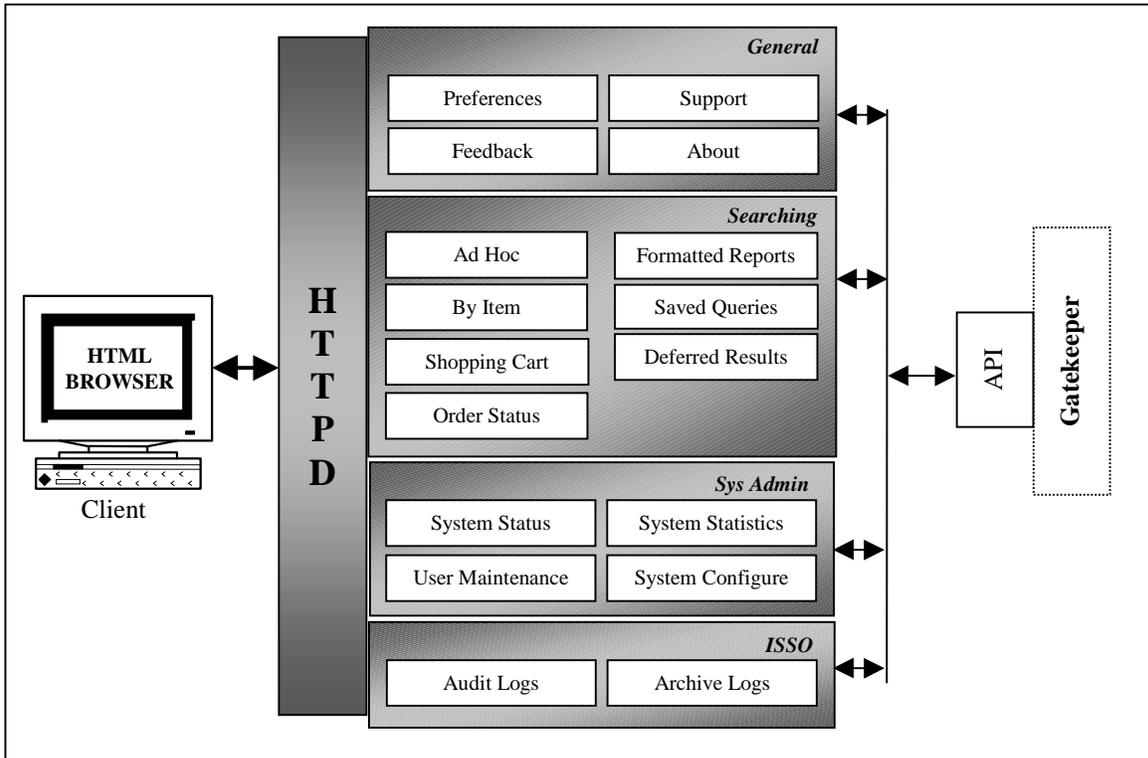


Figure 2.13 - Broadsword Client Architecture

2.5.2 Searching

Under searching, the user is provided with tools to discover, navigate and retrieve information across various sources. Searching capability is given to any user that has been given a login and password. Users are able to choose between a keyword search utility (Find), an SQL form-based utility (Query), or a spatial tool (Geographic Search). In addition, users are able to combine these search tools and configure what method they prefer through the Define Search Page preference. This preference represents the search mechanism they use the most, and that will be displayed. Should the user select search tools as their default first page, then this search

DRAFT

37-3.0-OVERVIEW-07 00-00

21 August 2000

mechanism will be displayed immediately after login. Thus, the Search Form page is a single user-selected page, tailored to each user's preference.

Provided off the spatial tool, is the ability to turn on broadcast feeds (e.g., TRAP/TRE). The user can use these feeds for tip off of potential activity within a given Area Of Responsibility (AOR) and request additional/available information of the area through the request mechanism.

The results page displays all records matching the user's query. Currently Broadsword supports ordering CSIL, IPL, 5D and IDEX products. There is a different process for requesting IDEX products, pulling IPL/5D products to a destination, and ordering CSIL products. Users are able to choose several products of differing types and put them into a "shopping cart". The ordering attributes for any product placed in the cart can be modified while in the cart. Items placed in the cart can be saved from session to session and across multiple queries. At any time the user can order the items in the cart by clicking the order button. The user can find out the status of any orders that they have placed by clicking on the Order Status capability. This function provides information as to whether the product has been successfully delivered or has been shipped out (depending on the source).

Formatted reports provide the ability for the user to generate a set of predefined reports. Specific report types and the attributes available to generate them are based on the source and type. Reports can be ordered to a specified destination or available on-line.

The Saved Queries page provides the user with a list of all queries, which the user saved through the Search Tools or Results Page, as well as functionality to process the queries in different ways. A saved query can be used interactively by the user, producing immediate results, as well as by background processing, producing deferred results. Interactive use of saved queries includes immediate execution of the query and loading of the query for display modification. Background processing of saved queries is done by the E-mail Notification and Batched Query utilities. E-mail Notification Processing periodically informs the user of new and updated products that match the saved query. Batched Query Processing allows the user to schedule the query to be executed at a later time. The results generated by these background processing utilities are viewed through the Deferred Results Page. The Deferred Results capability not only allows viewing of E-mail and Batched results, but also deletion of these results. For viewing, the standard display format is used to present product information.

The General User Interface portion resident on the analysts workstation requires a HTML 4.0 compliant web browser. There is no Broadsword software required to be installed on the workstation.

2.5.2.1 Performing a Local Query

Upon successful connection, the user is presented with a request page in which they can submit a request. As previously discussed, the request can be a keyword search, a form-based SQL query or a Geospatial query and is based on the user's individual preferences. The request is sent to the Gatekeeper and another audit record is built. The Gatekeeper routes a copy of the request to the appropriate sources (provided as part of the request) through the plug-ins. Each plug-in takes the request, validates it against its policy and converts the request to the format required by that source. The plug-in then forwards the request to the source itself.

The Gatekeeper waits for the responses from each of the sources. Once all returns are received, the Gatekeeper will join them together into a single response and audit the results. This response is then delivered to the client software and in turn provided back to the user. From the results page, the user can pull an available on-line product or order the product (when supported by that source) to be delivered to a specified destination. Figure 2.14 identifies the portions of the architecture that supports local query processing.

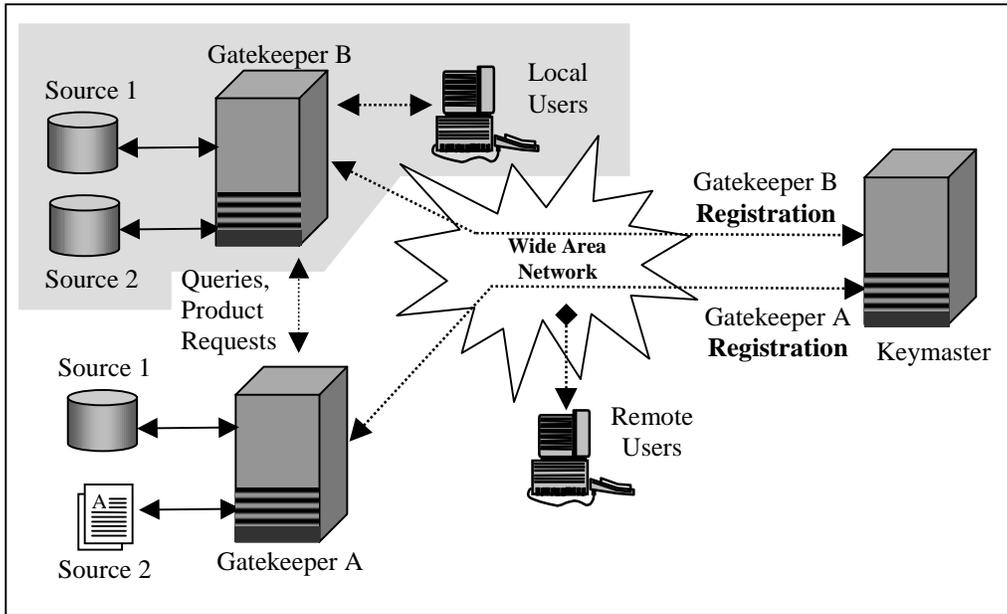


Figure 2.14 – Performing a Local Request

2.5.1.2 Performing a Local Product Request

Depending on the source, there are two possible mechanisms to pull a product through the Broadsword Interface: (1) Pull to View and (2) Deliver to Destination(s). From the Gatekeeper's viewpoint both mechanisms are the same - the only difference being the destination directory. To pull a product to view, the user clicks on the item/*anchor* provided in the middle column of the results page. The client sends the request to the Gatekeeper, which in turn audits the request, creates a status record into the status log and routes the request through the Plug-in. The Plug-in, in turn, routes the request to the source. The Gatekeeper supports a minimal set of conversion formats directly (NITF 2.0 to TIFF 6.0 and Commercial JPEG). If the product is an imagery product the Gatekeeper checks the format in which the user has requested to be delivered. If the source supports the conversion and/or compression directly, then the Plug-in will allow the request to pass through as requested. On the other hand, if the source does not support the request, the Plug-in will request the product as NITF 2.0 and the remaining portion of the conversion and/or compression can be performed by the utilities provided as part of the Gatekeeper.

Once the imagery product is in the desired format and compression, the product is delivered to the specified destination(s). In the case of a "pull to view", the product is delivered into a directory so that the client can set the content type and stream the file to the browser. If the request was a "deliver to destination(s)", the product will be delivered to the destination(s) and directory/(ies) specified by the user through FTP. In the case of a non-imagery source, the

product is brought through the plug-in “as is” and then written to the designated file. The components of the architecture that support local product delivery and status are the same as those used for query processing (refer to Figure 3.2).

2.5.1.3 Performing a Remote Query

When a request is made of a source that is connected to a remote Gatekeeper, an authentication process will first be initiated. This process is used to ensure that the local Gatekeeper and Remote Gatekeeper have permission to talk to each other. The process begins with the local Gatekeeper sending its certificate to the remote Gatekeeper. The remote Gatekeeper will verify the certificate using the Keymaster’s public key (that was sent down in the second certificate). The remote Gatekeeper will then send its certificate to the local Gatekeeper. The local Gatekeeper will then verify the certificate using the Keymaster’s public. At this point the local Gatekeeper’s request can be sent to the remote Gatekeeper and in turn the appropriate sources are queried. The remote Gatekeeper waits for responses from its sources, joins them together and then forwards the results to the local Gatekeeper. The local Gatekeeper collects all the results, from other Remote Gatekeepers and local sources and returns a single joined response back to the user. When the request is completed, the session is ended. Figure 2.15 summarizes this process.

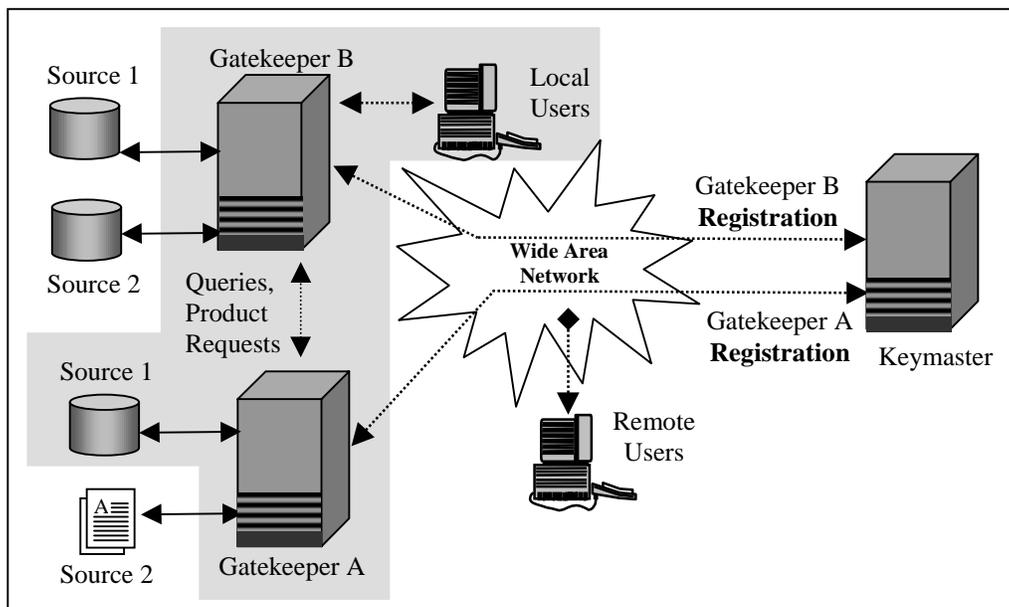


Figure 2.15 – Performing a Remote Product Request

2.5.1.4 Performing Remote queries (to low side)/product requests (from low side)

Once the existence of the TTA is known, the user at the high side Gatekeeper can see the availability of the low-side sources. From the user’s perspective, all they see is additional sources published by the TTA. When the user submits a query, the user’s Gatekeeper will route it to the high-side TTA. The high-side TTA checks the request for releasability down to the low side (by performing a dirty word check on the query), packages the request by sanitizing high side values and wrappers it so that the ISSE Guard can process it. TTA also creates an MD5 seal around the package to ensure that no one tampers with the package anywhere in the process.

Once the package is built, it is passed on to the ISSE Guard for routing down to the low-side TTA. The low side TTA routes the request to the appropriate low-side Gatekeepers (and sources) and gathers all the results into a single results set. At this point, the low-side TTA packages the results set, creates an MD5 seal and sends it back to the high-side Gatekeeper through the Guard. The high side Gatekeeper combines all the results sets into one and returns it back to the user. Product requests and delivery work in a similar manner. Figure 2.16 show the components that are used in allowing for high-side – low-side connectivity.

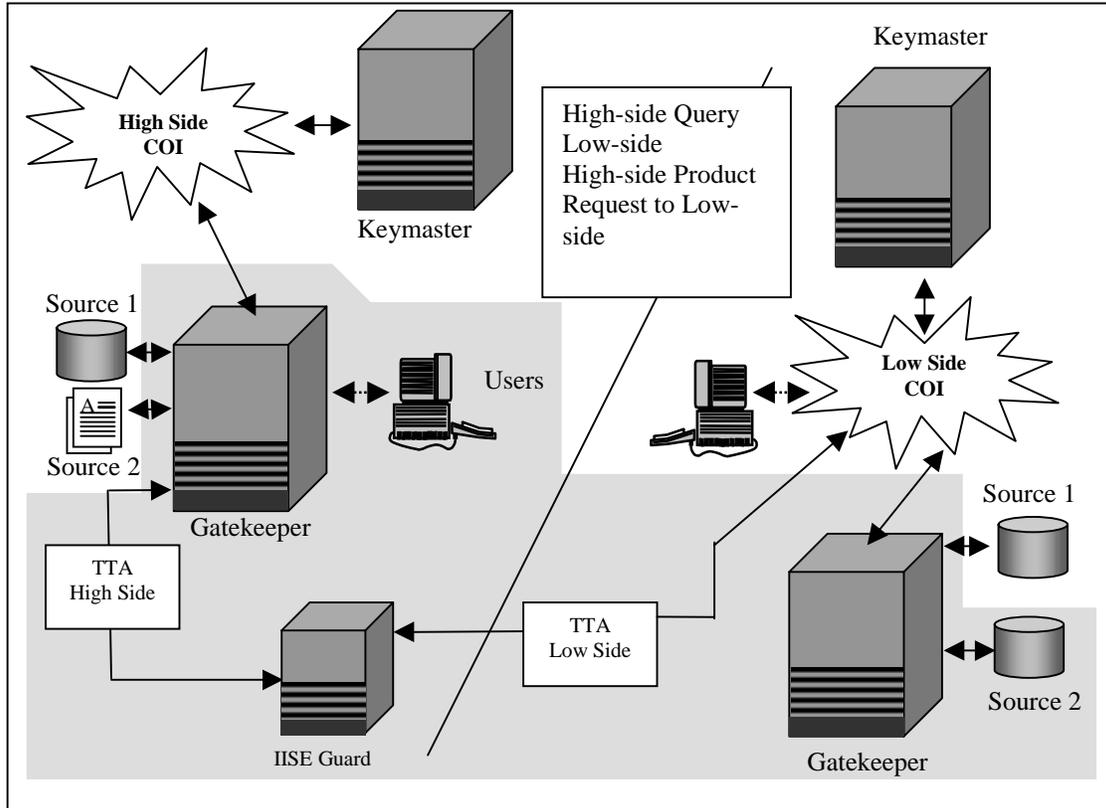


Figure 2.16 – High Side Query to Low Side Source

2.5.3 Administration

The System Administration (SA) section for the Gatekeeper provides system status, user/group maintenance, system statistics and system configuration. System Status provides the status of all processes associated with the Project Broadsword system, the ability to turn on debug flags and maintenance for Broadsword log files.

Under User Maintenance, the system administrator grants additional privileges (i.e., system administrator, and ISSO) and access to various sources. System Statistics provides Web, Gatekeeper and Batched jobs statistics. Web statistics is based on Web Usage and provides such information as the amount of bytes transferred, the top number of pages accessed and the total number of accesses. Gatekeeper statistics include a listing of the top 10 frequently accessed products and the top 10 frequently issued queries.

DRAFT

37-3.0-OVERVIEW-07 00-00

21 August 2000

The System Configuration section, allows the system administrator to modify or change the configuration information of the Gatekeeper, add/remove sources, define values for attributes (used for popdowns as part of the short form) and establish connectivity with other Gatekeepers through registration with the Keymaster.

2.5.4 ISSO

The ISSO Interface provides the ability to view, archive, or remove audit information from the Broadsword Sybase Database based on users(s), date/time and audit event. It also allows the ISSO to retrieve previously archived audits.

2.6 Supported Sources

The Gatekeeper can connect to a source in one of two modes: as a (1) Trusted User or (2) Brokered User. The Gatekeeper maintains the individual source's security policy and accesses each source on a read-only basis. If a source does not have the ability to support restricted access and retrieval, then the connection to the Gatekeeper will be through a trusted interface. A source can support restricted access if it is able to distinguish between users. In this case, the information or view returned is based on the user's login. A brokered login connection will maintain the user's individual login and password for that source. Table 2.7 shows the type of access provided by the Gatekeeper for the respective source.

Source	Access Type
Air Force Weather (AFWX)	NO LOGIN REQUIRED
Air Operations Data Base (AODB)	TRUSTED
Automated Message Handling System (AMHS)	BROKERED
Commercial Satellite Imagery Library (CSIL)	NO LOGIN REQUIRED – Registration required to order products
Demand Driven Direct Digital Dissemination (5D)	TRUSTED
Imagery Product Library 1.0 (IPL 1.0)	TRUSTED
Imagery Product Library 2.0 (IPL 2.1)	BROKERED
Imagery Exploitation Support System (IESS)	TRUSTED
Imagery Dissemination Exploitation (IDEX)	TRUSTED
Intelink (Hydra, MetaSearch)	NO LOGIN REQUIRED
Infosphere Management (ISM)	TRUSTED
Military Equipment Parametric and Engineering Database (MEPED)	NO LOGIN REQUIRED
Modernized Integrated Data Base (MIDB)	TRUSTED
Moving Target Indicator (MTIX)	NO LOGIN REQUIRED
TRAP/TRE	NO LOGIN REQUIRED
Space Data Base	NO LOGIN REQUIRED

Table 2.7 Summary of Access Types

DRAFT

37-3.0-OVERVIEW-07 00-00

21 August 2000

3. SYSTEM REQUIREMENTS

The Gatekeeper can be installed on an existing server (i.e., collocated with an existing server), or on a separate platform, depending on availability of hardware and performance requirements.

3.1 Hardware

The size of the system primarily depends on the number of users expected to access the system at a time and the number of imagery sources connected to it. To support the imagery conversion and compression, a higher end server is required. Table 3.1 provides various system configurations based on approximate number of users.

Number of Users	System Nomenclature	Number of Processors	RAM (GB)	Disk Storage (GB)
10-15	Ultra 60	2	1	36
15-25	ES450 or Ultra 80	4	2	72
25-40	ES3500	8	4	72

Table 3.1 – System Configurations

The server-based General User Interface functionality, including the session manager and all Common Gateway Interface-Binary (CGI-bins), are located on the same machine as their Gatekeeper. No additional hardware, over and above that outlined for the Gatekeeper, is required for the General User Interface. The General User Interface also includes a portion resident on the analyst’s workstation. This hardware is any platform capable of running a HTML 4.0 compliant web browser.

3.2 Software

Listed below is the software required by the Gatekeeper:

Basic Package includes:

- Sun Solaris version 2.6
- FTP Server and Client
- SendMail
- Sybase SQL Server version 11.5.1 or greater

If running with CSE-SS

- X-Windows X11R5
- CSE-SS v1.4.1.3

If running with LDAP

- Netscape LDAP Directory Server v4.1.1

The server-based General User Interface functionality has the same software requirements as the Gatekeeper, with the following addition:

- Apache HTTPD version 1.3.9
- PHP 4.0