Building Information for Emergency Responders

Stephen TREADO
Alan VINH
David HOLMBERG
Michael GALLER
Building Environment Division
Building and Fire Research Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

ABSTRACT

This paper describes a methodology for controlling access to building information to approved external entities such as police, fire and public safety officials. Building automation systems frequently monitor critical building information, including the status of alarms, locations of occupants, thermal and air quality conditions that could be extremely useful to emergency responders and incident commanders in the event of a building emergency. Therefore, it is desirable to provide a mechanism to enable public safety officials to access this building information, while at the same time preventing unauthorized access and use of the information. The methodology developed to provide this functionality includes a building information services and control system (BISACS) server, and standardized data modeling of the building automation system (BAS) using enhancements to the BACnet protocol. The description includes the requirements for the underlying information models, components, interfaces and functionality to provide secure remote access to building information to authorized users.

Keywords: access control, authentication, buildings, control systems, emergency responders, protocol, security

1. INTRODUCTION

As building automation systems become more sophisticated and powerful, the possibility of tapping into and distributing building information in real time to remote monitoring stations and emergency responders becomes more attractive. The components of a building automation system, including HVAC, lighting and access controllers, and fire detection and security systems, incorporate many sensors, detectors and cameras that could provide critical information about conditions inside of a building to public safety and operating personnel outside of the building. The availability of critical building information could help to improve the efficiency and effectiveness of incident responses, and minimize safety risks to emergency responders. Typical building information might include types and locations of alarms, building floor plans and system schematics, locations of occupants, and locations and types of hazardous materials. This emerging concept has been discussed previously in [1].

In order to make this sort of building information system a reality, several issues must be addressed. The building information must be collected, transferred and presented in a standard, understandable manner. The proper infrastructure must be in place to enable the building information to be accessed from remote locations, including dispatch centers and incident command posts. This may require both wired and wireless links at various locations. Another critical element is the secure dissemination of the building information only to authorized users. This consideration is not unlike that faced by designers and implementers of IT and ecommerce systems, which necessarily must incorporate identity verification, data security, privacy and authority mechanisms to function effectively.

This paper focuses on the development of a method to authenticate remote users of building information. A typical use case would be allowing public safety officials at a remote dispatch center, firehouse or police station to access building information in real-time. Another related use case would be to allow emergency responders en route or on the scene of a building related incident to access building information to help plan or coordinate their response.

2. APPROACH

The dynamic building information, such as sensor readings and video streams, would be provided by the building automation system, while the static building information, such as floor plans and equipment schematics, would reside in a building information model. While the specifics of the integration of the static and dynamic building information are beyond the scope of this paper, the delivery of the dynamic information is based on enhancements to the BACnet building automation system communication protocol [2]. The Life Safety and Security Working Group of the BACnet committee is currently in the process of developing enhancements to the BACnet standard to accommodate physical access control systems. These enhancements have been summarized in [3] and include new BACnet objects to represent access entities, access points, access zones and access rights. Ongoing efforts are underway to extend these enhancements to include logical as well as physical access.

The method for enabling and controlling access to building information is based on the following key elements:

1. A strong and secure proof-of-identity credential for each remote user- it is suggested that this be a version of a federal PIV (Personal Identity Verification) card, or similar credential
2. A hierarchical structure of public safety personnel databases
3. A building information services and control system (BISACS) with secure connection capability

4. A secure link between the BISACS and the BACnet building automation system (BAS) using a building services interface (BSI)

A strong identity credential is an essential element of a system for securely controlling access to building information. The right to access building information is tied directly to identity, along with other factors such as jurisdiction, duty status, incident status and chain-of-command. For example, access rules might limit access to building information only to personnel currently on duty, or only in certain jurisdictions, or only when an incident involving the specific building is underway. The federal PIV card provides a good model for a strong identity card, and for the purposes of this discussion, it is assumed that this or a similar format will be used. NIST Special Publication 800-73-1 [4] describes the characteristics of the federal PIV cards, including format, data elements, keys and certificates. It would be the responsibility of the issuing agency to properly verify and control the issuance of PIV cards for public safety personnel.

The issuing jurisdictions would create and manage the public safety databases that contain the identity information and rights and privileges of each individual. Public safety personnel would be enrolled in their local jurisdiction's database, which would be part of a hierarchical network of public safety databases spanning multiple jurisdictions. Negotiations between jurisdictions and mutual recognition and acceptance of databases would have to be implemented in accordance with higher-level policies, with adequate assurances for security and accuracy.

Figure 1 presents a schematic depiction of the functional components of the building automation system, the secure building information server (BISACS), the databases and the remote clients (i.e. dispatch centers, etc.). This is just a typical configuration, and does not show all of the detail or possible network configurations, and is meant to represent the necessary functions rather than specific hardware or software elements. The general idea is that there is a BACnet BAS network internal to the building, a network link to other building information systems such as human resources and IT, and a network link to the outside world. At the other end, public safety operations such as police, fire and dispatch also have network connectivity, as well as wireless communication capabilities.

The communication between the building and the public safety operations would be handled by the BISACS. This configuration has several advantages. First, all of the remote users would interact with the building through the BISACS, so the protocols can be standardized, and communication maintained in a secure manner. The method for establishing a secure connection to the BISACS is described in [5], and is based on an exchange of certificates and web services. The BAS would communicate directly with the BISACS, also using web services, so that that information exchange can be handled in a standardized and secure manner. Using the BISACS as the middleman avoids the need to provide multiple interfaces between the building and the outside, as well as eliminating the requirement for the BAS to maintain extensive databases related to remote users of building information.

The BAS in figure 1 is shown with two interfaces. The *credential reader interface* connects to the credential readers for the access control system. These would typically be located at access points such as doors and gates, but other uses are also possible. For physical access control, users present their identity credential to the credential reader at the desired access point. Local users are usually enrolled at the site, so their identity information and rights and privileges can be verified using the local database contained in the BAS. The BAS may also exchange information or access external databases through the *building services interface* (BSI). This external interface provides for information exchange, sharing of resources, and network visibility across the enterprise.

It is through the BSI that remote users would need to authenticate their identity in order to be allowed to access building information from the BAS, via the BISACS. The difference between remote logical access and physical access is that the authentication information would be collected in a public safety database rather than in the BAS database. The public safety database would need to be a secure implementation under the control of authorized public safety officials, who would manage the collection and modification of identity information, rights and privileges of the public safety personnel enrolled in under their jurisdiction. There would likely be a hierarchical structure of multiple public safety databases spanning police, fire and public safety districts, municipalities and geographical regions.

Figure 2 shows a more detailed overview of the BISACS structure. The BISACS base server is centrally located, and can be configured to manage data transfer going in or out of the building. In addition to the building services interface (in this case a BACnet Services Interface), a sensor network services interface (SNSI) is shown on the building side, the SNSI is just another network being accessed through the BISACS. As indicated in figure 2, notice that the BISACS may be configured to support a host of "services interfaces" (SI), these services interfaces serve as access points to their respective devices or network of devices. Alerts and commands can be monitored or generated from outside of the building, and are managed through the BISACS. One or more BISACS proxy servers may be implemented to facilitate scalability and to provide redundancy.

Figure 3 shows the BISACS communication and user validation processes in greater detail. To gain access to the BISACS, the remote/external user must connect and log into one of the nodes that is a part of the BISACS network. Although the user authentication process may pass through a BISACS Proxy Server (BPS), the accessing of the data store is actually done at the BISACS Base Server node (BBS). Notice that any drill down processing or commands/requests to access or control a device has to go through the BBS. The data stores containing the user information and certificate information may reside locally or externally to the building, this includes information for internal users such as employees of a building and/or external users such as first responders. The BISACS can be configured to handle the authentication of internal and external users, and maintains secure communication for each session. The BISACS server itself has a secure communication link to the BSI. More details about the BISACS can be found at the BISACS Web Page (http://cic.nist.gov/bisacs/index.html).

3. EXAMPLE USE CASE

The procedure for authenticating remote users of building information requires the initial implementation of a public safety database, a building information services and control system (BISACS), and a building services interface (BSI). At the public safety side, each of the public safety personnel at a specific organization, such as the city, county or state police department, or local fire department, would be issued a PIV card, in accordance with the requirements described in FIPS 201-1 [6], or similar procedures. It is essential that strict identity verification be conducted before a PIV card is issued, to prevent any fraudulent cards from being created. This is the reasoning behind the recommendation for the use of the federal PIV guidelines, since these have been extensively reviewed, and are considered a best practice for providing for a process to control the issuance of identity cards.

Once the public safety personnel have been issued a PIV card, the public safety database can be implemented. Essentially, each of the public safety personnel would be enrolled in an organization specific database, which would include their identity information along with their rights and privileges. This process is similar to enrollment in a physical access control system, except that the rights and privileges would include more than access points and zones, but would encompass logical access rights as well. There is no reason why the database could not do double duty both for physical access control and logical access control. All the security safeguards and login verifications would be required for the management of the organization specific public safety database, to ensure the validity of the information.

On the building side, a building information server would be established and configured for the specific building, or multiple buildings. The BISACS would exchange information with the BAS via the BSI, using a web services implementation that would publish dynamic building information, such as alarms and alerts to the BISACS for retransmission to remote consumers, such as public safety personnel. The BISACS would also provide static building information, such as floor plans and equipment schematics.

For the application of providing building information to emergency responders, the flow of information would be one-way; from the BAS to the BISACS. The building information, including both the static and dynamic components, would be available to authorized users only. This authorization would be handled by the BISACS. For the case of remote commands to the building, the BISACS would transfer the commands to the BSI, which would translate them into specific messages to the appropriate building automation system controllers. For example, smoke dampers could be opened remotely, or building elevators operated from outside of the building to provide emergency egress.

4. CONLUSIONS

A structural framework and data model has been developed for allowing the transfer of building information to emergency personnel outside of the building, and the remote control of building systems. The methodology incorporates a building information services and control system server, a building services interface and a user authentication capability to provide for secure access to building information only by authorized users. The data models and communication protocols required to implement the system have been identified, as well as the required functionality and operating procedures necessary to enable wide scale use.

The use of the type of system described here could greatly improve the ability of emergency responders to formulate and execute effective response plans during emergency events. This should result in reduced loss of life and property damage for building owners and occupants, as well as reducing the risks to emergency personnel.

5. REFERENCES

1. Holmberg, D., Davis, W., Treado, S., Reed, K., Building Tactical Information System for Public Safety Officials, NISTIR 7314, National Institute of Standards and Technology, Gaithersburg, MD 20899, 1/2006
2. ASHRAE, ANSI/ASHRAE Standard 135-2005, BACnet- A Data Communication Protocol for Building Automation and Control Networks, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Atlanta, GA, 2005
3. Ritter, D., Mundt, H., Isler, B., Treado, S., Access Control in BACnet, ASHRAE Journal Article, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Atlanta, GA, 2006
4. Dray, J., Guthery, S., Schwarzhoff, T., NIST Special Publication 800-73-1 Interfaces for Personal Identity Verification, National Institute of Standards and Technology, Gaithersburg, MD 20899, 3/2006
5. Vinh, A., Building Information Services and Control System (BISACS): Technical Documentation, NISTIR (in review), National Institute of Standards and Technology, Gaithersburg, MD 20899, 9/2006
6. FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, National Institute of Standards and Technology, Gaithersburg, MD 20899, 3/2006

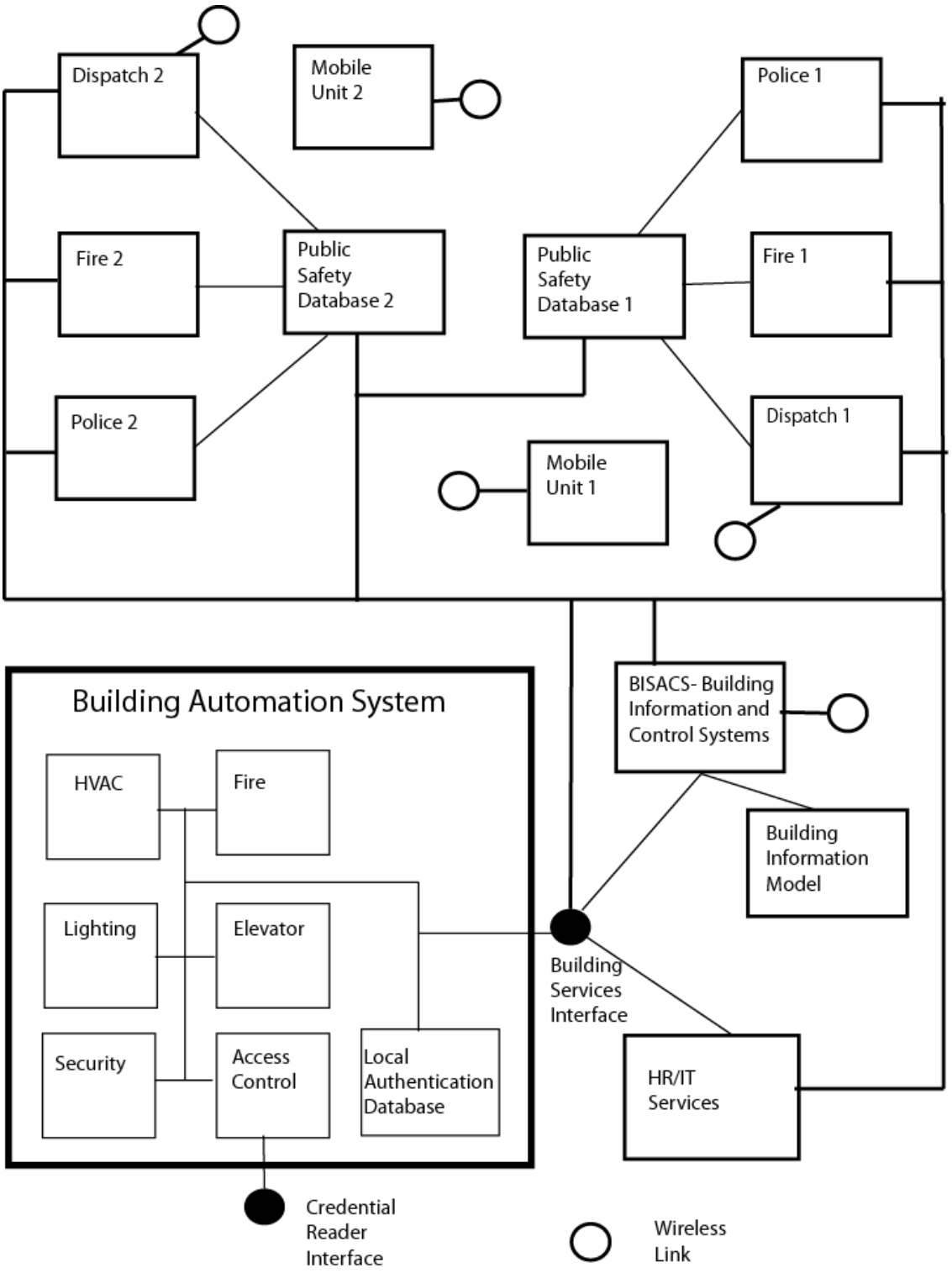

Figure 1. Schematic diagram of building automation system, building information server and public safety network

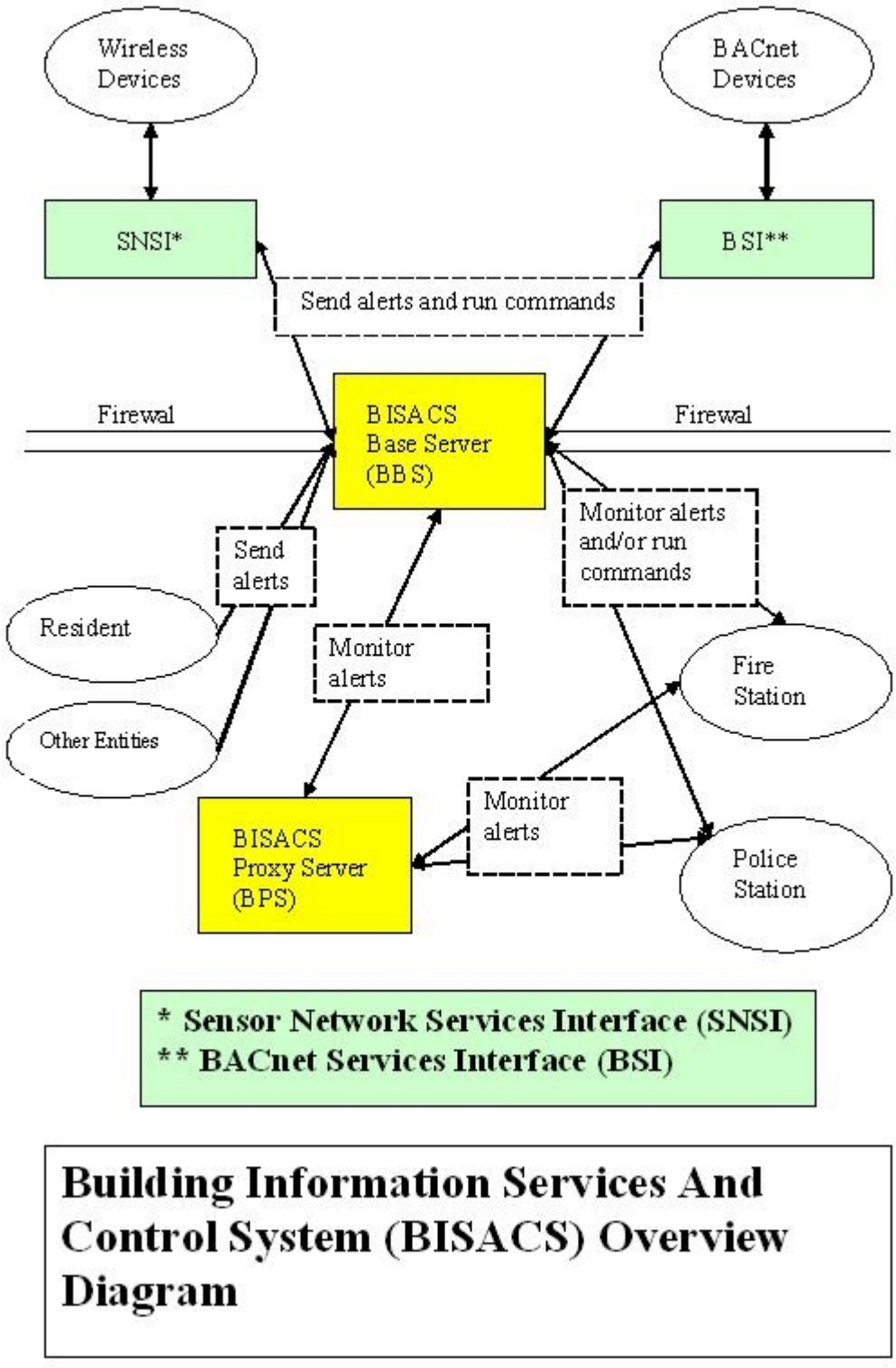

Figure 2. BISACS overview diagram

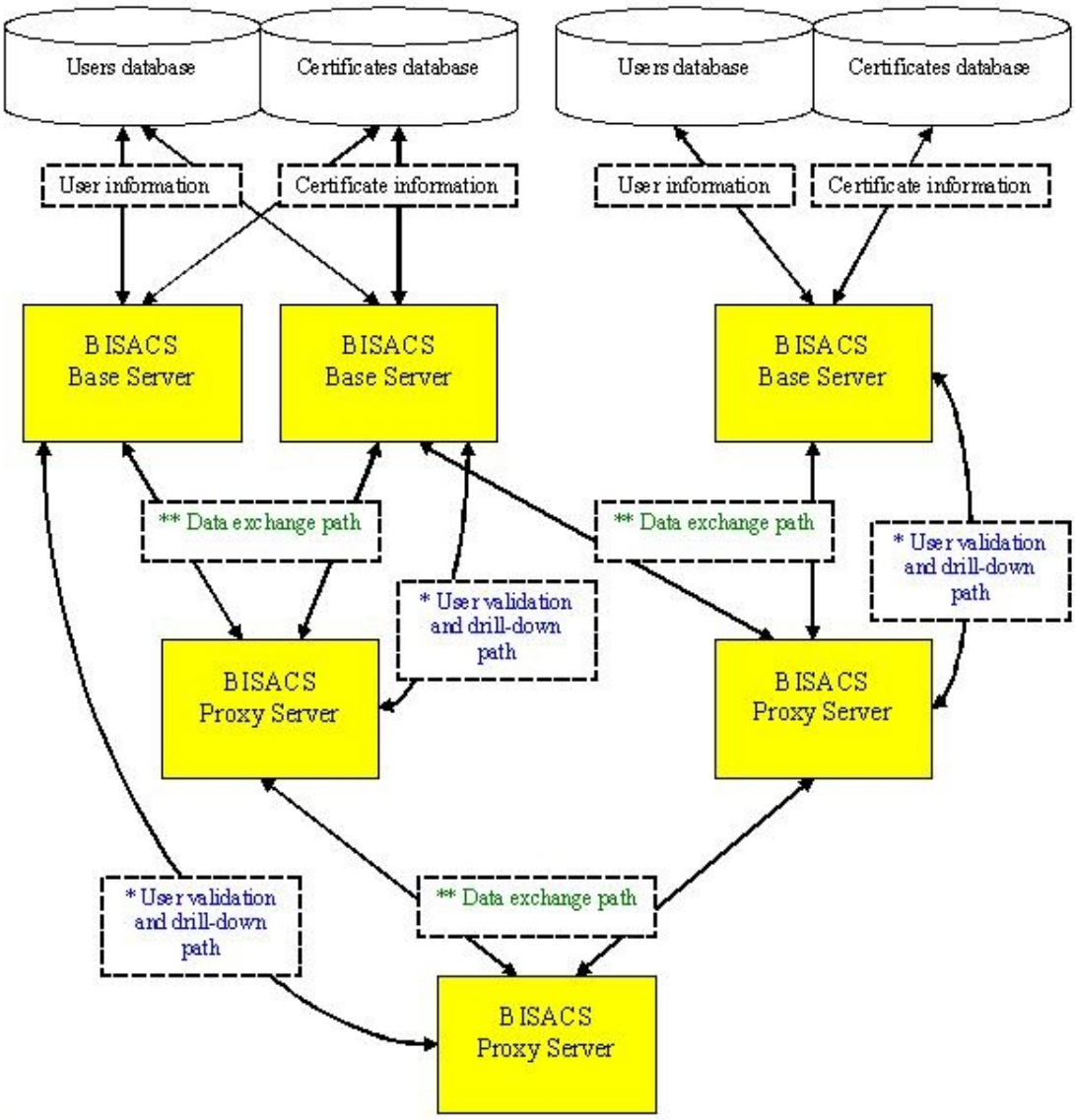

Figure 3. BISACS communication and data flow diagram