InnoVote Systems Network

Detailed Design

By
Erin Thead
Software Engineer
erin@erinthead.com

Table of Contents – Network Detailed Design

1. Introduction

1.1. Purpose.

The purpose of this document is to communicate a suggested design for the various communication networks that the InnoVote election products will use. The document provides a description of the network architectures, data flow restrictions, and cryptographic systems of the networks.

The intended audience of this document is the developer and any other persons interested in the project, including election reform activists, computer security professionals, political figures with an interest in election reform, and potential buyers of the design.

1.2. Scope.

The InnoVote line of election products will need to communicate with each other across networks. Since the integrity of the election data is of paramount importance, these networks must be designed to protect data transfers from one InnoVote machine to another. Existing election software and hardware is located mostly on public networks with little to no protection of the data.

As is described in references [2], [5], [6], and [7], numerous software functions of InnoVote products require a secure network to operate correctly. The network designs proposed in this document will provide the required security to protect the integrity of sensitive election data processed by InnoVote systems.

1.3. References.

[1] Thead, E. *InnoVote CardReader Hardware Requirements Overview*, 2005.
[2] Thead, E. *InnoVote CardReader Functional Design*, 2005.
[3] Thead, E. *InnoVote Database Access Matrix*, 2005.
[4] Thead, E. *InnoVote Database Detailed Design*, 2005.
[5] Thead, E. *InnoVote MyVotronic Hardware and Operating System Overview*, 2005.
[6] Thead, E. *InnoVote ReliaVote Central Server Functional Design*, 2005.
[7] Thead, E. *InnoVote ReliaVote Precinct Edition Functional Design*, 2005.
[8] Thead, E. *InnoVote SecureDRE Functional Design*, 2005.
[9] Thead, E. *Security Analysis of InnoVote Products*, 2005.

1.4. Overview.

The remainder of this document is organized in the following fashion:

Section 2: Provides general description of the network architecture for precinct- and county-level networks of InnoVote products.

Section 3: Provides specific security measures in place in private networks.

Section 4: Provides a detailed description of the proposed cryptosystem for authentication of data transceivers and protection of data.

2. Classes of Networks

2.1. General Network Design.

InnoVote products are networked with each other in a generally hierarchical architecture. The precincts are all private networks; all electronic voting machines and ballot scanner/kiosks have strictly private IP addresses that are not directly accessible from outside the network, and the precinct computer is the gateway to the public Internet. County-wide networks are distributed across the public Internet, with every node having a public IP address by which it will reach other nodes. Each network will have its own cryptographic key server for authentication of the machines that are part of the network.

Whether they take place over a private precinct network or a public county network, any network connections between machines are encrypted over the Kerberos protocol, and both machines must have correctly identified each other with valid cryptographic keys before any data transfer can take place.

2.2. County-level Networks.

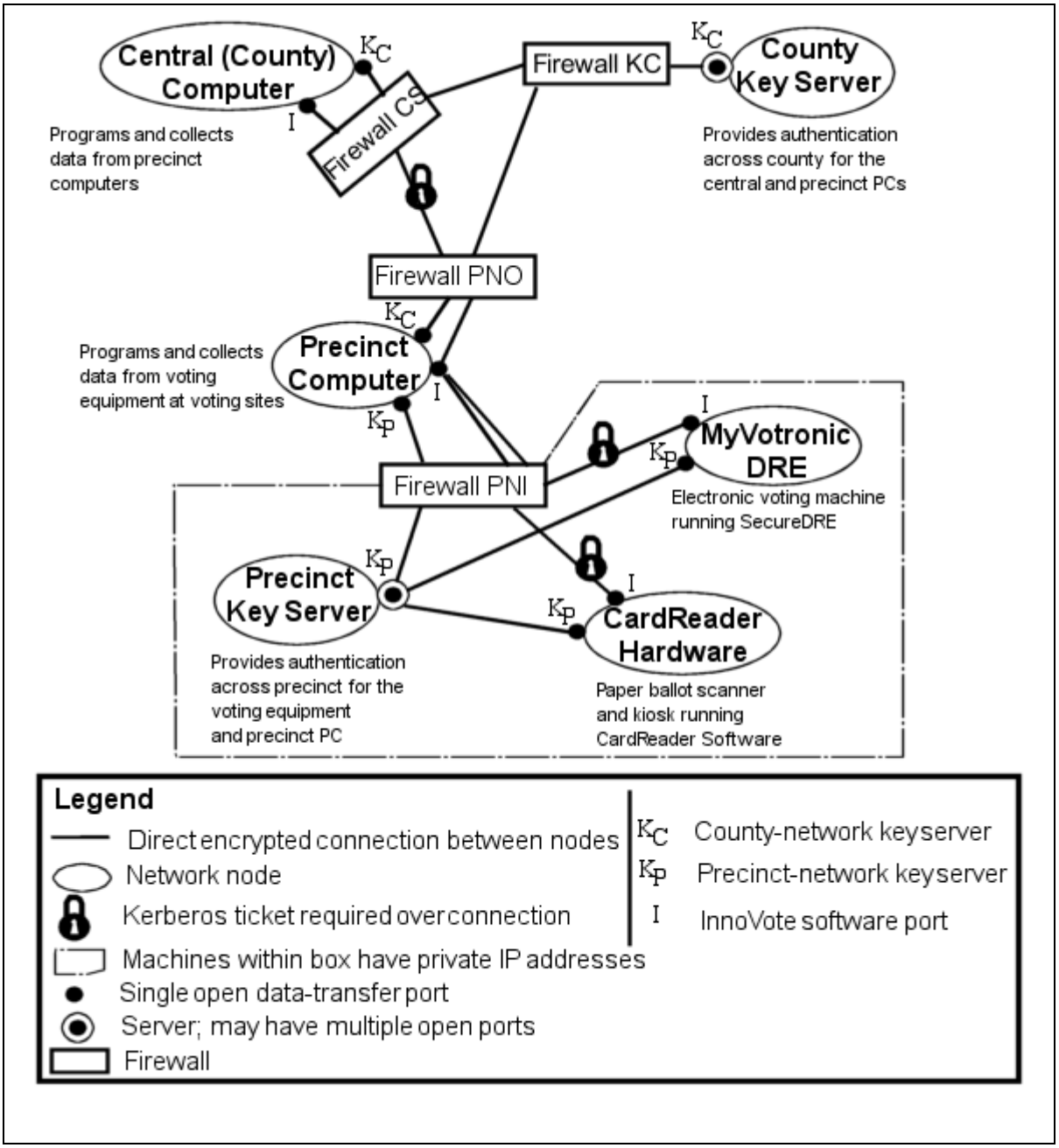
2.2.1. Graphical depiction

Figure 1 shows a general network diagram for county-level networks. The county-level network can contain as many precinct computers as necessary.

The diagram shows that traffic in and out of the county computer and county key server is restricted by firewalls, one for each machine, designated "Firewall CS" and "Firewall KC" respectively. More information about these firewalls is given in §3.3 of this document. The precinct computers have two firewalls, one restricting traffic into and out of it ("Firewall PNO"), and one restricting traffic into and out of a precinct-level private network ("Firewall PNI"). The reason for this is given in §2.3 of this document, with more information about the precinct computer's firewalls in §3.2 of the document.

The data ports are designated "K_C," "K_P," or "I." The ports designated "K_C" are for communication with the key server for a county network. Ports designated "K_P" are for communication with the key server for a precinct network. Ports designated "I" represent the single port number assigned for the use of *all* InnoVote software products.

Figure 1: County Network



2.2.2. County-level network design

This network is distributed across the public Internet. It consists of one central server (running ReliaVote CS or compatible software) and a precinct computer (running ReliaVote PE or compatible software) for every "precinct" or voting site in a county. Additionally, there is a Kerberos key management server which all computers in a county-level network can access. As detailed in §4, this server contains identification keys for all computers on the public network.

Each precinct computer will have one communication port over which ReliaVote PE will communicate with other machines that are operating an InnoVote software product, including ReliaVote CS on the county's central server. Each precinct computer will have another port for authenticating itself to the county key management server. The central computer has a firewall that restricts traffic to that originating at a precinct computer.

(However, as described in reference [6], ReliaVote Central Server further restricts the actions that instructions from remote machines can take, requiring that any machine sending packets remotely authenticate itself using encryption keys. Also, as described in reference [4], the Database disallows unauthenticated users from accessing it, and sensitive tables in it are encrypted. The decryption can be performed only by certain privileged software operations which will be granted access to the tables' decryption keys.)

2.3. Precinct-level Networks.

Three InnoVote software products—SecureDRE, CardReader, and ReliaVote Precinct Edition—will be connected to a private network in a voting site, or "precinct." For any precinct, there must be exactly one computer running ReliaVote PE. There are three possible combinations of voting equipment that could appear on a precinct-level network: only SecureDRE-compatible voting machines, only CardReader-compatible ballot scanners, or a combination of the two.

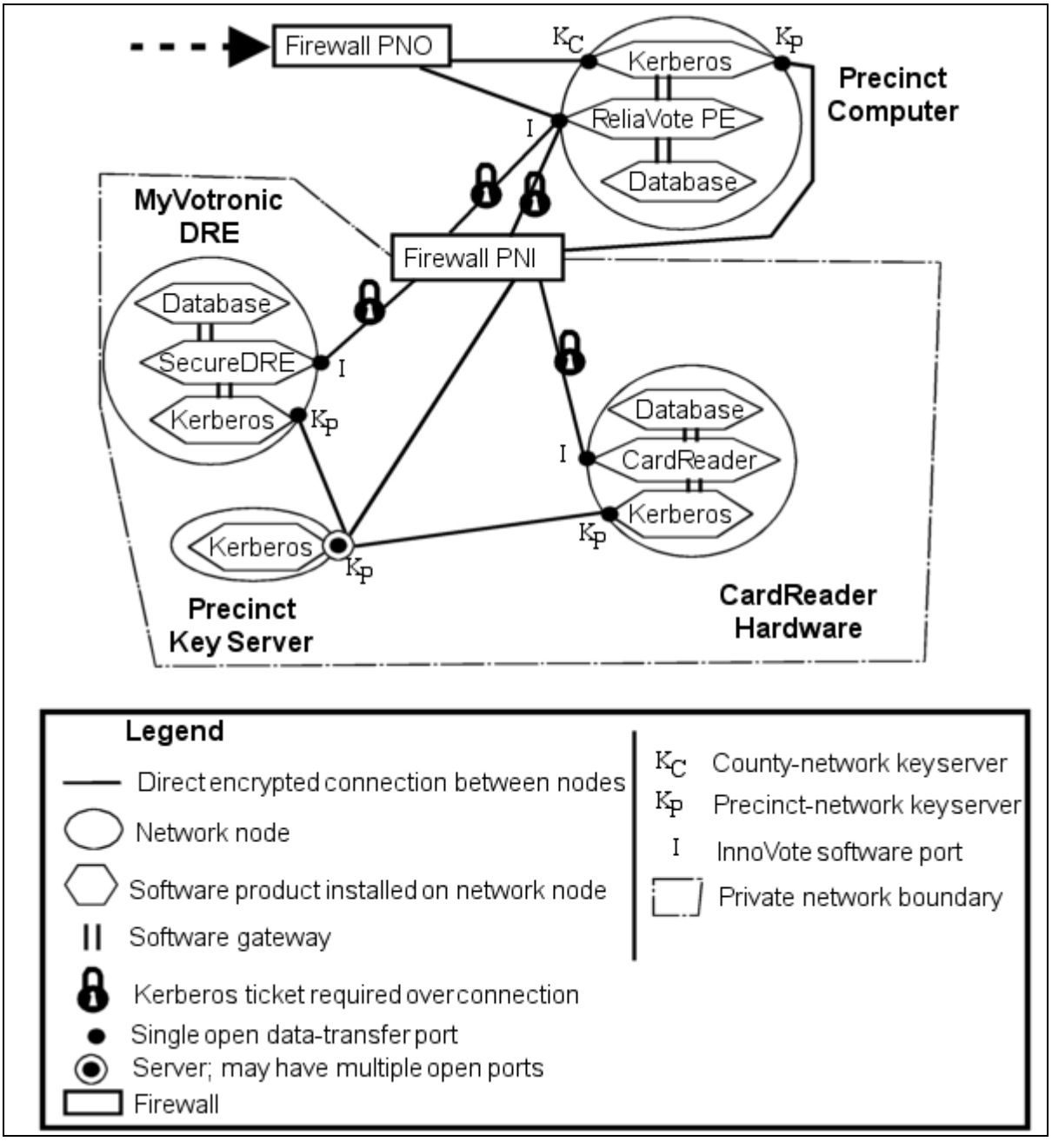
2.3.1. Graphical depiction

Figure 2 shows a general network diagram for precinct-level networks. This diagram is for a network containing DRE machines and paper ballot scanners. However, it is easily modifiable to depict a network of only one type of voting equipment.

The precinct computer has two firewalls, one restricting traffic into it ("Firewall PNO"), and one restricting traffic into and out of a precinct-level private network ("Firewall PNI"). More information about the precinct computer's firewalls is given in §3.2 of the document.

The data ports are designated "K_C," "K_P," or "I." The ports designated "K_C" are for communication with the key server for a county network. As with Figure 1, ports designated "K_P" are for communication with the key server for a precinct network. Ports designated "I" represent the single port number assigned for the use of *all* InnoVote software products. This diagram shows which software products may open a data port, as well as how many ports a software product may use at any given time. A "software gateway" indicates that data is being sent from one software application to another. For this diagram, the context is either that a Kerberos client-side installation is passing authentication information to an InnoVote product, or that an InnoVote product is using the local election database. It should be noted that no database is allowed to open a data transfer port; thereby prohibiting remote logins to the database software.

Figure 2: Precinct-level Network Diagram



2.3.2. Precinct-level network design

A precinct-level network consists of a "precinct computer" that has a public IP address and a private network containing a key server, one or more MyVotronic-compatible electronic voting machines, and/or one or more CardReader devices. Traffic into and out of the network is controlled by two firewalls. One – "Firewall PNO" for "private network outer" – restricts traffic from the public Internet that is destined for the precinct computer (or vice versa), and the other – "Firewall PNI" for "private network inner" – restricts traffic into or out of the private network.

Although the precinct computer could be said to be in a network "demilitarized zone" (DMZ) between the public Internet and the private network, the computer does *not* act as a network router, in the sense of forwarding traffic from the public to private network or vice versa. According to the specifications of the InnoVote software products, ReliaVote CS should not be requesting information directly from any voting device, and voting devices should not be sending information directly to the county computer. As the specifications detail, vote tallies from voting equipment are sent to the precinct computer, which adds the data to its own database, and once the election has ended, the precinct computer transmits its results to the county computer. Database "programming" instructions are also sent down the network from the county server to the precinct computers, not directly to the voting equipment.

It should be noted that, while "firewall" in this section represents a hardware firewall, the InnoVote software products have a built-in "software firewall" mechanism that automatically drops certain traffic. For instance, SecureDRE will drop traffic destined for it that originated at a CardReader device, because there is no need for CardReader to "talk" to SecureDRE.

3. Firewalls

3.1. County network firewall configuration

3.1.1. Firewall CS

As is shown in Figure 1, a county server will be protected by a firewall designated "Firewall CS." This firewall will restrict traffic in and out of the county server, and it will have *at least* the following rules:

1. All outbound packets will be dropped unless the destination IP address is on a "white list" containing the IP addresses of the precinct computers and the county key server.
2. If an outbound packet's destination IP address is that of a precinct computer, the destination port must be the standard InnoVote software product port.
3. All incoming packets must have source IP addresses of a precinct computer or the county key server.
4. If an incoming packet is from a precinct computer, its source port must be the standard InnoVote software product port.

3.1.2. Firewall KC

As is described in §4, every InnoVote product must authenticate itself using the Kerberos protocol when it sends a data transmission to another InnoVote product over a network. As shown in Figure 1, a county network will contain a Kerberos key server. Because of the distributed nature of a county network, this server has a public IP address. As is described in reference [9], this Kerberos server is therefore a vulnerable point. This concern requires that the county Kerberos key server be protected by a very strict firewall. This firewall will have *at least* the following rules:

1. Any packet destined for the key server must have a source IP address that appears on a "white list" containing the IP addresses of the county computer and the precinct computers.
2. Any packet destined for the key server must be a complete, non-fragmented, correctly formed packet.

This firewall configuration will restrict traffic to that originating on the precinct computers and county computer, provided that the list of allowed IP addresses is maintained properly. However, the Kerberos software can still decline to process packets that made it through the firewall if they contain invalid instructions or do not authenticate the source machine correctly.

3.2. Precinct computer firewall configuration

As shown in Figures 1 and 2, the precinct computer will have two firewalls that restrict access into and out of the private network. These firewalls are designated "Firewall PNO," the firewall that restricts traffic to and from the precinct computer, and "Firewall PNI," the firewall that restricts traffic in and out of the private network.

3.2.1. Firewall PNO

Firewall PNO will have *at least* the following rules:

1. An outbound packet will be dropped unless the destination IP address is on a "white list" of the county central server's IP address and the county Kerberos server's IP address.
2. A packet destined for the precinct computer will be permitted only if its IP address is on a "white list" of allowed public IP addresses containing the county computer and the county key server.

3.2.2. Firewall PNI

Firewall PNI will have *at least* the following rules:

1. Any packet destined for a machine on the private network must have originated at the precinct computer itself. The precinct computer should not be routing traffic from the public Internet to private nodes. If ReliaVote Precinct Edition needs to relay transmissions from the county's central server, it will have to repackage the data in a new packet with itself as source.
2. A packet originating at a voting device or the private network's Kerberos server that is destined for a public IP address will be dropped unless its destination is the precinct computer. (This is a safeguard in case the firewall for the machine in question experiences a failure.)
3. A packet originating at a voting device on the private network will be dropped unless the port from which it was sent is the single port permitted for communications. (This is a safeguard in case the firewall for the machine in question experiences a failure.)

3.3. Private-node "software firewalls"

As shown in §2.3, voting machines and ballot scanners in a precinct network have private IP addresses, and the private network is protected by two levels of firewalls. However, the SecureDRE and CardReader software products provide "software firewall" functionality that further restricts traffic *within* the private network. The private network's Kerberos server also has "software firewalls" in place. The "software firewalls" for InnoVote products will have *at least* the following rules:

1. An outbound packet originating at a MyVotronic or CardReader will be dropped unless its destination is the precinct computer or key management server (§4.1).
2. All data-transfer ports on the MyVotronic or CardReader will be closed except for two, one for communication with the precinct computer and one for communication with the key management server (§4.1). This port numbers will be entered into the firewall's configuration and will not automatically change if either number is changed on the machines; the firewall must be manually reprogrammed in such a case.
3. An incoming packet for a MyVotronic or CardReader will be dropped unless its source IP address is that of the precinct computer or key management server (if the key management server is located on a separate IP address). Note: The packet will be allowed, but the SecureDRE software on the MyVotronic and CardReader software on the CardReader hardware will not process any data or instructions contained in the packet unless it can be decrypted and determined to be from the precinct computer.

The "software firewall" for the Kerberos software will have at least the following rules:

1. An outbound packet will be dropped unless its destination is on a "white list" of allowed IP addresses within the precinct network.
2. An incoming packet will be dropped unless its source is on a "white list" of allowed IP addresses within the precinct network and the source port number is on a "white list" of valid client-side Kerberos port numbers (which, unlike the ports open on the Kerberos *server*, will be static).
3. No software other than the Kerberos system may have ports open for listening or for data transmissions.
4. The number of ports that the Kerberos system may have open is bounded by the number of nodes in the private network. This is the same number as the number of systems in the private network that have keys within the system.
5. The Kerberos software may not have more than one port open at a time for communication with a particular node on the network.

4. Secrecy and Authentication

4.1. Cryptosystems.

To ensure data integrity, all InnoVote products that send data transmissions to another InnoVote product must authenticate themselves. InnoVote products use a cryptosystem based on the Kerberos protocol. The design of this cryptosystem is the same for private precinct-level networks and public county-level networks. The only difference is that some machines on a private network do not have public IP addresses; whereas all machines on a public network have public addresses.

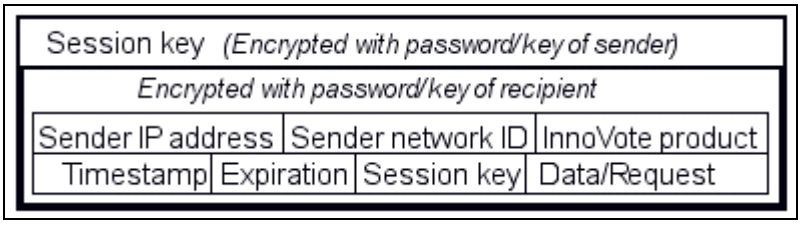
4.2. Kerberos.

The Kerberos protocol is based upon the idea of "tickets" and "authenticators." Every machine that authenticates itself on a Kerberos-enabled network has a password or passphrase which it shares with the Kerberos server and no other node on the network. A machine (the "Client") wishing to send a data transfer to another machine (the "Server") accesses the key distribution center, authenticates itself, and obtains a response from the key server. This response is a packet encrypted with the password or key for the system that the Client wishes to access. The Client sends this "ticket" to the Server.

In addition to the Client's data, Kerberos tickets contain timestamps, expiration times, and further identifying information for the sender such as IP address, a network identifier, and (in the InnoVote implementation) an identifier for the type of InnoVote software that is executing on the Client. A "session key" generated by Kerberos is also appended to the ticket. This session key is useful to the recipient in identifying the sender. All of this information is encrypted with the key of the Server, but the full packet also contains an additional copy of the session key. This entire packet is then encrypted with the key of the Client, so that the session key cannot be intercepted and read by some other host on the network.

Figure 3 shows a schematic representation of this InnoVote-specific Kerberos packet. The "ticket" portion is only that which is encrypted with the recipient's password. It is this part of the packet that will be retransmitted to the Server by the Client, not the part that is encrypted with the Client's own password or key.

Figure 3: Kerberos Packet



Before transmitting the ticket, the Client sends an "authenticator" to the Server containing its IP address, network identifier, and InnoVote software identifier. This "authenticator" is encrypted with the session key, which the Client extracted from the ticket using its own password. The session key cannot be "cracked" across the network in reasonable time if a sufficiently strong encryption standard is used. The Server cannot do anything with the Authenticator initially, since it does not have the session key, but when the Server receives the Kerberos *ticket* from the Client, it decrypts it using its own key or password, extracts the session key from it, and uses this key to decrypt the "authenticator" and validate the identity of the Client.

This protocol is extended in InnoVote products to support full encryption of all network transmissions, not just requests to use a service on another system. The Advanced Encryption Standard algorithm will be used with at least 192-bit encryption. InnoVote products will use Kerberos version 5.