



Integrated Conferencing Platform™ (ICP)

Security Overview

Rev. 1.02

Whitepaper



ICP Security Features

The following multiple security features are built into Arel's ICP platform:

Web security – Arel server technology uses SSL (Secure Sockets Layer) to protect HTTP transmissions from unwanted eavesdropping. By default, the Spotlight Campus portal is secured by an SSL encryption mechanism, providing security for login information as well as data related to content and participants. The portal's security protects usernames and passwords in order to prevent anyone from entering the portal uninvited and gaining access to important content. The Spotlight Campus SSL security can be optionally disabled during the installation process.

Content download encryption using SSL – Content will be optionally encrypted. This mechanism will block the capability to eavesdrop to the actual download of content but when it's on the client's hard drive, the content will not be in an encrypted mode.

Push content SSL encryption – All content that is "pushed" to the desktop clients using Arel's push content mechanism is encrypted using SSL.

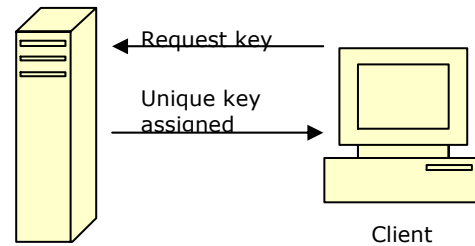
Client-server communication encrypted using SSL – All communications between the different clients and the servers can optionally be encrypted using SSL¹. This mechanism will block the capability to eavesdrop to the actual communications between the servers and the clients.

The use of public and private keys enables the server to send a client a public key that is used by the client to encrypt the messages while only the server can decrypt those messages as only the server knows the private key that is needed to decrypt the messages (the private key is never shared). In other words, a message that is encrypted using the public key can only be decrypted using the matching private key that is only known by the server.

¹ The SSL encryption for the **video stream** is planned for Q3 2004.

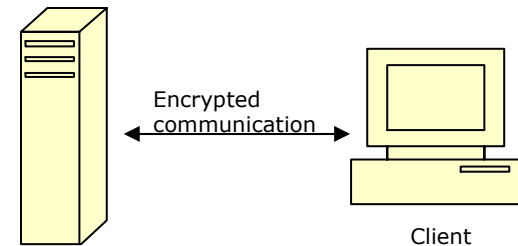
How the encryption mechanism works –

- 1) Connection initiated – Each time an Arel client opens a new connection to the Arel server, as part of the “handshake” both the server and the client randomly create a pair of public and private keys, then they exchange their public keys (the private keys are never exchanged).



This server’s public key is unique to this specific socket connection and no two keys are the same.

- 2) All communications between the server and the clients is now secured by encryption using a public key unique to the specific client or server and the specific socket.



- 3) Since the communications are now secured, the client and the server can now securely exchange symmetric keys such for 3DES or AES type encryption.

- 4) All communication are now encrypted using AES or 3DES encryption algorithm.

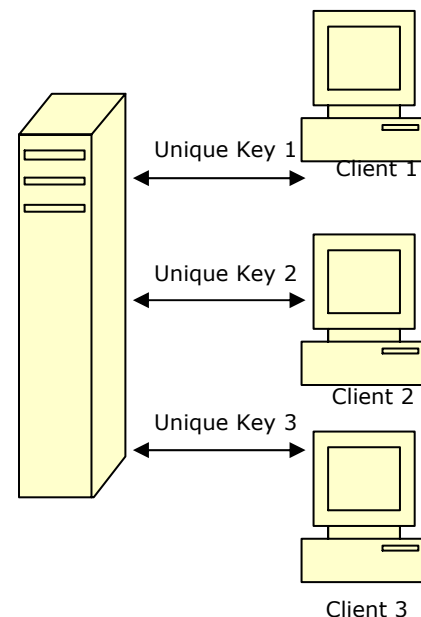
Why is it secure?

Each client owns a public/private key pair for itself, and when it connects to the server, the client will first negotiate an encrypted session with the server and then send the server the client's public key.

The advantage of public/private key authentication is that a private key (that is the only way to decrypt a message) is never sent across the line, even in an encrypted form. The private key was not communicated and therefore can't be intercepted; only the receiving party can decrypt the message.

Since each client receives its own unique key, even if a 3rd party is “listening” to the connection and manages to intercept a key, the intercepted key can't be used by the 3rd party because an attempt to open a new socket with the server using the wrong key will be rejected.

After the communication is secured it is possible to exchange symmetric keys for any encryption algorithm such as 3DES or AES.



Microsoft SQL Server™ security – Arel ICP servers support encryption of login and application role passwords stored in the SQL Server as well as any data sent between the client and the server as network packets.

Temporary file deletion – Content that was downloaded to a participant's PC during a session is deleted when the session is over.

Application and component security – Arel's client application is written in C++ and is composed from ATL (Automatic Template Library) components. All installations are secure by Verisign's digital signature for authenticity assuring the integrity of the download. All of Arel's ATL components include an activation code that is required by any application that tries to use them.²

² The ATL activation code mechanism is planned for Q3 2004.