

T E C H N O T E

Encryption in Pharos Communications

Sensitive communications between Pharos servers and clients are encrypted. This document describes the various encryption methods used by the Pharos system.

Pharos Encryption Methods

All client-server communications in the Pharos system use a proprietary layer on top of TCP/IP. The encryption methods used depend on the version of Pharos.

Pharos 6.1 and Earlier

RC4 encryption with 128-bit keys is used to encrypt passwords, and all of the information that accompanies a print job sent by the Popup Client, e.g. username, job password, cost centers

Pharos 7.0 and Later

All Pharos client-server communications are encrypted using AES encryption with 128-bit keys. The encryption process is as follows:

1. Each time a Pharos Server is rebooted, it generates a new public/private key pair.
2. A client connects to a server.
3. The Server sends the public key to the client.
4. The Client generates a random session key, encrypts it with the public key, and sends it to the server.
5. Client and server then exchange messages encrypted with AES, using the session key and a fixed key embedded in the client and server. (The fixed key means that to make a man-in-the-middle attack, an attacker would need to obtain the fixed key.)

Pharos Interfaces to Other Systems

Mac Popup Client

Macintosh clients are secured using RC4 encryption.

Gateways

Communication between the Pharos Billing Plug-in and Pharos Gateways is encrypted using linear congruent RNG. The Blackboard TIA Gateway offers AES encryption for communications between the gateway and billing service.

Pharos EDI

The Pharos External Device Interface (EDI) is installed as an add-on to Microsoft Internet Information Services, and uses HTTP to communicate with third-party devices and applications (this includes PS20 terminals and Pharos Omega). Communication to and from the Pharos EDI can be encrypted with SSL (documents on setting up SSL are available in the **InstallGuides** directory of the Pharos Documentation CD).