



2009 PKI Certificate Initiative

Digital **Public Key Infrastructure** (PKI) security certificates are used for data encryption on secure communications links in several Avaya products. By design, security certificates expire after a period of time, requiring system administrators to update them periodically. This advisory is to notify customers that many Communications Manager systems worldwide have PKI certificates with an expiration date of March 11, 2009. A small number of Application Enablement Services (AES) and Modular Messaging systems also have certificates that expire on this same date.

Below is a list of what systems are affected and how they are affected.

[Communication Manager releases 2.0 – 4.0.1](#)

1. **Translation file synchronization will fail** between the main server and any Local Survivable Processor (LSP) or Enterprise Survivable Server (ESS). In case of network disruption, failover to an LSP or ESS will proceed as normal after certificate expiration. If, after certificate expiration, the system administrator performs any station moves, adds, changes or any other action which modifies the translation file, the LSP and ESS will not be able to use this updated information.
2. **SIP trunk creation will fail.** SIP trunks created before the expiration date will continue to operate normally. Features which use SIP trunks include SIP phones, Expanded Meet-Me Conferencing, G860 media gateways, service provider connectivity and others.
3. **Links to Application Enablement Services (AES) and Modular Messaging adjuncts will fail.**
4. **The encrypted link option with software duplication between an S87xx server pair will fail.** Software duplication without encryption will continue to operate normally.
5. **The Upgrade Tool, found on the Communication Manager server's maintenance web page will fail.**

[Application Enablement Services](#)

The following features and capabilities of Application Enablement Services will not operate properly after the certificate expiration date:

- AES 3.x, 4.0 and 4.0.1 that are used with end user applications (e.g. NICE) with media encryption enabled (encrypted port 4722) will be impacted.**

[Modular Messaging](#)

The following features and capabilities of Modular Messaging will not operate properly after the certificate expiration date:

□ Only MM R3.x systems that use SIP are affected. SIP stops working when the certificate expires.

**** Technical procedures for obtaining a new Remote Feature Activation license can be accessed by clicking [here](#).**

Consultedge is here to help. Contact us at (800) 626-2515 or support@consultedge.com