Ferris Research

AOL Enterprise AIM Services Adopts PKI-Based Security over SSL

July 3, 2003

AOL announced new enterprise-oriented versions of its IM gateway server and IM client on Monday. The most interesting aspect is AOL's decision to embrace digital certificate, or public key infrastructure (PKI)-based encryption instead of Secure Sockets Layer (SSL)-based encryption. PKI-based encryption works by locating the public certificate of the intended recipient, and scrambling the outbound message with it. On receiving the message, the recipient's client uses their private (or secret) key to descramble the message. When it works seamlessly, PKI-based encryption is very elegant.

While PKIs offer superior security and encryption, they have generally been a failure in the market due to numerous technical issues. AOL's implementation may prove to be a breakthrough offering, however, since AOL manages the end-to-end system. This end-to-end control--from the IM clients, the digital certificate issuance via VeriSign, the Enterprise AIM Gateway, and the public IM servers--removes the challenges involving trust assertions and trust relationships in cross-organizational and cross-PKI implementations.

For encrypted IM, PKI-based encryption makes much more sense than SSL, because it provides end-to-end privacy. SSL encryption provides a clear text translation after receiving the message from the sender and before re-encrypting it for delivery to the intended recipient.

In closing, here are some other points to note:

- End-to-end encryption via PKI should put less load on the AIM servers, thereby enabling greater scalability. Incoming messages don't have to be decrypted and then re-encrypted for delivery to the end user, as is the case with SSL.
- The reliance on Class 2 digital certificates, in conjunction with tight control over which organizations get and implement the AIM Gateway, will give a reasonable level of assurance that end users are who they claim to be. Class 3 certificates, which involve a much higher degree of personal verification and confirmation, are a better option for particularly security sensitive situations. AOL provides an option for gaining Class 3 certificates (the highest assurance of identity), Class 1 certificates (the lowest assurance of identity), as well as any X.509v3 certificate generated by any Certificate Authority.
- AOL is delivering a very seamless enterprise plus public network IM service, all from a single client. Microsoft's IM strategy is less clear cut, with different IM client requirements depending on whether Office Real-Time Communications (RTC) Server 2003 is deployed or not. In addition, cross-enterprise connectivity requires federation between RTC servers, which does not come into play with the AOL Enterprise AIM offering.

This bulletin was published by market researchers Ferris Research as part of its Analyzer Information Service. The service studies and tracks network-based technologies that help people work together, such as email, instant messaging, desktop conferencing, and voice-over-IP.

Ferris Research Insight Bulletin. July 2003.

For subscriptions, contact us at +1 415 986 1414 or info@ferris.com.