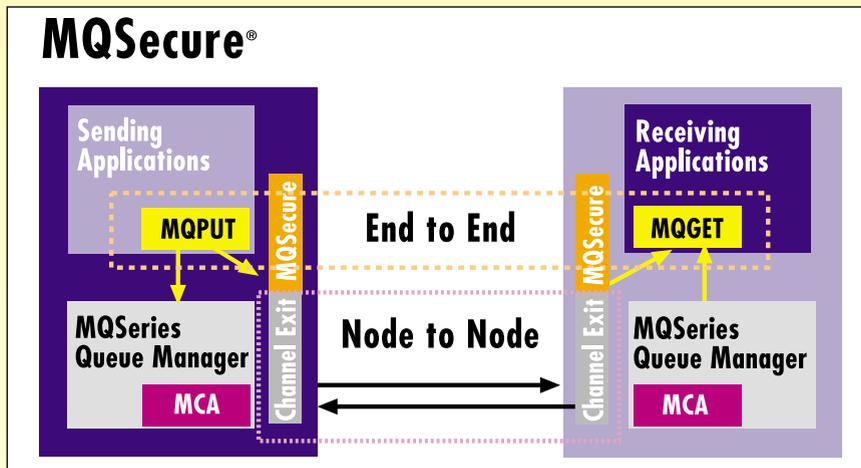# Candle Corp.'s MQSecure

Award-Winning WebSphere Solutions Features Point-to-Point Security

Today, more than ever, organizations must protect information and assets from unauthorized access. Developing, implementing, and maintaining a secure network infrastructure presents a number of challenges, ranging from policies and user management, virus protection, unauthorized access, hardware and software configuration, firewalls, virtual private networks, intrusion detection, disaster recovery, encrypted file storage, to security over e-business environments. Moreover, during periods of growth, enterprises hire new employees and retain contractors. With each new user and application, security vulnerabilities increase exponentially. Enterprises require tools that ensure the confidentiality and stability of critical business information, regardless of where it exists on the network.

Candle Corp. offers a suite of MQSeries, e-business solutions designed to simplify the complex challenges of testing, building, and managing applications across many platforms. MQSeries, a leading solution for transport mechanism for data and information, is part of IBM's WebSphere family and enables users to exchange information between applications across more than 35 platforms. Middleware and enterprise application integration is the heart of e-business, and Candle supports e-business infrastructures with this MQSeries family of products. Candle's MQSecure tool secures critical business information as it moves across the network, providing powerful security features that prevent message tampering and unauthorized reading. MQSecure enables users to implement security services for MQSeries

software and offers end-to-end security for MQSeries applications.

Added Value Features

MQSecure supplements the user authorization capabilities of various external security programs, such as RACF, ACF2, and Top Secret on OS/390, as well as operating system security tools on Unix and Windows systems. MQSecure also includes node identification and authorization for MQSeries channels. MQSecure protects MQSeries applications and valuable information from known sources of corruption, and provides vital security, such as validation to ensure that messages sent from one system or application have not been altered, confidentiality to ensure that message contents are confidential while traveling over the network, authentication to ensure that a message sent actually came from the person claiming to send the message, and non-repudiation to ensure that users cannot deny sending messages.

Enterprises can rely on the solution's built-in security features. MQSecure is based on the standard RSA public-key cryptography — the most secure distributed cryptography for protecting critical applications. It provides mutual authentication between two communicating plat-

forms and is available in client and server environments. Using RSA's RC2 technology to encrypt messages, MQSecure ensures that MQSeries messages are encrypted from the sending application to the target application. Validation of the received message ensures that messages are unaltered.

The Latest Version Offers Two Types of Security

MQSecure Version 200 includes a number of enhancements, including:

- LDAP-based distribution of public keys
- Friendlier APIs
- Support for hardware encryption devices
- Support for MQSeries clustering
- Performance enhancements for node-to-node encryption
- Enhanced database support
- Java API
- Dual log support.

MQSecure provides two types of security, depending on the appropriate level needed to protect critical business information. Node-to-node (machine-to-machine) ensures the safety of business information traveling between nodes or machines, while end-to-end (application-to-application) ensures the safety of business information between applications or user IDs.

MQSecure is available from Candle Corp., 201 North Douglas St., El Segundo, CA, 90245. Voice: 310-535-3600; Fax: 310-727-4287; Website: www.candle.com/websphere. eAI

— Ellen J. Silverman