INSURANCE BROKERS ASSOCIATION OF CANADA
ASSOCIATION DES COURTIERS D'ASSURANCES DU CANADA

SECURITY AUTHENTICATION FOR BROKER-INSURER DATA EXCHANGE

NATIONAL POSITION PAPER

Brokers and Insurers can deliver information to one another far more efficiently using electronic means than by traditional methods. The business purposes behind these exchanges, however, and the roles of the correspondents, have never changed; the distinct roles and separate responsibilities of broker and underwriter still persist. It follows, then, that the rules and security conventions for electronic data exchange must reflect the business model they serve.

Brokerage principals control their own operations, and are ultimately accountable for their employees' actions. Insurers grant binding authority on a brokerage-by-brokerage basis; indeed, Broker-Insurer contracts are abundantly clear that brokerages are responsible for errors or omissions, or infringement of binding authority, by their staff.

Traditionally, brokers have communicated with Insurers via various tools such as written memorandums, telephones, or more recently, email and EDI. Insurers have not determined a particular employee's authority to correspond with underwriters or relay client instructions; that duty has always rested squarely on the brokerage principals' shoulders.

Delivering information to Insurers electronically through web services does not alter that responsibility; brokerages still govern the training and actions of their own staff and have accountability for individual actions performed on behalf of the brokerage. That supervision includes the security of internal brokerage networks and BMS's, which make use of centrally-controlled individual user names and passwords. Once a user name is deleted or disabled, all access is also removed, including to all other dependent application(s) accessed through the broker's own central system.

Dangerous risks are created, however, when individuals can access Insurer systems directly without routing through an identified brokerage's system. Where the only prerequisite is an internet connection, persons recalling their usernames and passwords can access Insurer systems from anywhere. When an employee leaves the firm, brokerage principals must react immediately to cancel each and every Insurer password assigned to that person, but must frequently rely on various back-logged Insurer administrators to complete the task.

Aside from this high potential exposure, the programming complexity and ongoing maintenance needed to manage individual passwords for each brokerage employee, for multiple Insurers, adds untold expense both for brokers and especially for Insurers.

On the other hand, an authentication method using a single brokerage-level password reduces the potential for outside abuse by individuals, and eliminates multiple layers of unnecessary complexity and cost. The Insurer system verifies that the incoming message is indeed from an approved brokerage and that the information received is therefore sanctioned by that firm.

Of course, the sender of a communication, whether brokerage or Insurer staff, must still be identifiable for audit purposes. Further, brokerages must be diligent in ensuring that all user-level passwords are kept secure and confidential, and that access to internal broker systems is terminated immediately should an individual leave their employment.

IBAC reaffirms brokers' authority over their own operations and their staff. In the interests of all industry stakeholders, IBAC is committed to promoting the most effective use of technology in order to best serve consumers, moving away from portal-based communications models.

IBAC urges Insurers to consider the following when designing and building electronic interfaces with their broker partners.

IBAC Security Model Principles

- Brokerages, not individuals, contract with Insurers.
- Brokerages take responsibility for the training and actions of their staff, for the authority given to them, and for their access to network and communication resources.
- Electronic communications do not alter the traditional Broker-Insurer business model.
- Authentication for conveying information electronically to Insurers can be most securely controlled by brokerages when based at a system-level (i.e., brokerage system to insurer system).
- System-based authentication eliminates the additional expense, complexity, and the inefficiency inherent in individual username-password requirements.
- Individual correspondents must be identifiable but do not require additional authentication.