



Keys to trust

by Richard Bray

End-to-end electronic procurement will only become a reality when confidential information can be transmitted safely and securely between all involved parties. For any government, e-procurement security is essential for online bidding, for identifying people and groups on the supply chain network, to enable enhancements like comparison shopping and to ensure that catalogues are authentic.

E-procurement depends on reliable security and the Government of Canada has made a commitment to Public Key Infrastructure (PKI) as its security technology of choice. PKI is, for many people, difficult to understand at first, involving as it does one public and one private key – usually strings of numbers – to encrypt and de-encrypt data. If this column were being sent to an individual using PKI, for example, it would be encrypted using that person's public key, typically found online at a Certification Authority (CA). The CA would already have established, to some degree of certainty, the identity of the person holding that key. To unscramble the signal, the recipient uses the private key, which is typically stored on their computer or a smart card.

Especially within organizations, small-scale PKI deployments are manageable. Because the personal identity of key holders is all-important, people in smaller groups can receive their keys in person. When they lose a key or change jobs, their keys can be quickly cancelled and reissued. The problem becomes a little more difficult when people work in remote locations, but usually someone is delegated as “keeper of the keys.” The problem becomes more complicated when different organizations want to communicate confidentially, but more and more CAs are beginning to “recognize” one another as trustworthy.

A whole new PKI bureaucracy has grown up in the past several years, just to cope with secure communications between federal departments. At Public Works and Government Services Canada, the Government Telecommunications and Informatics Services manages the PKI solution through Secure Applications and Key Management Services (SAKMS). Besides managing CAs for more than 50 federal agencies and departments, SAKMS holds user group meetings, mans help desks, runs training sessions and trains and supports a network of local registration authorities.

While there has been substantial progress on securing communications within the federal government, discussions with consultants who have been working on PKI make it clear that the current deployments within the federal government constitute a patchwork. Some of the most effective solutions have been developed in a stovepipe manner by departments intent on solving a specific problem.

By definition, PKI is labour-intensive and expensive. When departments move forward and create islands of technology, their experience may have nothing to offer other departments or agencies. The result is a problem not just within government but also for companies and indi-

viduals that want to do business with them. If there is a multiplicity of security systems within government, that can only complicate life for vendors.

From governments' point of view, the challenge of using PKI in e-procurement is assigning a distinct, digital identity to anyone and everyone who wants to do business with them. The challenge is quite different from the vendors' perspective. If a purchasing organization mandates a certain level of technology or computer skills on the part of its vendors, some companies could find themselves on the outside looking in. Smaller companies would certainly find it difficult to implement systems that interoperate with multiple buyers. It would be even more difficult for them to implement systems to interact with different government departments that may not be using the same systems.

At this point, it appears that the Secure Channel project, and therefore federal e-procurement, will use a web-based PKI system for its dealings with business. Government purchasers will be able to verify transactions, keep an audit trail, provide electronic receipts, and, most of all, know that they are communicating with the right person.

No matter what the eventual solution looks like, governments have to create security systems that operate with the simplicity and reliability of telephones in order to reap the benefits of automated procurement while maintaining fair and open access to public business. Until that time, it is going to be difficult for the small- and medium-sized businesses to step up and use e-commerce tools in their dealings with government. ~~~

Richard Bray is an Ottawa-based freelance writer specializing in the IT sector. He has been published in magazines and newspapers in Australia, the US and Canada. Before freelancing, he worked as a producer, reporter and senior writer for CBC in Toronto.

**GET YOUR OWN
copy of SUMMIT today!**

SUBSCRIBE NOW

1-800-575-1146

(in Ottawa call 688-0768)

or visit us at:

www.summitconnects.com