

Designing a security-enhanced e-commerce payment solution using public key infrastructure for the Canadian Payments Association (CPA)



CPA: Building the virtual cash register.

The fading sound of cash registers

“Ca-ching!” In the traditional retail world, the sound of a cash register has the ring of security. Both buyer and seller know exactly with whom they are doing business. Money goes directly from one hand to another.

Not so in today’s connected world of e-commerce. Here, buyer and seller never meet. A retail transaction must be completed electronically, without any cash physically changing hands. In this environment, the challenge is to build a kind of virtual cash register, where payments from a business’s or consumer’s bank account can be processed with the “click” of a mouse as securely as that old, familiar “ca-ching.”

“IBM assembled a team with proven project management experience and first-class expertise in PKI and in the business.”

– Bob Hammond, General Manager, CPA

Building a new framework for e-commerce payments

The Canadian Payments Association (CPA) is working on a solution. In 1999-2000, the CPA, its member financial institutions and its stakeholder representatives have worked with IBM Global Services to build a new framework for security-enhanced e-commerce payments direct from businesses’ or individuals’ bank accounts. How? With one of today’s most advanced security technologies: public key infrastructure (PKI).

Challenge

Consumer concern about the security of personal and financial information transmitted via the Internet has hindered the growth of e-commerce in Canada.

Solution

IBM security consultants assisted the CPA with establishing the framework for a public key infrastructure that will facilitate security-enhanced e-commerce payments directly from accounts at financial institutions.

Benefit

The CPA’s leadership ultimately transforms how millions of transactions are carried out each day in Canada and internationally.



It is a bold initiative and not without its risks. But, according to CPA General Manager Bob Hammond, the relationship with IBM has helped the CPA prepare to manage those risks and move forward.

“IBM assembled a team with proven project management experience and first-class expertise in PKI and in the business,” says Hammond. “They not only have the world-class skills needed to develop a PKI solution; they have demonstrated that they fully understand the business and legal implications and helped us work through these issues to achieve our objectives. As a result, our PKI solution reflects our unique business model and what will work best for our members and for Canadian businesses and consumers.”

“We are very impressed with the IBM team’s understanding of the potential risks and their ability to help us work through the issues to achieve a consensus.”

– Bob Hammond, General Manager, CPA

Building the trust in e-commerce

The CPA is a nonprofit association created by an Act of Parliament in 1980. Its mandate is to establish and operate a national clearing and settlement system and to plan the evolution of the national payments system. Its current membership comprises virtually all of Canada’s bank and nonbank deposit-taking financial institutions.

Today, almost every financial transaction in Canada that involves a transfer of funds between financial institutions—from an automatic teller machine (ATM) bill payment to a multibillion dollar funds transfer—is cleared and settled via CPA systems. In fact, as Canada’s established and trusted payment authority, the CPA clears and settles transactions averaging \$120 billion Canadian each business day.

When it comes to e-commerce, however, establishing that trust for Canadians is a far more complex undertaking. As CPA Chairman Serge Vachon sees it, “Consumer concern about security of personal and financial information transmitted via the Internet has hindered the growth

of e-commerce in Canada. The CPA is already a trusted authority for clearing and settlement in Canada. Our leadership role will provide confidence that Internet payments using digital certificates will be secure and that sensitive information related to transactions will be safeguarded.”

In early 1999, a CPA Working Group assessed the role the Association might play in e-commerce and recommended a PKI initiative. PKI involves the use of cryptography to establish the unique identity of an individual, business or organization for the purpose of exchanging information. The technology is complex, and it is a real business challenge to sort out the roles and responsibilities needed to achieve safeguarded online transactions.

Enter the IBM consulting team, which included a number of leading industry experts rich in international experience. More importantly, the members collectively understood the issues and sensitivities surrounding the use and misuse of customer information, particularly in the context of e-commerce.

“We are very impressed with the IBM team’s understanding of the potential risks and their ability to help us work through the issues to achieve a consensus,” says Hammond. “It was not always easy, because our members had very different requirements and expectations. IBM was able to help us reconcile all these perspectives and develop a secure, stable framework for PKI within a time frame that worked for everyone. We are very pleased with the progress they have helped us achieve. We now have a solid basis to move forward with the technical solution and implementation.”

Building a unique PKI solution

The initiative was one of the largest consulting contracts ever won by IBM Canada and the first of its kind for the IBM Security and Privacy Services team worldwide. The IBM team participated in every aspect of designing the CPA’s PKI solution, including:

- Defining the PKI business and technical requirements, including system architecture
- Developing the certificate practice statement and certificate policies that set out the rules, policies and procedures governing the operation of the PKI system
- Establishing the registration and accreditation rules for subordinate Certification Authorities, primarily CPA members
- Developing criteria for cross-certification with other PKI systems, including those being developed internationally
- Developing criteria for selecting the technical solution to implement the PKI framework.

The CPA’s approach features a distinct business model, compared with other PKI solutions. In the exchange of information, the CPA will act as the “root” certification authority. This means it has the role of confirming the identity of its member financial institutions and other qualified entities through the use of digital certificates.

In turn, the financial institutions that make up the CPA will issue their own digital certificates. Each digital certificate uniquely identifies the certificate holder, like an electronic fingerprint. Put it all together and you have a distinct way to verify the identity of buyer and seller even though they have never met.

“Through the significant intellectual capital IBM brought to the table, we now have a well-constructed plan to move forward,” concludes Hammond.

For more information

To learn more about IBM Global Services, contact your local IBM sales representative or visit our Web site at:

ibm.com/services



© Copyright IBM Corporation 2000

IBM Global Services
Route 100
Somers, NY 10589

Produced in the United States of America
11-00
All Rights Reserved

IBM, the IBM logo and the e-business logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product and service names, may be trademarks or service marks of others.

Many factors have contributed to the results and benefits achieved by the IBM customer described in this document. IBM does not guarantee comparable results.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.