Industry Canada releases principles for electronic authentication

DR SIMON H HODGETT

On May 13, 2004, Canadian federal government's Minister of Industry, the Honourable Lucienne Robillard, released *Principles for Electronic Authentication: A Canadian Framework* (the 'Principles')[1]. The Principles are the culmination of two years work by a working group consisting of representatives of industry, government and consumer groups. They continue Industry Canada's efforts to promote electronic commerce by both the promulgation of guidelines and legislative initiatives, and by participating in ongoing dialogues at the international level. The Principles are not legislation and do not appear to foreshadow legislative action. At present, the federal government does not appear to have a legislative agenda to enforce uniform criteria for authentication systems outside the federal government.[2]

Authentications

Electronic commerce provides tremendous opportunities and efficiencies in both the private and public sectors. Confidence in such systems, which by their nature do not involve face to face interaction, is essential. Confidence is fragile, however. Incidents whereby personal information or funds are misdirected by fraudulent means or error dramatically set back the progress of electronic commerce. The Principles rightly identify authentication of electronic transactions as making a significant contribution to building user comfort in electronic commerce.[3]

Authentication refers to any process by which credentials of a person are confirmed to allow access to a service or rights. We undergo authentication processes all the time. Signature confirmation at a bank is the archetypical form of authentication. Presentation of a passport with a quick confirmation of the passport photograph is an authentication for obtaining access to government-sanctioned travel privileges. In the world of electronic commerce, proxies must be found for these face to face interactions. The most common electronic authentication process is the use of user names and passwords. The more sensitive the service, the more safeguards are added to the mix. For example, financial services web sites use encryption, additional back-up passwords, scoring systems based on answers to questions and call centre verification of identifying information.

The more sensitive the service, the more safeguards are added to the mix

In addition to systems that confirm credentials or the identity of the individual accessing the system, authentication systems also include measures to confirm the integrity of the received message itself. Integrity of messages is fundamental to ensuring that the credentials presented are real and that the request remains as originated by the person trying to obtain access to the service or right. For example, for an e-mail money transfer, it is certainly important to know whether it really is the account holder making the request, but it is also vitally important to know that the funds are directed to the person the account-holder intended.

At the present time, Public Key Infrastructure (PKI) is the technology of choice for authentication

[1] The Principles can be found at http://strategis.ic.gc.ca/authen.

[2] Interestingly, the release of the Principle coincides with circulation for comment of new regulations (http://canadagazette.gc.ca/partI/2004/20040508/html/regle6-e.html) relating to certification authorities under Part II of the *Personal Information Protection and Electronic Documents Act* (2000) ("PIPEDA"). Part II of PIPEDA was designed to provide for electronic alternatives to paper-based signatures where signatures are required under federal legislation. Failure to designate statutes to which Part II applies has left it inoperative, however. The regulation is more detailed than the Principles in that it sets out criteria for certification authorities for the purposes of authentication recognition. It remains to be seen whether the federal government will designate existing federal legislation (e.g. *The Bills of Exchange* Act) so that electronic signatures are treated as equivalent to paper signatures for the purposes of executing documents required by such legislation.

[3] Principles, p 2.

Whether countries or trade blocks are formulating legislative initiatives or merely making recommendations for industry implementation, common principles are an important element of promoting international trade through electronic means

systems. PKI relies on the interaction of two "keys", one public (that is, revealed by the owner) and one private (not revealed by the owner).[4] PKI rests on a secure infrastructure and, critically, on reliable certification authorities to administer and confirm keys within that system. If an institution is going to accept a transaction from an individual through a system supported by PKI, it must have confidence in the certification authority. This can be achieved either by carrying out the function within the umbrella of the institution itself or by relying on certification authorities that meet its criteria for reliability.

Currently, institutions running electronic systems rely for the most part on their own assessments of suitable authentication systems. There are no universally accepted authentication systems cutting across commercial and government sectors. Banks authenticate transactions for their own customers based on identifying information gathered by the bank. The legal foundation of the relationship is the traditional account agreement with the customer. Government also has its own authentication methodologies for tax filing and other services. Each sector and each player within sectors has its own risk tolerance and its own distinct methodology.

This 'silo' approach to authentication has disadvantages. Without widely accepted approaches and standards for authentication, an enterprise is hesitant to accept authentication from another enterprise for its customers. Different risk tolerances may exist between the organizations. Agreements are difficult to reach without common principles within which to frame the discussion.

The same issues exist on a broader scale at the international level. Whether countries or trade blocks are formulating legislative initiatives or merely making recommendations for industry implementation, common principles are an important element of promoting international trade through electronic means.[5] For example, the Canada-United Kingdom Joint Statement on Global Electronic Commerce and E-Government (the "Joint Statement") declares the desire of both countries to establish "a common framework and approach that would promote electronic transactions across borders and that support a variety of authentication technologies."[6] The acceptance of "made in Canada" authentication systems internationally is one of the stated aims behind the Principles.

The Industry Canada Principles

The Principles should be considered with this broader background in mind. The Principles are designed to be a framework and necessarily cover a broad spectrum of relationships.[7] Those who expect to receive clear direction from the government regarding design and technical aspects of authentication systems will not find that level of detail here. The working group appears to have concluded that detailed prescriptions would risk the exclusion of sector-specific concerns and future obsolescence as technology develops. Specific standards are better left to industry groups and standards organizations.[8]

What also does not appear in the Principles is a specific effort to promote interoperability between authentication products, or fostering competition in the certification-service-provider industry-goals, for example, found in Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Instead, the Principles are focussed on the broad issues, which should be addressed by companies developing agreements intending to create authentication systems. The Principles establish broad categories for continuing discussion.

Even though the Principles specifically state that they do not address consumer protection,[9] concern for the place of end users in the establishment of any system is a theme throughout. A number of the Principles acknowledge the importance of protecting the rights of end-users through information sharing, the protection of privacy and the handling of complaints. These concerns are in keeping with international initiatives like the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, and are the corollary of the working group's stated belief that robust authentication processes should enhance user confidence.

Each Principle consists of a core statement followed by explanatory text. The discussion remains high level however, suggesting a consistent intention to suggest rather than legislate for solutions.

[5] The Principles refer to the importance of OECD *Guidelines for the Security of Information Systems and Networks* (p 24) and state that the Principles have been drafted to be compatible with international developments in authentication.
[6] Joint Statement, p 4. The Joint Statement was signed by then Minister of Industry Brian Tobin and then President of the Treasury Board and Minster responsible for Infrastructure the Honourable Lucienne Robillard on February 20, 2001.
[7] Principles, p 9.
[8] The Internet Engineering Task Force's Public Key Infrastructure (X.509) Working Group, for instance, was established with the intent to develop the Internet standards needed to support an X.509-based PKI.
[9] Principles, p 5.

Principle 1 is a useful discussion of roles and responsibilities within authentication systems. The principle will assist those who are developing risk analyses or system-related agreements to identify and discuss the various roles and proper risk allocation. The desire to foster development of broadly based authentication systems (not restricted to one industry or sector) is clear. The commentary to Principle 1 states that authentication administrators must choose attributes for authentication so that "other participants may have credibility in the claimed attributes."[10] Similarly the Principle encourages Standards Developers to encourage uniformity in authentication implementation.

Principle 2 deals with risk assessment and management and is familiar ground for legal counsel who advises clients with respect to information technology systems. Authentication systems are by their nature complex. Risk assessment is compounded by the multiple parties who deal with various (relatively complex) responsibilities. As the commentary states, the functional roles identified under Principle 1 are useful to take into account of where risk lies. It suggests that risk be allocated to the most economically efficient result. This observation is theoretically sound, but any given system is likely to be the subject of negotiation between parties of various bargaining strengths rather than designed wholly with economic efficiency in mind. The commentary acknowledges this fact more clearly by discussing the need for weaker parties to be protected by industry codes or legislation in systems not freely negotiated.

Principle 3 recognizes that security will fall to the providers of authentication infrastructure and those who administer the system. The Principle correctly identifies the dynamic nature of security measures – both the threats and the development of technology to counter those threats. The Principle also refers to the need for balance between security and the need to respect the rights of participants in keeping with the principles of a democratic society.

Principle 4 relating to privacy does not add much to obligations already in place through Canadian legislation, whether through the federal Personal Information Protection and Electronic Documents Act ("PIPEDA") or similar provincial legislation. These legislative requirements must be built into any system. The useful insight here is that certain authentication systems may not require the collection of any personal information (and this is why authentication focuses on credentials, not identity). For example, transit passes can function by determining that the individual has the required money on a stored value device or valid pass. No information about the rider need necessarily be collected. The premise that the least amount of personal information possible should be collected provides a useful analytical starting point for designing systems that comply with privacy legislation.

Principle 5 requires disclosure to participants to promote awareness of risks and responsibilities. The principle is similar to rules regarding disclosure by investment funds to their investors, in that the goal is to allow for informed participation by end-users. The principle also aligns with the practice of placing terms of use on web sites and obligations found in legislation relating to collection and use of personal information.[11] The end-user should appreciate not only the features of the system but also the risk associated with use.

Principle 6 sets out requirements for complaint handling. Once again the similarity to legislation relating to privacy legislation is striking.[12] The stated aim to improve end-user confidence in authentication systems shines through most strongly here. Given that identity theft is one of the principal fears affecting e-commerce, the focus on confidence-building measures around perceived system problems is not surprising.

Conclusion

The Industry Canada Principles are far from establishing legislative criteria for authentication providers. Those who favour government setting out such criteria for certificate authorities for the economy generally will be disappointed. This was not the working group's goal, however. The Principles will not necessarily in and of themselves break down barriers between government, business, industry sectors or players within sectors relating to authentication systems. The clear intention has been to steer away from such overly ambitious goals in favour of a general framework under which players in various sectors can use common language to parse out their interests. This in itself is a useful dialogue that could contribute to maturation of electronic authentication within the economy. For lawyers formulating agreements the Principles provide broad guidance about general roles, responsibilities and risk allocation associated with authentication systems. ■

Simon H Hodgett practises law at Osler, Hoskin & Harcourt LLP, in Toronto, Canada in the Technology Business Group. His practice concentrates on corporate and commercial matters for software developers, hardware vendors, IT service providers and companies where business relies on technology, including many projects concerning payment systems in the financial services sector.

shodgett@osler.com
http://www.osler.com

[10] Principles, p 12.
[11] For example Principle 8 – Openness, Annex 1 to PIPEDA.
[12] For example Principle 10 – Challenging Compliance, Annex 1, PIPEDA.