



Authentication: Environmental Scan & Assessment of Market Trends

Presented to

Peter Ferguson
Jane Hamilton
Industry Canada

Presented by

Kristy Duncan
Duncan Consulting

March 31, 2006



duncan consulting

{ innovative banking strategies }

Table of Contents

Executive Summary	1
Introduction	3
Background & Objectives.....	3
Approach.....	4
Analysis	5
Current Use of Authentication in Industry	5
Trends and Future Use of Authentication in Industry.....	6
Challenges Around the Use of Authentication.....	8
Views on Types of Authentication	9
Existing Industry Guidelines	10
Standard Levels of Assurance.....	11
Privacy Requirements	12
Requirement for Strong Authentication	13
Cross Border e-Commerce.....	14
Recommendations & Next Steps	16
Conclusions	18

Appendices

- Appendix A- Discussion Outlines
- Appendix B- Discussion Summaries
- Appendix C- Glossary



duncan consulting

Industry Canada- Authentication Market Scan

Authentication: Environmental Scan & Assessment of Market Trends

Executive Summary

Electronic Commerce Branch of Industry Canada commissioned this environmental scan and assessment of market trends in the area of authentication for e-commerce applications in Canada. This research was conducted in the spring of 2006, to provide a qualitative analysis of stakeholder views of authentication, and identify trends in the Canadian market.

The following are highlights of the key findings and recommendations:

- The most common form of authentication in use in Canada today is single factor, using an ID and password¹. There are some pockets, most notably in financial services and government, which have moved, or plan to move, to two factor authentication solutions¹. To date, there has been little use of biometric authentication solutions in the market.
- A number of trends are emerging. One trend is toward use of two factor authentication in industry, although it is unclear what the leading form factors will be. Another trend is the movement from application level authentication to enterprise level. There is also evidence that there will be continued use of single-factor authentication for lower risk applications.
- The research identified a number of challenges around the use and implementation of authentication in e-commerce. First is the difficulty for organizations to identify an authentication solution which strikes an appropriate balance between the key components of cost, user-friendliness, and strength of security. In addition, organizations are reluctant to introduce anything to an e-commerce transaction, which has the potential to slow, divert, or otherwise negatively impact the customer experience, for fear of losing the business. Another challenge is the lack of infrastructure available to support some authentication solutions, such as chip card readers on PCs.
- On the question of whether standard levels of assurance are necessary, it was clear that certain industries are already moving to provide standard levels of assurance for common transactions (especially in financial services), and that

¹ See Appendix C for definitions.



general industry standards may not be necessary. Other respondents felt that standards would be useful in defining levels of assurance for authentication in e-commerce.

- There was a range of views on authentication held by the organizations we canvassed. Most agreed that single-factor authentication has been sufficient for e-commerce applications in the past. The representatives from financial services, vendors, and industry experts, expressed the view that strong (two-factor) authentication is required for e-commerce to grow in Canada, to provide an appropriate level of assurance of security. However, other players were of the view that single-factor authentication solutions have been effective for their applications in the past, and would continue to provide sufficient levels of assurance in the foreseeable future. All agreed that there needs to be a range of viable solutions available in the market, to meet the diverse needs of various e-commerce applications.
- Privacy issues were a key concern of most research respondents. Most respondents had taken tangible steps to ensure the privacy of their customers' data, including establishing and publishing policies which outline how they collect, use and manage or store the customer data required for their e-commerce transactions. Many organizations had adopted policies not to store any customer data, after the completion of the transaction, and most organizations also noted that they collect only the information which is absolutely required to complete a given e-commerce transaction.
- In order to address some of the issues which surfaced in this research, we recommend that Industry Canada consider the following:
 - promoting the use of authentication in e-commerce, by facilitating the development of industry-specific guidelines around the use of authentication for common applications where appropriate;
 - working with industry to develop an application risk assessment guideline and other authentication-specific educational materials for both consumers and the SME market;
 - representing Canadian industry on appropriate interoperability standards bodies;
 - monitoring the development of federations of authentication across multiple enterprises, and communicating those developments to Canadian market players; and
 - working with industries in Canada to identify and promote the implementation of appropriate authentication-enabling infrastructure.



duncan consulting

Industry Canada- Authentication Market Scan

{ page 2 }

Introduction

Duncan Consulting has performed an environmental scan and assessment of market trends in authentication in e-commerce on behalf of Industry Canada. The field research consisted of interviews with thirteen key industry participants, completed during the month of March, 2006.

Background & Objectives

Trust and confidence form a cornerstone of secure electronic commerce, without which e-commerce cannot expand and thrive in Canada. To help Canadians build this trust and confidence, Industry Canada convened the multi-stakeholder *Authentication Principles Working Group*, to develop Principles for Electronic Authentication, which it published in 2004. These Principles were designed to serve as benchmarks for the development, provision, and use of authentication services in Canada.

While some industries and players are quite familiar with authentication in e-commerce applications, others may not be as far down this new road. At this point, Industry Canada needs to take a pulse of the market, to determine the extent to which authentication is being used or contemplated, and to identify potential challenges faced by market players in implementing or using authentication in their e-commerce initiatives.

The objectives of the research were to answer the following questions, as they relate to B2B, B2C, and B2G authentication for applications in the e-commerce market:

- ✓ To what extent is e-commerce utilizing authentication solutions?
- ✓ What are current authentication trends in the market?
- ✓ What are the impediments to authentication of transactions?
- ✓ What views do market players have on different types of authentication?
- ✓ Should levels of assurance be standardized in some way?
- ✓ Do stakeholders perceive privacy as a concern, given that authentication requires personal information?
- ✓ Do stakeholders believe strong authentication is essential for e-commerce to thrive and grow? If so, how will that happen?

This research paper explores these issues, and provides some recommendations for Industry Canada to promote the use of strong authentication in Canadian e-commerce going forward.



duncan consulting

Industry Canada- Authentication Market Scan

{ page 3 }

Approach

The research was conducted via one-on-one discussions with senior management from a selection of e-commerce market participants. Representatives from key sectors were invited to provide input, including businesses, governments, authentication solution vendors, and industry experts. Discussions were held between March 1 and March 28, 2006.

Duncan Consulting began the project by developing four discussion guidelines (for businesses, governments, vendors, and industry experts) to guide the discussions with participants. The discussion outlines addressed the key questions which Industry Canada wished to learn from this research, and were approved by Industry Canada before commencing the discussions. They can be found in Appendix A of this report.

Duncan Consulting contacted a number of organizations from each of the four key sectors, inviting them to provide input to the research. Within the business sector, four enterprises came from the broad financial services sector, with the remainder coming from manufacturing and professional services. Two governments, three vendors, and one industry expert also provided input.

Organizations were provided with an electronic copy of the appropriate discussion outline, to allow them to familiarize themselves with the questions, and ensure the appropriate management personnel were present for the discussions.

In total, fourteen discussions were held (two with the Government of BC). The participants included the following:

Organization Type	Organization Name and Interviewee
Vendor	Entrust
Vendor	Proginet Canada
Vendor	MicroSoft Canada
Government	Province of Alberta
Government	Province of British Columbia
Business	Credit Union Central of BC
Business	Medicus
Business	Moneris Solutions
Business	ShawCor
Business	Sierra Wireless
Business	Toronto-Dominion Bank
Business	Visa Canada Association
Industry Expert	Advanced Card Technologies (ACT) Canada

The discussions are summarized in Appendix B.



duncan consulting

Industry Canada- Authentication Market Scan

{ page 4 }

Analysis

In general, we believe that the market has recognized the need for authentication, to assist in building trust and security for e-commerce transactions. Many existing e-commerce applications have incorporated single factor authentication solutions². Other e-commerce applications are contemplating upgrading to stronger authentication solutions, such as two-factor.

We observed that the financial services and government sectors are leaders in the use of strong authentication² for e-commerce today, as both sectors have already implemented two-factor authentication solutions for a number of e-commerce applications.

In the health care and government sectors, we identified at least one application requiring strong authentication for online applications. The Province of Alberta has introduced a token-based authentication solution for health care providers (doctors, labs, and hospitals) to access and update electronic health records of citizens.

From our discussions with market players, we understand that a range of authentication solutions will be required to meet the needs of the various e-commerce applications in the market. The range will likely include a range of strengths of authentication solution, as well as complexity and cost.

The following analysis addresses each of Industry Canada's key questions, which were stated at the outset of the project.

Current Use of Authentication in Industry

In the current market, we observed a mixture of authentication solutions being used for online e-commerce applications. The most common solution is single factor authentication², consisting of ID and password. This is very common in the retail banking sector, for customers who access their banking services online.

Another authentication solution in use today is the shared secret, which some still view as a single-factor solution (something the participant *knows*). We observed it being used for an application at the Government of Alberta, where citizens can renew their vehicle licenses online, using a pre-mailed shared secret as the password.

In financial services, two-factor authentication is being used for a number of B2B applications. For example, our research confirmed that, to authenticate business customers wishing to effect high value corporate payments (typically wire

² See glossary in Appendix C for definitions.



payments), at least one financial institution (FI) is currently using a token-based solution, and another FI is using fingerprints (a form of biometric authentication). On the B2C side, a number of banks are considering (or may have already) strengthening their single-factor authentication solutions, by adding additional security questions for retail customers logging on to their online banking applications. Alternatively, other FIs are considering authenticating customers by confirming both the user ID and password, as well as confirming the IP address of the computer the customer is using.

We observed some small pockets of two-factor authentication, especially in the financial services and government sectors. For example, the Government of Alberta uses a form of biometric authentication, having digitized the photograph from citizens' drivers licenses, and embedded it in a barcode on the back of the license. This can be used by police, who can scan the barcode and re-create the image to confirm that it matches the photo on the front of the document. As mentioned earlier, at least some FIs are using two-factor authentication for high value B2B payment transactions.

Trends and Future Use of Authentication in Industry

We identified a number of trends, and planned use of authentication in the industry. The first trend is that some applications are moving to strengthen existing single-factor authentication solutions. Examples of this can be seen in financial services, where some FIs are either introducing additional questions in addition to a logon ID and password, or confirming the users' IP address (as well as the logon ID and password), as part of the process to authenticate retail online banking customers. Other strengthened single-factor solutions being implemented include the CVV³ for credit card purchases, as well as Verified by Visa (VbV) and MCSecure (MasterCard Secure), solutions which require the user to enter a PIN in addition to the credit card number for online purchases.

A second trend is the move to true two-factor authentication. This is evidenced especially in financial services and government applications. For example, a token plus a PIN are required for Esso's new SpeedPass with debit, to effect debit card transactions at Esso kiosks. Chip cards with PINs are being implemented across Canada for use in debit and credit card transactions; this implementation is already under way, and is expected to be complete within six years or so, although it is as yet unclear how the chip card will be utilized in an online environment. The Province of Alberta is already using tokens for health record access. And a last

³ Cardholder Verification Value- a static number which is printed on the back of a credit card, and can be used to confirm that the customer is in possession of the card.



example is that at least one FI will require two-factor authentication for B2B banking applications at the user logon level within one year.

A third trend is the continued use of single-factor authentication. Based on our research, we believe that over the medium term (three to five years), at least some e-commerce applications will continue to use single factor authentication. These will tend to be applications of an informational nature, such as browsing an online catalogue.

We also note that, with the exception of one FI using fingerprints to authenticate customers for high value payment transactions, there do not appear to be very many existing or planned two-factor authentication solutions, which utilize biometrics as the second factor.

The fourth trend we identified is that organizations are beginning to move to enterprise-wide authentication solutions, thereby eliminating silos across different business units of an organization. This concept of single sign-on is especially noteworthy in both financial services and governments. BC OnLine is a prime example of a single sign-on process to authenticate businesses accessing numerous applications within the BC government. FIs demonstrate this concept also, offering clients the ability to access online banking, brokerage, and other services with a single sign-on. We observe that there may be increased risks inherent in this approach, as an incorrect or failed authentication would allow access to many more applications (this is discussed in more detail in the next section).

The last trend we identified, that of federations of authentication, is now only in the very early stages. Some industry players believe it will be the next phase of development to occur after enterprise-wide authentication. This trend will see enterprises adopting interoperability between themselves, forming federations of e-businesses. Some FIs, and at least one vendor interviewed for this research, noted that interoperability standards are evolving in the market. The evolving standards are both industry-specific (such as EMV for chip cards, and VbV, MCSecure in financial services), as well as cross-industry, such as Liberty Alliance⁴, and WS-I⁵. At this early stage, it is still unclear which of the cross-industry standards for authentication will be adopted by the market, and we did not identify any evidence of these federations in the market in Canada at this time.

⁴ The Liberty Alliance was created in 2001 to address the technical, business, and policy challenges around identity and identity-based Web services. More information can be found at <http://www.projectliberty.org/>

⁵ WS-I is an open industry organization chartered to promote web services interoperability across platforms, operating systems, and programming languages. More information can be found at <http://www.ws-i.org/>



duncan consulting

Industry Canada- Authentication Market Scan

{ page 7 }

Challenges Around the Use of Authentication

The most common challenge identified by organizations centred around balancing three key components of an authentication solution: cost effectiveness, strength of authentication solution, and user-friendliness. Organizations utilizing e-commerce applications must balance these three requirements when selecting their authentication solution. The organizations we spoke to found that increasing the strength of one requirement is often at the expense of another. For example, increasing the strength of the authentication technology solution generally is done at the expense of user-friendliness, and often at the expense of cost-effectiveness. Conversely, increasing the user-friendliness (or simplicity) of the solution is often at the expense of the strength of the authentication. In addition, a number of organizations indicated that they are reluctant to implement authentication solutions which interrupt, lengthen, or complicate, a customer transaction process. They fear that by doing so, customers may be dissatisfied, which could lead to lost sales, or worse, lost customers.

A second challenge faced by organizations when implementing authentication solutions, is the potential difficulty that they may have in conducting an application risk assessment (ARA), prior to selecting an authentication solution which appropriately addresses the risks and needs of the application⁶. An example was given of an application which allows access to health records, being compared to FIs offering consumers access to their financial records. Such a comparison could lead to a conclusion that logon ID and password provide an appropriate level of authentication for the health records application, when in fact, the risk of compromising the confidentiality of health records would suggest that a stronger authentication solution than simply logon ID and password should be required. We believe that industry may benefit from a high level ARA guide, which could suggest authentication solutions or levels which can appropriately mitigate the risks of e-commerce applications bearing certain risk levels.

A third issue which was identified, was that some organizations may not have access to the necessary infrastructure to effect a strong authentication solution. For example, since chip card readers are not generally installed on most PCs today, use of a chip card to authenticate a customer wishing to use a credit card for an online purchase is not a viable solution in today's market. The same lack of infrastructure can apply to mobile payments, since most cell phones in Canada today do not have chip card reading capabilities. Some industries are actively

⁶ Note that an enterprise-wide authentication solution may provide a base level of authentication, and each individual application utilizing that enterprise-wide solution must decide, via the ARA, whether supplementary authentication may be required.



building the infrastructure required to enable stronger authentication solutions, such as chip-enabling merchants in a bricks and mortar environment. However, other strong authentication solutions may require new infrastructure which is not currently on the horizon, such as chip-reading capabilities on PCs.

We believe a last challenge to be addressed is that of the increased risks associated with an enterprise-wide authentication solution being utilized for multiple applications. For example, with enterprise-wide authentication allowing customers access to multiple applications, the risks correspondingly increase in the event of compromise or failure of the authentication. This can be seen in the online retail banking environment today, where a single sign-on gives a customer access to multiple applications, including funds transfers, viewing images of cheques, brokerage transactions, bill payments, etc. Should the authentication for the single sign-on fail to correctly authenticate the customer, the customer faces the risk of multiple applications being compromised. This risk should be taken into account when performing the application risk assessment noted earlier.

Views on Types of Authentication

Generally, discussion participants agreed that single factor authentication has been sufficient for most e-commerce applications in the past. During our discussions, single factor authentication was described by one person as 'extremely weak', and by another as 'ineffective'. It was also described as 'sufficient for our needs' by some others. These comments reveal that there is a wide range of views of single-factor authentication in the market, and there is likely no 'one size fits all' solution. This is evidenced by the market moves by some players to upgrade to true two-factor authentication, while others are moving to stronger forms of single-factor authentication (adding questions to a logon process), and still others are satisfied with single-factor solutions for the short to medium term.

Most discussion participants agreed that dual-factor solutions will become the preferred authentication method for e-commerce applications over the medium term. However, as form factor solutions are still evolving in the industry, there was no consensus on what the preferred form factor might be. Among the form factors in the market, the following were mentioned in the discussions, and could be implemented either alone, or in combinations:

- Token- a device which generates a dynamic password
- Chip cards- cards containing a microchip with a highly secure memory and processing capabilities
- Bingo card- a grid-like challenge-based authentication mechanism⁷

⁷ The bingo card could also be described as a simple, but dynamic form of a CVV, and may be printed on the back of a debit or credit card .



- Bio authentication methods- including fingerprint, retina/iris scan
- Challenge/Response Units- units which create dynamic PINs based on user input and other data

The common view among research participants was the ongoing difficulty of balancing objectives of user-friendliness, cost-effectiveness, and strength of authentication solution. A few people suggested that this challenge may become easier over time, as authentication solutions become more affordable and simpler for users to understand.

It should also be noted that biometric solutions, although they can be extremely reliable, also carry with them very high data protection requirements. This is to ensure that organizations manage and safeguard the user biometrics with sufficient care to ensure that they will not be compromised. The risk to the user, in the event of compromise of a biometric, is much greater than with other form factors, as it is not possible to change one's biometric attributes, compared to changing a user's password or re-issuing a token.

Existing Industry Guidelines

Research participants mentioned the following industry guidelines, legislation, or other industry policies and regulations, which have implications to their use of authentication in the Canadian market:

- PIPEDA (Personal Information Protection and Electronic Documents Act)
- FOiPPA (Freedom of Information and Protection of Privacy Act- in BC and Alberta)
- Provincial Health Care information privacy legislation, where applicable
- In the financial services industry, some of the following may apply, depending on the particular business:
 - VbV⁸/MC Secure (Association requirements)
 - Payment Card Industry (PCI)- Data Security Standard⁹ (Association requirements)
 - Canadian Code of Practice for Debit Card¹⁰ (a voluntary code of best practice, defined by industry participants)
 - Interac Online Rules (Association requirements)
 - Credit Card Association Rules (Association requirements)
 - Canadian Payments Association Rule E2¹¹ (Association requirements)

⁸ Details can be found at <http://www.visa.ca/verified/factsheet.pdf>

⁹ Can be found at:

http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf

¹⁰ Found at: http://www.fcac-acfc.gc.ca/eng/compliance/DebitCardCode/DebitCardCode_e.asp

¹¹ Can be found at: http://www.cdnpay.ca/rules/pdfs_rules/rule_e2.pdf



duncan consulting

Industry Canada- Authentication Market Scan

{ page 10 }

As most of these requirements are either legislative requirements, or association requirements, the organizations we spoke to in our research were mandated to comply with the requirements, and were making every effort to do so. In addition, a number of research participants noted that the following legislation in other markets (particularly the US) is establishing new industry norms, which many players view to be evolving as best practises in the Canadian market. In some cases, some divisions of the organizations we spoke to operated in these other jurisdictions, and were therefore subject to the new legislation. In other cases, the organizations in our study indicated that they viewed the new requirements in other jurisdictions to be the leading edge of where the industry is going, and that, in time, Canadian laws or guidelines would move in the same direction. The laws or guidelines mentioned include the following from the US:

- Sarbanes Oxley
- HIPAA (Health Insurance Portability and Accountability Act)
- FFIEC Guidelines (Federal Financial Institutions Examination Council)

Due to the potential implications of these and other legislative guidelines to the players in the Canadian market, it may be helpful for Industry Canada to monitor the legislative direction in other markets, and communicate the direction of those markets to the players in Canada. This would provide Canadian market players advance warning of evolving requirements in other markets, before they become defacto standards in Canada.

We note that the Verified by Visa and credit card association rules are set by industry bodies, which operate on a global basis, with a Canadian membership. In this regard, credit card transactions must comply with global standards, especially cross-border credit card transactions.

Standard Levels of Assurance

The input we received for this research confirms that certain industries are already moving to provide standard levels of assurance for certain types of transactions. A prime example of this is the credit card industry, which, through the use of VbV and MC Secure, is moving to upgrade to a single-factor authentication solution for online consumer purchases. Visa Canada indicated that it expects the industry will move to further upgrade to a two-factor authentication solution over the medium to long term. It would seem entirely appropriate, both from a consistency of customer experience perspective, as well as to provide a standard level of assurance, that a common transaction, such as authenticating a customer for an online debit or credit card transaction, be standardized.

Other standard levels of assurance are evolving in other global markets; for example, NIST (the National Institute for Standards & Technology) has defined standard levels of authentication in terms of the consequences of the authentication



duncan consulting

Industry Canada- Authentication Market Scan

{ page 11 }

errors and misuse of credentials in its Special Publication 800-63¹². The standard provides technical guidance for implementing electronic authentication, covering remote authentication of users over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registrations, tokens, authentication protocols, and related assertions.

The question of whether standard levels of assurance are needed was met with mixed responses. Generally, the research participants were divided between those with less experience in e-commerce, who felt that standard levels of assurance would be helpful; while those with more experience in e-commerce were comfortable making their own decisions, or collaborating to produce industry-level standards for levels of assurance.

One research participant suggested that standard levels of assurance be established at the industry level. The industry standard levels of assurance could be similar to the standards outlined by NIST, but tailored to the specific needs of particular industries. This might be accomplished via the use of industry work groups, possibly co-ordinated by Industry Canada.

Privacy Requirements

All of the organizations we spoke to during the course of this research were very aware and concerned about privacy requirements for all their dealings with consumers. With both PIPEDA at the federal level, and FoIPPA and other Acts at the provincial level, organizations are highly aware and motivated to ensure that personal information is properly managed to assure privacy.

There were a number of approaches used to safeguard the privacy of private information. Most organizations we spoke to indicated they had established and published policies which outline how they collect, use and manage or store the customer data required for their e-commerce transactions. Many organizations had adopted policies not to store any customer data, after the completion of the transaction. Most organizations also noted that they collect only the information which is absolutely required to complete a given e-commerce transaction.

The financial services industry appears to be a leader in developing industry standards for the management of customers' personal information. For example, the credit card industry has collaborated to formulate the Payment Card Industry (PCI) Account Information Security data management standards, which must be followed by all parties who collect, manage, store, or process customer credit card or other personal data. Another example is that the design of payment related

¹² Outlined in http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf



authentication solutions (such as InteracOnline, VbV, and MCSecure) is such that the customer's private data is not disclosed to the merchant.

Another question which was posed during the course of our research discussions, was that of how to define private data. One FI we spoke to indicated that it had decided not to require its customers to answer pre-set authenticating questions, on the grounds that the questions could be construed as being too personal. The solution they settled on was to have the customers set and answer their own identifying questions.

The industry expert believes that consumers are willing to give up some private data, in exchange for a higher level of security. An example of this is the customer authentication process which is done when customers phone a telephone support line. Organizations must ask customers a number of identifying questions, and customers must provide a certain amount of personal data, in order to authenticate themselves. However, consumers are willing to do this, in order to ensure that their private data is not erroneously divulged to the wrong party.

A last note is that the question of privacy requirements is more applicable to e-commerce transactions involving consumers, than it is to B2B transactions, and the authentication solutions for B2B applications tend to reflect this. For example, two-factor B2B authentication solutions generally involve the use of tokens or other devices, thus eliminating the need for personal questions.

Requirement for Strong Authentication

There were two things that all research participants agreed upon. First was that they do not want any e-commerce authentication solution to cause them to lose business- either by interrupting or complicating the transaction flow, or by raising the consumer 'FUD Factor' (defined as Fear, Uncertainty, Dread). Second was that there needs to be a range of viable authentication solutions for organizations to choose from, in order to meet the needs of their particular applications, and provide appropriate levels of security, cost-effectiveness, and user-friendliness.

Most research participants agreed that strong (two factor) is required in the medium to long term, for e-commerce to thrive and grow. In most cases, organizations are committed to securing e-commerce transactions in order to protect private data, maintain customer trust, and provide transaction security. This was especially true of the FIs, the vendors, and the industry expert.

However, there were two organizations which felt that single factor authentication would meet their needs for the foreseeable future. First was the BC OnLine single sign-on application at the Province of BC, which currently has e-commerce in place with over 50,000 business users, processing over 6.9 million e-transactions



duncan consulting

Industry Canada- Authentication Market Scan

{ page 13 }

annually. The other exception was the research participants in the manufacturing sector, who conduct limited e-commerce transactions, and felt that logon ID and password were sufficient for their needs. These organizations felt that they had mitigated their risks in some additional manner (i.e. either the business party was already known to them, or the consumer transacting with them was doing only small dollar transactions). In both cases, it appears that organizations were aware of the risks and unable to justify stronger authentication solutions.

The question of whether electronic signatures are a key component of strong authentication drew mostly negative responses. Most people responding, who were knowledgeable on e-commerce security issues, indicated that true two-factor authentication (requiring the user to have something he/she *knows*, as well as something he/she physically *has*) can provide ample security in today's e-commerce market. The electronic signature (PKI) solution was viewed as being too complex for customers, costly to implement and maintain, and not sufficiently portable for widespread use in the market (people need to be able to access e-commerce applications from multiple locations, not just a single PC). Other authentication solutions, such as tokens, or bingo cards, provide a solution which our research participants felt were much easier for consumers to understand, as well as providing a much needed higher degree of portability.

Entrust and the Province of Alberta stood out in the research as being the only players who believe that PKI should be component of a strong authentication solution. The Province of Alberta suggested, however, that PKI could be part of the authentication solution which is not customer-facing, thereby remaining simple and easy to implement and understand at the customer end, while providing a strong authentication solution. In addition to PKI at the back end of the application, the Province of Alberta also felt that an authentication solution should require a low-cost second factor, such as a token or bingo card.

Cross Border e-Commerce

The implications of authentication in cross-border e-commerce were addressed throughout the discussions. Most respondents indicated that most, if not all of their e-commerce transactions are carried out entirely within Canadian borders. In the manufacturing sector, some of the B2B or B2C e-commerce is done with non-Canadian parties; however, these transactions are conducted in the same manner as their domestic transactions.

In financial services, some players indicated that they do have influences from beyond Canada. For example, the card services industry, being by its very nature global in scope, is guided by operating rules and guidelines which are set by the global card associations (such as Visa International, MasterCard International, EMV,



duncan consulting

Industry Canada- Authentication Market Scan

{ page 14 }

etc). Thus the FIs who belong to these associations are bound by those global association rules. The Canadian card industry has adopted the global EMV standards for its implementation of chip cards in Canada; however, in the absence of chip card readers on most PCs, it is unclear how, or if, chip cards will be utilized for online card transactions.

Another point noted by financial services respondents was that the new FFIEC guidelines in the US have, or potentially could impact the authentication solutions offered to clients for online banking. The FIs take the view that the FFIEC guidelines will certainly affect the US operations of the Canadian FIs, so they may as well make their Canadian operations compliant where possible, so as to avoid going through the process twice.

Finally, it must be noted that any customer data which crosses over to the US at any point during processing of the transaction, immediately becomes subject to the PATRIOT Act in the US, at which point the responsible party can no longer guarantee that the privacy of the customer information can be safeguarded. This concern has been raised recently with credit card transaction processing, where a number of the major processors now operate in the US.



duncan consulting

Industry Canada- Authentication Market Scan

{ page 15 }

Recommendations & Next Steps

Based on the input received from the field, Duncan Consulting presents the following action items which may assist Industry Canada to promote the development and use of strong authentication in e-commerce in Canada. These initiatives are centred around providing market education, standards development, and assisting to establish industry best practises and required infrastructure.

1. Industry Guidelines-The NIST Standard 800-63 defines four standard levels of assurance for authentication of e-commerce transactions. This standard could be used for all industries to benchmark against. In addition, it may be useful for industry work groups to develop industry-specific guidelines, which are more tailored to common applications in key industries. For example, in the US financial services market, the FFIEC guidelines have motivated the industry to provide enhanced levels of assurance for their e-banking clients. Similar industry-specific guidelines may be appropriate for some industries in Canada. We believe that some industries would be open to forming industry groups, possibly facilitated by Industry Canada, to collaboratively establish and define guidelines for common industry-specific e-commerce applications.
2. Education & Industry Best Practice-
 - a. Industry Best Practice- Risk Assessment- In order ensure consistent levels of consumer protection in e-commerce applications in Canada, it would be useful for industry to have a high level application risk assessment (ARA) guide, specifically to assist in defining requirements for an e-commerce authentication solution. Such a guide would walk the enterprise through a full risk assessment exercise for an application, to yield an application risk assessment, which focuses on the consequences of authentication errors and misuse of credentials. The guide might go as far as suggesting authentication solutions and/or standard levels of assurance (possibly NIST-based, or industry-based), which can appropriately mitigate the risks of e-commerce applications with certain attributes and/or risk levels. This work could draw on existing ARAs in industry or government, where available.
 - b. Education- As a companion to the ARA guideline above, we suggest that two educational pieces may help to promote understanding and use of authentication in e-commerce in Canada. The first would target enterprises in the SME market, and provide information on why authentication is important in e-commerce, outline different solutions, form factors, advantages and disadvantages of each, appropriate applications of each, etc. This piece would target organizations which are new to e-commerce, and could form a companion piece to both the *Principles for Electronic Authentication*, as well as the ARA mentioned



duncan consulting

Industry Canada- Authentication Market Scan

{ page 16 }

above. A second piece would target the consumer market, and address the consumer 'FUD Factor' (fear, uncertainty, and dread). It could potentially be delivered in partnership with the FCAC, the Retail Council, the Canadian Bankers Associations, and/or other leading consumer e-commerce services agencies.

- c. Guidance to Assist in Authentication Solution Selection- The research identified a number of challenges faced by organizations in selecting an authentication solution, which is appropriate to their needs. Industry Canada may be able to provide guidance and education to market players in assisting them in this important step toward providing an environment which supports secure e-commerce.
 - d. Monitor E-Commerce Authentication Requirements in Other Markets- Legislative guidelines in other global markets, especially the US, can impact players in the Canadian market. It may be helpful for Industry Canada to monitor the legislative direction in other markets, and communicate the direction of those markets to the players in Canada. This would provide Canadian market players advance warning of evolving e-commerce authentication requirements in other markets, before they become defacto standards in Canada.
3. Interoperability Standards Development- In order to ensure that Canada has input to e-commerce standards evolving in other markets, which may have implications to e-commerce standards in Canada, it may be beneficial for Industry Canada participate as an observer in development of interoperability standards, and/or other e-commerce standards on behalf of Canadian industry. Industry Canada may wish to seek input from Canadian industries, to ensure that its voice on these standards bodies reflects the desired direction of Canadian industry. It could also make available the developments of these standards bodies, for interested Canadian enterprises to access.
 4. Federations- It would be useful for Industry Canada to monitor the development of federations of enterprises as they begin form over the short to medium term. This information can be communicated to market players in Canada, to keep them abreast of market developments in which they may wish to play a part.
 5. Infrastructure- In order to facilitate two-factor authentication in the market, appropriate enabling infrastructure needs to be available. It may be useful for Industry Canada to work with key industry groups to identify enabling infrastructure, such as chip card readers on PCs, cell phones, etc, so that Industry Canada can in turn work with appropriate enabling bodies to promote the availability of that infrastructure in the market.



duncan consulting

Industry Canada- Authentication Market Scan

{ page 17 }

Conclusions

The research confirms that financial services and governments are the leading industry sectors in Canada when it comes to the understanding and use of authentication in e-commerce applications. Industry Canada has taken a leadership role in educating and promoting the use of authentication to secure the use of e-commerce in Canada. With the findings and recommendations of this study, we hope that Industry Canada will continue to help Canadian industries advance their competitiveness through the use of secure e-commerce.



duncan consulting

Industry Canada- Authentication Market Scan

{ page 18 }

Discussion Outlines

Authentication Research for Industry Canada Environmental Scan, Market Trends, and Cross-Border Applications

Background & Objectives

Trust and confidence form a cornerstone of secure electronic commerce, without which e-commerce cannot expand and thrive in Canada. To help Canadians build this trust and confidence, Industry Canada convened the multi-stakeholder *Authentication Principles Working Group*, to develop *Principles for Electronic Authentication*¹³, which it published in 2004. These Principles were designed to serve as benchmarks for the development, provision, and use of authentication services in Canada.

Industry Canada has commissioned Duncan Consulting to conduct this research, in order to:

- Determine the extent to which authentication is being used or contemplated in the context of domestic and cross-border communications and transactions;
- Identify and understand the type of applications, for which authentication is being used in the B2B, B2C, and B2G markets; and to
- Identify potential or actual barriers preventing market players from implementing or using authentication in their domestic and cross-border e-commerce initiatives.

Industry Canada has taken a leadership role in other domestic and international initiatives to promote e-commerce and authentication. Of particular interest to this study is the framework of common principles for electronic commerce that has been developed with the United States and Mexico under the *Security and Prosperity Partnership of North America*¹⁴. These principles acknowledge the key role authentication has to play in strengthening the Internet as a medium for electronic commerce.

We would like to arrange an interview or conference call with a representative of your organization between March 13 and March 24, 2006. We expect this discussion to take approximately 1 ½ to 2 hours. The following page provides an outline of the information we would like to learn from this research.

Your input will be valuable in assisting the E-Commerce Branch of Industry Canada to build trust and confidence in the online environment in Canada, and better recognize the key role authentication plays in building trust in that environment. We appreciate your participation.

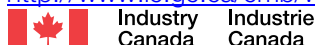
Further comments or questions may be directed to:

Kristy Duncan
Duncan Consulting
416-487-5691
kristy@duncanconsulting.com

Jane Hamilton
Manager, Strategic Security Initiatives
E-Commerce Branch, Industry Canada
613-991-0049
hamilton.jane@ic.gc.ca

¹³ These can be found at http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_qv00240e.html

¹⁴ Further information can be found at <http://www.ic.gc.ca/cmb/welcomeic.nsf/ICPages/SpecialReports>



Discussion Outline- Business Users

- a) Industry Role- Please describe the role and activities of your organization in the e-commerce market, and outline how authentication plays a part in that role.
- b) Authentication Use- To what extent does your firm utilize, or plan to utilize, authentication, or strong authentication for:
 - domestic e-commerce applications?
 - cross-border e-commerce applications?
 - Please describe these applications, and note whether they are B2B, B2C or B2G.
- c) Authentication Trends- Can you identify and describe current trends in the use of authentication in the domestic e-commerce market in your industry?
 - B2B
 - B2C
 - B2G
 - Do these trends apply equally to cross-border e-commerce transactions and communications in your industry?
- d) Barriers- Do you see any real or perceived impediments to authentication of domestic or cross-border transactions and communications in your business and/or industry?
- e) Types of Authentication- How does your firm view different types of authentication?
 - Single Factor
 - Two Factor
 - Other
- f) Industry Guidelines- Are there any legislative requirements, policies, regulations, standards, industry best practises, etc., issued by government or industry, that you are subject to, or have implications to:
 - Your firm's use of authentication in the domestic market?
 - Your firm's use of authentication in the cross-border market?
 - How do/will you use these policy instruments and/or practise guidelines, and in what context in your business?
- g) Standard Levels of Assurance- Does your firm believe that levels of assurance should be standardized in some way? If so, how would you see that happening?
- h) Privacy Requirements- How have you taken privacy considerations into account in the authentication component of your e-commerce products or services? How do your clients or trading partners perceive privacy, given that authentication typically requires collection of personal information (at least at some point in the process)?
- i) Strong Authentication- Do you believe strong authentication is essential for e-commerce to thrive and grow? Do you view electronic (digital) signatures as a key component of strong authentication? If so, how do you see that happening?

Discussion Outline- Government Users

- a) Industry Role- Please describe the role and activities of your organization in the e-commerce market, and outline how authentication plays a part in that role.
- b) Authentication Use- To what extent does your government (department) utilize, or plan to utilize, authentication, or strong authentication for:
 - i. domestic e-commerce applications?
 - ii. cross-border e-commerce applications?
 - iii. Please describe these applications, and note whether they are B2G or C2G.
- c) Authentication Trends- Can you identify and describe current trends in the use of authentication in the domestic e-commerce market in your government (department)?
 - i. B2G
 - ii. C2G
 - iii. Do these trends apply equally to cross-border e-commerce transactions and communications?
- d) Barriers- Do you see any real or perceived impediments to authentication of domestic or cross-border transactions and communications in your government (department) or others?
- e) Types of Authentication- How do you view different types of authentication?
 - i. Single Factor
 - ii. Two Factor
 - iii. Other
- f) Industry Guidelines- Are there any legislative requirements, policies, regulations, standards, industry best practises, etc., issued by government or industry, that you are subject to, or have implications to:
 - i. Your use of authentication in the domestic market?
 - ii. Your use of authentication in the cross-border market?
 - iii. How do/will you use these policy instruments and/or practice guidelines, and in what context in your business?
- g) Standard Levels of Assurance- Do you believe that levels of assurance should be standardized in some way? If so, how would you see that happening?
- h) Privacy Requirements- How have you taken privacy requirements into account in the authentication component of your e-commerce products or services? How do your clients or trading partners perceive privacy, given that authentication typically requires the collection of personal information (at least at some point in the process)?
- i) Strong Authentication- Do you believe strong authentication is essential for e-commerce to thrive and grow? Do you view electronic (digital) signatures as a key component of strong authentication? If so, how do you see that happening?

Discussion Outline- Industry Experts

- a) Industry Role- Please describe the role and activities of your organization in the e-commerce market, and outline how authentication plays a part in that role.
- b) Authentication use in Industry- To what extent do you see domestic e-commerce utilizing authentication solutions?
 - i. Do you see a more focused use of strong authentication in any particular industries? If so, are these B2B, B2C or B2G applications?
 - ii. Are you aware of the use of strong authentication for any cross-border applications? If so, are these B2B, B2C or B2G applications?
- c) Authentication Trends- Can you identify and describe current authentication trends in the domestic e-commerce market?
 - i. B2B
 - ii. B2C
 - iii. B2G
 - iv. Do these trends apply equally to cross-border e-commerce transactions and communications?
- d) Barriers- Do you see any real or perceived impediments to authentication of domestic or cross-border transactions and communications?
- e) Types of Authentication- How do you view different types of authentication?
 - i. Single Factor
 - ii. Two Factor
 - iii. Other
- f) Industry Guidelines- Are there any legislative requirements, policies, regulations, standards, industry best practises, etc., issued by government or industry, that have implications to the use of authentication in the domestic or cross-border e-commerce market?
- g) Standard Levels of Assurance- Do you believe that levels of assurance should be standardized in some way? If so, how would you see that happening?
- h) Privacy Requirements- How do you believe the market perceives privacy considerations, given that authentication typically requires personal information (at least at some point in the process)?
- i) Strong Authentication- Do you believe strong authentication is essential for e-commerce to thrive and grow? Do you view electronic (digital) signatures as a key component of strong authentication? If so, how do you see that happening?

Discussion Outline- Vendors

- a) Industry Role- Please describe the role and activities of your organization in the e-commerce market, and outline how authentication plays a part in that role.
- b) Authentication use in Industry- To what extent do you see domestic e-commerce utilizing authentication solutions?
 - i. Do you see a more focused use of strong authentication in any particular industries? If so, are these B2B, B2C or B2G applications?
 - ii. Are you aware of the use of strong authentication for any cross-border applications? If so, are these B2B, B2C or B2G applications?
- c) Authentication Trends- Can you identify and describe current authentication trends in the domestic e-commerce market?
 - i. B2B
 - ii. B2C
 - iii. B2G
 - iv. Do these trends apply equally to cross-border e-commerce transactions and communications?
- d) Barriers- Do you see any real or perceived impediments to authentication of domestic or cross-border transactions and communications?
- e) Types of Authentication- How do you view different types of authentication?
 - i. Single Factor
 - ii. Two Factor
 - iii. Other
- f) Industry Guidelines- Are there any legislative requirements, policies, regulations, standards, industry best practises, etc., issued by government or industry, that you are subject to, or that have implications to:
 - g) The use of authentication in the domestic or cross-border market?
 - h) Your products or service offerings as applicable?
 - i) How do/will you use these policy instruments and/or practice guidelines, and in what context in your business?
- j) Standard Levels of Assurance- Does your firm believe that levels of assurance should be standardized in some way? If so, how would you see that happening?
- k) Privacy Requirements- Have you taken privacy considerations into account in your authentication products or services? How do your clients perceive privacy, given that authentication typically requires the collection of personal information (at least at some point in the process).
- l) Strong Authentication- Do you believe strong authentication is essential for e-commerce to thrive and grow? Do you view electronic (digital) signatures as a key component of strong authentication? If so, how do you see that happening?

Glossary

AUTHENTICATION- A process that attests to the attributes of participants in an electronic communication, or to the integrity of the communication.

ATTRIBUTES- Information concerning the identity, privileges, or rights of a participant or other authenticated entity.

DUAL FACTOR AUTHENTICATION (also referred to as TWO FACTOR AUTHENTICATION)- An authentication processes which depends on two independent mechanisms for authentication; for example, an authentication which requires the participant to provide something he or she *has*, and something he or she *knows*. As an example, two factors could be a smart card and a password. Another factor which could be authenticated would be something the participant *is*, such as a biometric attribute (such as a voice print, retina scan, or fingerprint).

INTEGRITY- Assurance that the information in an electronic communication has not been modified or corrupted during the process of communication.

PARTICIPANT- An individual or organization participating in an authentication process, whether directly or through another authenticated entity, such as a data service or object, hardware device, or software program.

SINGLE FACTOR AUTHENTICATION- An authentication processes which depends only on a single factor being authenticated about the participant; for example, an authentication which requires the participant to provide something he or she *has* (such as a token or card), or something he or she *knows* (such as a password or shared secret).

STRONG AUTHENTICATION- An authentication process which confirms more than a static single attribute (such as a static password). It may utilize a dynamic password scheme for the participant to authenticate him/herself, or a combination of more than a single factor, such as something the participant *has*, *knows*, or *is*.



duncan consulting

Industry Canada- Authentication Market Scan

{ glossary }