Response to IDA on Proposed Framework on Building Trust and Confidence in Electronic Commerce

31 October 2000

Adopting a Secure Public Key Infrastructure

(i) In your view, do you think PKI is essential for secure transactions? If no, please explain your reasons and state your alternative solutions.

No. PKI is only one of the means available for delivering secure transactions. Most business relationships today are either one-to-one, or one-to-many, which transaction risks could be managed by a closed-loop system, not necessarily using PKI. The bank's ATM network is a classic example of such a business relationship, and it uses a symmetric key system to achieve its transaction security and user authenticity needs. As for non-repudiation, it relies on legally binding agreements signed between the service provider (bank) and the users, with the Monetary Authority giving assurance to the users that the bank will enforce a set of security best practices within its premises to protect the customers' information and transactions. Technologically, PKI provides a means to enforce non-repudiation more readily, but not necessarily fool-proof. It still requires a legal infrastructure in place, including the customer requirements and regulatory control policies to ensure the liability involved are adequately managed. Compare with a symmetric key based system, the basic business structure hasn't changed. However, the technological infrastructure is much more involved and complex. Its application therefore needs to be in line with the business needs, and users requirements.

If a PKI system were already in place, and using it is only a matter of "plugging-in", it would then make sense to use PKI for all secure transactions needs. Otherwise, it could be a costly to build an infrastructure just to support a specific or limited set of applications. However, putting a plug-able PKI in place is a formidable task, involving investment out-front, and substantial operating and maintenance (including security technology updates) in an ongoing basis. There might not be a good business case to do it if it does not provide the convenient and usability that end users will sort after, while delivering the security that businesses and regulators desired. Achieving these targets are not simple today as end-user technologies are moving much faster and converging much quicker than security technology can deliver. Today, PKI solutions can be delivered in desktop and notebook PC, and server systems easily. However, they are still not ready for PDA and mobile phones. Nevertheless, businesses and users are keener on doing commerce on these platforms than on PC, given the mobility and prospective market penetration. This catching-up trend between security and technology has been ongoing since technology started, and will continue as technology progresses.

(ii) Have you considered implementing a PKI setup for your online business? If yes, what are your considerations in deciding on PKI? If no, what are the factors/obstacles?

No. We do not run an online business at the moment. Our experience on PKI however shows that implementing it for online business today may not be appropriate, as it will bring about much inconvenient to the users, from registration, usage, to revocation. One of the reasons

for the low take-up of the SET™ approach for e-commerce credit card payment is due to the need to distribute electronic wallet to cardholders, need for cardholder to register for their certificates with the electronic wallet, and need for cardholder to use the same electronic wallet wherever she shops. Besides the administrative overheads to the user, this has indirectly locked the user to only those systems where she had her electronic wallet installed. In spite of the security that SET brought about, its inconveniences have put most consumers off. The use of PKI for business-to-business transactions is however something that may be more doable, given the natural "lock-in" of business users to specific desktop, and the possible enforcement of mandatory use of the digital certificate and electronic wallets for online transactions, through the use of company or industry policies, something that is not so doable to consumers at large.

(iii) In your view, what are the key impediments to PKI adoption? Can you provide the reason and nature of these impediments? How could we overcome them?

Lack of applications, inconveniences to the end-users, administrative overheads, usually high initial investment and ongoing operating cost, unknowns and caveats to watch out, and unnoticeable benefits (until something bad happened) are some of the impediments.

Reason – mainly due to the complex structure and components that a complete PKI must support, including non-technical infrastructure components such as Certification Policy, and Certificate Practice Statement.

We might not be able to overcome these impediments easily, as many are residual to the infrastructure requirements. Instead, we should look at limiting the scope of applications of PKI to only those that involve high risks and high values. So far, we have seen that there have been successful PKI stories, when they are focused for closed-loop applications or single-purpose services.

(iv) What are the key potential sectors and projects for PKI adoption? Are there any impediments to these? If so, what are these impediments and how should they be addressed? What roles should the Government play in PKI adoption and promotion?

An industry-specific PKI application should be the focus. One area that would be a useful application is in the healthcare industry, for facilitating the sharing and integrity/confidentiality control of medical records, validation of doctors' signature on prescriptions and remarks on patients' conditions, between private and public clinics, pharmacies, and hospitals. A closed-loop PKI focusing on delivering the security infrastructure specific to the applications and users requirements in this area will reap much benefit. This must not be mixed with other applications such as financial, or insurance, as they will require a different set of security policy and certification policy.

The Government may play the role of the PKI infrastructure provider, and policy enforcer to facilitate the linking up of the various entities involved in the healthcare services.

By focusing on a single industry needs, much experience can be gained and issues identified and resolved without the need to consider how the solution will impact other industry applications and business/legal policies. With the industry focus approach, it will also be easier for one country's PKI to interoperate with another country's PKI for the same industry, as there will be more common requirements, and less legal or local regulatory issues to

resolve. Interoperating the industry-specific PKI with other industry-specific PKI would then be the next step.

(v) Do you think that a Trust Association for Certification Authorities (TACA) will help promote the adoption of PKI in Singapore? If yes, what else can be the charter of TACA? If no, please explain why and suggest alternative measures.

No. It is not the lack of CA or CA-to-CA cooperation that result in poor adoption of PKI. Our view is that it is a lack of PKI-enabled application. There are already a few CA in place in Singapore and around the region. The number of applications for these CA certificates is small and they are mostly insignificant to consumers, i.e., consumers can use other alternatives rather than the inconvenient or expensive PKI based solution.

An association to identify, sponsor development, and promote use of PKI-based applications will be more useful.

Risk Assessment and Profiling

(i) Do you agree that risk assessment and profiling will help to lower e-business risk associated with the acceptance of online credit cards? If yes, are you using/intending to use such services and how does it help you address your e-business risks? If no, please provide reasons why and suggest alternative or other complimentary solutions.

No. Profiling is based on past experiences, historical information. Once a card is compromised and fraudulently used, and the cardholder did not know the compromise, good profile will make it acceptable to the merchant. If the transaction involved is large and accepted (due to the good profile), it will make the fraud worthwhile, and eliminate the savings that the merchant might have over the implementation of appropriate security controls. The blacklist system is already managing the risk of bad cards today. The limit placed on each card is already managing the risk of overspending. The profile therefore does not add much value to the business. It will however introduce privacy concerns to individuals.

The 3D-SET approach as defined by MasterCard, which will provide guaranteed transactions, is a better approach, as it focuses on managing the security risks involved in online credit card transactions, leaving the credit risks as BAU between cardholders, merchants, and banks.

(ii) How could the Government introduce risk assessment and profiling to the industry, especially the SMEs?

Through education/awareness courses, and case studies example. Risk assessment, focusing on whether a company should accept a certain payment instrument (e.g. credit card) over the Internet, for the type of business that it is doing, will be more useful. Profiling, as commented above, is of less use to day-to-day transactions, but more for statistical reporting and analysis to aid the risk assessment process.

(iii) E-Commerce Advisory Council on Trust

Not sure if this is useful. Not clear about its charter and objectives.

Introducing EC Insurance and Underwriters

(i) Are you already/intending to insure your online business? If yes, please indicate how such EC policies are meeting your needs. If no, please explain the reasons why.

No online business as yet. Availability of such a policy on EC insurance will be useful, but it should be catered to individual online business needs, and should enforce best practices for risk management and security management.

(ii) What roles can and should Government play in helping e-merchants towards insuring their online businesses?

Provide a framework on what should be insured, what can be insured, and how the premiums may be calculated. Provide advisory services on whether a proposed policy and premiums is reasonable. Ensure fair competition and prevent profiteering from e-merchant ignorance.

(iii) What are the suitable parties to offer such EC insurance policies?

A combination of insurance expertise and security expertise to have a fair view of the risks involved in terms of the online business and the technology infrastructure and security architecture.

Escrow Services

(i) What are your views on escrow services? Do you think they can help address the issue on trust and confidence in EC?

This is a role that banks have been playing traditionally in the trade services business. It is definitely a value add to trust and confidence in EC. However, the issue is, when everybody is online, how do each party trust the Escrow electronically? Also, will such a service increase the cost of services and transactions, and reduces performances and the "immediacy" experience in online transactions?

(ii) What are the parties that should provide escrow services in Singapore?

Banks are a natural choice. In fact, they are already doing it to a certain extend, for some debit card types of payment services (not necessarily in Singapore.)

(iii) Apart from escrow services, can you suggest alternative ways, by which such trust and assurances in payments can be addressed?

No comment.

Introducing Credit Bureau Services

(i) Are you currently using or intending to use such credit bureau services? If no, please provide reasons why and suggest alternative solutions.

No. Our business currently do not need such a service.

(ii) What do you think are the possible impediments or considerations in engaging the services of a commercial credit bureau?

Interoperability of e-business and credit bureaus across the globe will be the biggest challenge. This includes both security and data format. An global association with the technology infrastructure to support such an initiative worldwide is needed.

(iii) What are your views about the set up of a credit bureau in Singapore? What do you think should be the role(s) of the Government in this credit bureau?

It would be a good first step to start, but we can't do it alone. We need the support of other countries in order for it to be useful in the e-world.

The Government can help by defining frameworks, technical and operation guidelines, interoperability standards, and promulgate policies to ensure the integrity and trustworthiness of such an agency and the information they collected and supplied. There should also be regulations to ensure integrity and prevent misuse of the data collected by the bureau.

Alternative Dispute Resolution Mechanisms

(i) Do you think the industry should play a role here?

No. This is more of a process rather than a compliance or practice that industry can adopt directly. Use of such a mechanism is also very much a matter of awareness of its benefits and potential successes over other means of resolution.

(ii) What other alternative dispute resolution mechanisms should be put in place in Singapore?

A common standard on e-transactions evidence collection and archive will be important/useful to facilitate e-arbitration processes, and allow disputes to be handled more efficiently.

Trust Marks

(i) What is your view on accrediting e-merchants through the use of trust marks? Do you think this will help instill consumer confidence in EC transactions? If no, please explain why and suggest alternative solutions?

Although a Trust Mark may provide the necessary recognition that a site has followed best practices, maintaining the validity of the marking may be an issue. Furthermore, who will be qualified to validate the practice and issue the mark? What are the costs to the merchant year-to-year? Will these cost be passed on to the consumers? How do the trust mark issuer ensure that all trust marks on the web are valid trust marks? Can a merchant put on a trust mark even though the site has not been certified? How will the consumer validate this?

What if a site that has a trust mark get compromised? Will the mark continue to be valid?

Will the trust mark provide a false sense of security, given that technology is always changing and security vulnerabilities get discovered frequently, and maintenance of site security is not a one-time affair?

Alternative is to ensure that the site uses security technology that delivers the security requirements of the applications, from which provide assurance to the consumers/customers

of the site security. For merchant sites that did not practice good security or use appropriate security technology, when there is a compromise or dispute, they should stand to loose unless proven otherwise. The security inadequacies and lack of commitment to customer data confidentiality and transaction integrity should not be tolerated. There should be law/regulation to penalize security negligence for online merchants in order to encourage good practices.

(ii) What are some initiatives that the Government and the industry can develop to help instill greater consumer confidence in order to spur demand for online transactions?

Publish minimum requirements for security practices for online businesses to serve as guidance. Mandate needs for independent security assessment for sites that processes or handles value bearing transactions of certain values or risks.

Privacy

(i) In your view, do you think our businesses are doing enough to protect consumer privacy? If not, is this impeding the adoption of business-to-consumer e-commerce?

No. There is a lack of privacy protection in general. Businesses that collect personal data are allowed to sell them to others without control. This is a concern to consumers online, in particular, those consumers outside of Singapore who are used to personal data protection enforced in their country. Our online merchants targeting at selling to consumers in countries that have such data protection act in place will lose out if the products or services concerned involved collection of personal data.

(ii) What are the key privacy principles that businesses should adhere to in order to safeguard consumer privacy? Should compliance with these rules be on a voluntary or mandatory basis, and why?

Basic principles that should be promulgated include but not restricted to: (1) collecting only those data that are needed; (2) using the data only for its agreed/intended purposes; (3) not re-selling or giving away the data to third party without the owner's consensus; and (4) allow data owner to verify and correct its integrity and accuracy.

Mandatory is preferred as it will provide better assurances to consumers in other countries.

(iii) In your view, what framework can be developed to foster the development of effective privacy protection while still allowing e-commerce to thrive?

Enforcement of privacy protection should not slow down e-commerce. It will give more confidence to the consumers when shopping online, and that alone should encourage more merchants to go online.

(iv) What roles should the Government and industry play in the implementation of a privacy regime in Singapore?

Promote its usefulness to individuals and to the economy. Provide guidance, and training to ensure that its implementation is smooth and effective.

Increase Awareness

(i) Can you suggest how the above programs can be further expanded?

Can't think of any right now.

(ii) What are other programs that can be adopted to further raise the level of EC adoption among users and businesses?

Provide tax incentives for business to go online, and for users to use online services for purchase of goods and services (lower GST charges?)

Kang Meng Chow
Chairman, Security Standards Technical Committee, ITSC
CTO, PrivyLink International Ltd