A PROPOSED FRAMEWORK ON BUILDING TRUST AND CONFIDENCE IN ELECTRONIC COMMERCE

A Consultation Paper
26 September 2000

INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE (IDA)

A PROPOSED FRAMEWORK ON BUILDING TRUST AND CONFIDENCE IN ELECTRONIC COMMERCE

1. INTRODUCTION

1.1. On 1 Aug 2000, the Government announced the plan to Dotcom the Private Sector (please refer to Annex A), to position Singapore as an Electronic Commerce (EC) hub. EC has the potential to revolutionise the way business is done and improve the competitiveness of the Singapore industry. Indeed, globalisation and technological changes have brought new opportunities for businesses to enter international markets and to reduce business costs, as well as increase in transition costs, new competitive challenges and risks.

1.2. A Gartner survey reveals that 12 times more fraud exists on Internet transactions while WebAssured found that fear of fraud is the number one reason users decide against making online purchases. Electronic transactions provide the possibility of network fraud on a large scale. Hence, while the technology is available, consumers and businesses lack the trust and confidence in the network to conduct online transactions, and to optimise the vast opportunities offered by EC.

1.3. The Infocomm Development Authority of Singapore (IDA), together in consultation with other government agencies, issues this Consultation Paper to seek views from the industry and interested members of the public, on the strategies and initiatives that the Government can put in place to help build trust and confidence so as to facilitate EC growth. The list of strategies and initiatives identified below covers the Government’s current thinking, which are still works in progress. In developing this framework, the Government is seeking public comment and feedback in these or additional ideas.

2. THE NEED FOR TRUST AND CONFIDENCE

2.1. In order for E-commerce to take off even faster, it is essential that businesses and users have trust and confidence in EC and are prepared to embrace it. The key considerations/concerns are:

(i) Businesses – the need to distinguish between legitimate shoppers and fraudulent users in real time, adequacy of security, online fraud, high processing fees associated with online transactions and unauthorised access to network and data; and

(ii) Users – little confidence in e-merchants due to invisibility of store, low level of trust in impersonal transactions, making advance payment before delivery, privacy and fraudulent use of their information/details.

2.2. People are more likely to use EC if they trust it. Trust is thus viewed as the intermediary element that will determine if businesses and users are willing to embrace the online economy. In order to build an environment of trust and confidence so that EC will flourish, the Government have identified four key strategic thrusts:

(i) Establishing a secure EC environment;
(ii) Building confidence in E-businesses;
(iii) Building confidence in consumers to transact on the Internet; and
(iv) Educating and increasing awareness of the benefits of EC.

3. ESTABLISHING A SECURE E-COMMERCE ENVIRONMENT

3.1. People need to be confident of the identity of the person sending electronic messages, to be sure that they have not been tampered with, and that they have been kept confidential. Conversely, senders would also want to be able to identify the recipients of the messages, to ensure that they will not land on the hands of the unauthorised. Thus, establishing a secure EC infrastructure/environment in which online transactions can take place is the first and basic step to win confidence and trust amongst business and users in the global network.

Initiative: Adopting a Secure Public Key Infrastructure

3.2. The Internet is an open network and there are various risk elements faced by both business users and consumers. To address these risks and instil a higher level of trust in doing online transactions, the Government will identify as well as promote the adoption of the Public Key Infrastructure (PKI) to provide the highest level of security on the Internet. PKI is the combination of software, encryption technologies, and services that enable enterprises to protect the security of their communications and online business transactions. PKI integrates digital certificates, public-key cryptography, and certification authorities into a secure network and encompasses the issuance of digital certificates to individual users and servers. It is by far the most ready solution that addresses all four key elements of security: authentication, non-repudiation, confidentiality and integrity.

3.3. However, there are several obstacles faced by the industry and users in adopting PKI, including a lack of demand from users, lack of applications supporting PKI, system complexity, difficulty of use (requires software and/or hardware installation), and costs. The Government will identify major potential communities for the adoption of PKI based on those with large volume of transactions and the level of security needed. At the same time, we are also actively participating in international fora to promote cross-certification efforts with other countries. As a platform for the Government and the industry to work jointly to address these issues as well as promote the adoption of PKI, we are currently considering the establishment of a Trust Association for Certification Authorities (TACA), with the aim to help drive the adoption of PKI as well as to help address issues such as interoperability, ease of usage, liability, etc. The TACA will also be expanded to include certification authorities in other economies like Australia, Hong Kong SAR, Korea, Malaysia and Taiwan so as to achieve international interoperability and mutual recognition.

Questions:

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

(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?*

(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?*

(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?*

(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.*

Initiative: Risk Assessment and Profiling

3.4. Risk is unavoidable, but conducting businesses on the Internet is perceived to carry far greater risks. Thus, some banks impose higher transactional fees for online payments in order to cover the risks of irrecoverable payout to illegitimate online merchants or online credit card fraud. In addition, some banks may require a six-month fixed deposit from the e-merchants to cover possible charge backs arising from online transactions. It is noted that online credit card transaction rates may also vary according to the worthiness of the e-merchant, bank-client relationship and transaction volume.

3.5. Risk assessment and profiling is an effective means to help lower Internet risk-related cost. Currently, there are specialist companies that offer online risk assessment service, designed to minimise the risk associated with the acceptance of online credit cards. Based on the prior risk threshold established by the e-merchants, they can choose to reject a specific transaction if it is suspected to be fraudulent. Such risk assessment and profiling will provide a practical and cost-effective process for controlling risk. Depending on the risk threshold established for each online transaction, there can be different levels of security requirement. These tools can be built into the basic infrastructure so that the e-merchants can enjoy these services at the onset.

Questions:

(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 complementary solutions.*

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

(iii) *The Government is currently evaluating the set up of an E-Commerce Advisory Council on Trust[1], with the aim to spearhead the development of trust in online businesses and to help both businesses and consumers understand and lower online risks. Do you think such a Council is useful? If yes, what other areas should be addressed by the Council? If no, please explain why and suggest other alternative mechanisms/measures.*

4. BUILDING CONFIDENCE IN E-BUSINESSES

4.1. EC brings about new markets, more customers and global reach. However, businessmen are hesitant to exploit this potential opportunity which can be accompanied with an increased risk of network fault, online fraud and crime as well as capital investment that might become outdated through rapid technological obsolescence.

Initiative: Introducing EC Insurance and Underwriters

4.2. Due to the unique features of the Internet, e-businesses require more specialised insurance needs than the standard retail store. Some insurers and underwriters are offering new insurance products to help soften the financial impact of losses arising out of EC and Internet-related activities. Some of these insurance policies accept primary risk, while others wrap around existing property, business income, liability and crime. They may also require an inspection of all firewall, security, backup and contingency systems instituted by the e-businesses.

4.3. However, the EC risk management marketplace is still at its infant stage, and there are no defined industry leaders; policy pricing can be excessive. As the majority of our online merchants are relatively small and online business is still in the nascent stage; they may not be able to afford the perceived hefty premiums if undertaken individually.

[1] Proposed Council members will include representatives from various credit card associations, online retailers, retail promotion centres, banks, ISPs, research agencies and relevant government agencies.

Questions:

(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.*

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

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

Initiative: Escrow Services

4.4. When a credit card fraud occurs, the e-merchant will lose his goods, be charged for the costs and have to pay the issuing bank a charge-back fee. On the other hand, online consumers face the risk that they may not receive the goods, the goods that arrived are not what they had ordered or the goods are damaged upon receipt.

4.5. The solution to this is through an escrow provider, an impartial third party that acts to facilitate online buying and selling by providing both parties with trust, security and convenience. When an online purchase is being made, the buyer places the money in the custody of the escrow provider, which will in turn disburse the money to the seller only after the buyer acknowledges receipt and satisfaction of the goods when he receives it. Through the escrow provider, the buyer is assured that payment is not made until he receives his orders, while the seller is assured of payment from the escrow provider so long that he makes his delivery. Apart from assuring payment, escrow providers also act as independent mediators whenever dispute arises between its customers.

Questions:

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

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

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

Initiative: Introducing Credit Bureau Services

4.6. Due to the faceless nature of transacting on the Internet, the transacting parties on both sides of the Internet do not know each other and have no information on the credit worthiness of the other party. A credit bureau is essentially a central repository of credit data on businesses and consumers, containing information necessary to evaluate credit worthiness. From the database, the bureau puts together a credit report, which assesses whether the merchants, companies or consumers are reliable in meeting their obligations and payments. Such credit reports enable lenders, banks and businesses to distinguish good customers from bad customers.

Questions:

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

(ii) *What do you think are the possible impediments or considerations in engaging the services of a commercial credit bureau? (For example, cost of service subscription, information integrity, etc.).*

(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?*

Initiative: Alternative Dispute Resolution Mechanisms

4.7. As EC takes off and online transactions increases, there will be potential e-disputes that arises, thus the need for an alternative dispute resolution process to allow businesses and customers to have access to an independent and efficient way of resolving complaints. In this light, the Subordinate Courts have recently launched an initiative - e@dr, which offers dispute resolutions through the Internet. The Singapore Mediation Centre has started to develop a comprehensive framework for mediation, neutral evaluation and other hybrid consensual alternative dispute resolution processes to take place within cyberspace. The Singapore International Arbitration Centre is also gearing itself for the possibility of conducting e-arbitration.

Questions:

(i) *The Government is currently driving the alternative dispute resolution mechanisms. Do you think the industry should play a role here? If yes, what would be the role of the industry and suggest how this could done? If no, please explain the reasons.*

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

5. BUILDING USER CONFIDENCE IN EC TRANSACTIONS

5.1. For consumers to transact on the Internet, they must have trust that the site keeps information private and offers a secure site for them to purchase products. Consumers fear the risk of financial losses due to theft or fraudulent use of credit cards, or orders that disappear and products that never arrive. With thousands of e-merchants, how do you find the ones you can trust?

Initiative: Trust Marks

5.2. Building consumer trust and gaining consumer confidence are primary aspects to spur consumer demand and drive Business-to-Consumer (B2C) EC businesses to succeed. The Government will be driving programmes to educate businesses to adopt ethical best practices. The Government is considering plans to provide recognition for sites that conducts secure procurement and transactions.

Questions:

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

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

Initiative: Privacy

5.3. The ease with which personal information can be disseminated with the proliferation of infocomm technology has raised privacy concerns worldwide. Governments have responded in diverse ways, with measures spanning from the enactment of comprehensive privacy legislation to reliance primarily on industry self-regulation. In Singapore, the National Internet Advisory Committee (NIAC) drew up an E-commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce in 1998. This Code has been adopted by CaseTrust and incorporated into its Code of Practice as part of an accreditation scheme promoting good business practices among store-based and web-based retailers. The government is now exploring the adoption of a general privacy regime based on international best practice.

Questions:

(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?*

(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?*

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

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

6. EDUCATING AND INCREASING AWARENESS OF THE BENEFITS OF E-COMMERCE

6.1. The Government has put in place a number of programs to help educate and increase awareness of EC for the businesses and consumers. These include programs that encourage the fostering of an e-lifestyle amongst the people, e.g., e-Ambassadors, e-Festival, e-Celebrations, One Learning Place etc. The Government, in conjunction with industry chambers and associations, also creates EC awareness through seminars targeting at SMEs. To promote e-business thought leadership, the Government, together with industry associations and vendors, has launched the Singapore@Work television program, which portrays local companies that adopted EC successfully. Skills redevelopment programs are also in place to help train workforce in EC skills.

Questions:

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

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

7. INVITATION OF COMMENTS

7.1. In summary, the Government would like to seek the views and comments of the industry and interested members of the public on the strategies, issues and questions raised in the Consultation Paper. Respondents are also invited to add comment/feedback on any other initiatives that they consider of relevance to this objective of building trust and confidence in EC.

7.2. All views and comments should be **submitted in writing and in either hard or soft copy**, and should reach the following addressee on or before **20 Oct 2000.** Respondents are required to include their personal/company particulars as well as the correspondence contact (telephone, email, postal address) in their submissions.

7.3. Written comments and views should be addressed to:

Serene Ho (Ms)
Assistant Director, EC Infrastructure
Online Development
Infocomm Development Authority of Singapore
8 Temasek Boulevard, #14-00, Suntec Tower 3
Singapore 038988.

7.4. Electronic submissions may be sent as documents attached to e-mail messages and should be sent to: Serene_HO@ida.gov.sg.

7.5. The Government reserves the right to make public all or parts of any written submissions made in response to the Consultation Paper and to disclose the identity of the source. Any part of the submission that is considered commercially confidential should be clearly marked and placed as an annex to the comments and views raised. The Government will take this into account when disclosing the information submitted.