Electronic Transactions Policy Review and Regulations

Objective

This Questionnaire has been prepared in connection with the regional activities carried out under the HIPCAR project "*Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures*" and with the Saint Kitts-Nevis Electronic Transactions Bill 2011, and related National Policies.

The HIPCAR project has prepared Model Legislative Texts and Model Policy Guidelines for the Caribbean during stage 1, the project focused on:

1. Information Society Issues concerning E-Commerce (Transactions); E-Commerce (Evidence); Privacy and Data Protection; Interception of Communications; Cyber crimes / E-Crimes; and Access to Public Information (Freedom of Information) as well as on

2. Telecommunications matters such as Universal Access / Service; Interconnection and Access; and Licensing. In its current Stage 2, HIPCAR is offering in-country assistance upon request of the beneficiary countries to transpose these models into national policies and legislation.

The Government of St. Kitts and Nevis (GoSKN) has officially requested the project's support in this connection, in the following work areas:

(a) Interception of Communications; ; e-Evidence; Cybercrime; e-Transactions; Privacy & Data Protection and Access to Public Information (Freedom of Information)

The current assignment deals with one of these areas: **e-Transactions.**

This Questionnaire purports to raise questions which may help the stakeholders and the team of consultants in obtaining a more complete understanding of the issues and interests to be considered in the identification of policy and other substantive issues that should inform the drafting of theRegulatory Framework to accompany the Electronic Transactions legislative regime.

Questionnaire

Name:

Position/Title:

1. Are you a user of computers, smart phones, and data networks (Internet and/or Intranet)?
   ☐ Yes ☐ No

2. What mechanism do you use as evidence that your electronic communications were indeed sent by you?
   ☐ Write name in e-mail or SMS
   ☐ Use biometrical means[2]
   ☐ Other, please specify:
   ☐ Use electronic signature[1]
   ☐ None

3. (a) In your opinion, which of the practices below should be used to verify the signature of the Sender?
   ☐ (i) written name in an e-mail; comment (if any):

   ☐ (ii) use of any form of electronic signature; comment (if any):

   ☐ (iii) use of certified[3] electronic signature; comment (if any):

   (b) Should all these methods be acceptable regardless of the type of transaction?
   ☐ Yes ☐ No

[1] **Electronic signature** is an electronic means of codifying a data message so that it identifies the sender and makesit very difficult for persons other than the addressee to be able to read or change the data message; it is thusconsidered as a reliable means of providing safety, secrecy, and integrity to electronic communications.

[2] **Biometrical means are biological (and electronic)** means of identification of a person; for instance, fingerprints, iris, retina, are unique to each person, so the use of them as parameters to identify persons who has been considered a safe way to instruct computer programs aimed at such identification.

[3] **Certified (or "authenticated") electronic signature** is an electronic signature assigned to a person in accordance with strict procedures that ensure greater certainty on the identity of that person (who usually must appear before an E-notary or before a registered electronic authentication service provider to evidence his identity before being granted the electronic signature).

(c) For highly sensitive or valuable transactions which method would you accept ranking the most acceptable first and the least acceptable last?

☐ (iii) (ii) and (i)
☐ (ii) (iii) and (i)
☐ (i) (ii) and (iii)

(d) In your view what are the critical elements required to ensure that any electronic record, document and information are in fact authentic and the integrity of the information contained in such electronic record, document or information had been maintained?

4. Please state your position on the following: Consumers who buy via Websites should be given the "right to repent" (that is, the right to cancel purchases within a specified time after the purchase was electronically confirmed)?

(a) Yes, in all cases
(b) Yes in certain circumstances but not in all cases
(c) No, never.

If you selected (b) please indicate the kind of cases you think should merit the 'right to repent':

5. Who should offer mobile payment services[4]:
☐ (a) Banks;
☐ (b) Telecommunications companies
☐ (c) Government
☐ (a) only;
☐ (a) and (b) only

[4] Mobile payments are payments made via electronic mobile equipment such as cellular phones and smart phones; in some countries, the high popularity of mobile equipment may be a way to spread the use of electronic payments, which may be faster, cheaper, and more reliable; there is a debate on whether the financial authorities should be able to keep track of those payments, as it happens with Internet banking, for example; other countries, where there is a significant percentage of people and businesses in the informal economy (not even possessing bank account), it may be a strategy of social digital inclusion to have the telecommunications regulatory agency as the single regulator (at least, in a first phase).

6. Do you agree that electronic **"time-stamping"**[5] should be legally required in respect of:[please list situations]
   ☐From Internet Services Providers (access, hosting, contents);

   ☐From any services (ex.: on-line banking) or goods (ex.: e-commerce) provider via Internet;

7. The identification of individuals for purposes of assigning certified electronic signatures to them should be performed by

(a) E-notaries only	☐Agree	☐Disagree
(b) duly registered public notaries	☐Agree	☐Disagree
(c) banks	☐Agree	☐Disagree
(d) public bodies[6]	☐Agree	☐Disagree
(e) certification service providers	☐Agree	☐Disagree

8. In light of the critical role to be played by Electronic Authentication Service Providers, what should be the essential requirements that are to be met by such Service Providers in order to be registered to provide such services:

9. What should be the criteria for recognition of electronic signatures emanating out of the jurisdiction[7]?
   ☐Multilateral or bilateral international treaties between concerned countries;

[5] A digital time stamp gives you proof that the contents of your work existed at a point-in-time and that the contents have not changed since that time. The procedures maintain complete privacy of your documents them. The result is *simple*, *secure*, *independent* and *portable* proof of electronic record integrity.

[6] Banks and other merchants or services providers are usually closer to persons and legal entities in their day-today affairs, and already maintain a relationship with them where the identification of such persons or legal entities has been already accomplished. Therefore, in some countries, the task of identifying persons and legal entities before assigning some electronic code ("key") as their certified digital signature is somewhat "delegated" to them, to make easier the process of identification, and ultimately, the dissemination of certified digital signatures.

[7] The process of recognition of electronic signatures issued abroad may be dependent on the prior existence of an international treaty with the country where the digital signature was originated, which may be a cumbersome process. It may, however, be based on acceding to an international convention to which many countries have already joined, so there would be chance to provide recognition of digital signatures from various countries, all at once. It may be advantageous, though, not to depend solely on prior existence of international treaties, and rather accredit an international organization to verify whether the system adopted in the country of origin of the digital signature is as reliable as the one of the country which wishes to analyse such equivalence.

☐ Accredited international organization attesting equivalence of criteria and/or infrastructure between both countries;
☐ Other (please, specify):

10. Regarding e-mail marketing (promotional and advertising information sent via e-mail), what kind of entities should be accredited for producing co-regulation (Codes of Conduct, Services standards) on good practices in order to complement more generic provisions contemplated in statutory law?[8]

11. Regarding information security, what kind of entities should be accredited for producing co-regulation (Codes of Conduct, Services standards) on good practices in order to complement more generic provisions contemplated in statutory law?[9]

12. Is there any kind of document that should not be legally admissible in electronic form (besides negotiable instruments, wills, transfer of real estate, and immigration documents)? If positive, which one(s) can you think of?

[8] In some countries, the form of regulation is adopted to frame e-mail marketing so that it reconciles the interests of commercial entities and the rights of consumers has been of self-regulation, in which different commercial entities set up an association which becomes responsible for issuing rules inspired by market good practices. In other countries, it is the State which establishes such rules (for instance, on what is or not admissible as "spamming", and what shall be the penalties in the event of failure to comply with).

[9] Some countries have treated information security (technical and/or procedural standards to protect against theft of data, invasion of web sites, etc.) as purely "soft law" (non-binding standards). Other countries have converted those standards into legal rules, by incorporating them, by reference, into statutory law. There are also countries where standards organizations take part in multiple-constituency forums. ITU and ISO are examples of entities dedicated to producing and stimulating the consideration of standards. In the country national sphere, the entity in charge of creating or translating standards may have different kinds of mission and be subordinated to different kinds of administrative structures.

13. Which specific kinds of documents should be regulated in order to become admissible also in electronic form (examples: "single window" for cross-border trade), instead of just falling under general rules of acceptance of electronic documents?[10]

14. Is there any Internet-based activity (Access providers/Hosting providers/Contents providers?) Whose performance should be subject to prior official authorization? If yes, from which public body?[11]

15. What procedures should be followed by Internet Services Providers when they receive notification of some unlawful activity perpetrated by users of their services?[12]

16. Should there be a code of conduct or standard appointed for internet service providers and telecommunications service providers with regard to information transmitted electronically using such media?
☐ Yes ☐ No

[10] Customs processes are a point of convergence of many documents and relevant required approvals (for instance, for clearing export or import of products subject to health inspection). In order to expedite Customs clearance (making country import/export operations more competitive), it may be of interest to establish or adopt some kind of single pattern (like a template) for screens where the processes are controlled, merging or replacing applications from different stakeholders.

[11] Some countries have understood that the Internet is an open communications platform which may be used associal communication media for some businesses which offer services to the public. Therefore, in those countries where social communications vehicles are regulated, services offerings by Internet Service Providers (ISPs) may be regulated, so to impose some obligations on them (enrolment data, access data, traffic data record keeping, and others). Some other countries, however, have understood that Internet is a world platform, designed for free exchange of data, and do not intend to require prior approval or to control the activities of ISPs. There is a third group of countries which try to control the activities of ISPs for political reasons, including censorship of contents.

[12] ISPs may be routinely faced with a large amount of denouncements of wrongdoings perpetrated with the aid of their services. As they have no judicial adjudication powers and no Police investigation powers, resources and skills, they use to hesitate on how to address those denounces. In some countries, ISPs use to follow a procedure where they ask information from the accused user, before accepting the complaint by a third party and eventually suspending the services to the former. This is an intermediary approach, neither intending to replace Courts andPolice, nor refusing to cooperate in some reasonable manner.

If so what critical elements should be included in such code or conduct and standards?

17. What kind and extent of coverage, of insurance (if any) E-notaries, Internet Service Providers, and on-line merchants shall purchase to the benefit of their users?[13]

18. Should the Federation of Saint-Kitts-Nevis give consideration to acceding to regional and/or international conventions on e-commerce and on e-signatures, beyond having its own statutory laws on these matters?
☐ Yes ☐ No[14]

19. What kinds of on-line financial services shall be conditioned upon prior authorization from the Central Bank, and upon submission to its rules and controls?[15]

[13] The number of threats posed by the Internet as a platform for conducting business, communications, and so on, is quite impressive: web sites invasion, viruses, frauds, people defamation, and several others. Therefore, insurance companies have started to offer insurance coverage addressing those, specifically. Internet services providers and their users are better protected where insurance was bought by the former for protection of the latter. In some countries, the engagement in some activity which may have expressive social impact, such as the offering of certified digital signatures is only allowed in case specific insurance is previously acquired.

[14] Regional treaties or conventions may imply the possibility of a better bargain with international services providers (for instance, world-wide accepted certified digital signature providers). And international treaties or conventions provide a greater reach to the mutual safety an corresponding obligations that acceding countries agree to abide by Given that E-commerce is increasingly global, some level of compromise of country national autonomy for establishing its own rules may be necessary in order to participate and benefit from supra-national binding rules.

[15] E-cash, E-banking, E-trading, E-payments, are modalities of financial activities performed in electronic environments. In some countries, some of these modalities of activities are controlled by the Central Bank, which requires that they be performed by banks or by other financial institutions submitted to its rules. On the other hand, in some countries there is alternative, or multiple, regulatory mission, going from regulation of e-trading andE-broking by local Securities Exchange Commission, to m-payment or t-commerce regulated by thetelecommunications regulatory agency.

20. What kind of taxes (if any), or allocation of existing tax revenues, should be considered for enforcement in the on-line environment?[16]

21. What kind of control (if any) social networks shall be submitted to (example: should they be considered as social communications media?)?[17]

[16] In most countries (if not in all), not" bit tax" (a tax levied upon the volume of data traffic circulated through a data network) has been imposed so far. Several debates exist, for instance on which tax (telecommunications tax? communications tax? informatics services tax? no tax?) should be applicable to Internet access providing. In some countries, there have been inter-State agreement on sharing tax revenues arising from E-commerce, being a portion of which due the State where the web site is located (obs.: there are debates also on this topic, and some studies by the OECD in this regard, especially with regard to the concept of permanent digital establishment), and the other portion is due the State where the buyer resides.

[17] Similarly to what has been questioned above with reference to requiring, or not, prior official approval for performance of Internet services provision, there is currently some concern with the possible lack of control regarding social networks such as Facebook, Twitter, My Space or others. The name social networks indicates their purpose, which is to attract a large number of individuals and legal entities to exchange data as if they have set their own communities in the on-line world. Some countries have imposed some controls on those social networks (for instance, adoption of monitoring and reporting mechanisms by those social networks, regarding child pornography). It is also known that social networks have targeted by terrorism as a platform to disguise communications, or to attract adepts, so there is a trend to build a balance between preserving the free formation on-line communities, from one side, and keeping some kind of indirect control to track undesired standards of conduct.

22. What kind of policy should be adopted regarding domestic grant and control of domain names?[18]

Thank you for completing the Questionnaire.

[18] The grant of Internet domain names (the electronic address of a web site) is coordinated by the State, based on an international system of allocation of Internet addresses, which follow agreed upon Internet Protocols. In the process of granting those domain names, some important data are usually required, such as the identification of the applicant, his or its physical address, etc., which may contribute to (at least, partially) overcome the difficulty of finding in the off-line world person or institutions that should be liable for their acts or omissions in the on-line environment. Also, the grant of a domain name has a social function, that it be used in connection with a web site and not for the purpose of staying dormant up until some interested party wishes to buy it. Also, some administrative arrangements have been entered into in some countries to allow for the exchange of data and for the sharing of databases connecting the authorities in charge of registering trademarks and the authorities in charge of analysing and granting domain name applications.