The Use of Electronic Signatures in Courts and Beyond: Some Questions*

Gregory HAGEN**

I. CAN ELECTRONIC SIGNATURE TECHNOLOGY IMPROVE JUSTICE? 229

II. WHAT IS THE BALANCE BETWEEN SECURITY AND COMPETING CONCERNS? 231

III. WHAT IS INFORMATION SECURITY? 232

IV. WHAT ARE ELECTRONIC SIGNATURES? 233

V. DOES THE BLUEPRINT REQUIRE THE USE OF ELECTRONIC SIGNATURES? 234

VI. WHAT IS PUBLIC KEY ENCRYPTION AND PUBLIC KEY INFRASTRUCTURE? 236

VII. IS THERE A CASE FOR ELECTRONIC SIGNATURES AND PKI FOR COURTS? 242

VIII. DIGRESSION: SHOULD USERS OF ODR USE ELECTRONIC SIGNATURES? 245

IX. WHO SHOULD THE LEGAL CA BE FOR USERS OF PKI IN LEGAL SETTINGS? 248

X. CONCLUSION 251

* Prepared for the Canadian Institute for the Administration of Justice conference "The Courts and Beyond: The Architecture of Justice in Transition," October 10–12, 2012, Calgary, Alberta, Canada. Funding for part of this research was provided by the Social Sciences and Humanities Research Council of Canada.

** Gregory R Hagen is an Associate Professor in the Faculty of Law at the University of Calgary and a member of the Institute for Security, Privacy and Information Assurance at the University of Calgary.

I. CAN ELECTRONIC SIGNATURE TECHNOLOGY IMPROVE JUSTICE?

The Cyberjustice project aims to improve justice through the application of new uses of information technology in existing courts.[1] But the potential for improvement extends beyond courtrooms to include online dispute resolution, online courts, administrative hearings, the management of legal rights by government or private bodies (such as land title registries and corporate registries), as well as the management of client information by law firms. To what degree can information technology improve such systems without deterring their use because of the difficulty of accepting changes to rituals, practices and traditions?

This paper focuses on a particular kind of information security technology, an electronic signature, one that is created using a private key within a public key infrastructure (PKI). It asks whether such electronic signatures should be used in order to authenticate the identity of filers of court documents and their contents. The reason for focusing on signatures is that they have long been used in legal documents in order to identify the person signing them.[2] Typical signed documents include not only contracts, bills of exchange, and deeds of title, but also factums, pleadings, judgments, and court orders. The argument for the use of electronic signatures is based upon the principle of technological neutrality:[3] since they are necessary for paper-based documents, they are necessary for electronic documents.[4] This kind of thinking formed the basis of the creation of electronic signatures by Whitfield Diffie and

---

1 See Towards Cyberjustice, online: <http://www.versunecyberjustice.org/en-us/home.aspx> and more generally, François Senécal & Karim Benyekhlef, "Groundwork for Assessing the Legal Risks of Cyberjustice" (2009) 7 CJLT 41.

2 Chris Reed, "What is a Signature?" (2000) 3 JILT, online: <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed>.

3 Chris Reed, "Taking Sides on Technology Neutrality" (2007) 4 SCRIPTed 263, online: <http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.asp>.

4 *Ibid.*

Martin Hellman,[5] as well as the enactment of electronic signature legislation throughout the world during formative years of the world wide web.[6]

Nevertheless, few courts in Canada require the use of electronic signatures for electronic filing and the *Blueprint for the Security of Judicial Information* (*Blueprint*) has no explicit requirement for their use for authentication purposes.[7] At the same time, electronic signatures are extensively used for the management of legal rights by registries, such as land title or patent registries.[8] So, why are electronic signatures seldom used in one context and a lot more in others? Should electronic signatures be used in courts and other legal contexts for authentication purposes? This paper does not endeavour to answer these questions, but to raise them and a number of related questions and to provide background information for the purposes of future research in the Cyberjustice Project. The thoughts in this paper should be regarded as exploratory and preliminary. Further, since information security is also not a state of affairs that can be attained for all time but is a response to risks that may change over time as technology changes, the answers to such question may change over time as well.

First, this paper sets out the main issue of balancing the use of new information security technology with competing concerns. Second, it briefly describes the attributes of a secure information system. Third, it outlines the concept of information security. Fourth, it defines 'electronic signature.' Fifth, it notes that the *Blueprint* developed by the Canadian Judicial Council does not explicitly require the use of electronic signatures for judicial use. Sixth, it briefly describes public key cryptography and public key infrastructure. Seventh, it gives examples of the use of electronic signatures within a PKI in the electronic filing of

---

5 Whitfield Diffie and Martin E Hellman, "New Directions in Cryptography" (1976) IT-22 IEEE Transactions on Information Theory, online: <http://www-ee.stanford.edu/~hellman/publications/24.pdf>.

6 See D Bruce Ferrend, "Policy Considerations Behind Legislation Recognizing Electronic Signatures," Uniform Law Conference of Canada, online: <http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub=4g>.

7 Canadian Judicial Council, *Blueprint for the Security of Judicial Information* 3d ed (2009), online: Canadian Judicial Council <http://www.cjc-ccm.gc.ca/cmslib/general/JTAC-ssc-Blueprint-Third-edition-finalE.pdf>.

8 See the discussion below.

patent applications and, eighth, the use of electronic signatures within a PKI in land title document filing in British Columbia. Ninth, it discusses the case for the use of electronic signatures in offline courts. Tenth, it discusses the case for high assurance electronic signatures in online dispute resolution. Finally, it shows how the use of new technology (specifically electronic signatures) can result in new questions and problems such as who should the certification authority (CA) be in a legal context?

II. WHAT IS THE BALANCE BETWEEN SECURITY AND COMPETING CONCERNS?

If the goal of technology is to improve justice, then to what degree should technological change be allowed to upset the existing rituals and procedures of organizations and persons? Improvement of practices that increase access to justice may require technological change. Yet, technological improvement might also require new forms of practice that are not easy for people to use, thereby deterring the use of technology-enhanced courts so as to lessen access to justice. Technological improvements for dispute settlement may also bring with them new concerns, such as whether it challenges existing governance structures, concerns about information privacy, questions about who controls and owns the information infrastructure, whether managed services are acceptable, issues about the transparency of the architecture, the accountability of the organization respecting information technology standards, and whether the information infrastructure should be public or private.

For the reasons given above, this paper focuses on whether electronic signatures should be used in legal settings, particularly to sign court documents. The answer may depend upon the context and the state of the technology that is available. Thus, it may be appropriate currently to require the use of a high assurance electronic signature for access to judicial databases by authorized individuals. It may be reasonable for electronic court orders and electronic judgments to be electronically signed with a high degree of assurance. It may also be appropriate, to provide comfort to relying parties, to ensure that certain electronic registry filings (such as land title filings and patent applications) are electronically signed by lawyers (or patent agents, as the case may be). It is more questionable, despite the increase in security, as to whether high assurance electronic signatures are reasonably required at this time to sign

and submit electronic documents to courts given the, presumably, low risk of fraud. Further, for online courts and online dispute resolution providers, it may be asking too much for citizens to use high assurance electronic signatures when filing electronic documents where they are complex to use and onerous to obtain. At any rate, these are the kind of decisions that have to be made.

III. WHAT IS INFORMATION SECURITY?

Information security is needed to protect information from risks from attack.[9] For instance, there is a risk that a record of a conviction might be illegitimately changed to acquittal within a court information system. Further, there is a risk that electronic evidence within the court or tribunal's information system may be tampered with in order to change the outcome of a dispute. Similarly, there is also a risk that one might forge an electronic signature in an electronic filing of a land title transfer, a factum or an electronic court order.

In general, information security deals with the prevention and detection of unauthorized actions by users of an information system.[10] Information security is commonly said to require three attributes:[11]

- Confidentiality—Limited observation and disclosure of knowledge.
- Integrity—Completeness, wholeness, and readability of information and quality being unchanged from a previous state.
- Availability—Usability of information for a purpose.

There is a dispute about additional security attributes.[12] Donn Parker has added the following three attributes:[13]

---

9 See Dieter Gollmann, *Computer Security* (Chichester, UK: Wiley, 2011).

10 *Ibid* at 39, but 'computer' is replaced with 'information' in this definition.

11 *Ibid* at ch 3. The particular definitions of these attributes are taken from Donn Parker, "Toward a New Framework for Information Security" in Seymour Bosworth and ME Kabay, eds, *Computer Security Handbook*, 4th ed (Chichester, UK: Wiley, 2002).

12 *Ibid.*

13 *Ibid*.

- Utility—Usefulness of information for a purpose.
- Authenticity—Validity, conformance, and genuineness of information.
- Possession—Holding, controlling, and having the ability to use information.

IV. WHAT ARE ELECTRONIC SIGNATURES?

The function of a handwritten signature can be considered to provide evidence (a) of the identity of the signatory; (b) that the signatory intended to sign the document; and (c) that the signatory adopted the contents of the document.[14] Electronic signatures are intended to perform the same function as handwritten signatures, but by electronic means.[15]

Like most jurisdictions, Alberta had adopted a definition of "electronic signature" that does not refer to the use of any particular technology. Under the *Electronic Transactions Act*,[16]

> "Electronic signature" means electronic information that a person creates or adopts in order to sign a record and that is in, attached to or associated with the record;"
>
> Further,[17]
>
> 16 (1) Subject to subsection (2) and section 22, a legal requirement that a record be signed is satisfied by an electronic signature.
>
> (2) If a record is prescribed for the purposes of this subsection or belongs to a class prescribed for those purposes, the legal requirement that the record be signed is satisfied by an electronic signature only if in light of all the circumstances
>
> (a) the electronic signature is reliable for the purpose of identifying the person, and

---

[14] *Supra* note 2. See also Government of Alberta, *A Guide to Alberta's Electronic Transactions Act* (March 2003), online: Legislative Assembly of Alberta <http://www.assembly.ab.ca/lao/library/egovdocs/alis/2003/143290.pdf>.

[15] *Ibid*.

[16] SA 2001, c E-5.5, s 1(1).

[17] *Ibid* at s 16.

(b) the association of the electronic signature with the relevant record is reliable for the purpose for which the record was created.

By contrast, for example, under the *British Columbia Land Title Act*, the definition of 'electronic signature' presumes that public key cryptography will be used to sign documents for the purposes of filing documents with the Land Title Survey Authority (LTSA):[18]

"electronic signature" means a signature in electronic format that is

(a) created by a subscriber using a private cryptographic key under the control of the subscriber that corresponds to a public cryptographic key contained in a certificate, and

(b) incorporated into

(i) electronic applications and electronic instruments,

(i.1) electronic plan applications and electronic plans, and

(ii) electronic returns under the Property Transfer Tax Act;…

V. DOES THE BLUEPRINT REQUIRE THE USE OF ELECTRONIC SIGNATURES?

The *Blueprint* makes the very important point that an information security policy is not an IT policy that is *separate* from judicial practice, but it is "the set of rules, protocols and practices courts and judges follow in order to manage and protect their information resources."[19] In terms of judicial practice, historically, many court documents, like orders, factums and judgments, were signed, so one might argue, on the basis of technologically neutrality, an information security policy governing electronic transactions would require that electronic factums, orders and judgments should be electronically signed.

---

[18] RSBC 1996, c 250.

[19] *Supra* note 7 at 50.

However, while the Canadian Judicial Council has set out 19 policies regarding the security of judicial information in its *Blueprint for Security of Judicial Information*, none of them explicitly require the use of electronic signatures. Perhaps the closest that the *Blueprint* gets to explicitly requiring electronic signatures is to require 'robust system access controls' for judicial users in Policy 8:[20]

> Policy 8: Courts must implement robust system access controls to ensure that only authorized users have access to any court system, and that their level of access corresponds to their security clearance and the court's information classification scheme. Access rights to classified judicial information must be determined by the judiciary.

While policy 8 does not explicitly require electronic signatures, a case can be made that electronic signatures using public key encryption and high assurance digital certificates are sufficient for robust authentication that is itself a precondition for 'robust system access controls' that ensures that only authorized users have access to a court's information system.

One reason that the *Blueprint* may not explicitly deal with electronic signatures on electronic documents filed with the court, such as pleadings and factums, is that the *Blueprint*'s scope does not appear to cover documents that are electronically filed by lawyers. It is true that the *Blueprint* concerns the security of judicial information, which is considered to be (with some exceptions) "information gathered, produced or used for judicial purposes…"[21] and that this definition implies that judicial information includes some documents submitted by lawyers. Immediately, after that definition is given, however, the scope of 'judicial information' is limited: "Judicial information is created by judges, including judicial officers…."[22]

This limitation does not rule out the use of electronic signatures for e-filing, however, because the *Blueprint* is not intended to supplant generally accepted information security standards provided by standards

---

[20] *Ibid*.

[21] *Ibid* at 25.

[22] *Ibid* at 26.

organizations or by the government, unless the *Blueprint* is more stringent than, or contradicts, such standards.[23]

VI. WHAT IS PUBLIC KEY ENCRYPTION AND PUBLIC KEY INFRASTRUCTURE?

Public key encryption is one kind of technology that can enable electronic signatures.[24] Other technologies could potentially satisfy the legal requirements for electronic signatures as well.

Public key cryptography arose as a method to enable secret communications between two parties, say, Alice and Bob without the need to share a secret key. Historically, a secret key that was shared only between a sender and recipient was used to encrypt and decrypt messages. A simple example would be to change each letter to another letter in the alphabet in accordance with a shared secret key (e.g. a to b, b to c, etc.) and then change them back. This form of encryption is considered to be symmetric because both the sender and recipient know the secret encryption key.[25]

Several problems arise from the use of symmetric encryption. First, there is a need for a secret exchange of keys prior to the secret communication itself. Second, since there will be communications with multiple persons, multiple secret keys need to be shared. Third, it is difficult to communicate with those with whom you do not share a secret key.[26]

An alternative to symmetric encryption is public key cryptography, made famous by Diffie and Hellman.[27] This radical idea was to have two keys, one private and one public. The private key would be known only to, and controlled by, one person and the public key would

---

[23] *Ibid* at 29.

[24] Carlisle Adams and Steve Lloyd, *Understanding Public Key Infrastructure* (Indianapolis: McMillan, 1999), at 20–21. See also Michael E Whitman and Herbert J Mattord, *Principles of Information Security* (Boston: Course Technology, 2009).

[25] *Ibid* at 13–15.

[26] These points are taken from *ibid* at 15–16.

[27] *Supra* note 4.

be made available to the public. The crucial feature of this key pair is that one key (and no other key) must decrypt what the other one encrypts. The mathematics of cryptography is designed to ensure that this property holds. So, Alice can encrypt an electronic document with Bob's public key which can only be decrypted with Bob's private key.[28]

A private key can also be used to *sign* an electronic document. First, a document is strongly associated with a smaller amount of data—the message digest. Then Alice can sign the document by encrypting the message digest of the document with her private key so that it can be verified by decrypting the encrypted message digest (with her public key) to obtain the message digest and then ensuring that it is the identical message digest of the document that is signed.[29]

A digital certificate is a public key that is electronically signed (certified) by a trusted third party—a CA. A CA is an entity that issues digital certificates. The certificate is designed to give assurance of the identity (or other attributes) of the person to whom the certificate is issued. The need to sign a public key arises as follows. Suppose that Alice signs a document with her private key and that signature is verified by Bob using a public key that he believes belongs to Alice. How does Bob know that it is Alice's public key, when in fact, it might be Arnold's, who gave it to Bob? A CA signs the public key, which contains Alice's name, certifying that it is issued to Alice. If this third party CA can be trusted, then Bob knows that it is Alice's public key and that the document was signed by the corresponding private key. If that key is used only by Alice (e.g. because it was not 'stolen' or given to someone else by Alice), then Bob can verify that Alice signed the document at issue.[30]

A CA should be distinguished from a Registration Authority (RA) to whom some functions of the CA are delegated.[31] Thus, an organization might designate certain employees to establish the identity of an individual, assist in the generation of key pairs, or initiate the issuance of a digital certificate by the CA.

---

[28] For a discussion of these points, see Adams, *supra* note 24 at chapter 2.

[29] For information in this paragraph, see *ibid* at 20–21.

[30] For information in this paragraph, see *ibid* at 34 and chapter 6.

[31] *Ibid* at 89.

Public key infrastructure is a kind of trust infrastructure whose services are implemented and delivered using public key technology.[32] A public key infrastructure will typically include the technology needed to issue digital certificates.[33] It will also include rules and policies, such as a certification practice statement (CPS) which defines the operational rules of the PKI.[34] It will also include certificate policies which define the attributes of the certificates,[35] such as whether the issuance of the certificate requires being authenticated by a notary. A PKI will also include a subscriber agreement which defines the relationship between the subscriber and the person who issues a digital certificate to the subscriber.[36]

Example 1: What is the Case for PKI in the WIPO Electronic Filing Standard?

The World Intellectual Property Organization (WIPO) has created and published a standard in relation to the electronic filing, processing, and storage of international applications under the Patent Cooperation Treaty.[37] In terms of information security, the standard is the following:[38]

> Solutions implemented under this standard must satisfy the following four basic criteria for secure electronic data exchange:
>
> (a) authentication—the process of validating an identity claimed by or for an entity;
>
> (b) integrity—ability to verify that data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed;

---

[32] *Ibid* at 33 and chapter 9.

[33] *Ibid* at 34.

[34] *Ibid* at 85–86.

[35] *Ibid*.

[36] For instance, see the Government of Canada Fintrac Subscriber Agreement, online: <http://www.fintrac-canafe.gc.ca/reporting-declaration/pki/agr-acc-eng.pdf>.

[37] PCT Treaty, Regulations and Administrative Instructions, "Standard for the Filing and Processing in Electronic Form of International Applications," online: World Intellectual Property Organization <http://www.wipo.int/pct/en/texts/>.

[38] *Ibid* at 6.

(c) non-repudiation—ensure that strong and substantial evidence is available to the sender of data that the data has been delivered (with the cooperation of the recipient), and to the recipient of the sender's identity, sufficient to prevent either from successfully denying having possessed the data; this includes the ability of a third party to verify the integrity and origin of the data;

(d) confidentiality—ensure that information can be read only by authorized entities.

The case for using PKI was examined by the WIPO for receiving applications for patents under the Patent Cooperation Treaty. According to the WIPO:[39]

> This [security] standard supports, in particular, a solution relying on a public key infrastructure (PKI) for authentication and data security in the Internet environment. However, it also envisages that there may in the future be other solutions which satisfy the above four security criteria.

Unfortunately, little information is publicly available from the Canadian Intellectual Property Office regarding electronic filing under the Patent Cooperation Treaty, but the USPTO has extensive information available online regarding electronic filing with the USPTO more generally. The USPTO's case for electronic filing can be summarized as follows:

> The goal of the USPTO is to improve customer service, improve quality of our work products, reduce cycle time for examining patent and trademark applications, and lower costs. Strategies include:[40]
>
> Making electronic filing of applications and correspondence, payment, and communication so simple, inexpensive, and trusted that customers will prefer these to calling or filing paper documents and mailing;

---

[39] *Ibid*.

[40] *Request for Agreement (RFA) 60-PBPT-0-00001 for the USPTO Electronic Filing Partnership (EFP)*, online: United States Patent and Trademark Office <http://www.uspto.gov/web/rfa/rfaintro.html>.

> Providing through RFAs for private sector XML encoding software to facilitate preparation of documents and methods for electronic filing, payment, as well as support for the full range of two way communication with the USPTO;
>
> Aggressively protecting transaction integrity, authenticity and confidentiality where appropriate and required by law;
>
> Substantially reducing electronic filing processing costs;
>
> Seeking the best people, ideas and partners to assure our success; and
>
> Delivering the highest quality products and services as promised.

When the USPTO was creating its electronic filing system it decided that passwords were not sufficient for security:[41]

> The USPTO would consider a proposal unacceptable if it relied solely on password security. The USPTO has implemented an Entrust enterprise PKI in support of the authentication, integrity and confidentiality needs of our patents business.

The "USPTO provides the highest level of security for registered filers through a security architecture called Public Key Infrastructure (PKI)."[42] Its benefits include:[43]

- Certainty of the quality of information sent and received electronically;
- Certainty of the source and destination of that information;
- Assurance of the time and timing of that information (providing the source of time is known);
- Certainty of the privacy of that information; and

---

41 *Answers to Questions from Request for Comments on the Request for Agreement (RFA) 60-PBPT-0-00001 for the USPTO Electronic Filing Partnership (EFP)*, online: United States Patent and Trademark Office <http://www.uspto.gov/web/rfa/rfaattach5.html>.

42 *EFS-Web Security*, online: United States Patent and Trademark Office <http://www.uspto.gov/ebc/portal/efs/security.pdf>.

43 *Ibid*.

- Assurance that the information may be introduced as evidence in a court or law.

Under the USPTO 'Legal Framework for EFS-Web,' those who file electronically must use a PKI certificate for secure communication and authentication of the user: [44]

> In order to obtain a PKI certificate, the user must be a registered practitioner (i.e., an attorney or agent) or an inventor, and complete the appropriate paperwork (e.g., review the PKI subscriber agreement and complete the certificate action form, available on the USPTO Web site). Once the user has a PKI certificate, the user can authenticate himself or herself to the USPTO through the EFS-Web sign-on. This will generate a secure, encrypted connection with the USPTO.

This description does not explain how authentication works, but one way it could work is that, at sign on, a user signs a short message using the user's private key, and then the identity of the sender can be verified by the USPTO by using the user's digital certificate.

Example 2: What is the Case for PKI in the BC LTSA Authority Electronic Filing System?

Legislation requires that electronic signatures be used for electronic filing of most land title documents and plans in British Columbia:[45]

> In order to submit a document or plan electronically, it must first be electronically signed by a subscriber. Subscribers are issued digital certificates by the Law Society of British Columbia, a certification authority recognized under s 168.79 of the Act.

Based upon the definition of 'electronic signature,' a signer must use his or her private cryptographic key (that corresponds to a public

---

[44] *Legal Framework for EFS-WEB* (6 April 2011), online: United States Patent and Trademark Office <http://www.uspto.gov/patents/process/file/efs/guidance/New_legal_framework.jsp#heading-5>.

[45] LTSA, *Director's Requirements DR 06-11*, online: Dye & Durham Information & Legal Support Services <https://www.dyedurhambc.com/public/DR-06-11-Directors-Requirements-to-Submit-Land-Title-Forms-Electronically.pdf>.

cryptographic key contained in a certificate) to sign an electronic land title document.[46]

The rationale for electronic filing of land title documents includes the increased security associated with E-filing, along with other features.[47]

> E-filing is quicker, more convenient, more secure and generally less expensive than filing physical documents. The LTSA has developed EFS in response to general demand from professionals for modern e-business solutions....

Interestingly, however, new technologies can also provide criminals with new ways of perpetrating frauds.[48]

VII. IS THERE A CASE FOR ELECTRONIC SIGNATURES AND PKI FOR COURTS?

As mentioned, the *Blueprint* does not explicitly require electronic signatures, but it does mention the need for robust access control.[49] In discussing how to enable access control, it discusses several possible technologies that could be of use.[50]

> 114. A simple combination of unique username (or—login ID) and password offers a certain minimum level of security. Passwords are vulnerable to being shared, stolen, guessed or calculated. Stronger methods of authentication involve a

---

[46] *Supra* note 18.

[47] *FAQs—Electronic Filing System (EFS)*, online: BC Land Title & Survey <http://www.ltsa.ca/cms/using-the-electronic-filing-system>. For additional discussion in an Ontario context, see Alan Silverstein, "No More Paper: Practicing Real Estate Law Without Paper," online: The Frontenac Law Association <cfla.on.ca/cfla/docs/legalconference/kingstonpaper.doc>.

[48] Rouhshi Low, "From Paper to Electronic: Exploring the Fraud Risks Stemming From the Use of Technology to Automate the Australian Torrens System," (2009) 21:2 Bond L Rev, online: <http://epublications.bond.edu.au/blr/vol21/iss2/>; Sharon Christensen, "Electronic Land Dealings in Canada, New Zealand and the United Kingdom: Lessons for Australia" (2004) 37:1 MurUEJL 37, online: <http://www.austlii.edu.au/au/journals/MurUEJL/2004/37.html>.

[49] *Supra* note 7 at Policy 8.

[50] *Ibid*.

> combination of approaches and more elaborate technologies such as dynamic passwords, smart cards, USB tokens, digital certificates and biometrics.

While the *Blueprint* does not mandate the use of electronic signatures for the purposes of access control, generally, Policy 11 requires that up-to-date (i.e. public key) encryption technology be made available to judicial users for the storage and transmission of *classified* judicial information.[51]

> Policy 11: Courts must make up-to-date encryption technology readily available to judicial users for the storage and transmission of classified judicial information on networks, desktops, notebooks and all portable devices and media.

The commentary to Policy 11 is even stronger than the policy itself, in some respects, requiring encryption of classified judicial information over public networks.[52]

> 139. Judicial information that is classified should be encrypted before it is transmitted over a public network.

The *Blueprint* defines 'PKI' at paragraph 137, implying (it seems) that it should be used in relation to encryption:[53]

> 137. Software, standards and management protocols relating to the encryption of data through the use of digital certificates comprise what is known as PKI, or the Public Key Infrastructure.

Policy 11 does not require the use of a private key for electronic signing for authentication purposes. However, the commentary does describe the use of public key certificates that authenticate the identity of the recipient of the encrypted transmission, suggesting perhaps that they be used at least for the transmission of classified judicial information:[54]

> 138. A digital certificate, issued by a trusted third party, verifies the identity of a user and connects that user to a unique public key,

---

[51] *Ibid* at Policy 11.

[52] *Ibid*.

[53] *Ibid*.

[54] *Ibid*.

> which allows for the exchange and decryption of encrypted messages.

Because the *Blueprint* does not supplant other standards, however, one can turn to other standards to answer questions concerning e-filing. Insofar as government information security policies are available and applicable, they are useful to consult for guidance. The Canadian Government *Management of Information Technology Security* (*MITS*) policy goes further than the *Blueprint* by explicitly stating that PKI is one way that a department can fulfill information security requirements, generally speaking:[55]

> Public Key Infrastructure (PKI) is one way that departments can fulfill requirements for authentication, confidentiality, integrity and non-repudiation. PKI provides public key encryption and digital signatures as well as processes for managing public keys.

The *MITS* policy notes that cryptography can be used to satisfy various security requirements:[56]

> When properly used, cryptography is an effective means of ensuring confidentiality, integrity, authentication and non-repudiation. Departments must ensure effective key management, including the protection and recovery of cryptographic keys.

None of these information security policies require the use of electronic signatures to submit and sign electronic documents with a court. Indeed, it appears that there are few court electronic filing services that require electronic documents to be electronically signed. However, as a counter-example, the Alberta Court of Appeal does require electronic signing of factums.[57]

---

[55] Treasury Board of Canada Secretariat, *Operational Security Standard*: *Management of Information Technology Security*, online: Government of Canada <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=text>.

[56] *Ibid*.

[57] Alberta Court of Appeal, *Building Electronic Appeals (E-Appeals) Using Adobe Acrobat 7.0*, online: Alberta Courts <https://www.albertacourts.ca/CA/EFILING/Default.aspx?tabid=39>.

> 18.1 E-Appeals must be digitally signed with an invisible signature. Your document will be rejected if you submit it with a visible signature.

The e-filer creates a key pair in Adobe Acrobat.[58] Then, the public key is signed by the e-filer, so that the e-filer is the CA,[59] rather than a trusted third party such as the Law Society of Alberta or a commercial CA. Authentication appears to be done by the Court of Appeal Registry by comparing the fingerprint on the digital certificate to the fingerprint faxed to the Registry.[60] It seems, then, that authentication of identity of e-filers is done by relying upon a representation by the e-filer in a facsimile to the Court of Appeal Registry.[61]

> These digital signature fingerprints are unique to your Certificate. When you submit your digital signature at the E-Appeals website, you will be asked to fax a copy of these digital signature fingerprints to the appropriate Court of Appeal Registry.

One question that arises for the Alberta Court of Appeal, then, is whether a public key infrastructure that uses facsimile communication to authenticate users offers a high enough degree of assurance of identity.

VIII. DIGRESSION: SHOULD USERS OF ODR USE ELECTRONIC SIGNATURES?

The British Columbia Government recently passed the *Civil Resolution Tribunal Act*.[62] According to the Government press release, the intent is "to create the first-ever tribunal in Canada that offers a full array of online tools to allow British Columbians to solve common strata

---

58 *Ibid* at Appendix 43ff.

59 *Ibid* at Appendix 49–50.2.

60 *Ibid* at 22.3.

61 *Ibid* at 17.8.

62 Bill 44—2012 Civil Resolution Tribunal Act, 4th Session, 39th Parliament (2011–2012) (Royal Assent given May 31, 2012, but not yet in force), online: Legislative Assembly of British Columbia <http://www.leg.bc.ca/39th4th/3rd_read/gov44-3.htm>.

and small civil claims outside of courts…."[63] The press release states that "[i]t will use mainly online web technologies, with some assistance by phone or mail."[64] Should the tribunal require users of this system to use electronic signatures to gain access to the system or to sign electronic documents? It would seem initially unlikely given that the security requirements would exceed that of most offline courts, but perhaps the online context requires greater authentication than offline courts in order for users to feel comfortable that they are dealing with the intended party.

There is nothing published by the British Columbia Government to suggest that anything other than passwords will be required by the online system to gain access to it and submit materials. The main security standard published in the *Civil Resolution Tribunal Act* is as follows:[65]

> 86 (1) The tribunal must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Given that the online resolution system will be provided by the tribunal, the requirement of reasonableness will apply to security of the online system. Is it reasonable to *require* the use of high assurance electronic signatures (i.e. private keys that correspond to high assurance digital certificates) in order to authenticate identity for online dispute resolution? People need to know who they are dealing with on the Internet, but these high assurance signatures may not only be relatively complex for some to use, but onerous to obtain because they require identification documents that users may not have (e.g. passport) and authentication procedures which are daunting, complex or time-consuming to some potential users.

In some respects, then, the case for the use of high assurance electronic signatures by users of online dispute resolution seems weaker

---

[63] British Columbia Ministry of Justice, "Online civil dispute tools to save time, money" (7 May 2012), online: <http://www.newsroom.gov.bc.ca/2012/05/online-civil-dispute-tools-to-save-time-money.html>.

[64] *Ibid*. See also British Columbia Ministry of Justice, "Dispute Resolution Model for the Proposed Civil Resolution Tribunal," online: <http://www.ag.gov.bc.ca/legislation/civil-resolution-tribunal-act/pdfs/CRT-Business-Model.pdf>.

[65] *Supra* note 62.

than the case for use by judicial users and lawyers in courts, who are trained for procedural complexity. Courts are the most formal, rigorous, procedurally complex, slow and costly means for resolving disputes but also present the best context for lawyers and judges to be model users of high assurance electronic signatures.

The use of online dispute resolution, by contrast, is designed to allow the *choice* of access to dispute settlement without the procedural rigour, complexity, cost and delay of courts. This could also allow one to avoid the potential complexity of using electronic signing tools. At the same time, there is an argument that parties in an online transaction are at a greater risk of identity fraud than if they, or their lawyer, appeared physically in court. For instance, online a non-party may masquerade as a party (essentially acting as their lawyer) in order to gain an advantage for the party. Moreover, security standards that are set too low may also provide access to a less just means of dispute settlement, undermining the point of the service.

Governments are recognizing that there is a need for a framework for online identity management and authentication that defines a *suitable* form of authentication for online services.[66] The Draft *Identity Assurance Model* identifies four key factors that help to determine the suitability of an authentication scheme:[67]

- What are the identity attributes that are required?
- What evidence must be provided for the identity attributes?
- What are the authentication processes used to verify the accuracy of an assertion about an attribute?

---

[66] Identity Management and Authentication Task Force, *Provincial Identity Information Management Program*, online: Ministry of Technology, innovation and Citizens' Services, The Province of British Columbia <http://www.cio.gov.bc.ca/cio/idim/idmatf.page>. The Task Force on Inter-Jurisdictional Identity Management and Authentication, including members appointed by the governments of British Columbia, Québec and Ontario.

[67] Identity Management and Authentication Task Force, *Draft Identity Assurance Model*, online: Institute for Citizen-Centered Service <http://www.iccs-isac.org/en/km/transformative/docs/Identity%20Assurance%20Model.pdf>. See also the Assurance, Identity and Trust Working Group, *Pan Canadian Assurance Model* (3 March 2010), online: Institute for Citizen-Centered Service <http://www.iccs-isac.org/en/km/transformative/docs/Pan-Canadian%20Assurance%20Model.PDF>.

- What degree of assurance is needed that the entity possesses the attribute?

Ideally, the use of electronic signatures would be virtually seamless and supported by an authentication scheme that is suitable. Otherwise, they may become a barrier to accessing the online service. The trade-off between information security needs and the ease of use of technology is not the only concern, however. There has been a persistent concern with the need for privacy and, in particular, privacy-preserving uses of digital certificates.[68] There is a question as to whether biometric identity attributes, such as fingerprints, are suitable, given concerns about the privacy implications of providing such attributes to online service providers.

Perhaps the most that can be said in the circumstances may be that users who want a high level of authentication of identity be offered a *choice* of online dispute resolution using high assurance digital certificates but not required to do so.

IX. WHO SHOULD THE LEGAL CA BE FOR USERS OF PKI IN LEGAL SETTINGS?

The Pan Canadian *Identity Management Framework* uses the concept of an Authoritative Party (AP) as one who "is responsible for proving the identity of an individual or business, or maintaining an authoritative identity source that can be relied upon."[69] According to the *Framework*, the AP may be a government or a commercial enterprise, depending upon the context.[70]

---

[68] Information and Privacy Commissioner of Ontario, *Concerns and Recommendations Regarding Government Public Key Infrastructures for Citizens* (December 2002), online: Information and Privacy Commissioner, Ontario, Canada <http://www.ipc.on.ca/images/Resources/pki.pdf>.

[69] Identity Management and Authentication Task Force, *Trusting Identities* at 12, online: Institute for Citizen-Centered Service <http://www.iccs-isac.org/en/km/transformative/docs/IMSC%20Paper_Trusting%20Identities%20Consultation%20Draft_EN.pdf>.

[70] *Ibid*.

In the context of a public key infrastructure, the AP is the CA. Who should the CA be in legal contexts? Possible candidates include: commercial CAs, such as Verisign, Inc. (now Symantec, Inc.), organizational CAs, regulatory CAs, government CAs, court CAs, individual CAs and others.

The WIPO standard for e-filing allows that individual national patent offices will have their choice of CA:[71]

> Each receiving Office will specify the certification authorities that are recognized by that Office to issue certificates for purposes of the E-PCT. The list may include Office CAs or public [i.e. commercial] CAs.

Such CAs will typically be government CAs, such as a department of the Canadian Government, but could also be a commercial CA such as Verisign Inc. In fact, the WIPO customer digital certificate is issued by Verisign, Inc. (now Symantec, Inc.), a commercial CA.[72] The USPTO CA issues its own certificates.[73]

In September, 2000, the Law Society of British Columbia (LSBC) claimed that it should be the sole CA for lawyers in British Columbia on the basis that issuing certificates of standing is a core function of law societies.[74] The analogy relied upon by the LCBC is that digital certificates issued by a CA are analogous to certificates of standing (the certificate that a lawyer puts in her wallet) issued by law societies to lawyers. The LSBC, therefore, rejected the idea that an organization that is distinct from a law society, whether it be an independent not-for-profit organization, the Federation of Law Societies or a law firm, could (also) be a CA for lawyers, whether for land title filings or otherwise. The LSBC nevertheless took the position that *it* could be the CA for non-

---

[71] *Supra* note 37 at 80.

[72] WIPO Customer Certification Authority Information, Digital Certificates, online: World Intellectual Property Organization <http://www.wipo.int/pct-safe/en/certificates.html>.

[73] USPTO, *United States Patent and Trademark Office Public Key Infrastructure Subscriber Agreement*, online: United States Patent and Trademark Office <http://www.uspto.gov/patents/process/status/private_pair/PKI_Subscriber_Agreement.pdf>.

[74] Karl Warner, QC, *Information from the Law Society Respecting Resolution 2*, online: The Law Society of British Columbia < http://www.lawsociety.bc.ca/page.cfm?cid=1144&t=Information-from-the-Law-Society>.

lawyers, such as notaries, financial officers and land surveyors, in relation to land title filings, notwithstanding that its own case for being a CA was based upon its unique role as a regulator of *lawyers* in British Columbia.[75]

Although the LSBC made its case for being the sole CA for lawyers in British Columbia based upon the idea that issuing digital certificates is a core function of a legal regulator, it incorporated a subsidiary, Juricert Services Inc. with the intent that the LSBC "…carry out professional authentication directly through Juricert."[76] This gives rise to the question as to who is the CA, the LSBC or Juricert Services Inc.? Whether the LSBC is in fact the CA for land title filings in British Columbia is not easily ascertainable given contradictory information available from the LSBC, the LTSA and Juricert Inc. as to who the CA currently is.[77] In Ontario, digital certificates for the purposes of land title filings are issued to lawyers by Teranet, a publicly traded income fund.[78] In Alberta, digital certificates for the purpose of electronic appeals are issued by the certificate holders themselves.[79]

The *Blueprint* itself has little discussion as to who should be a CA for judicial information systems. It recommended, on the basis of independence of the CA, that a CA for judicial users should not be the judiciary or government:[80]

> 138. A digital certificate, issued by a trusted third party, verifies the identity of a user and connects that user to a unique public key, which allows for the exchange and decryption of encrypted messages. To ensure complete independence, it is recommended that the certification authority for judicial users be a trusted third party independent not only of the judiciary but of the government.

---

[75] See the outcome in LTSA, *Director's Requirements No. 02-11*, and also Juricert Services Inc, online: <http://www.Juricert.com>.

[76] *Supra* note 74.

[77] For instance, while the Director of Land Title has recognized the LSBC as the CA, the LTSA and Juricert Services Inc. both speak of digital certificates issued by Juricert Services Inc. on their websites.

[78] See Teranet, online: <http://www.teranet.ca/>.

[79] *Supra* note 57.

[80] *Supra* note 7.

This policy would rule out court administrative services being the CA, since it is a government service. However, the principle of CA independence might, therefore, also rule out self-regulatory organizations, such as law societies, for the purposes of filing electronic documents with courts.

X. CONCLUSION

Information technology can result in more efficient, less expensive and more secure legal information systems, but it may also upset existing norms and have additional drawbacks that ultimately make it a barrier to accessing justice. This paper has focused on the current and potential uses of electronic signatures using public key cryptography to satisfy information security needs. High assurance electronic signatures are widely used for land title filings and PCT patent applications to increase security of information, but not used much in courts.

The potential use of such electronic signatures raises a host of issues. Should electronic signatures be used in courts for signing judicial documents, for access to judicial databases, to access e-filing systems or to sign electronic pleadings and factums? Who should be the CA in legal contexts? Should high assurance digital certificates be used for online dispute resolution or might their use decrease access to the dispute resolution platform? The issue of trade-offs between security and other concerns, such as privacy, ease of use and suitability of authentication was raised and discussed but it is not unique to the use of electronic signatures in a PKI and is currently being wrestled with by governments in relation to their delivery of services online.