Canadian Journal of Law and Technology

Volume 13 | Number 1 Article 6

1-1-2015

Signing Your Next Deal With Your Twitter @Username: The Legal Uses of Identity-Based Cryptography

Jillian Friedman

Signing Your Next Deal With Your Twitter @Username: The Legal Uses of Identity-Based Cryptography

Jillian Friedman[*]

I. INTRODUCTION

A multi-jurisdictional legal framework has been built over the past decade to regulate electronic signatures and their use in evidence and to validate legal writings. Technology innovates, and in the domain of signatures the potential of identity-based cryptography excites the technology industry and academic researchers.[1] For centuries, cryptography has been an important tool in political, military, and business communications to secure communication and protect the secrecy of a message.[2] Cryptography is premised on the use of algorithms and keys to encrypt and decrypt messages. Depending on the system, the same key can be used to encrypt and decrypt a message or there can be separate keys for encryption and decryption.

Digital signatures rely on cryptography, a method of hiding or scrambling the contents of a message. This scrambling or disguising is called encryption, the resulting encrypted message is a cryptogram or ciphertext, and the return of the ciphertext into plain text is called decryption.[3] Public key encryption or public key infrastructure cryptography (PKI) is a cryptographic scheme designed to solve the problem of establishing secure communication between two parties using a communication medium not under their exclusive control. Through a PKI scheme, both the recipient and the sending party have a distinct "key." The sender's key is used to encrypt the message and the recipient's is used for decryption. The concept of two separate keys as opposed to one was so innovative that it gave rise to a paradigm shift in cryptography.

---

[*] Author footnote information needed.

[1] For example, Sanjit Chatterjee & Palash Sarkar, *Identity-Based Encryption* (New York: Springer, 2011) [Chatterjee & Sarkar]; Dan Boneh & Matthew Franklin, "Identity-Based Encryption from the Weil Pairing" (2003) 32(3) Siam J of Computing 586; Wikipedia contributors, "ID-based cryptography," online: *Wikipedia, The Free Encyclopedia* <http://en.wikipedia.org/w/index.php?title=ID-based_cryptography&oldid=634978063>.The concept of IBC was first published in 1985, Adi Shamir, "Identity-Based Cryptosystems and Signature Schemes: in George Robert Blakley & David Chaum, eds, Advances in Technology, Vol. 196 (Spain: Spring Berlin Heideberg, 1985) 47-53 [Shamir]. Shamir is also an inventor of the RSA cryptosystem—one of the first practical public key cryptosystems and widely used today to securely transmit data.

[2] Chatterjee & Sarkar, *supra* note 1 at 1.

[3] Stephen Mason, *Electronic Signatures in Law* (3rd edn, Cambridge University Press, 2012), 261-263; 280 at 259.

The great potential of PKI for digital communications and signatures has yet to be seen, and this novel scheme is not without flaws. Cryptographers have struggled with the problem of attackers intercepting messages and replacing them. Though this research is concerned with the digital world, the challenge of authentication pre-dates the digital era. The question authentication poses is *how can a recipient know the message is from who it purports to be from?* PKI schemes attempt to solve the authentication problem through the use of Certification Authorities (CA), trusted third parties who determine and verify the identity of a party.[4] The many problems associated with CAs, to be discussed at length, are said to be the cause for the absence of widespread adoption of PKI schemes.[5]

Identity-based cryptography (IBC) was developed in response to problems associated with earlier PKI cryptographic schemes, namely those related to CAs and authentication. IBC schemes do away with the need for a CA to verify the public key and identity of a party by using the party's identity as a public key. IBC is a type of "public key encryption scheme where the public key of a user can be any arbitrary string — typically an e-mail address" where the sender of a message will encrypt the message using the email ID of the recipient as a public key. IBC is seen as a scheme that solves and simplifies the authentication problem in part, by obviating the need for a CA to verify the public key of the recipient.[6]

This article will look at the legal framework for electronic signatures under Canadian law and through the UNCITRAL Model Law on Electronic Signatures and evaluate the potential use of identity-based cryptography as a type of electronic signature. While most jurisdictions permit electronic signatures to replace their handwritten predecessors, the criteria of validity for an electronic signature range from liberal to restrictive. Public key infrastructure (PKI) cryptography schemes are considered to meet the juridical conditions of a legal signature under more rigorous legislation that requires an electronic signature to possess certain security attributes. In common law jurisdictions, digital signature schemes such as PKI have not been widely adopted in the private sector for use as secure electronic signatures. This may be due to the fact that they are difficult and awkward for the general public to use, rather than because of doubts surrounding certification authorities. This is not entirely the case in Europe and Latin America, where PKI digital signature schemes have been adopted by various governments programs. Case examples of PKI schemes include electronic identity cards issued by European governments such as Belgium's eID.[7] Though used by the government, the European private sector has widely neglected PKI electronic signature products. This is partly due to a lack of customer demand.[8]

---

4 Chatterjee & Sarkar, *supra* note 1 at 2-6.

5 Chatterjee & Sarkar, *supra* note 1 at 7.

6 Chatterjee & Sarkar, *supra* note 1, at 8.

7 See "The electronic identity documents," online: eID <http://eid.belgium.be/en/find_out_more_about_the_eid/the_electronic_identity_documents/>.

Increasingly, people rely on the internet to transfer hypersensitive information and digital assets. E-commerce continues to grow at a breakneck pace, relying on third-party service providers and payment products such as credit cards or payment processing services to provide security of data and to ensure that there is no fraud. A secure digital signature scheme that is user friendly may be a necessary ingredient for the success of nascent e-commerce industries. New forms of transferring value online, such as cryptocurrency, place much greater responsibility on the consumer or user to protect their assets and to militate against fraud. Now, more than ever, people are alive to the fact that their personal information, including email and bank account information, is not safe from hackers. Identity based cryptography (IBC) can be used to create digital signatures through a scheme that some believe has greater potential for mass adoption and is even more secure than PKI.[9]

Looking at the law of electronic signatures in Canada and the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures (2001), we will examine whether these laws permit digital signatures using an identity-based cryptographic process.

II. ELECTRONIC SIGNATURES AND THEIR LEGAL REQUIREMENTS

Not all contracts are required by law to be in writing. Unless otherwise stipulated, a contract is validly formed between parties so long as the requisite elements of offer, acceptance, intention to be bound, and consideration are present. However, even unsophisticated business actors take the issue of validity very seriously, and, as an ancillary, the validity of signatures. Furthermore, there are many different types of contracts that are required by statute to be in writing. Even though many types of contracts do not have requirements as to form in Canadian and international law, there is a predisposition in practice and in law towards recording the common intentions of the parties and endorsing it with a signature.[10] Unsurprisingly, most commercial transactions are reflected in some form of writing.

For a signature affixed or applied to a writing to be valid in Canadian common law, there are three conditions that it must possess. These are

---

[8] Heiko Robnagel and Jan Zibuschka, "Integrating Qualified Electronic Signatures With Password Legacy Systems" (2007) 4 Digital Evidence & Elec Signature L Rev 7; see also Aniello Merone, "Electronic signatures in Italian law" (2014) 11 Digital Evidence & Elec Signature L Rev 85.

[9] Daniel Cawrey, "Keybase Project Plans to Make Cryptography as Easy as Twitter", online: Coindesk <www.coindesk.com/keybase-project-plans-make-cryptography-easy-twitter/>; regarding the difficulties related to exchanging keys with the PKI scheme see Stephen Mason, *supra* note 3.

[10] Mark Lewis, "Digital Signatures : Meeting the Traditional Requirements Electronically — A Canadian Perspective" (2002) 2 Asper Rev of Int'l Bus and Trade Law 63-84 at 2 [Lewis].

authenticity, integrity, and non-repudiation. The same conditions must be present for a contract executed in electronic form.[11] History has demonstrated that a signature can manifest in many forms and serve many functions. This can also be said of electronic signatures, and it is therefore important to clarify what is meant by electronic signatures and to distinguish the different formats that electronic signatures can take. The term "electronic signature" broadly encompasses anything digital that can be used for the purpose of indicating that a signatory intended their signature to have a legal effect.[12] Even manuscript signatures that are scanned, stored on a computer, and later printed onto a cheque have been considered sufficient electronic signatures.[13] Other examples of electronic signatures include electronic sounds, typing a name in an electronic document, clicking the "I accept" icon to confirm intention to enter a contract, browse-wrap consent, and the use of personal identification numbers and passwords. All of these actions have been considered to be electronic signatures in various jurisdictions under legislation and case law.[14]

(a) Authentication, Integrity, and Non-Repudiation

One of the qualities of a handwritten signature is that it provides the authenticity of the person using the signature. Most statutes on electronic signatures require this feature, at a minimum.[15] Each person's signature is meant to be unique, like a fingerprint. In principle, no one else should be capable of re-creating the signature of an individual, though in practice we know that this is not the case. One of the criticisms of electronic signatures is that they are not inherently unique and can be easily copied. Anyone can type the name of a person in place of a handwritten signature, and we have no way of knowing if the person who typed the name was actually that person who has authority to sign the writing.[16] However, this has not prevented the widespread use of electronic signatures, such as those mentioned above, that are lacking in this aspect.

Putting this reality aside, for any electronic signature scheme to be practical it must be possible to have confidence in the identity of the signatory.[17] This step of providing assurance that an asserted identity is valid for a given person is referred to as authentication.[18] The authenticating function of a signature pre-

---

11 *Ibid* at 3.

12 Mason, *supra* note 3 at 190.

13 Mason, *supra* note 3 at 190, citing *Tedco Mgmt Svcs (PVT) Ltd. v. Grain Marketing Board*, 1996 (1) ZLR 109 (S.C.).

14 For a well-researched review of different forms of electronic signatures, the author recommends Mason, *supra* note 3.

15 Mason, *supra* note 3 at 1.

16 Lewis, *supra* note 10 at 4.

17 Lewis, *supra* note 10 at 4; TJ Smedinghoff, "Electronic Contracts & Digital Signatures: An Overview of Law and Legislation" (1999) 564 Prac L Inst/Pat, Copyrights, Trademarks, and Literary Prop 560 at 147 [Smedinghoff].

dates the electronic age. There are several ways to describe authentication and it has been the topic of much academic discussion.[19] One is "the process by which a person or legal entity seeks to verify the validity or genuineness of a particular piece of information."[20] Authentication is also the "formal assertion of validity, such as the signing of a certificate."[21] Authentication can also be applied to the need to verify identity. As Stephen Mason explains, the signature on a cheque serves to authenticate by associating the name of the person on the cheque with the person claiming authority to draw on the account named on the cheque.[22] Even before the use of handwritten signatures, various methods of authentication existed, such as the use of objects, the sign of the cross, seals, and witnesses.[23] A chief function of a signature is to authenticate the identity of the signatory. One of the main distinctions between public key encryption cryptography schemes and identity-based cryptography schemes is the authentication process.

Regardless of the technology used, signatures can have any number of functions besides authentication. Assuring the integrity of the writing is another important function of a signature. Signatures are used as evidence by providing proof that the signatory approves and consents to the contents of a document or writing.[24] The integrity of a writing can be broken up into several aspects and a distinction should be made between the text of a message and the identity and authority of the signatory. Integrity of the text of the message relates to whether the content of the message received is the same as the message that was sent.[25] Integrity of the signatory is concerned with whether a person can be identified as having affixed a signature to the message. Satisfaction of this component will depend on the purpose of the signature, which is determined by the writing itself.[26] There should be a high degree of inseparability between the instrument and the signature itself.[27]

The third crucial function of a signature is non-repudiation. From a legal perspective non-repudiation is the "assurance of the origin or delivery of data in

---

[18] Barry Sookman, *Computer, Internet, and Electronic Commerce Law*, Chapter 10: Electronic Contracting, (Toronto: Carswell, 2014), at p 2 [Sookman].

[19] See, for further discussion, Mason, *supra* note 3.

[20] Mason, *supra* note 3 at 1.

[21] Mason, *supra* note 3 at 1.

[22] Mason, *supra* note 3 at 2.

[23] Mason, *supra* note 3 at 15.

[24] Mason, *supra* note 3 at 9.

[25] *Ibid.*

[26] Mason, *supra* note 3, referencing D Bruce Farrend, "Policy Considerations Behind Legislation Recognizing Electronic Signatures 1998", online: Uniform Law Conference of Canada < http://www.ulcc.ca/en/1998-halifax-ns/395-civil-section-documents/364-policy-considerations-behind-legislation-recognizing-electronic-signatures-1998 > .

[27] Lewis, *supra* note 10 at 4.

order to protect the sender against false denial by the recipient that the data has been received, or to protect against false denial by the sender that the data has been sent."[28] However, this definition is incorrect with respect to how it is used by technicians and cryptographers to whom "nonrepudiation provides proof of the integrity and origin of data that can be verified by a third party."[29] The difference, though nuanced, is important because there does not necessarily need to be technical non-repudiation in the form of a sophisticated IT system for a legal sense of non-repudiation to be met. Moreover, the presence of a non-repudiation feature of a certain cryptographic scheme will not always provide for non-repudiation in a legal sense. From a software engineering perspective, non-repudiation is the binding of users and identities to specific actions such that denial of the user demonstrates either deception or a failure to secure their private key. In the legal context, there are a number of scenarios where a signature can be repudiated. One example would be where a person's username or password is hacked. Just because a message is received from a username does not mean that it was sent by the person associated with that username.[30] Similarly, manuscript signatures can be disputed on the basis of being forged, or having been executed through fraud, error, or duress. Digital signatures provide non-repudiation insofar as they confirm that a message was signed by a private key. They do not necessarily prove that the individual who signed the key was the individual alleged to control or have authority over that key.

The signature, manifested through different technologies over centuries, continues to hold the same important functions as ever.[31]Whereas the above-mentioned criteria of authenticity, integrity, and non-repudiation are based on the practice of applying a signature by putting ink to paper, the same purpose can be achieved by applying an electronic signature to a document by a process.[32]

As mentioned, there are many forms of electronic signatures that may not meet the above-mentioned criteria and yet are still recognized as valid signatures. Take, for example, the act of typing a name in an electronic document. This action does little to prove that the signature belongs to the party with the authority to sign. Despite this, some American jurisdictions have confirmed that the act of typing a name into a document on screen has been considered an acceptable method of proving the intent of the signing party.[33] Typed signatures in email communications have also constituted signatures for the purpose of

---

[28] Lewis, *supra* note 10 at 4; Electronic Commerce and Information Technology Division Section of Science and Technology, Information Security Committee Digital Signature Guidelines (DSG), Legal Infrastructure for Certification Authorities and Secure Electronic Commerce (American Bar Association 1995, 1996) at 8 [ABA].

[29] Mason, *supra* note 3 at 319.

[30] Ibid.

[31] Mason, *supra* note 3 at 1.

[32] Donnie L Kidd, Jr & William H Daughtrey, Jr, "Adapting Contract Law to Accommodate Electronic Contracts: Overview and Suggestions" (2000) 26 Rutgers Computer & Tech LJ 215 at 253.

certain juridical acts, such as the termination of a lease.[34] Different types of electronic signatures have been found to be valid in a variety of legal contexts, including writings evidencing interest in property,[35] commercial contracts,[36] and the relevant writing under the Statute of Frauds.[37] The validity and probative force of an electronic signature is evaluated in light of the form used, the nature of the juridical act to which the signature is affixed, and all the surrounding evidence. This is where technical and legal perceptions as to the trustworthiness of an electronic signature diverge.

For technicians, there is a lack of trustworthiness associated with various electronic signature forms as they fail to satisfy the technical criteria of authentication, integrity, and non-repudiation. Different technical procedures exist to ensure the three elements of authentication, integrity, and non-repudiation. These include processes to "apply" an electronic signature in order to overcome a perceived absence of the trustworthiness that exists with paper-based signatures. These techniques or methods verify, from a technical perspective, that an electronic signature or record is that of a specific person or will "detect error or alteration in the communication, content, or storage of an electronic record since a specific point in time."[38] What is known as a digital signature is the procedure that is most widely used.

III. DIGITAL SIGNATURES

A form of electronic signature, a digital signature is a "mathematical scheme for demonstrating the authenticity of a digital message or document."[39] According to Mason, a digital signature is "data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data to prove the source and integrity of the data unit."[40] Cryptographic-based digital signatures function to provide, from a technical point of view, authenticity, integrity, and non-repudiation.[41] Often, digital signatures use what is called public key infrastructure to sign a message or document.

---

[33] Mason, *supra* note 3 at 193; see *Uniform Electronic Transactions Act*, s 2(8) definition of electronic signature, Official Comment 7.

[34] *Crestwood Shops, L.L.C. v. Hilkene*, 197 S.W.3d 641 (Mo. App. W.D., 2006).

[35] *Faulks v. Cameron*, [2004] NTSC 61, 32 Fam. L.R. 417 (Northern Territory S.C.).

[36] *Computer Sky Edv. v. Prime Medical Company Ltd.* (August 4, 2005), Doc. 29488/04 (Tel-Aviv Peace Court); Mason, *supra* note 3 at 197.

[37] *Polyad Company v. Indopco Inc.*, 2007 WL 2893638 (N.D. Ill. E.D., 2007); *Leoppky v. Meston*, 2008 ABQB 45, 2008 CarswellAlta 60 (Alta. Q.B.); *Golden Ocean Group Ltd. v. Salgaocar Mining Industries Pvt Ltd.*, [2012] 3 All E.R. 842 (Eng. C.A.).

[38] Lewis, *supra* note 10 at 5; Smedinghoff, *supra* note 17 at 144.

[39] David J Bilinsky, "Signed, sealed and delivered. . .online" (2006) 26:24 *The Lawyers Weekly*.

[40] Mason, *supra* note 3 at 189.

[41] Mason, *supra* note 3 at 259.

(a) Public/Private Key Infrastructure

Asymmetric cryptosystems, referred to as public key encryption, or public key infrastructure (PKI) are security infrastructure with a number of components and services.[42] PKI was developed to facilitate secure communications between numerous untrusted parties. It is distinct from symmetric cryptosystems, whereby parties share the same key for encryption and decryption—such systems are used by banks and their customers through a personal identification number (PIN).[43] Symmetric cryptographic systems are best suited for closed user groups with a strong degree of trust, as the senders and recipients use the same key. One of the weaknesses of a symmetric cryptosystem is that the security of the entire system depends on the secrecy of the secured shared key.[44]

It is important to understand the basic concepts of PKI in order to evaluate their legal classification. Cryptography in general operates by processing data in the form of binary digits and performing functions on this data. This tool allows for data, such as secret messages, to be transformed into an alternate representation that is unique to the original message.[45] Traditional digital signature methods involve two keys assigned to the signing party: a public key and a private key. The public key is the key used to identify the individual. The private key is held by the individual party and must not be shared or disclosed. Using their private key, a signatory encrypts their signature. The result is a digital signature. The recipient of the encrypted message uses the public key to decrypt the message (or signature). Only the public key can unscramble the encrypted message.

Two algorithms are used to create a digital signature: a hash algorithm and a signature algorithm. The hash function is an "algorithm which creates a digital representation or 'fingerprint' in the form or a 'hash value' or 'hash result' of a standard length which is usually much smaller than the message but nevertheless substantially unique to it."[46] This formula is sent to the recipient. Each message has a specific hash value such that if the original message were to be modified, the hash value would necessarily change. The hash function is applied to the original message to create a resulting set of data—a set of digits unique to the message—called a message digest. The signature algorithm, also referred to as the private key, is applied to the message digest and creates the digital signature.[47]

---

[42] Carlisle Adams & Steve Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations*, 2nd ed (Boston: Addison-Wesley, 2003) at 35.

[43] For a more detailed description of PKI and public/private keys see Carlisle Adams & Steve Lloyd, *ibid;* Bruce Schneier, *Applied Cryptography Protocols, Algorithms, and Source Code in C,* 2nd ed (Indiana: Wiley Publishing, 1996); Niels Ferguson and Bruce Schneier, *Practical Cryptography* (Indiana: Wiley Publishing, 2003).

[44] Mason, *supra* note 3 at 261.

[45] Lewis, *supra* note 10.

[46] ABA, *supra* note 28; Lewis, *supra* note 10 at 6.

When these algorithms are applied, the message changes. The recipient of the digital signature decrypts the message with the public key. When a public key is applied to a digital signature it gives a message digest that is identical to the message digest produced by the hash function to the original message.[48] Put simply, a message is encrypted with the private key and decrypted with the public key by the recipient. If the message is changed or altered in any way, it will be known because the hash value will change. The following is an example of a message sent using public key cryptography:

(a) David and Joseph want to exchange encrypted messages.
(b) David generates a public and private key with a software on his computer and gives Joseph the public key. David keeps his private key a secret.
(c) Joseph writes a message and encrypts it using David's public key, and sends it.
(d) David decrypts Joe's message using his private key.[49]

The relative strengths and weaknesses of different types of cryptography-based digital signatures will depend on how a particular system, its algorithms, and its ciphers work.[50] From a technical point of view, digital signatures generated through a PKI scheme by design satisfy most of the functions of a traditional handwritten signature with one exception. There is no way to be sure that the holder of the private key that signs the encrypted message is who he says he is. These problems emanate from how a person creates and controls their keys. It is possible for a message between parties to be intercepted, modified, or deleted if a third party intercepts a public key exchange and imposes himself as one of the parties. PKI uses certification authorities, also called the "Web of Trust" to solve this dilemma.[51] As will be discussed, this model leaves much to be desired.

(i) Certification Authority

In order for people to believe that your public key belongs to you, you can upload it to a key server and have other trusted people, often referred to as certifying authorities (CA), sign it with their own keys.[52] The role of the CA is to certify the correspondence or association between a public key and the alleged owner of the associated private key by digitally signing a certificate. The certificate issued by the certification authority will identify the certification authority, identify the subscriber and the subscriber's public key, and be signed with the CA's private key.[53]

---

47 Lewis, *supra* note 10 at 6.

48 *Ibid.*

49 Example derived from Mason, *supra* note 3 at 263.

50 Mason, *supra* note 3 at 261.

51 Klint Finley, "OkCupid's Founders Want to Bring Encrypted Email to the Masses" online: *Wired* < http://www.wired.com/2014/04/keybase/ > [Finley].

52 An example of this is the MIT PGP Public Key Server, online: < https://pgp.mit.edu/ > .

CAs must be trusted to play such an important role.[54] When verifying that a signature comes from the person it is supposed to, a recipient can check to see if a trusted CA has signed the person's authentication certification. A recipient can even verify one step further and check that a trusted CA has signed the certification of that trusted CA.[55] Certifying authorities are used to ensure that an assigned digital signature belongs to who it is supposed to. This service is necessary for the PKI method to be truly "trustworthy" and to achieve the authentication requirement. A sender will send their signed message as well as the CA certificate with their message, and both the digital signature of the sender and that of the CA can be verified.

Many are of the view that a digital signature using the above-described PKI methods with successful authentication ensures the integrity of the corresponding message and signature.[56] By certifying the connection between a person or legal entity and their public key the CA adds confidence that the associated signatory actually signed the message.[57] For this reason, digital signature schemes using PKI are commonly used to meet the legal requirements for electronic signatures under stricter electronic signature laws.

Important challenges resonate with relying on trusted third-party certification authorities. Though certain bodies, such as the European Telecommunications Standards Institute, have set out the requirements that a CA should comply with when confirming the identity of a person or entity, it is not always clear what the obligations of certification authorities are in connection with the issuance of digital certificates.[58] Furthermore, certification authorities can issue false certificates if their identity verification is not rigorous enough.[59]

A critical analysis of digital signatures would not be complete without returning to the important nuances between the technical and legal concepts of non-repudiation as they apply to digital signatures. PKI digital signatures are perceived to provide greater security than other electronic signature schemes. Because of this apparent security, a subscribing party is convinced to take responsibility for every use of their private key, thus attributing to the system a non-repudiation property. This non-repudiation element is somewhat misleading from a legal perspective. While the system does assure that a certain message was signed with a certain private key, the subscribing party is not immune from

---

53 Mason, *supra* note 3 at 264.

54 Christoph Sorge, "The Legal Classification of Identity-Based Signatures," University of Paderborn, Germany, online at: Cryptology ePrint Archive <https://eprint.iacr.org/2013/271.pdf> [Sorge].

55 Finley, *supra* note 51.

56 Lewis, *supra* note 10.

57 Sorge, *supra* note 54; Lewis, *supra* note 10; Mason, *supra* note 3 at 265.

58 Mason, *supra* note 3 at 275; Sookman, *supra* note 18 at 2.

59 For more details see Mason, *supra* note 3 at 274-284.

attacks that would result in theft or misappropriation of the private key, or corruption of the computer terminal that is used to sign with the private key.[60]

Email is susceptible to fraud and hacking and it always has been. Over the last few years businesses and individuals have grown aware of the fact that their email is less secure than previously thought. PKI is a potential solution to these security weaknesses. A private key can be used to "sign" messages to provide proof it was really you that signed them. In business transactions among small and medium enterprises it is normal to use email to communicate and negotiate terms and conditions of important commercial agreements. However, PKI is not widely used to encrypt messages and sign documents outside of the cryptographer enthusiast world because it is hard to use. It is difficult to keep your private key safe and the consequences of a hacker taking your private key and impersonating you can be grave, especially because of the implied non-repudiation that accompanies use of a digital signature scheme. The other problem relates to the public key, which is necessary to know in order to send a message to someone. The scheme is impractical because we cannot encrypt our signature without knowing the public key of the recipient—which is a long string of data bits and impractical to remember. Take note, however, that not all digital signature schemes are the same and certain methods are of great interest in the cryptography and business world, not least because they may be easier to adopt than the PKI signature schemes.

(b) Identity Based Cryptography

The necessity of the CA to authenticate in digital signature schemes has been much maligned.[61] However, not all cryptographic signature schemes involve a CA. Thirty years ago, world-renowned Israeli cryptographer Adi Shamir presented an idea called identity based cryptography (IBC).[62] This cryptographic-based solution partially solved the problem of retrieving certificates and public keys that are required with the PKI model.[63] The IBC scheme, wrote Shamir, enables "any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party."[64] The scheme requires the existence of trusted key generation centers that exist uniquely to give each user a personalized "smart card" or key when they join the network, thus eliminating the need for a CA.[65] The "smart card" allows a user to sign and encrypt messages, including signatures, and to decrypt and verify the messages he receives.

---

[60] Mason, *supra* note 3 at 266.

[61] Lewis, *supra* note 10 at 2; Sookman, *supra* note 18 at 2; Mason, *supra* note 3 at 274-284.

[62] Shamir, *supra* note 1.

[63] Sorge, *supra* note 54 at 2.

[64] Shamir, *supra* note 1 at 47.

[65] *Ibid.*

There are two powerful ideas behind IBC that are germane to electronic signatures in the age of online commerce. The first is that the IBC system does not generate a random pair of public/private keys and then publishes one of them (the public key). Rather, the user chooses his name and network address as his public key. The name and network address used can be anything. Shamir, writing before social media, explained a user can use "any combination of name, social security number, street address, office number or telephone number."[66]

Today what this means is that a person can use their social media accounts—such as a Twitter or Facebook profile—an email address, and even certain biometrics as their public key. This makes it extremely easy for anyone to find them and communicate with them. In the world of e-commerce, the linking of one's identity to their social media profiles has become an accepted practice.[67] It is commonplace to open an account online and have the option of signing in with your Twitter or Facebook account. This scheme simplifies the cryptographic elements of electronic signatures because it can be used and understood by people who know nothing about cryptographic protocols.[68]

The second disruptive idea with the IBC scheme is also derived from the use of personally identifying information as a public key. The identity-based scheme links the message with the identifying information of the user and ownership of the "smart card" ties it to the physical user. The key criteria for which personal information is used is that the information "identifies the user in a way he cannot later deny, and that it is readily available to the other party."[69] Thus, a degree of non-repudiation is available. The IBC scheme answers the quagmire as to how to prove that a person sending a message is who he says he is by requiring their public key to be associated with their online identity. For example, a person with a Facebook account who posts comments and personal photos and interacts with connections cannot easily claim that this Facebook profile is not theirs. The recipient of the message would just as easily be able to verify that the person is who he says he is by checking the identifying information. Current services experimenting with IBC cross-verify the identity of the user in different ways, one of which is requiring a user to post a tweet linking back to their IBC user profile.[70]

This IBC scheme is no panacea and is not above security failures. If a person's online identity is completely taken over, then legal non-repudiation is compromised. One security advantage of IBC that militates against impersonators is that the attacker would have to infiltrate a number of social identities of a specific person, such as their Facebook, Twitter, and LinkedIn account. It would be more difficult, though not impossible, for the attacker to

---

66 Shamir, *supra* note 1 at 47.

67 One example is Pinterest.

68 Cawrey, *supra* note 9.

69 Shamir, *supra* note 1 at 47.

70 Cawrey, *supra* note 9.

keep up the façade that they are the individual whose account they have taken over because they would have to maintain the authenticity of their victim through posts and photos that purport to be from the legitimate account holder.

Shamir wrote that the IBC scheme can even be used by countries as the basis for a new type of personal identification cards with which everyone can sign cheques and legal documents electronically. Identity-based cryptography schemes are similar to sending mail by the post—you can send someone a message if you know their name and address and, in principle, only the recipient can read the letter addressed to him. For example:

(a) Joseph wants to send a message to David.
(b) Joseph signs the message with his private key and then encrypts it by using David's name, which could be his Twitter username, and network address.
(c) Joseph then adds his name and network address to the message and sends it to David. Upon receipt of the message, David decrypts it using his secret key. David himself can verify Joseph's signature by using Joseph's name and network address as a verification tool.[71]

One might argue that IBC does not completely eliminate the need for a trusted third party; it simply shifts this trust to another party, a Private Key Generator (PKG). This is an important distinction from PKI. With an IBC scheme, private or secret keys are computed by a private key generation center instead of by users themselves. The reason for this is because if users could generate their own private keys, as is done with PKI schemes, user Allison could generate a private key corresponding with the public profile of Allison, but she could also generate one for the public profiles of Pamela and Kayla. The Private Key Generator generates all the private keys for users in a network. The PKG possesses privileged information, such as the algorithms that enable it to compute the secret keys. The PKGs are also responsible for thoroughly checking the identity of a person before issuing "smart cards" or registrations to the user. Users must also take care to prevent loss, duplication, or unauthorized use of their cards.[72] Notably, the PKGs role is a one-off; once the keys are generated there is no need for a PKG and their utility ceases to exist. This is different from certification authorities that must always stay vigilant and sign certificates and will thus always be a cost of using the PKI system.

Real-life examples of IBC include Keybase.io, a website as well as an open source command line program that uses the IBC scheme. It is a service that allows users to obtain a public key using their social media profiles. The site is an online directory that lets a user instantly locate someone online and trade the information needed to allow them to send private encrypted messages to each other.[73] Instead of the "Web of Trust" system that requires reliance on trusted

---

[71] Shamir, *supra* note 1 at 48.

[72] Shamir, *supra* note 1 at 48.

[73] Finley, *supra* note 51.

CAs, Keybase verifies the identity of the key holder by using the social Internet as a cross-referencing tool.[74] By placing your public key "signature" on your blog or twitter account, you can prove ownership of the key. This system is much harder to hack, as it would also require hacking all the social media and websites associated with that individual. As long as a sender is confident that a twitter account belongs to and is controlled by the person they are looking for, they can have confidence in the signature associated with that name. It allows users to search for others and will provide search results linking to someone's social media usernames, such as their Twitter username. By putting the social media username into a command line, the program will confirm the public key is owned by the associated Twitter user. Keybase can also provide the public bitcoin address associated with the person, which is signed by her private key.[75] The service is still in its alpha phase but has generated excitement about the use of identity to promulgate the popular adoption of cryptographic-based signatures.

The PKI and IBC techniques differ in how they go about authenticating the identity of the holder of a key pair. These cryptographic approaches must be understood from a legal perspective in order to determine whether and how different types of digital signatures can be considered under different legal classifications of electronic signatures.

IV. LEGAL CLASSIFICATION OF IDENTITY BASED CRYPTOGRAPHIC SIGNATURES

Laws that address electronic signatures attempt to articulate what constitutes a legal signature in the age of the Internet and all things digital. Most legal definitions of an electronic signature are purposefully vague and do not refer to any cryptographic scheme to achieve validity because they are technologically neutral. Therefore, under these broad strokes definitions, an identity-based crypto-signature will usually qualify as an electronic signature. However, some legislation is more specific as to its classification of electronic signatures, and it is these more rigorous specifications that are of interest. The legislative approaches to electronic signatures can be divided into three categories: technology neutral; semi-specific; and those requiring use of a digital signature by cryptographic means.[76] Another categorization describes these approaches as prescriptive, minimalist, and two-tier.

Technology neutral statutes are broadly worded so as to give legal effect to any electronic signature. These laws leave it to the courts to determine the probative value of an electronic signature based on the security of the technology used.[77] An example is the United States federal law entitled the *Electronic Signatures in Global and National Commerce Act (E-SIGN Act)*. The *E-SIGN*

---

[74] Finley, *supra* note 51.

[75] *Ibid.*

[76] Lewis, *supra* note 10 at 9.

[77] *Ibid.*

Act regulates the legal effect of electronic signatures in interstate and foreign commerce. This law defines an electronic signature as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[78] This minimalist approach has been widely adopted in common law jurisdictions.[79]

Semi-specific statutes provide specifications as to the security attributes that a valid electronic signature must have without requiring use of a particular technology. However, the semi-specific statutes often require security attributes found with PKI schemes.[80] The third category of laws requires the use of PKI digital signatures and usually in these cases the government is involved in creating the certifying authority. For example, Latin American states have licensing systems for certification authorities.[81]

(a) UNCITRAL

For many countries, the legal approach to understanding electronic signatures is the UNCITRAL Model Law on Electronic Signatures (2001) (UNCITRAL Model).

According to the UNCITRAL Model an electronic signature is:

> "data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message".[82]

UNCITRAL provides that the requirement to provide a signature is met if the electronic signature used is "as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement."[83] Reliability of the signature is achieved if:

(a) The *signature creation data* are, within the context in which they are used, *linked to the signatory and to no other person*;

---

[78] Section 106, *Electronic Signatures in Global and National Commerce Act*, Pub. L. 106-229, US Congress, (2000).

[79] Mason, *supra* note 3, pp. 153-186; Stephen E. Blythe, "Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security" (2005) 11 Rich JL & Tech, 2 [Blythe].

[80] Blythe, *ibid.*

[81] Mason, *supra* note 3, at 174; see also Blythe, *supra* note 79; W Everett Lupton, "The Digital Signature: Your Identity by the Numbers" (1999) 6 Rutgers JL & Tech 10 at 35.

[82] Article 2(a), *UNCITRAL Model Law on Electronic Signatures adopted by the United Nations Commission on International Trade Law*, (2001), A/56/588, online: <http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf> [UNCITRAL].

[83] Article 6(1), *ibid.*

(b) The signature creation data were, at the time of signing, *under the control of the signatory and of no other person*;
(c) Any *alteration to the electronic signature*, made after the time of signing, is *detectable*; and
(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any *alteration made to that information* after the *time of signing is detectable*.[84] [emphasis added]

The concept of an electronic signature under UNCITRAL requires that the technology is able to identify the signatory.[85] This is another iteration of the authentication requirement. Similar to PKI, there is no inherent identity authentication feature with IBC signatures since the public key can technically be associated with any arbitrary text or identity information.[86] Nonetheless, with IBC the sender's full name and other personally identifying information can be associated with their identity, as this data is their "public key." It is possible to identify the signatory insofar as it is possible to identify the individual by their Twitter and Facebook account that they use as the public key. Therefore, it is likely that an IBC electronic signature can satisfy the identity condition of a basic electronic signature under the UNCITRAL definition.

Paragraphs (*c*) and (*d*) of the UNCITRAL definition of a reliable signature stipulate that the scheme used must ensure that any alteration to the electronic signature and the contents of the message must be detectable.[87] This is necessary to assure the integrity of the document. This requirement is fulfilled by both the PKI and IBC schemes because this quality is intrinsic to any cryptographic signature scheme.[88] As mentioned above, the hash value that encrypts messages is unique to the specific message and signature encrypted. If the original message, including the signature, were to ever be modified, even by one character, the hash value would necessarily change and render the alteration detectable. This feature is present with both PKI and IBC cryptography schemes.

A *reliable electronic signature* requires a mapping or linking between the signature and identity of the signatory that is unique to that person and solely controlled by him. Article 6(3)(a)(b) of the UNCITRAL Model provides:

> An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:
>
> (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

---

84 Article 6(3), *ibid.*

85 Article 2(a), *ibid.*

86 Sorge, *supra* note 54 at 6.

87 Article 6(3)(c)(d), UNCITRAL, *supra* note 82.

88 Shamir, *supra* note 1.

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person[89].

A simple scan of a handwritten signature will not suffice as a reliable electronic signature because we have no way of knowing who actually signed it.[90] Nor is the legal requirement to link to identity a readily available function of the general framework of cryptographic signature schemes. With a PKI scheme this requirement is fulfilled by the CA, and by the linking to verified personal identifying information with an IBC scheme.

An important part of the reliable electronic signature category is the concept of "sole control." The UNCITRAL Model requires that a reliable electronic signature be under the sole control of the signatory. Specifically, the signature creation data must be, at the time of signing, under the control of the signatory and of no other person.[91] This means that for an IBC signature system, the private key must stay in the control of the user. The same applies to a PKI scheme. There is a human element to this requirement that technical sophistication cannot eliminate. If a person loses or shares their private key information with others then they are no longer in sole control of their private key, which is part of the signature creation data. However, like other cryptographic schemes, IBC provides the signatory with the ability to exclude anyone else from signing.[92]

Several authors have identified problems associated with the "sole control" concept, which directly relates to the security of signature creation.[93] From a technical perspective, sole control implies that the signatory can prevent others from using his signature creation data. In his legal analysis of IBC signatures, Dr. Christoph Sorge rightly points out that IT systems are far too complex to guarantee from a technical perspective that security measures are never circumvented.[94] Note that the UNCITRAL Model definition does not require that the signature creation data be *created* by the signatory. Therefore, the signatory does not necessarily have to generate the valid signature or private key, only exclusively control it. If it were required that the signatory generate the private key which he subsequently controls, then IBC would not be a valid form of reliable electronic signature because the private keys are generated by a PKG and not the signatory.[95]

If the "sole control" provision is to apply to the general cryptographic scheme as well as the overall security of the context, then a cryptographic scheme would have to be structured in a way so that *only* the legitimate signatory can

---

89 Article 6(3)(a)(b), UNCITRAL, *supra* note 82.

90 Sorge, *supra* note 54 at 4.

91 Article 6(3)(b), UNCITRAL *supra* note 82.

92 Sorge, *supra* note 54 at 9.

93 Sorge, *supra* note 54 at 9; Mason, *supra* note 3 at 123.

94 Sorge, *supra* note 54 at 9.

95 Sorge, *supra* note 54 at 11.

generate a valid signature. This requirement articulates the subtle difference between traditional PKI signature schemes and identity-based cryptographic schemes. If the PKG is a central authority that generates the key, then it may also be the case that a PKG can generate signatures for any identity. The existence of the PKG may leave open the possibility for another person, other than the original signatory, to sign messages valid for the same identity.[96] This scenario would fail under the sole control test. If this were the case, IBC signature schemes could not generate signatures that meet the reliable electronic signature requirements under the UNCITRAL Model. Note that the notion and requirement of sole control presents itself differently depending on the legislation, and the analysis with respect to different digital signature schemes, will vary accordingly. Furthermore, an IBC digital signature scheme would likely still be considered an electronic signature under the more liberal definitions cited above, such as the *E-Sign Act*.

Dr. Sorge rounds out concerns related to "sole control" and the PKG in several ways. One relies on the general liability rules of civil law. Just as is the case with certification authorities who can also generate new keys pairs and corresponding identities, there are serious legal liabilities for the PKG or CA who act with negligence or malevolence. In order to comply with this element of the law, the PKG must be able to delete its records of the private keys it generates.[97] If a PKG can delete the key immediately after giving it to the subscriber and if it cannot subsequently re-generate the key, then the signatory truly has "sole control," at least in a technical sense. The scheme must be structured in a way that the PKG is never able to retrieve or regenerate the private keys it created. According to the literature there are a number of identity-based cryptographic schemes that achieve the criteria of sole control of the private key using different techniques.[98] Finally, there must be a way to distinguish between signatures generated by the PKG and those generated using an original private key given to the subscriber. Sorge goes on to discuss a number of other workable technical solutions that help put the concern about "sole control" to rest.[99]

Even secure cryptographic schemes are vulnerable to what is referred to as a "key substitution attack." This is when a second public key is generated which links to a second entity but for which the same private key signature will be valid.[100] In this case person B can create another public key associated with person C but which person B really controls via his private key. One prevention tool for this is the use of certification authorities to include with the message to

---

[96] Sorge, *supra* note 54 at 8.

[97] Note that the provisions of the UNCITRAL Model Law only apply if a jurisdiction adopts the Model Law.

[98] Sorge, *supra* note 54 at 11.

[99] Sorge, *supra* note 54 at 10.

[100] Sorge, *supra* note 54 at 7.

be signed. For an IBC scheme, as Sorge explains, "a successful key substitution attack on an identity based signature scheme implies that a signature is valid for more than one identity; an attacker could thus retrieve the private key of one identity and, via the key substitution attack, get a second identity for which the signature is valid."[101]

At the risk of being overly technical, resisting attacks of the nature of the key substitution attack are part of the design objectives of identity-based signature schemes and the problem is the same, if not greater, with PKI. With PKI, a dishonest CA can impersonate a user by generating a certificate binding that users' identity information with the newly generated secret key.[102]An identity-based signature is linked to the identity of the signor through data that only belongs to the signor, like their phone number and social media account. This link is authenticated by the PKG. In the same sense that a CA could impersonate users, it is within contemplation that the PKG might generate another person aside from the original signatory with the ability to sign messages valid for the same identity.[103] Assuming the PKG is not malevolent, and does not assign the same private key to more than one signatory, the link to the signatory requirement under the UNCITRAL Model is met. Furthermore, technical solutions to this challenge are within the realm of possibility.

From this preliminary analysis it is possible to conclude that identity-based signature schemes are capable of fulfilling the requirements of a "reliable electronic signature" as defined in the UNCITRAL Model. In his paper, which focused on the European Union and Germany, Sorge arrives at the same conclusion by way of analysis of the European Signature Directive requirements for advanced electronic signatures, which is a more restrictive set of criteria.[104]

(b) Canada (PIPEDA)

In Canada, private law matters are the jurisdiction of the provinces but, as certain federal laws also address electronic signatures, the area has a double aspect.[105] Canadian law falls within the technology neutral and semi-specific electronic signature law classifications. This policy approach is criticized by some as putting unneeded pressure on the courts and the private sector to determine which technology provides adequate security for an electronic signature to have evidentiary value.[106] However, an advantage of this legislative strategy is that is leaves room for technological innovation that might otherwise be barred by overly-specific legislation.

---

[101] Sorge, *supra* note 54 at 7.

[102] Xiaofeng Chen, Fangguo Zhang, and Baodian Wei, "Comment on the Public Key Substitution Attacks" (2005) 1(3) International Journal of Network Security 168.

[103] Sorge, *supra* note 54 at 8.

[104] Sorge, *supra* note 54 at 12.

[105] *The Constitution Act*, 1867, 30 & 31 Vict, c 3, s 92.

[106] Lewis, *supra* note 10 at 9.

Most Canadian provincial and federal legislation that defines an electronic signature are substantially similar as they are drawn from the same source, the Uniform Electronic Commerce Act (UECA) prepared by the Uniform Law Conference of Canada in 1998 to implement the principles of the UNCITRAL Model.[107] An electronic signature is defined in Ontario's *Electronic Commerce Act* as "electronic information that a person creates or adopts in order to sign a document and that is in, attached to or associated with the document."[108] These provisions allow for any method to be used to electronically "sign" a document, and do not necessarily require a cryptographic scheme to achieve validity. This is interpreted to mean that any electronic activity that is intended by the signatory to be a signature will be considered as such.[109] Therefore, we can safely posit that a signature based on IBC would meet the definition of electronic signature under most Canadian provincial laws. Note, however, that the province of Quebec has a different approach to electronic signatures. As such, Quebec law as it pertains to electronic signatures has not been analyzed herein.

As mentioned, Canadian laws do not explicitly require the use of a specific digital signature technology for an electronic signature to be valid. The probative value of these signatures is left to the courts to evaluate. This is distinct from the approach taken by some European laws such as Germany's *Signature Act*, which specifically requires certain digital schemes in order to achieve legal validity for some electronic signatures.[110] One place where Canadian law is semi-specific as to the technology required is the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), which distinguishes between an electronic signature and a secure electronic signature.[111]

Article 31 of PIPEDA provides a definition of a secure electronic signature which implicitly requires the use of digital signature technology.[112] Under PIPEDA a secure electronic signature "means an electronic signature that results from the application of a technology or process prescribed by regulations made under subsection 48(1)."[113] Section 48(1) states:

---

[107] *Uniform Electronic Commerce Act*, Uniform Law Conference of Canada 2011, online: < http://www.ulcc.ca/en/uniform-acts-new-order/older-uniform-acts/703-electronic-commerce/1793-uniform-electronic-commerce-act-consol-2011 > .

[108] *Electronic Commerce Act,* SO 2000 c 17.

[109] Lewis, *supra* note 10 at 10.

[110] Germany's Signature Law is based on the European Directive (Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures) which classifies 4 types of electronic signature, some of which require cryptographic schemes. See *German Signature Law* of 2001, online: < http://www.gesetze-im-internet.de/sigg_2001/index.html > .

[111] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 31. [PIPEDA].

[112] Schedule 2 and 3, *PIPEDA*, *ibid.*

[113] *PIPEDA*, *ibid.*

> **48.** (1) Subject to subsection (2), the Governor in Council may, on the recommendation of the Treasury Board, make regulations prescribing technologies or processes for the purpose of the definition "secure electronic signature" in subsection 31(1).
> Characteristics
> (2) The Governor in Council may prescribe a technology or process only if the Governor in Council is satisfied that it can be proved that
>
> (a) the electronic signature resulting from the use by a person of the technology or process *is unique to the person*;
> (b) the *use of the technology* or process by a person to incorporate, attach or associate the person's electronic signature to an electronic document is *under the sole control of the person*;
> (*c*) the technology or process *can be used to identify the person* using the technology or process; and
> (*d*) the electronic signature can be linked with an electronic document in such a way that it *can be used to determine whether the electronic document has been changed since the electronic signature was incorporated* in, attached to or associated with the electronic document.[114]

The characteristics that a technology or process would have to possess for a valid secure electronic signature under PIPEDA are the same as those provided by public key encryption, or PKI.[115] We will now examine whether the characteristics of identity-based cryptography are also within the scope of the PIPEDA definition of secure electronic signature.

The first requirement is that the signature must be unique to the user whose identity is associated with the signature. This requirement is somewhat similar to that of UNCITRAL's Model Law article 6(3)(a) which requires that there be a link between the signatory and the signature (or signature creation data), which must be exclusively controlled by the signatory. Barring any key substitution attack, as discussed above, in principle, the private key generated by the PKG should be exclusively associated with the signatory's public profile or personally identifying information. In fact, IBC facilitates this by relying on the individual signatory's personal information to create a public key profile. In practice, PKGs should not generate the same private key twice. Most IBC schemes rely on a secure random number generator to generate private keys. While it is theoretically possible to accidentally generate the same key pair for two persons, this likelihood is negligible.[116] The PIPEDA definition is less strict than that of UNCITRAL as it does not appear to require that the signature creation data be exclusively linked to the signatory, just that it be unique to the signatory. This seems to impose less restrictive obligation on the PKG vis-à-vis the

---

[114] Section 48(1), *PIPEDA*, *ibid.*

[115] Lewis, *supra* note 10 at 12.

[116] Sorge, *supra* note 54 at 8.

destruction of the private keys it generates. As with the UNCITRAL Model Law, IBC satisfies this requirement by generating only one private key to pair with a person's identity profile.

The signatory must have the sole control of the technology used to associate a signature to an electronic document.[117] In the case of PKI and IBC crypography this means that a user must be in the sole possession and control of their private key. This appears to be the same criteria as UNCITRAL's reliable electronic signature. As discussed above, an IBC signature scheme can achieve this in a system whereby the PKG destroys its copy of the private key of the user once it has generated it and provided it to the user. The signatory must be responsible for ensuring that he does not share his private key with anyone.

The third criteria for a secure electronic signature under PIPEDA is that the technology or process used can be used to identify the person using the technology.[118] With PKI, this condition is met with the certification authorities. There is an important nuance in the PIPEDA text lacking from the corresponding UNCITRAL definition. PIPEDA requires that it be *possible* for the technology used to identify the person, not that the technology must, without fail, identify the person accurately. However, identity-based cryptography is, by its very nature, concerned with authenticating the identity of the person associated with the signatory. With the ability to cross reference a number of personally identifying characteristics of an individual, including social media accounts, the PKG can verify the true identity of the signatory and easily satisfies this requirement.

The fourth criteria of the secure electronic signature deals with integrity of the electronic document associated with the signature.[119] As discussed above, private and public key encryption, including PKI and IBC, is premised on the goal of discerning even the smallest of changes to an encrypted message. This is done via the hash function, which will indicate if there has been any alteration to a message once it has been encrypted with the hash algorithm.

Under the general technology-neutral provincial law definitions of electronic signatures[120] as well as pursuant to the more rigorous "secure electronic signature" under PIPEDA, digital signatures using identity-based cryptography schemes would qualify as legally valid electronic signatures.

V. CONCLUSION

This article is intended to be a preliminary assessment of the legal elements of identity-based cryptography. It begs questions relating to the probative force of different cryptographic signature schemes as well as privacy law implications of using social Internet profiles to identify individuals. Also of relevance are the

[117] Section 48(1)(b), *PIPEDA*, *supra* note 111.

[118] Section 48(1)(c), *PIPEDA*, *supra* note 111.

[119] Section 48(1)(d), *PIPEDA*, *supra* note 111.

[120] With the exception of Quebec, which has not been reviewed herein.

private international law issues regarding cross-border transactions executed using electronic signatures which, as we have seen, have differing legal requirements depending on the jurisdiction.

Cryptography has long been thought of as the closest thing humans have to a superpower. This superpower continues to creep into the mainstream. However, a number of caveats, including user adoption and inefficiencies related to authenticity, prevent its arrival on main-street. As one cryptographer laments, "Authenticity is the crown jewel of getting crypto right."[121] It may not be long before social Internet profiles and other personally identifying information are leveraged to solve both the user adoption and authenticity problems. One is left to ask: How many more data breaches must occur before people start taking their online data security seriously? A technology linked to the social media interfaces that our society has grown accustomed to and trustworthy of, and that satisfies the signature requirements of authentication, integrity, and non-repudiation, might just be the right mix for the next wave of e-commerce, such as cryptocurrency business models, to take off.

[121] Finley, *supra* note 51.