UTeM

اونيۏرسيتي تيکنيکل مليسيا ملاک

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Always A Pioneer, Always Ahead

UTeM

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

MyUTeM

BITS 2523
Cyberlaw & Security Policy
Lecture 3

By

Mohd Fairuz Iskandar Othman, Phd

mohdfairuz@utem.edu.my

Cyberlaw in e-commerce

Topics covered:

- Electronic Commerce Act 2006
- Electronic signatures
- Digital signatures & Digital Signature Act 1997

Electronic Commerce Act 2006

- ECA 2006 wasintroduced to provide for legal recognition of electronic messages* used in commercial transactions, the use of electronic messages to fulfil legal requirements and to enable as well as to facilitate commercial transactions through the use of electronic means.
- The Act is largely modelled on the United Nations Commission on International Trade Law ("UNCITRAL") Model Law on Electronic Commerce 1996 ("Model Law").
- In this regard, the UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with an additional Article 5 as adopted in 1998("Guide to Enactment"), is useful when interpreting the provisions of the Electronic Commerce Act 2006 as it sets out, among other things, the purposes and examples where the law applies. However, it is noted that the contents of the Model Law are not identical to the Electronic Commerce Act 2006

*"electronic message" is defined as "an information generated, sent, received or stored by electronic means".

Electronic Commerce Act 2006

- Nothing in the Electronic Commerce Act 2006 shall make it mandatory for a person to use, provide or accept any electronic message in any commercial transaction unless the person consents to the using, providing or accepting of the electronic message. A person's consent to use, provide or accept any electronic message in any commercial transaction may be inferred from the person's conduct.
- There are limitations to applicability of the Electronic Commerce Act 2006 and this can be seen in Schedule to the Act, which provides that the Act shall not apply to the following transactions or documents:
    1. a power of attorney;
    2. the creation of wills and codicils;
    3. the creation of trusts; and
    4. negotiable instruments.

Application of ECA 2006

- Section 2(1) of the Electronic Commerce Act 2006 provides that the Act applies to any commercial transaction conducted through electronic means including commercial transactions by the Federal and State Governments. The question here would be, does the Electronic Commerce Act 2006 apply if the commercial transaction was only done partly through electronic means or does it only apply to transactions which were done fully electronically? For example, if two parties entered into an oral agreement but subsequently communicated *via* electronic means, can the Electronic Commerce Act 2006 be used?
- Based on the Explanatory Statement of the Electronic Commerce Bill 2006, the law was introduced for "the legal recognition of electronic messages used in commercial transactions". It is not limited to a "commercial transaction which was conducted through electronic means".
- The provisions of the Electronic Commerce Act 2006 are only applicable to matters concerning commercial transactions, as stated in the preamble to the Act. It does not apply to family disputes or to support the admissibility of instant messages in family disputes.

Legal recognition of electronic messages

- Section 6 of the Electronic Commerce Act 2006 provides that any information shall not be denied legal effect, validity or enforceability on the ground that:
  - it is wholly or partly in an electronic form; or
  - the information is not contained in the electronic message that gives rise to such legal effect, but is merely referred to in that electronic message, provided that the information being referred to is accessible to the person against whom the referred information might be used.
- According to the Guide to Enactment, this provision embodies the fundamental principle that electronic messages should not be discriminated against, that is, that there should be no disparity of treatment between data messages and paper documents.

Formation and validity of contract

- Section 7 of the Electronic Commerce Act 2006 provides that, in the formation of a contract, the communication of proposals, acceptance of proposals and revocation of proposals and acceptances or any related communication may be expressed by an electronic message. A contract shall not be denied legal effect, validity or enforceability on the ground that an electronic message is used in its formation.
- According to the Guide to Enactment, this provision is not intended to interfere with the law on the formation of contracts but rather to promote international trade by providing increased legal certainty as to the conclusion of contracts by electronic means. It deals not only with the issue of contract formation but also with the form in which an offer and an acceptance may be expressed.
- Section 10(1) of the Contracts Act 1950 provides that all agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object and are not hereby expressly declared to be void.
- In view of the above, there is no doubt that electronic contracts are valid under the Contracts Act 1950 and the Electronic Commerce Act 2006.

Writing

- Section 8 of the Electronic Commerce Act 2006 provides that where any law requires information to be in writing, the requirement of the law is fulfilled if the information is contained in an electronic message that is accessible and intelligible so as to be usable for subsequent reference. Electronic messages would include short message service ("SMS") messages and instant messages (through WhatsApp, Facebook message, WeChat etc.).
- However, it is unclear if voice and video messages would be acceptable. It is submitted that they would be acceptable so long as they are accessible and intelligible so as to be usable for subsequent reference.

Signatures

- Section 9 of the Electronic Commerce Act 2006 provides that where any law requires a signature of a person on a document, the requirement of the law is fulfilled, if the document is in the form of an electronic message, by an electronic signature, which:
    1. is attached to or is logically associated with the electronic message;
    2. adequately identifies the person and adequately indicates the person's approval of the information to which the signature relates; and
    3. is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required.
- For the purposes of point (3) above, an electronic signature is as reliable as is appropriate if: (a) the means of creating the electronic signature is linked to and under the control of that person only; (b) any alteration made to the electronic signature after the time of signing is detectable; and (c) any alteration made to that document after the time of signing is detectable.
- The Digital Signature Act 1997 shall continue to apply to any digital signature used as an electronic signature in any commercial transaction.

Traditional signatures

Traditionally, a person may sign on the document and the signature may serve various purposes.

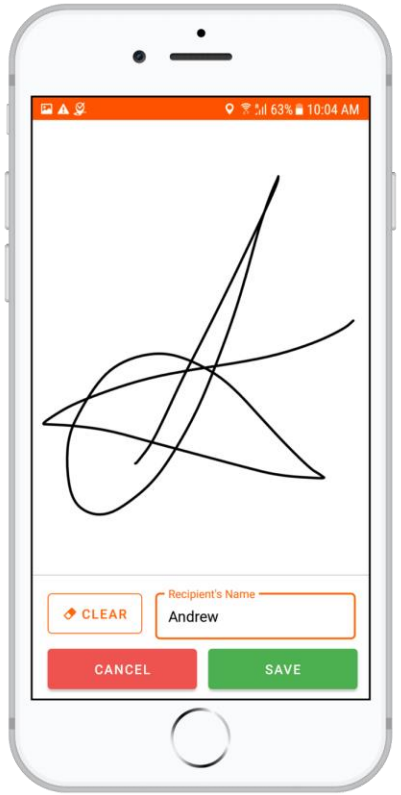
A “sign” is defined under section 3 of the Interpretation Acts of 1948 and 1967 (Consolidated and Revised 1989) (Act 388) to include the making of a mark or the affixing of a thumb-print. Signing a document serves the following general purposes:

- Firstly, a signature serves as a proof of evidence that the document is duly signed by a particular person. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.
- Secondly, the act of signing a document calls to the signer’s attention the legal significance of the signer’s act and thereby helps prevent poorly considered engagements.
- Thirdly, a signature expresses the signer’s approval or authorization of the writing’s content or the signer’s intent that it has legal effect and force

Electronic signatures

- An electronic signature is broadly defined under the Electronic Commerce Act 2006 (ECA) as “any letter, character, number, sound or any other symbol or any combination thereof created in an electronic form adopted by a person as a signature”.
- According to the ECA, if there is a requirement for a signature of a person on an electronic document, this is fulfilled by an electronic signature which is:
    1. attached to or logically associated with the document;
    2. adequately identifies the signer and his approval of the information to which the signature relates; and
    3. is as reliable as is appropriate given the purpose and circumstances for which the signature is required.
- Examples of electronic signatures include:
    - a scanned image of the person’s ink signature,
    - a mouse squiggle on a screen or a hand-signature created on a tablet using your finger or stylus,
    - a signature at the bottom of your email,
    - a typed name,
    - a biometric hand-signature signed on a specialized signing hardware device, a video signature, a voice signature, an “I Agree” checkbox, etc.

Electronic signatures (cont…)



Delivery Notification

Our Ref : 26507

PDF

YOUR LOGO HERE

Delivery Ref : DO1278897897
Your Ref : SO16289879001
Order Date : 11/23/2019

Client:
Candoxy Canada Inc.
5 Sphere Industrial Estate Campfield Road St Albans, Hertfordshire AL1 5HT

Shipper:
Contoso Inc.

#	Code	Description	Price	Qty	Rejected	Reject Reason
1	SD0101	Item A, pack D 12x10	100.20	2	0	
2	SD2002	Item B, pack C 10x10	95.00	2	0	
3	SD0004	Item C, pack A 14x12	99.00	2	0	

Your Company driver today was Paul. We hope everything went ok Don't forget, you can order 24 hours a day at www.company.com.

Delivery Status: Delivered
Reject reason:
Time: 11/24/2019 03:16 PM

Driver: Paul
Vehicle: DS 6799

Name: Steve
Signature/Photo:

Latitude: 53.8766820
Longitude: 27.5441360
Delivery location:

THANK YOU FOR YOUR ORDER

An opportunity to report damage / shortages was given on receipt of your items if present.

Digital signatures & Digital Signature Act 1997

- The Digital Signature Act 1997 was introduced to make provision for, and to regulate the use of, digital signatures and to provide for matters connected therewith. The term "digital signature" is not to be confused with an image of a signature or any form of visual markings.
- This Act provides for, among other things, a mandatory licensing scheme for certification authorities. The mandatory licensing scheme is proposed to establish a minimum regulatory system to provide a basic level of reliability in certification authority practice without undermining the reliability of any signature by invalidating it for lack of a regulatory licence.
- "digital signature" as defined in section 2(1) of the Digital Signature Act 1997 (DSA), means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine:
  - whether the transformation was created using the private key that corresponds to the signer's public key; and
  - whether the message has been altered since the transformation was made.

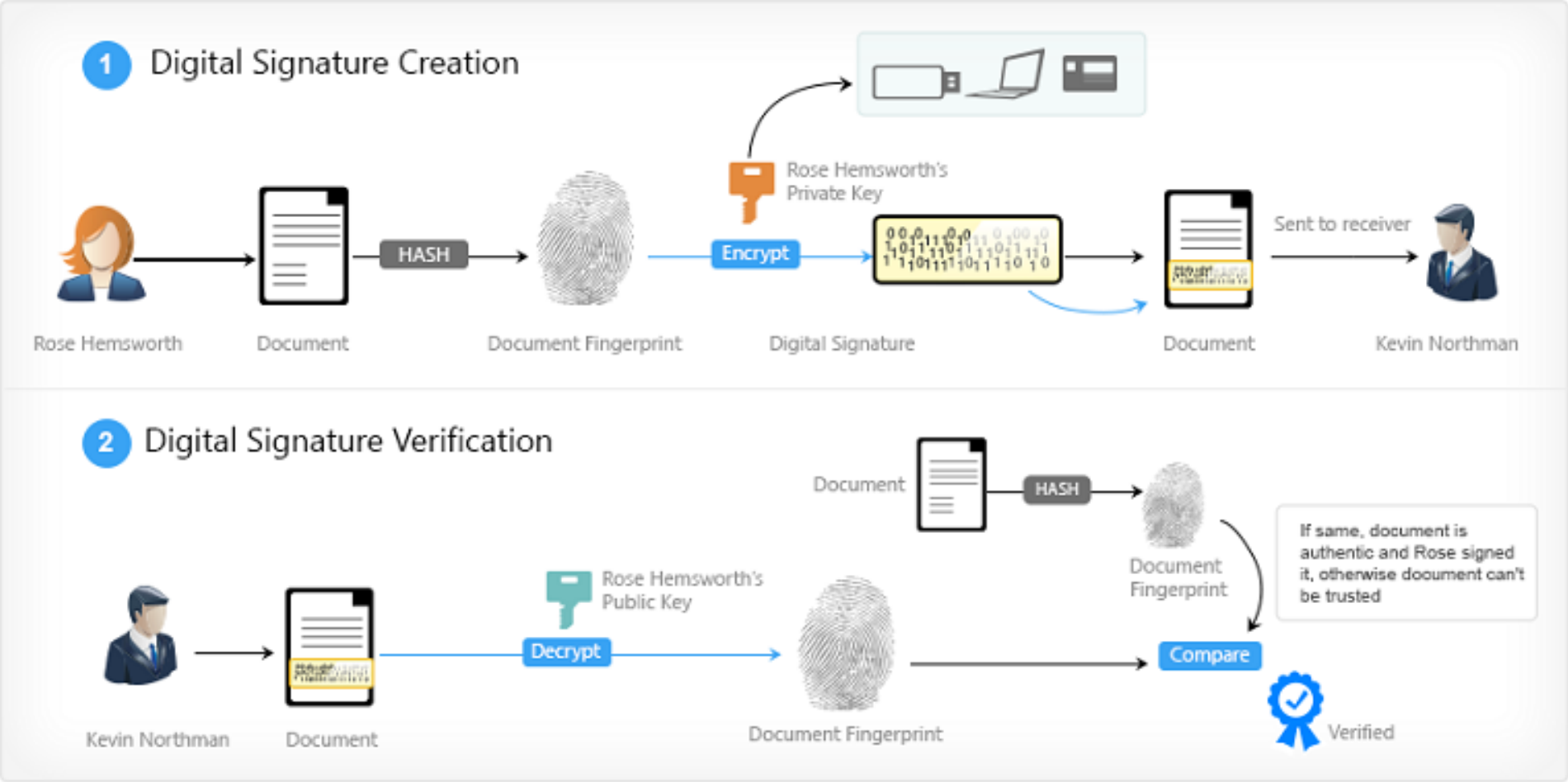
Digital signatures & Digital Signature Act 1997

- "Asymmetric cryptosystem" is defined in section 2 as an algorithm or series of algorithms which provide a secure key pair.
- In the digital world, digital signature can serve as analogues to paper signatures but are different in interesting ways. Digital signature appearing in digital documents transmitted in digital world may appear in many forms based on various systems, such as
  - symmetric cryptosystem,
  - asymmetric cryptosystem,
  - EES (Escrowed Encryption Standard),
  - biometric method (fingerprint validation and retinal scans),
  - SSL (secure socket layer)
  - and SET (secure electronic transaction).

Digital signatures & Digital Signature Act 1997

- Section 64(1) of the Digital Signature Act 1997 provides that a message shall be as valid, enforceable and effective as if it had been written on paper if:
  1. it bears in its entirety a digital signature; and
  2. that digital signature is verified by the public key listed in a certificate which:
     a) was issued by a licensed certification authority; and
     b) was valid at the time the digital signature was created

Digital signatures (cont...)



https://www.comparitech.com/blog/information-security/digital-signatures/

Why do we need digital signatures?

- The main issues in the online or electronic transactions are of trust and security. Parties to electronic contract must be satisfied that the sender and receiver in the electronic transactions are who they purported to be. The sender and receiver must also be convinced that their electronic record can be authenticated and not forged while in transit.
- Basically digital signatures provide assured provenance (only the person in possession of the private key could have created the signature) and non-repudiation (the object must have been signed by the possessor of the key, because the signature could not have been created in any other way).

Why do we need digital signatures? (cont…)

- Digital signatures have three main characteristics:
  - **Authentication:** the sender or signer is really the person who signed the message.
  - **Non-repudiation:** the signer cannot deny afterwards that he or she signed the document.
  - **Integrity:** the document data remains unchanged and cannot be altered after being signed.
- A digital signature should not be confused with digital signature certificate. It is a document which is issued by a trusted authority and certifies that you are the owner of the public key to your digital signature. Digital certificates are only valid for a limited time.

Why do we need digital signatures? (cont…)

- There is a variety of digital signature software that allows making a digital signature online. You can pick a digital signature app or solution from the list below.
  - HelloSign
  - DocuSign
  - Secured Signing
  - eSignLive
  - RPost

Digital signature vs. electronic signature

Digital signature	Electronic signature
Used to secure a document	Mainly used to verify a document
A digital signature certificate is authorized and regulated by certification authorities	Usually not authorized
Comprised of more security features	Comprised of less security features
Common types of digital signature are based on Adobe and Microsoft	Main types of electronic signature include verbal, electronic ticks or scanned signatures.
A digital signature can be verified	An electronic signature cannot be verified.
Preferred more than electronic signature due to high levels of authenticity	Easy to use but less authentic
Particularly concerned about securing the document	Shows intent to sign the contract

Digital signature vs. electronic signature

Digital signature	Electronic signature
Purpose	
to secure a document so that it is not tampered with by people without authorization	to verify a document. The source of the document and the authors are identified.
Regulation	
Digital signature is authorized and regulated by certification authorities. These are trusted third parties entrusted with the duty to perform such task.	Electronic signatures are not regulated, and this is the reason why they are less favorable in different states since their authenticity is questionable. They can be easily tampered with.
Security	
A digital signature is comprised of more security features that are meant to protect the document	An electronic signature is less secure since it is not comprised of viable security features that can be used to secure it from being tampered with by other people without permission.

Digital signature vs. electronic signature

Digital signature	Electronic signature
Types of signatures	
Two common types of digital signatures are mainly based on document processing platforms namely Adobe PDF and Microsoft	can be in the following forms: scanned image, verbal or a tick can be used on an electronic document. The main idea behind is to identify the person who has signed the document for contractual purposes
Verification	
can be verified to see if the document has not been tempered with. A digital certificate can be used to track the original author of the document.	It may be difficult to verify the real owner of the signature since it is not certified. This compromises the authenticity as well as integrity of the document.
Intention	
usually meant for securing a document so that it is not tampered with by unauthorized people. All the same, it is legally binding and preferred since it is authentic by virtue of its traceability to the owner of the document.	usually shows the intent to sign the document or contract. In most cases, when people want to enter into a contract, they show their commitment by signing a document that will become legally binding between them.

Key-takeaways

- Be aware of the difference between electronic signatures, and the more specific subset known as digital signatures;
- Be mindful of the legal conditions (such as reliability) that need to be met for e-signatures to be valid under the ECA;
- Using types of e-signatures other than digital signature may be more open to challenge on legal validity in cases where a seal is traditionally needed. In such instances , physically signing the document may still be prudent – discretion is advised;
- Although using e-signatures (incl. digital signatures) may be more convenient/quicker, there is still some practical uncertainty as to whether this approach on certain documents (e.g. share transfer forms and property transfer forms) will be acceptable to all Malaysian authorities without question.

Digital signature (DS) benefits

- authentication of the sender's identity to the receiver by an entrusted third party;
- verification of genuineness of the message (*i.e.* that it has not been altered);
- security of information sent (*i.e.* no one can tamper with the message without jeopardizing the verification process);
- the sender is unable to repudiate the effect of his signature (*i.e.* sender is not able to say that the signature is not his).

Technical mechanism of DS

- Please refer to part 3.2 of reference paper Siang06

Weaknesses of DS

Please refer to part 3.2 of reference paper. Can be looked upon in the following aspects of:

- *i.e.* the scope of its application,
- limitation/restriction in recognizing a sole digital signature regime,
- qualification and duties of the licensed certification authority and subscriber.

Scope of its application

- There is no amendment made to the Act for about 8 years since its inception in 1998. No court case has been reported so far on the operation of the Act generally and particularly the legal effect of digital signature has also not been judicially addressed.
- However, being one of cyberlaw statutes enacted [others are Computer Crimes Act 1997 (Act 563), Telemedicine Act 1997 (Act 564) and Copyright (Amendment) Act 1997 (Act A994)], the scope of its application is limited.
- The Act only governs the Malaysian within Malaysia, unlike the Computer Crimes Act 1997 which has a wider scope

Limitation/restriction in recognizing a sole digital signature regime

- Unlike traditional signature which has no duration (except if a natural person has died), the recognized digital signature under the Act has a maximum duration of three years from the date of its issuance as stipulated in the digital certificate under section 59(2). There is no provision on renewal of digital certificates; presumably, the subscriber may have to re-apply for a new certificate valid for another three years on the same process.
- by restricting itself to a technology specific system (asymmetric cryptography), the Act has precluded other technologies which have been in existence such as EES (Escrowed Encryption Standard) and biometric method (fingerprint validation and retinal scans); SSL (secure socket layer) and SET (secure electronic transaction) or may be developed in future. This has raised the concern on the security issue as the hardware and software used to create digital signature may be vulnerable to unauthorized access or unauthorized modification

Issues involving certification authority and subscriber

- The Act does not set the qualifications for a licensed certification authority. There is neither education or professional qualification nor specialised training requirement to be a licensed certification authority.
- There is no delineation of how financial accountability of certification authority and subscribers is to be determined.
- There is also no provision for the licensed certification authority to carry the liability insurance nor any specific amount required as surety bond. The Act does not establish any testing requirement to objectively insure that the licensed certification authorities understand the full range of their responsibilities (technological process, legal and ethical duties, statutory procedures and legal liabilities).
- The asymmetric cryptosystem does not reduce the risk involved in the signing of an electronic document but transfer risks to private key. The digital signature (in algorithm sequence) cannot be remembered as it is stored in computer device such as smart card, and thus the device must be kept in a safe place.

List of Certification Authorities

- License and Recognitions under the Digital Signature Act 1997
- Examples: **Digicert, Trustgate**
- Full list of Licensed Certification Authorities:

https://www.skmm.gov.my/sectors/digital-signature/list-of-licensees

Summary

- To ease the usage of this technology especially for those unskilled private individuals, the mechanism of the digital signature should be as comfortable and easy as – in much the same way as the average person can easily sign his own name in the physical documents.
- Digital signature provides a platform for the e-business. Thus, the government and all parties concerned shall ensure the mechanism to be secured and safe.
- The legislative body need to look into those issues highlighted above to safeguard the interests of parties transacted in the Internet (e-business). The Act shall extend its application to transactions by any person (whether Malaysian or non-Malaysian) within Malaysia, at least to be consistent with section 9(1) of the Computer Crimes Act 1997, the other cyberlaw legislation. It would be an ideal to have all nations to discuss over and adopt the best practices universally.

Summary (cont...)

- Instead of having various statutes governing various aspects of the e-business transactions, it is suggested that one comprehensive statute similar to the Singapore Electronic Transaction Act 1998 should be enacted
- There should also be inserted a clear provision on the renewal of the digital certificate so that a new digital key will be issued to the existing subscribers. By having a new key from time to time, this may prevent the chances of tampering activities.
- The qualification of a licensed certification authority is not satisfactory ("trustworthy person"). Thus we suggest that a much clearer guideline for qualified certification authority be laid down.
- The Act should be revised from time to time to ensure the legal equivalence among various new technological approaches. This is to ensure that the Act is not soon outdated and that the Act may survive technological changes.
- Awareness campaigns through public speeches, seminars, conferences are also needed to promote the public confidence on the usage of digital signature.

Thank You

MyUTeM

www.utem.edu.my