Funded by the European Union

EU TRADE RELATED ASSISTANCE PHASE II

Consultative Workshop on Draft Electronic Transactions Act

Celebrating 40 Years of Partnership
'Working Together - Wok Bung Wantaim'
#EUPNGPartnership

10 May 2018
Lamana Hotel

http://www.pngeutra2.org.pg

Implemented by the Department of Trade, Commerce and Industry

Section of the Draft Electronic Transactions Act – Electronic Signatures

Ms. Irina Kireeva, Legal Expert

What is an Electronic signature?

An **electronic signature**, or e-signature, refers to data in electronic form, which is logically associated with other data in electronic form and which is used by the signatory to sign.

This type of signature provides the same legal standing as a handwritten signature as long as it adheres to the requirements of the specific regulation it was created under (e.g., eIDAS in the European Union, NIST-DSS in the USA or ZertES in Switzerland).

The concept of Electronic signatures

The concept of electronic signatures is not new, with common law jurisdictions having recognized telegraph signatures as far back as the mid-19th century and faxed signatures since the 1980s.

Electronic signatures are a legal concept distinct from digital signatures, a cryptographic mechanism often used to implement electronic signatures.

While an electronic signature can be as simple as a name entered in an electronic document, digital signatures are increasingly used in e-commerce and in regulatory filings to implement electronic signatures in a cryptographically protected way.

Definitions from the ETA:

"Electronic signature" means 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 intention in respect of the information contained in the data message.

"Signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents.

When electronic signature can be used?

Electronic signatures can be used in a variety of situations. As their legal effects are equivalent to the ones of handwritten signatures, qualified electronic signatures can be used in any situation, even cross-border, where handwritten signatures are used, such as:

- Contracts (sales, employment, lease, insurance, etc.)
- Transactions (e-commerce, online banking, etc.)
- Administrative procedures (tax declarations, requests for birth certificates, etc.)

Electronic signatures in the European Union

Electronic signatures were first recognised in European legislation through the Directive on a Community framework for electronic signature (e-Signature Directive) adopted in 1999.

Since 1 July 2016, electronic signatures in the EU are governed by the Electronic Identification and Trust Services (eIDAS) Regulation.

eIDAS provides a predictable regulatory environment directly applicable to all EU Member States to enable secure and seamless electronic interactions between businesses, citizens and public authorities.

Three types of electronic signatures

The eIDAS Regulation defines three levels of electronic signature: **'simple'** electronic signature, **advanced** electronic signature and **qualified** electronic signature. The requirements of each level build on the requirements of the level below it, such that a qualified electronic signature meets the most requirements and a 'simple' electronic signature the least.

- ***'Simple' Electronic Signatures***

An electronic signature is defined as *"data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign"* (eIDAS Article 3) . Thus, something as simple as writing your name under an e-mail might constitute an electronic signature.

Advanced Electronic Signatures (AdES)

An advanced electronic signature (eIDAS Article 3) is an electronic signature which is additionally:

- uniquely linked to and capable of identifying the signatory;
- created in a way that allows the signatory to retain control;
- linked to the document in a way that any subsequent change of the data is detectable.

The most commonly used technology able to provide these features is the use of **a public-key infrastructure** (PKI), which involves the use of certificates and cryptographic keys.

Qualified Electronic Signatures (QES)

A qualified electronic signature (eIDAS Article 3) is an advanced electronic signature which is additionally:

- created by a qualified signature creation device;
- and is based on a qualified certificate for electronic signatures.
- Signature creation devices come in many forms to protect the electronic signature creation data of the signatory, such as smartcards, SIM cards, USB sticks. "Remote signature creation devices" can also be used where the device is not in the physical possession of the signatory, but managed by a provider. Those remote qualified signature solutions offer an improved user experience while maintaining the legal certainty offered by qualified electronic signatures.
- Qualified certificates for electronic signatures are provided by (public and private) providers which have been granted a qualified status by a national competent authority as indicated in the national 'trusted lists' of the EU Member State. Those lists can be accessed through the Trusted List Browser. Many providers of qualified certificates will deliver the corresponding private key on a qualified signature creation device.

While different levels of electronic signatures may be appropriate in different contexts, only qualified electronic signatures are explicitly recognized to have the equivalent legal effect of hand-written signatures all over the EU.

The fundamental principle of technology neutrality to electronic signatures technologies

The proposed article contains two exceptions:

- The first, refers to the possibility for private parties to agree on the signature technology of their choice. For instance, electronic banking authentication normally uses tokens and encryption (these are digital signatures). The Bank will bind the client to use that authentication method, in line with prevailing industry standards, in the contractual provisions related to the e-banking service.
- The second exception, introduced with the reference to "otherwise applicable law", gives the possibility for another law or regulation to set forth higher requirements. This could be the case, for instance, of e-government services.

Reliability of electronic signatures – how to ensure that?

The Draft ETA suggests "two tier" approach:

- Firstly, all forms of electronic signatures, as defined by the Act, **may have legal recognition** in light of all relevant circumstances.
- Secondly, certain electronic signatures that meet the specific requirements set forth in that paragraph may benefit from a presumption, i.e. their use would reverse the burden of proof on the other party with respect to origin, integrity and other information validated by the signature. This may be the case of digital signatures based on Public Key Infrastructure (PKI) encryption technology.
- A safeguard clause confirms that all presumptions may be reversed with adequate evidence.

CONDUCT OF THE SIGNATORY

The obligations for the holder of an electronic signature creation device are provided.

A signature creation device may consist of software, hardware or any other procedure or method. For instance, a mobile phone, a laptop or a tablet may contain an electronic signature creation device.

Important: the holder of those electronic devices **shall exercise care to ensure that unauthorized electronic signatures do not take place,** e.g. by allowing access to other parties. The holder shall also inform other concerned parties if signature creation data have been or may have been compromised.

CONDUCT OF THE SERVICE PROVIDER

- Specialized third parties may provide electronic signature services. This is also the case when digital signatures based on Public Key Infrastructure are used. In that case, the service provider issues an electronic signature, which could be a certificate, to be used to identify the author of the electronic communication and, possibly, provide additional information on the integrity of the message and on the time when the message was sent.
- **Important:** use by the service providers of trustworthy systems, procedures and human resources in performing their services, as they will bear the legal consequences for the failure to comply with the legal requirements. The oversight authority, if existing, may offer additional guidance by mean of regulations.

THE CONCEPT OF TRUSTWORTHINESS – what does it include and how it can be judged?

Trustworthiness of any systems, procedures and human resources utilized by a service provider includes the following factors:

- (a) Financial and human resources, including existence of assets;
- (b) Quality of hardware and software systems;
- (c) Procedures for processing electronic signatures and applications for electronic signatures and retention of records;
- (d) Availability of information to signatories identified in electronic signatures and to potential relying parties;
- (e) Regularity and extent of audit by an independent body;
- (f) The existence of a declaration by an accreditation body or the service provider regarding compliance with or existence of the foregoing; or
- (g) Any other relevant factor.

CONDUCT OF THE RELYING PARTY

The provisions of the Act on duties of each party involved in the electronic signatures (i.e., signatory, certification service provider and relying party) by indicating that the relying party may be held liable in certain cases, e.g. if steps to verify the reliability of the electronic signature are not taken. In particular, this may happen when the relying party relies on a revoked or expired certificate.

Note: *"Relying party" means a person that may act on the basis of an electronic signature.*

RECOGNITION OF FOREIGN ELECTRONIC SIGNATURES

- Foreign electronic signatures, including foreign certificates, should be recognized in Papua New Guinea on the basis of their level of reliability, and in light of any agreement of the concerned parties. Thus, the Electronic Transactions Act is not only technological neutral with respect to electronic signatures, but also geographic neutral, i.e. it does not attach any consequence to the place of origin of the electronic signature (as expected by the United Nations Convention on the Use of Electronic Communications in International Contracts).
- The Act contains a safeguard clause that recognizes different signature requirements contained in law other than the Electronic Transactions Act. For instance, those could be requirements established to access e-government services.

Thank you for your attention!
Any questions?