ICTA
ideas actioned
Information and Communication Technology Agency

Frequently Asked Questions on Digital Signatures and Digital Certificates

These FAQ's are categorized as 'General' and 'Technical' in nature. 'General' queries are questions that are generally asked by government officers who plan to implement Digital Signature solutions at respective organizations. The technical responses are only for those seeking more detailed information.

1) Category: General

1.1 Is there legal recognition for electronic communications and transactions in Sri Lanka?

Yes. All electronic communications and transactions are governed by the Electronic Transactions Act No. 19 of 2006 and by the Electronic Transactions (Amendment) Act No. 25 of 2017 (collectively referred to as the "**ETA**"). The ETA recognizes and facilitates the formation of contracts, the creation and exchange of data messages, electronic documents, electronic records, and other communications, in electronic form in Sri Lanka. It provides for the appointment of a certification authority and licensing and authorizing of certification service providers and gives effect to the provisions of the united nations convention on the use of electronic communications in international contracts.

1.2 What is an electronic record?

An 'Electronic Record' is a written document or other record created, stored, generated, received, or communicated electronically.

1.3 Does the law recognize electronic records in Sri Lanka?

Yes, it's recognized by law. Section 3 of the ETA states that "No data message, electronic document, electronic record or other communication shall be denied legal recognition, effect, validity or enforceability on the ground that it is in electronic form."

1.4 What is a Digital Signature?

Digital Signatures (standard electronic signatures) take the concept of traditional paper-based signing and transforms it into an electronic 'fingerprint'. This 'fingerprint' or coded message, is unique to both the document and the signatory, and binds both together. The digital signature ensures the sender's authenticity and that of who 'signs' the document. Any changes made to the document after it is signed, invalidates the signature; thereby protecting against signature forgery

and information tampering. Digital signatures sustain signatory authenticity, accountability, data integrity, and non-repudiation of documents and transactions.

1.5 What are the benefits of Digital Signatures?

Among the many benefits of Digital Signatures, the following are the key elements:

- **Cost saving**: The introduction of paperless documentation saves money previously spent on the physical resources, time, personnel, and office space used to manage and transport them
- **Positive environmental impact:** Reducing paper use also reduces the physical waste generated by paper and the negative environmental impact of transporting paper documents
- **Convenience:** Digitally signed documents are easy to handle compared to their physical equivalents, making this a more convenient option
- **Traceability:** Digital Signatures create an audit trail that makes internal record-keeping easier for businesses. Once everything is recorded and stored digitally, there are fewer risks for a manual signee or record-keeper to make a mistake or misplace a document
- **Timestamping:** The time of a Digital Signature is useful when the timing is critical, such as for stock trades, tender submissions, and legal proceedings
- **Global acceptance and legal compliance:** The public key infrastructure (**PKI**) standard ensures vendor-generated keys are made and stored securely. Because of the international standard, many countries are accepting Digital Signatures as legally binding (please also see 2.2 below)
- **Increased efficiency and saved time:** Digital signatures simplify the time-consuming processes of physical document signing, storage and exchange, enabling businesses to access and sign documents quickly

1.6 Are digitally signed documents recognized by Sri Lankan Courts?

Yes, Digital Signatures are legally recognized according to the ETA. Section 7 of the ETA specifies that where any Act or enactment of Parliament provides that any information or communication shall be authenticated by affixing the signature, or that any document should be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to be satisfied, if such information or matter is authenticated by means of an electronic signature.

1.7 Does a 'Digital Signature' mean pasting the image of a physical signature to a document?

No. That is not what Digital Signatures are about. That is not what we call a 'digitally signed document'. Pasting the image of a physical signature does not make a document valid. It does not necessarily mean the signature owner has endorsed the document or at least seen it. A third party that has the image can fix it without the knowledge of the claimed signee. Such documents are not legally accepted.

1.8 Will the print (hardcopy) of the digitally signed document, have the same validity?

No. A Digital Signature can be affixed only to a softcopy. The document must be in original soft form to verify the digital signature. The print (hardcopy) has no validity. For the same reason, there is no point in storing the hard copies of digitally signed documents. They must be kept in electronic format to be able to validate the same.

1.9 Can a scanned document/image be digitally signed?

Yes. Any document in soft form can be digitally signed. It does not matter whether the document is electronically generated or scanned.

1.10 What will happen if either the signatory or someone else changes the content of a digitally signed document?

The moment the signed document is changed, original signature will no longer be valid. There will be an indication that the document had been modified.

1.11 Can one deny digitally signing a document after doing so?

No. Digital Signature schemes are cryptographically based. If implemented effectively, they can also provide non-repudiation, meaning that the signatory cannot successfully claim they did not sign the relevant document, while also claiming his private key remains a secret.

1.12 What is a Digital Certificate?

Keeping aside all technical information, a Digital Certificate (sometimes also referred to as a Certificate in this FAQ) is simply an electronic file or an electronic credential which binds the identity of the owner of a Digtial Certificate to a pair of electronic encryption keys, (one public and one private – see the technical section for a detailed explanation), that can be used to encrypt and sign information/documents digitally.

Without Digital Certificates, one could send data encrypted with the private key and the public key would be used to decrypt the data, but there would be no assurance that the data originated from an exact person in particular. The receiver would know that a valid key pair was used. In essence, a Certificate Authority (**CA**) –is a commonly trusted third party that is relied upon to verify the matching of public keys to identity, e-mail name, or other such information. It is a CA that is authorized to issue a Digital Certificate (please see 1.14 below).

1.13. Why does one need a Digital Certificate?

A digitally signed document authenticates the identity of the sender digitally. It also provides one with a high level of security for online transactions by ensuring absolute privacy of the information such exchanged. One can use digital signatures to sign/encrypt information in a manner that only the intended recipient can read it. One can digitally sign information to assure the recipient that it has not been changed in transit, and also verify one's identity as the sender of the message.

Authentication is a critical issue for users of electronic commerce too. Banks must have confidence in the authenticity and the integrity of an electronic transaction received from another bank. This can be achieved through the use of Digital Signatures. Digital Signatures are aimed at achieving a higher level of trust where physical signatures are not possible. Digital signing helps the recipient of the electronic transaction to know with certainty that it was originated by the party who claims who they are and that no changes have been made after the transaction has been signed.

1.14 What is a Certification Authority (CA) in the context of Digital Certificates?

A Certification Authority (CA) is an organization that issues Digital Certificates. Such an organization sign a Certificate to prove the authenticity of the individual or organization that issued the request. A CA is responsible for managing domain control verification and verifying that the public key attached to the Certificate belongs to the user or organization that requested it. They play an important part in the PKI process and keeping internet traffic secure.

1.15 Who are the Digital Signature Certification Authorities in Sri Lanka?

Recognizing the need for a Digital Signature Certification Authority (CA), the Central Bank of Sri Lanka requested LankaClear (Pvt.) Ltd. (LCPL) to be the financial sector Certification Service Provider (CSP). LCPL launched Sri Lanka's first Certification Authority under the brand name LankaSign in accordance with the ETA.

In alignment with the ETA, LankaSign follows a stringent process on validating the Digital Certificate users and their respective organizations before issuing a Digital Certificate. Due to its high security standards, LankaSign was able to obtain certification on ISO 27001:2013 for its Information Security Management System in the year 2015.

LankaSign encourages more institutions in all sectors to adopt cost effective Digital Certificate based technology to achieve a greater level of information security for all their electronic communications and transactions. (Please also see 2.6 below).

Sri Lanka CERT |CC (www.cert.gov.lk) is Sri Lanka's National Root CA (https://nca.gov.lk) and they have recognised LankaSign as the CSP (Certification Service Provider) of them.

1.16 How can my organization introduce a Digital Certificate system?

One must first contact Lanka Clear (Pvt) Ltd – the parent company of LankaSign. (https://www.lankaclear.com) The homepage itself will provide guidance how to register to make the services available. When one responds to the pop-up window with a 'Yes', one is directed to the knowledge center at https://www.lankaclear.com/knowledge-center/lankasign that provides all the necessary information one needs.

1.17 Can I use LankaSign Digital Certificates to automate my document management system or other workflow system?

Yes, you can. There will not be any serious changes to the procedures. The only difference would be, instead of normal documents, one will handle digitally signed documents. LankaSign will provide the Digital Certificates and general guidelines.

1.18 What is the recommended use of Digital Certificates within an automated system?

The Certificates can be used in anyway within the application the developer and product owners wishes at the discretion of developer and product owners as per product, compliance, legal and other requirements as long as such functions does not violate rules and regulations of the CSP. Please note the CSP provides only the Certificates and related token driver software and does not provide any other software/application related services or support.

1.19 How is a Digital Certificate provided to a client?

It is provided in a security token which can be plugged to the USB port.

1.20 Is there a cost involved in obtaining a Digital Certificate?

Yes, however, the security token is a one-time purchase and the Digital Certificate needs to be annually renewed. A security token and a Digital Certificate should be purchased for each user. Apart from these nominal costs, there will not be any further charges for a Digital Certificate system.

2) CATEGORY : TECHNICAL

2.1 How does a digitally signed document work?

A digitally signed document explicitly associates the identity of an individual/device with two keys – a public and a private key (please see 2.2 below). The Digital Certificate contains information about a user's identity (for example, their name, PIN code, country, email address, the date on which the Digital Certificate was issued and the name of the Certificate Authority). One key will not work in the absence of the other. They are used by browsers and servers to encrypt and decrypt information regarding the identity of the Certificate user.

2.2 What is PKI (Public Key Infrastructure)?

PKI technology is the only proven technology available today that ensures non-forgeable signatures.

In a PKI system, each user has two keys: a public key and a private key. These keys can be used for encrypting and decrypting information, for digitally signing electronic information and for verifying the authenticity of their owner. The public key is distributed widely, whilst the corresponding private key is held by its owner in a secure place. Since both keys are mathematically related, the public key cannot reveal the private key. This makes PKI a great technology for Digital Signatures.

The private key is typically stored on the user's computer hard disk or on an external device such as a USB token. The user retains control of the private key; it can only be used with the issued password. The public key is disseminated with the encrypted information. The authentication process fails if either one of these keys is not available or do not match. This means that the encrypted data cannot be decrypted and therefore, is inaccessible to unauthorized parties.

2.3 Why do we need PKI (Public Key Infrastructure)?

The main purpose of the Digital Certificate is to ensure that the public key contained in the Certificate belongs to the entity to which the Certificate was issued, in other words, to verify that a person sending a message is who he or she claims to be, and to then provide the message receiver with the means to encode a reply back to the sender.

Encryption techniques using public and private keys require a PKI to support the distribution and identification of public keys. Messages can be encrypted with either the public or the private key and then decrypted with the other key.

2.4 What is the difference between a Digital Signature and a Digital Certificate?

A Digital Certificate is a file that verifies the identity of a device or user and enables encrypted connections. A Digital Signature is a hashing approach that uses a numeric string to provide authenticity and validate identity. A Digital Signature is typically fixed to a document or email using a cryptographic key. The signature is hashed, and when the recipient receives it, it performs that same hash function to decrypt the message. Put in another way, A Digital Certificate is a document with a Digital Signature that is certified by a Certification Authority (CA).

More on the difference between a Digital Signature and a Digital Certificate:

Digital Signatures and Digital Certificates (12 minutes)
https://www.youtube.com/watch?v=stsWa9A3sOM&t=314s

2.5 What is the role of a Certification Service Provider (CSP)?

A CSP is an authority on a network that issues and manages security credentials and public - private key pair's for message signing and encryption. As part of a public key infrastructure (PKI), a CSP checks with a Registration Authority (RA) to verify information provided by the requestor of a Digital Certificate. If the RA verifies the requestor's information, the CA can then issue a Digital Certificate that can be used for the purpose of signing and encrypting electronic transactions. LankaSign's role as a CSP is more detailed in the document at https://www.lankaclear.com/assets/images/knowledge-center/lankasign/downloads/38-CSP-Summary-Certification-Practice-Statement-V3-1.pdf.

2.6 What other roles does LankaSign play?

LankaSign in its first phase started providing Digital Certificates to Banks to be used in financial transaction clearing systems, such as SLIPS and CITS (Cheque Imaging and Truncation System), where the CSP and Public Key Infrastructure (PKI) was made available on LCPL's Virtual Private Network (VPN).

On February 9th, 2011 LankaSign launched its second phase of providing digital certificates for all financial sector enterprise applications, SSL Certificates and end Users (E-mail/Document signing Certificates) on both private and public networks. This adds great value to the financial sector in Sri Lanka as using Digital Certificates of LankaSign will save the country its valuable foreign exchange where the other alternative is to procure Certificates from foreign CSPs at a much higher cost. Upon LankaSign's expansion, it is now providing a customer focused local

service and solutions to reduce document management overheads associated with managing physical documents, as well as promoting Green initiatives.

Currently LankaSign is widely used in almost all financial sector organizations as well as few other sectors for automating their documentation process by digitally signing electronic copies of documents and adding high security for electronic documentation exchange process. As the next phase in their expansion plan, with a major upgrade to their system, LankaSign is now capable of providing Digital Certificates in real-time for mobile based payment applications for digitally signing and authenticating electronic documents. This has been enabled by a common API developed by LankaSign, which can be easily integrated with such mobile payment applications via a Software Development Kit (SDK) that is freely distributed to such developers.

The above has been issued by the Information and Communication Technology Agency of Sri Lanka to facilitate state organizations' transformation into the use of Digital Signatures and Digital Certificates.

Please direct all further inquiries to Mr. Chanuka Wattegama - Director, Policy, ICTA at chanukaw@icta.lk.