

Digital Signatures In Uzbekistan

TA 8260-UZB

E-Government for Effective Public Management

Business Process Review, Re-Engineering and Development of Online
Government Services

Sanjay Saxena / Shaan Stevens
International TA Consultants

What is the need for E-Signatures / Digital Signatures?

Why Electronic Records?

- Very easy to make share
- Very fast distribution
- Easy archiving and retrieval
- Environmental Friendly
- **Very easy to make copies and copies are as good as original**
- **Easily modifiable**

Why E-Signatures?

- To Provide
 - A. Authenticity**
 - B. Integrity**
 - C. Non-repudiation**for electronic documents
- To use the Internet as a safe and secure medium for e-Commerce and e-Governance

Businesses and individuals involved in commercial or monetary transactions or transactions which confer rights, need to have confidence in communications that are sent in relation to these transactions. There is a need to ensure that for all electronic communications / documents sent, the Sender can be easily recognized and cannot deny having sent the document; the communication / document cannot be altered in any way after it has been sent, and the document has the necessary security and remains confidential.

What is E-Signature (ES) and Digital Signature (DS)

Electronic Signature

An Electronic Signature (ES) is a **verified intent to sign a document**. This can be anything from a written authorization, an electronically signed authorization, logging in through a password, or just checking a box.

In ES, authorization is usually in the form of simply typing or signing your name on a document, but it could also be in the form of a symbol, or process that signifies intent to sign, like entering in a numbered code or password.

Digital Signature

A Digital Signature (DS) is a type of **asymmetric cryptography** used to simulate the security properties of a **signature** in digital, rather than written form.

- DS identifies the Certifying Authority issuing it.
- Has the name and other details that can identify the subscriber.
- Contains the subscriber's public key.
- Is digitally signed by the Certifying Authority issuing it.
- Is valid for either one year or two years.

***In a nutshell:** An electronic signature is an authorized way to sign a document, while a digital signature is a way to encode a document for security.*

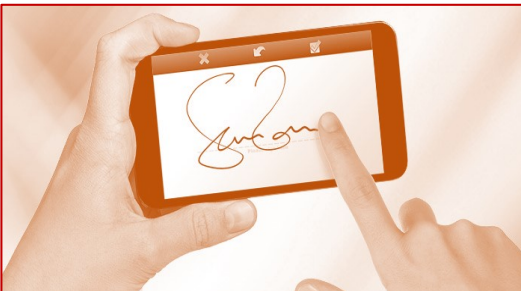
Difference Between ES and DS (1/2)

ELECTRONIC SIGNATURES (ES)

ES is **a lasting representation and capture** of someone's intent

Can be anything, from a **scripted text, image or voice** that illustrates an action of consent.

ES can be separated from its document but it is **impractical to separate** a digital signature from the contents it signs



DIGITAL SIGNATURES (DS)

DS is a encryption technology **underlying the ES**. Works **with** an ES; **NOT as an ES**

Mechanism that secures documents with **cryptography**

DS offers **independent verification** and a **strict adherence** to standard whereas e-signature doesn't



Difference Between ES and DS (2/2)

ES NEEDS TO PROVE



WHO Signed



WHAT was signed



Captures **INTENT** and Consent



Significantly **INCREASES** the **EASE** and **FLEXIBILITY** of signatory processes

DS SUPPORTS ES



SECURES SENSITIVE DATA associated with documents through encryption



DETECTS TAMPERING EFFORTS and invalidates associated documents



STRENGTHENS electronic signature as a trusted tool

Putting the ES & DS together ultimately produces



Persuasive, legally binding evidence



Peace of mind among all parties



A significantly faster document work flow

Superiority of Digital Signature over Manual Signature

Why Electronic Records?

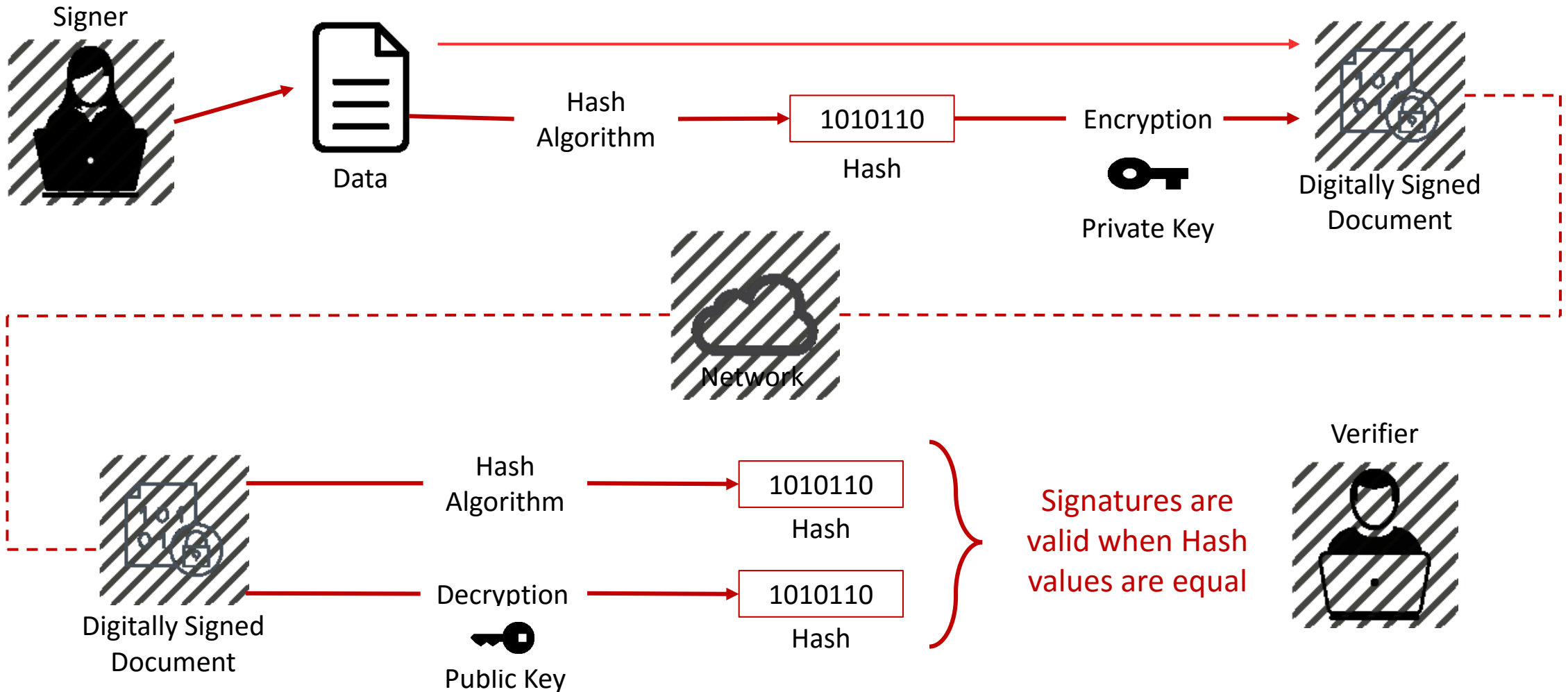
- Very easy to make share
- Very fast distribution
- Easy archiving and retrieval
- Environmental Friendly
- **Very easy to make copies and copies are as good as original**
- **Easily modifiable**

Why E-Signatures?

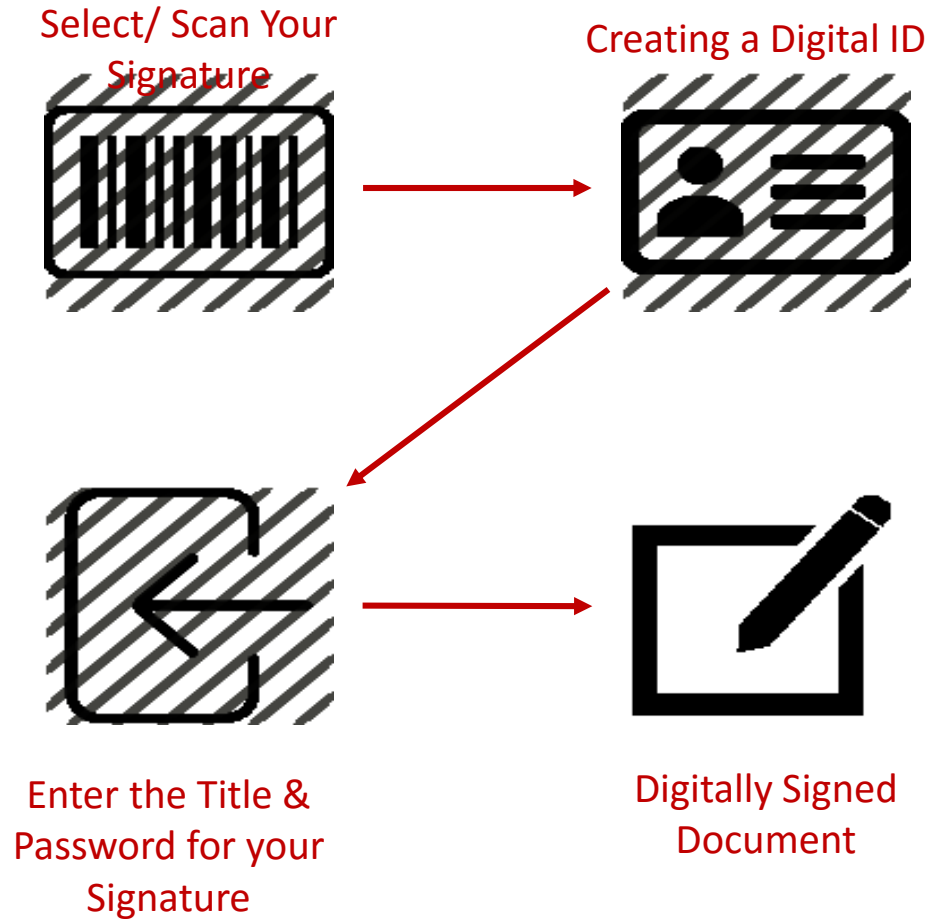
- To Provide
 - A. Authenticity**
 - B. Integrity**
 - C. Non-repudiation**for electronic documents
- To use the Internet as a safe and secure medium for e-Commerce and e-Governance

| Parameter | Paper | Electronic |
|-----------------|--|---|
| Authenticity | May be forged | Can not be copied |
| Integrity | Signature independent of the document | Signature depends on the contents of the document |
| Non-Repudiation | a. Handwriting expert needed b. Error prone | a. Any computer user b. Error free |

Process Involved in Creating Digital Signature



Create Simple Digital Signature at Document level



Add Digital ID

Enter your identity information to be used when generating the self-signed certificate.

Name (e.g. John Smith):

Organizational Unit:

Organization Name:

Email Address:

Country/Region:

Key Algorithm:

Use digital ID for:

Add Digital ID

Enter a file location and password for your new digital ID file. You will need the password when you use the digital ID to sign or decrypt documents. You should make a note of the file location so that you can copy this file for backup or other purposes. You can later change options for this file using the Security Settings dialog.

File Name:

C:\Users\svish\AppData\Roaming\Adobe\Acrobat\11.0\Security\D.pfx

Browse...

Password:

Not Rated

Confirm Password:

Cancel

< Back

Finish

Why Digital Signature Certificates (DSC)?

DIGITAL SIGNATURE (DS)

Digital Signature (DS) is an electronic method of signing an electronic document that establish the following assurances:

- **Authenticity:** that the signer is who he or she claims to be.
- **Integrity:** that the content has not been changed or tampered with since it was digitally signed.
- **Non-repudiation:** to prove to all parties the origin of the signed content. "Repudiation" refers to the act of a signer's denying any association with the signed content.



DIGITAL SIGNATURE CERTIFICATE (DSC)

Digital Signature Certificate (DSC) is a computer based record that:

- Requires Public Key Infrastructure (PKI) for generating a pair of keys - **a private key** and **a public key**. PKI enforces additional requirements, such as the Certificate Authority (CA), a digital certificate, end-user enrolment software, and tools for managing, renewing, and revoking keys and certificates.
- Identifies the Certifying Authority Issuing it
- Has the name and other details that can identify the subscriber
- Is valid for either one or two years
- Is digitally signed by the Certifying Authority issuing it.

Entities Involved in Providing DSs

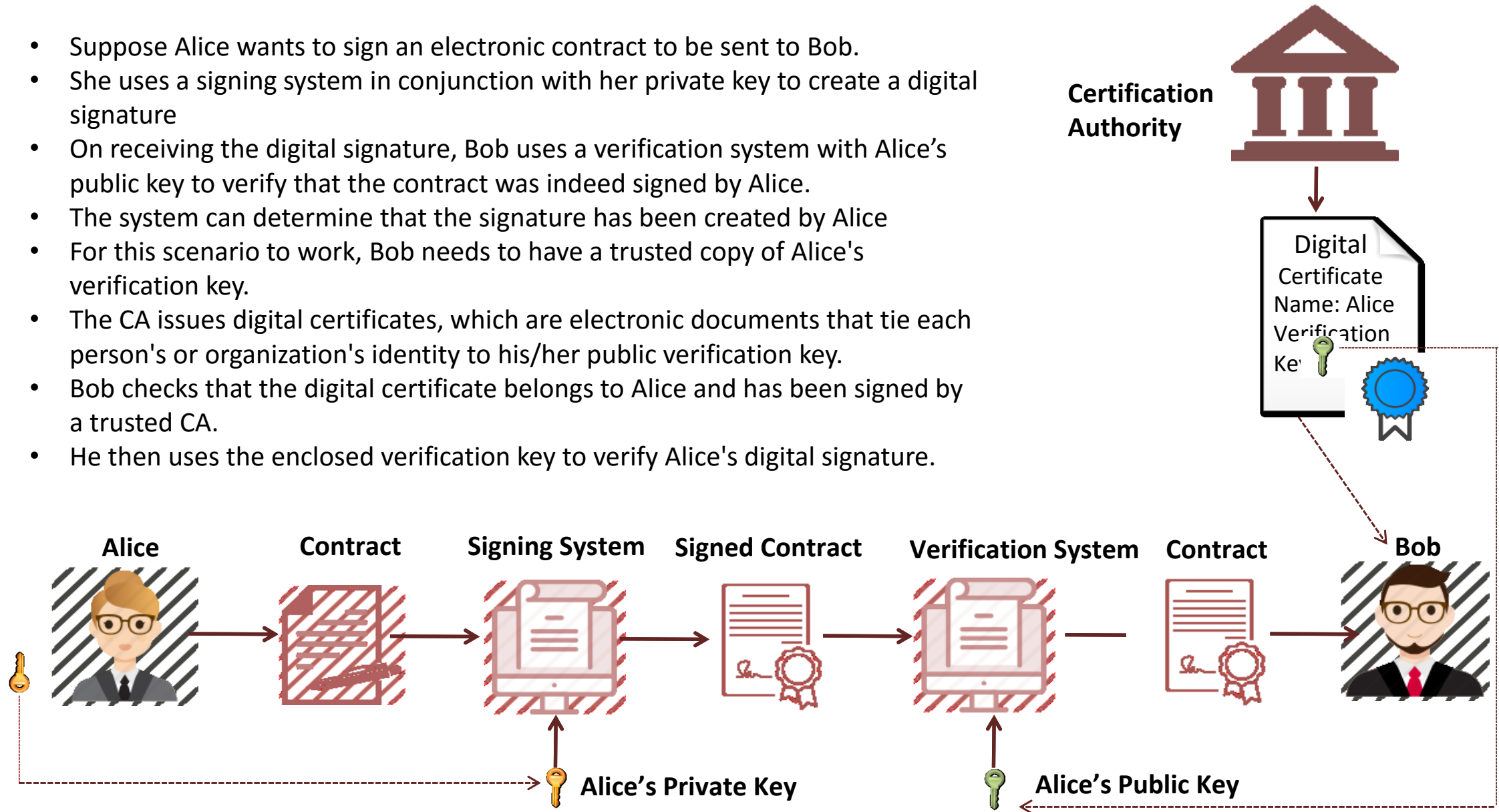
- A licensed Certifying Authority (CA) issues the digital signature.
- CAs are the digital world's equivalent to passport offices. They issue digital signature certificates and validate holders' identity and authority.
- CAs embed an individual or institution's public key along with other identifying information into each digital certificate
- CAs cryptographically sign it as a tamper-proof seal verifying the integrity of the data within it, and validating its use.

Certifying Authority (CA)

- Trusted Third Party
- An organization which issues Public Key Certificates
- Assures the identity of the parties to whom it issues certificates
- Maintains online access to the public key certificates issued

Technology Involved in Creating DS

- Suppose Alice wants to sign an electronic contract to be sent to Bob.
- She uses a signing system in conjunction with her private key to create a digital signature
- On receiving the digital signature, Bob uses a verification system with Alice's public key to verify that the contract was indeed signed by Alice.
- The system can determine that the signature has been created by Alice
- For this scenario to work, Bob needs to have a trusted copy of Alice's verification key.
- The CA issues digital certificates, which are electronic documents that tie each person's or organization's identity to his/her public verification key.
- Bob checks that the digital certificate belongs to Alice and has been signed by a trusted CA.
- He then uses the enclosed verification key to verify Alice's digital signature.



Transactions Recommended for ES and DS

Electronic Signature (ES)

- Contracts & Agreements
- Invoices and Payment Receipts
- Insurance Papers
- Public complaints
- Request for information
- Request for empanelment
- Request for providing a non-financial service



Digital Signature (DS)

- Any kind of Financial Transactions – Payments for taxes, dues, contractual payments etc.
- Any kind of transaction which bestows or transfers rights from one entity to another – property transfer, Will, etc.
- E- Commerce – online purchase of items or services



Legal and Non-Legal Status of e-Signatures in Different Countries

Countries enjoying the same Legal Status for both e-signatures as well as Physical Signatures

- United States, Australia, United Kingdom, Canada, Spain, Finland, Singapore, Hong Kong, Chile, Switzerland, United Arab Emirates, South Africa, New Zealand, Colombia, Portugal, Ireland, the Netherlands, South Korea, Peru and Philippines

Countries where e-signature Enforcement Laws are present, but Physical Signatures are considered Superior

- Russia, Japan, China, Czech Republic, France, Belgium and India

Countries Missing Clear Directives on the Implications and Legality of e-signatures

- Brazil, Malaysia, Sweden, Mexico, Thailand, Indonesia, Austria, Germany, Macao, Taiwan, Uruguay, Argentina, Denmark, Italy, Poland, Turkey, Hungary, Israel, Romania and Norway

ES and DS Around the World



Electronic and digital signatures around the world.

Countries where e-signatures are legal, admissible and enforceable.

The following countries treat electronic and written signatures equally. There are sometimes exceptions for highly regulated industries (e.g. real estate) or contracts with the government. The only additional requirement is that the agreement includes language where the parties agree to conduct business electronically. This statement is automatically added to all agreements signed through Adobe Document Cloud.

| | | |
|----------------|-------------|--------------|
| Argentina | Hang Kong | Singapore |
| Australia | Hungary | South Africa |
| Austria | Ireland | South Korea |
| Belgium | Italy | Spain |
| Bermuda | Japan | Switzerland |
| Canada | Mexico | Taiwan |
| Chile | Netherlands | Thailand |
| China | New Zealand | Uruguay |
| Colombia | Norway | UA Emirates |
| Czech Republic | Poland | UK |
| Finland | Portugal | USA |
| France | Romania | |
| Germany | Russia | |

Countries where digital signatures are legal, admissible and enforceable.

In these countries, electronic signatures do not have the same enforceability as other types of signatures. This is sometimes the case where a country has stated an explicit preference for the usage of authenticated digital signatures.

Because of this, it may be helpful to insert a clause stating that U.S. law (or governing law of another country where e-signatures are accepted) shall apply to the agreement or to have signers return their signatures via fax.

Brazil
Denmark
Indonesia
Israel
Macao
Malaysia
Peru
Philippines
Sweden
Turkey

International Landscape

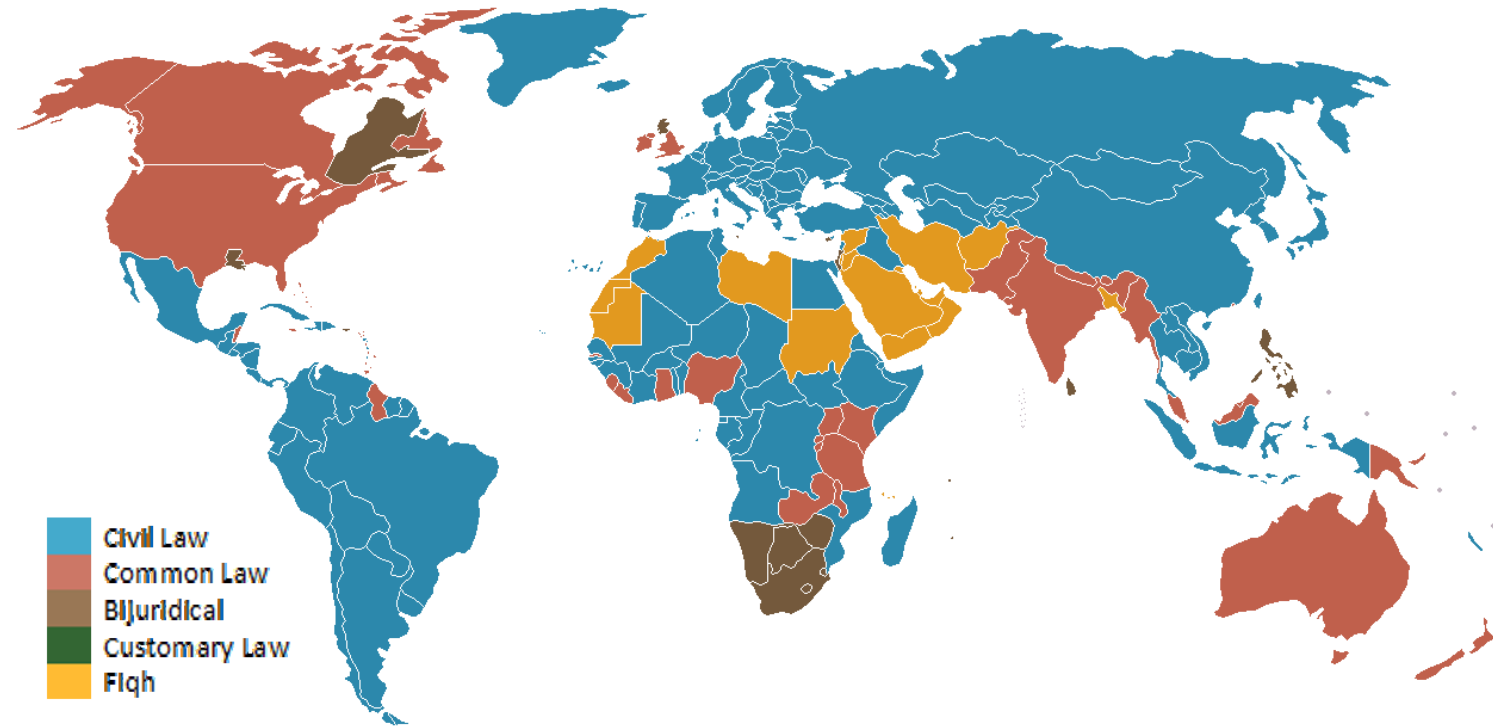
Most Common Law countries (including the **US**, **Canada**, the **UK**, and **Australia**) **follow a “Minimalist” model**, where electronic signatures are the legal equivalent of a handwritten signature.

Most Civil Law countries (including most of **Europe** and **Latin America**) **follow a “Two Tier” model** to electronic signature, modelled on the 1996 UNCITRAL Model law on Electronic Commerce:

“Simple” E-Signature is admissible as evidence, and generally sufficient for commercial transactions

“Qualified Electronic Signature” also called Digital Signature, may have extra-legal weight (such as a presumption of authenticity), or may be required for certain purposes, such as submitting documents to government agencies.

- QES must use specific cryptographic technology called Public Key Infrastructure (PKI)
- The PKI process involves a digital certificate, which must be issued by a Certificate Authority that is approved by the government (or issued by the government itself)



DS Issuance in Different Countries

- Different countries have different types of Laws or use of Digital Signatures
- Private / Public Organizations issue DS both through Online and Offline process, **WHICHEVER THE USER PREFERS.**
- Signatory has to provide credentials verifying their right to sign: a proof of ownership of a unique e-mail address and a password to login.

In almost all Developed Countries, DS can be issued through an Online Application process

Singapore

New Zealand

China

United States

Sweden

United Kingdom

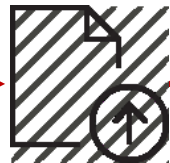
Keys Steps for Getting Digital Signatures Through Online Application



Log in to E-Signature Issuing Portal



Upload Required documents/ Unique Identification details for the signer



Upload the document to be digitally signed



Add a signature



To reposition/ move the signature block



Public Key Generated for Verification



Signing Successful!

Methods for Providing Digital Signatures to Individuals and Legal Entities

Private Key Protection

- The Private key generated is to be protected and kept secret. The responsibility of the secrecy of the key lies with the owner.
- The key is secured using
 - PIN Protected soft token
 - Smart Cards
 - Hardware Tokens



Smart Cards

- The Private key is generated in the crypto module residing in the smart card.
- The key is kept in the memory of the smart card.
- The key is highly secured as it doesn't leave the card, the message digest is sent inside the card for signing, and the signatures leave the card.
- The card gives mobility to the key and signing can be done on any system. (Having smart card reader)



PIN Protected Soft-Tokens

- Private key is encrypted and kept on the Hard Disk in a file, this file is password protected.
- Forms the lowest level of security in protecting key, as
 - The key is highly reachable.
 - PIN can be easily known or cracked.
- Soft tokens are also not preferred because
 - The key becomes static and machine dependent.
 - The key is in known file format.



Hardware Tokens

- They are similar to smart cards in functionality as
 - Key is generated inside the token.
 - Key is highly secured as it doesn't leave the token.
 - Highly portable.
 - Machine Independent.
- iKEY is one of the most commonly used token as it doesn't need a special reader and can be connected to the system using USB port.



Different Classes of Digital Signatures issued Online as well as in Person

Class 1 : Simple Requests for Information requiring Identification

Class 1 certificates issued to individuals.

Simple E-Signature sufficient, no need for PKI based DS.

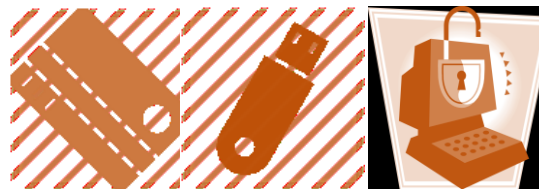
These certificates will confirm that user's name (or alias) and E-mail address form an unambiguous subject within the Certifying Authorities database.



Class 2: Request for providing Services or Accessing Financial Information

Class 2 certificates issued to both business personnel and private individuals.

These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well recognized consumer databases.



Class 3: Carrying out Financial Transactions or Transactions which bestow or transfer rights

Class 3 certificates issued to individuals as well as organizations.

These are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals on their personal (physical) appearance before the CAs or going through a Video Screening Process.



How an Individual Can Get a DS

Individuals and Legal Entities can get DS / DSC by applying ONLINE to the Certifying Authority (CA)



Selecting the best Delivery Mechanism for issuing DSCs

Apply in Person

Merits

- Perceived to be more secure
- Easier to hand over Private Key – less risk of impersonation

Demerits

- Huge inconvenience to public – compromises the GoU's purpose and goals of E-Government of making life easier for Business and individual
- Puts an enormous additional workload on field offices and staff
- Higher financial and economic cost
- Longer gestation and implementation period

Issue Online

Merits

- Much more convenient to public
- Lower workload on government machinery
- Tighter Security – better Audit Trail than paper based process; relies on IT security strength, rather than on individual's competence and integrity
- Lower Total Cost of Ownership in the long run

Demerits

- Perceived to be less secure
- Higher investment in upfront technology costs

Global Best Practices : Recommendations

- **Evaluate and define what kind of ES or DS is most relevant to which kind of services / transactions**, based upon risk and strategic considerations
- **Establish a 2 or 3 Tier Digital Signature system** modelled on the 1996 UNCITRAL Model law on Electronic Commerce, as is the case in most Civil Law countries.
- **DS Law should not force contracting parties** (whether the government or the private sector) to use or accept electronic signatures and records, **EXCEPT where the GoU is convinced of** the need to make it mandatory to use DS only due to its **overwhelming public benefits**, in order to substantially improve the quality (reliability), availability (efficiency) and access (transparency and accountability) of critical electronic data.
- **Provide viable solution and support to individuals and entities which do not have easy access to technology infrastructure** for undertaking DS transactions. For instance provide facilitation through Single Window Kiosks or through private sector service providers.
- **Adopt a standardized system**, based upon international best practices and protocols, for generating DSCs across the country which can be used for ALL services.

Global Best Practices : Recommendations

- **Issue Guidelines to existing six Certifying Authorities** (CAs), under the Root Certificate Authority (RCA), under ICT Ministry. RCA to issue Public Key Certificates to the licenced CAs (who will issues the Digital Signature Certificates to the end Users) to use the same platform, technology and protocols to generate the **DSCs so that interoperability across CAs can be assured**.
- **Implement** Hyper Text Transfer Protocol Secure (**HTTPS**) as the standard protocol over which data is sent between the user's browser and the GoU's Single Portal **and adopt SSL** (Secure Sockets Layer) protocols, preferably with Extended Validation Certificate.
- **Implement an ISO/IEC 27001** - Information security management Standard for the entire process, organisations and infrastructure involved in Digital Signature Certification process.
- **Provide multiple delivery choices to citizens** to select which is the preferred process through which they would like to receive DSCs
- Develop a phased plan to ensure that all the affected agencies, laws, regulations, policies, and procedures are aligned for the implementation of DS Law.
- **Develop detailed guidelines for specific sectors and transactions**, if required.

Rahmat



Sanjay Saxena
Sanjay@tscpl.com

Case Study : India

How to make Digital Signatures Work

Entities Involved in Providing DSs

- Root Certificate Authority (RCA) issues Public Key Certificates to the licenced Certifying Authorities (CAs)/ DSC Providers
- CAs issues the DSC to the end User
- CAs are the digital world's equivalent to passport offices. They issue digital signature certificates and validate holders' identity and authority.
- CAs embed an individual or institution's public key along with other identifying information into each digital certificate
- CAs cryptographically sign it as a tamper-proof seal verifying the integrity of the data within it, and validating its use.
- In various countries different DSC providers issue DSCs in compliance to the Electronic Signature Law of the respective country

Certifying Authority (CA)/ DSC Providers

- Trusted Third Party
- An organization which issues DSC to the end User
- Assures the identity of the parties to whom it issues certificates
- Maintains online access to the public key certificates issued

In India, CCA as the 'Root' Authority certifies the technologies & practices of all the CAs. Certifying Authorities (CA) has been granted a license to issue a digital signature certificate by Controller of Certifying Authority (CCA) under Section 24 of the Indian IT-Act 2000.

How to Get DS / DSC in India

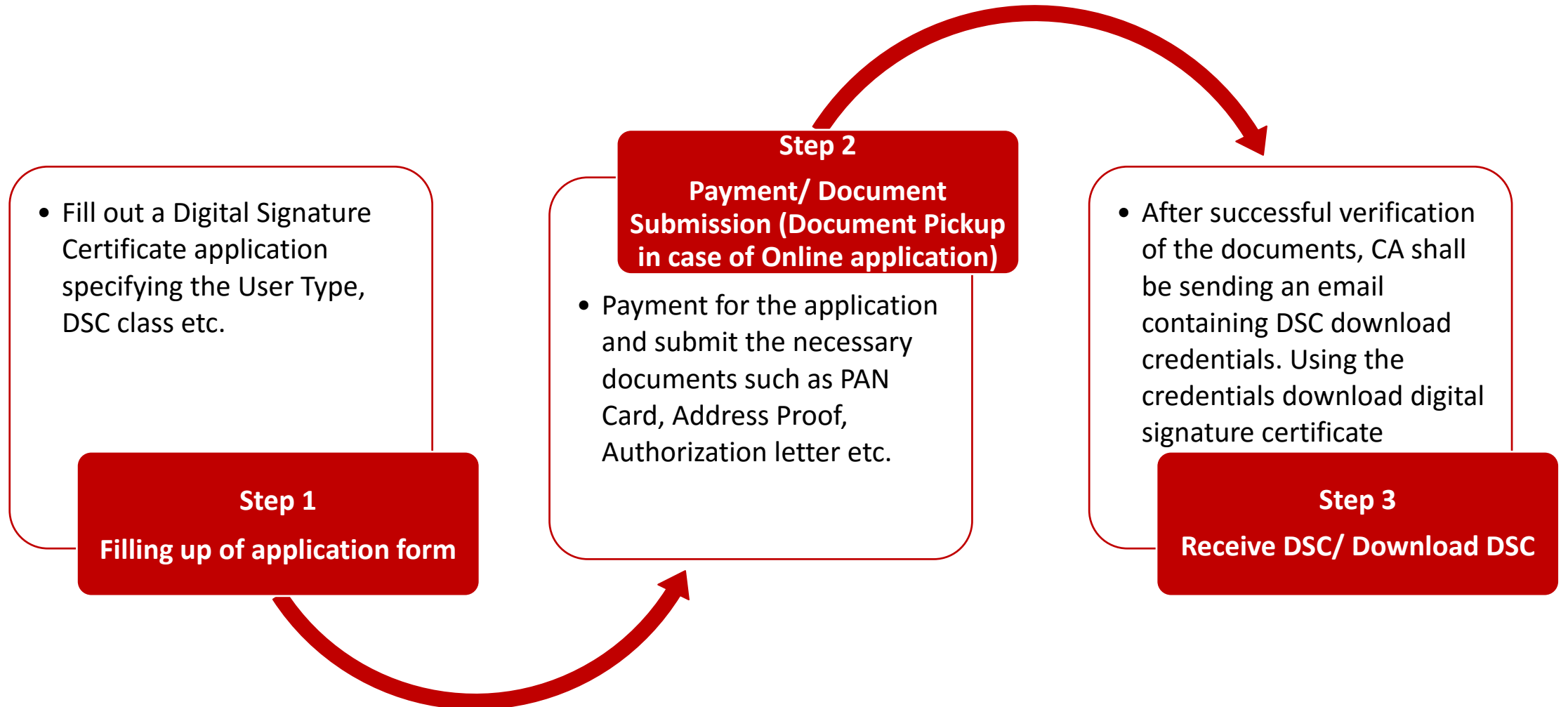
- DSC applicants can directly approach Certifying Authorities (CAs) with original supporting documents.
- DSCs can also be obtained, wherever offered by CA, using Aadhar eKYC based authentication.



Certifying Authorities in India



Process of Getting DS in India



Typical Digital Signature Certificates Categories

Assurance Level

CLASS 1

Class 1 certificates issued to individuals / private subscribers. These certificates will confirm that user's name (or alias) and E-mail address form an unambiguous subject within the Certifying Authorities database.

CLASS 2

Class 2 certificates issued to both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well recognized consumer databases.

CLASS 3

Class 3 certificates issued to individuals as well as organizations. These are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals on their personal (physical) appearance before the Certifying Authorities or going through a Video Screening Process.

Applicability

Basic level of assurance where risks and consequences of data compromise are not considered to be of major significance.

Suitable for access to private information where the likelihood of malicious access is not high.

Suitable for environments where risks and consequences of data compromise are moderate. This may include transactions having monetary value or involving access to private information where the likelihood of malicious access is moderate.

This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

Class 1 Digital Signature Certificates

- Class 1 Certificates offer the lowest level of assurance individual certificates, whose issuance is without validation process and issued to E-Mail address of the applicant.
- They are appropriate for digital signatures, encryption, and access control for non-commercial or low-value transactions where proof of identity is unnecessary.
- Certificates do not facilitate strong authentication of the identity of the Subscriber; hence are not intended for, and shall not be relied upon, for commercial use where proof of identity is required.
- **CA's issue them on special request and in bulk orders as Class 1 certificates are not accepted by the government.**

Steps for Getting an Individual Class 1 Digital Certificate Online

DSC Class 1 Form **can be filled** on the website of the CA



Online Enrollment - In the first step, you will be providing your Digital Certificate details and generating a cryptographic key pair.

Monitoring the Progress of Your Application
You will receive an automated e-mail updates on the status of your application.



Downloading your Digital Certificate

Once your certificate is generated, you will receive an e-mail notification. It will include detailed instructions and an **Authentication Code** that needs to be entered at the time of certificate download.

Class 2 Digital Signature Certificates

- A Class 2 Digital Signature Certificate is used by individuals and is available for download after verification based on a trusted and pre-verified database.
- Class 2 Digital Signature Certificates are generally used for filing documents Income Tax, Registrar of Companies and VAT



Steps for Getting an Individual Class 2 Digital Certificate Online

DSC Class 2 Form **can be filled** on the website of the CA



On filling the form using Adhaar (UIDAI) eKYC with required details, user goes through a video screening process.

On successful submission of the form, CA processes the Digital Signatures and issues the DSC.



Username and password are sent to applicant mailbox in order for him/her to log onto CA website and download the DSC.

The **cryptographic device** is mailed to the user for storing the DSC.



Class 3 Digital Signature Certificates

- Class 3 Digital Signature provides highest level of security and can be used by individuals or organizations for personal or commercial purpose like e-tendering, e-ticketing, e-auction, e-bidding and e-procurement. It is the upgraded version of Class 2 Digital Signature and comes with next level of security.
- The main reason to use Class 3 DSC is Security, Confidentiality and Integrity. A Class 3 Digital Signature Certificate contains the company name and is issued to only those person of the organization which are authorized to represent that organization



Steps for Getting an Individual Class 3 Digital Certificate Online

DSC Class 3 Form **can be filled** on the website of the CA



On filling the form using Aadhaar eKYC with required details, user goes through a video screening process.

On successful submission of the form, CA processes the Digital Signatures and generates the **DSC**.







Username and password are sent to applicant mailbox in order for him/her to log onto CA website and download the DSC.

The **cryptographic device** is mailed to the user for storing the DSC.



Example - Applying for DSC Online Through One of the Listed Certifying Authorities

Select the type of certificate desired (e-Mudhra Portal)

| CERTIFICATES BY USAGE | | | | | |
|--|---|---|--|---|---|
| <div>MCA (ROC)</div> <div>Class 2 Signature</div> <div></div> <div>Rs. 899 Onwards</div> <div>APPLY NOW</div> | <div>INCOME TAX</div> <div>Class 2 Signature</div> <div></div> <div>Rs. 899 Onwards</div> <div>APPLY NOW</div> | <div>E-TENDER</div> <div>Class 3 Signature</div> <div></div> <div>Rs. 899 Onwards</div> <div>APPLY NOW</div> | <div>FOREIGN-TRADE</div> <div>DGFT Signature</div> <div></div> <div>Rs. 2499 Onwards</div> <div>APPLY NOW</div> | | |
| | | | | | |
| INDIVIDUAL | | DIGITAL CERTIFICATES | | | |
| <div>CLASS 2 SIGNATURE</div> <div>Rs. 899 Onwards</div> <div>APPLY NOW</div> | <div>CLASS 2 ENCRYPTION</div> <div>Rs. 899 Onwards</div> <div>APPLY NOW</div> | <div>CLASS 3 SIGNATURE</div> <div>Rs. 1999 Onwards</div> <div>APPLY NOW</div> | <div>CLASS 3 ENCRYPTION</div> <div>Rs. 1999 Onwards</div> <div>APPLY NOW</div> | <div>CLASS 2 COMBO</div> <div>Rs. 1899 Onwards</div> <div>APPLY NOW</div> | <div>CLASS 3 COMBO</div> <div>Rs. 2999 Onwards</div> <div>APPLY NOW</div> |
| | | | | | |
| ORGANISATIONS | | DIGITAL CERTIFICATES | | | |
| <div>CLASS 2 SIGNATURE</div> <div>Rs. 899 Onwards</div> <div>APPLY NOW</div> | <div>CLASS 2 ENCRYPTION</div> <div>Rs. 899 Onwards</div> <div>APPLY NOW</div> | <div>CLASS 3 SIGNATURE</div> <div>Rs. 1999 Onwards</div> <div>APPLY NOW</div> | <div>CLASS 3 ENCRYPTION</div> <div>Rs. 1999 Onwards</div> <div>APPLY NOW</div> | <div>CLASS 2 COMBO</div> <div>Rs. 1899 Onwards</div> <div>APPLY NOW</div> | <div>CLASS 3 COMBO</div> <div>Rs. 2999 Onwards</div> <div>APPLY NOW</div> |



Example - Applying for DSC Online Through One of the Listed Certifying Authorities

Lets assume that an individual user wants the DSC, I have chosen Individual Class 3 Certificate (Process for Class 2 Certificate is entirely similar, only difference being in the Cost, which is Rs - 1269 for Class 2 Certificate)

| CHOOSE YOUR CERTIFICATE | | |
|---|--|---|
| 1 <input type="radio"/> Class 2 Certificates <input checked="" type="radio"/> Class 3 Certificates <input type="radio"/> DGFT | CLASS 3 SIGNATURE - INDIVIDUAL 1 YEAR Rs. 1999 | |
| 2 <input checked="" type="radio"/> Individual <input type="radio"/> Organization | | |
| 3 <input checked="" type="radio"/> 1 Year <input type="radio"/> 2 Years | | |
| 4 <input checked="" type="radio"/> Signature <input type="radio"/> Encryption <input type="radio"/> Both (Combo) | | |
| PAPERLESS ONLINE PROCESS | WALK INTO OUR OFFICE | PHYSICAL DOCUMENT SUBMISSION |
| Have an Aadhaar Number registered with Mobile / eMail ID and a webcam or a smartphone. Discount of Rs. 300/- | Visit any of our offices and get your Digital Signature through Aadhaar. | Fill up the application form and apply through the conventional mode. |
| PROCEED | PROCEED | PROCEED |

Example - Applying for DSC Online Through One of the Listed Certifying Authorities


User chose 'Paperless Online Process' and filled the required details as shown below


| APPLICANT DETAILS | |
|---|--|
| Aadhaar | <input type="text" value="661720033255"/> <input type="button" value="GET OTP"/> |
| OTP | <input type="text" value="412266"/> |
| Define your own password (Challenge Code) to download your DSC, once approved by eMudhra CA. The same will also be sent to you over SMS / email after approval. | |
| Challenge Code | <input type="text" value="....."/> |
| Confirm Challenge Code | <input type="text" value="....."/> |
| PAN is optional. However, we recommend to provide it, as PAN is mandatory in case you are using DSC for Income Tax Filing, Tenders, etc. | |
| PAN | <input type="text" value="GFVPS7198M"/> |

| DSC DETAILS | |
|---|--|
| Class Type | <input type="radio"/> Class 2 <input checked="" type="radio"/> Class 3 |
| User Type | <input checked="" type="radio"/> Individual |
| Certificate Type | <input checked="" type="radio"/> Signature <input type="radio"/> Encryption <input type="radio"/> Both |
| Validity | <input checked="" type="radio"/> 1 Year <input type="radio"/> 2 Years |
| Need USB Token* | <input checked="" type="radio"/> Yes (Rs.550) <input type="radio"/> No |
| <input type="checkbox"/> USB token has to be sent to a different address (other than Aadhaar address) | |

| PRICE | |
|------------------|-------------|
| Certificate Cost | Rs. 1999 |
| Discount Amount | (- Rs. 300) |
| Token Cost | Rs. 550 |
| Taxes (ST/VAT) | Rs. 285 |
| Total Amount | Rs. 2534 |

Captcha





RESET

PROCEED

Live C

Example - Applying for DSC Online Through One of the Listed Certifying Authorities

User was shown his/her Personal Details linked with the Adhaar Card (UIDAI) and was asked to proceed for payment

| APPLICATION DETAILS | |
|-----------------------------|---|
| Application ID | 3243707 |
| Aadhaar Number | 661720033255 |
| Common Name | Gunraj Singh |
| Gender | Male |
| Date Of Birth | 15-Nov-1991 |
| Address | House No 48,Near Officer Enclave,Hem Bagh,Patiala,Patiala,Patiala,P atiala,Punjab,147001 |
| State | Punjab |
| Town/City/District | Patiala |
| Postal Code | 147001 |
| Mobile | 9780509005 |
| Email ID | Not available |
| Nationality | INDIAN |
| Email ID | <input type="text" value="gunraj.singh91@gmail.com"/> |
| Class of Certificate | Class 3 |
| User Type | Individual |
| Certificate Type | Signature |
| Certificate Validity | 1 Year |
| PAN of Applicant (optional) | GFVPS7198M |
| Total Amount | Rs. 2534 |

I provide my consent to use my eKYC done in previous step, to process an electronic signature and affix on DSC application form being generated.

PROCEED FOR PAYMENT

Example - Applying for DSC Online Through One of the Listed Certifying Authorities

Next Step was to provide the payment details

| PRODUCT | AMOUNT PAYABLE |
|--|----------------|
| Class 3 Individual Signature 1 Year With Token (Aadhaar OTP) | ₹ 2534.00 |

MAKE PAYMENT

Credit Card

Debit Card

Net Banking

Cash Card

VISA

MasterCard

Diners Club International

Maestro

AMERICAN EXPRESS

SafeKey

SECURED BY PAYU

Card Number

Card Number

Name on Card

Name on Card

Expiry Month

Month

Expiry Year

Year

CVV

CVV

Note: After clicking on the "Make Payment" button you might be taken to your bank's website for 3D secure authentication.

Make Payment

VERIFIED by VISA

MasterCard SecureCode

VeriSign Secured

PCI Security Standards Council

Example - Applying for DSC Online Through One of the Listed Certifying Authorities

After making the payment, In the final step user underwent a video verification process, where he was supposed to answer vocally three questions being displayed on the screen.



Example - Applying for DSC by Walk-In Process Through One of the Certifying Authorities

User chose 'Walking Into Our office' process, he/she was asked to choose the preferred location.

CHOOSE YOUR PREFERRED LOCATION



Select Branch

Ahmedabad
Bangalore
Chennai
Cochin
Coimbatore
Delhi
Hyderabad
Indore
Kolkata
Mumbai
Pune
Patna
Salem
Surat

Example - Applying for DSC by Walk-In Process Through One of the Certifying Authorities

User Chose Delhi as preferred location and filled the required details

CERTIFICATE DETAILS

Certificate Cost :

Rs. 1999

Token Cost :

Rs. 550

Taxes (ST/VAT):

Rs. 330

Total Amount:

Rs. 2879

Class Type *

☐ Class 2

☒ Class 3

User Type *

☒ Individual

Certificate Type*

☒ Signature

☐ Encryption

☐ Both

Certificate Validity*

☒ 1 Year

☐ 2 Years

Need USB Token

☒ Yes (Rs.550)

☐ No

* Mandatory

APPLICANT DETAILS

Applicant Name*

Gunraj

Singh

Initial (Optional)

Aadhaar*

661720033255

Email*

gunraj.singh91@gmail.com

The email ID should belong to the applicant only

Mobile No*

9780509005

The mobile number should belong to the applicant only

Selected Branch :

Delhi

Address to Visit :

109(Ground Floor), Vikas Complex,36,
Veer Savarkar Block Vikas Marg,
Delhi - 110092
Phone: +91 11 42404143

RESET

PROCEED TO PAYMENT

Example - Applying for DSC by Walk-In Process Through One of the Certifying Authorities

Next Step was to provide the payment details

| BASE PRICE | SERVICE TAX 15% | TOKEN PRICE | VAT 5.5% | AMOUNT PAYABLE |
|------------|--------------------|-------------|-------------|----------------|
| ₹ 899.00 | ₹ 134.85 | ₹ 550.00 | ₹ 30.25 | ₹ 1614.00 |








MAKE PAYMENT

Credit Card

Debit Card

Net Banking

Cash Card



Card Number

Name on Card

Expiry Month

Month





Expiry Year

Year

CVV

Note: After clicking on the "Make Payment" button you might be taken to your bank's website for 3D secure authentication.

Make Payment



After making the payment, user was required to walk in with the receipt to the selected branch and get the DSC

Leading Countries

How are they making Digital Signatures work

Electronic Signature Law - Hong Kong

Electronic signature law

Electronic Transactions Ordinance

Are electronic signatures legal, admissible and enforceable?

Yes, Section 6(1) states that an electronic signature may be used to satisfy the legal requirement for a handwritten signature. Section 17(2) states that electronic records may be used in place of paper records and that those records will have the same legal enforceability as paper records.

Summary of law

Hong Kong follows the European Union and the UNCITRAL model law in that its laws provide for the enforcement of both simple electronic signatures and digital signatures (sometimes called advanced electronic signatures). It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

One must get consent to do business electronically, but that consent doesn't need to be explicit. It can be inferred from behavior such as receiving and signing documents electronically.

Key restrictions

The law excludes wills, powers of attorney, government leases and some real estate transactions.



Digital Signature in Hong Kong

Currently there are 2 recognized CAs under the Electronic Transactions Ordinance (ETO) in Hong Kong –

- Postmaster General (Hong Kong Post Certification Authority)
- Digi-Sign Certification Services Limited

| Types of Digital Certificates | Usage |
|-------------------------------|---|
| Personal | For Individuals to conduct secure message transmissions as well as electronic transactions by means of digital signing and encryption/decryption |
| Organizational | For staff of organizations to conduct secure message transmissions as well as electronic transactions by means of digital signing and encryption/decryption |
| Encipherment | For individuals or staff organizations to conduct secure message transmissions by means of encryption/decryption |
| Server | For single or multiple server(s) authentication |
| Governmental | For staff of Government bureaux/departments to conduct secure message transmissions as well as electronic transactions by means of digital signing and encryption/decryption |
| Organizational Role | For staff of organizations to conduct secure message transmissions as well as electronic transactions by means of digital signing and encryption/decryption or and on behalf of their role in the organizations |

Steps for Getting a Personal Id-Cert Class 1 Certificate Online

Personal Id-Cert Class 1 Form **can be filled** on the website of the Digi-Sign Certification



Fill the form using **HKID No.** with required details,

At the end of the form, user gets an option to get the **Certificate delivered** at the desired location (Within HongKong)



At the time of Certificate Delivery, User has to **sign the physical application form**

Id-Cert Class 1 Form Online (Hong Kong)

Online Application Form For Personal ID-Cert Class 1

Privacy Statement

Digi-Sign Certification Services Limited recognizes the importance of protection of personal data governed by the Personal Data (Privacy) Ordinance (Cap. 486). Digi-Sign has a framework in place for protection of the privacy of personal data collected in the subscriber application. Please refer to the [Privacy Policy Statement - Digi-Sign Certification Services Limited](#), a copy of which is available from the Digi-Sign Office and the Digi-Sign web site at www.dg-sign.com.

Important Notice

You should note carefully the [Certification Practice Statement \(CPS\)](#) and the [Subscriber Terms and Conditions](#) before completing this form.

You will have to sign the physical application form at the time of collecting your Personal ID-Cert Class 1 with your presence in Hong Kong.

For the subscription fee and other relevant charges for online applications, Digi-Sign accepts payment by Visa / Master Card, cheque or e-Cheque.

Fields with *are mandatory and all inputs must be in English

Salutation*

☐ Mr. ☐ Mrs. ☐ Ms. ☐ Miss

(Surname, Given Name and Date of Birth must be the same as appeared on your identity document.)

Surname*

Given Name*

Date of Birth*

Year Month Day

Identity Document*

☐ HKID No.

()

☐ Passport No./Travel Document No.

Issuing Authority

Correspondence Address*

Blk/Bldg

Street

District

Area

☐ HK ☐ KLN ☐ NT ☐ Others

Country*

Hong Kong

Telephone No. *

Home

Office

Mobile/Pager

Fax No.

Email address to be displayed on ID-Cert

(Note: If you choose to provide an email address, it will be displayed on your certificate and published at Digi-Sign's repository. If you choose not to provide an email address, your certificate may not be used for signing or encrypting emails.)

☐ Check this if your contact email address is the same as above. Otherwise please indicate your contact email address below.

Email address for contact purposes

☐ Check this if you would like to apply for an Encipherment ID-Cert Class 3.

(Note: If you apply for the Encipherment ID-Cert Class 3 now, the application fee will be waived. The holding device for the Encipherment ID-Cert Class 3 HK\$30 will be charged.)

Please select one of the options below:

☐ I will collect my Personal ID-Cert Class 1 at Digi-Sign's office

☐ Digi-Sign will deliver my Personal ID-Cert Class 1 to me (within the Hong Kong territory only) and I will pay Digi-Sign the delivery charge.

For the charge, please refer to the Digi-Sign [website](#).

Digi-Sign Reference (for use by Digi-Sign's partners)

Declaration by the Applicant

I hereby apply for a Personal ID-Cert Class 1 (*and, if applicable, Encipherment ID-Cert Class 3) to be issued by Digi-Sign Certification Services Limited in my name as stated above and I have read and understood and agreed to be bound by the Subscriber Terms and Conditions and the provisions in the Certification Practice Statement (CPS).

Submit

Clear

Electronic Signature Law - Singapore

Electronic signature law

Electronic Transactions Act 2010

Are electronic signatures legal, admissible and enforceable?

Yes, Section 8 states that one can meet the legal requirement for a handwritten signature by using an electronic signature or communication.

Summary of law

Singapore is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Under the law, the signature method used must be either “(i) as reliable as appropriate for the purpose for which the electronic record was generated or communicated, or (ii) proven in fact to have identified the signatory and to indicate signatory’s intention with respect to the information by itself or together with further evidence.”

Key restrictions

The law excludes wills, negotiable instruments, powers of attorney and some real estate transactions.



Electronic Signature Law - New Zealand

Electronic signature law

Electronic Transactions Act

Are electronic signatures legal, admissible and enforceable?

Yes, Section 8 provides that information will not be denied legal effect solely because it is in electronic form.

Summary of law

New Zealand's electronic signature law can be classified as permissive or minimalist. Under the law, parties to an agreement can freely agree on the type of signature to use, including simple electronic signatures. The primary requirements are that the parties agree on the form of signature, and the electronic document remains readily accessible to the parties.

Key restrictions

While the law does not exclude particular types of agreements, some agreements, like real estate transfers and wills, have additional requirements.



Electronic Signature Law - Republic of Korea

Electronic signature law

Digital Signature Act

Are electronic signatures legal, admissible and enforceable?

Yes, as long as the parties explicitly consent to electronic signatures per Article 3(3) of the enactment.

Summary of law

The Republic of Korea's e-signature laws are modeled after a combination of the EU Directive on Electronic Signatures and UNCITRAL Model Law. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Like many other countries, consent is required for allowing electronic signatures. However, if no such explicit agreement exists between the parties or the identity of the signer or the authenticity or integrity of the message sent is questioned, the effect of the electronic signature has to be determined by interpreting the true intention of the parties in accordance with the general principle of contract interpretation.

Key restrictions

There are no critical restrictions.



Electronic Signature Law - China

Electronic signature law

Electronic Signature Law of the People's Republic of China



Are electronic signatures legal, admissible and enforceable?

Yes, Article 14 recognizes electronic signatures as legal and enforceable, while Articles 7 and 8 provide for the admissibility.

Summary of law

China's law is modeled on a combination of the EU Directive on Electronic Signatures, UNCITRAL Model Laws and United Nations Conventions on Electronic Communications in International Contracts. It provides for the enforcement of both simple electronic signatures and digital signatures. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case. Electronic signatures are presumed valid unless proof to the contrary is produced.

Despite the clear legal support for electronic signatures, some judges in China are still averse to recognizing them. As a result, you may wish to use handwritten signatures for more sensitive matters like employment contracts.

Key restrictions

Agreements related to personal relationships (such as marriage, adoption, inheritance), some real estate agreements and agreements related to the suspension of public utilities are exempted from the law.

Electronic Signature Law - United States

Electronic signature law

Electronic Signatures in Global and National Commerce Act (ESIGN) and Uniform Electronic Transactions Act (UETA)

Are electronic signatures legal, admissible and enforceable?

Yes, both the ESIGN Act and UETA provide that a signature will not be denied legal effect or enforceability solely because it is in electronic form.

Summary of law

The federal government adopted ESIGN in 2000. In addition, every state has adopted an electronic signature law, with 47 adopting a version based on UETA. These minimalist, or permissive, laws permit the use of electronic signatures for virtually all types of agreements. However, it is important to obtain the prior consent of all parties to conduct business electronically.

Key restrictions

The ESIGN Act and most state laws exclude real property transfers, wills and some legally required notices to consumers.



Electronic Signature Law - Norway

Electronic signature law

Electronic Signatures Act 2001 (no translation available)

Are electronic signatures legal, admissible and enforceable?

Yes, Section 6 recognizes electronic signatures as legal and enforceable.

Summary of law

Norway follows the European Union model. It is considered a two-tier jurisdiction because it gives digital signatures the same status as handwritten signatures but also recognizes simple electronic signatures as legal and enforceable. Countries that follow this model give companies the opportunity to select different forms of signatures and customize their business processes based on the form that is most convenient and appropriate for each use case.

Electronic signatures are presumed valid unless proof to the contrary is produced, but they do not have the same status as digital (or qualified electronic) signatures.

Key restrictions

Debt certificates, premarital agreements and a board's signing of annual accounts are examples of excluded transactions.



Electronic Signature Law - Russian Federation

Electronic Signature law

Federal Law No. 63-FZ, “On Digital Signature” (July 01, 2011)
Federal Law No. 149-FZ, “On Information, Information Technology and Protection of Information” (July 27, 2006) Part Four of Civil Code of the Russian Federation (Art. 160)
(no links available)

Are electronic signatures legal, admissible and enforceable?

Yes, Russian law recognizes electronic signatures as legal, admissible and enforceable when the parties explicitly agree to use them. However, for enforceable digital signatures, Russia requires that one use a certificate and service provider that has been certified by the Russian government.

Summary of law

Russian courts have held that a signature may not be denied validity simply because it is electronic. However, to be clearly enforceable, digital signatures must be exchanged through a government-certified, specialized service provider that acts as an electronic courier in order to enable electronic document exchange.

Key restrictions

There are no critical exceptions to the law.



Electronic Signature Law - European Union (1/2)

Electronic signature law

Electronic Identification and Authentication Services Regulation (910/2014/EC)

Are electronic signatures legal, admissible and enforceable?

Yes, electronic signatures are valid with prior consent.

Summary of law

In 1999, the European Union passed the Electronic Signature Directive (1999/93/EC) which member states used as the foundation for country-specific laws. On July 23, 2014, the EU adopted its replacement, the Electronic Identification and Trust Services Regulation (910/2014/EC). Commonly referred to as eIDAS, the regulation establishes a new legal structure for electronic identification, signatures, seals and documents throughout the EU. eIDAS will come into effect on July 1, 2016. On that date, the existing EU directive as well as any laws of EU member states that are inconsistent with eIDAS will be automatically repealed, replaced or modified. For the first time, there will be a consistent legal framework and a single market for the recognition of electronic signatures and identities across all of the EU. This provides companies with a predictable legal environment in which to develop and expand the use of electronic signatures in the EU.

Article 25 of the eIDAS maintains the fundamental legal rule that all electronic signatures and verification services shall be admissible as evidence in legal proceedings. This includes electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication.



Electronic Signature Law - European Union (2/2)

eIDAS and Basic Electronic Signatures

The basic definition of electronic signature is unchanged under eIDAS with respect to the earlier regulation. The law holds that an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely based on the fact that it is in electronic form.

eIDAS and Advanced Electronic Signatures

The regulation introduces a new definition for advanced electronic signatures. Advanced electronic signatures allow unique identification and authentication of the signer of a document enable the verification of the integrity of the signed agreement, typically through the issuance of a digital certificate by a certificate authority to that signer.

eIDAS and Qualified Electronic Signatures

Another new definition under eIDAS is the qualified electronic signatures. While both advanced and qualified electronic signatures are uniquely linked to the signer, qualified electronic signatures are based on qualified certificates. Qualified certificates can be issued only by a certificate authority that has been accredited and supervised by authorities designated by the EU member states and must meet the requirements of eIDAS. Qualified certificates must also be stored on a qualified signature creation device such as a smart card, a USB token or a cloud-based hardware security module (HSM). While both basic electronic signatures and advanced electronic signatures are legal, admissible and enforceable under eIDAS, only qualified electronic signatures are deemed to be legally identical to handwritten signatures. Importantly, they are also the only type of electronic signature that will be mutual recognized by all of the EU member states. Thus, while it is not necessary to use a qualified electronic signature in every instance, it is a useful tool when executing some types of agreements.

