Digital Signature FAQs

❖ **What is a Digital Signature**?

A digital signature is an electronic form of a signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and also ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable and cannot be imitated by someone else. The ability to ensure that the original signed message arrived means that the sender cannot easily disclaim it later.

❖ **What is a Digital Signature Certificates?**

Digital Signature Certificates (DSC) is the electronic format of physical or paper certificate like a driving License, passport etc. Certificates serve as proof of identity of an individual for a certain purpose; for example, a Passport identifies someone as a citizen of that country; who can legally travel to any country. Likewise, a Digital Signature Certificate can be presented electronically to prove your identity, to access information or services on the Internet or to sign certain documents digitally.

❖ **Where can I purchase a Digital Signature Certificate?**

Legally valid Digital Signature Certificates are issued only through a Controller of Certifying Authorities (CCA), Govt. of India, licensed Certifying Authorities (CA), such as eMudhra. eMudhra, a Certifying Authority (CA) licensed by CCA, offers secure digital signatures through various options tailored to suit individual as well as organizational needs.

❖ **How does Digital Signature Certificate Works?**

A Digital Signature Certificate explicitly associates the identity of an individual/device with a pair of electronic keys - public and private keys - and this association is endorsed by the CA. The certificate contains information about a user's identity (for example, their name, pincode, country, email address, the date the certificate was issued and the name of the Certifying Authority that issued it). These keys complement each other in that one does not function 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 during information exchange processes. The private key is stored on the user's computer hard disk or on an external device such as a 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 in not available or do not match. This means that the encrypted data cannot be decrypted and therefore, is inaccessible to unauthorized parties.

❖ **Are Digital Signature Certificate legally valid in India?**

Yes, subsequent to the enactment of Information Technology Act 2000 in India, Digital Signature Certificates are legally valid in India. Digital Signature Certificates are issued by licensed Certifying Authorities under the Ministry of Information Technology, Government of India as per the Information Technology Act.

❖ **What are the errors may come in the time Digital Sign?**

As per e-Mudhra manuals, there may be list of errors as mentioned below

List of Error Messages
Invalid arguments supplied.
Invalid argument length.
Unable to contact biometric device.
Device is in use.
RD service is not running.
Invalid argument supplied for device name.
Additional information is not enabled in the configuration file.
Invalid argument CSP Provider.
Invalid argument subject.
Invalid argument thumbprint.
Invalid argument data to sign.
Invalid argument certificate.
Invalid argument type of data to sign.
Invalid argument PKCS7 Data.
Update required for emBridge.
Unable to reach eMudhra server to check for update.
Invalid argument original text.
Unable to fetch certificate for thumbprint.
Unable to connect token.
Invalid Hash length.

Digital Signature FAQs

Invalid Provider Name.
Unable to find slot
Invalid argument Keystore name
Invalid argument Keystore id
Invalid argument Keystore passphrase
PKCS11 driver not found please list token again and try
Invalid argument Provider Name.
Unsupported platform, Windows store not present.
Incorrect token password
Incorrect token password, user pin has been locked
Incorrect token password, final retry left
Token userpin has to be changed
User pin has been locked
Token may be full
Unable to perform operation,Token full
Invalid Encryption
Invalid Encrypted Json
Invalid argument Encrypted Request
Invalid argument Time stamp
Invalid format argument Time stamp please use yyyyMMddTHHmmss
Invalid Hex data length
Updated emBridge version ‘version’ is required
Invalid argument RSA cipher request type
Byte array length of the data is more than accepted (accepted length is ‘data length that can be encrypted’)
Invalid Base-64 data
Invalid certificate or Invalid data
Something went wrong. Error: ‘exception’
Invalid license/license path
Invalid license, license signature is not valid
License is expired please update license.
Invalid license for this product.
Something went wrong while validating License
Unable to decrypt
Data is corrupted
Unable to encrypt
Does not accepts null value for ‘parameter name’
‘property name’ is missing
please provide Input of ID: ‘bulk input id’
please provide ID of data to sign at index of ‘data index’
Invalid request, Request cannot be null
Temp file does not exist
Temp file is not correct
Temp folder path can not be empty
Input list can not be empty
Unable to generate appreance
Unable to genearte Key and IV for AES Cipher due to ‘exception’
AES Encryption failed due to ‘exception’
AES Decryption failed due to ‘exception’