



*How Issuers can Digitally Bulk Sign  
Documents for DigiLocker*

*v1.0*

*Sept 2015*

# Digital Signatures

- “ Currently Signature Certificates (DSC) are given in 3 forms
  - . FIPS certified Hardware (USB Token/HSM)
  - . .pfx/.p12 file
- “ All the 2 types are password protected and follow PKCS (Public Key Cryptography Standard) and contain the private key and public x.509 certificate
- “ X.509 contains the public key, CRL and certificate path validation algorithm

# Types of Certificates

- ” 2 types of certificates can be used to digitally sign documents
- . Digital Signature Certificate
  - . Document Signer Certificate

| Digital Signature Certificate                                       | Document Signer Certificate   |
|---|---|
| Class 2 issued to individuals on a USB Token only                   | Issued to Organizational software applications. Class 2 can be either USB token or soft token |
| Class 3 Issued to Individuals and Organizations on a USB Token only | Class 3 is a USB Token  |
| Signed document will have the signer individual's name              | Signed document will have the organization's name   |

# Bulk Signing Option - 1

## “ Use USB Token:

- . Issuer to obtain any one of the following signing certificates

### “ Class 2 or 3 Digital Signature Certificate

Signature valid

Signed by: Amit Jain  
Using: eSign In DigiLocker  
Date: 04-09-2015 11:36:19

### “ Class 2 or 3 Document Signer Certificate

Signature valid

Signed by : DS EMUDHRA  
CONSUMER SERVICES LTD (3)  
Signed on : 07-Sep-2015 12:34  
Reason : Sample Signing

# Bulk Signing Option - 1

## “ Use USB Token:

- . Attach the USB token with the application server.
- . Use the utilities available that allow an application to use the signing certificate stored in dongle and bulk sign the un-editable documents (preferably PDF) in batch mode or run time mode.

# Bulk Signing Option - 2

## “ Use Soft Token :

- . Issuer to obtain a Class 2 Document Signer Certificate as soft token (.pfx or .p12 file)
- . Store the soft token on the application server.
- . Use the utilities available that allow an application to use the Signing certificate stored in the file and bulk sign the un-editable documents (preferably PDF) in batch mode or run time mode.

