(n)Code® Solutions

License Certifying Authority

CCA Guidelines

- For encryption certificates, CA shall provide key escrow facility, where key pair is securely stored and managed by CA. The key shall be retrievable again by the DSC applicant at any point of time, even after expiry of the certificate. This shall be retained by CA for minimum of 7 years from the expiry of the certificate. CA shall allow the download of the escrowed key only after a successful video verification of the applicant.

- The encryption keys and certificates shall be preserved by subscriber also.

License Certifying Authority

Encryption Cert. Downloads Process

- End User Apply for Sign + Encryption DSC.
- After Final Verification by Verification officer will receive Certificate Downloads Credentials will be shared on Registered Mobile number of END USer.
- End user Downloads the Encryption DSC by Providing Customer ID , Authorization Code, Reference Code , Password for PFX.
-
- On successful validation , .PFX file will be downloaded in the Desktop/Laptop Downloaded Folder. End User can import the Password protected .PFX file in Browser / Token.
- Escrow Key Pairs will be stored in secure Database location.

License Certifying Authority

Escrow Request Process

- End User Request the Escrow key , by accessing the publically available ESCROW URL

  https://usercenter.ncodesolutions.com:8080/DSCApplication/escrowRequest.do

- Validate by Customer ID , First Five character of Customer name and OTPs on Email and mobile separately.

- A fresh Video capture Link will be sent on register email/Mobile of End user.

- After successful Video capture and Verification by two Independent verification officer , Certificate Download Credentials will be shared on Register mobile number of End user.