INTRODUCTION OF DSC

Before delving into the specifics of Class 3 DSC, let's establish a foundational understanding of digital signature certificates. A digital signature serves a similar purpose to a handwritten signature. It provides proof that a digital document or message is authentic and has not been tampered with, ensuring its integrity and genuineness.

Moreover, it provides assurance that the information sent or received has not been tampered with and originates from the identified sender. Digital signature certificates link an individual or organization to a digital key. This creates trust and security during online transactions.

We often do most of our activities online such as filling out forms, using government websites, etc. But with more online activities, there's also more risk of cyber threats, which can threaten our transactions, personal identity, and crucial information. To fight against these risks, many businesses are now using Digital Signature Certificates (DSCs). These are important tools for online safety. As the online world changes, using DSCs is becoming key to staying safe for both individuals and businesses against increasing online threats.

Class 3 Digital Signature Certificates (DSCs) are issued by Certifying Authorities (CAs) and are primarily used for e-commerce applications and online transactions where a high level of security is required. These certificates are utilized to confirm the identity of the signer, as well as to ensure the integrity and authenticity of the digital documents being signed.

Class 3 Combo DSC (Signing + Encryption) especially used to authenticate the identity of the vendors as well as buyers in any e-Procurement, e-Tendering and e-Bidding process. Class 3 Digital Signature Certificate come in three validity, One Year, Two Years and Three Years. A Digital Signature Certificate Class 3, on the other hand, is of a higher level as it is issued only after the registrant’s identity verification has been done by a Registration Authority. There are many types of DSC that cater to specific needs.

BASICS OF DIGITAL SIGNATURE CERTIFICATES

A DSC is a cryptographic key pair consisting of a private key and a public key. The private key is kept confidential, known only to the certificate holder, while the public key is made available publicly. The pairing of these keys enables the creation of digital signatures and verification of the signer's identity. Digital signatures are generated using algorithms that provide a high level of security.

The most common algorithms used for DSCs include RSA (Rivest–Shamir–Adleman) and DSA (Digital Signature Algorithm). These algorithms ensure that the digital signature is unique to the signed data and the signer's private key. The digital certificate verifies your identity, while an encryption certificate encrypts the chest's contents, scrambling them into unreadable code accessible only with the right key. This key generated by the certificate ensures only authorised individuals can unlock and decrypt the information.

CRYPTOGRAPHIC COMPONENTS OF CLASS III DSC

1. **Key Pair Generation**
The cryptographic key pair is the foundation of any DSC, including Class 3. The private key is generated securely, often using hardware security modules (HSMs) to protect against key compromise. The corresponding public key is derived from the private key using mathematical algorithms.
2. **Hash Functions**
Hash functions are employed to create a unique representation (hash value) of the signed data. This hash value is then encrypted with the private key to generate the digital signature. Commonly used hash functions include SHA-256 (Secure Hash Algorithm 256-bit).
3. **Public Key Infrastructure (PKI)**
Class 3 DSCs operate within a PKI, a framework that manages digital certificate generation, distribution, and revocation. Certification authorities (CAs) are responsible for issuing and managing these certificates. In the context of Class 3, CAs, such as Capricorn CA follow a rigorous process to verify the identity of the certificate holder.

AUTHENTICATION AND VERIFICATION PROCESSES

1. **Identity Verification** : Obtaining a Class 3 DSC involves a comprehensive identity verification procedure. The certificate applicant must submit various identity documents, undergo in-person verification, and comply with the CA's stringent requirements. This multi-layered verification process ensures a high level of confidence in the certificate holder's identity.

2. **Certificate Issuance** : Once the identity verification is completed, the CA issues the Class 3 DSC. The certificate contains the public key of the key pair and information about the certificate holder, including their name, organization, and the expiration date of the certificate.

3. **Certificate Revocation** : In cases of key compromise or other security incidents, the CA has the authority to revoke a Class 3 DSC. Revocation information is maintained in a Certificate Revocation List (CRL) or through Online Certificate Status Protocol (OCSP) responses.

CRYPTOGRAPHIC ALGORITHMS IN CLASS 3 DSC

- **RSA Algorithm**

The RSA algorithm is widely utilized in Class 3 DSCs for key pair generation and digital signature creation. Named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, RSA is based on the mathematical properties of large prime numbers. The protection of RSA depends on the difficulty of factoring the product of 2 enormous prime numbers. The key sizes used in RSA for Class 3 DSCs are typically 2048 bits or higher, providing a robust level of security against current cryptographic attacks.

- **SHA-2 Hash Functions**

Class 3 DSCs commonly use SHA-2 family hash functions, such as SHA-256 and SHA-384, to create hash values of the signed data. SHA-2 is considered more secure than its predecessor, SHA-1, which is susceptible to collision attacks. The use of SHA-2 ensures the integrity of the digital signature and the data it is associated with.

SECURITY MEASURES IN CLASS 3 DSC

- **Hardware Security Modules (HSMs)**

To enhance the security of Class 3 DSCs, hardware security modules are often employed. HSMs are specialized devices that provide secure key storage, key generation, and cryptographic operations. By keeping the private key within an HSM, the risk of unauthorized access or key compromise is significantly reduced.

- **Pin Encryption**

Many Class 3 DSCs utilize PIN (Personal Identification Number) protection to secure access to the private key. The PIN acts as an additional layer of authentication, ensuring that only authorized individuals can use the digital signature. PIN encryption prevents unauthorized use even if the physical token is lost or stolen.

ENCRYPTIONS IN DSC

Class 3 Digital Signature Certificates (DSCs) primarily utilize asymmetric encryption algorithms for various cryptographic operations. These algorithms are chosen for their robustness and security in ensuring the confidentiality and integrity of digital communications. Here are some common encryption algorithms used in Class 3 DSCs:

1. **RSA (Rivest-Shamir-Adleman)**

RSA is one of the most widely used asymmetric encryption algorithms. It relies on the mathematical difficulty of factoring large prime numbers to secure communications. In Class 3 DSCs, RSA is typically used for key exchange during encryption processes. The strength of RSA encryption depends on the size of the key pairs used, with larger key sizes providing greater security.

2. **DSA (Digital Signature Algorithm)**

DSA is a standard for digital signatures. While it's primarily used for digital signatures, DSA can also be adapted for encryption purposes. In Class 3 DSCs, DSA may be used for signing operations, which indirectly contributes to the authentication and integrity of encrypted communications.

3. **Diffie-Hellman (DH)**

Diffie-Hellman is a key exchange algorithm used to securely establish a shared secret key between two parties over an insecure communication channel.
It enables secure communication without the need to exchange secret keys directly. In Class 3 DSCs, Diffie-Hellman key exchange may be used in conjunction with symmetric encryption algorithms to establish a secure communication channel.

4. **Elliptic Curve Cryptography (ECC)**

ECC is an asymmetric encryption algorithm based on the algebraic structure of elliptic curves over finite fields. It offers equivalent security to RSA with smaller key sizes, making it particularly suitable for resource-constrained environments. Class 3 DSCs may employ ECC for key exchange or digital signatures, depending on the specific requirements and cryptographic standards.

5. **AES (Advanced Encryption Standard)**

While primarily a symmetric encryption algorithm, AES is occasionally used in Class 3 DSCs for specific encryption purposes, especially in conjunction with asymmetric algorithms for hybrid encryption schemes. AES provides strong encryption and is widely adopted in various cryptographic applications.
These encryption algorithms, when used in Class 3 DSCs, contribute to the security, confidentiality, and integrity of digital transactions and communications. By leveraging these algorithms, Class 3 DSCs enable trusted digital interactions in applications where a high level of security and assurance is required.

In summary, the encryption strength provided by Class 3 DSCs depends on the specific cryptographic algorithms and key sizes used. Generally, these certificates offer robust encryption capabilities suitable for securing digital transactions and communications in high-security applications.

SHA-2 Algorithms

1. SHA-224: Produces a 224-bit hash value. It is derived from SHA-256 but truncated to produce shorter output.
2. SHA-256: Produces a 256-bit hash value. It is the most commonly used variant of SHA-2 and is widely implemented in various cryptographic protocols, including SSL/TLS, PGP, SSH, and cryptocurrencies like Bitcoin.
3. SHA-384: Produces a 384-bit hash value. It provides higher security compared to SHA-256 due to the longer hash length.
4. SHA-512: Produces a 512-bit hash value. It is more computationally intensive but provides stronger security compared to SHA-256.
5. SHA-512/224 and SHA-512/256: These are truncated versions of SHA-512, producing 224-bit and 256-bit hash values, respectively. They provide shorter output lengths while retaining the security of SHA-512.

LIST OF DOCUMENTS REQUIRED FOR ISSUANCE OF CLASS III SIGNING OR CLASS III COMBO DSC

A. Summary of Documents required - Indian Citizen Individual Certificate / Organization Certificate either

For individual

1. Aadhaar Offline XML

or

1. PAN (Softcopy)
2. Address proof (Softcopy)
3. Photo (Softcopy)

2. Identity proof like driving licensee , passport,
3. Organizational proof
4. Authorized Signatory proof

For Organisation

1. PAN (Softcopy)
2. Address proof (Softcopy)
3. Photo (Softcopy)

2. Identity proof like driving licensee , passport,

3. Organizational proof
4. Authorized Signatory proof

B. List of accepted documents - Indian Individual

Identity Proof (Any one of below) Address Proof (Any one of below)

1. Aadhaar (eKYC Service)
2. Passport
3. PAN Card
4. Driving Licence
5. Post Office ID Card
6. Bank Account Passbook/statement containing the photograph and signed by an individual with attestation by the concerned Bank official.
7. Photo ID card issued by the Ministry of Home Affairs of Centre/State Governments.
8. Any Government issued photo ID having Name & address. 1. Aadhaar (eKYC Service)
2. Telephone Bill
3. Electricity Bill
4. Water Bill
5. Gas connection
6. Bank Statements signed by the bank
7. Service Tax/VAT Tax/Sales Tax registration certificate
8. Driving License (DL)/ Registration certificate (RC)
9. Voter ID Card
10. Passport
11. Property Tax/ Corporation/ Municipal Corporation Receipt
12. Any Government issued photo ID having Name & address

C. List of accepted documents - Indian Organization

Document Name

Company
Partnership
Proprietorship

Copy of the GST registration
Copy of Organizational PAN Card, if GST No. not provided
Copy of Recent Bank Statement / Bank Certificate, if GST No. not provided

Copy of Incorporation, If GST No. not provided
Copy of Business Registration Certificate (S&E / etc)
Copy of Partnership deed containing list of Partners / Authorization Letter
Proof of Authorized Signatory (List of Directors / Board Resolution / Resolution)
Authorized Signatory ID Proof (Organizational ID Card / PAN Card / etc) (If applicant is not a proprietor)
Copy of Applicant PAN Card

USERS OF CLASS III DSC

1. **Government Agencies and Departments**: Government bodies often use Class 3 DSCs for digitally signing official documents, forms, and transactions. This includes ministries, departments, regulatory authorities, and public sector undertakings.
2. **Corporate Entities**: Businesses, corporations, and other commercial entities use Class 3 DSCs for various purposes, including signing contracts, agreements, financial documents, and regulatory filings. Industries such as banking, finance, insurance, and legal services rely on Class 3 DSCs to ensure the authenticity and integrity of digital transactions.
3. **Legal Professionals**: Lawyers, solicitors, and legal practitioners use Class 3 DSCs to sign legal documents electronically, including affidavits, petitions, contracts, and court filings. Electronic signatures facilitated by Class 3 DSCs offer a secure and legally recognized alternative to traditional wet signatures.
4. **E-commerce Platforms**: Online platforms and e-commerce websites may require Class 3 DSCs for secure transactions, especially in cases involving high-value purchases, digital contracts, or sensitive customer information. Class 3 DSCs help establish trust between buyers and sellers in the digital marketplace.
5. **Financial Institutions**: Banks, financial services providers, and investment firms utilize Class 3 DSCs to secure electronic transactions, customer agreements, loan documents, and financial reports. Class 3 DSCs help

ensure the authenticity and integrity of financial transactions while complying with regulatory requirements.

6. **Healthcare Providers**: Hospitals, clinics, and healthcare organizations use Class 3 DSCs for digitally signing medical records, prescriptions, patient consent forms, and other healthcare-related documents. Class 3 DSCs help protect the privacy and integrity of sensitive medical information.
7. **Individual Professionals**: Professionals such as doctors, engineers, architects, chartered accountants, and consultants use Class 3 DSCs to sign professional documents, certifications, reports, and proposals. This ensures the authenticity of their work and enhances trust among clients and stakeholders.

Overall, Class 3 Digital Signature Certificates are used by a wide range of individuals, organizations, and entities across various sectors to facilitate secure and legally binding digital transactions, communications, and interactions

CHARACTERISTICS OF CLASS III SIGNING DSC – SIGNING

1. **Identity Verification**: Before issuing a Class 3 DSC for signing purposes, the Certifying Authority conducts a thorough verification process to confirm the identity of the applicant. This often involves in-person verification and scrutiny of official documents.
2. **Private Key Generation**: Once the identity is verified, the CA generates a pair of cryptographic keys - a private key and a corresponding public key - for the applicant. The private key remains securely stored with the applicant and should never be shared.
3. **Digital Signing:** When digitally signing a document, the signer uses their private key to create a unique digital signature. This signature is appended to the document and can be verified using the corresponding public key, ensuring the document's integrity and authenticity.
4. **Certificate Authority's Role**: The CA's role in the signing process is to validate the authenticity of the signer's digital signature. This validation is done by verifying the digital signature against the public key associated with the signer's Class 3 DSC.

CHARACTERISTICS OF CLASS III DSC (COMBO) (SIGNING AND ENCRYPTION)

1. **Key Exchange**: Encryption using Class 3 DSCs typically involves asymmetric encryption algorithms. When encrypting a message, the sender uses the recipient's public key to encrypt the message. The recipient, in turn, uses their private key to decrypt the message.
3. **Confidentiality**: By encrypting data with the recipient's public key, the sender ensures that only the intended recipient, who possesses the corresponding private key, can decrypt and access the original message. This ensures the confidentiality of the communication.
4. **Data Integrity**: While encryption primarily focuses on confidentiality, it also indirectly contributes to data integrity. Any tampering with the encrypted message would render it undecipherable or produce a decryption error, thus alerting the recipient to potential unauthorized changes.
5. **Authentication**: While encryption alone doesn't authenticate the sender's identity, it can be combined with digital signatures for a more robust authentication and confidentiality solution. In such cases, the sender signs the encrypted message with their private key, providing both authentication and confidentiality.