Process Flow - DSC Mapping/Verification at Login

1. **Start**: The beginning of the workflow.
2. **User Login Attempt:** User enters username and password.
3. **Validate Credentials:** System verifies the username and password.
4. **First-time Login Check:** Determines if the user is logging in for the first time.
    - If **Yes**:
        - Prompt for DSC Mapping: User is asked to map their DSC.
        - Insert DSC: User inserts their DSC into the system.
        - Capture DSC Details: System extracts and stores DSC details.
        - Store DSC Details: Store DSC information securely.
        - Confirmation: User receives confirmation of successful DSC mapping.
        - Proceed to Dashboard: User is directed to the main dashboard.
    - If **No** (Concurrent Login):
        - Prompt for DSC Insertion: User is prompted to insert their DSC.
        - Verify DSC: System verifies that the DSC matches the previously stored DSC.
        - Compare DSC Details: Ensure DSC details match.
        - Verification Outcome:
            - If Matches: Proceed to Dashboard.
            - If Mismatches: Notify user of mismatch, request re-insertion or contact support.
5. Error Handling:
    - Invalid Credentials: User is prompted to re-enter credentials.
    - DSC Mapping/Verification Failure: User is informed of the failure and given instructions.

Digital Signature Certificates (DSCs) follow Public Key Infrastructure (PKI) standards and are issued by Certifying Authorities (CAs) such as the Controller of Certifying Authorities (CCA). When a DSC is used with a web application, several details from the DSC can be fetched and utilized. Here are the key details that can be extracted from a DSC via a web application:

1. Certificate Information

- **Subject Name**: The name of the individual or organization to whom the DSC is issued.
- **Issuer Name**: The name of the CA that issued the DSC.
- **Serial Number**: A unique number assigned to the DSC by the issuing CA.
- **Public Key**: The public key associated with the DSC, used for encryption and digital signatures.

2. Validity Period

- **Start Date**: The date when the DSC becomes valid.
- **End Date**: The date when the DSC expires.

3. Certificate Type

- **Type of DSC**: Information about whether the DSC is for an individual, organization, or government.

4. Certificate Details

- **Certificate Version**: Version of the X.509 standard used.
- **Signature Algorithm**: The algorithm used to sign the DSC (e.g., SHA-256 with RSA encryption).
- **Public Key Algorithm**: The algorithm used for the public key (e.g., RSA, ECDSA).

5. Extensions

- **Key Usage**: Defines the purpose of the key (e.g., digital signature, non-repudiation, key encipherment).
- **Extended Key Usage**: Additional purposes for which the key can be used (e.g., server authentication, client authentication).
- **Subject Alternative Name**: Additional identities or email addresses associated with the certificate.

6. Certificate Policies

- **Certificate Policy Identifier**: Identifiers or URLs specifying the policies under which the DSC was issued.

7. CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol) Status

- **Revocation Status**: Whether the DSC is still valid or has been revoked. This can be checked via CRL or OCSP.

8. Digital Signature

- **Signature Value**: The digital signature of the certificate, used to verify its authenticity.

9. Certificate Fingerprints

- **SHA-1 Fingerprint**: A hash of the certificate used for quick identification.
- **SHA-256 Fingerprint**: A more secure hash value of the certificate.

10. Certificate Policies and Practices

- **Policy URL**: Link to the policies and practices followed by the CA for issuing DSCs.