DSC SIGNER

A cross-platform, browser independent plugin-free Digital Signature Solution

DSC Signer is a cross-platform, browser independent solution for digital signature using DSC tokens. The DSC Signer comprises of two components namely a client-based component and server-side API. DSC Signer solution is supported in all the major operating systems viz Windows, Linux and MacOS.

T. MOHAN DHAS
Dy. Director General & SIO
mohandhas.t@nic.in

T. EDWARD SAM
Technical Director
edwardsam@nic.in

ARUN K. VARGHESE
Scientist B
arun.kv@nic.in

Edited by
REUBAN K

At present, most of the government services are provided through online and the certificates are issued electronically as a PDF document to the citizen. Most of these certificates are signed digitally to provide authenticity, integrity and non-repudiation. The digital signature also provides a viable solution for creating legally enforceable electronic records. An applet based digital signature solution was developed and integrated with the web applications developed using various technologies. The support for applet has been withdrawn from JDK 1.9 and major browsers are also not supporting the applet due to security threat.

DATA SIGNATURE

- To protect integrity of records in a database
- Data signatures comply Cryptographic Messaging Standards
- Signature is a combination of the signature bytes and the certificate byte
- Signature is not attached to the signed data (detached)
- Verification service provided at server side to check integrity of data

OVERVIEW

DSC Signer is a cross-platform, browser independent solution for digital signature using DSC tokens. The DSC Signer comprises of two components namely a client-based component and server-side API. The client-based component is installed in the client machine as a background service. The signing of data is carried at the client side and the verification of signature is carried out at the server side. The solution is capable of signing data, PDF and XML documents. The solution is also capable of signing PDF files with visible signature stamping in the document. DSC Signer solution is supported in all the major operating systems viz Windows, Linux and MacOS. The solution can be integrated by applications developed in Java, PHP and .NET etc. The server API can be exclusively used by a project or shared across many projects.

KEY FEATURES

- Browser independent and plug-in free solution
- Supports data, PDF and XML signing
- Supports all major client operating systems like Windows, Linux and macOS.
- Supported by all major browsers like Google Chrome, Mozilla Firefox, Microsoft Internet Explorer and Apple Safari.
- Easily integrated with any application irrespective of the technology.
- Generated in PKCS#7 Cryptographic Messaging Standard, the signature is interoperable across various applications.
- The DSC Server-side API service can be hosted centrally and shared across different applications.
- Certificate Revocation List (CRL) check may be done using daily updated CRL files while registering certificates and during the signing process.
- Supports auto-token-detection and configuration of digital signature certificate tokens on signing attempt.
- Digital signature stamping in the PDF document.
- Wet ink signature placement on last page on all pages.
- Server time is used for PDF signing.
- Time stamping of PDF documents using trusted Time Stamping Authority (TSA).

Process-flow for Digital Signature Solution | Digital Signer Solution Architecture

SOLUTION ARCHITECTURE

The DSC signer solution provides three components namely a client-side tool to carry out the signing process, a set of wrappers that helps the application to access the DSC signer APIs from a browser and a server-side service that enables the registration of DSC prior to signing and verification of a signed content. The server-side component is provided as a war file that can be hosted in a web container. The client component of DSC client tool is provided for Windows, Linux and macOS platforms. The appropriate version of the tool is to be downloaded and installed in the client system depending upon the operating system of the client.

CLIENT SIDE SERVICE

The client-side service is a Java application running on the end-user client machine and facilitates registration of DSC, and signing using a DSC.

The client-side service consists of two components:

DSC SERVICE

It is a background service, which listens for USB device attached or device detached events. When a DSC token is attached, the DSCSigner component will be started and the component will be stopped when the USB token is detached.

DSC SIGNER

It provides REST API based access to the PKCS#11 token stores and facilitates certificate selection and signing operations. It provides basic methods to initialize and authorize the PKCS#11 token store, read public key certificate information, and sign data using the private key after validating the token pin.

CLIENT HELPER LIBRARY

The client-side helper library is a Query based helper library that can be used by the developer to access the DSCSigner APIs from an application running on the client browser. The client helper library can be referenced in web application pages that provide DSC registration and signing functionalities.

SERVER-SIDE API

The server-side API provides the server-side functionalities such as verification of certificate, decryption and verification of a signature content and decryption of a signed PDF file. The server-side API provides a Restful interface which needs to be consumed by applications developed in any platform.

PDF SIGNATURE

- Signature and signing certificates are embedded in the signed document
- Signed PDF is tamper-proof and can be exchanged and trusted by the receiver
- At the time signing, Server time used for signing to ensure the validity of certificate
- Trusted Time Stamping service (TSA) integration to embed a trusted timestamp
- Provision for wet ink signature and digital signature stamping at a given location
- Signature can be verified by any user using popular PDF readers

XML SIGNATURE

- XML is a popular format for data exchange across different applications
- Signature and signing certificates enveloped in the XML document
- Used in secure data exchange and to establish cross application trust
- Verification services are provided for quick verification of signed XML

DSC SIGNER SETUP AND USE

- Install DSC token driver corresponding to your token
- Install DSC Signer client application by running the installation setup
- Plug-in the DSC token
- Verify whether the DSC Signer is running (see tray icon)
- Register certificate with the web application by providing the PIN (one time)
- Signed by providing PIN when requested

For further information, please contact:

STATE INFORMATICS OFFICER
NIC Kerala State Centre
CDAC Building, Vellayambalam
Thiruvananthapuram-695033, KERALA

Email: sio-ker@nic.in
Phone: 0471-2729894