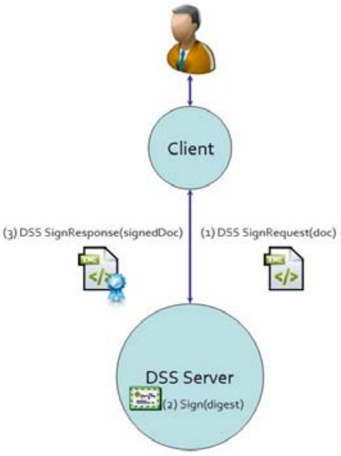
Extending DSS with local signature computation

E.J. van Nigtevecht
Sonnenglanz Consulting BV
Februari 6, 2012

DSS-Core

The Digital Signature Services (DSS) standardizes a protocol by which a client can send documents (or document hashes) to a server and receive back a signature on the documents; or send documents (or document hashes) and a signature to a server, and receive back an answer on whether the signature verifies the documents. These operations could be useful in a variety of contexts – for example, they could allow clients to access a single corporate key for signing press releases, with centralized access control, auditing, and archiving of signature requests. They could also allow clients to create and verify signatures without needing complex client software and configuration.

The DSS protocol assumes that the signature computation is performed at the DSS server (server-side) using a (secure) signature creation device (SSCD or SCD). Stated differently, the DSS server will sign a document on behalf of a certain client.



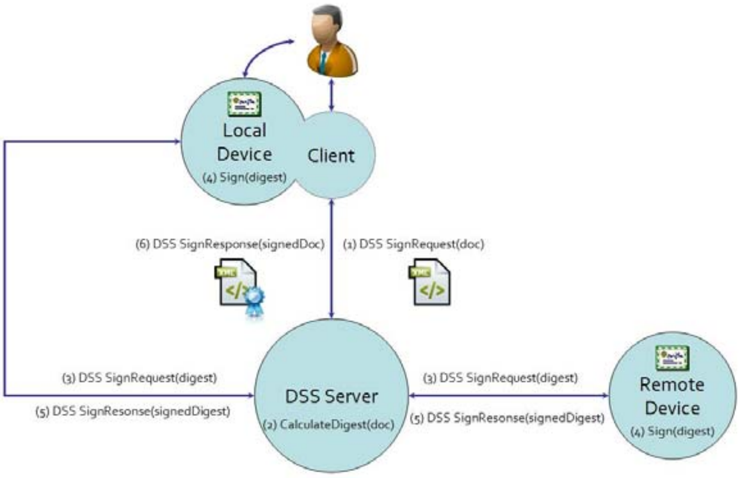
Extending DSS-Core

It is our intention to extend the DSS protocol such that:

(i) It enables a signature computation at the client-side by means of a Local Device (containing an SSCD or SCD) under the direct control of the user *and* local to (nearby) the user.

(ii) It enables the delegation of a signature computation to a remote device (containing an SSCD or SCD): a device under the control of the user but not available locally to the user.

The Local Device as well as the Remote Device may have limited software and performance capabilities and hence may be supported by a DSS server to handle the complexities of the signature creation and document manipulation.

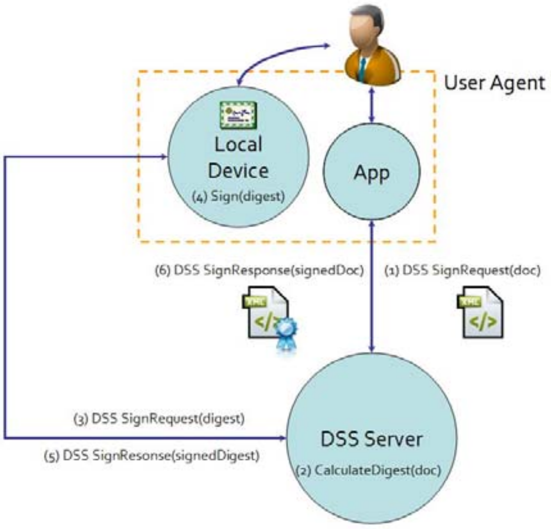

Local Device
(4) Sign(digest)
Client
(6) DSS SignResponse(signedDoc)
(1) DSS SignRequest(doc)
(3) DSS SignRequest(digest)
(5) DSS SignResonse(signedDigest)
DSS Server
(2) CalculateDigest(doc)
(3) DSS SignRequest(digest)
(5) DSS SignResonse(signedDigest)
Remote Device
(4) Sign(digest)

The former option (i) has to delegate the signing operation 'back' to the client. But the client-server setup requires the client to initiate the request. Therefore, some design choices have to be made to fulfil this requirement. (The design choices are not yet presented in this document.)

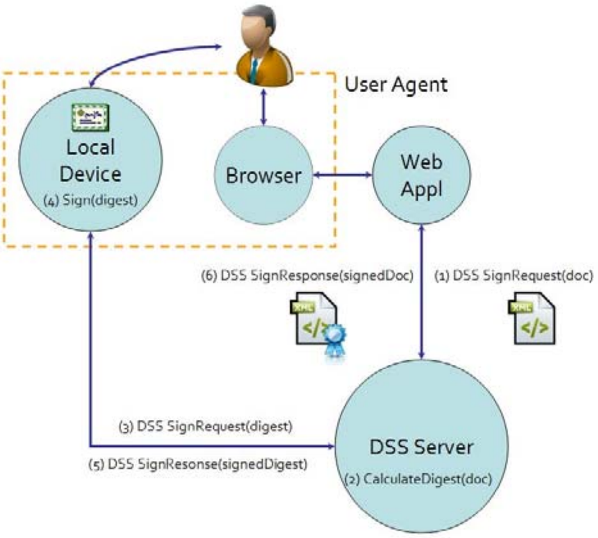
Local Signature Computation

Option (i) can be detailed in several ways, depending on the nature of the actual set-up of the 'client'. Three examples are presented.

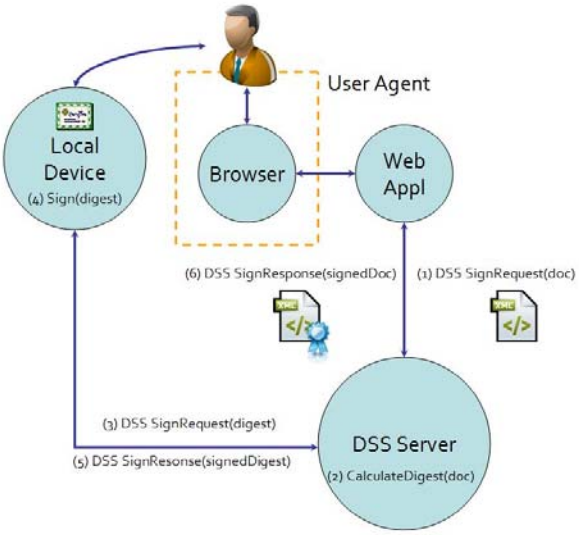
1. The signature creation is done by means of a Local Device as part of a User Agent. The user initiates a request by means of an application at the User Agent. The User Agent is capable of (a) creating the DSS SignRequest and processing the DSS SignResponse and (b) providing a user interface for several activities, such as selecting a document, providing the proper action buttons, or presenting the document. This setup resembles, for instance, an App at a Smartphone or an application at a laptop.



2. The client consists of a User Agent and a web application. The user initiates a request via the browser (as part of the User Agent) to the web application. The web application (a) creates the DSS SignRequest and processes the DSS SignResponse and (b) provides a user interface for several activities, such as selecting a document, providing the proper action buttons, or presenting the document. The actual signature creation is done by means of a Local Device, also part of the User Agent.



3. The client consists of a User Agent and a web application, but the Local Device is not connected to the User Agent. The user initiates a request via the browser (as a part of the User Agent). The web application (a) creates the DSS SignRequest and processes the DSS SignResponse and (b) provides a user interface for several activities, such as selecting a document, providing the proper action buttons, or presenting the document. The actual signature creation is done by means of the Local Device, separated from the User Agent. This setup resembles, for instance, a mobile phone capable of creating a signature and a laptop by which the user accesses a web application.



Local Device

The Local Device will serve a request to sign a given digest. It is assumed that the interface to the actual signature creation device (SSCD or SCD) is accessed through one of the possible standards, such as:

- APDU (ISO 7816);
- IFD-Client (ISO/IEC 24727 / CEN 15480);

This shows that the DSS interface, as indicated in the diagrams in the previous section by (3) DSS SignRequest(digest), should not depend on the actual interface of the SSCD or SCD. It is assumed that there will be some middleware that abstracts from the vendor-specific implementation of the SSCD or SCD.