March 06, 2019

A METHOD TO VERIFY SIGNATURE OF DIGITALLY SIGNED DOCUMENTS ON PRINTER AND ENABLE PRINT

HP INC

A Method to verify signature of digitally signed documents on printer and enable print.

ABSTRACT

It is a common practice in enterprises such that when sending confidential documents across, it has to be digitally signed to maintain both the integrity, confidentiality and establish sender identity.

When there is need to print such digitally signed document, user need to verify the signature on the PC first and then has to give it for print. When the document is directly sent to the recipient or to the web enabled printer as e-print job through cloud, there is no way he can verify validity and integrity on printer itself as of today.

The proposed solution addresses the need to how a recipient can print a digitally signed document without the need for any PC to verify the signature. It describes how a digitally signed document being sent as e-print job will be rendered on cloud to fetch sender credentials, how to send credentials to printer, a proposed design solution to verify signature on the printer and a way to enable user to accept sender validity and then allow print.

This avoids lot of hassles for user to understand the verification process as printer can do it for him. Even when submitting the document from PC, there is no need to verify signature on PC. Instead printer can handle that as it would have the same root CA installed on it. In case if there is no CA installed on PC to verify the signature, printer can efficiently handle if it has proper CA installed.

DESCRIPTION

Here is how the entire proposed solution works on the printer. Also briefing the whole signing process to give more clarity.

Method I:

1. Sender obtains a certificate signed by a trusted CA authority. It has a private key and public key associated with it.

2. Sender wants to send a confidential document to the recipient. Sender signs the document using his digital signature. The digital signature is basically nothing but encrypting the hash of document content using sender's private key.

3. Sender sends the document to recipient directly or sends it to recipient's web enabled printer as e-print job. Sender should know the email address of the printer for this purpose. (recipient has to share the email address with sender)

4. Recipient receives digitally signed document sent by sender if sent directly to him and he submits the document for print without doing signature verification on his PC or submits it through mobile app if received on mobile. Note: The print protocol that is used to submit the print job is not of relevance here.

5. Printer receives signed document and will extract the certificate details and its public key from that.

6. If there is proper root CA installed on the printer the sender certificate verification go success and trust can be established for sender identity otherwise it would fail. Usually in enterprises it is common practice to use same root CA across everywhere where there is need for security.

7. Printer decrypts document signature using sender’s public key and compares hash to verify the message integrity.

8. Based on verification result, the verification status (VERIFIED OR UNKNOWN) will be displayed on printer control panel and then user decides to accept it or not to print depending on status.

9. If user accepts to print, printer will print the document along with verification status as VERIFIED or UNKNOWN.

Method II:

1. Sender obtains a certificate signed by a trusted CA authority. It has a private key and public key associated with it.

2. Sender wants to send a confidential document to the recipient. Sender signs the document using his digital signature. The digital signature is basically nothing but encrypting the hash of document content using sender's private key.

3. Sender sends the document to recipient directly or sends it to recipient's web enabled printer as e-print job. Sender should know the email address of the printer for this purpose. (recipient has to share the email address with sender)

4. Sender sends the document as e-print job if printer is web enabled. Cloud receives the signed document and then extracts the sender credentials from the signed document such as sender's public certificate, public key and Digital signature and stores.

5. Cloud stores the actual print document.

6. Cloud submits print job request to printer. Printer accepts it and returns a job-id in return. This job-id is used for all further communications between cloud and printer and for few of the printer internal component interactions.

7. (a) Cloud shares sender's certificate with printer. This is Push model. Or

(b) Cloud shares certificate location URI with printer. Printer will need to go and fetch sender certificate from cloud later. This is PULL model.

8. Printer receives sender's certificate either through 7(a) or 7(b).

9. If there is proper root CA installed on the printer the sender certificate verification go success and trust can be established for sender identity otherwise it would fail. Usually in enterprises it is common practice to use same root CA across everywhere where there is need for security.

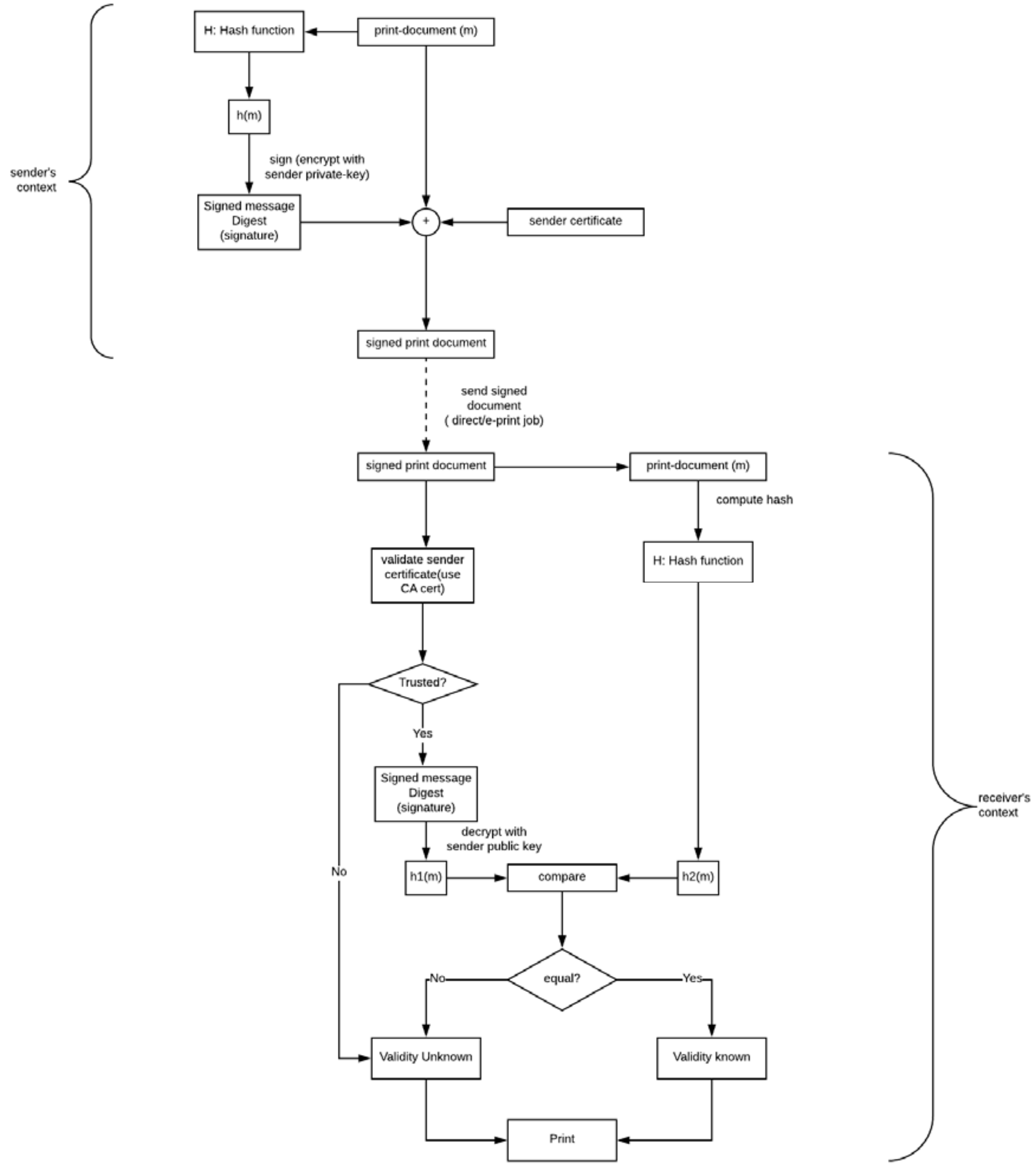
10. Cloud shares print document-uri to printer.

11. Printer decrypts document signature using sender’s public key and compares hash to verify the message integrity.

12. Based on verification result, the verification status (VERIFIED OR UNKNOWN) will be displayed on printer control panel and then user decides to accept it or not to print depending on status.

13. If user accepts to print, printer will print the document along with verification status as VERIFIED or UNKNOWN.

The below drawing explains the typical design both from sender and receiver perspective.



Disclosed by Prasad Phanti Sreenivasa, HP Inc.