IBM Software Services
for Enterprise Content Management

IBM FNSignature-Solution

Vertraulich / Confidential
Nur für den internen Gebrauch / Internal use only

First View

Bernd Geiß, Dorothea Vulcan
IBM Germany

File name: Fist View 001.doc
Date: 03.July 2007
Version: 10.8

History

Version	Date	Author; Firma	Observation
0.0	07.10.2004	Bernd Geiß; FileNet GmbH	created
0.5	28.10.2004	Bernd Geiß; FileNet GmbH	End of Signature Description and Software Architecture.
0.6	03.11.2004	Bernd Geiß, FileNet GmbH	Technical Specification of IBM FN Capture components
0.7	05.11.2004	Bernd Geiß, FileNet GmbH	Updates in chapters 5.4 ff.
0.8	30.11.2004	Bernd Geiß, FileNet GmbH	Updates in chapters 5.3. und 5.4
0.81	04.07.2008	Dorothea Vulcan; IBM Deutschland	First View in English

Figures summary

1 Introduction

1.1 Scope

IBM FnSignature creates a digital signature solution, which can be integrated in all IBM FileNet Document Management repositories.

IBM FnSignature implements a solution for archiving, safekeeping and verification of signed documents. IBM FnSignature archives and maitains the documents and their signatures in an IBM FileNet backend system (Repositories), like Image Services (IS), Content Services (CS) or P8 Content Engine as well as in the IBM DB2 Content Manager. Creation and verification of the signatures are based on integration of standard digital signature suppliers, developed in the FnSignature structure as an open provider. IBM FnSignature is currently offering support and an interface for SecCommerce digital signature product. These signature providers are involved in creating, verification and maintaining the accreditation of digital signatures.

IBM FNSignature solution implements the following functions:

- Signature of one document during the archiving process to an ECM repository,
- Signature of an document, which is included in an ECM repository (archived document)
- Batch signing of input batch documents
- Multi signing of archived documents
- On- and offline signature verification during archiving the document
- On- and offline signature verification of an already archived document
- Online signature verification of signed archived documents

IBM FnSignature offers 2 possibilities:

- An out of the box solutions to sign and verify, for some of the IBM FN ECM applications, as IDM DT, IBM FN Capture and IBM P8 AE - Workplace and
- An FnSignature API (Application Programming Interface) for a further implementation in customized applications, using FnSignature.

IBM FnSignature solution is not an out-of-the-box product. Thus, each customer needs to analyze their needs, with help from IBM, to determine the scope of their FNSignature project.

2 IBM FNSignature Overview

This chapter gives an overview of the IBMFnSignature solution functionality in a client-server architecture.

2.1 Client-Server Architecture

IBM FnSignature solution implements a Client-Server-Architecture (Fig. 1), consisting of IBM FnSignature client and server components PSEC Sign Service.

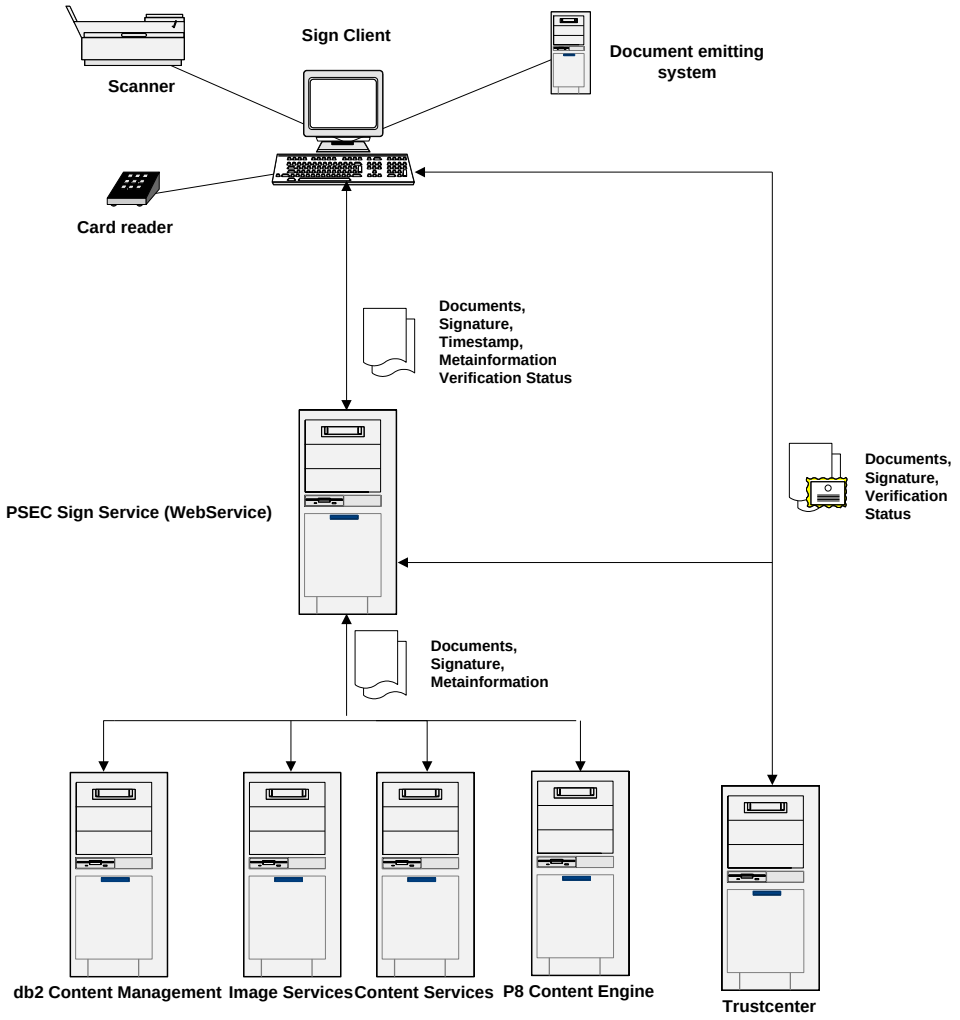

Fig. 1 Client-Server Architecture FnSignature solution

IBM FnSignature client implements the application and the user interface of the signature solution, based on an API - PSECSign. The IBM FnSignature API (PSECSign) offers the possibility to sign multi-sign and verify the signature of a document. The client is open implemented to use a signature

provider. The provider part implementation can be changed depending of the provider API. SecCommerce provider is currently used to sign and verify.

FnSignature client implements an interface to IBM ECM Repository API to add the documents and their signatures, depending on the type of the ECM repositories.

The server part, PSEC Sign Services (Web Services) implements the interface to the IBM FN Repositories and the connection between the signature and the repository signed document.

2.2 Main FnSignature Flowcharts

2.2.1 Drawing up a Signature during Adding the Document to Repository

The document to be signed can either be an electronic or paper document.

Preparation of the document requires several steps. Prior to the committal, the signing step, must be added to the workflow.

Based on IBM FnSignature Client API the document is signed, verified and both the signature and document is committed to the repository of your choice.

A sample of the client scan includes the following steps: scan assembly, index and sign input documents. Because of the signature integrity, the digital signing must be the last step in the flowchart, before committal.

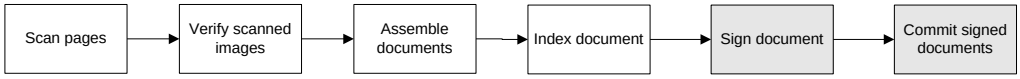

Fig. 2 Workflow of a scan document with digital Signature

Remarks

IBM FnSignature permits sign documents with documents, file-by-file or batch of documents in a single step also known as “batch signing”. Batch signing can be done only in case the signature provider offers this functionality. The batch signing is based on percentage content checking of the files.

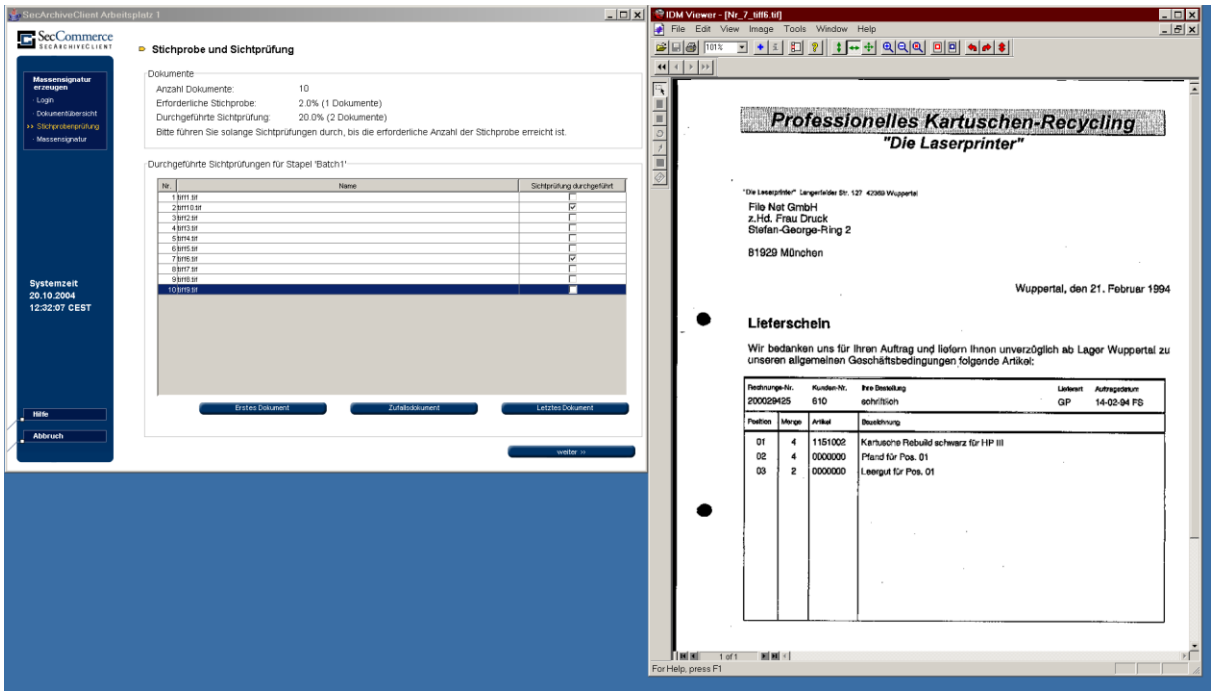

Fig. 3 Batch Signing Sample: Percentage checking of batch contents

Based on PSECSign Service the documents will be indexed and committed to the required repository.

2.2.2 Signing a Repository existing Document

Based on document identifier (GUID in P8, ItemId in CS, F_DOCNUMBER in IS) IBM FnSignature Services Server components obtain the content and send it to the IBM FnSignature client. Based on the signature provider interface, (AuthentiDate, SecCommerce) the file is checked by the user,who signs and approves the signature. As result of signing, the signature provider creates a signature file on the client.

The verification either takes place inside the signature provider step, on the client or after sending the files to the IBM FnSignature Services on the server.

Between signing and archiving signatures, no other steps should be inserted to preserve the signature integrity. The verification between the client and server signature is achieved by the signature provider which is SecCommerce, AuthentiDate, etc.

.

2.2.3 Signature Verify of Repository existing Documents

Based on the unique document identifier IBM FnSignature services checks if one or more signature for the document exists. If at least one signature exists, the signature file and the document file are loaded from the repository and used as input to the signature verify provider.

.

2.3 Storage of signed Documents in Repository

IBM FNSignature permits signing of one or more file documents. For one file documents, IBM FNSignature archived only one file signature document. In case the content of the document consist of more files, for each file a signature file is created. All the signature files will be archived as a signature document, linked to the signed document.

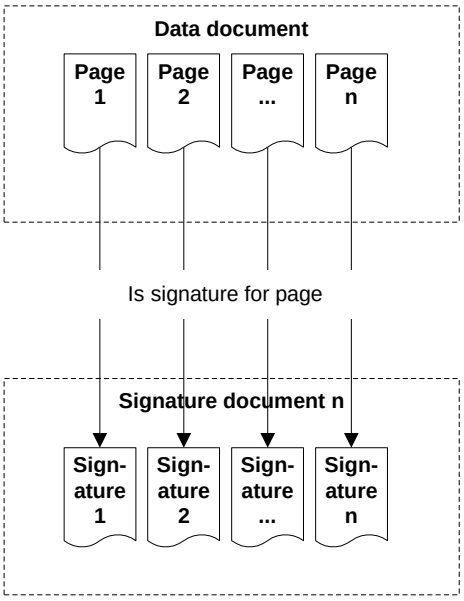

Fig. 4 Signature of a more files document

2.3.1 Data and Signature Document Linking

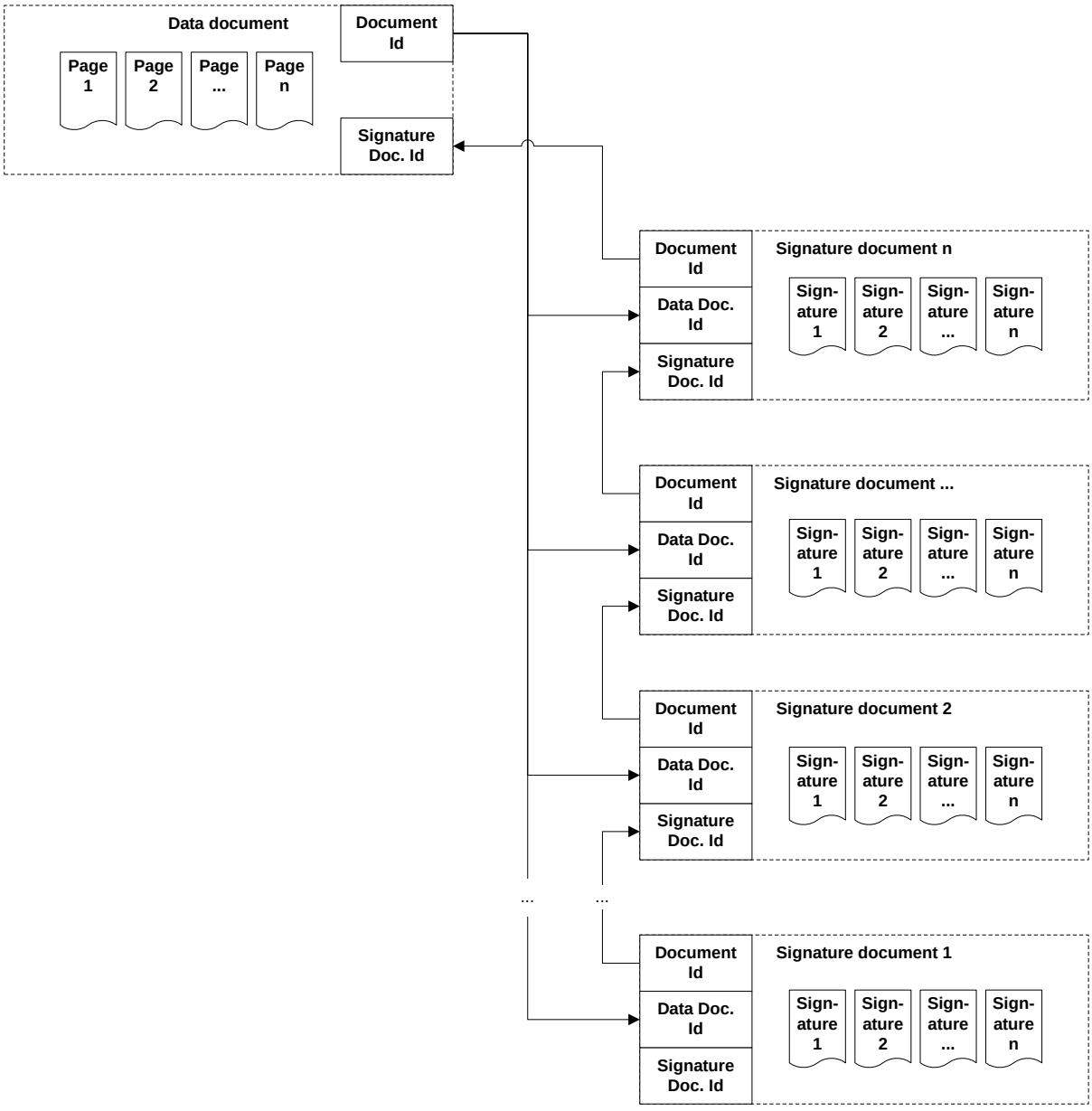

Fig. 5 Linking of Data Documents and Signature Documents

3 FnSignature Software Architecture

IBM FNSignature is based on client-server software.

IBM FNSignature has 2 possibilities, depending on repository needed:

- Thick- client based on IBM FileNet Capture and IDM DT software,
- Thin client based on Workplace Plug-In / Actions.

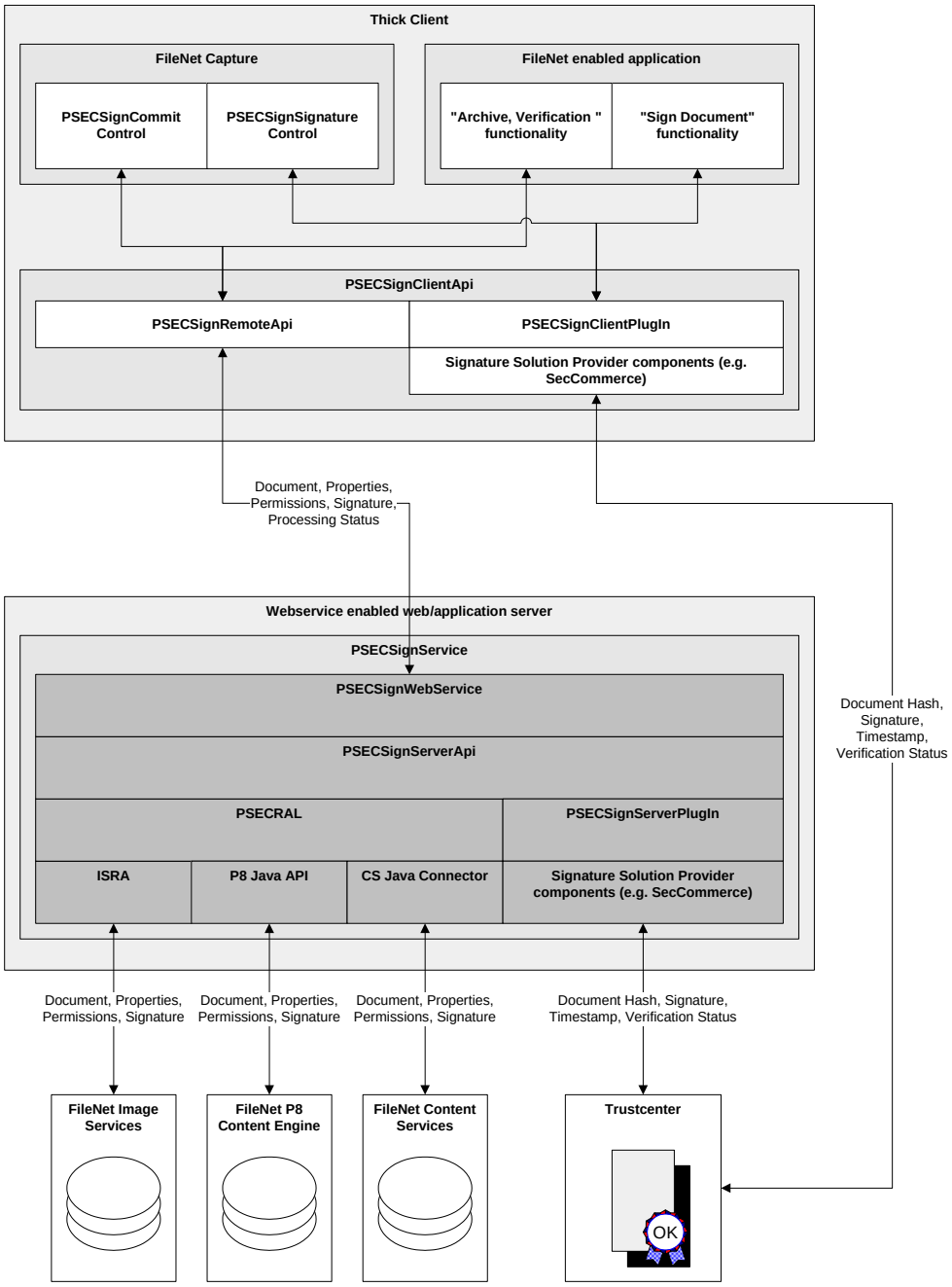

Fig. 6 FnSignature Thick Client Software Architecture

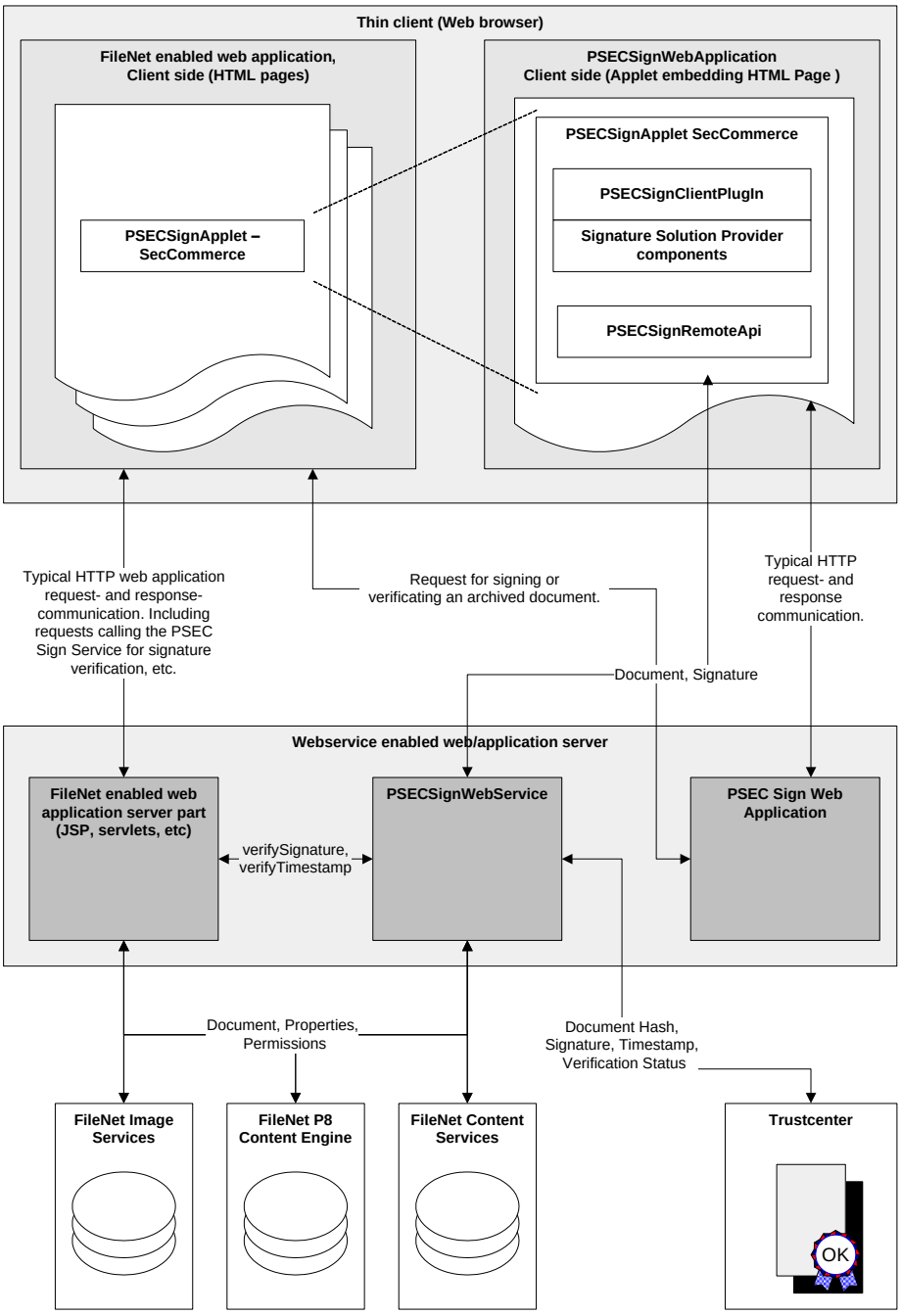

Fig. 7 FnSignature Thin Client Software Architecture