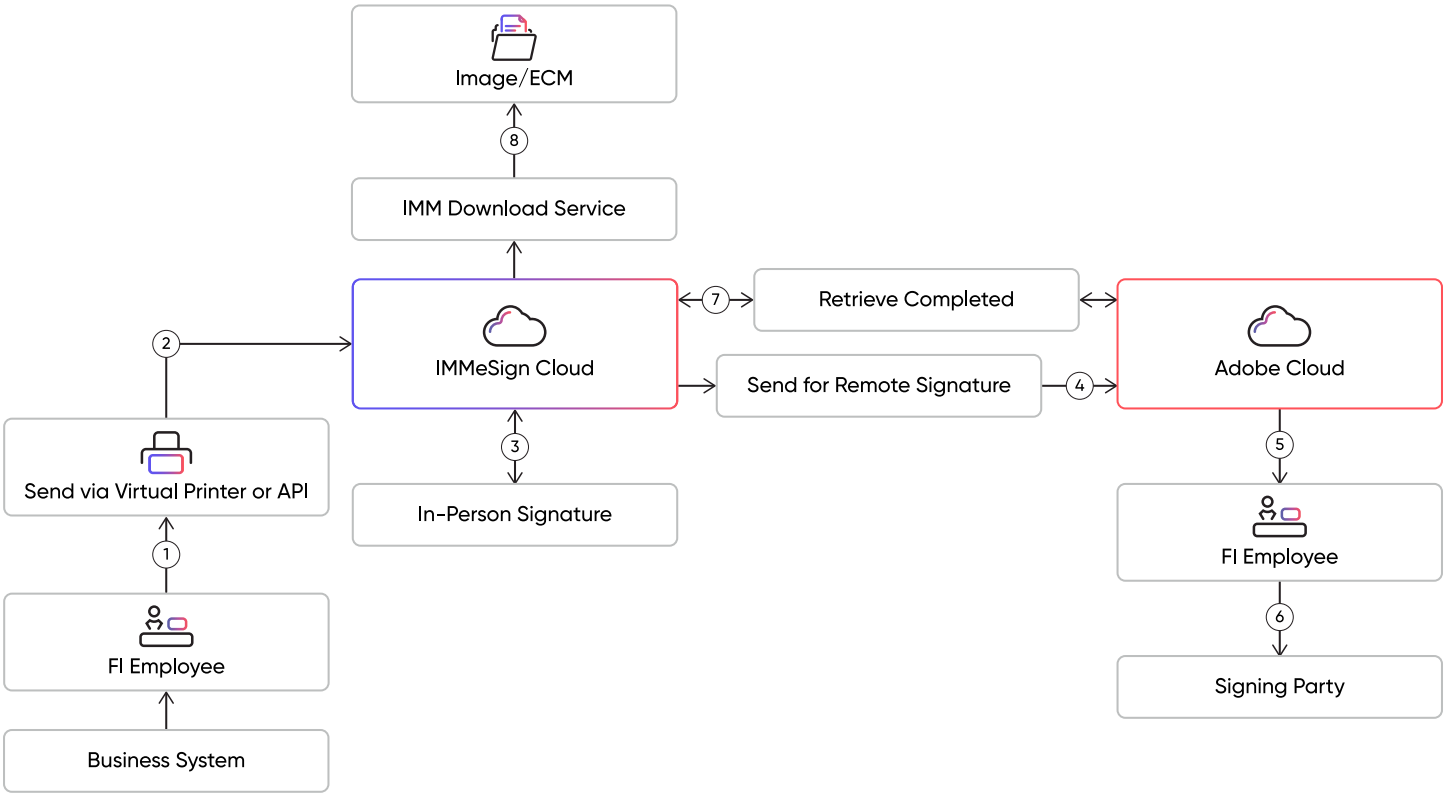
Process Flow Overview

IMM eSign Cloud



1. The FI employee performs a "Print to" function from the business system or a "send to" function if an API integration exists for the business system. In the "Print to" environment, the employee additionally selects the IMM Virtual Printer as the target printer. With either initiation method, the documents selected will be submitted to IMM for eSignature processing.

2. The virtual printer/eSign workstation component securely connects to the IMM eSign Cloud Service (via certificate) and moves the submitted documents to the eSign application, initiating the eSign session. The FI employee then uses the eSign user interface to control and manage the eSigning event(s), whether in-person and/or remote.

3. When an in-person signing ceremony is performed, the physical document does not leave the IMM eSign Cloud Service. An image of the document is presented within the signing ceremony user interface and used for allowing the customer to perform the in-person signing event. The signatures are actually being applied to the physical documents within the IMMeSign Cloud Service.

4. When a remote signing session is initiated, the IMMeSign Cloud Service opens an SSL connection to the Adobe Document Cloud to transmit the document(s) and required transaction information securely to the Adobe Cloud service to facilitate the remote signing event. This transmission is an API-only outbound transmission and contains unique API security keys (uniquely generated for each individual FI client) that authenticate and validate the transmission to the Adobe Cloud service.

5. An email notification is then sent to the signing party notifying them that they have documents ready to be signed.

6. After successful identity authentication and explicit consent is obtained, the signer is then presented with an image view of the document(s) to be signed. As in #3 above, the physical document(s) are not sent to the signer – but are rather displayed within the user interface to enable viewing and signing. However, the signatures are actually being applied to the physical documents being managed within the Adobe Document Cloud.

IMM eSign Cloud

7. The IMMeSign Cloud Service monitors the Adobe Document Cloud for completed signing sessions. Once a remote session is completed, the IMMeSign Cloud Service initiates a "pull" session via the secure API connection and retrieves the signed documents along with their corresponding audit trail and returns the documents back to the IMMeSign Cloud Service.

At this time, the FI has 2 options available for the management of the remote signed documents processed via the Adobe Cloud:

a. Leave the documents in the Adobe Document Cloud. Many of our clients select this option as it becomes a "free" backup copy of the signed documents if an issue were to occur with the institution's imaging/ECM system.

b. The Institution can choose to implement a "Retention Policy" which instructs Adobe to purge the documents from the Adobe Document Cloud after an institution-defined number of days following the completed signing ceremony. When purged, the documents are no longer maintained within Adobe's Document Cloud – but the audit trail is retained by Adobe for audit and compliance purposes. The audit trail does not contain PPI.

8. IMM's Download Service (operated within a FI's data center/network environment) monitors the IMMeSign Cloud Service via secure connection for completed documents ready to be archived into Imaging/ECM. As documents are moved successfully from IMMeSign, the documents are purged from the IMMeSign Cloud Service. The transaction data records (session) are maintained in the IMMeSign Cloud Service for 365 days (for audit purposes). Once that time has expired, the transaction data record is purged, and no information is retained in the IMMeSign Cloud Service.