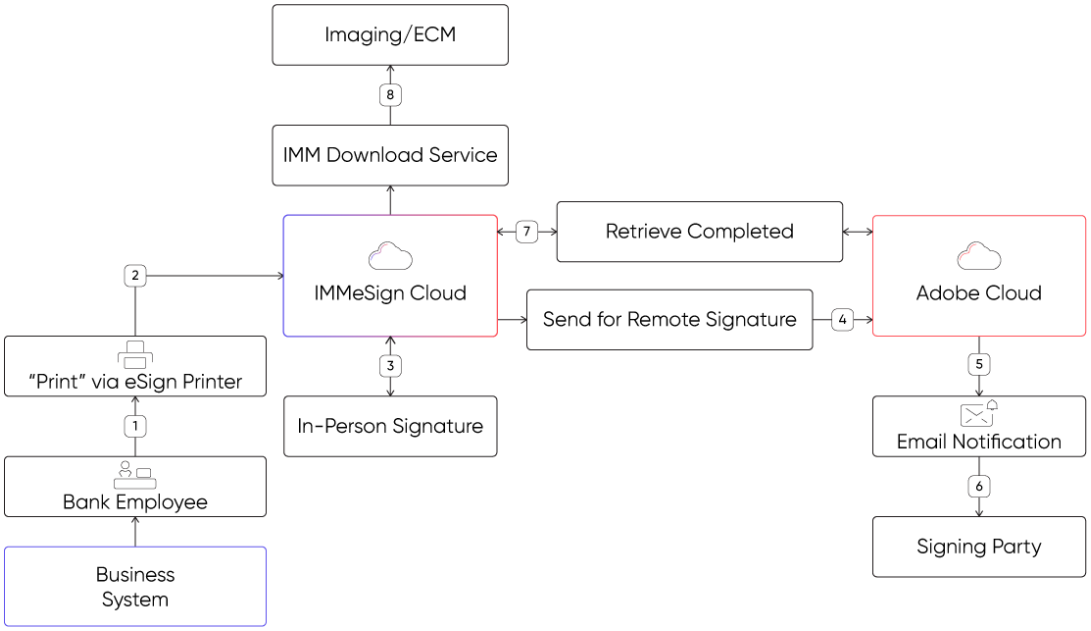
IMM eSign Cloud Process Flow

The eSignature process with IMM eSign Cloud is managed primarily “in the cloud.”



Process Flow Description

1. The institution employee chooses the documents to be sent to IMM eSign from the business system or other source location and selects the eSign Printer in the print dialogue.

2. The eSign (virtual) printer places an electronic file copy of the source documents in a designated folder on the user workstation. The eSign Client component then securely connects to the IMM eSign Cloud Service (via certificate) and moves the “printed” document to the IMM eSign application, initiating the eSign session.
   IMM eSign uses the available template definitions to recognize the “printed” documents, extract index values, place the signature field location(s), and identify signer information for the signing sessions. The institution employee then manages the eSigning ceremonies, 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 applied to the physical documents within the IMM eSign Cloud Service.

4. When a remote signing session is initiated, the IMM eSign 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. This transmission is an API-only outbound transmission and contains unique API security keys (uniquely

generated for each individual institution) that authenticate 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. The signatures are actually applied to the physical documents within the Adobe Document Cloud.

7. The IMM eSign Cloud Service monitors the Adobe Document Cloud for completed signing sessions. Once a remote session is completed, the IMM eSign Cloud Service initiates a “pull” session via the secure API connection and retrieves the signed documents along with their signing ceremony audit trail and returns the documents back to the IMM eSign Cloud Service. At this time, the institution has 2 options for available for the management of the documents in the Adobe Cloud:
   a. Leave the documents in the Adobe Document Cloud. (The vast majority 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” with Adobe (facilitated via IMM) 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. However - the audit trail does not contain PPI.

8. The IMM Imaging Index Service (also called the Download Service and operated within the institution’s data center) monitors the IMM eSign Cloud Service via secure connection for completed documents ready to be archived into Imaging/ECM. Documents and associated indexing files are moved securely from the IMM Cloud to a server in the institution’s environment ready to be archived to the institution’s Imaging/ECM system. Documents and transaction data are maintained in the IMM eSign Cloud Service for a configurable number of days (for audit purposes). Once that time has expired, the documents and transaction data records are purged, and no information is retained in the IMM eSign Cloud Service.