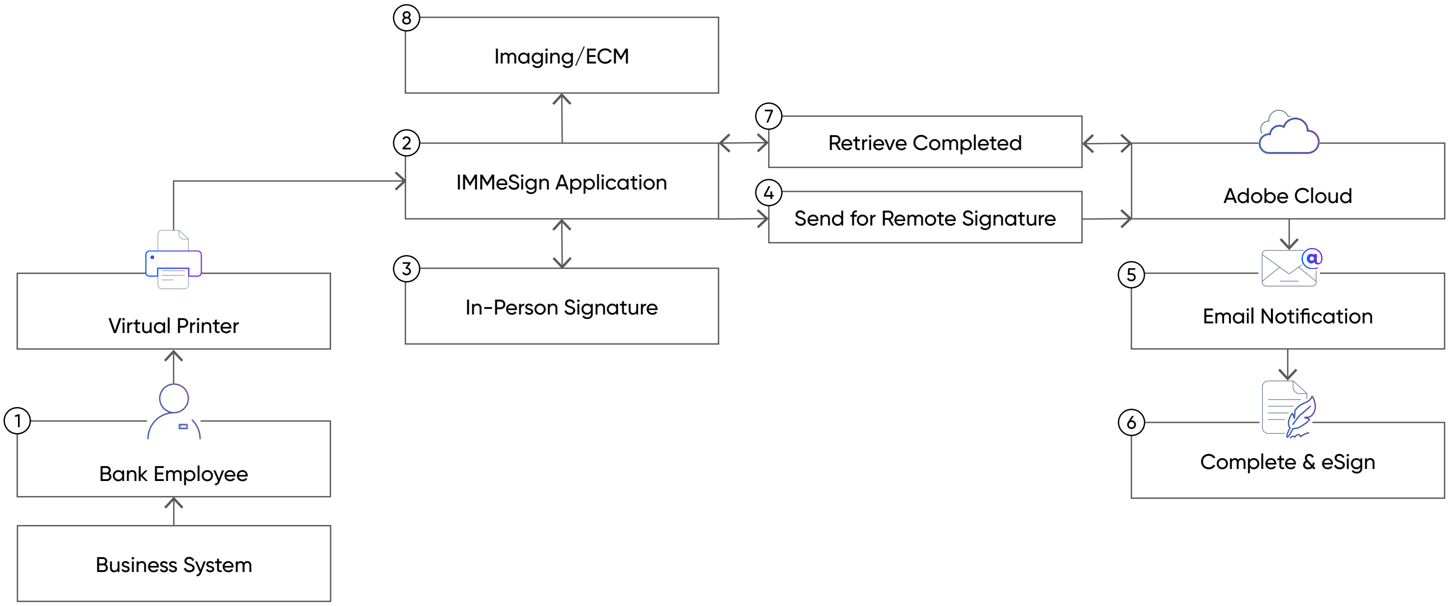

1. The Bank employee performs a "Print to" function from the business system creating the documents that are to be signed, by selecting the "eSign Printer" from the available printers list.

2. The virtual printer/eSign workstation component securely connects to the IMMeSign application (via certificate) and moves the "printed" document to the IMMeSign application, initiating the eSign session.

   The Bank employee then manages the eSigning session and the appropriate signing ceremonies, whether in-person or remote.

3. When an in-person signing ceremony is performed, the physical document does not leave the IMM eSign server. An image of the document is presented within the signing ceremony user interface and used to allow the customer to view the document and perform the in-person signing event. The signatures are applied to the physical documents housed within the IMMeSign application server.

4. When a remote signing session is initiated, the IMMeSign server 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 Bank client) 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 stated 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 applied to the physical documents residing within the Adobe Document Cloud.

7. The IMMeSign application monitors the Adobe Document Cloud for completed signing sessions on a periodic basis. When completed documents (remote signing session) are found, the IMMeSign 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 IMMeSign server.

    At this time, the Bank has 2 options available for the management of completed documents in the Adobe Document 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. IMM's archive function will then move the completed documents along with their relevant audit trails – fully indexed – to the location where the handoff to the Imaging/ECM system occurs. (Or other method of delivery dependent upon the target Imaging/ECM system).

    As documents are moved successfully from IMMeSign, the documents are purged from the IMMeSign server. The transaction data records (session) are maintained in the IMMeSign application for a default 365-days (for audit purposes – can be customer defined period). Once that time has expired, the transaction data record is then purged, and no further information about the transaction is retained in the IMMeSign server.