eSign Products: Survey

IMM eSign

Instructions

This document is used to gather information to ensure a successful implementation. Please answer the questions and return to your project manager's secure mail drop. Please inquire with your project manager if their secure mail drop address has not been shared with you. **Delays in completing this survey impact the Project Timeline.**

Customer Information

Financial Institution Name: Time Zone:

Financial Institution Name: Time Zone:

Project Manager: This is the primary contact during the implementation phase. This person will coordinate communications and information between internal groups and the IMM Project Manager. Please ensure that we have a cell phone for the project manager (at minimum). It is very important that we are able to reach the project manager for setup questions.

Name: Title:
Phone: Cell:
Email:

Technical Lead: This is the primary contact for all IT related questions and tasks.

Name: Title:
Phone: Cell:
Email:

Operations Contact: This is the primary contact regarding operational issues for both implementation and ongoing support.

Name: Title:
Phone: Cell:
Email:

Lead Document Tester: This is the primary contact who will be working closely with IMM's designer to finalize the documents.

Name: Title:
Phone: Cell:
Email:

Environment

Please list the Business Applications you plan to implement with IMM eSign.

Business Applications	Name	Version	*Install Options	Live Yes/No
Core System			Select One	
In-Branch Membership Application System			Select One	
Online Membership Application System			Select One	
In-Branch Loan Origination System (LOS)			Select One	
Online Loan Origination System (LOS)			Select One	
Home Banking Site			Select One	

***Install Options** - **(A):** In-House **(B):** Cloud Enviornment **(C):** Dedicated Data Center **(D):** Dedicated Data Center Using Secured Connection *(certificate should be installed on eSign server)*

What is your target eSign Live date?

Are there any deadlines tied to this go live date?

Documents

Who is designing your documents: ☐ IMM ☐ Financial Institution ☐ Both ☐ Other

How many fill-able documents (*PDF/Microsoft Word*) will be electronically signed and/or archived?

Server

Specify your virtual environment: ☐ VM Ware ☐ Hyper-V ☐ Other

Is the virtual environment: ☐ In-House ☐ Hosted Hosted by:

Server Name: Server IP Address:

Note: *The server may not be a domain controller.*

Database: ☐ SQL Express *(Currently installed on image)* ☐ FI's Dedicated SQL Server *(Requirement for eSign Plus)*

If the preference is Dedicated SQL Server, what is the name of the SQL cluster:

Note: *Your DBAdmin must have the credentials for the sa account (or similar account with equal privileges) and password*.

Antivirus software:

Workstation

Refer to IMMs **Product Specifications** for hardware configurations: Resource Center

Operating Systems:

Thin Client Information:

Note: For Thin-Client, Software must be in the publishing company's current full support lifecycle.

Load Balanced *(Request the System Requirements)* ☐ Yes ☐ No

Number of thin client servers:

Number of thick client workstations:

Operating System:

☐ RDP Server Version

☐ Citrix Server: Citrix XenApp Version

☐ VMWare Horizon Server Version

In-Person Signature Devices

List the type and quantity of in-person signature devices you plan to use with IMM eSign:

Refer to **Oder Forms** for the **In- Person Signature Device Order Form**: Resource Center

Manufacturer	Model	Quantity

Imaging System Settings

These settings will be specific to your Imaging System requirements. eSign can generate an output file necessary for your imaging system to recieve archived PDFs with index fields. The output file can be XML, CSV, TXT and etc. IMM will need to create these fields within eSign to match the predefined indexes in your Imaging System.

Please forward a sample of the output file that your Imaging System is importing today to your Project Manager.

Output File Extension:

You will need to provide IMM the index fields which are predefined in your Imaging System. If there are any special requirements for any specific index

Index Field 1:

Index Field 2:

Index Field 3:

Index Field 4:

Index Field 5:

Index Field 6:

If there are any special requirements for any specific index, please specify below:

eSign Remote: "Add-on Module"

Financial Institution Administrators:

Each transaction submitted for Remote Signature/Adobe Sign will require an active Adobe Sign account registered with your institutions domain. An Adobe Sign Administrator will have the ability to create accounts as needed.

First Administrator:

First Name: _____ Last Name: _____

Email: _____

Second Administrator:

First Name: _____ Last Name: _____

Email: _____

Environment Information:

Provide your Financial Institution's website URL: _____

Provide a high quality color logo to your Project Manager. The specifications are 60 pixels tall x 200 pixels wide. The file must be a PNG.

Authentication Service Options:

Select the type(s) of authentications you would like to use with Remote signing.

☐ **Email Verification**

This is the lowest level of signer identity authentication available. Within eSign, the submitter will send the transaction for remote signing using the Email service. The signer will receive the secure email and click on a link within the email and is presented with the documents to view and sign.

☐ **Password Authentication**

Password service is a medium level signer identity authentication. Within eSign, the submitter will enter a unique password and send the transaction for remote signing. This case-sensitive password will be shared (verbal communication is recommended) with the signer. The signer will receive and click on a link within the email and is prompted to enter the password for authentication. Once the signer is authenticated they are presented with the documents to view and sign.

☐ **Phone/Text Authentication**

Phone Authentication service is a high level signer identity authentication combined with the Email Verification service. Within eSign, the submitter will enter the signers email address and telephone number and send the transaction for remote signing. The signer will receive and click on a link within the email and is prompted to select a Verification Option (Voice Call or Text Message). A verification code will be delivered either via voice call or text messaging to the telephone number provided at the time of the transaction. Once the signer is authenticated they are presented with the documents to view and sign. **Note: Cost associated with use. Please refer to your signed proposal.**

☐ **Knowledge Based Authentication (KBA)**

This is the highest form of signer identity authentication available within the eSign Remote system. When this option is selected at transaction setup time, the signer(s) will be first prompted to enter standard personal information (Name, Address, etc.) that will be used to establish their identity and then they will be presented with a series of "knowledge-based" questions that only they should know the answers to. The correct answering of these questions (non-credit based) will then be used to authenticate and verify the correct identity of the signer(s). **Note: Cost associated with use. Please refer to your signed proposal.**

☐ **Government ID Authentication**

The user enters the signers cell phone number within the eSignature Management screen for the signers smart phone, which then sends an email to the signer. This is required for the image capturing application that will compare the ID to the government database. There is a 10-minute time limit to complete the verification process that starts once the email link is clicked. The recipient is given the option to authenticate with either a Driver License or a Passport. The scanned Government ID is authenticated in real time by validating dozens of elements within the document. Once both steps are successfully completed, the recipient is granted access to the documents for viewing and signing. The name of the recipient as presented on the Government ID is imported to the signature field and cannot be edited.
Note: Cost associated with use. Please refer to your signed proposal.

Adobe eSign Administration Settings

These settings will be specific to your Adobe Sign. The settings will control access to your web portal and how your consumers will access their documents. The Adobe Sign Administrator(s) that you have declared on the prior page MUST change these settings after they activate their account. **It is strongly recommended to use the same security protocol that you use for your local Active Directory.**

Please review the **Remote Sign Portal Admin Training Videos** found on this page **IMM Training Videos** for more information about these Administration Settings:

Security Settings:

Login Password Policy

- ☐ Enable password duration policy? If checked, users will be required to change their passwords every 1 months.
- ☐ Enable password history policy? If checked, users will not be able to resuse their last 1 passwords.

Allow users 1 attempts to login before locking their accounts.

Login Password Strength

- ☐ Standard - At least 6 characters
- ☐ Medium - At least 7 characters, must include uppercase or number
- ☐ Strong - At least 8 characters, must include lowercase, uppercase and numbers **(Recommended)**

Allowed IP Ranges

- ☐ Only allow access to the system from IP addresses that are listed below (use CIDR format and please add IMM's IP range so that we may continue to access your portal in a Support capacity - 24.38.96.178/28)

Agreement Signing Password

Apply a password policy when protecting document signing or viewing

- ☐ Restrict number of attempts?

Allow signer 1 attempts to enter the agreement password before cancelling the agreement.

Document Password Strength

- ☐ None - Any password is allowed
- ☐ Standard - At least 6 characters
- ☐ Medium - At least 7 characters, must include uppercase or number
- ☐ Strong - At least 8 characters, must include lowercase, uppercase and numbers

Phone Authentication

Apply a phone authentication policy when protecting document signing.

Allow signer 1 attempts to resend the phone authentication code or enter a valid code before cancelling the agreement.

Knowledge Based Authentication

- ☐ Restrict number of attempts?

If checked, signers will have 1 attempts to validate their identity before cancelling the agreement.

Knowledge Based Authentication difficulty level:

- ☐ Default (3 questions)
- ☐ Hard (4 questions)

Send Settings:

Reminders

☐ Send a default reminder for agreements created by users in this account.

Send a reminder every **Select One** until completed.

Enter reminder note here.

Document Expiration

☐ Enable document expiration?
If checked, limit the number of days signers will have to sign documents to:

eMail Settings:

Custom Email Message Footer

This text will appear at the bottom of every Adobe Sign email notification sent by any of the users in your account. Please enter the desired message below:

Signer Messaging Settings

After a document is signed, you have the opportunity to interact with your signers in the confirmation pop-up shown to them. You can display a message of your choice and optionally encourage them to spread the word about your institution or programs via their social networks.

☐ Enable Signer Messaging?
If checked, enter a message to your signers in the box below. Hyperlinks can be added to the signer message by enclosing them in square brackets [ ]. For example, [https://documents.adobe.com] would become https://documents.adobe.com
You can also add a label to display as the link by using the following format, [https://documents.adobe.com | Adobe Sign], which would make a link that looked like this: Adobe Sign Anything in the brackets after the | symbol will be the label.