OneSpan
Be bold. Be secure.

FINANCIAL AGREEMENT AUTOMATION RFP GUIDE

A GUIDE FOR FINANCIAL INSTITUTIONS PURCHASING TECHNOLOGY TO AUTOMATE ACCOUNT OPENING, DIGITAL LENDING, LEASING, AND OTHER FINANCIAL AGREEMENTS

WHITE PAPER

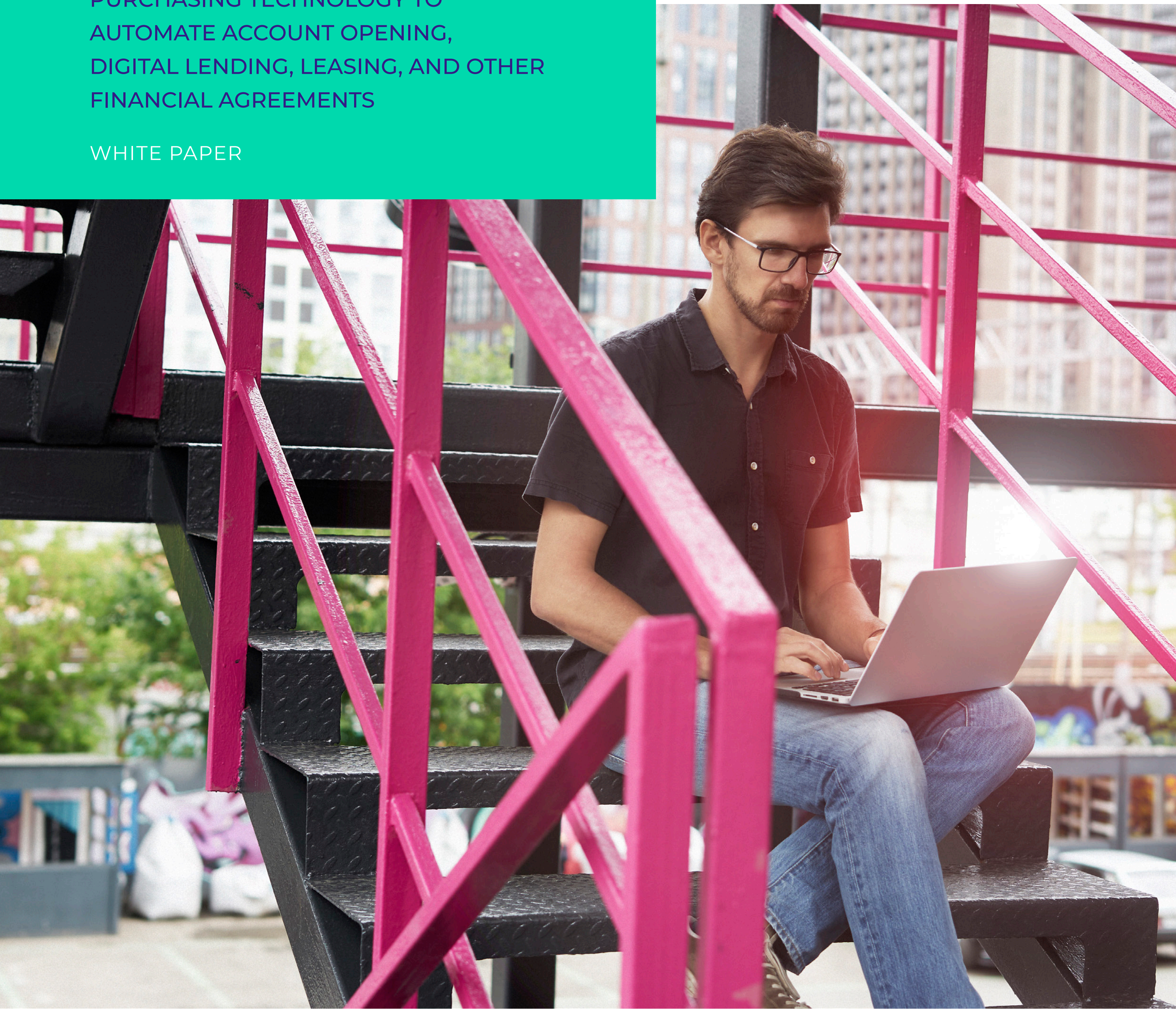


TABLE OF CONTENTS

INTRODUCTION

WHY READ THIS GUIDE

Trillions of dollars in financial agreements are processed each year. This includes credit agreements, loan/lease agreements, new account openings, mortgages, pensions and annuities. Despite the rise of digital adoption within consumer industries, the majority of these financial agreements still rely on manual, semi-manual or disjointed paper processes.

Disjointed manual agreement processes are a huge risk for financial institutions (FIs). They frustrate customers, leading to high drop-out rates; they create inefficiencies, contributing to high operating costs; and they do not provide any visibility into whether agreements are executed in a consistently secure and legally enforceable way. These issues can lead to legal disputes and regulatory non-compliance.

Today's financial services customer is looking for speed, ease and convenience – whether online, mobile, through an intermediary, or in-branch. Innovative financial service companies looking to win new customers and increase customer loyalty are turning to technology to help improve the customer experience, without compromising on risk. Automating the agreement process in today's digital world not only involves digitizing how agreements are prepared, signed and managed, but also how customers involved in the agreement process are verified and authenticated.

WHAT YOU WILL FIND IN THIS GUIDE

This guide is for financial institutions (FIs) looking for **technology that can automate the customer agreement process** – from a customer's initial application, through to digital identity verification, the electronic delivery, presentation, signing and secure storage of an agreement, and the capture and management of all supporting audit trails. It is intended to assist organisations in determining their requirements, building a business case, and evaluating options for implementation.

The guide contains information about what technology to consider when looking for an agreement automation solution, what functionality to consider, and which stakeholders to involve in the process. We also include a list of sample RFP questions to consider for the procurement process.

JUMP STRAIGHT TO THE RFP QUESTIONS

WHAT IS AGREEMENT AUTOMATION

Agreement Automation is the name given to the digitization of the customer agreement process within a financial transaction.

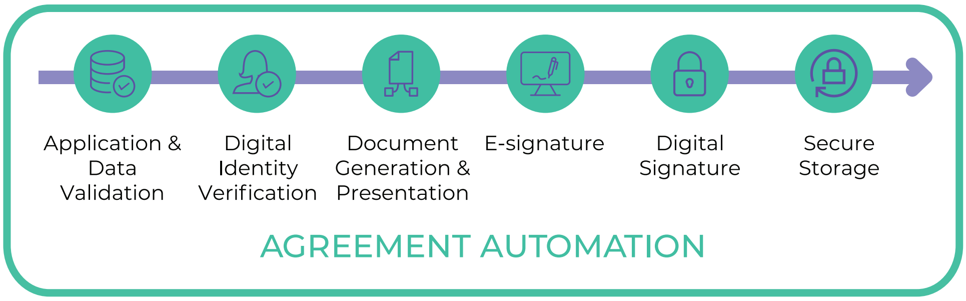
When a customer decides to open a new account, take out a new loan, sign a leasing agreement, or sign up for any number of financial products, they are transacting with a financial institution. The agreement will detail the exact terms of the financial transaction and will need to be agreed on by both parties for the agreement to be completed and the product or service delivered.

Before online and mobile banking, customers transacted with financial institutions in-person through a branch or intermediary using paper documents and manual identity checks.

In today's world, financial institutions need to offer their customers fully digital experiences, so that customers can carry out these transactions remotely. This means that the customer agreement process needs to be digitized. We call this process 'Agreement Automation'.

Agreement Automation is the digitization of the customer journey from a customer's initial application, through to digital identity verification, the electronic delivery, presentation, signing and secure storage of an agreement, and the capture and management of all supporting audit trails.

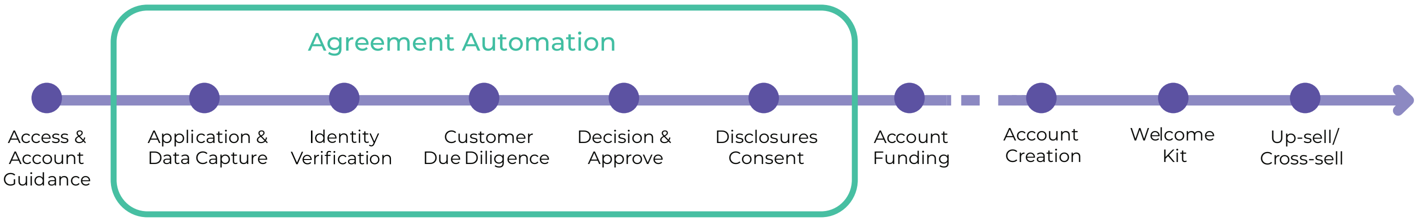
This guide is for financial institutions (FIs) looking for technology that can automate these processes.


Application & Data Validation
Digital Identity Verification
Document Generation & Presentation
E-signature
Digital Signature
Secure Storage
AGREEMENT AUTOMATION

How Agreement Automation Supports the End-to-End Customer Journey

Agreement automation is just one aspect of the entire customer journey, which includes customer acquisition, account opening (when applicable) and customer onboarding. The diagram below shows where agreement automation fits into the overall customer journey. Financial institutions looking to automate the entire customer journey should look for technologies that are able to integrate with one another to deliver a seamless digital journey for the customer.

Fig: Key customer journey steps and where agreement automation fits in



WHY AUTOMATE

Financial institutions automate their agreement processes for three key reasons:

1. Improve customer experience:

Speeding up the agreement process, removing arduous manual steps, and offering a fully digital solution improves the customer experience. Digitization also allows customers to complete the process on their own device and in their own time.

BETTER CX = HIGHER CONVERSION = INCREASED REVENUE REDUCED RISK

2. Deliver commercial and operational benefits:

By streamlining the customer agreement process and reducing decision times, financial institutions can increase and improve the velocity of sales. Automating the agreement process also leads to a reduction in errors which means the cost of error-checking is eliminated, driving down operational costs when compared to paper-based alternatives.

IMPROVED SALES VELOCITY + REDUCED ERRORS + LESS PAPER = INCREASED REVENUE + REDUCED COST + DECREASED RISK

3. Reduce risk:

If set up correctly, automation can reduce risk because it allows FIs to control the workflow from beginning to end – meaning that the process is carried out compliantly. Digitizing the agreement process also allows financial institutions to capture evidence throughout the process. This could be evidence of compliance, evidence of the customer’s identity, or evidence of their intent to be bound by the agreement. If stored in a tamper-evident package, the evidence can help prove that the resulting agreements are legal, compliant, and enforceable if challenged.

INCREASED COMPLIANCE + INCREASED ENFORCEABILITY = DECREASED RISK

HOW END-TO-END SOLUTIONS COMPARE TO STANDALONE TECHNOLOGIES

END-TO-END SOLUTIONS

An end-to-end agreement automation approach is where each step of the agreement process is automated via one solution.

The agreement process (part of customer acquisition and onboarding workflows), refers to the following steps in the customer's financial agreement journey:

- a customer's initial application
- digital identity verification
- the electronic delivery, presentation, signing, and secure storage of an agreement
- the capture and management of complete audit trails

An end-to-end approach makes it possible to gather evidence at each stage of the customer journey and link that evidence to the resulting agreement. The result is a single secure package containing all the evidence needed to ensure the agreements are fully enforceable.

End-to-end agreement automation is particularly valuable for financial institutions transacting with their customers via financial agreements that carry risk (such as credit agreements, new account openings, loan agreements, leasing agreements, mortgages, pensions and annuities).

STANDALONE TECHNOLOGIES

Standalone technologies such as traditional e-signature differ from end-to-end agreement automation solutions as they automate one element of the agreement process.

Standalone and point solutions (such as standalone ID verification or standalone e-signature) can be beneficial for financial institutions that have already digitized one element (or multiple elements) of the agreement process and are looking to fill in the gaps in their workflow.

Standalone e-signature is also valuable for ad-hoc or user-initiated agreement processes such as HR agreements or single purchases, or when a high volume of low-risk documents require signing, such as internal policy documents.

To determine whether end-to-end agreement automation or traditional e-signature would be most beneficial to your business, ask yourself these questions:

1. Does your business involve the execution of a high volume of customer agreements that carry financial risk?
2. Does the regulatory environment in which you operate require you to prove that your customer exists?
3. Do you have a need to validate that your customer is who they say they are?
4. Do you need to validate that the person who is giving their consent to be bound by the agreement, is the person whose identity you have validated?
5. Do you need the flexibility to conduct different identity verification checks on customers dependent on differing factors such as their creditworthiness, the value of the transaction, or their geography?
6. Do you need to collect evidence that a fair and compliant process has been followed?
7. Do you want to avoid arduous manual steps for the customer?
8. Do you want to improve the customer experience without compromising on risk?
9. Do you require signed agreements to be made tamper-proof so that they have integrity if they are relied on as evidence in court?
10. Do you require secure storage which is compliant with local data protection laws?

Mainly Yes =
End-to-end solution could be considered.

Mainly No =
eSignature could be considered.

Equal =
Evaluate end-to-end solutions as well as standalone.

FUNCTIONALITY TO CONSIDER

When determining what functionality is required, review each stage of the customer's agreement journey. The stages to consider are as follows:

Step 1: Application

End-to-end agreement automation starts with an application via an online form or app. This stage captures and validates the customer's personal information, such as name, address, date of birth and bank details, among other information.

Step 2: Digital Identity Verification

Automated ID checks allow financial institutions to prove they know who the applicant is (KYC verification), and that the applicant is genuinely the person that the financial institution is interacting with (referred to as Prove Your Customer verification), instantaneously.

Know Your Customer (KYC) Verification: This can be achieved digitally by matching application data (such as name, address, date of birth, and bank details) to trusted data sources such as electoral roll and credit bureaus. This mitigates risk by screening customer identity against negative data to identity fraud and anti-money laundering activity. IP geolocation, device verification, and corporate checks also contribute to building a strong verification profile of a customer.

Prove Your Customer (PYC) Verification: This can be achieved digitally via methods such as two-factor authentication, SMS verification, knowledge-based authentication, document verification, or facial recognition.

Step 3: Document Generation and Presentation

This is the stage in which agreement document(s) are generated (using the verified application data) and presented to the customer.

Step 4: E-Signature

This step involves the actual signing of an agreement, signaling the customer's intent to be bound to the terms and conditions of the agreement. When digitizing the entire agreement process, the signature element is often experienced by the customer as "click here to sign". E-signatures have the same legal status as handwritten ink signatures in the United States, Canada, the European Union, Australia, China, Brazil, Japan, and many other countries, under the following:

- United States: ESIGN Act and the Uniform Electronic Transactions Act (UETA)
- Canada: Uniform Electronic Commerce Act (UECA)
- European Union: Electronic Identification and Trust Services Regulation (eIDAS)
- UK: Electronic Communications Act 2000 (ECA)
- Australia: Electronic Transactions Act
- China: Law of the People's Republic of China on Electronic Signature
- Brazil: Provisional Measure No. 2200-2 of 2001
- Japan: Law Concerning Electronic Signatures and Certification Services

For global e-signature laws, see Electronic Signature and the Law: Global Legislation Review.

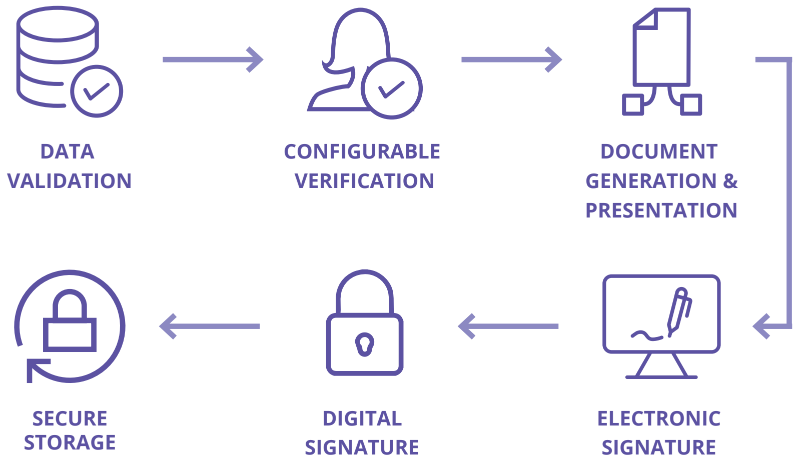
Step 5: Tamper-proofing the Evidence Package

A digital signature is the encryption technology that secures the e-signed document(s) and evidence package. Based on public-key cryptography, the digital signature proves whether the digitally signed content has been tampered with.

Step 6: Secure Storage

This final step in the process involves the secure storage of the audit trails, the agreement, and all related information. Digitizing this step means storing everything in a secure digital environment.

Graphic: End-to-end customer agreement process



STAKEHOLDERS TO INVOLVE IN THE PROCESS

The digital readiness of financial institutions will influence the ease with which an agreement automation solution can be adopted, and the time taken to recognise the benefits.

Those which have fully implemented digitalization and have a pervasive digital infrastructure will be at an advantage.

Cross-functional teams are an important factor in successful agreement automation implementations, which typically involve specialists from operations, sales, compliance, risk, legal, digital, and IT departments.

Since the RFP process takes place before a supplier has been chosen, it is essential that business sponsors and those who will ultimately make the decision on which solution will be purchased, should be present.

For more information about which internal stakeholders to involve in an agreement automation project, refer to the Stakeholders Guide below.

Stakeholders Guide

STAKEHOLDER	WHY THEY SHOULD BE INVOLVED	RFP SECTIONS THEY WOULD BE INTERESTED IN
Digital Strategy / Transformation	With a mandate to transform businesses through innovation, digital teams are an important stakeholder in the automation solution buying process. Digital can use their knowledge of customer experience trends, new technologies, and the organisation's transformation agenda to advise other stakeholders on the innovation, and whether it will deliver on the organisation's core digitisation goals. The digital team should ensure that a chosen solution will improve the customer experience by reducing friction during the customer agreement process.	· Business benefits · Functionality · User experience · Use cases · Client references · Pricing model & commercial terms
Commercial / Sales	The commercial team should be involved to ensure that the solution delivers tangible business benefits. These include higher conversion rates, reduced turnaround times, and increased sales velocity. The commercial team should evaluate whether the business case stacks up and ensure that the solution will have a positive impact on the commercial success of the company.	· Functionality · Use cases · Client references · Business benefits · Pricing model & commercial terms
Operations	Operations are likely to be one of the primary teams involved in the purchasing decision. With a mandate to look at ways to operationally transform the business, they will want to ensure that the solution can reduce operating costs and increase the efficiency of people and processes. They should also look for evidence that an evaluated provider can deliver the project on time and on budget.	· Functionality · Business benefits · Use cases · Client references · Integration, architecture and deployment · Workflow and control · Pricing model & commercial terms

STAKEHOLDER	WHY THEY SHOULD BE INVOLVED	RFP SECTIONS THEY WOULD BE INTERESTED IN
Risk	There is a high volume of business that will potentially go through the solution. Therefore, the risk team should be involved with the purchasing decision so that they can assess the solution for multiple risks; ranging from safeguards against applicant fraud, third-party and staff fraud, to whether the necessary fraud and AML checks are in place. The risk team should evaluate whether the solution shows signs of hidden risk (e.g., legal, operational, fraud-based, or other), how the solution mitigates risk, and how could the solution be configured to address future risks.	· Functionality · Business benefits · Compliance, agreement enforceability, and evidence management · Information security and data privacy
Compliance	The compliance team is responsible for ensuring that the business is compliant with industry and customer protection regulations. The compliance team should ensure that a solution delivers compliant signing ceremonies and an agreement process in compliance with all relevant regulation. They should ask questions about whether a financial institution has control over the workflow, and how the solution collects evidence to prove that a fair and compliant process has taken place.	· Functionality · Business benefits · Compliance, agreement enforceability, and evidence management · Information security and data privacy
Legal	Because financial agreements are legal documents, companies should always include the legal department in the purchase decision process. Legal will want to be sure that an agreement automation solution can create agreements that are executed legally and enforceable (with the right evidence to support them should they be challenged).	· Functionality · Business benefits · Compliance, agreement enforceability, and evidence management · Information security and data privacy
IT / Technical Architects	Representatives from the IT and technical team should be involved in the process to assess how the solution would be integrated with the company's existing technology architecture, and the speed and ease of integration. They should also assess the ease at which the solution can be updated or new features added, to future-proof the solution.	· Integration, architecture, and deployment · Workflow and control · User experience
Procurement	The procurement team will be involved in the procurement process to select a vendor. Procurement will be interested in the following information from vendors: transparent costing; scalability across the business; a proven ability to support similar customers; and ROI.	· Functionality · Business benefits · Use cases · Client references · Integration, architecture, and Deployment · Pricing model and commercial terms

RFP CHECKLIST

A comprehensive RFP that outlines your organization's requirements and asks questions about a provider's ability to meets those requirements, is an essential first step in identifying and partnering with the right agreement automation provider.

Asking questions will enable you to compare providers and technologies to get the best solution for you. To help you do this, we have put together a sample RFP that you can use for your procurement process.

The questions suggested in this guide are provided for general information only. They are not intended to be prescriptive or to provide legal advice.

These questions will help you to determine whether the benefits a solution delivers align with the benefits your organisation is looking to achieve. Consider whether a single benefit is most valuable to you, or whether you are looking to achieve multiple benefits through a single solution.

SECTION 1: BUSINESS BENEFITS

#	QUESTIONS TO ASK	CHECKLIST
1	Explain how the solution delivers the following business benefits for a financial services company: a) Reduction in sales turnaround times b) Increase in sales conversions due to improved customer experience c) Reduction in operating costs d) Increase in compliance e) Reduction in risk f) Reduction in paper usage g) Higher pass rates for identity verification	✓

Ask these questions to assess the functionality the provider's technology delivers. You should look for answers that demonstrate that a provider can deliver the necessary functionality to digitize each stage of the customer's agreement journey (application; electronic ID verification; document generation and presentation; e-signature; tamper-proofing the evidence package; and secure storage.)

You should also ask questions which determine whether the solution collects an audit trail at each stage of the transaction and stores that audit trail in a data package which is intrinsically linked to the signed agreement.

SECTION 2: VENDOR'S FUNCTIONALITY

#	QUESTIONS TO ASK	CHECKLIST
1	How does the solution support customer ID and identity verification?	✓
2	How does the solution authenticate that the correct signatory is present during the signing process?	✓
3	Does the solution offer a multi-layered identity verification approach that ensures multiple identity checks can be used together to meet compliance requirements and in accordance with transaction risk?	✓
4	Does the solution allow for the following types of verification checks? Please give details for each: a) Bureau-based electronic ID checks b) Bank/payment verification c) AML and sanctions screening d) Knowledge-based authentication (KBA) e) Fraud checks f) Device/IP geolocation g) Device integrity h) KYB and director checks i) Identity document capture j) Identity document verification k) Facial comparison and biometrics l) Two-factor authentication	✓
5	What provision is made for service resilience if one of more identity verification method is unavailable (e.g. in the event of a bureau partner being unavailable)?	✓
6	How are Prove Your Customer (PYC) checks undertaken? What PYC tools are available?	✓
7	What happens to the identity data once captured (e.g. decision making, evidence, storage, etc.)?	✓
8	How do you ensure that customers do not drop out of the process at the identity verification stage? Please demonstrate how your technology/solution maximizes the number of applicants who complete the ID verification stage of their agreement journey.	✓
9	Can different verification technologies be used for different transactions (e.g. segmented by risk, value, channel, product, etc.)?	✓

#	QUESTIONS TO ASK	CHECKLIST
10	How does the solution support agreement creation and presentation to ensure that the agreement the customer views is accurate and consistent?	✓
11	How does the solution support document templates so that contracts can be customized and personalized?	✓
12	How are existing agreement templates updated, and new ones created?	✓
13	Can document templates support configurable field placement, saved tags?	✓
14	What methods are used to capture customer consent?	✓
15	What methods are used to capture customer intent?	✓
16	How is the functionality of your solution aligned to local law and regulations regarding the legality and use of e-signatures?	✓
17	Can the solution cater to different customer locations (e.g. in-store assisted, e-commerce unassisted, mobile/PC, etc.)?	✓
18	What methods for customer signature can be used?	✓
19	How does the solution support multiple signers? How would the solution support multiple remote signers, if signing from different locations?	✓

Ask these questions to determine whether the solution collects evidence to prove that the customer is who they say they are, that their identity is not fraudulent, and that they intended to electronically sign the agreement.

You should also look for answers that demonstrate that the evidence is stored in a tamper-proof way, that it cannot have been lost, deleted, or changed after it was created (either by accident or design), and that it is easily retrievable and understandable by non-technical individuals. These qualities will help determine whether the solution is capable of capturing, storing and managing evidence which can prove that a fair and compliant process took place, and support the enforceability of an agreement if challenged.

SECTION 3: COMPLIANCE, AGREEMENT ENFORCEABILITY, AND AUDIT TRAIL MANAGEMENT

#	QUESTIONS TO ASK	CHECKLIST
1	How does the solution provide an audit trail of each stage of the customer agreement journey?	✓
2	How does the solution integrate identity verification checks as evidence to support an electronic signature?	✓
3	How does the solution integrate identity verification checks into the e-signature user experience to help prove the signer's identity?	✓
4	How does the solution ensure that all electronic evidence (audit trails) have integrity? *(By 'integrity' we mean that it cannot have been tampered with, either by accident or design. You could ask the question 'How does the solution ensure that the evidence could not have been tampered with, amended or deleted, either by accident or design?')*	✓
5	Does the solution support time/date stamping of key customer actions?	✓
6	What data points and audit trails are included within a final contract package?	✓
7	How do you prove that all evidential components are uniquely linked? *(By 'uniquely linked' we mean that the evidence and the signed agreement are linked together and that the evidence is embedded into the signed agreement.)*	✓
8	How do you prove the process which a customer followed during signing?	✓
9	What is the process for accessing and utilizing the audit trail in the event of a customer challenge?	✓
10	Does the audit trail prove that the customer saw the agreement before signing it?	✓
11	On a slow internet connection, how does the system ensure that the document has been fully presented to the user before being allowed to sign?	✓
12	Does the solution provide an audit trail of exactly what the customer did during the signing process?	✓
13	In the case of a document with multiple signers, does the audit trail reflect the unique date/time stamps for each signer?	✓

#	QUESTIONS TO ASK	CHECKLIST
14	Does the system store the audit trail in a single place?	✓
15	How easy is it to find and access the audit trail pertaining to each transaction?	✓
16	Does the financial institution need to rely on internal IT or third parties to retrieve, explain, or verify the audit trail? If so, is the audit trail accessible in perpetuity?	✓
17	Is it possible to print out the audit trail if necessary?	✓
18	Is it possible to store and move the audit trail without compromising its integrity?	✓
19	Is the audit trail persuasive? *(By 'persuasive' we mean 'Is the evidence simple and clear, and does it use non-technical language that could be understood by a non-IT expert, such as a customer, judge or regulator?' The more easy it is to access and understand, the more likely a judge would find it persuasive in the event of an enforceability challenge.)*	✓
20	How does the system ensure that all of the captured audit trail is easily understandable by non-technical individuals who may be required to view the audit trail, such as judges, regulators, or auditors?	✓
21	How are the agreement and audit trail securely stored?	✓
22	How are agreements and audit trails accessed?	✓
23	How does the system capture persuasive or conclusive evidence of the customer's intent to electronically sign the document?	✓
24	Has the solution been endorsed by leading lawyers specializing in financial services and electronic transactions?	✓

Ask these questions to determine how a solution will be deployed across your organization. Good answers will outline how the solution integrates with existing systems, how easily new functionality can be added to the solution, and whether the solution can be scaled across an organization (for example, to support other products or countries).

It is also important to consider the structure of the organization you will be working with, whether they offer a bespoke integration, and whether they have integration and deployment expertise in the organization, such as a professional services team. You should also ensure that the provider is able to provide both standard and customized reporting.

SECTION 4: INTEGRATION, ARCHITECTURE, AND DEPLOYMENT

#	QUESTIONS TO ASK	CHECKLIST
1	What APIs are provided for integration with existing solutions?	✓
2	Explain the level of expertise in your organization to help deliver the implementation of this project?	✓
3	What is the structure of your delivery organization?	✓
4	How is the deployment team structured?	✓
5	What level of integration support do you offer?	✓
6	Do you offer a bespoke integration?	✓
7	Do you have a professional services offering to project manage integration?	✓
8	What does a typical project engagement plan look like?	✓
9	What KPIs do you deliver against? How do you ensure that they are met?	✓
10	What is the process of introducing new verification technologies to the solution?	✓
11	Are all verification checks and e-signature services available under a single integration?	✓
12	Are all verification checks and e-signature services available under a single SLA?	✓
13	What are the deployment options for the solution? Please describe.	✓
14	What environments are available during the project, e.g. testing, production?	✓
15	Can the solution integrate with existing document management/storage solutions?	✓
16	Can the solution notify a customer that a document is ready for signing and/or remind them of outstanding documents ready for signing?	✓
17	What countries is the solution available in?	✓

#	QUESTIONS TO ASK	CHECKLIST
18	Does the solution meet regional/in-country data residency requirements?	✓
19	How does the solution cater to changing contract content, e.g. version control?	✓
20	How are ongoing change requests managed?	✓

These questions will enable you to assess the level of ongoing support that the provider is able to offer post-deployment. Look for evidence that solution providers can provide assurances on service levels. Indicators such as system uptime and response protocols will help you assess service level quality.

SECTION 5: SERVICE LEVELS, SCALABILITY, AND SUPPORT

#	QUESTIONS TO ASK	CHECKLIST
1	What KPIs do you deliver against? How do you endure that they are met?	✓
2	Do you stress-test the system regularly to ensure that it is scalable?	✓
3	Please provide an overview of your support capabilities.	✓
4	What hours is your support desk available?	✓
5	What is the SLA for response time if your service goes down or there is an issue with any of our transactions?	✓
6	Describe your response protocols to both minor and major incidents and explain how we will be informed of the incident, resolution steps, and preventive actions for future incidents.	✓
7	What is the target resolution time for both minor and major incidents?	✓
8	What is the SLA for uptime of your service?	✓
9	What is the system uptime % in the last 24 months?	✓
10	How do you define uptime, and are there any exceptions (e.g. scheduled maintenance)?	✓
11	Through what channels can we expect support (e.g. phone, email, web chat etc.)?	✓
12	How do you work with your customers on an ongoing basis to ensure they're getting the best out of the system?	✓
13	What reporting functionality does the solution provide? Does the solution provide: a) Standard reports? b) Bespoke reporting?	✓

Ask these questions to make sure the solution gives an organization granular control of every aspect of the transaction process.

Good answers will show that the solution offers the ability to control the workflow and setup and track contract documents throughout the contract lifecycle in a way that matches the organization's needs, such as the ability to deal with multiple signatories and set up notifications.

SECTION 6: WORKFLOW AND CONTROL

#	QUESTIONS TO ASK	CHECKLIST
1	Does the solution support workflow? If so, how are workflow rules are created and maintained in the solution.	✓
2	Please indicate how the workflow capabilities cover multiple user sessions.	✓
3	Can workflow be sequenced in serial, parallel, and mixed routing?	✓
4	Does the workflow allow for the same document(s) to be sent to multiple recipients simultaneously?	✓
5	Are there any limitations to the number of workflow scenarios that can be deployed by the system?	✓
6	Are multiple workflows handled as a single integration to the service?	✓
7	What real-time control of workflows can the solution provide?	✓
8	How are central IT systems updated with the status of a transaction?	✓
9	How do you ensure consistency in omni-channel customer journeys?	✓
10	How do you ensure that a customer has a consistent customer experience (CX) across multiple channels? For example: - In-store? - On mobile? - At home?	✓
11	How do you ensure that a customer has a consistent customer experience (CX) across multiple devices? For example: - Desktop computer/laptop? - Mobile? - Tablet?	✓

Ask these questions to check that the solution will offer an easy to use experience for the customer. Difficult or bad user experiences will lead to customers becoming disengaged and a decrease in sales, so the delivery of a great customer experience should be a top priority.

Good answers will show the solution is accessible from multiple solutions and devices, is constantly available, and can be configured to match the organization's branding and chosen formats.

SECTION 7: USER EXPERIENCE

#	QUESTIONS TO ASK	CHECKLIST
1	Describe the features and functionality in your solution that contribute to ease-of-use and an improved customer experience.	✓
2	Is the user interface available across devices and browsers?	✓
3	Does the user interface use responsive design?	✓
4	Can the user interface be configured easily? What tools are provided to implement this?	✓
5	Is it possible to white-label every aspect of the agreement automation process? Please identify how the solution allows the following to be customized: a) Language, including localization b) Colors, logo and the visibility of elements such as header, navigation bar, footer, etc. c) Content and look-and-feel of email notifications d) Dialog boxes and error messages	✓
6	Are there configurable session timeouts and transaction expiry times?	✓
7	Can users access documents once they have signed? If so, how is this implemented?	✓
8	Can the user print documents that have been signed?	✓
9	Can the user print documents that have not been signed?	✓

Ask these questions to establish that the solution can meet all relevant legal and regulatory requirements regarding information security and data privacy.

Good answers will indicate that the solution has been designed to support the organization in meeting data compliance requirements (e.g. GDPR in the EU or other local standards); that the provider is compliant with all necessary information security accreditation standards; and that the solution is future-proofed against new or updated regulatory requirements.

The ability to future-proof a solution against new legislation is an important feature. Solutions which cannot be updated run the risk of becoming outdated, non-compliant, and expensive to fix. This can lead to both financial and reputational damage.

SECTION 8: INFORMATION SECURITY AND DATA PRIVACY

#	QUESTIONS TO ASK	CHECKLIST
1	Are appropriate policies, procedures and controls in place to protect the privacy of personal information in accordance with national and international legislation and regulation?	✓
2	Please describe your processes for securing customer data.	✓
3	Has your system or database(s) ever been breached (e.g. and the data exposed to phishing or other risks)?	✓
4	How is the solution future-proofed against new regulatory requirements relating to data privacy, including data erasure and data portability requirements?	✓
5	Does the solution support compliance with local data protection laws and regulations with regards to: a) the ability to capture consent during the agreement process; and b) compliant storage of personal data? How is this implemented?	✓
6	What are the solution provider's data protection and retention policies and procedures? Are they transparent, enforced, and easily accessible?	✓
7	What technical and organizational measures are in place to ensure our customer data is protected from unauthorized access, misuse, or theft?	✓
8	What is the testing frequency for policies, procedures, and control processes to ensure compliance?	✓
9	What security policies are in place in respect of data hosting and transfer?	✓
10	How does your system protect customer and signature data at rest and when being transmitted?	✓
11	Are data feeds of Personal Identity Information (PII) encrypted or controlled to ensure confidentiality and integrity? If yes, how is the information protected?	✓
12	Are technical security reviews carried out manually or using automated tools? How is technical compliance achieved (e.g. penetration testing and vulnerability assessments)?	✓

#	QUESTIONS TO ASK	CHECKLIST
13	Is the solution continuously tested and audited to meet security controls set forth by independent certification authorities (e.g. ISO 27001, SOC 2, etc.)?	✓
14	Describe how your application and its associated data is hosted (i.e. cloud, bare metal, local vs. remote, etc.). If you use any external providers, specify them and explain why they were chosen.	✓

Ask these questions to assess whether the solution provider has deep expertise in your industry, and whether they can demonstrate having implemented successful solutions for other clients.

Look for evidence of quality feedback, deep industry expertise, and the ability to deliver business outcomes (such as reduced cost and wastage, increased revenue and conversion, and improved compliance).

SECTION 9: USE CASES AND CLIENT REFERENCES

#	QUESTIONS TO ASK	CHECKLIST
1	Provide examples of your experience delivering this solution to a similar organization.	✓
2	Who are your largest clients? Please describe their use cases.	✓
3	Provide two relevant client references.	✓
4	Please provide details of your expertise delivering your solution to other companies within our industry.	✓
5	Please indicate the industries you work in and your industry specialties, if applicable.	✓
6	Please provide details of your business's credit rating and profitability. *(Ask this question to ensure that the business is credible and profitable).*	✓

Ask these questions to assess the provider's pricing model and identify all relevant fees. Consider the true cost of ownership when it comes to implementation. Make sure you are aware of what you will be required to take on during the implementation process, and what the solution provider will take on and manage. Make sure that you are happy with the levels of support the provider includes as part of their fees.

SECTION 10: PRICING MODEL & COMMERCIAL TERMS

#	QUESTIONS TO ASK	CHECKLIST
1	What is the pricing model?	✓
2	What setup fee do you charge?	✓
3	Do you charge a licensing fee? If so, is this charged on a weekly or monthly basis? Please give details of the weekly or monthly licensing fee.	✓
4	What is the standard length of a contract with a client (e.g. 1, 3 or 5 years)?	✓
5	What fee do you charge per transaction? Does this change as our transaction numbers scale?	✓
6	What fee do you charge for training?	✓
7	What fee do you charge for ongoing support?	✓
8	Given the monthly transaction volumes specified [X transactions per month], what is the all-in monthly cost of the service? Annual cost?	✓
9	Are there any additional fees charged apart from the types specified in questions 1-7?	✓
10	What is the total cost of implementation?	✓
11	What is the total cost of ownership? How much of the implementation falls to the internal IT team and the provider's technical team?	✓

GETTING STARTED

Financial institutions looking to remove friction and improve their customer experience need to embrace digitalization.

Whether opening a new bank account, applying for a credit card or personal loan, taking out a mortgage or agreeing to an asset finance agreement – customers want to be able to transact at home, on their mobiles and outside of the branch.

Financial agreement automation is the first step in enabling digital financial transactions. Agreement automation includes digitizing the application, ID verification and agreement signing steps in the transaction process.

Financial institutions looking to automate their agreement processes should start by following these four steps:

1. **Decide which stakeholders to involve in the process** – Use guide on page 8 to assist you.
2. **Select which vendors to assess** – Review vendor websites and product information.
3. **Ask detailed questions to determine vendor functionality and capabilities** – Use RFP questions on pages 10 – 24 as a template.
4. **Select a vendor** – Chose a vendor who can deliver an agreement automation solution that improves the customer experience without compromising on risk.

Why Choose OneSpan Agreement Automation?

Complete Automation

Automate any agreement type across your channels – online, mobile, call center and branch.

Digital Identity Verification

Leverage the OneSpan V-Hub for real-time Know Your Customer (KYC) and Prove Your Customer (PYC) checks, including ID document verification and liveness detection.

E-Signature

Digitize agreement workflows and capture the customer's consent with secure, legally binding electronic signatures – on any device.

End-To-End Audit Trails

Collect complete audit trails – from verification to signature – to prove exactly what the customer saw and did at each stage of the digital customer journey.

Fully White-Labeled Solution

Every aspect of the agreement automation process can be white-labeled, allowing you to customize language and branding, dialog boxes, buttons and navigation.

Contact us today to learn more about how OneSpan can help you make bold advances in your digital transformation.

OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

CONTACT US

For more information:
info@OneSpan.com
OneSpan.com

Last Update November 2018.