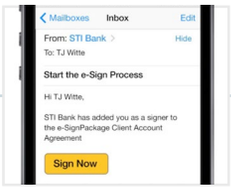
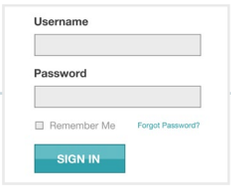
eSignLive by VASCO

FLEXIBLE AUTHENTICATION OPTIONS FOR E-SIGNATURE TRANSACTIONS



EMAIL AUTHENTICATION

- The signer is told to expect an email invitation. An embedded link will take them to the e-signing ceremony.
- The authentication happens when the signer logs in to their personal or corporate email account.
- He/she clicks the link in the email and is taken to the documents requiring signature.
- This establishes a connection to the signer due to the uniqueness of their email address.

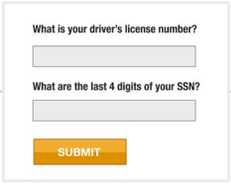


LOGIN CREDENTIALS (USERNAME/PASSWORD)

- The signer is authenticated through the sender's system. This could be an online banking portal, a government services portal or even an eSignLive SaaS account.
- Using the online banking portal example, the customer logs in to their account, is presented with the documents and e-signs from within the portal.

SMS AUTHENTICATION

- A unique PIN is automatically generated by eSignLive and sent to the customer's cell phone.
- The signer types it into the login page and gains access to the documents that require signature.



STATIC KNOWLEDGE-BASED AUTHENTICATION (AKA SECRET QUESTION CHALLENGE)

- Challenge questions are commonly referred to as "shared secrets" since the sender needs to know something about the customer to establish the questions.
- The two parties agree to the question/answer sets before initiating the transaction.
- Common questions include last four digits of a SSN, application ID number, etc.

DYNAMIC KNOWLEDGE-BASED AUTHENTICATION

- eSignLive integrates with third-party ID verification services such as Equifax, Experian or TransUnion, to present the signer with a list of out-of-wallet questions generated on the fly.
- eSignLive captures the responses and presents them back to the service provider for confirmation of the customer's identity and approval to provide access to the e-signing ceremony.

CAC & PIV CARDS

- Government users routinely e-sign with a digital certificate stored on their CAC or PIV smartcard.
- This provides two- and even three-factor authentication with something the user knows (the PIN for their smartcard), something the user has (the card) and sometimes even a biometric identifier (something the user is).

CERTIFICATE-BASED AUTHENTICATION

- eSignLive leverages digital certificates issued by third-party certificate authorities (CA).
- Before using a digital certificate, eSignLive verifies its validity dates.

HAND-SCRIPTED SIGNATURE

- If the signer has a touchscreen mobile device, they can use it to capture their signature.
- The digitized handwritten signature can be compared against a signature sample already on file or used for forensic analysis to authenticate the signer.
- This is the closest thing to a wet ink signature on paper.

www.eSignLive.com