Technical Brief on DocuSign eSignature

The World Bank Group uses **DocuSign eSignature** as its electronic signature solution. DocuSign enables you to electronically send and sign documents, conveniently and securely from any computer or mobile device.

1. **Signing Overview**
   - DocuSign eSignature is cloud-based, Software as a Service (SaaS).
   - The most common method of collecting signatures in DocuSign is via email, where the DocuSign system sends each signer an email containing a secure link to the envelope that requires signature.
   - For documents sent by the WBG, if the signer is registered with DocuSign, they are required to login – username and password, or if the signer's organization uses Single Sign-On (SSO) – to view and sign the document. If they are not registered with DocuSign, they can simply click to view and sign the document.
   - Do not forward DocuSign emails. They are intended for the recipient of the email only. Access codes and identity verification methods can mitigate unintended recipients from viewing and acting on documents.
   - There is a custom Electronic Record and Signature Disclosure (written by the legal departments of IBRD, IFC, MIGA, ICSID) that signers must agree to before they can view the document and sign electronically.

2. **Technical & Security Information**
   - For documents sent by the WBG, they are encrypted (AES 256-bit encryption for the most recent FIPS-approved methods) by security appliances installed in our data centers and protected by our corporate firewalls. This means that the vendor, DocuSign, cannot access the documents we initiate at any time.
   - DocuSign uses PKI (Public Key Infrastructure) technology with X.509-compliant certificates. A Certificate Authority ensures the key security. The World Bank does not maintain or store any keys for signing and does not store data for registering the identity of individuals.
   - Regarding document retention, the WBG chooses to remove documents on the vendor's cloud after 90 days. After this period all documents are purged from DocuSign. All signed documents are stored in a WBG institutional records system, and managed according to retention and disposition policy, instead of remaining in the vendor's cloud.
   - You can read about DocuSign eSignature's security on their Trust Center website.
     - DocuSign eSignature is based on PKI with X.509 certificates.
     - DocuSign is compliant with ISO 27001 and SOC 1 Type 2 and SOC 2 Type 2, and the PCI Data Security Standard (DSS).
     - DocuSign is GDPR compliant.
   - DocuSign follows industry best practices to logically separate individual customer data and encrypt customer data—all data access and transfer activities use HTTPS and other secure protocols, such as SSL, SSH, IPsec, SFTP, or secure channel signing and sealing.
   - Recipients may request an additional level of security around the signing through the use of an access code, such as a one-time passcode, that would be entered before viewing and signing the document. Access codes are a simple way to provide a higher level of confidentiality and non-

repudiation. Only the sender of the document and its signer know the access code, which must be shared outside of DocuSign.

- Recipient organizations can whitelist DocuSign domains and IP addresses.
- Recipients can also implement Sender Policy Framework (SPF) lookup functionality and Domain-based Message Authentication, Reporting & Conformance (DMARC) to mitigate phishing.

3. Signature Types

- By default DocuSign uses their platform signature to sign all PDF documents that are downloaded from their system with an X.509 compliant digital certificate issued by Entrust.
    - This is a basic or **Standard Electronic Signature**. The PDF is signed using DocuSign's platform signature and notes "Signed by DocuSign, inc." Non-repudiation and signer information relies on a separate summary document with the audit trail showing who signed, when they signed, and how they signed, relying on email authentication.

4. Authenticity, Integrity, and Non-Repudiation

- If standard signatures are used, DocuSign signs the PDF with their platform signature to provide a tamper proof seal. Any changes to the document will be noted in the Signature Panel of your PDF software.
- An additional summary document and an audit trail, that DocuSign calls a Certificate of Completion, lists all of the events related to the signing transaction (who signed, when they signed, how they signed, etc.). This information is provided to all recipients in the workflow. Any changes to the document will be noted in the Signature Panel of your PDF software.