Resumo Técnico sobre a DocuSign eSignature

O Grupo Banco Mundial usa a **DocuSign eSignature** como sua solução para assinatura eletrônica. A DocuSign permite que você envie e assine documentos eletronicamente, de forma conveniente e segura a partir de qualquer computador ou dispositivo móvel.

1. **Visão geral do processo de assinatura**
   - A DocuSign eSignature é um software como serviço (SaaS) em nuvem.
   - O método mais comum de coleta de assinaturas na DocuSign é por e-mail, e o sistema DocuSign envia a cada signatário um *link* seguro para o envelope que requer assinatura.
   - No caso de documentos enviados pelo GBM, se o signatário for cadastrado na DocuSign, ele deverá fazer *login* - com nome de usuário e senha, ou se a organização do signatário usar Single Sign-On (SSO) - para visualizar e assinar o documento. Se o signatário não for cadastrado na DocuSign, ele deverá simplesmente clicar para visualizar e assinar o documento.
   - Não encaminhe os e-mails da DocuSign. Eles se destinam apenas ao recipiente específico. Códigos de acesso e métodos de verificação de identidade podem evitar que outros destinatários, que não aqueles pretendidos, visualizem e tomem qualquer ação em relação aos documentos.
   - Os signatários devem concordar com o Termo de Assinatura e Registro Eletrônico personalizado (elaborado pelos departamentos jurídicos do BIRD, IFC, MIGA, ICSID) antes de visualizar e assinar o documento eletronicamente.

2. **Informações técnicas e de segurança**
   - Os documentos enviados pelo GBM são criptografados (criptografia AES de 256 bits para os métodos mais recentes aprovados pelo FIPS) por equipamentos de segurança instalados em nossas bases de dados e protegidos por nossos *firewalls* corporativos. Isso significa que o fornecedor, DocuSign, jamais pode acessar os documentos enviados pelo Banco.
   - A DocuSign usa a tecnologia PKI (*Public Key Infrastructure*) com certificados compatíveis com o X.509. Uma autoridade certificadora garante a segurança da chave. O Banco Mundial não mantém ou armazena nenhuma chave para assinatura nem armazena dados de registro da identidade de indivíduos.
   - Quanto à retenção de documentos, o GBM opta por remover todos os documentos da nuvem do fornecedor após 90 dias. Após esse período, todos os documentos são apagados da DocuSign. Todos os documentos assinados são armazenados em um sistema institucional de registros do GBM e gerenciados segundo a política de retenção e descarte ao invés de permanecerem na nuvem do fornecedor.
   - Você pode ler sobre a segurança da DocuSign eSignature no site Trust Center da empresa.
     - A DocuSign eSignature é baseada em PKI com certificados X.509.
     - A DocuSign está em conformidade com a ISO 27001 e SOC 1 Tipo 2 e SOC 2 Tipo 2, e com o PCI *Data Security Standard* (DSS).
     - A DocuSign está em conformidade com a GDPR.
   - A DocuSign segue as melhores práticas do setor para separar de forma lógica os dados de clientes individuais e criptografar os dados dos clientes; todas as atividades de acesso e transferência de

dados usam HTTPS e outros protocolos seguros, como SSL, SSH, IPsec, SFTP ou assinatura e autenticação em canal seguro.

- Os destinatários podem solicitar um nível adicional de segurança ao processo de assinatura com o uso de um código de acesso, como uma senha de uso único, que deve ser inserida antes da visualização e assinatura do documento. Os códigos de acesso são uma maneira simples de oferecer um nível de confidencialidade mais alto e não repúdio. Somente o remetente do documento e seu signatário conhecem o código de acesso, que deve ser compartilhado fora da DocuSign.
- As organizações destinatárias podem ter uma lista de permissões de domínios e endereços de IP da DocuSign.
- Os destinatários também podem implementar a funcionalidade de pesquisa *Sender Policy Framework* (SPF) e *Domain-based Message Authentication*, *Reporting & Conformance* (DMARC) para reduzir o *phishing*.

3. Tipos de assinatura

- Por padrão, a DocuSign usa a sua plataforma de assinatura para assinar todos os documentos em PDF baixados de seu sistema com um certificado digital compatível com o X.509 emitido pela Entrust.
    - Isso é uma assinatura básica ou a**ssinatura eletrônica padrão**. O PDF é assinado usando a plataforma de assinatura da DocuSign e vem com a observação "Assinado por DocuSign, inc." As informações de não repúdio e do signatário ficam em um histórico separado do documento e a trilha de auditoria mostra quem assinou, quando assinou e como assinou, com base na autenticação por e-mail.

4. Autenticidade, integridade e não repúdio

- Se forem usadas assinaturas padrão, a DocuSign assina o PDF com sua plataforma de assinatura para uma autenticação à prova de adulteração. Quaisquer alterações no documento ficarão registradas no Painel de Assinaturas do seu software de PDF.
- Um histórico do documento e uma trilha de auditoria adicionais, que a DocuSign chama de certificado de conclusão, lista todos os eventos relacionados ao processo de assinatura (quem assinou, quando assinou, como assinou, etc.). Essas informações são fornecidas a todos os destinatários no fluxo do trabalho. Quaisquer alterações no documento serão registradas no Painel de Assinaturas do seu software de PDF.