GUIDELINES FOR

DIGITAL SIGNATURE

Issued under section 7(1) (a) of the Financial Services Act

23 OCTOBER 2023

CONTENTS

Financial Services Commission
FSC House, 54 Cybercity
Ebene, 72201 Mauritius
T: (+230) 403-7000 • F: (+230) 467-7172
E: fscmauritius@intnet.mu
www.fscmauritius.org

1. INTRODUCTION

1.1 The Electronic Transactions Act ("ETA") allows a public sector agency to *inter alia* –

(i) accept the filing of documents, or the creation or keeping of documents in electronic form;

(ii) issue any notice, claim, licence, permit, authorisation or approval in electronic form; or

(iii) make and receive payment in electronic form.

1.2 Where a public sector agency decides to perform any of the functions referred to in paragraph 1.1, it may, by virtue of sections 40(3)(b) and 40(3)(c) of the ETA specify -

(b) where the electronic records have to be signed, the type of electronic signature required including, where applicable, a requirement that the sender uses a digital signature or other electronic signature; and

(c) the manner and format in which the signature shall be affixed to the electronic record, and the identity of or criteria that shall be met by any certification authority used by the person filing or issuing the document.

1.3 The purpose of these Guidelines is to specify the minimum standards which the Commission would expect its applicants[1] and licensees to observe, with respect to the adoption of Digital Signatures as a means for electronically signing documents, in the course of the conduct of their financial business activities.

1.4 These Guidelines shall be read together with the relevant provisions of the ETA and the relevant Acts and any other applicable laws in Mauritius.

[1] Applicant means a person making an application for licence, authorisation and approval.

Financial Services Commission
FSC House, 54 Cybercity
Ebene, 72201 Mauritius
T: (+230) 403-7000 • F: (+230) 467-7172
E: fscmauritius@intnet.mu
www.fscmauritius.org

2. DEFINITIONS

In these Guidelines, unless the context otherwise requires,

"Adobe Reader" refers to the software program developed by Adobe Systems Inc. to view PDF files;

"Adobe Acrobat" is a suite of application software and web services developed by Adobe Systems Inc. that allow users to view, create, edit, and manage PDF files;

"Commission" means the Financial Services Commission, Mauritius;

"digital format" means in digital form;

"digital signature" has the same meaning as in the Electronic Transactions Act;

"digital signature software" refers to the software program that enables users to legally and compliantly give or receive a binding signature;

"eIDAS" means EU Regulation No. 910/2014;

"FSC One Platform" refers to the online portal developed by the Commission to enable the processing of applications, filing of statutory documents and administration of post-licensing submissions by licensees to the Commission;

"Licensees" has the same meaning as in the Financial Services Act;

"Portable Document Format" or "PDF" refers to the file format developed by Adobe Systems Inc. for use with Acrobat;

Financial Services Commission
FSC House, 54 Cybercity
Ebene, 72201 Mauritius
T: (+230) 403-7000 • F: (+230) 467-7172
E: fscmauritius@intnet.mu
www.fscmauritius.org

"relevant Acts" has the same meaning as in the Financial Services Act;

"Wet signatures" mean the process of signing a physical paper document, form or contract with pen and ink.

3. OBJECTIVES

The objectives of these Guidelines are to:

(a) specify the criteria and standards, which applicants and licensees shall observe for the Commission to recognise and accept the use of digital signatures under certain specific criteria, as a substitute for wet signatures; and

(b) establish a high degree of assurance in the course of using digital signatures and ensure that such signatures are not denied legal effect, validity or enforceability for the purposes of the ETA.

4. APPLICATION

These Guidelines govern the use of digital signatures for signing documents related to:

(a) application for a licence through the FSC One platform, involving the electronic submission of PDF document(s) by an applicant, which are digitally signed;
(b) post-licensing requests through the FSC One platform, involving the electronic submission of PDF document(s) by a licensee, which are digitally signed;
(c) inspections organised by the Commission whereby licensees are required to provide documentary demonstrations of PDF documents that include digital signatures; and
(d) submissions of other digitally signed PDF documents as may be determined by the Commission.

Financial Services Commission
FSC House, 54 Cybercity
Ebene, 72201 Mauritius
T: (+230) 403-7000 • F: (+230) 467-7172
E: fscmauritius@intnet.mu
www.fscmauritius.org

5. CRITERIA OF USE

The Commission recognises and accepts the use of digital signatures for the purposes, specified in Paragraph 4 above, subject to the following criteria:

(a) **Criterion 1: The signatory shall be a natural person.**

(b) **Criterion 2: The digitally signed document shall be in the PDF format and the digital certificate used to sign the document shall have been issued by a Certificate Authority listed on the Adobe Approved Trust List (AATL).**

Explanatory notes:

PDF is a file format used for the creation, distribution, and viewing of electronic documents. PDF documents are designed to be self-contained, meaning that they contain all the necessary fonts, images, and other resources needed to display the documents and they also natively support encryption and digital signatures.

The AATL is a list of trusted digital certificate authorities that have been approved by Adobe. When a digital certificate is issued by one of the certificate authorities on the AATL, it is automatically trusted by Adobe software such as Adobe Acrobat and Adobe Reader.

(c) **Criterion 3: The digital signature shall meet the PAdES LTV standard.**

Explanatory notes:

PAdES LTV (PDF Advanced Electronic Signatures with Long-Term Validation) is a specific type of advanced digital signature used to ensure the long-term validity and reliability of digital signatures in PDF documents. PAdES is a set of technical

Financial Services Commission
FSC House, 54 Cybercity
Ebene, 72201 Mauritius
T: (+230) 403-7000 • F: (+230) 467-7172
E: fscmauritius@intnet.mu
www.fscmauritius.org

specifications for PDF-based digital signatures that are compliant with the European Union's (EU)'s eIDAS regulation, which sets standards for electronic identification and trust services across the EU.

PAdES LTV specifically refers to the ability of a PAdES signature to maintain its validity and reliability over time, even if the digital certificates used to create the signature expire or are revoked. This is achieved by embedding additional data into the signature, such as timestamp information and certificate revocation status, which allow the signature to be verified and validated long after it was originally created.

(d) **Criterion 4: The validity of the digital signature shall be automatically verifiable within Adobe Reader/ Adobe Acrobat through the "Signature Panel", "Certificate Details" and "Signature Validation" capabilities.**

Explanatory notes:

Signature Panel: In Adobe Acrobat / Adobe Reader, the Signature Panel displays the digital signature status and provides a summary of the signature details. It shows whether the signature is valid or not, whether the signer's identity has been verified, and whether any changes have been made to the document since it was signed.

Certificate Details: By right clicking on a signature field in Adobe Acrobat / Adobe Reader and selecting "Show Signature Properties," users can view the certificate details associated with the digital signature. This includes information such as the signer's name, the date and time of the digital signature, and the issuer of the digital certificate.

Signature Validation: Adobe Acrobat / Adobe Reader allows users to validate digital signatures by clicking on the Signature Panel or the Signature Field and selecting

Financial Services Commission
FSC House, 54 Cybercity
Ebene, 72201 Mauritius
T: (+230) 403-7000 • F: (+230) 467-7172
E: fscmauritius@intnet.mu
www.fscmauritius.org

"Validate All Signatures". This initiates a process to check the digital signature against the certificate authority's public key infrastructure and verify that it is valid.

(e) **Criterion 5: The security level of the digital signature must meet or exceed the security level required by the eIDAS regulation for Advanced Electronic Signatures (AES).**

Explanatory notes:

An eIDAS AES type of signature provides a higher level of security and legal validity than a Simple Electronic Signature (SES) as it uses advanced cryptographic techniques to bind the signature to the signer's identity and the contents of the document. This ensures the integrity of the signed document and provides a higher degree of assurance that the signature belongs to the person who claims to have signed it.

The digital signature shall, at a minimum, have the following properties:

(i) Unique Signer Identity: The digital signature must be linked to a unique identifier that can be used to verify the identity of the signer through a **digital certificate** issued by a trusted third-party provider.

(ii) Strong Authentication: The digital signature shall require a high level of authentication to ensure that the signer is who they claim to be. This shall involve, at minimum, an SMS-based multi-factor authentication process as an additional layer of security.

(iii) Data Integrity: The digital signature shall ensure that the signed document has not been altered or tampered with since the time of the signature, through

Financial Services Commission
FSC House, 54 Cybercity
Ebene, 72201 Mauritius
T: (+230) 403-7000 • F: (+230) 467-7172
E: fscmauritius@intnet.mu
www.fscmauritius.org

cryptographic hash functions that create a unique digital fingerprint of the document.

(iv) Non-Repudiation: The digital signature shall provide a high level of non-repudiation, meaning that the signer cannot deny having signed the document, by using additional cryptographic techniques such as **time-stamping** and **secure audit trails**.

(f) **Criterion 6: For record-keeping and auditing purposes, a Certificate of Completion (CoC) shall be generated and retained by the digital signature software for every digitally signed document.**

Explanatory notes:

The CoC generated by the digital signature software is used as evidence to establish proof of the digital signature event and based on the following attributes:

(i) Authentication: The CoC shall, at a minimum, contain information about the signer, the date and time of the signature, and other relevant information that can be used to verify the authenticity of the signature.

(ii) Integrity: The CoC shall, at a minimum, contain information about the document being signed, including the document name and the number of pages.

(iii) Compliance: The CoC may be requested by the Commission for the purposes of compliance checks or investigations that require additional verification.

Financial Services Commission
FSC House, 54 Cybercity
Ebene, 72201 Mauritius
T: (+230) 403-7000 • F: (+230) 467-7172
E: fscmauritius@intnet.mu
www.fscmauritius.org

(g) **Criterion 7: The signed document shall include an embedded timestamp.**

Explanatory notes:

An embedded timestamp, within a digital signature, is a digital timestamp that is securely embedded in the signature, providing proof of the exact time when the signature was created. This timestamp is typically generated by a trusted third party. A Time Stamp Authority (TSA) that receives a hash value of the document from the signer and thereafter adds its own timestamp for the creation of a unique identifier. The identifier is subsequently embedded into the signature, along with the signer's digital certificate.

The use of embedded timestamps is an important aspect of ensuring the integrity and authenticity of digitally signed documents. By linking the signature to a specific date and time, the embedded timestamp provides an independent and verifiable record of when the signature was created.

6. DIGITAL SIGNATURE SOFTWARE

6.1 A vendor neutral approach is advisable for the selection of the digital signature software by the applicants and licensees of the Commission. Therefore, the Commission does not prescribe nor recommend any specific vendor. However, the vendor's digital signature software must support a minimum set of security and safety functionalities that would satisfy the criteria set in Paragraph 5, together with a strong audit trail that demonstrates an intention to sign by the signatories.

6.2 The digital signature software must provide the ability for signing parties to download/retain executed documents. In particular, storage, so-called 'shelf life' of documents and their audit trails shall be clearly identified by the signing platform to enable informed choice by signatories. For guidance purposes, the levels of security and safety

Financial Services Commission
FSC House, 54 Cybercity
Ebene, 72201 Mauritius
T: (+230) 403-7000 • F: (+230) 467-7172
E: fscmauritius@intnet.mu
www.fscmauritius.org

functionalities of the digital signature platform shall not be inferior as compared with *DocuSign's EU Advanced Signature.*[2]

6.3 The digital signature software or service provider must, at minimum, be ISO 27001[3] and SOC 2 TYPE 2[4] certified.

7. RECORD KEEPING

These Guidelines shall not have any diminishing or derogation effect for applicants and licensees of the Commission insofar as their record keeping obligation(s) are concerned, in compliance with the existing laws and rules/guidelines issued by the Commission.

8. NON-COMPLIANCE

Failure to comply with the requirement of these Guidelines shall result in the non-acceptance of the digital signature by the Commission and other regulatory actions.

[2] Further information about *DocuSign* in a digital signature software is available at the following website - https://www.docusign.co.uk/products/electronic-signature .
[3] ISO 27001 is an information security standard created by the International Organization for Standardization (ISO), which provides a framework and guidelines for establishing, implementing and managing an information security management system (ISMS).
[4] SOC 2 compliance offers reporting options beyond financial objectives. It covers controls relevant to the trust services principles (TSP): security, availability, processing integrity, confidentiality, and privacy.

Financial Services Commission
FSC House, 54 Cybercity
Ebene, 72201 Mauritius
T: (+230) 403-7000 • F: (+230) 467-7172
E: fscmauritius@intnet.mu
www.fscmauritius.org