Regulation to Establish the Procedure for the Use and Management of Digital Signatures, Signatures, and Electronic Transactions of the General Services Administration of the Government of Puerto Rico

Table of Contents

Chapter I: General Provisions

Article 1.1: Title

This Regulation shall be called the "Regulation to Establish the Procedure for the Use and Management of Digital Signatures, Signatures, and Electronic Transactions of the General Services Administration of the Government of Puerto Rico."

Article 1.2: Legal Basis

1) This Regulation is enacted pursuant to the Law of the General Services Administration for the Centralization of Government Purchases of Puerto Rico, Act No. 73-2019.
2) In Article 5, this Law establishes the General Services Administration (hereinafter, "GSA") as the agency of the Executive Branch responsible for:
   a) Establishing the public policy of Puerto Rico on matters related to the purchase of goods, works, and services for governmental entities.
   b) Implementing the centralization of purchases within the Government.
3) Additionally, Article 11, subsection (j) of the Law empowers the Administrator of the GSA to:
   a) Adopt, amend, and repeal regulations that ensure compliance with this Law and other applicable laws.
4) This Regulation is also enacted pursuant to the following laws:
   a) Act No. 151-2004, as amended, known as the “Electronic Government Law,” which establishes the public policy of incorporating information technologies into governmental administration.
   b) Act No. 148-2006, as amended, known as the “Electronic Transactions Law,” which delegates to the Puerto Rico Innovation and Technology Service (PRITS) the responsibility to establish standards and regulations concerning electronic transactions and the use of digital signatures.
   c) Act No. 38-2017, known as the “Uniform Administrative Procedure Law of the Government of Puerto Rico”, which establishes the rules for the approval, amendment, and publication of administrative regulations.

d) Act No. 75-2019, known as the "Puerto Rico Innovation and Technology Service Act", which establishes the public policy of the Government of Puerto Rico that information and communication technologies be managed with optimal levels of efficiency.

e) Act No. 40-2024, known as the "Cybersecurity Law of the Commonwealth of Puerto Rico", which establishes that every agency, in collaboration with PRITS, will be responsible for developing, documenting, and implementing cybersecurity programs.

Article 1.3: Purpose and Executive Summary

1. The purpose of this Regulation is to establish rules and standards regulating the use of digital and electronic signatures in all operations, both internal and external, of the GSA.
2. The approval of this Regulation aims to:
   a) Minimize the risk of forgery and fraud in electronic signatures.
   b) Ensure the legal validity and security of electronic transactions conducted by the GSA.
   c) Provide clear guidelines for the proper use of digital and electronic signatures in accordance with applicable laws and regulations.
   d) Streamline administrative processes through the digitization of documents and internal procedures.
   e) Adopt confidentiality, integrity and availability of information as essential objectives.
   f) Recognize the importance of establishing GSA network access on a zero-trust architecture basis.
3. Upon the entry into force of this Regulation, the GSA acknowledges and recognizes the validity of digital and electronic signatures in all its transactions and official documents.
4. Pursuant to Law No. 38-2017, supra, it is certified that the adoption, approval, and enforcement of this Regulation will not result in any additional economic impact for the GSA or for the general public.

Article 1.4: Applicability

1. The provisions of this Regulation shall apply to
    a) All dependencies, offices, and officials of the GSA.
    b) Any transaction or administrative procedure in which the GSA uses digital or electronic signatures.
    c) Any interaction between the GSA and governmental entities, contractors, suppliers, or citizens, when the use of electronic signatures is required.
2. This Regulation shall be binding on all officials and employees of the GSA, who must strictly comply with its provisions.
3. The Minimum Safety Standards and Principles established by PRITS must be observed at all times.

Article 1.5: Definitions

a. Administration: General Services Administration.
b. Administrator: Administrator of the General Services Administration.
c. Certification Agency (“CA”): Organization that issues digital signatures via digital certificates and guarantees the authenticity and security of electronic transactions.
d. Authentication: Process of verifying the identity of a person.
e. Zero Trust Architecture: It means that no connection, user or asset is assumed to be trusted until it is verified.
f. Multifactor Authentication: Process of authenticating users that requires more than one mechanism within the authentication triangle (¿What I know?, ¿What I have?, ¿Who I am?). It is based on at least two of the following factors:
    a. Something the user knows (password or PIN)
    b. Something the user has (access card or mobile device).
    c. Something the user is (biometrics such as fingerprint or facial recognition).
g. Authorization to Sign: Permission granted or delegated by the Administrator to sign contracts, receipts, or other documents on behalf of the GSA or any of its dependencies.

h. Bridge Letter: Document issued by an auditor confirming that an organization continues to meet audit standards while awaiting the completion of a formal report.
i. CISA (Certified Information Systems Auditor): Global certification granted by the Information Systems Audit and Control Association (ISACA), which validates a professional's competence in auditing, control, and security of information systems.
j. Certification of Funds: Document issued by the budget department validating the availability of financial resources to cover the costs of a contract.
k. Digital Certificate: File certifying the identity of the user and containing their public key. It is used in various transactions, such as supporting encrypted communications and signing email messages. Its purpose is to validate that the user is authorized to use the public and private keys issued by a Certification Agency.
l. Verification Code: Result of an asymmetric technique that confirms the integrity of encoded information using a unique fixed-size code (number of bits).
m. Confidentiality: Shall mean the prevention of damage to, protection and restoration of computers, systems and/or electronic communication services, including the information contained therein, to guarantee their availability, integrity, authenticity, confidentiality and non-repudiation.
n. CPA (Certified Public Accountant): Professional title granted to certified public accountants who meet the education, experience, and examination requirements in accounting and financial auditing.
o. Document: Information recorded in a tangible medium or stored in an electronic medium, capable of being retrieved in a perceivable manner.
p. Electronic Document: File created, generated, sent, communicated, received, or stored by electronic means.
q. Electronic: Technology that uses electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
r. Employee: A person who provides services to the Administration through appointment with probationary status, regular career service, trust status, temporary, or irregular status.
s. Digital Signature: A type of electronic signature represented as a set of data, sounds, symbols, or processes in electronic form, created by a private key that uses an

asymmetric technique to ensure the integrity of the data message and link the signature holder with the sent message.
A digital signature allows verification of:

i. The conversion was done using the private key corresponding to the signer's public key.
ii. The message or communication has been altered since the conversion.

t. Federal Digital Signature or "Federal Bridge PKI" (FBPKI): A program of the U.S. Federal Government that establishes a public key infrastructure (PKI) to enable interoperability between different governmental entities and digital certifiers.
u. Electronic Signature: A set of data in electronic form attached to a message, document, or transaction, or logically associated with them, that identifies the signer and indicates their approval.
It can appear in various forms:

i. A digitized handwritten signature
ii. An acceptance gesture within an electronic platform. If complemented by a digital signature, it can guarantee the identity of the signer depending on the use of keys and the certifying entity that issues it.

v. Signer: An individual who signs a document manually, digitally, or electronically on their own behalf or on behalf of an entity that has granted them authority.
w. Official: A person vested with state authority or holding a position within the Administration, involved in the formulation or implementation of institutional policies.
x. Incident Management: Means all administrative, physical, and technical procedures applied to investigate and mitigate the suspected or reported incident. This includes notifications of violations or breaches to the parties or individuals impacted by the incident, as applicable by federal and local regulations.
y. Information Security Incident: – Means an event that (i) poses an actual or imminent risk, without authority, to the integrity, confidentiality, or availability of information, a system, a process, or an Information Resource; or (ii) represents a

misuse of an Information Resource or a violation or imminent threat of violation of law, security policies, security procedures, acceptable use policies, or standard computer security practices.

z. ISO 27001 (International Organization for Standardization 27001): An international standard for information security management that establishes best practices for protecting sensitive data and ensuring the integrity and confidentiality of information.

aa. Key Usage for Non-Repudiation: A parameter in digital certificates that prevents a signer from denying authorship of an electronic signature, ensuring the authenticity and legal validity of the digitally signed transaction.

bb. Ransom payment: Means the transfer of money or other property or assets, including virtual currencies, or any portion thereof, made in connection with a ransomware attack, excluding legitimate payment for incident response services.

cc. PIV-I (Personal Identity Verification – Interoperable): A digital credential standard adopted by the U.S. Federal Government to ensure secure authentication in electronic systems.

dd. PIV-C (Personal Identity Verification – Compatible): A variant of PIV-I that offers compatibility with the federal standard without necessarily being issued by a governmental entity. It is used to ensure secure digital authentication in governmental systems.

ee. PRITS (Puerto Rico Innovation and Technology Service): A Government of Puerto Rico agency responsible for establishing standards and regulations for the implementation of information technologies and digital security in governmental agencies.

ff. Risk: means any reasonably identifiable circumstance or fact that has a potential adverse effect on the security of networks and information resources.

gg. SSAE18 (Statement on Standards for Attestation Engagements No. 18): An auditing standard issued by the American Institute of Certified Public Accountants (AICPA) that sets control requirements for certification and compliance reports in the management of third-party data and information systems.

hh. SOC2 (Service Organization Control 2): A compliance report based on SSAE18, focused on the security, availability, processing integrity, confidentiality, and privacy of an organization's information systems.

ii. SOC3 (Service Organization Control 3): A variant of the SOC2 report, designed for public disclosure. It certifies that a company complies with required security controls without revealing internal report details.

jj. Asymmetric Technique: A mathematical algorithm based on the public/private key structure, used to digitally sign or encode messages.

kk. Electronic Transaction: Interaction between people, systems, or governmental entities carried out through electronic means, including the generation, transmission, and storage of electronic documents.

ll. WebTrust for Certification Authorities: An auditing program for Certification Authorities that issue digital signatures and certificates.

Chapter II: Regulation and Use of Electronic and Digital Signatures

Article 2.1: Minimum Usage Requirements

In accordance with PRITS guidelines, the General Services Administration (GSA) shall comply with the following minimum requirements for the use of electronic and digital signatures.

1) Electronic Signatures
   a) Certification Requirements
      i) Possess a Bridge Letter from the SSAE18 SOC2/SOC3 Report; or
      ii) Hold SSAE18 SOC2/SOC3, ISO27001 or equivalent reports.
   b) Contracting Services

   The Administration may contract, for one (1) year, an electronic signature service provider that complies with the following:

      i) Provide a control letter issued by a Certified Information Systems Auditor (CISA) or a Certified Public Accountant (CPA) certifying the information controls implemented.

ii) To renew the contract after the first year, the provider must meet any of the requirements outlined above.

c) Internal Development

i) If the Administration decides to develop its own electronic signature, it must comply with the information controls established in SSAE18, SOC2 and/or SOC3 and PRITS guidelines.

d) Additional requirements

i) Any tool used must support encryption of data in transit and at rest, multifactor authentication, and layered controls.

2) Digital Signatures

a) Issuance Requirements

i) Digital signatures must be issued by a Certification Agency that

(1) Possesses the WebTrust for Certification Authorities Audit Report; or

(2) Is an authorized provider under the Federal Government and the FBPKI/PIVI program.

b) Internal Use

i) If the Administration implements digital signatures for internal use, these must comply with the controls stipulated in SSAE18, SOC3, or PIV-C.

c) Federal Transactions

i) For transactions with the Federal Government, the federal digital signature must be used.

d) Maximum Security

i) Digital signatures certified under the FBPKI/PIV-I program are considered of maximum security, as they include:

(1) Multifactor authentication

(2) Key Usage for Non-Repudiation.

Article 2.2: General Provisions

1. Applicability: The provisions established in this Regulation shall apply to all transactions and administrative procedures, both internal and external, between the GSA and any:
    a) Government agency or dependency,
    b) Private entity, or
    c) Natural person.
2. Responsibility for Implementation: The Director of the Information Systems Division of the GSA, in conjunction with the Administrator, shall be responsible for:
    a) Selecting, authorizing, and validating specific methods for digital and/or electronic signatures.
    b) Determining and managing user authentication mechanisms.
    c) Ensuring compliance with the required level of certainty for identity authentication in various administrative processes.
3. Preferred Use of Electronic and Digital Signatures
    a) Unless otherwise agreed, electronic or digital signatures shall be the preferred method of signing any transaction or document signed between the GSA, governmental entities or agencies, private entities, or natural persons.

Article 2.3: Implementation of Digital and Electronic Signatures

1. When a digital or electronic signature is required by the GSA, it shall be accepted as equivalent to a handwritten signature and shall be legally binding, provided the following requirements are met:
2. Just like with a handwritten signature, the signing party must demonstrate a clear intention to sign the document electronically. This intent can be expressed through:
    a) The use of a cursor or "pad" to draw the signature.
    b) Typing the name on the keyboard.
    c) Pressing an "accept" button or selecting the appropriately identified option.
3. Consent for Electronic Transactions

a) The Administration will validate the consent of the signer by including the following clause in documents to be electronically signed:

"The parties agree that this document may be signed electronically. The parties accept that the electronic signatures appearing on this document are as valid as if they were handwritten, for purposes of validity, binding, consent, applicability, and admissibility."

4. Identification and Authentication of the User
   a) The Administration must ensure that the selected technological solution allows:
      i) Identification of the signer.
      ii) Validation of the signer's consent.
      iii) Verification of the relationship between the document and the electronic signature.
      iv) It is imperative that the solution ensures that the document and the electronic signature are correlated and/or inseparably linked, preserving both its integrity and authenticity.
5. The GSA must carry out technical audits of the platforms to be used at least once every six (6) months.

Article 2.4: Preferential Use of Electronic and Digital Signatures

1. Electronic or digital signatures shall be the preferred signing mechanism for all administrative transactions of the GSA.
2. Unless otherwise agreed, all documents signed between the GSA, government agencies, private entities, or individuals shall use this signing method.
3. The use of digital signatures will ensure:
   a) Legal validity in accordance with the applicable legislation.
   b) Increased efficiency in administrative processes.
   c) Reduction of costs associated with the printing and storage of physical documents.
   d) Increased security using multifactor authentication mechanisms.

4. In cases where the use of a digital or electronic signature is not feasible, its exclusion must be justified in the corresponding administrative file.
5. At all times, the adopted solution must comply with the principles of security by design, in addition to the zero trust architecture.

Chapter III: Signing Procedures and Security

Article 3.1: Procedure for the Use of Digital Signatures

1. The GSA will adopt procedures to ensure that digital signatures are used securely, efficiently, and in accordance with current regulations.
2. All digital signatures must comply with the security and authentication standards set by PRITS.
3. It will be ensured that each authorized user of a digital signature has the necessary access, permissions, and certifications.
4. Protocols will be implemented for the secure storage of digitally signed documents, ensuring their integrity and traceability.
5. The authenticity and validity of digital signatures will be verified before they are accepted in any government transaction.

Article 3.2: Voluntary Exclusion Clause

1. If a signer chooses not to use an electronic signature, the Administration must provide clear and accessible instructions on how to manually sign the document.
2. The use of an electronic signature in a transaction will not require the signer to use this method for future transactions.
3. If opting for a manual signature, the document must be processed under the same terms and conditions applicable to electronic signatures.

Article 3.3: Signed Copies and Document Retention

1. The Administration will ensure that all signers receive a copy of the signed document once the transaction is completed.

2. The signed document copy may be downloaded in PDF format or any other electronic format that guarantees the document’s integrity.
3. The retention of electronic documents will be carried out in accordance with Article 11 of Law No. 148-2006, known as the "Electronic Transactions Law."
4. Measures will be implemented for the preservation, access, and retrieval of electronic documents in compliance with the applicable legal provisions.
5. Mandatory encryption will be required for documents that are signed electronically.
6. Access controls must be included to prevent unauthorized manipulation or disclosure.

Chapter IV: Compliance, Supervision, and Sanctions

Article 4.1: Responsibility of the Information Systems Division

1. The Information Systems Division shall be the unit responsible for ensuring the correct implementation and compliance with this Regulation concerning the use of digital and electronic signatures within the GSA.
2. The Division's responsibilities include, but are not limited to:
    a) Contract Management: Manage the contracting of a Certifying Agency for the issuance of digital signatures and ensure that these meet regulatory requirements
    b) System Maintenance: Implement and manage technological systems that allow for the creation, validation, and secure storage of digital and electronic signatures.
    c) Information Security: Apply security measures to protect digital signatures stored in GSA systems, preventing unauthorized access or improper alterations.
    d) Regulatory Compliance: Ensure that authentication and identity validation standards comply with applicable regulations, including the Electronic Government Law, the Electronic Transactions Law, and PRITS guidelines.
    e) Technical Guidance and Training: Provide technical advice and support to all GSA administrative units regarding the correct use of digital and electronic signatures.

f) Monitoring and Internal Audits: Oversee the compliance with the Regulation through audits and periodic reviews of the digital and electronic signature processes.

3. The GSA shall be obliged to cooperate with the PRITS in any management incidental to the security of the adopted solution.
4. In turn, it must adopt the practice of sending periodic incident reports to the PRITS.

Article 4.2: Violations and Sanctions

Violations:

1. Any action or omission that fails to comply with the established standards for the use, handling, and management of digital and electronic signatures within the GSA will be considered a violation of this Regulation.
2. Violations include, but are not limited to:
   a) Improper or fraudulent use of digital or electronic signatures.
   b) Issuance, creation, or manipulation of digital signatures without meeting the established legal and technical requirements.
   c) Non-compliance with security protocols in the storage and management of digital signatures.
   d) Unauthorized use of private keys, digital certificates, or credentials issued to the Administration or its dependencies.
   e) Alteration, modification, or manipulation of digitally or electronically signed documents.
   f) Implementation of technological solutions that do not meet the standards set forth in this Regulation and PRITS guidelines.
   g) Failure to update or maintain systems related to digital and electronic signatures.
   h) Unauthorized access to digital signature systems or attempts to impersonate identity in authentication processes.

Sanctions:

Violations of this Regulation are subject to sanctions, depending on the nature and severity of the offense.

1. Sanctions for GSA Employees
    a) Written Warning: For minor or unintentional violations that do not pose a significant risk to the security of systems or the integrity of documents.
    b) Suspension: For a determined period, in cases of non-compliance with security measures, negligent use of digital signatures, or repeated violations of the established standards.
    c) Dismissal: For serious violations, such as fraudulent use of digital signatures or intentional manipulation of electronic documents.
2. Sanctions for Contractors, Suppliers, or Third Parties
    a) Contract Termination: If a supplier fails to comply with the provisions of this Regulation, the GSA may terminate the contract immediately.
    b) Disqualification: The contractor may be temporarily or permanently barred from future contracts with ASG by being excluded from the Single Register of Bidders and/or Professional Service Providers.
    c) Legal Claims: If the violation causes economic harm to the GSA, legal actions may be initiated to claim damages.
3. Additional Sanctions
    a) Civil Sanctions: Damages resulting from non-compliance with the provisions of this Regulation may lead to a civil action before the First Instance Court.
    b) Criminal Sanctions: If the conduct constitutes a crime, those responsible will be subject to the penalties provided under applicable criminal laws, including the Anti-Corruption Code of Puerto Rico and the Government Ethics Law. In such cases, the GSA will refer the matter to the relevant law enforcement authorities.

Chapter V: Final Provisions

Article 5.1: Interpretation of the Regulation in the Event of Amendments to the Law

1. If, after the approval and entry into force of this Regulation, any of the laws cited as the legal basis are amended, their provisions shall be interpreted in accordance with the new applicable regulatory framework.
2. Any provision of this Regulation that is incompatible with updated legislation shall be automatically repealed, without affecting the validity of the remaining provisions.
3. In case of doubt regarding the interpretation of this Regulation, the prevailing legal and regulatory provisions governing the use of electronic and digital signatures in the GSA shall apply.
4. The GSA shall have an ongoing duty to review the binding regulations in order to ensure that this Regulation remains as useful as possible.
5. Any future review should consider new developments, both in terms of opportunities and risks, that arise with technological evolution.

Article 5.2: Severability Clause

1. If any article, section, paragraph, sentence, word, or provision of this Regulation is declared unconstitutional, null, or invalid by a court with jurisdiction, such ruling shall not affect, harm, or invalidate the remaining provisions.
2. The judicial declaration’s effect will be limited solely to the specific part declared unconstitutional or null in the legal dispute.
3. In the event that part of this Regulation is declared unconstitutional and its applicability is affected, amendments may be made through the appropriate administrative processes to ensure compliance with current legislation.

Article 5.3: Periodic Review

1. This Regulation shall be reviewed every three (3) years, or sooner if circumstances require, to ensure its alignment with legal, technological, and administrative changes.
2. The review shall be overseen by the Administrator of the General Services Administration or their Authorized Representative.
3. As part of the review process, the opinions of experts in technology, cybersecurity, and legal matters may be solicited to ensure the Regulation's update and effectiveness.

Article 5.4: Effective Date

1. This Regulation shall come into force thirty (30) days after its submission to the Department of State of Puerto Rico, in accordance with Law No. 38-2017, known as the "Uniform Administrative Procedure Law of the Government of Puerto Rico," as amended.
2. It shall remain in effect until amended, repealed, or replaced by a new duly approved regulation.

In San Juan, Puerto Rico, on April __, 2025.

_____

Karla G. Mercado Rivera, Esq.
Administrator and Chief Procurement Officer