

**General Service Administration  
Government of Puerto Rico**

**Number: 9686**

**Date: August 18, 2025**

  
**Approved: Rosachely Rivera Santana**  
**Secretary of State**  
**Department of State**  
**Government of Puerto Rico**

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

<b>Chapter I: General Provisions .....</b>	<b>1</b>
<b>Article 1.1: Title .....</b>	<b>1</b>
<b>Article 1.2: Legal Basis .....</b>	<b>1</b>
<b>Article 1.3: Purpose and Executive Summary .....</b>	<b>2</b>
<b>Article 1.4: Applicability .....</b>	<b>2</b>
<b>Article 1.5: Definitions .....</b>	<b>3</b>
<b>Chapter II: Regulation and Use of Electronic and Digital Signatures .....</b>	<b>5</b>
<b>Article 2.1: Minimum Usage Requirements .....</b>	<b>5</b>
<b>Article 2.2: General Provisions .....</b>	<b>6</b>
<b>Article 2.3: Implementation of Digital and Electronic Signatures .....</b>	<b>7</b>
<b>Chapter III: Signing Procedures and Security .....</b>	<b>7</b>
<b>Article 3.1: Procedure for the Use of Digital Signatures .....</b>	<b>7</b>
<b>Article 3.2: Voluntary Exclusion Clause .....</b>	<b>7</b>
<b>Article 3.3: Signed Copies and Document Retention .....</b>	<b>8</b>
<b>Chapter IV: Compliance, Supervision, and Sanctions .....</b>	<b>8</b>
<b>Article 4.1: Information Systems Office .....</b>	<b>8</b>
<b>Article 4.2: Violations and Sanctions .....</b>	<b>9</b>
<b>Chapter V: Final Provisions .....</b>	<b>10</b>
<b>Article 5.1: Interpretation of the Regulation in the Event of Amendments to the Law .....</b>	<b>10</b>
<b>Article 5.2: Severability Clause .....</b>	<b>11</b>
<b>Article 5.3: Effective Date .....</b>	<b>11</b>

## **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, Electronic Government Act, which establishes the public policy of incorporating information technologies into governmental administration.
  - b. Act No. 148-2006, 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, 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, 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. It includes as well any circular letters, guidance documents and other norms approved by PRITS
- e. Act No. 40-2024, Cybersecurity Act 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, in so far as the necessary tools have been adopted.
2. The approval of this Regulation aims to:
  - a. Provide clear guidelines for the proper use of digital and electronic signatures in accordance with applicable laws and regulations.
  - b. Streamline administrative processes through the digitization of documents and internal procedures.
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 Act 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. The Minimum Safety Standards and Principles established by PRITS must be observed at all times.

### **Article 1.5: Definitions**


- 
- 1. Administration: General Services Administration.
  - 2. Administrator: Administrator of the General Services Administration.
  - 3. Certification Agency ("CA"): Organization that issues digital signatures via digital certificates and guarantees the authenticity and security of electronic transactions.
  - 4. Authentication: Process of verifying the identity of a person.
  - 5. Multifactor Authentication: Process of authenticating users that requires more than one mechanism within the authentication triangle (What do I know?, What do I have?, Who am I?). It is based on at least two of the following factors:
  - 6. 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.
  - 7. Bridge Letter: Document issued by an auditor confirming that an organization continues to meet audit standards while awaiting the completion of a formal report.
  - 8. 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.
  - 9. Certification of Funds: Document issued by the budget department validating the availability of financial resources to cover the costs of a contract.
  - 10. 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.
  - 11. Verification Code: Result of an asymmetric technique that confirms the integrity of encoded information using a unique fixed-size code (number of bits).



- 
12. CPA (Certified Public Accountant): Professional title granted to certified public accountants who meet the education, experience, and examination requirements in accounting and financial auditing.
  13. Document: Information recorded in a tangible medium or stored in an electronic medium, capable of being retrieved in a perceivable manner.
  14. Electronic Document: File created, generated, sent, communicated, received, or stored by electronic means.
  15. Electronic: Technology that uses electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
  16. Employee: A person who provides services to the Administration through appointment with probationary status, regular career service, trust status, temporary, or irregular status.
  17. 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.
  18. 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.
  19. 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:

- a. A digitized handwritten signature
  - b. An acceptance gesture within an electronic platform.
20. 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.
  21. PIV-I (Personal Identity Verification – Interoperable): A digital credential standard adopted by the U.S. Federal Government to ensure secure authentication in electronic systems.

- 
22. 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.
  23. 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.
  24. 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.
  25. 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.
  26. 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.
  27. Asymmetric Technique: A mathematical algorithm based on the public/private key structure, used to digitally sign or encode messages.
  28. Electronic Transaction: Interaction between people, systems, or governmental entities carried out through electronic means, including the generation, transmission, and storage of electronic documents.
  29. 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. At all times these will be subject to the minimum requirements established in Act No. 40-2024 or any other statute that in the future may replace it.

1. Electronic Signatures

- a. Possess a Bridge Letter from the SSAE18 SOC2/SOC3 Report; or
- b. Hold SSAE18 SOC2/SOC3, ISO27001 or equivalent reports.
- c. The Administration may contract with an electronic signature service provider that possesses a control letter certifying the information controls implemented.

2. Digital Signatures

- a. Digital signatures must be issued by a Certification Agency that
  - i. Possesses the WebTrust for Certification Authorities Audit Report; or
  - ii. Is an authorized provider under the Federal Government.
- b. For transactions with the Federal Government, the federal digital signature must be used.
- c. Digital signatures certified under the FBPKI/PIV-I program are considered of maximum security.

**Article 2.2: General Provisions**

- 1. 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. The Administration 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.
- b. All invitations to bid or requests for quotations shall contain a warning informing the interested persons of the preference for digital or electronic signatures, the possibility of their use and their right to request the use of physical signatures.

### **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.
2. Just like with a handwritten signature, the signing party must demonstrate a clear intention to sign the document electronically.
3. 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."

### **Chapter III: Signing Procedures and Security**

#### **Article 3.1: Procedure for the Use of Digital Signatures**

The GSA will adopt procedures to ensure that digital signatures are used securely, efficiently, and in accordance with current regulations.

#### **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.

### **Article 3.3: Signed Copies and Document Retention**

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

## **Chapter IV: Compliance, Supervision, and Sanctions**

### **Article 4.1: Information Systems Office**

1. The Information Systems Office 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. Among its responsibilities are the following:
  - a. System Maintenance: Implement and manage technological systems that allow for the creation, validation, and secure storage of digital and electronic signatures.
  - b. Information Security: Apply security measures to protect digital signatures stored in GSA systems.
  - c. Regulatory Compliance: In collaboration with the Office of Legal Affairs, pursue that the authentication and identity validation standards comply with applicable regulations, including the Electronic Government Law, the Electronic Transactions Law, and PRITS guidelines.
  - d. Technical Guidance and Training: Provide technical advice and support to all GSA administrative units regarding the correct use of digital and electronic signatures.
3. The GSA will cooperate with PRITS in any management incidental to the security of the adopted solution.

## **Article 4.2: Violations and Sanctions**

### **1. Violations**

- a. 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.
- b. Violations include, but are not limited to:
  - i. Improper or fraudulent use of digital or electronic signatures.
  - ii. Issuance, creation, or manipulation of digital signatures without meeting the established legal and technical requirements.
  - iii. Non-compliance with security protocols in the storage and management of digital signatures.
  - iv. Alteration, modification, or manipulation of digitally or electronically signed documents.
  - v. Failure to update or maintain systems related to digital and electronic signatures.
  - vi. Unauthorized access to digital signature systems or attempts to impersonate identity in authentication processes.

### **2. Sanction**

- a. Violations of this Regulation are subject to sanctions, depending on the nature and severity of the offense.
- b. Sanctions for GSA Employees
  - i. Written Warning: For minor or unintentional violations that do not pose a significant risk to the security of systems or the integrity of documents.
  - ii. 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.
  - iii. Dismissal: For serious violations, such as fraudulent use of digital signatures or intentional manipulation of electronic documents.

- c. Sanctions for Contractors, Suppliers, or Third Parties
  - i. Contract Termination: If a supplier fails to comply with the provisions of this Regulation, the GSA may terminate the contract immediately.
  - ii. 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.
  - iii. Legal Claims: If the violation causes economic harm to the GSA, legal actions may be initiated to claim damages.
- d. Additional Sanctions
  - i. Civil Sanctions: Damages resulting from non-compliance with the provisions of this Regulation may lead to a civil action before the First Instance Court.
  - ii. 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.
  - iii. Administrative sanctions: The GSA in its discretion may also impose any fines or sanctions for which it is legally authorized in conformance with Act No. 73-2019.

## **Chapter V: Final Provisions**

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

1. 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.
2. The GSA shall have an ongoing duty to review the binding regulations in order to ensure that this Regulation remains as useful as possible.
3. 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.

### **Article 5.3: 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.

In San Juan, Puerto Rico, on August 1, 2025.

A handwritten signature in blue ink, appearing to read 'Karla G. Mercado Rivera', with a stylized flourish at the end.

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