A Strategy for Adopting Post-Quantum Cryptography in the Digital Signature Service of the Federal Government

Ramon L. V. Medeiros[1] **Edna Dias Canedo**[2]

[1]National Institute of Information Technology (ITI), Brasilia, DF – Brazil
[2] University of Brasília (UnB), Department of Computer Science, Brasília, DF, Brazil
E-mail:ramonleonn@gmail.com, ednacanedo@unb.br

Abstract. *The advent of quantum computing poses a significant threat to current cryptographic systems, particularly digital signatures. Governments and organizations globally must prepare for the transition to post-quantum cryptography (PQC) to safeguard the integrity and security of digital communications in the quantum era. In Brazil, the ongoing digitalization of public services through platforms like GOV.BR highlights the urgent need to secure systems against quantum threats. This paper analyzes the current landscape and future prospects of transitioning to PQC within the Brazilian federal government's digital signature service. As existing cryptographic systems, such as the widely used RSA, become vulnerable to quantum attacks, transitioning to quantum-resistant algorithms has become imperative. The study evaluates the current state of Brazil's federal digital signature service, reviews international PQC initiatives, and proposes a comprehensive transition strategy. It identifies key challenges, including technical complexity, interoperability with legacy systems, limited expertise, high costs, and regulatory uncertainties. To address these challenges, the study suggests mitigation strategies such as hybrid cryptographic solutions, public-private partnerships, phased implementation, and an emphasis on education and awareness. The findings underscore the critical importance of collaboration between government, industry, and academia in developing flexible and robust solutions tailored to Brazil's specific needs.*

1. Introduction

Digital signatures, driven by their ability to ensure authenticity, integrity, and non-repudiation, have become a cornerstone of the modern digital economy, enabling secure and efficient transactions across various sectors. By eliminating the need for physical documents and time-consuming bureaucratic processes, digital signatures streamline contracts, commercial agreements, and other critical operations, reducing operational costs and optimizing response times for businesses [Abbes et al. 2024]. This efficiency translates into productivity gains, allowing organizations to focus on strategic activities and innovation, fostering a more dynamic and competitive business environment. Moreover, digital signatures enhance trust in online transactions, encouraging broader participation in the digital economy and driving the growth of e-commerce and other digital industries [Alagheband and Mashatan 2022].

The Brazilian Federal Government provides a digital signature service known as Advanced Electronic Signature. This service is offered by the National Institute of Information Technology (ITI) through the GOV.BR Platform, which is managed by the Secretariat of Digital Government (SGD) under the Ministry of Management and Innovation

in Public Services (MGI). The Advanced Electronic Signature allows users to sign digital documents using their GOV.BR account, either through the Electronic Signature Portal or via public applications integrated with the GOV.BR Platform through an API provided by ITI [ITI 2023]. However, with the advent of quantum computing [Xu et al. 2022] and, consequently, post-quantum cryptography [Sedghighadikolaei and Yavuz 2023], new digital signature algorithms are being developed to withstand attacks from quantum computers. Traditional digital signature algorithms, such as RSA and DSA, which rely on factorization and discrete logarithm problems, become vulnerable in this new computational paradigm [Seo 2020].

The transition to post-quantum digital signatures is particularly critical for government services such as Advanced Electronic Signature. This shift involves not only updating cryptographic algorithms but also revising the entire Public Key Infrastructure (PKI) and adapting the protocols and applications that rely on digital signatures [Alagic et al. 2022],[Campos and Rosa 2023]. An important aspect to consider is backward compatibility. During the transition period, it will be necessary to support both traditional and post-quantum digital signatures, ensuring that systems remain operational while the migration takes place [Guerra and Tavolaro 2021], [Ferreira et al. 2023].

For the Federal Government and other organizations that heavily rely on digital signatures, it is essential to begin planning for this transition as soon as possible. This leads to the following research question: **How can a process be established for adopting Post-Quantum Cryptography in the Advanced Electronic Signature service of the Brazilian Federal Government?**

The implementation of post-quantum digital signatures also introduces technical challenges, such as the increase in key and signature sizes, which may impact performance and storage in existing systems [Mosca 2018]. Therefore, the transition strategy must carefully consider these factors to minimize disruptions to current services. This includes: risk assessment; inventory of systems relying on digital signatures; prioritization of critical areas; and development of a phased implementation plan [ITI 2023],[NIST 2022]. In summary, the transition to post-quantum digital signatures is a key component of a long-term cybersecurity strategy, especially for critical government services. This shift demands careful planning, investment in research and development, and a phased approach to ensure a smooth and secure transition into the quantum computing era.

2. Background

Current cryptography, widely used in digital security systems, primarily relies on public-key algorithms, also known as asymmetric cryptography. These systems, such as the Rivest-Shamir-Adleman (RSA) algorithm and Elliptic Curve Cryptography (ECC), serve as the backbone of modern digital security [Alagic et al. 2022],[Acar et al. 2023]. In the context of digital signatures, these algorithms play a important role. A digital signature is a cryptographic technique that ensures the authenticity, integrity, and non-repudiation of electronic documents [Misoczki and Barreto 2008], [Gyongyosi et al. 2019]. The process involves generating a cryptographic hash of the document, which is then encrypted using the signer's private key [Misoczki and Barreto 2008], [Campos and Rosa 2023].

The Public Key Infrastructure (PKI) is fundamental in this process, as it manages

the issuance and validation of digital certificates. In Brazil, ICP-Brasil, coordinated by the National Institute of Information Technology (ITI), sets the standards for the issuance of digital certificates with legal validity [ITI 2023], [Hussain et al. 2018]. The basic functioning of a digital signature is illustrated in Figure 1.

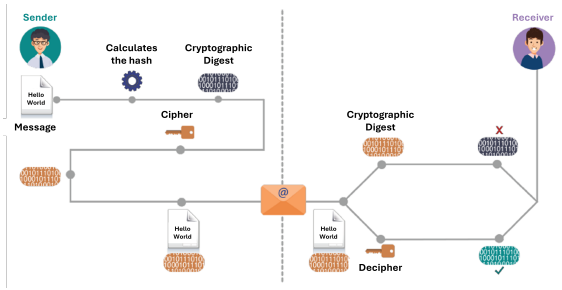

Figure 1. Phases in the digital signature process

Considering that the "Sender" is the one performing the signature, when using a signing system/service, they submit the document to a hash calculation function. The signature process follows these steps [Misoczki and Barreto 2008], [Gyongyosi et al. 2019], [Campos and Rosa 2023]: 1) The result of the hash calculation is a cryptographic hash; 2) The private key stored in the subscriber's certificate encrypts the cryptographic hash; 3) The result is the file containing the digital signature; 4) The file can be sent via email, USB drive, or attached to a digital system or file (e.g., PDF or XML); 5) The recipient uses the subscriber's public key to decrypt the signature file, gaining access to the cryptographic hash previously encrypted by the signer; and 6) Simultaneously, the recipient submits the original document to the cryptographic hash function (used in generating the signature) to compare the current hash with the previous one: a) If the values are the same, the signature is valid and b) If the values are different, the signature is invalid.

This system ensures that only the holder of the private key can create the signature, while anyone with access to the corresponding public key can verify its authenticity [Shaikh et al. 2019], [ITI 2023].

2.1. Post-Quantum Cryptography (PQC)

Quantum computing represents a paradigm shift in computational power, leveraging principles of quantum mechanics such as superposition and entanglement [Bernstein et al. 2017, Acar et al. 2023]. Unlike classical bits, qubits can exist in multiple states simultaneously, enabling massively parallel computations [Acar et al. 2023, Mosca 2018].

The most significant impact of quantum computing on current cryptographic systems is its potential to break widely used public-key algorithms [Alagic et al. 2022, Acar et al. 2023]. Shor's algorithm, for example, can factor large numbers exponentially faster than the best-known classical algorithms, compromising the security of RSA [Alagic et al. 2022, Mosca 2018, Dwork and Roth 2014]. The main threats posed by quantum computing to current cryptographic systems can be summarized as follows: 1) Efficient breaking of RSA and ECC algorithms; 2) Compromise of key exchange protocols; 3) Vulnerability of digital signatures based on classical algorithms; and 4) Risk of retroactive decryption of currently protected data [Guerra and Tavolaro 2021, Mosca 2018].

It is anticipated that sufficiently powerful quantum computers capable of breaking current cryptographic systems may emerge in the coming years, creating an urgent need for the development of quantum-resistant alternatives [Guerra and Tavolaro 2021, NIST 2022]. Post-Quantum Cryptography (PQC) refers to the development of cryptographic systems that are secure against attacks from both classical and quantum computers [Guerra and Tavolaro 2021, NIST 2022]. The following challenges must be addressed in the implementation of PQC: a) Larger key and signature sizes compared to current systems; b) Need for upgrades to existing infrastructures; c) Ensuring computational efficiency across diverse systems; and d) Rigorous validation of security against both classical and quantum attacks [Guerra and Tavolaro 2021, Peikert 2016, NIST 2022].

The goal is to develop algorithms that can be implemented in current systems while remaining secure even in the presence of powerful quantum computers [NIST 2022]. The National Institute of Standards and Technology (NIST) is leading a standardization process for post-quantum algorithms, aiming to establish widely adoptable standards [Guerra and Tavolaro 2021, NIST 2022]. The main approaches in PQC include: 1) Lattice-based cryptography: Relies on mathematically hard problems in lattice structures [Peikert 2016, NIST 2022]; 2) Code-based cryptography: Based on the difficulty of decoding general linear codes [Ferreira et al. 2023, Peikert 2016]; 3) Multivariate cryptography: Uses systems of multivariate polynomial equations [Ferreira et al. 2023, Peikert 2016]; 4) Hash-based cryptography: Exploits the properties of cryptographic hash functions [Pirandola et al. 2020, Ferreira et al. 2023]; and 5) Isogeny-based cryptography: Utilizes mappings between elliptic curves [Pirandola et al. 2020, Guerra and Tavolaro 2021]. The transition to post-quantum cryptography is a complex process that requires careful planning, risk assessment, and a gradual implementation to ensure the continued security of digital communications in the quantum era.

3. Advanced Electronic Signature

The Brazilian Federal Government's digital signature service, based on the Brazilian Public Key Infrastructure (ICP-Brasil), has undergone significant advancements in recent years. The GOV.BR platform, established by Decree No. 8,936/2016, has become a central hub for providing digital public services, including digital signature functionality [Presidência da República do Brasil 2016].

Since April 2022, the Federal Government has offered free digital signatures to citizens through the GOV.BR portal. This initiative has democratized access to a service that was previously limited to holders of paid digital certificates. To use the service, citizens must have a GOV.BR account with a silver or gold verification level, which can be obtained through biometric validation or via accredited banks. Law No. 14,063/2020 regulates the use of electronic signatures in interactions with public entities [Presidência da República do Brasil 2020b]. This law was further detailed by Decree No. 10,543/2020, which granted electronic signatures the same legal validity as physical signatures in various interactions with the government [Presidência da República do Brasil 2020a].

Ordinance No. 2,154/2021, issued by the Special Secretariat for Bureaucratization, classified electronic signatures generated by the GOV.BR platform with Silver and

Gold digital identities as advanced electronic signatures [Mibnistério da Economia 2021]. The GOV.BR Signature Platform was developed to meet the growing demand for digital public services in Brazil, providing a comprehensive and continuously improving solution. This platform consists of three main components: The GOV.BR Signature Portal; The GOV.BR Electronic Signature Services API; The Electronic Signature Validation Service [1].

This infrastructure enables integrated systems to generate electronic signatures in a simplified, reliable, and cost-free manner. In just January and February 2025, approximately 28.7 million signatures were recorded [ITI 2025]. Figure 2 illustrates the transactions involved in the digital signature process of the Advanced Electronic Signature service.

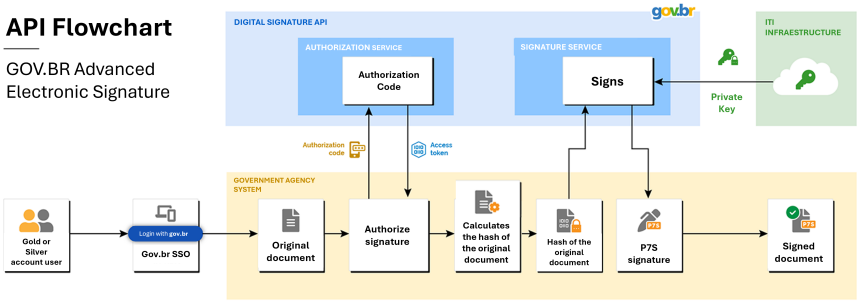

Figure 2. API Workflow of the Advanced Electronic Signature Service [SGD 2025]

The security infrastructure supporting this system requires constant updates to address evolving cyber threats. This includes not only protection against conventional attacks but also preparation for future threats, such as those posed by quantum computing. Therefore, the current landscape presents significant challenges: 1) Uneven Adoption: Although the use of digital signatures is growing, there remains a significant disparity in adoption across different sectors and regions of the country [Bernstein et al. 2017, Alagic et al. 2022]; 2) Technical Complexity: Many users still face difficulties in using the system, particularly when it comes to obtaining and managing digital certificates [Acar et al. 2023, Mosca 2018]; 3) Security Infrastructure: Despite progress, the security infrastructure still requires constant updates to counter evolving cyber threats [Misoczki and Barreto 2008, Gyongyosi et al. 2019]; 4) Integration with Legacy Systems: Transitioning from older systems to the new digital infrastructure remains a challenge in many government institutions [Guerra and Tavolaro 2021, Shaikh et al. 2019].

In addition to these challenges, ensuring interoperability between different platforms and compliance with national and international regulations adds complexity to the modernization process. The adoption of post-quantum cryptography (PQC) emerges as an important strategy to mitigate future risks, ensuring the continuity and reliability of electronic signature services as new threats emerge. Currently, the system provides a robust platform for digital signatures with legal validity, meeting a wide range of governmental and business needs [Bernstein et al. 2017, Acar et al. 2023]. Processes that previously required signatures on physical documents can now benefit from the convenience and

[1] available at https://validar.iti.gov.br

security offered by the GOV.BR Electronic Signature. This transition not only reduces bureaucracy but also significantly drives the digitalization of public services in Brazil.

3.1. Initiatives for Transitioning to Post-Quantum Cryptography

Whether at the national or international level, the transition to post-quantum cryptography (PQC) is driven by the growing threat that quantum computers pose to current cryptographic systems. Several nations and organizations are at the forefront of this movement, developing strategies and implementing solutions to ensure the security of digital communications in the quantum era. In Brazil, a partnership between the Central Bank of Brazil (BCB), Brazil Quantum, Microsoft, and the National Federation of Associations of Central Bank Employees (Fenasbac) led to a study on the use of post-quantum cryptography to enhance the security of the Instant Payment System, PIX. The research examined the feasibility of algorithms resistant to quantum computer attacks in PIX, as the evolution of this technology could pose security threats to the system in the future [Fenasbac 2025, Ferreira et al. 2023].

The United States, through the NIST, has been leading a global effort to standardize PQC algorithms [NIST 2025]. In 2022, NIST selected the CRYSTALS-Kyber algorithm for key encapsulation and CRYSTALS-Dilithium for digital signatures as initial standards [NIST 2022]. Recently, as a key step in the standardization process, NIST published NIST IR 8547, which establishes transition standards for Post-Quantum Cryptography [NIST 2024a]. In the context of PQC algorithms for digital signatures, NIST defines that the CRYSTALS-Dilithium, FALCON, and SPHINCS+ algorithms are currently selected [NIST 2024b].

Countries such as Japan, China, and Canada are also making significant contributions to the advancement of PQC through research initiatives and funding programs. International cooperation has been important in this transition process. This is further enhanced when combined with initiatives from continental or global entities, such as the European Union Agency for Cybersecurity (ENISA) [Chen et al. 2023] and the European Telecommunications Standards Institute (ETSI) [Bodson 2013]. These initiatives offer valuable lessons and potential models for transitioning Brazil's digital signature system to a post-quantum environment. Brazil has the opportunity to learn from these experiences and adapt best practices to the national context, taking into account the specificities of ICP-Brasil and the GOV.BR system.

4. Proposed Transition Strategy

The transition to post-quantum cryptography (PQC) is a complex and multifaceted process that requires a strategic, systematic, and comprehensive approach. This section outlines a detailed strategy for this transition, divided into seven critical subsections, each addressing a fundamental aspect of the process. We will begin with a detailed assessment and a comprehensive inventory of existing cryptographic systems, necessary for understanding the scope of the transition. Next, we will address phased planning, which is important for a gradual and controlled implementation. The selection and implementation of PQC algorithms form the technical core of the transition, followed by the necessary updates to infrastructure and software.

Training and awareness are vital to ensure that all stakeholders are prepared and

aligned with the change. Continuous monitoring and adjustments will ensure the effectiveness of the transition over time. Finally, we will address compliance and legal aspects, which are essential to ensure that the transition aligns with regulations and legal requirements. The following sections present a comprehensive roadmap for a successful transition to post-quantum cryptography within the context of the Advanced Electronic Signature service.

4.1. Assessment and Inventory

The assessment and inventory phase serves as the foundation for the entire post-quantum cryptography (PQC) transition strategy. This step involves a thorough analysis and documentation of all systems, protocols, and cryptographic practices currently in use. First, a complete mapping of all systems utilizing cryptography must be conducted, including: 1) Systems for generating and verifying digital signatures; 2) Public Key Infrastructure (PKI); 3) Secure communication protocols (e.g., TLS, SSL); 4) Systems for storing encrypted data; and 5) Authentication mechanisms.

For each identified system, the following details should be documented: a) Cryptographic algorithms in use; b) Key sizes; c) Specific protocols; d) Key life-cycles; and e) Integrations with other systems. It is also necessary to assess the criticality of each system, considering: sensitivity of the protected data, potential impact of a breach, and expected lifespan of the protected data . This evaluation should include a risk analysis, identifying which systems are most vulnerable to quantum attacks and which should be prioritized in the transition. Furthermore, it is important to consider the dependencies between systems, as changes in one component can affect others. A detailed inventory will help identify these interdependencies and plan the transition in a holistic manner. Finally, this phase should result in a comprehensive report that will serve as the foundation for all subsequent phases of the transition strategy.

4.2. Phase-by-Phase Planning

Phase-by-phase planning is important for a smooth and controlled transition to post-quantum cryptography. This approach allows for a gradual implementation, minimizing risks and disruptions to existing services. **Phase 1. Preparation and Pilot (6-12 months)**: 1) Establish a multidisciplinary team dedicated to the PQC transition; 2) Develop a detailed plan based on the evaluation and inventory; 3) Select non-critical systems for pilot projects; and 4) Begin testing PQC algorithms in controlled environments.

Phase 2. Initial Implementation (12-18 months): 1) Start implementation in less critical systems; 2) Develop and test hybrid solutions (combining classical and PQC algorithms); 3) Assess performance impact and make necessary adjustments; and 4) Initiate training programs for technical teams. **Phase 3. Expansion and Optimization (18-24 months)**: 1) Expand implementation to medium-importance systems; 2) Optimize hybrid solutions based on initial results; 3) Start transitioning long-term data storage systems; and 4) Expand awareness programs for all users.

Phase 4. Critical Implementation (24-36 months): 1) Migrate critical systems to PQC solutions; 2) Perform extensive security and performance testing; 3) Begin the gradual deactivation of vulnerable cryptographic algorithms; and 4) Update organizational policies and procedures. **Phase 5. Consolidation and Review (36+ months)**: 1)

Complete the transition for all systems; 2) Conduct a comprehensive post-implementation security review; 3) Adjust and optimize as necessary; and 4) Establish processes for continuous maintenance and updates.

In each phase, it is need to: i) Set clear and measurable milestones; ii) Conduct regular progress and risk assessments; iii) Maintain flexibility to adjust the plan as needed; iv) Ensure continuous communication with all stakeholders. This phased approach allows for a controlled transition, providing opportunities for learning and adjustments throughout the process, which is essential for the successful large-scale implementation of PQC.

4.3. Selection and Implementation of PQC Algorithms

The selection and implementation of post-quantum cryptography (PQC) algorithms is a critical step in the transition strategy. This phase requires careful analysis of available algorithms, considering their security, efficiency, and compatibility with existing systems. The selection criteria include demonstrated resistance against both quantum and classical attacks, efficiency in terms of processing speed and resource usage, flexibility for integration with existing systems, maturity in terms of review and validation by the cryptographic community, and the status in the standardization process by NIST or other relevant bodies – Security: Proven resistance to both quantum and classical attacks; Efficiency: Performance in terms of processing speed and resource usage. Flexibility: Ability to integrate with existing systems. Maturity: Level of review and validation by the cryptographic community. Standardization: Status in the standardization process by NIST or other relevant bodies.

Among the recommended post-quantum cryptography (PQC) algorithms, CRYSTALS-Dilithium, FALCON, and SPHINCS+ are available options for digital signatures [NIST 2024b]. Both CRYSTALS-Dilithium and FALCON, which are lattice-based, provide robust and efficient digital signature schemes, each with its own advantages in terms of signature size and generation speed. SPHINCS+, on the other hand, offers a hash-based approach that provides long-term security, albeit with some disadvantages in terms of signature size and processing speed.

The implementation of these algorithms involves several crucial steps, including: 1) **In-depth Study:** Conduct a thorough analysis of the algorithm's security features, performance, and integration requirements; 2) **Prototyping:** Develop prototypes to test the algorithms' functionality and suitability for the existing infrastructure; 3) **Integration Testing:** Test the integration of the PQC algorithms with current systems to ensure compatibility and smooth operation; 4) **Performance Evaluation:** Assess the performance of the algorithms in terms of speed, resource usage, and scalability; 5) **Hybrid Implementation:** Deploy hybrid systems that combine classical and PQC algorithms to ensure smooth transition and backward compatibility; 6) **Security Monitoring:** Continuously monitor the security of the PQC algorithms and their resistance to emerging quantum threats; and 7) **Continuous Updates:** Regularly update the algorithms to incorporate improvements, patches, and advancements in cryptographic research.

Initially, a thorough study of the specifications and characteristics of each selected algorithm is necessary. Following this, prototyping in testing environments that simulate real-world usage conditions allows for an initial evaluation of the algorithm's feasibility and performance. Integration testing is essential to assess compatibility with existing sys-

tems and identify any necessary adaptations. Performance evaluation, comparing PQC algorithms with classical cryptography, provides valuable insights into the impact of the implementation. The selection and implementation of post-quantum cryptography algorithms is a critical step in the transition strategy. This phase requires careful analysis of the available algorithms, considering their security, efficiency, and compatibility with existing systems.

A hybrid approach, combining classical algorithms and PQC, is often recommended during the transition phase. This ensures backward compatibility and provides an additional layer of security. Continuous security monitoring is essential to detect potential vulnerabilities or attacks, and continuous system updates are required to stay aligned with the latest PQC developments. Key considerations in the implementation process include: 1) Crypto-agility: Designing systems that allow for easy replacement of cryptographic algorithms in the future; 2) Key Size: Considering the impact of increased key sizes on storage and transmission systems; 3) Compatibility: Ensuring that the PQC implementation does not impair interoperability with external systems; and 4) Validation: Seeking independent validation of the implementation by cryptography experts.

The successful implementation of PQC algorithms requires a meticulous and iterative approach, with a focus on security, efficiency, and compatibility. It is important to remain flexible and prepared to adapt to the continuous developments in the field of post-quantum cryptography, ensuring that federal government digital signature systems remain secure and effective in the face of emerging quantum threats.

4.4. Infrastructure and Software Update

The transition to post-quantum cryptography requires a comprehensive and meticulous update of existing infrastructure and software. This process is necessary to ensure that all components of the federal government's digital signature system are compatible and secure in the post-quantum context. Hardware upgrades are an important aspect of this transition. It is necessary to thoroughly assess the existing processing capacity to determine whether upgrades are needed to support PQC algorithms, which typically require more computational resources. In some cases, it may be beneficial to consider the implementation of hardware accelerators specifically designed for PQC, optimizing the performance of the new algorithms. Additionally, hardware security modules (HSMs) must be updated to versions compatible with PQC, ensuring that the system's root of trust remains robust.

In terms of software, updates must be comprehensive and systematic. Operating systems need to be upgraded to versions that support post-quantum cryptographic libraries. This may involve applying patches and security updates specifically related to PQC. Existing cryptographic libraries should be replaced or updated with versions that include implementations of PQC algorithms. It is necessary to ensure that these new libraries are properly validated and certified by recognized authorities in cryptographic security. Digital signature applications require significant modifications to utilize the new PQC libraries. This involves not only the internal cryptographic logic but also updating user interfaces to accommodate new formats and signature processes. The Public Key Infrastructure (PKI) requires special attention, including updating certificate authority software to support PQC-based certificates and modifying the processes for certificate generation, distribution, and revocation.

The communication protocols, such as TLS/SSL, must be updated to versions compatible with PQC. This involves implementing support for new key exchange and signature algorithms in network protocols, ensuring that communications remain secure against quantum threats. Storage systems also need to be evaluated and updated to accommodate the increase in key and signature sizes in PQC, which are generally larger than their classical counterparts. The update process should follow a methodical and phased approach, where we can define: 1) **Detailed Planning**: Create a detailed inventory of all components that require updating. Develop an update schedule, prioritizing critical systems; 2) **Testing Environment**: Establish a testing environment that replicates the production infrastructure. Perform extensive updates and tests in this environment before implementation in production; 3) **Gradual Implementation**: Start with non-critical systems and gradually expand to more critical ones. Use phased or segmented implementation approaches to minimize risks; 4) **Regression Testing**: Conduct comprehensive testing after each update to ensure that existing functionalities are not affected; 5) **Rollback Plan**: Develop and maintain rollback plans for each update, enabling a quick return to the previous state in case of issues; 6) **Continuous Monitoring**: Implement real-time monitoring during and after updates to detect and respond quickly to any problems; and 7) **Documentation**: Maintain detailed documentation of all changes made to infrastructure and software.

The update of infrastructure and software to support PQC is a complex process that requires meticulous planning, careful execution, and constant monitoring. It is important to observe the following considerations: a) Compatibility: Ensure that updates maintain compatibility with legacy and external systems; b) Security During the Transition: Maintain robust security measures throughout the update process; c) Service Continuity: Plan updates in a way that minimizes downtime of critical services; and d) Scalability: Consider the impact of updates on the future scalability of systems. The success of this phase is essential to ensure the security and effectiveness of the Advanced Electronic Signature system in the post-quantum era, protecting sensitive information from future threats while maintaining operational efficiency.

4.5. Training and Awareness

The transition to post-quantum cryptography (PQC) is not merely a technological change; it is a transformation that impacts the entire organization. Training and awareness are fundamental pillars to ensure that everyone involved, from the technical team to end-users, understands and supports this critical transition. The training process must be comprehensive and strategic. Initially, it is necessary to conduct a detailed assessment of the training needs across the organization. This involves identifying existing knowledge gaps and defining clear learning objectives for different groups within the institution.

Creating internal certification programs in PQC can be an effective strategy to encourage continuous learning and recognize the expertise developed within the organization. At the same time, promoting the attainment of relevant external certifications can enhance the overall level of knowledge and credibility of the team. Awareness, in turn, should be an ongoing and comprehensive initiative. Internal communication campaigns, using various mediums such as emails, newsletters, and infographics, can disseminate important information about PQC in an accessible manner.

It is essential to establish feedback and engagement channels, allowing employees

to ask questions, share concerns, and provide suggestions about the PQC transition process. Regular surveys to assess the level of understanding and acceptance of PQC can help refine and improve training and awareness programs. Finally, it is important to recognize that different groups within the organization will have distinct needs. The technical team, security team, developers, end-users, and senior management require tailored approaches. Adapting the content and format of training and awareness initiatives for each group will maximize their effectiveness.

4.6. Monitoring and Adjustments

Continuous monitoring and the ability to make agile adjustments are crucial elements for the success of the transition to post-quantum cryptography. This phase ensures that the PQC implementation remains effective, secure, and aligned with organizational goals, adapting to changes in the technological and threat landscape. The monitoring process should begin with the establishment of KPIs specific to PQC. These metrics should cover various aspects, such as the processing time of digital signatures, the success rate of signature verifications, the use of computational resources, and the occurrence of security incidents related to cryptography. These metrics provide a quantitative foundation to evaluate the performance and effectiveness of the PQC implementation.

The implementation of real-time monitoring systems is essential for tracking the performance of PQC systems. Threat monitoring is a critical aspect of this phase. It involves maintaining constant vigilance over new quantum threats and advancements in cryptanalysis. Automated log analysis, using advanced data analysis techniques, can identify patterns and anomalies that may not be immediately apparent, providing valuable insights into the system's operation. User feedback is an invaluable source of information. Establishing channels to collect continuous feedback from both internal and external users, as well as conducting regular satisfaction and usability surveys, can reveal practical issues and improvement opportunities that may not be evident from purely technical metrics.

Based on the information collected through monitoring, the organization must be prepared to make adjustments. A periodic review process should be established, with quarterly meetings involving key stakeholders to assess the performance of the PQC system and discuss potential improvements. The update of algorithms is a important aspect of these adjustments. As new PQC algorithms are developed and validated, the organization should have a process in place to evaluate and incorporate these innovations. This requires a balance between adopting cutting-edge technologies and maintaining the stability and reliability of the system. Other important points that must not be neglected include: **Policies and Procedures**: Ensuring that policies and procedures related to PQC are continuously updated and aligned with the latest developments; **Scalability**: Constantly evaluating the scalability of the system to ensure that it can accommodate future growth and increased demand; **Incident Response Plans**: Developing and continuously refining incident response plans specifically tailored to PQC; and **Advanced Tools**: The use of advanced tools, such as big data analysis platforms and customized dashboards, to monitor and respond to potential issues in real time. In summary, effective monitoring and the ability to make agile adjustments are essential to maintaining the robustness and effectiveness of the PQC implementation over time.

4.7. Compliance and Legal Aspects

The transition to post-quantum cryptography (PQC) is not only a technical challenge but also an undertaking that must comply with a range of legal and regulatory requirements. This phase is critical to ensure that the PQC implementation meets not only the technical security standards but also all relevant legal obligations, maintaining the integrity and reliability of the digital signature system. In the context of national legislation, it is essential to analyze and ensure compliance with fundamental laws such as the General Data Protection Law (LGPD) [da República 2018], the Civil Internet Framework, and other relevant regulations. The LGPD, in particular, imposes strict requirements on the processing of personal data, including technical and organizational security measures. The transition to PQC should be seen as an opportunity to reinforce compliance with these requirements, demonstrating a proactive commitment to data protection.

A critical aspect to consider is the legal implications of the transition to post-quantum cryptography concerning the legal validity of digital signatures. It is essential to ensure that digital signatures based on PQC maintain the same legal status as conventional signatures. This may require collaboration with legislative bodies to update, if necessary, the laws recognizing digital signatures, ensuring that the legal foundation for the use of digital signatures remains solid in the post-quantum context. Sector-specific regulations for the public sector must also be carefully considered. This includes adhering to standards set by the National Institute of Information Technology (ITI) and the Brazilian Public Key Infrastructure (ICP-Brasil) [2]. The transition to PQC may necessitate updates to certification policies and practices, as well as technical standards governing the issuance and use of digital certificates within the scope of ICP-Brasil.

On the international stage, it is essential to align with relevant standards, such as those established by the United States' National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI). While these standards do not have the force of law in Brazil, they are widely recognized and can influence global cybersecurity practices. Additionally, for organizations dealing with the data of European citizens, compliance with regulations such as the General Data Protection Regulation (GDPR) [Parliament and European Union 2016] may be necessary, even in the context of Brazilian government services. The review and update of existing contracts with suppliers, partners, and users is a critical aspect of legal compliance. These documents should be revised to reflect changes resulting from the implementation of PQC, including new responsibilities, security standards, and operational procedures. Furthermore, new contract models that incorporate PQC considerations should be developed for future agreements.

To ensure compliance, it is important to conduct a comprehensive impact assessment of the PQC implementation in relation to legal and regulatory compliance. This assessment should identify potential risk areas and develop mitigation strategies. A PQC governance policy should be developed, outlining responsibilities, procedures, and compliance requirements, ensuring that this policy aligns with existing information security policies. Collaboration with regulatory bodies is important during the transition to PQC. Maintaining open communication with relevant entities, participating in public consultations, and joining working groups related to the regulation of cryptographic technologies

[2] https://www.gov.br/iti/pt-br

can not only help the organization stay informed but also influence the development of future regulations. In conclusion, legal and regulatory compliance during the transition to PQC is a complex process that requires constant attention, collaboration between institutions, and a proactive approach. Ensuring compliance with all relevant laws and regulations not only protects the organization from legal risks but also strengthens public trust in the integrity and security of government digital services in the post-quantum era.

5. Challenges and Mitigations

The transition to post-quantum cryptography (PQC) for Advanced Electronic Signatures presents a series of significant challenges that require careful attention and mitigation. One of the main obstacles is the technical complexity inherent in implementing PQC algorithms. These algorithms typically demand more computational resources and greater bandwidth compared to current cryptographic systems, which may lead to performance degradation in existing systems. To mitigate this challenge, it is necessary to adopt a gradual implementation approach, starting with non-critical systems and progressing to more sensitive infrastructures. Additionally, investments in more powerful hardware and software optimization can help offset the additional resource demands.

Interoperability represents another significant challenge. The coexistence of legacy systems with new PQC implementations may create incompatibilities and vulnerabilities. To address this issue, it is essential to develop and implement hybrid solutions that support both classical and post-quantum algorithms during the transition period. This not only ensures operational continuity but also provides an additional layer of security against current and future threats. The shortage of qualified professionals in post-quantum cryptography is another significant challenge. The highly specialized nature of this field demands expertise that is still rare in the market. To mitigate this problem, it is essential to invest in comprehensive training programs, not only for technical teams but also for managers and decision-makers. Partnerships with academic institutions and research centers can be valuable in bridging this knowledge gap and fostering continuous innovation.

The cost associated with the transition to PQC is a factor that should not be underestimated. Infrastructure upgrades, the development of new systems, and the implementation of additional security measures represent substantial investments. To mitigate the financial impact, it is advisable to adopt a phased implementation approach, prioritizing critical areas and spreading the costs over time. Additionally, seeking public-private partnerships and leveraging research and development resources can help distribute the financial burden.

Finally, the regulatory and compliance challenge cannot be overlooked. As new standards and regulations emerge in response to the quantum threat, organizations must stay updated and compliant. Mitigating this challenge involves proactive engagement with regulatory bodies, participation in standardization forums, and the development of a robust governance framework that can quickly adapt to regulatory changes. Addressing these challenges requires a holistic and multidisciplinary approach. Collaboration between different sectors of government, industry, and academia will be essential to overcome these obstacles and ensure a successful transition to a secure digital signature environment in the post-quantum era.

6. Conclusion

The transition to post-quantum cryptography is not merely a technical necessity but a strategic imperative to ensure the security and integrity of digital communications in the quantum era. Throughout this study, it has become clear that the threat posed by quantum computers to current cryptography is real and imminent, necessitating immediate action and careful planning. The analysis of the current scenario revealed that, although Brazil has made significant progress in the digitization of government services, including the implementation of digital signatures through the GOV.BR platform, there is still a long way to go to ensure the security of these operations against quantum threats. The proposed transition strategy in this study emphasizes the importance of a phased approach, starting with a comprehensive assessment and inventory of existing cryptographic systems. Careful planning, the meticulous selection of post-quantum cryptography (PQC) algorithms, the gradual update of infrastructure and software, and a strong focus on training and awareness are important elements for the success of this transition.

The identified challenges, including technical complexity, interoperability issues, scarcity of expertise, significant costs, and regulatory uncertainties, are substantial. However, the proposed mitigation strategies, such as the implementation of hybrid solutions, investments in research and development, public-private partnerships, and the adoption of a crypto-agility approach, offer viable paths to overcome these obstacles. Looking ahead, it is clear that the success of this transition will depend on close collaboration between various sectors of government, industry, and academia. The sharing of knowledge, resources, and best practices will be crucial in developing robust solutions that are adaptable to Brazil's specific needs.

Finally, it is important to emphasize that while the challenges are significant, the risks of inaction are even greater. The successful implementation of post-quantum cryptography will not only protect government data and communications against future threats but also position Brazil as a leader in digital security in Latin America and beyond. The journey to a secure digital future in the quantum era is just beginning. With careful planning, sustainable investment, and a commitment to continuous innovation, the Brazilian Federal Government can not only face the challenge of quantum computing but emerge stronger and more secure, ready for the opportunities and challenges of the digital world.

References

Abbes, M., Julien, A., Hao, S., and Touzani, M. (2024). Adopting digital signatures for complex financial products in the french banking sector: How technology acceptance and user literacy matter. *IEEE Trans. Engineering Management*, 71:5536–5546.

Acar, A., Kayaalp, K., Çetin, G., and Turan, M. S. (2023). A survey of post-quantum cryptographic hardware: Challenges, solutions, and future directions. *ACM Computing Surveys*, 55(8):1–35.

Alagheband, M. R. and Mashatan, A. (2022). Advanced digital signatures for preserving privacy and trust management in hierarchical heterogeneous iot: Taxonomy, capabilities, and objectives. *Internet Things*, 18:100492.

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y., Miller, C., Moody, D., Peralta, R., et al. (2022). Status report on the third round of the nist

post-quantum cryptography standardization process. *NIST Interagency/Internal Report (NISTIR)*, 8413:1–60.

Bernstein, D. J., Buchmann, J., and Dahmen, E. (2017). *Post-quantum cryptography*. Springer, Berlin, Heidelberg.

Bodson, D. (2013). IEEE standards association and the european telecommunications standards institute renew memorandum of understanding [standards]. *IEEE Veh. Technol. Mag.*, 8(1):101–103.

Campos, B. A. R. and Rosa, E. (2023). A evolução da computação quântica: impacto na criptografia rsa e a segurança nacional.

Chen, J., Hsu, J., Ahmadi, C., Atmaja, B. T., Lin, C., Wang, S., and Lin, S. (2023). Development of security target for router based on ENISA common criteria framework. In *25th International Conference on Advanced Communication Technology, ICACT 2023, Pyeongchang, Korea, Republic of, February 19-22, 2023*, pages 117–121. IEEE.

da República, Presidência, N. C. (2018). Brazilian general data protection law (lgpd). *Nartional Congress, accessed in April 10, 2022*, 1(1):1–31.

Dwork, C. and Roth, A. (2014). Algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 9(3-4):211–407.

Fenasbac (2025). Com apoio da fenasbac, banco central, brazil quantum e microsoft exploram o uso de criptografia pós-quântica para melhorar segurança do sistema pix. `https://www.fenasbac.com.br/noticias/com-apoio-da-fenasbac-banco-central-brazil-quantum-e-microsoft-explor`

Ferreira, R., Ripper, P., Veríssimo, R., and Neto, A. A. C. (2023). Análise da viabilidade de aplicação de métodos de criptografia pós-quântica aplicados ao sistema de pagamentos instantâneos brasileiro (pix). Technical report, Banco Central do Brasil (BCB).

Guerra, H. and Tavolaro, C. R. C. (2021). Criptografia pós-quântica: protocolo dente de leão. *Scientia Prima*, 7:e111.

Gyongyosi, L., Imre, S., and Nguyen, H. V. (2019). A survey on quantum channel capacities. *IEEE Communications Surveys I& Tutorials*, 20(2):1149–1205.

Hussain, S., Chang, E., and Dillon, T. (2018). Digital certificate management: A survey. *Journal of Network and Computer Applications*, 104:69–85.

ITI (2023). Infraestrutura de chaves públicas brasileira - icp-brasil.

ITI (2025). Assinatura eletrônica avançada. Technical report, Instituto Nacional de Tecnologiada Inofrmação (ITI). `https://www.gov.br/iti/pt-br/assuntos/assinatura-eletronica-avancada`.

Mibnistério da Economia (2021). Portaria sedggme nº 2.154, de 23 de fevereiro de 2021. `https://www.in.gov.br/web/dou/-/portaria-sedggme-n-2.154-de-23-de-fevereiro-de-2021-304916270`.

Misoczki, R. and Barreto, P. S. L. M. (2008). Criptografia pós-quântica. *Instituto de Matemática e Estatística, Universidade de São Paulo*.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: will we be ready? *Journal of Physics: Conference Series*, 1065(10):102007.

NIST (2022). Nist announces first four quantum-resistant cryptographic algorithms.

NIST (2024a). Nist ir 8547 - transition to post-quantum cryptography standards (initial public draft).

NIST (2024b). Post-quantum cryptography pqc - selected algorithms.

NIST (2025). Post-quantum cryptography pqc - overview.

Parliament, E. and European Union, C. o. (2016). General Data Protection Regulation (GDPR). `https://gdpr-info.eu/`,Last access on 10 April 2022.

Peikert, C. (2016). Lattice cryptography for the internet. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 3–15.

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., et al. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012–1236.

Presidência da República do Brasil (2016). Decreto nº 8.936, de 19 de dezembro de 2016. `https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8936.htm`.

Presidência da República do Brasil (2020a). Decreto nº 10.543, de 13 de novembro de 2020. `https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10543.htm`.

Presidência da República do Brasil (2020b). Lei nº 14.063, de 23 de setembro de 2020. `https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm#view`.

Sedghighadikolaei, K. and Yavuz, A. A. (2023). A comprehensive survey of threshold digital signatures: NIST standards, post-quantum cryptography, exotic techniques, and real-world applications. *CoRR*, abs/2311.05514.

Seo, J. H. (2020). Efficient digital signatures from RSA without random oracles. *Inf. Sci.*, 512:471–480.

SGD (2025). Assinatura eletrônica gov.br: Integração para órgãos e entes públicos. Technical report, Secretaria de Governo Digital (SGD) / Ministério da Gestão e da Inovação em Serviços Públicos (MGI). `https://www.gov.br/governodigital/pt-br/identidade/assinatura-eletronica/assinatura-eletronica-para-orgaos`.

Shaikh, A. A., k. Garg, Bhatia, M., Kumar, N., and You, I. (2019). Secure and efficient certificateless signature scheme for cloud computing. *Journal of Ambient Intelligence and Humanized Computing*, 10(6):2409–2422.

Xu, J., Ren, Z., Chen, Y., Zhang, C., and Wang, Q. (2022). Optimal resource allocation of quantum digital signatures with machine learning. *Quantum Inf. Process.*, 21(9):338.