Security, Privacy and Interoperability Requirements for Peruvian Remote Digital Signatures

Erik Alex PAPA QUIROZ
Departamento de Ciencias, Universidad Privada del Norte
Facultad de Ciencias Matemáticas, Universidad Nacional Mayor de San Marcos
Lima, Perú

Ever CRUZADO QUISPE
Estudios Generales, Universidad Nacional Mayor de San Marcos
Facultad de Ciencias Naturales y Matemática, Universidad Nacional del Callao
Lima, Perú

Rosalia QUIROZ PAPA DE GARCIA
Facultad de Letras y Ciencias Humanas, Universidad Nacional Mayor de San Marcos
Lima, Perú

ABSTRACT

There are several technological solutions currently available in the market that allow customers/citizens to digitally sign electronic documents through their smartphones. Regardless of how user-friendly they are, most of these platforms use proprietary schemes designed for particular use cases, which could not necessarily be applied to open, interoperable scenarios and where there could be legal consequences. To establish a general framework that may provide manufacturers with minimum safety, reliability, and legal requirements, several international organizations have proposed standards for both manufacturers and potential users. Within this context, this paper presents, for the first time in Peru, a list of security, privacy, and interoperability requirements for remote digital signature for the Peruvian state. This research was based on features of the current state of the art, the existing international standards and the current state of the technology. The relevance and viability of these requirements were validated by RENIEC (Spanish acronym of National Registry of Identification and Civil Status) specialist personnel through an inter institutional cooperation agreement between RENIEC and PNICP (Spanish acronym of National Program of Innovation for the Competitivity and Productivity).

Keywords: Remote Signature, Security Requirements, Privacy Requirements, Interoperability, Digital Signature in Peru.

1. INTRODUCTION

Currently, both companies and government entities, strongly motivated from the COVID-19 pandemic, are implementing zero-paper projects, which replace printed documents with electronic documents to facilitate and improve the services provided to their customers/citizens. This process would be easy if there was no possibility to subsequently demonstrate that the agreement or transaction was indeed executed, or that one of the signatories refuses to acknowledge performing said deed. Likewise, while electronic documents are easy to produce, they are also easy to modify, unlike printed documents. In addition, electronic documents may be easily duplicated, which hinders the easy recognition of their original versions.

Therefore, organizations have been adopting the use of Public Key Infrastructure (PKI)-based digital signatures to provide three new characteristics to electronic documents: authenticity, integrity, and non-repudiated. Thus, users can easily identify whether an electronic document is authentic and whether it has been modified or tampered. In addition, none of the signatories would be able to deny executing the document.

However, PKI-based digital signatures require customers/citizens to use a cryptographic device (token or smartcard) as these devices can guarantee the security and reliability required for the creation of legally effective and valid digital signatures. Furthermore, customers/citizens are required to use a desktop computer (PC), which is now an outdated scenario. In this sense, this paper proposes a solution for the peruvian context. That is, we propose a list of security, privacity and interoperability requirements for peruvian remote digital signature. These requirements, have been obtained according to current state of the art, the existing international RFC 3647 (Request for Comments 3647) standards, [1], and the current state of technology.

The content of this paper is as follows. Section 2 presents the basic aspects of digital signature, remote digital signature and some legal aspects of the digital signature in Peru. Section 3 presents the research activities. Section 4 introduces the requirements for peruvian remote digital signature. Section 5 presents the validation of the proposal. Section 6 shows the conclusions and Section 7 presents the acknowledgment. Finally, in Section 8, we give the references.

2. BASIC ASPECTS

Digital Signature

According to [2], Section 3.1, a typical digital signature scheme[1] comprises three algorithms:

[1] There are various digital signature schemes. For example: RSA, ElGamal, DSA and ECDSA. The last two are based on discrete logarithms defined by NIST standards.

- **Key Generation Algorithm:** It uniformly selects a random private key from a set of possible private keys. The output is a private key and a public key.
- **Signature Creation Algorithm:** Given a message and a private key, it generates a digital signature for the message.
- **Signature Verification Algorithm:** Given a message, a public key, and a digital signature, it accepts or rejects the message based on its authenticity and integrity.

Remote Digital Signature

Remote signatures are generated using a private key stored with private keys used by other users in an HSM (Hardware Security Modules) cryptographic device remotely managed by a third party. Remote signatures must be distinguished from local signatures, which use private keys locally stored in cryptographic devices, such as tokens or smartcards, managed by signatories themselves. In this paper we consider the following scenario schematized in Figure 1.

Step 1 and step 2: The signer accesses a service offered by a provider and receives a document on his personal device.
Step 3: The device creates a remote signature request.
Step 4: The device sends a signature generation request to the signature service and for the signature service to select the correct private key, the request is authenticated.
Step 5: The digital signature is calculated in the cryptographic module and the AdES (Advanced Electronic Signature) signature is assembled by the service itself.
Step 6: The response is sent to the client.
Step 7: The response is sent optionally to the supplier.

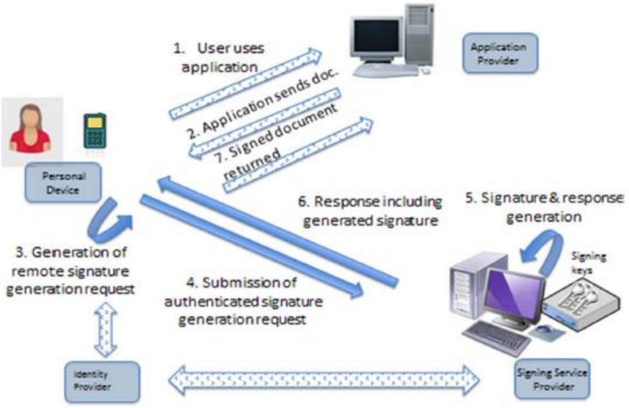
1. User uses application
Application Provider
2. Application sends doc.
7. Signed document returned
Personal Device
6. Response including generated signature
5. Signature & response generation
Signing keys
3. Generation of remote signature generation request
4. Submission of authenticated signature generation request
Identity Provider
Signing Service Provider

Figure 1 - Scenario of remote signatures

The Digital Signature in Peru

Regarding digital signature regulations currently operational in Peru, Regulations[2] of Law No. 27269[3], established in its Article 8 Item a), among the assumptions for "documents signed digitally using digital certificates generated within the IOFE (Official Electronic Signature Infrastructure), that the subscriber of the digital certificate holds exclusive control of the corresponding private key". Likewise, in its Article 9, subscribers are defined as "… the physical persons responsible for the generation and use of private keys, with the exception of digital certificates for use through automated agents…"

Among the subscriber obligations, Article 10, Item b) of the Regulations provisions that "Subscribers are hereby required to generate private keys for signing documents digitally strictly through the procedures specified by the Certification Entity." Also, Item c) reads that "Private Keys must be strictly controlled, managed and safeguarded by the corresponding Subscriber." In addition, private key responsibilities extend to the certificate holder, who, in case if it's a company, shall be the organization that processes certificates to be used by its staff members, as verified in Article 15, Item c), where we find among the corresponding obligations that "Subscribers shall request the cancellation of their digital certificate if the confidentiality of the private key under their responsibility has been compromised." It should be added that this legal liability is both administrative and functional.

Regarding the legal nature of the signatures generated under a remote signature scheme, it should be noted that in Section 41.4 of the Regulations, the "Security principles used in the implementation and use of electronic means for the provision of Electronic Government Services, according to which the government shall require Public Entities to observe the security standards and accreditation requirements necessary to provide technological support and sufficient legal presumption to the operations performed by electronic means, as established for said purposes by a competent administrative authority."

From what has been analyzed, it can be affirmed that, while the framework for remote digital signature generation solutions is not developed at the regulatory level, of Accreditation Guides (with the corresponding recognition of standards, specifications, specific protection profiles for their certification, etc.), policies and practices, its use in Peru, by not necessarily providing the guarantees of the case, would be taking place outside the accrediting framework of the IOFE, so it would not have the legal prerogatives and legal validity and effectiveness that this framework confers on the digital signature.

3. RESEARCH ACTIVITIES

This scientific research was developed thanks to the Service Order 001272 funded by PNICP (National Program of Innovation for the Competitivity and Productivity) of the Peruvian state. The results have been reviewed and evidenced by the specialists of the Management of Digital Register of RENIEC (National Registry of Identification and Civil Status).

The activities carried out to obtain the results of this paper are given in Figure 2.

[2] Regulation of the Law on Digital Signatures and Certificates approved by Executive Order No. 052-2008-PCM (18JUL2008, https://www.gob.pe/institucion/pcm/normas-legales/292462-052-2008-pcm), which regulates the use of Digital Signatures for the public and private sectors, granting Digital Signatures generated within the Official Electronic Signature Infrastructure (IOFE) the same legal validity and effect of a handwritten signature.

[3] Law No. 27269 - Law on Digital Signatures and Certificates, which regulates the use of electronic signatures and digital certificates in Peru and establishes Digital Certification Service Providers.

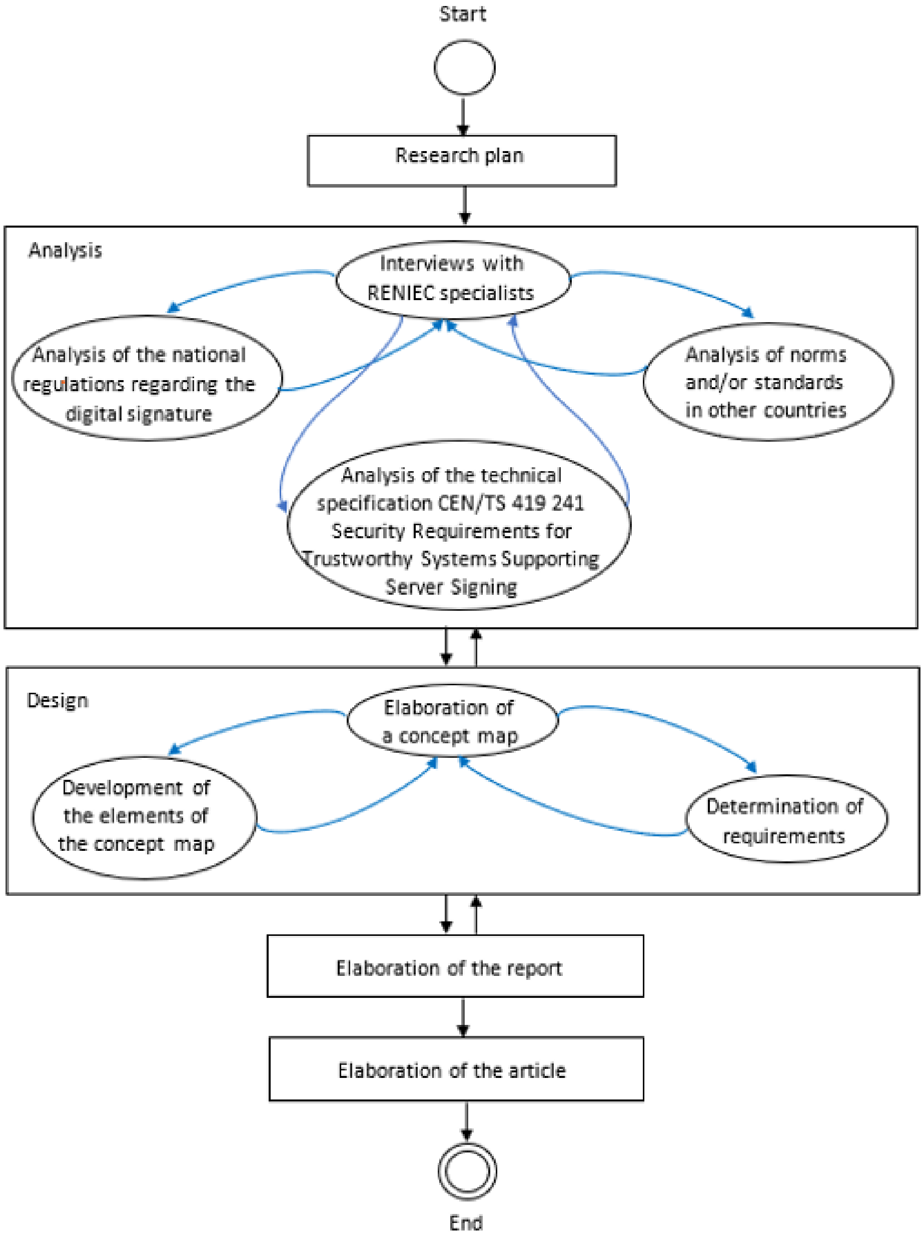
Start
Research plan
Analysis
Interviews with RENIEC specialists
Analysis of the national regulations regarding the digital signature
Analysis of norms and/or standards in other countries
Analysis of the technical specification CEN/TS 419 241 Security Requirements for Trustworthy Systems Supporting Server Signing
Design
Elaboration of a concept map
Development of the elements of the concept map
Determination of requirements
Elaboration of the report
Elaboration of the article
End

Figure 2- Research activities

4. REQUIREMENTS

In this section, we describe the proposed security, privacy, and interoperability requirements applicable to remote digital signature systems organized according the structure RFC 3647, [1]. The model, given in Figure 3, was motivated from the lecture of the CEN/TS 419 241 [3], the CWA 14170 [4] and INDECOPI (Spanish acronym of National Institute for the Defense of Competition and the Protection of Intellectual property) requirements [5-8].

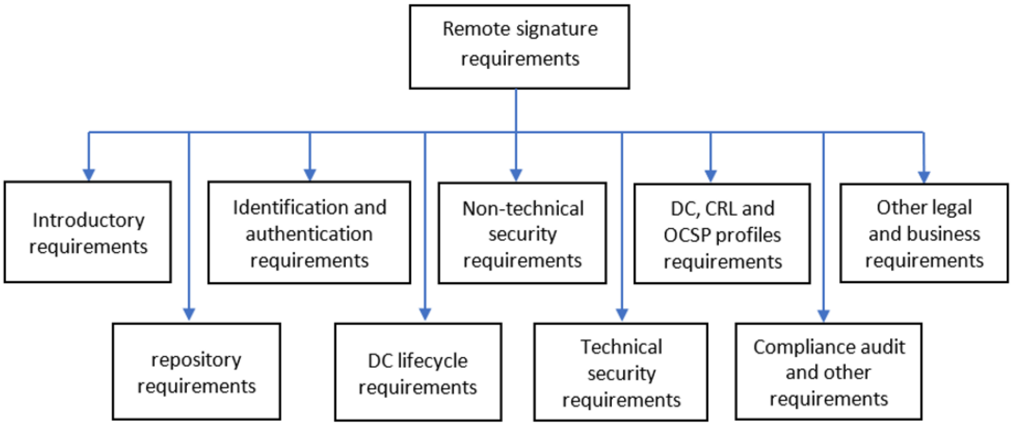
Remote signature requirements
Introductory requirements
Identification and authentication requirements
Non-technical security requirements
DC, CRL and OCSP profiles requirements
Other legal and business requirements
repository requirements
DC lifecycle requirements
Technical security requirements
Compliance audit and other requirements

Figure 3 – Requirements to remote digital signature

Introductory Requirements
These requirements provide an overview of the system, the participants, and the terminology used in the rest of the provisions.

- REQ-INT-001: A general system description must be provided, including two different environments: a local environment and a remote environment.
  - The system must operate under renowned best practices and must include controls and procedures outlined in the Remote Signature Practice Statement (RSPS).
  - The SCDev (Signature Creation Device), comprising the signature activation module and the cryptographic module, must comply with *EN 419 241-2 QSCD for server signing* specifications. In particular, the cryptographic module must comply with the *EN 419 221-5 Crypto Module for TSP* specifications.
  - The SAP (Signature Activation Protocol) and the SAD (Signature Activation Data) must also comply with *EN 419 241-3 SAD+SAP* specifications.
- REQ-INT-002: An object identifier must be specified for the document (OID-Object Identifier).
- REQ-INT-003: Entities engaged or those that interact with the RSSP (Remote Signature Service Provider) must be identified and described: CE (Certification Entity), RE (Registration Entity), subscribers, trusted third parties, and others.
- REQ-INT-004: Scenarios must be established to determine where the use of the digital certificates issued by the Remote Signature Service Provided may be allowed or forbidden.
- REQ-INT-005: The name and email address of the organization responsible for managing this document must be explicitly defined.
- REQ-INT-006: A list of definitions for terms used in the document must be provided as well as the meaning of all abbreviations and acronyms used.

Repository Requirements
These requirements contain provisions regarding the identity of the organization that manages the repository or repositories, its responsibilities and obligations, update frequencies, and the corresponding protection control statements.

- REQ-RRP-001: The identity of the organizations that operate the RSSP repositories must be described.
- REQ-RRP-002: The RSSP must publish a RSCP (Receive Signal Code Power) and establish its corresponding publication mechanisms. Existing documents which are not publicly available must also be identified.
- REQ-RRP-003: The RSSP must also determine when the RSCP will be published and its update/review frequency.
- REQ-RRP-004: The RSSP must also determine the logical access controls for the published information.

Identification and Authentication Requirements
These requirements provision the procedures used to authenticate the identity of digital certificate applicants, as well as the subscribers who use remote signature services

- REQ-I&A-001: The corresponding CE must establish the naming convention (X500 DN, RFC-822, X.400) for the different digital certificates issued to subscribers. However, the RSSP must clearly state which alternatives offered by the CE have been adopted.
- REQ-I&A-002: First-time subscriber ID validation and authentication.
- REQ-I&A-003: Identification and authentication for reissuance requests with key renewals.
- REQ-I&A-004: Identification and authentication for cancellation requests. For the last three requirements, the procedures for subscriber identification and authentication are established by the registration entity.
- REQ-I&A-005: The signatory must be authenticated against the SSA, and any possible authentication errors must be effectively managed.
- REQ-I&A-006: System administrators must be properly identified and authenticated before they may perform any action.

Digital Certificate Lifecycle Requirements
These requirements provide the procedures used to perform the operations related to the digital certificate lifecycle.

- REQ-CVC-001: Digital certificate requests
- REQ-CVC-002: Certificate processing requests
- REQ-CVC-003: Certificate issuance
- REQ-CVC-004: Certificate acceptance

- REQ-CVC-005: Using key and digital certificate pairs
- REQ-CVC-006: Certificate renewals without key generation or data modifications
- REQ-CVC-007: Digital certificate reissuance with key renewals
- REQ-CVC-008: Certificate modifications without key generations
- REQ-CVC-009: Digital certificate cancellations and suspensions
- REQ-CVC-010: Certificate status monitoring services
- REQ-CVC-011: Service subscription terminations
- REQ-CVC-012: Key custodies and recovery

Non-Technical Security Requirements
These requirements describe the non-technical security controls (i.e., physical or human resource controls) used to provide services.

- REQ-CNT-001: Physical controls
- REQ-CNT-002: Procedural controls
- REQ-CNT-003: Staff controls
- REQ-CNT-004: Audit log procedures
- REQ-CNT-005: File requirements. The RSSP must clearly specify the types of records archived, their retention periods, security and protection procedures, and backup procedures.
- REQ-CNT-006: Disaster and compromised operations recovery.
- REQ-CNT-007: Service terminations. The RSSP must describe all service termination procedures.

Technical Security Requirements
These requirements describe the security measures that must be implemented to protect the private keys issued to the subscribers as well as the corresponding activation data.

- REQ-CTS-001: Key pair generation. The private keys issued to subscribers must be generated by the RSSP through a SCDev.
- REQ-CTS-002: Private key protection and engineering controls for the cryptographic module
- REQ-CTS-003: The public keys issued to subscribers must be stored for a period of or greater than 10 years.
- REQ-CTS-004: Activation data. Activation data can be represented by one or more authentication factors.
- REQ-CTS-005: Computer security controls
- REQ-CTS-006: Technical lifecycle controls
- REQ-CTS-007: Network security controls. The network security controls applied to the remote signature system (including firewalls) must be described.
- REQ-CTS-008: Date and time. The RSSP must clearly define the accuracy levels for the system date and time.
- REQ-CTS-009: Only the algorithms and parameters of the algorithms defined by the ETSI/TS 102 176 series [SRC_SC.1.1] must be used for signature generation.

DC (Digital Certificate), CRL (Certification Revocation List) and OCSP (Online Certificate Status Protocol) Profiles Requirements

- REQ-CCO-001: Digital certificate profile
- REQ-CCO-002: CRL profile
- REQ-CCO-003: OCSP profile.

The three previous requirements are not applicable to RSSPs. These profiles are established by certification entities.

Compliance Audit and Other Assessment Requirements
These requirements describe audit types and frequency, auditor identifications, and the action items that must be performed as a result from audits.

- REQ-AUD-001: A list of topics, aspects covered by the assessment, and/or the assessment methodology used for the audits must be clearly defined.
- REQ-AUD-002: Audit periodicity and/or the circumstances that may generate a repeated assessment.
- REQ-AUD-003: auditor identities and qualifications
- REQ-AUD-004: independence between the auditor and the audited entity
- REQ-AUD-005: actions to be taken against shortcomings identified during the audit process
- REQ-AUD-006: who receives audit assessment results and how they are communicated.

Other Legal and Business Requirements
These requirements address aspects such as rates, financial liabilities, confidentiality, privacy, intellectual property, guarantees, indemnities, standards, and applicable laws.

- REQ-OTR-001: The RSSP must clearly define the payment mechanism and service procedures.
- REQ-OTR-002: financial liabilities
- REQ-OTR-003: business information confidentiality
- REQ-OTR-004: personal information privacy
- REQ-OTR-005: intellectual property rights, such as copyrights, patents, trademarks, or trade secrets
- REQ-OTR-006: The RSSP must include warranty and liability clauses, including limitations and exemptions.
- REQ-OTR-007: The RSSP must include any exemption from liability.
- REQ-OTR-008: The RSSP must also clearly specify any applicable limitation of liability.
- REQ-OTR-009: The RSSP must clearly provision any applicable indemnities.
- REQ-OTR-010: The RSSP must clearly specify the effective and expiration dates for the document.
- REQ-OTR-011: The notification and communication mechanisms used for all stakeholders must also be established.
- REQ-OTR-012: The RSSP must specify the procedure using which the document can be amended.
- REQ-OTR-013: The RSSP must also state the procedures used to resolve service provision disputes.
- REQ-OTR-014: The RSSP must establish the applicable legal framework under which the service is provided.
- REQ-OTR-015: The RSSP must provision strict compliance with applicable laws and regulations from participants.
- REQ-OTR-016: The RSSP must include the following clauses: full agreement, subrogation, divisibility, execution, and force majeure.
- REQ-OTR-017: The RSSP may also include additional clauses and terms that were not provisioned in other sections.

5. VALIDATION

The requirements presented in the previous section have been evaluated iteratively by the specialists of the Management of Digital Certification Register of RENIEC. In each iteration, incremental versions of the requirements were presented. Suggestions for improvements were received and incorporated in subsequent versions until reaching a stable version.

6. CONCLUSIONS

In recent years, a series of technological solutions have been appearing on the market (known as remote signature creation platforms) that allow a client or citizen to digitally sign electronic documents without the need to have a token or smartcard in their hands. However, the multiple advantages offered by these platforms, it is not possible to know their degree of maturity and security because they lack specific certifications and / or accreditations that would enable them to be deployed in open scenarios.

In order to establish a general framework that allows manufacturers of remote signature creation platforms to have a minimum threshold of requirements, is that some international organizations are proposing a series of standards that must be considered by both manufacturers and by potential users. For example, in 2014, the European Committee for Standardization published the technical specification: CEN / TS 419 241 Security Requirements for Trustworthy systems supporting server signing. In the Latin American sphere, some countries are also modifying their regulations to adopt the use of technology based on remote digital signatures: Argentina (Decree 892/2017 of 11/01/2017) and Brazil (Resolution 132 of 11/10/2017).

The modification of the regulatory framework of the IOFE should contemplate the inclusion of a new modality of Provider of Added Value Services (PSVA) that could be called: Remote Signature Service Provider. To become part of the IOFE, as well as an EC, ECEP, ER, EREP, etc., this new PSVA should be accredited to the AAC, also developing a Declaration of Remote Signature Practices (RSPS). In order not to contravene the provisions of the Regulations of the Law and the EC Accreditation Guides, regarding the exclusive control of the private key of the signatory, a scheme equal to or equivalent to the exclusive control of level 2 described in the CEN / TS 419 241 Security Requirements for Trustworthy systems supporting server signing specification.

RSPS to be developed by the RSSP must follow a policy framework aligned to some additional standards or recommendations.

The Peruvian IOFE is an open certifying PKI infrastructure overseen by INDECOPI in its role as the competent administrative authority. The IOFE recognizes and assumes that certain electronic signatures are legally equivalent to a handwritten signature. However, neither the law on digital signatures and certificates nor its regulations or the accreditation guides for digital certification service providers contain provisions related to remote digital signatures. Therefore, Peru requires a regulatory framework that may regulate the use of remote digital signatures. This regulatory framework would allow digital signatures generated with remote signature platforms to acquire the same legal value as handwritten signatures. In addition, it would allow users to fully leverage the strengths of digital signatures such as mobility and usability.

A specific justification of each requirement presented in this work exceeds the length of this paper and we hope to publish it soon in another article.

The theoretical validation of the requirements, based on good practices, experience of specialists, international standards and the current state of technology has been evaluated by the specialists of the Management of Digital Certification Register of RENIEC. A practical implementation and its respective validation may be considered as a future research.

7. ACKNOWLEDGMENT

This study could not have been developed without the valuable participation and contributions of RENIEC specialists Alvaro Cuno, Alfredo Gallo, Ronald Martinez and Ricardo Saavedra.

8. REFERENCES

[1] RFC 3647, https://tools.ietf.org/html/rfc3647

[2] Pass R. and A. Shelat, A course in Cryptography, 2015

[3] European Committee for standardization. CEN/TS 419 241 Security Requirements for Trustworthy systems supporting server signing. March 2014.

[4] European Committee for standardization. CWA 14170:2004 Security requirements for signature creation applications. May 2014.

[5] INDECOPI. Certification entities accreditation guide (in Spanish), Version 3.3. March 2008.

[6] INDECOPI. Register entities accreditation guide (in Spanish), Version 3.3. March 2008.

[7] INDECOPI. Value Added Service provider accreditation guide, Version 3.3. March 2008.

[8] INDECOPI. Software applications accreditation guide, Version 3.4. March 2008.