Digital signature guidelines

This guideline aims to provide some guidance in the proper user and application of the electronic signature in line with the laws of the Government of Rwanda.

- Some definitions
- Classifications of Electronic Signature
- Use and application of the electronic signature
- Digital signature application guidelines
- Management of the digitally signed documents
- Methods used to apply the digital signatures
- Storage and archiving of the digitally signed documents
- Some useful contact and user guides

Some definitions

Electronic Signature (e-signature): is an electronic sound, symbol or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record.

Classifications of Electronic Signature

1. **Simple e-signatures:** provide little or no authentication at minimal or no cost.
2. **Advanced e-signatures:** are linked to specific signers but can still be vulnerable to fraud.
3. **Qualified e-signatures:** include third-party authentication and offer strong security making them legally binding.

> Digital signature (Qualified e-signatures): an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem.

Use and application of the electronic signature

In line with the ICT law (*Article 146:*), electronic signature is legally accepted if:

1. the method used indicates the originator of the record and that the originator approves the information contained in the record.
2. that method is reliable for the purpose for which the electronic record was generated or communicated, in the light of agreement.

According to the above description, the legally accepted electronic signatures are the Qualified Electronic Signatures i.e., the Digital signatures provided by service providers accredited by the Regulatory Authorities. The qualified electronic signature (Digital signature) fulfils the requirement to be related to the electronic signature admission.

Digital signature application guidelines

1. We strongly encourage people to use the individual digital certificate (with their names) instead of using the digital signature with the name of institution and their position.
2. The image in the digital signature has not much consideration
3. It is not advisable to put the image of the stamp in the digital signature, in place of this we strongly recommend preparing a template that contains the stamp image or with the institutions' heading, then have it signed after all the information are filled with the document reference number and date.
4. Only the high-level authorities within the institutions are allowed to get the digital signature with the name of the institution and their positions.
5. The server certificate will contain the name of the institution, the name of the system and the e-mail of that institution.

Management of the digitally signed documents

1. A digitally signed document remains original as long as it is kept into the digital format. (It can be renamed, but it cannot be converted into another form such as zipping it as it may invalidate the signature)
2. A printed digitally signed document is considered as a copy and cannot be trusted.
3. The digital signature can be either visible or invisible. For the convenience of the signature validation, we strongly recommend using visible digital signature.
4. Any manipulation of the print of a digitally signed document, does not revive the trust of the initial digital signature that were applied to it before the printout.

Methods used to apply the digital signatures

1. **Signing through the integrated systems**: This is the highly recommended method, as it is easy to use and does not require any configuration by the end user. A copy of the signed documents is mostly kept in the system making it easier for document archiving. It is highly recommended to use the newly updated smart admin system for all the exchanged documents and information within and out of the institutions.
2. **Signing using Acrobat PDF reader digital singing tools using digital certificate**. This method is not recommended is it requires the user to go through some setups and no reliable timestamp applied.

Storage and archiving of the digitally signed documents

The digitally signed documents are stored and archived in the original formatting. Binary or bit to bit storage is also possible.

Some useful contact and user guides

Contacts:

RISA PKI Division
E-mail: pki@risa.gov.rw
Phone: +250788 390 212
Toll Free: 4046

Website: www.govca.rw

User guide:

https://www.govca.rw/guide/issuance.sg

Laws and regulations:

https://www.govca.rw/terms/lawsAndRegulations.sg