



Digital Administration

The Digital Administration Code (DAC)

- Understanding e-government concepts, electronic administration, documental dematerialization, electronic document. The Digital Administration Code (DAC)
- Being aware that Digital Administration will radically change work tools and how to work in a context of administrative processes completely redesigned, economic benefits
- Recognizing PA's obligations and citizens and businesses' digital rights. PA's electronic cards and web sites
- Recognizing the range of the digital revolution that involves: digital signature, certified electronic mail, electronic protocol, e-invoicing, substitute maintenance.

Definitions, purpose and sphere of the DAC

- Understanding the role of certifier. The electronic certificate, the qualified certificate.
- Understanding the concept of computer authentication; computer document; computer management of the document. The legal value of information document.

The digital signature

Subjects and objects of the digital signature

- Understanding the importance of cryptography; symmetric and asymmetric cryptographic keys, the pair of public and private keys.
- Understanding characteristics and usefulness of the Hash function and fingerprint. Non-repudiation
- Recognizing the different signature devices: smart card, USB token, Secure Signature Creation Device (SSCD)
- Recognizing the different types of signatures and their legal effect: electronic signature, advanced, qualified, digital; strong and weak, light and heavy; signatures 5.1 and 5.2
- Recognizing the functions of the National Center for Informatics in Public Administration (NCIPA), of the qualified Certifiers and accredited Certifiers. Certifier's civil liability

Legal aspects

- Recognizing the inappropriate use of digital signature; the digital equivalent signature to an autographic signature and the authentication process. Signatory power on an information document and the use of digital signatures in PA.
- Understanding the different characteristics of various electronic signatures in legal proceedings: the probative value of the digital signature and the probatory value of weak signatures
- Understanding the legal validity of digital signature: equal to handwritten signature, correspondence to the legal requirement of writing, the disavowal of digital signature
- Understanding the characteristics of temporal validity of digital signature. The service of temporal mark and equivalent methods to obtain a temporal mark that can be opposed against third parties
- Recognizing the vulnerability of the digital signature: the safety of the process of signing, WYSIWYS, documents containing macros and executable code

Technological aspects

- Recognizing and using the various formats of digital signature: PKCS # 7 (p7m), PDF, XML.
- Being able to have a digital signature. The list of certifiers. Certifiers for special groups. Recognition de visu. Request of a considerable number of kits for digital signatures
- Being able to choose the appropriate digital signature kit to one's needs and being able to use it by configuring the included software or any other suitable. The expiration and renewal of certificates. The importance of operational manual of each Certifier.

Working with digital signatures

- Recognizing the individual steps to work with digital signature.
- Being able to place and verify the signature of a document in PKCS # 7 (p7m)
- Being able to apply the procedure for a complete verification of digital signature affixed to an information document, either manually or automatically. The verification validity of certificates, expired, suspended and depending on content of document
- Being able to affix signatures and carry out checks using PDF
- Being able to affix a temporal mark to an information document that contains a set of fingerprints

Certified E-Mail

Characteristics of Certified E-Mail

- Understanding that Certified E-Mail is an e-mail system usable in cases where it is necessary a proof that can be opposed against third parties of mailing and delivery of an electronic document.
- Recognizing the main objectives of the Certified E-Mail: to generate enormous savings and facilitate transactions between individuals and among them and the PA. The exchange among applications
- Recognizing the extreme reliability of the Certified E-Mail as it relies on minimum levels of service guaranteed by the standard, on the operational manual concerning services and on additional services made available by the selected operator
- Understanding the roles of actors in the Certified E-Mail: sender, recipient, operators, network communication, subject of transmission. Receipts, notices and envelopes
- Understanding that the Certified E-Mail is a transport service and does not go deeply into a matter of what is being transferred from sender to recipient. Appropriate use of the Certified E-Mail
- Understanding that the Certified E-Mail system facilitates archiving and searching messages and receipts. Even in case of accidental deletion or loss of receipts, you can consult the log file manager
- Recognizing the strengths of the Certified E-Mail: transmission of any digital content; simplicity and low cost of transmission, forwarding, copying, filing and research, multiple sending; speed of delivery, access from any location, high standards of quality and continuity of service
- Understanding that the legal value of the message of Certified E-Mail is preserved only in the case of transmission among Certified E-Mail boxes .
- Understanding that for the PA, using the Certified E-Mail is both an opportunity and an obligation
- Understanding the limits of the Certified E-Mail. Alternatives to the Certified E-Mail, S / MIME certificates.

Working with the Certified E-Mail

- Recognizing that the Certified E-Mail can be simply used, without having to install special software and having to change operative habits of those who adopt it: you can send and receive registered electronic letters any day, time and place and from any device connected to the computer network.
- Understanding that the sender and the recipient must have a PC (or other suitable device) and connection to one's Certified E-Mail operator
- Learning all the operational steps for sending a Certified E-Mail message and being able to perform virtually
- Recognizing situations and notices of deficiency, such as: viruses in messages, formal controls that have not been overcome, reception of a message from a not certified mailbox.