ABSTRACT

Electronic documents with legal value can be used due to legislation that equates qualified electronic signatures with handwritten signatures. With the entry into force of the eIDAS Regulation, users can apply qualified electronic signatures without physically owning a cryptographic device. In such a system, the user's private keys are generated, stored and used in the cloud. This change entails certain challenges, the most important of which is: ensuring exclusive control of the user over private keys stored in the cloud and ensuring the interoperability of signature applications with signing services exposed by certification service providers. The main advantage of electronic signatures in the cloud is increased mobility and usability.

In the context in which more and more companies and states are following digitization processes, the development of the field to obtain more secure and easy-to-use electronic signature systems is gaining significant importance. Thus, a general objective of this thesis is to identify elements that can be improved, so that electronic signatures in the cloud are more secure and easier to use. More specifically, the objectives of the thesis revolve around the new electronic signature infrastructures, addressing three important issues: security, usability, and how to use electronic signatures in the cloud.

From a usability perspective, cloud electronic signature systems have considerable potential, but it is not yet fully realized. The transition from local signature applications to cloud signatures can be difficult for two reasons: the user experience is altered, and applications need to change the implementation by which signatures are processed. In order to harmonize the standards of local electronic signature with those for electronic signature in the cloud, two software cryptographic modules are proposed in the thesis. They allow signature applications compatible with PKCS\#11 or CNG to make electronic signatures in the cloud in a transparent way, without the need for any changes within the application.

In terms of how to use signatures in the cloud, it is worth noting the potential to relieve other systems that manage private keys for this task. Thus, another contribution is to identify the systems that can benefit from this facility. From this perspective, it is proposed to modify the authentication protocols based on QR codes. In this way, mobile devices are relieved of the task of managing private keys and the protocol becomes more secure and more flexible.

From the security point of view, all the requirements mentioned in the legislation and in the standards can be summarized into a single one: the user's private keys are under his exclusive control, even if they are stored in the cloud. For this purpose, the SABRES solution is proposed in the thesis. It provides users with a distributed trusted source, which immutably stores all access to private keys and complies with applicable laws and standards.