

RESUMO

É geralmente assumido que, no futuro, uma das componentes chaves, do chamado governo electrónico será a votação electrónica. Esta terá o objectivo de facilitar a participação dos cidadãos nas eleições e nos debates públicos, numa tentativa de contrariar o decréscimo de participação dos mesmos neste tipo de solicitações. No entanto, ainda existe um grande caminho a percorrer até a votação electrónica, especialmente se baseada na Internet, ser aceite como um sistema fidedigno e alternativo aos métodos convencionais.

Neste tese, propomos uma nova e simples plataforma de votação electrónica, totalmente baseada em software “*open source*”, que poderá e deverá ser utilizada, numa fase inicial, em pequenas e médias comunidades, com o objectivo de criar alicerces sólidos, principalmente na área da confiabilidade e da experiência, para poder ser, mais tarde, ser usada em maiores e mais importantes eleições.

Tentamos também providenciar respostas adequadas aos vários requerimentos / critérios necessários, tais como, exactidão, democracia, privacidade, auditabilidade e mobilidade. Estes, são atingidos através da utilização de sistemas distribuídos com suporte para a diferenciação de papéis, de técnicas criptográficas na interacção entre os vários componentes e por último, através da publicação de todo o trabalho efectuado para utilização livre da comunidade, quer seja apenas para fins de auditabilidade, quer seja para desenvolvimentos paralelos.

Além da apresentação da nossa plataforma, foi ainda desenvolvido, no âmbito desta tese, um pequeno protótipo funcional com o objectivo de demonstrar a validade da mesma e que é aqui apresentado.

ABSTRACT

It is generally considered that a key component of electronic government in the future will be electronic voting, as a means of facilitating the participation of citizens in elections and public debates, in an attempt to oppose the decrease of participation in this type of requests. However, a long path has to be pursued before electronic voting, particularly if based on Internet, is accepted as a reliable system alternative to conventional methods.

In this thesis, we propose a new and simple platform, based on open software, which can be used primarily in small to medium sized communities, as a means to build confidence and experience for future larger elections.

We try to provide adequate answers to multiple requirements, such as accuracy, democracy, privacy, verifiability and mobility. This can be done by establishing a distributed system which supports the different roles of a voting system, by using cryptography techniques in the interactions between these components and through the publication of all the work so it can be used by the community for auditability or for parallel developments

Beside the presentation of our platform, we have also developed it, in the scope of this thesis. It is a small functional prototype with the objective to demonstrate the validity it