Chapter 3.6
Securing an Electronic Legislature Using Threshold Signatures

Brian King
Indiana University – Purdue University Indianapolis (IU–PUI), USA

Yvo Desmedt
University College of London, UK

INTRODUCTION

Today a significant amount of research has focused on trying to apply the advances in information technology to governmental services. One endeavor has been the attempt to apply it to "electronic voting." Unfortunately, while questionable secure e-voting technology has been widely deployed, the same cannot be said for cryptographic based ones. There is one type of "voting" which has received only limited attention concerning applying these technology advances, the type of voting that takes place within a legislative body. At first glance, it may not appear difficult to institute electronic voting in a legislature, for it may seem that one only needs to apply the traditional security mechanisms that are used to safeguard networked systems, but as we soon outline there will be significant security risks associated with an electronic legislature. One of our concerns is that entities may attempt to implement an electronic version of a legislature without realizing all the risks and implementing all the needed security mechanisms. In fact, there have been occasional instances of some entities attempting to create some electronic/digital form of legislature, for example (Weidenbener, 2004).

In any legislative vote, the legislature's ability to pass or to not pass legislation should be interpreted as the legislature deciding whether to "sign the proposal" into "law." Thus, "law" is a signature; anyone can verify that a "proposal" is a "law" by applying the signature verification procedure. As we move towards electronic applications of governmental services, it is only natural when this is applied towards legislatures we will replace the "written law" by a "digital signature" (here the use of the term law can be replaced by any internal regulation and a legislature by any regulatory body). The underlying aspect of the article is the security considerations that need to be applied when this is implemented.

The question *why consider an electronic legislature* is important. The fundamental reasons for applying today's information technology to government and its services have always focused on that it would bring improved services and allow greater accessibility of government to its constituents. An electronic legislature would most certainly improve the legislative service. It will allow for the legislators to be *mobile*, they will no longer need to be tied to the legislative house to provide representation. Many industrial employers allow their workers to telecommute to work, it is a realization by the employers that these workers are valuable, as well as a recognition that the workforce and the time constraints on the workforce has changed. In many cases, without this option, these workers may leave the workplace. This same reasoning of a valued worker should be applied to our legislators. Further, it does not make sense that today we would allow a subset of the legislature to make and pass laws due to absenteeism, especially in light that many of the required mechanisms to bring about a mobile "electronic legislature" are available. One can argue that by allowing legislators to occasionally telecommute will provide an improved workforce (this argument is motivated by the same reason that private industry utilizes "telecommuting"). We also observe that an electronic legislature should provide the constituents greater access to their legislators. A final argument for an electronic legislature is that it will provide continuation of government in the case of some drastic action like a terrorist attack. In the fall of 2001, the legislative branch of the U.S. federal government came under two attacks. The first attack was performed by Al Qaeda operatives (who it is speculated intended to fly one of the planes into the U.S. capital), and a second attack by an unknown entity who contaminated parts of the U.S. senate (and it offices) with anthrax spores. This second attack was successful in that it denied the Senate the ability to convene for several days. Although such terrorist's attacks on the legislative branch may appear novel, at least in the U.S., such attacks have been precipitated in other countries for some years (PBS, 2001). The U.S. government has recognized the need to develop a means for the continuity of government in the wake of such disasters (Continuity of Government Commission, 2002), one such solution is to utilize an e-legislature.

The concept, model, and a protocol for an e-legislature was first described in Desmedt and King (1999). In Ghodosi and Pieprzyk (2001), the authors described an alternative, which required the use of a trusted administrator. Later in Desmedt and King (2002), we pointed out the weaknesses and disadvantages of the system in Ghodosi and Pieprzyk (2001) and clarified some aspects of the protocol in Desmedt and King (1999).

SECURITY CONCERNS

One reason to be concerned about the security of an electronic legislature (e-legislature) is that one can "view" the e-legislature as a "network." Represent the legislators as computers/hosts and their communications as the network communications. All problems that affect a network can affect an e-legislature; however there are several more reasons to be concerned. First observe that as a "law making body," an e-legislature and the results derived from its communications need to possess a high integrity. In addition, the participation of members from the legislative body will dynamically vary from time-to-time. Further, since the decisions made by the body (i.e., law) are determined by some fixed percentage of those members present/active, there will need to be some *"transfer of power"* which allows this percentage of the legislators present to pass legislation. For example, suppose that the legislature makes decisions based on majority rules and that the original legislature contains 50 members. Thus 26 legislators are required to approve a proposal into law. Later we have seven legislators absent. At this time, 22 legislators are needed to pass legislation. Thus, there will need to be some mechanism