The advent of information society has enabled people to perform most of their activities in a direct, electronically automated, and efficient way. To keep up with the need to provide citizens with the ability to participate and benefit from services over the Internet, as well as to reduce the cost and bureaucracy of public administration, contemporary states are striving to transfer an ever-increasing number of their activities to the new medium.

An indicative example is that of Internet based electronic voting systems. In terms of functional requirements a system supporting electronic voting should exhibit as many of the following characteristics as possible: a) provide all required services for organizing and conducting an opinion expressing process, b) support all actors involved; namely: organizers, administrators, candidates and voters (set-up and conduct the election, calculate the final tally), c) feature an easy and user-friendly environment for the interaction of the voter with the system through conventional WWW browsers, d) incorporate, in terms of its design, the appropriate sociological and behavioral aspects, e) support the registration of all persons that are eligible to vote and, at the same time, provide some kind of unique identification (password, smart card, etc.) that will allow the system to validate the voter’s credentials, f) ensure applicability to a wide range of voting processes (polls, general elections, internal elections, decision making etc) g) cover large geographical regions, h) generate in an automatic way the vote tally.

However, it becomes evident that there are numerous opportunities for corruption during the performance of the above mentioned tasks. Furthermore, the existing European law is generally predicated on conventional voting systems and probably not sufficient to address the new elements and risks introduced by e-voting. More specifically, the constraints imposed by the legal framework are highlighted through the following principles: a) Generality: All citizens above a certain age have the right / obligation to vote, b) Freedom: Everyone is free to vote for the party he/she considers more appropriate (uncoercibility), c) Equality: Only eligible voters can vote. Each eligible voter can vote only once, No-one can duplicate his or someone else’s vote, No-one can change someone else’s vote, The voter must have the possibility to verify the his/hers vote has been calculated in the final vote tally, Voters should have undiscriminating access to the voting infrastructure, d) Secrecy: No-one involved in the voting process should be able to link a ballot to a voter, e) Directness: Voters select directly (with no intermediates) their representatives.

Along these lines, it is rather usual to identify the “requirements” of an electronic voting system merely as the guidelines for conforming to the legislation governing elections or, alternatively, as the identification of the fundamental technological problems associated with the provision of an adequate level of security (anonymity, authentication, data security, tractability, etc).

We are in the process of producing a common User Requirement Specification for electronic voting systems, based on a Generic Voting Model that takes into account: a) the existing European Legal Framework, b) the organizational details of conventional voting processes, c) the required security attributes and d) the opportunities offered and the constraints imposed by the state-of-the-art technology.

The requirements elicitation process has been based on the Rational Unified Process with each “Use Case” referring to a functional requirement of the system. Its “security attributes” (mainly imposed by the legal framework) are being expressed as non-functional
requirements which are either “use case specific” or “system wide”.