



New York State Technology Enterprise Corporation

Digital Signatures and Electronic Records Requirements

Clarification and response to vendor questions

New York State Board of Elections

Submitted to:

New York State Board of Elections
40 Steuben Place, Albany NY 12207

August 28, 2007
Version 2

Table of Contents

- 1. STATEMENT OF REQUIREMENTS 2
- 2. VENDOR QUESTIONS AND ANSWERS 2
- 2.1 QUESTION 1 2
- 2.2 QUESTION 2 3
- 2.3 QUESTION 3 3
- 2.4 QUESTION 4 4
- 2.5 QUESTION 5 4

1. STATEMENT OF REQUIREMENTS

At the New York State Board of Elections and voting system vendor's status call a lengthy discussion of the requirements for digital signatures took place. During this discussion many questions were raised and many of them were discussed and answered.

For example, what is the intent of using digital signatures on electronic records? Simply put, the intent is to:

1. Protect the integrity of ballots on the voting machine and election configuration objects that are created on the EMS system and loaded on voting machines.
2. Protect the integrity of ballots and election configuration objects as they are transported between voting system components via any electronic media.
NOTE: Under NYS regulations electronic communications is not permitted. This then only pertains to media including but not limited to CD's, DVD's, USB thumb drives, floppy disks, chips etc.
3. Protect the integrity of the ballot (including individual votes) as they are cast
4. Protect the integrity of the election results as they are transported to the EMS system or any other system designed for tallying votes.
5. Ensure that at any time the electronic image of the ballots and votes can be trusted to be accurate and cast as intended by the voter.
6. Help to ensure that voting system components are free of unauthorized software. The use of digital signatures provides the most secure and achievable method of ensuring that no unauthorized software is present on voting equipment and will permit vendors to meet the requirements in 7.4.6 of VVSG Volume 1.

After the discussion of the above it appeared that all on the call were in agreement that the intent is logical to protect the integrity of the vote. Based on this, additional discussions took place regarding how to accomplish this.

2. VENDOR QUESTIONS AND ANSWERS

As an outcome of the above discussion the vendors were asked to provide their issues, concerns, and requests for clarification to the NYSBOE in writing.

Four of the vendors did so and we believe the four documents actually represent the concerns of all the vendors as stated in the meeting. Since the issues are global we opted to answer all the issues in one response.

2.1 Question 1

If my system is not currently in compliance with the NYS requirements will I be able to continue testing while we work on a solution?

Answer

Yes.

This however does require additional comments. It must be understood that as long as you wish for your system to be in contention we will continue testing them. As the test progresses there will be feedback to the vendors in the form of "Anomalies" for the vendors to correct. When resolutions are provided testing will either be restarted or continued based on the severity of the change implemented. This process could delay the certification of your system which of course would give other vendors the advantage of moving further into the process and become eligible for purchase sooner. In other words, the race is on to become eligible for purchase in New York. Additionally, efforts to include the appropriate use of digital signatures on existing machines may be significant and vendors should not delay in beginning that work.

2.2 Question 2

Does the use of digital signatures on electronic records only apply to digitally signing electronic records for the ballot image associated with DRE's and VVPAT's?

Answer

Although it is true that the requirement for digital signatures on electronic records appears primarily in the VVPAT sections of both the VVSG and the NYS regulations, it is important to take into account the protections it is meant to provide.

The premise here was that the paper and the electronic records should be considered valid and auditable "with trust" at any point in time. It is the opinion of the NYSBOE that the intent of this protection should apply to any voting system that has both paper and electronic records to provide for the same level of integrity as outlined in the opening comments of this document.

Additionally, VVSG Vol1 section 7.4.6 talks extensively about the use of digital signatures as a means to verify software present on systems. NYSTEC as well as other security experts believe that properly implemented digital signatures are necessary to ensure that requirements in this section of the VVSG are met.

2.3 Question 3

Is there a better way or a reasonable alternative to digitally signing each individual vote record that is cast? The common concern here is that having to sign each record could cause significant overhead that could impact both system performance and storage needs.

Answer

One of the vendors proposed a solution that as each record was written to the file a checksum would be calculated for the total of the new record and all records that were previously written. The new checksum of the file would be compared to the prior

checksum (minus the value of the new record) to determine if any records had been added that were not legitimate, or any records were altered, or if the file was corrupted in some other fashion. The file would then be digitally signed with a combination of the digital signature and the new checksum. This could in fact ensure that no records could be written by other than the authorized program.

The VVSG, sections 7.9.3 (d and e) make it fairly clear that digital signatures shall be calculated for the entire set of voting records and the digital signature of each associated individual record. This is required to ensure that records are not missing or substituted. If a vendor proposes an alternative method it will be evaluated by the ITA and NYSTEC for compliance with the VVSG and NYS requirements.

If you wish to use a similar solution NYSBOE would be agreeable to review the solution with you prior to implementation to determine compliance.

2.4 Question 4

Since the New York State regulation does not define what a digital signature is, is it necessary for us to use digital signatures for the purpose of protecting electronic records?

Answer

Yes. The NYS regulations made the use of digital signatures mandatory (stronger than the VVSG) however; the definition of digital signatures in the VVSG and further clarification by NYSTEC was deemed satisfactory and did not require a separate NYS regulation.

2.5 Question 5

Is the use of digital signatures for the purpose of protecting electronic records the only possible way of accomplishing this?

Answer

The use of digital signatures on electronic records is clearly not the only possible way to meet the requirements of the NYS Law, Regulations and the VVSG; it is simply the best way and balances strong security with ease of implementation. NYS will entertain any proposal made by the vendors to implement an "electronic" means of protecting the ballot and the vote. If a vendor proposes an alternative method it will be evaluated by the ITA and NYSTEC for compliance with the VVSG and NYS requirements.