NYSTEC

New York State Technology Enterprise Corporation

NYSTEC Response to ES&S Request for Interpretation of VVSG 2005 Volume 1 Sections 7.8,7.9, and C.2 and NYS Regulation 6209.2f.10(a)

For

New York State Board of Elections

Submitted to:

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

August 23rd, 2010
Version 2.1

Table of Contents

1. BACKGROUND

NYSBOE has requested that NYSTEC respond to the accompanying ES&S RFI "Request for Interpretation by the NYS Board of Elections" for an interpretation of the following Voluntary Voting System Guidelines (VVSG) and NYS Regulations requirements:

VVSG 2005 Volume 1 Sections 7.8, 7.9, and C.2.

NYS Regulation 6209.2.f.10(a)

More specifically, the following requirements:

> ***VVSG 2005 7.9.3 Electronic and Paper Record Structure***
> *a. All cryptographic software in the voting system shall be approved by the U.S. Government's Cryptographic Module Validation Program, as applicable.*
>
> *Discussion: Cryptographic software may be used for a number of different purposes,*
> *including calculating checksums, encrypting records, authentication, generating random numbers, and digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program (CMVP). There may be cryptographic voting*
> *schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP approved software should be used where feasible but is not required. The CMVP website is http://csrc.nist.gov/cryptval.*
>
> ***6209.2.F.10a***
> *(a) All cryptographic software in the voting system shall have been approved by the U.S. Government's Crypto Module Validation Program (CMVP) as applicable.*

ES&S is seeking clarification on the required use of CMVP approved software and a decision on three specific categories of cryptographic software test findings where they are claiming cryptographic functions are either not necessary or are unused in the NY systems. ES&S believes that the "as applicable" clause in the above cited requirements allows them to use non-CMVP approved software within a voting system. Based on this interpretation, ES&S is seeking to have three groups of cryptographic software findings closed.

2. EXECUTIVE SUMMARY

The accompanying ES&S RFI is seeking a direct ruling on where CMVP approved software is required relevant to three groups of cryptographic findings that are outstanding from the 2009 certification testing. ES&S has cited 2005 VVSG Vol. 1 requirements that are relevant to Independent Verification (IV) voting systems which, in some cases, permit the use of non-CMVP approved software. IV systems produce independent records of voter ballot selections that permit highly precise levels of auditing. It is not the intent of this response to determine if the NYS ES&S certified optical scan systems are IV systems or not; based on past NYSBOE guidance, we assume they are. The specific requirement, VVSG Vol. 1 7.9.3a (cited above) relaxes the requirement for CMVP approved software for IV voting systems that implement cryptographic voting schemes. Cryptographic voting schemes are clearly defined in the 2005 VVSG Vol. 1, Appendix C, section C.1.2.2 and C.5. The discussion portion of requirement 7.9.3a states that where cryptographic algorithms are used as part of a cryptographic voting scheme the requirement for a CMVP approved module is relaxed because the modules may not lend themselves to this purpose. This VVSG discussion goes on to say that when cryptographic software is used for other purposes including checksums, encrypting records, authentication, generating random numbers, and for digital signatures, that the software should be reviewed and approved by the CMVP. The NYS certification testing that was completed in 2009 was consistent with this guidance.

Cryptographic voting schemes provide the voter with a printed receipt that permits the voter to verify that choices were recorded correctly. This information is provided using cryptographic techniques that prevent the voter from revealing his or her selections (See 2005 VVSG Appendix C, C.1.2.2). The ES&S DS200 voting system does not implement any form of cryptographic mechanism that can be used by the voter to verify that ballot selections were recorded correctly. Because this is a key requirement of cryptographic voting scheme, the DS200 would not be covered by the permitted use of non-CMVP approved software under the requirements specified in the RFI, namely VVSG Vol. 1 7.9.3a.

NYSTEC has concluded that none of the findings referenced by ES&S in the RFI are related in any way to a cryptographic IV component within the voting system and cannot be closed under VVSG Vol. 1 7.9.3a. Despite this, NYSTEC does believe there is some merit in the ES&S request to consider the closure of some of the groups of findings. NYSTEC has investigated these findings and believes that many of them can be closed. The following section addresses each group of findings and presents our recommendations.

3. NYSTEC Detailed Response to ES&S Proposed Interpretations

RFI Group 1 findings: Code within a system that is not utilized within the New York configuration (Crypto Findings: 12,13,15,64,65,66,75,76,77,78)

In this group, ES&S has identified findings where non-CMVP approved cryptographic software was used and has requested the findings be closed because the code is not executable in the NYS configuration. NYSTEC believes that cryptographic software that is not utilized within the NY configuration and is not CMVP approved can be allowed to exist within the system and will not pose a significant security risk. NYSTEC recommends however that ES&S, in the next version of NYS software, either remove unused code from the source or conditionally compile it out. This provides for more manageable code and adheres to good coding practices.

NYSTEC has independently verified the cryptographic findings included in Group 1 above, and agrees that the cryptographic functionality is not utilized in the NYS build. NYSTEC performed an analysis of the relevant code modules and calling sequences to validate the vendor claim that the findings represent legacy code that is not used in NY. Based on this analysis, NYSTEC agrees with the vendor and recommends that the Group 1 findings 12, 13, 15, 64, 65, 66, 75, 76, 77 and 78 be closed.

Group 2: Code within a system that performs cryptography where cryptographic usage is not required

(Crypto Findings: 1,2,3,4,5,6,7,8,9,10,11,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,67,68,86,87,88,89,90,93,94,95,96,97,98,99,100,101,102,103,104,105,106,107,108,109,110; (Open-Security Tab) Finding #353)

In this group, ES&S has identified findings where non-CMVP approved cryptographic software was used and has requested them to be excluded because they believe it was used where encryption was not required. NYSTEC believes that the existence of non-CMVP approved cryptographic software in places where encryption is not required does not pose a significant security risk and may even improve security vs. not encrypting the data.

Several of the Group 2 findings identified by ES&S have been shown to implement encryption or hashing in places where it was unnecessary as per NYS requirements and past NYSTEC guidance to the vendor. This would include the encryption of data that is not passed to or from the precinct site or that is maintained only within the Election Management System. NYSTEC has completed a review of the relevant code modules and function calls and we agree in many instances with the vendors' claim that these findings represent the use of cryptography where it was not required. NYSTEC has concluded that the following Group 2 findings fall into this category and can be closed:
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 40, 41, 42, 43 and 353.

There are numerous other findings in Group 2 however where NYSTEC does not agree with the vendor. These findings involve the required use of CMVP software for passwords or were findings where NYSTEC could not validate the vendor's conclusion that cryptography was not needed. NYSTEC recommends these findings (44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 67, 68, 86, 87, 88, 89, 90, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110) remain open.

Group 3: Validation of digital signature in locations other than where the system intends (Findings: 306, 308, and 317)

The group 3 findings identified by ES&S represent places where digital signatures were used improperly, namely were digital signatures were applied but not validated. In these findings ES&S believed that digital signatures were not required. NYSTEC has analyzed the group 3 findings and does not agree with the vendor. We believe that digital signatures must be applied as per NYS Election Law and past guidance to vendors and that a digital signature is as defined in the VVSG. Digital signature usage assumes the application of a digital signature and its verification. Therefore, NYSTEC recommends findings 306, 308 and 317 remain open.

4. NYSTEC CONCLUSION

When considering the discussion following 7.9.3a in the 2005 VVSG, NYSTEC does not believe it changes the guidance that has been provided to the vendors to date on the use of encryption and cryptographic modules in general. By allowing many of the Group 1 and Group 2 findings to be closed NYSTEC is consistent with our past recommendations on the use of cryptography and we do not believe the NYS voting systems will be exposed to any significant risk by closing these findings. In addition to the code analysis performed by NYSTEC we also researched past Election Assistance Committee (EAC) voting system certifications against the 2002 and 2005 VVSG. We found no evidence of any voting system that was certified where the use of CMVP software was required or assessed. We have a pending question into the EAC to confirm our interpretation of requirement and will report to NYSBOE any information received that conflicts with the recommendations stated here.

When considering the discussion following 7.9.3a in the 2005 VVSG, NYSTEC does not believe it changes the guidance that has been provided to the vendors to date on the use of encryption and cryptographic modules in general. The discussion following 7.9.3a in the VVSG states that cryptography used the following purposes should be reviewed and approved by the CMVP (FIPS 140 validated):

- Calculating checksums (hashes)
- Encrypting records
- Authentication
- Generating random numbers
- Digital signatures
-

NYSTEC agrees that when vendors implement cryptography for these purposes it shall be implemented via CMVP approved modules. Testing done for the 2009 NYS Certification also reflected this and is consistent with past NYSTEC guidance.

5. REFERENCES

1) “Digital Signatures and Electronic Records Requirements – Clarification and response to vendor questions”
(http://www.elections.state.ny.us/NYSBOE/hava/Voting_Machines/CIBERDigital.pdf)

2) “Use of Encryption.doc (Data Encryption Testing Guidelines for NYS Voting System Certification” (Available from NYSTEC)