Voting Applications of The Event Verification System: **Answers to Common Questions**

1) Are there any licensing fees associated with the use of EVS in voting machines?

No. Anyone who wishes to incorporate EVS into their voting machine design will be allowed to do so free of licensing fees for the life of the patent.

2) How can EVS insure that no party can connect the voter to the vote they cast?

Regardless of the method used to confirm voter intent, the "reconstruction" problem can be overcome by simply decreasing the resolution of the timestamp. If, for example, the tamperproof module incremented its timestamp clock once per hour, there might be 22 votes recorded during that period. It would therefore be highly unlikely that one could gain knowledge about how any specific individual voted unless, of course, only one voter voted per time increment, or all voters voted the same way (in either of these exceptional cases no system has an advantage). Longer clock increments might be more appropriate depending on local voting patterns. The point is, it's possible to have the best of both worlds - preserving the anonymity of the voter, and establishing securely the knowledge of when and where an authentic and tamperproof record was produced.

While it might not be as practical to implement, another approach would be for pairs of (or possibly multiple) machines to be hardwired at the time of their initial programming so that they share IDs (the pairs could reside in the same physical voting space). The timestamp for each "vote event" would record both machine IDs. Auditors would know that the vote came from one of the two machines but nothing about how the individual votes were apportioned between the two sets of voters.

3) How can the voter be sure that their vote was recorded exactly as they cast it?

Decrypt the “confirmed” vote with the published public key.

This does point to the issue of just how far one has to go to assure a reasonable degree of security. After all, voters have faith that once they press their old-fashioned levers and pull the curtain bar, that their intent is properly recorded. As with lever-type devices, if all machines adhere to strict manufacturing, testing, and administrative regulations and oversight, at some point voters must have faith that when they press the “confirm” button, their vote has been properly recorded. Indeed, even Open Source designs require protocols for maintaining system integrity.

4) How does EVS provide for the auditing of confirmed votes?

Using the public key, decrypt the record of "vote events." In theory, this could be done by *any* concerned party. If the record can be successfully decrypted, then it represents an accurate record that was not tampered with. The record could contain the time window and the physical location of the confirmed vote events, along with the ID of the machine from which the vote originated (paired machines not withstanding). It would not contain sufficient information to allow a malevolent party to successfully connect the individual votes to specific voters.

An interesting possibility is presented by the fact that the EVS patent also describes the transmission of tamperproof digital records to a remote location for secure storage.

5) Is paper necessary for confirmation of intent and secure auditing?

The question of whether it is necessary to produce paper records is, essentially, a two-fold issue revolving around:

1) the practical security of offering a low-tech, tamperproof record and
2) the psychological security of a macro-physical object with familiar and time-tested properties.

We know that, generally speaking, people don't trust what they can't see and touch. In reality, however, paper is secure only as far as the administrative system is secure. Unless the paper were a certified, currency grade material, it would be trivial to print a forged voter log. An encrypted record, on the other hand, cannot easily be counterfeited regardless of administrative lapses or malfeasance. Furthermore, unlike paper records, a secure electronic record of votes can be stored in multiple locations and is thereby less susceptible to damage, loss, or tampering.

There are ways to safely do away with paper records. Douglas Jones at the *University of Iowa* has described a system wherein a screenshot of the "verify ballot" display is logged along with the state of pushbuttons that confirm or reject the displayed vote. In this system, the logging function interfaces only with the screen interface electronics and the pushbuttons.

Another method would be to actually take a secure physical snapshot of the screen which, in conjunction with button states, could later be used for *either* manual or electronic auditing.

In the end, paper or no paper, an EVS-based system would be inherently more secure than current designs.

6) How can a secure paperless design save money?

Electrons are cheap (especially in small quantities). While there would clearly be an upfront expense for development of an EVS-based system, there would be no ongoing economic cost for the countless reams of paper used over the course of decades and no expenses associated with the maintenance and repair of printing mechanisms. Importantly, there would also be no direct environmental cost as compared with producing paper records. Furthermore, there would be no overhead connected to the storage and management of paper records, especially in the event of a recount.

7) Are there other advantages to using EVS?

EVS allows a higher level of functionality in its ability to offer fast, independent audits and transmit data to a secure remote location. Furthermore, an EVS-based system would allow *independent tabulation of results*, thereby assuring that this critical step in the election process does not remain subject to the vagaries of proprietary code.