REFERENCE SOURCE CODE IMPLEMENTATION

INTRODUCTION DOCUMENT

APRIL 6, 2004

SECTION 1

WHAT IS INCLUDED IN THIS PACKAGE?

VHTi_Introduction.pdf
This document provides background information on VoteHere, VHTi, and this Reference Source Code Release. It also contains information on how to provide feedback, why this is important and a roadmap of where VHTi is in the process.

VHTi_License.pdf
This is the document form of the license that was accepted as part of the download. This is an evaluation-only license.

VHTi_API.pdf
This describes the VHTi Application Programming Interface (API).

VHTi_KnownIssues.pdf
These are issues uncovered during internal reviews and will be addressed in a later release.

VHTi_MediaFAQ.pdf
The non-technical FAQ answers some questions related to the review process and VHTi.

README.txt
This is the introduction in plain text form.

README.license.txt
This is the License Agreement in readme form.

README.building.txt
This describes how to build the source.

README.sample.txt
This describes the functions of the provided samples.

README.protocols.txt
The cryptographic protocols used in VHTi are outlined in the protocol papers released for review in September 2003. Those papers can be found at http://www.votehere.com/downloads.html

SECTION 2

VOTEHERE BACKGROUND

Founded in 1996, VoteHere, a privately-held company headquartered in Bellevue, Washington, is an industry leader in developing secure e-voting software through the use of patented security protocols and the world's most advanced election technology. VoteHere's technology has been used in over 90 elections in the US and Europe, for over 50 worldwide clients and partners, reaching nearly 13 million voters.

Between 1999 and 2002, VoteHere filed patents on the technology that underlies the VHTi protocols. In September 2003, detailed papers describing the VHTi cryptographic protocols were released. Now, VoteHere is releasing reference source-code that implements the cryptographic protocols.

SECTION 3

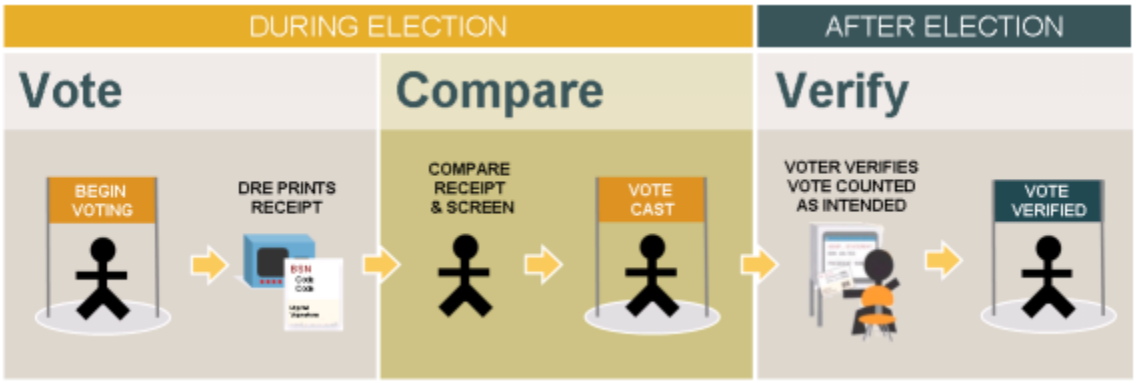
WHAT IS VHTi?

VHTi guarantees election confidence, ensuring that ballots were counted as intended, while maintaining voter privacy. This licensed technology is available for the manufacturers of any electronic voting system.

VHTi gives voters the ability to see, end-to-end, that their ballots went into the ballot box as they intended, were correctly received, and were included in the tabulation of the results. VHTi allows election officials to perform an end-to-end audit of the election to determine if ballots were tampered with, deleted or changed. After the election, all interested parties are able to review the election data to confirm that the election was run correctly.

- VHTi proves, in every election, that electronic voting machines worked correctly and did not cheat.
- VHTi provides for a meaningful recount and audit trail.
- VHTi provides voters with verification that their vote was counted as intended.

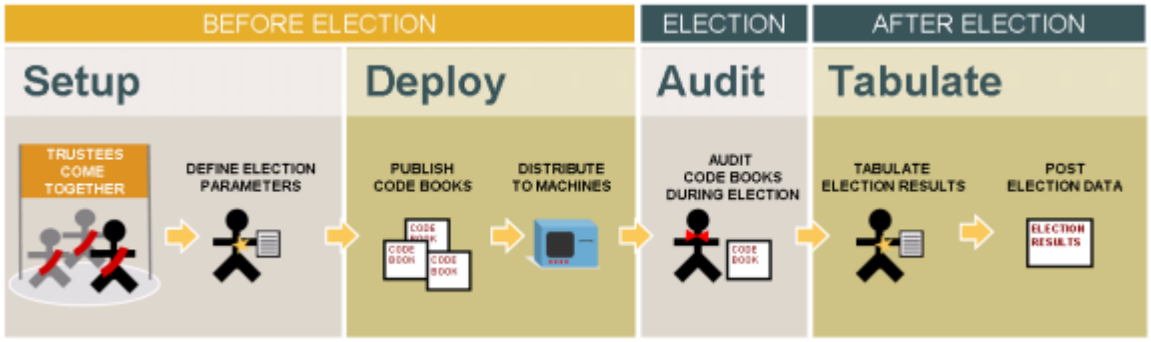
VOTING PROCESS



Voting with VHTi is 3 simple steps.

1. Vote normally on any electronic voting machine.
2. Compare the printed receipt with the selections shown on the confirmation screen.
3. After the election, verify that your vote was counted as intended by comparing the receipt with the verification report on the county website.

ELECTION PROCESS



Before the election

- Trustees and Election Officials define election parameters and codebooks.
- Codebooks are published and available for 3rd party review.
- Election parameters and codebooks are distributed to the electronic voting machines during the machine preparation.

During the election

- Observers audit codebooks to confirm they are being generated correctly.

After the election

- Trustees and Election Officials decrypt and tabulate the election results.
- Election results and verification reports are posted for public and 3rd party review.

VHTi PROTOCOLS

The cryptographic principles used in VHTi are outlined in two papers called *Detecting Malicious Poll Site Voting Clients* and *Verifiable Mixing (Shuffling) of ElGamal Pairs*, both by Dr. C. Andrew Neff. These papers were released in September 2003 and can be found at http://www.votehere.com/documents.html. Along with the papers, a VHTi threat analysis, which is a comprehensive matrix of potential attacks and countermeasures, was also released. The protocols are the key to a full understanding of VoteHere's technology.

VHTi API

VoteHere has packaged a ***reference implementation*** of the protocols in an application programming interface (***API***) and is now releasing a reference implementation of the API source code for public review and evaluation. The VHTi API is ***not*** a voting system. It makes electronic voting systems trustworthy by adding end-to-end verification and audit capabilities. The VHTi protocols and reference implementation API are not freeware, shareware, or open source. They are proprietary and protected under patent, trademark, and copyright law.

SECTION 4

IMPORTANCE OF TRANSPARENCY

VHTi is based on the concept of transparent provable elections. We believe that public disclosure of our protocols and reference source code is essential to providing this transparency. It is important that voters have confidence that their votes are cast and counted as intended. This is achieved by an open, transparent voting system.

In order to fully understand VHTi, refer to both the Protocols and the Reference Source Code. The Protocols can be found http://www.votehere.com/documents.html. The VHTi Reference Source Code Implementation includes the VHTi_KnownIssues document that outlines known issues, instructions to build the source and samples.

How to provide feedback

We welcome constructive feedback as part of this review process. You can submit any feedback you have to vhtifeedback@votehere.com. We will address any valid issues and/or suggestions.

SECTION 5

ROADMAP

VHTi Implementation Roadmap

The creation of secure mission-critical software is a multi-step process that requires repeated review and validation. The VHTi reference implementation is in the public review stage of this process. This process will be repeated over time as the capabilities of the protocols and API evolve.

We believe public disclosure of these components is critical for credibility and public confidence in our election systems. Review by academics, peers, public officials, the media, and the voting public is part of this process and the feedback and criticism will be evaluated and incorporated into our technology as a appropriate.