

Cryptography provides world's first large-scale verifiable political election

December 20 2013

Controversial election results could be a thing of the past, as a secure e-voting system developed by computing experts at the University of Surrey moves one step closer to implementation.

The team at Surrey has signed a contract with the Victorian Electoral Commission (VEC) in Australia to develop the 'back end' software for the supervised e-voting system it will be using at the Victorian State [election](#) in 2014. The project will be the world's first large-scale verifiable political election. Victorian law allows the VEC to make e-voting kiosks available for those living with a [vision impairment](#) or who have insufficient English literacy skills, as well as those who live outside the State of Victoria.

The key novelty of the system is 'end-to-end verifiability'—this means that the system provides confirmation information about the election that can be checked independently. It does this using cryptography. Voters are given a receipt of their [vote](#) in encrypted form so they can check their encrypted vote is included. The secrecy of the ballot is ensured because votes are decrypted in a cryptographically secure and verifiable way, so that no-one can tell which decrypted vote corresponds to which encrypted vote. Verifiability gives the public a way to check that the voting system has processed the votes correctly. The code itself and its design will also be made open for transparency, fostering greater trust in this method of voting.

Steve Schneider, Professor of Computing at the University of Surrey,

and project lead, comments: "Concerns about security in e-voting meant that the VEC wanted end-to-end verifiability in their [voting system](#). The University of Surrey is actively involved in this area, having won 'best design' at the VoComp 2007 Universities Voting Systems Competition, and they approached us to adapt and apply our design to their election requirements. After the 2014 Victorian State election we aim to roll out our system more widely."

Victorian Electoral Commissioner, Warwick Gately, AM, says: "For the VEC, ensuring every Victorian can actively participate in their democracy is our goal. E-voting aids accessibility for people who live with a disability or who cannot read English.

"The strength of end-to-end verifiability is that all participants—the VEC, candidates, scrutineers and voters—can be completely sure that the actual vote cast is the same as that received and counted."

Provided by University of Surrey

Citation: Cryptography provides world's first large-scale verifiable political election (2013, December 20) retrieved 8 May 2024 from <https://phys.org/news/2013-12-cryptography-world-large-scale-political-election.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--