

Gemäß § 3 Abs. 1 WVO wählen die teilnehmenden Kassen einen Anbieter aus: das System TIVI von Smartmatic, einem Anbieter von Wahlmaschinen und Online-Wahlssystemen. Dieses Unternehmen wurde 2000 von venezolanischen Ingenieuren gegründet. Der erste und für das Unternehmen wohl entscheidende Großauftrag scheint das (ablehnend ausgegangene) Referendum über die Abwahl von Hugo Chávez 2004 gewesen zu sein. Der Unternehmenssitz ist seit 2012 London.

§ 8 Abs. 1 WVO fordert eine rein funktionale Prüfung des Online-Wahlsystems gemäß einem „Testfallkatalog“; hingegen keine Prüfung der Einhaltung der Wahlgrundsätze. Abs. 3 fordert die Prüfung des Wahlsystems durch einen externen und unabhängigen Sachverständigen, allerdings nur in Bezug auf die Einhaltung des IT-Grundschutzes. D. h. der Sachverständige prüft z. B., ob ein Ausfallkonzept vorhanden ist oder der Webserver mit TLS (https) betrieben wird, nicht aber, ob das System die Wahlrechtsgrundsätze einhält.

Die TR-03162 verlangt, dass Penetrationstests durchgeführt werden müssen (S. 24). Einen Absatz später heißt es aber, dass ein Penetrationstestkonzept erstellt werden sollte. Was also gilt? Dazu muss gesagt werden, dass eine erfolgreiche Abwehr von standardisierten Penetrationstests noch lange

# Sozialwahlen online

Ein Fall für die Wahlgerichte?

**(BS/Prof. Robert Müller-Török/Prof. Alexander Prosser\*) Mit 52 Millionen Wahlberechtigten ist die Sozialwahl eine der größten Wahlen in Europa, 2023 findet sie erstmals auch online statt. Grundlagen sind die Online-Wahl-Verordnung (WVO) des Bundesministeriums für Gesundheit (BMG) und die technische Richtlinie TR-03162 des Bundesamtes für Sicherheit in der Informationstechnik (BSI), auf die sich die WVO in §4 auch bezieht. Indirekt anwendbar ist wohl auch die Empfehlung des Europarates CM/Rec(2017)5 zu E-Voting, die allerdings weder in der WVO noch in der TR-03162 erwähnt wird, wiewohl die Wahl in der WVO als „Modellprojekt“ bezeichnet wird.**



E-Voting: Im Rahmen der Sozialwahl 2023 haben die Wählerinnen und Wähler erstmalig die Möglichkeit, ihre Stimme auch online abzugeben.

Foto: BS/Aleksandr Marko, stock.adobe.com

nicht bedeutet, dass das System die Wahlrechtsgrundsätze einhält und etwa einem Angriff auf das Stimm-

geheimnis standhält oder das Wahlergebnis transparent und nachvollziehbar ist. Anfragen bezüglich der

Prüfung des Wahlsystems an das BSI, das BMG und den Verband der Ersatzkassen (VDEK) konnten die Redaktionsschluss nicht beantworten. Das BSI verwies hier auf die teilnehmenden Krankenkassen. Wir müssen daher davon ausgehen, dass hier – verordnungskonform – eine im Hinblick auf die Wahlgrundsätze ungeprüfte Software zum Einsatz kam. In diesem Zusammenhang wäre ein Blick in den Vertrag mit Smartmatic interessant, inwieweit diese den deutschen Stellen überhaupt Einblick in den Sourcecode der Software gewährt hat.

## Envelope-Verfahren

Das TIVI-Wahlssystem funktioniert nach dem sog. Envelope-Verfahren. Dabei hat die Wahlkommission ein Schlüsselpaar aus öffentlichem und privatem Schlüssel (Public, Domestic). Die abgegebene Stimme  $S$  wird mit dem öffentlichen Teil verschlüsselt, dies ergibt  $P(S)$ , den inneren Umschlag. Der Wähler signiert die Stimme mit seiner  $eID$ ,  $sign(P(S))$ , dies ist der äußere Umschlag. Die Information, wer wie gewählt hat, liegt in der Urne, nur geschützt durch den privaten Schlüssel der Wahlkommission. Beim Öffnen der Urne wird zunächst der äußere Umschlag geprüft und der innere Umschlag mit dem privaten Schlüssel  $D$  der Wahlkommission entschlüsselt:  $D(P(S)) = S$ . Dann wird gezählt.

Es ist offensichtlich, dass der gemeinsame Besitz der Urne und des privaten Schlüssels  $D$  das Brechen des Wahlgeheimnisses ermöglicht. Auch ist ein Nachzählen durch Dritte nicht möglich, da diese dann die Information erhielten, wer wie gewählt hat. Damit erfüllt diese Sozialwahl gleich mehrere zentrale Vorgaben der Europaratsempfehlung nicht, v. a. die Standards 19, 25, 26, 29, 30, 34 und wohl auch 39. Aus diesen Gründen wurden bereits vor über zehn Jahren E-Voting-Wahlen in Finnland und Österreich von den Höchstgerichten aufgehoben und im UK von der obersten Wahlbehörde beendet.

Die bei der Sozialwahl eingesetzte „homomorphe“ (gemeint ist wohl semi-homomorphe) Verschlüsselung ändert daran nichts. Dabei wird (additive Verfahren vorausgesetzt) der Stimmzettel in elementare Ja/Nein-(0/1-)Entscheidungen

zerlegt. Für jede dieser Entscheidungen kann aus der Summe der verschlüsselten Stimmen das verschlüsselte Gesamtergebnis abgeleitet werden, also bspw. bei drei abgegebenen Stimmen  $P(1) + P(0) + P(1) = P(2)$ . Um aber an die Summe zu gelangen, muss wieder mit  $D$  entschlüsselt werden, also  $D(P(2)) = 2$ . Und mit  $D$  kann natürlich auch  $sign(P(1))$  geöffnet und dem Wähler zugeordnet werden – es stellt sich also dasselbe Problem wie beim reinen Envelope-Verfahren. Die in E-Voting seit über zwanzig Jahren wissenschaftlich ausgewiesenen Autoren sind überzeugt, dass Envelope-Verfahren ganz grundsätzlich ungeeignet sind, Wahlrechtsgrundsätze und CM/Rec(2017)5 einzuhalten.

## Fehlende digitale Signatur

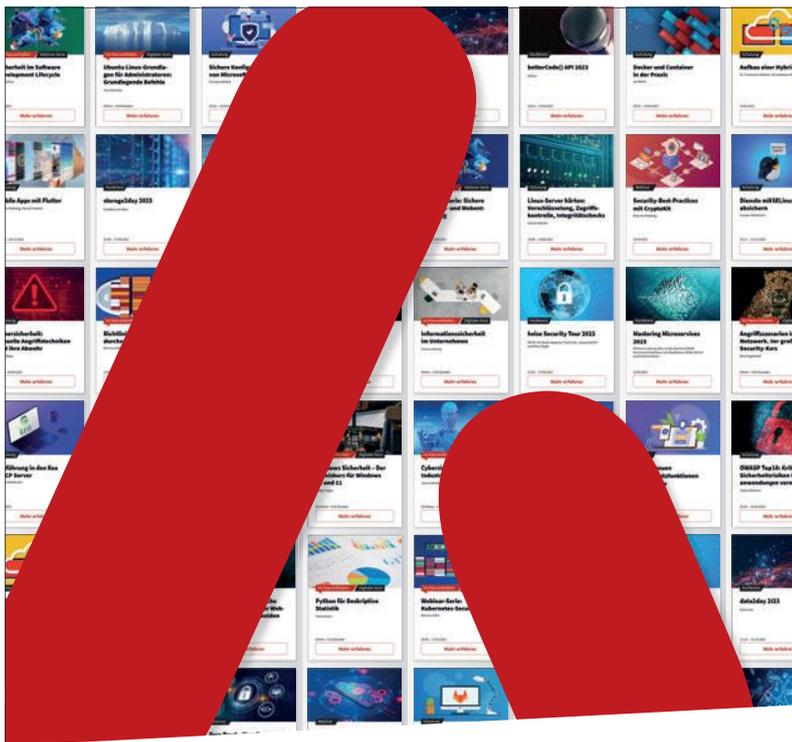
Ein weiteres Problem ist die Ermangelung einer tatsächlich verbreiteten digitalen Signatur in Deutschland. Es kann somit keine sicher vom Wähler erzeugte  $sign(P(S))$  wie etwa im estnischen Wahlssystem geben. Dieser Mangel zwingt die TR-03162 zu einer Vorgabe, die ziemlich befremdlich erscheint: Jeder Wähler erhält zusätzlich postalisch ein Wählerkennzeichen (WKZ) zugesandt. Bei der Stimmabgabe über die Wahlplattform sollen das WKZ und die verschlüsselte Stimme über getrennte Kommunikationswege abgegeben und gespeichert werden – technisch vermutlich durch Abgabe an zwei unterschiedliche Webserviceadressen realisiert (vgl. Abschnitt 4.5.2). Die verschlüssel-

„Leider hat man hier die Erfahrungen anderer Länder, Höchstgerichte und auch des Europarats sowie den Stand der E-Voting-Forschung negiert – wie bei so vielen gescheiterten E-Government-Projekten vom elektronischen Grundbuch über De-Mail bis jüngst zum OZG.“

te Stimme enthält beim Einlegen nur die digitale Signatur des Wahlervers. Damit ist jeder Form von Administratorbetrug, aber auch dem Einschleusen von Stimmen am Kommunikationsweg Tür und Tor geöffnet – und das System ist nicht einmal ein Envelope-Verfahren.

Die Autoren bereiten eine Journalpublikation vor, in der die Online-Sozialwahl und die TR-03162 einer ausführlichen wissenschaftlichen Würdigung unterzogen werden. Es stellt sich aber anhand der Vorgangsweise durchaus die Frage, ob den Beteiligten überhaupt bewusst war, dass ihr „Modellprojekt“ am Kern eines demokratischen Gemeinwesens rührt. Zusammenfassend muss festgestellt werden, dass dieses Projekt weit davon entfernt ist, ein Modell für Deutschland zu sein. Es fügt sich leider nahtlos in eine Reihe gescheiterter Digitalisierungsprojekte im öffentlichen Bereich ein.

\*Robert Müller-Török lehrt an der Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg, Alexander Prosser an der WU Wien am Institut für Produktionsmanagement.



## Wissenslücken? Nicht mit uns!

Wir helfen Ihnen dabei, die IT-Themen zu lernen, die heute – und morgen – wichtig sind.

### Die Zukunft des Lernens ist digital:

Die heise Academy bietet Ihren IT-Teams die Weiterbildungslösungen an, die Sie benötigen. Lassen Sie Ihre Fachkräfte nach Bedarf und direkt am Arbeitsplatz lernen.

Intensivieren Sie diese Lernerfahrung mit relevanten, topaktuellen Schulungen und Webinaren. Sichern Sie sich das IT-Wissen, das Ihr Unternehmen heute – und morgen – braucht: bei **heise Academy, dem Zuhause Ihrer professionellen IT-Weiterbildung.**

heise Academy

Jetzt entdecken:  
heise-academy.de

