uk engage

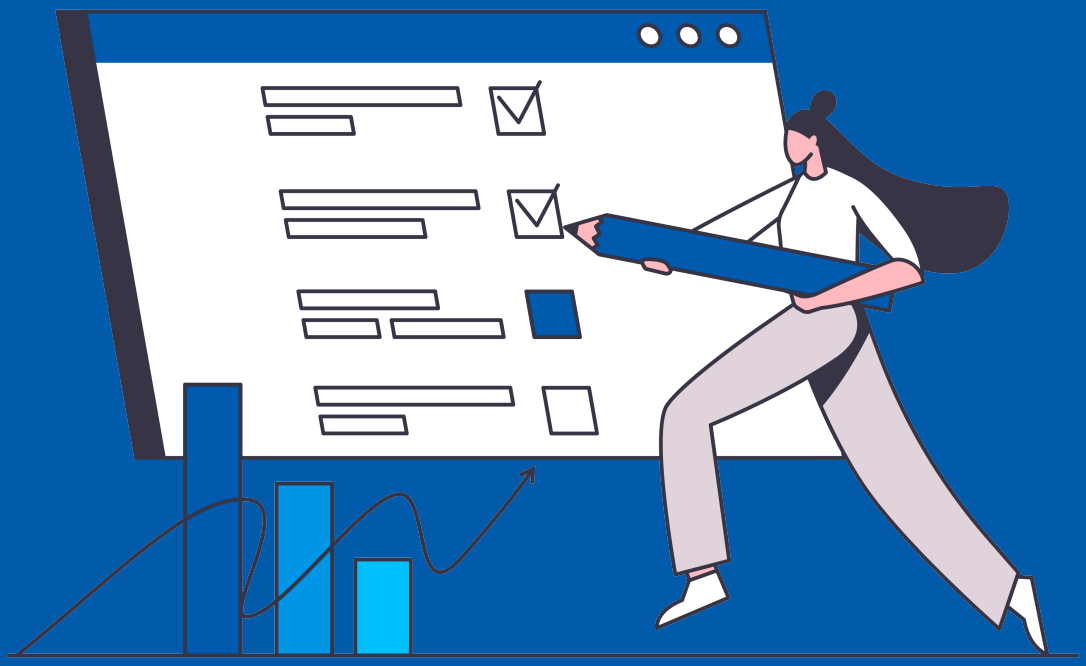
Democracy Driven by Print Image Network Ltd

End-to-End Verifiable Election Systems

Background

As online systems in general are increasingly targeted by 3rd party malicious actors, we look at how to protect future online democracy from such threats, whilst maintaining trust and user confidence in the election result and outcome. We compare the differences between the most used online voting systems today 'Trusted election systems' against 'End-to-End verifiable election systems'. Further aspects we consider include transparency, system features, trust/security and the user experience.

Online Voting



Trusted Election System

Trusted vs End-to-End Verifiable Systems

Who has access to what information?

Typically, an independent organisation is used to setup and manage the online election process. They can see the votes coming in, who has voted and how they have voted, they have access to all parts of the process at every stage. Those that have access to the administration of the online voting system are therefore trusted that they will not do anything that impacts the election result or the process. In the UK currently most if not all online election processes are provided as 'Trusted' solutions. Some organisations mention they have End-to-End online election systems and services, these are still trusted solutions whereby the organisation has end to end control of the process, however, are not comparable to a true End-to-End Verifiable solution.

Most online voting systems operate based on a trusted solution. This means that the security and integrity of the system is dependent on the administration team operating it. End-to-End Verifiable solutions are designed to remove any aspect of Administrator interference of the solution, giving the voter the ability to check the system directly. There are significant differences between the two types of solutions.

End-to-End Verifiable election system

Verifiable systems work independently of any administrator once setup and are locked prior to any votes being cast. At the close of the election, they can only be unlocked by those authorised to do so, and typically can include several authorised persons each with a part of the unlock key. Meaning that a number of those authorised persons must use each part of the key to unlock the results. During the election period voters, independent auditors, academia, and observers can check that the system is performing as expected using universal verification measures such as:

Cast as intended	**Individual verifiability:** Systems contain a mechanism for the voter to get proof the vote has not been changed during the process of casting the vote and ballot encryption process.
Registered as cast	**Individual verifiability:** Systems should include "append-only" publicly available bulletin board functions to allow voters to check their encrypted vote has not been altered or removed throughout the election process.
Counted as registered	**Universal verifiability:** The count process generates proof that certify the correctness of the calculated results. Meaning the election result corresponds to the content of all encrypted votes cast during the election process.

Systems also should offer considerable security controls to ensure no external interference occurs, these at a minimum should include:

Digital signature

These provide verification mechanisms that assure all cast votes come from eligible voters only. In addition, digital signatures certify the fact that no votes have been tampered with during the voting process.

End-to-End encryption

This ensures that under no circumstances results can be read without the necessary key(s) being used to unlock them.

Mix-net

A Mix-net is the virtual equivalent of a physical ballot box being shaken prior to opening to ensure the sequence in which the ballots are cast is mixed up. Also, the mixing procedure breaks any connection between a voter identity and their vote. After the mixing procedure, all votes are safely decrypted and are completely anonymised.

End-to-End Verifiable Online Voting

In the digital age, where virtually every aspect of our lives have become intertwined with technology, the call for modernising traditional systems has reached the realm of democracy. Voting, the cornerstone of any democratic society, has undergone a transformation with the advent of end-to-end verifiable online voting systems.

Imagine a world where citizens can cast their votes securely and conveniently from the comfort of their homes, using their smartphones or computers. The concept of online voting promises to revolutionise elections, making them more accessible, transparent, and efficient. But how does end-to-end verifiable online voting work, and what sets it apart from traditional methods?

At its core, end-to-end verifiable online voting employs cryptographic techniques to ensure the integrity of the entire voting process, from ballot casting to counting. Unlike conventional paper ballots, which can be susceptible to human error, tampering, or logistical issues, this technology utilises encryption and digital signatures to safeguard each vote's authenticity and confidentiality.

The process begins with voter authentication, employing stringent measures to verify the identity of the voter. This step is crucial in maintaining the security and credibility of the entire system, preventing fraudulent activities and ensuring that only eligible voters participate.

Once authenticated, voters can cast their ballots through a user-friendly online platform. Here, encryption techniques encode the votes, ensuring that they remain confidential and tamper-proof. Each encrypted vote is accompanied by a digital signature, uniquely linked to the voter, guaranteeing its authenticity.

One of the most significant advantages of end-to-end verifiable online voting is its transparency. Unlike traditional methods where the counting process may be opaque, this system allows voters to verify that their votes were accurately recorded and included in the final tally. Through cryptographic proofs, voters can independently verify that their encrypted vote matches the one stored in the system without compromising anonymity.

In conclusion

The concept of end-to-end verifiable online voting holds the promise of evolutionising democracy by making voting more convenient, transparent, and efficient. Advancements in technology and a commitment to security and inclusivity pave the way for a future where the democratic process is more accessible and resilient than ever before.

Trust and Security

Trust and Security

In the ever-evolving landscape of digital technology, the concept of online voting has emerged as a beacon of convenience and accessibility in the democratic process. However, the paramount concern surrounding this innovation remains its security. **How can we ensure that end-to-end verifiable online voting systems are robust enough to withstand potential threats and uphold the integrity of elections?**

At the heart of the debate lies the need for airtight security measures to safeguard against various vulnerabilities. End-to-end verifiable online voting operates on complex cryptographic principles, utilising algorithms to ensure the confidentiality, integrity, and authenticity of each vote cast.

One of the fundamental pillars of security in these systems is encryption. Votes are encrypted to shield them from unauthorised access or tampering. Each encrypted vote is accompanied by a digital signature, a unique identifier linked to the voter, allowing for verification without compromising anonymity. The use of robust encryption technology ensures that votes remain confidential throughout the entire process.

The decentralised nature of these systems adds another layer of security. By dispersing data across multiple servers or nodes, the risk of a single point of failure is mitigated. Even if one node is compromised, the entire system remains resilient, ensuring the sanctity of the votes cast.

To address these concerns regarding potential threats and hacking to any systems deployed, continuous and rigorous testing is imperative. Security audits, conducted by independent experts, help identify and rectify potential weaknesses in the system. Additionally, implementing robust authentication protocols and intrusion detection systems adds another layer of defence against unauthorised access or manipulation.

Ensuring transparency and auditability is equally crucial in bolstering trust in online voting systems. End-to-end verifiable systems allow voters to independently verify that their votes were accurately recorded and counted. Cryptographic proofs enable voters to confirm that their encrypted vote matches the one stored in the system, ensuring the integrity of the process without compromising anonymity.

In conclusion

End-to-end verifiable online voting holds immense promise in revolutionising the democratic process. Robust encryption, decentralised architectures, rigorous testing, and transparency mechanisms are pivotal in ensuring the trustworthiness of these systems. Addressing cybersecurity threats through continuous innovation and collaboration is essential to pave the way for a future where online voting is both secure and accessible, safeguarding the cornerstone of democracy.

User Experience

User Experience

The evolution of technology has permeated almost every aspect of our lives, and the democratic process is no exception. End-to-end verifiable online voting systems are a revolutionary means to make the voting experience more accessible, convenient, and transparent for all. But beyond the technical aspects, what does the user experience look like in this transformative approach to democracy?

Accessibility lies at the heart of online voting systems. Traditional voting methods often present barriers for individuals with disabilities or those living in remote areas. End-to-end verifiable online voting aims to bridge these gaps by offering a user-friendly interface accessible via various devices, allowing citizens to cast their votes from anywhere with an internet connection.

User authentication serves as the gateway to the voting process. Stringent yet intuitive authentication protocols verify the identity of voters, ensuring the security and credibility of the system. This step is crucial in maintaining the integrity of the electoral process while providing a seamless and trustworthy experience for users.

Once authenticated, the voting interface is designed to be intuitive and straightforward. User experience designers play a pivotal role in crafting interfaces that are easy to navigate, with clear instructions guiding voters through the ballot. Visual aids, and interactive elements help streamline the voting process, making it accessible even to individuals with limited technological proficiency.

Privacy and anonymity are paramount in any voting system. End-to-end verifiable online voting employs cryptographic techniques to ensure the confidentiality of votes while maintaining the ability for voters to verify their ballots. Through encryption and digital signatures, each vote remains anonymous yet verifiable, instilling confidence in the integrity of the process.

Transparency is a cornerstone of these systems. Users can independently verify that their votes were accurately recorded and included in the final count. The system provides proofs allowing voters to confirm that their encrypted vote matches the one stored in the system, enhancing trust and transparency without compromising anonymity.

Ensuring inclusivity is vital and efforts must be made to mitigate the digital divide, ensuring that all demographics, including marginalised communities and the elderly have equal access to, and understanding of, the online voting process. This might involve offering alternative voting methods or providing support for individuals who face technological barriers.

In conclusion

The user experience in end-to-end verifiable online voting systems is a critical factor in shaping the future of democracy. By prioritising accessibility, intuitive design, privacy and transparency the systems have the potential to revolutionise the way we all engage with the electoral process.

Summary

End-to-End verifiable systems are built on prominent scientifically reviewed crypto algorithms. They provide full documentation, transparency, and auditability from end-to-end during the election process. They remove the human administration aspect of running an election and creating the result. Consequently, they can be audited and checked during the processes ensuring trust and credibility of both processes and the result.

Our Promise

To provide a customer service which matches and exceeds your current or previous supplier

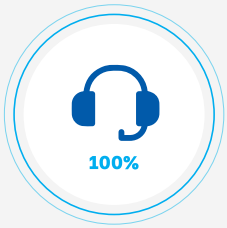
90% of respondents said we were an improvement on their previous supplier

10% said we were the same

0% said we weren't an improvement

To provide you with an excellent overall impression of our customer service

100% of responders said that we provided them with a 'good' or 'excellent' overall impression of customer experience.



To provide you with unrivalled project management and support by your dedicated account manager

Our account managers scored 100% for their project management and support

To make you want to continue to use us again

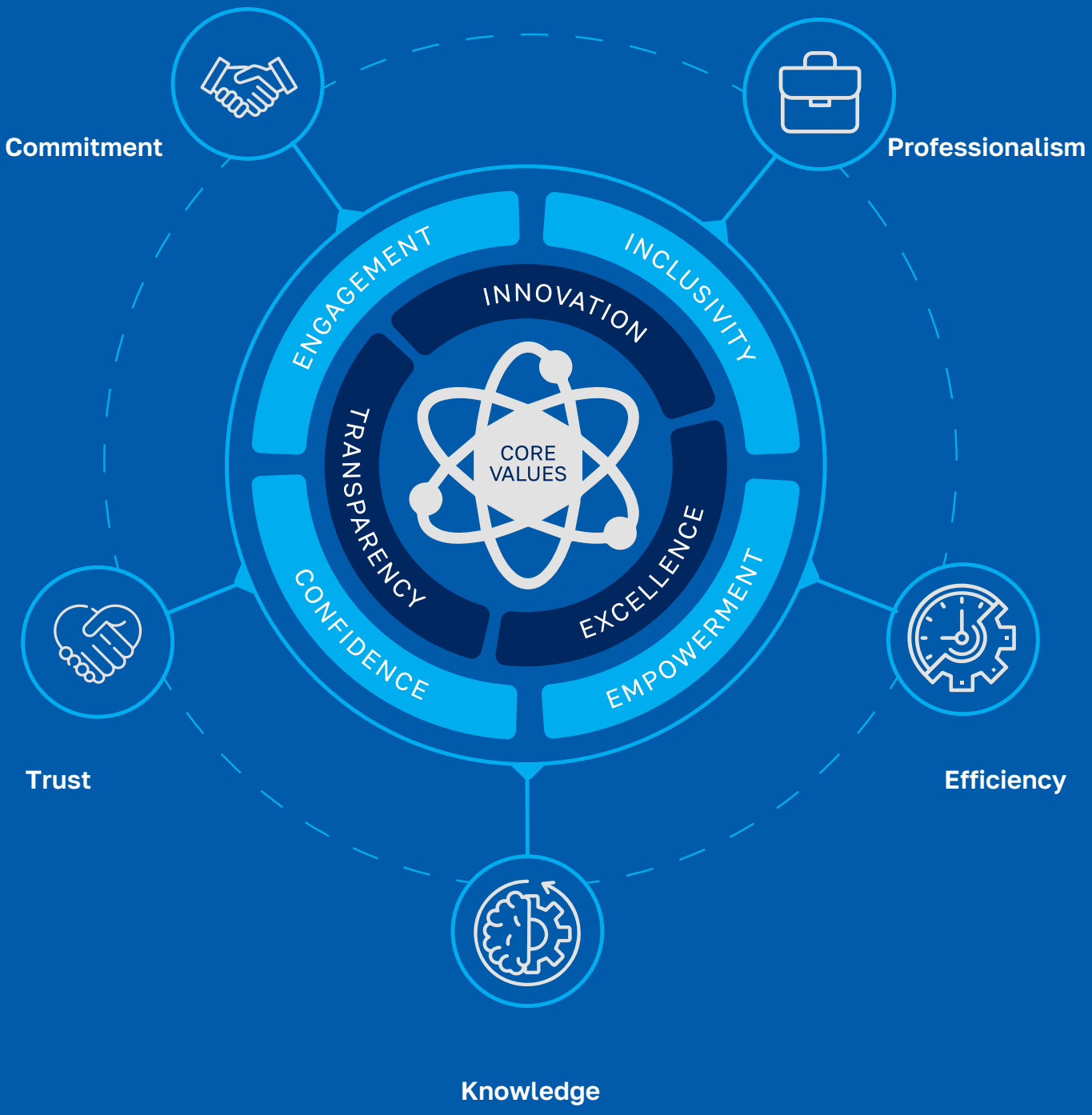
100% of responders said they would use our services again.

To make you want to recommend us to your industry peers

100% of respondents said they would give us a recommendation.

Our Values

Our employees are what make our business.
That’s why our core values have been defined entirely by our team.



Our values don’t stop here; they ultimately shape the way we do business with our customers, our partners and each other. Our core values influence every facet of our operations.

UK Engage

Democracy Driven by Print Image Network Ltd

UK Engage are an experienced election services provider with both Trusted and End-to-End Verifiable solutions and a dedicated team of election professionals delivering elections daily. Both postal and online services can be provided as part of our ISO9001 and ISO27001 certifications.

Security guaranteed

With encryption protection, multi-factor authentication, data security and secure servers, you're in safe hands.

Unrivalled customer service

We hold the Customer Service Excellence Standard (CSE) and have a 100% customer satisfaction score.

User friendly

You'll find all our systems are mobile-friendly and easy to use even for those who aren't tech-savvy, making voting an enjoyable experience for all.

Bespoke to your brand

The platform can be customised for your brand or group identity complete with image and logo, helping to further inspire confidence.

Contact us on 0161 209 4808 to discuss your requirements.

ISOQAR REGISTERED

CUSTOMER SERVICE EXCELLENCE CSE

CYBER ESSENTIALS CERTIFIED

Greater Manchester Chamber of Commerce

Crown Commercial Service Supplier

FSQS REGISTERED

Manchester Digital