Submission for Digital Democracy Commission

Setting out an approach for Electronic Voting

Matthew Margetts

Client Services Director – A&O

Microsoft UK**

Statement of intent

The purpose of this document is to set out an approach for delivering an electronic voting system in the UK by 2020.

The document is written without prejudice and whilst reference will be made to suppliers and brands this is not a sales pitch much less a technical specification, but is intended to provide guidance on how in a cost efficient manner a secure voting platform can be introduced into the UK ahead of the timeframe set out.

Subject to review with the appropriate parties the intention is provide a comprehensive scope of works document to support the introduction of such a system.

All ideas expressed herein remain the property of the author and the author's employers and may be not be published, in whole or part without the author's written permission. Punitive measures will be sort against any person and organization using the material herein contained for all commercial applications or commentary, without written approval by the author.

Executive Summary

The task of introducing a voting platform for General, Local and Mayoral elections can be broken down into 4 distinct challenges:

1. Identification
2. Security
3. Adoption
4. Verification – the voting process

Electronic voting is not (initially) seen as a replacement for existing forms of voting:

- In person
- Postal

But as a compliment to these services and as a means of engaging with a wider voting base, only eclipsing these methods over time as public demand grows.

The investment needed to introduce and service a voting platform has been based on creating a comparable cost to the postal vote and over time to realize benefits from the need for staffing in ballot stations

A digital voting experience can be introduced in via a Federation of parties acting in concert to deliver a common goal on a common standard (in principle) on a cost neutral basis

The Voting Platform Described

The intention is to deliver a safe, secure system of voting that allows members of the public to vote by using mobile devices: telephones and tablets, and from personal computers (PCs).

The system is intended to treat each vote – General Election, Local, Mayoral etc. as a separate occurrence and as such whilst the process of Identification, Security, Adoption and Verification will be the same for each occasion the user will be required to re-register for every vote; in effect the Application will close after each vote and a new App created per event.

The platform has been conceived as being politically neutral and will only carry information to the end user concerned with the process of voting.

As such the roll out of digital voting platform can form part a broader transformation process that enables the online citizen – both transactional (passport, driving license etc.) but also social and informational services.

The Process

In broad terms the process can be broken down into 4 key headings:

1. Identification
2. Security
3. Adoption
4. Verification

Each heading covers specific, linked challenges and solutions that will provide the foundation for the technical specification documentation that would form part of the ongoing consultation process.

Identification

The challenge for any system is to recognise and verify the identity of the user, unlike other systems that require online registration – for example an Microsoft user account, voting requires a double guarantee of proof: firstly for the identity of the user and secondly for the user to a specific device.

The risk in meeting this challenge is to look to devise a new set of protocols and inputs around personal data without frustrating the consumer or creating liabilities around management. The solution therefore is not to build a new system but rather adopt existing, trusted processes and adapt them for purpose; the answer is to use retail banking identification processes and scale out to the users.

Over the past 2-3 years the UK banking sector has invested heavily in online account management partly in a bid to save money and partly in order to better manage customers and their information. Whilst the adoption of online account management by customers varies from institution to institution the protocols are in place for millions of individuals to access their accounts digitally.

The coverage of the UK population offered by the banks (approx. 94%) is significant and therefore provides a cornerstone for the roll out of UK online voting.

The process would see individual looking to vote online as being verified through their bank. An individual would on visiting their account details behind the secure firewall of the bank be offered the opportunity to download the voting APP – this will require the Government and the banking sector to agree on the credentials necessary to prove an individual ID is accepted by both parties.

As part of the App down load the individual would be sent a text – to their nominated mobile account number by their bank confirming that they were downloading the APP and containing a unique password that would act to unlock the application.

The sending of the text in addition to being an added level of security will also act to verify the device. Furthermore if the voter is tied to this one device then the system is additionally secure – they have 2 factors – the password and the device. If they lose the device then they need to go through registering another or be passed directly to the Electoral Commission for reinstatement of the in person option.

The individual can only download the App once.

As the APP is downloaded at activated a message, synchronized through the bank's systems is sent to the Electoral Register notifying them of the individual's decision to vote electronically.

As a matter of choice the user may opt to change the user name and password on the front of the APP but the unique identifier of the data package would be set: Individual, individual address.

The federated approach of using the banks to validate and transmit the APP acts both to reassure the consumer on the integrity of the system and to provide validation that the person and device are genuine.

Moreover, the approach provides a benefit to banks and a further benefit to Government; for the banks it provides an enhancement to their services and encourages the further adoption of online services – *for example Barclays Digital Eagles programme*. For Government it provides an engagement opportunity around the digital passport and a protocol for mass adoption.

For example the Government's introduction of the Digital ID for vehicle licence renewal already sees the use of an ID albeit provided by a third party provider – Experian, Callsign etc. The concept is to evolve this process and recognise that a bank acts as the primary custodian of an individual's identity and as agreed with the consumer support the delivery of services.

Security

As the responsibility for the identification of the voter lies within the banking system the security issues are around the safe transfer and recording of the vote itself.

The process of voting, is based on the download of an App which, with the text security message acts to lock down the voter to the device. The device is being used as a second factor to bolster security, it makes for excellent security with a slight loss of usability. The App itself will only display candidate information relevant to the individual's address as recorded on their bank statements

The function of the App is therefore limited to candidate information and the ability to vote – a period which will correspond to the timelines set out for postal votes. The screen is therefore open to vote for a specific timeframe.

Once a vote has been cast, the data packet is transferred to a secure data area - the recommendation would be to work with an existing government supplier, housed on a proprietary server.

The assumption made it that the key used to decrypt the results is managed and **only released on the day of the election**. This requires a trusted party, *ideally external to the development of the process who provides the other half of the key.* This is standard public/private asymmetric key.

The mathematical puzzle of being able to time lock encryption does not have a useful solution from reading the literature

As with the Identification leg of the process the opportunity is to use existing suppliers and systems such as Azure Mobile Services that manage denial of service to ensure that the data is transmitted from device to server in a way that is safe from hacking. The data transfer is encrypted and should also be signed to prove validity.

As with the Postal Vote system the public will be made aware of how to approach the voting process, ensuring that their vote is a private affair and that they do not allow access to the system to third parties.

Adoption

The method described is heavily reliant on using proven technology to safeguard the consumer with an emphasis on using Financial Services Technology and process to manage voting.

The banks collective reputation for security acts to guarantee the integrity of the system.

Given the constraints in respect to accounting for people against the electoral register it is recommended that digital voters in the first instance are registered and their votes recorded – though not published, ahead of the polling day.

The described approach, furthermore should resonant with consumers as voting is in many ways similar to making online banking payments. The popularity of systems such as PayPal, Pingit and M-Pesa demonstrate consumers' willingness to adopt "utility" type apps to manage their affairs, so long as the process is proven to be secure.

The advantages of offering a digital voting platform, in terms of this document are focused around cost savings and benefits realisation through removing paper process and changing the staffing levels in polling stations.

A secondary set of benefits are that it might widen the level of engagement in the process of voting with certain demographics, specifically 18-24year olds.

Whilst voting levels for General Elections in this country remain around the 61-65% levels it is tempting to think that new platform may encourage more people to vote it would be naïve to think that the methodology is the blocker.

That said the popularity of making payments digitally is rapidly growing indicating that the methodology is sound, forty four percent of 2000+ consumers polled by Zapp* said they would be prepared to switch accounts if their current bank was unable to offer mobile payments and had no plans to do so. Of these, a third (33%) say they would do so within a year.

The research also found that enthusiasm for mobile payments has significantly grown over the last 15 months. Twenty eight percent of consumers have already used their phone to make a payment (up 64% from September 2013) and 59% say they would use their phones to pay if a simple system existed that didn't require extra set up.

Consumers say their mobile will become their preferred method of payment before the end of the decade for all kinds of purchases, including: sandwiches (51%); car fuel (52%); and travel tickets (57%). Almost half plan to use their mobile to pay for electronic products and one in five (20%) even say they would buy a house using a mobile payment.

Given the extent of the growth in mobile usage to manage utility functions the challenge with encouraging people to adopt online voting as the norm is not insurmountable; arguably it is playing to the trend.

The challenge as it exists is whether it will act to widen the engagement with Parliamentary process, and to educate consumers on the work of Parliamentarians outside of the reported political debates.

Certainly any opportunity to engage with the public on the topic should be seized as at the very least it begins a process of enquiry and research that may result in more people taking an interest in the day to day workings of Government, and associated bodies. And in turn drive consumer traffic to www.parliament.uk and www.gov.uk.

To this end the recommendation is to devise a public facing advertising campaign that acts to generate enthusiasm for the idea around the concept of the vote "being in your hand" and starting a process of engagement and education.

The campaign cost can be broken out as:

Cost of promoting the service

If a federated approach is taken via the banks and public facing government services awareness of the service can be brought to public awareness relatively cheaply as it would be promoted via these sites and given that there is a benefit in kind for the banks in delivering the message the communications line can be carried via existing channels.

Additional charges for advertising the service are covered in the Considerations section of this paper and are based on costs being offset by an income or benefit in kind to the App promoter.

Cost of download.

In the first instance this is met by the consumer under the terms of their mobile or internet contract. The data file though is likely to be relatively small so the cost of download, activation and delivery (voting) is likely to be negligible. Ultimately the cost of the download and the transmission of data could be offset against the cost of the postal vote and refunded via their bank to the user.

Cost of reconciliation

The benefits realised through the removal of cost at both the local ballot level and the cost of supplying and monitoring postal voting should act to make the system cost neutral.

An electronic vote is automatically machine counted removing the cost of human error and is directly auditable. Equally the cost of posting out and returning a vote is removed.

Whilst for the most part the aim is to reduce cost within the election process some unique costs will be generated such as the cost of raising awareness of the platform to the electorate.

A further consideration will have to be made for the cost of establishing the design of the voting interface. Whilst the design of the App is relatively simple it will require a design house to set out the experience and will have to be built to work across all devices: Android, Blackberry, IOS and Microsoft.

Furthermore, it is likely that the overall party responsible for hosting the delivery of the platform (recommendation: Electoral Commission) will have to provide both a web based Q&A as well as a call centre support – again it is probable that the cost of these services can be met within existing budgets as the platform acts to remove costs in the existing system.

The voting App will have to be designed to work on the principle mobile and devices platforms: IOS, Android and Win 8, and in respect to functionality the recommendation again is to borrow from existing banking payments systems, and to make the App work around 4-5 screens:

- Sign up and pass word screen
- Candidate list
- Vote
- Vote confirmation – confirming vote
- Despatch and thank you

The App would be live for an agreed period prior to the General Election.

In the case of a lost device – mobile or PC once the APP had been downloaded, a protocol notification could be introduced that would allow the individual to vote in person. The technology to link to the Electoral Register is again proven and it would be a matter of mapping out the process. Again it is likely that the circumstances would require a period of at 24hours prior to the election in order to qualify.

As with the Postal Vote all notices would stress the idea of privacy and responsibility of the individual to take charge of the matter and act in way that did not make their vote the property of others.

Verification

The voting process is straightforward and follows a proven pathway of using an encrypted message – the vote, that is then consolidated at a secure location and finally unlocked.

The vote is sent via a private key – embedded in the APP at the individual device level, and using a public key read by a government vetted, yet independent party (Logica, Fujitsu, etc.) who allocate the vote to the corresponding party.

As with the identification process the intention is to make use of existing, trusted partners who operate under agreed protocols and who have worked with government. The safeguards are in effect built into the voting process by using existing norms.

Moreover, it would, under current circumstances be a challenge for anyone to download the App on the day of voting or at least 36 hours prior as the registrant has to be accounted for on the electoral roll. Over time the vote timings can be extended to allow votes to be cast on the day.

Whilst the description of the process has tended to be built around the use of Smart phone Apps the service can be extended to PCs on the basis that using an ordinary mobile phone to download a pin the APP can accessed online.

Votes would only be unlocked and recorded after the closure at 10PM of Ballot Offices or in line with agreed timeframes

Further considerations

The process set out is aimed at being a low cost, straightforward in its implementation approach. Moreover, the wholesale adoption of Electronic voting presents some unique opportunities.

Ownership of the Platform

Whilst ultimately the platform and process should be owned by the Electoral Commission as part of the cost reduction/recovery process the services could be offered out to foreign jurisdictions under licence.

The application and sale of the services would be offered by one of the partners in the process and income earned shared back in part to government

Targeting of registered voters

Whilst the cost of promoting the system can be met as part of the overall promotion of voting methods the opportunity exists to sell access to those individuals who have downloaded the APP - in accordance with existing guidance regarding advertising around personal data.

No data based on voting behaviour would be offered for sale post-election and as the App would go dark immediately post-election the targeting segment would also be expunged.

Scaling of system

The system is scalable out to anyone who has a bank account – approximately 94% of the population. And as the use of APP technology grows, as it will do based on the increasing use of Telematics to manage and monitor lifestyles it is likely that the approach can be expended out to cover paperless voting as a new ballot experience. Individuals casting their vote in a Ballot office could be presented with a tablet device to vote with, again acting to reduce ballot counting fraud and speeding up the process of counting.

Exporting the system for use in other markets.

As identified earlier as the process described relies on using existing technology it is likely that the approach could be translated in to other markets; particularly those with high penetration of digital banking transactions. Providing services and savings as well as in emerging markets a barrier to election fraud.

The UK would act as a case study or example of best practice effectively endorsing the approach and process and so providing a touchstone for other countries or bodies looking to adopt digital voting.

Ultimately significant cost savings arise by moving a population to a digital engagement using a verified digital id so it is likely that foreign governments would be interested in making use of a system developed by the "Mother of all Parliaments".

System upgrades.

The process is built around natural redundancy, after each election the App is scrapped, and learnings around consumer experience taken into account and put into practice for the next time.

The benefit of this system is that it removes the need to continually manage legacy systems and invest in technology that might be supplanted by a better provider in the 4 years between elections. The optimum is to devise a system whereby the delivery is scaled up to suit and that investment is focused on building an interface API that is compatible across devices and mobile operators.

The cost of managing this can again be met from either the sale of services to third parties – the cost of delivering a managed service in a foreign jurisdiction provides both improvement learnings as well as an income stream.

References:

****

Author contact:

Matthew Margetts

Client Services Director

Microsoft A&O

Cardinal Place

100 Victoria Street

London

SW1E 5JL

**ZAPP – Research as reported in Fin Extra December 2014.*

The author acknowledges and is grateful for the support of colleagues at Microsoft in debating and consulting around the ideas expressed herein.