Mobile eDemocracy and voting

L-F Pau, Prof. Mobile business, Copenhagen Business School+Rotterdam School of Management

lfp.inf@cbs.dk

Abstract

Combining theoretical results in eParticipation, and the capabilities for e-Identity electronic identification and authentification offered by wireless access terminals, this paper focusses on Mobile eDemocracy, defined as the capability to exercise governance and to vote using mobile terminals and infrastructure. It is shown that Mobile eDemocracy, and voting via the mobile phone, offer significant advantages in terms of speed, security, governance and costs over voting by Internet. Experiments are surveyed across 7 european countries, as well as some lessons learnt from elsewhere in the use of Mobile eDemocracy. It is also discussed how this capability is not just relevant in public elections, but also in business and social governance processes such as votes at shareholder meetings and in social communities, thus enhancing the commercial prospects for appointed service suppliers. The known reasons for skepticism are addressed, as are the conclusive technical feasibility strong points, including in terms of multi-country interoperability. References are provided.

Introduction and COST WG2 alignment

- « Communications is an economic ressource and a right » (S. Mendonça , COST Workshop Stockholm); WG2 work on social tariffs for the needy has dealt with the rights to communicate linked to social status, but not yet with citizen rights in general as enhanced by communications.
- WG2 work on mobile payments and related regulatory changes (COST Workshop in Paris) was hinging on security and identification features enabled by infrastructure and multi-usage wireless access terminals (COST Workshop in Rome).
- ICT 2015 policy agenda (COST Workshop in Stockholm) mentions Soft Infrastructure , and eGovernment, but restricts governance to « how to balance openess and transparency with the private interests of the different stakeholders »
- Public Governance, much in need, does not exploit the mobile systems capabilities, incl. in privacy management (author's IEEE paper) .
- e-Identity on wireless terminals is becoming a capability, business and offers interoperability solutions

eDemocracy via Mobile terminals

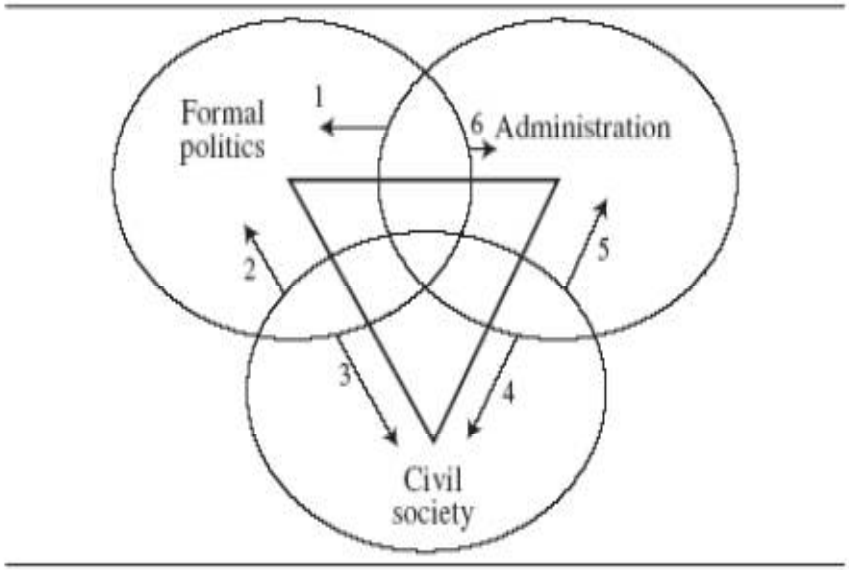
- **Scope:** Use the identification & authentification technologies and processes linked to wireless access terminals, to allow their owners to vote (public elections, company AGM's, unions and social groups) and possibly to get involved in opinion polls and debates.
- **Motivation**:

a) in most countries with civil registries , adoption rate for mobile terminals is higher than the existence of national ID cards;

b) this capability would empower citizens views and rights for better governance in the public as well as commercial spheres;

c) the requirements from the above on the user interface are compatible with the use and terminal's ubiquity+graphical interfaces.

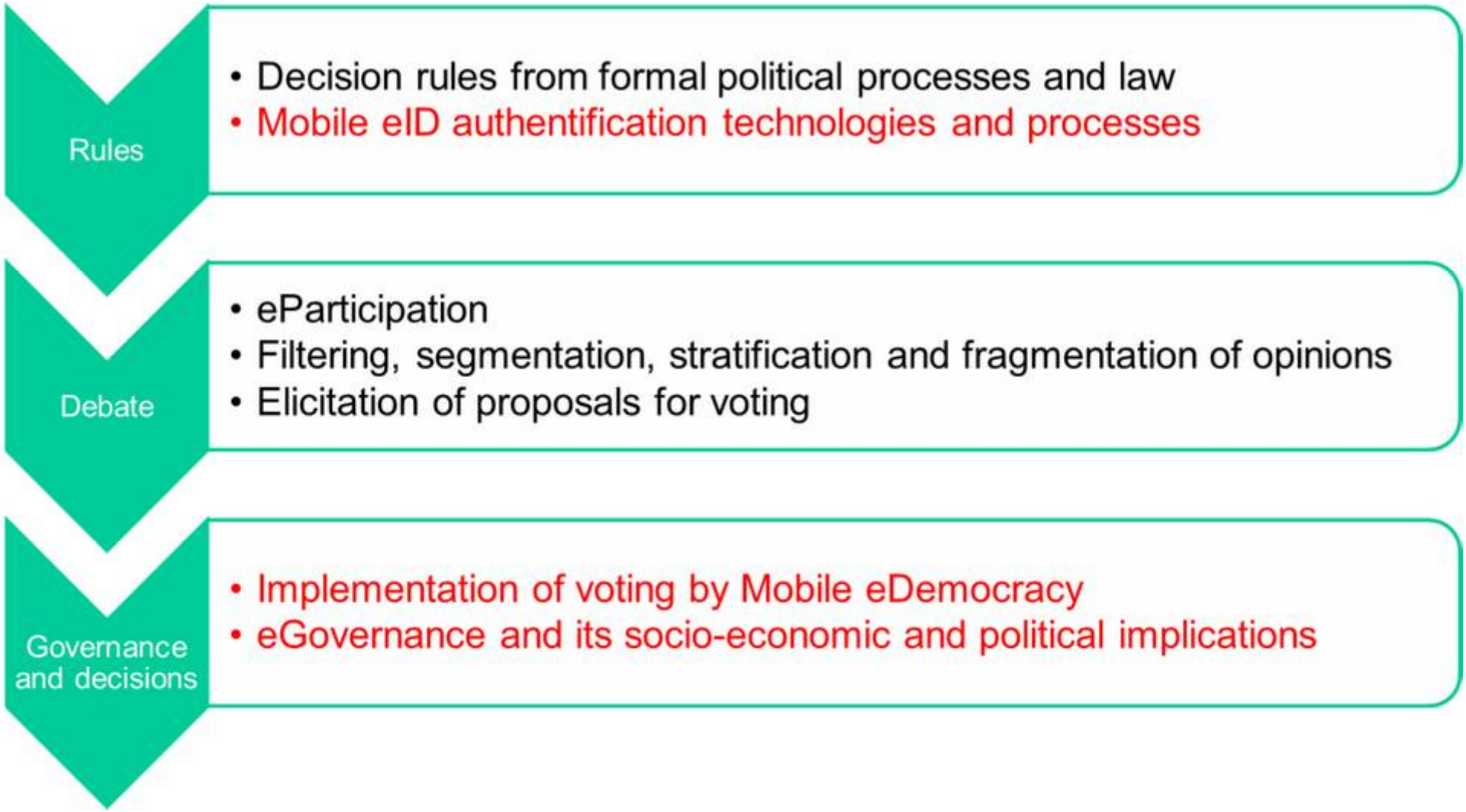
eDemocracy process steps



Mobile enabled process steps:

- 4: Administration issues questions for a vote upon a Formal political decision received in Step 6 (possibly after an eParticipation process 2+3 mediated by the Administration in Step 1);
- 5: Citizen votes on the questions received in Step 4 (possibly after an eParticipation process)

Hierarchy of eDemocracy concepts

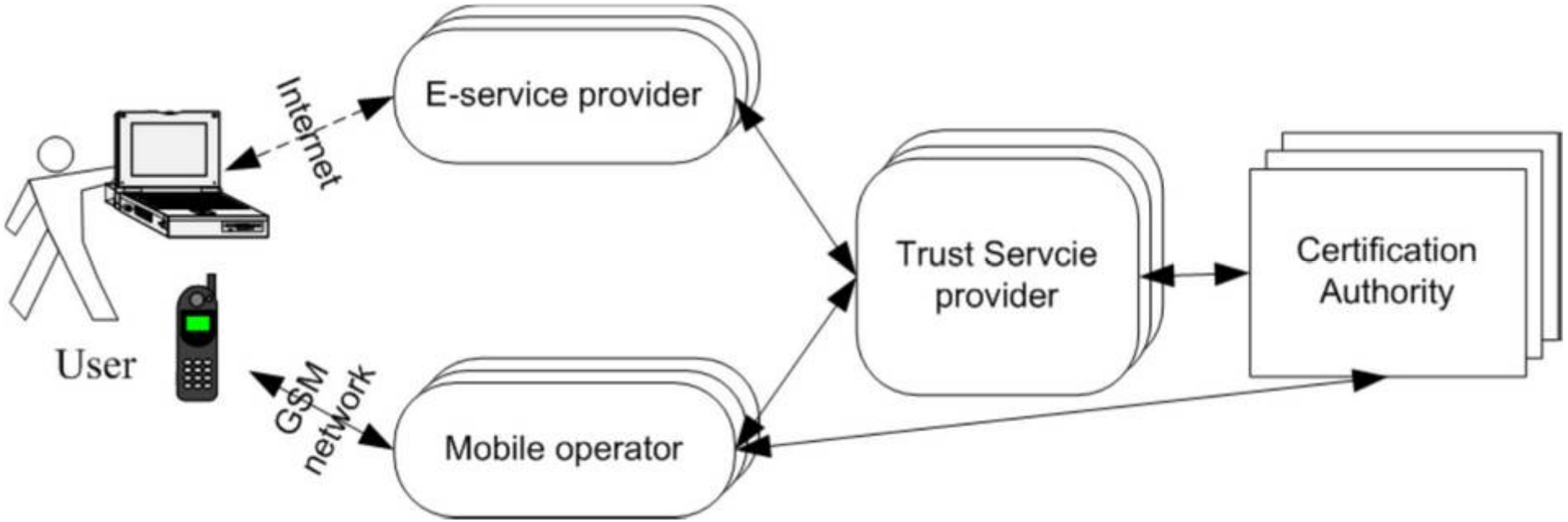


Red: Addressed in this research

eDemocracy : Case of Estonia

- Extensive eGovernment platform in Estonia
- eVote in place since 2005 from computers using ID Kaart (double PIN code, distributed to 90 % of population) + card reader
- 1 st PIN is for identification and 2 nd to confirm vote; one can re-vote for one full week with only last vote accounted for; manual physical vote can override electronic vote
- Usage: 16 % for European elections in 2009 vs 2 % for municipal elections of 2005
- Fear for denial of service attacks
- Certified card issuer SK
- Voting error rates in line with those of manual votes

eDemocracy: Case of Estonia (II)



Authentified user sees the resolutions and enters his votes on the mobile access terminal; user gets outcome same way ; this service can co-exist with service from fixed access points

The “cultural” scepticism arguments

- “Mobile voting is not for all”: obvious
- “I have no trust in any electronic voting” : this is a generation issue mostly
- “They will listen in on my vote”: hard to crack many more or less simultaneous encrypted votes
- “2 % error on the votes is unacceptable”: paper votes have higher error rates but people don't know
- “Mobile voting is dangerous because too direct and fast” yes for vote riggers”
- “eDemocracy is very costly and projects always failed “: Mobile voting is very very cheap, reduces need for voting posts, and extensive traceability is provided

Other experiences in eDemocracy

- Switzerland: eVote possible but unsafe as code is sent by email; for strange reasons max 20 % of voters can eVote on Cantonal elections with required double majority;
- Norway: building up a capability
- Finland : trials in 2008 but little user uptake and much policy-maker scepticism, with many mistakes on Internet terminals set up at physical voting sites (2 % errors in Grankulla, vicinity of Helsinki); there are though polls to identify preferred candidates (“candidate selector function”), but voters can change their mind at voting time...)

How Mobile eDemocracy differs from Internet eDemocracy voting

- Higher level of citizen and user inclusion than fixed terminal based voting
- Offers the capability of real time situation dependent voting, due to simpler and faster assembly of the texts of proposals
- Scalability and shorter emissions delay offered by Cell Broadcast functionality in 2G/3G/4G
- Far lower exposure to virus and spam risks in ensuring receipt of voting forms
- More frequent potential business exploitation for trusted operators thanks to commercial opportunities (AGM's, mobile marketing feedback, etc) , than the few public vote usages over a given time period
- Unexpected true governance side-effects

Cases of unique Mobile eGovernance aspects : Africa

- Ghana elections in 2000 : radio stations urged population to SMS irregularities or attempts for intimidation
- Zimbabwe elections f 2008: it took government 3 months to falsify the results because the real election results were sent from voting stations by mobile, faster than the falsification time..
- Iran, Ruanda: Twitter and SMS heled in the first case and could have helped in the second time

eParticipation : Theoretical model

- Different e-participation user groups co-construct technology through the use in practice of interaction platforms
- “Sensemaking” (Weick and others) is the primary theoretical framework for eParticipation with a special focus on situation-specific cue-frame-relations. Weick sees technology as « equivocal » in the sense that it allows for many different interpretations and therefore also for many different usages (Weick et al, 1990; Weick, 2005) .The individuals shape the technology (here the eParticipation platform)
- eParticipation supports the use of technology in democratic processes (called eDemocracy) (Grönlund, 2003a; Chadwick & May, 2003; Hoff, et al., 2003; Sæbø & Päivärinta, 2005; Olsen et al, 2002; Tyles, 2004).
- In a broader sense, eParticipation covers the involvement of the citizen in the development and provisioning of e-services (Macintosh, 2006; Ekelin, 2007;Löfstedt, 2008; Roeder et al., 2005; Bingham et al., 2005).

Cases : on-line mobile debate fora (e.g. Twitter and others)

- Mobile messaging social networks show how politicians and the administration use online debates.
- Politicians and the administration participate in very distinct ways in the debate fora and thereby create specific forms of citizen communication and participation.

Mobile eID for citizen authentification

- "Electronic Identity" is defined as : “a collection of identity attributes in an electronic form”. Electronic identity only becomes legally recognized when linked to the identity issued by the national authority entrusted with said legal executive powers (typically Ministry of Interior, or Social security administration, or Ministry of Defense, etc) . Electronic identity can also only be recognized and trusted inside a specific company or community, etc . These attributes specify characteristics, like a name, a membership, a role or any other information suitable to uniquely identify a person or a thing.

- The term "mobile electronic identity" implies these electronic identities to be portable. This involves device and user mobility, meaning that the service can be accessed with a device while moving as well as that a service can be used independently from device and location .

- The mobile devices must have security features such as : a) the mobile device's memory (software), b) an internal card such as a Universal Integrated Circuit Card (UICC) containing the Subscriber Identity Module (SIM) application (non-removable hardware), c) a secure hardware chip that is typically accessed by a ISO/IEC 7816**7** smart card standard compliant protocol, the same also used in a phone's SIM card, d) SD or microSD card (removable hardware).

- Most of the case studies which have been investigated are based on additional cryptographic operations in the mobile device, such as amending the SIM by a crypto co-processor to fulfill the requirements of a secure signature-creation device (SSCD) needed for the creation of qualified signatures. There are also solutions where no functionality, in addition to what exists in widely deployed mobile terminals, is needed.

- Examples : + Access terminals with embedded RFID on SIM card , with RFID issued by same process as passport or national identity card , with asymmetrical security (reader operates with a public key, private key with crypto elliptical algorithm, and non programmable circuit elements) (Siemens, Gemalto, etc)

  +Mobile terminals with biometrics certified by national authorities

Authentification procedure

- A user wants to authenticate against a service provider.
- The service provider redirects the user to the authentication authority.
- The user enters his phone number and a password. The password is needed in order to prevent misuse of the service.
- The authentication authority transmits a TAN valid only for a short time period optionally together with a hash value of the authentication message to be signed to the clients phone via SMS.
- The user checks the authentication message he is going to sign online, and compares its hash value with the value he has just received.
- If the values match, the user enters the TAN together with the PIN related to his private key in a web form.
- The server signs the authentication message using the HSM and the PIN code provided.
- The result of this signature is sent to the service provider.
- The service provider performs a signature verification as well as a certificate validation.
- Upon a successful verification the service provider accepts the user's authentication.

Mobile eID solutions in Europe (I)

- Austria: A server-based signature solution that has been operational from 2004-2007

Starting with April 2004 Austrian citizens had the choice between chip card based eID solutions or the mobile-phone based "A1-Signatur" operated by the mobile service provider "Mobilkom Austria". The legal basis of the mobile solution was the E-Government Act (as for any Citizen Card) and in particular the Administrative Signature Regulation. For a transitional period it allowed for administrative signatures – a signature type that has been chosen for the mobile eID – to co-exist with qualified signatures. This regulation allowed – under well-defined security requirements – private keys to be stored on secured servers. When the transitional phase ended in December 2007, administrative signatures needed to migrate to the qualified signature level. The signature laws allow for solutions such as the mobile A1 Signature to provide qualified signatures, the mobile provider however decided to discontinue the service.

- Estonia: A wireless public key infrastructure (WPKI) recently launched in 2007

Mobiil-ID was launched in Estonia in Spring 2007 by the mobile operator EMT in cooperation with Sertifitseerimiskeskus acting as certificate authority (CA). There were more than 20000 SIM WPKI cards issued, approximately 9000 of these are active users. Two other mobile operators launched the service during 2009. The Estonian Mobiil-ID by its functionality offers an alternative to electronic functions of national ID-cards. Mobiil-ID enables providers of Internet services to identify users, and the users to sign legally binding documents, like bank transfers, etc. Currently all major providers of internet services support WPKI authentication including the biggest banks and also governmental portals. Mobiil-ID is issued in accordance with the Digital Signatures Act. The precondition to apply for Mobiil–ID is that the applicant has to hold a national ID-card.

- Finland: 1999 Sonera was one of the first to amend SIM by signature crypto-coprocessors

The Finnish eID concept is based on a Citizen Certificate serving as the citizen's electronic identity. This certificate contains the first name, the last name and a unique identifier which is automatically created by the Population Information System. In 1999 electronic eID smart cards containing personal information about the citizen as well as the Citizen Certificate were issued. Actually the Citizen Certificate is a set of two certificates, one for authentication and encryption and a qualified certificate for creating electronic signatures. In 2005 Finland introduced a SIM based mobile signature as a mobile alternative to the eID chip card. This service includes the mobile phone as a secure signature creation device for qualified signatures. The Finnish Government has supervised the deployment of the common directive of the ETSI-based mobile signature service standard, allowing Finnish mobile operators to offer mobile signature services. Since the service was intended to be used for electronic authentication by mobile phones, both for public and private sector applications, the Finish Population Information System (which acts among others as a register of residents) closely collaborated with two major mobile service provider, Elisa and Telia Sonera.

Mobile eID solutions in Europe (II)

- Norway: similar to Finland, Telenor started early (2001) to deploy crypto-SIMs

In 2001 Telenor developed a SIM based mobile signature implementation (the security elements are located on the SIM card) originally aimed at mobile commerce. Since that point in time each SIM card shipped by Telenor was equipped with PKI functionality providing half of the Norwegian population with mobile authentication/signature capabilities. These SIM cards produced by Gemalto and Giesecke & Devrient provide 32 KB of RAM as well as an integrated key generation engine allowing the generation of 1024 bit RSA keys. Electronic signatures created by these SIM cards are based on the PKCS#1 standard using RSA and SHA-1. The SIM card solely contains the owner's private key. The public qualified certificate linked with the owner's private key is stored on a server provided by the certification authority. A verification authority may retrieve the certificate by using the particular SIM card's unique ICCID

- Sweden: Common WPKI specifications by Swedish banks and mobile operators

In comparison to standard PKI, WPKI is less a standard than an actual implementation, while PKI is a specification of an infrastructure. Regarding the actors of WPKI a mobile operator when involved is responsible for the following tasks: a) provision of mobile access b) issuance of SIM cards with WPKI functionality c) distribution of signature requests to the user and reception of signature responses from the user. WPKI allows cryptographic keys to be physically implemented in hardware, protected against tampering or alternatively allows an on-board key generation after the enrolment. Keys physically implemented in hardware provide a higher protection from being tampered; but since the keys are generated by the SIM card manufacturer, precautionary arrangements have to be made up in order to keep the private keys safe. On-SIM generated keys provide a slightly lower security factor but they also provide the advantage that private keys never leave the scope of the user.

- Netherlands: Digital authentication of citizens using the mobile phone as additional authentication factor

DigiD stands for Digital Identity and is an authentication system established in 2004 among Dutch public administrations. Each citizen with a unique Citizen Service Number (CSN) and with a registration in a Dutch municipality is able use the service in order to authenticate his/her electronic identity in the course of an application for electronic services. Traditional public administration basically depends on the unique Social Security Number (SSN). Since that number is subjected to various legal restrictions the Citizen Service Number was introduced which allows a much broader usage. The authentication solution is however not bound to use by the public administration. Organizations carrying out public tasks or organizations that are permitted by law to use the CSN are also allowed to equip their services with support for DigiD.

- Turkey: Turkcell launched a mobile signature service in 2007

One of the major benefits of Turkcell Mobile Signature is the fact that users do not have to buy additional tokens or other electronic gadgets. Instead of that they may use their existing mobile phones. The mobile signature is solely carried out by the mobile phone's SIM card. Nevertheless there are special requirements for the SIM card. In order to be able to use the service, SIM cards must be so called "SIMPlus" cards. Since SIMPlus cards provide plenty of memory in comparison to common SIM cards, the certificate is also stored on the SIM card. The certificates being used are qualified certificates issued by E-Güven, a Turkish Certificate Authority, in accordance with the EU's Digital Signature Directive as well as with the Turkish law.

Feasibility of Mobile eID authentification for eDemocracy

- In terms of security issues, an ENISA position paper has been issued that explicitly deals with security issues in the context of authentication using mobile eIDs. In order to complete the big picture several relevant standardizing organizations have been introduced, describing their tasks and their influence on mobile eIDs.
- In order to evaluate solutions already up and running, the mobile eID implementations of Austria, Estonia, Norway, Turkey, Finland, Sweden and The Netherlands have been investigated. Most of these solutions are based on similar technologies relying on mobile phones in combination with PKI enabled SIM cards providing secure elements.
- The main conclusion is that sufficient experience with mobile eID in e-government exists from the case studies. Mature technologies and solutions exist.
- Interoperability of national eID solutions is allowed by middleware or SAML 2.0 protocol enabled solutions such as STORK ; this makes it possible for nationals to be authenticated and to vote, when present in a STORK partner country different from the country of citizenship, using their national mobile credentials

Reference : ENISA Position Paper, "Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID)", Version 1.0.1 (final), 2008-11-21, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_mobile_eID.pdf (2009-04-27)

eGovernance implications

Public elections :

- Engaging large fractions of the population in a citizen-friendly way for otherwise low-turnout expensive elections
- Adding flexibility for citizens not in their normal residence at voting time
- Generation of electronic traces and proofs for later verification

Company and community votes (company AGM's, unions, parties, cultural and other associations, and communities at large:

- Reduce costs and increase potential frequency of votes for better governance
- Reduce dependency on proxies or clearinghouses , and resulting lack of transparency
- Empower boards by allowing them to validate views and decisions, but empowers also executive managements by allowing them to activate consultative votes

Social implications:

- Allow sick, displaced , rural or non-educated voters to participate thanks to higher mobile terminal « litteracy » than « textual litteracy »

Recommendations and conclusion

- Mobile eID solutions, plus interoperability platforms, empower efficient eGovernance, and must be promoted e.g. by European and the Commission
- When implemented and regulated they allow for better eDemocracy for voting in a public or commercial context
- Financial market regulators, could empower much better eGovernance by allowing share registrars to extend their services to AGM’s etc ; US far ahead
- Communities of all sorts, as well as Mobile marketing companies, can create a business and services around Mobile eDemocracy

For further reading (I)

BINGHAM, L. B., NABATCHI, T. & O'LEARY, R. (2005) The New Governance: Practices and Processes for Stakeholder and Citizen Participation in the Work of Government. *Public Administration Review,* 65**,** 547-558.

CHADWICK, A. (2003) Bringing e-democracy back in - Why it matters for future research, on e-governance. *Social Science Computer Review,* 21**,** 443-455.

CHADWICK, A. & MAY, C. (2003) Interaction between states and citizens in the age of the internet: "e-government" in the United States, Britain, and the European Union. *Governance-An International Journal Of Policy And Administration,* 16**,** 271-300.

CHANG, W.-Y. (2005) Online civic participation, and political empowerment: online media, and public opinion formation in Korea. *Media, Culture & Society,* 27**,** 925-935.

DOCTER, S. & DUTTON, W. H. (1998) The First Amendment Online: Santa Monica's Public Electronic Network. IN TSAGAROUSIANOU, R., TAMBINI, D. & BRYAN, C. (Eds.) *Cyberdemocracy.* London, Routledge.

DUTTA-BERGMAN, M. J. (2005) Access to the Internet in the context of community participation and community satisfaction. *New Media & Society,* 7**,** 89-109.

FOUNTAIN, J. E. (2001) *Building the Virtual State: Information Technology and Institutional Change,* Washington, D. C., Brookings Institution Press.

FOUNTAIN, J. E. (2003) Prospects for improving the regulatory process using e-rulemaking. *Communications of ACM*. 46(1), 43-44.

GIBSON, R. (2001) Elections Online: Assessing Internet Voting in Light of the Arizona Democratic Primary. *Political Science Quarterly,* 116**,** 561-583.

GOFFMAN, E. (1974) *Frame Analysis,* London, University Press of New England.

GRONLUND, A. (2005) What's In a Field - Exploring the eGoverment Domain. *Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 5 - Volume 05.* IEEE Computer Society.

GRÖNLUND, A. (2003a) Emerging Infrastructures for E-democracy. *e-Service Journal,* 2**,** 62-89.

GRÖNLUND, A. (2003b) Emerging electronic infrastructures - Exploring democratic components. *Social Science Computer Review,* 21**,** 55-72.

GRÖNLUND, Ã. K. (2002) Introduction to the Special Issue on E-democracy in Practice. *e-Service Journal,* 2**,** 3.

GRÖNLUND, Å. & RANERUP, A. (2001) *Elektronisk förvaltning, elektronisk demokrati,* Lund, Studentlitteratur.

HOFF, J., LOFGREN, K. & TORPE, L. (2003) The state we are in: E-democracy in Denmark. *Information Polity: The International Journal of Government & Democracy in the Information Age,* 8**,** 49-66.

KING, W. R. (2001) Envisioning the Future Impact of IT on Society. *Information Systems Management,* 18**,** 84.

For further reading (II)

LÖFSTEDT, U. (2008) e-Services for and by Citizens: Towards e-Participation and Social Systems Design for Development of Local Public e-Services. *Department of Information Technology and Media.* Sundsvall, Sweden, Mittuniversitetet.

MACINTOSH, A. (2006) eParticipation in Policy-Making: The research and the challenges.In P. Cunningham & M. Cunningham (eds), Exploiting the Knowledge Economy: Issues, Applications and Case Studies. IOS Press, 364-369.

MACINTOSH, A. (2007) eParticipation and eDemocracy research in Europe. In *Digital Government: eGovermenet research, case studies, and implementation*, (eds.) Chen, H., Brandt, L., Gregg, V., Traünmuller, R., Daves, S., Hovy, E., Macintosh, A., Larson, C.A., Springer, 85-102.

MACINTOSH, A., COLEMAN, S. & SCHNEEBERGER, A. (2009) *eParticipation: The Research Gaps*, In ePart 2009, (eds.) Macintosh, A. & Tambouris, E., LNCS 5694, 1-11.

MACINTOSH, A. & SMITH, E. (2002) Citizen participation in public affairs. IN LENK, R.T. A. K. (Ed.) *EGOV 2002.* Berlin, Springer-Verlag.

MACINTOSH, A. & WHYTE, A. (2006) Evaluating how eparticipation changes local democracy. IN IRANI, Z. & GHONEIM, A. (Eds.) *The eGovernment Workshop 2006.* Brunel University.

NORRIS, D. F. (2006) E-democracy and e-participation among local governments in the US. S*ymposium on E-participation and Local Democracy.* Budapest.

OUDSHOORN, N. & PINCH, T. (2003) *How users matter. The co-construction of users and technology,* Cambridge, MIT Press.

PFEFFER, J. & SALANCIK, G. R. (1978) *The external control of organizations,* New York, Harper & Row.

ROSE, J. & SÆBØ, Ø. (2005) Democracy Squared: designing on-line political communities to accommodate conflicting interests. *Scandinavian Journal of Information Systems, E-government special issue,* 17**,** 133–168.

SANFORD, C. & ROSE, J. (2007) Characterizing eParticipation. *International Journal of Information Management,* 27**,** 406-421.

SCHAUPP, L. C. & CARTER, L. (2005) E-voting: from apathy to adoption. *The Journal of Enterprise Information Management,* 18**,** 586-601.

SCOTT, J. K. (2006) E the People: Do U.S. Municipal Government Web Sites Support Public Involvement? *Public Administration Review,* 66**,** 341-353

SEGAARD, S. B. (2009) Veje til lokalt e-demokrati - organisering, mål, virkemidler og resultater. *Institutt for statsvitenskap.* Oslo, Universitetet i Oslo.

SVENSSON, J. & LEENES, R. (2003) E-voting in Europe: Divergent democratic practice. *Information Polity,* 8**,** 3-15.

SÆBØ, Ø., ROSE, J. & FLAK, L. (2008) The Shape of eParticipation: characterizing an emerging research area. *Government Information Quarterly,* 25**,** 400-428.

TAMBOURIS, E. & GORILAS, S. (2003) Evaluation of an e-democracy platform for European cities. IN TRAUNMÜLLER, R. (Ed.) *EGOV 2003.* Berlin, Springer-Verlag.

For further reading (III)

TORPE, L., AGGER NIELSEN, J. & ULRICH, J. (2005) *Demokrati på nettet : Offentlighed, deltagelse og digital kommunikation*, Aalborg Universitetsforlag.

UN (2005) UN Global E-government Readiness Report 2005: From E-government to Einclusion. UN.

WEICK, K. E. (1983) Managerial thought in the context of action. IN SRIVASTAVA, S.(Ed.) *The executive mind.* San Francisco, Jossey-Bass.

WEICK, K. E. (1990) Technology as equivoque: Sensemaking in new technologies. In GOODMAN, P. S. & SPROULL, L. S. (Eds.) *Technology and Organizations.* San Francisco, CA, Jossey-Bass.

WEICK, K. E. (1993a) Organizational Redesign as Improvisation. IN HUBEN, G. P. & GLICK, W. H. (Eds.) *Organizational Change and Redesign.* New York and Oxford,Oxford University Press.

WEICK, K. E. (1993b) Sensemaking in Organizations: Small Structures with Large Consequences. IN MURNINGHAM, J. K. (Ed.) *Social Psychology in Organizations:Advances in Theory and Research.* Englewood Cliffs, NJ: Prentice-Hall.

WEICK, K. E. (1995) *Sensemaking in Organizations*, Thousand Oaks, CA: Sage.

WEICK, K. E. (2001) *Making Sense of the Organization,* Malden, MA, Blackwell Publishing.

WEICK, K. E., SUTCLIFFE, K. M. & OBSTFIELD, D. (2005) Organizing and the Process of Sensemaking. *Organization Science*, vol. 16, 4:409-421.

WHYTE, A. & MACINTOSH, A. (2001) Transparency and teledemocracy: issues from an 'econsultation.'*Journal of Information Science,* 27**,** 187-198.

WHYTE, A. & MACINTOSH, A. (2003) Analysis and Evaluation of E-Consultations. *e-Service Journal,* 2**,** 9-34.