Fraser Henderson: www.particitech.com

Trust for the masses, authentication on the move

This paper explores the concept of trust, security, authentication and identity in relation to the requirements of the digital aspect of the European Citizens' Initiative (ECI) as ratified by the Lisbon Treaty. It draws on the similarity between ECI and petitioning, in particular pan-European petitions, as implemented by the EuroPetiton and eMPOWER projects.

Authentication is the technical component of the ECI whereas recognition and trust are of social and human construct. Possible solutions are explored in-line with the latest description of the ECI.

Principals of the ECI

The proposed ECI has a number of critical design requirements relating to its integrity:

- The validity of signatures must be assure by each member state (random sampling is suggested),
- The privacy of supporters must be upheld,
- The system should be secure and preferably able to detect fraud,
- It must be capable of action based on a set of defined thresholds,
- It must be easy to use and free at the point of use.

Initial Observations

Related information can be extracted from the suggested ECI template and includes a number of assets which can be logged by the system. For example:-

Requested	Hidden
Date	Time stamp
Personal Identity Number (e.g. passport)	I.P. address
Name (first and family name)	
Nationality	
City and postcode	

Thus, a number of desirable design characteristics can be formed, including:-

- A suitable privacy policy. This should include disclaimers relating to 'digital dust' or scraping of signees. We suggest that only the names and corresponding member states are revealed to other participants.
- Encryption, particularly where sensitive personal information is held in a database
- Failover and redundancy
- VeriSign (to assure authenticity of the site itself and circumvent Phishing)

Measures to prevent fraud include:-

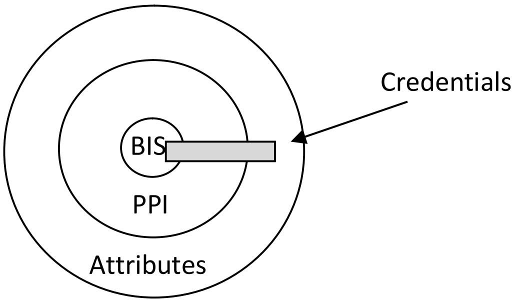
- Human only gates (to prevent automation of the submission process)
- Detection of rapid succession(although this could be triggered due to transposition)
- Signing pattern (e.g. by geography or time-line)
- Referral monitoring (i.e. where was the supported directed *from*)
- I.P. Logging (providing a basic level of traceability in co-operation with ISPs)
- Self certification

All of these countermeasures can be used to generate a level of certainty about a particular ECI or focus sampling. Each ECI could be assessed based on the above and:-

- For flagged (suspicious) ECI:-
    - Focused sampling
    - Manual checks (e.g. contacting the organiser)
- For non-flagged ECI, random sampling occurs

The identity and privacy relationship

The onion model below {future identity Ltd} describes the dimensions of identity. For the purposes of doubt, identity is what identifies you uniquely within a population.



In the centre of this diagram is the BIS (Basic Identifier Set) which is proof of uniqueness (e.g. your passport number). The problem with BIS is that it is unreliable.

Your credentials (the bar in the above diagram) encapsulate data from the various rings. Credentials try and take various segments of the onion to reliable identity.

Outside this is PPI (Other Personally Identifiable Information, e.g. your address).

The next ring is the Attributes. This tends to be the physical such as blood type, colour of eyes. This can be a mix of factors. However, this can also be reliable as it is susceptible to change over time (e.g. height or colour of hair)

Most people feel privacy is compromised when personal data appears out of context. Privacy is therefore maintaining integrity between the segments of the onion model above, ensuring there is no leakage. Privacy is how we manage the relationship between rings of the onion model.

In the digital space this has a tendency to get ignored (either there is no choice or the application is ill respecting).

Beyond the onion there are more layers, specifically DAO (Data About You) and DAPLY (Data About People Like You). This might include data on your behaviour (g. how long you spent on a page). In other words, with DAO you are categorised & other people categorise you. DAPLY contains information which is partly your behaviour.

With this in mind it is worth considering what privacy enhancing technologies can be applied to the ECI. For example:-

- Flags to prevent ECI data being indexed by search engines (data mining)
- The use of text based images to prevent data being indexed
- Consent in terms of what personal information can be treated as transparent

The EC funded project PRIME life looks at privacy in social networks and may be able to offer some guidance on this.

We therefore suggest that a digital ECI has:-

- A means for the ECI organiser to contact supporters a maximum of 2 times during the open period on the basis this is done through 'blind' copy
- For supports to opt out of allowing their name and nationality to be listed alongside support for any particular ECI
- Built-in mechanisms to prevent data mining

Technology challenges

Some member states already have nationalised digital identity schemes (e.g. UK, Government Gateway) and duplication might be resisted. **T**he main challenge is releasing data with the right controls and remaining control. Digital Rights Management (DRM) is actually what we would like to achieve with personal data.

The EDPS suggests that trust is only secured if ICTs are "reliable, secure and under individuals control", in other words, privacy by design. It is particularly important in this case as we are trying to preserve privacy beyond national borders. The main problem is that trust is regarded differently by different people and possibly, therefore, by different nationalities.

The ECI will only be as good as the weakest point in the chain, there is a real risk that rouge states could exercise direct democracy. Inter-state trust is therefore important and arguably the validity of signatures should be crosschecked at a central point or with reciprocal agreements between member states.

The following FP7 projects might already offer part of the solution:-

- GEMOM resilient infrastructure (preventing failover)
- STORK wider identity project
- FAST (digital certificates for secure transactions)

Digital certificates

One of the most reliable mechanisms for verification of identity is the digital certificate.

The main problem with them is issuing. For individuals to get digital certificates the process itself is reliant on some form of 'over the counter' or in-person identification. There is a real risk that the process of signing or setting-up an ECI becomes a burden and the benefits of online transactions are thwarted by a return to traditional means of authentication (e.g. face to face).

However, there are a number of ways in which the certificate can be held by an individual. One way is through the use of SmartCards, another is to provision them on a mobile device. The latter is a very real plausible option in terms of minimising the barriers to entry for a typical consumer. This trust mechanism could be issued in the form of a mobile application which receives your digital certificate over the air {additional identifiers include phone IMEMI, Network, Triangulation LBS and number}. The phone is wrapped with Bluetooth or RFID communication technology and a PIN code.

The mobile phone could be used to sign an ECI electronically (via a computer/web), over the air (via a mobile website) or in-person with a proximity sensing device. Moreover, the information exchange could be two-way allowing the phone to display information about the status of ECI's already signed.

It is conceivable that below the 300,000 threshold whereby an ECI is ratified there is no requirement for implementing any additional checks and balances. Above this, supporters could be retrospectively asked to verify their identity/support.

Hype in terms of the idea that trust is commonly abused can also create a backlash; as such services which adopt secure transactions need to be very clear about their rationale.

Other options

One of the most convenient mechanisms is biometric. However, few citizens have scanning devices and biometric s can be perceived negatively in terms of individual privacy.

Random Sampling

If the mobile approach was taken then phone number of all signees are automatically recorded. Moreover, SMS could be used in an automated two-way exchange which verifies a particular unique identifier (e.g. date of birth).

Conclusion

The use of digital certificates and mobile technologies are extremely powerful agents for achieving ECI authentication and trust, particularly as they enable a range of interactions and the two-way flow of information. A workable process is defined below:-

1. Certificate Issue / Registration. Options:-

- Register via PC, certificate issued to a mobile handset over the air
- Register in person, certificate issued to a mobile handset over the air
- Application layer downloadable over the air, from Bluetooth proximity nodes or installed via PC

2. Sign an ECI . Options:-

- With a PIN, application and certificate in person from a Bluetooth proximity node
- By SMS with the certificate as an attachment and PIN + ECI ID as message content (or via scanning of QR code)
- Using the ECI website directly on the phone (via phone browser)
- Using a computer with the certificate, provisioned by email after registration.

3. Monitoring / Sampling

- By SMS (asks for a unique identifier)
- By call-back (automated voice menu)

The net result is an improved security model:-

Requested	Hidden
Date	Time stamp
Personal Identity Number (e.g. passport)	I.P. address
Name (first and family name)	LBS (triangulated physical geography)
Nationality	Phone IMEMI
City and postcode	Phone number (and keepers’ address)
	Registered network