S

Problems in Mandating Strong Personal EOI in PKI

Doc no:

telwg23/ estg/07

ESTG agenda item:

eSecurity Task Group

Submitted by:
Australia

Problems in Mandating Strong Personal EOI in PKI

Contact: **Steve Orlowski**
Email: **steve.orlowski@bigpond.com**

APEC Telecommunications and Information Working Group
23rd Meeting I 12-16 March 2001 I Canberra, Australia

Problems in mandating strong personal EOI in PKI

Introduction

There is a view in some policy circles that all certificate holders should be subject to strong identity checks. This position derives from the concern that forensic investigation of fraud will be more difficult in e-commerce than it is in conventional business. Historically it may have been fuelled by the association of cryptography development and controls with defence agencies and national interest concerns. Furthermore, some of the earlier PKI applications were associated with government services like taxation and national health, which attract criminal sanctions in the event of fraud. This naturally leads to strenuous checks on personal identity.

Perhaps inadvertently, a strong onus on personal evidence of identity has carried over into PKI in general. Yet there are major problems and new risks introduced by what might appear to merely be prudence. This paper argues that there should be no minimum EOI mandated across-the-board in open PKI schemes, such as Gatekeeper. Instead, Certification Authorities in concert with their respective communities of interest should be allowed to set registration rules fit for the purpose of their certificates. It is not disputed that certain applications – such as social security, banking, and areas of national interest like defence, customs and immigration – have legitimate requirements for strong EOI, especially if criminal liabilities are attached. But these applications should be treated as communities of interest like any other, and left to decide what EOI standards are appropriate. They should not act to raise unnecessary burden of proof across all types of certificates.

What are the real requirements for EOI?

- In applications conferring criminal liabilities on the individuals concerned, strong evidence of personal identity is naturally warranted.

- On the other hand, in most business applications, civil liabilities are attached, and it is the company not the individual who carries the immediate risk. It is customary for businesses and organisations to decide for themselves what information they gather and file on their employees and members, to protect the business in the event of individual wrongdoing, and to equip the business to recover damages from those individuals. In practice, businesses weigh up all sorts of practical, ethical and legal considerations for and against the gathering of personal information.

- Very few employers in fact gather extensive personal identification on their people. Some might ask for a drivers licence number on an employment form but rarely is the licence actually checked. And yet employees represent their organisations in all manner of transactions. Plainly, the vast majority of routine business is conducted amongst parties that have not submitted to strong identity checks.

- Where is the threat assessment or risk analysis that shows that passport-level identity checks can be expected to mitigate real risks in regular e-business?

- In Gatekeeper, where is the analysis that shows that anti money laundering measures happen to carry over into risk management for *all* types of Internet business, including non-payments transactions like medical records?

- Early conceptions of digital certificates often assumed a one-size-fits-all certificate, which would have contributed to a conservative identity requirement. Now, the strong trend is towards application-specific certificates. Modern software benefits from sophisticated means for discriminating automatically between different types of certificates, which in turn allows for different communities of interest to set registration rules fit for purpose.

- Since we no longer seek a single certificate for all applications, it is no longer imperative that all certificates be equivalent. Rather, it is important that relying parties have the means to determine if a given certificate is fit for purpose.

- We should generally start with the assumption that existing communities of interest – employers, professional societies, trading groups and so on – have developed robust and secure membership processes, fit for purpose. Trust in the on-line world then depends only on the secure transfer of the fact of registration to digital certificates. This is best achieved by delegating RA responsibilities functions to the existing membership. Complicating existing membership processes will not improve the fidelity of the resulting electronic credentials.

New risks are imposed by strong EOI checks

- If an employer or professional organisation has to gather personal identification data where none was needed before, in order to electronically register its members, then it is taking on new, unfamiliar processes with possible legal ramifications and inevitable regulatory obligations.

- In non-financial applications, gathering strong EOI to register a user would appear to be in violation of the National Privacy Principle Number 1: "Personal information shall not be collected … unless … (a) the information is collected for a purpose that is a lawful purpose **directly related to a function or activity of the collector**; and (b) the collection of the information is **necessary for or directly related to that purpose**." (emphasis added).

Has the electronic passport metaphor outlived its usefulness?

- For years, it was simply assumed that a digital certificate *necessarily* entailed passport level identity checks. This assumption derived from the longstanding metaphor of certificates as electronic passports – an intuition as to what a certificate might mean. Crucially, the metaphor pre-dates modern e-business!

- A better metaphor is the certificate as electronic *membership card*. Business is often conducted on the basis of one's membership of some organisation, professional group, buying group, credit scheme, or other community of interest. Membership rules for these communities of interest are for the most part sovereign. The detailed membership rules are typically of no direct interest to others transacting with members of the group. Rather, in many cases such groups are trusted to implement proper rules, fit for purpose.

Conclusion

Instead of imposing strenuous EOI checks across the board on all certificate subjects in a PKI, communities of interest should be allowed to set their own registration rules, fit for purpose. There is no argument that some communities will set 100 point checks or even stricter identification standards, but equally, many will decide to apply their existing membership and employment rules to the issuance of digital certificates.

Now, if communities of interest managing digital certificates are to be allowed to vary their registration rules, how is a consistent level of trust to be maintained?

Note that in the past, the one-size-fits-all assumption meant that certificate equivalence was a central objective in constructing uniform registration rules. Now, with different applications using different certificates, the objective must be to ensure fitness for the intended purpose. This shifts the focus from uniformity of registration to uniformity of registration *controls*.

In most areas of commerce, where people rely upon the integrity of processes within some business, it is standard to invoke an independent audit of such processes. Mature and robust controls exist to ensure the quality of such audits, in all disciplines. You do not need to know the registration rules for doctors, lawyers, company employees, financial advisers, or auditors, to be able to rely upon them. Because they are all subject to trusted independent controls.

Most PKI schemes – whether they involve strong EOI checks or not – are in fact adopting information security audits to help improve their standing. This trend can be leveraged to provide for independent review and audit of a CA's registration rules – whatever they may be – in the context of the intended application of the certificates.