Request for an On-line (Web) Signature Standards Effort

Background: I have on behalf of a client, taken the liberty to investigate the state of client-side PKI support in web-browsers with respect to standards and interoperability. A major reason for performing this study was that we have found that none of the pretty large Nordic e-government initiatives and on-line banks actually utilizes the browsers' built-in client-side PKI mechanisms. The majority of these providers rather rely on Java applets developed by various ISVs. The reason for this is very obvious:

Practically every aspect of client-side Web-PKI, ranging from on-line key generation and certification support, to on-line (web-form) signing, is currently entirely vendor-dependent

The net effect of this is that costs are sky-high and interoperability is very limited. Most of the proprietary signature "plugins" available also requires signed NDAs for just accessing the documentation.

⇨ That is, we are as far away from a "standard" (de-facto or "real"), as one can possibly be ⇦

That it seems to "work" anyway, is because current on-line systems are *closed networks*, but this is in my opinion neither what we (=the SW industry), nor the consumers should expect to last forever.

Particularly e-governments and enterprise systems cannot depend on *artificial technological barriers* between the parties in an emerging "e-society".

What are On-line Signatures?

On-line signatures denote users signing data (typically in the form of web pages), when connected to on-line services like Internet banks, e-government webs, or company intranets. In such scenarios there is usually an interaction between the user and the service provider.

Is not signed e-mail (S/MIME) supported by just about every mail client?

Yes, X.509 (the global PKI standard) was essentially invented to support e-mail, *which is an off-line type of activity*. But the market has for many (good) reasons selected to rather use the web as the primary information exchange tool. *All Internet banks and e-government initiatives are to my knowledge entirely based on the on-line, real-time web paradigm*.

But is there any "market" for this?

At the time of writing (November 2003) only in Scandinavia, *millions* of consumers use digital signatures for performing on-line bank transactions over the web. In about 3-5 years from now (here assuming that a widely supported on-line signature standard really is created), there could be *billions* of *daily* users of such a system!

How is this supposed to be delivered and by whom?

It is in my opinion not enough that a standard is created, *this mechanism should eventually be an integral part of the default installation of every browser regardless of operating system or device.*

Do you have an idea of how such a standard could be engineered?

Yes I do but I consider this simply as "input" to a standards process that I hope will be populated not only by the leading SW vendors, but by knowledgeable representatives from banks and e-governments as well. Since the goal is really a new "core" web-standard, I believe the World Wide Web Consortium (W3C) is the most appropriate forum for hosting such an effort.

The most important PKI standard since X.509.v3?

Since on-line signatures and authentications are likely to be the #1 usage of PKI, it seems that a *successful* on-line signature standard effort (including on-line key-generation and certification support), could very well be the thing that makes the long-time awaited PKI "breakthrough" actually come true.

Sincerely,
Anders Rundgren, Consultant, PKI and e-Business
+46 70 627 74 37, anders.rundgren@telia.com

Stockholm, Sweden
November 2003