PrimeKey

"Two-factor Authentication for the Cloud"

One of the more prominent IT trends is the reliance on "Cloud" services. A drawback with this development is that users (be it in their role as consumers, citizens or employees), are faced with an ever-increasing number of passwords.

In addition being inconvenient, passwords have well-known security issues, particularly when used and created by an average, typically not very security-aware Internet user.

The standard "cure" for this is two-factor authentication. However, there are several impediments associated with two-factor authentication which have limited this to organizations having strong economic or political incentives for such measures. The following hurdles are the most apparent:

- No standard (or sub-standard) for on-line issuance of two-factor credentials like PKI
- Highly variant middleware and token schemes make deployment of suitable containers a pure guesswork for non-experts

That the most popular electronic device ever (the mobile phone), also lacks this basic feature is also a reason why two-factor authentication after all these years still is lagging. In theory this could be supported by the SIM-card but the SIM is exclusively controlled by the operators and is therefore more or less useless for general purpose usage on the Internet.

> All software needed for two-factor authentication, from *provisioning*, *management*, and *usage* of credentials MUST eventually be featured as a part of the computing platform, otherwise we might as well stick to passwords forever!

The author of this paper has worked with such a scheme since 2007 and is interested in hooking up with other parties set creating a better Internet. The project consists of two tightly matched components:

- **KeyGen2**. Browser-based credential enrollment and management protocol
- **SKS**. A universal container system featuring end-to-end security provisioning (which no browser solution to date do), transaction-based operation, issuer isolation, logotypes, and support for PKI, OTP, Information Cards etc

It appears that President Obama's recently announced NSTIC program would benefit from a low-cost and efficient system enabling large-scale experimentation with different approaches to secure identities, from state IDs to attribute schemes vouching for "over 18" and similar.

Submitter: Anders Rundgren, PrimeKey Solutions AB
anders@primekey.se, +46 70 720 91 02

A full disclosure of this open source project is available at:

http://webpki.org/auth-token-4-the-cloud.html