

Non-Technical Presentation Proposal  
Internet Safety Technical Task Force  
Public Meeting at Harvard Law School

\*Please submit completed form as a pdf to [jttatlock@cyber.law.harvard.edu](mailto:jtatlock@cyber.law.harvard.edu) with "Presentation" as the subject, no later than August 16, 2008. Please note that although the internal review committee will consider each submission carefully, a limited number of invitations to present will be issued, time permitting and based on relevance to the scope of the ISTTF's inquiry. The committee reserves full rights to make decisions in its sole discretion. If the reviewers are interested in or have questions about your proposal, we may request additional information.

Name: **Phillip Hallam-Baker**

Organization/Affiliation (if any): **VeriSign Inc.**

Email address: **pbaker@verisign.com**

Topic and title of proposed presentation: **Authentication: Repurposing Existing Tools**

**1). Please briefly tell us what aspect(s) of youth on-line safety your presentation will address:**

- 1) Telling parents and children which areas of the Internet they may regard as safe.
- 2) Ensuring that adults are not able to pass themselves off as children in these areas.
- 3) Establishing critical mass.

The third problem is the hardest. The Internet has a billion users and this means that there is an immense amount of inertia to be overcome. We have to be strategic in our choice of technology and deployment strategies and ensure that every party we require buy in from has a sufficient motive to participate.

Since any attempt to authenticate children must involve a party that has the necessary resources and regular contact with the child, any such project is likely to require schools to take an active role and thus a participation motive for the schools and in particular for the early adopter schools who join before the safety benefits of the program can be proven:

- 4) Enabling site licensing of educational materials to all children within a district.

**2). Please explain how your topic is relevant to the scope of the Task Force's inquiry:**

We have an abundance of technical infrastructure to ship bits around: SAML, WS-Federation, OpenID. What we lack is the social infrastructure to create trustworthy information to distribute.

The Extended Validation (EV) Criteria for SSL certificate issue is designed to provide a means of verifying that an organization can be held accountable. The EV criteria are set through an open process and are designed to enable the activities of issuers to be audited. Multiple providers are available for both issue services and audit services.

I propose to repurpose these criteria to authenticate kid-friendly Web sites directly and to authenticate children's ages indirectly through the child's school or local education authority. The existing network of EV issuers provide a read-made competitive market for providing the missing authentication function.