Enterprises, governments, finance and telecom providers; in fact, all users of the Internet, look to browser providers and certification authorities to ensure that the underlying architecture of trust is maintained and strengthened. The Internet will never reach its full potential if consumer trust is lost.

The following organizations have been invited.

- Top 8 browser providers
- Top 5 global Certification Authorities
- Leading web standards organization
- Leading antiphishing organization

**INDUSTRY ROUND TABLE**

May 17th 2005
New York

Wall Street District. Tuesday 17th May 2005. 9:00am – 16:00pm

15 Gold Street at the Corner of Platt Street
New York, New York 10038

Phone: 212-232-7700
Reservations: 212-232-7800

http://www.holidayinnwzd.com/index.htm
Background

Recent cases of identity theft and the fact that no central authority is responsible for monitoring, maintaining and issuing best practice guidelines for the issuance of digital certificates has resulted in a loss of public confidence. This same issue is a factor contributing to a wider problem, wherein the lack of standardisation of authentication methods is responsible for attack vectors seen today such as Phishing and Pharming. With no agreed differentiation method from browser providers for alternative certificate types (where authentication methods vary), consumer confidence is decreased.

No action form an industry group will see consumers shy away from e-commerce to the detriment of all Internet related businesses and service providers. We all have a moral duty to ensure this does not happen.

The “Pain Points” from “Identity Theft” today.

Phishing – Lack of authentication within e-mail
Spoofing – Lack of authentication of web page content
Man In the middle attacks – Lack of authentication within an SSL certificate
Spyware/Bots – Lack of authentication within applications

The Infrastructure for trust

<table>
<thead>
<tr>
<th>Level</th>
<th>Primary Responsibility</th>
<th>Area of concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>The User Interface</td>
<td>Browser providers and OS providers</td>
<td>Lack of standards for differentiation of trust level – Open to abuse and misuse</td>
</tr>
<tr>
<td>Applications</td>
<td>Service providers</td>
<td>Correct selection of appropriate trust level for the appropriate business type</td>
</tr>
<tr>
<td>Trust Infrastructure</td>
<td>Security providers</td>
<td>Effective processes and procedures allowing differentiation – Ongoing improvements and clear indication of trust levels (Classes)</td>
</tr>
</tbody>
</table>

Initial meeting Schedule  Industry Round Table  9:00am – 16:00pm 17th May 2005

The inaugural round table meeting will establish clear goals with the intention of submitting to a working group charter to a web standards organisation. Open discussion will drive a multistage plan to ensure trust integrity is maintained on the Internet. The first stage will address many of the immediate concerns and allow browser providers to move towards a more standardised trust model over the coming 12-18 months. The second stage in the evolution of the working group will encompass a wider number of issues affecting service providers and will pull from other standards groups.

Basic Work Schedule – Stage 1

May 17th 2005 – Industry Round table – New York – Outcome will be a working Charter

June 2005 – Charter proposals are migrated through to a web standards organisation, With an incubator group established – Security and Usability

Open to all existing group members to contribute and form a final working group.

July-September 2005 – Initial proposals and guidelines for best practice are created.


November 05 – 06 - During the following 12 months WebTrust audits will ensure compliance to the best practices.

Please submit attendance confirmation to:-
Steve Roylance, Technical Marketing Director at Comodo Inc (steve@comodo.com) or
Dr. Phillip Hallam-Baker – Principal Scientist at VeriSign Inc (pbaker@verisign.com)