Dear NIST,

Please find hereunder our proposal for the workshop "Improving Trust in the Online Marketplace"

We are very thrilled to attend the workshop because we want to present our research for the improvement on current CA model.

In this topic, there are two lines of opinion: those who wants to change the model (Convergence is the most publicity project) and others like us, who think the actual model is good, although needs fixes and minor changes.

The focus of our research is the problem that suppose the big number of valid CAs you can find in the modern browsers and operating systems. We believe many of these CAs are used in E-goverment for localized countries, so these CAs are useless for people who live outside of these countries. Nevertheless, certificates issued by these CAs are valid for everybody.

You can find the best example in Turktrust, the Turkish CA that has been compromised and issued certificates from Google.

As a prove of this research, we want to share a tool called 'SSLCop'
that currently works for Windows and Mac OS X, which allows the user to trust only on those CAs that makes sense, according to its nationality, blocking the other CAs and thus, delimiting the risk.

Looking forward to attend the workshop.

Best regards,

--

Lorenzo Martínez Rodríguez