Title: Building Trust and Containing Risk Technology Space: Browsers and Root CA Programs
Authors: Sid Stamm and Kathleen Wilson, Mozilla Proposed Presenter: Sid Stamm (sid@mozilla.com)

The technologies in Firefox as well as Mozilla's CA Certificate policy are evolving with the rapidly changing security landscape.

Attacks on CAs and network infrastructure are becoming more frequent and higher profile (some even make the news), so we are working to improve the way the PKI system works to keep users safe and give them confidence their Internet transactions are protected. This involves building up better validation mechanisms and reinforcing existing ones with the ultimate goal to prevent, quickly detect, and contain misuse of certificates.

Fundamentally, we want to detect all such misuse. Using more information in making trust decisions increases our ability to find a breakdown of trust. Instead of relying only on signatures and revocation queries to determine whether a connection is trustworthy, we are empowering web site operators to contribute their point of view with certificate pinning, HSTS, and other tools.

In parallel, we are tightening our root program so that any breaches of the system can be quickly identified and better contained. Moving towards the principle of least privilege, to contain any mis-use. Additionally, we have begun requiring auditing and public disclosure of publicly-issuing intermediate certificates that are not technically constrained. Our goal is to have better controls and visibility of publicly-trusted issuing certificates in order to make better trust decisions, detect security incidents faster, and limit the impact of each security incident.