CA WORKSHOP
IMPROVING TRUST IN THE ONLINE MARKETPLACE

NIST – Green Auditorium
Gaithersburg, Maryland
April 10-11, 2013

Wednesday, April 10, 2013

9:00-10:15	**Session 1** **Welcome & Purpose** Andrew Regenscheid, *NIST* **Keynote - Web Security in the Real World** Steve Bellovin, *Federal Trade Commission*
10:15-10:45	**BREAK**
10:45-12:30	**Session 2: Trust Architectures** **State of PKI for SSL/TLS** Russ Housley, *Vigil Security, LLC* **Revocation Process** Ryan Koski, *GoDaddy* **Certificate Transparency - protocol design and implementation** Emilia Kasper, *Google* **DANE: TLS Domain Name Authentication using the DNS Itself** Richard Barnes, *BBN Technologies*
12:30-1:30	**LUNCH** *(West Square Cafeteria, 2nd cafeteria entrance)*
1:30-1:40	**NSTIC Update** Jeremy Grant, *NIST*
1:40-2:20	**Session 3: Analysis Frameworks** **Transparency and alternative certification, distribution or confirmation of key information** Alexandra Grant, *Dartmouth College* **Talk: TBD** Eric Rescorla, *RTFM, Inc.*

Wednesday, April 10, 2013

2:20-3:00 **Session 4: Experiences**

A Window of Opportunity: How Certificate Transparency Increases Online Trust Accountability and Security: A CA Perspective
Ben Wilson, *DigiCert*

The ICSI Notary: Lessons and Insights from a Large-Scale Study of the SSL/TLS Ecosystem
Bernhard Amann, *International Computer Science Institute*

3:00-3:30 **BREAK**

3:30-5:00 **Session 5**
Panel: What Do We Need to Improve Trust?
Moderator: Sean Turner, *IECA, Inc.*

Panelists
- Sid Stamm, *Mozilla*
- Rick Andrews, *Symantec Corporation*
- Chris Sutherland, *BMO*
- Eric Osterweil, *Verisign*

5:00 **End of Day**

Thursday, April 11, 2013	
9:00-9:15	**Opening Remarks** Ari Schwartz, *Department of Commerce*
9:15-10:00	**Session 6: Keynote Talk** **Lessons Learned from the DigiNotar Case** Aart Jochem, *National Cyber Security Centrum*
10:00-10:20	**TBD** Peter Eckersley, EFF
10:20-10:50	**BREAK**
10:50-12:30	**Session 7: Requirements, Auditing and Evidence** **Federal PKI Approach to Auditing and Requirements** Deb Gallagher, *GSA* **Reference Certificate Policy** Andrew Regenscheid, *NIST* **CA Self-Governance: CA/Browser Forum Guidelines and Other Industry Developments** Ben Wilson, *DigiCert* **Enhancing Trust by Enhancing the Audit Process** Jens Bender, *German Federal Office for Information Security, BSI* **European Approach to Oversight of "Trust Service Providers"** Arno Fiedler, *Nimbus Technologieberatung GmbH*
12:30-1:30	**LUNCH** *(West Square Cafeteria, 2nd cafeteria entrance)*
1:30-2:30	**Session 8: Management and Risk Mitigation** **Reducing the Tail Risk of CA Compromise by Enabling Trust in Regional CAs Using Language Community and Locale Annotations** Brad Hill, *PayPal* **Verifying Keys through Publicity and Communities of Trust** Eric Osterweil, *Verisign* **Using Least Privileged Design Principals to Improve Trust in the Online Marketplace** Ryan Hurst, *GlobalSign*
2:30-3:00	**BREAK**

Thursday, April 11, 2013	
3:00-4:30	**Session 9:** **Panel: Where Do We Go from Here?** Moderator: Tim Polk, *OSTP* Panelists: - Ben Wilson, *CAB Forum* - Russ Housley, *Vigil Security, LLC* - Joe Hall, *CDT* - Peter Eckersley, *EFF* - Stephen Schultze, *Princeton*
4:30-5:00	**Closing Session** **Building Consensus** Tim Polk, *OSTP* **Final Remarks** Andrew Regenscheid, NIST
5:00	**End of Day**