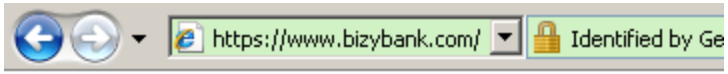
CA/Browser Forum Update

November 29, 2012

CAB Forum: A Brief History



- ✓ CABF starts as a loose association of CAs and browsers to draft guidelines for EV SSL Certificates
- ✓ Membership expands globally, currently 32 CAs and 5 browsers
- ✓ EV Guidelines generated and approved
- ✓ Baseline Requirements formulated and passed
- ✓ Network Security document created and finalized
- ➢ All publicly trusted CAs, whether members of CABF or not, must adhere to guidelines!

General Updates

- Baseline Requirements 1.0: Passed (1.1 added)
- EV Guidelines 1.4, including EV Code Signing: Passed
- Network Security Requirements: Passed
- IPR policy: Passed (but being revised)
- Various Errata: Passed
- Governance Reform: New proposal passed
- WebTrust audit criteria for BRs expect to be finalized in CY Q1 2013
- Baseline Requirements are included in Draft ETSI TS 102 042 V2.2.3 (2012-10) and referenced as “PTC-BR Publicly-Trusted Certificate-Baseline Requirements”

➢ **CAB Forum is moving forward to effect positive changes to improve Internet security**

Overall CA Security

- As good as the weakest player
- Compromise of one CA can lead to an overall Internet security incident:
- Examples:

  Diginotar → Negligent in maintaining proper security

  – Weak passwords

  – No A/V

  – Improper network segregation

  Comodo

  – Reseller compromised, allowing issuance of any type of certificate

  – SQL Injection vulnerabilities, insecure application/credential management

What about Audits?

- Two types of Audits trusted by browsers:
  - WebTrust: AICPA/CICA
  - ETSI: Country accredited auditors (European)
- Diginotar passed an ETSI audit performed by PwC
  - Audits are a snapshot at a point in time
  - How did Diginotar perform on the audit?
    - Attestation letter
  - How do we explain their security lapses?
  - Is PwC at fault? Who determines this and who punishes (if applicable)?
- CAB Forum → working with AICPA and ETSI to improve audit accountability

CA/Browser Forum Baseline Requirements

- Forum had been working on Baseline Requirements for 2+ years
- Version 1.0 released in Fall 2011 (after Diginotar/Comodo)
- 1.0 did not address physical/network security
- Separate document developed for network security which may become part of Baseline Requirements
- CABF released V1.1 to include updates and improvements to 1.0

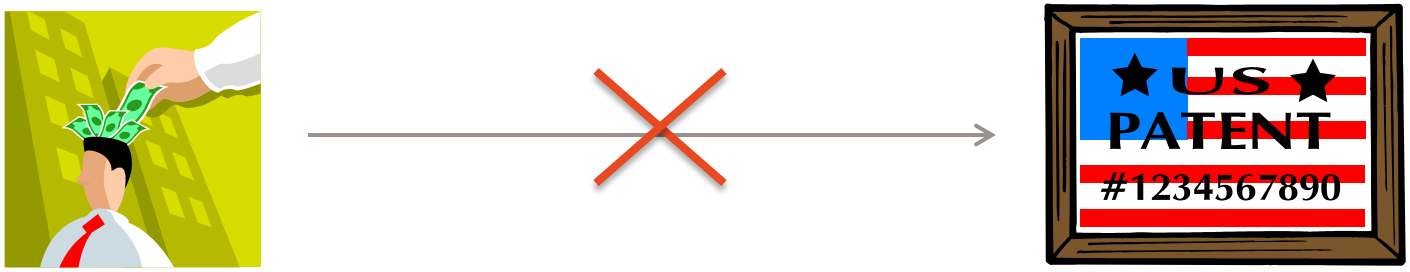
- Will be added to audit regime once auditors approve

CA/Browser Forum restructuring

- CAB Forum seen as closed group, not open to outside
- Governance working group formed to solicit proposals for reform
  - Transparency
  - Openness
  - Voting rights
  - Incorporation
- Multiple proposals received ranging from complete restructuring to minor changes to allow visibility in current process
- Goal is to better represent other stakeholders (relying parties, users) in CABF rulemaking
- Proposal from Trend Micro voted in. Reforms to start after ratification

Intellectual Property Rights (IPR)

- CABF needs an IPR policy
  - RF licensing, some members uncomfortable without one
- V1.0 passed August 2012→Several members did not sign
- IPR WG formulating compromise to satisfy all
- Exceptions proposed for standards bodies and govts



Symantec's Experience

- CAB Forum participation requires extensive coordination between internal groups
  - Policy, Engineering, Product management, Legal, Sales
- Consideration: Four brands, several systems, global auth teams, global revocation infrastructure, millions of certs
- Monthly meetings held to review status
- Forming the right balance between customer needs and security

➢ CABF membership is an important commitment for Symantec

Raising the bar for Physical, Network Security, Revocation infrastructure

Thank you!

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.