Authentication. Security. Trust.

GlobalSign®

enisa

Mitigating the impact of security incidents in trust services providers

WORKSHOP ON SECURITY ASPECTS OF TRUST SERVICE PROVIDERS

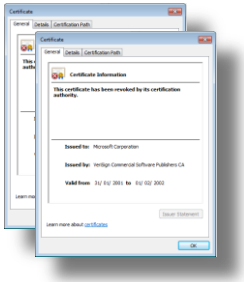
Who am I?

- **Steve Roylance, Business Development Director – GlobalSign (from 2006)**
- A decade of experience as a Certification Authority
- 23+ years in the IT industry
- Founder of the CA/Browser Forum
- Pleased to be able to speak today!

GlobalSign History

- Founded in 1996 by BE Chambers of Commerce, ING Bank & Vodafone.
- Founding Member of CA/Browser Forum/ CASC
- Acquired by GMO Internet Inc (ticker 9449 on the Tokyo Stock Exchange) & re-launched in 2006
- A ‘Pure Play’ CA.

2011 - "Annus Horriblis"



VeriSign Issues
Microsoft Certificates
2001

Paypal
Null Prefix
2009

MD5 Collision
Attack
2008

Ichsunx2
Diginotar
Attack
2011

Ichsunx2
Comodo
Attack
2011

Ichsunx2
GlobalSign
Attack
2011

1995 2000 2005 2010 2011 2012

GlobalSign
1996/8

CABForum
1st F2F
2005

EV SSL 1.0
2007

EV SSL 1.1
2008

EV SSL 1.2
2009

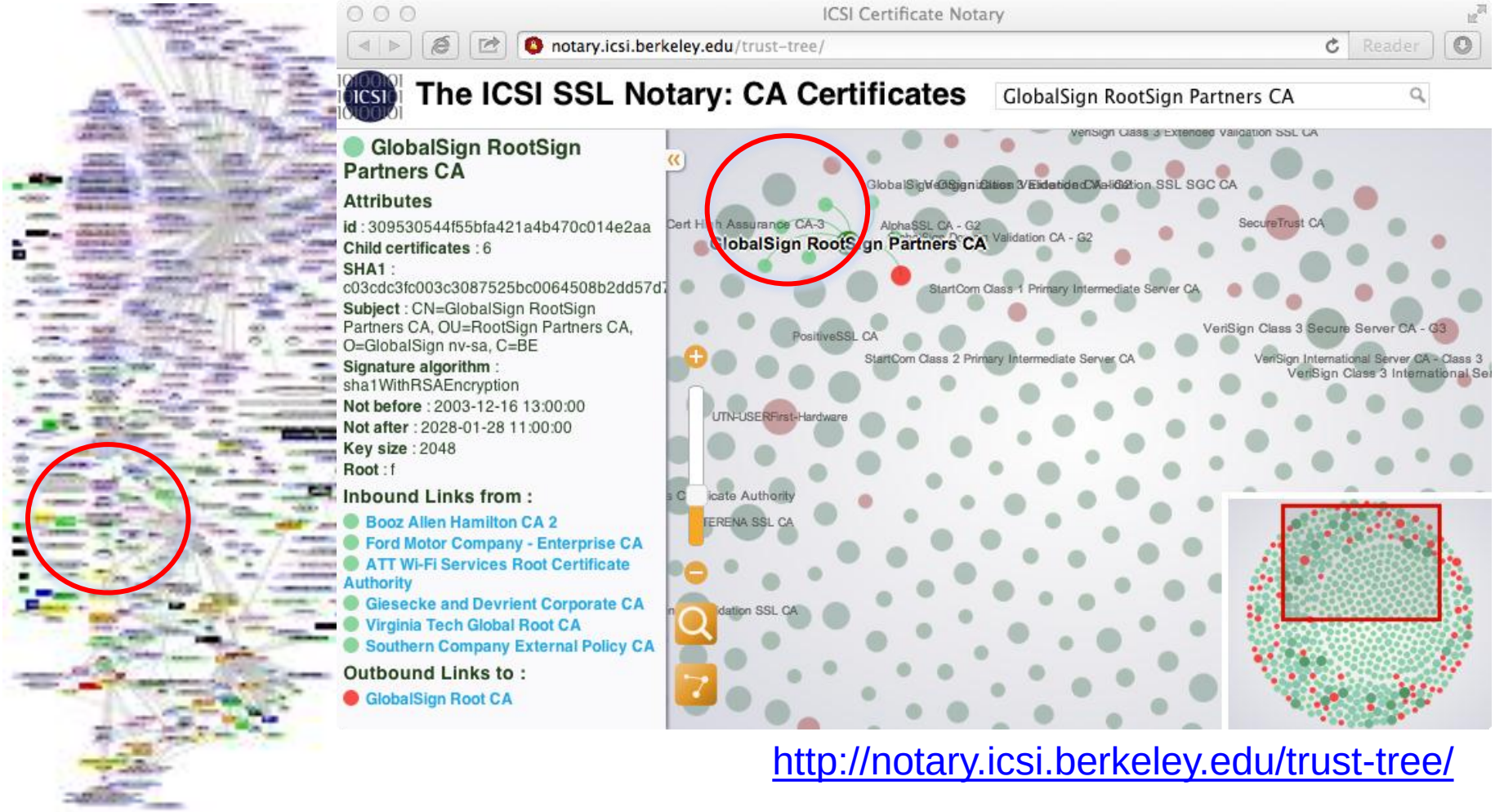
EV SSL 1.3
2010

BR1.0
2011

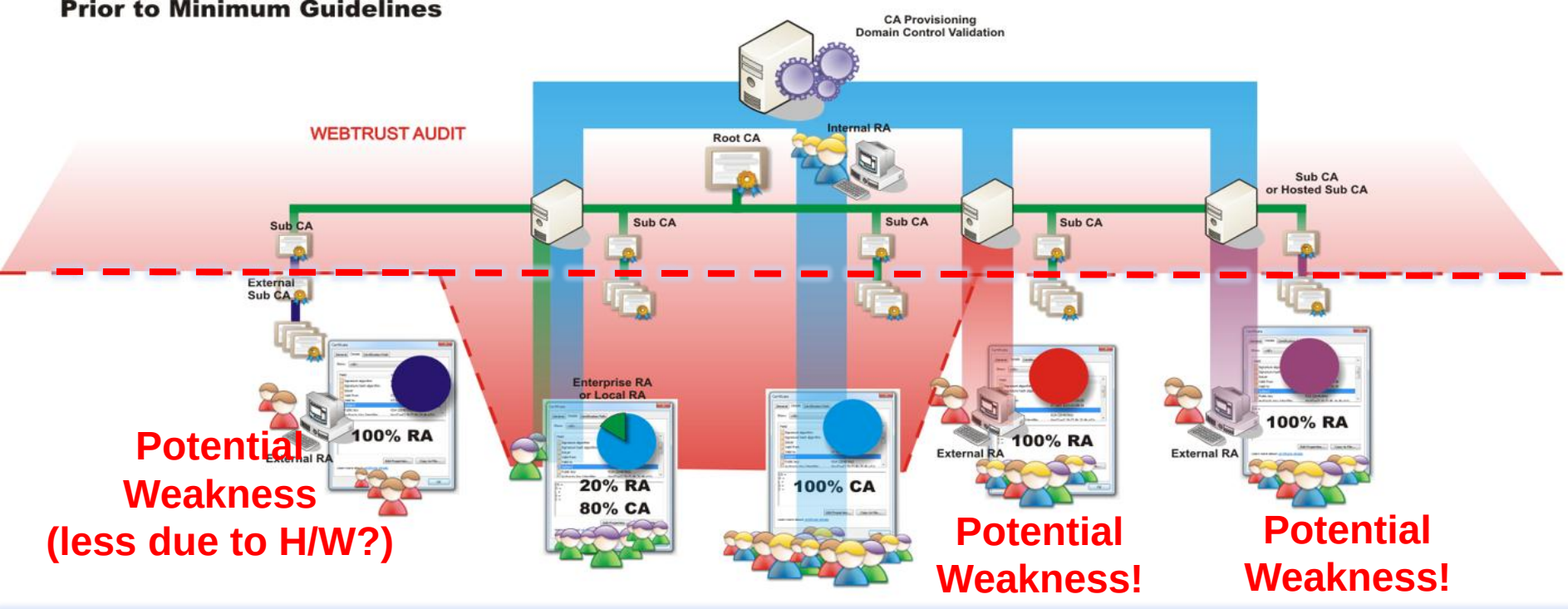
BR1.1.6
2013

EFF and ICSI list attack targets!

http://www.eff.org/files/colour_map_of_CAs.pdf



http://notary.icsi.berkeley.edu/trust-tree/


Prior to Minimum Guidelines
CA Provisioning
Domain Control Validation
WEBTRUST AUDIT
Root CA
Internal RA
Sub CA
Sub CA
Sub CA
Sub CA
Sub CA
or Hosted Sub CA
External
Sub CA
External RA
100% RA
Enterprise RA
or Local RA
20% RA
80% CA
100% CA
External RA
100% RA
External RA
100% RA
Potential
Weakness
(less due to H/W?)
Potential
Weakness!
Potential
Weakness!

Name Constraints – Baseline Requirements

Document History

Ver.	Ballot	Description	Adopted	Effective*
1.0.0	62	Version 1.0 of the Baseline Requirements Adopted	22-Nov-11	01-Jul-12
1.0.1	71	Revised Auditor Qualifications	08-May-12	01-Jan-13
1.0.2	75	Non-critical Name Constraints allowed as exception to RFC 5280	08-Jun-12	08-Jun-12
1.0.3	78	Revised Domain/IP Address Validation, High Risk Requests, and Data Sources	22-Jun-12	22-Jun-12
1.0.4	80	OCSP responses for non-issued certificates	02-Aug-12	01-Feb-13 01-Aug-13
--	83	Network and Certificate System Security Requirements adopted	03-Aug-13	01-Jan-13
1.0.5	88	User-assigned country code of XX allowed	12-Sep-12	12-Sep-12
1.1.0	--	Published as Version 1.1 with no changes from 1.0.5	14-Sep-12	14-Sep-12
1.1.1	93	Reasons for Revocation and Public Key Parameter checking	07-Nov-12	07-Nov-12 01-Jan-13
1.1.2	96	Wildcard certificates and new gTLDs	20-Feb-13	20-Feb-13 01-Sep-13
1.1.3	97	Prevention of Unknown Certificate Contents	21-Feb-13	21-Feb-13
1.1.4	99	Add DSA Keys (BR v.1.1.4)	3-May-2013	3-May-2013
1.1.5	102	Revision to subject domainComponent language in section 9.2.3	31-May-2013	31-May-2013
1.1.6	105	Technical Constraints for Subordinate Certificate Authorities	29-July-2013	29-July-2013

* Effective Date and Additionally Relevant Compliance Date(s)

Open tasks (For GlobalSign)

- Move customers to Name Constraints
- Ask EFF and ICSI to distinguish constrained CAs
- Work with Apple to support Name Constraints!
- After XX years force Name Constraints to be mandatory.
- Perform outreach highlighting best practice techniques.