RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: MBS-R04

Mobile CA State of the Union

Andrew Blaich
Lead Security Analyst
Bluebox Security
@ablaich

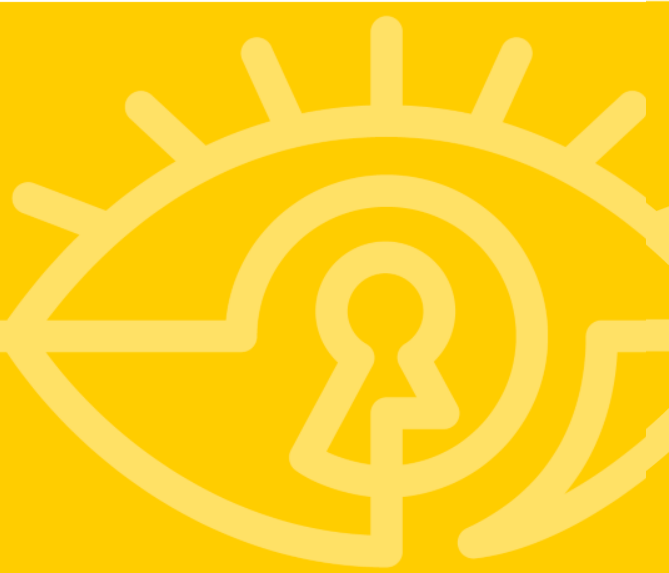
Jeff Forristal
CTO
Bluebox Security
@j4istal

Objectives

- What are CAs and how do they secure your communications?
- How can CAs be classified?
- What are the top apps doing to verify trust?
- How can you apply what you've learned?

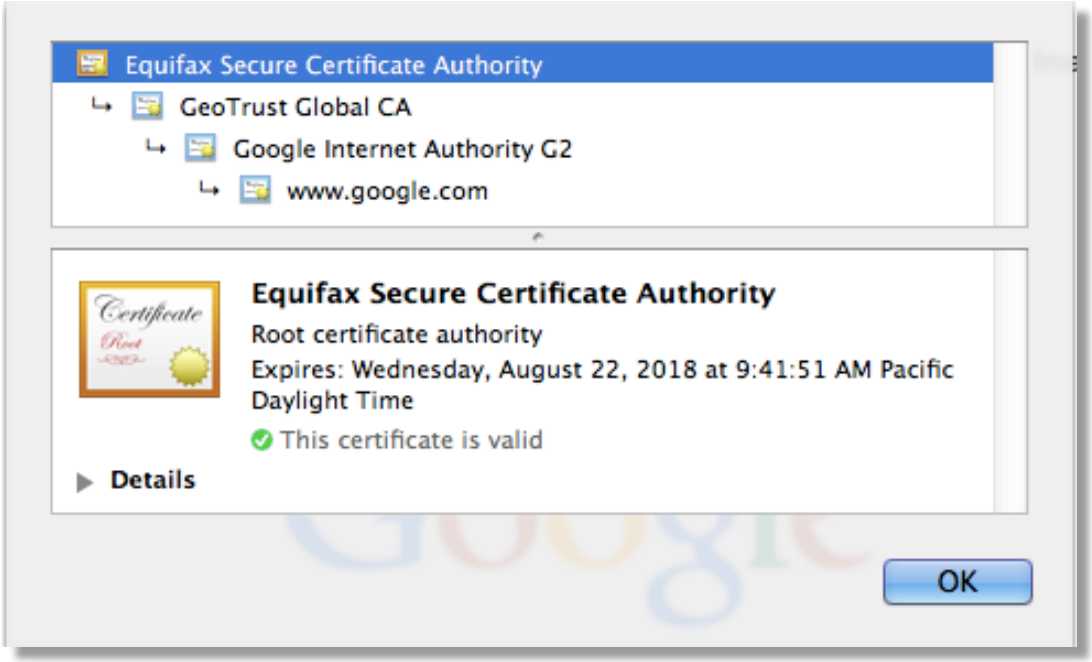
What is a CA?

- Certificate Authorities are the providers of trust for our communications over the Internet.
  - The Internet's security is built on top of trusted secure transactions
  - CAs provide assurance of the identity of a web server (trust chain)
  - Self-signed certs do not provide this assurance



What is the trust chain?

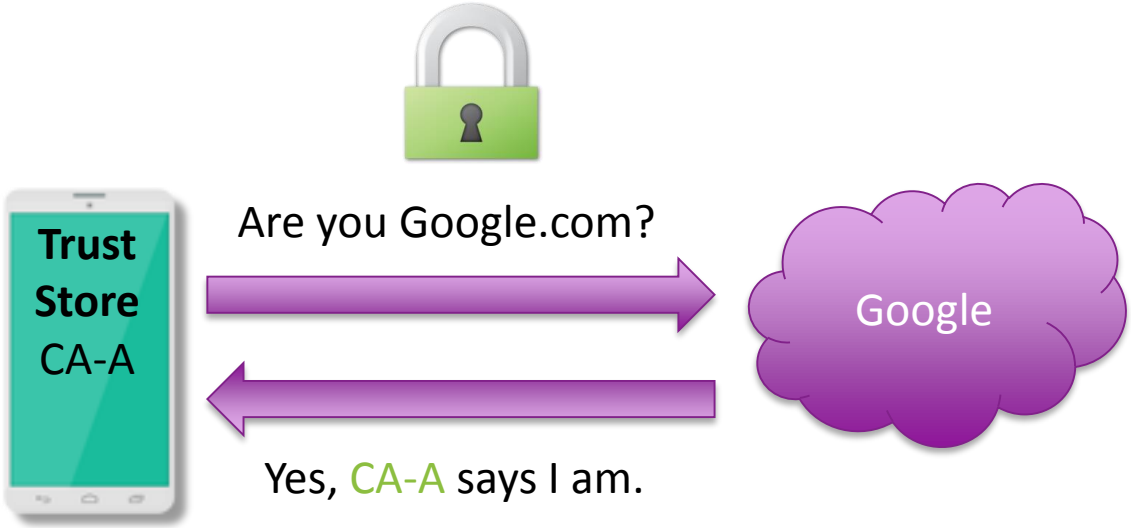
Trusted Certificate Chain



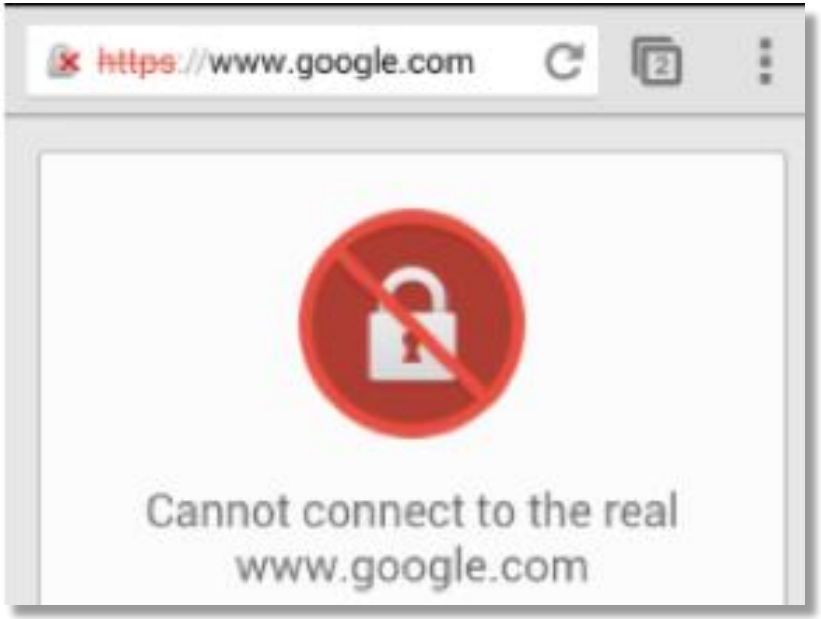
Verified == Trusted Chain

The root CA to verify this chain is installed on the device, thus making the chain verifiable and trusted.

Site Verification - Success



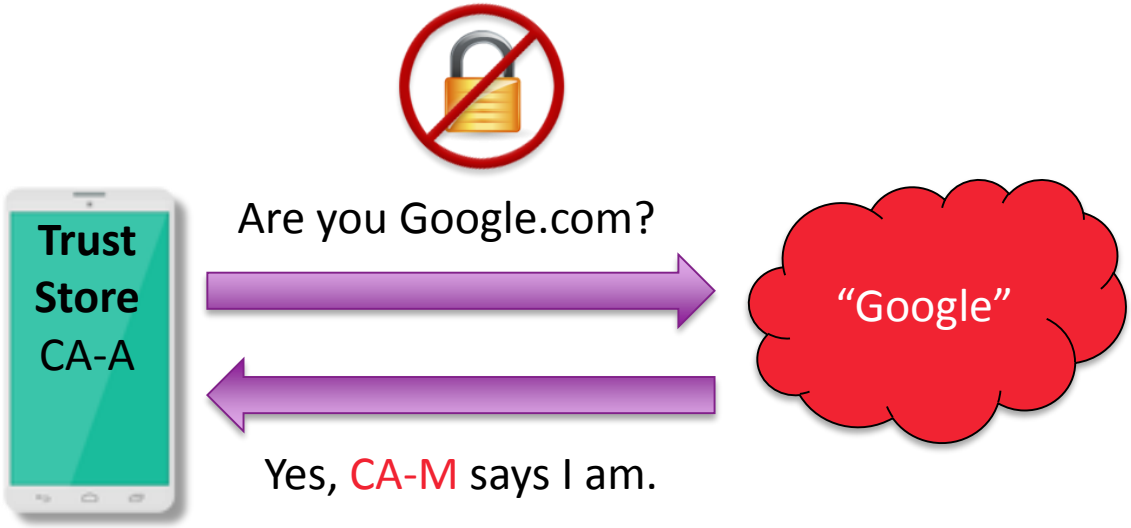
Un-trusted Certificate Chain



Un-verified == Un-Trusted Chain

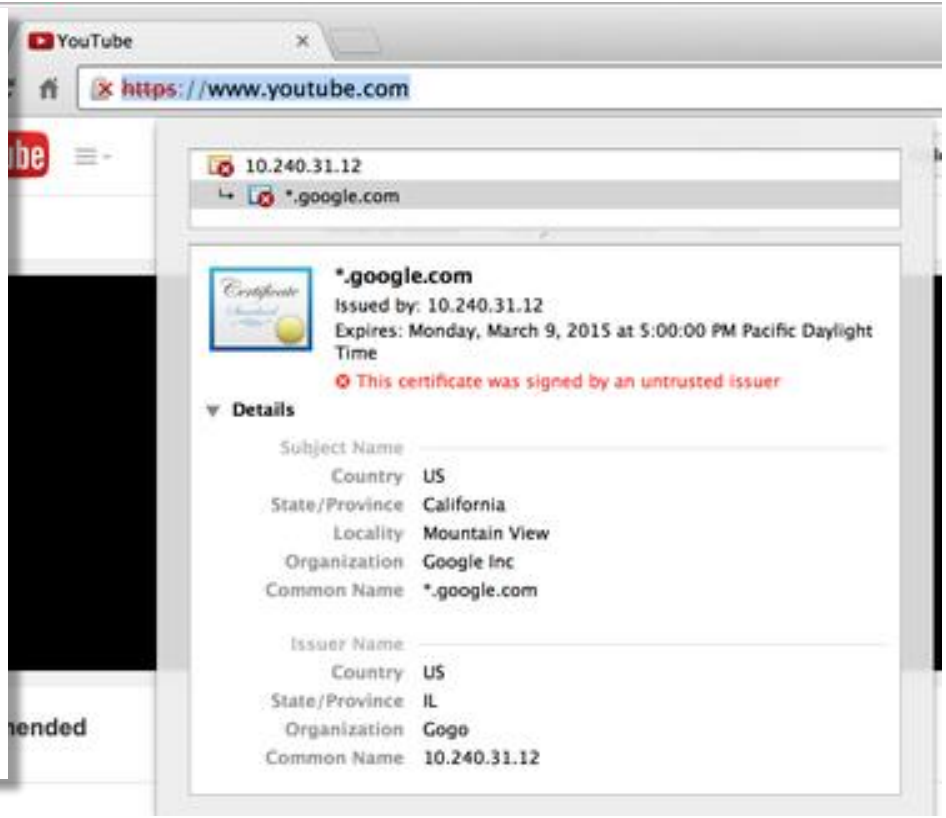
The root CA to verify this chain is missing from the device making the trust chain un-verifiable.

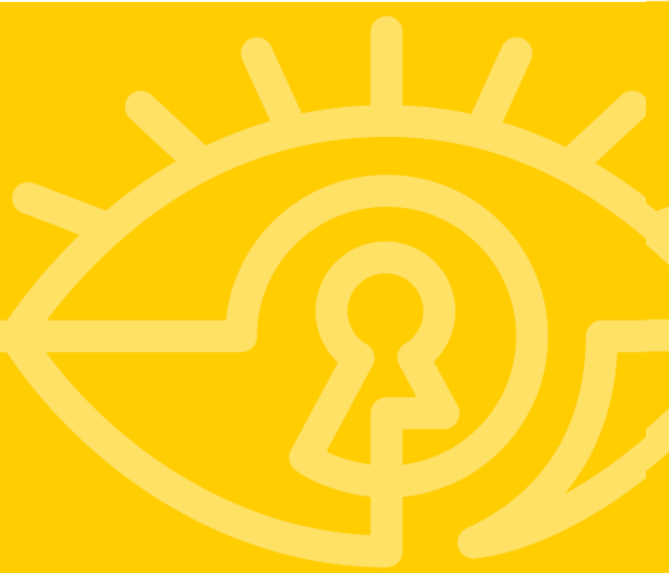
Site Verification - Failure



NOT A TRUSTED CONNECTION

Un-trusted Certificate Chain





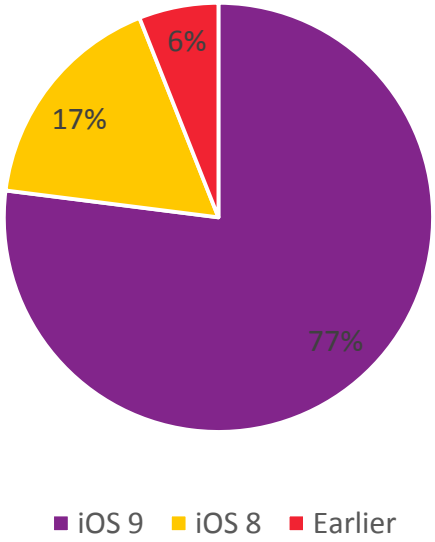
Certificate Authorities on mobile

How many root certs?

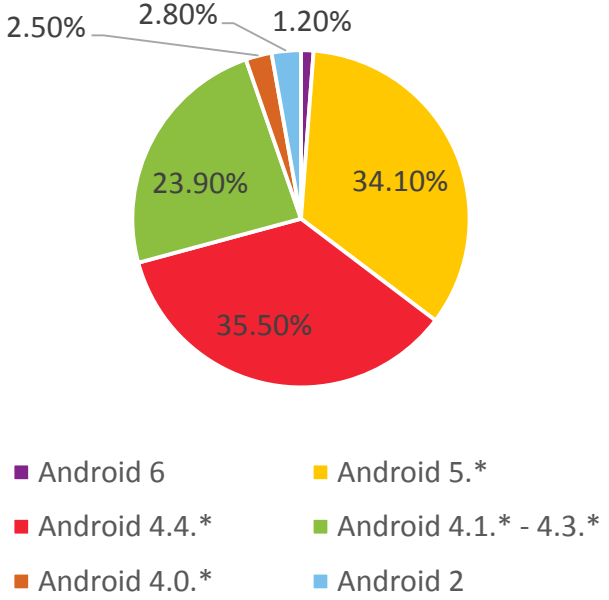
OS (2015)	Cert Count	OS (2016) as of January 8, 2016	Cert Count
Android 5.*	**162**	**Android 6.***	**158**
iOS 8.*	**223**	**iOS 9.***	**200**
- iOS 8.* Trusted	210	- iOS 9.* Trusted	187
- iOS 8.* Always Ask	13	- iOS 9.* Always Ask	13
- iOS 8.* Blocked	17	- iOS 9.* Blocked	18

OS Version Distribution

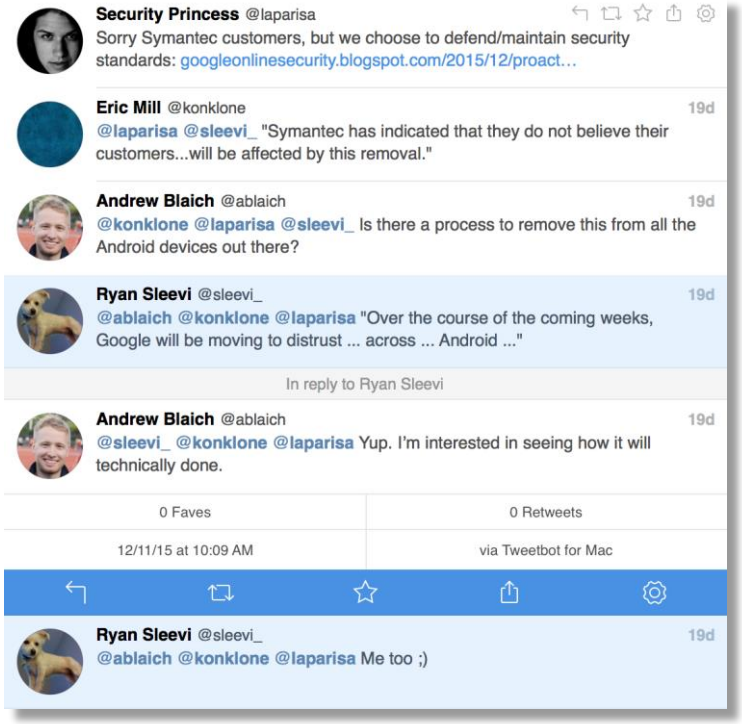
iOS Versions



Android Versions



Root Cert Changes – Long Tail



Security Princess @laparisa
Sorry Symantec customers, but we choose to defend/maintain security standards: googleonlinesecurity.blogspot.com/2015/12/proact…

Eric Mill @konklone 19d
@laparisa @sleevi_ "Symantec has indicated that they do not believe their customers...will be affected by this removal."

Andrew Blaich @ablaich 19d
@konklone @laparisa @sleevi_ Is there a process to remove this from all the Android devices out there?

Ryan Sleevi @sleevi_ 19d
@ablaich @konklone @laparisa "Over the course of the coming weeks, Google will be moving to distrust ... across ... Android ..."

In reply to Ryan Sleevi

Andrew Blaich @ablaich 19d
@sleevi_ @konklone @laparisa Yup. I'm interested in seeing how it will technically done.

0 Faves	0 Retweets
12/11/15 at 10:09 AM	via Tweetbot for Mac

Ryan Sleevi @sleevi_ 19d
@ablaich @konklone @laparisa Me too ;)

Further Technical Details of Affected Root:
Friendly Name: Class 3 Public Primary Certification Authority
Subject: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority
Public Key Hash (SHA-1): E2:7F:7B:D8:77:D5:DF:9E:0A:3F:9E:B4:CB:0E:2E:A9:EF:DB:69:77
Public Key Hash (SHA-256):
B1:12:41:42:A5:A1:A5:A2:88:19:C7:35:34:0E:FF:8C:9E:2F:81:68:FE:E3:BA:18:7F:25:3B:C1:A3:92:D7:E2

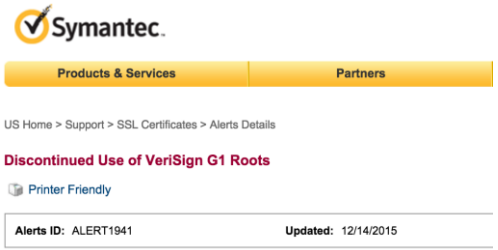
MD2 Version
Fingerprint (SHA-1): 74:2C:31:92:E6:07:E4:24:EB:45:49:54:2B:E1:BB:C5:3E:61:74:E2
Fingerprint (SHA-256):
E7:68:56:34:EF:AC:F6:9A:CE:93:9A:6B:25:5B:7B:4F:AB:EF:42:93:5B:50:A2:65:AC:B5:CB:60:27:E4:4E:70

SHA1 Version
Fingerprint (SHA-1): A1:DB:63:93:91:6F:17:E4:18:55:09:40:04:15:C7:02:40:B0:AE:6B
Fingerprint (SHA-256):
A4:B6:B3:99:6F:C2:F3:06:B3:FD:86:81:BD:63:41:3D:8C:50:09:CC:4F:A3:29:C2:CC:F0:E2:FA:1B:14:03:05

"…it will likely take years to reduce the number of users and devices at risk from certificates issued by Symantec from this root…" - Ryan Sleevi

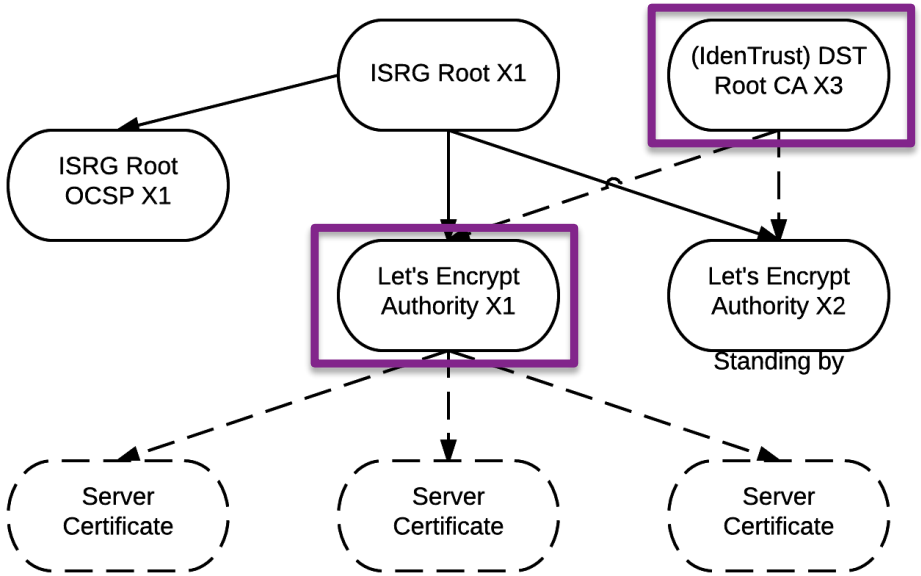
Root Cert Changes - OEMs

- **BlackBerry Priv (Android)**
  - 17 Supplemental Certificates:
    - att_suplcert1_v0.der
      - **SHA-1 Hash**: A1:DB:63:93:91:6F:17:E4:18:55:09:40:04:15:C7:02:40:B0:AE:6B




```
att_suplcert1_v0.der
att_suplcert2_v0.der
att_suplcert3_v0.der
bell_mobility_suplcert1_v0.der
bell_mobility_suplcert2_v0.der
cmcc_suplcert1_v0.der
google_suplcert1_v0.der
mts_mobility_suplcert1_v0.der
rogers_suplcert1_v0.der
rs_cacertv1_v0.der
rs_cacertv3_v0.der
sasktel_suplcert1_v0.der
t_mobile_us_suplcert1_v0.der
telus_suplcert1_v0.der
verisign_class3_v0.der
verisign_spirent_interm_suplcert1_v0.der
vodafone_suplcert1_v0.der
```

Root Cert Changes - Let's Encrypt

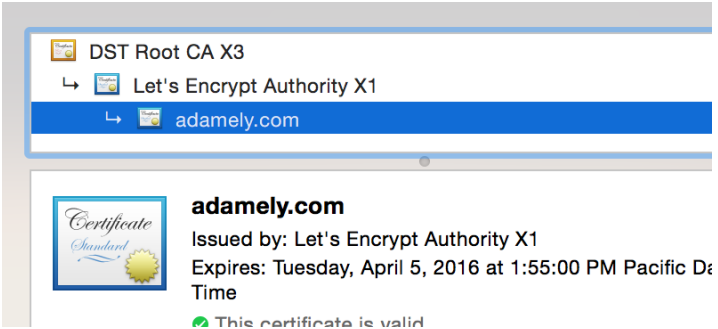


Source: https://letsencrypt.org/certificates/

How does your browser or device already trust Let's Encrypt?

ISRG Root X1 is not yet trusted in most browsers (or devices), e.g.

https://bugzilla.mozilla.org/show_bug.cgi?id=1204656
https://code.google.com/p/chromium/issues/detail?id=53
https://code.google.com/p/android/issues/detail?id=1863



SHA-1 Deprecation

- Community Controversy
- Among the mobile platforms, Android added SHA256 support in version 2.3. Earlier versions—still used in large numbers—support only SHA1.
- Firefox 43 does not validate against new SHA-1 CAs from 1/1/2016 or after (reverted)
- When will mobile apps enforce the deprecation of SHA-1?

Microsoft Trusted Roots Removal

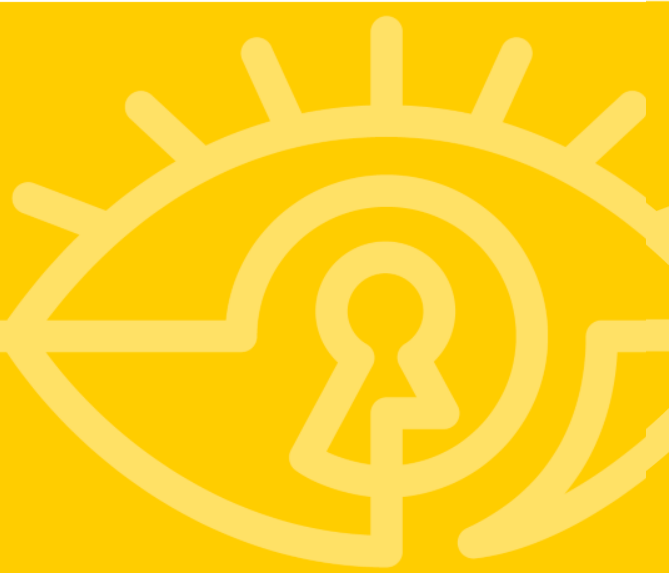
Original

CA Subject to Removal	Root
DanID	DanID
e-Tugra	EBG Elektronik Sertifika Hizmet Saglayicisi
e-Tugra	E-Tugra Certification Authority
LuxTrust	LuxTrust Global Root CA
Secom	SECOM Trust Systems Co Ltd.
Secom	SECOM Trust Systems CO LTD
Secom	SECOM Trust Systems CO LTD
Wells Fargo	WellsSecure Public Certificate Authority
Wells Fargo	WellsSecure Public Root Certification Authority 01 G2
CyberTrust	Japan Certification Services, Inc. SecureSign RootCA1
CyberTrust	Japan Certification Services, Inc. SecureSign RootCA2
CyberTrust	Japan Certification Services, Inc. SecureSign RootCA3
Certigna	Certigna
Ceska Posta	PostSignum Root QCA 2
E-Certchile	E-Certchile Root CA
Nova Ljubljanska	NLB Nova Ljubljanska Banka d.d. Ljubljana
Post.Trust	Post.Trust Root CA
Serasa	Serasa Certificate Authority I
Serasa	Serasa Certificate Authority II
Serasa	Serasa Certificate Authority III

Updated

CA Subject to Removal	Reason for Removal	Root Subject to Removal
DanID	Audit	DanID
~~e-Tugra~~	~~Audit~~	~~EBG Elektronik Sertifika Hizmet Saglayicisi~~
~~e-Tugra~~	~~Audit~~	~~E-Tugra Certification Authority~~
~~Wells Fargo~~	~~Audit~~	~~WellsSecure Public Certificate Authority~~
~~Wells Fargo~~	~~Audit~~	~~WellsSecure Public Root Certification Authority~~
~~CyberTrust~~	~~Contract Compliance~~	~~Japan Certification Services, Inc. SecureSign R~~
~~CyberTrust~~	~~Contract Compliance~~	~~Japan Certification Services, Inc. SecureSign R~~
~~CyberTrust~~	~~Contract Compliance~~	~~Japan Certification Services, Inc. SecureSign R~~
E-Certchile	Contract Compliance	E-Certchile Root CA
~~Nova Ljubljanska~~	~~Contract Compliance~~	~~NLB Nova Ljubljanska Banka d.d. Ljubljana~~
Post.Trust	Contract Compliance	Post.Trust Root CA
Serasa	Contract Compliance	Serasa Certificate Authority I
Serasa	Contract Compliance	Serasa Certificate Authority II
Serasa	Contract Compliance	Serasa Certificate Authority III

Source: *http://social.technet.microsoft.com/wiki/contents/articles/31680.microsoft-trusted-root-certificate-program-updates.aspx*



CA Classifications

CA Classifications

- **Known Failures in Keeping Trust**
- Government-Based Roots of Trust
- Cause for Concern
- **Artificial Constraints**
- Everything else

Known Failures with CAs

- **Highlights in failures of trust:**
  - Symantec [2015]
  - CNNIC/MCS Holdings [2015]
  - Comodo [2011]
  - DigiNotar [2011]
  - GlobalSign [2011]
  - India CCA [2014]
  - RapidSSL (indirect) [2008]

Artificial Constraints

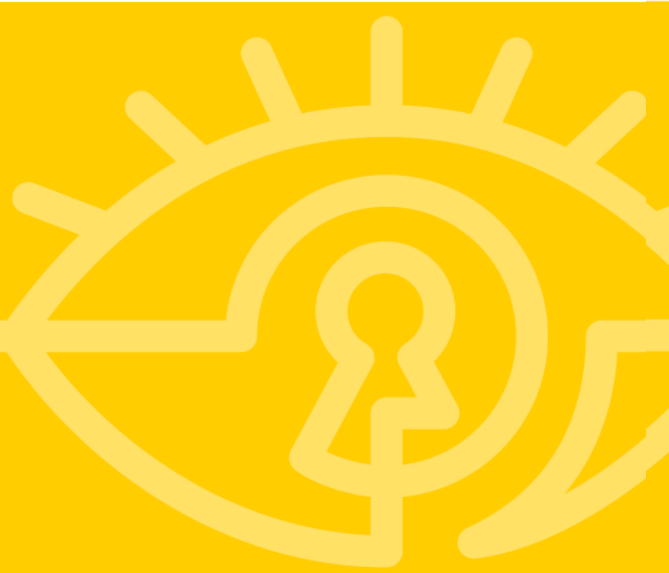
Cert Subject	Reason For Constraint
CN=IGC/A,OU=DCSSI,O=PM/SGDN,L=Paris,ST=France,C=FR	Issued several un-authorized certificates for Google domains. TLD restrictions: *.fr (France), .gp (Guadeloupe) , .gf (Guyane) , .mq (Martinique) , .re (Réunion) , .yt (Mayotte), .pm (Saint-Pierre et Miquelon) , .bl (Saint Barthélemy) , .mf (Saint Martin) , .wf (Wallis et Futuna) , .pf (Polynésie française) , .nc (Nouvelle Calédonie) , .tf (Terres australes et antarctiques françaises)]*

Artificial Constraints –cont'd.


```
1559  /* Add name constraints to certain certs that do not include name constraints
1560   * This is the core of the implementation for bug 952572.
1561   */
1562
1563  static SECStatus
1564  getNameExtensionsBuiltIn(CERTCertificate  *cert,
1565                           SECItem *extensions)
1566  {
1567    const char constraintFranceGov[] = "\x30\x5D" /* sequence len = 93*/
1568                                       "\xA0\x5B" /* element len =91 */
1569                                       "\x30\x05" /* sequence len 5 */
1570                                       "\x82\x03" /* entry len 3 */
1571                                       ".fr"
1572                                       "\x30\x05\x82\x03" /* sequence len5, entry len 3 */
1573                                       ".gp"
1574                                       "\x30\x05\x82\x03"
1575                                       ".gf"
1576                                       "\x30\x05\x82\x03"
1577                                       ".mq"
1578                                       "\x30\x05\x82\x03"
1579                                       ".re"
1580                                       "\x30\x05\x82\x03"
1581                                       ".yt"
1582                                       "\x30\x05\x82\x03"
1583                                       ".pm"
1584                                       "\x30\x05\x82\x03"
1585                                       ".bl"
1586                                       "\x30\x05\x82\x03"
1587                                       ".mf"
1588                                       "\x30\x05\x82\x03"
1589                                       ".wf"
1590                                       "\x30\x05\x82\x03"
1591                                       ".pf"
1592                                       "\x30\x05\x82\x03"
1593                                       ".nc"
1594                                       "\x30\x05\x82\x03"
1595                                       ".tf";
```

```
// static
bool CertVerifyProc::HasNameConstraintsViolation(
    const HashValueVector& public_key_hashes,
    const std::string& common_name,
    const std::vector<std::string>& dns_names,
    const std::vector<std::string>& ip_addrs) {
  static const char kDomainsANSSI[][kMaxDomainLength] = {
    "fr",  // France
    "gp",  // Guadeloupe
    "gf",  // Guyane
    "mq",  // Martinique
    "re",  // RÃ©union
    "yt",  // Mayotte
    "pm",  // Saint-Pierre et Miquelon
    "bl",  // Saint BarthÃ©lemy
    "mf",  // Saint Martin
    "wf",  // Wallis et Futuna
    "pf",  // PolynÃ©sie franÃ§aise
    "nc",  // Nouvelle CalÃ©donie
    "tf",  // Terres australes et antarctiques franÃ§aises
    "",
  };

  static const char kDomainsIndiaCCA[][kMaxDomainLength] = {
    "gov.in",
    "nic.in",
    "ac.in",
    "rbi.org.in",
    "bankofindia.co.in",
    "ncode.in",
    "tcs.co.in",
    "",
  };
```



CA Cryptography Analysis

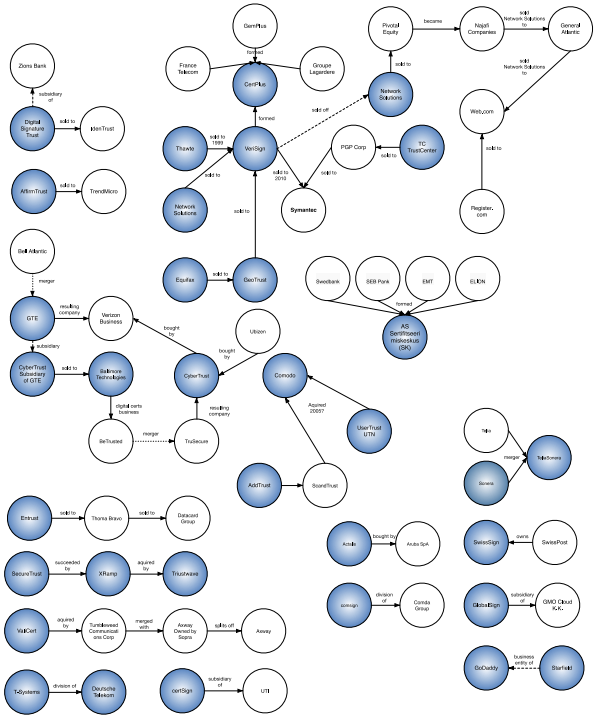
Public Key-Size

Key Type/Size	2015	2016	Notable Entities
RSA / 1024 bit	15	5	GTE CyberTrust, Equifax, VeriSign, ValiCert, Entrust
RSA / 2048 bit	101	96	N/A
RSA/ 4096 bit	14	46	N/A
Elliptic Curve	6	11	GeoTrust, VeriSign, COMODO, Thawte, Entrust, AffirmTrust

Hash Algorithm

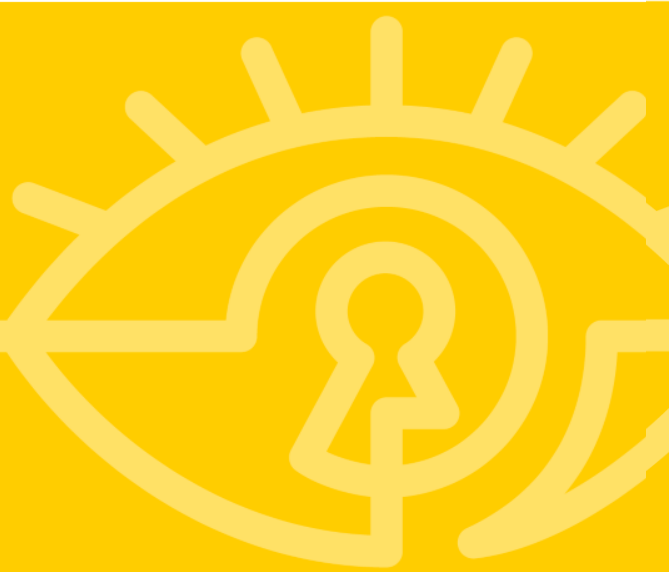
Signature Algorithm	2015	2016	Notable Entities
md5WithRSAEncryption	6	2	GTE CyberTrust (expires 2018), NetLock (expires 2019)
sha1WithRSAEncryption	115	98	N/A
sha256WithRSAEncryption	28	43	N/A
sha384WithRSAEncryption	1	4	N/A
ecdsa-with-SHA256	0	1	GlobalSign
ecdsa-with-SHA384	6	10	GeoTrust, VeriSign, COMODO, Thawte, Entrust, AffirmTrust, …

CA Consolidation



Symantec Owned Entity	2015	2016
GeoTrust	7	7
VeriSign	7	6
TC Trust Center	3	0
Thawte	5	3
Equifax	3	1
Total:	**Symantec controls 24 of the total 156 certificates or ~15% ownership of the Android roots of trust**	**Symantec controls 17 of the total 158 certificates or ~11% ownership of the Android roots of trust**

Source: https://bluebox.com/questioning-the-chain-of-trust-investigations-into-the-root-certificates-on-mobile-devices/



Case Study: Mobile Apps and Trust

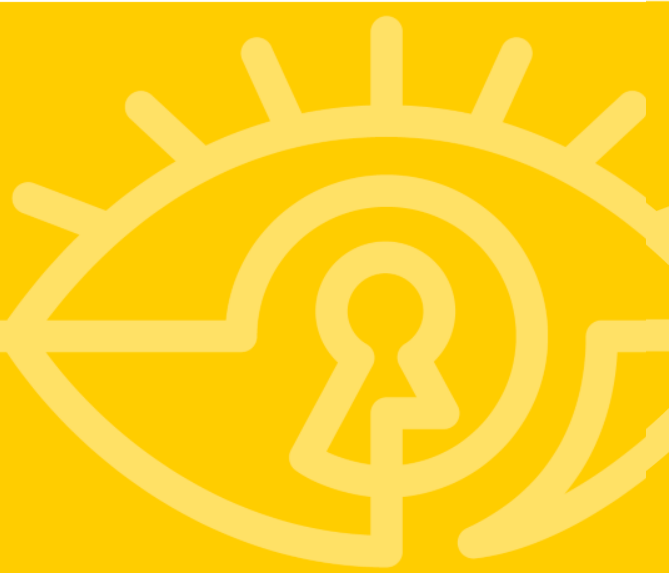
Mobile apps and trust

- Who are the top Android apps trusting?
- Most apps trust the certificates on your device
  - Your browser may distrust the CNNIC root cert, but **your** mobile app may trust it
  - Some apps even disable hostname verifications (trusting everything)

Top Android Apps

X509HostnameVerifier	% of Apps
ALLOW_ALL_HOSTNAME	**35% (29% 1st party code; 86% 3rd party code)**
	e.g. Facebook, Baidu, Conviva, Comscore, Nielson,…
STRICT_HOSTNAME	30.31%
BROWSER_COMPATIBLE_HOSTNAME	19.29%

Other Features	Number of Apps
Custom Trust Store	6.30%
	Average: 13 CAs; **Min**: 1 CA (8 apps); **Max**: 129 CAs (1 app)



Protecting Yourself

Protecting yourself

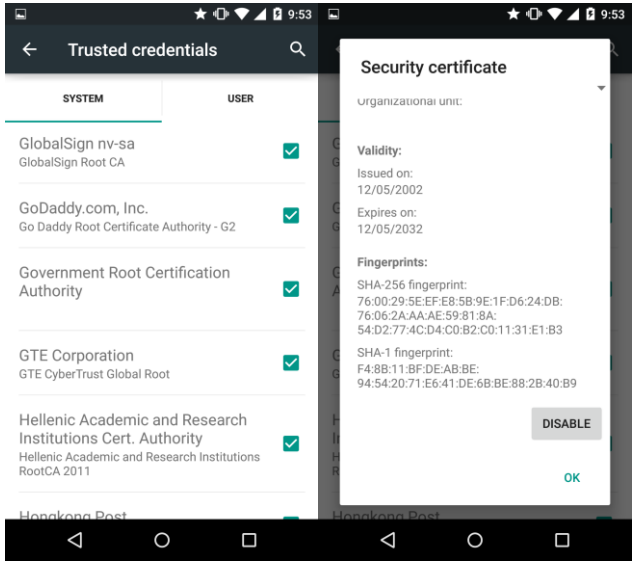
- Beware of government controlled root CAs, example: Kazakhstan (December 2015)
  - User installed (at this time)
  - http://www.zdnet.com/article/kazakhstan-forces-its-citizens-into-installing-internet-backdoors/
  - https://bugzilla.mozilla.org/show_bug.cgi?id=1232689

Managing your Security

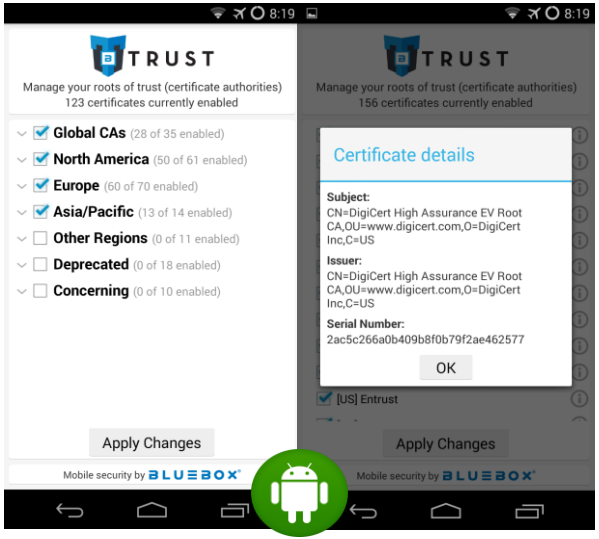
- Traveling or worried about security?
  - Remove or disable any CAs that concern you (government, deprecated, or others)
    - Test that the sites you need access to work with your restricted CA list
  - Be wary of installing **iOS profiles**, **device admin apps**, or **3rd party certificates**
    - Check your Security (Android) and Profile (iOS) settings
    - Some organizations use these to manage your device (check with your IT department)
    - Manage/disable root access when traveling (malware can exploit this)
  - Disable/remove apps you don't need (they're chatty and may be using insecure communications)
  - Beware of free / un-secured WiFi

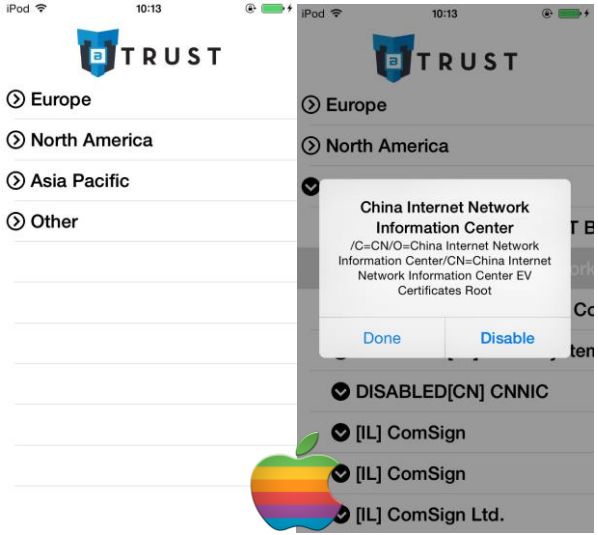
Managing your CAs

- **Android:**
  - System Settings
    - Settings -> Security -> Trusted credentials
    - Disable or Enable each CA
  - Programmatically or via shell
    - (requires root access)
- **iOS:**
  - No manual method on iOS
  - Programmatically or via shell
    - (requires root access)



Bluebox Trust Managers





https://bluebox.com/technical/trust-managers/

Apply

- **Executive / Management Team**
  - Secure the apps and data your company and employees use
  - Always use secure communications and apps; be aware of the trust chain
- **Developer**
  - Apply browser strategies for root certs to your app
  - Check, Validate, and enforce the expected chain of trust to your servers
- **Consumer**
  - Review, disable, and remove certificates you don't trust
  - Keep your trust store up to date

Summary

- CAs provide the trust for the internet's security model
- CAs are known to have failures in trust
- Mobile operating systems vary with their support for the vast number of CAs
- Mobile apps should not rely on the device (or CAs) to be trustable
- Users can take action to reduce the amount of 3rd parties they trust.
- Protect yourself

Q&A

- **Contact us**
  - **Andrew Blaich**
    - Lead Security Analyst at Bluebox Security
    - Twitter: @ablaich
    - Email: andrew@bluebox.com
  - **Jeff Forristal**
    - CTO at Bluebox Security
    - Twitter: @j4istal
    - Email: jeff@bluebox.com

References

- https://bluebox.com/questioning-the-chain-of-trust-investigations-into-the-root-certificates-on-mobile-devices/
- https://bluebox.com/technical/trust-managers/