RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: MBS-R03

Decrease Your Circle of Trust: An Investigation of PKI CAs on Mobile Devices

Andrew Blaich, PhD

Lead Security Analyst
Bluebox Security
@ablaich

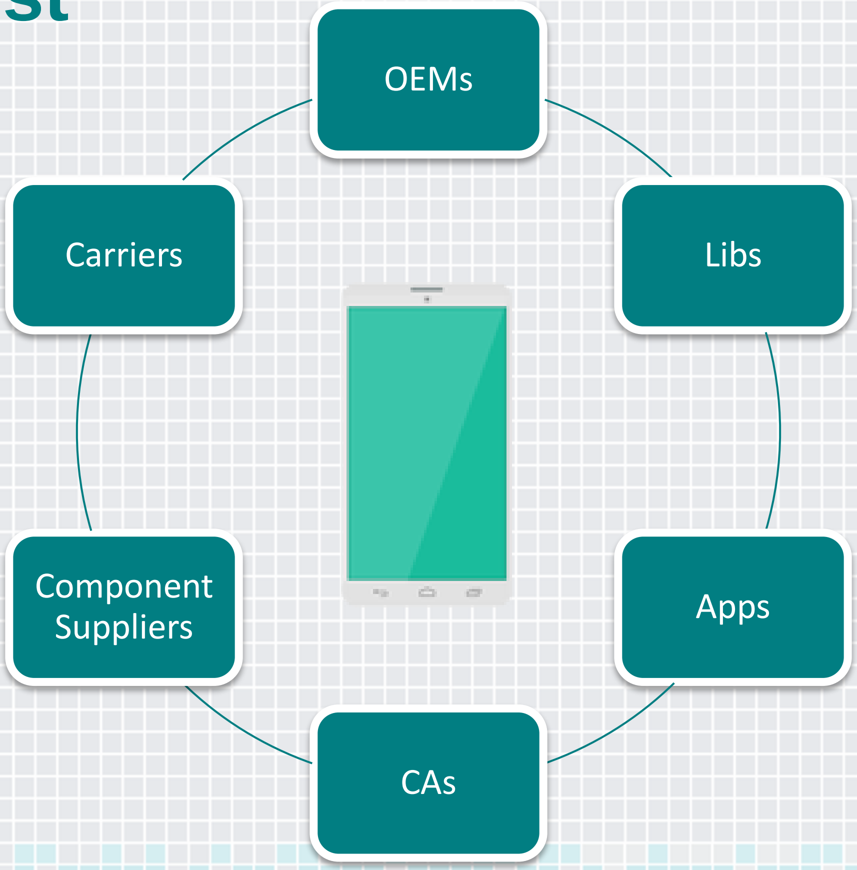
Who are you trusting?

- How much trust do you put in your phone?
  - How many vendors have modified your OS?
  - How many applications and services are running on your device?
  - How many libraries are loaded for an app?
  - How many roots of trust exist for network connections?

Who are you trusting?

- How much trust do you put in your phone?
  - How many vendors have modified your OS?
    - Google -> Samsung -> Qualcomm -> AT&T -> Others?
  - How many applications and services are running on your device?
    - 300+ apps/services on a Samsung Galaxy Note 3
  - How many libraries are loaded for an app?
    - 100+ shared libraries on a Samsung Galaxy Note 3
  - How many entities are trusted for network connections?
    - 150 + on Android
    - 200+ on iOS

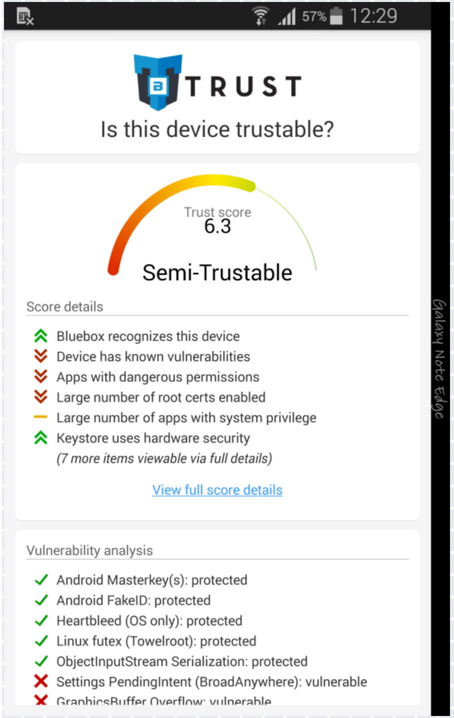
Circle of Trust



Trust

Circle

Trustable by Bluebox



Is this device trustable?

Trust score
6.3

Semi-Trustable

Score details

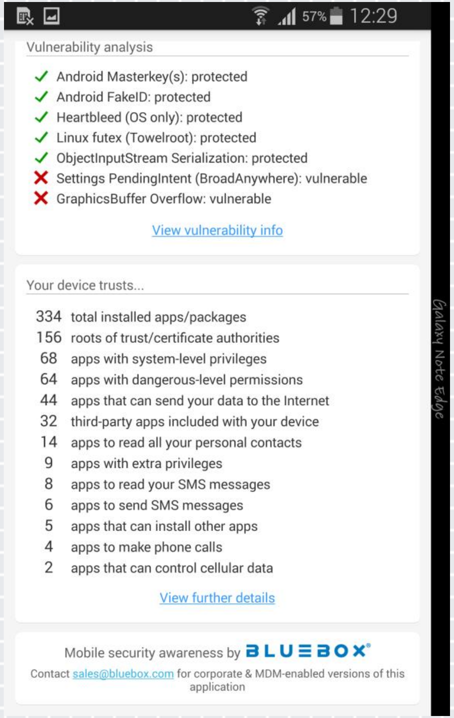
- ▲ Bluebox recognizes this device
- ▼ Device has known vulnerabilities
- ▼ Apps with dangerous permissions
- ▼ Large number of root certs enabled
- — Large number of apps with system privilege
- ▲ Keystore uses hardware security

(7 more items viewable via full details)

View full score details

Vulnerability analysis

- ✓ Android Masterkey(s): protected
- ✓ Android FakeID: protected
- ✓ Heartbleed (OS only): protected
- ✓ Linux futex (Towelroot): protected
- ✓ ObjectInputStream Serialization: protected
- ✗ Settings PendingIntent (BroadAnywhere): vulnerable
- ✗ GraphicsBuffer Overflow: vulnerable



Vulnerability analysis

- ✓ Android Masterkey(s): protected
- ✓ Android FakeID: protected
- ✓ Heartbleed (OS only): protected
- ✓ Linux futex (Towelroot): protected
- ✓ ObjectInputStream Serialization: protected
- ✗ Settings PendingIntent (BroadAnywhere): vulnerable
- ✗ GraphicsBuffer Overflow: vulnerable

View vulnerability info

Your device trusts...

334	total installed apps/packages
156	roots of trust/certificate authorities
68	apps with system-level privileges
64	apps with dangerous-level permissions
44	apps that can send your data to the Internet
32	third-party apps included with your device
14	apps to read all your personal contacts
9	apps with extra privileges
8	apps to read your SMS messages
6	apps to send SMS messages
5	apps that can install other apps
4	apps to make phone calls
2	apps that can control cellular data

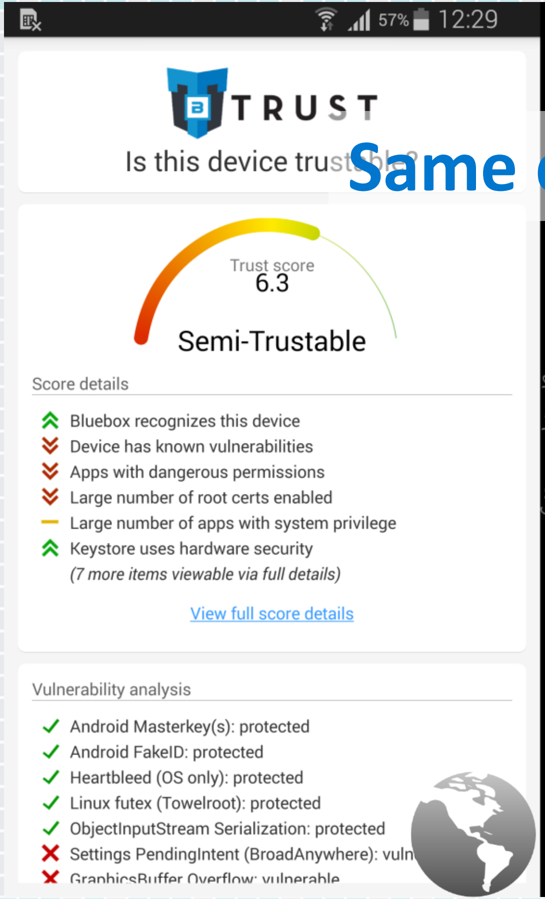
View further details

Mobile security awareness by BLUEBOX®

Contact sales@bluebox.com for corporate & MDM-enabled versions of this application

Example of a brand new out of the box device and all the entities that you would trust on it.

Same device, different carriers



12:29 57%

TRUST

Is this device trust

Trust score
6.3
Semi-Trustable

Score details

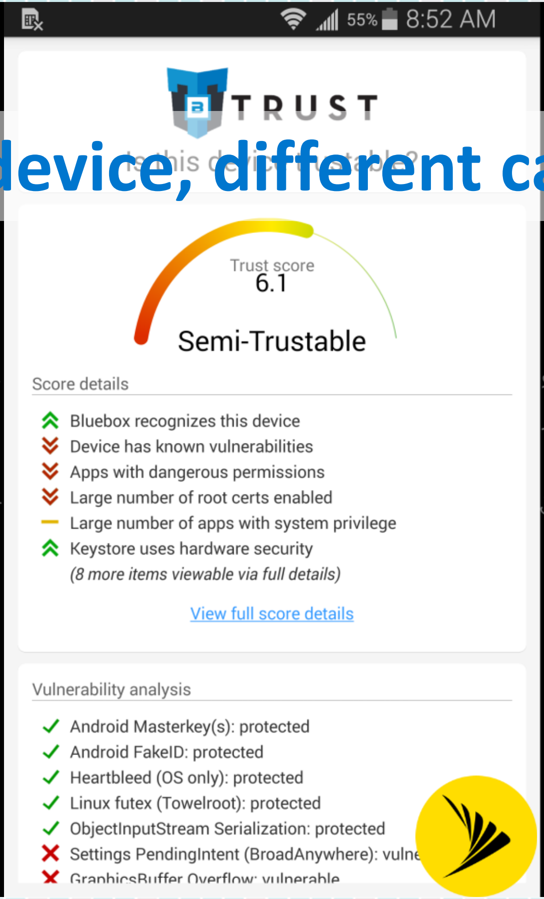
- ▲ Bluebox recognizes this device
- ▼ Device has known vulnerabilities
- ▼ Apps with dangerous permissions
- ▼ Large number of root certs enabled
- — Large number of apps with system privilege
- ▲ Keystore uses hardware security

(7 more items viewable via full details)

View full score details

Vulnerability analysis

- ✓ Android Masterkey(s): protected
- ✓ Android FakeID: protected
- ✓ Heartbleed (OS only): protected
- ✓ Linux futex (Towelroot): protected
- ✓ ObjectInputStream Serialization: protected
- ✗ Settings PendingIntent (BroadAnywhere): vuln
- ✗ GraphicsBuffer Overflow: vulnerable



8:52 AM 55%

TRUST

Is this device trustable?

Trust score
6.1
Semi-Trustable

Score details

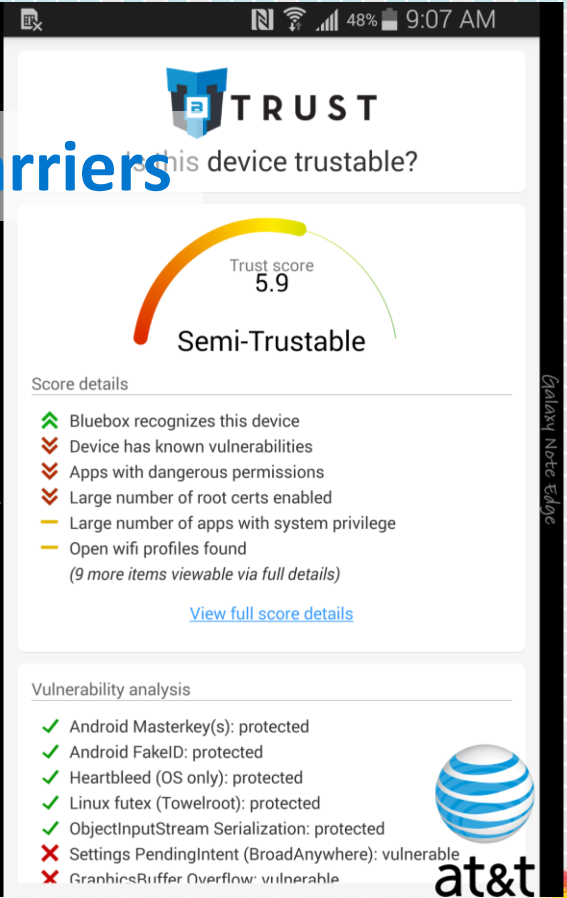
- ▲ Bluebox recognizes this device
- ▼ Device has known vulnerabilities
- ▼ Apps with dangerous permissions
- ▼ Large number of root certs enabled
- — Large number of apps with system privilege
- ▲ Keystore uses hardware security

(8 more items viewable via full details)

View full score details

Vulnerability analysis

- ✓ Android Masterkey(s): protected
- ✓ Android FakeID: protected
- ✓ Heartbleed (OS only): protected
- ✓ Linux futex (Towelroot): protected
- ✓ ObjectInputStream Serialization: protected
- ✗ Settings PendingIntent (BroadAnywhere): vulne
- ✗ GraphicsBuffer Overflow: vulnerable



9:07 AM 48%

TRUST

Is this device trustable?

Trust score
5.9
Semi-Trustable

Score details

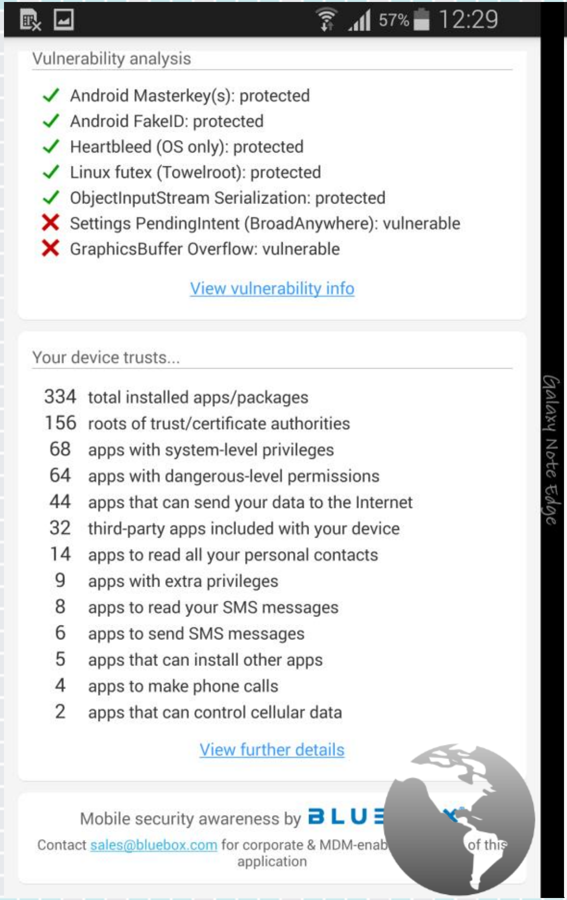
- ▲ Bluebox recognizes this device
- ▼ Device has known vulnerabilities
- ▼ Apps with dangerous permissions
- ▼ Large number of root certs enabled
- — Large number of apps with system privilege
- — Open wifi profiles found

(9 more items viewable via full details)

View full score details

Vulnerability analysis

- ✓ Android Masterkey(s): protected
- ✓ Android FakeID: protected
- ✓ Heartbleed (OS only): protected
- ✓ Linux futex (Towelroot): protected
- ✓ ObjectInputStream Serialization: protected
- ✗ Settings PendingIntent (BroadAnywhere): vulnerable
- ✗ GraphicsBuffer Overflow: vulnerable



Vulnerability analysis

- ✓ Android Masterkey(s): protected
- ✓ Android FakeID: protected
- ✓ Heartbleed (OS only): protected
- ✓ Linux futex (Towelroot): protected
- ✓ ObjectInputStream Serialization: protected
- ✗ Settings PendingIntent (BroadAnywhere): vulnerable
- ✗ GraphicsBuffer Overflow: vulnerable

View vulnerability info

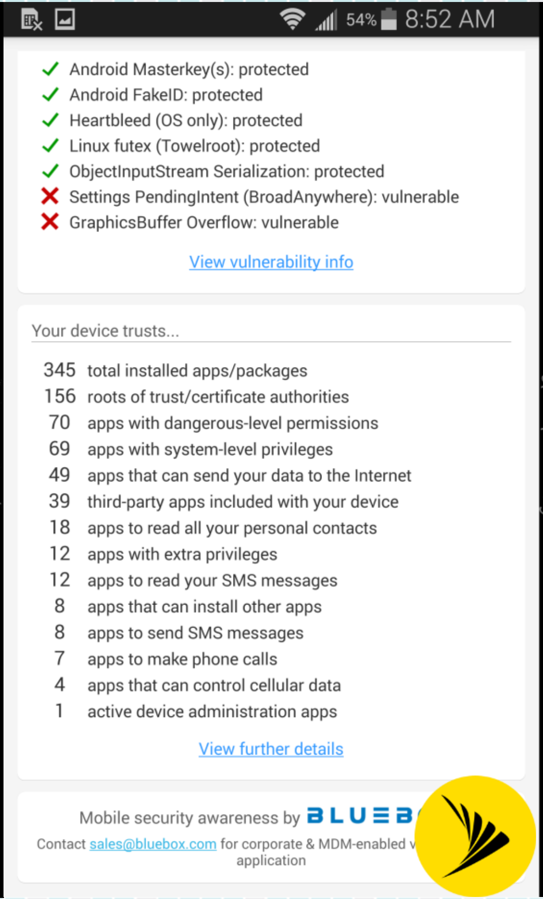
Your device trusts...

334	total installed apps/packages
156	roots of trust/certificate authorities
68	apps with system-level privileges
64	apps with dangerous-level permissions
44	apps that can send your data to the Internet
32	third-party apps included with your device
14	apps to read all your personal contacts
9	apps with extra privileges
8	apps to read your SMS messages
6	apps to send SMS messages
5	apps that can install other apps
4	apps to make phone calls
2	apps that can control cellular data

View further details

Mobile security awareness by BLU

Contact sales@bluebox.com for corporate & MDM-enab of this application



- ✓ Android Masterkey(s): protected
- ✓ Android FakeID: protected
- ✓ Heartbleed (OS only): protected
- ✓ Linux futex (Towelroot): protected
- ✓ ObjectInputStream Serialization: protected
- ✗ Settings PendingIntent (BroadAnywhere): vulnerable
- ✗ GraphicsBuffer Overflow: vulnerable

View vulnerability info

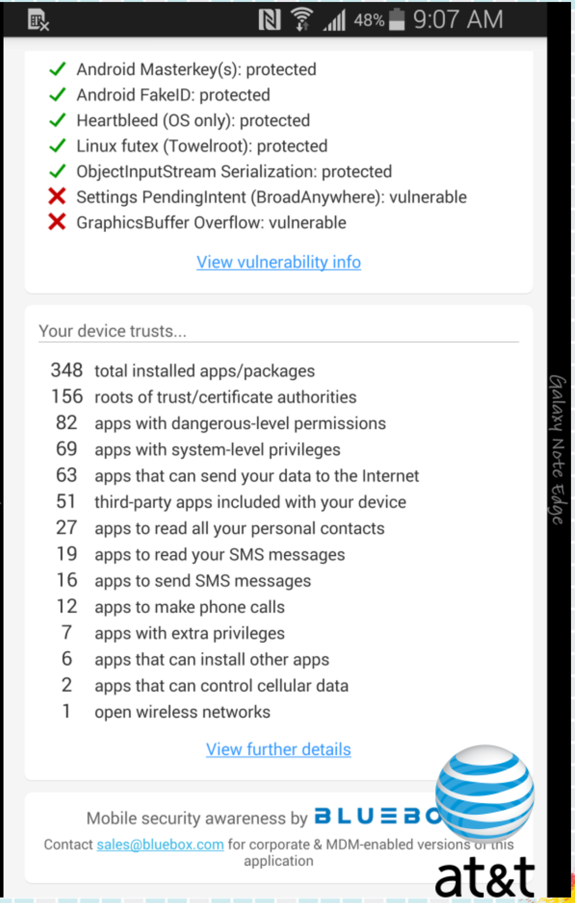
Your device trusts...

345	total installed apps/packages
156	roots of trust/certificate authorities
70	apps with dangerous-level permissions
69	apps with system-level privileges
49	apps that can send your data to the Internet
39	third-party apps included with your device
18	apps to read all your personal contacts
12	apps with extra privileges
12	apps to read your SMS messages
8	apps that can install other apps
8	apps to send SMS messages
7	apps to make phone calls
4	apps that can control cellular data
1	active device administration apps

View further details

Mobile security awareness by BLUEB

Contact sales@bluebox.com for corporate & MDM-enabled v application



- ✓ Android Masterkey(s): protected
- ✓ Android FakeID: protected
- ✓ Heartbleed (OS only): protected
- ✓ Linux futex (Towelroot): protected
- ✓ ObjectInputStream Serialization: protected
- ✗ Settings PendingIntent (BroadAnywhere): vulnerable
- ✗ GraphicsBuffer Overflow: vulnerable

View vulnerability info

Your device trusts...

348	total installed apps/packages
156	roots of trust/certificate authorities
82	apps with dangerous-level permissions
69	apps with system-level privileges
63	apps that can send your data to the Internet
51	third-party apps included with your device
27	apps to read all your personal contacts
19	apps to read your SMS messages
16	apps to send SMS messages
12	apps to make phone calls
7	apps with extra privileges
6	apps that can install other apps
2	apps that can control cellular data
1	open wireless networks

View further details

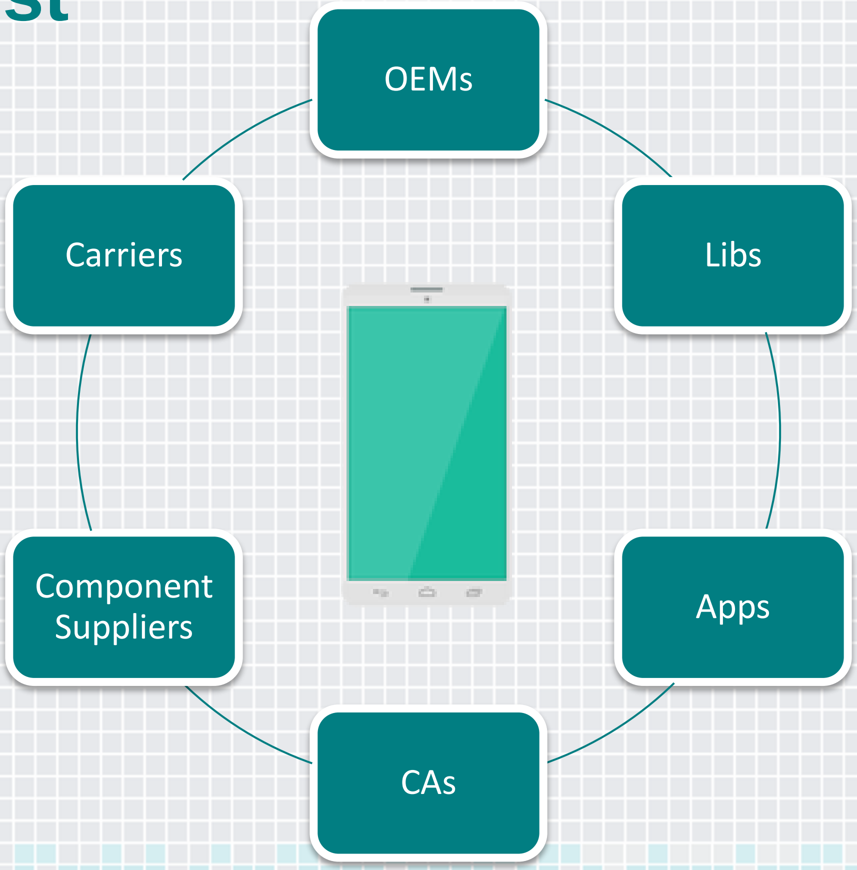
Mobile security awareness by BLUEBO

Contact sales@bluebox.com for corporate & MDM-enabled versions of this application

BLUEBOX

Circle of Trust

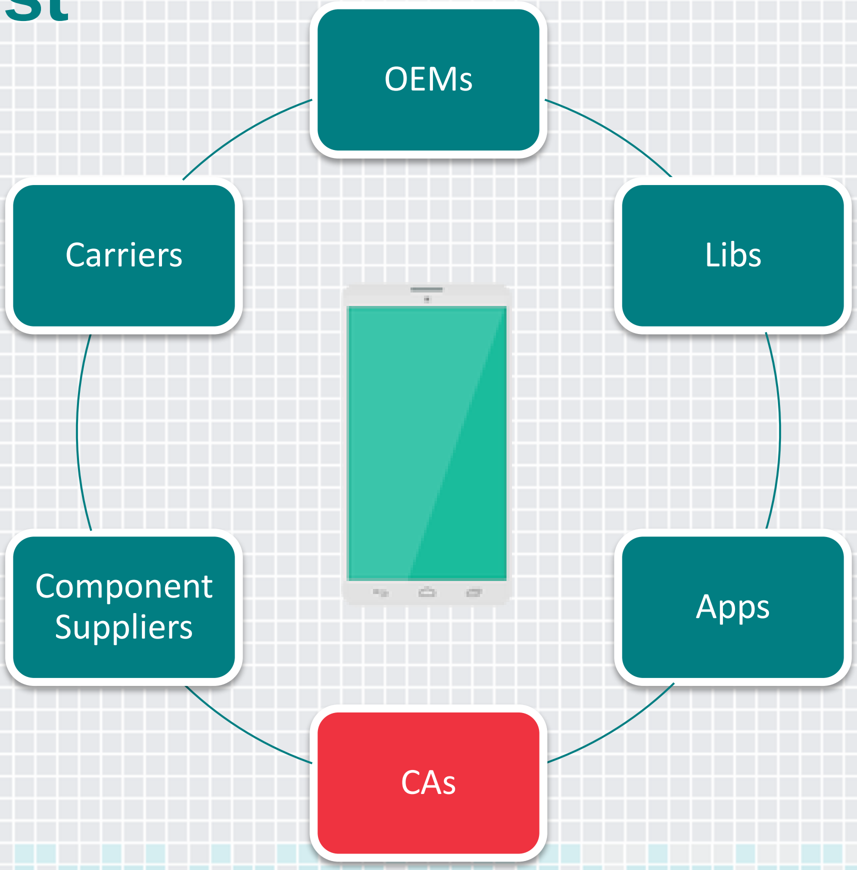
Trust



Circle

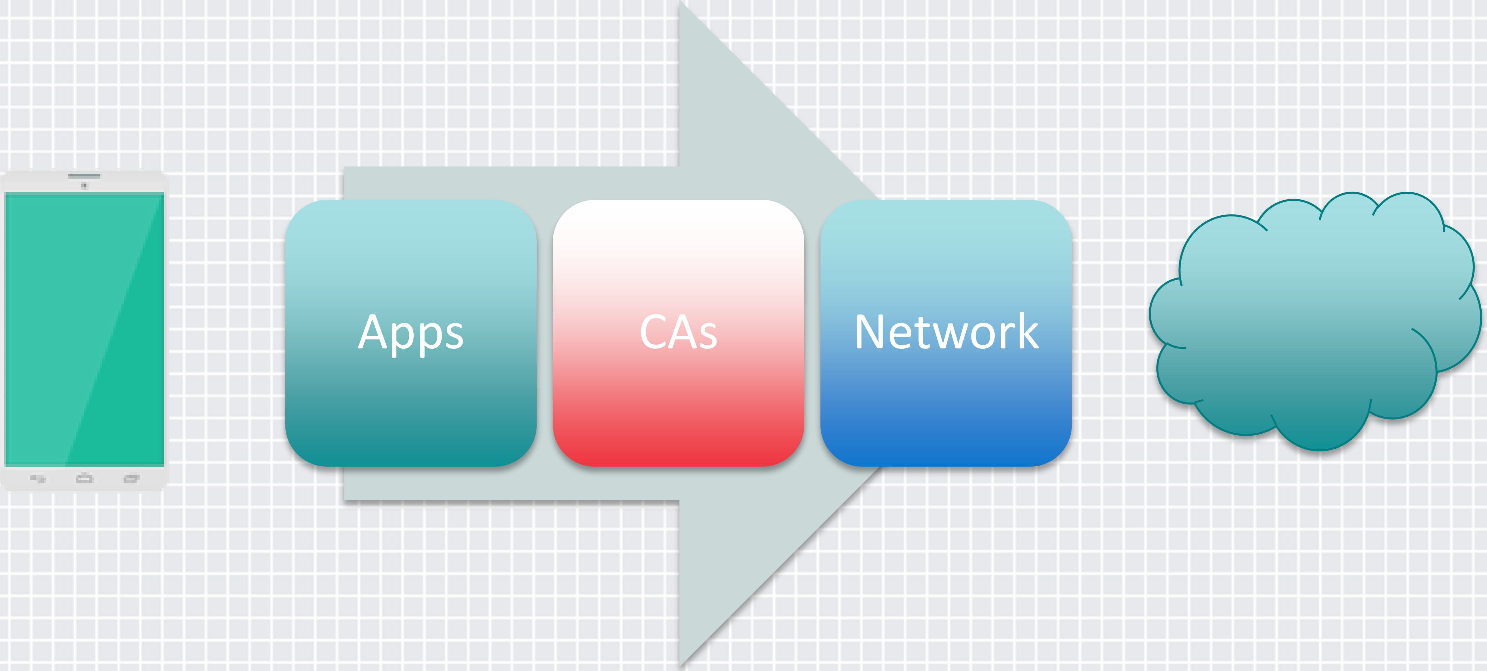
Circle of Trust

Trust

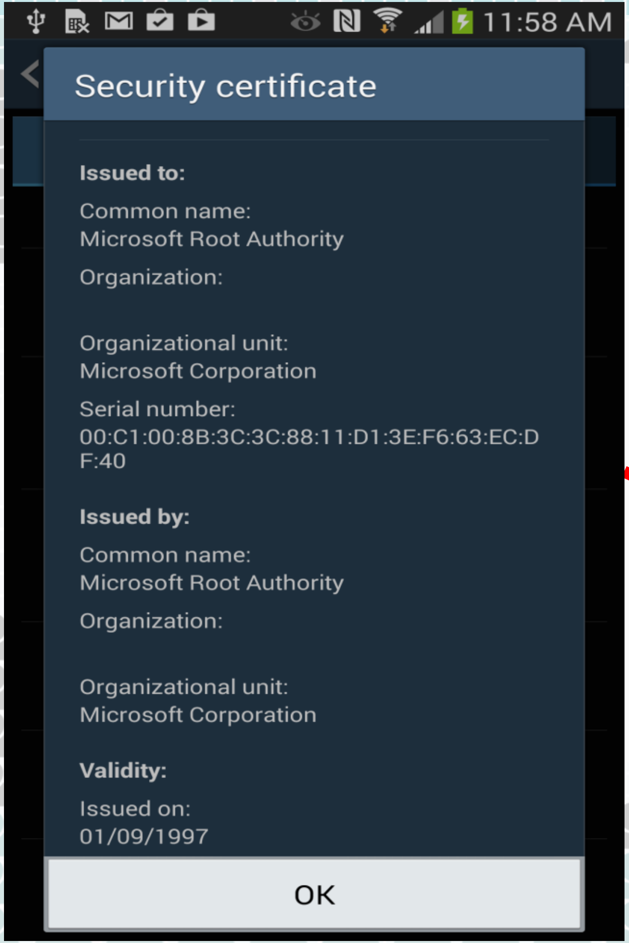


Circle

Secure Connections



SAMSUNG
QUALCOMM



11:58 AM

Security certificate

Issued to:

Common name:
Microsoft Root Authority

Organization:

Organizational unit:
Microsoft Corporation

Serial number:
00:C1:00:8B:3C:3C:88:11:D1:3E:F6:63:EC:D
F:40

Issued by:

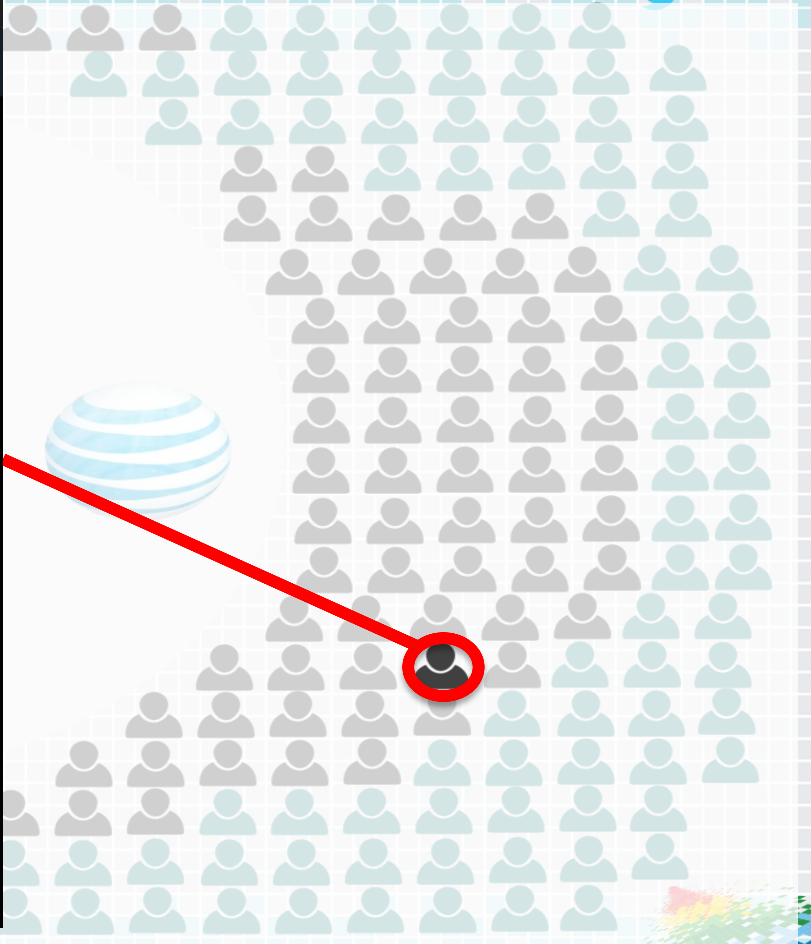
Common name:
Microsoft Root Authority

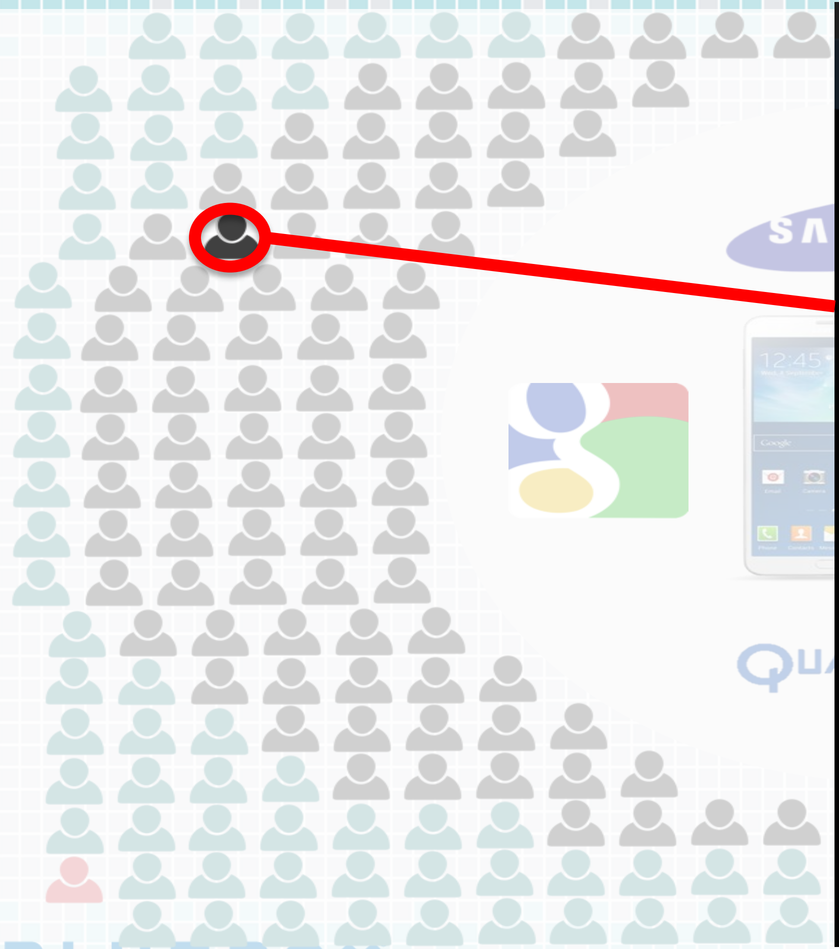
Organization:

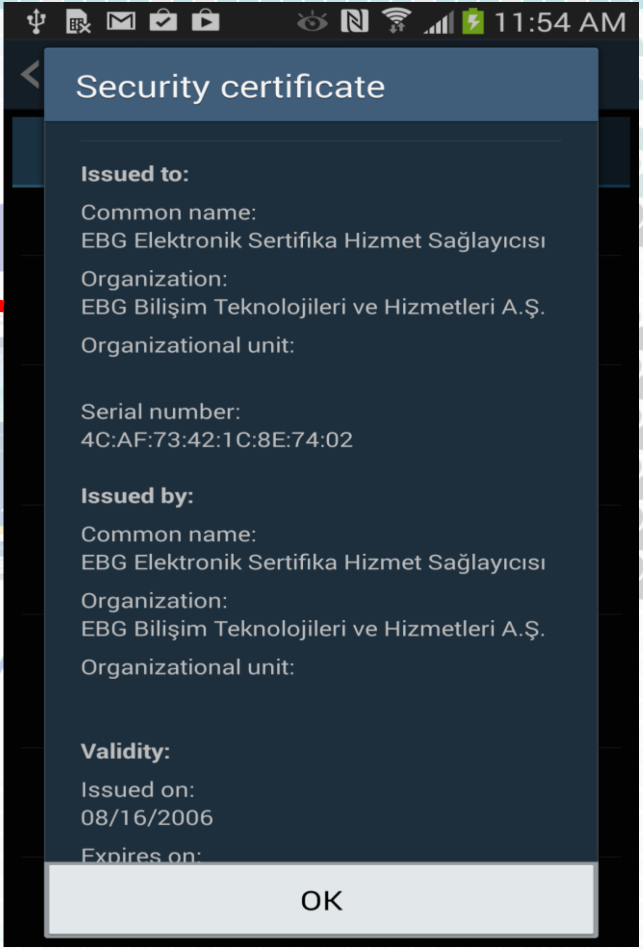
Organizational unit:
Microsoft Corporation

Validity:

Issued on:
01/09/1997







Security certificate

Issued to:

Common name:
EBG Elektronik Sertifika Hizmet Sağlayıcısı

Organization:
EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.

Organizational unit:

Serial number:
4C:AF:73:42:1C:8E:74:02

Issued by:

Common name:
EBG Elektronik Sertifika Hizmet Sağlayıcısı

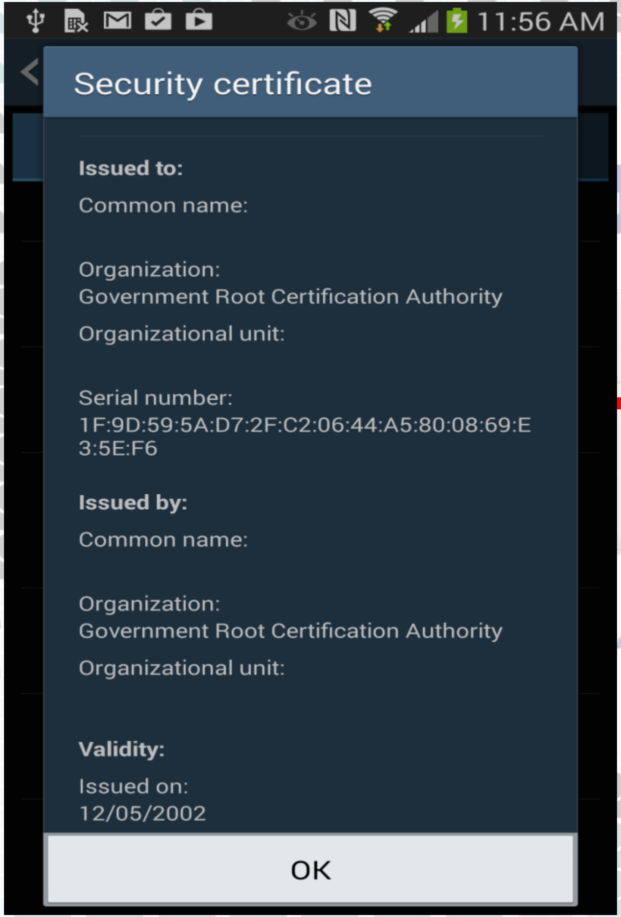
Organization:
EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.

Organizational unit:

Validity:

Issued on:
08/16/2006

Expires on:



Security certificate

Issued to:

Common name:

Organization:
Government Root Certification Authority

Organizational unit:

Serial number:
1F:9D:59:5A:D7:2F:C2:06:44:A5:80:08:69:E
3:5E:F6

Issued by:

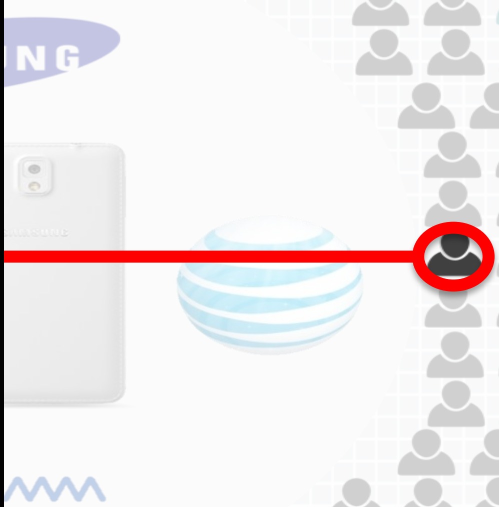
Common name:

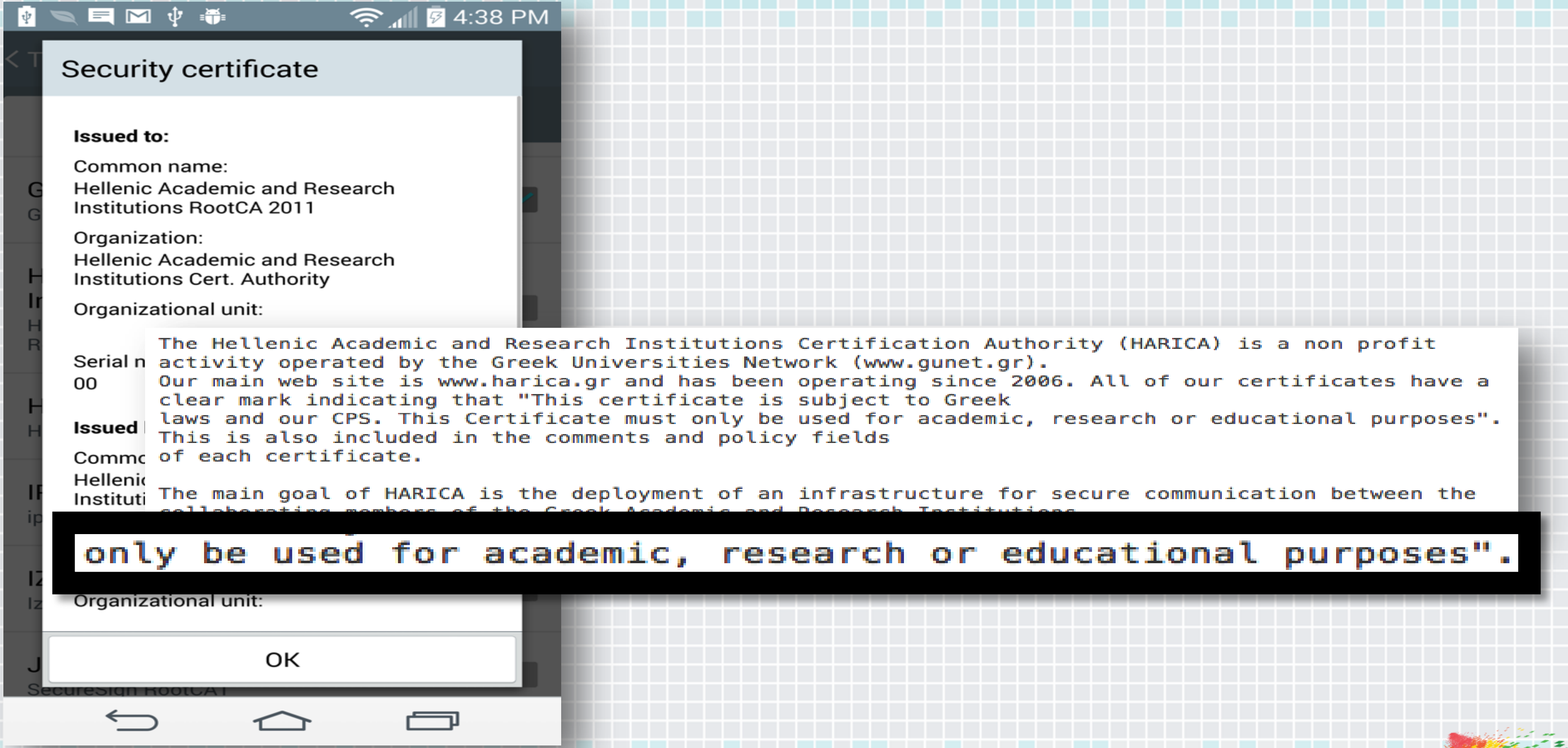
Organization:
Government Root Certification Authority

Organizational unit:

Validity:

Issued on:
12/05/2002





Security certificate

Issued to:

Common name:
Hellenic Academic and Research Institutions RootCA 2011

Organization:
Hellenic Academic and Research Institutions Cert. Authority

Organizational unit:

Serial n
00

Issued

Commo
Helleni
Instituti

Organizational unit:

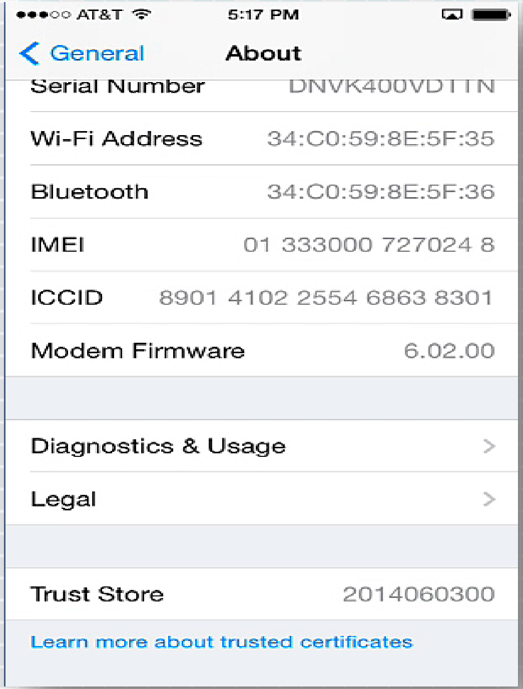
OK

SecureSign RootCA1

```
The Hellenic Academic and Research Institutions Certification Authority (HARICA) is a non profit
activity operated by the Greek Universities Network (www.gunet.gr).
Our main web site is www.harica.gr and has been operating since 2006. All of our certificates have a
clear mark indicating that "This certificate is subject to Greek
laws and our CPS. This Certificate must only be used for academic, research or educational purposes".
This is also included in the comments and policy fields
of each certificate.

The main goal of HARICA is the deployment of an infrastructure for secure communication between the
collaborating members of the Greek Academic and Research Institutions
```

only be used for academic, research or educational purposes".

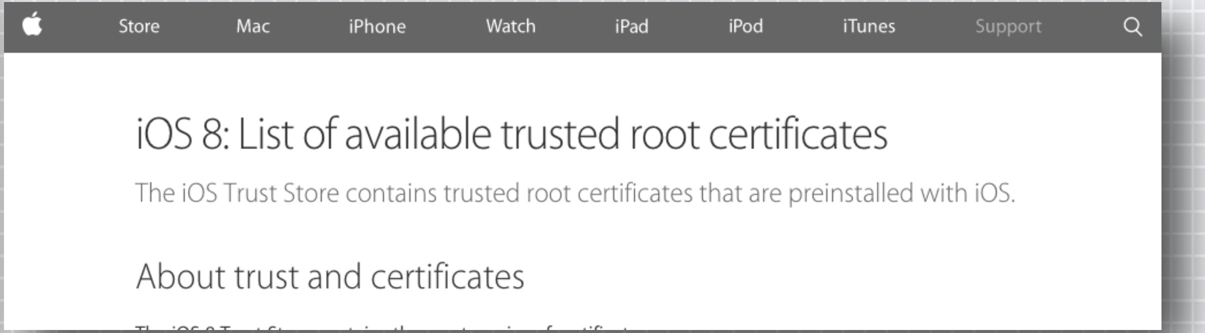


●●●○○ AT&T 5:17 PM

< General About

Serial Number	DNVK400VDTTN
Wi-Fi Address	34:C0:59:8E:5F:35
Bluetooth	34:C0:59:8E:5F:36
IMEI	01 333000 727024 8
ICCID	8901 4102 2554 6863 8301
Modem Firmware	6.02.00
Diagnostics & Usage	>
Legal	>
Trust Store	2014060300

Learn more about trusted certificates

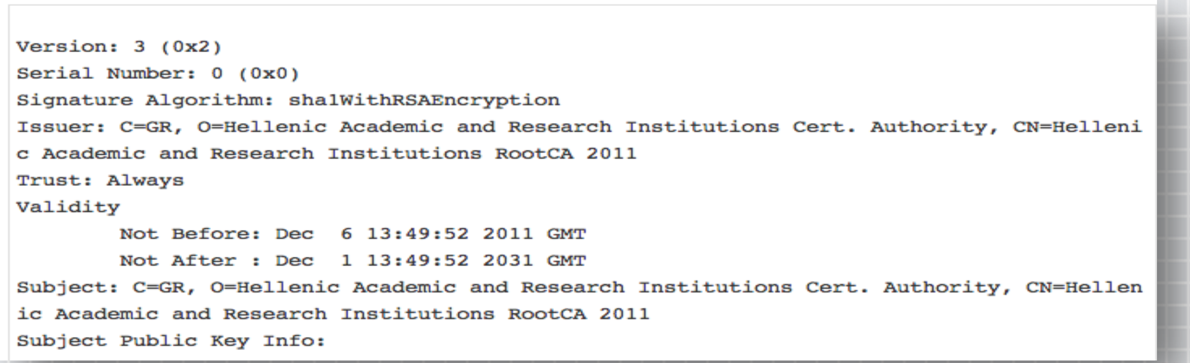


iOS 8: List of available trusted root certificates

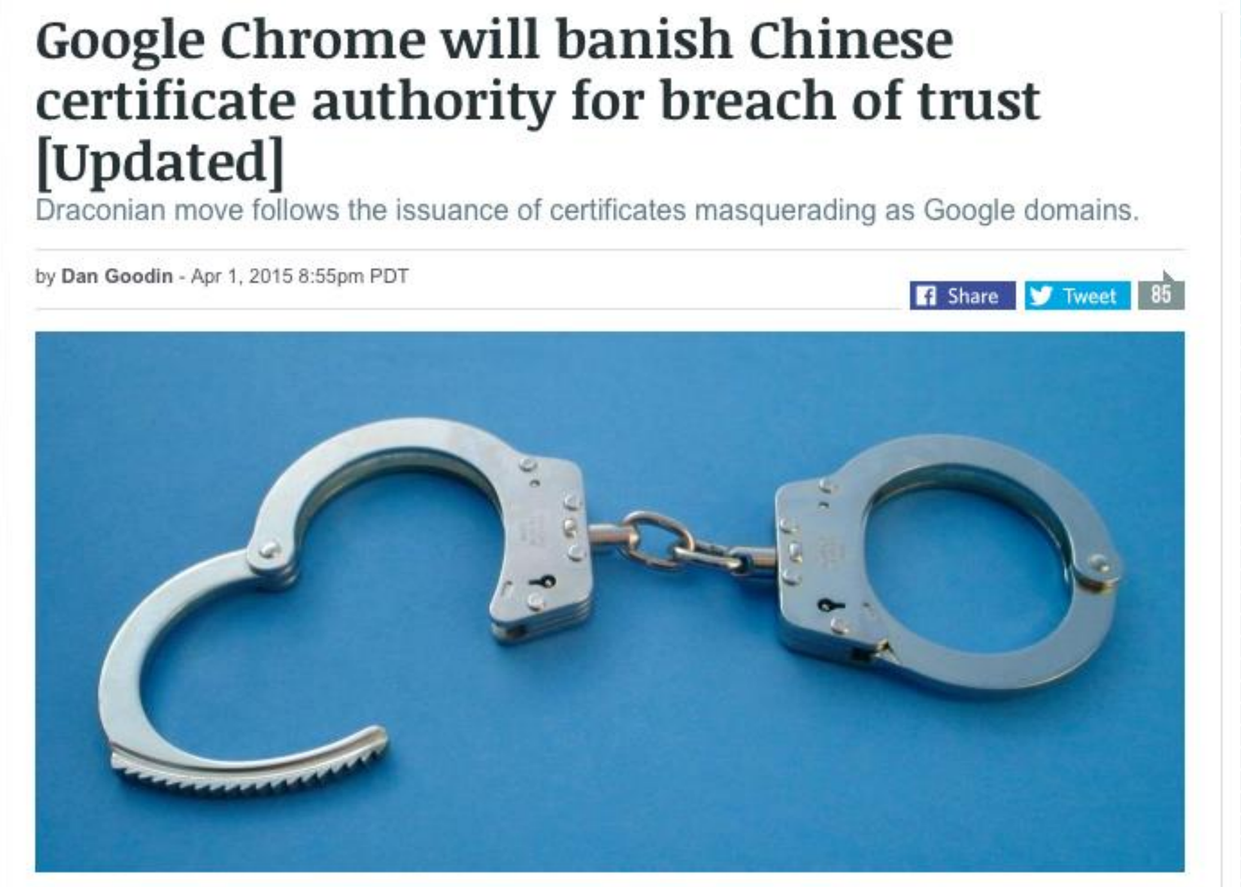
The iOS Trust Store contains trusted root certificates that are preinstalled with iOS.

About trust and certificates

...



```
Version: 3 (0x2)
Serial Number: 0 (0x0)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Helleni
c Academic and Research Institutions RootCA 2011
Trust: Always
Validity
        Not Before: Dec  6 13:49:52 2011 GMT
        Not After : Dec  1 13:49:52 2031 GMT
Subject: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellen
ic Academic and Research Institutions RootCA 2011
Subject Public Key Info:
```



Google Chrome will banish Chinese certificate authority for breach of trust [Updated]

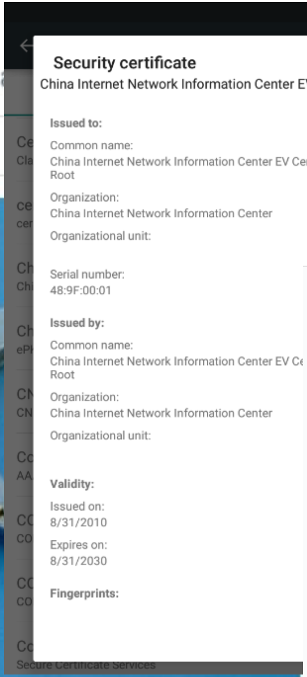
Draconian move follows the issuance of certificates masquerading as Google domains.

by **Dan Goodin** - Apr 1, 2015 8:55pm PDT

Google Chrome will banish Chinese certificate authority for breach of trust [Updated]

Draconian move follows the issuance of certificates masquerading

by **Dan Goodin** - Apr 1, 2015 8:55pm PDT



Security certificate

China Internet Network Information Center EV Certi..

Issued to:

Common name:
China Internet Network Information Center EV Certificates Root

Organization:
China Internet Network Information Center

Organizational unit:

Serial number:
48:9F:00:01

Issued by:

Common name:
China Internet Network Information Center EV Ce
Root

Organization:
China Internet Network Information Center

Organizational unit:

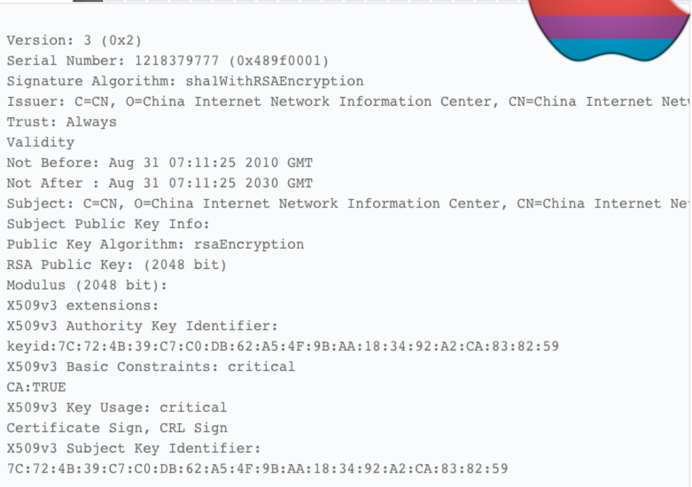
Validity:

Issued on:
8/31/2010

Expires on:
8/31/2030

Fingerprints:

Secure Certificate Services



```
Version: 3 (0x2)
Serial Number: 1218379777 (0x489f0001)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=CN, O=China Internet Network Information Center, CN=China Internet Net
Trust: Always
Validity
Not Before: Aug 31 07:11:25 2010 GMT
Not After : Aug 31 07:11:25 2030 GMT
Subject: C=CN, O=China Internet Network Information Center, CN=China Internet Ne
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
X509v3 extensions:
X509v3 Authority Key Identifier:
keyid:7C:72:4B:39:C7:C0:DB:62:A5:4F:9B:AA:18:34:92:A2:CA:83:82:59
X509v3 Basic Constraints: critical
CA:TRUE
X509v3 Key Usage: critical
Certificate Sign, CRL Sign
X509v3 Subject Key Identifier:
7C:72:4B:39:C7:C0:DB:62:A5:4F:9B:AA:18:34:92:A2:CA:83:82:59
```

Not only browsers…

Certificate Authorities

- What certificate authorities are on my device?
- How many are there?
- Who are these certificate authorities?
- How did they get on my device?
- What security concerns are there?

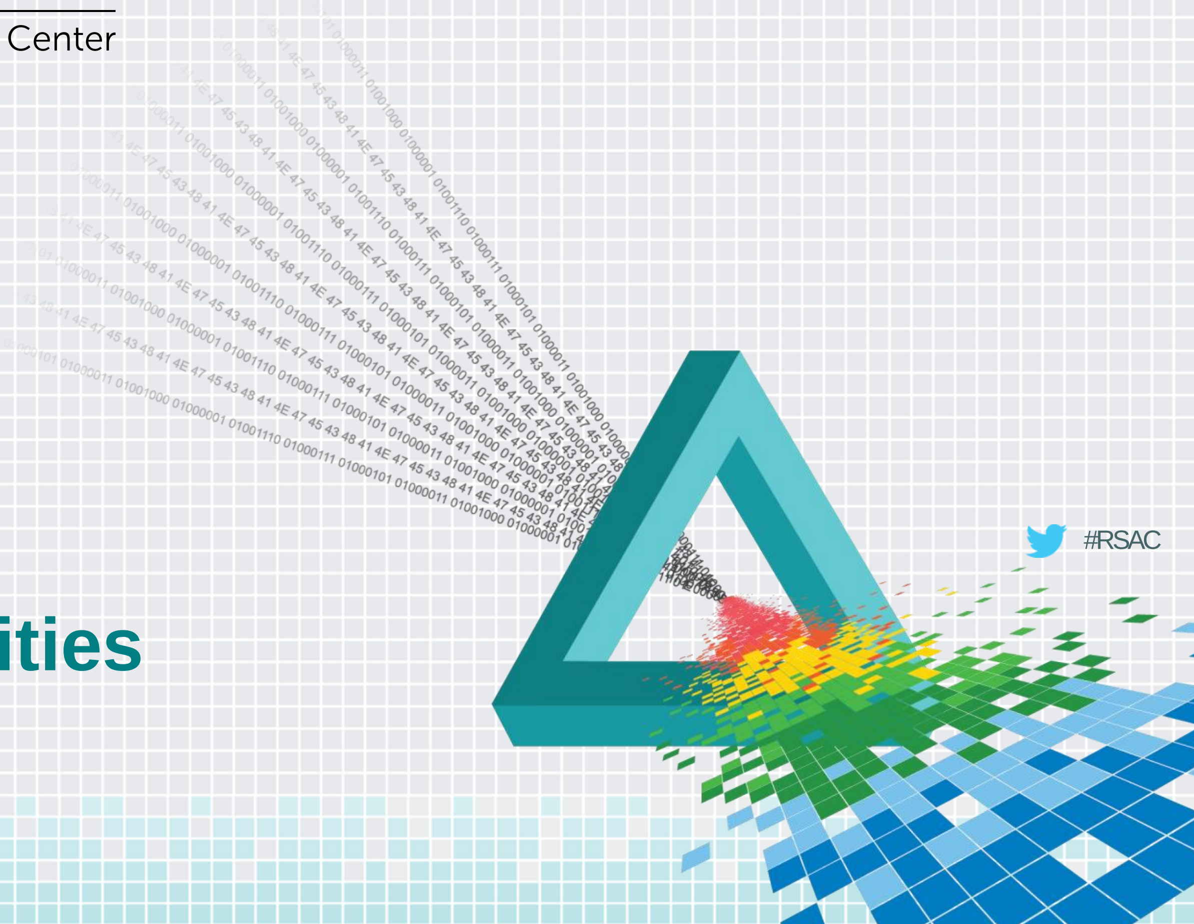
Objectives

- Learn more about who your device is trusting
- Learn about the roles CAs play in secure communications
- Learn the history behind these CAs
- Learn how you can take action to decrease your circle of trust

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Background - Certificate Authorities



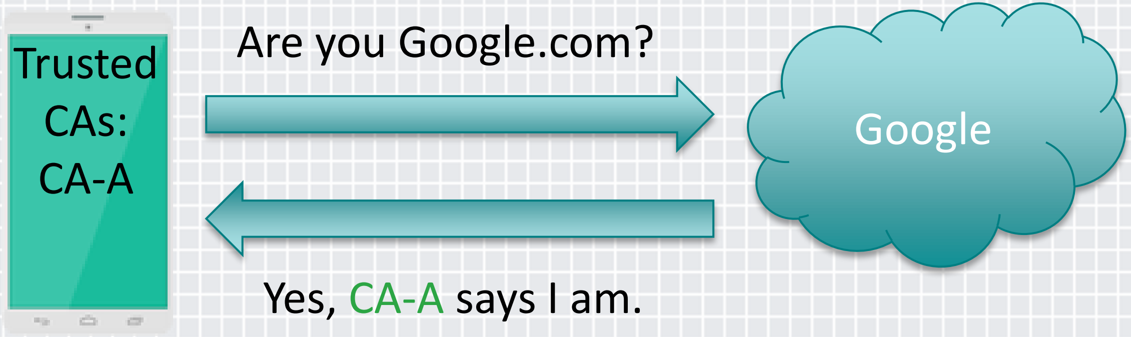
#RSAC

Body

- What is a CA?
- How do they get on the device?
- How many are there?
- User installable vs. system pre-loaded (also talk about carrier and OEM additions or removals)
- iOS VPN and Android VPN case study

Certificate Authorities

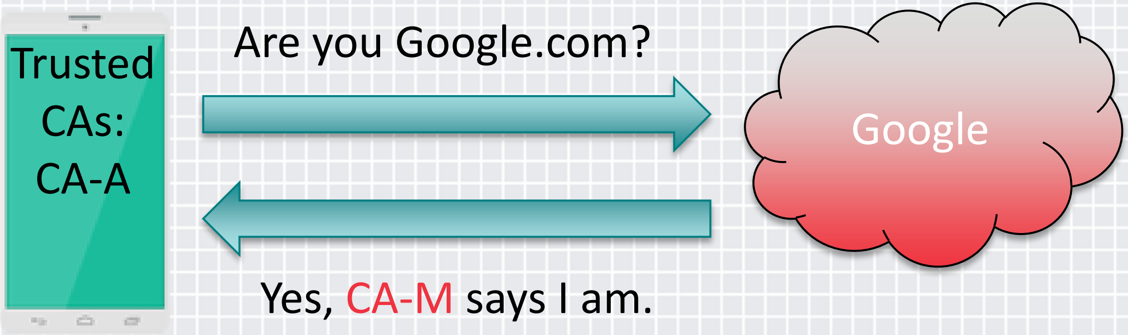
- What is a certificate authority?
  - They validate that who you are talking to is who they say they are



TRUSTED CONNECTION

Certificate Authorities

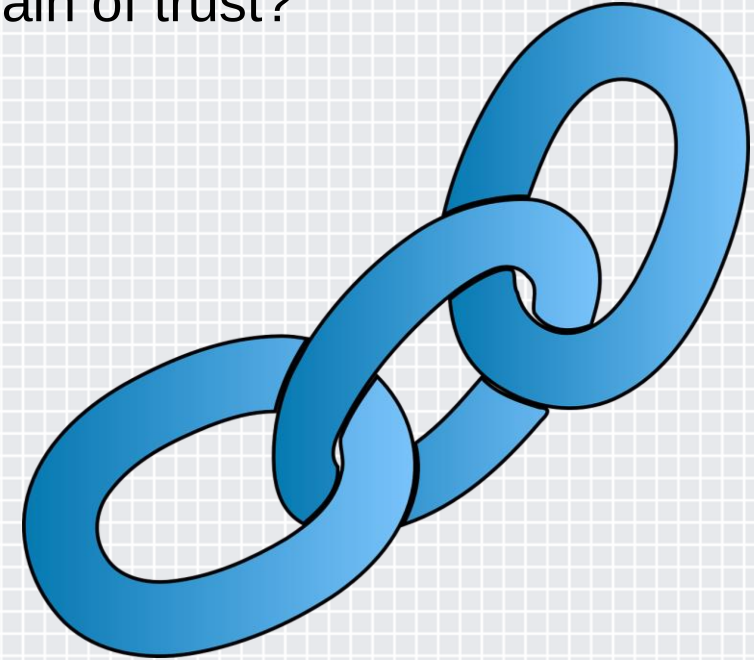
- What is a certificate authority?
  - They validate that who you are talking to is who they say they are



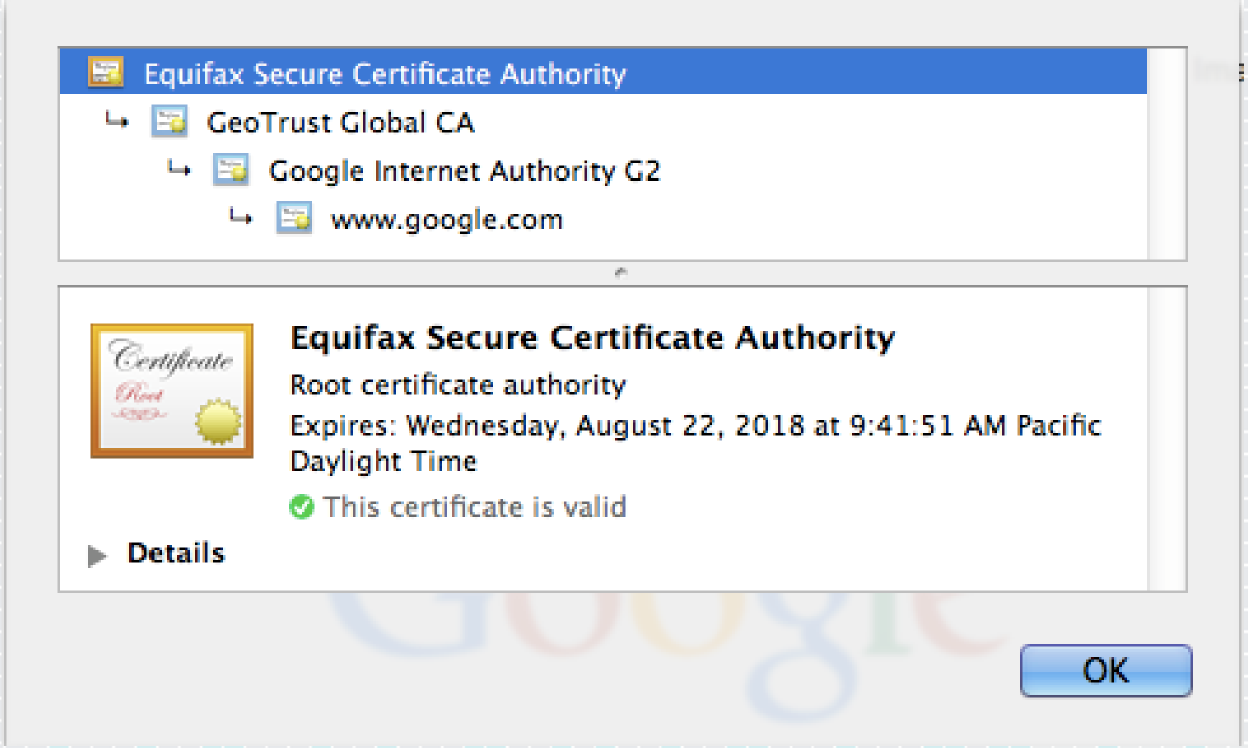
NOT TRUSTED CONNECTION

CA Chain of Trust

- What is the chain of trust?



Trusted Certificate Chain



Equifax Secure Certificate Authority

↳ GeoTrust Global CA

↳ Google Internet Authority G2

↳ www.google.com

Equifax Secure Certificate Authority

Root certificate authority

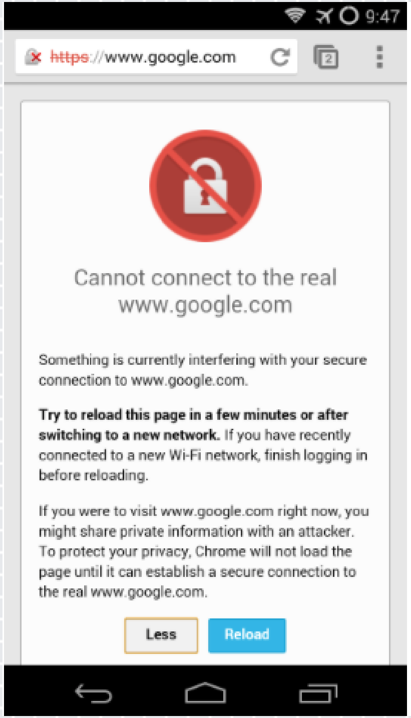
Expires: Wednesday, August 22, 2018 at 9:41:51 AM Pacific Daylight Time

✓ This certificate is valid

Verified == Trusted Chain

The root CA to verify this chain is installed on the device making the trust chain verifiable and thus it is considered a trusted and secured connection.

Un-trusted Certificate Chain

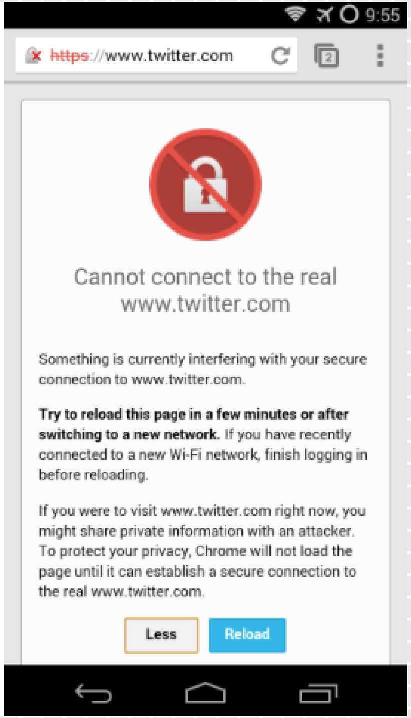


Cannot connect to the real www.google.com

Something is currently interfering with your secure connection to www.google.com.

Try to reload this page in a few minutes or after switching to a new network. If you have recently connected to a new Wi-Fi network, finish logging in before reloading.

If you were to visit www.google.com right now, you might share private information with an attacker. To protect your privacy, Chrome will not load the page until it can establish a secure connection to the real www.google.com.



Cannot connect to the real www.twitter.com

Something is currently interfering with your secure connection to www.twitter.com.

Try to reload this page in a few minutes or after switching to a new network. If you have recently connected to a new Wi-Fi network, finish logging in before reloading.

If you were to visit www.twitter.com right now, you might share private information with an attacker. To protect your privacy, Chrome will not load the page until it can establish a secure connection to the real www.twitter.com.

Un-verified == Un-Trusted Chain

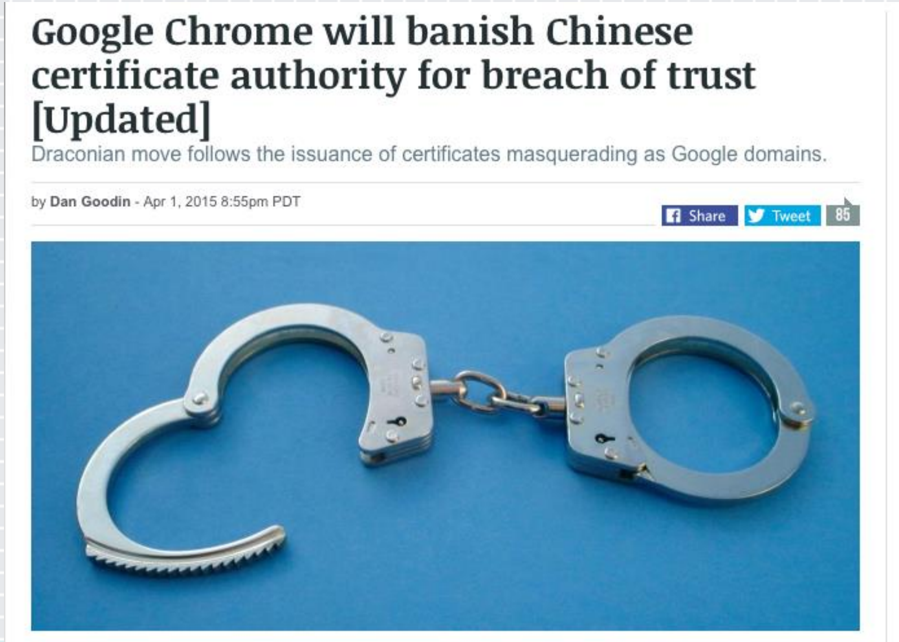
The root CA to verify this chain is missing from this device making the trust chain un-verifiable and thus not-trusted and in-secure.

Types of Root CAs

- Pre-installed root CAs
- User-installed root CAs

Why is this a concern?

- A malicious or compromised root CA can read your secure traffic
  - CNNIC and MCS Holdings
  - Lenovo and Superfish
  - …



Google Chrome will banish Chinese certificate authority for breach of trust [Updated]

Draconian move follows the issuance of certificates masquerading as Google domains.

by **Dan Goodin** - Apr 1, 2015 8:55pm PDT

RSAConference2015

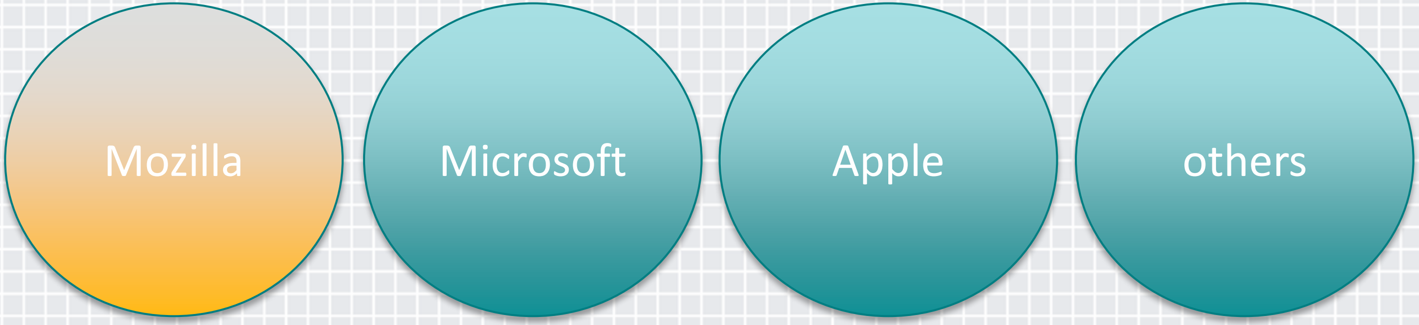
San Francisco | April 20-24 | Moscone Center

#RSAC

Pre-installed Root CAs

Root CA Approval Process

Root Certificate Programs



Mozilla

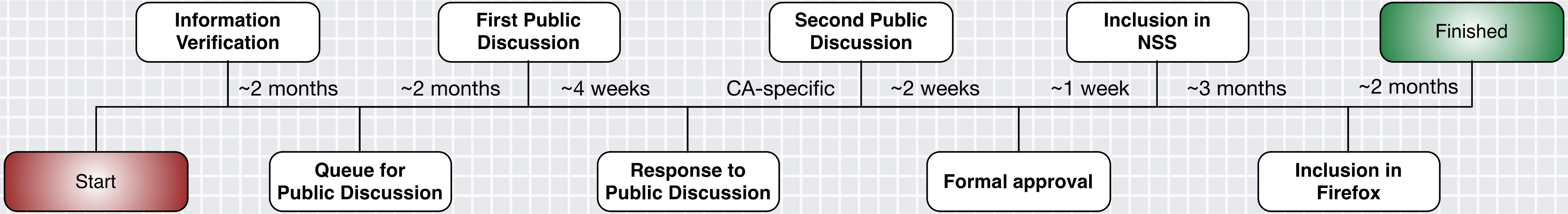
Microsoft

Apple

others

Mozilla Root CA Approval Process

How a CA gets included into Firefox
https://wiki.mozilla.org/CA:How_to_apply#Timeline



Start

~2 months

Information Verification

~2 months

Queue for Public Discussion

~2 months

First Public Discussion

~4 weeks

Response to Public Discussion

CA-specific

Second Public Discussion

~2 weeks

Formal approval

~1 week

Inclusion in NSS

~3 months

Inclusion in Firefox

~2 months

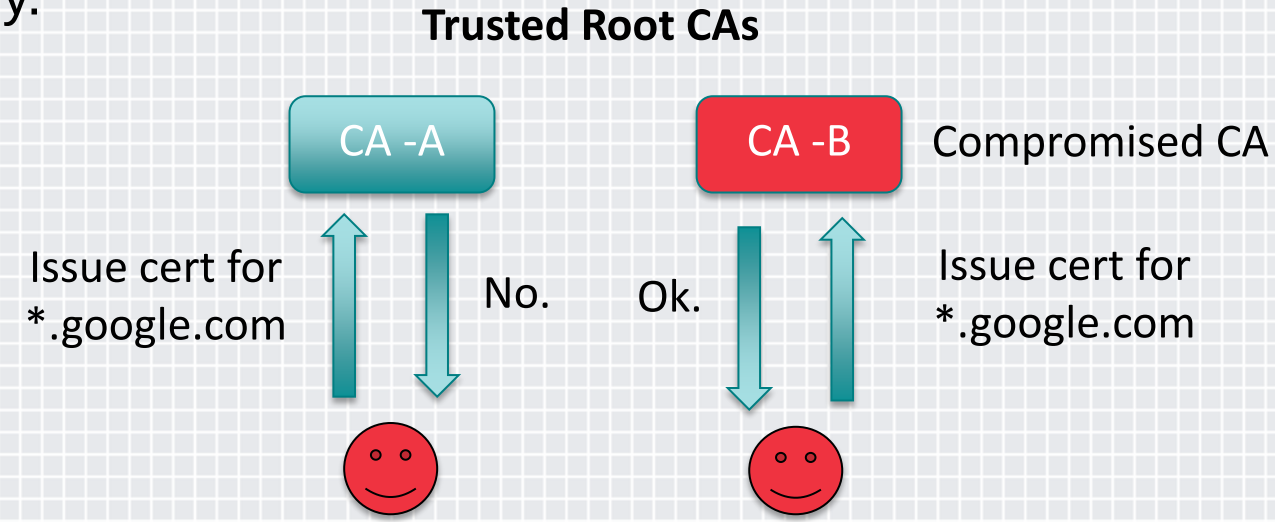
Finished

The whole process can take approximately 11 months or more.

Linux and Android are strongly tied to the Mozilla process.

CA Trust Infrastructure

- The effectiveness of the global PKI trust infrastructure relies on keeping the designated roots of trust fully secure and operating correctly.



CAs on Mobile Devices

5.1	162
8.3	227

System Installed Certificates

Root CA Reference Links

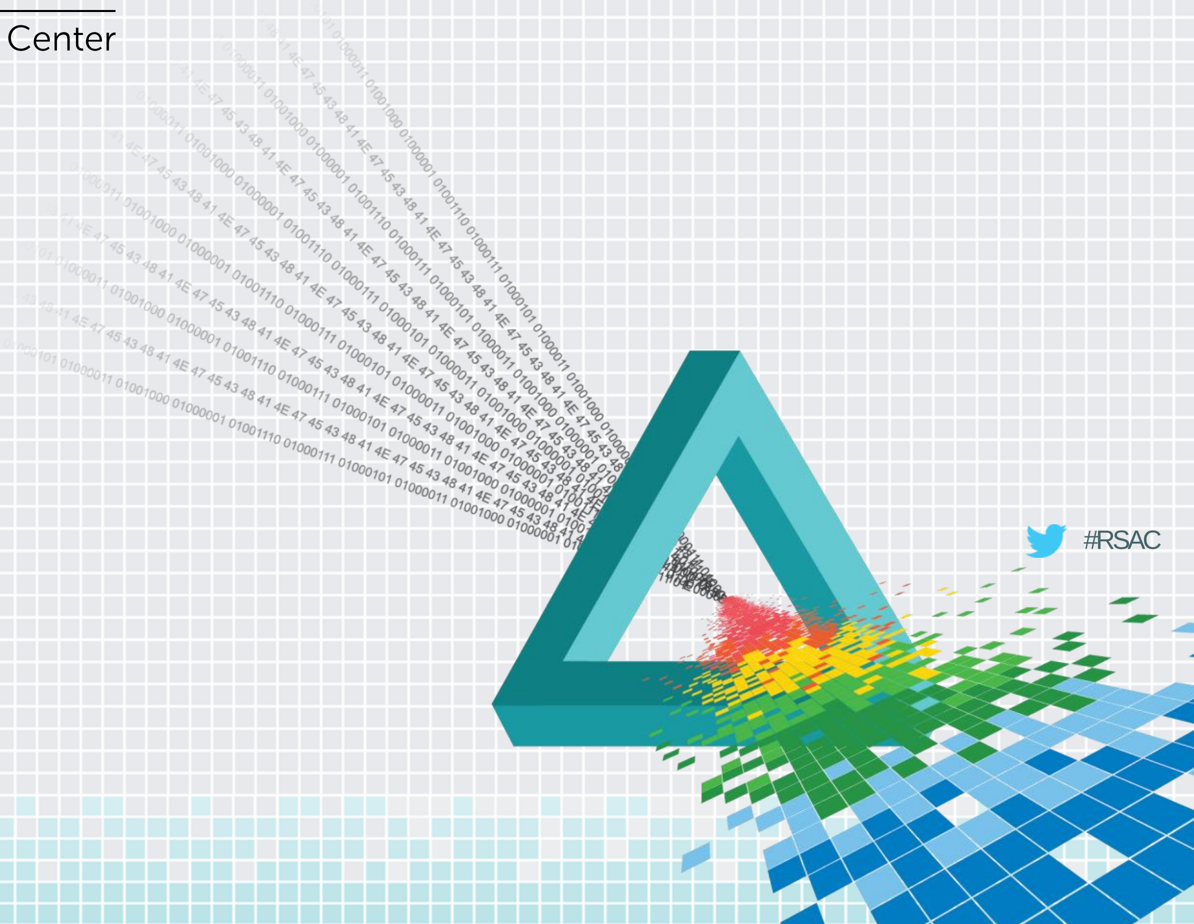
- **iOS:**
  - http://support.apple.com/en-us/HT204132
    - Trusted
    - Always Ask
    - Blocked
- **Android:**
  - https://android.googlesource.com/platform/libcore/+/master/luni/src/main/files/cacerts/

CA Classifications

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

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

Known Failures

Known Failures with CAs

- **“Hacked” CAs:**
  - CNNIC/MCS Holdings [2015]
  - Comodo [2011]
  - DigiNotar [2011]
  - GlobalSign [2011]
  - India CCA [2014]
  - RapidSSL (indirect) [2008]

COMODO
Creating Trust Online™

CNNIC
中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

GlobalSign.

DigiNotar
Internet Trust Services

NATIONAL
INFORMATICS
CENTRE
NIC

RapidSSL

Apple's Blocked CA List

CA Name	Reasons
TurkTrust	Issued an inappropriate sub-CA cert that was used to issue a *.google.com cert
Entrust	Issued a wildcard cert for Apple domains
GTE CyberTrust Solutions	Issued 4 sub-CA certs for DigiNotar
DigiNotar	Issued itself another sub-CA cert
Entrust	Issued 2 sub-CA certs for DigiNotar
Entrust	Issued a sub-CA cert for Digicert Sdb. Bhd (practices of this CA in Malaysia were found to be inappropriate)

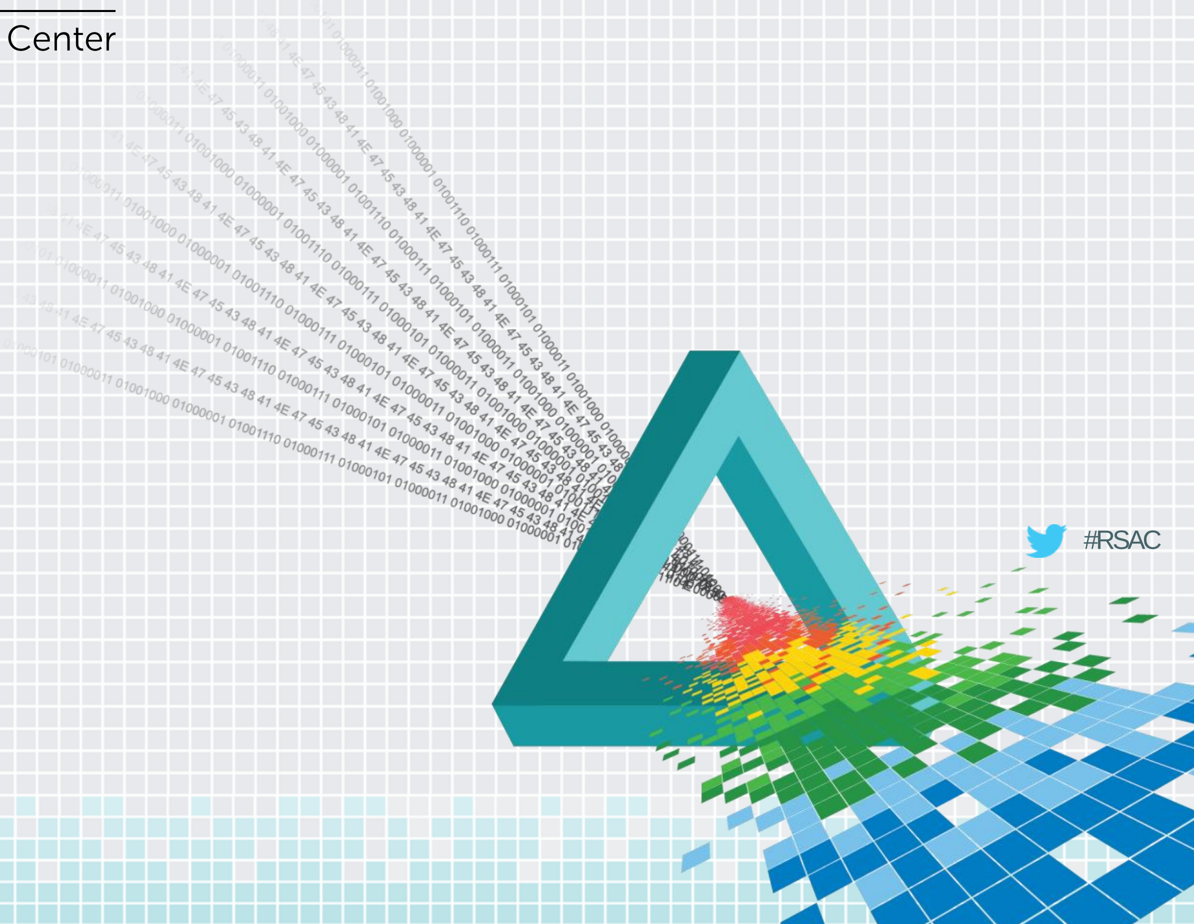
Apple’s Blocked CA List – cont’d.

CA Name	Reasons
GTE	Issued a sub-CA cert for Digicert Sdb. Bhd
Trustwave	Issued a sub-CA cert to Micros Systems
Xramp	Issued a sub-CA cert to Trustwave
TurkTrust	Issued a sub-CA cert to KKTC Merkez Bankasi

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Government CAs



#RSAC

Government Related CAs

Government CAs

- Govt. of Spain
Izenpe S.A.
- Govt. of Spain
ACCV
- Govt. of France
DCSSI
- Govt. of HongKong
HongKong Post Root
- Govt. of The Netherlands
Staat der Nederlanden
- Govt. of Taiwan
Government Root CA
- Govt. of South Korea
KISA
- Govt. of Japan
- Govt. of Turkey
Kamu SM
- Spanish FNMT

Suspected of affiliation with a government entity

- JCSI SecureSign
- SOCIEDAD CAMERAL DE CERTIFICACIÓN
- AC Camerfirma S.A.
- Agencia Catalana de Certificacio
- Chunghwa Telecom Co
- Autoridad de Certificacion Firmaprofesional
- CNNIC
- e-tugra
- TURKTRUST
- Elektronik Bilgi Guvenligi A.S.
- HARICA

Other nationally-operating entities

- French Postal Service
Certinomis
- Switzerland Post Office
SwissSign

Allowed to use an internal audit for approval.

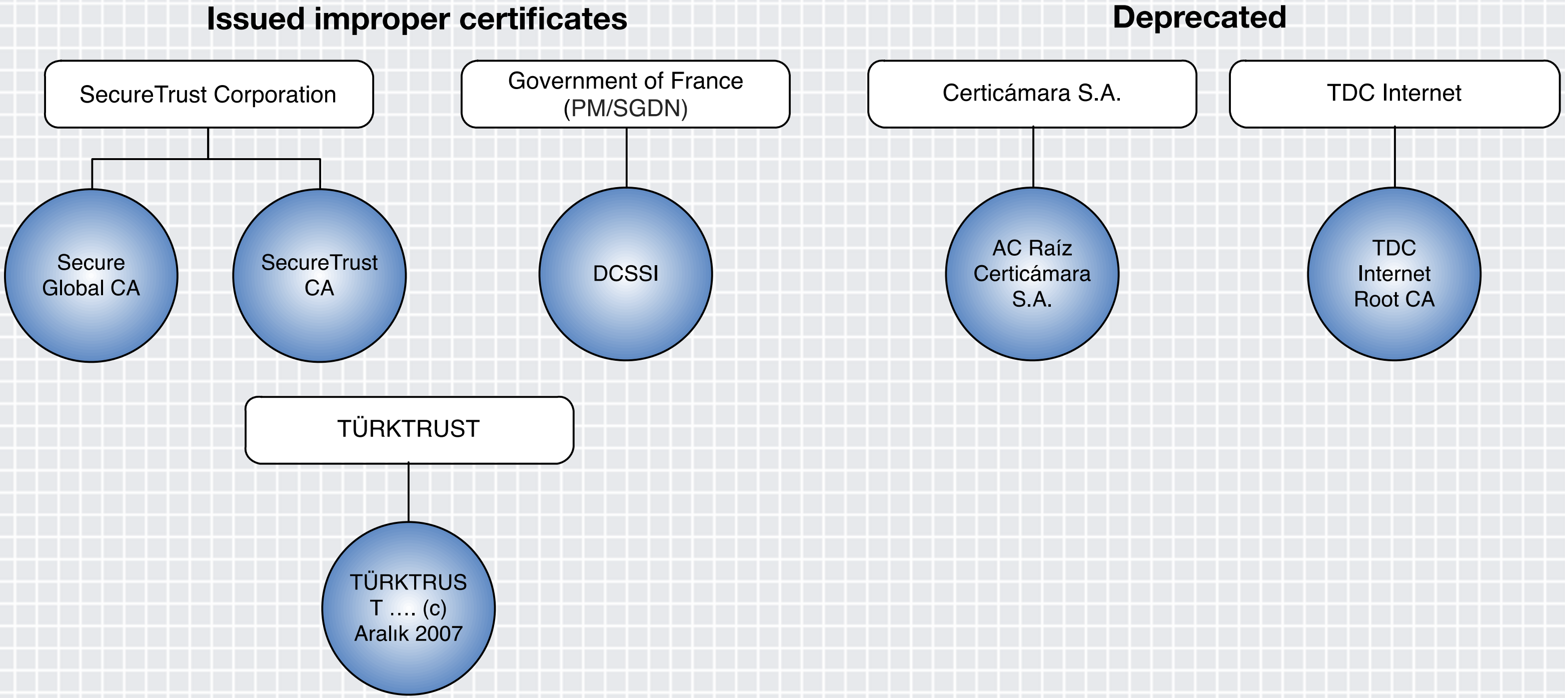
RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

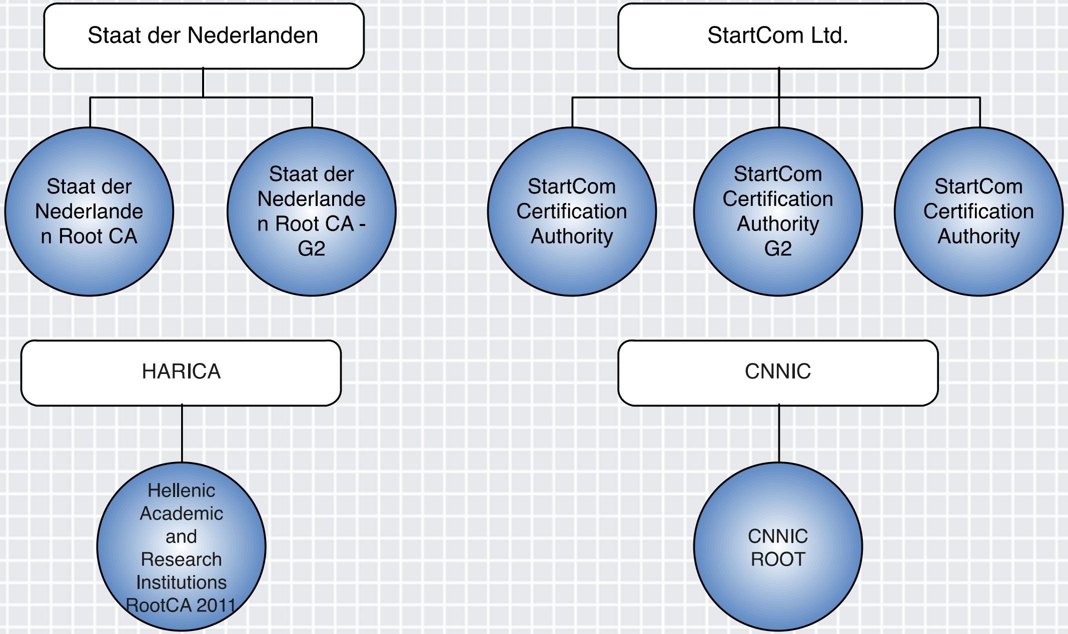
Causes for Concern - CAs

Causes for Concern



Causes for Concern – cont’d.

Community Controversy



Staat der Nederlanden

Staat der Nederlanden Root CA

Staat der Nederlanden Root CA - G2

StartCom Ltd.

StartCom Certification Authority

StartCom Certification Authority G2

StartCom Certification Authority

HARICA

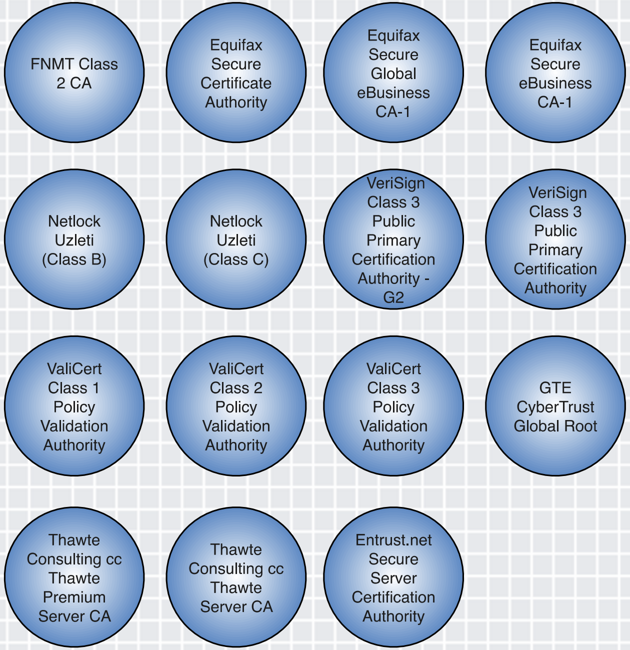
Hellenic Academic and Research Institutions RootCA 2011

CNNIC

CNNIC ROOT

Causes for Concern – cont’d.

Certificate Authorities using a 1024 bit key



FNMT Class 2 CA

Equifax Secure Certificate Authority

Equifax Secure Global eBusiness CA-1

Equifax Secure eBusiness CA-1

Netlock Uzleti (Class B)

Netlock Uzleti (Class C)

VeriSign Class 3 Public Primary Certification Authority - G2

VeriSign Class 3 Public Primary Certification Authority

ValiCert Class 1 Policy Validation Authority

ValiCert Class 2 Policy Validation Authority

ValiCert Class 3 Policy Validation Authority

GTE CyberTrust Global Root

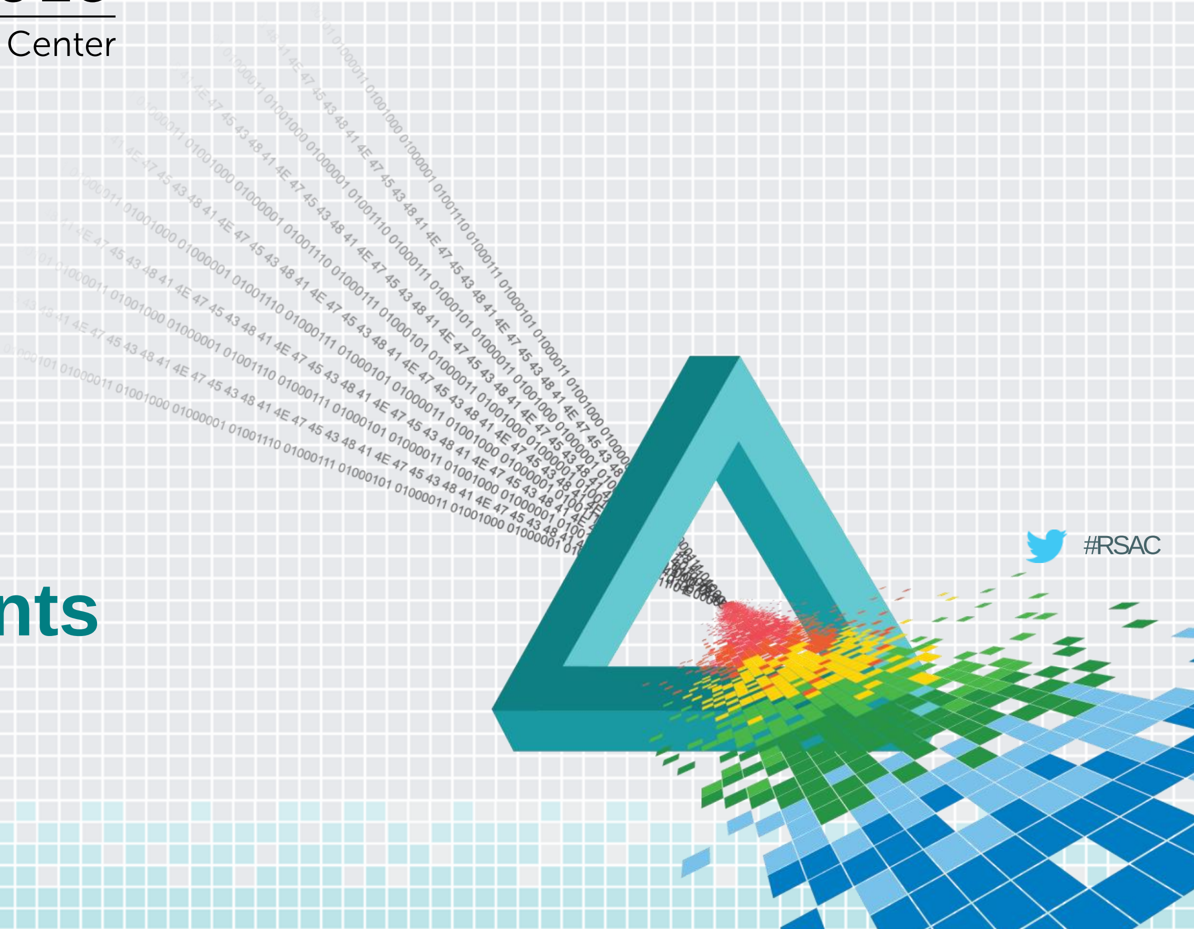
Thawte Consulting cc Thawte Premium Server CA

Thawte Consulting cc Thawte Server CA

Entrust.net Secure Server Certification Authority

RSAConference2015

San Francisco | April 20-24 | Moscone Center



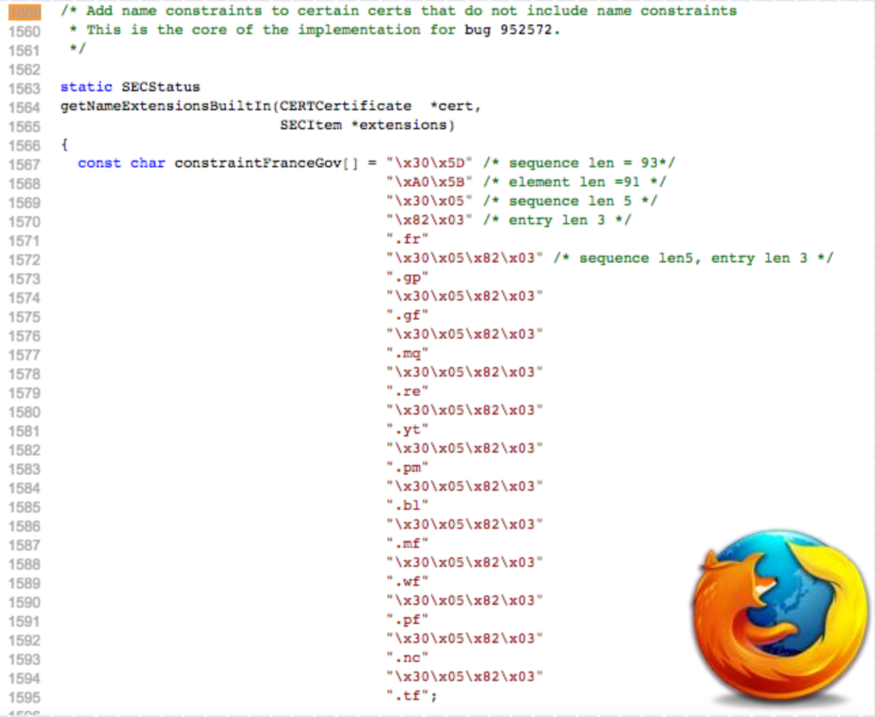
#RSAC

Artificial Constraints

Artificial Constraints

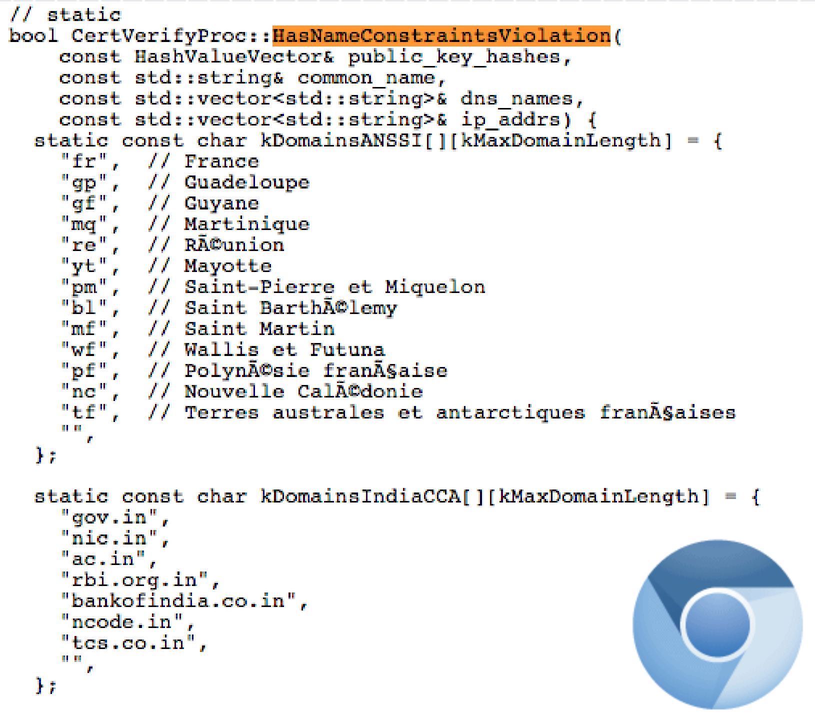
Cert Subject	Reason For Constraint
CN=IGC/A,OU=DCSSI,O=PM/SGDN,L=Paris ,ST=France,C=FR	Issued several un-authorized certificates for Google domains. TLD restrictions: *.fr (France), .gp (Guadeloupe) , .gf (Guyane) , .mq (Martinique) , .re (Réunion) , .yt (Mayotte), .pm (Saint-Pierre et Miquelon) , .bl (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.



```
/* Add name constraints to certain certs that do not include name constraints
 * This is the core of the implementation for bug 952572.
 */

static SECStatus
getNameExtensionsBuiltIn(CERTCertificate  *cert,
                         SECItem *extensions)
{
  const char constraintFranceGov[] = "\x30\x5D" /* sequence len = 93*/
                                     "\xA0\x5B" /* element len =91 */
                                     "\x30\x05" /* sequence len 5 */
                                     "\x82\x03" /* entry len 3 */
                                     ".fr"
                                     "\x30\x05\x82\x03" /* sequence len5, entry len 3 */
                                     ".gp"
                                     "\x30\x05\x82\x03"
                                     ".gf"
                                     "\x30\x05\x82\x03"
                                     ".mq"
                                     "\x30\x05\x82\x03"
                                     ".re"
                                     "\x30\x05\x82\x03"
                                     ".yt"
                                     "\x30\x05\x82\x03"
                                     ".pm"
                                     "\x30\x05\x82\x03"
                                     ".bl"
                                     "\x30\x05\x82\x03"
                                     ".mf"
                                     "\x30\x05\x82\x03"
                                     ".wf"
                                     "\x30\x05\x82\x03"
                                     ".pf"
                                     "\x30\x05\x82\x03"
                                     ".nc"
                                     "\x30\x05\x82\x03"
                                     ".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",
    "",
  };
```

Artificial Constraints –cont’d.

?

Apple’s Extended Trust

Type	Count	Notes
US Federal Certificates	5	4 are not on Android 1 is under review by Mozilla
Present on iOS, but requested for removal on Mozilla/Android	3	2 deprecated from AOL/Time Warner 1 deprecated from Danish IT
Other Entities added by Apple	15	5 from Apple 3 from Denmark 2 from Swiss Government 2 from Belgium 1 from Cisco 1 from Czech Republic 1 from Canada

RSA Conference2015

San Francisco | April 20-24 | Moscone Center

CA Cryptography Analysis

#RSAC

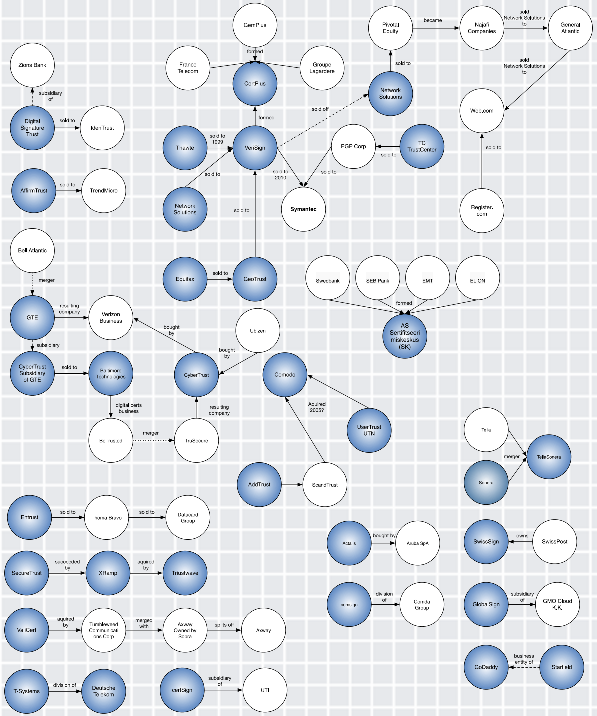
Public Key-Size

Key Type/Size	Count	Notable Entities
Elliptic Curve	6	GeoTrust, VeriSign, COMODO, Thawte, Entrust, AffirmTrust
RSA / 1024 bit	**15**	**FNMT, GTE CyberTrust, Equifax, Netlock Halozatbiztonsagi, VeriSign, ValiCert, Thawte Consulting, Entrust**
RSA / 2048 bit	101	N/A
RSA/ 4096 bit	14	N/A

Hash Algorithm

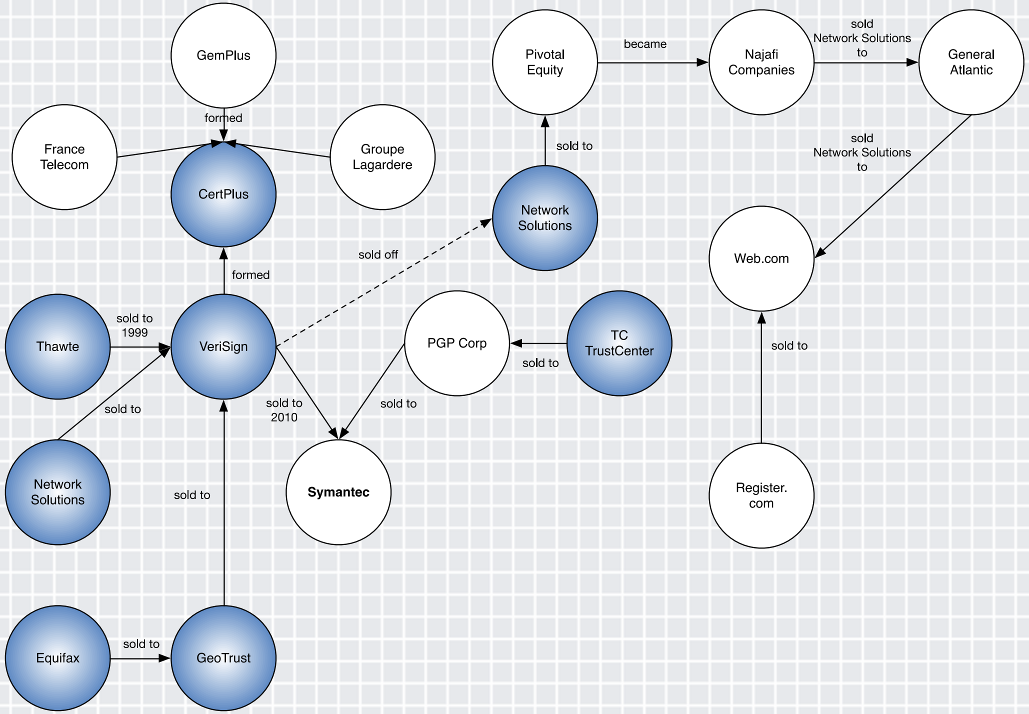
Signature Algorithm	Count	Notable Entities
ecdsa-with-SHA384	6	GeoTrust, VeriSign, COMODO, Thawte, Entrust, AffirmTrust
md5WithRSAEncryption	**6**	**GTE, Netlock, Equifax**
sha1WithRSAEncryption	115	N/A
sha256WithRSAEncryption	28	N/A
sha384WithRSAEncryption	1	N/A

CA Consolidation

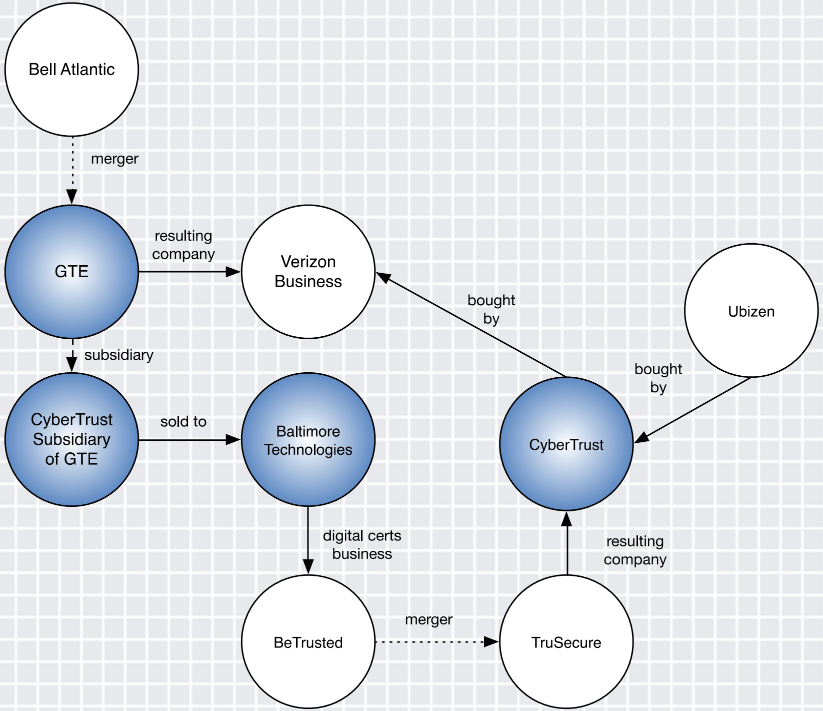


Symantec Owned Entity	Number of Certificates on Android
GeoTrust	7
Verisign	7
TC Trust Center	3
Network Solutions	1
Thawte	5
Equifax	3
Total:	**Symantec controls 25 of the total 156 certificates or ~16% ownership of the Android roots of trust**

CA Consolidation – cont'd.

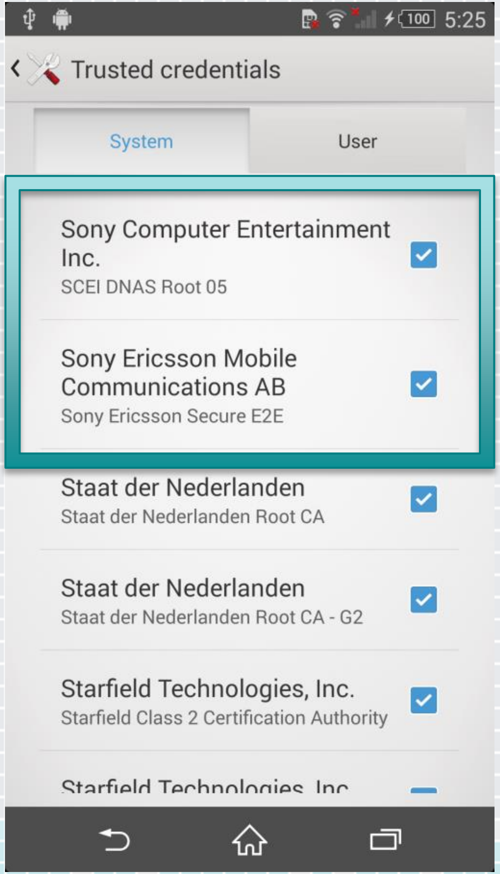


CA Consolidation – cont'd.



Additional CAs

- Some OEMs and carriers add additional certificates into the ROM that are not found in AOSP:
  - Sony Xperia running 4.4.4 includes two root certs for Sony
  - iOS has several additional certificates that Android does not currently* have e.g.: Cisco and US Government



Sony Computer Entertainment Inc. ☑
SCEI DNAS Root 05

Sony Ericsson Mobile Communications AB ☑
Sony Ericsson Secure E2E

Staat der Nederlanden ☑
Staat der Nederlanden Root CA

Staat der Nederlanden ☑
Staat der Nederlanden Root CA - G2

Starfield Technologies, Inc. ☑
Starfield Class 2 Certification Authority

Starfield Technologies, Inc.

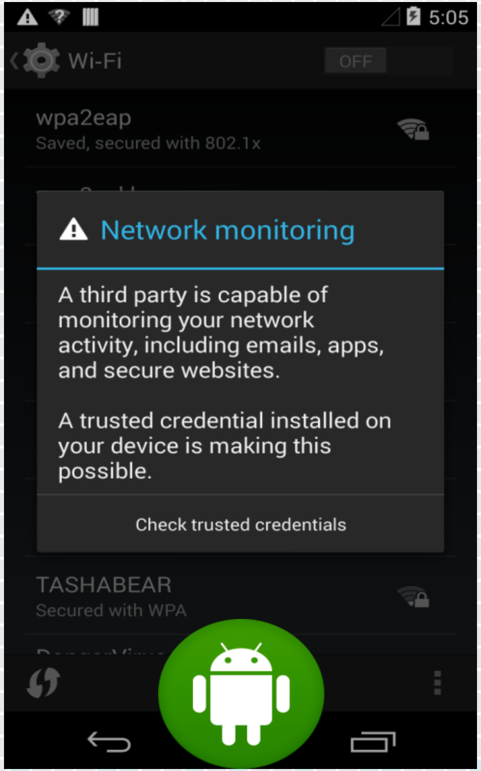
RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

User-installed Root CAs

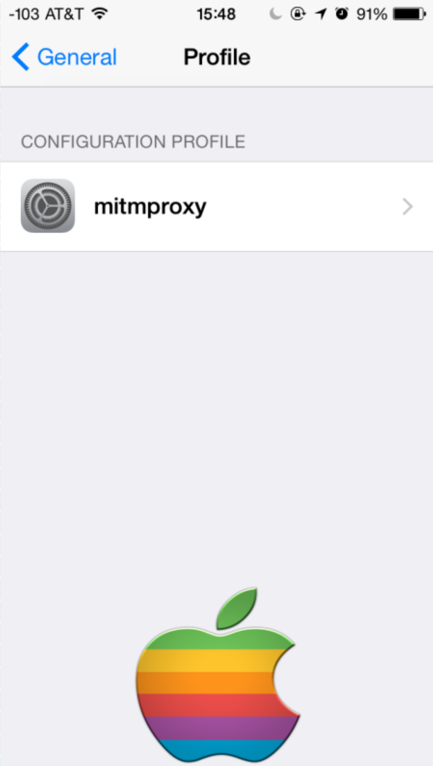
User installed root CAs



Network monitoring

A third party is capable of monitoring your network activity, including emails, apps, and secure websites.

A trusted credential installed on your device is making this possible.

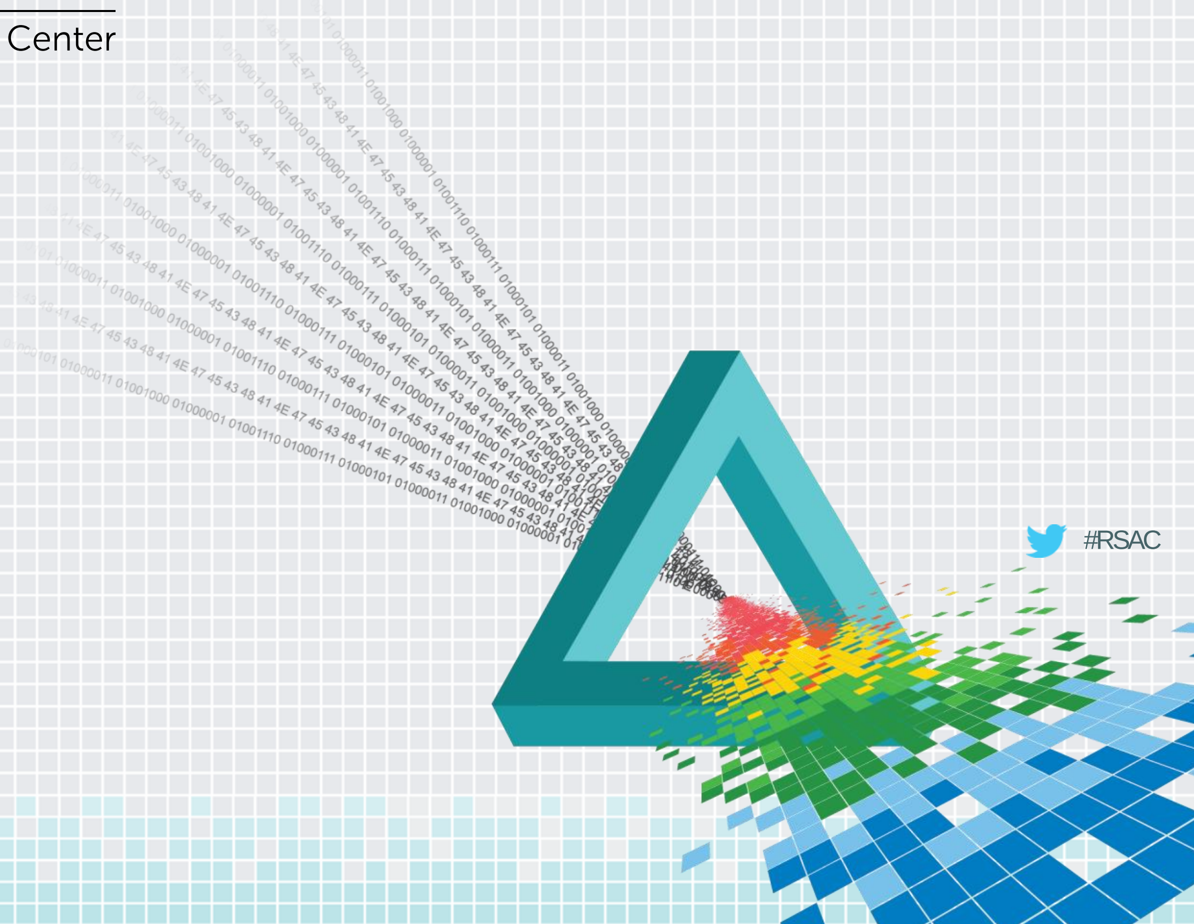


CONFIGURATION PROFILE

mitmproxy

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

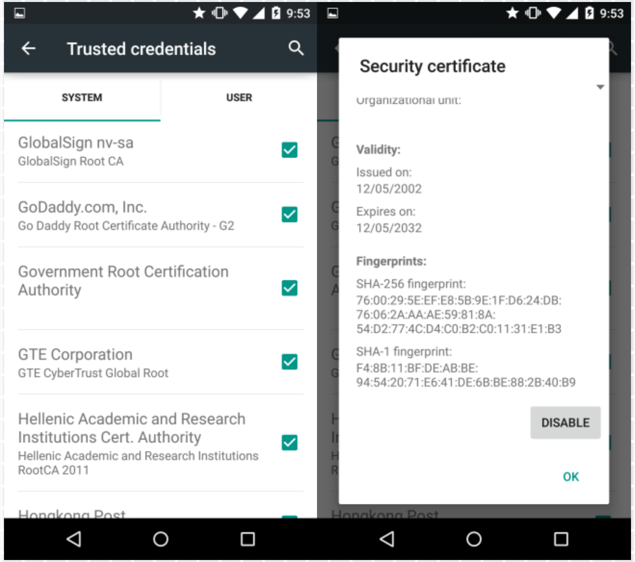
VPN Case-Study

VPN, Anonymization, Privacy Providers

- Looked at 10 of the top VPN Service Provider services in the Apple App Store and the Google Play Store:
  - iOS – App Store
    - 6 out of 10 of the iOS Apps used an MDM VPN Profile that **DID** install a 3rd party certificate
  - Android –Google Play Store
    - 10 out of 10 of the Play Store apps did not install a 3rd party certificate

Decreasing your Trust Circle

- Android:
  - Manually
    - Settings -> Security -> Trusted credentials
    - Disable or Enable each CA
- iOS:
  - No direct method on iOS…



9:53

Trusted credentials

SYSTEM USER

GlobalSign nv-sa
GlobalSign Root CA ☑

GoDaddy.com, Inc.
Go Daddy Root Certificate Authority - G2 ☑

Government Root Certification Authority ☑

GTE Corporation
GTE CyberTrust Global Root ☑

Hellenic Academic and Research Institutions Cert. Authority
Hellenic Academic and Research Institutions RootCA 2011 ☑

Hongkong Post

9:53

Security certificate

Organizational unit:

Validity:

Issued on:
12/05/2002

Expires on:
12/05/2032

Fingerprints:

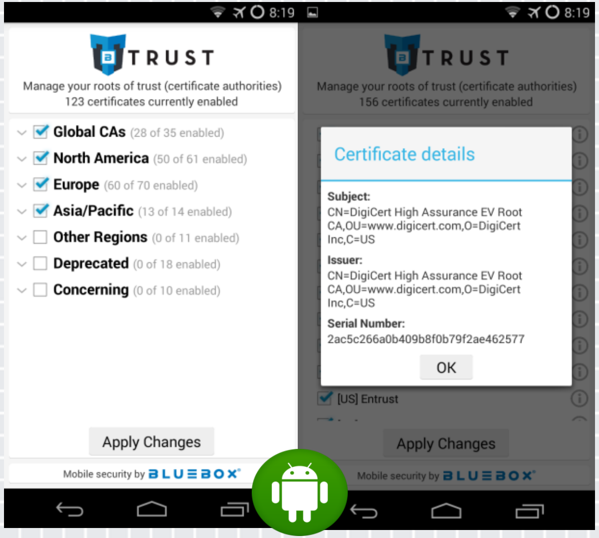
SHA-256 fingerprint:
76:00:29:5E:EF:E8:5B:9E:1F:D6:24:DB:
76:06:2A:AA:AE:59:81:8A:
54:D2:77:4C:D4:C0:B2:C0:11:31:E1:B3

SHA-1 fingerprint:
F4:8B:11:BF:DE:AB:BE:
94:54:20:71:E6:41:DE:6B:BE:88:2B:40:B9

DISABLE

OK

Bluebox Trust Managers



8:19

TRUST

Manage your roots of trust (certificate authorities)
123 certificates currently enabled

- ☑ **Global CAs** (28 of 35 enabled)
- ☑ **North America** (50 of 61 enabled)
- ☑ **Europe** (60 of 70 enabled)
- ☑ **Asia/Pacific** (13 of 14 enabled)
- □ **Other Regions** (0 of 11 enabled)
- □ **Deprecated** (0 of 18 enabled)
- □ **Concerning** (0 of 10 enabled)

Apply Changes

Mobile security by BLUEBOX

8:19

TRUST

Manage your roots of trust (certificate authorities)
156 certificates currently enabled

Certificate details

Subject:
CN=DigiCert High Assurance EV Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US

Issuer:
CN=DigiCert High Assurance EV Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US

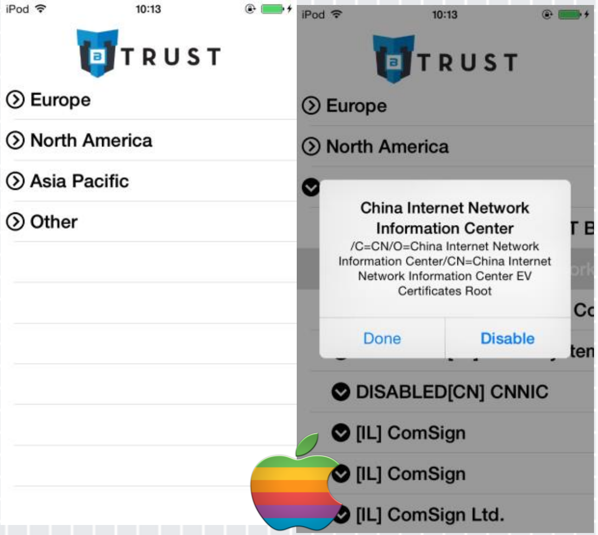
Serial Number:
2ac5c266a0b409b8f0b79f2ae462577

OK

☑ [US] Entrust

Apply Changes

Mobile security by BLUEBOX



iPod 10:13

TRUST

- Europe
- North America
- Asia Pacific
- Other

iPod 10:13

TRUST

- Europe
- North America

China Internet Network Information Center
/C=CN/O=China Internet Network Information Center/CN=China Internet Network Information Center EV Certificates Root

Done | Disable

- DISABLED[CN] CNNIC
- [IL] ComSign
- [IL] ComSign
- [IL] ComSign Ltd.

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

Summary

- Learn more about who your device is trusting
  - iOS and Android have an increasing amount of roots of trust
- Learn about the roles CAs play in secure communications
  - Without a CA we cannot verify that who we are talking to is legitimate
- Learn the history behind these CAs
  - Sometimes things go wrong with CAs
- Learn how you can take action to decrease your circle of trust
  - Manual certificate management
  - Bluebox Trust Manager for iOS and Android

Apply

- Learn more about what your device is trusting:
  - Trustable by Bluebox
    - (https://play.google.com/store/apps/details?id=com.bluebox.trust)
- View the root CAs on your device:
  - Android System Settings
  - Bluebox Trust Manager (Android and iOS)
- Manage the root CAs on your device (root/jailbreak) required:
  - Android System Settings
  - Bluebox Trust Manager (Android and iOS)

Q & A