

App Revocation Checking

Why is this still so hard?

Kevin Bock • Dave Levin • Jingjing Ren • Dave Choffnes • Alan Mislove



HotSec '18

ATTEND ACTIVITIES

HotSec '18

2018 USENIX Su

AUGUST 14, 2018
BALTIMORE, MD, USA

Co-located with **USENIX Security '18**

DST Root CA X3
↳ Let's Encrypt Authority X3
↳ 5767409591910400-fe4.pantheonsite.io



5767409591910400-fe4.pantheonsite.io

Issued by: Let's Encrypt Authority X3

Expires: Sunday, September 30, 2018 at 4:59:20 PM Eastern Daylight Time

✔ This certificate is valid

▼ Details

Subject Name _____
Common Name 5767409591910400-fe4.pantheonsite.io

Issuer Name _____
Country US
Organization Let's Encrypt
Common Name Let's Encrypt Authority X3

Serial Number 03 93 7F 7D FA DC B7 04 2F F1 52 D0 04 11 8F F4

OK

REVOKED



A dense, overlapping collection of colorful, 3D-style app icons. The icons are in various colors (blue, orange, green, red, yellow, purple, brown) and represent different app categories: social media (speech bubbles, person silhouettes, camera), communication (Wi-Fi, mail), shopping (shopping cart), and general utility (hashtag, magnifying glass, keyboard). The icons are arranged in a chaotic, piled-up manner, creating a sense of abundance and variety.

400+ Unique Apps



5177 .pcaps, 6283 .dumps

252,603 captured certificates

A conceptual image where a person's hands, wearing a light-colored shirt, hold a white rectangular sign with the word "HELP" written in black, handwritten-style capital letters. The hands are positioned above a large, dense pile of crumpled white paper that fills the lower two-thirds of the frame. The background is a dark, solid color, making the white paper and sign stand out.

HELP

0

Revocations

0







Google's senior staff software engineer's take:
<https://www.imperialviolet.org/2014/04/19/revchecking.html>

Android's TrustManagerImpl:

```
try {
```

```
    PKIXParameters params = new PKIXParameters(trustAnc
```

```
    params.setRevocationEnabled(false);
```

```
    params.addCertPathChecker(new ExtendedKeyUsagePKIXC
```

*“The details... of the revocation checking policy are **deliberately not documented** because they are subject to change.”*

- Still fails soft at least up to iOS 10.3



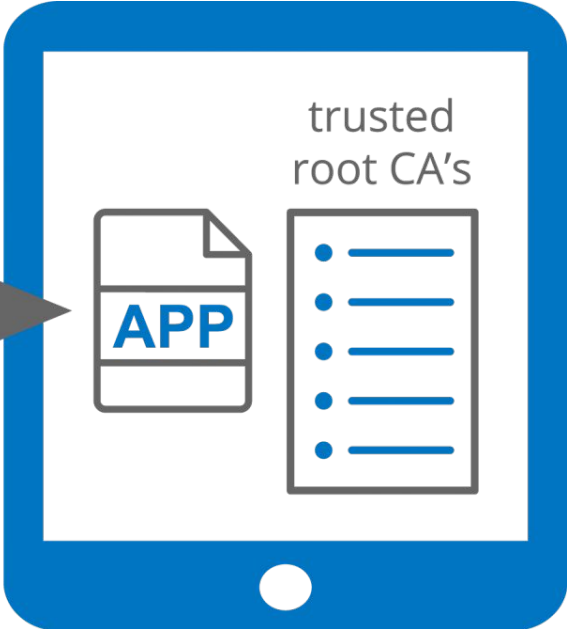
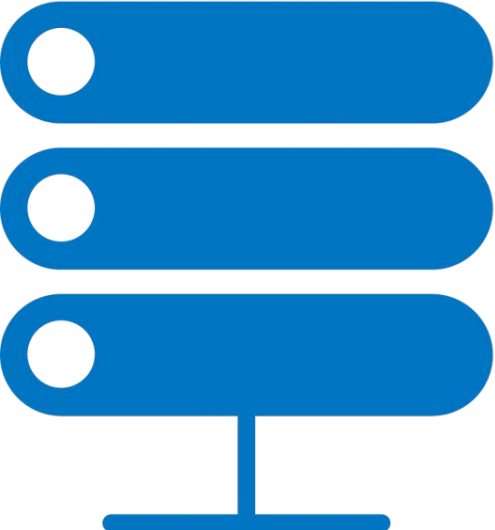
See <https://forums.developer.apple.com/thread/24298>



See <https://github.com/square/okhttp/issues/2348>



server





App Store

The background is a textured blue surface, possibly a canvas or paper, with a bright light source in the center. This light source creates a sunburst effect, with rays of light radiating outwards. The colors range from a deep, dark blue at the edges to a bright, almost white light in the center. The texture is visible as fine brushstrokes or fibers.

No Shame



SOLUTIONS **NEW**