Securing Network Communication Using Certificate Authorities and Certificate Pinning

Nitin Singh
MOBILE DEVELOPER

Customizing Certificate Authorities (CAs) Trusted by an App

What is a CA

A certificate authority (CA) is an entity that issues digital certificates

An app only allows HTTPS requests which are signed by the CAs trusted by the app

By default apps trust the pre-installed CAs that ship with Android and the user-installed CAs, in case of API level <= 23

When to Customize Trusted CAs

When connecting to a host with a custom CA which is self-signed or org specific

When you don't want to trust all pre-installed CAs

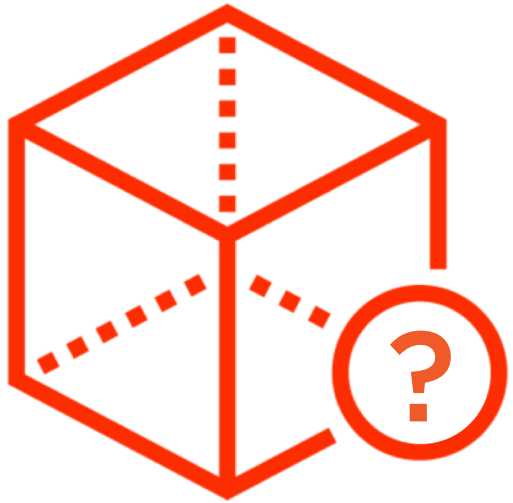
When you want your app to trust CAs not included in the system's pre-installed CAs

```
<domain-config>
    <domain includeSubdomains="true”example.com</domain>
    <trust-anchors>
        <certificates src="@raw/my_ca"/>
    </trust-anchors>
</domain-config>
```

Change List of Trusted CAs

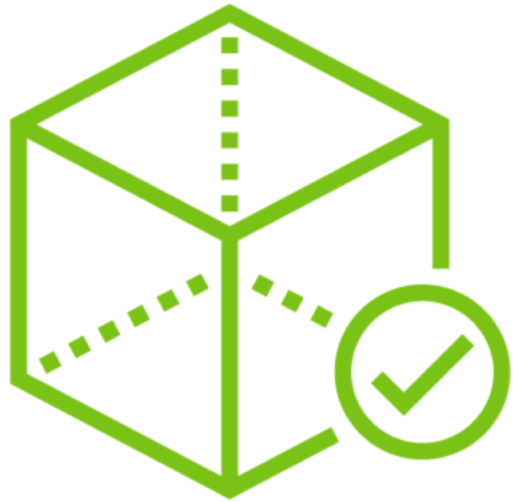
- Use <trust-anchors> tag with one or more <certificates> tag
- Can be used with <domain-config>, <base-config> or <debug-overrides>

Understanding <certificates> Tag



src

Controls what certificates from what sources are trusted



overridePins

Indicates whether certificate pinning should be respected or not

<certificates> ‘src’ Attribute

1

src attribute used to define sources of CAs trusted

2

Possible values system, user, raw resource

3

In case of raw resource it should point to a file containing X.509 certificates encoded in PEM format

<certificates> ‘overridePins’ Attribute

1

Indicates if CAs listed in the src should by pass certificate pinning or not

2

Possible values true, false. Default false unless inside <debug-overrides> tag

3

This is useful while debugging CAs or testing man in the middle attacks

```
<debug-overrides>
    <trust-anchors>
        <certificates src="@raw/debug_cas"/>
    </trust-anchors>
</debug-overrides>
```

Debug-only Overrides

- Use different settings while debugging
- Avoids conditional code that can lead to app shipping with wrong set of trusted CAs or wrong network configuration

Demo

Contact application

See what happens when a host serves a certificate signed by a non-system CA

Add support for a self signed CA

Certificate Pinning

What happens if a CA issues a fraudulent certificate

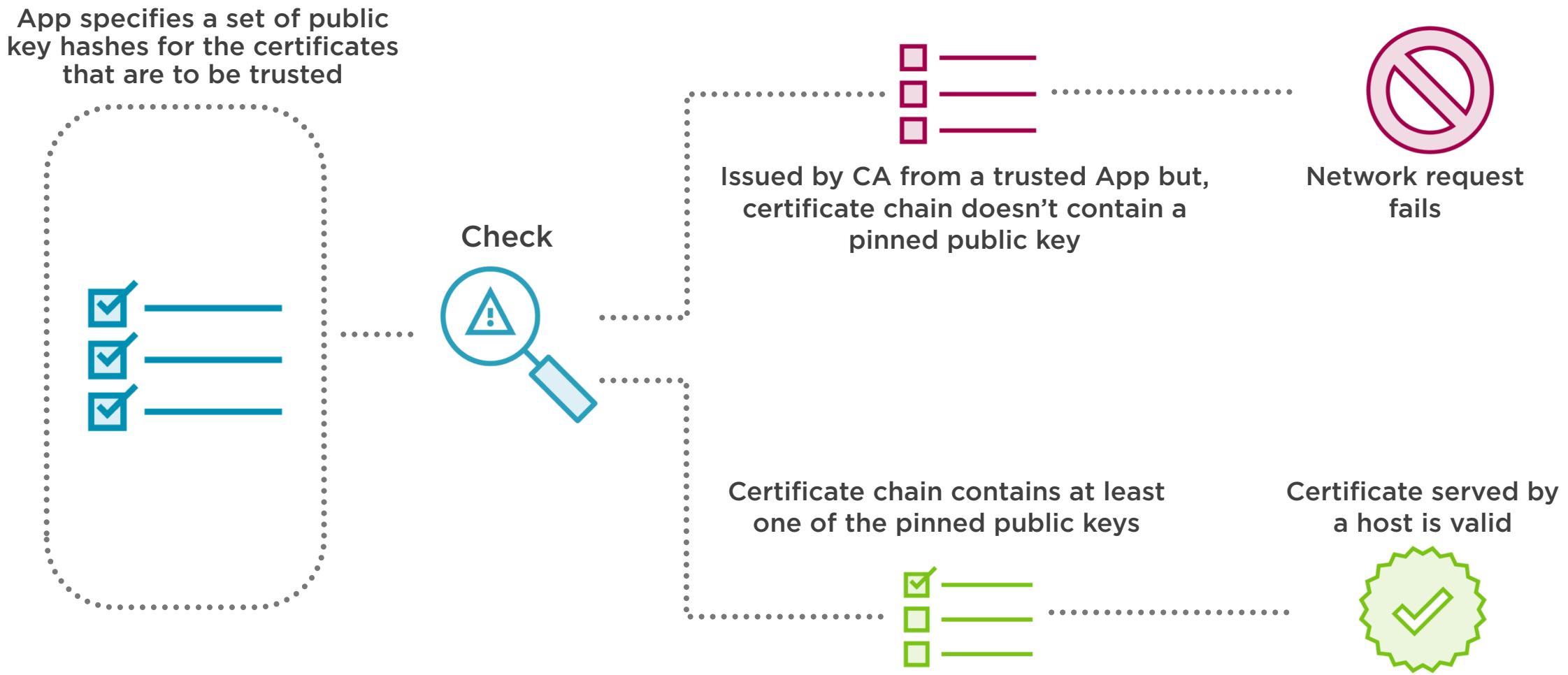
How a Bad Certificate can Compromise Security

CA issues fraudulent certificate

App trusts CA issued certificate as its in the trusted CA list

Man in the middle attack is now possible by entity owning the fraudulent certificate

How Certificate Pinning Works



Tags for Configuring Certificate Pinning

<pin-set>

List of certificates to be pinned

<pin>

Used to specify the public key SHA-256 hash for the certificate to be pinned

<pin-set> Tag

1

Can be specified in <domain-config> or <base-config>

2

Can contain one or more <pin> tags

3

expiration attribute used to specify date in yyyy-MM-dd format after which pinning expires so that apps keep working if user doesn't update for a long time

<pin> Tag

1

Specified within <pin-set> tag

2

Digest attribute specifies algorithm to use to generate hash. Currently only SHA-256 is supported

3

Holds base64 encoded digest of X.509 public key of certificate to be pinned

Precautions to Take When Using Pinning

Always include a backup key to allow switching to new keys

Set expiration on pins to support old apps

Keep in mind that setting expiration might allow pinning bypass

```
<domain includeSubdomains="true">example.com </domain>
  <pin-set expiration="2018-01-01">
            <pin digest="SHA-256">public_key_hash</pin>
            <!-- backup pin -->
            <pin digest="SHA-256">public_key_hash</pin>
  </pin-set>
```

Certificate Pinning Sample

Demo

Contact application

Pin a certificate using network configs

See what happens when a non-pinned certificate is served

Summary

- When to customize the set of CAs trusted by your app
- How to configure your app to trust a custom set of CAs
- How to configure different settings while in debug mode
- Why certificate pinning is needed
- How certificate pinning works
- How to pin certificates in your app
- Precautions to take when pinning certificates

Thank you