Is your app secure?

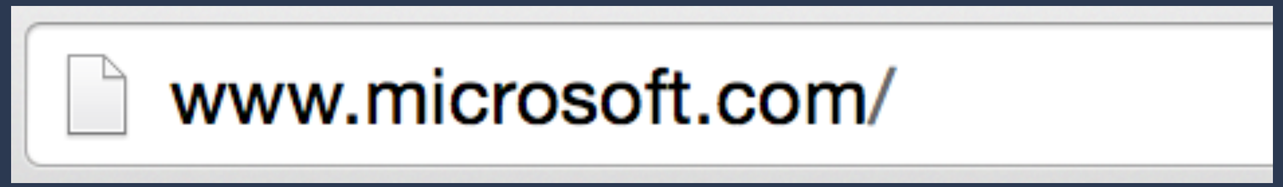
Kerry W. Lothrop
Zühlke
@kwlothrop


zühlke
empowering ideas


Gold member
John Doe
234 564 789
2738 Reward Points
Redeem


GSM


Wi Fi
TM


www.microsoft.com/


https://www.microsoft.com/


https://www.microsoft.com/


Close
Mobile Express...
Reload
SaurikIT, LLC
My total:
$1.99 USD
Review
PayPal
Payment method:
Bank xx-
$1.99 USD
Ship to:
United States
Pay Now

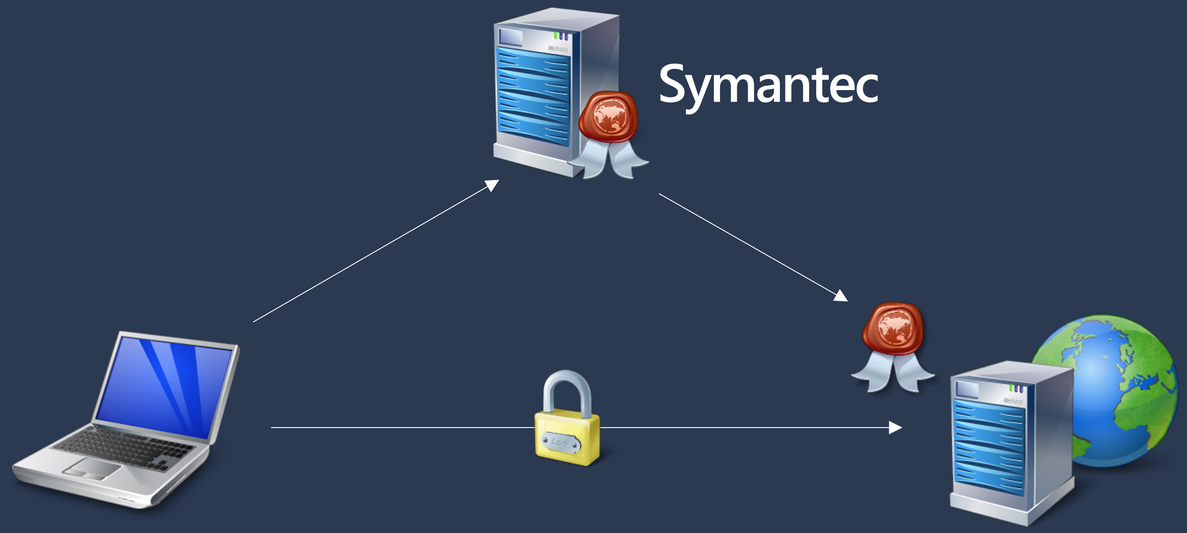

Close
Mobile Express..
SaurikIT, L
My total:
Review
Payment method:
Bank xx-
Ship to:
United States
Pay Now

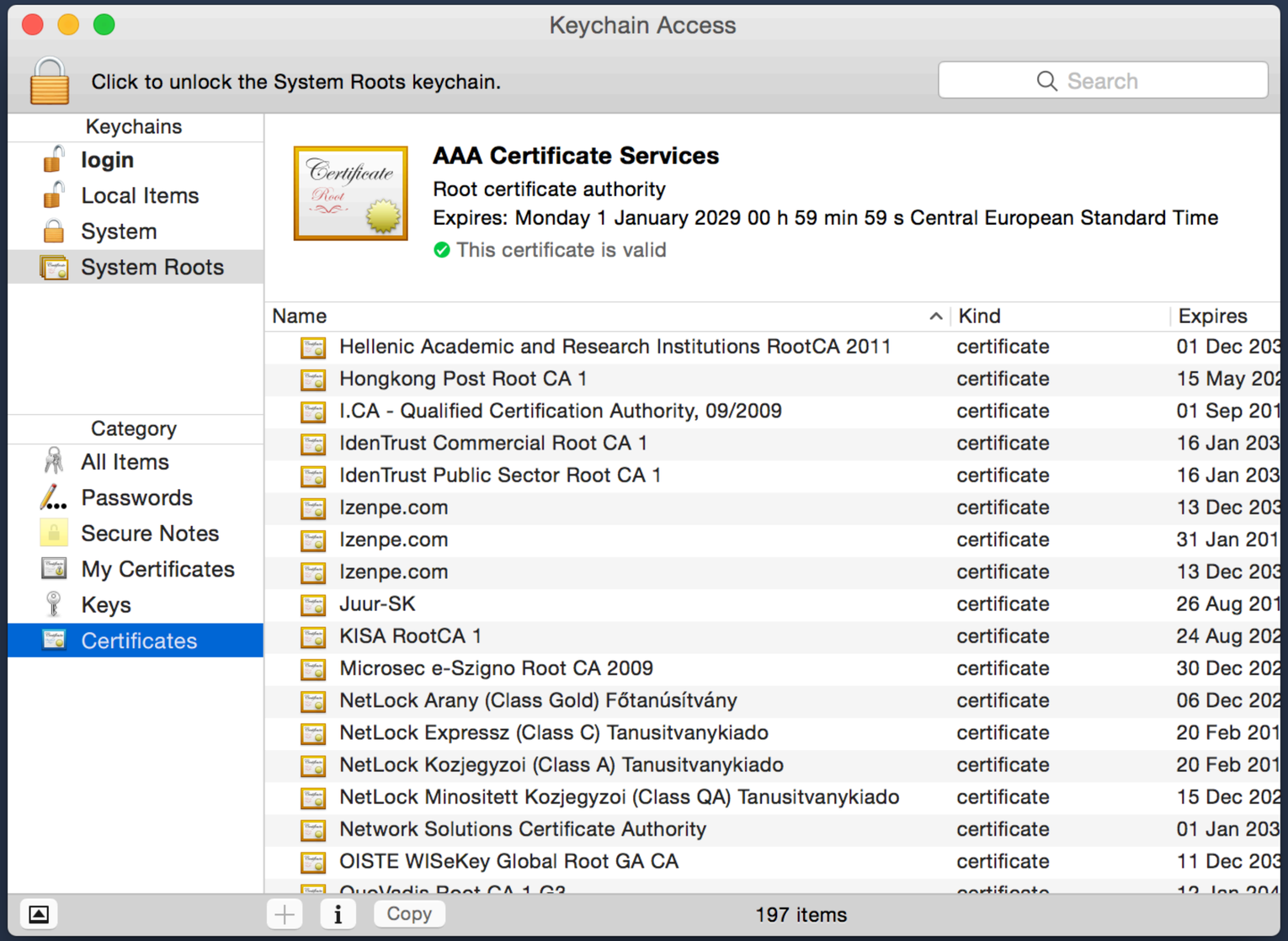
“The app store review will catch security issues.”

Communication

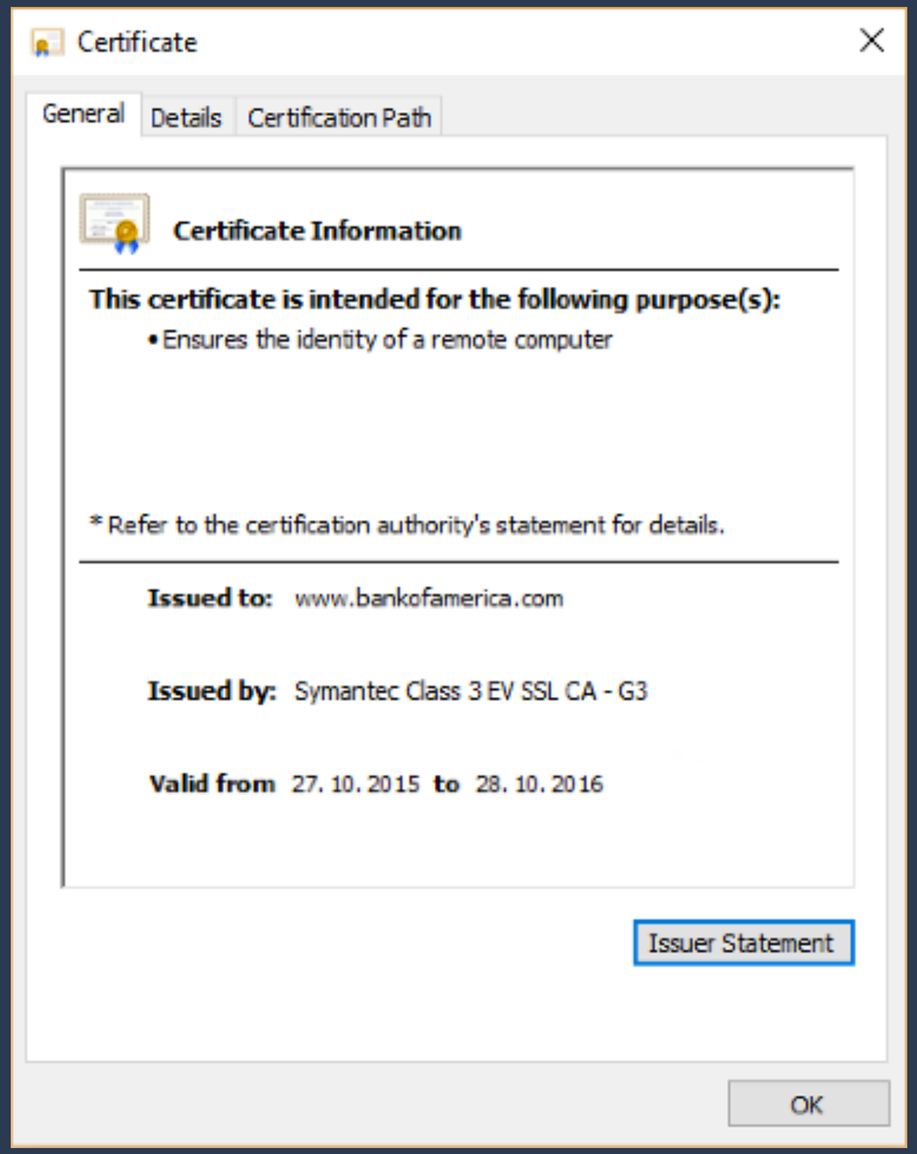
http://

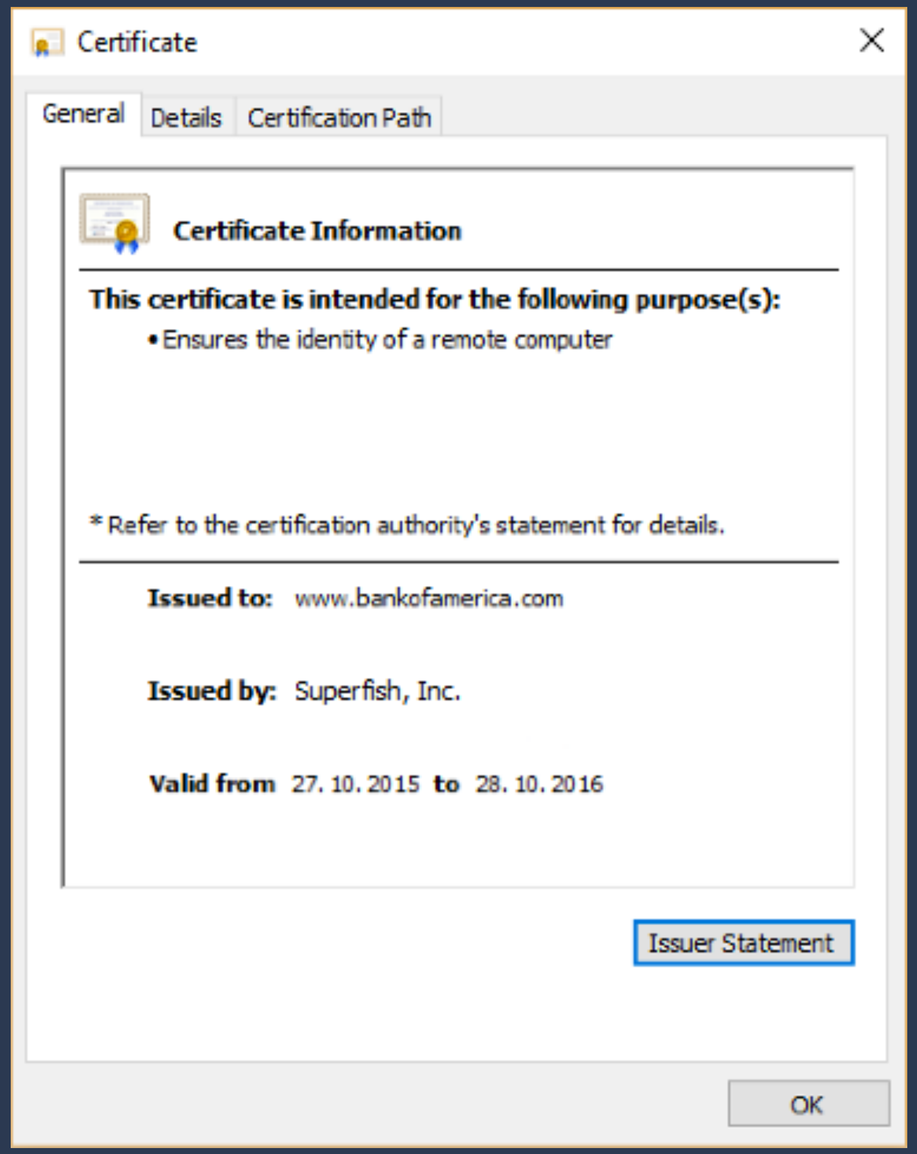
https://

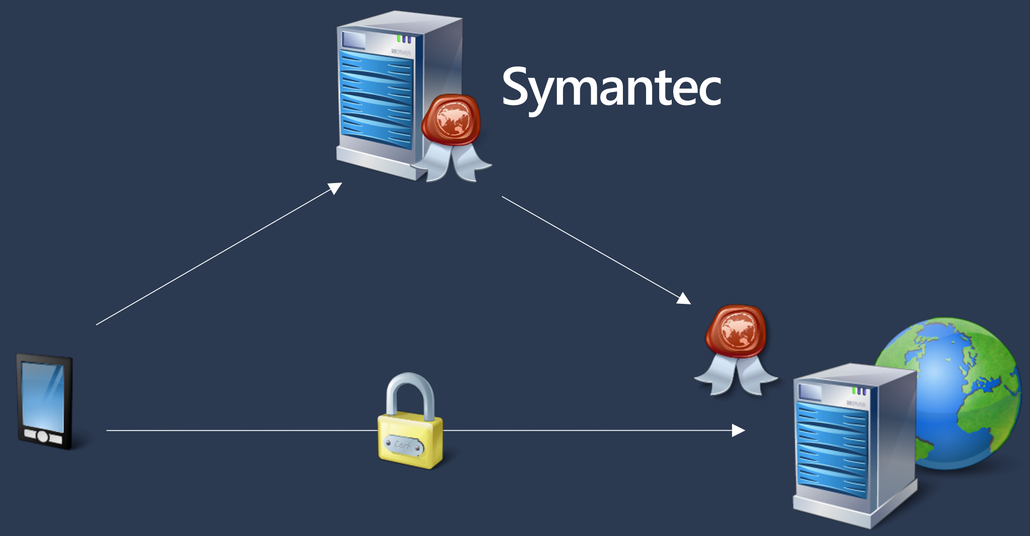

Symantec


Keychain Access
Click to unlock the System Roots keychain.
Search
Keychains
login
Local Items
System
System Roots
Category
All Items
Passwords
Secure Notes
My Certificates
Keys
Certificates
AAA Certificate Services
Root certificate authority
Expires: Monday 1 January 2029 00 h 59 min 59 s Central European Standard Time
This certificate is valid
Name
Kind
Expires
Hellenic Academic and Research Institutions RootCA 2011 certificate 01 Dec 203
Hongkong Post Root CA 1 certificate 15 May 202
I.CA - Qualified Certification Authority, 09/2009 certificate 01 Sep 201
IdenTrust Commercial Root CA 1 certificate 16 Jan 203
IdenTrust Public Sector Root CA 1 certificate 16 Jan 203
Izenpe.com certificate 13 Dec 203
Izenpe.com certificate 31 Jan 201
Izenpe.com certificate 13 Dec 203
Juur-SK certificate 26 Aug 201
KISA RootCA 1 certificate 24 Aug 202
Microsec e-Szigno Root CA 2009 certificate 30 Dec 202
NetLock Arany (Class Gold) Főtanúsítvány certificate 06 Dec 202
NetLock Expressz (Class C) Tanusitvanykiado certificate 20 Feb 201
NetLock Kozjegyzoi (Class A) Tanusitvanykiado certificate 20 Feb 201
NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado certificate 15 Dec 202
Network Solutions Certificate Authority certificate 01 Jan 203
OISTE WISeKey Global Root GA CA certificate 11 Dec 203
Copy
197 items

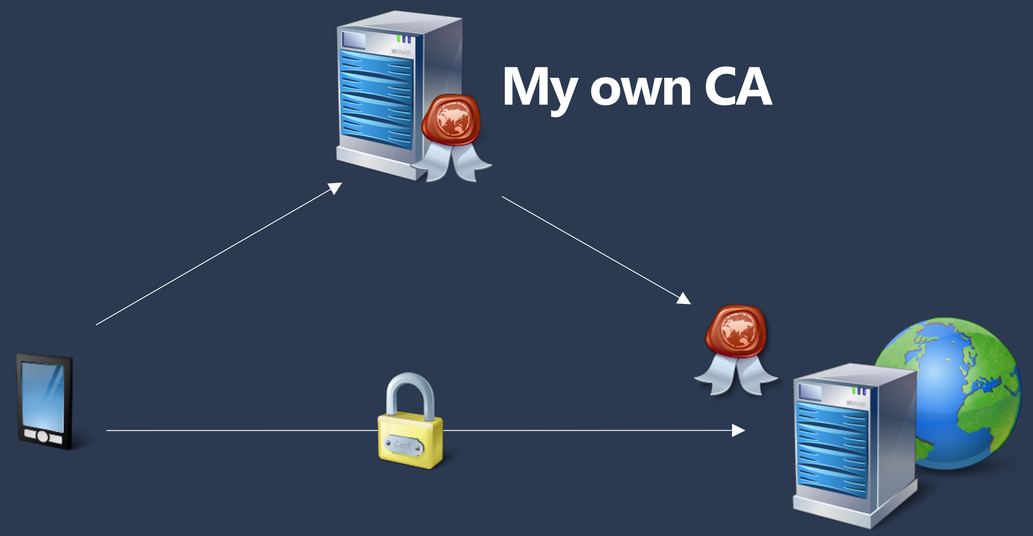

Demo


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: www.bankofamerica.com
Issued by: Symantec Class 3 EV SSL CA - G3
Valid from 27. 10. 2015 to 28. 10. 2016
Issuer Statement
OK


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: www.bankofamerica.com
Issued by: Superfish, Inc.
Valid from 27. 10. 2015 to 28. 10. 2016
Issuer Statement
OK


Symantec


https://www.microsoft.com/


My own CA


https://www.microsoft.com/

Certificate pinning

Certificate Pinning

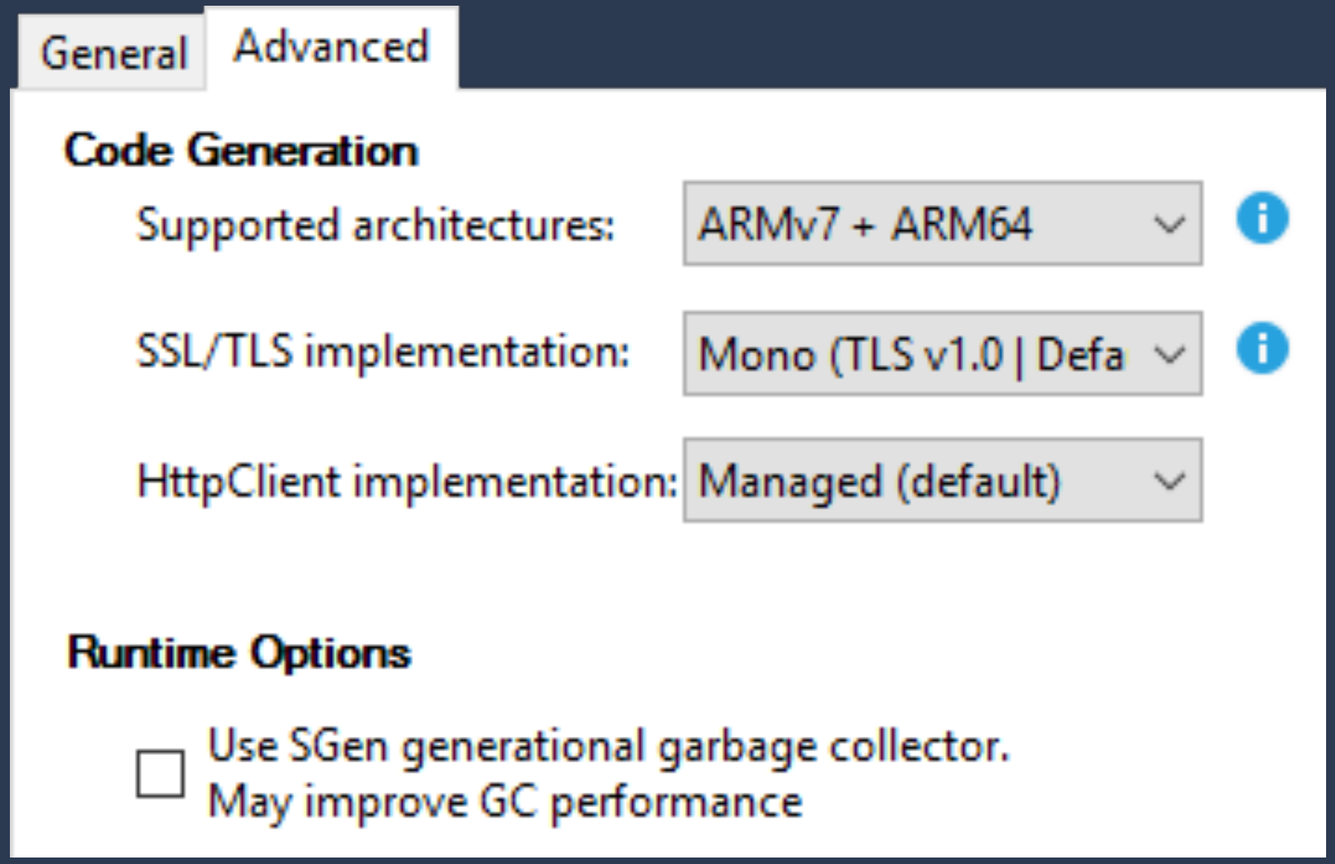
```
ServicePointManager.ServerCertificateValidationCallback
    = CheckCertificate;

private static bool CheckCertificate(
    object sender, X509Certificate certificate,
    X509Chain chain, SslPolicyErrors sslpolicyerrors)
{
    return // TODO: Is certificate chain valid?
}
```


Demo

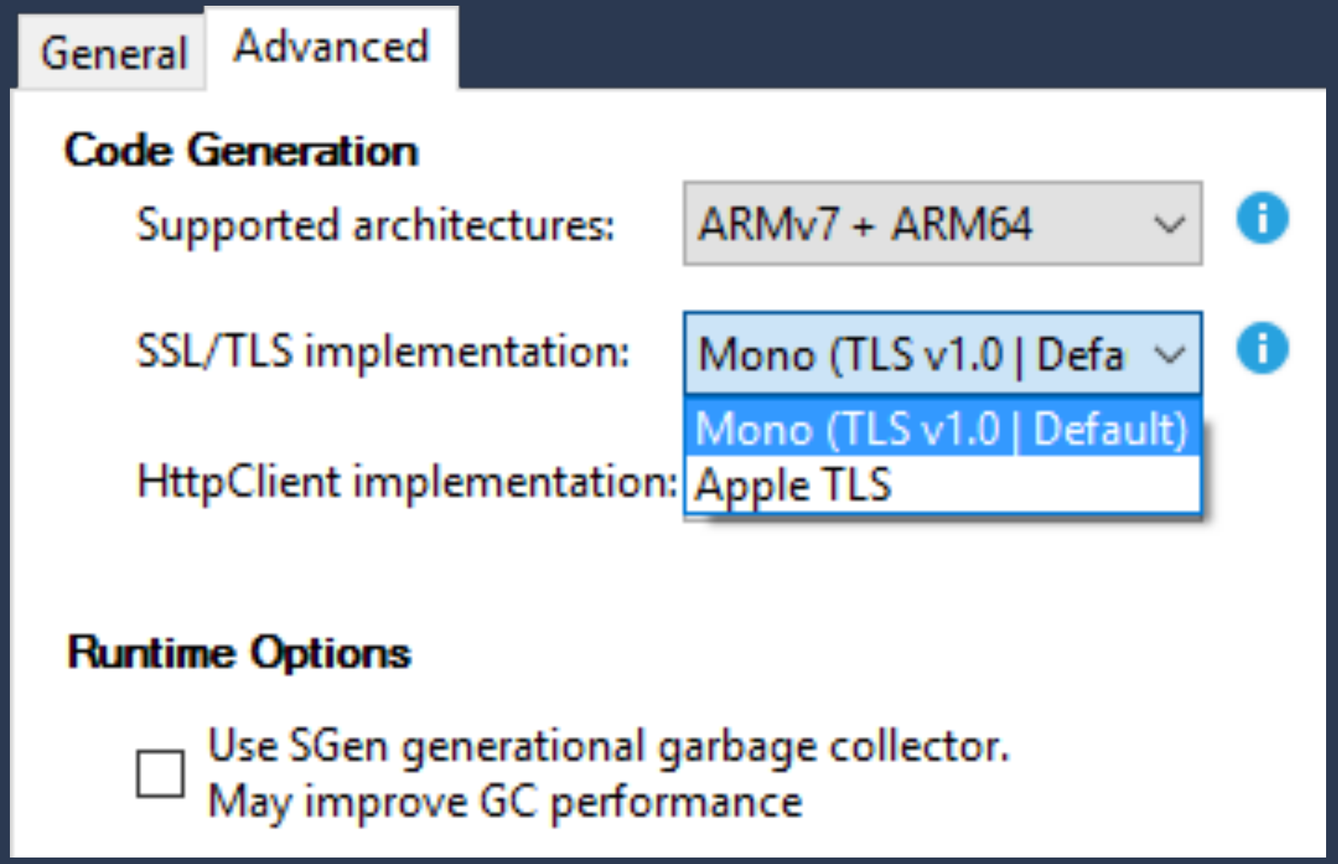
App Transport Security (ATS)

```
<key>NSAppTransportSecurity</key>
<dict>
  <key>NSExceptionDomains</key>
  <dict>
    <key>www.example.com</key>
    <dict>
      <key>NSExceptionMinimumTLSVersion</key>
      <string>TLSv1.0</string>
      <key>NSExceptionRequiresForwardSecrecy</key>
      <false/>
      <key>NSExceptionAllowsInsecureHTTPLoads</key>
      <true/>
      <key>NSIncludesSubdomains</key>
      <true/>
    </dict>
  </dict>
</dict>
```

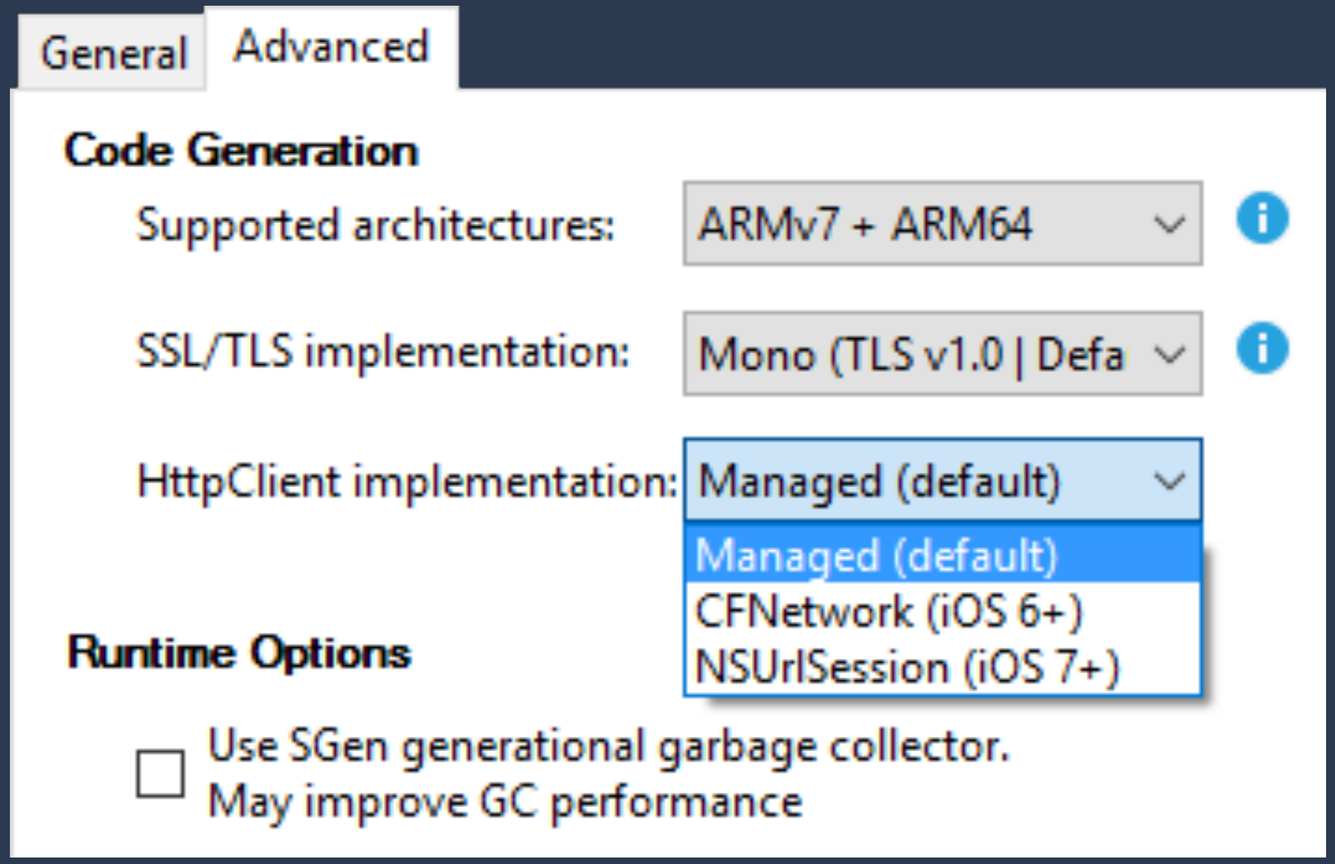
HttpClient


General
Advanced
Code Generation
Supported architectures:
ARMv7 + ARM64
SSL/TLS implementation:
Mono (TLS v1.0 | Defa
HttpClient implementation:
Managed (default)
Runtime Options
Use SGen generational garbage collector.
May improve GC performance

HttpClient


General
Advanced
Code Generation
Supported architectures:
ARMv7 + ARM64
SSL/TLS implementation:
Mono (TLS v1.0 | Defa
Mono (TLS v1.0 | Default)
Apple TLS
HttpClient implementation:
Runtime Options
Use SGen generational garbage collector.
May improve GC performance

HttpClient


General
Advanced
Code Generation
Supported architectures:
ARMv7 + ARM64
SSL/TLS implementation:
Mono (TLS v1.0 | Defa
HttpClient implementation:
Managed (default)
Managed (default)
CFNetwork (iOS 6+)
NSUrlSession (iOS 7+)
Runtime Options
Use SGen generational garbage collector.
May improve GC performance

Native HttpClientHandler

```
new HttpClient(new System.Net.Http.CFNetworkHandler());

new HttpClient(new System.Net.Http.NSUrlSessionHandler());

new HttpClient(new Xamarin.Android.Net.AndroidClientHandler());

new HttpClient(new ModernHttpClient.NativeMessageHandler());
```

HttpClient

	Mono	Native HttpClientHandler	Modern HttpClient
OS Proxy settings used		✔	✔
TLS 1.2 support	w/Apple TLS or BoringSSL	iOS & Android 5+	iOS & Android 5+
ATS restrictions apply		iOS 9 only	iOS 9 only
Certificate pinning with ServicePointManager	✔		iOS: yes Android: limited
Instantiate from PCL	✔	✔	✔


APIs

“You can use our existing web service for that.”

“Which IP address will you be accessing the web service from?”

"You'll need to use these credentials to access the web service."

```
public AppDelegate ()
{
    // Initialize the Parse client with your Application ID and .NET Key found on
    // your Parse dashboard
    ParseClient.Initialize("YOUR APPLICATION ID", "YOUR .NET KEY");
}
```

Don’t store credentials inside your app bundle.

Don’t authenticate the app, authenticate the user.

Store user-specific tokens in the device’s secure storage.

Design your backend security like you would design security for a web site.

If an API requires an API key, call it from your backend.


Summary

Challenge the security of your app and backend.


Business
WWW
@
WORK
NEWS
NO
PLAN
Team
innovation
IDEA
Concept
SOCIAL
Time
Team
SMS
Motivation
money
innovation
Business
Time

Questions?

Is your app secure?

Kerry W. Lothrop
Zühlke
@kwlothrop