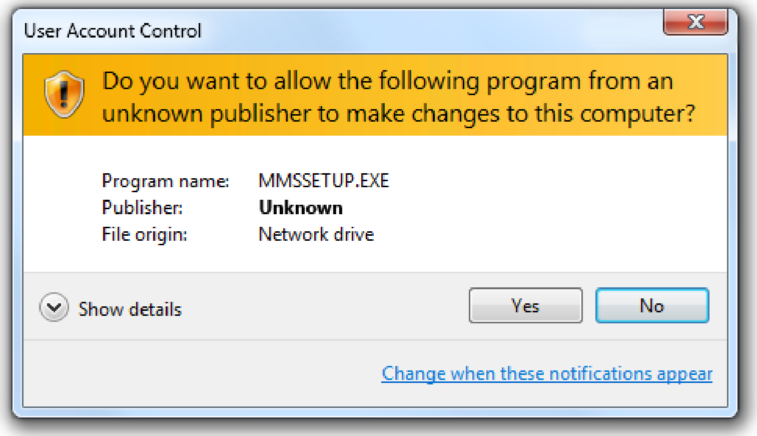
Code Signing, Hashing Implementations, and The Importance of Security

CHRIS NUTTER, AUSTIN KIM | CPSC 351-91

What is it and why is it important?

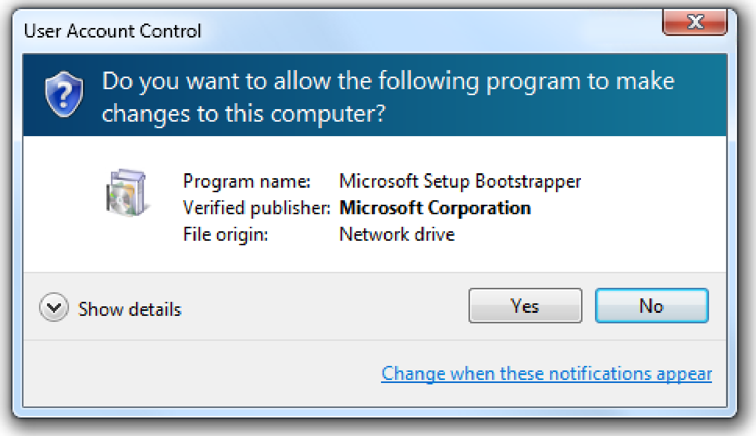
- Security and Protection
- Ensuring safety for consumers
- Verified through authorized CAs


User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: MMSSETUP.EXE
Publisher: **Unknown**
File origin: Network drive

Not Code Signed


User Account Control

Do you want to allow the following program to make changes to this computer?

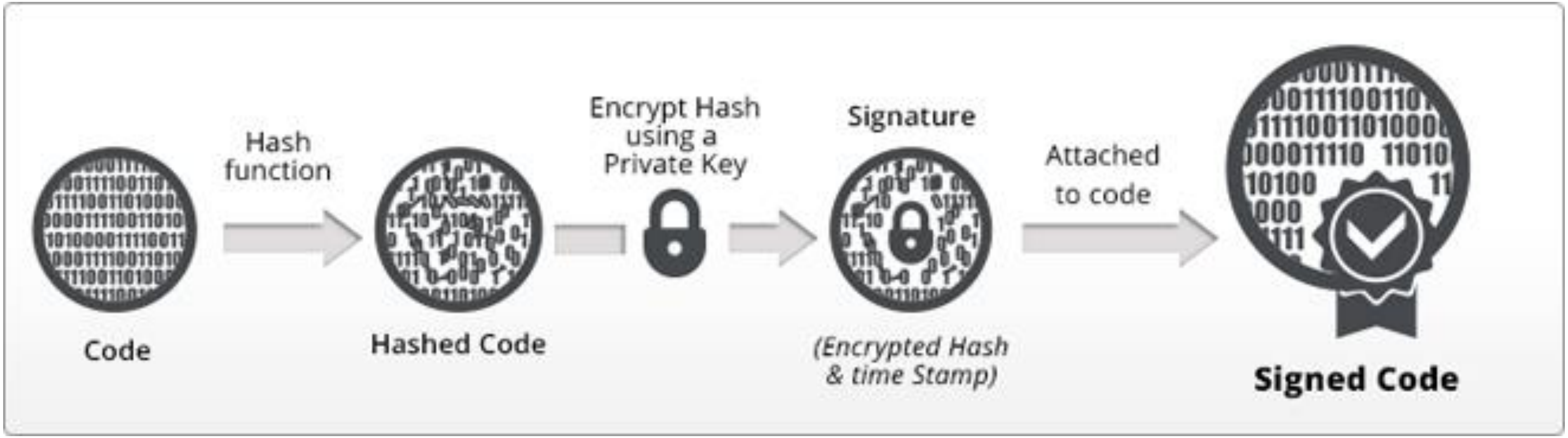
Program name: Microsoft Setup Bootstrapper
Verified publisher: **Microsoft Corporation**
File origin: Network drive

Code Signed

https://www.ssl2buy.com/wiki/wp-content/uploads/2015/01/code-signing-certificates-warning-massage.png

Authentication and Integrity

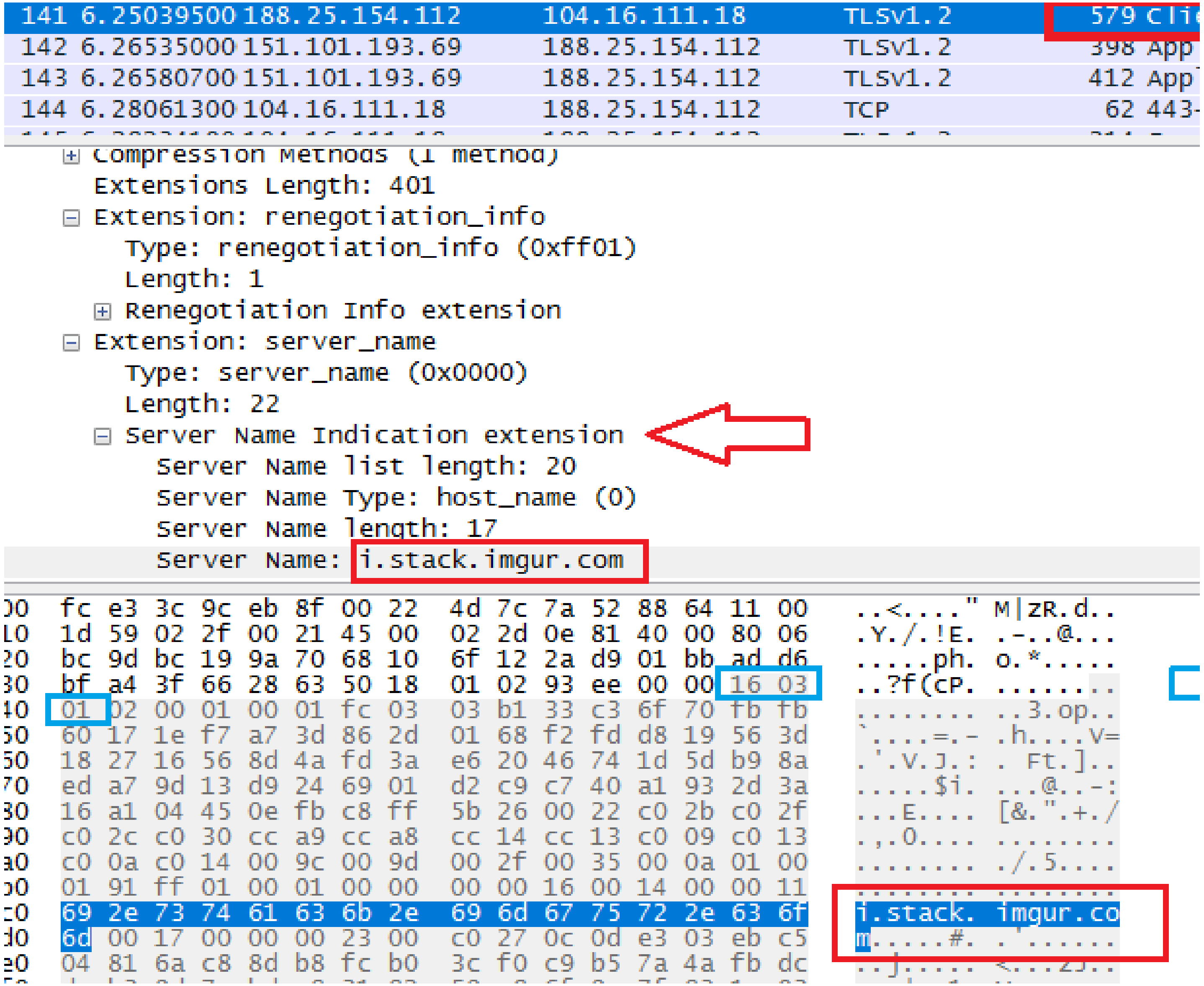
- Authentication: Allows consumer to verify author
- Integrity: Verification of untampered code



https://www.ssl2buy.com/wiki/wp-content/uploads/2015/01/code-signing-certificate.jpg

SSL/TLS Encryption

- Secure Sockets Layer
- Transport Layer Security
- Encrypted link between server and client
- Used for web servers around the world
- Very important for trusted businesses
- TLS evolved from SSL

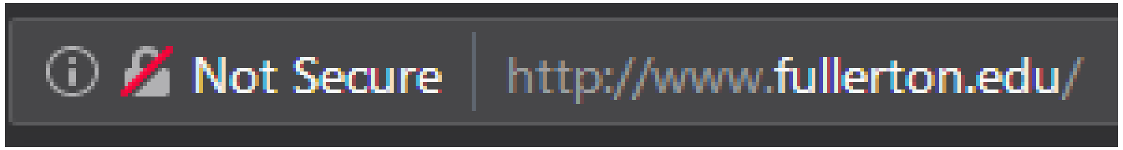


```
141 6.25039500 188.25.154.112    104.16.111.18    TLSv1.2     579 Clie
142 6.26535000 151.101.193.69    188.25.154.112   TLSv1.2     398 App
143 6.26580700 151.101.193.69    188.25.154.112   TLSv1.2     412 App
144 6.28061300 104.16.111.18     188.25.154.112   TCP          62 443-
```

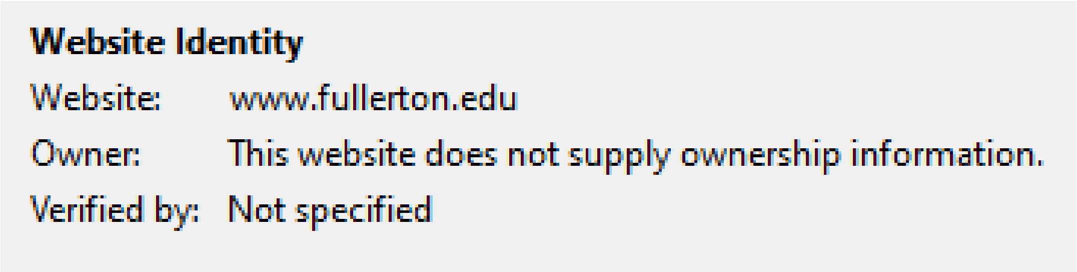
```
 ⊞ Compression Methods (1 method)
   Extensions Length: 401
 ⊟ Extension: renegotiation_info
     Type: renegotiation_info (0xff01)
     Length: 1
   ⊞ Renegotiation Info extension
 ⊟ Extension: server_name
     Type: server_name (0x0000)
     Length: 22
   ⊟ Server Name Indication extension
       Server Name list length: 20
       Server Name Type: host_name (0)
       Server Name length: 17
       Server Name: i.stack.imgur.com
```

```
00  fc e3 3c 9c eb 8f 00 22  4d 7c 7a 52 88 64 11 00   ..<...." M|zR.d..
10  1d 59 02 2f 00 21 45 00  02 2d 0e 81 40 00 80 06   .Y./.!E. .-..@...
20  bc 9d bc 19 9a 70 68 10  6f 12 2a d9 01 bb ad d6   .....ph. o.*.....
30  bf a4 3f 66 28 63 50 18  01 02 93 ee 00 00 16 03   ..?f(cP. ........
40  01 02 00 01 00 01 fc 03  03 b1 33 c3 6f 70 fb fb   ........ ..3.op..
50  60 17 1e f7 a7 3d 86 2d  01 68 f2 fd d8 19 56 3d   `....=.- .h....V=
60  18 27 16 56 8d 4a fd 3a  e6 20 46 74 1d 5d b9 8a   .'.V.J.: . Ft.]..
70  ed a7 9d 13 d9 24 69 01  d2 c9 c7 40 a1 93 2d 3a   .....$i. ...@..-:
80  16 a1 04 45 0e fb c8 ff  5b 26 00 22 c0 2b c0 2f   ...E.... [&.".+./
90  c0 2c c0 30 cc a9 cc a8  cc 14 cc 13 c0 09 c0 13   .,.0.... ........
a0  c0 0a c0 14 00 9c 00 9d  00 2f 00 35 00 0a 01 00   ........ ./.5....
b0  01 91 ff 01 00 01 00 00  00 00 16 00 14 00 00 11   ........ ........
c0  69 2e 73 74 61 63 6b 2e  69 6d 67 75 72 2e 63 6f   i.stack. imgur.co
d0  6d 00 17 00 00 00 23 00  c0 27 0c 0d e3 03 eb c5   m.....#. .'......
e0  04 81 6a c8 8d b8 fc b0  3c f0 c9 b5 7a 4a fb dc   ..j..... <...zJ..
```

https://stackoverflow.com/questions/499591/are-https-urls-encrypted?rq=1

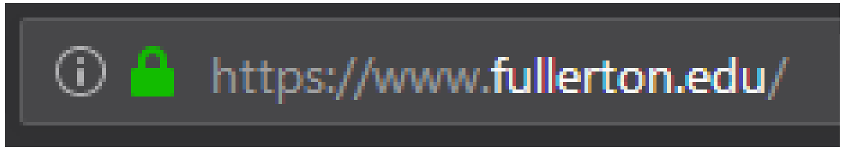


Not Secure http://www.fullerton.edu/

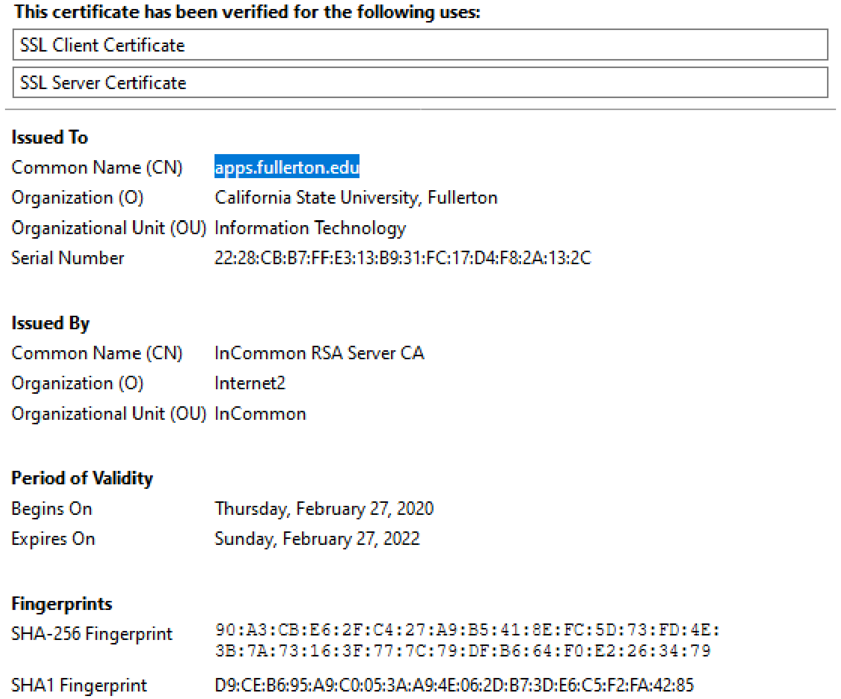


Website Identity

Website:	www.fullerton.edu
Owner:	This website does not supply ownership information.
Verified by:	Not specified



https://www.fullerton.edu/



This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To

Common Name (CN)	apps.fullerton.edu
Organization (O)	California State University, Fullerton
Organizational Unit (OU)	Information Technology
Serial Number	22:28:CB:B7:FF:E3:13:B9:31:FC:17:D4:F8:2A:13:2C

Issued By

Common Name (CN)	InCommon RSA Server CA
Organization (O)	Internet2
Organizational Unit (OU)	InCommon

Period of Validity

Begins On	Thursday, February 27, 2020
Expires On	Sunday, February 27, 2022

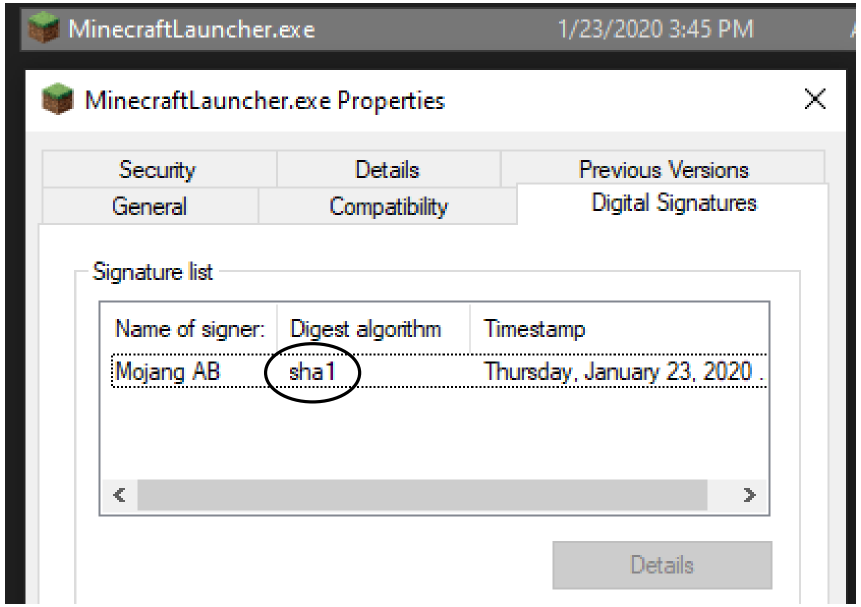
Fingerprints

SHA-256 Fingerprint	90:A3:CB:E6:2F:C4:27:A9:B5:41:8E:FC:5D:73:FD:4E: 3B:7A:73:16:3F:77:7C:79:DF:B6:64:F0:E2:26:34:79
SHA1 Fingerprint	D9:CE:B6:95:A9:C0:05:3A:A9:4E:06:2D:B7:3D:E6:C5:F2:FA:42:85

Process of Code Signing

- https://docs.microsoft.com/en-us/windows/win32/appxpkg/how-to-create-a-package-signing-certificate
- https://docs.microsoft.com/en-us/windows/win32/appxpkg/how-to-sign-a-package-using-signtool

1. Buy or generate certificate using `makecert`. Buying = production.
2. Signing process `signtool sign /tr http://timestamp.digicert.com /td sha256 /fd sha256 /f "c:\path\to\mycert.pfx" /p pfxpassword "c:\path\to\file.exe"`



MinecraftLauncher.exe 1/23/2020 3:45 PM

MinecraftLauncher.exe Properties

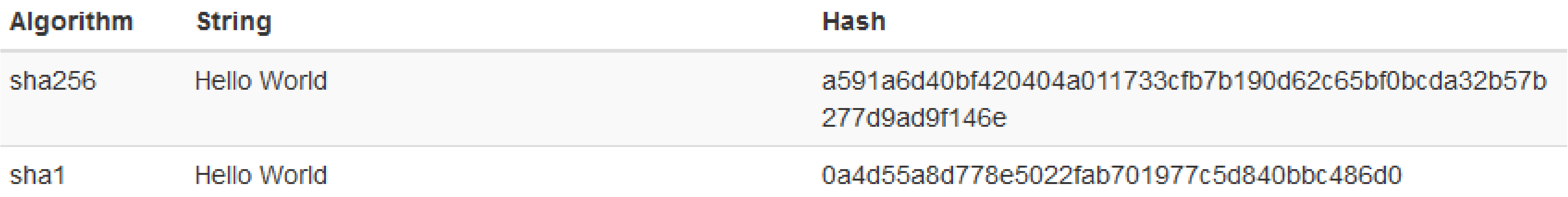
Signature list

Name of signer:	Digest algorithm	Timestamp
Mojang AB	sha1	Thursday, January 23, 2020 .

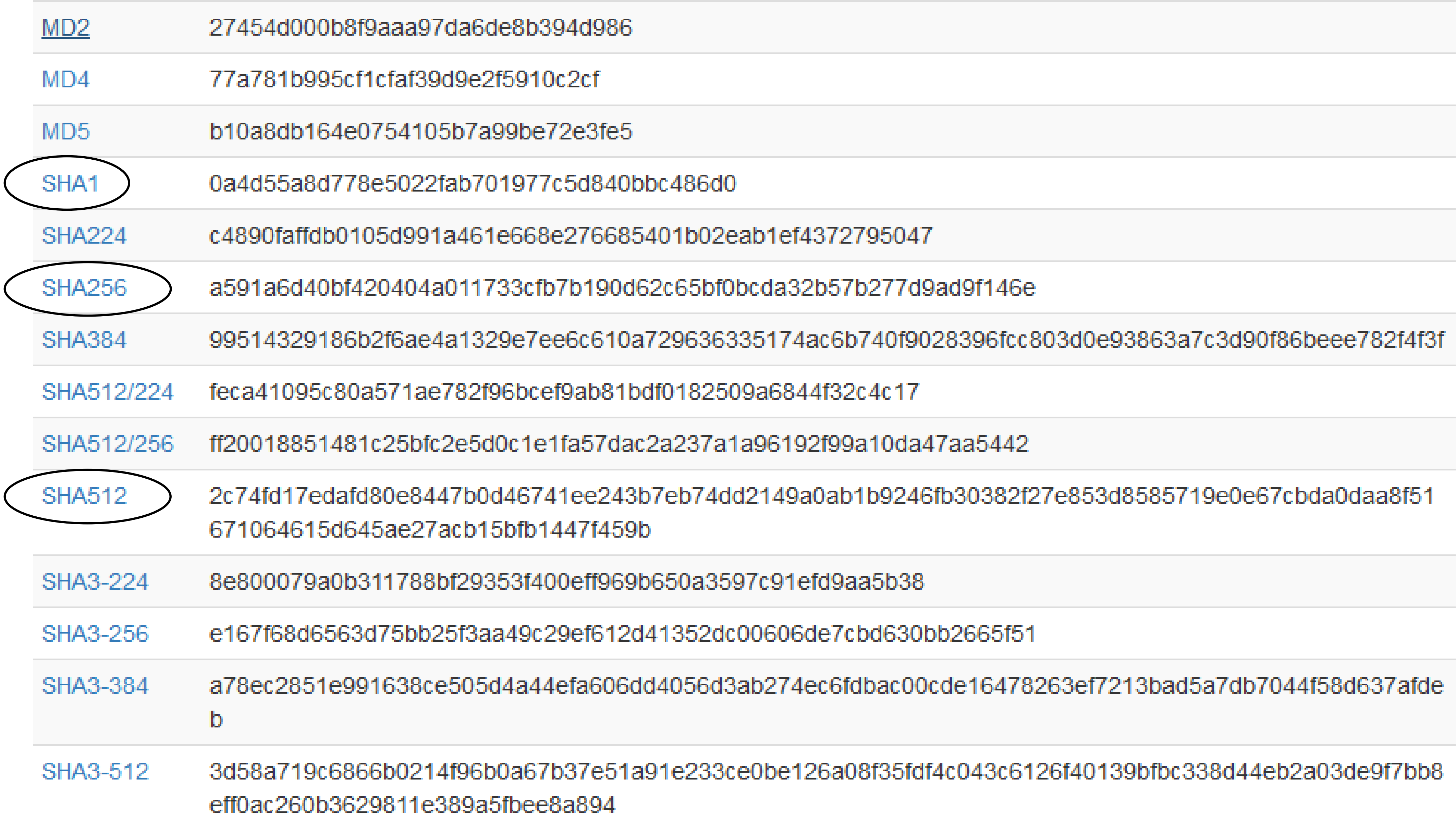
https://docs.microsoft.com/en-us/dotnet/framework/tools/signtool-exe
https://stackoverflow.com/questions/252226/signing-a-windows-exe-file

SHA-0 vs SHA-1 vs SHA-2

- Secure Hashing algorithms
- SHA-0: Created by National Security Agency
- SHA-1: Popular today but weak
- SHA-2: Recommended for high security

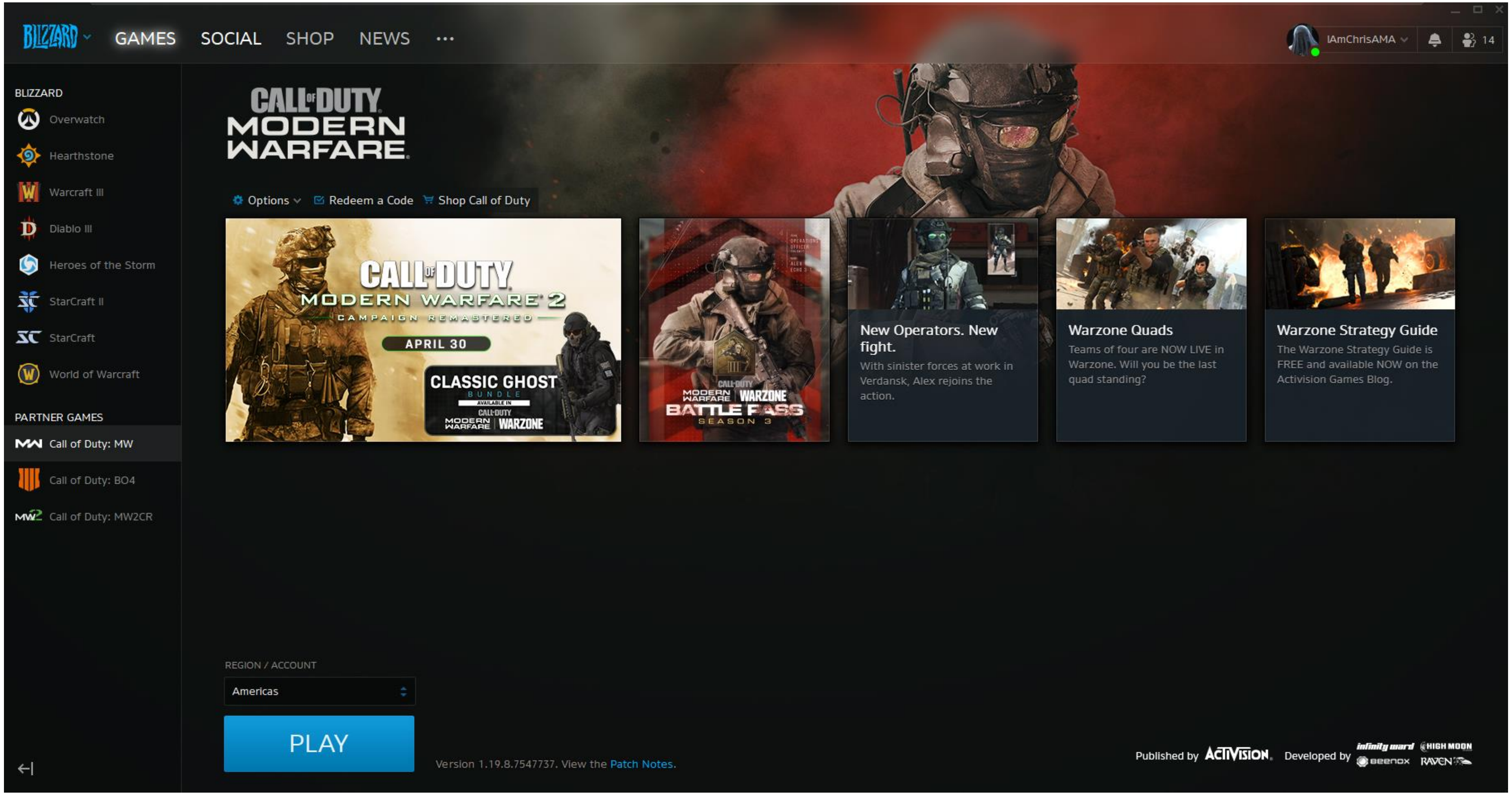


Algorithm	String	Hash
sha256	Hello World	a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e
sha1	Hello World	0a4d55a8d778e5022fab701977c5d840bbc486d0



MD2	27454d000b8f9aaa97da6de8b394d986
MD4	77a781b995cf1cfaf39d9e2f5910c2cf
MD5	b10a8db164e0754105b7a99be72e3fe5
SHA1	0a4d55a8d778e5022fab701977c5d840bbc486d0
SHA224	c4890faffdb0105d991a461e668e276685401b02eab1ef4372795047
SHA256	a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e
SHA384	99514329186b2f6ae4a1329e7ee6c610a729636335174ac6b740f9028396fcc803d0e93863a7c3d90f86beee782f4f3f
SHA512/224	feca41095c80a571ae782f96bcef9ab81bdf0182509a6844f32c4c17
SHA512/256	ff20018851481c25bfc2e5d0c1e1fa57dac2a237a1a96192f99a10da47aa5442
SHA512	2c74fd17edafd80e8447b0d46741ee243b7eb74dd2149a0ab1b9246fb30382f27e853d8585719e0e67cbda0daa8f51671064615d645ae27acb15bfb1447f459b
SHA3-224	8e800079a0b311788bf29353f400eff969b650a3597c91efd9aa5b38
SHA3-256	e167f68d6563d75bb25f3aa49c29ef612d41352dc00606de7cbd630bb2665f51
SHA3-384	a78ec2851e991638ce505d4a44efa606dd4056d3ab274ec6fdbac00cde16478263ef7213bad5a7db7044f58d637afdeb
SHA3-512	3d58a719c6866b0214f96b0a67b37e51a91e233ce0be126a08f35fdf4c043c6126f40139bfbc338d44eb2a03de9f7bb8eff0ac260b3629811e389a5fbee8a894

Example in Practice



New Operators. New fight.

With sinister forces at work in Verdansk, Alex rejoins the action.

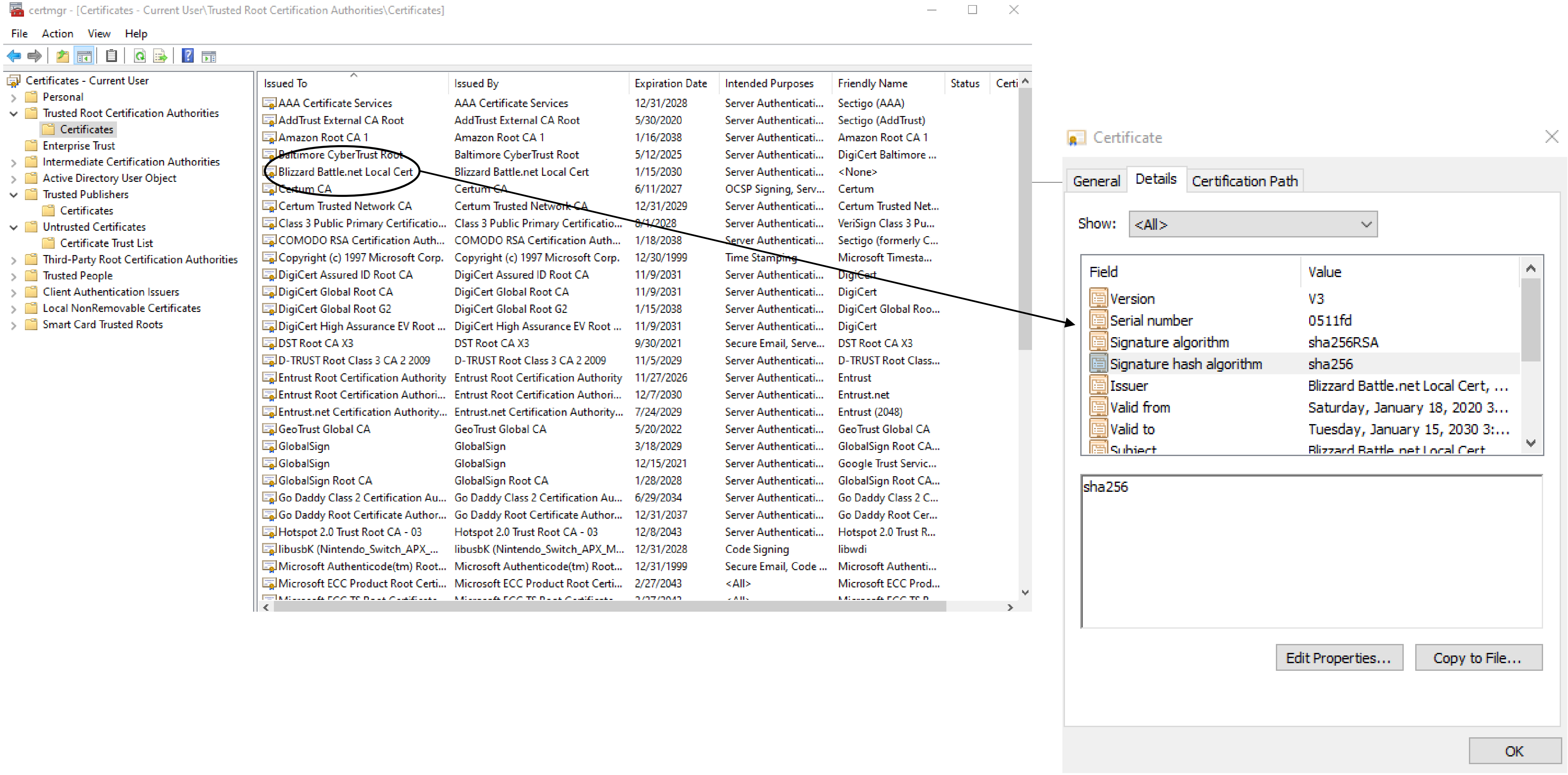
Warzone Quads

Teams of four are NOW LIVE in Warzone. Will you be the last quad standing?

Warzone Strategy Guide

The Warzone Strategy Guide is FREE and available NOW on the Activision Games Blog.

Version 1.19.8.7547737. View the Patch Notes.



certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]

- Certificates - Current User
  - Personal
  - Trusted Root Certification Authorities
    - Certificates
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Active Directory User Object
  - Trusted Publishers
    - Certificates
  - Untrusted Certificates
    - Certificate Trust List
  - Third-Party Root Certification Authorities
  - Trusted People
  - Client Authentication Issuers
  - Local NonRemovable Certificates
  - Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi
AAA Certificate Services	AAA Certificate Services	12/31/2028	Server Authenticati...	Sectigo (AAA)		
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	Sectigo (AddTrust)		
Amazon Root CA 1	Amazon Root CA 1	1/16/2038	Server Authenticati...	Amazon Root CA 1		
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	DigiCert Baltimore ...		
Blizzard Battle.net Local Cert	Blizzard Battle.net Local Cert	1/15/2030	Server Authenticati...	<None>		
Certum CA	Certum CA	6/11/2027	OCSP Signing, Serv...	Certum		
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticati...	Certum Trusted Net...		
Class 3 Public Primary Certificatio...	Class 3 Public Primary Certificatio...	8/1/2028	Server Authenticati...	VeriSign Class 3 Pu...		
COMODO RSA Certification Auth...	COMODO RSA Certification Auth...	1/18/2038	Server Authenticati...	Sectigo (formerly C...		
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...		
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticati...	DigiCert		
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticati...	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Server Authenticati...	DigiCert Global Roo...		
DigiCert High Assurance EV Root ...	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...	DigiCert		
DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, Serve...	DST Root CA X3		
D-TRUST Root Class 3 CA 2 2009	D-TRUST Root Class 3 CA 2 2009	11/5/2029	Server Authenticati...	D-TRUST Root Class...		
Entrust Root Certification Authority	Entrust Root Certification Authority	11/27/2026	Server Authenticati...	Entrust		
Entrust Root Certification Authori...	Entrust Root Certification Authori...	12/7/2030	Server Authenticati...	Entrust.net		
Entrust.net Certification Authority...	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...	Entrust (2048)		
GeoTrust Global CA	GeoTrust Global CA	5/20/2022	Server Authenticati...	GeoTrust Global CA		
GlobalSign	GlobalSign	3/18/2029	Server Authenticati...	GlobalSign Root CA...		
GlobalSign	GlobalSign	12/15/2021	Server Authenticati...	Google Trust Servic...		
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...	GlobalSign Root CA...		
Go Daddy Class 2 Certification Au...	Go Daddy Class 2 Certification Au...	6/29/2034	Server Authenticati...	Go Daddy Class 2 C...		
Go Daddy Root Certificate Author...	Go Daddy Root Certificate Author...	12/31/2037	Server Authenticati...	Go Daddy Root Cer...		
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Server Authenticati...	Hotspot 2.0 Trust R...		
libusbK (Nintendo_Switch_APX_...	libusbK (Nintendo_Switch_APX_M...	12/31/2028	Code Signing	libwdi		
Microsoft Authenticode(tm) Root...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...		
Microsoft ECC Product Root Certi...	Microsoft ECC Product Root Certi...	2/27/2043	<All>	Microsoft ECC Prod...		
Microsoft ECC TS Root Certificate...	Microsoft ECC TS Root Certificate...	2/27/2043	<All>	Microsoft ECC TS R...		

Certificate

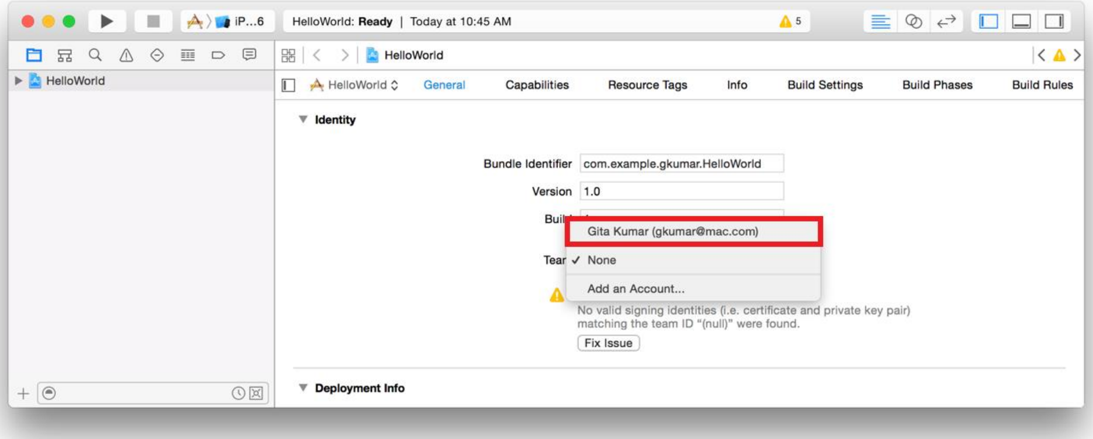
Show: <All>

Field	Value
Version	V3
Serial number	0511fd
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Blizzard Battle.net Local Cert, ...
Valid from	Saturday, January 18, 2020 3:...
Valid to	Tuesday, January 15, 2030 3:...
Subject	Blizzard Battle.net Local Cert

sha256

Apple Implementation

- Requires Apple Developer ID to submit
- Easy to use and obtain however requires higher monetary compensation
- Deteriorates independent developers with pricing through Apple's end



HelloWorld: **Ready** | Today at 10:45 AM

Identity

Bundle Identifier com.example.gkumar.HelloWorld

Version 1.0

No valid signing identities (i.e. certificate and private key pair) matching the team ID "(null)" were found.

Deployment Info

https://devcenter.bitrise.io/img/code-signing/ios-code-signing/xcode_team_selector.png

Drawbacks

- Doesn’t 100% guarantee safe code
- Not typically free when using in business sense (with exceptions)
- Still not trustworthy with closed-source software

Conclusion

- Recommended and acceptable
- Mandated by various operating systems (Windows, MacOS, etc.)
- Essential for running trusted software