LET'S ENCRYPT WITH LET'S ENCRYPT

A BETTER WAY TO MANAGE CERTIFICATES

WHO AM I?

- Tony Morrow
  - @a_gizm0
  - https://lookanotherblog.com
- Principal Solutions Architect @ Bellarmine University
- 12 years working at Bellarmine (10 in the Infrastructure Team)
- Focus
  - Networking
  - Wireless
  - Servers/Virtualization
  - Systems integration
  - AD & AAD management
  - Microsoft Endpoint (Intune & System Center)
  - VoIP

DISCLAIMER ☺

- I am not a Microsoft MVP or Partner
- All technologies showcased are using free, trial, or paid licenses
- All the opinions here are my own
- Nobody is paying me for this presentation
- Nobody has reviewed or approved this presentation before hand

TOPICS

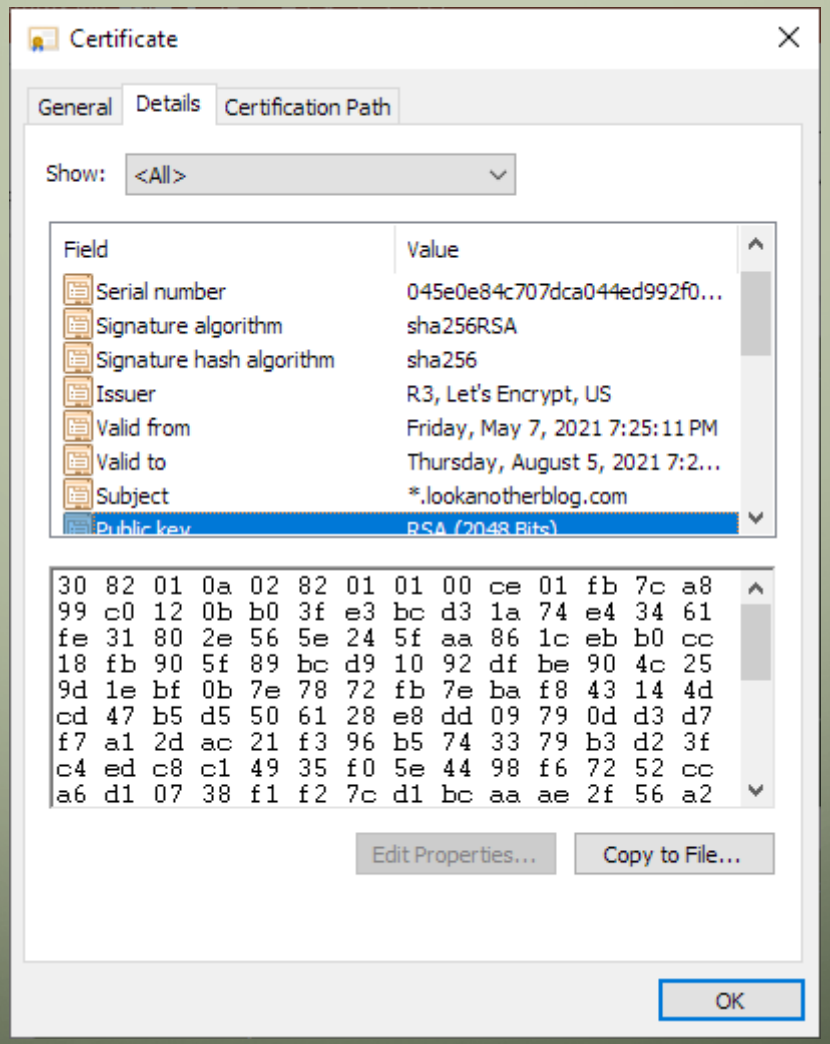
- What are Certificates (x509)
- The state of certificate life cycling today
- How certificate maintenance can be automated for some situations
- Demo!!!

WHAT ARE CERTIFICATES?

MAGIC

WHAT ARE CERTIFICATES

- Most simplified terms:
  - A key (aka cryptographically generated set string of numbers or letters)
  - + Information about the owner of that public key
  - + A digital signature to verify the authenticity of the certificate


Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Serial number
045e0e84c707dca044ed992f0...
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
R3, Let's Encrypt, US
Valid from
Friday, May 7, 2021 7:25:11 PM
Valid to
Thursday, August 5, 2021 7:2...
Subject
*.lookanotherblog.com
Public key
RSA (2048 Bits)
30 82 01 0a 02 82 01 01 00 ce 01 fb 7c a8
99 c0 12 0b b0 3f e3 bc d3 1a 74 e4 34 61
fe 31 80 2e 56 5e 24 5f aa 86 1c eb b0 cc
18 fb 90 5f 89 bc d9 10 92 df be 90 4c 25
9d 1e bf 0b 7e 78 72 fb 7e ba f8 43 14 4d
cd 47 b5 d5 50 61 28 e8 dd 09 79 0d d3 d7
f7 a1 2d ac 21 f3 96 b5 74 33 79 b3 d2 3f
c4 ed c8 c1 49 35 f0 5e 44 98 f6 72 52 cc
a6 d1 07 38 f1 f2 7c d1 bc aa ae 2f 56 a2
Edit Properties...
Copy to File...
OK

```
1   Add-Type -AssemblyName System.Security
2
3   $cert = [System.Security.Cryptography.X509Certificates.X509Certificate]::CreateFromCertFile("C:\users\tony\OneDrive\Documents\Blogs and Videos\LetsEncrypt\lookanotherb
4
5
6
7   $props = [ordered]@{
8       Subject = $cert.GetName()
9       Serial = $cert.GetSerialNumberString();
10      Issuer = $cert.GetIssuerName();
11      StartDate = $cert.GetEffectiveDateString();
12      EndDate = $cert.GetExpirationDateString();
13      PublicKey = $cert.GetPublicKeyString();
14
15
16  }
17
18
19  $out = New-Object -TypeName psobject -Property $props
20
21  Write-Output $out
```

```
PS C:\Users\Tony> Add-Type -AssemblyName System.Security

$cert = [System.Security.Cryptography.X509Certificates.X509Certificate]::CreateFromCertFile("C:\users\tony\OneDrive\Documents\Blogs and Videos\LetsEncrypt\lookanotherblog-cc



$props = [ordered]@{
    Subject = $cert.GetName()
    Serial = $cert.GetSerialNumberString();
    Issuer = $cert.GetIssuerName();
    StartDate = $cert.GetEffectiveDateString();
    EndDate = $cert.GetExpirationDateString();
    PublicKey = $cert.GetPublicKeyString();


}


$out = New-Object -TypeName psobject -Property $props

Write-Output $out


Subject   : CN=*.lookanotherblog.com
Serial    : 045E0E84C707DCA044ED992F0B8112F19D1B
Issuer    : C=US, O=Let's Encrypt, CN=R3
StartDate : 5/7/2021 7:25:11 PM
EndDate   : 8/5/2021 7:25:11 PM
PublicKey : 3082010A0282010100CE01FB7CA899C0120BB03FE3BCD31A74E43461FE31802E565E245FAA861CEBB0CC18FB905F89BCD91092DFBE904C259D1EBF0B7E7872FB7EBAF843144DCD47B5D5506128E8DD
            09790DD3D7F7A12DAC21F396B5743379B3D23FC4EDC8C14935F05E4498F67252CCA6D10738F1F27CD1BCAAAE2F56A23482550BEEF1214517AB1EC3198B764853BBA5E30EB8AD7562B92E5C1BB5D950
            082A2F6E8CA7942621BF0484F1FC1761070B63B2CE4D9E4B80FD63450C60B7D45263031DE92EC4D5E44A299FDF683AE8B86F4604CDFB5530398672D420EE9261C03123BEAAA57F14FFF0FC8D947817
            FDA72F73744A921E5435FB1F095A90C8731D3EE3CF27A4309F59A3310203010001
```

isengard.mordor - PuTTY

```
tony@isengard:~$ openssl s_client lookanotherblog.com:443 | openssl x509 -dates -issuer -serial -pubkey -noout
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R3
verify return:1
depth=0 CN = *.lookanotherblog.com
verify return:1
notBefore=May  7 23:25:11 2021 GMT
notAfter=Aug  5 23:25:11 2021 GMT
issuer=C = US, O = Let's Encrypt, CN = R3
serial=045E0E84C707DCA044ED992F0B8112F19D1B
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzgH7fKiZwBILsD/jvNMa
dOQ0Yf4xgC5WXiRfqoYc67DMGPuQX4m82RCS376QTCWdHr8Lfnhy+366+EMUTclH
tdVQYSjo3Ql5DdPX96EtrCHzlrV0M3mz0j/E7cjBSTXwXkSY9nJSzKbRBzjx8nzR
vKquLlaiNIJVC+7xIUUXqx7DGYt2SFO7peMOuKllYrkuXBul2VAIKi9ujKeUJiG/
BITx/BdhBwtjss5NnkuA/WNFDGC3lFJjAx3pLsTV5Eopn99oOui4b0YEzftVMDmG
ctQg7pJhwDEjvqqlfxT/8PyNlHgX/acvc3RKkh5UNfsfCVqQyHMdPuPPJ6Qwnlmj
MQIDAQAB
-----END PUBLIC KEY-----
```

WHY DO WE USE CERTIFICATES?

- Establishing **TRUST** between systems
- Verifying **IDENTITY** of a person or system
- **ENCRYPTING** communication between systems

THE CERTIFICATE LIFECYCLE

STAB ME IN THE EYE EVERY 13 MONTHS

https://cabforum.org

Search

Getting Started Most Visited

CA/BROWSER FORUM

About Us » | Baseline Requirements » | Extended Validation » | Working Groups » | Proceedings » | Resources »

CA/BROWSER FORUM

WELCOME TO THE CA/BROWSER FORUM

Information for the Public

Organized in 2005, we are a voluntary group of certification authorities (CAs), vendors of Internet browser software, and suppliers of other applications that use X.509 v.3 digital certificates for SSL/TLS and code signing.

>read more

to search type and hit enter

RECENT NEWS

- Ballot SC45: Wildcard Domain Validation June 3, 2021
- Ballot SC46: Sunset the CAA exception for DNS Operator June 2, 2021
- 2021-05-26 Minutes of the S/MIME Certificate Working Group May 26, 2021
- 2021-04-29 Minutes of the CA/Browser Forum Teleconference May 13, 2021
- 2021-04-29 Minutes of the Server Certificate Working Group May 13, 2021
- 2021-05-12 Minutes of the S/MIME Certificate Working Group May 12, 2021

Certification Authorities

- Actalis S.p.A.
- Amazon Trust Services LLC
- Asseco Data Systems (formely Certum)
- Buypass AS
- Camerfirma
- Certinomis
- CERTIGNA
- certSIGN
- CFCA
- Chunghwa Telecom Co., Ltd.
- China Internet Network Information Center
- ComSign Ltd
- D-TRUST GmbH
- DigitalTrust
- DigiCert, Inc.
- Digidentity
- Disig, a.s.
- E-TUGRA Inc.
- eMudhra Technologies Limited
- Entrust
- Firmaprofesional
- Global Digital Cybersecurity Authority Co., Ltd
- GlobalSign
- GoDaddy Inc
- Hellenic Academic and Research Institutions Certification Authority (HARICA)
- iTrusChina
- Izenpe S.A.
- JPRS
- Kamu Sertifikasyon Merkezi
- KPN Corporate Market BV
- Let’s Encrypt
- Logius PKIoverheid
- MSC Trustgate
- National Center for Digital Certification
- NAVER Cloud
- Network Solutions, LLC
- OISTE Foundation
- Open Access Technology International
- Prvni certifikacni autorita, a.s.
- SECOM Trust Systems
- SecureTrust
- Sectigo Ltd.
- Shanghai Electronic Certification Authority Center Co. Ltd
- SK ID Solutions AS
- Skaitmeninio sertifikavimo centras (SSC)
- SSL.com
- SwissSign AG
- TAIWAN-CA Inc.
- Telia Company
- TrustCor Systems, S. de R.L.
- Visa

Certificate Consumer Members

- 360
- Apple
- Brave
- Cisco
- Comodo
- Google Inc.
- Microsoft Corporation
- Mozilla Foundation
- Opera Software AS
- Zertificon

HOW WE GET CERTIFICATES

1. Generate a certificate request
2. Pay a Certificate Authority a large sum of money
3. Submit request to CA
4. Receive the certificate
5. Apply certificate to your system
6. Repeat

CERTIFICATE VALIDATION PERIOD

- 2011: 60 months
- 2015: 39 months
- 2018: 825 days (27 months)
- 2020: 398 days (13 months)

office365.bellarmine.edu SharePoint

Search this site

CM

Certificate Management

- Home
- Conversations
- Documents
- Notebook
- Pages
- Wildcard 2021-May
- Site contents
- Recycle bin
- Edit

New | Page details | Analytics

Wildcard 2021-May

New | Edit in grid view | Share | Export to Excel

MindMeld	Complete	Tony Morrow	nginx
Moodle-27v2	Complete	Brian N. Henry	
Moodle-32	Complete	Brian N. Henry	
Moodle-35	Complete	Brian N. Henry	
MoodleWeb	In Process	Brian N. Henry	
MoodleWeb-ed	Complete	Brian N. Henry	
MoodleWeb-nm	Complete	Brian N. Henry	

IS THERE A BETTER WAY?

YES

Let’s Encrypt

WHAT IS LET'S ENCRYPT?

- A free, automated, and open certificate authority (CA), run for the public's benefit. It is a service provided by the Internet Security Research Group (ISRG).
- Started in 2013 by Josh Aas with sponsorship from Mozilla, EFF, and University of Michigan
- In 2015 certificates became trusted by all major browsers

MAJOR SPONSORS AND FUNDERS

moz://a
CISCO
EFF
OVHcloud
chrome
Internet Society
facebook
aws
BILL & MELINDA GATES foundation
IdenTrust
FORD FOUNDATION
avast
Reprise SOFTWARE
AUTOMATTIC
shopify
Akamai
ALA American Library Association
cyon
infomaniak
HOSTPOINT
SiteGround
VULTR
PlanetHoster
fastly
3CX
SQUARESPACE
HawkHost
thebestvpn
JIMDO
VTEX
DigitalOcean
zendesk
netlify
HOSTPAPA
PANTHEON Website Management Platform
dnsimple
discourse
driving-tests.org
SAKURA internet
DuoCircle
ise
ServerPilot
domainnameshop

WORLD4YOU INTERNET SERVICES GMBH
GitHub
UNRAID
KEENETIC
HAPROXY
datto
AXIOM
THE BEST RUN SAP
verizon digital media services
mongoDB
IBM
Livesport
nazwa.pl
clever cloud
render
ipinfo.io
GreenGeeks WEB HOSTING
Red Hat
NABU CASA
WiX.com
Engine Forex
HEROKU
SNIPE-IT
smallstep
VPNCompare
wpbeginner
HostScore
HOSTSTAR GO LIVE
vmware
one.com
DAN.COM
CLOUDERA
HACKTHEBOX
eukhost
LINE
CARGO
MANUALSBRAIN.COM
DEUTSCHE TELEKOM PAN-NET
RACKSPEED
4K Video Downloader
duda
ads
Teleport

COMPATIBILITY

- Platforms that trust DST Root CA X3
  - Windows >= XP SP3
  - macOS (most versions)
  - iOS (most versions)
  - Android >= v2.3.6
  - Mozilla Firefox >= v2.0
  - Ubuntu >= precise / 12.04
  - Debian >= squeeze / 6
  - Java 8 >= 8u101
  - Java 7 >= 7u111
  - NSS >= v3.11.9
  - Amazon FireOS (Silk Browser)
  - Cyanogen > v10
  - Jolla Sailfish OS > v1.1.2.16
  - Kindle > v3.4.1
  - Blackberry >= 10.3.3
  - PS4 game console with firmware >= 5.00

- Platforms that trust ISRG Root X1
  - Windows >= XP SP3 (assuming Automatic Root Certificate Update isn't manually disabled)
  - macOS >= 10.12.1
  - iOS >= 10 (iOS 9 does not include it)
  - iPhone 5 and above can upgrade to iOS 10 and can thus trust ISRG Root X1
  - Android >= 7.1.1 (but Android >= 2.3.6 will work by default due to our special cross-sign)
  - Mozilla Firefox >= 50.0
  - Ubuntu >= xenial / 16.04 (with updates applied)
  - Debian >= jessie / 8 (with updates applied)
  - Java 8 >= 8u141
  - Java 7 >= 7u151
  - NSS >= 3.26

HOW WE GET CERTIFICATES FROM LET'S ENCRYPT

1. Install an application or script on the server requesting a cert
2. The app/script initiates a cert request to Let's Encrypt
3. Let's Encrypt responds with a verification string
4. App/script places verification string on web host or in DNS entry
5. Let's Encrypt verifies the string exists
6. Let's Encrypt issues a certificate to the requesting server

ACME Client Implementations

Last updated: Jun 21, 2021 | See all Documentation

Let's Encrypt uses the ACME protocol to verify that you control a given domain name and to issue you a certificate. To get a Let's Encrypt certificate, you'll need to choose a piece of ACME client software to use.

The ACME clients below are offered by third parties. Let's Encrypt does not control or review third party clients and cannot make any guarantees about their safety or reliability.

Some in-browser ACME clients are available, but we do not list them here because they encourage a manual renewal workflow that results in a poor user experience and increases the risk of missed renewals.

Recommended: Certbot

We recommend that most people start with the Certbot client. It can simply get a cert for you or also help you install, depending on what you prefer. It's easy to use, works on many operating systems, and has great documentation.

If Certbot does not meet your needs, or you'd simply like to try something else, there are many more clients to choose from below, grouped by the language or environment they run in.

Other Client Options

All of the following clients support the ACMEv2 API (RFC 8555). We'll be entirely phasing out support for ACMEv1 soon. If you're already using one of the clients below, make sure to upgrade to the latest version. If the client you're using isn't listed below it may not support ACMEv2, in which case we recommend contacting the project maintainers or switching to another client.

Bash

- GetSSL (bash, also automates certs on remote hosts via ssh)
- acme.sh (Compatible to bash, dash and sh)
- dehydrated (Compatible to bash and zsh)
- ght-acme.sh (batch update of http-01 and dns-01 challenges is available)
- bacme (simple yet complete scripting of certificate generation)
- wdfcert.sh (Only supports DNS-01 challenges and ECDSA-384 bit keys for both accounts and certificates, native Joker DNS support including wildcard plus roor domain support for single-TXT-record DNS providers)

C

- OpenBSD acme-client
- uacme
- acme-client-portable
- Apache httpd Support via the module mod_md.
- mod_md Separate, more frequent releases of the Apache module.
- CycloneACME (client implementation of ACME dedicated to microcontrollers)

C++

- acme-lw
- esp32-acme-client allows IoT devices to get certificates

Clojure

- certificaat

Configuration management tools

- Ansible acme_certificate module
- Terraform ACME Provider

D

- acme-lw-d

Domino

- CertMatica (ACME certificate installation and renewals for HCL Domino™ servers)
- HCL Domino (Full ACME V2 flow integration for HCL Domino™ servers)

Docker

- ZeroSSL

Go

- Caddy
- Lego
- acmetool
- Lets-proxy2 (Reverse proxy to handle https/tls)
- autocert
- Traefik
- ACMEz
- Step CLI

HAProxy

- HAProxy client

Java

- PJAC
- ManageEngine Key Manager Plus

Lua

- Mako Server's ACME Plugin The plugin's main objective is to provide certificates for servers on private networks.

Microsoft Azure

- Azure WebApp SSL Manager (Serverless, Compatible with any App Service, requires Azure DNS)
- App Service Acmebot (Compatible to Azure Web Apps / Functions / Web App for Containers)
- Key Vault Acmebot (Work with Azure Key Vault Certificates)
- Nginx ACME
- lua-resty-acme

Node.js

- Greenlock for Express.js
- acme-http-01-azure-key-vault-middleware (Express middleware for storing certificates securely on Azure Key Vault)

OpenShift

- openshift-acme

Perl

- acme (Simple json config, autogen keys, issue cert, refresh cert, apache/nginx integration)
- Crypt::LE

PHP

- Hiawatha
- FreeSSL.tech Auto
- Yet another ACME client
- ltr-acme-client PHP library
- Acme PHP
- RW ACME client

Python

- ACME Tiny
- simp_le
- acmebot
- sewer
- acme-dns-tiny (Python 3)
- Automatoes ACME V2 ManuaLE replacement with new features
- acertmgr
- acme-cert-tool
- serverPKI PKI for internet server infrastructure, supporting distribution of certs, FreeBSD jails, DNS DANE support

Ruby

- unixcharles/acme-client
- acme-distributed
- Combine-acme: Generate and upload crt to CloudFlare(enterprise) and GCP.

Rust

- ACMEd
- acme-redirect

Windows / IIS

- ZeroSSL project
- win-acme (.NET)
- Posh-ACME (PowerShell)
- Certes
- ACME-PS (PowerShell)
- Certify The Web (Windows)
- WinCertes Windows client
- GetCert2 (simple GUI - .Net, C#, WPF, WCF)

Libraries

4D

- acme component ACME Client v2 for 4D v18+

C++

- acme-lw
- esp32-acme-client allows IoT devices to get certificates

D

- acme-lw-d

Delphi

- DelphiACME (Embarcadero Delphi)

Go

- Lego
- acmetool
- eggsampler/acme
- ACMEz

Java

- ACME4j

.NET

- Certes (.NET Standard)
- PKISharp/ACMESharpCore (.NET Standard)

Node.js

- Greenlock for node.js
- publishlab/node-acme-client

Perl

- acme (Simple json config, autogen keys, issue cert, refresh cert, apache/nginx integration)
- ZeroSSL project
- Crypt::LE
- Net::ACME2

WHAT IS LET’S ENCRYPT GOOD FOR?

- Public web servers (Apache, Nginx, IIS, Tomcat)
- IOT
- Internet accessible services

WHAT IS LE **NOT** GOOD FOR?

- Internal Systems
- Applications that require manual certificate installation

CONCLUSIONS

CONCLUSIONS (JOKE)

- Certificates are magic
- Certificate Authorities are the Mafia
- Let’s Encrypt is the people’s CA

CONCLUSIONS

- Certificates are critical to a secure Internet
- The CAB Forum are setting important standards and practices around certificates
  - Even if we (administrators) complain about the extra work it creates
- There are ways to automate certificate renewals
  - Let’s Encrypt is just one option

DEMO

CITATIONS

- CAB Forum SSL/TLS Requirements: https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.7.4.pdf
- Let's Encrypt: https://letsencrypt.org/about/
- ISRG: https://www.abetterinternet.org/about/
- Sponsors/Funders: https://letsencrypt.org/
- LE becomes Trusted: https://letsencrypt.org/2015/10/19/lets-encrypt-is-trusted.html
- Compatibility: https://letsencrypt.org/docs/certificate-compatibility/