Global Information Assurance Certification Paper

Defending Against the Weaponization of Trust: Defense in Depth Assessment of TLS

GIAC (GSNA) Gold Certification

Author: Sandra (Sandy) Dunn, sandra.dunn@hp.com
Advisor: Stephen Northcutt

Accepted: April 6th, 2016

Abstract

X.509 certificates are the cornerstone of brokered trust across the digital landscape both inside and outside the firewall. Often they are too trusted and become the weapon of choice for attackers looking for the easiest way to bypass the first layers of controls. Implementing additional layers of certificate quality controls using a Defense in Depth strategy reduces the X.509 certificate attack surface and ensures a reliable trust anchor.

X.509 certificates are the best and in almost all cases the only way to establish who and what services to trust. They are the trusted courier that delivers the public key bound to a unique distinguished name, the subject, and owner of the asymmetric key pair that validates the invisible person or service to be trusted. Just like any security workforce, they do require management, auditing, and a regular physical examination to ensure they can still do their job of protecting the business.

An assessment of the existing current environment is the first step in establishing the organizational TLS maturity level and prioritizing any required X.509 Certificate remediation.

This paper focuses on two X.509 certificate services, domain web servers, and code signing that are frequently deployed without an organized strategy. It is important to note an organization's assessment and audit plans should include all of the X.509 certificates that support services.

1. Introduction

Public Key Infrastructure (PKI) and X.509 certificates support nearly all secure web and application trust and communication. There has been an explosion of X.509 certificates on the network because of the increased need to secure communication, business's application migration to cloud services, concerns for personal privacy, and an increase in services that rely on X.509 certificates for trust and to secure communications.

Contributing to the difficult and chaotic environment is a lack of strategic planning, limited availability of X.509 management tools, and increased complexity of X.509 certificate configuration. This hyperbolic environment has offered an opportunity for the creative cybercriminal, allowing them to bypass overly trusted X.509 certificates and in some cases, using them to compromise businesses they should be protecting.

One defense in depth security control all organizations should implement is reviewing Certificate Transparency (CT) logs. Google designed CT is an "open auditing and monitoring system that lets any domain owner or certificate authority (CA) determine whether their certificates have been mistakenly issued or maliciously used." (Google, 2016) CT is now an Internet Engineering Task Force (IETF) experimental standard RFC6962, (B. Laurie, 2013) CT has been effective in enforcing trust in X.509 certificates by exposing both miss issuance of X.509 domain certificates as well as questionable practices by many public Certificate Authorities. (Armasu, 2016) Information on X.509 code signing certificate is not available in current CT logs and is a trust and transparency gap in the current capturing, monitoring, and alerting of issued X.509 certificates.

Microsoft's solution to the escalating threat of code signing certificate compromise is Microsoft SmartScreen. Microsoft SmartScreen is similar to CT in that it provides more visibility to the trustworthiness of the code-signing signature of code-signed applications. It uses both whitelist, blacklists, and EV certificates to determine the applicable level of trust for an application. Unlike CT, SmartScreen is enabled by default and administrators face a different dilemma, how much they allow users to turn off since most users find it annoying and intrusive.

An X.509 certificate assessment is used to evaluate an organization's current state and existing risk based on existing policy, procedure, and implemented security controls

Author Name, email@address

such ast Certificate Transparency and Microsoft's SmartScreen. Risks are calculated based on the controls that are and aren't in place.

Provided examples for web servers X.509 certificates and code signing certificates can be modified to support any service X.509 certificates support.

2. X.509 Certificate Overview

A public key infrastructure (PKI) issues X.509 certificates and includes roles, policies, and procedures to issue the X.509 certificates and to manage them. A Certificate Authority (CA) is an organization that issues and digitally sign a certificate to an authorized and authenticated person or entity requesting a certificate.

Baseline requirements for Domain Validated (DV), Organizational Validated (OV), and Extended Validated (EV) certificates, as well as other standards and requirements for CA and X.509 Certificates, are provided through the Certification Authority Browser Forum (CA/BF). The CA/BF is a voluntary group of CA, browser providers, operating system provider, and other related PKI parties who establish security guidelines that are interoperable and consistent (CA / Browser Forum, 2016).

Google is an active participant in the CA/BF and a positive force in improving the trustworthiness of X.509 certificates. They have received the most publicity from their Certificate Transparency project, but it is only one of many improvements in X.509 and the Public PKI ecosystem Google is driving.

2.1. Differences of Public and Private CA

Symantec, Comodo, and GoDaddy are examples of public Certificate Authorities. The X.509 certificates issued to people and or organizations from large public CAs are trusted because default trusted root stores in applications like Windows operating systems, or in browsers like Safari or Firefox include a trusted root certificate for the public Certificate Authorities.

It is not required to purchase a X.509 certificate from a public CA. Any entity can manage their PKI environment and manage a Private CA. Private CA's are self-contained and generates all the certificates from the original root certificate to the end entity certificates.

Partially self-contained / self-managed CA merges the public and private PKI Certificate ecosystem. In a partially self-managed CA, the root certificate is purchased, but an authorized certificate administrator manages the intermediate and end-entity certificates within the purchasing organization.

The Private PKI owner must provide both types of Private PKI CA root certificates to the end user and imported into their trusted root store. Private CA certificates are not revoked through the standard certificate revocation list (CRL) process even if a recognized CA issued the private PKI root certificate.

2.2. Certificate Transparency

Certificate Transparency addresses the potential for abused trust in the issuance of rouge X.509 domain certificates. There are over 600 public CAs, who can accidently or purposely miss issue an X.509 certificate for any domain. The sheer numbers heightens the risk as does the different political climates, the CAs government's possible misaligned view on citizens' rights, different legal jurisdictions, and the existing hostile relationships between countries.

Monitoring public CT logs alerts the domain owner of any X.509 certificate request and suspicious activity. Organizations may choose to monitor only their domain certificates or extend their trust boundary and monitor any domain where trust assurance is critical to their business. Certificate Transparency has proven two things in the short time it has been monitoring logs; how effective it is at exposing certificate irregularities, and how frequently certificate irregularities happen. Facebook and Google both discovered cases of miss issued X.509 Certificates for their domains. In each case, the issuance of the requested X.509 certificates was reported as an accident and the X.509 certificates were revoked before any impact to customers. CT logs have also exposed unethical X. 509 issuance Symantec, Bluecoat, and StartEncrypt (Ottow, 2016). Until recently CT only supported the expensive high assurance EV certificates. Google recently announced plans to also support OV and DV certificates.

The evidence of trust abuse in issuance of domain X.509 certificates builds a strong case CT should provide the same visibility and accountability for the issuance of X.509

code signing certificates. Code signing CT logs would provide a way users, security vendors, and security researchers could identify legitimate or illegitimate stolen or nefariously purchased code signing certificates.

Considering the current deficiencies in revoking code signing certificates the additional transparency provided by CT X.509 code signing certificates is urgently needed. As designed in the PKI lifecycle, when a certificate is no longer trustworthy it is revoked. Unfortunately, in actual practice, completely revoking a code signing certificates is almost impossible because of how many ways and widely applications are distributed. Microsoft introduced time stamping to address this challenge. Time stamping code with the digital signature allows it to be revoked by a timestamp date. A time stamp indicates "Don't trust this key after this date, but before this date, you can still trust the provided X.509 certificate and provided a public key." Once again theory and real world practice conflict. In practice, it may take years before the discovery of a compromised certificate and knowing exactly when in the timestamp to revoke the X.509 certificate is at best a guessing game. That is if it gets revoked, frequently the legitimate owner of the code signing certificate is unaware it is gone and signing malware (DiMaggio).

Security researchers and malware authors have both discovered revocation of code signing certificates are ineffective, making little difference in establishing what code is signed with an untrustworthy certificate. (Platon Kotzias, 2015) Despite the need for CT logs for X.509 certificates and the benefit to users, vendors, and other members of the PKI ecosystem, Google has not provided any encouraging information on plans to include code signing certificates in the future (R, Ronca, personal communication, June 27, 2016).

This monopoly on the future features CT roadmap highlights another existing challenge with CT. In a good ecosystem, there is a balance of power between all the dependent entities. Google's dominance in the current PKI ecosystem allows them to bully other PKI enterprises to conform to their strategy even if it primarily benefits Google.

In another example of clashing giants; Chrome, FireFox, Safari, and Opera support CT, but Microsoft's Internet Explorer and Microsoft's new Edge browser do not support

it. (Anoosh, 2014) Microsoft has not shown any indication they plan to support CT in future browser versions.

2.2.1. Microsoft SmartScreen Application Reputation

It is possible that code signing Certificate Transparency has been a lower priority for the Google team because Google applications are not as dependent on code signing as a single source of trust. Windows applications have a different distribution model than either IOS applications or Android applications and rely more on the code signing signature to determine if an application is trustworthy. There are other types of files besides Windows, Android, and iPhone OS (IOS) that use code signing such as JAR files, FireFox extensions, and Adobe files but Microsoft Authenticode certificates are what thieves and malware author's target.

Microsoft provides its version of a certificate reputation service in the SmartScreen application. The SmartScreen solution builds reputation filters using data captured from Microsoft Edge, Internet Explorer, Bing, Defender, and the Enhanced Mitigation Experience Toolkit (Microsoft Edge Team, 2015). If there is no available information on the provided code signing organization or the code signing certificate, the application is flagged as untrusted. The application increases trust reputation with the capture of positive reputation information.

Instead of being a positive security differentiator for Microsoft, SmartScreen Application has been critically received by users, developers and security researchers. Users are frustrated by the flags and warnings and find using it intrusive. Developers, especially developers from smaller organizations, believe the reputation scores unfairly hamper their distribution and favor larger organizations. Security researchers have voiced concerns on the lack information disclosure on how SmartScreen determines what makes an application trustworthy (Buttyan, 2015).

Even with the rocky start, SmartScreen is an opportunity for Microsoft to lead and differentiate establishing application trust. SmartScreens builds a much-needed trust layer into X.509 code signing signatures.

2.2.2. Lack of Centrally Visible Code Signing Blacklists

A common way to track bad domain X.509 certificates is community maintained blacklists. A similar well-maintained list is not available for code signing certificates. The Computing Security Standards organization maintains the only community-driven code signing certificate blacklist and it lists only a small fraction of the known bad X.509 code signing certificates.

It is possible to build a code signing certificate blacklist as described by researchers in the abstract" Certified PUP: Abuse in Authenticode" (Kotzias, Matic, Rivera, & Caballero). They built a code signing signature blacklist of 2170 X.509 certificates by looking at the malware files listed on VirusTotal and making a list of X.509 certificate serial numbers from the signatures. VirusTotal, which is an Alphabet owned entity, could easily provide the blacklist service but an email correspondence with their development team indicates there is no upcoming plan to do so (Benito, 2016).

2.2.3. The Challenge of Revocation

Revoking a certificate removes the trust in the X.509 certificate. The revoked X.509 certificate's serial number is advertised on CRL, through Online Certificate Status Protocol (OCSP), and through updates to trusted root stores. Certificates are revoked for many reasons; it's not always because of a key compromise, although for code signing that is the primary reason.

Microsoft applications are the primary applications that are impacted by certificate revocation. Attackers target Microsoft Authenticode code and the poor revocation process as seen in the malware advertisement in Fig. 1.

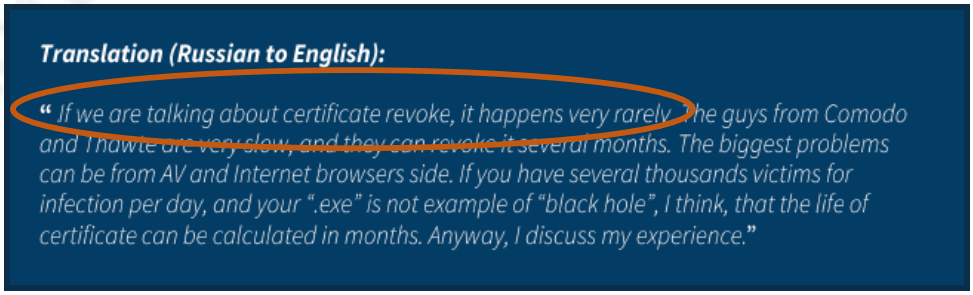


Figure 1. Hidden Lynx – Professional for Hire (Doherty, Gegeny, Spasojevic, & Baltazar, 2013)

Numerous studies and researcher papers examining code signing, time stamping, and effective malware techniques confirm Microsoft applications and Authenticode certificates are the primary targets. A summary of the biggest concerns raised:

- Malware signed with revoked certificates (Kotzias, Matic, Rivera, & Caballero)
- The length of time for a certificate to be revoked (average 133 days) (Kotzias, Matic, Rivera, & Caballero)
- Need for a verbose malware certificate Blacklist. The CSSS Forum provides a blacklist, but research has found that it only a limited number of the existing compromised X.509 certificates
- Lack of visible communication process to notify CA vendors of compromised certificates found in the wild (Kotzias, Matic, Rivera, & Caballero)
- Expired Timestamped certificates are often removed from CRL lists even though the CA/BF code signing guidelines state they should remain on the list for a minimum of 10 years past the certificate expiration date. (Platon Kotzias, 2015)

Less studied, but potentially more dangerous, private X.509 Certificate revocation is completely opaque to users and system administrators. Private CA X. 509 certificates are used to establish trust in BIOS, Internet of Things (IOT) firmware, and IOT applications. The possible impact is concerning when discussing printers, routers, and laptop BIOS but even more sobering when the list is expanded to Jeep vehicles, Chrysler vehicles, or medical devices.

The Superfish, eDellRoot, and PrivDog vulnerabilities are recent cases of the exposure and damage caused by Private CA issued X.509 certificate tampering with certificate deployments. Each of these cases mismanaged the deployment of the X.509 certificates and the trusted root store. There was no visibility or information provided to to users on how the trust in the X.509 certificates was modified and their risk of compromise (Constantin, 2015).

How Private CA establish root CA trust varies on the application and use. For software applications like the Fiddler, they are asked during the installation of the software if they would like to add the Fiddler Root CA to the user's trusted root store. For base level hardware software like BIOS or firmware, a trusted root store and the appropriate root certificate for validation are bundled together out of view for the user or system administrator.

Author Name, email@address

3. Assessment of X.509 Certificates

Web Servers use X.509 Certificates for two main purposes. First, to validate their identity to web clients, and secondly to prevent disclosure or modification of communication between the web client and the web server while the information is in transit. X.509 certificates can validate the client to the web server, but the web server rarely uses it. [1]Code Signing uses digital signatures to validate the identity of the software publisher. It provides authenticity, the identity of the author, and integrity, the code is the same code that the author published for download. [2]

To determine an organization existing X.509 risk use these steps. Perform a policy and procedure assessment of how X.509 certificates are used in the organization look for:

- Up to date policy written for each service that X.509 certificates support.
- A mapping of compliance requirements to written policy requirements
- Documented standards and specifications written to support the policy.
- X.509 certificates for each type of service are managed centrally through a documented process.
- Consolidated dashboards presented to executive staff with columns for known vulnerabilities, risks, and a remediation timeline mapped to a strategically defined TLS maturity roadmap.

Perform a physical assessment. Locating the X.509 certificates will depend on the type of service the X.509 certificate is supporting. There is a list of tools for locating X.509 Certificates provided in the appendix. Physical assessment of security and additional controls for certificates are broken into three high-level areas. Further define requirements by specific assessment requirements based on the service X.509 certificates is supporting.

[1] More detailed description of the value of web server certificates available in SANS Gold Paper, "The Business Case for TLS Certificate Enterprise Key Management of Web Site Certificates: Wrangling TLS Certificates on the Wild Web"
[2] In depth description of code signing available in SANS Gold paper, "The Scary and Terrible Code Signing Problem You Don't Know you have"

(1) Discovery X.509 certificate, (the key courier,) ensuring only approved X.509 certificates and know where they are (no rouge).
(2) Health Management, validating the X.509 certificates using secure configurations with appropriate key length, lifecycle, and cryptographic suites.
(3) Trust Authentication and Authorization, process that establishes the owner and appropriate protection of the private key.

3.1. Auditing X.509 Webserver Certificates

	Tool[3]	Expected results	Red Flags
Discovery			
Internal Network	OpenSSL NMAP Powershell certmgr	All discovered certificates are validated on a known managed list through the approved vendor	Finding any unknown X.509 certificates. Finding expired certificates.
External Network	Censys.io https://crt.sh/	All discovered certificates are validated on a known managed list have through the approved vendor	Finding any unknown X.509 certificates. Finding expired certificates.
Health			
Internal Network	Powershell OpenSSL NMAP	All certificates are up to date and meet enterprise policy	Expired Certificates, unsafe configurations
External Network	https://securityheaders.io/ Qualys SSL Labs High-Tech Bridge	All certificates are up to date and meet enterprise policy	Expired Certificates, unsafe configurations
Trust			
	Documented process and web server X.509 certificate roles and responsibility	Web server certificate requestors follow a process.	No documented process, responsibility unclearly defined and managed by emergency resolution.
	Centrally managed web	Centrally managed	Purchasing X.509

[3] There are many commercial tools that are designed for X.509 certificate discovery, health, Trust, and management. This list and the Tools appendix only lists free or open source tools.

	server X.509 issuance application that requires authentication and approval through appropriate IT manager.	web server X.509 issuance application that requires authentication and approval through appropriate IT manager.	certificates driven by marketing or application teams who purchase from random CA's.

3.2. Auditing X.509 Code Signing Certificates[4]

	Tool	Expected results	Red Flags
Discovery			
Code Repository Shared Files	Osslsigncode	All Code is signed All Code is signed through a centrally approved process	Unsigned files, files signed with certificates obtained outside of approved code signing process
Validate network monitor includes signatures for malware that steals X.509 Certificates	Snort	Signatures are included in malware network monitoring tool.	Malware such as Backdoor.Beasty or Infostealer.Snifula that steals code signing certificates
Health Management			
Are binaries being signed correctly	Authenticode Lint	All binaries are signed correctly	Look for any abuses of padding spaces in Authenticode signatures like extra certificates in the certificate chain.
Validate SHA256 signatures	Certutil PowerShell	Files with a SHA1 signature are timestamped. New signatures use SHA256	SHA1 signatures without a timestamp
Trust			
Confirm that there is a centralized auditable code signing authorization process.	Centrally managed code signing X.509 service that requires authentication and approval through	Centrally managed code signing X.509 service that requires authentication & approval through appropriate IT or product manager. HSM used. Strategic key rotation used.	No central service Single key used for all code signing Keys in and out of an HSM

[4] Auditing by vendor who signs code. Auditing the trusted signatures of applications is valuable but not included in "Auditing X.509 Code Signing Certificates" table.

	appropriate IT or product manager. HSM		
Ask for auditable log that confirms the files chain of custody and integrity process	Documented Policy and auditable process on how files from other vendors are obtained and validated for integrity.	Files included in product .inf or .exe files obtained from other vendors are a known source	Unsigned files from outside the organization included in signed packages. Files provided through email.
Check representative sample of signed code	Sigcheck.exe	Appropriate sample size of code signed applications uploaded to VirusTotal does not report as malware	Applications signed at organization report as untrustworthy

3.3. TLS Maturity Levels

Ivan Ristic, author of Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Application, and one of the recognized leaders in TLS has suggested environments approach TLS deployment in maturity stages.

TLS Maturity levels measure organization's existing TLS maturity, identify missing elements and provide a way to measure against other organizations or different business units within the same organization.

He has proposed five levels of TLS deployment maturity. I have added additional items to his initial list with an * asterisk for Mr. Ristic's original list items. (Ristic, 2015)

	Applies to all certificates	Web Server Certificates	Code Signing Certificates
Level 1 Chaos/ initial implementation*	• No policy or standards* • Vendor default* • Ad hoc*	• No specific team assigned responsibilities • No strategy (updating golden images)	• Unsigned code released • No control over who purchases a code signing certificate • No established policy or process for what is included in signed

			packages.
Level 2 Configuration*	• Focus on the TLS protocol*	• Target web server configuration	• Time-stamped certificates • Established key strategy, i.e., by product line • Audit of released software packages for any unknown keys
Level 3 Application Security*	• Central management of all certificate deployments	• Remediating mixed content on web pages – i.e., the entire application surface must be encrypted* • Use of secure cookies*	• Consistent use of code signing • Audit of released software packages for any unknown keys • Auditable process for signed files
Level 4 Commitment*	• Careful review of issuing CA CP & CPS statement • Individual policies that address specific use of certificates • Monthly Executive Dashboard of current TLS issues • Network scanning for rogue keys • Malware scanning for known key	• Use of HSTS* • Use of HTTPS across all domain pages	• Key rotation by product • Proactive search for malware with compromised code signing certs
Level 5 Robust Security protecting against CA issues*	• Centralized Authentication & Authorization of key use • Reduce attack surface by removing	• Key Pinning* • Certificate Transparency	• Central code repository • Signatures for private key stealing malware

Author Name, email@address

	unneeded CA's • Planned emergency strategy in the case of a CA, RA, or IA compromise		

4. Summary

X.509 certificates are the reliable personal security guards needed to watch and protect organizations and establish which person, domain, or application should be trusted. That trust requires verifying, validating, monitoring and oversight which is accomplish through layers of Defense in Depth X.509 certificate security controls and assessments of X.509 certificates at every trust boundary. An evaluation of the maturity and health of X.509 certificates inside and outside of the network firewall requires a deep understanding of X.509 certificates. It is not easy, and the devil is in the details, but using tools like Nmap, and Powershell, and establishing policy, procedures, standards, and checklists provide proactive management to tame chaotic environment.

Include X.509 certificate information in general organizational security training so users understand the different warning messages and can be the first line of defense protection.

Include all X.509 services and trust anchors in risk and vulnerability dashboard summaries to executives with risk, priorities, and a status update on the TLS maturity matrix so there is appropriate prioritization of risk and security funding.

It is the responsibility of the entire digital community to ensure X.509 certificate trust remains trustworthy. Get involved and be an advocate for PKI ecosystem transparency. Support initiatives that benefit the whole system and not one specific PKI contributor's vested interest.

It's important to raise awareness within organizations and the security community on the importance of sharing information through community-driven blacklists, support for Certificate Transparency for code signing certificates, and required accountability for both public and private certificate authorities.

Author Name, email@address

5. References

Anoosh, S. (2014, 2 21). A Novel Method in IE11 For Dealing With Fraudulent Digital Certificates. Retrieved 24 7, 2016, from https://blogs.technet.microsoft.com/pki/2014/02/21/a-novel-method-in-ie11-for-dealing-with-fraudulent-digital-certificates/

ANSI. (n.d.). Registration Programs. Retrieved July 28, 2016, from https://www.ansi.org/other_services/registration_programs/reg_org.aspx?menuid=10

Armasu, L. (2016, March 23). StartCom Will Now Issue All SSL Certificates Under 'Certificate Transparency' System. Retrieved July 26, 2016, from http://www.tomshardware.com/news/startcom-adopts-certificate-transparency-log,31470.html

B. Laurie, A. L. (2013, June). Certificate Transparency. Retrieved 7 24, 2016, from https://tools.ietf.org/html/rfc6962

Benito, C. (2016, July 28). VirusTotal. (S. Dunn, Interviewer)

Buttyan, L. (2015, June 15). Repository of Signed Code. Hungary. Retrieved July 26, 2016, from https://www.virusbulletin.com/uploads/pdf/conference_slides/2015/Papp-etal-VB2015.pdf

CA / Browser Forum. (2016, July 8). *https://cabforum.org/baseline-requirements-documents/*. Retrieved July 27, 2016, from cabforum: https://cabforum.org/baseline-requirements-documents/

Constantin, L. (2015, November 24). *What you need to know about Dell's root certificate security debacle*. Retrieved July 2016, 2016, from http://www.itworld.com/: http://www.itworld.com/article/3008391/what-you-need-to-know-about-dells-root-certificate-security-debacle.html

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008, May). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. *rfc-5280*. Retrieved July 28, 2016, from http://www.rfc-base.org/txt/rfc-5280.txt

DiMaggio. (n.d.). Suckfly: Revealing The Secret Life of Your Code Signing Certificates. Retrieved 7 24, 2016, from http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates

Doherty, S., Gegeny, J., Spasojevic, B., & Baltazar, B. (2013). *Hidden Lynx - Professional Hackers for Hire.* Symantec.

Google. (2016, 7 28). *https://www.certificate-transparency.org/faq*. Retrieved from https://www.certificate-transparency.org/faq: https://www.certificate-transparency.org/faq

Kent, s. (1993, February). Privacy Enhancement for Internet Electronic Mail:. *rfc1422*. Retrieved July 28, 2016, from https://www.ietf.org/rfc/rfc1422

Author Name, email@address

Kotzias, P., Matic, S., Rivera, R., & Caballero, J. (n.d.). Certified PUP: Abuse in Authenticode Code Signing. *Conference on Computer and Communications Security .* Denver, Colorado, USA.: ACM. doi:10.1145/2810103.2813665.

Let's Encrypt. (2016, 7 28). *About*. Retrieved from https://letsencrypt.org.

Microsoft Edge Team. (2015, December 16). Evolving Microsofte SmartScreen to Protect You From Drive-by Attacks. Retrieved 7 24, 2016, from https://blogs.windows.com/msedgedev/2015/12/16/smartscreen-drive-by-improvements/

Ottow, C. (2016, 30 June). *startencrypt-considered-harmful-today*. Retrieved July 27, 2016, from https://www.computest.nl: https://www.computest.nl/blog/startencrypt-considered-harmful-today/

Platon Kotzias, S. M. (2015, october). Certified PUP: Abuse in Authenticode Code Signing. Washington DC. doi:http://dx.doi.org/10.1145/2810103.2813665.

Ristic, I. (2015, June 8). *Introducing TLS Maturity Model*. Retrieved from introducing-tls-maturity-model: https://blog.qualys.com/ssllabs/2015/06/08/introducing-tls-maturity-model

Author Name, email@address

6. Appendix

6.1. Decoding Certificate Details

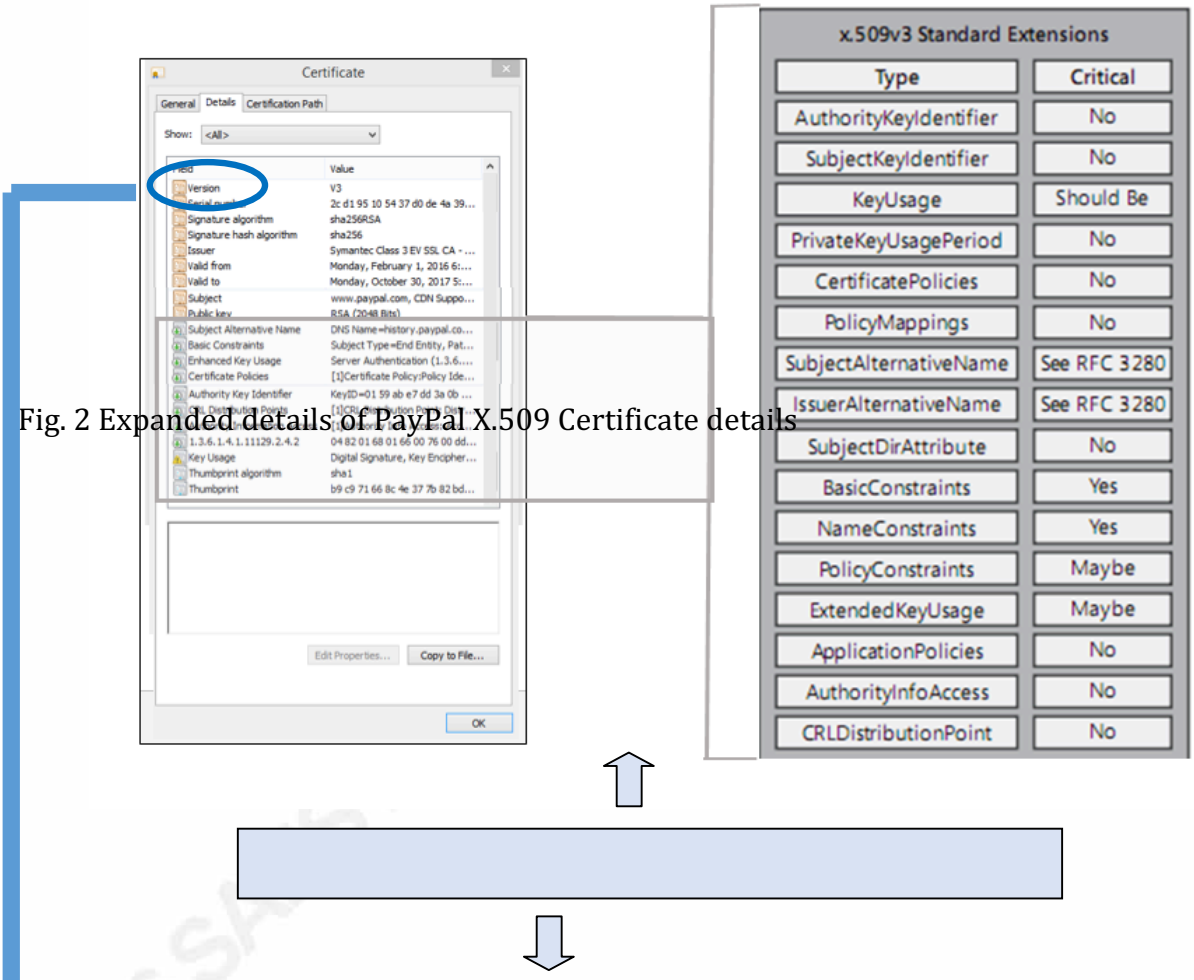


Fig. 2 Expanded details of PayPal X.509 Certificate details

This lists V.3 X.509 Certificate attribute fields with the associated value shown in Fig. 2, and a description of the attribute.

Field	Fig. x Value	Description
Version	V3	X.509 supported by the certificate
Serial Number	2C d1 95 10 54 37 d0 de 4a 39 20 05 6a f6 c2 7f	Unique certificate per CA positive serial numbers. There is no standard on how many characters long the

		serial number is as long as it is less than 20 octets
Signature algorithm	Sha256RSA	The algorithm used to sign the content using the subject's private key
Signature hash algorithm	Sha256	The single way function algorithm used to create the certificate hash
Issuer	Symantec Class 3 EV CA	The Distinguished Name of the authority that signed and issued the certificate.
Valid from	Monday, February 1, 2016	The trust starts day of the certificate
Valid to	Monday, October 30, 2017	The end trust day of the certificate (except for code signing certificates with timestamps)
Subject	www.paypal.com	Distinguished name used to uniquely identify the subject
Public Key	RSA2048	The provided public key. Viewing this field provides the complete 2048 public key. 30 82 01 0a 02 82 01 01 00 da 43 c8 b3 a6 33 5d 83 c0 63 14 47 fd 6b 22 bd bf 4e a7 43 11 55 eb 20 8b e4 61 13 ee de 7e c6 e2 45 34 a3 a2 5f 7e 49 5e 51 37 9a 4a 15 f3 a7 be 98 1b 01 44 14 18 fb ba 70 b2 39 3d 87 45 b8 b5 06 e8 d1 b1 91 84 06 46 4f 11 fb dd 26 6b b9 4d 69 ef 9a 14 dd 7d 8d f2 87 02 d0 10 5d 76 50 3d ec a3 ed 72 93 62 63 4a 89 d9 2f 53 5e 15 e4 6e 9f 70 3d b9 04 19 2b 95 47 c1 f7 f1 e7 93 1a 84 88 17 40 77 30 bc 83 56 22 a1 3e 3a 70 fb ff 81 0e 38 25 f0 10 0d 82 84 64 05 04 bd 30 83 c5 08 6d 24 b9 19 46 1e 3b 9b 02 4a 7e 6e cc df ee b2 c7 f1 8c 36 ee ed 62 b5 54 90 67 4f 9a 14 66 8d b9 72 f4 d4 9b 87 94 80 8c 30 ef 2e 40 b4 95 d1 aa a2 d5 ee 44 8e 7e 76 86 92 eb eb f5 77 a2 53 ff a4 b6 79 1e 6d 3f 9f 7e 5e d7 b1 7a 15 00 c5 01 69 b5 10 16 a5 85 f8 fd 07 84 9a c9 14 91 02 03 01 00 01
X.509 V3 Extensions		

Author Name, email@address

Subject Alternative Name	DNS Name=history.paypal.com DNS Name=t.paypal.com DNS Name=c.paypal.com DNS Name=c6.paypal.com DNS Name=developer.paypal.com DNS Name=p.paypal.com DNS Name=www.paypal.com	
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Lists what the public key can be used for. The usage can either object short names or the dotted-OID.
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.840.1.113733.1.7.23.6 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://d.symcb.com/cps [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=https://d.symcb.com/rpa	
Authority Key Identifier	KeyID=01 59 ab e7 dd 3a 0b 59 a6 64 63 d6 cf 20 07 57 d5 91 e7 6a	The X. 509 certificate issuer and serial number from the issuer certificate
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name:Full Name: URL=http://sr.symcb.com/sr.crl	Where to access X.509 certificate revocation information.
Authority Information Access	1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://sr.symcd.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://sr.symcb.com/sr.crt	How to access specific information from the issuing CA.
1.3.3.1.4.1.11129.2.4.2	04 82 01 68 01 66..	X.509 V3 Certificate Transparency extension
Key Usage	Digital Signature, Key Encipherment (a0)	List of the permitted key usage. Supported options: digitalSignature,

Author Name, email@address

Fig 2 : Viewing Certificate details

		nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly and decipherOnly
Thumbprint algorithm	Sha1	Thumbprint is another name for the hash function. This is the algorithm used on the certificate itself. Censy.io and the CT provide search by thumbprint.
Thumbprint	`b9 c9 71 66 8c 4e 37 7b 82 bd ee 9b 07 f9 c1 91 b6 ee 59 de`	The thumbprint (hash) of the certificate.

6.2. Steps to View Certificate Details

To view domain server X.509 certificate details:

Using the Chrome browser follow these steps. 1 Right clicking the mouse button on the green lock icon in the url which initiates the security overview option. 2 To see the certificate click the view certificate button. 3 Choosing the "Copy to File" on the second tab in the certificate details enables saving the file to a different location.

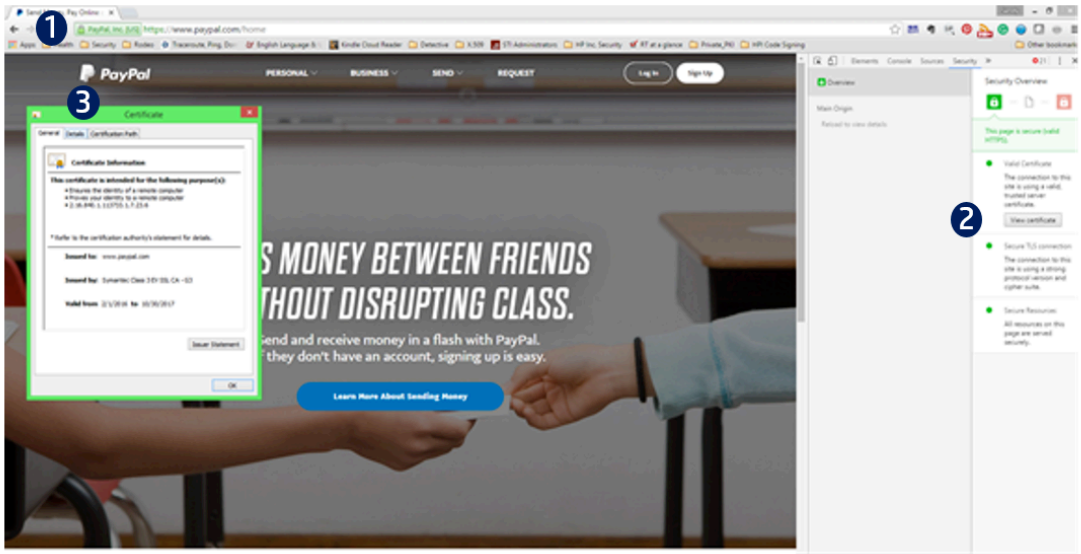
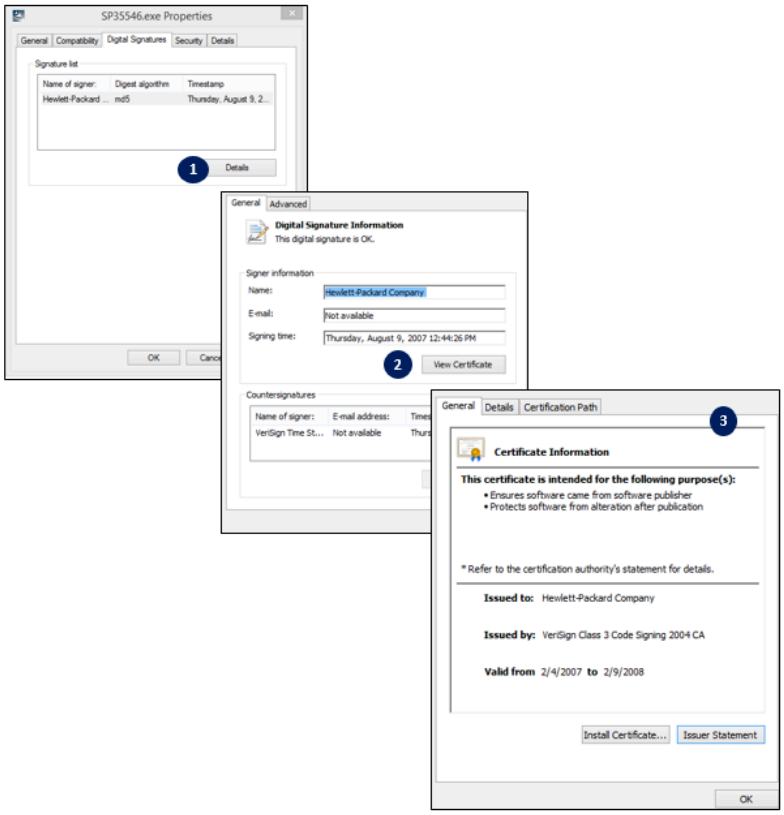


Fig. 3 . Viewing Certificate details

To view code signing certificate details

Locate the file that you are checking. Use a single right mouse button click to choose the file without opening it. Locate the properties option and open it with a single left mouse button click. If the file has been digitally signed, there will be four available tabs. If it has not been digitally signed, there will be only three tabs for the file. 1 Open the Digital Signature tab and click on the name of the signer. 2 Click Details. 3 Click View Certificate.



Author Name, email@address

6.3. Types of certificates

There are different types of domain web server X.509 certificates and code signing X.509 certificates.

6.3.1. The Three Types of Domain Validated Code Signing Certificates

Domain Validated X.509 Certificates: are checked against the domain registry. Often just receiving an email at the requesting domain is the only requirement for validating the identity of the certificate requestor. DV certificates are the least expensive and the only type of certificate that can be updated through automation. Many organizations such as Let'sEncrypt and Amazon provide DV certificates for free. (Let's Encrypt, 2016)

Organization Validated X.509 Certificates: require more validation documentation from the organization requesting the X.509 certificate. The provided information is validated by a CA employee against public records like Dun&Bradstreet, Better Business Bureau, or through other sources like a letter from a Certified Public Accountant.[ref]

Extended Validation X.509 Certificates: include many more checks and validation of the person or organization against public records and require the person making the request to provide proof of identity. Extended Validation certificates are the most expensive type of X.509 certificates. [ref]

Fig. 4 provides examples of three different websites using one of the three types of X.509 certificates viewed with the Chrome browser.

Fig. 5 . DV Certificates in Chrome browser

Fig 4 . Viewing different types of Certificates in Chrome browser

Fig. 5. The Linkedin certificate in the first URL is a Domain Validated (DV) certificate which is identified by the Digicert OID 2.16.840.1.114412.1.1

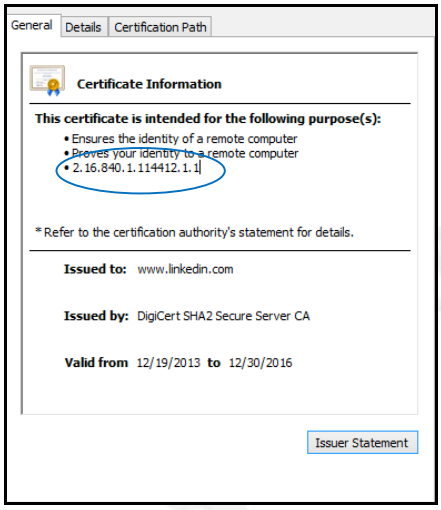


Fig. 6. The sysadmin certificate in the second URL is an Organization Validated (OV) certificate which is identified by the Digicert OID 2.23.140.1.2.2

Author Name, email@address

Fig. 6. OV Certificate in Chrome browser

Fig. 7. OV Certificate in Chrome browser

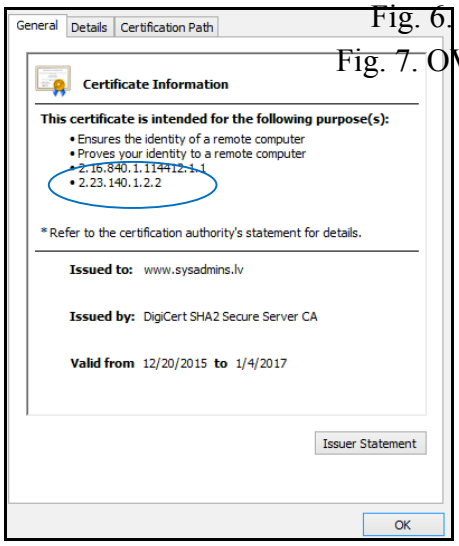
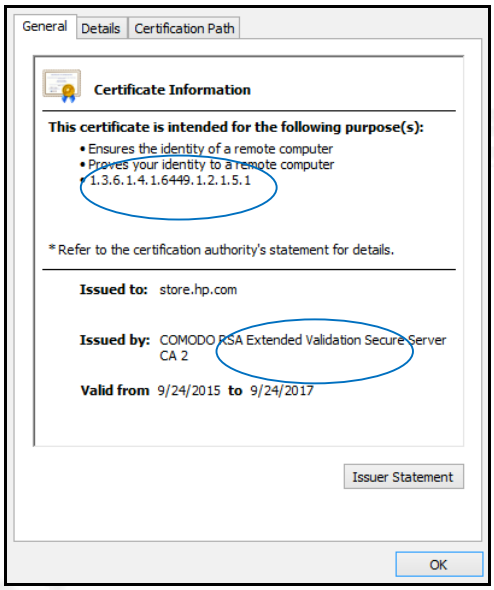


Fig. 7. The store.hp.com X.509 certificate in the third URL is an Extended Validation (EV) Certificate identified by the Comodo OID 1.3.6.1.4.1.6449.1.2.1.5.1 and the "Issued by" statement.



The different levels of trust for each type of certificate is significant and should be carefully considered when providing financial or personal information.

Author Name, email@address

6.3.2. There are Two Types of Code Signing X.509 Certificates

Standard Code Signing Certificate: Code signing certificates are purchased by platform. All available code signing certificate platforms such as JAVA, Android, Windows, and Adobe use Standard Code Signing Certificates.

EV Code Signing Certificates: The only application that differentiates between standard and Extended Validation of code signing certificates is the Microsoft platforms. The EV Code Signing Certificates requirements are from the Extended Validation Code Signing Certificate Guidelines developed by the CA/Browser forum.

6.4. X.509 V3 Certificate Attributes

An X.509 certificate is a digitally signed group of bits signed by a CA. The CA is responsible for validating the information that is included in the X.509 public key details The X.509 certificate defines the certificate owner as the subject and binds the subject to a unique asymmetric key pair. In most cases, the owner is a person, organization, or a device, but a service can also be an X.509 certificate owner. Version three is the current version of the X.509 standard and the one most often seen in the field.

Asymmetric keys are key pairs that have a public key and a private key. The public key is publically visible and because of some very complex math proves that the only key that could have mathematically encrypted or hashed a file is the private key of the asymmetric key pair. The private key must be protected by the X.509 certificate requestor. Whoever has that private key "is" the key owner. Each unique certificate is issued a serial number. The serial number must be unique to the issuing CA although a different CA could issue a certificate with the same serial number.

X.509 Certificates have different lifecycles which vary from 90 days, the recommendation for the Let's Encrypt Certificates to twenty-five years or longer.

X.509 Certificates support only one common name in the subject field and are associated with only one host name. In theory and as designed this ensures that only one entity can validate that the issued certificate is assigned to a single entity. In practice, managing a large number of domains and subdomains with individual X.509 certificates is almost impossible because of the complexity and overhead X.509 certificate management requires. SAN names, wild cards, and the use of SNI.

Author Name, email@address

Subject Alternative Names (SAN) and wildcard domains provide two different options for supporting multiple domain names in a certificate. Subject Alternative Names lists all the alternative hostnames in the SAN extension field. The wildcard option (*) indicates to associate the certificate with the provided base domain and any subdomains with that base name.

The Server Name Indication (SNI) is an important TLS extension in an environment where a single IP address hosts multiple hostnames. The client indicates to the server in the connection process which host it would like to connect to so the appropriate X.509 certificate can be provided. Reference (Kent, 1993) (Cooper, et al., 2008)

6.4.1. X.509 V3 Certificate Extensions

The update to version three of the X.509 standard added attribute extensions. Extensions are added to standards to update supported features which provided more features and to add flexibility to the standard.

The added extensions provide additional information about the X.509 certificates through uniquely identified object identifier (OID)'s which use a formal ASN.1 syntax notation. Any enterprise or organization can name and register an OID. In the United States, OID's are issued by the American National Standards Institute. (ANSI)

Some X.509 certificate extensions are listed as "critical". If an extension is a critical extension the certificate is rejected if the extension is not recognized. If the extension is considered "not critical" the extensions is processed if the extension is recognized but ignored if it is not. (Cooper, et al., 2008)

6.5. Policy, Practice Statement, & Profiles

The X.509 Certificate Policy (CP) is the "warranty" or assurance of the issued X.509 certificate. [5]

The Certificate Practices Statement (CPS) supports the CP by providing the technical, operational, and management practices to meet the defined requirements in the

[5] X.509 Certificate Policy should be not be confused with organizational polices that provide specific guidance on actions within a business or agency. X.509 Certificate Policies are more similar to insurance or warranty policies.

certificate policy. The CP is what the CA does; the CPS is how they do it. RFC3647 provides the basic framework for both the CP and CPS.

Certificate profiles are used as templates to issue certificates. They are issued by different standard bodies which can be by country, industry organization, or government agency. Profiles provide specific definitions and limits for fields that the X.509 standard loosely defines. This works as long as only one standard needs to be supported. Renowned PKI expert Peter Guttmann describes the different profiles as similar to "various monotheistic religions where you either do what we say or burn in hell". In kinder terms conforming to one profile generally means it will not work with any others

6.6. Tools List

Tool	Description	Where to find it
All Certificates		
OpenSSL	View Certificate information on host: openssl s_client -connect HOSTNAME:443 -prexit -showcerts -state -status -tlsextdebug -verify 10	https://www.openssl.org/
	21 OpenSSL Examples to Help You In the Real-World	https://geekflare.com/openssl-commands-certificates/
NMAP	Ssl-cert.nse Retrieves a server's X.509 certificate. With no extra verbosity, it prints the validity period and CommonName, organizationName, stateOrProvinceNam e, and countryName of the subject -v adds the issuer name and fingerprints -vv adds the PEM-encoded contents of the entire certificate Example usage: nmap –sV –sC <target>	https://nmap.org/ http://nmap.org/svn/scripts/ssl-cert.nse
certmgr	Windows manager certificate manager	Default Windows tool. Access through MMC
MakeCert	Generates X.509 certificates for testing purposes. It creates a public and private key pair for digital signatures and stores it in a certificate file. This tool also associates the key pair with a specified publisher's name and creates an X.509 certificate that binds a user-specified name to the public part of the key pair.	https://msdn.microsoft.com/en-us/library/bfsktky3(v=vs.100).aspx
Certutil	Command line tool from Microsoft	https://teckadmin.wordpress.com/2015/01/16/certutil-windows-command/
KeyStore Explorer	KeyStore Explorer is a free GUI replacement for the Java command-line utility keytool and jarsigner	http://www.keystore-explorer.org/
TLS file type converter	Converts PEM files to DER converts PKCS#7 files to PKCS#12	https://www.sslshopper.com/ssl-converter.html
CSR	Validates CSR request is formatted correctly	www.cryptoreport.websecurity

		.symantec.com/checker/views/csrCheck.jsp
Creating an X.509- Based PKI for Testing	Instructions on building a PKI test environment	https://developer.ibm.com/integration/blog/2016/03/29/creating-an-x-509-based-public-key-infrastructure-for-testing-integration-applications/
Web Server Certificates		
SSL Server Test	Analysis of TLS Web server configuration	https://www.ssllabs.com/ssltest/
High-Tech Bridge	Analysis of TLS Web server configuration. Includes compliance information for NIST and PCI DSS	https://www.htbridge.com/ssl/
Scan Security headers	Checks HTTP connection for Content-Security-Policy, X-Content-Type-Options, X-Frame-Options, and X-XSS-Protection. Over an HTTPS connection, there is check for two additional headers which are Strict-Transport-Security and Public-Key-Pins.	https://securityheaders.io/
OWASP DeepViolet TLS/SSL Scanner	DeepViolet is a TLS/SSL scanning library/tool written in Java. Check server certificate trust chains, revocation status, check certificates for pending expiration, weak signing algorithms and more.	OWASP DeepViolet TLS/SSL Scanner Code Project
testssl.sh	A CLT that checks a server's service on any port for TLS ciphers, protocols, cryptographic flaws and other TLS issues.	https://testssl.sh/
Symantec CryptoReport	Check your SSL/TLS certificate installation. Provides information on the type of certificate.	https://cryptoreport.websecurity.symantec.com/checker/
Lemur	Lemur is a certificate management framework that acts as a broker between certificate authorities and internal deployment and management tools.	http://techblog.netflix.com/2015/09/introducing-lemur.html
Certbot	Automatically enable HTTPS Domain Validated certificates from Let's Encrypt	https://certbot.eff.org/
Sslyze	A python script which can do mass scanning and XML output. It is one of the most complete and versatile tools for SSL/TLS testing.	https://github.com/iSECPartners/sslyze
Censys.io	Censys is a public search engine that enables researchers to ask questions about the hosts and networks	www.censys.io https://censys.io/overview#
certlint	A tool that can help verify if certificates are following X.509, PKIX, and CA/B Forum specifications and guidelines	http://cert-checker.allizom.org/
Authenticode Lint	Validates if binaries correctly	https://vcsjones.com/2016/04/15/authenticode-stuffing-tricks/
SSL Client Test	TLS capability of the client browser	www.ssllabs.com/ssltest/viewMyClient.html
Comodo's certificate search tool	Easy to use search tool for CT logs (even though Google has their own search tool, this seems to be the one most people use)	https://crt.sh/
Google's certificate search tool	Search tool for CT logs	https://www.google.com/transparencyreport/https/ct/
Code Signing Certificates		
SignServer PKI by PrimeKey	Server Side Key Management Sign document: PDF, XML, XAdES Sign Code: MS Authenticode, Java including Android APK	https://www.signserver.org/

Author Name, email@address

	Timestamping	
Sigcheck.exe	Sigcheck is a command-line tool that has file version number, timestamp information, and digital signature details, including certificate chains. It includes an option to check a file's status on VirusTotal	https://technet.microsoft.com/en-us/sysinternals/bb897441.aspx
AnalyzePESig.exe	When a signature is not valid, AnalyzePESig will tell you why and display information about the invalid signature and related certificates.	https://blog.didierstevens.com/programs/authenticode-tools/
PEstamp	CTL that shows the UTC compilation timestamp of any executable	http://trax.x10.mx/apps.html
Nugget	Curl like tool for Windows	http://trax.x10.mx/apps.html
View all Windows Trusted Certificates	Windows currently trusts 342 root certificates – see them all buy following these steps: (1) Launch a cmd prompt and browse to where you want to store your list (2) Type: certutil –generateSSTfromWU roots.sst (3) Import and view using certmgr	http://security.stackexchange.com/questions/108951/how-much-of-a-problem-is-it-that-windows-hides-some-of-the-trusted-root-ca-cer
RCC	Scans and audits trusted root CAs in Microsoft Windows and Mozilla Firefox. Highlights potentially rogue certificates based on reference baselines and timestamp metadata.	http://trax.x10.mx/apps.html
VirusTotal	A free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware. The hash of a file can be queried in the VirusTotal database. File hashes from malware can be used to identify rouge certificates.	https://www.virustotal.com/
Wine / with OpenSSL	Using Wine with Windows based tools overcomes the challenge of conflicting Windows / Linux based tools.	https://appdb.winehq.org/index.php
Osslsigncode	Platform-independent tool for Authenticode signing of PE(EXE/SYS/DLL/etc.), CAB and MSI files.	https://sourceforge.net/projects/osslsigncode/

6.7. Common Certificate Filename Extensions

Extension	Description	Where it's seen
.csr	A Certificate Signing Request.	The CSR contains all the key details of the certificate being requested such as subject, organization, state, and other required information. It also includes the public key of the certificate to get signed. This is signed by the CA, and a certificate is returned to the requestor. The returned certificate is the signed public certificate.
.pem	(Privacy-enhanced Electronic Mail) Base64 encoded DER certificate, enclosed between "-----BEGIN CERTIFICATE-----"	A container format that may include just the public certificate, or may include an entire certificate chain including the

	and "-----END CERTIFICATE-----"	public key, private key, and root certificates. The name is from Privacy Enhanced Mail (PEM), a base64 translation of the X.509 ASN.1 keys.
.key	A PEM formatted file	File format used for the private key
.cer, .crt, .der	Usually in binary DER form, but Base64-encoded certificates are common too.	PEM file with a different extension
.p7b, .p7c	PKCS#7 SignedData structure without data, just certificate(s) or CRL(s) .p12 – PKCS#12, may contain certificate(s) (public) and private keys (password protected)	PKCS#7 - is a standard for signing or encrypting (officially called "enveloping") data. Since the certificate is needed to verify signed data, it is possible to include them in the Signed Data structure. Format used by Windows for certificate exchange. It includes a defined way to include certification paths. (unlike PEM)
.p12	PKCS#12 may contain certificate(s) (public) and private keys (password protected)	PKCS#12 developed from the personal information exchange (PFX) standard. Used to exchange public and private objects in a single file
.pfx	PFX, predecessor of PKCS#12 (usually contains data in PKCS#12 format, e.g., with PFX files generated in IIS)	A .pfx file is a PKCS#12 archive file. It includes a certificate and may also include other CA certificates, and the corresponding private key. (compare to a .cert, .cert or .crt file which contains a single certificate which is not password protected)

6.8. CA Type Reference

Certificate Authority or Root CA	An entity that issues digital certificates. The issuer and subject fields are the same. The keyUsage field has KeyCertSign set, and the basicConstraints field has the cA attribute set TRUE
Registration Authority or RA	RAs can sign certificates (as subordinate CAs) after the appropriate end entity validation.
Intermediate Certificates	Form a chain and there is no defined limit on the number of Intermediate CA between an end entity certificate and the Root CA certificate.
Time Stamping Authority	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) addresses the challenge of expiring X.509 code signing certificates in software that has been widely distributed. During the code singing process, the signed code is sent to a Time Stamping Authority (TSA) that adds its own counter signature. Code that is timestamped contains

	two certificate chains, the signing chain, and the timestamping chain. https://www.ietf.org/rfc/rfc3161.txt

Author Name, email@address