



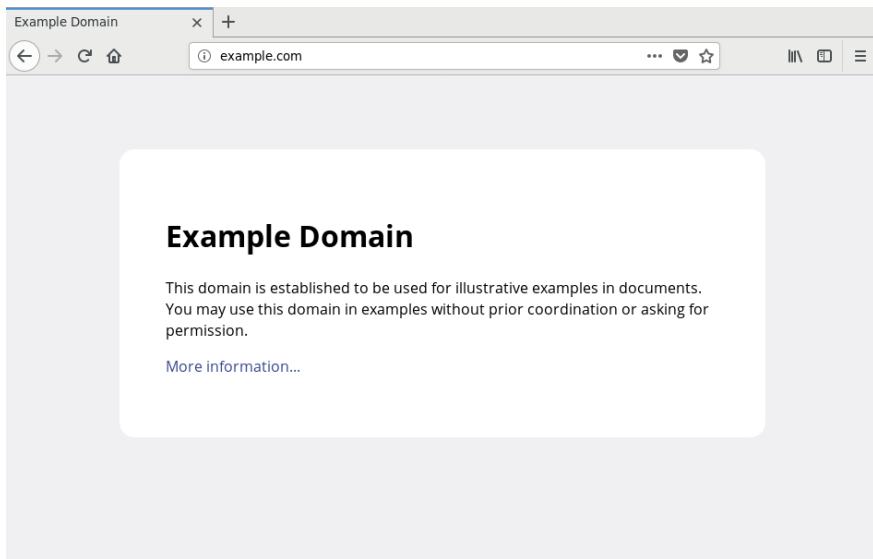
An Introduction to Certificate Transparency

Rasmus Dahlberg and Tobias Pulls

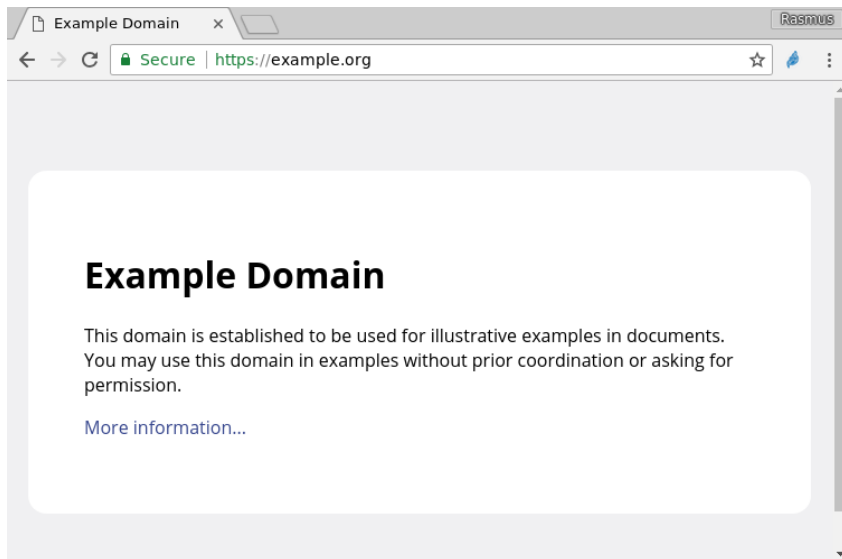
1. Background
2. Principles
3. Status quo
4. Your role



How is trust established on the web?



How is trust established on the web?

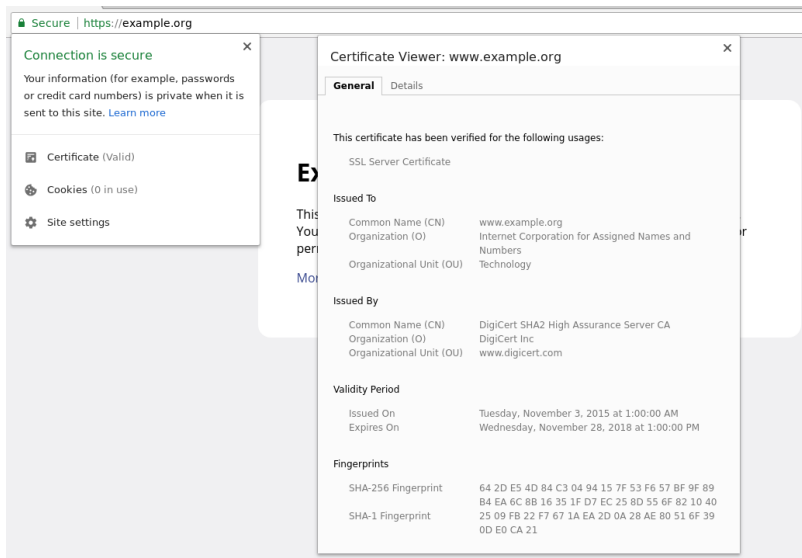


What is the meaning of the padlock?

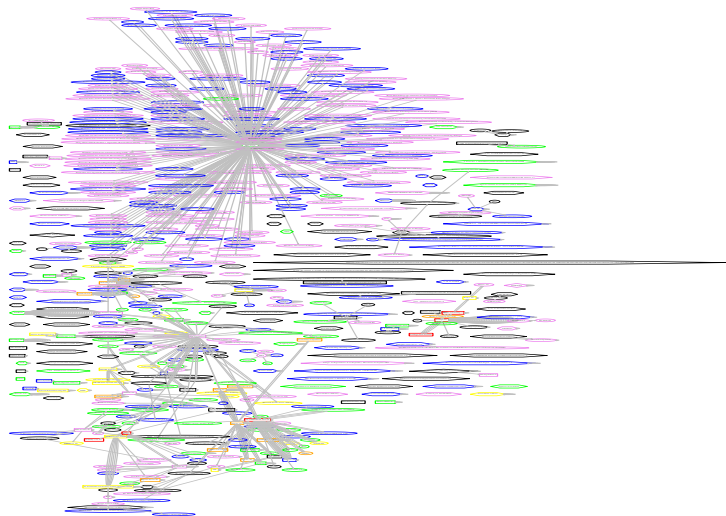
- ✓ Communication is encrypted
- ✓ Communication is not tampered with
- ✓ Server identity is verified



Server verification relies on certificate issuance



Tracking certificate issuance is a mess



https://www.eff.org/files/colour_map_of_cas.pdf

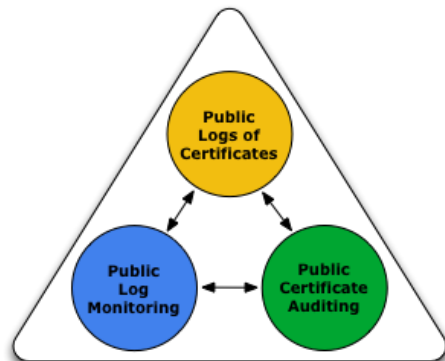
Certificate issuance gone wrong...

Year	Issuer	Mis-issued certificates affected e.g.
2010	Versign	Unkown
2011	Comodo	Google, Mozilla, Yahoo
2011	DigiNotar	Google ¹ , Skype, Tor...
2012	Trustwave	Enterprise employees
2012	TürkTrust	Google
2013	ANSSI	Google
2013	Thawte	Google
2016	Let's Encrypt	Facebook
...

¹These certificates were used to attack $\approx 100,000$ gmail users in Iran

Certificate Transparency (CT) to the rescue

- Publicly log all certificates
- Clients require proof of logging
- Anyone can inspect the logs
- Goal is to **detect** mis-issuance



<https://www.certificate-transparency.org/what-is-ct>

Adoption status of CT among common platforms



incrementally



incrementally soon



unclear

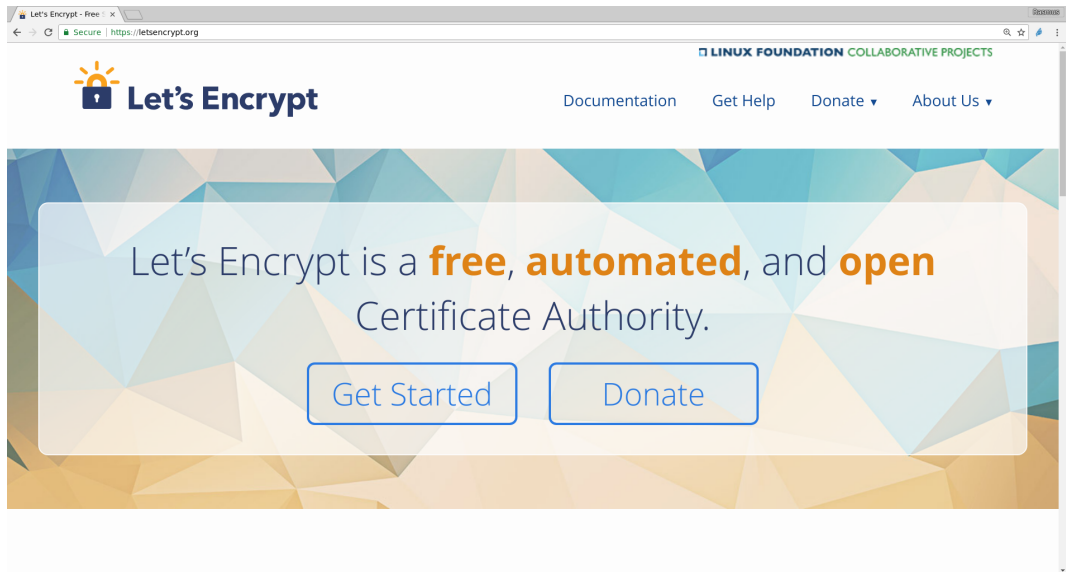
- Clients require at least two promises of log inclusion
- Log is trusted until auditing hits deployment

Who are the log operators?

- Google Chrome includes 27 different CT logs
- Three logs found cheating while auditing (mistakes)
 - ▶ Same key for test and production log (Izenpe)
 - ▶ Time rollback after power outage (Venafi)
 - ▶ Invalid promises of log inclusion (Cloudflare)

Log operator	Number of logs
DigiCert	10
Google	9
Cloudflare	4
Comodo	2
CNNIC	1
Venafi	1

Ensure that your web solutions get the padlock




Inspect certificates interactively

Browser window showing the crt.sh Identity Search interface. The search criteria is set to Identity = 'soleilit.se'.

Certificates	crt.sh ID	Logged At ↑	Not Before	Not After	Issuer Name
	323197688	2018-02-05	2018-02-05	2021-03-12	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	123190358	2017-04-18	2017-01-07	2018-03-13	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA

© COMODO CA Limited 2015-2018. All rights reserved.



Inspect certificates interactively (cont.)

The screenshot shows the Facebook Certificate Transparency Monitoring tool. The browser address bar displays <https://developers.facebook.com/tools/ct/>. The page header includes the Facebook logo and navigation links for Docs, Tools, and Support. The main heading is "Certificate Transparency Monitoring". Below this, a paragraph explains that the tool helps log, audit, and monitor publicly-trusted TLS certificates. The interface has two tabs: "Search" (selected) and "Subscriptions". In the "Search" tab, there is a search input field containing "soleit.se" and a "Search" button. Below the search bar is a table of search results. The table has five columns: Domains, Subject, Issuer, Validity, and Certificate. It lists seven certificates issued to domains associated with soleit.se. Each row includes a "Show Details" button. At the bottom of the table, there is a "Show 10" dropdown, navigation arrows, and a page indicator "1-7 of 7".

Certificate Transparency Monitoring

Certificate Transparency is an open framework which helps log, audit and monitor publicly-trusted TLS certificates on the Internet. This tool lets you search for certificates issued for a given domain and subscribe to notifications from Facebook regarding new certificates and potential phishing attacks.

Search Subscriptions

soleit.se Search

Domains	Subject	Issuer	Validity	Certificate
intrahybrid.intern.soleit.se	CN=intrahybrid.intern.soleit.se	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Feb 09, 2018 - May 10, 2018	Show Details
.soleit.se soleit.se	C=SE, L=Karlstad, O=Soleit IT Sweden AB, CN=.soleit.se	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA	Feb 04, 2018 - Mar 12, 2021	Show Details (CT Precertificate)
api.jamfor.soleit.se	CN=api.jamfor.soleit.se	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Oct 03, 2017 - Jan 01, 2018	Show Details
api.jamfor.soleit.se	CN=api.jamfor.soleit.se	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Jul 25, 2017 - Oct 23, 2017	Show Details
api.jamfor.soleit.se	CN=api.jamfor.soleit.se	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Apr 05, 2017 - Jul 04, 2017	Show Details
api.jamfor.soleit.se	CN=api.jamfor.soleit.se	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Apr 05, 2017 - Jul 04, 2017	Show Details
.soleit.se soleit.se	C=SE, ST=Karlstad, L=Karlstad, O=Soleit IT Sweden AB, CN=.soleit.se	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA	Jan 06, 2017 - Mar 13, 2018	Show Details

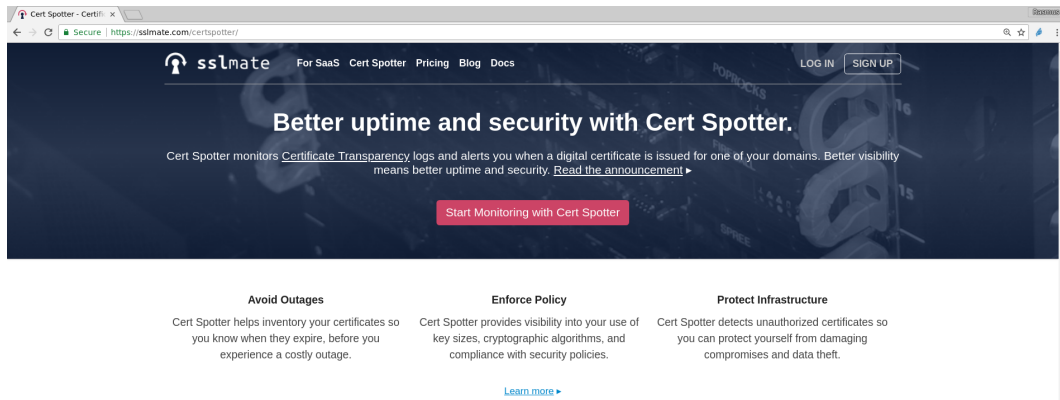
Show 10 1-7 of 7

Sign up for certificate notifications

The screenshot shows the 'Certificate Transparency Monitoring' page on the Facebook for developers website. The page has a dark blue header with the 'facebook for developers' logo and navigation links for 'Docs', 'Tools', and 'Support'. A search bar is also present. Below the header, the main content area is titled 'Certificate Transparency Monitoring' and includes a description of the tool. A tabbed interface shows 'Subscriptions' as the active tab. Below this, there is a table with five columns: 'Subscribed Domain', 'Certificate Alerts', 'Phishing Alerts', 'Notification Email', and 'Action'. The first row of the table contains a text input field for the domain, dropdown menus for alerts and phishing notifications, a text input for the email address, and a green 'Subscribe' button.

Subscribed Domain [?]	Certificate Alerts [?]	Phishing Alerts [?]	Notification Email [?]	Action [?]
<input type="text" value="Domain"/>	Email, Push, On-Site ▼	Email, Push, On-Site ▼	rasmus.gd.d... ⬇	Subscribe

Sign up for certificate notifications (cont.)



The screenshot shows the Cert Spotter website homepage. The browser's address bar displays 'https://sslmate.com/certspotter/'. The website has a dark blue header with the 'sslmate' logo on the left and navigation links 'For SaaS', 'Cert Spotter', 'Pricing', 'Blog', and 'Docs' in the center. On the right side of the header are 'LOG IN' and 'SIGN UP' buttons. The main content area features a large heading 'Better uptime and security with Cert Spotter.' followed by a paragraph: 'Cert Spotter monitors [Certificate Transparency](#) logs and alerts you when a digital certificate is issued for one of your domains. Better visibility means better uptime and security. [Read the announcement](#) ►'. Below this is a prominent pink button labeled 'Start Monitoring with Cert Spotter'. The lower section of the page is divided into three columns, each with a title and a description: 'Avoid Outages' (Cert Spotter helps inventory your certificates so you know when they expire, before you experience a costly outage), 'Enforce Policy' (Cert Spotter provides visibility into your use of key sizes, cryptographic algorithms, and compliance with security policies), and 'Protect Infrastructure' (Cert Spotter detects unauthorized certificates so you can protect yourself from damaging compromises and data theft). A 'Learn more ►' link is centered at the bottom of this section.

Cert Spotter - Certifi x

Secure | <https://sslmate.com/certspotter/>

sslmate For SaaS Cert Spotter Pricing Blog Docs

LOG IN SIGN UP

Better uptime and security with Cert Spotter.

Cert Spotter monitors [Certificate Transparency](#) logs and alerts you when a digital certificate is issued for one of your domains. Better visibility means better uptime and security. [Read the announcement](#) ►

Start Monitoring with Cert Spotter

Avoid Outages

Cert Spotter helps inventory your certificates so you know when they expire, before you experience a costly outage.

Enforce Policy

Cert Spotter provides visibility into your use of key sizes, cryptographic algorithms, and compliance with security policies.

Protect Infrastructure

Cert Spotter detects unauthorized certificates so you can protect yourself from damaging compromises and data theft.

[Learn more](#) ►

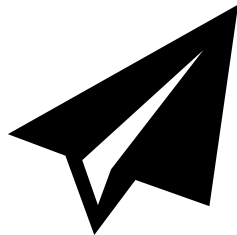
Get your hands dirty by running your own CT monitor

- Continuously fetch certificates from all logs
 - ▶ Rest API²
 - ▶ Certstream³
- Verify cryptographic properties
 - ▶ Is yesterday's log included in today's log?
 - ▶ Are promises of inclusion honored?

²<https://tools.ietf.org/html/rfc6962>

³<https://github.com/CaliDog/certstream-server>

- Certificate issuance has undergone a paradigm shift
 - ▶ Automated and free certificates: Let's Encrypt
 - ▶ Transparency: CT, mandatory logging of certificates
- CT does nothing for you without involvement
 - ▶ Setup secure connections on your web services
 - ▶ Monitor domain names for mis-issued certificates



Any questions?

