Automatic Certificate Management Environment (ACME)

Derek Simmel dsimmel@psc.edu, TAGPMA Chair

IGTF All-Hands Meeting, Academia Sinica, Taipei, Taiwan

April 1, 2019

© 2019 Pittsburgh Supercomputing Center

Automatic Certificate Management Environment

Topics:

- Interest in ACME
- Certificate Validation Terminology
- IETF RFC 8555 - ACME
- IGTF Profile (Elm) for ACME CAs?
  - Should we develop a new profile for automated CAs?
  - If so, what problems must we solve?
    - What additional requirements beyond DV must be implemented?

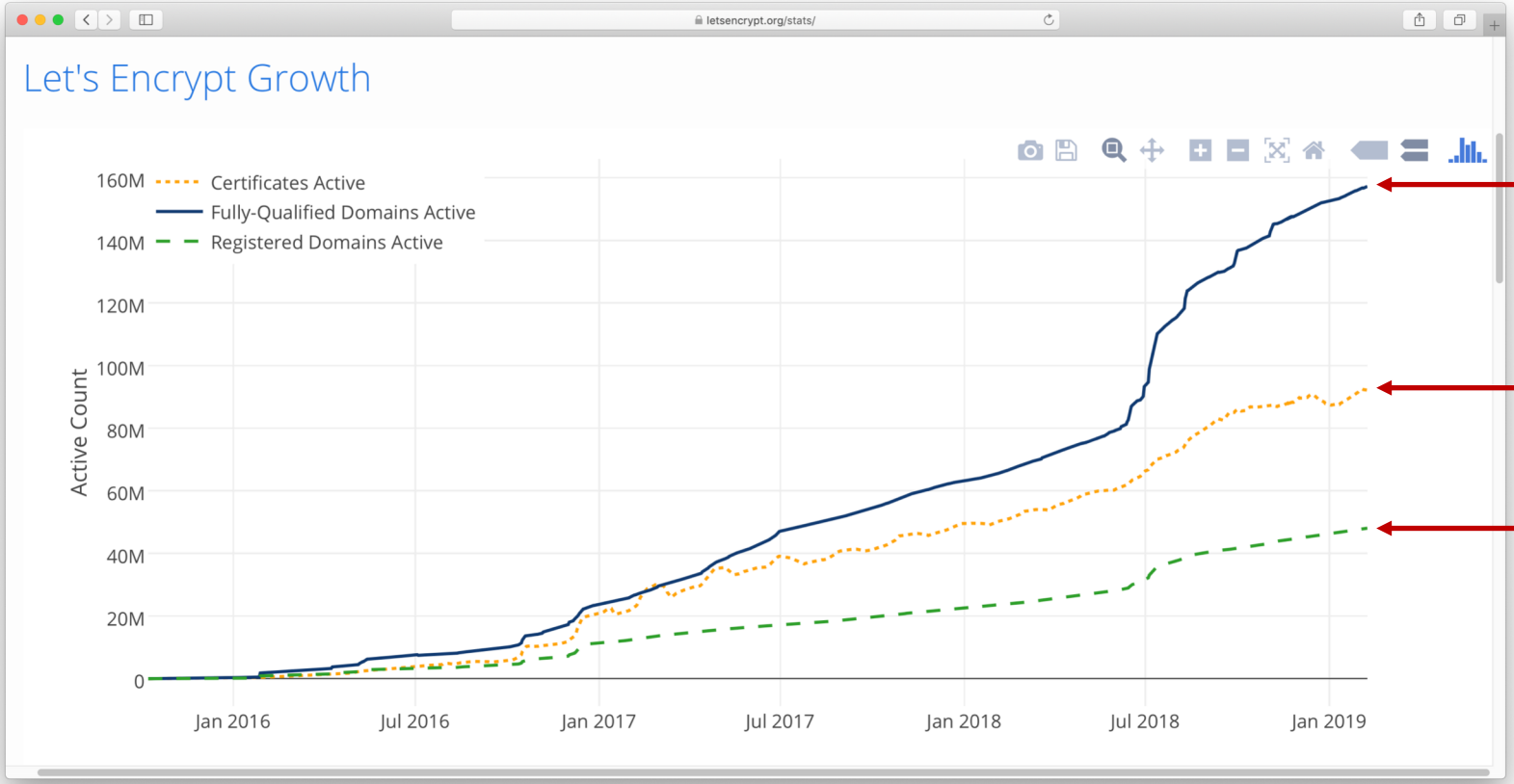
IGTF AP|EU|TAG
TAGPMA
PITTSBURGH SUPERCOMPUTING CENTER

Interest in ACME

- Popularity / Marketing of LetsEncrypt
  - Non-profit CA operated by “Internet Security Research Group” (ISRG)
  - Founded in 2013; now supported by >65 corporate sponsors
- Sudden decommissioning of OSG CA relied upon for host/service certificate issuance to U.S. DoE sites
  - Urgency mitigated by allowing DoE sites to request and obtain certificates from the InCommon CAs
- Rapid increase in container-based web services and automated provisioning technologies

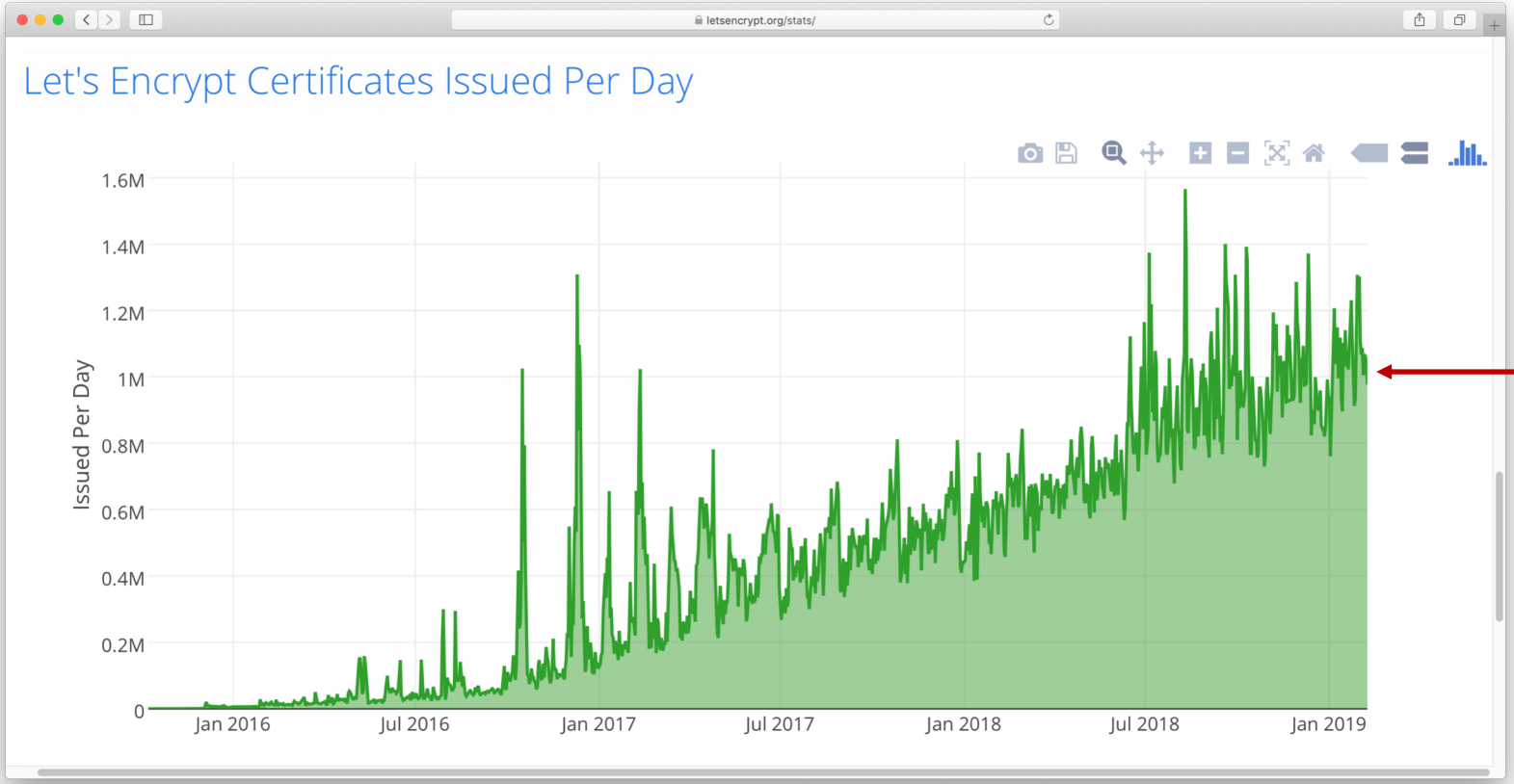
IGTF AP|EU|TAG
TAGPMA
PITTSBURGH SUPERCOMPUTING CENTER

LetsEncrypt Statistics



https://letsencrypt.org/stats/, accessed 2019-04-01

LetsEncrypt Statistics



https://letsencrypt.org/stats/, accessed 2019-04-01

Certificate Validation Terminology

Certificate Validation Types:

- **DV** (Domain Validation)
- **OV** (Organization Validation)
- **EV** (Extended Validation)

Domain Validation

- CA verifies only that the
  - Requester *has effective control of the domain*, **OR**
  - Requester *has the right to use their domain*

- Traditionally done via e-mail to WHOIS contact for domain

IGTF AP|EU|TAG
TAGPMA
PITTSBURGH SUPERCOMPUTING CENTER

Organization Validation

- CA verifies that the requester's *organization identity* and *physical address* in at least one of:
  - Listing in an official government agency database
  - Listing in a "reliable, regularly updated" 3rd party database, e.g.
    - Dun & Bradstreet, Hoovers, Better Business Bureau
  - Letter from a CPA, Legal Notary, or official Legal Opinion

- Some CAs will issue a DV certificate to requesters for use until OV validation process is completed
  - How long are these "temporary" DV certificates valid for?
  - How soon are these "temporary" DV certificates revoked when the OV validation fails?

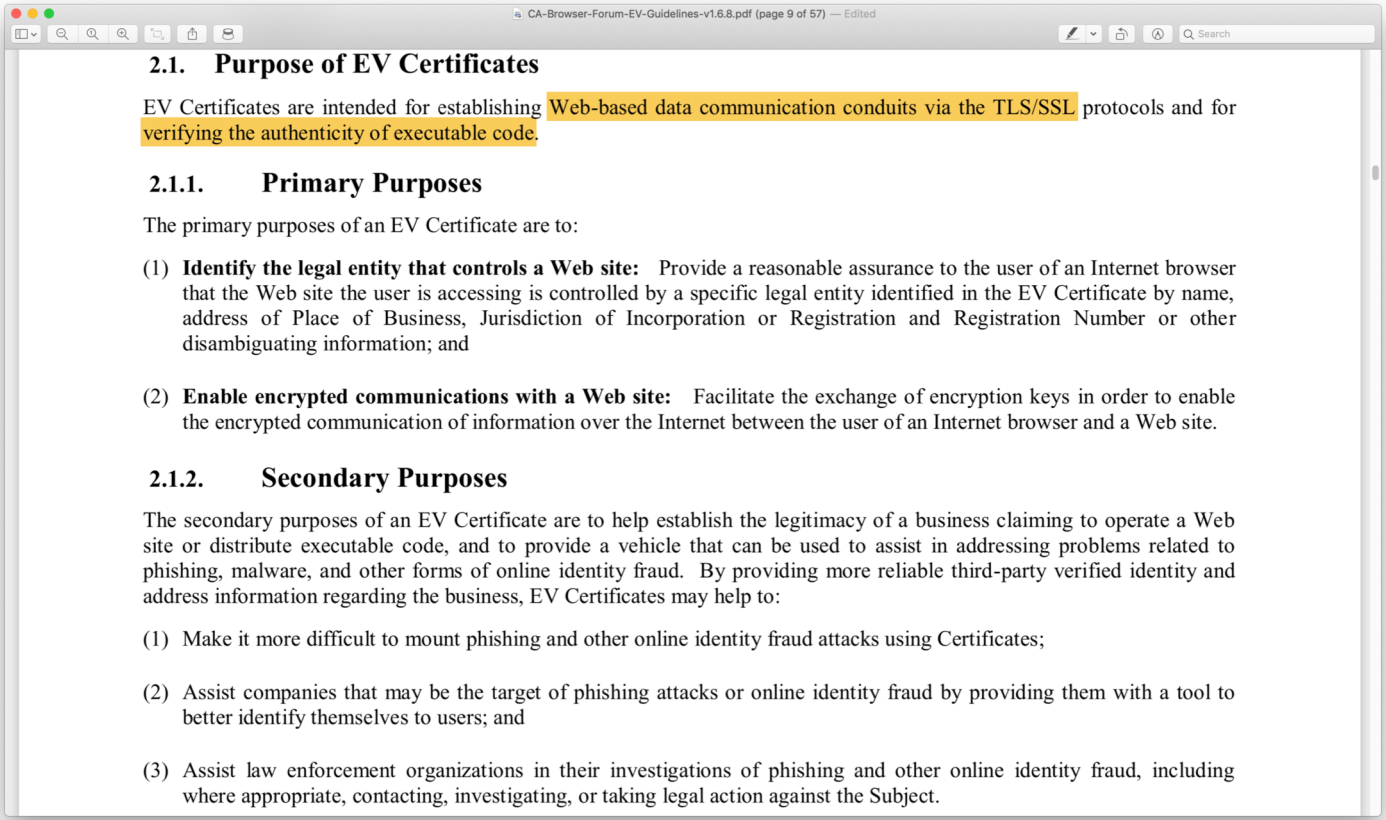
IGTF AP|EU|TAG TAGPMA PITTSBURGH SUPERCOMPUTING CENTER

OV for Individual Requesters

- CAs validate individuals (persons) requesting an OV certificate for themselves by verifying proof of the requester's identity with:
  - Government issued identity documents
    - Valid Passport, State ID, driver's license, military ID
  - "Acceptable financial institution document" in the requester's name
  - Secondary documents in the requester's name
    - e.g., utility bills or tax bills at a fixed address
  - Notarized "face-to-face" document attesting to examination of above documents by Notary in the physical presence of the requester

IGTF AP|EU|TAG TAGPMA PITTSBURGH SUPERCOMPUTING CENTER

Extended Validation (as defined by CABForum)



CA-Browser-Forum-EV-Guidelines-v1.6.8.pdf (page 9 of 57) — Edited

2.1. Purpose of EV Certificates

EV Certificates are intended for establishing Web-based data communication conduits via the TLS/SSL protocols and for verifying the authenticity of executable code.

2.1.1. Primary Purposes

The primary purposes of an EV Certificate are to:

(1) **Identify the legal entity that controls a Web site:** Provide a reasonable assurance to the user of an Internet browser that the Web site the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information; and

(2) **Enable encrypted communications with a Web site:** Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a Web site.

2.1.2. Secondary Purposes

The secondary purposes of an EV Certificate are to help establish the legitimacy of a business claiming to operate a Web site or distribute executable code, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the business, EV Certificates may help to:

(1) Make it more difficult to mount phishing and other online identity fraud attacks using Certificates;

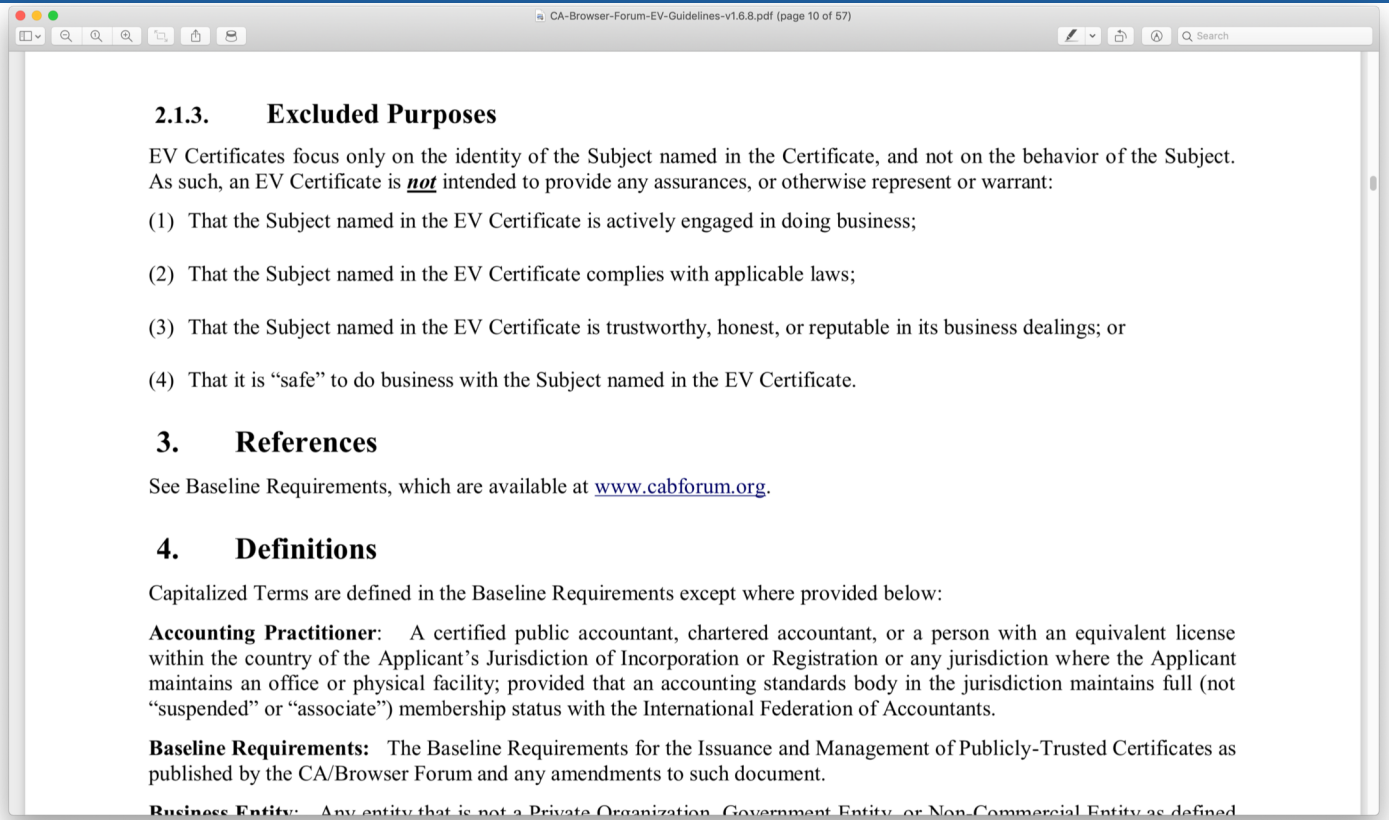
(2) Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and

(3) Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

https://cabforum.org/wp-content/uploads/CA-Browser-Forum-EV-Guidelines-v1.6.8.pdf, accessed 2019-04-01

IGTF AP|EU|TAG · TAGPMA · PITTSBURGH SUPERCOMPUTING CENTER

Extended Validation “Excluded Purposes”



2.1.3. Excluded Purposes

EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, an EV Certificate is ***not*** intended to provide any assurances, or otherwise represent or warrant:

(1) That the Subject named in the EV Certificate is actively engaged in doing business;

(2) That the Subject named in the EV Certificate complies with applicable laws;

(3) That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or

(4) That it is “safe” to do business with the Subject named in the EV Certificate.

3. References

See Baseline Requirements, which are available at www.cabforum.org.

4. Definitions

Capitalized Terms are defined in the Baseline Requirements except where provided below:

Accounting Practitioner: A certified public accountant, chartered accountant, or a person with an equivalent license within the country of the Applicant’s Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility; provided that an accounting standards body in the jurisdiction maintains full (not “suspended” or “associate”) membership status with the International Federation of Accountants.

Baseline Requirements: The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates as published by the CA/Browser Forum and any amendments to such document.

Business Entity: Any entity that is not a Private Organization, Government Entity, or Non-Commercial Entity as defined

https://cabforum.org/wp-content/uploads/CA-Browser-Forum-EV-Guidelines-v1.6.8.pdf, accessed 2019-04-01

IGTF AP|EU|TAG · TAGPMA · PITTSBURGH SUPERCOMPUTING CENTER

IETF RFC 8555 - ACME

Internet Engineering Task Force (IETF)
Request for Comments: 8555
Category: Standards Track
ISSN: 2070-1721

R. Barnes
Cisco
J. Hoffman-Andrews
EFF
D. McCarney
Let's Encrypt
J. Kasten
University of Michigan
March 2019

https://tools.ietf.org/html/rfc8555
(95pp.)

Automatic Certificate Management Environment (ACME)

Abstract

Public Key Infrastructure using X.509 (PKIX) certificates are used for a number of purposes, the most significant of which is the authentication of domain names. Thus, certification authorities (CAs) in the Web PKI are trusted to verify that an applicant for a certificate legitimately represents the domain name(s) in the certificate. As of this writing, this verification is done through a collection of ad hoc mechanisms. This document describes a protocol that a CA and an applicant can use to automate the process of verification and certificate issuance. The protocol also provides facilities for other certificate management functions, such as certificate revocation.

IETF RFC 8555 ACMEv2 Protocol Overview

1. Client requests account w/ACME server
   a. Client generates key pair
   b. Sends signed request bundle to server with contact info, terms of service agreement, external account association data
2. Client certificate request
   a. Submit signed order for request
   b. Prove control of identifiers requested in certificate (HTTP-01 or DNS-01)
   c. Submit CSR
   d. Submit signed POST-as-GET request, await issuance and download certificate
3. Client revocation request
   a. Submit signed revocation request
   b. Await confirmation from server

IGTF AP|EU|TAG
TAGPMA
PITTSBURGH SUPERCOMPUTING CENTER

IETF RFC 8555 ACMEv2 Protocol Identifier Validation

- Key authorizations
  - Requester (re)authentication
- Retrying challenges
  - Clients do not respond to server challenges until ready
- HTTP-01 challenge
  - Server validates key authorization content (constructed by client with token and client's account key) placed in client's HTTP content tree
- DNS-01 challenge
  - Server validates DNS TXT resource record (constructed by client with token and client's account key) provisioned by client

IGTF AP|EU|TAG TAGPMA PITTSBURGH SUPERCOMPUTING CENTER

IETF RFC 8555 ACMEv2 Protocol Protections

- Client / Server communications via HTTPS
  - Except for HTTP-01 challenge by Server to Client, necessarily HTTP
- Request authentication
  - all non-empty payloads in JSON Web Signature objects
- Replay protection
  - server-side session nonce generation and updates
- POST-as-GET requests
  - server reauthenticates sender and verifies access control rules
- Rate Limits

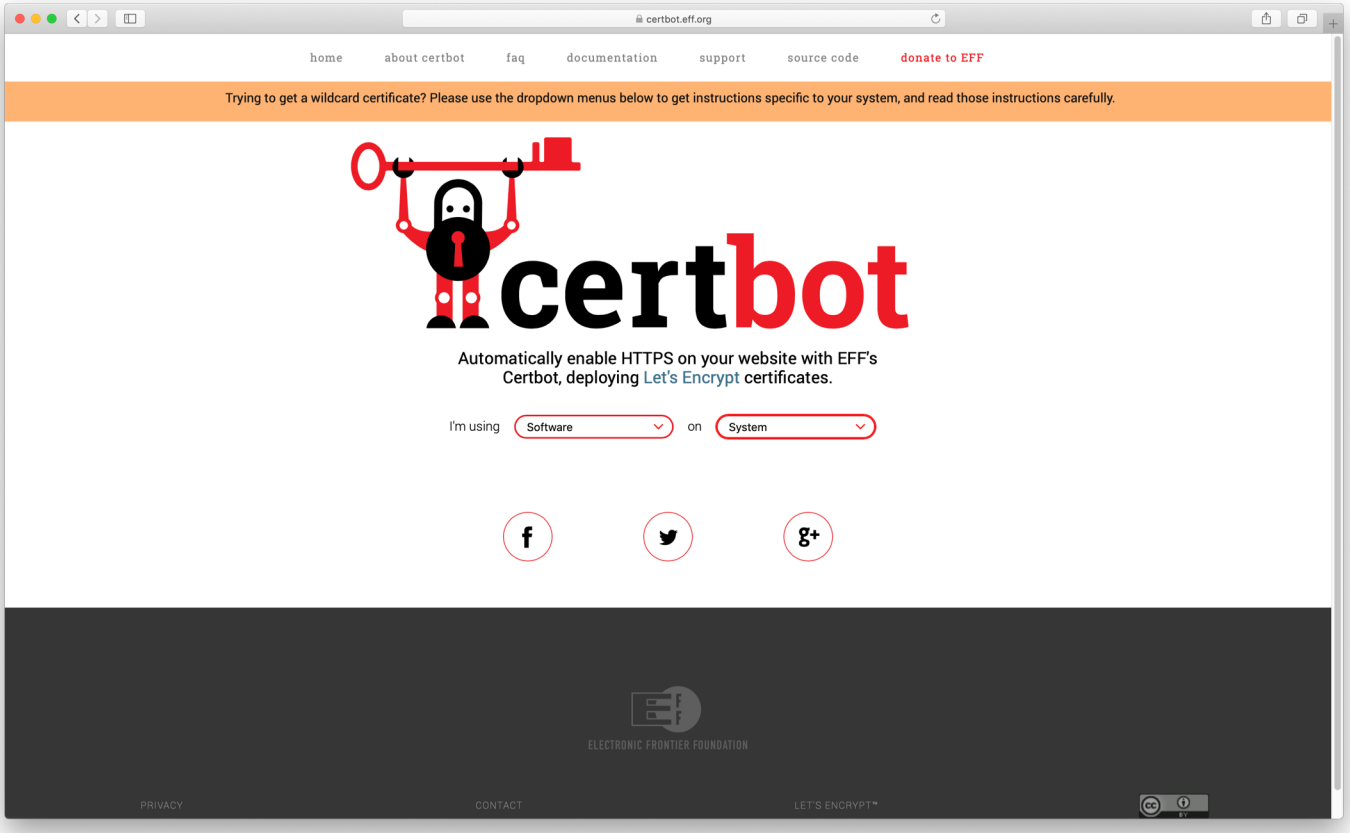
IGTF AP|EU|TAG TAGPMA PITTSBURGH SUPERCOMPUTING CENTER

IETF RFC 8555 ACMEv2 Protocol Protections

- External account binding
  - New account requests may be bound to an existing external account management system
- Account deactivation
  - Shut off future requests from this account
- Preauthorization
  - Enable an external, non-ACME process for authorizing a client to issue certificates for an identifier
- IETF RFC 6844 Certificate Authority Authorization (CAA) validation
  - Enable DNS Resource Record query for CAs authorized to issue certificates to a domain

IGTF AP|EU|TAG TAGPMA PITTSBURGH SUPERCOMPUTING CENTER

ACME Client Example: CertBot for LetsEncrypt



https://certbot.eff.org, accessed 2019-04-01

ACME Client Example: CertBot for LetsEncrypt

https://certbot.eff.org, accessed 2019-04-01

Questions about LetsEncrypt vs. IETF RFC 8555

Current LetsEncrypt vs. IETF RFC 8555

- Divergences list
  - https://github.com/letsencrypt/boulder/blob/master/docs/acme-divergences.md
  - pre-authorization not yet supported
  - POST-as-GET not yet implemented
- How are requester accounts managed?
- How to establish trust with hosting providers?
- Multi-network (DNS) validation not yet implemented (ETA Q2 2019)
- ECDSA Root and Intermediates (ETA Q3 2019)

An IGTF Profile (Elm) for ACME CAs?

Should we develop a new authentication assurance profile “Elm” for ACME-like automated CAs?

- Rapid expansion of container-based web service deployment with automated management in R&E
  - Kubernetes, Nomad, and other container orchestration infrastructures
- Browsers declining/suppressing access to non-HTTPS sites
- Must we do so for IGTF to sustain relevance to our community?
  - Sites and web developers are already using LetsEncrypt for in-house and web services not required by (or waived from) policy for stronger validation
  - Is it too late? Will anyone care by the time we get it done?

IGTF AP|EU|TAG TAGPMA PITTSBURGH SUPERCOMPUTING CENTER

An IGTF Profile (Elm) for ACME CAs?

- No? Then let's stop here.
- Thanks for your kind attention. Let's go get lunch.

IGTF AP|EU|TAG
TAGPMA
PITTSBURGH SUPERCOMPUTING CENTER

An IGTF Profile (Elm) for ACME CAs?

- Yes? OK, then:

- "Elm" is the next available assurance label in our tree
- Who is our Audience? (ACME) implementers, APs
  - What are their driving Use Cases?
- Following the basic rules of design[1]:
  - What are the Correct Problems to Solve? ← *Requirements*
  - How are these Problems Solved Correctly Together? ← *Solution*

[1]Donald Norman. (2013) The Design of Everyday Things, Revised and Expanded Edition. ISBN 978-0-465-05065-9.

IGTF AP|EU|TAG TAGPMA PITTSBURGH SUPERCOMPUTING CENTER

What are the Correct Problems to Solve?

Discussion:

- What problems MUST be addressed in the Elm Profile?

- Certificate Management Automation: ACME +/- what?
  - Wildcard certificate support?
- GFD 225: Uniqueness of Names
- Vetting, Roles & Responsibilities of Authorized Requesters
- What else?

How are the Problems Solved Correctly Together?

Discussion:

- What solutions are feasible for each problem?
- What feasible permutation(s) of the solutions sufficiently solve all problems together?

IGTF AP|EU|TAG
TAGPMA
PITTSBURGH SUPERCOMPUTING CENTER

IGTF Elm Authentication Assurance Profile

Objective: Publish Elm Profile for Automated CAs with DV

- Lead Author
- Co-authors
- Funding for this effort?
- Timeline
- Meeting schedule
- Mailing lists