internet2.edu

InCommon Steering - Certificate Service CPS review

May 1, 2023

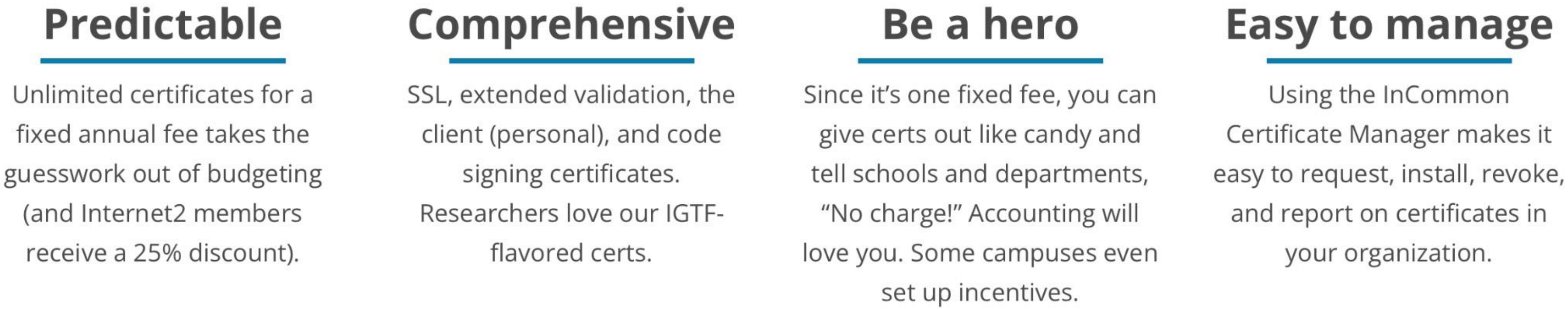
Presented by Sara Jeanes, Internet2

AGENDA

- What is the InCommon Certificate service?
- What is the role of InCommon?
- What is a CPS and what changes have been requested?

InCommon Certificate Services

InCommon Certificate Service



Predictable

Unlimited certificates for a fixed annual fee takes the guesswork out of budgeting (and Internet2 members receive a 25% discount).

Comprehensive

SSL, extended validation, the client (personal), and code signing certificates. Researchers love our IGTF-flavored certs.

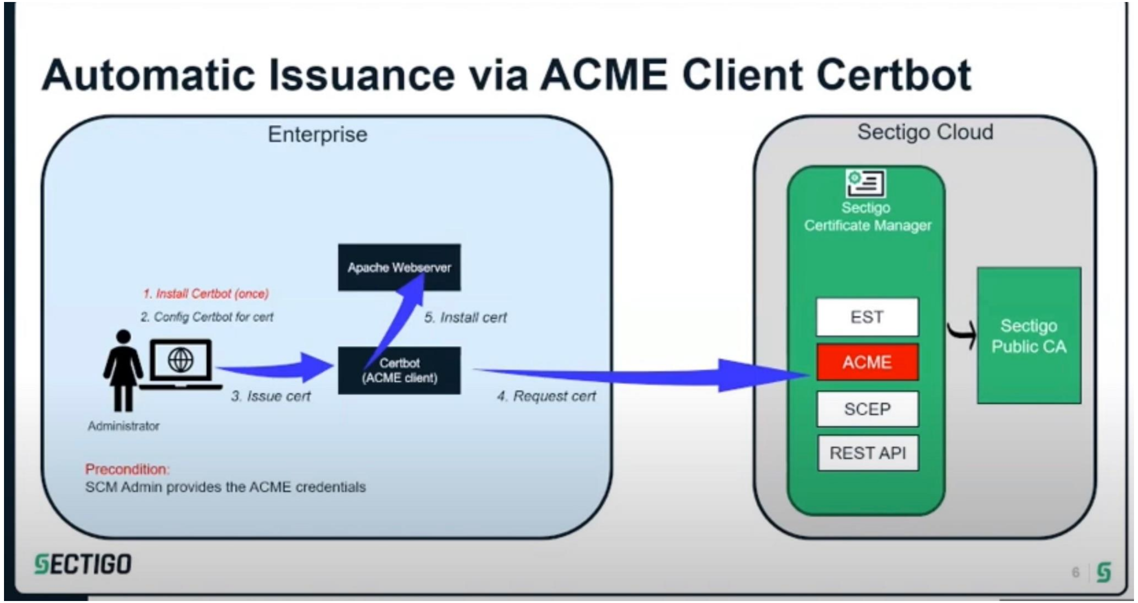
Be a hero

Since it's one fixed fee, you can give certs out like candy and tell schools and departments, "No charge!" Accounting will love you. Some campuses even set up incentives.

Easy to manage

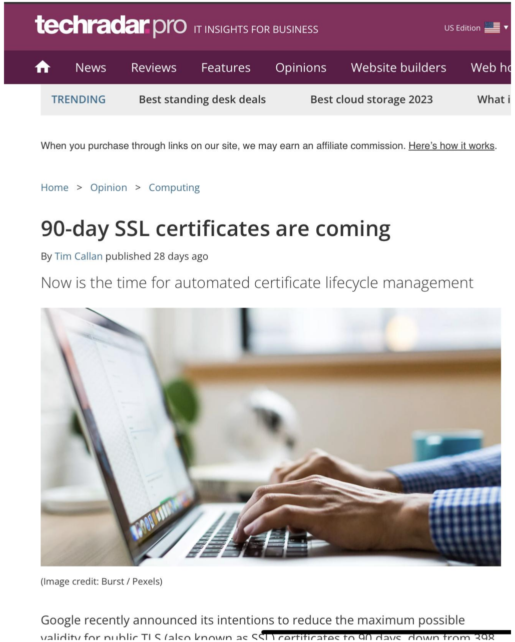
Using the InCommon Certificate Manager makes it easy to request, install, revoke, and report on certificates in your organization.

Automating Certificate Deployment



Automatic Issuance via ACME Client Certbot

Precondition:
SCM Admin provides the ACME credentials



techradar pro IT INSIGHTS FOR BUSINESS US Edition

News Reviews Features Opinions Website builders Web ho

TRENDING Best standing desk deals Best cloud storage 2023 What i

When you purchase through links on our site, we may earn an affiliate commission. Here's how it works.

Home > Opinion > Computing

90-day SSL certificates are coming

By Tim Callan published 28 days ago

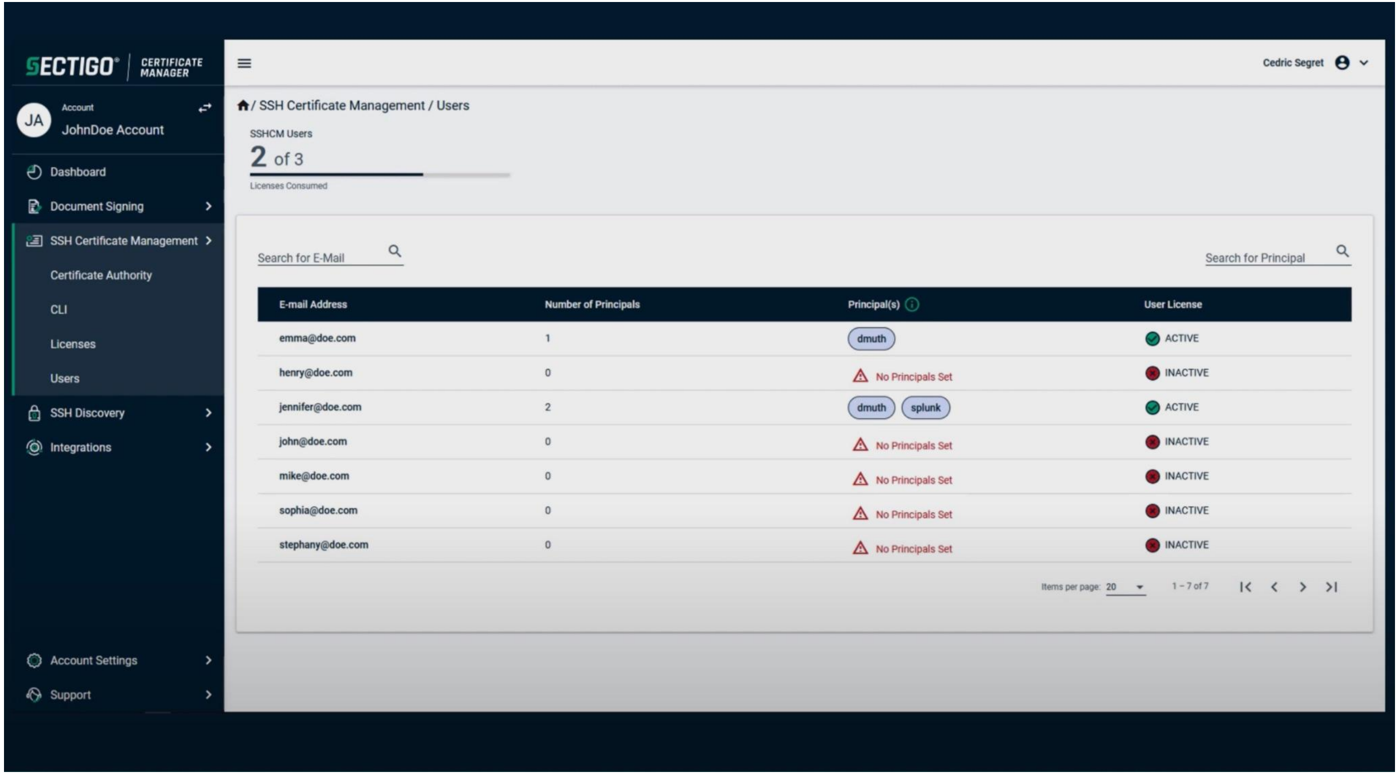
Now is the time for automated certificate lifecycle management

(Image credit: Burst / Pexels)

Google recently announced its intentions to reduce the maximum possible validity for public TLS (also known as SSL) certificates to 90 days, down from 398

https://www.techradar.com/opinion/90-day-ssl-certificates-are-coming

Delegating Management and Administration of Certificates



/ SSH Certificate Management / Users

SSHCM Users

2 of 3

Licenses Consumed

E-mail Address	Number of Principals	Principal(s)	User License
emma@doe.com	1	dmuth	ACTIVE
henry@doe.com	0	No Principals Set	INACTIVE
jennifer@doe.com	2	dmuth splunk	ACTIVE
john@doe.com	0	No Principals Set	INACTIVE
mike@doe.com	0	No Principals Set	INACTIVE
sophia@doe.com	0	No Principals Set	INACTIVE
stephany@doe.com	0	No Principals Set	INACTIVE

Items per page: 20   1 – 7 of 7

https://www.youtube.com/watch?v=zYbWwxpfKhw

Types of Certificates Available

- Secure Websites (like services offered in the *InCommon Federation)* - SSL/TLS Certificates
- Websites with a ‘green lock’ - Extended Validation (EV) and Anchor Certificates
- Secure *eduroam* and Email - Client (Personal) Certificates
- Software Code Validation - Code Signing Certificates
- Grid Computing - IGTF Server Certificates
- Next Generation - ECC (Elliptical Curve Cryptography) Certificates

~1300 websites are secured with InCommon certificates
~200 organizations secure their custom-developed applications with Code Signing certs
650+ organizations are using the InCommon Certificate Service

Operational Overview

- InCommon offers security services from Sectigo to US Higher Ed and Research organizations

- Community Subscribers to the Certificate Service pay one annual fee to InCommon
  - Based on their Carnegie Classification

- InCommon is the nearly complete ‘sales’ channel for Sectigo’s US Higher Education market

Support Overview

- **Legal**: InCommon owns the customer agreement
- **Rev Ops**: InCommon owns the billing/receivables risk and lifecycle
- **Support**: Support is shared between InCommon and Sectigo:
  - Operations of Technical components: Sectigo
  - Organizational Validation: Sectigo (now, used to be InCommon)
  - Password Reset and some domain approval work: InCommon
  - Billing and Legal: InCommon

What is a Certification Practices Statement (CPS) and what changes are being made?

CPS Overview

- A **Certification Practice Statement**, defined in IETF RFC 2527, is (from Gartner):

  > *"A document defining all the operational practices that will be used to maintain the required level of public-key infrastructure (PKI) security."*

- A CPS makes clear the "rules of the game" by which certificates are issued.
- It can used:
  - By external organizations to review and decide whether or not to trust the issued certificates
  - By auditors to determine whether or not actual operational procedures comply with stated practices
- *InCommon maintains three CPS documents: SSL certificates, IGTF certificates, User certificates*

Proposed Changes to IGTF CPS

- The changes made in this version of the CPS were to modernize it and to reflect the latest instance of the IGTF CA (the existing one is expiring).
    - Comodo changed their name to Sectigo.
    - InCommon’s address changed.
    - The name of our CA changed very slightly (version 2).
    - There have been changes in certificate registration duties between InCommon and Sectigo.
    - Because these changes constitute a “material” change, we are incrementing and generalizing the OID that is minted into our IGTF SSL certificates.

Review Process

- ***1.5.4 CPS Approval Procedures***
  - *InCommon's CPS (and any amendments made to it) are reviewed and approved by InCommon's Policy Authority and approved by TAGPMA before signing any certificates under the new CP/CPS. Amendments to the CPS may be made by reviewing and updating the entire CPS or by publishing an addendum.*

    - *TAGPMA = The Americas Grid Policy Management Authority*
    - *InCommon's Policy Authority = InCommon Steering*

Questions?

Sara Jeanes: sjeanes@interenet2.edu