Entrust situation

An overview and suggested actions

digicert®

Today’s speakers

Jeremy Rowley
Chief Security Information Officer

Brian Trzupek
Senior VP of Product

Entrust distrust – what's going on here

What

- Google announced that Chrome (market share ~65%) will no longer trust TLS certificates issued by Entrust, effective October 31, 2024
- Blocking action will begin on approximately November 1, 2024, affecting certificates issued at that point or later (Chrome 127 onwards)

Why

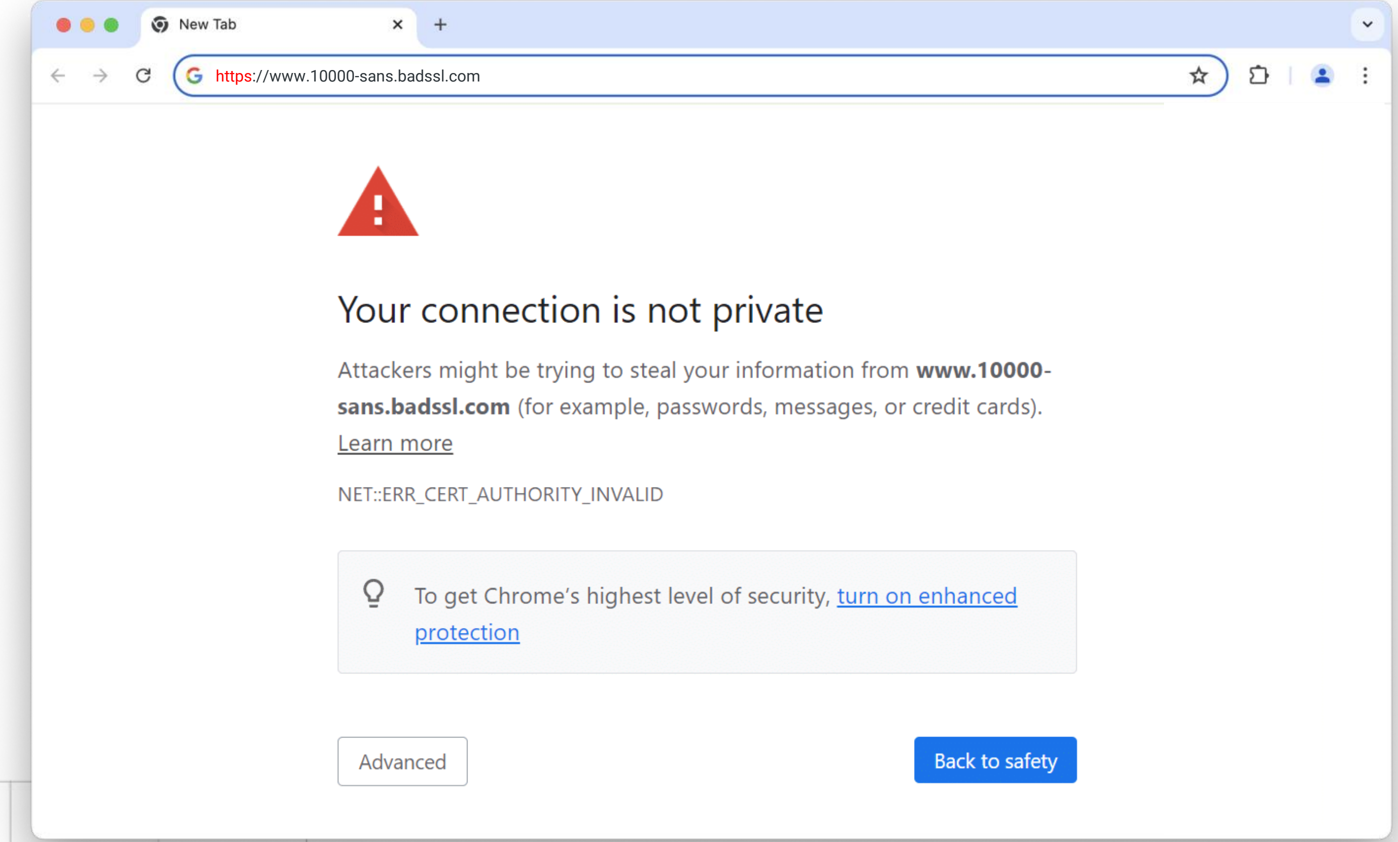
- Google "*highlighted a pattern of concerning behaviors by Entrust*"
- Summary: Systemic failures in transparency, response times, and issuance of compliant certificates.

Next steps

- Google recommends that, "*affected website operators transition to a new publicly-trusted CA owner as soon as reasonably possible*" to avoid adverse impact.

User impact of Entrust distrust

“Chrome users who navigate to a website serving a certificate ***issued*** *by Entrust or AffirmTrust off the roots that will be distrusted after October 31, 2024 will see a full page similar to this one”*



Your connection is not private

Attackers might be trying to steal your information from **www.10000-sans.badssl.com** (for example, passwords, messages, or credit cards). Learn more

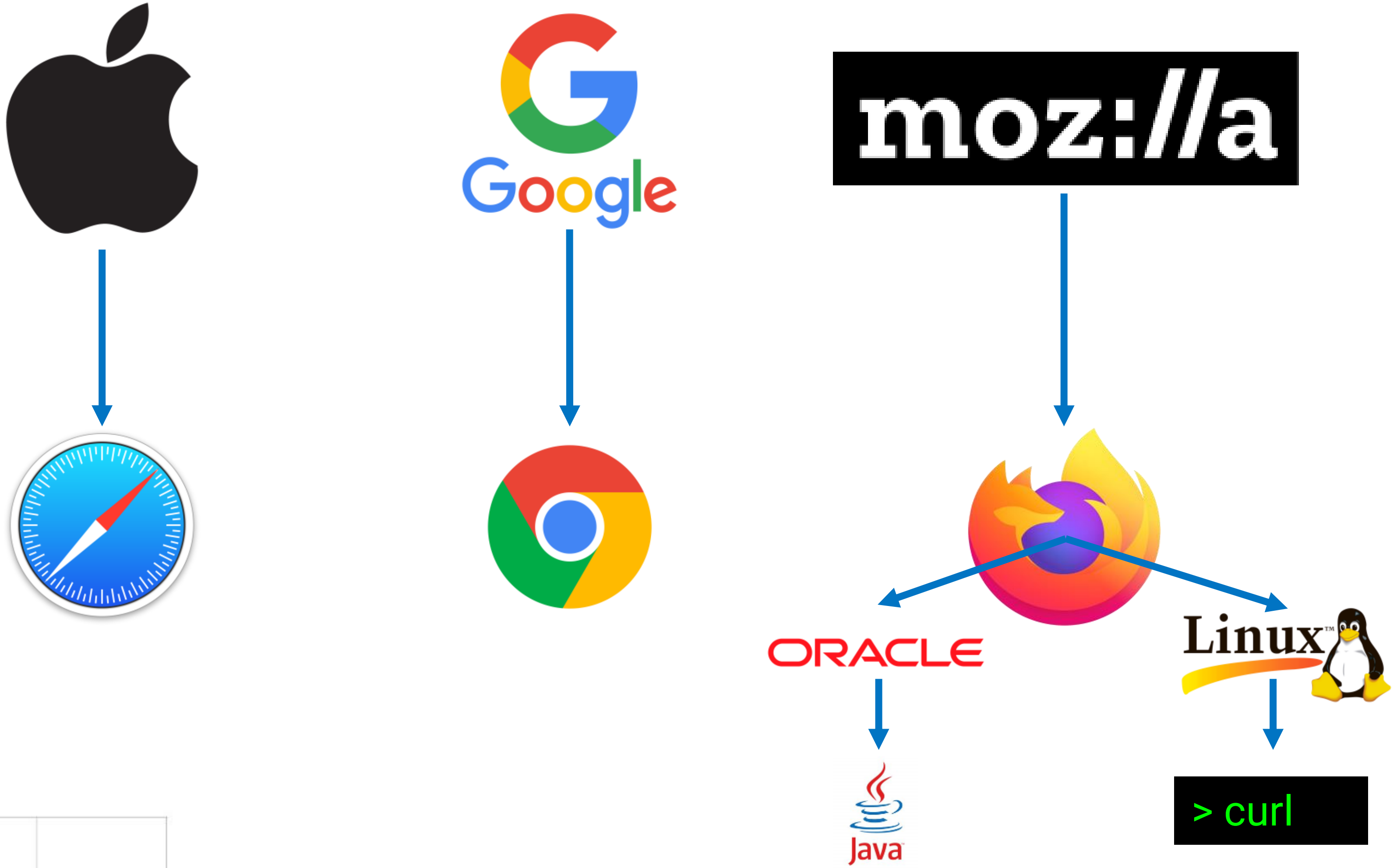
NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome’s highest level of security, turn on enhanced protection

Implications for customers

- Customers would need to migrate all issuance to another public CA by Oct 31, 2024
- Any network, device, or trust store configurations with Entrust might need to change

The Web-PKI Trust Ecosystem



History of distrust

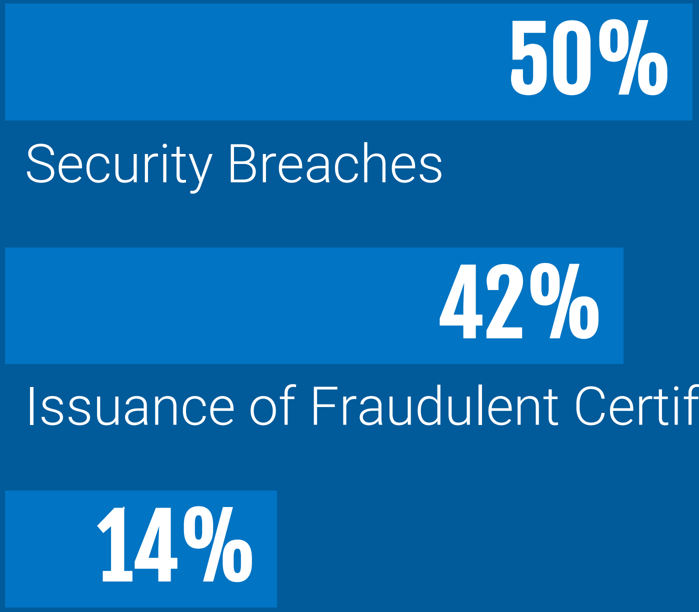
14

Certificate Authorities
Distrusted by major browsers Since 2011

ex: Symantec, WoSign, Visa, DigiNotar

68% of all distrust:
Poor compliance handling

Other Reasons:



50%

Security Breaches

42%

Issuance of Fraudulent Certificates

14%

Limited Value to the ecosystem

*Source https://unmitigatedrisk.com/?p=850

DigiCert: proven leaders in distrust management

2,100,000+	Symantec Certificates Migrated
160,000+	Organizations Validated
100,000+	Domains Validated
Only 4	Months to build, deploy, & migrate.

How DigiCert handled Symantec distrust

- **Communicated** with the browsers and stakeholders
- Developed an **integration plan** and system
- Established trust in the process by **communicating** a plan and timelines
- Provided **transparency** on the Symantec transfer
- Worked rapidly to **migrate customers** and kept commitments
- Kept the goal in sight of **shutting down legacy systems**
- Shut down Symantec systems once **migration completed**

How can DigiCert help

1 Migrate Entrust SSL Certificates

- Get new certificates quickly from **Digicert CertCentral**.
- Get inventory of Entrust certificates & Reissue with DigiCert.

2 Automate certificate lifecycle management

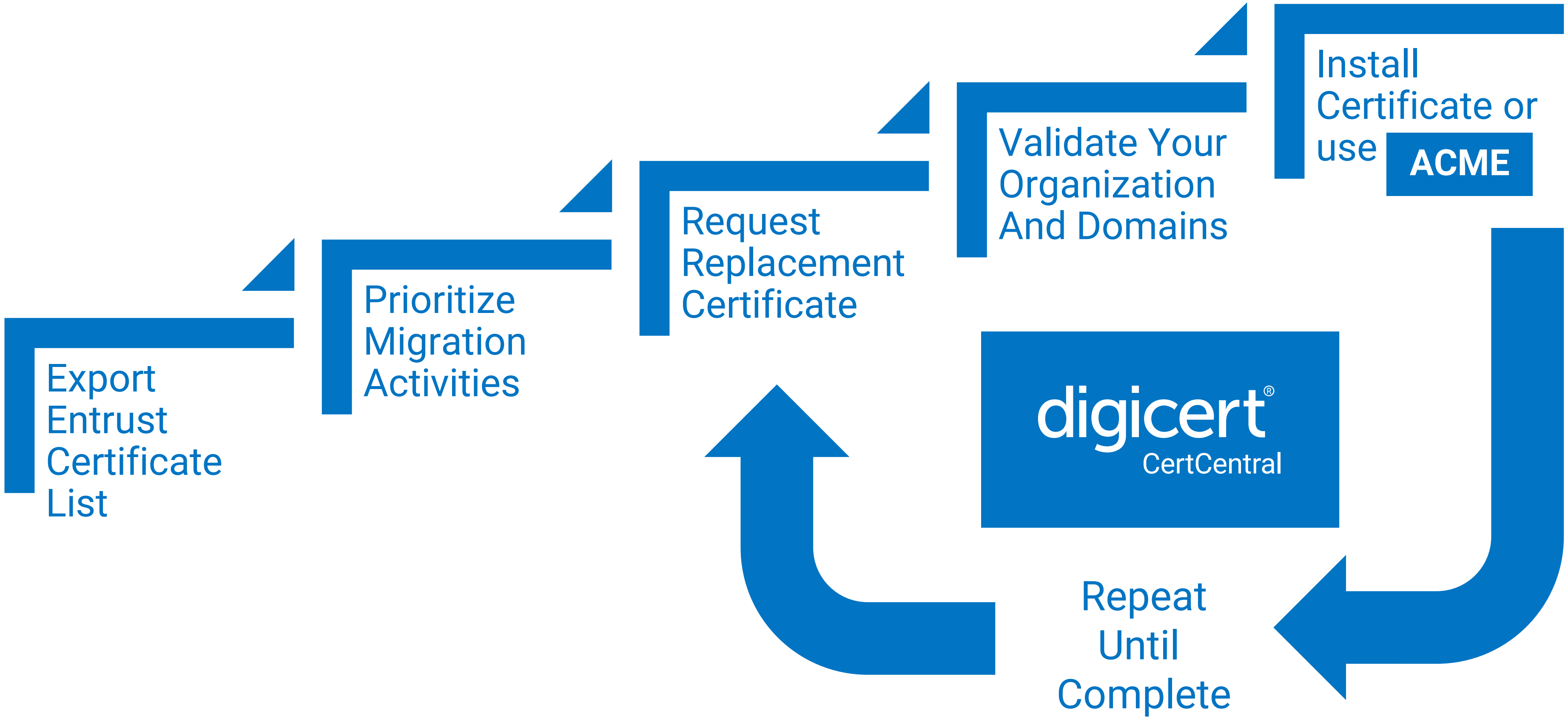
- Deploy powerful tooling to automate certificate reissuance.
- Utilize ACME or any of the numerous support automation technologies.
- Future proof your **crypto-agility with DigiCert Trust Lifecycle Manager**

3 Centralize public and private PKI

- DigiCert Trust Lifecycle Manager provides a single tool to manage your public and private PKI(s)
- **Modernize PKI** - Manage private and public PKIs together
- Establish Private Enterprise Roots with DigiCert.

Migrating less than 50 certificates?

Follow this path for simple migration use cases.



Export Entrust Certificate List

Prioritize Migration Activities

Request Replacement Certificate

Validate Your Organization And Domains

Install Certificate or use ACME

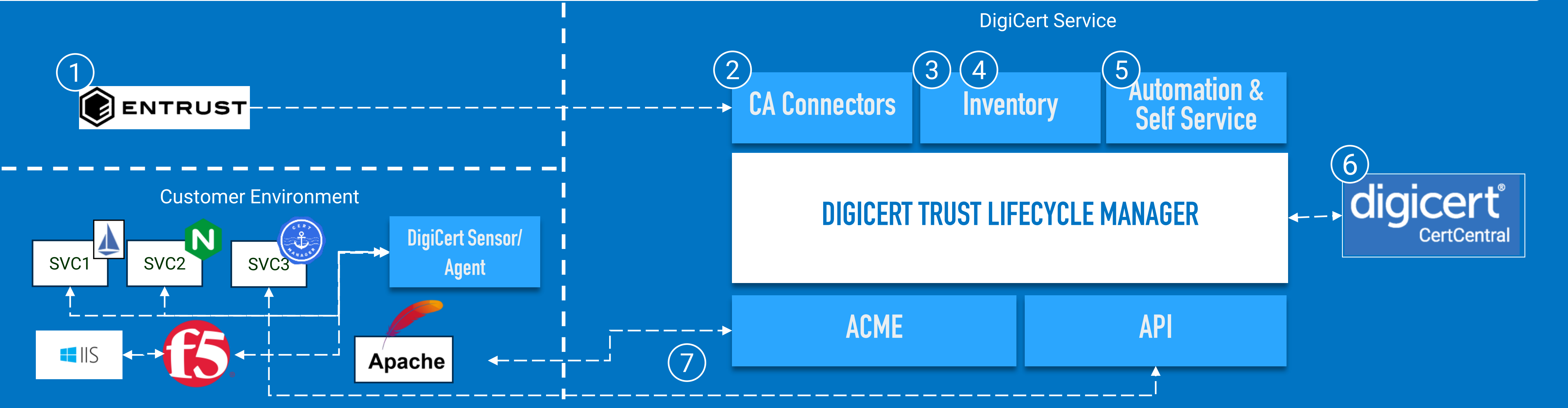
digicert® CertCentral

Repeat Until Complete

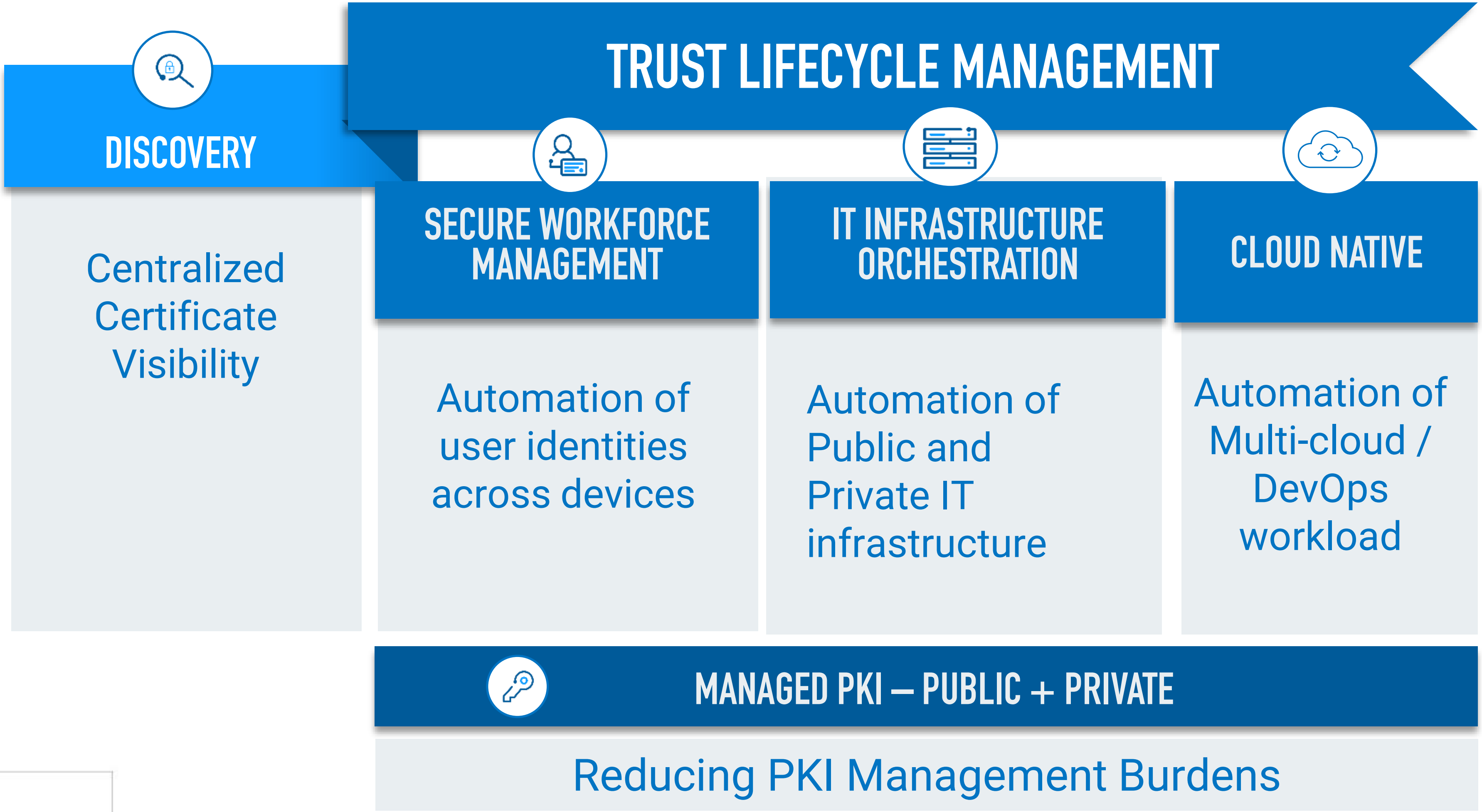
Migrating more than 50 certificates?

Follow this path for more than 50 certificates.

1. Connect DigiCert Trust Lifecycle Manager to Entrust.
2. Import Entrust Certificates
3. Prioritize and Plan Migration
4. Configure Automated Installation or Initiate Self-Service Migration
5. New Certificates Issued by DigiCert
6. Deploy Certificate to target systems



Trust lifecycle manager – delivering crypto agility



TRUST LIFECYCLE MANAGEMENT

DISCOVERY

Centralized Certificate Visibility

SECURE WORKFORCE MANAGEMENT

Automation of user identities across devices

IT INFRASTRUCTURE ORCHESTRATION

Automation of Public and Private IT infrastructure

CLOUD NATIVE

Automation of Multi-cloud / DevOps workload

MANAGED PKI – PUBLIC + PRIVATE

Reducing PKI Management Burdens

Why trust DigiCert

History	Transparency	Expertise	Customer Focus
25+ Years of Industry Leadership	Compliance Focused Operations	700+ Security Experts / Engineers	5 Star Customer Support (NPS 80)
Widest Root Ubiquity	Lead key industry groups	Operate Infra for CT Logging industry	Solutions for many PKI workflows
We are a PKI company	Communications, actions & plans	Provide OSS PKI Linting (hygiene)	Trusted by 97% of F100 Banks

DigiCert: Setting the standard for digital trust

Investing in standards for trust

- Leadership in technology & industry standards
- Strong compliance; 25+ annual audits
- Managing over 2600 PKI systems worldwide

CAB CA/BROWSER FORUM

NIST

CI+

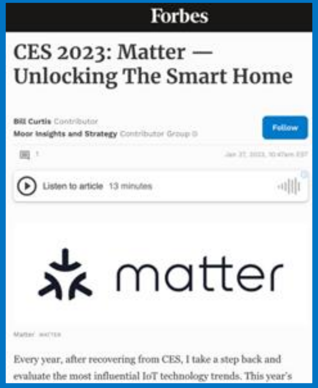
CableLabs®

CLOUD SIGNATURE CONSORTIUM

PCI

IETF

matter



Forbes

CES 2023: Matter — Unlocking The Smart Home

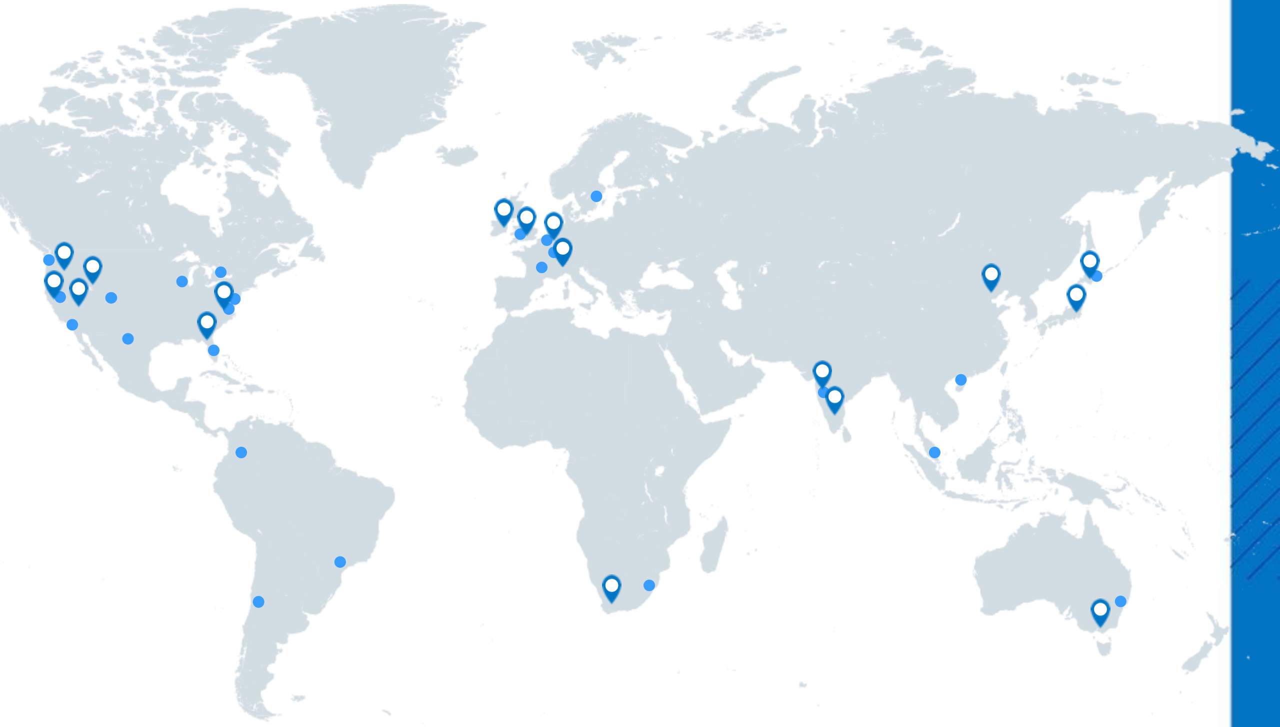
Bill Curtis Contributor
Moor Insights and Strategy Contributor Group

Matter MATTER

Every year, after recovering from CES, I take a step back and evaluate the most influential IoT technology trends. This year's

Global footprint, local delivery

- Customers in 180 countries
- 24/7/365 follow-the-sun, world-class support



How DigiCert manages incidents

- **Be a partner** with the ecosystem and establish trust
- Respond to inquiries **promptly** and with **humility**
- Provide **transparency** into the CA operations challenges
- Create **meaningful steps that improve**
  - both the ecosystem and your CA operations
- Find a **never-again plan** that works
- Establish a mind-set of **continuous improvements**
- Have **good data practices**
- **Automate** as much as possible
- Perform **regular audits**

> I do want to say, even as a preliminary incident, this is a great example of what a CA that issues EV/OV certs should do when they're facing a delayed revocation.
>
> - Amir (Mozilla forums)

DigiCert

Best in class SSL/ PKI Management

120,000+

customers

Global operations

Best support - 24/7/365

★★★★★

97%

world’s largest banks

Experts

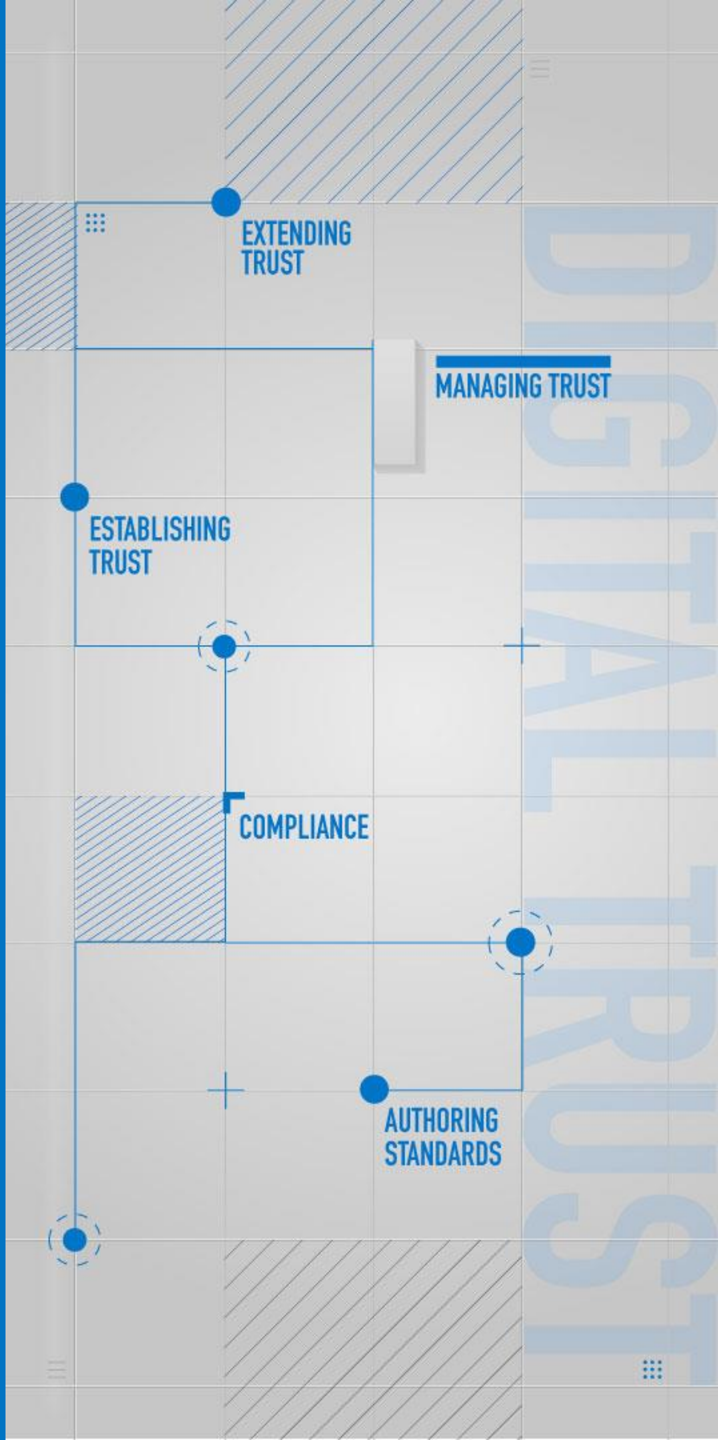
Manage 2600+ Roots
Manage 5700+ ICAs
60+ Key Ceremonies/Week

80

industry-leading NPS score

Questions?

digicert®



Thank you

digicert®