New Adventures in PKI

Jeremy Rowley

DigiCert, Inc.

digicert® YOUR SUCCESS IS BUILT ON TRUST®

Overview

- Deprecation of SHA-1
- Certificate Transparency (CT)
- Certificate Lifecycles
- Internal Name Deprecation
- Certificate Authority Authorization (CAA)
- Heartbleed Bug

SHA-1 Transition

Microsoft SHA-1 Deprecation Timeline

- January 1, 2016: Cease issuance and deprecation for code signing certificates
- January 1, 2017: Deprecation of SSL

Mozilla SHA-1 Deprecation Timeline

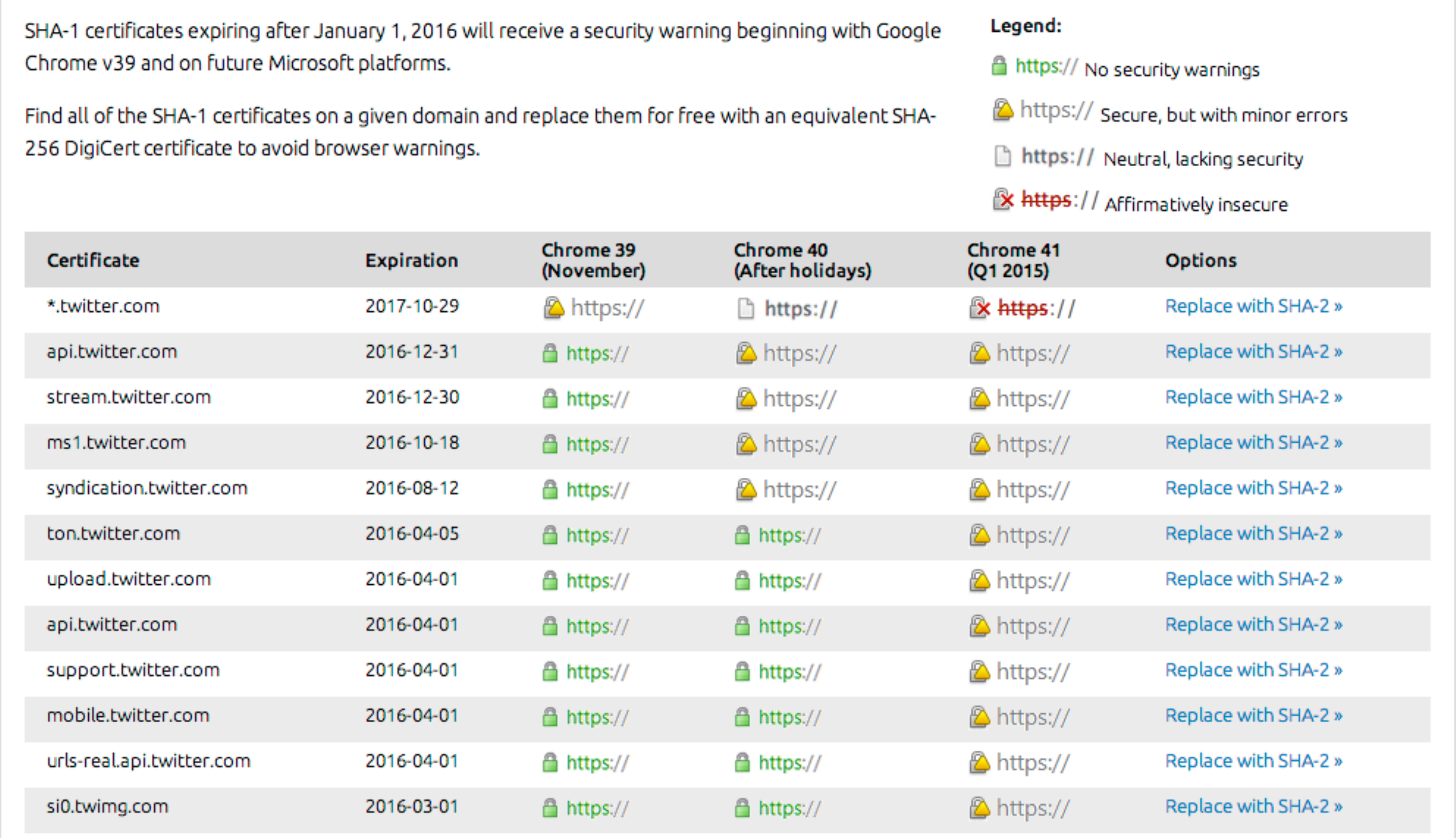
- Early 2015: Security warning for 2017 certificates
- Firefox 2016 release: “Untrusted Connection” for new SHA-1 certificates
- Firefox 2017 release: “Untrusted Connection” for all SHA-1

SHA-1 Transition

Google SHA-1 Deprecation Timeline

- September 2014: Mixed content warning for SHA-1 expiring in 2017
- November 2014: Mixed content warning for SHA-1 expiring after June 1, 2016
- Q1 2015: Mixed content warning for all certificates expiring in 2016 and interstitial for 2017 and non-secure indicator for 2017

SHA-1Sunset Tool



SHA-1 certificates expiring after January 1, 2016 will receive a security warning beginning with Google Chrome v39 and on future Microsoft platforms.

Find all of the SHA-1 certificates on a given domain and replace them for free with an equivalent SHA-256 DigiCert certificate to avoid browser warnings.

Legend:

- 🔒 https:// No security warnings
- ⚠ https:// Secure, but with minor errors
- 🗋 https:// Neutral, lacking security
- ✗ ~~https~~:// Affirmatively insecure

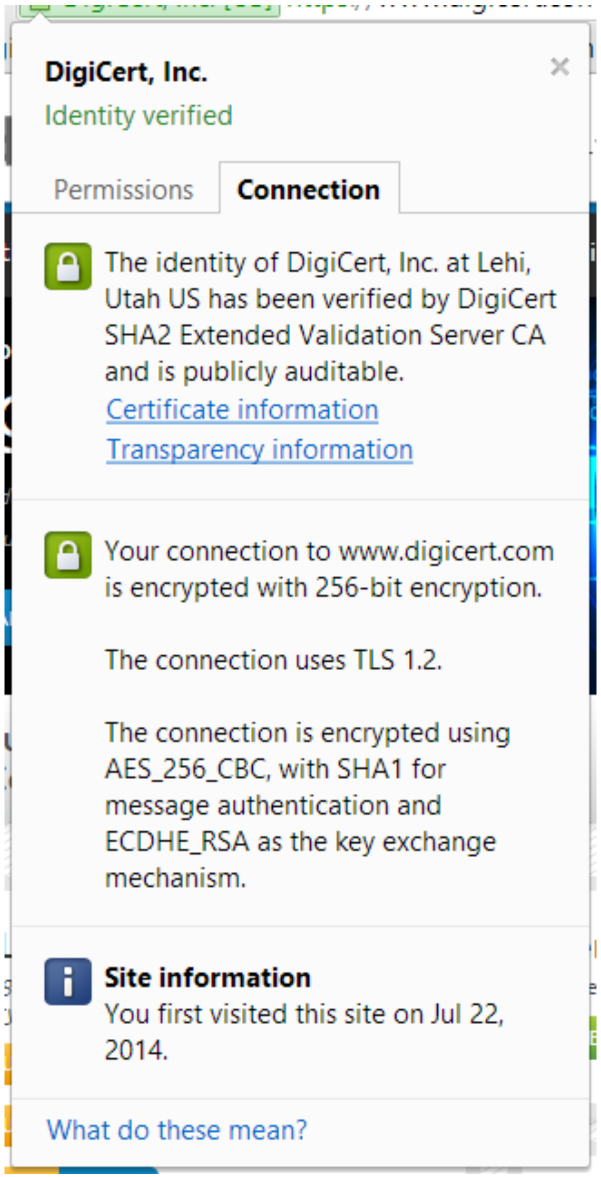
Certificate	Expiration	Chrome 39 (November)	Chrome 40 (After holidays)	Chrome 41 (Q1 2015)	Options
*.twitter.com	2017-10-29	⚠ https://	🗋 https://	✗ ~~https~~://	Replace with SHA-2 »
api.twitter.com	2016-12-31	🔒 https://	⚠ https://	⚠ https://	Replace with SHA-2 »
stream.twitter.com	2016-12-30	🔒 https://	⚠ https://	⚠ https://	Replace with SHA-2 »
ms1.twitter.com	2016-10-18	🔒 https://	⚠ https://	⚠ https://	Replace with SHA-2 »
syndication.twitter.com	2016-08-12	🔒 https://	⚠ https://	⚠ https://	Replace with SHA-2 »
ton.twitter.com	2016-04-05	🔒 https://	🔒 https://	⚠ https://	Replace with SHA-2 »
upload.twitter.com	2016-04-01	🔒 https://	🔒 https://	⚠ https://	Replace with SHA-2 »
api.twitter.com	2016-04-01	🔒 https://	🔒 https://	⚠ https://	Replace with SHA-2 »
support.twitter.com	2016-04-01	🔒 https://	🔒 https://	⚠ https://	Replace with SHA-2 »
mobile.twitter.com	2016-04-01	🔒 https://	🔒 https://	⚠ https://	Replace with SHA-2 »
urls-real.api.twitter.com	2016-04-01	🔒 https://	🔒 https://	⚠ https://	Replace with SHA-2 »
si0.twimg.com	2016-03-01	🔒 https://	🔒 https://	⚠ https://	Replace with SHA-2 »

Certificate Transparency

- **Goals**
  - Provide insight into issued SSL certificate
  - Provide faster remediation
  - Ensure CAs are aware of what they issue

- **Benefits**
  - Fast detection means better mitigation
  - Greater visibility means better accountability
  - Visible trust in operations
  - Easier evaluation of certificate use

- **Deployment**
  - Number of logs dependent on lifecycle
  - Required for EV starting Jan 2015
  - Nothing required from server operators
  - Two logs approved, two pending



DigiCert, Inc.

Identity verified

The identity of DigiCert, Inc. at Lehi, Utah US has been verified by DigiCert SHA2 Extended Validation Server CA and is publicly auditable.

Certificate information

Transparency information

Your connection to www.digicert.com is encrypted with 256-bit encryption.

The connection uses TLS 1.2.

The connection is encrypted using AES_256_CBC, with SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism.

Site information

You first visited this site on Jul 22, 2014.

What do these mean?

Certificate Lifecycles

- **Short lived Certificates**
  - Issued with a 48 hour validity period
  - Used for remote location
  - Alternative form of revocation
  - Mozilla discussion:
  https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/T11up58JkFc

- **3-year Maximum Lifecycle**
  - Required April 2015
  - Permits “rapid” changes in standards
  - Ensures revalidation is occurring

Internal Name Deprecation

CAs may no longer issue certificates that contain Internal Names and expire after November 1, 2015.

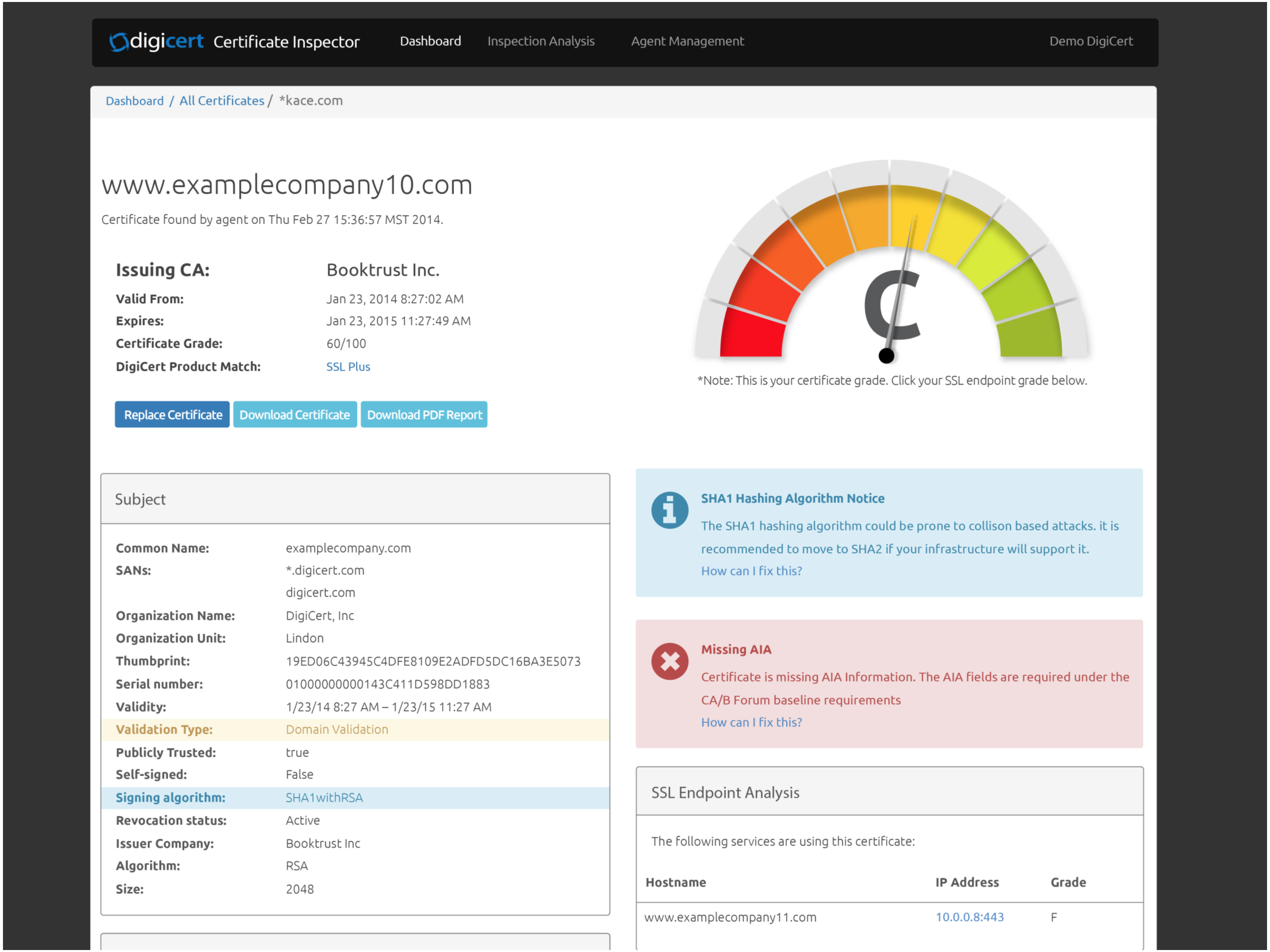
All certificates are revoked within 120 days of the contract signing date.

Finding Internal Names

- Gather all Certificates
- Look at each common name
- Look at each SAN
- Evaluate if there is an internal name

Certificate Inspector Tool

- Scans a network range and port range
- Evaluates each Certificate to determine if any internal names exist
- Compares against the latest policy changes
- Lists all internal name Certificates



www.examplecompany10.com

Certificate found by agent on Thu Feb 27 15:36:57 MST 2014.

Issuing CA:	Booktrust Inc.
Valid From:	Jan 23, 2014 8:27:02 AM
Expires:	Jan 23, 2015 11:27:49 AM
Certificate Grade:	60/100
DigiCert Product Match:	SSL Plus

*Note: This is your certificate grade. Click your SSL endpoint grade below.

Subject

Common Name:	examplecompany.com
SANs:	*.digicert.com digicert.com
Organization Name:	DigiCert, Inc
Organization Unit:	Lindon
Thumbprint:	19ED06C43945C4DFE8109E2ADFD5DC16BA3E5073
Serial number:	01000000000143C411D598DD1883
Validity:	1/23/14 8:27 AM – 1/23/15 11:27 AM
Validation Type:	Domain Validation
Publicly Trusted:	true
Self-signed:	False
Signing algorithm:	SHA1withRSA
Revocation status:	Active
Issuer Company:	Booktrust Inc
Algorithm:	RSA
Size:	2048

SHA1 Hashing Algorithm Notice

The SHA1 hashing algorithm could be prone to collison based attacks. it is recommended to move to SHA2 if your infrastructure will support it.

How can I fix this?

Missing AIA

Certificate is missing AIA Information. The AIA fields are required under the CA/B Forum baseline requirements

How can I fix this?

SSL Endpoint Analysis

The following services are using this certificate:

Hostname	IP Address	Grade
www.examplecompany11.com	10.0.0.8:443	F

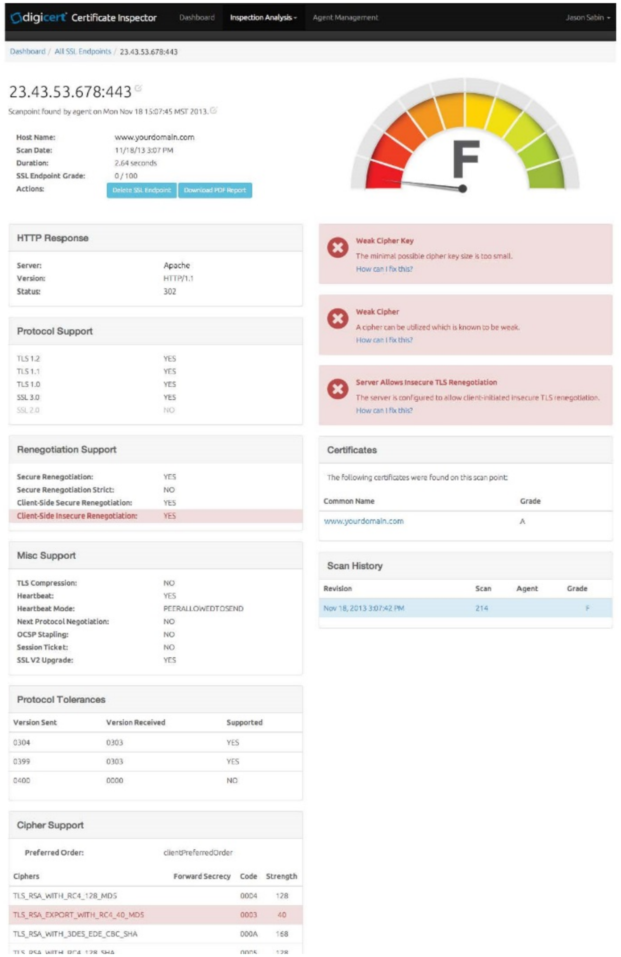
Certification Authority Authorization (CAA)

- **Advantages**
  - Reduces risk of unintended certificate mis-issuance
  - Simple way to express your preference of CAs
  - Add CAA information to DNS and change it when you wish
- **Disadvantages**
  - Compliance is voluntary
  - Not uniformly applied
  - Partial solution
  - May slow certificate issuance
- **Deployment**
  - CAs required to list policy and interpretation in CP
  - CAs may elect not to check CAA

DigiCert Certificate Inspector

Advanced SSL analysis examines common problems and weaknesses including:

- Vulnerability to Heartbleed Bug, CRIME, BEAST, or BREACH attacks
- Certificates with weak private keys
- Expiring certificate dates
- Internal names
- Missing fields and values
- Certificate name mismatch
- Weak cipher suites
- SHA1 vs SHA2
- Broken chains



Dashboard / All SSL Endpoints / 23.43.53.678:443

23.43.53.678:443

Scanpoint found by agent on Mon Nov 18 15:07:45 MST 2013.

Host Name:	www.yourdomain.com
Scan Date:	11/18/13 3:07 PM
Duration:	2.64 seconds
SSL Endpoint Grade:	0 / 100
Actions:	Delete SSL Endpoint Download PDF Report

Weak Cipher Key

The minimal possible cipher key size is too small.

How can I fix this?

Weak Cipher

A cipher can be utilized which is known to be weak.

How can I fix this?

Server Allows Insecure TLS Renegotiation

The server is configured to allow client-initiated insecure TLS renegotiation.

How can I fix this?

HTTP Response

Server:	Apache
Version:	HTTP/1.1
Status:	302

Protocol Support

TLS 1.2	YES
TLS 1.1	YES
TLS 1.0	YES
SSL 3.0	YES
SSL 2.0	NO

Renegotiation Support

Secure Renegotiation:	YES
Secure Renegotiation Strict:	NO
Client-Side Secure Renegotiation:	YES
Client-Side Insecure Renegotiation:	YES

Misc Support

TLS Compression:	NO
Heartbeat:	YES
Heartbeat Mode:	PEERALLOWEDTOSEND
Next Protocol Negotiation:	NO
OCSP Stapling:	NO
Session Ticket:	NO
SSL V2 Upgrade:	YES

Protocol Tolerances

Version Sent	Version Received	Supported
0304	0303	YES
0399	0303	YES
0400	0000	NO

Cipher Support

Preferred Order: clientPreferredOrder

Ciphers	Forward Secrecy	Code	Strength
TLS_RSA_WITH_RC4_128_MD5		0004	128
TLS_RSA_EXPORT_WITH_RC4_40_MD5		0003	40
TLS_RSA_WITH_3DES_EDE_CBC_SHA		000A	168
TLS_RSA_WITH_RC4_128_SHA		0005	128

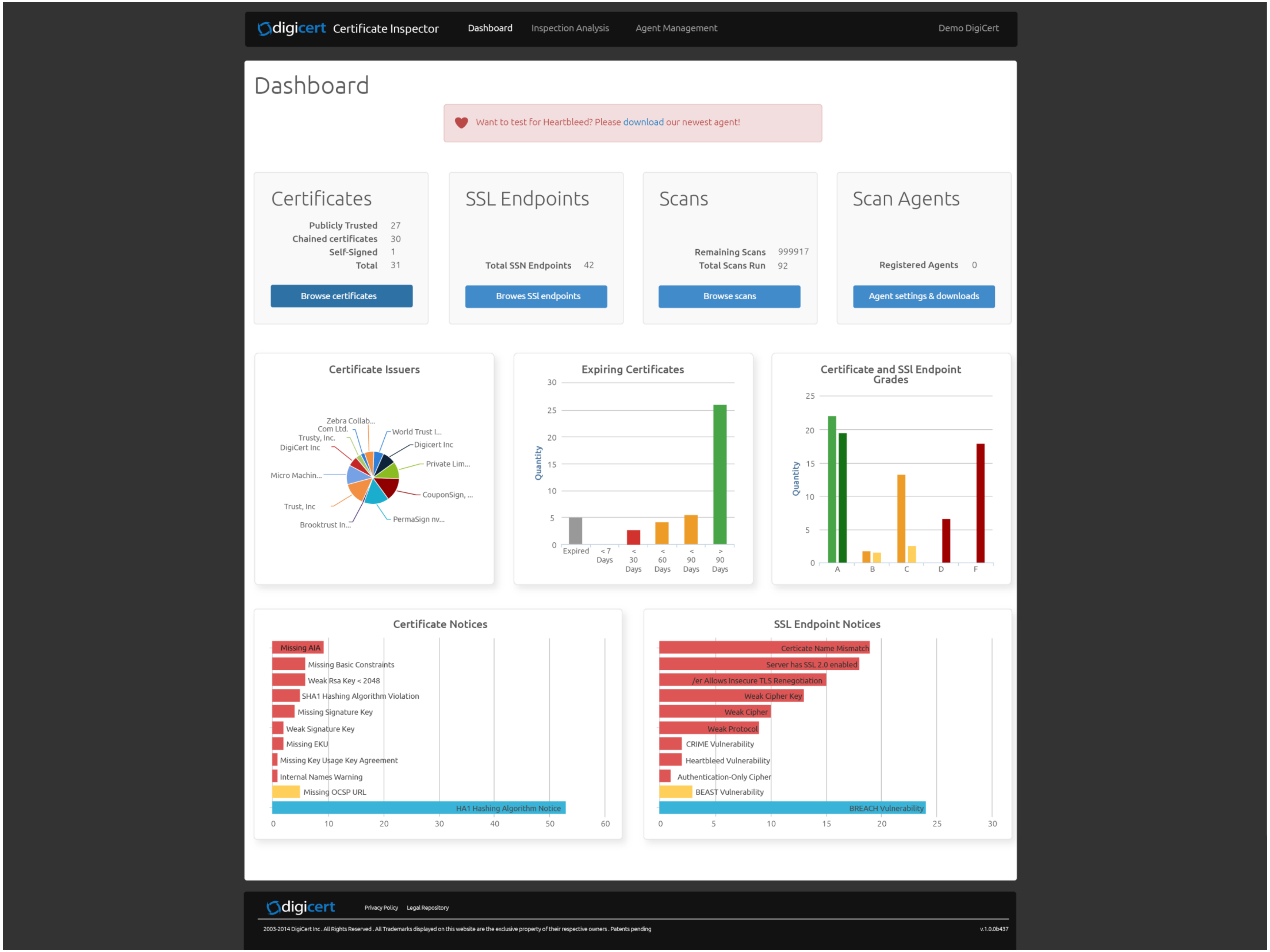
Certificates

The following certificates were found on this scan point:

Common Name	Grade
www.yourdomain.com	A

Scan History

Revision	Scan	Agent	Grade
Nov 18, 2013 3:07:42 PM	214		F



Dashboard

Want to test for Heartbleed? Please download our newest agent!

Certificates

Publicly Trusted	27
Chained certificates	30
Self-Signed	1
Total	31

SSL Endpoints

Total SSN Endpoints	42

Scans

Remaining Scans	999917
Total Scans Run	92

Scan Agents

Registered Agents	0

v.1.0.0b437

Tools

SSL Analysis Tools

- https://www.digicert.com/cert-inspector.htm
- https://www.digicert.com/sha1-sunset/
- https://www.ssllabs.com
- http://www.whynopadlock.com/

Jeremy Rowley

jeremy.rowley@digicert.com

801-701-9676