18F

Migrating .gov to HTTPS

Eric Mill, 18F/GSA

M-15-13: Require Secure Connections

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 8, 2015

M-15-13

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Tony Scott
Federal Chief Information Officer

SUBJECT: **Policy to Require Secure Connections across Federal Websites and Web Services**

This Memorandum requires that all publicly accessible Federal websites and web services[1] only provide service through a secure connection. The strongest privacy and integrity protection currently available for public web connections is Hypertext Transfer Protocol Secure (HTTPS).

https.cio.gov

The HTTPS-Only Standard

Why HTTPS for Everything?

HTTP has become central to today's way of life. HTTP is currently the primary protocol for applications used on computers, tablets, smartphones, and many other devices.

As our dependency on the internet has grown, the risk to users' privacy and safety has grown along with it.

Every unencrypted HTTP request reveals information about a user's behavior, and the interception and tracking of unencrypted browsing has become commonplace.

Today, **there is no such thing as insensitive web traffic**, and public services should not depend on the benevolence of network operators.

- **Confidentiality.** The visitor's connection is encrypted, obscuring URLs, cookies, and other sensitive metadata.
- **Authenticity.** The visitor is talking to the "real" website, and not to an impersonator or through a "man-in-the-middle".
- **Integrity.** The data sent between the visitor and the website has not been tampered with or modified.

The HTTPS-Only Standard

Why isn't DNSSEC good enough?

DNSSEC attempts to guarantee that domain names are resolved to correct IP addresses.

However, DNS resolution is just one aspect of securely communicating on the internet. DNSSEC does not fully secure a domain:

- Once DNS resolution is complete, DNSSEC does not ensure the confidentiality or integrity of communication between a client and the destination IP.
- No major web browsers inform the user when DNSSEC validation fails, limiting its strength and enforceability.

HTTPS guarantees the confidentiality and integrity of communication between client and server, and web browsers have rigorous and evolving HTTPS enforcement policies.

The HTTPS-Only Standard

How does HTTPS protect against DNS spoofing?

In practice, HTTPS can protect communication with a domain even in the absence of DNSSEC support.

A valid HTTPS certificate shows that the server has demonstrated ownership over the domain to a trusted certificate authority at the time of certificate issuance.

To ensure that an attacker cannot use DNS spoofing to direct the user to a plain `http://` connection where traffic can be intercepted, websites can use HTTP Strict Transport Security (HSTS) to instruct browsers to require an HTTPS connection for their domain at all times.

This means that an attacker that successfully spoofs DNS resolution must also create a valid HTTPS connection. This makes DNS spoofing as challenging and expensive as attacking HTTPS generally.

If the attacker spoofs DNS but doesn't compromise HTTPS, users will receive a notable warning message from their browser that will prevent them from visiting the possibly malicious site. If the site uses HSTS, there will be no option for the visitor to disregard and click through the warning.

HTTPS and HSTS work together to protect a domain against DNS spoofing.

HTTPS at NCBI: Guidance for users of NCBI Web APIs

What is happening?

To improve security and privacy, and by Federal government mandate, NCBI is moving all of its Web sites and services, including Web APIs, to HTTPS only by **September 30, 2016**.

If you use NCBI only through a Web browser (like Safari, Firefox, Chrome, Internet Explorer, Opera, etc.), **this document is not of interest to you.** The only change you should notice after the deadline is that a green lock icon should appear inside the box, and the web addresses of the NCBI pages you visit will start with `https://`.

If you maintain software that uses NCBI APIs or accesses NCBI servers through the Web, you should understand and act before the deadline to ensure uninterrupted service.

NCBI Web services include APIs such as NCBI eutilities and BLAST URLAPI that client applications use to access NCBI data. A number of them (though not a comprehensive set) are listed on or linked from our APIs page.

Applications that access NCBI web servers using http: URLs, instead of https:// URLs, may fail partially or completely after NCBI switches to HTTPS-only.

This document explains our transition plan, and provides guidance to developers about how to update their applications (scripts, server-side applications like CGIs, browser plugins, etc.), before the switchover, to prevent failure.

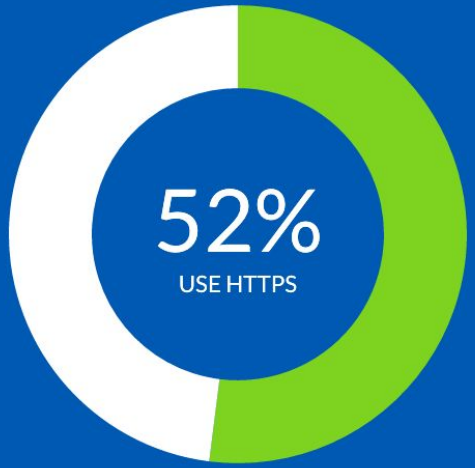
NCBI is moving all web services to HTTPS

The HTTP protocol does not provide encryption, so anyone who can see web traffic between a client (for example, a web browser) and a server can intercept potentially sensitive information, and/or inject malware into users' browsers or operating systems. HTTPS solves this problem. It works just like HTTP, except that traffic is encrypted in both directions, so observers between the client and the server can't intercept or tamper with the requests or responses. It also provides authentication, ensuring that the client is communicating with the intended server given by the hostname, and not some impostor.

The Federal Office of Management and Budget requires all Federal Web sites to switch to HTTPS-only (meaning, HTTP will be disabled) by December 31, 2016. However, NCBI, being a part of the National Library of Medicine, has an earlier deadline of September 30, 2016.

Current migration status

pulse.cio.gov



Secure HTTP (HTTPS)

Last updated August 05, 2016

This data measures whether federal domains support the HTTPS protocol (`https://`), and the strength of that support. HTTPS provides a secure connection across the internet between websites and their visitors, and is becoming the new baseline for public web services. As part of this shift, the U.S. federal government is in the process of transitioning **entirely to HTTPS**.

Note that HTTPS generally **does not affect** whether a website is vulnerable to hacking. For more information on what HTTPS does (and doesn't do), **visit the HTTPS FAQ**.

HTTPS and TLS data was last collected through a scan of the public internet on **August 05, 2016**.

pulse.cio.gov

Domain	Uses HTTPS	Enforces HTTPS	Strict Transport Security (HSTS)	SSL Labs Grade
911.gov	Yes	No	No	
abilityone.gov	No			
abmc.gov	Yes	No	No	A
access-board.gov	Yes	Yes	No	
acquisition.gov	Yes	Yes	No	
acus.gov	Yes	No	Yes, and preloaded	A-
ada.gov	Yes	Yes	Yes, and preload-ready	
adlnet.gov	Yes	Yes	No	B

Executive, legislative, judicial branches

Uses HTTPS	28% → **52%**
Enforces HTTPS	15% → **37%**
Strict Transport Security	3% → **14%**

REQUIRED

RECOMMENDED

Preloading	1% → **3%**

pulse.cio.gov, July 2015 to August 2016, ~1,150 parent .gov domains, no subdomains, federal only (all branches)

by April King

https://pokeinthe.io/2016/04/15/state-of-security-alexa-one-top-million-2016-04/

Having recently gotten the HTTP Observatory to a usable state, I decided to scan the Alexa Top 1M sites to see how well that engineers and developers on the biggest sites on the Internet are doing. As Scott found out, the results are pretty dismal. I'll be doing more detailed posts on each of these sections as I find the time, but even the basic statistics are depressing.

Content Security Policy (CSP)	.005%[1] / .012%[2]
Cookies[3]	42.05%
Cross-origin Resource Sharing (CORS)[4]	93.78%
HTTPS	29.64%
HTTP → HTTPS Redirection	5.06%[5] / 8.91%[6]
Public Key Pinning (HPKP)	0.43%
— HPKP Preloaded[7]	.414%
Strict Transport Security (HSTS)[8]	1.75%
— HSTS Preloaded[7]	.158%

HSTS

HTTP Strict Transport Security

- Agencies must make all existing websites and services accessible through a secure connection [3] (HTTPS-only, with HSTS) by December 31, 2016.
- The use of HTTPS is encouraged on intranets [4], but not explicitly required.

```
$ curl --head https://www.whitehouse.gov

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
X-Drupal-Cache: MISS
X-Content-Type-Options: nosniff
ETag: "1468905085-1"
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

Without HSTS

http://whitehouse.gov

hopefully **https://**whitehouse.gov

With HSTS

definitely **https://**whitehouse.gov

*(and whitehouse.gov **does** use HSTS, as of March 2015)*

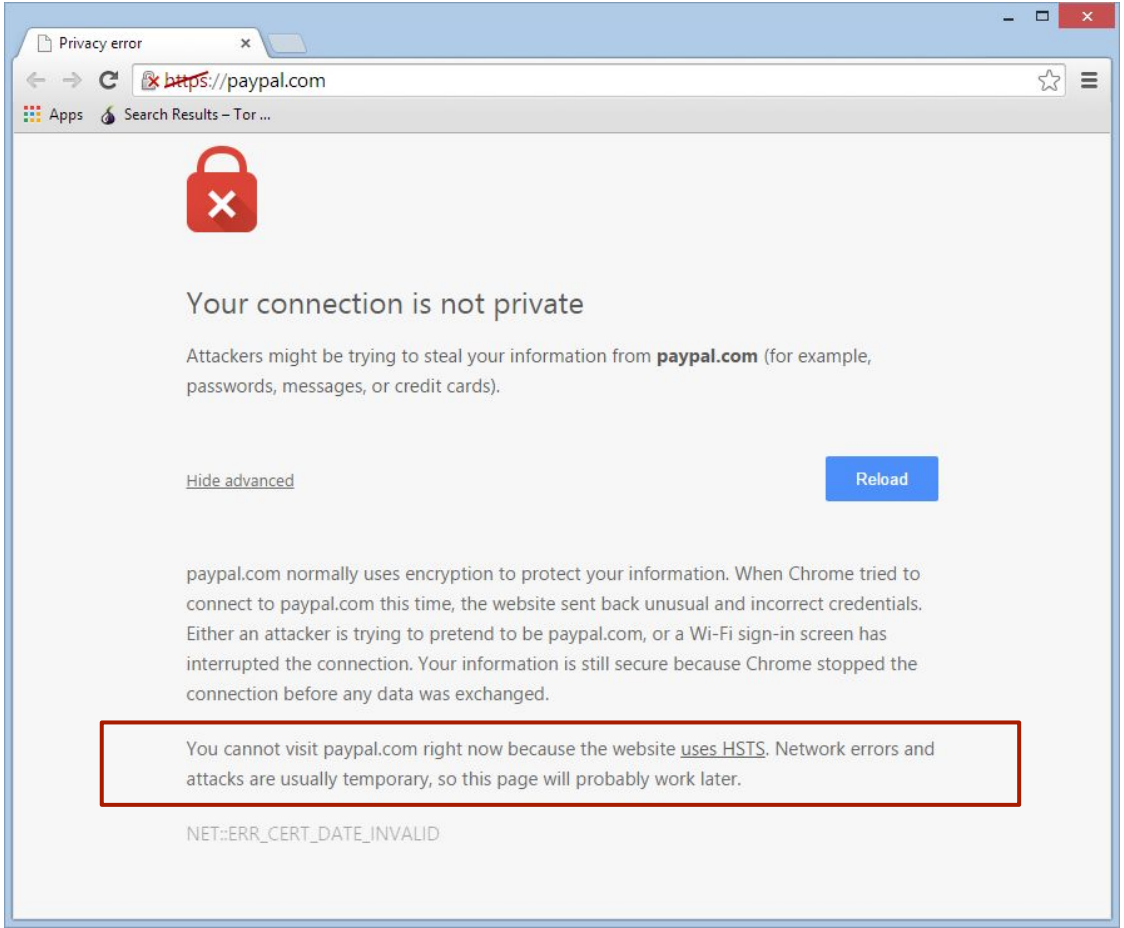
Insecure External Redirect

Name	Method	Status	Type	Initiator	Size	Time	Timeline
www.opm.gov	GET	302	text/html	Other	337 B	178 ms	
www.opm.gov	GET	200	document	http://www.opm.gov/	12.3 KB	120 ms	

Secure Internal Redirect

www.aids.gov	GET	307		Other	0 B	1 ms
www.aids.gov	GET	200	document	http://www.aids.gov/	13.9 KB	87 ms

HSTS = no clicking through certificate warnings



HSTS lets browsers actually enforce HTTPS:
the way it should have been from the beginning

The first .gov domains hardcoded into your browser as all-HTTPS

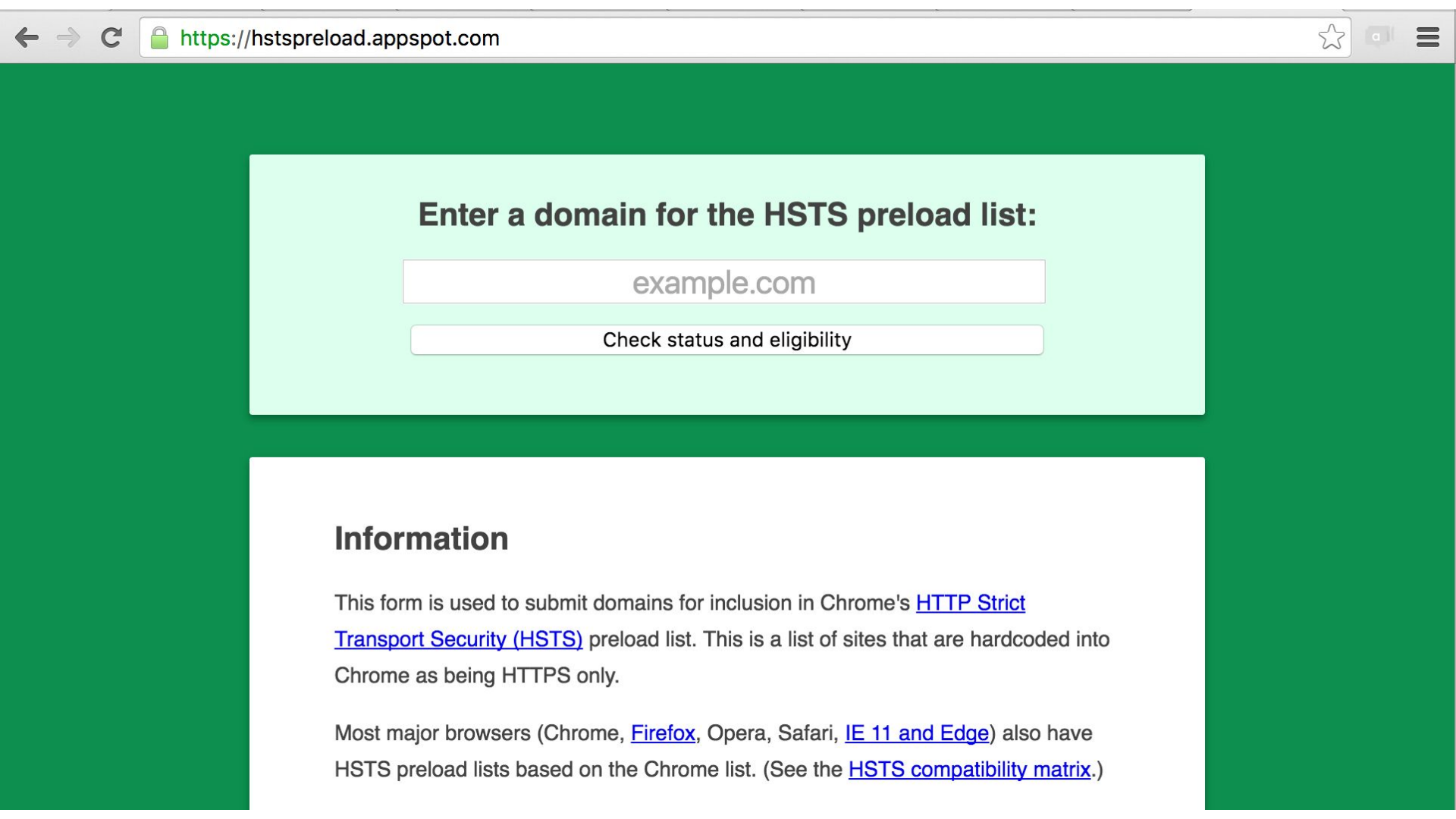
February 9, 2015

Tagged / **https** / **security** / **policy** / **hsts** /

by Eric Mill

```
1778.     { "name": "uspsoig.gov", "include_subdomains": true, "mode": "force-https" },
1779.     { "name": "notalone.gov", "include_subdomains": true, "mode": "force-https" },
1780.     { "name": "aids.gov", "include_subdomains": true, "mode": "force-https" },
1781.     { "name": "itdashboard.gov", "include_subdomains": true, "mode": "force-https" },
1782.     { "name": "paymentaccuracy.gov", "include_subdomains": true, "mode": "force-https" },
1783.     { "name": "cao.gov", "include_subdomains": true, "mode": "force-https" },
1784.     { "name": "cfo.gov", "include_subdomains": true, "mode": "force-https" },
1785.     { "name": "cio.gov", "include_subdomains": true, "mode": "force-https" },
```

Every `.gov` website, no matter how small, should give its visitors a secure, private connection. Plain HTTP (`http://`) connections are neither secure nor private, and can be easily intercepted and impersonated. In today's web browsers, the best and easiest way to fix that is to use HTTPS (`https://`).


https://hstspreload.appspot.com
Enter a domain for the HSTS preload list:
example.com
Check status and eligibility
Information
This form is used to submit domains for inclusion in Chrome's HTTP Strict Transport Security (HSTS) preload list. This is a list of sites that are hardcoded into Chrome as being HTTPS only.
Most major browsers (Chrome, Firefox, Opera, Safari, IE 11 and Edge) also have HSTS preload lists based on the Chrome list. (See the HSTS compatibility matrix.)

preloading a domain means you are done, but you need to have all of its subdomains ready for HTTPS

https://https.cio.gov/hsts/

In its simplest form, the policy tells a browser to enable HSTS for that exact domain or subdomain, and to remember it for a given number of seconds:

```
Strict-Transport-Security: max-age=31536000;
```

In its **strongest and recommended form**, the HSTS policy **includes all subdomains**, and indicates a willingness to be "preloaded" into browsers:

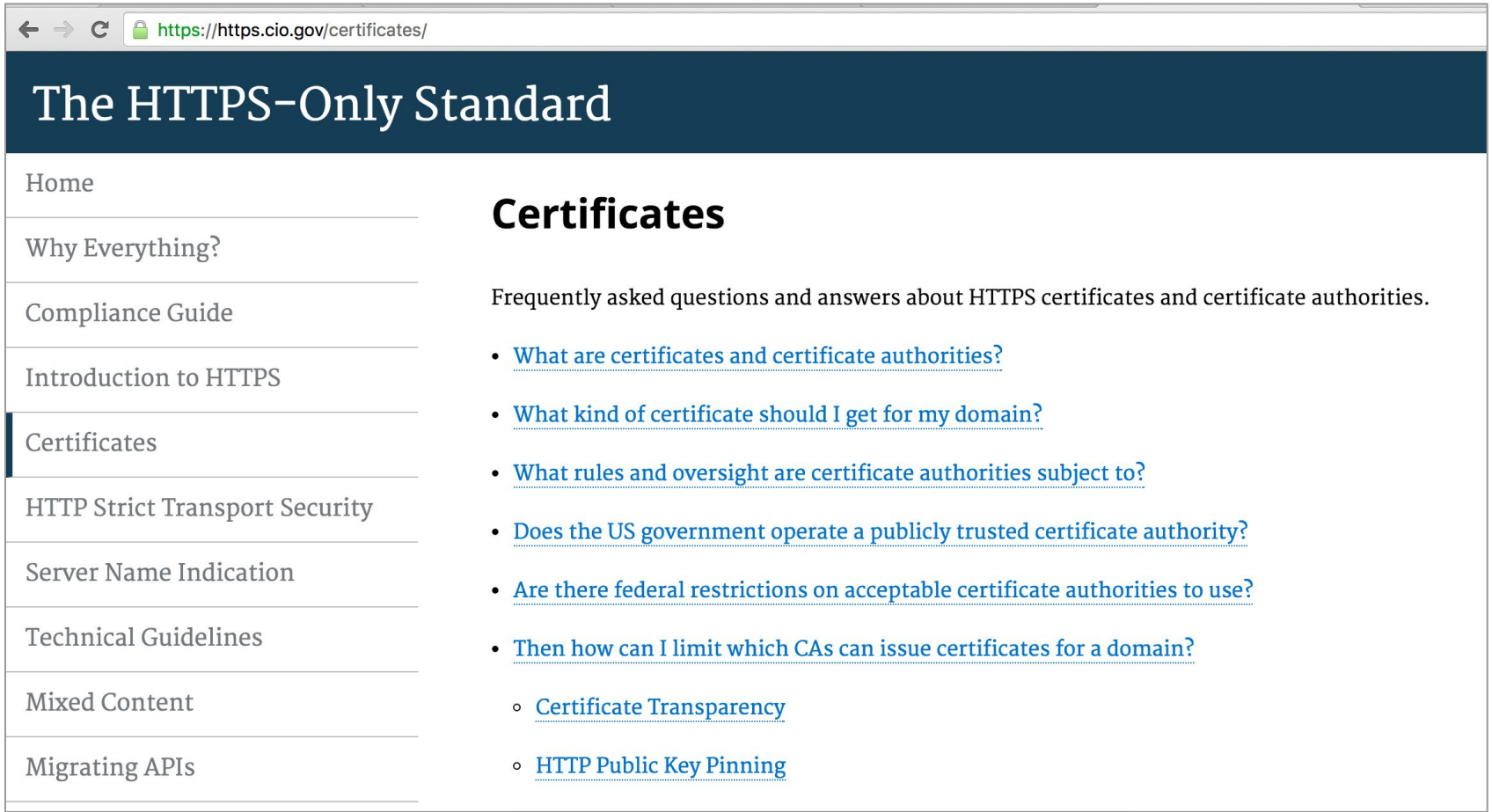
```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

When using this form, bear in mind:

- The policy should be deployed at `https://domain.gov`, *not* `https://www.domain.gov`.
- **All subdomains** associated with the parent domain must support HTTPS. (They do not have to each have their own HSTS policy.)

Certificates

https://https.cio.gov/certificates/



Certificate Validation Types

$	**Domain (DV)**	I'm 18f.gsa.gov	
$$	**Organization (OV)**	I'm also 18F at GSA	
$$$	**Extended (EV)**	I'm also the government	

DV / OV

EV

https://https.cio.gov/certificates/

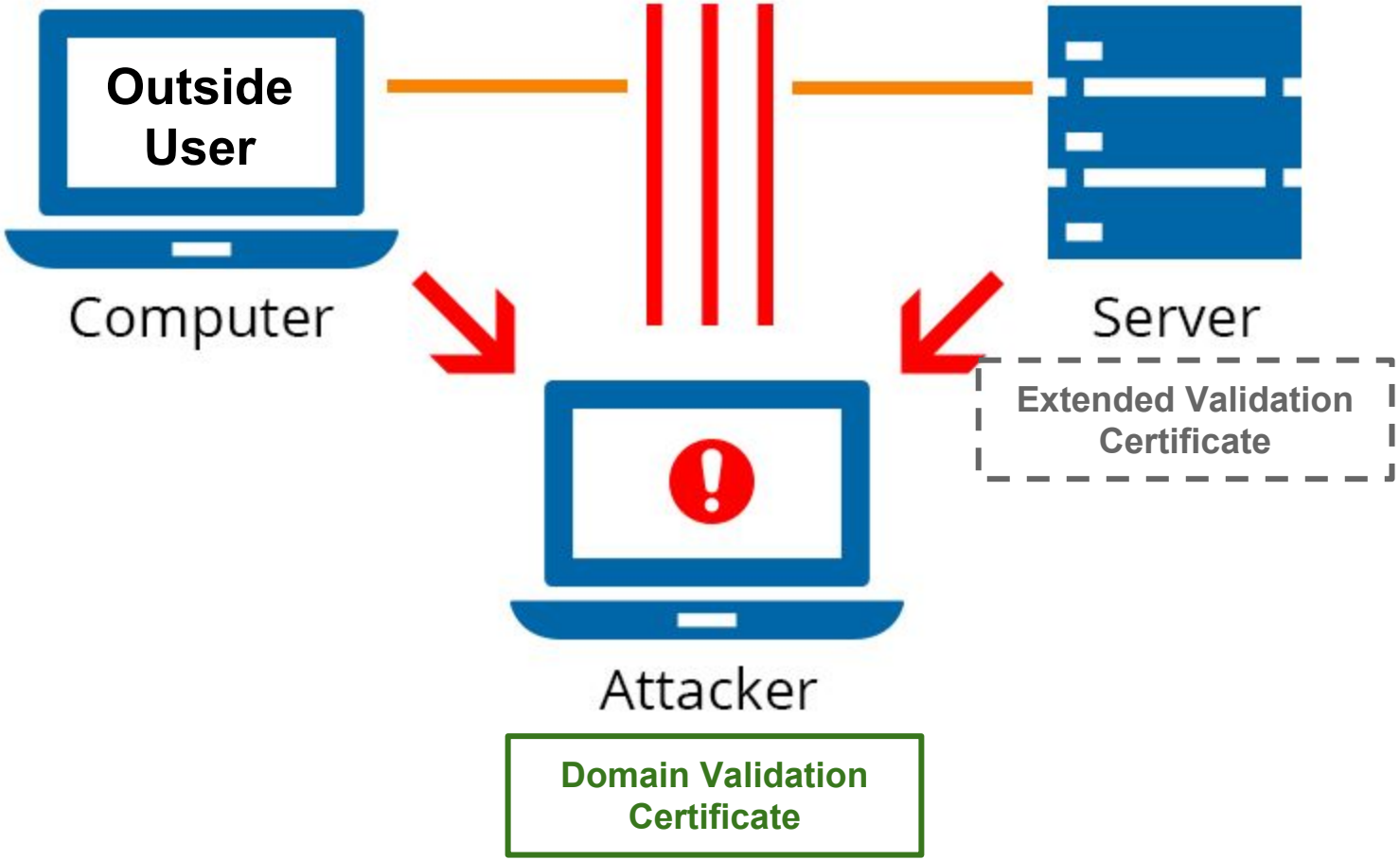
What kind of certificate should I get for my domain?

There are many kinds of certificates in use in the federal government today, and the right one may depend on a system's technical architecture or an agency's business policies.

In general:

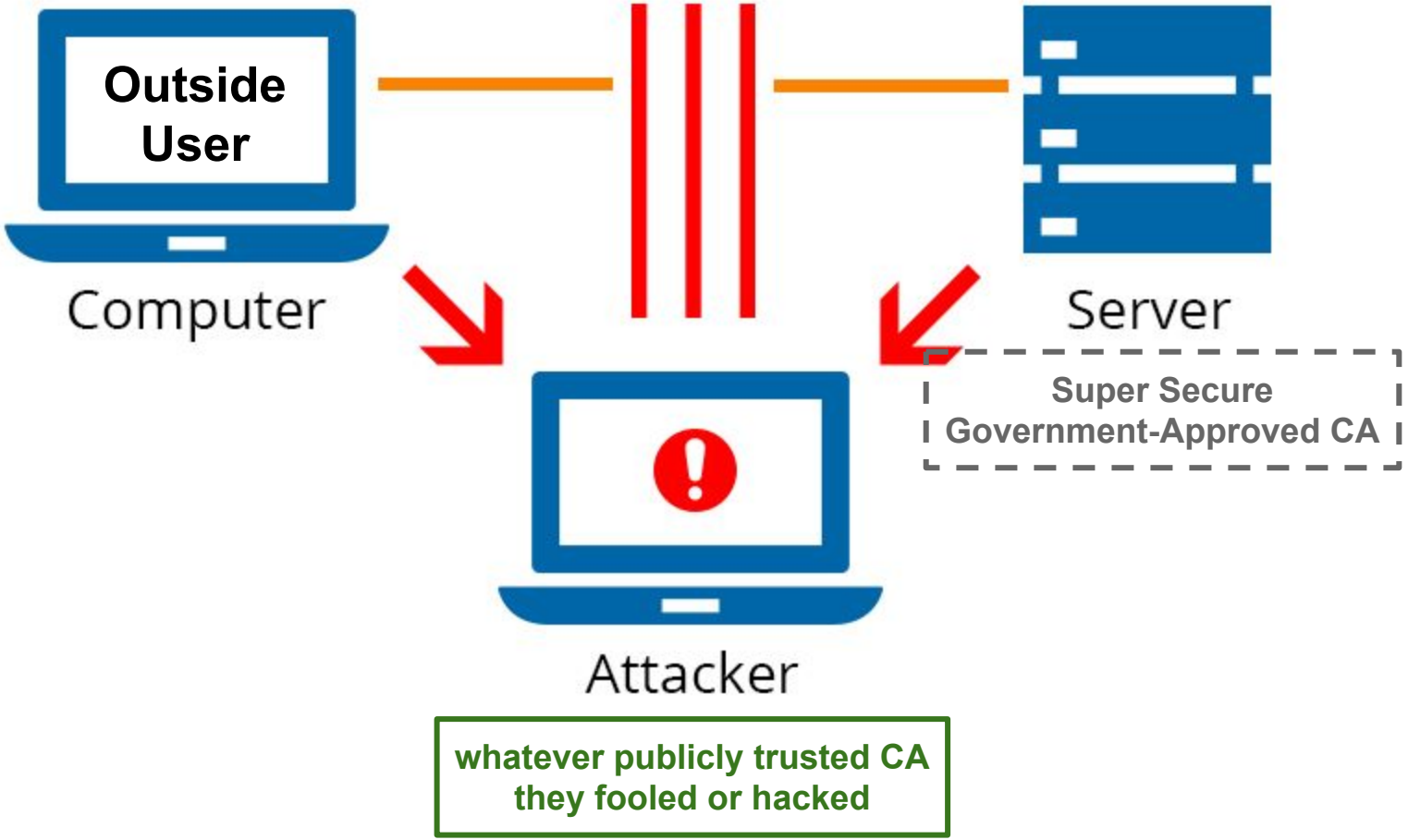
- "Domain Validation" (DV) certificates are usually less expensive and more amenable to automation than "Extended Validation" (EV) certificates. EV certificates generally result in the domain owner's name appearing in the browser URL bar visitors see. **Ordinary DV certificates are completely acceptable for government use.**
- Certificates can be valid for anywhere from years to days. In general, **shorter-lived certificates offer a better security posture**, since the impact of key compromise is less severe. Automating the issuance and renewal of certificates is an overall best practice, and can make the adoption of shorter-lived certificates more practical.

free or inexpensive
DV certificates
are completely acceptable
for government use



original image source: https://sfletter.com/?_lng=en&_action=blog-08-12-2014

policies restricting the use of certificate authorities alone have no security value for outside users



original image source: https://sfletter.com/?_lng=en&_action=blog-08-12-2014

Certificate Transparency

Certificate Transparency (CT) allows domain owners to **detect missuance of certificates after the fact**.

CT allows CAs to publish some or all of the publicly trusted certificates that they issue to one or more public logs. Multiple organizations run CT logs, and it is possible to automatically monitor the logs for any certificates that are issued for any domains of interest.

Comodo has released an open source Certificate Transparency log viewer that they operate at crt.sh. For example, it is possible to see all recent certificates for whitehouse.gov, and details of specific certificates.

The strength of Certificate Transparency increases as more CAs publish more certificates to public CT logs. Certificate Transparency is not currently a requirement for CAs – however, as the use of CT increases, so does the viability of requiring CT for publicly issued certificates.

2016-06-03	2016-06-03	search.whitehouse.gov	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2016-05-31	2016-05-31	search.whitehouse.gov	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2016-05-27	2016-05-27	search.whitehouse.gov	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2016-05-23	2016-05-23	search.whitehouse.gov	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2016-05-18	2016-05-16	11111011100.api2.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
2016-05-18	2016-05-16	11111011100.bot.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
2016-05-18	2016-05-16	11111011100.dashboard.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
2016-05-18	2016-05-16	11111011100.petitions.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
2016-05-18	2016-05-16	22222022200.dashboard.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
2016-05-18	2016-05-16	api2.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
2016-05-18	2016-05-16	correspondence.11111011100.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
2016-05-18	2016-05-16	correspondence2.11111011100.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
2016-05-18	2016-05-16	crmfra.11111011100.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
2016-05-18	2016-05-16	m.11111011100.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
2016-05-18	2016-05-16	m.22222022200.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
2016-05-18	2016-05-16	mobile.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
2016-05-18	2016-05-16	sandbox.api2.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
2016-05-18	2016-05-16	sandbox.petitions.whitehouse.gov	C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3

Early Impacts of Certificate Transparency

PROTECT THE GRAPH · MONDAY, APRIL 11, 2016

A Certificate Authority (CA) is an entity that can issue publicly-trusted certificates used for establishing secure connections over the internet. In practice, hundreds of root CA certificates are currently trusted by browsers or other web clients. These trusted CAs are expected to maintain secure processes for issuing certificates and protecting their keys because an improperly issued certificate can be used by an adversary to mount Man-in-the-Middle attacks on encrypted connections. Further, a security breach of a single CA can compromise the security of sites protected by other well-behaved CAs, as highlighted in the DigiNotar CA incident of 2011.

A key improvement to the current system is to provide the public with the ability to audit and monitor certificate issuances of the trusted CAs. Google's Certificate Transparency (CT) is one of the proposals to address this problem, defined by RFC 6962. A CT log is a public network service that provides an append-only, cryptographically-verifiable record of all the valid TLS certificates being submitted. In short, CT makes it possible to detect maliciously or mistakenly issued certificates. In 2015, we started running an experimental Certificate Transparency monitoring service to continuously check all public

Sustaining Digital Certificate Security

October 28, 2015

Posted by Ryan Sleevi, Software Engineer

This post updates our previous notification of a misissued certificate for google.com

Following our notification, Symantec published a report in response to our inquiries and disclosed that 23 test certificates had been issued without the domain owner's knowledge covering five organizations, including Google and Opera.

However, we were still able to find several more questionable certificates using only the Certificate Transparency logs and a few minutes of work. We shared these results with other root store operators on October 6th, to allow them to independently assess and verify our research.

Symantec performed another audit and, on October 12th, announced that they had found an additional 164 certificates over 76 domains and 2,458 certificates issued for domains that were never registered.

What about Federal PKI certificates?

What about Federal PKI certificates?

- The Federal PKI is working to ensure the Federal Common Policy CA is recognized by all public trust stores.

- Working on alignment of Federal Common Policy Certificate Policy requirements with the CA/Browser Forum Baseline Requirements.

- They expect the Federal Common Policy CA will be included in the Mozilla public trust store **by 2019**.

- The process may take longer or shorter depending on the result of public discussion of the Federal PKI's application.

https://https.cio.gov/guide/

What if I'm using a federally issued certificate – such as from the Federal PKI or Department of Defense – for my web service?

There are no restrictions on acceptable certificate authorities agencies might use to meet the requirements of M-15-13.

However, M-15-13 requires agencies to do more than just redirect HTTP traffic to HTTPS. It also requires agencies to enable **HTTP Strict Transport Security** (HSTS), as described above. HSTS ensures that HTTPS is always used, and protects users from several common vulnerabilities.

One important effect of HSTS is that it **disables the ability for users to click through certificate warnings** in supporting browsers. This means that **agencies cannot instruct users to click through certificate warnings** to use their web service while also complying with M-15-13.

This is also consistent with security best practices, as instructing users to click through certificate warnings defeats the point of HTTPS, and will subject users to potential network attacks.

https://https.cio.gov/guide/

In practice, to deploy HSTS while using federally issued certificates, an agency will likely need to separate its web services by hostname, based on their expected audience:

- Federally issued certificates may be practical for web services whose users can be consistently expected to trust the issuing federal certificate authority (CA). Users whose devices do not trust the issuing CA will experience a connection failure and be unable to use the web service.
- Federally issued certificates will not be practical for web services whose users may not always be expected to trust the issuing federal certificate authority. These web services will likely require the use of a certificate from a publicly trusted (commercial) CA.

Whatever strategy an agency employs to manage the use of federally issued certificates, it should allow the practical deployment of HSTS across all of its publicly accessible websites and web services.

Resources

- https://https.cio.gov ← lots of compliance and implementation guidance from GSA and OMB

- https@cio.gov ← direct email to core M-15-13 support staff

- HTTPS-HELP listserv
  - A support listserv for the migration process.
  - To subscribe, email listserv@gsa.gov with an empty subject, and a body of “**subscribe https-help**”.

President Obama Opens 'American Idol' Finale, Urges Americans to Vote

4/7/2016 by Billboard Staff

“So go to Vote.gov and register today.”

we need to make it
a plain HTTP preload list

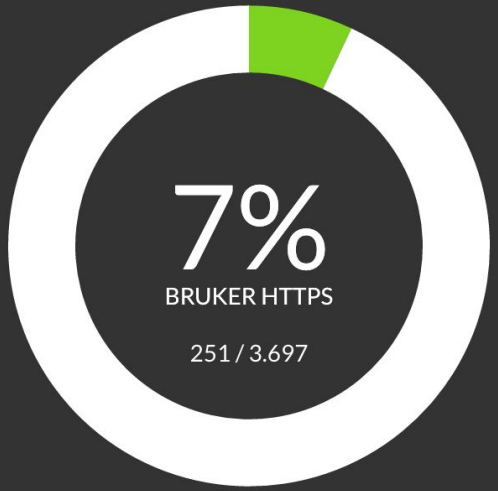
so much more HTTP left to get rid of

maybe Norway will do this

https://nrkbeta.no/2016/05/11/https-status-i-norge-oversikten/

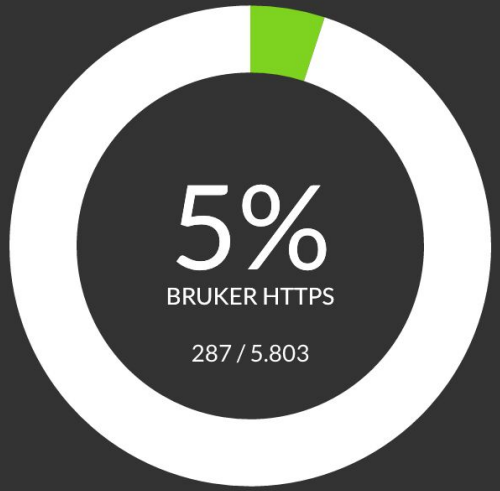
Hvor stor andel av domener eid av det offentlige i Norge bruker HTTPS?

Statlige



VIS RESULTATER

Lokale og regionale



VIS RESULTATER

DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Nasjonal sikkerhetsmyndighet
Postboks 814
1306 SANDVIKA

Nasjonal sikkerhetsmyndighet

NSM

Vår saksbehandler	Vår dato	Vår referanse
	2016-05-25	A03 - S:16/01408-2
	Deres dato	Deres referanse
	2016-04-01	16/2346 - ROKO
	Antall vedlegg	Side
		1 av 3

Oppdrag NSM - sikker tilkobling; HTTPS

Nasjonal sikkerhetsmyndighet viser til brev fra Justis- og beredskapsdepartementet av 1. april 2016 der NSM bes å vurdere bruk av sikker tilkobling for statlige webtjenester innen 6. mai 2016 (med innvilget fristutsettelse til 31. mai 2016). NSM vil i dette brevet vurdere hensiktsmessigheten av å innføre krav om sikker tilkobling for statlige webtjenester ved bruk av *Hypertext Transfer Protocol Secure* (HTTPS). Brevet omtaler også de nasjoner NSM er kjent med som har innført tilsvarende krav eller anbefalinger.

NSM har utarbeidet en rapport om bruk av HTTPS i for offentlige tjenester. Rapporten er vedlagt dette svaret i sin helhet og utdyper emnet ytterligere.

Vurdering av hensiktsmessigheten av å innføre krav om sikker tilkobling til statlige webtjenester

NSMs anbefaling

NSM mener at alle offentlige tjenester på web alltid skal benytte HTTPS. Dette vil gi både

Tilsvarende anbefalinger fra andre nasjoner

NSM er kjent med at amerikanske og tyske myndigheter har innført krav om bruk av HTTPS i offentlig forvaltning. I USA kravstilte Office of Management and Budget i memorandum av 8.

it’s time for TLDs to begin preloading

18F

Migrating .gov to HTTPS

Eric Mill, 18F/GSA