SAC057
SSAC Advisory on Internal Name Certificates

An Advisory from the ICANN Security and Stability Advisory Committee (SSAC)
15 March 2013

Preface

This is an advisory to the ICANN Board from the Security and Stability Advisory Committee (SSAC) concerning security and stability implications for internal name certificates. The SSAC advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services). The SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no official authority to regulate, enforce, or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

A list of the contributors to this advisory, references to SSAC members' biographies and statements of interest, and SSAC members' objections to the findings or recommendations in this advisory are at end of this advisory.

Table of Contents

Executive Summary

The SSAC has identified a Certificate Authority (CA) practice that, if widely exploited, could pose a significant risk to the privacy and integrity of secure Internet communications. This CA practice could impact the new gTLD program. The SSAC thus advises ICANN take immediate steps to mitigate the risks.

1. Introduction

Certificate Authorities, also known as Certification Authorities, (CAs) are organizations that issue digital certificates. These digital certificates certify the ownership of a public key by the named subject of the certificate. This allows others to rely upon signatures or assertions made by the private key that corresponds to the certified public key.

The CAs typically validate the identities of requestors before they issue certificates. For example, when Internet users browse to https://www.myicann.org/, their browsers know it is the real myicann.org because GoDaddy, a CA, has vouched the registered holder of myicann.org and issued a certificate to it. This system breaks down, however, if CAs are unable to validate the applicants they vouch for and their authority over the domain name for which the certificate is applied.

One such instance is the "Internal Name" certificate (also known as "non-fully qualified domain names" or non-FQDNs). An Internal Name certificate contains a name that is not currently resolvable using the public Domain Name System (DNS) and which is assumed to be for private use only.

An internal name is a domain or Internet Protocol (IP) address that is part of a private network. These internal names are not allocated to any specific organization and therefore cannot be verified. Common examples of internal names are:

- Any server name with a non-public domain name suffix. For example, www.company.local or server1.company.corp.
- NetBIOS names or short hostnames, anything without a public domain. For example, Web1, ExchCAS1, or Frodo.
- Any IP address in the RFC1918[1] range. These addresses are reserved for private networks only.

Internal names are not verifiable by CAs because it is not possible to look up who owns them. When determining whether a certificate application is for internal use or not, CAs often rely on the list of currently delegated Top Level Domains (TLDs) and not, for instance, against the list of the TLDs applied for in ICANN's new Generic TLD (gTLD) program. For instance, although `www.exampletld` is currently an internal name,

[1]Note: RFC 1918 is updated by RFC 6761.

`exampletld` could be an applied-for-TLD and `www.exampletld` may later become operational.

In this advisory, the SSAC examines the prevalence of internal name certificates, analyzes the security risk it imposes, and advises ICANN to take a few mitigation steps. The SSAC also wishes to highlight that although this practice has immediate impact to new gTLDs, it has larger security ramifications.

2. SSAC Preliminary Research

2.1 Empirical Analysis

The SSAC performed analysis with data from the Secure Sockets Layer (SSL) Observatory to examine the prevalence of internal name certificates and their potential for impact to ICANN's new gTLD program.

The SSL Observatory is a project sponsored by the Electronic Frontier Foundation (EFF) to investigate the certificates used to secure sites encrypted with Hypertext Transfer Protocol Secure (HTTPS) on the Web. The dataset contains all of the publicly visible SSL certificates on the Internet Protocol Version 4 (IPv4) Internet as of August 2010.[2]. The observatory data is made available as a My Structured Query Language (MySQL) database and contains 1,377,067 unique valid certificates signed by 1,482 certificate authorities.

The SSAC notes that in the EFF dataset, the term "certificate authorities" means roots and intermediate authorities used to issue certificates. So, although many of these are controlled by the same organization, the EFF dataset treats them as different entities. In reality, there are about 70 organizations that control the issuance of these certificates.

According to security researchers,[3] in total there are 37,244 internal name certificates issued by 157 CAs, 2.7 percent of all the public certificates available in the SSL repository. The top 10 certificate authorities that issue internal name certificates are:

Table 1: Top 10 Issuers of internal name certificates. Data Source: SSL Observatory

Number of non-FQDN certs issued	Issuer
11615	Go Daddy Secure Certification
6663	Positive SSL CA
4807	DigiCert Hi Assurance CA-3
1967	Starfield Secure Certification Authority
1731	AAA Certificate Services

[2]See The EFF SSL Observatory Project at: https://www.eff.org/observatory.
[3]See https://www.eff.org/deeplinks/2011/04/unqualified-names-ssl-observatory.

1520	DigiCert Global CA
1155	USERTrust Legacy Secure Server CA
930	GlobalSign Domain Validation CA
889	Equifax Secure Certificate Authority
799	Entrust Certification Authority

The SSAC queried the SSL observatory for internal name certificates that ends in an applied for TLD string. There are 1,053 such certificates that end in 63 applied-for TLD strings. Among those, 210 have not expired and are therefore still valid and working.

In the following example, we show a valid internal name certificate that conflicts with an applied for gTLD, .corp.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:02:c2:90:e4:43:22
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc.,
OU=http://certificates.godaddy.com/repository, CN=Go Daddy Secure
Certification Authority/serialNumber=07969287
        Validity
            Not Before: Dec 22 10:07:40 2009 GMT
            Not After : Jan  8 22:08:22 2013 GMT
        Subject: O=webmail.quiksilver.com.au, OU=Domain Control
Validated, CN=webmail.quiksilver.com.au
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)

            X509v3 Subject Alternative Name:
                DNS:webmail.quiksilver.com.au,
DNS:www.webmail.quiksilver.com.au, DNS:owa.quiksilver.com.au,
DNS:autodiscover.quiksilver.com.au, DNS:webmail.dcshoes.com.au,
DNS:webmail.dcaus.com, DNS:qsauhub01,
DNS:qsauhub01.sea.quiksilver.corp, DNS:qsauhub02,
DNS:qsauhub02.sea.quiksilver.corp, DNS:autodiscover.sea.quiksilver.corp
```

Figure 1: A certificate that has internal names that end in an applied for TLD string.

The above certificate was issued to webmail.quiksilver.com.au. However, it is also valid for qsauhub01, qsauhub01.sea.quiksilver.corp, qsauhub02, qsauhub02.sea.quiksilver.corp, and autodiscover.sea.quiksilver.corp.

This is due to a known feature called "Subject Alternative Names" in X.509 certificates. A Subject Alternative Name is an attribute that lists an alternate name for the subject of the certificate. In a web context that subject is the hostname. This functionality provides SSL-secured communication for servers using multiple domain names and host names – within a single SSL certificate. In the example above, the certificate is also valid for qsauhub01.sea.quiksilver.corp, qsauhub02.sea.quiksilver.corp, and autodiscover.sea.quiksilver.corp, all of which end in the applied for TLD string "corp".

Limitation of the empirical analysis: The SSAC notes that, due to the following reasons, the above analysis could *significantly* undercount the number of internal name certificates that collide with ICANN's applied-for-TLD string.

1) The SSL observatory database only contains publicly available certificates on the IPv4 network. Its methodology is not capable of discovering internal certificates that are not associated with a public certificate. Since the key purpose for internal name certificates is for internal use, it is highly likely that many internal certificates are unaccounted for.

2) It is also possible that the SSL observatory is not scanning ports typically used with mail servers. Many certificates with internal server names are used to secure these systems, therefore undercounting the number of such certificates.

3) The dataset is from 2010.

2.2 Case Study

The SSL observatory data dates back to 2010. To examine whether it is still possible today to register internal name certificates, an SSAC member tried to obtain an internal name certificate (www.site) that ends in an applied for TLD string (.site) in the fourth quarter of 2012. This section outlines the steps he took to obtain the certificate.

Step 1: Request – The researcher created a certificate-signing request (CSR) for www.site. Additional details of the request are listed below.

```
Data:
Version: 0 (0x0)
Subject: C=US, ST=XX, L=XXXX,
O=XXXXXX,
OU=IT - Internal WWW Site.,
CN=www.site/emailAddress=XXXX@XXXX.net
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:da:ef:bd:d0:ee:db:.. (omitted)
```

Figure 2: Certificate Request for www.site. "SITE" is currently an applied for TLD in ICANN's new gTLD program. The contact information of the requester is redacted for privacy purposes.

Step 2: Interaction with the CA – The CA detected that www.site is not a fully qualified domain name, and asked the requester to confirm it is intended for internal use.

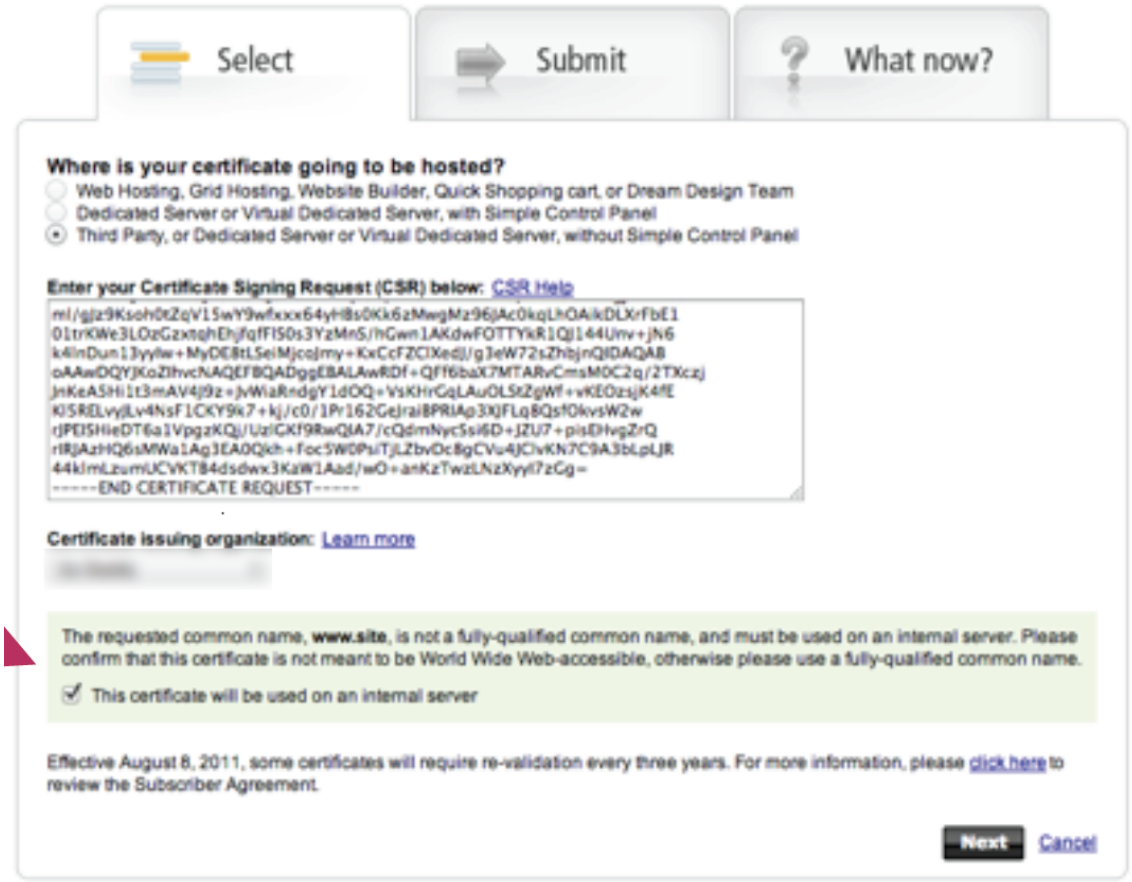


Figure 3: Interaction with CA. The boxed content says, "The requested common name, www.site, is not a fully-qualified common name, and must be used on an internal server. Please confirm that this certificate is not meant to be World Wide Web-accessible, otherwise please use a fully qualified common name. [check box] This certificate will be used on an internal server.

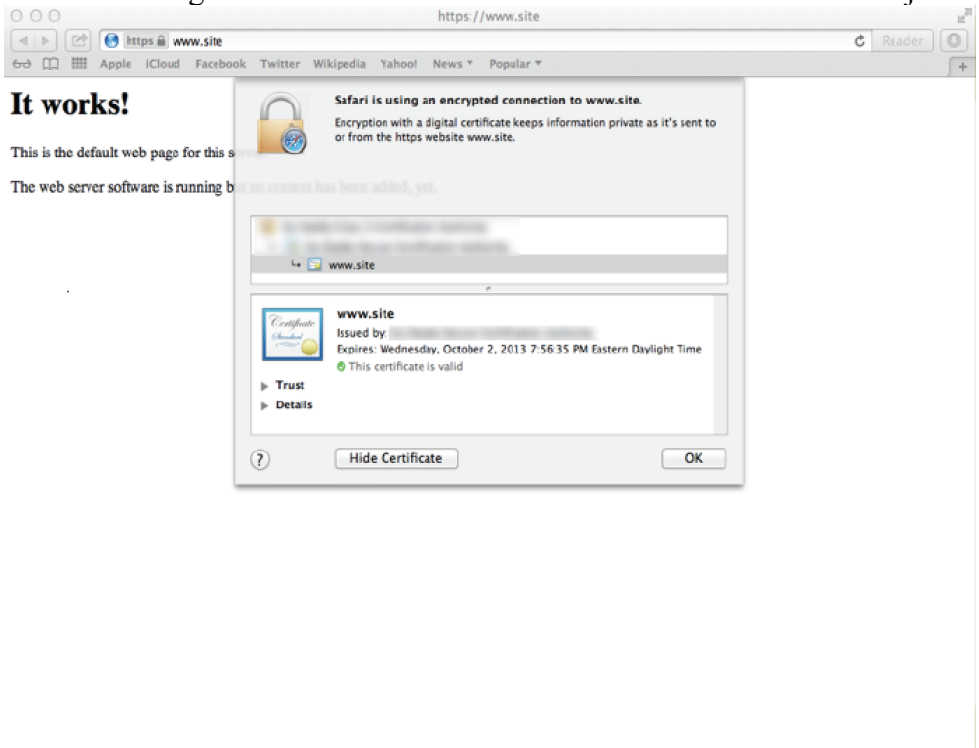
Step 3: Certificate Issued – After the researcher confirmed that he understood that this is for internal use the CA issued a certificate valid for one year. Additional details of the certificate are listed below.

```
Version: 3 (0x2)
Serial Number: 27:e7:22:63:59:11:b0
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, ST=XXX, L=XXX, O=XXX, OU=XXX,
CN=XXX/serialNumber=XXXXXXXX
Validity
Not Before: Oct 2 23:56:35 2012 GMT
Not After : Oct 2 23:56:35 2013 GMT
Subject: O=www.site, OU=Domain Control Validated,
CN=www.site
X509v3 Subject Alternative Name:
DNS:www.site, DNS:site
```

Figure 4: Certificate issued by the CA. The name of the CA is redacted for security reasons.

Step 4: Verification – The SSAC member set up www.site[4] and verified that various

Browsers recognize the certificate. Below is a screenshot from one major browser.



[4]Using a "fake" / local root with .site delegated.

3. Findings

Based on the preliminary research above, the SSAC offers the following findings.

Finding 1: The SSL observatory data shows that at least 157 CAs have issued internal name certificates. If these practices do not change, any of them could issue certificates that end in an applied for new gTLD. Our case study shows that as of this writing this is possible with at least one CA.

Finding 2: The exact number of internal name certificates that end in an applied for new gTLD cannot be known unless CAs voluntarily disclose the list.

The SSL observatory database only contains certificates that were publicly visible (could be found by probing port 443 from the Internet). There could be many certificates issued that are only used internally and would not have been visible to the SSL observatory project. Thus there is no way of knowing how many of those certificates exist unless certificate authorities voluntarily disclose them.

Finding 3: Enterprises use internal name certificates for a variety of reasons.

According QuoVadis Group, a certificate authority, one use case for internal name certificate is for convenience:

> As a convenience for users, many servers in corporate networks are reachable by local names such as "mail", "wiki" or "hr". Most publicly trusted certificates for non-unique names are deployed in the context of local networks to enable trust in these local names without the additional cost of provisioning a new trust root to clients. This may be especially desirable for networks lacking centralized policy deployment and management tools, such as "Bring Your Own Device" environments.[5]

As shown in our empirical analysis, there are at least 37,000 internal name certificates used in thousands of enterprises. Although this practice *might* make sense in the previous two autonomous systems (DNS and CAs), with the introduction of new gTLDs, namespace collisions and other man-in-the-middle attacks (see Finding 4) will become more apparent. In addition, because many of the applied for TLDs are common, generic terms the risk of collisions increases.

---

[5]See QuoVadis Group. 2012. Internal Server Names and IP Address Requirements for SSL at: https://support.quovadisglobal.com/AvatarHandler.ashx?radfile=%2fCommon%2fSSL+General+Topics+%28KB%29%2fQV_DeprecatedCertsGuidance_v2.pdf.

Finding 4: The practice for issuing internal name certificates allows a person, not related to an applied for TLD, to obtain a certificate for the TLD with little or no validation, and launch a man-in-the-middle attack more effectively.

If an attacker obtains a certificate before the new TLD is delegated, he/she could surreptitiously redirect a user from the original site to the attacker site, present his certificate and the victim would get the Transport Layer Security/SSL (TLS/SSL) lock icon. This poses a significant risk to the privacy and integrity of HTTPS communications as well as other protocols that use X.509 certificates (e.g. TLS/SSL-based email communication).

To date, at least two security researchers have confirmed this is possible. In both cases, they were able to obtain certificates for applied-for new gTLDs.

Finding 5: The CA / Browser (CA/B) forum is aware of this issue and requests its members to stop this practice by October 2016. The vulnerability window to new gTLDs is at least 3 years.

In the "Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates" that went into effect on 1 July 2012, the CA/B forum states that:

> As of the Effective Date [1 July 2012] of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name, the CA SHALL notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. Also as of the Effective Date [1 July 2012], the CA SHALL NOT issue a certificate with an Expiry Date later than 1 November 2015 with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name. Effective 1 October 2016, CAs SHALL revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Server Name.[6]

Although this is welcome news, this is still *problematic* because ICANN plans to delegate new TLDs in 2013, introducing vulnerability for potential new gTLDs until October 2016.

[6]CA/Browser Forum. Baseline Requirements for the Issurance and Management of Publicly-Trusted Certificates, v. 1.0. 22 November 2012. Available at: https://www.cabforum.org/Baseline_Requirements_V1.pdf.

4. Recommendation

Recommendation: The ICANN Security Team should immediately develop and execute a risk mitigation plan.

The mitigation plan should include at least:

- Outreach to the CA/B forum[7] and CAs, requesting that they treat applied for new gTLDs as if they were delegated TLDs as soon as possible, as well as discussing the broader implications and mitigation steps.

  In doing so, ICANN should seek to create trust relationships between ICANN and CA/B Forum and CAs. Because of the potential for collateral harm to users if disclosure is made public before mitigation is effected, the SSAC believes it is important to conduct correspondence confidentially.

- A Disclosure Policy as informed by industry best practices for vulnerability disclosure (e.g. CERT / CC vulnerability disclosure.[8] Such a policy should take into consideration that once the disclosure is public, it is trivial to exploit the vulnerability.

- A communication plan on informing affected parties as determined by the disclosure policy.

- A contingency plan to be executed if the vulnerability is leaked to the public prematurely, as well as a proactive vulnerability disclosure plan.

5. Acknowledgments, Statements of Interests, and Objections and Withdrawals

In the interest of greater transparency, these sections provide information on three aspects of our process. The Acknowledgments section lists the members who contributed to this particular document. The Statements of Interest section points to the biographies of the Committee members and any conflicts of interest, real, apparent or potential, that may bear on the material in this document. The Objections and Withdrawals section provides a place for individual members to disagree with the content of this document or the process for preparing it.

[7]See Certificate Authority / Browser Forum: https://www.cabforum.org. As of the publication of this advisory the outreach is already in progress.

[8]See CERT/CC. CERT/CC Vulnerability Disclosure Policy at: http://www.cert.org/kb/vul_disclosure.html.

5.1 Acknowledgments

The committee wishes to thank the following SSAC members and external experts for their time, contributions, and review in producing this advisory.

SSAC members

Steve Crocker
Patrik Fältström
Ondrej Filip
James Galvin
Warren Kumari
Danny McPherson
Ram Mohan
Doron Shikmoni

ICANN staff

Jeff Moss
Dave Piscitello
Barbara Roseman
Steve Sheng (editor)

During the production of this advisory, the SSAC reached out to the certificate authority community to get feedback. For their time and contributions during this outreach process, the SSAC wants to specifically thank the following persons/organizations:

Certificate Authority Browser Forum (CA/B Forum)
Certificate Authority Security Council (CASC)
Ben Wilson (Digicert)
Jeremy Rowley (Digicert)

5.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: http://www.icann.org/en/groups/ssac/biographies-01feb13-en.htm..

5.3 Objections and Withdrawals

There were no objections or withdrawals.

Appendix A: SSAC Publication of This Advisory and Chronology of Mitigation

Due to the sensitive nature of this issue, the SSAC did not follow its customary publication procedures; instead, the SSAC delivered an interim advisory to the ICANN Security Team. The ICANN Security Team took immediate action. This section, jointly contributed by the ICANN Security Team, provides a chronology of events related to the mitigation of this risk as of the time of publication of this advisory.

SSAC Advisory Formation: During its annual workshop on 14 – 16 November 2012, a SSAC member presented to the SSAC the process he used to register an internal name certificate that ended in an applied-for-gTLD string. Recognizing the seriousness of this issue, the SSAC formed a work party to develop some advice for ICANN. The work party met weekly from 30 November to 17 December and produced a first draft of this advisory.

On 8 January 2013, a briefing call was conducted between SSAC work party members and staff from ICANN's Security Team and Legal Department. During that call, ICANN agreed to start preparing mitigation options in anticipation of the SSAC advisory.

On 19 January 2013, the SSAC work party finished its work on the internal name certificate advisory, and sent the advisory for full SSAC review.

On 28 January 2013. The SSAC completed the review of the advisory. During the SSAC deliberation, the best path of disclosure became an issue of active discussion. It was apparent that 1) this information is not widely exploited yet, and if leaked could lead to security attacks, 2) no means to mitigate the problem exist at this time. Thus the SSAC decided to send the advisory to the ICANN Security Team first to give them an opportunity to act on the mitigation plan recommendation, and requested ICANN keep this advisory confidential until otherwise directed by the ICANN Chief Security Officer. The Chief Security Officer (or his/her authorized delegate) would approve and record selected release of the advisory to appropriate individuals and would judge when confidentiality is no longer warranted, informed by the recommended mitigation plan.

On 31 January 2013, the SSAC submitted the advisory to the ICANN Security Team.

ICANN and CA/Browser Coordinated Mitigation: Shortly after 8 January briefing, ICANN formed a risk mitigation team composed of staff from policy, security, new gTLD and DNS industry engagement. The team held regular meetings to plan the mitigations.

On 23 January 2013, the ICANN Security Team scheduled a preliminary teleconference with the Certificate Authority and Browser Forum (CA/B) Chairperson to alert him of this issue. Recognizing the seriousness of this issue, the chairperson invited ICANN to brief the CA/B forum members in its upcoming annual meeting.

On 5 February 2013, ICANN presented the SSAC advisory to the CA/B Forum annual meeting and re-iterated its commitment to work with CAs and Browsers to address this issue. As a result of this meeting, the CA/B Forum advanced Ballot 96 on new gTLDs. The ballot called for CAs to stop issuing certificates that end in an applied-for-gTLD string within 30 days of ICANN signing the contract with the registry operator, and revoke any existing certificates within 120 days of ICANN signing the contract with the registry operator *[NOTE: the original CA timeline for not issuing internal name certificates was 1 July 2015, with revocation starting on 1 October 2016]*. The full text of the ballot is included as Appendix B to this document. The voting period for this ballot started at 21:00 UTC on 13 February 2013 and closed at 21:00 UTC on 20 February 2013.

Responding to some questions on the ballot, on 15 February 2013 ICANN provided the following statement to the CA/B Forum:

> "All current registry agreements are published at the following URL: https://www.icann.org/en/about/agreements/registries. New gTLD registry agreements will be published to this page as they become available. In addition, ICANN plans to implement a notification or web feed for the items on this page. If this URL should change, ICANN will notify visiting users of the new location of the registry agreements.
>
> ICANN is willing to work with the CA/B forum, and other interested parties, to understand additional notification needs."

On 20 February 2013, the CA/B Forum passed Ballot 96 (Wildcard certificates and new gTLDs) with 14 in favor, 2 opposed, and 4 abstentions.

On 12 March 2013, the SSAC finalized its advisory based on the mitigations and additional input provided by the Certificate Authority Security Council.

The SSAC commends the ICANN security team and CA/B forum for its timely attention and mitigation of this risk, and requests ICANN to continue work with CAs, browser developers and other relevant parties to further mitigate the risk.

Appendix B: CA/B Forum Ballot 96

... Motion Begins ...

... Erratum Begins ...

Add the following as new Section 11.1.3:

11.1 Authorization by Domain Name Registrant

11.1.3 Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, the CA MUST establish and follow a documented procedure† that determines if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation).

If a wildcard would fall within the label immediately to the left of a registry-controlled† or public suffix, CAs MUST refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace. (e.g. CAs MUST NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.).

Prior to September 1, 2013, each CA MUST revoke any valid certificate that does not comply with this section of the Requirements.

†Determination of what is "registry-controlled" versus the registerable portion of a Country Code Top-Level Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. Current best practice is to consult a "public suffix list" such as http://publicsuffix.org/. If the process for making this determination is standardized by an RFC, then such a procedure SHOULD be preferred.

Add the following as new Section 11.1.4:

11.1.4 New gTLD Domains

CAs SHOULD NOT issue Certificates containing a new gTLD under consideration by ICANN. Prior to issuing a Certificate containing an Internal Server Name with a gTLD that ICANN has announced as under consideration to make operational, the CA MUST provide a warning to the applicant that the gTLD may soon become resolvable and that, at that time, the CA will revoke the Certificate unless the applicant promptly registers the domain name.

Within 30 days after ICANN has approved a new gTLD for operation, as evidenced by publication of a contract with the gTLD operator on [www.icann.org] each CA MUST (1) compare the new gTLD against the CA's records of valid certificates and (2) cease issuing Certificates containing a Domain Name that includes the new gTLD until after

the CA has first verified the Subscriber's control over or exclusive right to use the Domain Name in accordance with Section 11.1.

Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], CAs MUST revoke each Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name.

... Erratum Ends ...

The review period for this ballot shall commence at 21:00 UTC on 6 February 2013 and will close at 21:00 UTC on 13 February 2013. Unless the motion is withdrawn during the review period, the voting period will start immediately thereafter and will close at 21:00 UTC on 20 February 2013. Votes must be cast by posting an on-list reply to this thread.

... Motions ends ...