WHITE PAPER:

New gTLDs and their impact on your SSL Certificates

digicert®

YOUR SUCCESS IS BUILT ON TRUST®

In June 2011, ICANN (Internet Corporation for Assigned Names and Numbers), the organization that coordinates the Internet naming system, announced a new generic Top-Level Domain (gTLD) Program. This program permitted individuals, organizations, and governments to apply for new top level namespaces. Prior to this decision, ICANN has only recognized about two dozen generic Top-Level Domains (TLDs) such as .com, .net, and .org, along with many country-specific TLDs known as ccTLDs (country code Top-Level Domains).

The new program opened the path for the potential addition of hundreds, if not thousands, of new TLDs, which will impact how companies are able to configure their networks and domains. Once these new domains are resolvable in the DNS, networks using previously unregisterable extensions (internal names), such as .corp or .email, will likely experience problems with system confusion and be exposed to potential Man-in-the-Middle exploits.

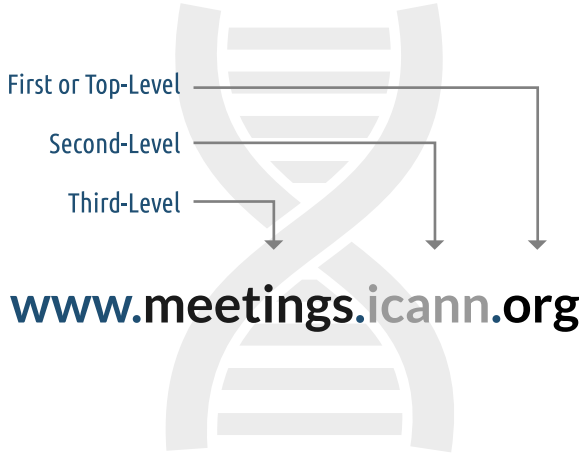
To help limit potential attacks, the Certification Authority/Browser Forum (CA/B Forum) has agreed with ICANN to require CAs to revoke all existing SSL Certificates for containing an approved new gTLD within 120 days of publication of the contract between ICANN and the gTLD applicant. DigiCert has gone a step further and created a complimentary Internal Name Tool for Microsoft Exchange to help administrators reconfigure their network and avoid potential collisions.

http://www.digicert.com/internal-domain-name-tool.htm

TERMS TO KNOW

- **CA/B Forum**: Certificate Authority/Browser Forum
- **CA**: Certificate Authority
- **ccTLDs**: Country Code Top-Level Domains, such as .CA, .FR, and .UK
- **DNS**: Domain Name System
- **gTLDs**: generic Top-Level Domains, such as .COM, .NET, .ORG, and .BIZ
- **ICANN**: Internet Corporation for Assigned Names and Numbers
- **SCP**: Service Connection Point
- **TLDs**: Top-Level Domains
- **TMCH**: Trademark Clearinghouse

ANATOMY OF A DOMAIN NAME



BACKGROUND

In the past, domain owners had the ability to use a wide assortment of non-registered TLDs for internal sites across their networks. Using names such as .corp, .dev, .mail, and .site on internal servers was a widely accepted practice. If ICANN approves these names as new TLDs, the names will become resolvable in the DNS. The Security Advisory Committee which advises ICANN on security related matters reports that internal names make up 10% of the queries that reach the DNS root servers." [1]

Certification authorities issuing publicly trusted certificates are required by industry standards to verify that the certificate applicant owns or controls the domain names specified in the certificate request. Once these names are resolvable, certification authorities will not be permitted to issue certificates trusted by browsers that contain these new gTLDs. Existing certificates with affected names will be also be revoked, and a new certificate will only be available to the verifiable domain owner or operator.

The number of impacted networks and certificates will slowly expand as additional TLDs are approved by ICANN, accelerating the gradual phasing out of SSL Certificates for internal names previously set by the CA/B Forum. In November 2011, the CA/B Forum set a hard end date in October 2016, after which certificates using internal names would be revoked. A multi-year phase-out schedule was established to give organizations time to plan for the changes. To learn more about this requirement, visit:

http://www.digicert.com/internal-names.htm

WHY IS ICANN ADDING NEW gTLDs?

ICANN has stated that they are adding additional TLDs to promote competition in the domain name market. New generic Top-Level Domains (gTLDs) will theoretically increase consumer choice through greater competition among registry service providers. Although registration for new

gTLDs is currently closed, ICANN has indicated that they may make registration available again in the near future.[2]

WHAT HAPPENS IF .CORP IS ACCEPTED AS A TLD?

PayPal has warned of potential disruption to the stability of the Internet if certain TLDs are approved by ICANN.

"Consider a typical enterprise laptop configured to look for network services ending in '.corp.' What happens when that system roams to a public network, such as the user's home or a public WiFi hotspot? Potentially dozens of services may attempt to resolve their endpoints and reconnect, including:

- Browser bookmarks, homes pages and saved tabs
- Email client
- Chat clients
- File synchronization services
- Administrative policy services and agents
- Directory services

Most of these services use stored authenticators or credentials, and authenticate their server endpoint using HTTPS, accepting any certificate that chains to a trusted root. If the recipient of an ICANN delegation '.corp' set up, for example, wildcard records and buys a legitimate wildcard certificate, that organization will find itself bombarded with sensitive data from such clients, including:

- Usernames and passwords in plaintext
- NTLM authentication blobs subject to forwarding attacks
- Kerberos tokens with bearer semantics
- HTTP cookies

If the appropriate service endpoints are available, these clients will next begin to dump confidential data and potentially pull incorrect information and apply damaging state changes. The potential for malicious abuse is extraordinary, the incidental damage will be large even in the absence of malicious intent, and such services will become immediate targets of attack as they inadvertently collect high-value credentials and private data from potentially millions of systems."[3]

WHAT DOES THIS MEAN FOR YOU?

As a website owner, you now have a wide range of Top-Level Domains to consider when purchasing new domain names. With TLDs tailored to specific industries and interests, it is now easier to find just the right domain name, especially in namespaces that formerly had fierce competition.

On the downside, if you have a network or SSL Certificates that uses an approved gTLD, you will need to either quickly register the corresponding domain names or re-configure your network to use a different name. Although industry guidelines provide a 120 day window for revocation after a contract is signed, because of significant security risks, many CAs may immediately revoke SSL certificates that contain an approved name.

Unified Communications certificate users will experience the greatest impact by the new gTLDs since use of internal names in these systems is common. Fortunately, DigiCert has created a complimentary Internal Name Tool for Microsoft Exchange that provides an easy way for you to reconfigure Exchange's Autodiscover service and SCPs to use public names on your network.

To download the tool, please visit:
www.digicert.com/internal-domain-name-tool.htm

WHICH NEW gTLDs WILL BE APPROVED?

Despite costing $185,000 each, approximately 2,000 new gTLDs have been applied for to date. Some of the popular server names that could get approved as TLDs include:

.ads	.dev	.new
.app	.email	.prod
.bank	.home	.search
.blog	.mail	.services
.cloud	.mobile	.site
.corp	.network	.web

For a comprehensive list, view the list of requested names here.

We're here to help

For over a decade DigiCert has been providing SSL Certificates to the top ecommerce websites around the globe. Over 70,000 customers in 146 countries, including half of the Alexa U.S. Top Ten websites, rely on DigiCert to secure their sites. With unmatched issuance speed, 2048-bit encryption, award-winning customer support, and countless product innovations, it's no wonder that DigiCert is the fastest-growing high-assurance Certificate Authority in the world.

If you are unsure whether your current SSL Certificates are going to be affected by this change, you are welcome to contact DigiCert's support team by phone at +1-801-701-9600, support@digicert.com, or via live chat. While we don't have any control over what new domains get approved by ICANN, we can help you navigate your way through these changes to your SSL Certificates.

CORPORATE HEADQUARTERS
2600 West Executive Parkway Suite #500
Lehi, Utah 84043

TECHNICAL SUPPORT
support@digicert.com
Direct Phone: 1-801-701-9600
Spanish: 1-801-701-9601
Spanish Website: www.digicert.com/es/

TELEPHONE & FAX
Toll Free: 1-800-896-7973
Fax: 1-801-705-0481
Media & PR: 1-801-877-2123

EMAIL
Sales & Marketing: sales@digicert.com
Corporate Office: admin@digicert.com
Enterprise/Managed PKI: enterprise@digicert.com
Partner Information: channel@digicert.com

www.digicert.com
www.facebook.com/digicert
www.twitter.com/digicert (@digicert)
http://www.digicert.com/newsroom.htm
support@digicert.com

(1) www.icann.org/en/groups/ssac/documents/sac-045-en.pdf
(2) http://newgtlds.icann.org/en/about/benefits-risks
(3) http://forum.icann.org/lists/bc-gnso/pdfNFDozNA9Ka.pdf

Additional references:

http://www.digicert.com/internal-names.htm
http://www.digicert.com/new-generic-top-level-domains.htm
gTLD Applicant Guidebook, Version 2012-06-04