How to Leverage an fTLD Domain:

EXECUTIVE GUIDE TO SECURITY REQUIREMENTS

fTLD
Registry Services, LLC

TABLE OF CONTENTS

EXECUTIVE GUIDE TO SECURITY REQUIREMENTS

INTRODUCTION

The fTLD Registry Services' ("fTLD") Executive Guide to Security Requirements (the "Requirements") is designed for chief information, technology and information security officers (i.e., CIOs/CTOs/CISOs) of financial organizations implementing a .BANK or .INSURANCE domain name (collectively "fTLD Domain"). This guide focuses on the requirements that must be deployed by registrants (organizations that register domain names) and registrars[1] (entities authorized by fTLD to distribute an fTLD Domain) in order to comply with and fully benefit from their fTLD Domains.

The following are related guides to this document and available at `ftld.com/guide`:

- Technical Guide to Security Requirements offers detailed implementation guidance to your operational IT and security personnel or third-party providers.
- Planning and Communications Guide is designed for officers, marketing managers and others. It focuses on strategies for planning and communicating your organization's move to an fTLD Domain.

The Requirements can be accessed at `ftld.com/enhanced-security`, and its Annex A, Authorizations for Defined Services[2] Deployed on Non-.BANK and Non-.INSURANCE Domains, is included in this Executive Guide as Annex A for immediate reference.

fTLD has compiled a list of publically available, free resources that can be helpful in understanding whether the implementation of an fTLD Domain addresses the defined Requirements, and it's available at `ftld.com/resources`. Although these resources are useful, they are not the basis for fTLD's Requirements monitoring service and are not exact checks against the Requirements.

Why the Additional Requirements?

An fTLD Domain is a trusted, verified, more secure and easily identifiable location on the internet for the global banking and insurance communities and the customers and stakeholders they serve. fTLD Domains have been designed and built by the international banking and insurance communities specifically for banks, insurers (inclusive of providers and distributors) and others in the financial services sector. The goal of these internet domains is assuring greater online security for financial services organizations and their customers. Owned, operated and governed by the financial community, an fTLD Domain is where organizations can enhance their online presence, create new marketing and branding opportunities, differentiate themselves in a competitive market, secure shorter and more relevant and memorable domain names and communicate more securely with customers, third-party providers and other stakeholders.

To achieve and sustain the overall goal of a trusted and more secure place online, registering and operating an fTLD Domain name requires a greater commitment to security than registering your bank's or insurer's name in most other internet web extensions or Top-Level Domains (TLDs). fTLD requires its registrars and its registrants to deploy robust security technologies and practices.

[1] See the list of Approved Registrars at `https://www.ftld.com/approved-registrars`

[2] Defined Services currently includes hosted email solutions, content delivery networks, security and fraud services and aliasing to legacy domains (e.g., .COM, .NET)

We also ensure that these measures are routinely monitored for compliance with the Requirements. When fTLD's monitoring service detects a compliance issue the respective registrar and/or registrant will be contacted about an appropriate remediation plan.

Our Commitment to You

- We will fulfill our security obligations noted in the Requirements, and will continue to work with industry and security experts to ensure our practices and Requirements are relevant and robust.
- We will ensure that our Requirements represent up-to-date and respected best practices that continue to enhance security and improve customer trust.
- We will ensure that only legitimate and verified members of the global banking and insurance communities register an fTLD Domain.
- We will operate effective processes and monitoring to ensure all registrants and registrars comply with the Requirements.
- We will work with the global financial services community to maintain the most resilient online environment for the global banking and insurance sectors.

Your Commitment to Security

- You will implement the Requirements either directly through your own operations or in partnership with third-party providers.
- You will work with fTLD as needed to resolve compliance issues in a timely manner.
- You will put in place the processes and practices needed to ensure compliance with the Requirements.

How You Will Benefit

For you and your customers, an fTLD Domain internet experience takes place in a protected and highly controlled environment, free from many of the malicious and fraudulent activities found in the existing TLD space. The Requirements for an fTLD Domain and its customer protection safeguards will help you to:

- Reduce the risk, incidence and scope of phishing, spoofing and cybersquatting.
- Limit intellectual property rights infringements by those attempting to register your name(s).
- Protect confidentiality and integrity of communications and transactions over the internet.
- Improve customers' trust in doing business with you online, creating opportunities for you to deepen relationships with new and existing customers.
- Capitalize on branding and differentiation opportunities for your company as a progressively secure, resilient and customer-focused organization.

OVERVIEW OF THE SECURITY REQUIREMENTS

To mitigate key online threats and vulnerabilities impacting financial services organizations and their customers, the Requirements include:

- Verification and re-verification of charter/licensure/authorized person/names for regulated entities to ensure only legitimate members of the global banking and insurance communities are awarded domain names.
- Multi-factor authentication by registry and registrars to ensure that any change to registration data is made only by authorized users of the registered entity thereby reducing the risk of an unauthorized individual or organization fraudulently transferring or interrupting service of your domain name.
- Domain Name System Security Extensions (DNSSEC) to ensure internet users are landing on legitimate websites and not being misdirected to malicious ones.
- Email Authentication to ensure brand protection by mitigating spoofing, phishing and other malicious email-borne activities.
- Strong encryption (i.e., Transport Layer Security) to ensure confidentiality and integrity of communications and transactions over the internet.
- Prohibition on proxy/privacy registration services to ensure full disclosure of domain registration information so bad actors cannot hide.
- fTLD Domain DNS Name Servers hosting to ensure they are trusted and verifiable.

Implementing the Requirements will mean your customers, third-party providers and other stakeholders:

- Can be certain that only verified banks and insurers in good standing with relevant government regulatory authorities are using an fTLD Domain.
- Can rely on trustworthy security technology and established best practices for higher assurance that they are visiting the intended website, and to assure that authorized email communications are from you.
- Can be reassured and further encouraged to use the full range of online financial services your organization provides, maximizing your service productivity and reducing operational costs.

HOW TO MEET THE SECURITY REQUIREMENTS

This Executive Guide is an overview of the Requirements. For more detailed technical information about each of the topics below, please consult the Technical Guide to Security Requirements.

Using Third-Party Providers

Using a third-party provider does not obviate or transfer your responsibility for compliance with the Requirements.

Any arrangement with a third-party provider supporting or hosting an fTLD Domain must be compliant with the Requirements, and this may mean that the registrant needs to contractually bind its third-party providers to implement the relevant Requirements.

Initial Eligibility and Ongoing Verification Requirements

Verification of Charter/Licensure/Authorized Person/Names

An fTLD Domain will not be awarded until your organization's credentials and identity have been checked against the relevant government regulatory authority's records, if applicable, as well as fTLD's Registrant Eligibility and Name Selection Policies.[3] The process conducted by Symantec[4], fTLD's verification agent, involves verification of your charter/license/authorized person/names, if applicable, ensuring the requestor is a full-time employee of the registrant and authorized to register domains on its behalf and that the fTLD Domain selected corresponds to the trademark, trade name or service mark of the registrant.

Ongoing Re-Verification of Registration Data

While all registrants must provide prompt and accurate Whois information to their registrars every year, fTLD additionally requires an fTLD Domain registrant to provide positive verification of eligibility and contact information every two years or upon domain renewal, whichever comes first.

Your organization must ensure the ongoing accuracy of eligibility and contact information and timely response to fTLD and Symantec inquiries. Failure to provide positive, timely and accurate responses to these regular queries could result in the suspension or loss of your domain name.

Prohibition of Proxy/Privacy Registrations

Proxy/privacy registrations—i.e., registrations through a third party that obscures the contact and other details of the registrant—are prohibited. This is to ensure transparency of the true identity of the fTLD Domain registrant.

[3] See fTLD's Policies at `https://www.ftld.com/policies`

[4] See the verification overviews at `https://www.ftld.com/registrar-toolkit`

Authentication for Domain Registration Changes

fTLD requires that only fully authenticated communications occur between the registrant and registrar, and that changes to registration data can be made only by authorized personnel. To ensure the integrity and reliability of registration data, multi-factor authentication must be deployed by your registrar for interactions you have with them. This requirement applies also to registrars in their communications with Verisign, fTLD's registry services provider. If you wish to change your registration details with your registrar, your organization will need to use both a username/password and a second factor such as a physical token or fob as defined by your registrar. You will need to ensure a robust internal policy and procedure around storing and accessing the second authentication factor.

This feature significantly reduces the risk of an unauthorized individual or organization fraudulently transferring or interrupting service of your fTLD Domain.

Improving Trust in the Domain Name System (DNS)

Deploy Domain Name System Security Extensions (DNSSEC)

All fTLD Domain registrants are required to implement DNSSEC. Implementing DNSSEC will not only allow you to meet the Requirements, it is the primary means to avoid DNS cache poisoning and is a more secure Domain DNS platform on which to build future security functionality.

DNSSEC is a set of specifications used to complement the DNS to authenticate name servers and prove the authenticity of DNS traffic. DNSSEC uses public key cryptography to authenticate domain names and verify the integrity of traffic to and from those names. DNSSEC must be deployed and/or supported by the registry, registrar and registrant in order to establish and maintain the chain of trust for domain names at every level in an fTLD Domain.

For registrants, DNSSEC must be deployed for all sub-zones for domains that resolve in the DNS. This means that if you use names at the second or third level—`www.yourbank.bank` or `www.newservice.yourbank.bank`—you or your relevant third-party providers will need to deploy DNSSEC at each level that resolves in the public DNS.

If your organization is architected so that legacy domains (e.g., .COM, .NET) provide Defined Services to your fTLD Domain, your third-party provider must implement DNSSEC on their domain according to the timeline in Annex A. More information about Defined Services and legacy domain third-party provider obligations are provided in Annex A.

Authoritative DNS Name Servers Must End in an fTLD Domain Suffix

Your domain's authoritative DNS name servers must end in an fTLD Domain suffix (e.g., `ns1.yourbank.bank` or `ns1.yourinsurancecompany.insurance`). If you use third-party hosted DNS solutions, consider delegating a subdomain to your third-party provider from which they may operate the contracted services. Be aware that third-party providers operating domains and subdomains within an fTLD Domain environment must fully comply with the relevant Requirements outlined in this document. It is your responsibility to ensure your DNS third-party provider is fully aware of and compliant with the relevant Requirements.

[5] In addition to the more detailed information on DNSSEC in the Technical Guide to Security Requirements, we recommend you follow the best practices described in the Internet Engineering Task Force (IETF) RFC 6781 (`https://tools.ietf.org/html/rfc6781`). We also recommend reviewing Verisign's DNSSEC Practice Statement (`https://www.verisign.com/assets/tld-gtld-zone-v1.3.pdf`).

Prohibition of Aliasing Resource Records Outside of an fTLD Domain

While you may redirect web traffic to an fTLD Domain from another domain name, aliasing from an fTLD Domain to other TLDs is prohibited with limited exceptions for Defined Services. When you alias, users may think they are on a trusted website providing security when they may not be because their true URL destination is masked. The aliasing restriction is so that your customers and others do not perceive themselves to be at the more secure fTLD Domain site when they are actually in another domain such as `www.yourbank.com` or `www.yourinsuranceagency.countrycode`.This could prevent you from realizing the benefits of an fTLD Domain in both security and branding.

fTLD Domain registrants are also restricted in their use of certain DNS resource records. DNS resource records—such as CNAME, DNAME, MX and others—are the identifying information stored in the zone files of the DNS that are specific to your domain name. An fTLD Domain must maintain a logical separation from domains with less rigorous security requirements. To do this, DNS resource records used within an fTLD Domain may only point or alias to a fully qualified domain name ending in an fTLD Domain suffix, unless the legacy domain qualifies by providing a Defined Service and meets the relevant Requirements (see Annex A).

Restrictions on URL Redirection

An fTLD Domain registrant may wish to redirect web traffic to a domain outside its fTLD Domain, but providing content on an fTLD Domain maximizes the value and trust in your domain. While domain redirection using DNS resource records may be used for this purpose provided the relevant Requirements are met, URL redirection techniques may be used under other circumstances (see Security Requirement #30: Redirection). Organizations that redirect customers from an fTLD Domain to a non-fTLD Domain are strongly encouraged to inform them of this action (e.g., use of a speed bump[6]) to avoid confusion and the misperception by customers that they are accessing information on an fTLD Domain. This practice keeps a clear technical distinction between fTLD Domain services and services hosted in other domains.

Strong Encryption

Implement Transport Layer Security (TLS)

TLS is a set of protocols that encrypts the content of data packets as they move between clients and servers, especially web-browser communications, and creates an HTTPS address and padlock in the browser address bar. For organizations that have purchased an Extended Validation Certificate[7] (EV-Cert) to comply with the TLS requirement, customers will see URL information in a green address bar. fTLD Domain registrants are required to implement TLS for all communications with their registrars and also for all public-facing fTLD Domain services to secure interactions with customers, employees, third-party providers and other stakeholders. TLS in your fTLD Domain service-related operations protects sensitive information and credentials that traverse the Internet.

Implementing TLS means that information sent across the public internet is protected. These communications and transactions are not readable if intercepted, for example, via a “man in the middle” attack.

[6] A message to the website visitor that they are about to leave the current website and asking them to take a manual step (e.g., click “yes”) to proceed. An example of this may be when the visitor seeks to access social media (e.g., Twitter) hosted by the registrant.

[7] An EV-Cert is not required by fTLD to meet the TLS requirement

TLS also provides the capability to authenticate web-based communication so customers are assured that they are communicating with their bank and not a phishing website.

If your organization is architected so that legacy domains (e.g., .COM, .NET) provide Defined Services to your fTLD Domain, your third-party provider must implement TLS on their domain according to the timelines in Annex A. More information about Defined Services and legacy domain third-party provider obligations are provided in Annex A.

Use of Encryption in Common Legacy Services

fTLD requires that registrants avoid using unencrypted public facing services where commercially reasonable. Common services such as FTP, Telnet, HTTP, SMTP and many others have corresponding services that default to encrypted communications. fTLD Domain registrants must make best efforts to use these encrypted services in place of unencrypted legacy services and, where TLS is used, implement and maintain the Requirements.

Email Authentication

fTLD requires you to publish a DMARC (Domain-based Message Authentication) record. DMARC is an internet Engineering Task Force (IETF) specification[8]. This technology, when overlaid with email authentication protocols DomainKeys Identified Mail (DKIM) and/or Sender Policy Framework (SPF), allows you to authenticate your outbound email. It gives customers and their email-service providers higher assurance that mail purporting to originate from your domain in fact came from your organization and not from a malicious actor.

Publishing your DMARC record and implementing DKIM and/or SPF are key steps to preventing phishing emails associated with your domain from being received by your customers. A strong email authentication policy will reassure customers of the legitimacy of email coming from you— their trusted financial organization. An expanded discussion of DMARC, SPF and DKIM is available in the Technical Guide to Security Requirements.

If your organization is architected so that legacy domains (e.g., .COM, .NET) provide Defined Services to your fTLD Domain, your third-party provider may need to implement email authentication on their domain. More information about Defined Services and legacy domain third-party provider obligations are provided in Annex A.

[8] See `https://www.ietf.org`

OTHER CONSIDERATIONS

Additional information about these topics is provided in the Planning and Communications Guide.

Network Resources

Although some organizations have already implemented measures such as DNSSEC or TLS, many of the Requirements may necessitate changes to the way you deliver services to your customers and the public. Public-facing services such as web sites and electronic mail may require you to implement new controls as a result of the Requirements. In order to meet the Requirements, additional tasks and features will likely be required in your network.

The Technical Guide to Security Requirements describes in more detail how to meet the Requirements and best practices for running common services in a highly secure TLD.

Staffing Resources

The staffing resources needed to implement an fTLD Domain will vary according to the type and size of your organization. Larger organizations will likely have the expertise and resources internally to effect the implementation, and will therefore want to concentrate on communication and coordination.

Smaller organizations, or those that have outsourced related IT functions to third-party providers, will likely need to work closely with those providers to understand and communicate their evolving needs and ensure that they are met in a cost-efficient and timely way. Smaller organizations may not have the depth of in-house technical expertise needed to effect a full implementation or may need those resources to support current operations. These organizations may need to work with providers of existing functions such as email, web services, API between services and banking records, and payment services to implement the Requirements.

Whatever the size or type of your organization, the first step will be to identify and work with both internal and external partners, including your domain name registrar and any third-party web, communications and security providers.

The project to implement an fTLD Domain should also include externally-facing activities to communicate the benefits to your customers and business partners and help them adjust to the change associated with your planned use of an fTLD Domain, which is covered in the Planning and Communications Guide.

Using a project management methodology may be advisable to plan and implement the Requirements; for example, publishing a basic DMARC record should be relatively straightforward and adopting TLS, if it is new to your organization, requires implementation across a range of internet technologies and may be challenging.

Following the implementation of an fTLD Domain, you may require additional staff resources for on-going management and maintenance of the Requirements. An organization implementing DNSSEC for the first time, for example, will need to plan for the additional workload to maintain it. You may also need to dedicate resources from web design, content management and networking.

Working with Third-Party Providers

On-going expenditures will be necessary to maintain, monitor and demonstrate compliance with the Requirements. To illustrate, in a DNSSEC deployment, if you add a new name or level to your second-level domain—for example, you create a new product or service and a new name to go along with it—`www.newservice.yourbank.bank`—you will need to re-sign the zone and re-publish it. If you change mail servers or use third-party email senders you will need to immediately update the DMARC record to reflect this.

You may wish to investigate specialized DNS or email authentication providers that can meet the Requirements, and find new partners to facilitate your implementation. New third-party providers have emerged whose business is built around helping clients meet these kinds of requirements.

You also need to check how the activities of your third-party providers may impact your compliance with the Requirements. For example, if you use a vendor to manage marketing mail-outs to your existing customers then you will need to modify your DMARC, DKIM and SPF records to include your authorized third-party email senders. It is your responsibility to ensure your third-party providers comply with the Requirements.

If your organization is architected so that legacy domains (e.g., .COM, .NET) provide Defined Services to your fTLD Domain, your third-party provider must implement the relevant Requirements on their domain according to the timelines in Annex A.

Implementation Sequencing

Implementation and use of your fTLD Domain must be in compliance with all relevant Requirements. The timing of the activities required to implement the Requirements will be different for every organization. A large organization may be in full control of its own IT staff and can prioritize and schedule according to its own objectives. A smaller organization may not directly control the necessary third-party resources or be able to set a fully directed implementation process. In all cases, you must meet all relevant Requirements before finalizing the launch and use of your fTLD Domain.

SECURITY REQUIREMENTS

Emergency Situations With Security Requirements

If a response to a significant security incident ("Emergency Situation")[9] requires action that conflicts or contravenes the Requirements, fTLD will provide temporary compliance relief upon written notification[10] of the incident.

Keeping Up to Date With the Security Requirements

fTLD will periodically review and update the Requirements. As these updates occur, you will be provided reasonable notice to implement the updated, relevant Requirements to your fTLD Domain,

The fTLD security framework will continue to evolve to stay ahead of the threats it is designed to mitigate. As new technologies emerge that improve the trust between customers and providers of financial services, the Requirements and best practices will also change.

Our promise to you is that fTLD will continue work collaboratively with industry and security experts to ensure that the Requirements of an fTLD Domain represent proven measures to assure your security and your customers' well-placed trust.

[9] See requirement #31

[10] See the Incident Notification form at `https://www.ftld.com/incident-form`

Annex A

Authorizations for Defined Services Deployed on Non-.BANK and Non-.INSURANCE Domains

Requirements/ Defined Services	#23–DNSSEC	#25 & #29–TLS/ Encryption Practices	#26–Email Authentication	#27–DNS Resource Record Restrictions
Hosted Email Solutions	Required by January 1, 2018	Required for Email and Web Services Only Required by April 1, 2017		Exceptions for CNAME and MX
Content Delivery Networks	Required by January 1, 2018		N/A	Exception for CNAME
Security* and Fraud Services	Required by January 1, 2018		N/A	Exception for CNAME
Aliasing to Legacy Domains				Exception for CNAME

Key:

Green – fTLD Security Requirements apply now

Yellow – Delayed implementation of fTLD Security Requirement

Red – Enduring changes to fTLD Security Requirements

Orange – N/A (Not Applicable)

* The Security Requirements do not apply to Distributed Denial of Service mitigation services that do not use DNS Resource Records within the .BANK or .INSURANCE Domain Name System.

fTLD
Registry Services, LLC