# Registrant Security Requirements

## Verification

**Verify:**
1. The domain name corresponds to your organization’s legal name or brand;
2. Your organization is eligible to apply for the domain name;
3. The employee requesting the domain name on behalf of your organization is authorized to do so.

Verification prevents cybersquatting and makes it impossible for bad actors to register a domain name or contact your customers while posing as your organization.

### Who Can Help
- fTLD
- Approved registrars

## Zone 1

**Ensure** authoritative name server host names are within the .BANK domain zone.

In-zone name servers place the same security requirements on the name server as the .BANK domain itself.

### Who Can Help
- DNS provider
- Approved registrars

## Zone 2

**Implement** Domain Name System Security Extensions (DNSSEC).

DNSSEC ensures that internet users reaching your organization online and have not been redirected to a fraudulent website.

### Who Can Help
- DNS provider
- Approved registrars

## Encryption

**Obtain** a digital identity certificate.

Your .BANK domain will resolve to HTTPS, which ensures all data is secure in transit.

### Who Can Help
- Certificate authority
- Registrar
- Web host

## Encryption

**Ensure** Transport Layer Security (TLS) has been implemented using version 1.2 or greater where possible.

TLS creates an encrypted connection, protecting your website and visitors, securing email communications, and supporting the safe and secure transmission of information and transactions.

### Who Can Help
- Certificate authority
- Registrar
- Web host
- Email provider

## Electronic Authentication

**Publish in DNS as a text record:**
1. Domain-based Message Authentication, Reporting, and Conformance (DMARC) record;
2. Sender Policy Framework (SPF) and/or DomainKeys Identified Mail (DKIM) records when domain is used for email.

DMARC helps protect against phishing and spoofing, and increases the deliverability of email to your customers, especially when used in combination with SPF and/or DKIM.

### Who Can Help
- Email security provider
- Approved registrars

## Third-Party Provider

**Ensure** any vendors utilizing DNS resource records are currently using DNSSEC (#2) and TLS (#4).

Services provided by vendors working with a .BANK domain will be more secure as they are held to the same security requirements as your organization.

### Who Can Help
- Third-party providers (e.g., hosted email, content delivery networks, security and fraud services)

---

For more detailed information on any of these requirements, please consult fTLD’s Implementation Hub.

[go.ftld.com/Implementation-Hub](http://go.ftld.com/Implementation-Hub)

Updated June 2019