Los Angeles Headquarters
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA
+1 310 301 5800
+1 310 823 8649

Registry Services Evaluation Policy (RSEP) Request

October 21, 2022

Registry Operator
fTLD Registry Services LLC

Request Details
Case Number: 01173868

This Registry Services Evaluation Policy (RSEP) request form should be submitted for review by ICANN org when a registry operator is adding, modifying, or removing a Registry Service for a TLD or group of TLDs.

The RSEP Process webpage provides additional information about the process and lists RSEP requests that have been reviewed and/or approved by ICANN org. If you are proposing a service that was previously approved, we encourage you to respond similarly to the most recently approved request(s) to facilitate ICANN org's review.

Certain known Registry Services are identified in the Naming Services portal (NSp) case type list under "RSEP Fast Track" (example: "RSEP Fast Track – BTAPPA"). If you would like to submit a request for one of these services, please exit this case and select the specific Fast Track case type. Unless the service is identified under RSEP Fast Track, all other RSEP requests should be submitted through this form.

Helpful Tips

- Click the "Save" button to save your work. This will allow you to return to the request at a later time and will not submit the request.
- You may print or save your request as a PDF by clicking the printer icon in the upper right corner. You must click "Save" at least once in order to print the request.
- Click the "Submit" button to submit your completed request to ICANN org.
- Complete the information requested below. All fields marked with an asterisk (*) are required. If not applicable, respond with "N/A."

1. PROPOSED SERVICE DESCRIPTION

1.1. Name of proposed service.

Public Suffix Domain - Domain-based Message Authentication, Reporting & Conformance

1.2. Provide a general description of the proposed service including the impact to external users and how it will be offered.

Background:
Email authentication, including DMARC, is required for all domains in the .BANK and .INSURANCE zones. Specifically, second-level domains (SLDs) in the zone must have DMARC and Sender Policy Framework (SPF) records and if the SLD is used for email DMARC must be at enforcement (i.e., p=reject) within 90 days of deployment of email. For SLDs not used for email, DMARC must be at enforcement (i.e., p=reject). See Security Requirement #5 for .BANK here: https://www.register.bank/securityrequirements/ and .INSURANCE here: https://www.register.insurance/securityrequirements/. Additional detail about implementing the requirement is available here: https://go.ftld.com/dmarc-implementation.

Summary:
While DMARC has historically only been implemented at the SLD, fTLD's approach to domain security has led us to consider how to achieve this at the top-level (i.e., PSD DMARC) for two purposes. First, this approach would protect NXDOMAINs (i.e., non-existent domains) from being used to perpetrate phishing and related email abuse for .BANK and .INSURANCE. For fTLD's TLDs, there are two types of NXDOMAINs (i.e., domains that have not been registered and registered domains that do not appear in the .BANK or .INSURANCE zone because they have not met Security Requirements #1 and #2, Registry requirements for a domain to be in DNS, available at the previously referenced URLs). Second, implementing PSD DMARC would add heightened security and reputational protections for .BANK and .INSURANCE as well as registrants using SLDs by ensuring compliance with the email authentication requirement.

Impact to external users: fTLD believes that the impact on Internet users will be positive by further enhancing the overall security and stability of the .BANK and .INSURANCE ecosystems. Over the last several years as part of the IETF review process, which led to the publication of RFC 9091, and our own external engagement, fTLD has consulted with several infrastructure operators that have been researching the use of DMARC in their respective TLDs. This review,

as explained in further detail in this RSEP, has taken a holistic approach involving technical, legal and policy considerations. It is based on the totality of this research that fTLD believes that this RSEP is in the best interest of the respective banking and insurance communities that each fTLD TLD serves as well as all Internet users that rely on the Internet for financial services by adding default phishing abuse prevention.

How it will be offered: The PSD DMARC approach to security is something fTLD would undertake at the TLD level of .BANK and .INSURANCE and as such there is no offering. All NXDOMAINs will be automatically protected and SLDs without a DMARC record would have the PSD DMARC applied when mail service providers query the DNS for the record.

1.3. Provide a technical description of the proposed service.

Most PSD DMARC related processing is performed by email receivers. Email receivers which implement PSD DMARC will query DMARC records published by .BANK or .INSURANCE for SLDs within .BANK or .INSURANCE that do not publish their own DMARC record and use this as an input into their email system to support that any email purporting to originate from them must not be delivered/rejected.

DMARC records are DNS records of type TXT that are published in the _dmarc subdomain of the protected domain (in this case .BANK and .INSURANCE).

The DMARC records will specify requested email handling policy for messages that fail DMARC checks and the reporting address for DMARC feedback. Details are specified by RFC 7489 Section 6.1 and Section 6.3 as modified by RFC 9091 Section 3.2.

When the service is implemented, TXT records similar to the following will be published in _dmarc.bank and _dmarc.insurance:

v=DMARC1; p=reject; sp=reject; np=reject; rua=mailto:dmarc_reports@ftld.com

Processing for email receivers that retrieve these records is defined in RFC 7489 and RFC 9091. Authorized content of the record is defined by the IANA DMARC Tag Registry: https://www.iana.org/assignments/dmarc-parameters/dmarc-parameters.xhtml#tag

fTLD will not make use of the defined RUF tag in its records without notice to and approval by ICANN. See section 2.4 below.

1.4. If this proposed service has already been approved by ICANN org, identify and provide a link to the RSEP request for the same service that was most recently approved.

N/A

1.5. Describe the benefits of the proposed service and who would benefit from the proposed service.

As documented by APWG in its Q1 2022 report, "OpSec Security found that phishing attacks against the financial sector, which includes banks, remained the largest set of attacks, accounting for 23.6 percent of all phishing." This fact is why fTLD, since its founding, has remained committed to advocating and enforcing enhanced email security features and protocols within the TLDs it operates.

The benefits of the proposed service include, but are not limited to, are:
1. Registrants whose SLDs are not in the .BANK or .INSURANCE zone will be protected from phishing and other email-borne abuses purporting to originate from them.
2. Registrants whose SLDs are in the .BANK or .INSURANCE zone, but not properly protected with DMARC will be protected by the PSD DMARC at the top-level for .BANK and .INSURANCE.
3. fTLD will be protected reputationally as NXDOMAINs will be protected from phishing and other email-borne abuses purporting to originate from them.
4. Email receivers (e.g., Google, Microsoft, Yahoo!) will be armed with a means to reject (i.e., not deliver) email purporting to be from a .BANK or .INSURANCE SLD that does not have DMARC implemented.

1.6. Describe the timeline for implementation of the proposed service.

Upon ICANN approval, fTLD will provide a minimum of 90-days' notice to .BANK and .INSURANCE Registrants to educate and inform them of the implementation of PSD DMARC. fTLD will produce a FAQ to educate Registrants about what PSD DMARC does and does not do. Registry Operator will also provide notice to Registrars about the implementation of PSD DMARC a minimum of 120 days in advance given their role in compelling compliance with fTLD's Security Requirements by way of their registration agreements, and in some cases, their role in providing email authentication services to their clients. fTLD has had contractual DMARC requirements in place since its TLDs were launched in 2015 (.BANK) and 2016 (.INSURANCE). Additionally, fTLD actively monitors for compliance daily and reports failures via email to Registrars on a weekly basis and Registrants monthly. Therefore, there should be negligible impact to Registrants due to the implementation of PSD DMARC.

1.7. If additional information should be considered with the description of the proposed service, attach one or more file(s) below.

RFC 9091_ Experimental Domain-Based Message Authentication, Reporting, and Conformance (DMARC) Extension for Public Suffix Domainspdf

1.8. If the proposed service adds or modifies Internationalized Domain Name (IDN) languages or scripts that have already been approved in another RSEP request or are considered pre-approved by ICANN org, provide (a) a reference to the RSEP request, TLD(s), and IDN table(s) that were already approved or (b) a link to the pre-approved Reference Label Generation Rules (LGR). Otherwise, indicate “not applicable.”

Not Applicable

The most current IDN requirements will be used to evaluate a submitted table.

2. SECURITY AND STABILITY

2.1. What effect, if any, will the proposed service have on the life cycle of domain names?

None

2.2. Does the proposed service alter the storage and input of Registry Data?

No

2.3. Explain how the proposed service will affect the throughput, response time, consistency or coherence of responses to Internet servers or end systems.

No effect

2.4. Have technical concerns been raised about the proposed service? If so, identify the concerns and describe how you intend to address those concerns.

RFC 9091 identifies both potential privacy (Section 4) and security (Section 5) considerations associated with PSD DMARC. The planned fTLD service addresses these considerations as follows:

- Privacy Considerations:
  - RFC 9091 recommends that PSD DMARC deployment be limited to TLDs that either control domains for a single entity (e.g., brand TLDs) or to those which mandate that registrants implement DMARC for their domains. fTLD meets the latter requirement (See paragraph 1.2, above). From an ICANN policy perspective, this should be a key consideration for this and future requests by Registry Operators to implement PSD DMARC.
  - fTLD will limit requested feedback to aggregate reports (see the sample DMARC record in the service description (paragraph 1.3, above). Aggregate reports will be used for the purposes of abuse/threat detection, enforcing compliance with the DMARC requirement for SLDs (i.e., , fTLD's Security Requirements are accessible here: https://www.ftld.com/security/ and detailed information for DMARC is accessible here: https://go.ftld.com/dmarc-implementation.) and enhancing the overall security and stability of the .BANK and .INSURANCE TLDs.
  - Aggregate reports do not contain inherent personal data since the information is not related to an individual and rather it's the machine or device sending the email. fTLD has been reviewing relevant technical and legal analysis regarding data privacy considerations involving DMARC. One such document that fTLD reviewed was prepared by ECO and is entitled Report on the compliance of DMARC with the EU GDPR. fTLD believes that its proposed deployment of PSD DMARC is consistent with the guidance set forth in the ECO report.
  - Access to data from aggregate reports will be restricted to select fTLD staff and external consultants/vendors on a need-to-know basis as part of fTLD's overall security and data privacy safeguards associated with this function.
  - fTLD will not activate failure/forensic reports (i.e., RUF) per the guidance set forth in the ECO report. However, as fTLD continues to engage in technical and policy discussions with the growing community of operators that have deployed or are considering deploying PSD DMARC, fTLD may become aware of enhanced security and stability benefits associated with failure/forensic reports. Prior to any future activation of these reports, fTLD would provide notice and seek approval from ICANN.
  - Several of the operators that fTLD has spoken with as part of its PSD DMARC engagement and outreach are based in Europe. fTLD intends to maintain these relationships

and will be actively monitoring any guidance that European Data Protection Authorities may provide in connection with DMARC that may impact the proposed service.

- Security Considerations:
  - fTLD and Registrants benefit from improved additional data on abuse/threats.
  - Other RFC 9091 security considerations do not require mitigation at the registry level.
  - Data received in feedback reports will be securely maintained and segregated from other fTLD business data to provide security and privacy protections for fTLD Registrant related data.

2.5. Describe the quality assurance plan and/or testing of the proposed service prior to deployment.

Testing with .GOV, .GOV.UK (which functions like a TLD within the .UK ccTLD), and .MIL was successfully completed during the development of RFC 9091. Recently, .POLICE.UK has also published a PSD DMARC record. Once approved, fTLD will verify planned PSD DMARC records prior to deployment with appropriate subject matter experts. Actual deployment will follow fTLDs normal internal DNS update process.

.MIL Statement: The United States Department of Defense (DoD) implemented in its Domain Name System (DNS) a Domain-based Message Authentication, Reporting, and Conformance (DMARC) record in January 2020. This DMARC DNS record was added as a ‘TXT’ resource record at the well-known ‘_dmarc’ subdomain under the ‘.mil’ top-level domain DNS zone, as currently specified in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 9091 document titled "Experimental Domain-Based Message Authentication, Reporting, and Conformance (DMARC) Extension for Public Suffix Domains". DoD has not experienced any adverse effects based on this DMARC record.

The DMARC record provides a default indication for all of .mil to recipient email servers for the steps they should take to authenticate and handle incoming email messages seemingly from .mil or any .mil subdomain. In addition, it requests feedback reports to be sent to a centralized DoD email address for DMARC-related reports. Over the past 19 months since adding the .mil DMARC DNS record, DoD has seen DNS requests from external entities for this DMARC record and has received reports to the centralized feedback email address. DoD has not experienced any adverse effects based on this DMARC record and looks forward to having a better security posture for both DoD and all recipients of email claiming to be from DoD by leveraging it.

2.6. Identify and list any relevant RFCs or White Papers on the proposed service and explain how those papers are relevant.

See RFC 9091 here: https://www.rfc-editor.org/rfc/rfc9091. fTLD began internal work on PSD DMARC in June 2018, which led to the first Internet Draft being published by the IETF in October 2018. Since that time, fTLD and IETF work has continued, which led to publication of the RFC in July 2021.

3. COMPETITION

3.1. Do you believe the proposed service would have any positive or negative effects on competition? If so, please explain.

No impact at all on competition as this is solely about security for fTLD's TLDs and .BANK and .INSURANCE Registrants. The related technologies are all defined by public standards which could be implemented by any Registry Operator.

3.2. How would you define the markets in which the proposed service would compete?

This is not a competitive service and thus this is not applicable.

3.3. What companies/entities provide services or products that are similar in substance or effect to the proposed service?

This is not a competitive service and thus this is not applicable.

3.4. In view of your status as a Registry Operator, would the introduction of the proposed service potentially affect the ability of other companies/entities that provide similar products or services to compete?

This is not a competitive service and thus this is not applicable.

3.5. Do you propose to work with a vendor or contractor to provide the proposed service? If so, what is the name of the vendor/contractor and describe the nature of the services the vendor/contractor would provide.

As data in aggregate reports is provided in an XML format, it needs to be parsed and converted into a user-friendly format for interpretation. fTLD currently works with an email security vendor to obtain aggregate reports for the seven domain names it uses and expects to do the same for PSD DMARC for .BANK and .INSURANCE. fTLD's vendor(s) will be contractually required to protect the data. Data would be initially received via email by fTLD prior to its transmission to the processing vendor. Access to this email account and the associated RUA data will be restricted to select fTLD staff and consultants/vendors on a need-to-know basis as part of fTLD's overall security and data privacy safeguards associated with this function. This is not directly part of the service, but data that would be received as a result of the service being enabled.

3.6. Have you communicated with any of the entities whose products or services might be affected by the introduction of your proposed service? If so, please describe the communications.

Yes. See section 6.2, below, for a description of the consultations.

3.7. If you have any documents that address the possible effects on competition of the proposed service, attach them below. ICANN will keep the documents confidential.

4. CONTRACTUAL PROVISIONS

4.1. List the relevant contractual provisions impacted by the proposed service. This includes, but is not limited to, Consensus Policies, previously approved amendments or services, Reserved Names, and Rights Protection Mechanisms.

Add: 4 - Public Suffix Domain - Domain-based Message Authentication, Reporting & Conformance

Registry Operator may implement PSD DMARC, which includes adding a DNS resource record (e.g., _dmarc.bank and _dmarc.insurance) into its TLDs' DNS Zones. This augments the above Section 1, DNS Service - TLD Zone Contents.

4.2. What effect, if any, will the proposed service have on the reporting of data to ICANN?

None

4.3. What effect, if any, will the proposed service have on Registration Data Directory Service (RDDS)?*

None

4.4. What effect, if any, will the proposed service have on the price of a domain name registration?

None

4.5. Will the proposed service result in a change to a Material Subcontracting Arrangement (MSA) as defined by the Registry Agreement? If so, identify and describe the change. Please note that a change to an MSA requires consent from ICANN org through the MSA change request process. The RSEP request must be approved prior to submitting the MSA change request.

No

5. AUTHORIZATION LANGUAGE

5.1. A Registry Agreement (RA) amendment is required when the proposed service: (i) contradicts existing provisions in the RA or (ii) is not contemplated in the RA and, therefore, needs to be added to Exhibit A of the RA and/or as an appropriate addendum/appendix. If applicable, provide draft language (or a link to previously approved RA amendment language) describing the service to be used in an RA amendment if the proposed service is approved. If an RA amendment is not applicable, respond with “N/A” and provide a complete response to question 5.2.*

For examples or for IDN services, you may refer to the webpage for standard RA template amendments for commonly requested Registry Services.

Registry Operator may implement the Domain-based Message Authentication, Reporting & Conformance ("DMARC") extension for Public Suffix Domains ("PSD") in the TLD’s DNS service, as follows:

● Registry Operator may activate, in the TLD’s DNS service, the ASCII label "_dmarc" as owner of a DNS resource record of type TXT, class IN, and RDATA defining a PSD-DMARC policy (as described in RFC 9091).
● Once Registry Operator has activated PSD DMARC as described above, Registry Operator must signal that the domain name is a public suffix domain name as described in Appendix B of RFC 9091 or as otherwise specified in future revisions to the method of signaling public suffix domain names in the DMARC standard.
● Registry Operator may enable the reception of Aggregate Reports (as defined by Section 7.2 of RFC 7489) solely for the purposes of detecting abuse or threats, enforcing compliance with the DMARC requirement for domains under registration, and enhancing the overall security and stability of the TLD.
● Registry Operator must not enable other types of reports (e.g., Failure Reports) defined in the DMARC standard (as defined in relevant RFCs).
● Registry Operator must restrict access to data from Aggregate Reports to select staff of Registry Operator and external consultants or vendors on a need-to-know basis as part of Registry Operator's overall security and data privacy safeguards associated with this function.
● Registry Operator must ensure that registrants are informed about the implementation of PSD DMARC no less than ninety (90) calendar days in advance.
● Registry Operator will provide written notice to registrars about the implementation of PSD DMARC no less than one hundred twenty (120) calendar days in advance.

5.2. If the proposed service is permissible under an existing provision in the Registry Agreement, identify the provision and provide rationale. If not applicable, respond with “N/A” and provide a complete response to question 5.1.

N/A

6. CONSULTATION

6.1. ICANN org encourages you to set up a consultation call through your Engagement Manager prior to submitting this RSEP request. This is to help ensure that necessary information is assembled ahead of time.

Identify if and when you had a consultation call with ICANN org. If you did not request a consultation call, provide rationale.

fTLD initially met with Cyrus Jamnejad on July 15, 2021, and then again on July 28, 2021. fTLD submitted its informal RSEP on August 12, 2021. fTLD has had numerous conversations with ICANN since the informal RSEP submission and ICANN provided written feedback on August 15, 2022.

6.2. Describe your consultations with the community, experts, and/or others. This can include, but is not limited to, the relevant community for a sponsored or community TLD, registrars or the registrar constituency, end users and/or registrants, or other constituency groups. What were the quantity, nature, and results of the consultations? How will the proposed service impact these groups? Which groups support or oppose this proposed service?

fTLD formed its DMARC Working Group in June 2018 and in addition to including Registrar and Registrant representatives, it includes or has included the following organizations: Agari, Amazon, Canadian Centre for Cyber Security, Cybersecurity and Infrastructure Security Agency (CISA for .GOV), dmarcian, Geekdom, Global Cyber Alliance, Google, LinkedIn, Microsoft,

National Cyber Security Centre (NCSC for .GOV.UK), National Cyber Security Centrum (.NL), Proofpoint, U.S. Department of Defense (.MIL), Universal Postal Union (.POST), and Valimail.

Furthermore, since fTLD introduced this concept to ICANN staff in 2018, primarily with Francisco Arias, the topic has also been discussed with David Conrad, John Crain, Carlos Alvarez, Gustavo Lozano Ibarra, Amanda Fessenden, Michelle Wilson, and Rod Rassmussen.

In the early stages of the development of the approach to PSD DMARC, the Working Group met bi-weekly until October 2018 when the IETF published the first Internet Draft. Since that time the Working Group has continued to meet as necessary, however much of the evolution of PSD DMARC occurred through comments and discussion on the IETF DMARC Working Group List. Information on the IETF DMARC Working Group is available at https://datatracker.ietf.org/group/dmarc/about/. In addition to the IETF engagement, fTLD presented the proposed capability to members of M3WAAG (https://www.m3aawg.org/about-m3aawg).

The fTLD consultations and coordination through its own private working group, the IETF Working Group resulted in extensive dialogue with email service operators, DNS service operators, email and email authentication technology subject matter experts, DNS subject matter experts, fTLD TLD registrants, internet security experts, and civil society groups.

How will the proposed service impact these groups?

The proposed service will not affect any of these groups unless they choose to implement the RFC 9091 changes for email receivers. As email receivers implement their support for this capability, they and their customers will benefit due to reduced delivery of unwanted and dangerous email payloads. fTLD TLD registrants will benefit due to reduced risk of their customers being misled by falsified email. Once implemented there will be a small increase in the number of DNS queries sent by email receivers and received by fTLD's DNS provider. It is not expected that this small change will have any impacts.

Which groups support or oppose the proposed service?

As discussed above there was IETF technical consensus to support PSD DMARC. The Cybersecurity and Infrastructure Security Agency, U.K. NCSC, and U.S. Department of Defense support PSD DMARC as demonstrated by their decision to publish PSD DMARC records. No groups have opposed the proposed service.

7. OTHER

7.1. Would there be any intellectual property impact or considerations raised by the proposed service?

No

7.2. Does the proposed service contain intellectual property exclusive to your gTLD registry?

No

7.3. Provide any other relevant information to include with the request. If none, respond with "N/A."

N/A

7.4. If additional information should be considered, attach one or more file(s) below.

Affected TLDs

Current Registry Operator	Top Level Domain	Registry Agreement Date
fTLD Registry Services LLC	bank	9/25/2014 12:00:00 AM
fTLD Registry Services LLC	insurance	2/19/2015 12:00:00 AM