Registry Services Evaluation Policy (RSEP) Request

June 30, 2022

Registry Operator
VeriSign, Inc.

Request Details
Case Number: 01131370

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.

Registry-Registrar Two-Factor Authentication Service

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

This submission is an update to Verisign's June 25, 2009 Registry-Registrar Two-Factor Authentication Service Request for the .com and .net TLDs (the "2009 2FA RSEP Request") and Verisign's February 1, 2011 Two-Factor Authentication Service Request for the .name TLD (the "2011 2FA RSEP Request") (collectively, the "2FA RSEP Requests"). In order to improve the security of registrar-registry communications, Verisign's 2FA RSEP Requests proposed implementing two factor authentication ("2FA") by requiring each registrar to provide a one-time password and a username and password in order to enable registrar access to Verisign's web-based "registrar portals."

Verisign's registrar portals enable registrars to: (a) access and manage certain registrar and registry information, such as transaction reports, invoices, maintenance notifications and marketing program information; (b) perform certain account management functions, such as designating points of contact and updating registrar contact information; and (c) manually perform certain domain name transactions for domain names for which the registrar is the registrar-of-record, such as updating, deleting or renewing a domain name.

The 2FA RSEP Requests indicated that Verisign's implementation of 2FA would "initially [be] an optional service for registrars who elect to use it", but that "once the service becomes widely adopted" Verisign intended for 2FA to become a requirement to protect the security of registry-registrar communications.

On July 10, 2009 and February 16, 2011, ICANN approved Verisign's 2FA RSEP Requests, authorizing Verisign's deployment of 2FA a "voluntary optional" service, including in Verisign's web-based registrar portals.

In the 10+ years since the 2FA RSEP Requests were filed, the use of 2FA has become an essential and standard security measure to protect web-based access to confidential or sensitive customer information that is a widely-implemented industry best practice, including by ICANN and within the broader ICANN community. Mandating the use of 2FA, particularly in the context of critical infrastructure, has been cited by the Biden administration and CISA as one of the tools that must be executed "with urgency" to protect critical infrastructure services.

Verisign is seeking ICANN's authorization to deploy 2FA as a requirement for registrar access to Verisign's web-based registrar portals. Following ICANN's approval, all registrar users will be required to provide a Time-based One-Time Password ("TOTP") and a valid username and password in order to login to Verisign's registrar portals.

By way of clarification, except as described herein, Verisign is not seeking any other changes or further authorizations to the prior 2FA RSEP Requests, including (i) in relation to the implementation of 2FA to communicate directly with Verisign's customer service via telephone, email and chat, which will continue to be voluntary and will evolve with technology standards to utilize TOTP as the authentication mechanism with plans to sunset VIP; or (ii) in relation to 2FA for EPP transactions.

1.3. Provide a technical description of the proposed service.

Verisign will implement 2FA using an Initiative for Open Authentication ("OATH") TOTP algorithm described in RFC 6238 or subsequent industry standard determined by Verisign. Verisign will use server-side code to create TOTP shared secrets, and generate and verify TOTP passwords, whereas registrars may use any compatible OATH TOTP-compliant client application of their choice, such as Authy, Google Authenticator, Microsoft Authenticator, etc, to generate the client-side TOTPs.

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.

https://www.icann.org/en/system/files/files/verisign-auth-request-25jun09-en.pdf
https://www.icann.org/en/system/files/files/verisign-name-request-1-01feb11-en.pdf

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

The implementation of mandatory 2FA in Verisign's registrar portals will benefit registrars and registrants by requiring an additional layer of security to protect registrar-registry communications against cyber-intrusions.

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

Following ICANN's approval, Verisign intends to provide 30-days prior notice to .com, .net and .name registrars in short order.

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

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?

The implementation of mandatory 2FA in Verisign's registrar portals will have no effect on the life cycle of domain names.

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

The implementation of mandatory 2FA in Verisign's registrar portals will not alter the storage and input of Registry Data.

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

The implementation of mandatory 2FA in Verisign's registrar portals will have no impact on throughput, response time, consistency or coherence of the responses to Internet servers or end systems.

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.

No technical concerns have been raised about the implementation of mandatory 2FA in Verisign's registrar portals.

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

Registrars users have had the ability since 2010 to optionally use a one-time password, in addition to a username and password, to access to Verisign's web-based registrar portals. Verisign has tested the 2FA-related server-side software throughout its development, including Quality Assurance (QA), and User Acceptance (UA) testing cycles. These tests have included manual, automated and user acceptance testing that covers a variety of customer-oriented use cases in preparation for the deployment of mandatory 2FA in Verisign's registrar portals.

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

Verisign will implement 2FA using an Initiative for Open Authentication ("OATH") TOTP algorithm described in RFC 6238.

3. COMPETITION

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

Verisign does not believe the implementation of mandatory 2FA in Verisign's registrar portals will have any positive or negative effects on competition.

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

Not applicable. The deployment of 2FA as a requirement for registrar access to Verisign's registrar portals is not a competitive service.

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

The use of 2FA as an essential security measure to protect web-based access to confidential or sensitive customer information has become a widely-implemented industry best practice, including by ICANN and within the broader ICANN community.

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?

Not applicable. The deployment of 2FA as a requirement for registrar access to Verisign's web-based registrar portals is not a competitive service. As noted above, registrars may use a TOTP-compliant application of their choice to generate the client-side TOTP necessary to enable 2FA access to Verisign's registrar portals.

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.

No.

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.

Verisign intends to provide prior notice to .com, .net and .name registrars and begin requiring the use of 2FA credential for access to Verisign's registrar portals beginning on or around July 1, 2022.

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.

No contractual provisions will be impacted by the implementation of mandatory 2FA in Verisign's registrar portals. Section 2.12(b) of Appendix 8A (Registry-Registrar Agreement) of the .com, .net and .name Registry Agreements provides that Verisign may establish "[o]perational standards, policies, procedures and practices for the Registry TLD. . . ." The deployment of 2FA as a requirement for registrar access to Verisign's web-based registrar portals will be deployed on a non-discriminatory basis to apply to every ICANN-accredited .com, .net and .name registrar.

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

The implementation of mandatory 2FA in Verisign's registrar portals will have no effect on the reporting of data to ICANN.

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

The implementation of mandatory 2FA in Verisign's registrar portals will not change the functionality, performance, or availability of RDDS.

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

The implementation of mandatory 2FA in Verisign's registrar portals will have no effect on the price of domain name registrations.

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.

The implementation of mandatory 2FA in Verisign's registrar portals will not result in a change to any subcontracting arrangements for the .com, .net and .name TLDs. Verisign notes that the Material Subcontracting terms set forth in the Base Registry Agreement are not applicable to the .com, .net and .name TLDs.

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.

N/A

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.

Section 2.12(b) of Appendix 8A (Registry-Registrar Agreement) of the .com, .net and .name Registry Agreements provides that Verisign may establish [o]perational standards, policies, procedures and practices for the Registry TLD. . . ."

While the deployment of 2FA as it relates specifically to the portion of Verisign’s 2FA RSEP Requests regarding authentication to Verisign’s web-based registrar portals is not a "Registry Service," and the updates set forth herein are not material changes to a Registry Service, Verisign is submitting this RSEP in response to ICANN’s approval of Verisign’s 2FA RSEP Requests (which contemplated further consultation in the event authentication moved from voluntary to mandatory).

The use of 2FA as a security measure to protect web-based access to confidential or sensitive customer information is widely-implemented industry best practice, including by ICANN and other registry operators.

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.

Verisign verbally consulted with ICANN on May 18, 2022 regarding the submission of this RSEP request.

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?

Verisign developed the concept of implementing 2FA in Verisign's registrar portals based on discussions with registrars who represent diverse market segments and who sought the added security resulting from adding 2FA, in addition to a user-name and password, to enable web-based access to Verisign's customer portals. Following ICANN's prior approval of the 2009 and 2011 RSEPs, Verisign held informal discussions with members of the RrSG. Verisign understood from those discussions that the RrSG members were concerned solely about the operational impact that could occur from requiring end-to-end 2FA authentication for EPP registry-registrar communications. These concerns were related to Verisign's 2009 RSEP that referenced a two-phased approach for implementing 2FA. The first phase related to implementation of 2FA in Verisign's web-based registrar portals and when communicating with Verisign's customer service department, and the second phase related to implementation of 2FA in EPP registry-registrar communications. As noted in response to question 1.2, Verisign has not implemented 2FA in EPP registry-registrar transactions and is not seeking authorization to implement 2FA in EPP registry-registrar transactions in this request.
Further, since Verisign's original RSEP requests in 2009 and 2011, the use of 2FA to protect web-based access to customer information has become a widely-implemented best practice, implemented within the ICANN community and by ICANN. Over 200 registrar users current utilize 2FA on an optional basis when accessing Verisign's customer portals and Verisign is unaware of any groups which would oppose the deployment of 2FA as a requirement for registrar access to Verisign's web-based registrar portals. As noted in question 1.6, Verisign

intends to provide registrars with 30-days written notice prior to deployment, and given the limited nature of the RrSG's original operational concerns, and the widespread use of 2FA within the industry, Verisign does not believe further consultation is necessary at this time.

7. OTHER

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

VeriSign is not aware of any intellectual property impact or considerations raised by the proposal to implement mandatory 2FA in Verisign's registrar portals.

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

Copyright and trade secret protection may exist or arise in connection with server-side code written by Verisign to create the TOTP shared secrets code or other materials created in connection with the implementation of mandatory 2FA in Verisign's registrar portals.

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

Verisign has no additional relevant information to submit.

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
VeriSign, Inc.	com	2020-03-27
VeriSign, Inc.	name	2012-12-01
VeriSign, Inc.	net	2017-07-01