ICANN Registry Request Service

Ticket ID: L5B1T-9A5R6
Registry Name: VeriSign, Inc,
gTLD: .COM, .NET, .NAME
Status: ICANN Review
Status Date: 2009-06-25 23:04:26
Print Date: 2009-06-25 23:04:33

Proposed Service

Name of Proposed Service:

Registry-Registrar Two-Factor Authentication Service

Technical description of Proposed Service:

Background:

The frequency and scope of domain name modification incidents that have not been requested or authorized by the registrant are increasing. Incidents include, but are not limited to, inadvertent modifications and errors processed by registrars and domain name hijacking involving compromised account credentials. The proposed Registry-Registrar Two-Factor Authentication service is part of a comprehensive domain name security enhancement program designed, among other things, to improve domain name security, and assist registrars in protecting registrants' accounts (the "Program"). The program addresses the two primary points of transactions:

o Registry-registrar - Phase I
o Registrar-registrant - Phase II

As part of VeriSign's proposed Registry-Registrar Two-Factor Authentication Service, the username and passwords currently used to process update, transfer and/or deletion requests will be augmented with dynamic passcodes, which will enable end-to-end transaction processing to be based on registrant requests that are validated by "what they know" (i.e., their username and password) and "what they have" (i.e., a two-factor authentication credential with a one-time-password).

o Phase I - Registrars will be able to use the one-time-password when communicating directly with VeriSign's Customer Service department and through the use of the Registrar portal when making manual updates, transfers and/or deletion transactions.
o Phase II - End-to-end security of the registrant's domain name is enhanced by requiring the addition of the one-time-password to the existing username and passwords for requests from a registrant to their registrar, and including the one-time-password in the EPP transaction from the registrar to the registry. Registrars would have the option to use either VeriSign credentials or any other vendor's credentials that comply with the open standard established by The Initiative for Open Authentication ("OATH") (see http://www.openauthentication.org).

Both phases of thee Registry-Registrar Two-Factor Authentication Service would initially be an optional service for registrars who elect to use it. Once the service becomes widely adopted, two-factor authentication credentials will become a

requirement for Registry-Registrar transactions.

Domain Name Security Enhancement Program

The Registry-Registrar Two-Factor Authentication Service is part of a larger domain name security enhancement program launched by VeriSign.

(1) Registrar-Registry Communications. The first component entails providing registrars with two-factor authentication credentials for their employees who are authorized to interact with VeriSign's Customer Service via web interface in order to authenticate specified actions requested for a domain names for which such registrar is the registrar-of-record. Two-factor authentication credentials will merely augment the current security practices. VeriSign's goal is to increase the ability to authenticate and track requests by individual authorized employees of the registrars and improve the ability for registrars to maintain security when there are personnel changes. VeriSign will deploy the VeriSign Identity Protection Service (VIP) and will distribute Oath-based two factor authentication credentials to protect the registry-registrar transactions. VeriSign will provide the VIP service authorized registrar representative at no cost to the registrar. A description of the VIP two factor authentication service is provided in Exhibit A.

(2) Registrar-Registrant Communications -- Best Practices. The second component entails educating registrars about, and offering them an opportunity to implement, two-factor authentication credentials for communications between registrars and their registrants. VeriSign's goal is to encourage registrar to registrant two-factor authentication as a best practice in order to improve security for domain name modifications, transfers and deletions from registrant to registrar.

(3) Registrar-Registrant Communications. The third component entails providing registrants with two-factor authentication credentials so they can authenticate themselves when accessing their accounts with an ICANN accredited registrar and passing that authentication confirmation to the Registry. Two-factor authentication credentials will augment the current EPP commands for transfers, updates and deletes. VeriSign's goal is to increase the ability to authenticate and track requests by individual registrants helping a registrar provide a more secure transactional experience for their customers. Registrars will have the option to use either VeriSign credentials (VeriSign Identity Protection or VIP) or any other vendor's credentials that comply with the open standard established by OATH.

Consultation

Please describe with specificity your consultations with the community, experts and or others. What were the quantity, nature and content of the consultations?:

a. If the registry is a sponsored TLD, what were the nature and content of these consultations with the sponsored TLD community?:

Not applicable

b. Were consultations with gTLD registrars or the registrar constituency appropriate? Which registrars were consulted? What were the nature and content of the consultation?:

VeriSign developed the concept for the Registry-Registrar Two-Factor Authentication Service based on discussions with several registrars who represent diverse market segments. VeriSign has also received positive feedback from registrars who have already begun work on implementing two factor authentication credentials for communications between registrars and their registrants as described above in paragraph (2) (Registrar-Registrant Communications -- Best Practices).

c. Were consultations with other constituency groups appropriate? Which groups were consulted? What were the nature and content of these consultations?:

Not Applicable

d. Were consultations with end users appropriate? Which groups were consulted? What were the nature and content of these consultations?:

While we have anecdotal evidence that this is a valuable service for the registrar and registrant segments of the community, we do not (and will not) have any systematic data owing to the fact that we do not have direct relations with registrants. VeriSign intends, however, to obtain feedback from registrants through the registrar channel. Such feedback will be incorporated into the development and implementation processes for the Registry-Registrar Two-Factor Authentication Service - Phase II

e. Who would endorse the introduction of this service? What were the nature and content of these consultations?:

Registrars and registrants would likely endorse the introduction of the Registry-Registrar Two-Factor Authentication Service since it will enhance domain name security from end-to-end.

f. Who would object the introduction of this service? What were(or would be) the nature and content of these consultations?:

To date, no one has objected to the introduction of either phase of the Registry-Registrar Two-Factor Authentication Service.

We are not aware of any constituency or community that would object to this service, especially in light of the fact that the service will be offered to all registrars as an optional, value-add service, and the service does not require that the two factor authentication credentials be obtained from VeriSign. Under the program, registrars would have the option to use either VeriSign credentials or any other vendor's credentials that comply with the open OATH standards. Those standards are currently supported by at least 70 vendors. .

Timeline

Please describe the timeline for implementation of the proposed new registry service:

Implementation for Registry-Registrar Two Factor Authentication Service - Phase I

- VeriSign publishes the EPP extension technical documentation and processes for the implementation of the proposed service. (Q3 2009)
- VeriSign will deploy the EPP extensions into the .com and .net Operational Test and Evaluation ("OTE") environment for registrars to test their systems (Q1 2010).
- VeriSign will then enable the VIP two factor authentication solution on the registry-registrar web interface and Registrars could choose to adopt. VeriSign will provide registrars two factor authentication credentials at no cost.
- Once the service becomes widely adopted, two-factor authentication credentials will become a requirement for Registry-Registrar transactions. There is no proposed timeline for this milestone at this time.
- The proposed service supports all appropriate EPP domain name transactions (i.e., modifications, transfers and deletes) (TBD).

Implementation for Registrar-Registrant Two Factor Authentication Service - Phase II
- As a best practice, registrars may choose VeriSign's VIP service to protect the registrar-registrant transactions or choose to deploy a strong authentication solution from another solution provider.
- VeriSign will deploy the EPP modifications into the automated interface between the registry and registrar.(Q2 2010)
- Registrars will choose to adopt the service or not for some or all of their registrants. Registrars will modify the affected commands within the EPP protocol prior to passing authentication information to the registry.

- If a registrar chooses the VIP, they will be presented and sign the standard VeriSign Master Service Agreement (required for the VIP Service). The registrars may use Oath credentials provided by VeriSign or any other certified supplier of Oath credentials.
- If a registrar chooses to use another strong authentication (OATH) solution, VeriSign will qualify that solution and then make it a part of the EPP modifications.
- The proposed service supports all appropriate EPP domain name transactions (i.e., modifications, transfers and deletes) (TBD).

Business Description

Describe how the Proposed Service will be offered:

VeriSign will implement the Registry-Registrar Two-Factor Authentication Service in phases:

-Registrars will have the ability to implement the two-factor authentication with their registrants, either on a per domain name basis, or on a per registrant basis.
- VeriSign will operate the proposed service for registry-registrar transactions in a transitional period during which time one-time passwords are accepted through EPP. The transitional period will be designed to allow registrars to ramp up implementation and gain experience.
- VeriSign provides support and requires two-factor authentication for selected services, such as Registry Lock.

Registry-Registrar - Phase I

VeriSign will not charge registrars for the Two-Factor Authentication Service used to protect the registry-registrar transactions as long as VeriSign operates the .com and .net registries.

Registrar-Registrant - Phase II

As part of best practices registrars are recommended to deploy a two factor authentication solution from VeriSign or another solution provider to protect the registrar-registrant transactions.

As part of VeriSign's commitment to support end-to-end security of the transaction, VeriSign will provide the VIP two factor authentication services at no cost to registrars for a minimum of three years assuming the registrar has contracted with VeriSign for the service by October 31, 2009 and commit to have the service operational by June 30, 2010. Registrars may also use OATH-based mobile credentials provided by VeriSign at no cost. VeriSign will charge registrars a minimal fee for

any hardware based credentials. Registrars also have the option to purchase Oath based credentials directly from any certified supplier of OATH credentials.

Describe quality assurance plan or testing of Proposed Service:

VeriSign has demonstrated the ability to deliver scalable and reliable registry services. The rigorous development processes, extensive suite of quality assurance tests, and performance testing will be applied to maintain the functionality, data integrity and data accuracy of the Registry-Registrar Two-Factor Authentication Service.

Testing the implementation of the proposed service will include the internal testing that is part of VeriSign's software development lifecycle process, plus a beta testing phase with registrar participation. Upon successful completion of the beta testing, registrars will be able to test service implementation in the .com/.net Operational Test and Evaluation environment.

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

None.

Contractual Provisions

List the relevant contractual provisions impacted by the Proposed Service:

No contractual provisions will be impacted.

What effect, if any, will the Proposed Service have on the reporting of data to ICANN:

The service will not change or add to the reporting of data to ICANN.

What effect, if any, will the Proposed Service have on the Whois?:

The service will not change the functionality, performance, or availability of Whois

Contract Amendments

Please describe or provide the necessary contractual amendments for the proposed service:

No contractual amendments will be required. The implementation specifications would be defined in an EPP extension that VeriSign will publish in advance for registrars and post with technical implementation documents on the registrar section of the registry website.

Benefits of Service

Describe the benefits of the Proposed Service:

As more fully described above, the Registry-Registrar Two-Factor Authentication Service is intended enhance domain name security resulting in increased confidence and trust by registrants.

Competition

Do you believe your proposed new Registry Service would have any positive or negative effects on competition? If so, please explain.:

The Registry-Registrar Two-Factor Authentication Service would have no negative effects on competition especially in light of the fact that Registrars will be permitted to use any authentication vendor that complies with the open OATH standard. There are at least seventy (70) vendors who currently support the OATH standard.

How would you define the markets in which your proposed Registry Service would compete?:

The intended market for this service is all .com and .net accredited registrars.

What companies/entities provide services or products that are similar in substance or effect to your proposed Registry Service?:

At least seventy (70) vendors provide two-factor authentication credentials that comply with the OATH standard.

In view of your status as a registry operator, would the introduction of your proposed Registry Service potentially impair the ability of other companies/entities that provide similar products or services to compete?:

No. Under VeriSign's proposal, registrars may use VeriSign's VIP service, or choose another vendor that complies with the OATH standard, which is an open standard currently supported by at least 70 vendors

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

No

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

No

Do you have any documents that address the possible effects on competition of your proposed Registry Service? If so, please submit them with your application. (ICANN will keep the documents confidential).:

VeriSign has no documents to submit.

Security and Stability

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

No

Please explain how the proposed service will affect the throughput, response time, consistency or coherence of reponses to Internet servers or end systems:

The Service will have no impact on throughput, response time, consistency or coherence of the responses to Internet servers or end systems.

Have technical concerns been raised about the proposed service, and if so, how do you intend to address those concerns?:

No

Other Issues

Are there any Intellectual Property considerations raised by the Proposed Service:

VeriSign is not aware of any intellectual property considerations.

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

(1) Trademark or similar rights may exist or arise with respect to trade names or terminology used in connection with the proposed Service. (2) Copyright protection may exist or arise in connection with code written or materials created in connection with the proposed service. (3) Certain information or processes related to the service may be confidential to VeriSign and/or subject to trade secret protection. (4) VeriSign is not aware of the issuance of any patents by any party with respect to the service.

List Disclaimers provided to potential customers regarding the Proposed Service:

We expect to include in the agreement governing the service certain industry standard disclaimers of warranties.

Any other relevant information to include with this request:

Exhibit A - Overview of VeriSign Identity Protection Service (VIP)

VeriSign Identity Protection (VIP) is a comprehensive suite of identity protection and authentication services that enable web applications to provide a secure online experience for end users at a reasonable cost. The VIP Validation Services are hosted by VeriSign and are accessed through standard network protocols for easy integration into existing Internet applications. To minimize costs and maximize security by sharing intelligence and resources, the VIP Services are backed by the power of the VIP Network. The VIP Network enables sharing authentication credentials through the VIP Shared Authentication Network. The unique values of VIP include:

o Easy - VIP enables a higher security experience for the consumer in a way that is friendly to their current Web lifestyle. VIP's unique service-based approach allows the enterprise to outsource complexity and quickly deploy strong authentication.
o Trusted - For the past decade, VeriSign has provided authentication services to over 400,000 websites including 93% of the Fortune 500, 94% of the largest e-commerce sites and 100% of the world's largest banks. As a result, customers recognize and trust the VeriSign logo.

Use of VIP Service

1. User downloads VIP Mobile Application from https://mobile.verisign.com/ or iTunes for the iPhone application. Note that SMS OTP or standalone hardware devices can provide the same or similar functionality.
2. User logs into registrar application.
3. User is directed to bind or register their VIP Mobile Application with their account to protect their account (user needs to enter the credential ID, and two consecutive One Time Passcodes from their VIP mobile application).
4. User can also enable other authentication means (e.g. a simple Q&A, an automated call to a pre-registered phone or other out-of-band methods) in case they need access when they aren't in possession of the VIP Mobile Application.
5. User can also enable a simple Q&A in case they need access when they aren't in possession of the VIP Mobile Application.
6. Account is now protected by VIP.
7. Every time the user logs in, they will be asked to enter their username and password as well as a one time passcode from their VIP Mobile Application.

The VIP Service leverages a shared validation infrastructure operated by VeriSign that enables enterprises such as registrars to deploy strong authentication without bearing the burden of managing and operating a self-standing authentication infrastructure.

VIP Mobile Two Factor Authentication Credentials
VeriSign provides an OTP token that can work on the mobile phone supporting 170 Mobile devices including the popular iPhone, Blackberry (Storm, Curve, Pearl and Bold), Motorola RAZR and others from Motorola, Nokia, Sony Ericsson, LG and Samsung.

In this approach, the user's existing phone or PDA becomes an OTP token. The appropriate software and personalization information can be provisioned on the mobile device over-the-air from a VeriSign hosted service. To download the VIP Mobile Application and get a VIP Credential, follow this link:

https://mobile.verisign.com/

Alternative Credentials
VIP, built on the Open Authentication (OATH) standard, allows VeriSign to provide a range of two factor authentication mechanisms to VeriSign. Providing a range of authentication solutions may be necessary in order to ensure ubiquity across a diverse user group.

User credentials can be provisioned, fulfilled, and validated using the same platform. Electing to utilize the VIP solution will allow <<Customer>> to cost effectively introduce new authentication mechanisms and credentials in the future, without the need to re-engineer applications or deploy new infrastructure.

OTP Token and SMS OTP
VeriSign one-time password token is based on proven one-time password technology. The low-cost token is ideal for large consumer application because it is cheap, robust and very easy to use. Additionally, it is 'platform neutral' which is important for deploying a solution that is ubiquitous. The token requires no additional client software and is not dependent on a user's desktop configuration or operating system.

To obtain an OTP, the user presses a button on the token to trigger the next OTP value. The resulting value is displayed on a small LCD. To authenticate to an application, the user enters this value, along with his or her traditional username and password combination.

This token today supports a time-based algorithm for OTP generation. VeriSign will also have this form factor available that supports a time and event-based algorithm for OTP generation

SMS Validation delivers an OTP via SMS via out-of-the-box integration with VIP Service and the VeriSign Messaging Gateway. There are three use cases:

o The Primary authentication mechanism, where the user does not have a mobile phone capable of supporting the VIP Mobile application

o An interim credential to enable immediate VIP protection while other credentials are being sent to the customer

o Temporary password support for hardware VIP credentials