ICANN Registry Services Technical Evaluation Panel

# Report on Internet Security and Stability Implications

of the

# Public Interest Registry (PIR)

# Technical Bundling Proposal

24 July 2014

# Preface

This report presents the findings of a technical evaluation of the proposal[1] by Public Interest Registry (PIR) to amend their registry agreement with ICANN in order to implement mandatory technical bundling of second level domain registrations for .NGO and .ONG.

On 8 November 2005 ICANN adopted[2] a consensus policy developed by its Generic Names Supporting Organization (GNSO) concerning the review and approval of requests by gTLD registry operators for new registry services.[3] This policy was implemented on 25 July 2006[4] as the Registry Services Evaluation Policy.[5] The policy provides for the evaluation of a proposed registry service by a team of experts selected from a standing Registry Services Technical Evaluation Panel (RSTEP)[6] when ICANN determines that the service could raise significant security or stability issues.

The process begins with a preliminary determination by ICANN that an RSTEP review is or is not required for a particular proposed registry service.[7] If ICANN determines that a review is required, an RSTEP review team investigates and evaluates the proposed service with respect to its potential impact on security or stability, as defined by the consensus policy:

> **Security**—An effect on security by the proposed Registry Service shall mean (a) the unauthorized disclosure, alteration, insertion, or destruction of Registry Data, or (b) the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards.
>
> **Stability**—An effect on stability shall mean that the proposed Registry Service (a) is not compliant with applicable relevant standards that are authoritative and published by a well-established, recognized, and authoritative standards body, such as relevant Standards-Track or Best Current Practice RFCs sponsored by the IETF, or (b) creates a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems operating in accordance with applicable relevant standards that are authoritative and published by a well-established, recognized, and authoritative standards body, such as relevant Standards-Track or Best Current Practice RFCs and relying on Registry Operator's delegation information or provisioning services.

[1] https://www.icann.org/en/resources/registries/rsep/pir-request-21may14-en.pdf

[2] http://www.icann.org/minutes/resolutions-08nov05.htm

[2] http://www.icann.org/minutes/resolutions-08nov05.htm

[3] The ICANN Board resolution adopting the GNSO consensus policy (see footnote 2) specifies that implementation of the policy in contractual terms should be guided by the provisions of the .NET registry agreement (http://www.icann.org/tlds/agreements/net/net-agreement-new.html), which includes a precise definition of "Registry Services."

[4] http://www.icann.org/announcements/rsep-advisory-25jul06.htm

[5] http://www.icann.org/registries/rsep/rsep.html

[6] http://www.icann.org/registries/rsep/rstep.html

[7] The consensus policy also provides for the separate review of potential competition issues, which lie outside the scope of the RSTEP review.

The review team completes its evaluation within 45 days, and prepares a written report of its findings, containing:

> (a) a detailed description of the technical issue(s) raised by the proposed registry service, and the assumptions, information,[8] analysis, and reasoning upon which the review team's evaluation is based;
>
> (b) the team's expert assessment of the potential impact of the proposed registry service on security or stability; and
>
> (c) a response to any specific questions from ICANN that were included in the referral from ICANN staff in its request for the RSTEP review.

The review team's report is delivered to the ICANN Board as input to the Board's consideration of the proposed registry service and action on the registry operator's request to deploy the service within the context of its contract with ICANN.

It is important to recognize that the RSTEP review is a technical evaluation of a proposed registry service with respect to the likelihood and materiality of effects on security and stability, including whether the proposed registry service creates a reasonable risk of a meaningful adverse effect on security or stability. Because many other questions and issues may be relevant to the overall assessment of a proposed registry service, it is not a recommendation to the ICANN Board concerning whether or not the Board should approve or reject the registry operator's proposal.

[8] RSTEP review teams are expected to gather information from as many sources as necessary in order to conduct a thorough and comprehensive evaluation, including, but not limited to, information provided by the registry operator, by ICANN, and by contributors to the ICANN public comment forum that is associated with each registry service request.

# Table of Contents

Table of Contents ........................................................................................ 4

1. Introduction............................................................................................. 5

1.1 PIR's Summary of the Proposal.........................................................................5

1.2 RSTEP Process Summary..................................................................................5

1.3 Key Definitions..................................................................................................6

1.3.1 Security .........................................................................................................6

1.3.2 Stability .........................................................................................................6

1.4 Members of the RSTEP Review Team for this Proposal ....................................6

1.5 Support for the Review Team ............................................................................7

2. Summary of Findings ................................................................................. 8

3. Analysis of Security and Stability Issues .................................................. 9

3.1 User Expectations ..............................................................................................9

3.2 Registrar Implementation May Create Registrant Confusion Leading to Resolution Failure .....................................................................................................................9

3.3 Taking Down Both Names In a Bundle............................................................10

3.4 Reporting and Handling of Inconsistent Data Between .ngo and .ong..............11

3.5 DS Record Addition for a Second Zone in a Bundle........................................11

3.6 DS Records Without Matching DNSKEY Records..........................................12

3.7 Registrant Confusion About Non-Separability of whois Data .........................12

Appendix A. Additional Material Supplied by PIR ..................................... 14

# 1. Introduction

## 1.1 PIR's Summary of the Proposal

PIR's proposal is to offer as a registry service support for mandatory technical bundling of second level domain registrations for .NGO and .ONG. As described in the proposal, PIR's summary is:

> A Technical Bundle is a set of two domain names in different TLDs, with identical second level labels for which the following parameters are shared:
>
> - Registrar Ownership
> - Registration and Expiry Dates
> - Registrant, Admin, Billing, and Technical Contacts
> - Name Server Association
> - Domain Status
> - Applicable grace periods (Add Grace Period, Renewal Grace Period, Auto-Renewal Grace Period, Transfer Grace Period, and Redemption Grace Period)
>
> [a]nd for which at least the following parameters are unique:
>
> - DS records as required based on RFC 5910
>
> Technical Bundling is defined as the process of managing a Technical Bundle.

## 1.2 RSTEP Process Summary

The RSTEP review team evaluated the PIR proposal with respect to its potential impact on Internet security and stability.

The review team took the following actions during the 45-day period beginning with the referral from ICANN to the Chair of the Registry Services Technical Evaluation Panel[9] on 9 June 2014:

- Participated in an email-based discussion of the potential security and stability impact of the mandatory technical bundling service that PIR wants to provide for the gTLDs .ngo and .ong;
- Prepared questions for PIR concerning the proposal, which were sent to ICANN on 24 June 2014;
- Received answers to those questions and a package of additional PIR marketing material[10] related to the Technical Bundling service on 10 July 2014;

[9] https://www.icann.org/en/system/files/correspondence/papac-to-chapin-06jun14-en.pdf

[10] .ngo | .ong Product Description Version 1.1 – May 2014 (provided by PIR)

- Reviewed the answers and additional material and prepared follow-up questions for PIR, which were sent to ICANN on 14 July 2014;
- Participated in a teleconference on 14 July 2014 with representatives of PIR to discuss the follow-up questions; and
- Received answers to the follow-up questions on 18 July 2014.

## 1.3 Key Definitions

### *1.3.1 Security*

As defined by the GNSO Recommendation concerning the establishment of the Registry Services Evaluation Process,[11] an effect on security by the proposed Registry Service shall mean (A) the unauthorized disclosure, alteration, insertion or destruction of Registry Data, or (B) the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards.

### *1.3.2 Stability*

As defined by the GNSO Recommendation concerning the establishment of the Registry Services Evaluation Process, an effect on stability shall mean that the proposed Registry Service (A) is not compliant with applicable relevant standards that are authoritative and published by a well–established, recognized and authoritative standards body, such as relevant Standards–Track or Best Current Practice RFCs sponsored by the IETF or (B) creates a condition that adversely affects the throughput, response time, consistency or coherence of responses to Internet servers or end systems, operating in accordance with applicable relevant standards that are authoritative and published by a well–established, recognized and authoritative standards body, such as relevant Standards–Track or Best Current Practice RFCs and relying on Registry Operator's delegation information or provisioning services.

## 1.4 Members of the RSTEP Review Team for this Proposal

The five members of the RSTEP review team for the PIR Technical Bundling proposal are:

- Susan Estrada
- Paul Hoffman (chair)
- Merike Kaeo
- Jim Reid
- Wil Tan

[11] http://gnso.icann.org/issues/registry-services/final-rpt-registry-approval-10july05.htm#5

The members of the review team were assisted in their work by the Chair of the Registry Services Technical Evaluation Panel, Lyman Chapin.

## 1.5 Support for the Review Team

Staff support was provided by Krista Papac, ICANN Director of Registry Services. The review team thanks ICANN for providing teleconference facilities.

# 2. Summary of Findings

**Our technical evaluation of this proposed registry service with respect to the likelihood and materiality of effects on security and stability concludes that it does not create a reasonable risk of a meaningful adverse effect on security and stability.**

This finding is predicated on PIR demonstrating to ICANN's satisfaction throughout the lifetime of the service that PIR is capable of operating the service as it is specified in the combination of registry service application and the answers to the questions asked by the review team.

In order to present a complete analysis of the issues facing all of the parties affected by the PIR proposal (registrants of .ngo and .ong domain names, users of the DNS who look up names in those zones, registrars, users of the DNS as a whole, and PIR itself), the review team identified and analyzed many real but less critical potential stability issues in addition to those summarized above. These are included in Section 3 of this report.

# 3. Analysis of Security and Stability Issues

## 3.1 User Expectations

The review team recognizes that there are numerous security and stability considerations when users expect two domain names to “give the same result” or to “act the same.” Such expectations can arise when a registrant or registry makes such claims. Common cases are SLDs that have semantically similar names (such as “example.com” and “examplecorp.com”), the same second level name that appears in possibly–related TLDs (such as two TLDs that translate to the same semantic word or name), and so on. Such situations already exist throughout the DNS.

PIR describes the motivation for the Technical Bundling service in their proposal as:

> The proposed Technical Bundling service will serve the NGO community by protecting against public confusion that reasonably may ensue if different NGO entities were able to register the same second-level domain. It also will help mitigate the need for defensive registrations.
>
> Technical Bundling of .NGO and .ONG would serve to protect against public confusion that reasonably may ensue if different NGO entities were able to register the same second-level domain name, one in .NGO and the other in .ONG. Also Technical Bundling will help mitigate the need for defensive registrations, thereby allowing NGO community registrants, whether in .NGO or in .ONG, to focus on their mission and outreach in a transparent and effective manner.

The review team finds that this wording, as well as the similar wording about motivation in the Product Description, does not cause any new expectations for users beyond what is already common in the DNS. There is no indication that PIR will market the service as causing a pair of names from a bundle to “be the same,” to “act the same,” or other phrases that would cause more significant security and stability issues. However it would be prudent to expect that registrars will perceive both names in the bundle to be “the same” because most EPP transactions on one name will automatically apply to the other. That is likely to pervade their thinking, both in terms of provisioning and engineering. This in turn is likely to trickle down into customer communications, perhaps in an even more garbled form, that reach registrants and the general public. It will require great care by all parties to make sure that wrong or misleading expectations are not set over “sameness” or at least kept to a minimum.

## 3.2 Registrar Implementation May Create Registrant Confusion Leading to Resolution Failure

Registrants who use both domains in the bundle may think that the two are standalone domains, distinct from an operations perspective. The review team believes that a likely scenario is that registrants will redirect traffic (using different technical means for different protocols) from one of the two names in a bundle to the other name. Such a registrant may also believe that they can change the name servers for the two names independent of each other, due to lack of education or support from their registrar or DNS provider.

At some point, a registrant with such a redirected name pair might decide to move the name to different nameservers, such as at a new hosting provider. A reasonable way to do this move would be to move the unimportant name first. However, if the registrant has forgotten that the two name servers will move in tandem, they will move the name servers for the more important name in the pair.

The review team notes that registry literature seldom reaches registrants or Internet users. Registries rely on registrar channels to get the word out. However, registrars may not be motivated to customize their software or processes to support the technical bundle, unless it is enforced by the registry-registrar agreement of the TLD, and PIR's proposal does not discuss any such enforcement. The review team thus concludes that there are stability issues inherent in the system in the proposal. These issues can be partially mitigated by better education from the registrars to the registrants.

## 3.3 Taking Down Both Names In a Bundle

In response to the question "Please describe what actions would be taken if only one of the two names in a bundle was determined to be used for abusive behavior such as phishing scams or spam," PIR says:

> In cases where one of the two domain names are determined to be abusive, and is scheduled for a takedown process, to ensure consistency, both domain names within the Technical Bundle will be scheduled for the takedown process.

The review team finds that this presents a potentially small risk of adverse effect on stability because an otherwise "innocent" zone could be removed, affecting those using any name in that zone, even though the zone was not involved in a complaint or takedown request.

It is unclear whether or not registrants and registrars will be aware that domain names in a technical bundle will inherently share the same fate with respect to takedowns. Although it would be reasonable to expect this to be included in the registry's terms and conditions, that might not be enough to explain matters to affected stakeholders, some of whom will not be the registrar or registrant.

The review team considered an alternative approach in which only the "guilty" domain in the bundle was taken down, but this is also likely to present stability issues. There could also be security concerns if the registrant is unwilling to act on the takedown complaint while the other name in the bundle remains active. If just one name in the bundle is removed in a takedown request, this would create discrepancies that undermine the rationale for Technical Bundling. That is likely to create confusion for stakeholders and the broader Internet community.

Given that both approaches have a small risk of adverse effect on stability, the review team is satisfied with the option chosen by PIR. However, the review team suggests that ICANN require PIR to monitor and evaluate the effects of takedowns in .ngo and .ong, and possibly consider changing how takedowns in bundled TLDs should be handled in the future.

## 3.4 Reporting and Handling of Inconsistent Data Between .ngo and .ong

In its answers to the review team's questions, PIR commits to scanning the two zones daily to look for incorrect differences between the two zones. However, there is no method mentioned in the proposal or the answers to the review team's questions for someone outside PIR (such as a registrant or registrar) to report incorrect differences. This means that such differences can exist in the zone for a day (or longer, depending on how quickly PIR remediates the problem). Differences could mean that the delegation NS records for one domain in the bundle are missing, or it could mean that the set of NS records used for both domains are different, or other inconsistencies. This can have stability issues for users of the domains.

The proposal and the answers are also unclear about what PIR would do if an inconsistency were found between the two TLDs in the bundle. In the interests of stability, the review team suggests that PIR document clear procedures, roles, and responsibilities when dealing with any detected inconsistencies found. This would include the definition and anticipated classes of inconsistency, along with stakeholders, responsible parties, procedures, communications, and remedies required for each class of inconsistency discovered. Since the service described in the proposal is uncommon in the gTLD environment, the documentation for these procedures would be invaluable for transitioning to an EBERO provider if that became necessary.

## 3.5 DS Record Addition for a Second Zone in a Bundle

The review team finds that the process described in the proposal for adding DS records for the two names in the bundle can lead to some confusion on the part of registrars, and thus to possible security and stability issues if registrars do not follow PIR's instructions carefully. The proposal says:

> Domain Create - If any DS information is specified at the time of a domain create, those records will only be associated to the domain name specified in the create command. In order to associate DS records to the appropriate domain names within the bundled set of domain names, the domain update command must be utilized.
>
> Domain Update - If DS records are specified in the domain update command, those records will only be associated with the domain name specified in the domain update request.

The registrar for the bundle of example.ngo and example.ong can supply DS records only for the name registered, not the second name that comes in the technical bundle. If the registrant has supplied the registrar with DS records for both of the names, the registrar needs to take a second action after the Domain Create command: it must give a Domain Update command for the second name.

This is a new process for registrars, one with which they are probably unfamiliar, and thus they might not give the Domain Update command correctly, or at all. The result of that would be that only one of the two names had a DS record in the zone and therefore the second name is not protected by DNSSEC.

There are associated situations related to registrant error that are possibly made worse by the service. A registrant that wants to run DNSSEC on all their domains, even the ones that they don't care about, might start to neglect the DNSSEC records for the second domain in the bundle. By automatically giving every registrant a second domain name, PIR is offering a service to those who want it and possibly a burden to those who don't. If the response to the burden is to neglect the DNSSEC keys, it increases the risk of validation failures.

The review team believes that such a situation can be ameliorated by training and outreach on the part of PIR. The extent of such training is not covered in their proposal. However, even with lots of training, the review team expects higher likelihood of DNSSEC–related errors caused by registrars or registrants in the service than there are in typical TLDs.

## 3.6 DS Records Without Matching DNSKEY Records

The review team notes that the Product Description allows a situation that has significant adverse security and stability implications: it allows the addition of a DS record in the .ngo or .ong zones even when there are no DNSKEYs in the child zone. The wording in the Product Description is:

> Because DS records may exist in the parent zone before the corresponding DNSKEY exists in the child zone, Afilias cannot immediately check that a DS record offered by the registrar "completes the trust chain" to the child zone.

The Product Description does not say whether PIR would first check whether there is already a DNSKEY record in the child zone that has a corresponding DS record in the parent. If such a check is not made and none of the domain's DS records in the parent zone have corresponding DNSKEY records in the child zone, the child zone would immediately be considered insecure by any validating resolver.

However, the review team also notes that it does not know of any case in which a TLD that is contracted with ICANN is required to make such a check. The review team encourages ICANN, possibly after consultation with SSAC and the DNSSEC operations community, to consider placing such a requirement on all contracted TLDs that support DNSSEC.

## 3.7 Registrant Confusion About Non-Separability of whois Data

Registrants may forget that the two names in a bundle are bound to each other, such as if their registrar's tools allows them to manage either name in the same fashion. The review team believes that if registrants do forget this, it may lead to unexpected results and confusion when such a registrant updates their whois contact data. This is unlikely to create any significant security or stability concerns because the registry guarantees that the same whois data are published for both domain names in the bundle. Clear communication from the registrars should reduce the potential for confusion to the registrant and other stakeholders.

# Appendix A. Additional Material Supplied by PIR

During the course of the review team's deliberations, it asked PIR for additional information concerning its proposal in two sets of questions. This Appendix contains a verbatim transcript of PIR's response to the second set of questions. It includes both the questions from the review team and PIR's responses.

## Technical Bundle Technical Design Description

This section is to describe the technical design and implementation approach in regards to Technical Bundling. This section is intended to answer many of the questions raised by the RSTEP panel, and potentially additional questions may arise further in the review process. This section will also be referenced throughout the document.

Both the .NGO and .ONG TLDs will reside within a single instance of the Registry System, with one master database. Registrars will connect to one instance of the Registry System via EPP to perform all related EPP transactions for both .NGO and .ONG.

In addition to the EPP service, the following Registry Services will interface with the master database as the authoritative source of all domain name related information for both .NGO and .ONG:

- WHOIS Service
- DNS Zone File Generation Service
- Data Escrow Service
- Web Administration & Reporting

As a result, atomicity, correlation and updates are maintained across the two TLDs.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

In order to ensure consistency of both domain names and its parameters within the Technical Bundle, for each Technical Bundle registered via the EPP Domain Create command, the Registry System stores one domain attribute object that is referenced by the .NGO and .ONG domain names within the Technical Bundle. This ensures that the domain attribute object along with its associated objects such as domain contacts, domain statuses, and domain nameservers needs to be updated only once for the changes to be reflected for each domain name within the Technical Bundle.

DS Data, however, is tied directly to the domain name because DS data can be different between the TLDs for a given domain name within a Technical Bundle. Each domain name can have multiple DS records for each TLD within the Technical Bundle.

**Domain Registration Process**

In order to further clarify how the above data model is implemented; the following high level steps will describe the registration process of a bundled .NGO and .ONG domain name:

1. Registrar submits via EPP, one EPP create command for either the .NGO or the .ONG domain name, along with its appropriate parameters such as term of registration, contact associations and nameserver associations.
2. The Registry System, through confirmation internally that the desired domain name is part of a Technical Bundle. The Registry System will check to ensure that the domain name within the Technical Bundle is available for registration and is not reserved or blocked. If the name is available, then the bundle is available.
3. If the bundle is available for registration, the [redacted] data objects are created:

   [redacted]

   d. Upon successful creation of all relevant objects, the database transaction is committed.
4. Upon successful completion of step 3, the Registry System will respond to the Registrar with the appropriate successful EPP create response.

This implementation approach will ensure that all relevant parameters that are shared for the two domain names within the Technical Bundle are always synchronized within the Registry System.

The following lists captures the parameters that are shared between the .NGO and .ONG domains names within the Technical Bundle [redacted]:

- Registrar Ownership/Sponsor; [redacted]

- Registration Date; [redacted]
- Domain Expiry Date; [redacted]
- Registrant, Admin, Billing, and Technical Contacts; [redacted]
- Name Server Association; [redacted]
- Domain Status, including both client and server statuses; [redacted]
- Applicable grace periods [redacted]

## Responses to Questions from RSTEP Review Team – Part 1

***<u>The proposal is not clear about the atomicity of operations. Please state whether the implementation is a bundle object or simply bundled operations.</u>***

Referencing the above section, "Technical Bundle Technical Design Description", the same domain attribute object is referenced by both the .NGO and .ONG domain names within the Technical Bundle; thus utilizing a bundled object implementation approach.

***<u>Please describe the atomicity of zone file publication. How will the two zone files be correlated?</u>***

There will be two zone files that will be generated, one for .NGO and another for .ONG. Zone generation for both .NGO and .ONG zone files involves the creation of DNS zone information (resource records, or RRs) using the Registry System master database as the authoritative source of domain names and their associated hosts (nameservers).

Referencing the above section, "Technical Bundle Technical Design Description", the same domain attribute object is referenced by both the .NGO and .ONG domain names within the Technical Bundle. Given that associated hosts (nameservers) are shared parameters for both .NGO and .ONG domain names within a Technical Bundle in the Registry System master database, a successful update to these parameters will immediately be reflected for both domain names within the Technical Bundle. The successful update to the master database will immediately trigger the DNS zone update process for both .NGO and .ONG zone files. Given that both zone generation processes will utilize the shared updated parameters for both the .NGO and .ONG domain names within the Technical Bundle; this will ensure consistency between the two zone files.

***Please describe the atomicity of whois updates. Will there be any validation that the information for a name in the two zones is the same?***

Referencing the above section, “Technical Bundle Technical Design Description”, the same domain attribute object is referenced by both the .NGO and .ONG domain names within the Technical Bundle. This ensures that the relevant parameters are consistent and updated simultaneously for both the .NGO and .ONG domain names within the Technical Bundle (and answers the second question above).

The following lists the relevant parameters that are shared for the domain names within the Technical Bundle and are utilized by the WHOIS Service:

- Registrar Ownership/Sponsor
- Registration and Expiry Dates
- Registrant, Admin, Billing, and Technical Contacts
- Name Server Association
- Domain Status, including both client and server statuses

This implementation will ensure that the WHOIS responses for both the .NGO and .ONG domain names within the Technical Bundle will have the same shared parameters within its response.

***Please describe the atomicity of the transfer of domains. How will PIR assure that the two names have been transferred to the same entity?***

Similarly to the above response describing the atomicity of WHOIS updates, the same domain attribute object is referenced by both the .NGO and .ONG domain names within the Technical Bundle. Given that the Registrar ownership/sponsor is a parameter within the domain attribute object, an update to this parameter, which can only be triggered by a successful domain transfer or a bulk transfer operation, will immediately be reflected for both domain names within the Technical Bundle.

***Please describe the atomicity of updates resulting in state changes such as pendingTransfer or pendingDelete. How will PIR assure that if one name in a pair***

***transitions to a particular state, that the other name in the pair enters the same state at the same instance?***

Similarly to the above response describing the atomicity of WHOIS updates and transfer of domains, the same domain attribute object is referenced by both the .NGO and .ONG domain names within the Technical Bundle. Any updates to the domain attribute object and its list of parameters, including domain statuses, such as pendingTransfer (triggered by a successful domain transfer request) and pendingDelete (triggered by a successful domain delete request) will immediately be reflected for both domain names within the Technical Bundle.

***Depending on registry configuration and policies, the objects related to a TLD can be shared, independent of each other, or a mixture (such as contacts and hosts external to both TLDs are shared, while child hosts are local to each TLD). The proposal does not explicitly state the configuration and policy. The pictures suggest that the objects will reside in a single registry, but there is no explicit statement to that effect. The pictures can also be seen to suggest that the objects are discrete registry instances for each TLD. The choice could potentially have implications on how objects are managed.***

Both the .NGO and .ONG TLDs will reside within a single instance of the Registry System, with one master database. Please refer to the section “Technical Bundle Technical Design Description” above for details on the technical design of Technical Bundling.

***Please state explicitly the registry configuration and policy, specifically discussing how the objects are stored.***

The following describes all registry features, functionality and policies required as prerequisites for the technical bundling of .NGO and .ONG.

Please refer to the section “Technical Bundle Technical Design Description” above for details on the technical design of Technical Bundling and how objects are stored within the Registry System.

| | |
|---|---|
| Registrars | Registrars must be accredited for .NGO and .ONG within the technical bundle before given authorization to access the Registry System for these TLDs. |
| | |

| | |
|---|---|
| TLD Launch Scheduling | Launch scheduling, including all phases within a launch process for both .NGO and .ONG must be synchronized.<br>[redacted] |
| | |
| Domain Policies | The following are key domain policies that must be identical for both .NGO and .ONG<br>● Minimum/maximum Domain Term; as well as minimum/maximum Domain Terms per relevant operation.  These operations include: domain create, domain renewal, and domain transfers.<br>● Minimum/maximum Domain String Length<br>● All grace period policies, including: Add Grace Period, Renew Grace Period, Auto Renew Grace Period, Transfer Grace Period, Redemption Grace Period<br>● Required contact associations; these include Registrant, Admin, Billing and Technical contacts |
| | |
| IDNs | .NGO and .ONG within the Technical Bundle must support the same IDN features, launch scheduling and policies.<br>[redacted] |
| | |

| | |
|---|---|
| Restricted Registration | TLDs bound by a technical bundle must support the same restricted registration requirements if applicable.<br>[redacted] |
| | |
| Bulk Transfer | In situations where ICANN may request the registry to perform a bulk transfer of some or all registered objects (includes domain, contact and host objects) from one registrar to another registrar, both .NGO and .ONG bundled domain names will be transferred to the gaining registrar. |
| | |
| Data Escrow | For each TLD within the Technical Bundle, .NGO and .ONG, both will fully conform to all requirements for the technical specifications of escrow defined in Specification 2. |
| | |
| WHOIS | WHOIS services will be available for both .NGO and .ONG Registries.  WHOIS services for both TLDs will comply with all ICANN policies, including Specification 4 and Specification 10 of the new gTLD Registry Agreement, and RFC 3912.<br>WHOIS services will be available at the locations defined by Specification 4 of the new gTLD agreement:<br>● **whois.nic.ngo** for the .NGO Registry; will be available via port 43 as well as with a web based searchable interface on port 80.<br>● **whois.nic.ong** for the .ONG Registry; will be available via port 43 as well as with a web based searchable interface on port 80. |

***Please describe how PIR intends to handle the differing set of SLDs to block under the Alternate Path to Delegation Report. Will the two TLDs implement the same bundling strategy in such a way that the union of both lists of SLDs are blocked?***

In order to ensure consistency and atomicity both domain names within the Technical Bundle, any SLDs to be blocked under the Alternate Path to Delegation Report for NGO will be blocked for ONG. Any SLDs to be blocked under the Alternate Path to Delegation Report for ONG will be also be blocked for NGO.

Therefore the UNION of both sets of SLDs to be blocked under the Alternate Path to Delegation Report for both NGO and ONG will be blocked from both TLDs.

***If PIR decides to release any reserved or blocked names in the future, will the bundling mechanism apply to those names as well?***

The Technical Bundling mechanism will apply to both the reservation/blocking of domain names as well as the release of these domain names. If a domain name is to be reserved/blocked for .NGO, the corresponding .ONG name will be reserved/blocked. In the case that PIR decides to release a reserved or blocked domain name, both domain names within the Technical Bundle will be released and made available for general registration.

***How will domains in a bundle will be represented in the respective TLD zone files when glue records are used, such as a domain delegating to its subordinate hosts? Please provide an example that includes the relevant parts of the two zone files for such a delegation.***

Host operations are unchanged and are compliant with the core EPP RFCs. Child hosts can be created for any of the domain names in the Technical Bundle and be assigned their own IP addresses. These child hosts can be associated to any domain in the Registry as name servers. Updates to the child hosts will be reflected on all associated domain names.

For example, if the bundled domain names example.ngo and example.ong have been registered, it is possible that ns1.example.ngo can exist as a child host of example.ngo, however, ns1.example.ong does not exist at all. Similarly, it is possible that ns2.example.ong exists as a child host of example.ong while ns2.example.ngo does not exist at all.

The following examples describe the relevant parts of the two zone files for such a delegation:

**Example 1 - NGO & ONG Child Hosts as Name Servers**
example.ngo / example.ong

ns1.example.ngo
ns2.example.ong

```
     NGO zone
     example.ngo     IN    NS   ns1.example.ngo
     example.ngo     IN    NS   ns2.example.ong
     ns1.example.ngo IN    A    1.2.3.4

     ONG zone
     example.ong     IN    NS   ns1.example.ngo
     example.ong     IN    NS   ns2.example.ong
     ns2.example.ong IN    A    2.3.4.5
```

**Example 2 - NGO Child Hosts as Name Servers**
example.ngo / example.ong
ns1.example.ngo
ns2.example.ngo

```
     NGO zone
     example.ngo     IN    NS   ns1.example.ngo
     example.ngo     IN    NS   ns2.example.ngo
     ns1.example.ngo IN    A    1.2.3.4
     ns2.example.ngo IN    A    2.3.4.5

     ONG zone
     example.ong     IN    NS   ns1.example.ngo
     example.ong     IN    NS   ns2.example.ngo
```

**Example 3 - ONG Child Hosts as Name Servers**
example.ngo / example.ong
ns1.example.ong
ns2.example.ong

```
     NGO zone
     example.ngo     IN    NS   ns1.example.ong
     example.ngo     IN    NS   ns2.example.ong

     ONG zone
     example.ong     IN    NS   ns1.example.ong
     example.ong     IN    NS   ns2.example.ong
     ns1.example.ong IN    A    1.2.3.4
     ns2.example.ong IN    A    2.3.4.5
```

**Example 4 - External Hosts as Name Servers**
example.ngo / example.ong
ns1.example.com
ns2.example.com

```
NGO zone
example.ngo      IN    NS    ns1.example.com
example.ngo      IN    NS    ns2.example.com

ONG zone
example.ong      IN    NS    ns1.example.com
example.ong      IN    NS    ns2.example.com
```

***<u>Please describe what actions would be taken if only one of the two names in a bundle was determined to be used for abusive behavior such as phishing scams or spam.</u>***

In cases where one of the two domain names are determined to be abusive, and is scheduled for a takedown process, to ensure consistency, both domain names within the Technical Bundle will be scheduled for the takedown process.

***<u>Please give the EPP protocol commands PIR will use for each of the actions given in the proposal.</u>***

This solution will require no custom extensions and is based on existing core EPP RFC functionality. This solution is compliant with the following relevant EPP RFCs:

- RFC 5730 Extensible Provisioning Protocol (EPP)
- RFC 5731 Extensible Provisioning Protocol (EPP) Domain Name Mapping
- RFC 5732 Extensible Provisioning Protocol (EPP) Host Mapping
- RFC 5733 Extensible Provisioning Protocol (EPP) Contact Mapping
- RFC 5734 Extensible Provisioning Protocol (EPP) Transport over TCP
- RFC 3735: Extensible Provisioning Protocol (EPP) Guidelines for Extending the EPP
- RFC 3915: Extensible Provisioning Protocol (EPP) Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP)
- RFC 5910: Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)

The following table below provides a summary of available domain EPP commands and the relevant EPP syntax.

### Sample Domain Check Command

```
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0" xmlns:xsi='http://www.w3.org/2001/XMLSchema-
instance' xsi:schemaLocation='urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd'>
<command>
 <check>
  <domain:check xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
xsi:schemaLocation='urn:ietf:params:xml:ns:domain-1.0 domain-1.0.xsd'>
   <domain:name>example.ngo</domain:name>
  </domain:check>
 </check>
</command>
</epp>
```

### Sample Domain Create Command

```
<epp xmlns='urn:ietf:params:xml:ns:epp-1.0' xmlns:xsi='http://www.w3.org/2001/XMLSchema-
instance' xsi:schemaLocation='urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd'>
<command>
 <create>
  <domain:create xmlns:domain='urn:ietf:params:xml:ns:domain-1.0'
xsi:schemaLocation='urn:ietf:params:xml:ns:domain-1.0 domain-1.0.xsd'>
   <domain:name>example.ngo</domain:name>
   <domain:period unit='y'>1</domain:period>
   <domain:ns>
    <domain:hostObj>ns1.example.org</domain:hostObj>
    <domain:hostObj>ns2.example.org</domain:hostObj>
   </domain:ns>
   <domain:registrant>Contact-1</domain:registrant>
   <domain:contact type='tech'>Contact-2</domain:contact>
   <domain:contact type='admin'>Contact-3</domain:contact>
   <domain:contact type='billing'>Contact-4</domain:contact>
   <domain:authInfo>
    <domain:pw>password</domain:pw>
   </domain:authInfo>
  </domain:create>
 </create>
</command>
</epp>
```

## Sample Domain Update Command

```
<epp xmlns='urn:ietf:params:xml:ns:epp-1.0' xmlns:xsi='http://www.w3.org/2001/XMLSchema-
instance' xsi:schemaLocation='urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd'>
<command>
 <update>
  <domain:update xmlns:domain='urn:ietf:params:xml:ns:domain-1.0'
xsi:schemaLocation='urn:ietf:params:xml:ns:domain-1.0 domain-1.0.xsd'>
   <domain:name>example.ngo</domain:name>
   <domain:chg>
    <domain:registrant>Changed-1</domain:registrant>
    <domain:authInfo>
     <domain:pw>new password</domain:pw>
    </domain:authInfo>
   </domain:chg>
   <domain:add>
    <domain:contact type='admin'>Changed-2</domain:contact>
    <domain:contact type='tech'>Changed-3</domain:contact>
    <domain:contact type='billing'>Changed-4</domain:contact>
    <domain:ns>
     <domain:hostObj>ns1.changed.org</domain:hostObj>
     <domain:hostObj>ns2.changed.org</domain:hostObj>
    </domain:ns>
   </domain:add>
   <domain:rem>
    <domain:contact type='admin'>Contact-2</domain:contact>
    <domain:contact type='billing'>Contact-3</domain:contact>
    <domain:contact type='tech'>Contact-4</domain:contact>
    <domain:ns>
     <domain:hostObj>ns1.example.org</domain:hostObj>
     <domain:hostObj>ns2.example.org</domain:hostObj>
    </domain:ns>
    <domain:status s="clientRenewProhibited"/>
   </domain:rem>
  </domain:update>
 </update>
 <extension>
  <secDNS:update xmlns:secDNS="urn:ietf:params:xml:ns:secDNS-1.1">
   <secDNS:rem>
    <secDNS:dsData>
     <secDNS:keyTag>12345</secDNS:keyTag>
     <secDNS:alg>3</secDNS:alg>
     <secDNS:digestType>1</secDNS:digestType>
     <secDNS:digest>38EC35D5B3A34B33C99B</secDNS:digest>
    </secDNS:dsData>
   </secDNS:rem>
   <secDNS:add>
    <secDNS:dsData>
     <secDNS:keyTag>12346</secDNS:keyTag>
     <secDNS:alg>3</secDNS:alg>
     <secDNS:digestType>1</secDNS:digestType>
     <secDNS:digest>38EC35D5B3A34B44C39B</secDNS:digest>
    </secDNS:dsData>
   </secDNS:add>
  </secDNS:update>
 </extension>
</command>
</epp>
```

### Sample Domain Info Command

```
<epp xmlns='urn:ietf:params:xml:ns:epp-1.0' xmlns:xsi='http://www.w3.org/2001/XMLSchema-
instance' xsi:schemaLocation='urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd'>
<command>
 <info>
  <domain:info xmlns:domain='urn:ietf:params:xml:ns:domain-1.0'
xsi:schemaLocation='urn:ietf:params:xml:ns:domain-1.0 domain-1.0.xsd'>
   <domain:name>example.ngo</domain:name>
  </domain:info>
 </info>
</command>
</epp>
```

### Sample EPP Renew Command

```
<epp xmlns='urn:ietf:params:xml:ns:epp-1.0' xmlns:xsi='http://www.w3.org/2001/XMLSchema-
instance' xsi:schemaLocation='urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd'>
<command>
 <renew>
  <domain:renew xmlns:domain='urn:ietf:params:xml:ns:domain-1.0'
xsi:schemaLocation='urn:ietf:params:xml:ns:domain-1.0 domain-1.0.xsd'>
   <domain:name>example.ngo</domain:name>
   <domain:curExpDate>2013-01-01</domain:curExpDate>
   <domain:period unit="y">1</domain:period>
  </domain:renew>
 </renew>
</command>
</epp>
```

### Sample Domain Delete Command

```
<epp xmlns='urn:ietf:params:xml:ns:epp-1.0' xmlns:xsi='http://www.w3.org/2001/XMLSchema-
instance' xsi:schemaLocation='urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd'>
<command>
 <delete>
  <domain:delete xmlns:domain='urn:ietf:params:xml:ns:domain-1.0'
xsi:schemaLocation='urn:ietf:params:xml:ns:domain-1.0 domain-1.0.xsd'>
   <domain:name>example.ngo</domain:name>
  </domain:delete>
 </delete>
</command>
</epp>
```

### Sample Domain Restore Command

```
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd">
<command>
 <update>
  <domain:update xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0 domain-1.0.xsd">
   <domain:name>example.ngo</domain:name>
   <domain:chg/>
  </domain:update>
 </update>
 <extension>
  <rgp:update xmlns:rgp="urn:ietf:params:xml:ns:rgp-1.0"
xsi:schemaLocation="urn:ietf:params:xml:ns:rgp-1.0 rgp-1.0.xsd">
   <rgp:restore op="report">
    <rgp:report>
     <rgp:preData>Domain ID:D12345-LROR
     Domain Name:EXAMPLE.NGO
     Created On:01-Jan-2013 00:00:00 UTC
     Last Updated On:02-Jan-2013 16:53:27 UTC
     Expiration Date:01-Jan-2014 00:00:00 UTC
     Sponsoring Registrar:GoDaddy.com, LLC (R91-LROR)
     Status:DELETE PROHIBITED
     Status:TRANSFER PROHIBITED
     Status:UPDATE PROHIBITED
     ...
     </rgp:preData>
     <rgp:postData>Domain ID:D12345-LROR
     Domain Name:EXAMPLE.NGO
     Created On:01-Jan-2013 00:00:00 UTC
     Last Updated On:02-Jan-2013 16:53:27 UTC
     Expiration Date:01-Jan-2014 00:00:00 UTC
     Sponsoring Registrar:GoDaddy.com, LLC (R91-LROR)
     Status:DELETE PROHIBITED
     Status:TRANSFER PROHIBITED
     Status:UPDATE PROHIBITED
     Status:RENEW PROHIBITED
     ...
     </rgp:postData>
     <rgp:delTime>2013-02-01T22:00:00.0Z</rgp:delTime>
     <rgp:resTime>2013-02-02T22:00:00.0Z</rgp:resTime>
     <rgp:resReason>Registrant error.</rgp:resReason>
     <rgp:statement>This registrar has not restored the
     Registered Name in order to assume the rights to use
     or sell the Registered Name for itself or for any
     third party.</rgp:statement>
     <rgp:statement>The information in this report is
     true to best of this registrar's knowledge, and this
     registrar acknowledges that intentionally supplying
     false information in this report shall constitute an
     incurable material breach of the
     Registry-Registrar Agreement.</rgp:statement>
     <rgp:other>Supporting information goes
     here.</rgp:other>
    </rgp:report>
   </rgp:restore>
  </rgp:update>
 </extension>
</command>
</epp>
```

Sample Domain Transfer Request Command

```
<epp xmlns='urn:ietf:params:xml:ns:epp-1.0' xmlns:xsi='http://www.w3.org/2001/XMLSchema-
instance' xsi:schemaLocation='urn:ietf:params:xml:ns:epp-1.0 epp-1.0.xsd'>
<command>
 <transfer op="request">
  <domain:transfer xmlns:domain='urn:ietf:params:xml:ns:domain-1.0'
xsi:schemaLocation='urn:ietf:params:xml:ns:domain-1.0 domain-1.0.xsd'>
   <domain:name>example.ngo</domain:name>
   <domain:period unit="y">1</domain:period>
   <domain:authInfo>
    <domain:pw>password</domain:pw>
   </domain:authInfo>
  </domain:transfer>
 </transfer>
</command>
</epp>
```

## Responses to Questions from RSTEP Review Team – Part 2

***Please state whether PIR will accept Delegation Signer (DS) information, public key information, or both, in its implementation of RFC 5910.***

PIR will only accept Delegation Signer (DS) information in its implementation of RFC 5910.

Please refer to the section “Technical Bundle Technical Design Description” above for details on the technical design of Technical Bundling and how DS information are stored within the Registry System.

***Please state affirmatively that a single SLD can have a different public key in .ngo than it has in .ong.***

A SLD can have different keys for .NGO than it has in .ONG. The Registry System, via EPP, will accept different DS records for SLDs within each TLD of the Technical Bundle.

***Please state affirmatively that a single SLD can have a public key in .ngo and no public key in .ong.***

A SLD can have keys for .NGO but not .ONG. The Registry System, via EPP, will accept DS records for SLDs under .NGO, even if no DS records exist for the corresponding SLD under .ONG.

***Please state affirmatively that a single SLD can have a public key in .ong and no public key in .ngo.***

A SLD can have keys for .ONG but not .NGO. The Registry System, via EPP, will accept DS records for SLDs under .ONG, even if no DS records exist for the corresponding SLD under .NGO.

***Will PIR be actively scanning the DNS zones for .ngo and .ong for TLD differences where there should be none, that is for an SLD that exists in one zone but not the other? If so, please state how often PIR will perform this scan and say how PIR will respond if it finds a difference where there should be none.***

A test will be preformed daily to examine incorrect differences between the two DNS zones (note that these DNS zones will differ in many other legitimate ways, such as serial number, DNSKEYs, RRSIGs, glue, etc.).

In the event that an incorrect difference is found, the reconciliation process will be as follows:

1) Compare the relevant registry EPP data objects for this SLD against the DNS Resource Records that exist for this SLD in each TLD DNS zone. If either TLD DNS zone differed from the registry, correct the discrepancy, and open a trouble ticket to examine how the discrepancy originated.

2) If the DNS TLD zones have resource records which sufficiently describe the EPP data objects in the registry, examine the EPP transactions themselves to determine the order and course of events leading up to the discrepancy. If this analysis obviates the problem, correct the discrepancy, and open a trouble ticket to examine how the discrepancy originated.

3) If none of the above actions correct the issue, the Registry Operator will contact the Registrar to further investigate the issue.

***Will PIR be actively scanning the DNS zones for .ngo and .ong for SLD data differences where there should be none? If so, please state how often PIR will perform this scan and say how PIR will respond if it finds a difference where there should be none.***

The process mentioned above will also remediate this problem.

***Will PIR be actively scanning the whois Service for .ngo and .ong for TLD differences where there should be none, that is for an SLD that exists in one zone but not the***

***other? If so, please state how often PIR will perform this scan and say how PIR will respond if it finds a difference where there should be none.***

Referencing the above section, “Technical Bundle Technical Design Description”, the WHOIS service for both .NGO and .ONG utilize the master database in the Registry System as the authoritative source of all domain name related information for both .NGO and .ONG. The same domain attribute object is referenced by both the .NGO and .ONG domain names within the Technical Bundle.

Given this implementation approach, an hourly test will be performed against the master database within the Registry system to ensure the correctness of the referential integrity of the data objects stored in the database. If the results determine a disruption of the referential integrity of the data objects stored in the database, we will correct the discrepancy, and open a trouble ticket to examine how the discrepancy originated.

***Will PIR be actively scanning the whois Service for .ngo and .ong for SLD data differences where there should be none, that is for an SLD that exists in both zones that has different domain attributes shown? If so, please state how often PIR will perform this scan and say how PIR will respond if it finds a difference where there should be none.***

The process mentioned above will also remediate this problem.