Dear Ms. Willett and ICANN Staff,

On behalf of our client, Donuts Inc., we respectfully submit the attached comments on the Community Priority Evaluation for <.GMBH>, along with supporting annexes. Please contact the undersigned with any questions you may have. Thank you.

Respectfully,

John M. Genga
Counsel for DONUTS INC.

TLDDOT Application for <.GMBH>: Comment to Community Priority Evaluation

INTRODUCTION

The Community Priority Evaluation ("CPE") is a serious undertaking. It allows for top-level identification of communities by the names for which they are known. Yet, a "successful" CPE also disqualifies applicants that otherwise have met the rigorous criteria to obtain a new gTLD:

> [A] qualified community application eliminates all directly contending standard applications, regardless of how well qualified the latter may be. This is a fundamental reason for very stringent requirements for qualification of a community-based application.

Applicant Guidebook ("Guidebook" or "AGB") § 4.2.3 at 4-9. Accordingly, ICANN created scoring to "identify qualified community-based applications," while preventing "false positives" – *i.e.*, "awarding undue priority to an application that refers to a 'community' construed merely to get a sought-after generic word as a gTLD string." *Id.*

To obtain community priority, an application must score 14 out of 16 possible points. *Id.* at 4-10. "In cases of generic words submitted as community based strings, test runs by [ICANN] staff show that the threshold is difficult to attain …." *See* http://www.icann.org/en/topics/new-gtlds/agv1-analysis-public-comments-18feb09-en.pdf.

An objective analysis demonstrates that the application under review for <.GMBH> ("Application"), copy submitted for the Panel's convenience as **Annex A**, does not meet the stringent criteria to garner the 14 points to satisfy CPE and disqualify the other applicants. TLDDOT GmbH ("TLDDOT" or "Applicant") appears to have concocted a community around a group as diverse and unconnected as its purported "members."

The Application proposes registration policies that do not advance its stated goals for the alleged community. While the Applicant suggests understandable eligibility criteria, it puts forth extremely watered-down name selection rules and no content or use restrictions whatsoever. While it may articulate some "enforcement" mechanisms to achieve the "protections" it claims to offer the asserted community, these become largely irrelevant due to the lack of meaningful restrictions capable of being enforced.

Finally, the Applicant provides *no support* whatsoever for the actual *Application* under review. Rather, it offers a few letters from certain organizations located exclusively *within Germany* – and no other German-speaking jurisdiction, such as Austria, Lichtenstein or Switzerland. These letters – often using the same language, suggesting that Applicant may have drafted it – say very little at all about TLDDOT's own Application, but instead simply put forth the need for registrants of a <.GMBH> domain to be registered in at least one jurisdiction. These questionable "support" letters hardly merit a full two points.

The Applicant undertakes the CPE essentially as a low cost, high reward gamble. It tries inappropriately to use the CPE to circumvent the appropriate contention set resolution process defined by ICANN.

This does not diminish the Application; it simply does not meet the community criteria. The Applicant thus cannot attain community priority and must instead compete for <.GMBH> on the same level as all other applicants for the string.

ANALYSIS

The Guidebook allows the CPE Panel to award up to four points in each of four categories (maximum points in parentheses):

- "Community establishment," which involves "delineation" (2) and "extension" (2), AGB at 4-10 *et seq.*;
- "Nexus," meaning both “nexus” (3) and "uniqueness" (1), *id.* at 4-12 *et seq.*;
- "Registration policies," consisting of "eligibility" (1), "name selection" (1), "content and use" (1) and "enforcement" (1), *id.* at 4-14 *et seq.*; and
- "Community endorsement," which considers "support" (2) and "opposition" (2), *id.* at 4-18 *et seq.*

Applying the standards established by ICANN for these criteria, the Application cannot reach four points on any of them. Giving Applicant the benefit of all doubts on each at most yields about 8 points, well short of the 14 points needed out of 16.

CRITERION 1: The Application does not "establish" a "community" under either the "delineation" or "extension" tests, thus clearly yielding less than the maximum four points.

A "community" as described in the Guidebook "impl[ies] more cohesion than a mere commonality of interest." AGB at 4-11. As such, the Guidebook calls for examining the claimed community in terms of its "delineation" and "extension." The test for "delineation" considers:

- The "level of public recognition of the group as a community," the existence of "formal boundaries around the community" and "what persons or entities … form" it (hereafter referred to as the "Identification" factors);
- Whether the alleged community pre-dates the commencement of the new gTLD program in 2007 (the "Existence" factor); and

- The level of "organization" of the community through at least one dedicated entity with documented evidence of community activities ("Organization").

AGB at 4-11. "Extension" relates to "the dimensions of the community, regarding its number of members, geographical reach, and foreseeable activity lifetime …." *Id.* The Application cannot earn the full number of available points under either prong of the first "community" test.

The Application reflects no clear "delineation" of any "community."

Satisfying all three of the Identification, Existence and Organization factors will allow an application to score up to a 2. AGB at 4-12. The Application under review does not meet those criteria, and therefore cannot receive 2 "delineation" points.

The Application demonstrates no community "Identification."

Regarding Identification, the Application can be said to "identify" the entities that make up the purported community – companies registered in accordance with the laws of certain German-speaking sovereignties. However, it fails to show in any way that the public recognizes the over "1.4 million companies with the legal form of a GmbH in Austria, Germany, Liechtenstein and Switzerland" *collectively* as a *single community*.

As stated, "community" implies "more cohesion than a mere commonality of interest." AGB at 4-11. The dictionary defines "cohesion" as "the act or state of cohering; tendency to unite, to 'stick together.'" The Application does not demonstrate or even claim any "cohesion" among those to whom it would make a <.GMBH> domain available. Indeed, it is extremely difficult to see how these "1.4 million" GmbH entities – no doubt ranging from huge conglomerates to family-owned companies that may run a corner bakery – have any real common *interests*, let alone *cohesion*, across their "membership."

The Application goes beyond even this diverse population and artificially combines not only the many disparate GmbH businesses, but also various interests that work with them. According to the Application:

> The GmbH Community includes regulatory authorities, courts, institutions, associations, chambers and the GmbH companies [themselves].

Applic. § 20(c). In addition to "courts," which few people would see as constituting a legitimate part of any "GmbH community,"[1] one cannot tell what other "institutions" or "associations" also would belong. The Applicant's membership definition is far from "clear and straightforward" as the Guidebook requires.

[1] While some "courts" may *store local copies* of company registers (*see, e.g.,* https://www.handelsregister.de/rp_web/div/info-lang/en-GB.pdf) they typically do not perform any significant registration or licensing function.

Even just factoring in "the GmbH companies themselves," membership could include a host of disparate companies — located in several different countries — that have no connection whatsoever. For example, "Blaupunkt GmbH" sells stereo equipment; "Red Bull GmbH" markets energy drinks; and "Volkswagen R GmbH" sells performance cars. "The Swatch Group (Deutschland) GmbH" handles wristwatches and "Nestlé Kaffee & Schokoladen GmbH" sells coffee and chocolate. These companies would have about as much in common with one another as United Airlines would with Nike, Chrysler or McDonald's in the U.S. — *i.e.* nothing other than the simple fact that these companies are all engaged in business, in a certain form, and trying to make profit.

At best, TLDDOT's alleged "community" is based simply on a "mere commonality of interest" and should not be considered a "cohesive" unit. This "insufficient delineation" alone leads to a score of 0 for the "delineation" sub-factor. AGB 4-10.

The Application does not show that GmbH entities "existed" *as a community* prior to the New gTLD program.

No one can dispute that GmbH entities have existed prior to the inception of the ICANN New gTLD Program in September 2007. If simply calling all of those "members" a "community" makes it so, then it could satisfy the "Existence" criterion.

The high threshold for CPE requires more, however. It is not at all clear whether these entities have the "requisite awareness and recognition" themselves, and by others, *as a community*, rather than just as individual actors with separate interests who happen to share a common label. AGB at 4-12. The CPE inquiry questions whether there is "clear evidence of such awareness and recognition." CPE Guidelines version 2.0 ("EIU Guidelines") at 5. The Application demonstrates none. Instead, the Applicant appears to have created a "false positive" by "an application that refers to a 'community' construed merely to get a sought-after generic word as a gTLD string." *Id.* at 4-9.

The Application does not show the requisite community "Organization."

The EIU Guidelines also ask: "Is there at least one entity mainly dedicated to the community?" Even a cursory review of the Application itself casts significant doubt on this conclusion. Aside from the obvious issues concerning disparate rules and procedures adopted for GmbH entities in various countries (*e.g.* Germany vs. Austria or Switzerland), the Applicant acknowledges that the alleged "community" encompasses not just "GmbH companies" but many other "layers," namely government regulators, "courts," "institutions," "associations" and "chambers." Applic. § 20(a).[2]

[2] With the Application comes a flow chart of dubious accuracy, made to appear as if it accompanies a letter from IHK Berlin, but seemingly instead created by the Applicant. *See* https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails:downloadattachment/141615?t:ac=1080.

Nothing in the Application demonstrates that "at least one entity" is "mainly dedicated to serving all the GmbH companies and these various ancillary interests. On the contrary, no overarching singular "authority" over GmbH entities exists in any particular jurisdiction, and most certainly not one that *spans multiple countries*.[3]

The same is true with respect to "chambers" of commerce organizations. While some countries (notably Germany and Austria) may require that a GmbH join a particular "chamber," chambers of commerce serve no regulatory functions and have no authority over GmbH entities other than what the members voluntarily bestow upon them. Often they act in a lobbying capacity. *See, e.g.*, IHK Berlin homepage (http://www.ihk-berlin.de/English/en/809492/aboutus_index.html).

As TLDDOT is unable to demonstrate that there is "at least one entity mainly dedicated" to its purported "community," the Application cannot score the full 2 points.

Other than describing an identifiable type of entity denoted by the term "GMBH," the Application satisfies none of the "delineation" criteria – Identification, Existence, or Organization. It must meet *all* of them to earn 2 points, which the foregoing analysis shows it cannot do. Even giving the weak or non-existent showings the fullest benefit of all doubts, TLDDOT should still only be awarded no more a single point.

The Application cannot receive two points for community "extension."

To receive 2 points for "extension," an application must demonstrate a "community of considerable size and longevity." A "community of *either* considerable size *or* longevity, but not fulfilling the requirements for a score of 2," can earn 1 point. AGB at 4-10 (emphasis added). One that meets neither gets a zero. These size and longevity factors relate "to the dimensions of the community, regarding its number of members, geographical reach, and foreseeable activity lifetime …." *Id.* at 4-11.

Regarding "longevity," the Application states that the GmbH community has existed for "over 100 years in Austria and Germany and over 70 years in Liechtenstein and Switzerland." Applic. § 20(a) at 12. However, longevity in Guidebook terms "means that the pursuits of a community are of a lasting, non-transient nature." AGB at 4-12. The Application identifies no particular "pursuit" of companies uniting them *as a community*,

[3] In Germany for example, aside from implementing an overarching legal mechanism for the *creation* of a GmbH, *see* http://www.gesetze-im-internet.de/gmbhg/index.html, the German national government conducts very little central oversight on GmbH companies, which, like American corporations, typically can be formed for any lawful purpose. Instead, regulation is for the most part limited to specific sectors – *e.g.*, finance, medicine, etc. – with each handled according to its own subject matter.

other than business interests generally that apply to other types of entities as well as individuals engaged in commerce.

Nor does the Application ascribe any such "pursuits" to a specific period of time. If a community exists, it has, by the requirements stated in the Guidebook, a specific beginning. The Applicant provides none because no specific “GmbH community" exists.

As to size, Applicant cites to the "1.4 million companies with the legal form of a GmbH in Austria, Germany, Liechtenstein and Switzerland." Applic. § 20(a) at 13. "Size" relates both to number of members and geographical reach. AGB at 4-11. However, no GmbH "community" of the size described by the Application exists. Rather, it is fragmented by many different sets of formal rules and legal standards corresponding to the various German-speaking countries. Too, as described by the Applicant, it consists of other vaguely described “institutions,” “associations” and other members that make ascertaining its size impossible.

In short, the Application does not construe a well-defined community of certain size and origination date, and certainly not with the precision required for an award of two points, especially when considering the lack of any real "delineation.” If the Panel sees any points at all available, it cannot award more than one.

Even that would be generous. The Guidebook makes clear that a "community" can exist only where "the requisite awareness and recognition of the community is at hand among the members. Otherwise the application would be seen as not relating to a real community and score 0 on both ’Delineation’ and ’Extension.’" AGB at 4-12 (emphasis added).

CRITERION 2: The Application does not establish a sufficient "nexus" to any "community" known as "GMBH," and certainly not "uniquely."

Criterion 2 requires a "nexus" between the asserted community and the applied-for string. AGB at 4-12. The test consists of a "nexus" factor of up to three points, and a "uniqueness" score of zero to one.

The Application does not show that the claimed “community,” if it even exists, goes by the specific name "GMBH" in the same sense that, for example, the "Navajo" and "Boy Scout" communities go by those precise names. The "GMBH" label has many uses made by diverse groups such that it cannot attach uniquely to an identifiable community designated by that term. As such, the application can achieve no more than two of the possible four "nexus" points.

The <.GMBH> string does not "match" a "community."

The Guidebook scores "nexus" as follows:

- For a score of 3: The string matches the name of the community or is a well-known short-form or abbreviation of the community name;
- For a score of 2: String identifies the community, but does not qualify for a score of 3; and
- For a score of 0: String nexus does not fulfill the requirements for a score of 2.

AGB § 4.2.3. The Guidebook also cautions against "substantial overreaching" by a would-be CPE applicant. *Id.* at 4-13. The Panel is urged to pay particular attention to the Guidebook's example concerning a "local tennis club applying for <.TENNIS>":

> If the string appears *excessively broad* (such as, for example, a globally well-known but local tennis club applying for ".TENNIS") then it would *not* qualify for a 2.

Id. (emphases added). This example illustrates precisely the type of "substantial overreach" that TLDDOT is engaged in here.[4] By applying for community scoring priority, the Applicant attempts to usurp control over the very broad "GMBH" string, when its only real connection to that label is its having been formed under that legal mechanism. While it claims a "long-standing relationship," the Applicant is still just a *domain registration* company formed specifically to apply for the <.GMBH> TLD. It is not "globally well-known," nor does it register, license or provide any meaningful services (aside from proposed second-level domain registrations) for GmbH entities. As such, the Applicant has no connection to the alleged GmbH community, as it has essentially admitted in another context:

> [T]he term ".GMBH" is not a standard term within the domain name industry and has *no inherent connection* to the Internet space in general or to the registration or license of domain names or *additional services reasonably offered by potential registry operators in connection with the management of a TLD space in particular*.

See TLDDOT GmbH v. InterNetWire Web-Development GmbH, WIPO Case No. LRO 2013-0052 (July 22, 2013) (emphases added), available at: http://www.wipo.int/export/sites/www/amc/en/domains/lro/docs/lro2013-0052.pdf. TLDDOT has no more right to anoint itself as overseer of <.GMBH> than "Chrysler LLC" would over <.LLC>, or "Macy's Inc." would over <.INC>.

Based on the foregoing, the TLDDOT application *should* receive a score of zero for nexus, but certainly cannot garner any more than two points even in a "best-case" scenario.

[4] *See also* EIU Guidelines at 7: "'Over reaching substantially' means that the string indicates a wider geographical or thematic remit than the community has."

The term "GMBH" does not "uniquely" identify the claimed "community."

"'Uniqueness' relates to the meaning of the string." *See* http://www.icann.org/en/topics/new-gtlds/summary-analysis-agv3-15feb10-en.pdf, p.65. An applicant can earn a "uniqueness" point if the applied-for string has no other significant meaning beyond identifying the community described in the application; a score of zero does not fulfill this requirement. AGB § 4.2.3.

> To be an unambiguous identifier, the "ideal" string would have no other associations than to the community in question. This arguably can be achieved by using the community *institution* abbreviation as string ....

See http://www.icann.org/en/topics/new-gtlds/agv1-analysis-public-comments-18feb09-en.pdf, p.103 (emphasis added). ICANN has put the necessary balancing in the hands of applicants. For example, does an applicant select a popular, well-recognized term that fails to *uniquely* identify a community, such as <.SCOUTS> or <.SCOUTING> (which could refer to "Girl Scouts," "Boy Scouts" among other things)? Or does the applicant select its own *unique* and specific organizational name, such as <.BOYSCOUTSOFAMERICA>? The latter may deserve a scoring point, while the former may not.

Here, TLDDOT did not apply for <.TLDDOTGMBH>, it applied for <.GMBH>. It also did not apply for <.GERMAN-GMBH>, while the Application and its accompanying "support" documentation focuses almost exclusively on Germany. TLDODOT is simply one small "GmbH," formed specifically in 2010,[5] to apply for the <.GMBH> TLD and no other purpose, with little (if any) formal connection to or oversight on any "GmbH Community" in Germany, much less other countries. Yet, it still attempts to usurp control over the broad "GmbH" term with no documented authority or support.[6]

Evidence of common use of the term "GMBH" may make it an excellent choice for a top-level domain. However, it does not "match" the community as named by the Applicant; nor does it "identify" the defined community *uniquely*. Of the four total points available for "nexus," the Application can earn no more than two.

CRITERION 3: The Application should receive few, if any, points for registration policies.

"Registration policies" represent the conditions that the registry will set for prospective registrants – *i.e.*, those desiring to register second-level domains. A community application will receive one point for each of the four following policies:

---

[5] *See, e.g.*, printout of search from German Companies Register, included as **Annex B**.
[6] *See* discussion regarding Criterion 4, below.

- Eligibility restricted to community members (a largely unrestricted approach to eligibility receiving zero points);
- Name selection rules consistent with the articulated community-based purpose of the applied-for gTLD;
- Rules for content and use consistent with the articulated community-based purpose of the applied-for gTLD; and
- Specific enforcement mechanisms.

Guidebook at 4-14 to 4-15. The Panel should score the Application "from a holistic perspective, applying these categories to the particularities of the community explicitly addressed." *Id.* at 4-16. Particularly as to "restrictions and corresponding enforcement mechanisms," the Guidebook instructs that these measures "should show an alignment with the community-based purpose of the TLD and demonstrate continuing accountability to the community named in the application." *Id.*

The Application's broad eligibility requirements do not meet the specific Guidebook criteria. As detailed below, the shortcomings in the Application potentially eliminate all four "registration" points. However, even with a "liberal interpretation" should yield no higher than three, and more likely two or less.

The domain's "eligibility" criteria are not particularly definitive.

A point for eligibility must meet strict criteria. In a policy advisory, ICANN notes:

> Registration policy is a criterion where a balance is needed between what is reasonably the most appropriate registration policy for a community and the risk for gaming of the process by an "open" application declaring itself as "community-based" to get an advantage in a contention situation. The approach taken is conservative in this respect, with the high score reserved for a registration policy only permitting members of the community to register. A *widening has been considered, but it appears reasonable to maintain the chosen approach* ….

See http://www.icann.org/en/topics/new-gtlds/agv1-analysis-public-comments-18feb09-en.pdf, at 103 (emphasis added). The Application, by contrast, creates a liberal ability to register a <.GMBH> domain name.

While the Applicant states some candidate eligibility restrictions, it does so in a wide "funnel." As mentioned, the Application's community definition encompasses many "layers," with not only GmbH companies but also government regulators, "courts," "institutions," "associations" and "chambers." Applic. § 20(a); *see also* discussion re Criterion 1, *supra*. The eligibility requirements also go beyond just GmbH entities, but also a variety of other interests. Applic. § 20(e)(5). While some token exclusions appear – *e.g.* "GmbH & Co. KG" entities, or entities that are not fully formed or that are

involved with bankruptcy proceedings – those alone do not merit a full scoring point in light of the otherwise relatively unencumbered ability to register a domain.

While not fully tantamount to "open" application eligibility, the vagueness of the criteria makes it seem as if TLDDOT is "gaming" the CPE procedure in a way discouraged by ICANN. Of course, opening up registrations to as many potential registrants as possible would be a logical approach for any registry trying to maximize its profits, and nothing in this analysis should serve to criticize this — *except* to the extent where Applicant seeks to falsely characterize its policies as narrowly tailored in order to eliminate competitors *via CPE.* As such, the Applicant cannot properly earn a point for "eligibility criteria."

The Application's "name selection" restrictions are vague and over-inclusive.

Name selection restrictions protect the identified community by ensuring that the names under a particular TLD "align" with community interests and "demonstrate continuing accountability" to it. AGB at 4-16. Under close scrutiny, the Applicant's "restrictions" show little, if any, "alignment" or accountability" with its alleged community. Of particular note, TLDDOT would allow GmbH entities not only to register a domain that corresponds "fully or in relevant parts with the company's name," but also any "goods and services as mentioned in the corporate purpose of a company as mentioned in the Company register concerned." *See* Applic. § 20(e)(7). Presumably, this would allow Blaupunkt to register not only <BLAUPUNKT.GMBH> (its name) but also <CAR-STEREO.GMBH>, <HEADPHONES.GMBH> and <SPEAKERS.GMBH>, while Red Bull could procure <ENERGYDRINK.GMBH> in addition to <REDBULL.GMBH>.

While a business case theoretically could be made for why a TLD operator might want to permit companies to have product designations as second-level domains along with organizational monikers, this does not *also* mean that it should be awarded a *scoring point for name selection* in CPE analysis for attempting to widen its reach. On the contrary, such broadening cuts firmly *against* it. No point should be given.

The Application does not describe any "content and use" policy consistent with its claimed community-based purpose.

The Applicant fares even worse with respect to "content and use" restrictions, which practically do not exist. The Guidebook provides a potential scoring point where a community TLD operator restricts the content and use of any second-level domain name in a manner that "show[s] an alignment with the community-based purpose of the TLD and demonstrate[s] continuing accountability to the community named in the application." AGB at 4-16.[7] In other words, the Application must impose content and use restrictions that serve and protect the interests of the identified "community" in order to score a point on this element. *Id.*

[7] *See also* EIU Guidelines at 13, providing for a scoring point where an application's "[p]olicies include rules for content and use consistent with the articulated community-based purpose of the applied-for TLD."

The Application completely fails under this standard. All the Applicant requires is that websites operating under <.GMBH> domains:

- Be "accessible under a domain directly related to the eligibility requirements (Registrant, Content and Use, Domain Name Selection)" and

- Be "in use within 12 months of registration."

See Applic. § 20(e)(6). As with name selection, these so-called "restrictions" on use and content regulate very little at all, and certainly do nothing to ensure "alignment" and "accountability" toward any GmbH community. Further, unlike the TLD's proposed name selection rules, the content and use need not even be specifically tied to any "corporate purpose." *Id.* Virtually *any* second-level domain name would satisfy such amorphous policies. A website that is "accessible" under a domain name such as <BERLIN-BEAUTY-SUPPLY.GMBH> could discuss automobiles, sporting events, the weather or just about anything, so long as the information is posted "within 12 months of registration."

Again, a TLD operator may decide that it makes good strategic business sense to allow a GmbH complete freedom to discuss whatever it wants to on websites accessible under that TLD. This does not *also* mean, however, that such a TLD should garner a scoring point for CPE. The Application must score a zero for the content and use sub-factor.

The Applicant's "enforcement" procedures also lack rigor.

Award of a point on enforcement requires *specificity*. A well-drafted CPE application should lay out a "coherent set" of detailed investigation practices, penalties, and takedown procedures in the event the registry's policies are not adhered to. AGB at 4-16; *see also* EIU Guidelines at 14. Of course, as the subject Application contains very few registration policies and restrictions, it matters little how they will supposedly be "enforced." However, even assuming some policies can be identified here, the Application still falls short of the precise detail required for a full point.

While the Application does provide some overarching parameters – *e.g.*, a proposed "ERDRP" – the enforcement plan still fails to approach the necessary level of particularity. It also fails to lay out fully all aspects of day-to-day enforcement, such as budget, staffing, resources and other indicia that a meaningful enforcement plan or compliance regime would consider. Although the Applicant signals a general willingness to enforce restrictions, this alone does not rise to the level of specificity to earn a point.

In sum, the Application should earn no more than two points in the area of registration policies. It establishes certain registration criteria, and at least attempts to formulate a plan for "enforcement" of whatever rules may be imposed. The Panel may deem one or both of these aspects worthy of a scoring point. Its point total must stop at those two, however, since the Application deserves *no* points whatsoever for name selection,

which are extremely vague and prone to abuse, and content and use "restrictions" that would provide no real limitation at all.

CRITERION 4: The Application does not demonstrate "documented support" from a majority of its purported "community," nor any "documented authority" to represent it.

The "support" criterion actually looks at both support and opposition in awarding up to four points to an application. For "support," the applicant must demonstrate that:

- It is, or has documented support from, the recognized community institution(s)/member organization(s) or has otherwise documented authority to represent the community. It must have documented support from institutions/organizations representing a *majority* of the overall community in order to score 2.

- Documented support from *at least one group with relevance may allow* a *score of 1*, but does not suffice for a score of 2.

See AGB at 4-17 (emphases added). On the opposition side, an application will earn two points where it lacks any opposition of relevance, and one where it has "relevant" opposition from "one group of non-negligible size." It will receive no points in the case of "relevant opposition from two or more groups of non-negligible size." *Id*. at 4-17.[8]

The Application's "support" letters do not show anything of the sort.

The Applicant has not shown evidence of its "documented authority to represent" all GmbH entities in Germany, much less those in Austria, Switzerland, Lichtenstein or any other German-speaking jurisdiction where this business form enjoys popularity. As mentioned, TLDDOT is a domain registration company, formed in 2010 specifically for the purpose of applying for a <.GMBH> TLD. It does not itself register or issue licenses to any GmbH entities. It does not provide (aside from potentially allowing the registration of second-level domain names) any goods or services that facilitate GmbH entities. Its only real connection to any "GmbH Community," if one even exists, is the simple fact that it is a registered German GmbH, which practically anyone can set up.[9]

The Application cannot even reasonably be said to have "documented support" from a "majority" of German-speaking jurisdictions. Although "support" does not depend

[8] "Relevance" refers to the communities addressed. *Id.* at 4-18. Thus, "relevant" support or opposition means that which comes from those in the named community.
[9] *See, e.g.:* http://www.doingbusiness.org/data/exploreeconomies/germany/starting-a-business/

solely on the number of expressions of support received,[10] the Applicant nevertheless proffers very few "support" letters. Further, flaws become readily apparent upon closer examination. First, they all come from government or business interests *in Germany*, with no Austrian, Swiss, Belgian or other nationalities represented. The letters also do not specifically describe how the organization came to support the application.

For consideration as relevant support, documentation *must contain a description of the process and rationale used in arriving at the expression of support*, and does not receive a point based merely on the number of comments or expressions of support received. *Id.* at 4-18. Documentation accompanying the Application does not demonstrate this, if it even can fairly be characterized as "support" at all.

As to that point, many of the letters merely make high-level, general statements that do not specifically "support" the actual Application under consideration. Rather, the discussion largely centers around a single common theme: a potential registrant of a second-level <.GMBH> domain name should be registered with at least one government agency that licenses such entities. However one chooses to view such a policy, the simple fact is that this position does not by itself represent a specific "endorsement" of the Application. The Applicant attempts to *imply* support that does not plainly appear.[11]

In a similar vein, the Application accomplishes little when it refers generically to unspecified "relationships" with "other organizations representing GmbH companies." *See* Applic. § 20(b). Aside from Applicant's failure to present evidence substantiating or detailing the precise scope of these "relationships," a number of these are simply *lobbying* organizations with no formal authority over GmbH entities whatsoever. *See, e.g.,* http://www.medianet-bb.de/EN/Profil/. TLDDOT also provides no evidence of its supposed "consultations" with the governments in Austria, Germany and Switzerland via the members of the Governmental Advisory Committee at ICANN. Applic. § 20(b).

The Application simply does not contain the "documented" evidence of support necessary to garner two points under the analysis. Indeed, the lack of documented authority to speak on behalf of GmbH entities, or even a legitimate basis to infer support from a "majority" of them worldwide, should result in a score of *zero* in this factor. *At most*, TLDDOT offers little more than "[d]ocumented support from at least one group with relevance," which according to the Guidebook *may* be worth just 1 point "but does not suffice for a score of 2." AGB 4-17.

---

[10] *See also* EIU Guidelines at 18: "A majority of the overall community may be determined by, but not restricted to, considerations such as headcount, the geographic reach of the organizations, or other features such as the degree of power of the organizations."

[11] Additionally, one of the letters (*see https://gtldresult.icann.org/application-result/applicationstatus/applicationdetails:downloadattachment/37733?t:ac=1080*) is over four years old (February 2010) and addressed to an officer and director of ICANN who no longer occupy those positions.

As mentioned, nothing here diminishes the effort and preparation exhibited by the Application and supplementary materials. One would expect to find it exceedingly difficult to gain the requisite support required from such a large, unbounded "community" that TLDDOT attempts to create. This is why ICANN has set the CPE bar so high—to prevent the creation of artificial communities to gain an advantage in the new gTLD process.

The Application has encountered relevant opposition.

Several public comments oppose the Application. At least one, submitted by the Delaware Secretary of State,[12] specifically criticizes the enforcement mechanisms as wholly inadequate.[13] This opposition is particularly germane when considering that TLLDDOT relies so heavily upon on how it will supposedly "ensure" all registrants are licensed GmbH entities (and justifies eliminating all competing TLD applicants via community priority). *See, e.g.,* Applic. § 20(b). This makes it "relevant" for purposes of CPE analysis, as it comes from a group "implicitly" addressed by the Application. *See* EIU Guidelines at 19. A point therefore should be deducted since there is "[r]elevant opposition from one group of non-negligible size." AGB at 4-17.

In sum, the Application should lose at least 2 out of 4 points this factor. The letters offered by the Applicant do not describe how the organizations came to "support" the Application, and provide little more than guarded language that hardly constitutes an "endorsement" of the Applicant itself or its particular Application, making two "support" points unattainable. And, the existence of relevant opposition results in subtraction of one "opposition" point.

CONCLUSION

Reviewing the categories considered by the CPE process, this analysis concludes as follows out of the 16 total possible points:

- "Community delineation" (2) and "extension" (2), AGB at 4-10 *et seq.*:
    - ***Zero*** based on the Guidebook statement requiring "awareness and recognition of the community … among the members. Otherwise the application would be seen as not relating to a real community and score 0 on both 'Delineation' and 'Extension.'" AGB at 4-12. ***Maximum*** of ***two*** even apart from this statement.
- "Nexus," meaning both "nexus" (3) and "uniqueness" (1), *id.* at 4-12 *et seq.*:

[12] https://gtldcomment.icann.org/applicationcomment/commentdetails/8014

[13] "[N]one of the applications contains a fully thought out, achievable, transparent and enforceable system for fully safeguarding that a firm remains legally registered with a company registry at all times." *Id.*

- ***Maximum*** of ***two*** on the first part of the “nexus” test, and ***zero*** for “uniqueness.”

- "Registration policies," consisting of "eligibility" (1), "name selection" (1), "content and use" (1) and "enforcement" (1), *id.* at 4-14 *et seq.*:
  - ***One*** each regarding eligibility and enforcement, and ***zero*** for naming and content and use restrictions, , for a total of ***two***.

- "Community endorsement," which considers "support" (2) and "opposition" (2), *id.* at 4-18 *et seq.*:
  - ***Maximum*** of ***one*** for support and ***one*** for opposition; total possible of ***two***.

The Application can earn no more than 8 of the 14 points needed to gain community priority, and thus fails CPE.

DATED: March 4, 2014

Respectfully submitted,

THE IP & TECHNOLOGY LEGAL GROUP, P.C.
dba New gTLD Disputes

By:_____/jmg/_____
John M. Genga
Attorneys for DONUTS INC.

ANNEXES

The following Annexes are offered with and in support of this submission:

Annex A: TLDDOT Application for <.GMBH>, App. ID No. 1-1273-63351
Annex B: Printout of German Companies Register search for TLDDOT GmbH

Annex A

New gTLD Application Submitted to ICANN by: TLDDOT GmbH

String: gmbh

Originally Posted: 13 June 2012

Application ID: 1-1273-63351

Applicant Information

1. Full legal name

TLDDOT GmbH

2. Address of the principal place of business

Akazienstrasse 2
Berlin Berlin 10823
DE

3. Phone number

+49 30 49782354

4. Fax number

+49 30 49782356

5. If applicable, website or URL

http://www.dotgmbh.de

Primary Contact

6(a). Name

Mr. Dirk Krischenowski

6(b). Title

Chief Executive Officer

6(c). Address

6(d). Phone Number

+49 30 78711907

6(e). Fax Number

+49 30 78711907

6(f). Email Address

dk@dotgmbh.de

Secondary Contact

7(a). Name

Mr. Johannes Lenz-Hawliczek

7(b). Title

Chief Communication Officer

7(c). Address

7(d). Phone Number

+49 30 6690 9287

7(e). Fax Number

+49 30 6690 9285

7(f). Email Address

jlh@dotgmbh.de

Proof of Legal Establishment

8(a). Legal form of the Applicant

GmbH (company with limited liability)

8(b). State the specific national or other jursidiction that defines the type of entity identified in 8(a).

The legislation that defines the GmbH legal form can be found at the website of the German Ministry of Justice at http://www.gesetze-im-internet.de/gmbhg/

8(c). Attach evidence of the applicant's establishment.

Attachments are not displayed on this form.

9(a). If applying company is publicly traded, provide the exchange and symbol.

9(b). If the applying entity is a subsidiary, provide the parent company.

9(c). If the applying entity is a joint venture, list all joint venture partners.

Applicant Background

11(a). Name(s) and position(s) of all directors

11(b). Name(s) and position(s) of all officers and partners

Dirk Krischenowski	Chief Executive Officer

11(c). Name(s) and position(s) of all shareholders holding at least 15% of shares

DOTZON GmbH	Not Applicable
InterNetX GmbH	Not Applicable

11(d). For an applying entity that does not have directors, officers, partners, or shareholders: Name(s) and position(s) of all individuals having legal or executive responsibility

Applied-for gTLD string

13. Provide the applied-for gTLD string. If an IDN, provide the U-label.

gmbh

14(a). If an IDN, provide the A-label (beginning with "xn--").

14(b). If an IDN, provide the meaning or restatement of the string in English, that is, a description of the literal meaning of the string in the opinion of the applicant.

14(c). If an IDN, provide the language of the label (in English).

14(c). If an IDN, provide the language of the label (as referenced by ISO-639-1).

14(d). If an IDN, provide the script of the label (in English).

14(d). If an IDN, provide the script of the label (as referenced by ISO 15924).

14(e). If an IDN, list all code points contained in the U-label according to

Unicode form.

15(a). If an IDN, Attach IDN Tables for the proposed registry.

Attachments are not displayed on this form.

15(b). Describe the process used for development of the IDN tables submitted, including consultations and sources used.

15(c). List any variant strings to the applied-for gTLD string according to the relevant IDN tables.

16. Describe the applicant's efforts to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.

We anticipate that the introduction of the .GmbH TLD will cause no operational or rendering problems. New gTLDs have been used at least with 6 characters for over 10 years, therfore we are confident that the operation of the .GmbH TLD presents no new challenges. The rationale for this opinion includes that the string is not complex and is represented in standard ASCII characters and follows relevant technical, operational and policy standards for characters. The string length is within lengths currently supported in the root (63 characters) and should work with Internet programs such as web browsers and mail applications.

17. (OPTIONAL) Provide a representation of the label according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/).

Mission/Purpose

18(a). Describe the mission/purpose of your proposed gTLD.

* DEFINITIONS *

GmbH, abbreviation for „Gesellschaft mit beschraenkter Haftung"(English: company with limited liability) is the most common type of legal entity in Austria, Germany, Liechtenstein and Switzerland. The name of the GmbH form emphasizes the fact that the partners (Gesellschafter, also known as members) of the entity are not personally liable for the company's debts. The laws governing this type of legal entity (GmbH-Gesetz - GmbHG) were adopted in Germany in 1892, in Austria in 1906 and in Liechtenstein and Switzerland in 1936.

Companies with the "GmbH" type of legal entity are mandatory listed in the respective company registers of Austria, Germany, Liechtenstein and Switzerland, which are governed by the respective Chambers of Commerce in the countries. The highest institutions responsible for the term GmbH are the governments of the countries.

More than 1.4 mio. companies with the legal form of a GmbH are currently registered in
Austria, Germany, Liechtenstein and Switzerland.

* MISSION *

The mission for the .GMBH top-level domain is to provide a dedicated namespace that is intended to be used by GMBHs.

The .GMBH is the independent top-level domain for companies which are allowed to use GmbH as denotation of their legal entity (the Community). The domain names available with the .GMBH top-level domain are concise and create an individual identity for companies with this legal form. The .GMBH domain names will bring providers and customers of information, goods and services more intuitively together. The .GMBH domain names will lead to an improved image and attractiveness and will strengthen the legal form GmbH against other legal forms.

* PURPOSE *

The purpose of the .GMBH top-level domain is to serve the needs of the companies with this type of legal entity (the Community). The Community consists of companies that are at the time of registration and consecutively during the registration duration registered as a GmbH in the company registers of Austria, Germany, Liechtenstein and
Switzerland (the Members). Associated to the community are the company registers and the institutions responsible for legislation of GmbHs.

The needs of the Members of the GmbH Community are

- new and precise domain names which offer an alternative for the company's identity to the overcrowded namespaces .at, .ch, .de and .li.
- descriptive domain names which lead to competitive advantages by better search engine positions
- short domain names that are ideal for communication and advertising
- validated domain names that lead to greater trust in business with customers

The purpose in order to serve the needs incorporates a reasonable name space management including (i) the reservation and delegation of domain names for institutions relevant for GmbHs and their purposes such as company register

services, (ii) measures to mitigate domain grabbing, cybersquatting, speculation and other unlawful activities and (iii) measures to facilitate intuitive search for the public.

TLDDOT GmbH, the applicant, has worked at any time since its existence with the GmbH Community, its Members, and the regulatory authorities to incorporate their interests.

18(b). How do you expect that your proposed gTLD will benefit registrants, Internet users, and others?

i.

* SPECIALITY: An own namespace for the GmbH Community *

The speciality of the .GMBH top-level domain is, that it aims to become a new namespace exclusively dedicated for the communication and interaction of GmbH companies (the Community) among each other, with customers and Internet users in general.

* SERVICE LEVEL: A Quality Seal *

The Registry will offer a voluntary quality seal by which the Registrant may show to the public that he operates a trusted website and that he has been validated.

* REPUTATION: Secure and trustworthy Namespace *

The .GMBH namespace managed under the legislation of Germany and technically operated by
TLD-Box, an affiliate of the operator of the Austrian ccTLD .at, brings with it security, reliability, trust and credibility in an even higher level than already established by the national ccTLDs. The registration policies and the start-up planning ensure that only Community members may register a .GMBH domain name. Internet users can trust the ownership data 100% since all Registrants and domain names will be validated. This is a service level that is sought after by the global Internet community and which will contribute to the already positive reputation of the .GmbH namespace.

ii.

* COMPETITION – New choice in overcrowded namespaces *

When starting a new business in Germany with the legal form of a GmbH 67% of the companies do not get the desired domain name corresponding to their company names and need to choose a second- or third-best choice domain name according to a study we conducted in 2008. Many of the remaining 33% of companies choose a company name in dependence of the availability of a domain name or else need to buy the desired domain name on the domain aftermarket.

This is due to the overcrowded namespaces in .de (app. 15 mio domain names), .at (app.

1,1 mio), .ch (app. 1,8 mio) and also in the gTLD namespaces like .com or .org. And the situation is even getting worse over time, with a growing number of GmbHs, Internet users and domain names.

Not getting a good domain name which equates the company name means a competitive disadvantage for a new company right from the start, sometimes a severe one.
The .GmbH top-level domain name promises relief from this situation by offering a new namespace where short, descriptive, memorable, intuitive and suitable new domain names for GmbH companies will become available again.

Even if the price for a .GmbH domain name will be higher than a .de or .com one, the competitive advantages a company may gain from a suitable domain name will outpace a higher price by far. For more than 1.4 mio. GmbH existing companies .GmbH domain names will be an ideal supplement to their gTLDs and ccTLDs portfolio. Imagine that it might be much easier for a company to communicate ABC GmbH instead of ABC Service GmbH as a company name if they register abc.gmbh.

* DIFFERENTIATION – A speaking TLD with validated Registrants *

The .GMBH top-level domain and its .GMBH domain names are clearly differentiated to existing TLDs due to their descriptive and speaking nature which has a clear meaning and value to the targeted Registrants and Internet users: This is a GmbH company's domain name.

By validation of each single Registrant upon registration of a .GmbH domain name and an annual revalidation, the .GMBH namespace will offer security, reliability, trust and credibility in an even higher level than already established by the national ccTLDs. Internet users can trust the ownership data 100% since all Registrants are validated. This is not the case with the national ccTLDs and definitely not the case with gTLDs, where apart from the missing validation, proxy and⁄or privacy services complicates to identify the registrant.

Aim of the Registry is to reach 100% Whois accuracy.

* INNOVATION – The Domain Name Quality Seal (DNQS)*

After registration of a .GmbH domain name the Registry will offer to the Registrant a quality seal which the Registrant may place at its website to show that he is a validated domain name owner. The quality seal will have a displayed lifetime of one (1)
year and will be re-issued after revalidation of the Registrants eligibility. This is an absolute novelty in the domain name business. We are further planning to support the
GmbH Community Members by innovative services such as making websites more easy accessible for mobile devices, offering directory services and search engine optimization. The new .GMBH domain names will be suitable for search engines and other forms of communication.

iii.

Internet users in Austria, Germany, Liechtenstein and Switzerland will intuitively understand that domain names ending on .GMBH and the information and services found on such domain names are offered by GmbH companies. The intuitive and descriptive domain names under a "speaking TLD" like .GMBH will enable consumers to navigate and

search
more easily for information and services from GmbH companies on the Internet. It is also expected that search engines will give ranking preference to .GMBH domain names compared to other TLDs, if the .GMBH namespace is managed well and offers advantages over other TLDs. This will increase the visibility along with the strong marketing efforts for

.GMBH. But still the strongest argument is that the validated domain names will lead to greater trust in information and services offered by GmbH Companies.

iv.

.GMBH second-level domain names are restricted to the GmbH Community Members and regulatory authorities (Registrants). The Registry intends to offer the registration of domain names under .GMBH according to the following policies.

* START-UP and ALLOCATION SCHEDULE *

The .GMBH top-level domain will have a straight forward start-up schedule with the phases noted below:

Phase 1 - RESERVATION
- Reservation of names for the regulatory authorities, courts and institutions and their services to the GmbH Community Members such as a company register or legislative information.
- Reservation of names for defined interest groups of the GmbH Community including names for associations and chambers representing GmbH companies and their interests.
- Reservation of names for the technical operation, the namespace management, marketing and purpose of the .GMBH top-level domain as defined in #18a.
- Reservation of names in accordance with the ICANN specification 5 (2-characters, country names, others)

Phase 2 – SUNRISE
Sunrise according to the Trademark Clearinghouse rules. Eligible are all registrants who meet the eligibility criteria of .GMBH described below and whose trademarks were validated by the Trademark Clearinghouse. The TMCH Sunrise has a duration of 30 days; allocation follows the first-come, first-served principle.

Phase 3 – LANDRUSH
Registration of domains names that are corresponding with the name of registered GmbH company names by GmbH companies. Allocation follows the first-come, first-served principle.

*** .GmbH Registration Policy Description ***

The following text is a shortened and descriptive version of the full registration policy text which highlights the relevant information.

1 Structure of the namespace
This section will describe the structure of the namespace.
The namespace under .GMBH is not divided into second-level domain names.

2 Registrable characters
This section will describe the registrable characters
A .GMBH domain name can only consist of digits (0-9), hyphens, the letters a through z, the Latin Unicode character sets (Basic, Extended-A and Extended-B).

3 Priority Principle
This section will describe the priority principle
If no special allocation method is provided for a domain name, it is assigned categorically to this eligible Registrant whose application has been first received by the Registry in the technically correct manner and in accordance with the registration policy and has been first written in the Registry database (also called priority principle, ”first come, first served”).

4 Eligibility Requirements – General
This section will describe the general eligibility requirements for registering a .GmbH
domain name.

With the registration of a .GMBH domain name each Registrant implicitly signs the registration requirements and agrees with the fact that he acknowledges compliance with the registration requirements.

5 Eligibility Requirements – Registrant
This section will describe the eligibility requirements applicable to the registrant. The .GMBH top-level domain is intended to serve the GmbH Community. To meet the requirements of ICANN to a community-based designation of the top-level domain and to meet a sufficient reference to the legal form GmbH, the group of Registrants is limited.

6 Eligibility Requirements - Content and Use
This section will describe the eligibility requirements applicable to content and use. To meet the requirements of ICANN to a community-based designation of the of the top- level domain, the Registrant must satisfy criteria for the content and the use of .GMBH domain names.

7 Eligibility Requirements - Domain Name Selection
This section will describe the eligibility requirements applicable to the domain name selection.
To meet the requirements of ICANN to a community-based designation of the top-level domain, the Registrant must satisfy the criteria for the domain name selection of .GMBH domain names.

8 Registration Agreement
This section will describe the registration agreement
The contract for the registration of the domain is entered into between the Registrant and a Registrar accredited by ICANN.

9 Registration
This section will describe the registration procedure.
The domain name registration of a Registrant is electronically sent by the Registrar to the registration system of the Registry using the EPP protocol.

10 Transfer of Domain Names
This section will describe the transfer of domain names
Domain names can be transferred only to applicants who are eligible to register .GMBH

domain names and fulfill all eligibility requirements.

11 Whois
This section will describe the Whois requirements.
The administrative contact of a .GMBH domain shown in the Whois database (Admin Contact) has to be a natural person who as an agent for the domain owner (Registrant Contact) has the right and obligation to make binding decisions on all matters concerning the domain.

12 Phased Registration
This section will describe the registration schedule.
The holders of prior rights enjoying protection are eligible to register domain names during the phased registration first phase, the ”Trademark Clearinghouse” Sunrise period, before the free registration (Landrush) for the top-level domain .GMBH begins.

13 Enforcement, Termination and Deletion
This section will describe the enforcement, termination and deletion procedures.

The Registry is entitled to lock, cancel, initiate the gTLD-deletion cycle or transfer domain names that do not meet the registration criteria if …

14 Dispute Procedures
This section will describe the dispute procedures.
To prevent bad faith registration and use of domain names under the top-level domain .GMBH, every domain name Registrant has to subject to the dispute resolution procedure proposed by ICANN or the Registry (UDRP, URS, PDDRP and the Eligibility Requirements Dispute Resolution Policy (ERDRP)).

15 Validation
This section will describe the validation of .GmbH domain names.
It is the role of the Registry to assure and control the compliance with the eligibility requirements for any domain name to guarantee the Community aspect and integrity of the
.GMBH namespace and to avoid disputes.

v.

The use of proxy and privacy services to protect the privacy or confidential information of registrants or users will be not allowed. The reasons are that legal entities such as a GmbH cannot demand privacy under the Austria, Germany, Liechtenstein and Switzerland legislation and that proxy and privacy services would not allow a proper validation and
a public visibility of accurate Whois data in line with the eligibility criteria.

vi.

The applicant has already conducted manifold outreach regarding the benefit of the upcoming new GmbH namespace including

- speeches at public target group events, such as from the German Chamber of Commerce and Industry, investment forums and at other occasions,
- publications together with industry associations and chambers about .GmbH,
- presentation of .GmbH in constituencies of industry associations and chambers,
- presentation of .GmbH in front of politicians,

- publically on its intuitively accessible website www.dotgmbh.de and at ICANN meetings,
- by press releases.

In preparation of the forthcoming launch and beyond the Registry will use its network of national associations, multipliers, media and advertising partners to promote .GMBH in order to reach the projected domain name registrations and to transport the benefits of
.GMBH to the farest corner of the Community.

For the .GMBH top-level domain, the Registry will cooperate closely with the media departments of chambers and associations, as well as with a number of publishing and broadcast partners from the Community, in order to plan and implement a comprehensive communication strategy with the aim to gain awareness within the GmbH Community. We will continue to communicate the benefits of .GMBH domains names within the community. We are confident that our broad outreach program, which is part of our marketing efforts, will help us to achieve the projected benefits of .GMBH.

18(c). What operating rules will you adopt to eliminate or minimize social costs?

i.

All available .GMBH domain names will be registerable on a ”first-come, first-served” basis, except of reserved names. All allocations mechanisms shall be in accordance with the community-based purpose of .GMBH. The reserved names in Phase 1 (see #18b iv) have special allocation mechanisms as described as follows:

- Names for the regulatory authorities, courts and institutions will be released by the
Registry upon request of the entity for their own use.

- Names for defined interest groups of the GmbH Community including names for associations and chambers representing GmbH companies will be released by the Registry upon request of the entity for their own use.
- Reservation of names for the technical operation, the namespace management, marketing and purpose of the .GMBH top-level domain as definded in #18a. These names will be released by the Registry for its own use.
- Reservation of names for the technical operation, the namespace management, marketing and purpose of the .GMBH top-level domain as defined in #18a.
- Reservation of names in accordance with the ICANN specification 5. These domain names may be released based on ICANN defined procedures and can be registered by eligible registrants.
- Disputed Domain Names - The Registry may set aside during regular operations domain names that are being reviewed under dispute resolution procedures. These domain names may become available for registration after the dispute is concluded.

ii.

As of today no cost benefits are planned. However, the Registry will, in its own

discretion and depended on the development of the .GMBH namespace, decide to implement cost benefits, if appropriate.

iii.

.GMBH domain names will be available through ICANN accredited registrars who will be provided non-discriminatory access to registry services. The registration period for Sunrise and general availability will have a term of one to ten years.
The Registry reserves the right to reduce pricing for promotional purposes in a manner available to all accredited registrars. The Registry reserves the right to work with ICANN to initiate an increase in the wholesale price of domains if required. The Registry will provide reasonable notice to the registrars of any approved price increase.

Community-based Designation

19. Is the application for a community-based TLD?

Yes

20(a). Provide the name and full description of the community that the applicant is committing to serve.

* DELINEATION *

The GmbH Community and its members are clearly and sharply delineated because they (i) are all entities, (ii) are all registered in official registers and (iii) are operating, representing or overseeing a company or companies with the legal form of a GmbH as described in #18.

The GmbH Community includes regulatory authorities, courts, institutions, associations, chambers and the GmbH companies tehmselves. The core of the community are the companies with the legal form of a GmbH.

* STRUCTURE and ORGANIZIATION *

The GmbH Community is well organized along the lines of the following model:

Layer 1 - Governments (Oversight)
The governments of Austria, Germany, Liechtenstein and Switzerland are the guardian and oversight and regulatory bodies of the national legislation regarding companies with the legal form of a GmbH. The governments have also installed the official company registers where GmbH companies need to be registered and operate services regarding administrative needs of GmbH companies.

Layer 2 - Chambers and Associations (Representation)

Chambers and associations play an important role in the distribution and dissemination of information from the legislative bodies of layer 1 to the GmbH companies and in the lobbying of the interests of GmbH companies in the public and opposite to the governments. In some countries like Austria and Germany the GmbH companies are mandatory member of a chamber.

Layer 3 – The GmbH companies (Operation)
These are the sole companies with the legal form of a GmbH.

* General *

A GmbH is formed in three stages: the founding association, which is regarded as a private partnership with full liability of the founding partners/members; the founded company (often styled as "GmbH i.G.", with "i.G." standing for in Gründung – literally "in the founding stages", with the meaning of "registration pending"); and finally the fully registered GmbH. Only the registration of the company in the Commercial Register (Handelsregister) provides the GmbH with its full legal status. The founding act and the articles of association have to be notarized. The GmbH law outlines the minimum content of the articles of association, but it is quite common to have a wide range of
additional rules in the articles.

* ESTABLISHMENT and ACTIVITIES *

The GmbH Community as described above exists since over 100 years in Austria and Germany and over 70 years in Liechtenstein and Switzerland (http://en.wikipedia.org/wiki/Gmbh). The activities of the GmbH Community include all facets of political and economic activities with regards to GmbH's including legislation, parliamentary hearing, large events and conferences, publication of information, annual reports, scientific research and others. The topic of GmbH companies is integral part of the daily business in Austria, Germany, Liechtenstein and Switzerland.

* SIZE, MEMBERSHIP and GEOGRAPHIC EXTENT *

The GmbH Community comprises of about 1.4 million companies with the legal form of a GmbH in in Austria, Germany, Liechtenstein and Switzerland, thereof about 1.15 million in Germany.

The membership to the Community is clearly regulated by law in all the countries – you can only operate a GmbH and be member of the GmbH Community if you are officially registered. The publication of the registration data (GmbH business number) is done differently in the countries but all registers are publicly accessible.
An additional membership to the national or local Chambers of Commerce and Industry with individual costs is mandatory in Austria and German, not in Liechtenstein and Switzerland.

20(b). Explain the applicant's relationship to the community identified in 20(a).

* RELATIONSHIP TO COMMUNITY ORGANIZATIONS *

The applicant, TLDDOT GmbH, is a member of the community since it is registered as a GmbH with the Chamber of Commerce and Industry in Berlin (IHK zu Berlin) with the registration number HRB 124498 as mentioned in the applicant profile.

TLDDOT GmbH is also member of the largest association representing the interests of GmbH companies, the BVMW (The German Association for Small and Medium-sized Businesses). The Berlin-based BVMW is a politically independent association which caters for all commercial branches and professions, and represents the interests of small and medium- sized businesses in politics, with administrative authorities, with trade unions and
with major companies. The BVWM has around 80.000 GmbHs as members.

By this the applicant, TLDDOT GmbH, is a member that is eligible according to the GmbH Community criteria.

* RELATIONSHIP TO THE COMMUNITY PARTS *

The applicant, TLDDOT GmbH, has a relationship to all layers of the GmbH Community structure as described in #20a.

1. TLDDOT GmbH maintains a long-standing relationship to the governments in Austria, Germany and Switzerland via the members of the Governmental Advisory Committee at ICANN (Liechtenstein is represented by Switzerland), and has consulted with them on the creation of the .GmbH namespace. TLDDOT GmbH has various other contacts to governmental representatives. The government of Germany has already pre-reserved several names for its reserved names list under .GmbH.

2. TLDDOT GmbH and its managers maintain also relationships to other organizations representing GmbH companies, such as the Deutsche Industrie- und Handelskammer (www.dihk.de), Wirtschaftskammer Österreich (www.wko.at), Association of Berlin Merchants and Manufacturers e.V. (www.vbki.de), medianet Berlin-Brandenburg e.V. (www.medianet-bb.de), Unternehmerverband Berlin-Brandenburg e.V. (www.uv-berlin.de), eco Verband der deutschen Internetwirtschaft e.V. (the association for the German Internet economy, www.eco.de), BITKOM - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (the German association for information technology, telecommunications and new media, www.bitkom.org).

3. TLDDOT is a GmbH itself.

* ACCOUNTABILITY MECHANISMS *

1. Advisory Board
The applicants advisory board will be set up in 2012, it has a consultative and supporting position for the approval activities and for the subsequent operation of the top-level domain .GMBH. The advisory board also helps to anchor, in a socially responsible way, the top-level domain .GMBH in the GmbH Community made up of political, commercial, cultural, social and individual interests. It also advises the Registry on policies such as the issuing of domains, taking account of the various interests fairly and transparently. The heterogeneous composition of the advisory board can make use of a variety of experience, knowledge and contacts. The advisory board includes (in
alphabetic order):

- Ruediger Eisele – In-house counsel of the BVMW (German Association for Small and Medium-sized Businesses)
- Dr. Hagen Hultzsch – Former ICANN director and former member of the management board of Deutsche Telekom AG
- Hans-Joachim Reck – Managing Director of the VKU (Association of municipal Companies in Germany)

2. Annual Reports
The Registry will publish annual reports on operations of the .GMBH top-level domain and inform the public on other relevant developments in the .GMBH name space.

3. Ombudsman
The Registry will establish an ombudsman.

4. Education
The Registry will publish educational papers, speeches and other public awareness creating measures (already ongoing).

* DISCLOSURE *

Shareholder of the applicant is the ICANN accredited Registrar PSI USA Inc/InterNetX GmbH.

20(c). Provide a description of the community-based purpose of the applied-for gTLD.

* REGISTRANTS *

Eligible and intended registrants of .GMBH domain names are

- companies which are at the time of registration registered as with the legal form of a GmbH (including mbh, gGmbH, GesmbH and Ges.m.b.H.) in an official company register in Austria, Germany, Liechtenstein, Switzerland or any other country where the registration of a GmbH company may be allowed, and
- regulatory authorities and institutions in Austria, Germany, Liechtenstein and Switzerland that are involved in any proceedings regarding companies with the legal form of a GmbH, and
- registered associations and chambers representing GmbH companies and their interests

* END-USERS *

Intended users of .GMBH second-level domain names are members of the GMBH Community and Internet users worldwide which are looking for GmbH related information especially targeting Austria, Germany, Liechtenstein, Switzerland.

* ACTIVITIES *

The applicant has carried out a set of activities to support the purpose of the .GMBH TLD. The most important activities included the consulting with the German Chamber of Commerce and Industry (DIHK) and the Austrian Business Chamber (WKO) in

order to define eligible Registrants as well other policies regarding Registrant validation, reserved names and other topics. Both chambers have, on a daily basis, major tasks with the foundation, maintenance and deletion of GmbH companies.

The applicant spoke with many community members in the respective countries, discussed the concept for a .GMBH TLD, the benefits, usage and prices. Furthermore the applicant has conducted outreach regarding the benefit of the upcoming new GmbH namespace including

- speeches at public target group events, such as from the German Chamber of Commerce and Industry, investment forums and at other occasions,
- publications together with industry associations and chambers about .GmbH,
- presentation of .GmbH in constituencies of industry associations and chambers,
- presentation of .GmbH in front of politicians,
- publically on its intuitively accessible website www.dotgmbh.de and on ICANN meetings,
- by press releases.

Other activities that are intended to serve the purpose of the .GMBH namespace included the definition of safeguards to avoid and mitigate domain grabbing, cybersquatting, speculation and other unlawful activities as well as policies against domain name abuse and an Eligibility Requirements Dispute Resolution Policy (ERDRP).

* LASTING PURPOSE *

It is not expected that the legal form of a GmbH will disappear within the next decade in Austria, Germany, Liechtenstein, Switzerland. In opposite, the countries are doing everything to make the legal form or a GmbH more attractive against its competitor, the Limited (Ltd.), e.g. in Germany the requirements to found a GmbH have been modernized (Gesetz zur Modernisierung des GmbH-Rechts und zur Bekämpfung von Missbräuchen - MoMiG). By this the basis for the .GmbH business will even grow.

The .GMBH top-level domain and its purpose are of a long-lasting nature since digital marketing and distribution and individual digital addresses (domain names) have become an integral component of general business and individual and personal practices and thereby also for the .GMBH Community as a whole. It is foreseeable and anticipated that digital instruments and tools such as .GMBH domain names will play an ever increasing role for any society’s interaction within the next decade and beyond. The .GMBH top- level domain will thereby serve the GmbH Community and its members in a lasting nature and will fulfill its purpose of providing validated, meaningful and easily recognizable domain names.

20(d). Explain the relationship between the applied-for gTLD string and the community identified in 20(a).

* RELATIONSHIP TO THE COMMUNITY *

The proposed top-level domain name, “GMBH”, is without any doubt widely known among the general public as the most often used legal form of a legal form designation of companies. All companies with the ending “GmbH” have to be registered before using the name. Therefore there is a very strong relationship between the applied-for string and the name of the community.

* RELATIONSHIP TO THE COMMUNITY MEMBERS *

The .GMBH Community Members are over 1.4 million companies that are currently using GmbH as their legal form. There cannot hardly be a stronger relationship between those entities and the applied-for string, since the string “Gmbh” identifies their legal representation.

* FURTHER CONNOTATIONS *

The string “GMBH” has to the applicant’s knowledge no further connotations.

20(e). Provide a description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD.

* .GmbH Registration Policy Description (community-relevant part)*

The following text is a shortened and descriptive version of the full registration policy text which highlights the relevant information.

4 Eligibility Requirements – General

With the registration of a .GMBH domain name each Registrant implicitly signs the registration requirements and agrees with the fact that he acknowledges compliance with the registration requirements. However, it is validated on the discretion of the Registry if the registration of every single domain name registration fulfills the registration requirements (eligibility). Eligibility is necessary on both, the Registrant’s identity and the domain name selection. Additionally anyone can check the compliance with the registration requirements by initiating an extrajudicial dispute resolution procedure (Eligibility Requirements Dispute Resolution Policy, ERDRP).

5 Eligibility Requirements – Registrant

The .GMBH top-level domain is intended to serve the GmbH Community. To meet the requirements of ICANN to a community-based designation of the top-level domain and to meet a sufficient reference to the legal form GmbH, the group of Registrants is limited. Exclusively eligible to register domain names under the top-level domain .GMBH are:

- companies which are at the time of registration of a .GmbH domain name registered with the legal form of a GmbH (including mbh, gGmbH, GesmbH and Ges.m.b.H.) in an official company register in Austria, Germany, Liechtenstein, Switzerland or any other country where the registration of a GmbH company may be allowed,
- regulatory authorities and institutions in Austria, Germany, Liechtenstein and Switzerland that are involved in any proceedings or functions regarding companies with the legal form of a GmbH, and
- registered associations and chambers representing GmbH companies and their interests.

Not eligible are companies that
- have the legal form of a GmbH & Co. KG or comparable legal forms where the GmbH is not the constitutive legal entity, or
- GmbH companies in foundation (GmbH i.Gr.), or
- GmbH companies after filing an insolvency notice,
- companies with the legal form of a Unternehmergesellschaft (UG).

In the event a Registrant's GmbH company has been deleted from the Company Register the Registrant must delete the domain name at latest at the next annual renewal date. In the event a Registrant changes the GmbH company's name or the object of a company the registered domain name must still fulfill the registration requirements or must be deleted otherwise at latest at the next annual renewal date. It's in the discretion of the Registrant not to lead to the conclusion that a not existing GmbH exists.

6 Eligibility Requirements - Content and Use

To meet the requirements of ICANN to a community-based designation of the top-level domain, the Registrant must satisfy the following criteria for the content and the use of .GMBH domain names:

(i) The contents of the website must be accessible under a domain directly related to the eligibility requirements (Registrant, Content and Use, Domain Name Selection), and (ii) the domain must be in use within 12 months of registration.

7 Eligibility Requirements - Domain Name Selection
To meet the requirements of ICANN to a community-based designation of the top-level domain, the Registrant must satisfy the following criteria for the domain name selection of .GMBH domain names:
A .GmbH domain name selected in the discretion of the Registrant must correspond either
- fully or in relevant parts with the company's name or
- with goods and services as mentioned in the corporate purpose of a company as mentioned in Company Register concerned. It is up to Registrant to define which parts of the company's name are relevant.

12 Enforcement, Termination and Deletion

The Registry is entitled to lock, cancel, initiate the gTLD-deletion cycle or transfer domain names that do not meet the registration criteria if

i the domain name owner has persistently breached the registration policies and continues to do so after a warning and a deadline or
ii. The domain name contains in itself a manifestly illegal statement, or
iii. The domain name owner has agreed in writing, under penalty of law, not to use the domain name, or has issued a corresponding final declaration or an injunction has been issued a corresponding final national or international main judgment against him or
iv. it has been determined in a final and absolute national or international judgment that the registration of the domain name owner violates the rights of third parties, or the domain name owner has made a final declaration to a corresponding injunction, or
v. the registration of the domain name to the domain name owner blatantly violates third party rights or is otherwise unlawful regardless of the specific use, or

vi. the use of the domain name or content under it is obviously abusive or can do harm to the public, for instance through illegal and fraudulent activities, spam, phishing, pharming, malware propagation, botnet activities, child pornography or unusual network activities (eg fast flux hosting), or
vii. the data given to the Registry for the domain name owner or the administrative contact is incorrect or the identity of the Registrant or the administrative contact cannot be found with the given data.

Without prejudice to further legal rights, as part of abusive use rules required by ICANN for gTLDs (".GMBH Anti-Abuse Rules") the Registry can under certain circumstances, remove a domain name and its technical data from the name servers for top-level domain
.GMBH (disconnection), change the contact data, or delete a domain name.

13 Dispute Procedures

To prevent bad faith registration and use of domain names under the top-level domain .GMBH, every domain name Registrant has to subject to the dispute resolution procedure proposed by ICANN or the Registry (UDRP, URS, PDDRP and the Eligibility Requirements Dispute Resolution Policy (ERDRP)). The involvement of national courts is at liberty as a dispute resolution procedure. A domain may be deleted due to a dispute resolution process, or transfer, if

i. the domain name is identical or confusingly similar to a brand or a label from which the complainant has rights,
ii. the domain name owner has no right or legitimate interest in the domain name,
iii. The domain name has been registered and is used in bad faith,
iv. a domain name, which was subject to a special registration procedure, is used or transmitted contrary to the contractual agreements,
v. the registration of a domain name violated the registration policies.

14 Validation

It is the role of the Registry to assure and control the compliance with the eligibility requirements for any domain name to guarantee the Community aspect and integrity of the
.GMBH namespace and to avoid disputes. The Registry anticipates that disputes over eligibility will be minimal within the GmbH Community. Nevertheless it has put in place an adequate procedure to assist the GmbH Community's Registrants in dealing with denials of eligibility in a way that supports community needs and values. The Registry's
informal denial procedures will not super-cede any formal dispute procedures.

Any .GmbH domain name registered is subject to a subsequent eligibility requirements validation process which will start immediately after the registration process starts. Eligibility validation will occur after domain name registration but before the registered domain name can be used for web services and protocols like email, website, and FTP. This is to avoid mass fraudulent domain name registrations.

20(f). Attach any written endorsements from institutions/groups representative of the community identified in 20(a).

Attachments are not displayed on this form.

Geographic Names

21(a). Is the application for a geographic name?

No

Protection of Geographic Names

22. Describe proposed measures for protection of geographic names at the second and other levels in the applied-for gTLD.

TLDDOT GmbH will protect names as per the requirements in the New TLD Registry Agreement (Specification 5, paragraph 5) by reserving the country and territory names at the second level and at all other levels within the TLD. A list of those names will be compiled and published to relevant audiences before the TLD is introduced. These domains will be blocked following the Governmental Advisory Committee (GAC) advice "Principles regarding new gTLDs", at no cost to the relevant organization, so that no parties may register them as a domain name.

Together with the respective governments and ccTLDs as well as with ICANN we will define procedures and set-up agreements by which the above reserved domain(s) may be released to the Registry Operator and may be registered consecutively by eligible and appropriate parties.

Registry Services

23. Provide name and full description of all the Registry Services to be provided.

*** DISCLAIMER ***

THE RESPONSE FOR THE QUESTIONS 23-44 MAY USE ANGLE BRACKETS (THE " 〈" and "〉 " CHARACTERS, or < and >), WHICH SEEM TO NOT BE PROPERLY RENDERED IN TAS DUE TO SECURITY CONCERNS. HENCE, THE ANSWER AS DISPLAYED IN TAS MAY NOT RENDER THE FULL RESPONSE AS INTENDED.

Technical operations of the Registry will be outsourced to "TLD-Box Registrydienstleistungen GmbH", and a signed contract for the provision of those services with TLD-Box exists. A more detailed description of that outsourcing relation is described in response to question 31.

The Registry operating the proposed gTLD will provide the following Registry Services (Services are numbered according to the Questions and Notes in ICANN's application guidebook):

(A), (i): "Receipt of data from registrars concerning registration of domain names and name servers": The interface for receipt of such data (Shared Registry Service - SRS) is fully based on the Extensible Provisioning Protocol (EPP) and conforms to the relevant RFCs (see answer to Question 25). Beyond the standard EPP object mappings and commands, no proprietary EPP extensions are used (unless ICANN requirements necessitate the use of draft level specifications, i.e. for the Trademark Clearing House integration). This Registry Service is operated on a cluster of at least two physically independent servers as an active-active load-balanced group which interact with a clustered registry database backend (detailed in response to Question 33). Access to that interface is controlled by two-factor authentication mechanisms with one factor being the IP address of the registrar's EPP client and the second factor being the registrar's credentials (username⁄password). Traffic is encrypted with TLS. Access attempts from an IP addresses that is not registered with the Registry Operator are denied. A detailed specification of the EPP interface is contained in answer to Question 25, while the architecture of the EPP frontend is included in response to Question 32. The software used to provide the EPP service is readily available at the time of this writing. The software is based on the EPP software used to provide Registry services for the ".at", ".no" and ".bh" ccTLDs with the domain lifecycle and periods adapted to the requirements for new gTLDs. The EPP service is available over both IPv4 and IPv6 transport.

(ii): "Provision to registrars of status information relating to the zone servers for the TLD": The registry operator will operate an announcement mailing list where updates regarding the operational status of the zone servers of the TLD will be posted. Additionally, registrars can query for the zone server status of an individual domain name under the TLD via the EPP or WHOIS interfaces - both interfaces will contain the relevant EPP status values (refer to the answer to Question 27 Registration Life Cycle which lists the domain's zone server status depending on the domain status).

(B), (iii): "Dissemination of TLD zone files": Zone generation and the subsequent DNSSEC signing of that zone is performed in parallel on two physically separate zone generators based on the current data in the registry database. After performing offline checks for the integrity of the zone file, the TLD zone file is loaded onto two hidden master nameservers (the zone file of the second zone generator is only used in case of an emergency situation with the first zone generator). These hidden masters supply the public nameserver network with the current zone file. For zone dissemination the standard DNS mechanisms of NOTIFY and IXFR⁄AXFR, protected by TSIG, are used. Integrity checks are performed to detect errors such as incomplete zone generation, incorrect DNSSEC key usage, key signing keys not matching DS records in the parent zone or an NSEC⁄NSEC3 chain problem.

The DNS query based verification procedures include the following set of checks on the published KSK and ZSK:

** Check if the published KSK matches a published DS-Record in the parent zone

** Check if the signature of the SOA and the Zone-NS-Records are included and correct
** Query (with DO-bit set) for 20 predefined existing domain names, check the results and validate the received signatures
** Query (with DO-bit set) for 20 predefined non-existing zone names, check the results and validate the received signatures
** Query (with DO-bit set) for 20 new (or changed) domains since the last zone generation, check the result and validate the received signatures (the zone generator generates a diff-file with the changes made and the verification tools choose 20 records randomly)
** Query (with DO-bit set) for the predefined end-of-zone-record of the zone, check the results and validate the received signatures.

Only if these checks succeed is the zone file propagated to the hidden masters - otherwise the rollout of this zone file is stopped and operations staff are notified. Consistency checks of the loaded zonefile are also performed on the hidden masters. Zone file access as required by ICANN is also provided. These procedures are the result of practical experience and knowledge gained from operating the ".at" TLD for over 15 years.

(iv) "Operation of the Registry Zone servers": The TLD zone servers will consist of a mix of Anycast and Unicast servers in order to ensure high availability in accordance with ICANN SLA requirements and to achieve a high level of diversity in terms of software and IP connectivity. A stable high-performance DNS network with 100% availability is one of the major key components of a successful gTLD operation. As a result the DNS network is carefully designed to fulfil those requirements. Anycast-DNS with multiple geographic locations is utilized to minimize latency, distribute traffic and increase resilience against attacks. Unicast servers are used to increase diversity across the DNS network. The zone for the TLD will not contain any wildcards or other means to modify NXDOMAIN responses. More details about the DNS network structure is contained in response to Question 35.

(C), (v) "Dissemination of contact and other information concerning domain name registrations" (WHOIS service): A port-43 WHOIS (and a lightweight alternative) as well as a web-based WHOIS will be provided. In accordance with Specification 4 of the Registry Agreement, the WHOIS service is fully compliant with RFC 3912, and provides information about domain names, registrars and nameservers. Free public access to that information is granted. Web based access is also supported. The service is based on a scalable and redundant architecture to meet the required SLAs. To address privacy considerations, rate limiting on a per-IP-address basis is employed on the WHOIS interfaces. In addition to the WHOIS service, the Registry will also offer a "Domain Availability Service" using the "Finger" protocol as defined in RFC 1288. This service can be used by registrars to check whether a domain name is available or not but does not provide any other information. The implementation is fully RFC compliant. Since finger is a very simple protocol with a minimum of overhead, requests can be processed quickly by the registry systems, which saves on computing resources for both the registry and registrar. The Finger service is a read-only interface and does not pose any security risks for the registry. Instead, providing such an interface (which is functionally identical to the IRIS dchk) offloads pure "availability" checks from the more heavyweight WHOIS and EPP interfaces which helps to improve the overall performance of those services.
(D) "Internationalized Domain Names": The registry will offer IDNs as detailed in the response to Question 44. IDN support in the proposed registry will strictly adhere to all relevant standards. Only labels with explicitly permitted code points will be allowed. The registry will be conservative in allowing additional code points and will only allow code points that do not carry risks such as user confusion or technical issues caused by lack of client support etc.

(E) “DNS Security Extensions (DNSSEC)”: The registry will perform zone signing activities in accordance with ICANN requirements and industry best practice. The respective Delegation Signer (DS) Records will in full compliance with established procedures be sent to IANA for inclusion in the root zone to establish a chain of Trust. The EPP interface of the Registry will also accept key material to extend that chain of trust down to individual domain name registrations. Further information about DNSSEC procedures is contained in response to question 43.

Regarding ICANN’s “Consensus Policies”, the Registry will provide the necessary services to comply with these policies (as well as any Temporary Policies as adopted by ICANN). This includes support for ICANN’s UDPR and URS processes. The Registry Operator will also restrict Registrar use of the “Add Grace Period” (AGP) as required by the “Add Grace Period Limits Policy”.

The registry system (software, documentation, test infrastructure) providing the above mentioned Registry Services is readily available at the time of this writing and most of the components are in production use by one or more TLDs.

All registry services are based on well-known industry standards and implement RFCs developed by the Internet Engineering Task Force.

The Registry will not operate any services that are specific or unique to the particular TLD. Hence, it is expected that potential registrars will require only minimal effort to connect to the Registry Systems to be able to perform registrations of domain names under the TLD.

Registrar Web: Registrars will be provided with a “Registrar Web”, a web site specifically targeted at registrars that will support registration procedures and allow registrars to change the configuration of their Registry account. This will include administration of their EPP login (particularly their client IP addresses) details, invoice downloads and financial functions such as topping up prepaid credit with the registry. Terms and conditions as well as registry policies are also available for download. Moreover the registrar web page provides statistics to registrars, gives them an overview of transactions requiring payment and shows available credit.

Registrar Helpdesk

A helpdesk will also be provided for registrars. This helpdesk will handle technical, legal and administrative inquiries from registrars. Helpdesk agents can be reached via email, telephone and fax. A professional ticketing system and qualified agents will ensure that all queries are handled within an appropriate turnaround time. Helpdesk services will be available during working hours on business days and an additional emergency contact will be available 24⁄7.

Security

The Registry Operator takes significant measures against (1) the unauthorized disclosure, alteration, insertion or destruction of Registry data and (2) the unauthorized access to or disclosure of information or resources on the internet. This includes a detailed security policy (contained in answer to Question 30), a secure architecture (see response to Question 32), a multi-layered backup strategy (details in response to Question 37) and a domain name lifecycle that makes it extremely unlikely that third parties can gain control over the registration record of a domain (see response to Question 27).

Stability

The operation of the TLD and the Registry Services offered do not involve any technology or business practice that has the potential to adversely affect the stability of the TLD's services and/or the DNS as a whole. All protocols used are based on authoritative standards published by well-established and recognized standards organizations. For example, the DNS service provided for the TLD is in strict compliance with the relevant RFCs created by the Internet Engineering Task Force and as a result will be fully compatible with existing and deployed internet technology. Specifically, the TLD will not engage in any DNS "tricks" such as wildcard or NXDOMAIN redirection and will ensure that no conditions affecting the throughput, response time, consistency or coherence of responses to Internet servers or end systems arise.

In order to fulfill the functions described above, the Registry Backend Operator also performs operations of standard business components, such as:

Permanent office location infrastructure in two cities (Vienna and Salzburg), including three meeting rooms, with additional emergency office space contracted. Rented datacenter space at various locations.

Billing and Financial administration and infrastructure

Technical office infrastructure such as IT systems (file storage, email/fax systems, document management), call-center enabled PBXes with integrated mobile devices, Teleconferencing equipment, fail-safe networking infrastructure between office locations themselves, and between office and datacenter locations.

These basic "business building blocks" are established since nearly 15 years, and are used for the day to day operations of the registry backend operations. Since some of the the elements listed above are assumed to be standard business commodities that are not specific to the operations of a gTLD registry, they are not described in further detail in subsequent answers (eg. enterprise PBX).

A number of the Registry Back-end Operator's staff are actively engaged in numerous working groups within the Internet Engineering Task Force, particularly those focused on DNS, ENUM, emergency services and geographic location. In addition several of these employees are authors of published and draft IETF RFCs.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

High-level SRS systems description:

The Shared Registry System is based on the Extensible Provisioning Protocol (EPP) and employs a multi-tiered architecture with public facing interfaces completely segregated from backend functions (such as database and management interfaces). An overview of the functionality provided by the SRS is as follows:

Registrars connect to and authenticate against the EPP frontend systems.
Those frontends receive and parse all EPP commands to perform checks of business logic (including any policy requirements) and subsequently perform (or reject) the requested action against the back-end data storage.
The back-end data storage is handled by a Relational Database Management System (described in detail in response to Question 33).

The server elements used for the SRS employ a number of technologies to ensure service availability and reliability. These include the use of multiple, virtualised Linux servers and several layers of high-availability functionality such as active-active load balancing, standby components and replication of full virtual machine images. A significant amount of design and implementation effort has focussed on removing any potential single point of failure in the SRS architecture. This architecture has also been fully tested and verified on a functionally identical prototype system, and is operational for the ".bh" migration. Some of that work included training and verification by independent third party system architecture experts, in particular the critical system availability functions such as cluster failover and real-time block device level replication.

The SRS software itself is readily available at the time of this submission. It is implemented and operated in accordance with the requirements of Specification 6 („Registry Interoperability and Continuity Specifications") and the respective SLAs in Specification 10. The SRS uses EPP as its core provisioning protocol and supports, amongst other RFCs, the following provisioning RFCs as required in Section 1.2 of Specification 6:

RFC 5730 (EPP Base Specification)
RFC 5731 (EPP Domain Name Mapping)
RFC 5732 (EPP Host Mapping)
RFC 5733 (EPP Contact Mapping)
RFC 5734 (EPP TCP Transport).
RFC 3735 (EPP Extension Guidelines)
RFC 5910 (DNSSEC Mapping)
RFC 3915 (Grace Period Mapping)

For maximum interoperability, only EPP functionality that is documented in the above RFCs is implemented – i.e. there are no proprietary EPP extensions used in the SRS. Further details about the implementation of the EPP Registry Services are contained in response to Question 25 ("EPP").

It is understood that SRS availability and 100% data integrity are absolute key requirements for the deployment of a successful TLD operation. As a result the SRS implementation was developed with a strong focus on those key factors.

The core software platform employed by the SRS, with its powerful modular policy functionality has been in production use for the „.at" ccTLD (nic.at) since 2003, additionally the „.no" ccTLD (norid) successfully migrated to the registry software over the course of 2010. Another installation of the software was recently rolled out to support the migration of the ".bh" ccTLD (Kingdom of Bahrain) from the incumbent operator to the Regulatory Authority of Bahrain. Furthermore, this core software is currently being used to provide SRS implementations for ENUM (Electronic Numbering) Registries in Austria (+43) and Ireland (+353). Finally, test instances of this customised software for ENUM are deployed in The Netherlands and Australia.

The modular and highly extensible structure of the SRS software allows for customized per-TLD policies that are implemented on top of an identical core registry system. This allows for code reuse between different TLD implementations,

regardless of the policy framework required.

The implementation of this software, specifically for this new gTLD, has been customized to the needs of the registry operator and to meet or exceed ICANN's policy and SLA requirements set out in the Applicant Guidebook for new gTLDs. A detailed description of the architecture supporting the SRS software is contained in answer to Question 32 (Architecture).

Details for the DNS elements of the TLD service, including zone file creation, signing, dissemination and testing procedures are contained in answers to Question 35 (DNS) and answers to Question 43 (DNSSEC).

Policy and additional documentation about Internationalized Domain Name (IDN) usage in the TLD is contained in answer to Question 44 (IDN).

The SRS is fully IPv6 compliant: It accepts IPv6 addresses as Glue Records for host objects and is reachable via native IPv6 transport. Additional details about IPv6 support are contained in answer to Question 36 (IPv6).

For reference, the Performance Specifications relevant to the SRS as required by Specification 10 (Registry Performance Specifications) are included in Table Q24-01. As indicated, the SRS performance meets or exceeds all SLA requirements and significant effort has been taken to verify these SLA requirements on a physical installation of the SRS architecture/software. Hence, the performance metrics included in Table Q24-01 are real measurements, rather than theoretical assumptions or estimations.

Note: The performance SLAs have been verified by setting up a prototype system that is functionally and architecturally identical to the registry system, but has limited hardware resources compared to the proposed production architecture. Hence, the performance of the actual production system is expected to exceed the measured performance values on the prototype system indicated in Table Q24-01. Details on the measurements are contained in the responses to Question 33.

Table Q24-01: see attachment

The measurements used to achieve the individual Service Levels are discussed in the following sections:

Performance – Shared Registry Service (EPP)

EPP service availability

The EPP interface of the SRS is provided by two front end server processes on two physically separate machines. Both front ends are accessible via a single IP address, and the load is dynamically shared between these two frontends. In the case that a single frontend system is unresponsive, it is automatically removed from the load balanced group. When a frontend returns to service, it is automatically added back into the load balanced group configuration. In addition, alerts to the NOC are triggered for all such events so that the operations team is notified of error conditions immediately.

For security reasons, access to all EPP interfaces is restricted and is only permitted from network ranges of authorized registrars.

Using this architecture, the SRS for the proposed TLD will exceed ICANN's „EPP service availability" requirement of 98%. A production implementation of the

Registry System (for the ".at" TLD) with similar software & architecture has surpassed 99.6% monthly availability for each month during 2009, 2010 and 2011 (with most months above 99.9% availability).

EPP command performance notes

The performance of the SRS for EPP session, query and transform commands was extensively evaluated. Please refer to the response to question 33 for the measurements and figures indicating the performance under a realistic base load of the proposed registry system. These figures show that the EPP session, query and transform command RTTs clearly meet the 2000ms and 4000ms thresholds, respectively, for at least 90% of the commands.

Additional Performance figures

The response to Question 33 (Database) contains some additional performance figures for the SRS, again gathered on a prototype system.

Network Overview & Number of Servers

The SRS servers make use of the two data center locations "Vienna" and "Salzburg", (distance approximately 300km⁄185miles). The data centers are equipped with multiple, independent upstream connections to the internet (from different service providers) and two Layer 2 crosslinks. The backend registry operator also operates a Local Internet Registry (LIR), allocates IP space from its own address pool, and operates its own Autonomous Systems (ASes). The high-level network structure is shown in Figure Q-24-02, it is further detailed in Figures Q-32-07 and Q-32-08 as part of the answer to Question 32.

As shown, a significant focus of the network design work has been to remove any single point of failure. Also, each server is connected to two access routers, so that an outage of any single network component does not affect server and consequently service availability. More information about the network infrastructure at each individual location is contained in response to Question 35. A complete and detailed overview of machinery in place for this TLD is given in Table Q32-11 of the answer to Question 32.

The server infrastructure of the gTLD's SRS consists of the following set of machines (this list does not include the actual DNS network):

Two physically separate, dedicated servers running SRS frontend instances and the production database, clustered in active-active (Frontends) and active-standby (Database) configuration. Database as well as SRS frontends are segregated from each other via virtualization. In terms of scalability, should the TLD exceed 500,000 registered domains, provisions are in place to add further, dedicated machines as needed.
A total of 6 physical machines provide the additional functions of the gTLD, including zone generation, DNSSEC signing, zone deployment (via Hidden Masters), backup, management, and a test instance of the SRS. The functions on those 6 "infrastructure" machines are shared among up to 4 gTLD installations, and adding more machines is planned depending on growth projections for each individual TLD. The existing infrastructure scales to at least 500,000 domain names per TLD without requiring additional servers. Services on those physical servers are again segregated from each other using virtualization.
Additionally, several other servers are involved in supplementary functionality, such as monitoring, tape backup, logging & reporting services.

All servers used for the operation of the TLD are (and will be) rack mountable, data center grade machines with active maintenance contracts from the supplier.

Interconnectivity with other Registry Services

The SRS, as well as the infrastructure required to perform the other critical Registry Services are installed on servers located in the same data center (under emergency conditions, services may be moved to servers in the backup data center). Therefore, the services are inter-connected using either Local Area Networking (LAN) or redundant private layer 2 links (linking the "Vienna" and "Salzburg" locations). In addition to the redundant layer 2 links, infrastructure is in place to securely tunnel traffic between those two locations over the public internet in the unlikely case that both the private site cross-links fail. From a security perspective, multiple firewall layers are used to filter network traffic between the various network segments, i.e. between the public Internet, perimeter and internal networks.

Zone dissemination or transfer from the hidden primary to the public nameserver network is performed over the public internet however all such communications are cryptographically secured. Both locations have redundant upstream connectivity from independent providers with a minimum total bandwidth of 2x1 Gbit⁄s.

Both networks are also connected to the "Vienna Internet Exchange" (VIX), where peering relationships with many other organizations have been established. This provides an optimal routing path to the Registry Systems and services for those organisations.

In terms of data integrity and consistency the following provisions have been put in place to ensure correct synchronization of Registry systems:

The active and standby database servers are synced in real-time using block device level replication functionality provided by the DRBD technology.
DNS zone servers are synchronized every 15 minutes.
For failover purposes, full machine images or snapshots of all virtual machines are copied to the standby data center once per day (please see the response to Question 37 for details)
Synchronization between SRS and registry helpdesk systems occurs every few minutes.
It is important to note that as WHOIS data is provided directly from the backend registry database there is no need to synchronize WHOIS data.

The synchronization strategy used differs from service to service. For the SRS frontends themselves, an active-active setup with OSPF-based load-balancing is employed. The registry database uses an active-standby setup with real-time synchronization and automatic failover.

Resourcing Plan

It should be noted that the architecture and basic development work for the SRS software has already been completed at the time of this submission (except policy adjustments for the TLD), which reduces the time and number of personnel required to perform the necessary development and maintenance work.

The Registry Backend Operator employs 4 developers (totalling to 3 FTEs) responsible for developing and maintaining the SRS software, for example implementing per-TLD policy customisations. Those developers also work on the development and maintenance of RDDS, and their work is shared amongst the operation of multiple TLDs.

Additionally, 2 system engineers (2 FTEs) are responsible for performing the actual deployment of the SRS for a new TLD including the subsequent hand over of the newly installed systems to the Network Operations team.

A minimum of 8 people are fully trained to perform day-to-day and ongoing maintenance operations of the SRS systems and software.

The required hardware for the SRS is described above and all related costs are bundled with the "Software as a Service" fees that the Registry Operator pays to the Registry Backend Operator. This also includes all resources that are required to operate the hardware for the SRS, such as data center or other infrastructure expenses, maintenance contracts and hardware replacement.

25. Extensible Provisioning Protocol (EPP)

1 Overview

The SRS of this proposed gTLD will use EPP for communication with registrars. The EPP interface is and in full compliance with the following RFCs and, where possible, entirely based on common standards:

- 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 5910 - Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)
- RFC 3915 - Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP)
- RFC 3735 - Guidelines for Extending the Extensible Provisioning Protocol (EPP)

Note that the objective is to base the EPP interface entirely on published RFCs and it is hence not planned to use any proprietary EPP commands. However, it is understood that some functionality required by ICANN cannot be implemented by means of EPP extensions specified in published RFCs. This includes support for:

- Trademark Clearing House: integration in the domain registration process (sunrise and claiming phase)
- IDN: exposure of language tags in the EPP interface
- IDN: selection of variants to be included in the DNS zone

Currently the following documents related to the topics listed above are available:

- draft-tan-epp-launchphase
- draft-obispo-epp-idn
- draft-kong-epp-variants-mapping

The registry backend operator participates in the standardization process and understands that the community is currently working on the respective documents. It is expected that specifications are published and implementable before the registry

goes operational, which allows the registry operator to stick to its strategy of using only IETF RFC specified EPP extensions.

However, if such specifications are not available in a timely manner before the registry intends to go operational, draft specifications that reflect industry and community consensus will be considered instead in order to cover ICANNs functional requirements.

Via EPP, the following objects can be managed by registrars:

- domain objects
- host objects
- contact objects

The following commands are supported by the EPP interface:

- Session Management

** Login
** Logout
** Poll
** Hello

- Domain Commands

** Check domain
** Info domain
** Create domain
** Delete domain
** Renew domain
** Transfer domain
** Update domain (including “restore”)

- Host commands

** Check host
** Info host
** Create host
** Delete host
** Update host

- Contact commands

** Check contact
** Info contact
** Create contact
** Delete contact
** Update contact

According to the definitions in RFC 5730, the registry operator will apply for an EPP repository identifier with the IANA registry (http://www.iana.org/assignments/epp-repository-ids) as follows:

ID: foo, #x0066 #x006F #x006F
Registrant Contact: Registry Name 〈registry-email〉

The only language supported for message elements in EPP is English.

2 Session Management

The transport layer between EPP clients and the SRS EPP interface is protected using TLS with X.509 certificates. The registry will only use strong ciphers such as those required by the EPP RFC and listed below, but reserves the right to modify the list of ciphers depending on cryptographic developments.

- TLS 1.0 [RFC2246]: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS 1.1 [RFC4346]: TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS 1.2 [RFC5246]: TLS_RSA_WITH_AES_128_CBC_SHA

On top of the TLS based identity verification, login to the SRS's EPP interface is protected using two additional authentication factors, with one factor being the IP address of the client and the other factor being the clients' credentials. Failed login attempts are logged and reported. The administration of authorised IP address ranges can be performed by registrars via the Registrar's web interface or by contacting the helpdesk. Passwords can be changed via the EPP login command as described in RFC 5730, Section 2.9.1.1.

EPP sessions will be terminated by the server either after an idle timeout of 20 minutes or after the maximum session length of 24 hours. The registry operator reserves the right to restrict the number of concurrent EPP sessions per registrar (a limit of three sessions is currently defined but this may be amended depending on registry and TLD scaling requirements).

The EPP service also employs infrastructure elements and software measures to perform rate-limiting of EPP sessions (such measures may, for example, be required during landrush phases).

The SRS does not support EPP command pipelining.

3 Object Management

The registry supports the provisioning of contact, host and domain objects as defined in the respective RFCs and according to the lifecycle described in response to question 27.

Registration periods apply for domain objects only (in one year increments). The default initial registration and renewal period is 1 year. The client may choose another period of up to 10 years when issuing the respective request (total registration period of a domain must never exceed 10 years).

Since the registry uses grace periods, the grace period mapping of RFC 3915 is supported by the EPP interface. In particular, a restore command is issued as an extension to the update command, as described in this RFC. Furthermore, the restore report is also delivered to the registry via EPP.

The registry operator reserves the right to perform a garbage collection process on unlinked contact and unlinked external host objects. Internal hosts follow the lifecycle of their superordinate domain and are not subject to garbage collection (for details refer to responses to question 27, 28).

For contact objects, only internationalized postalInfo elements are supported. All child elements as listed in the RFC are supported. Note that since the registry does not support contact transfers, contact authInfo is not used.

For the provisioning of DNSSEC trust chains, the EPP interface supports the extension described in RFC 5910 for accepting DS data (key data interface is not supported). Details on DNSSEC support are contained in response to question 43.

4 Domain Transfer

The domain transfer command has several subcommands. Note that a transfer can only

be requested on domain objects but that the registry system will automatically transfer subordinate host objects when the superordinate domain is transferred. Contact objects are never transferred.

The set of transfer commands consists of the following subcommands: “request”, “approve”, “reject”, “cancel” and “query”. To request a domain transfer, the requestor sends a transfer request with a valid authInfo. The losing registrar is subsequently notified and can either reject or approve this request. In the event that the losing registrar doesn’t explicitly reject or approve the request, the registry will auto-approve the request after 5 calendar days. Before the transfer is approved, auto-approved or rejected, (i.e., the domain is in pendingTransfer state) the requestor may cancel it. A detailed description of the domain transfer lifecycle is contained in response to question 27 (Figure Q27-02).

AuthInfo is required for all domain objects. This information is necessary in order to authenticate a domain transfer process. The registry system requires that the authInfo is at least 8 characters long with a maximum length of 32 characters. Furthermore, at least one alphanumeric character (‘A’ to ‘Z’; both lower and uppercase letters), and at least either one numeric character (‘0’ – ‘9’) or one special character are required for each authInfo.

5 Status values

The domain object supports the following status values (as described in Section 5 of RFC 5731):

- inactive (to indicate that no hosts are associated with the object). This status value is set automatically by the server.
- ok (default status) set automatically by the server. This status value is never combined with any other status values.
- pendingCreate is set by the server to indicated that the domain create command was processed but is subject to offline review.
- pendingTransfer is set by the server when the domain name is subject to a pending transfer
- pendingDelete is set by the server when the domain name is subject to deletion. Note that the registry also supports the RGP grace periods - redemption and pending delete as listed below.
- serverHold/clientHold set when the domain object should not appear in the zone.
- serverUpdateProhibited/clientUpdateProhibited set when the domain name cannot be updated due to server or client policy.
- serverTransferProhibited/clientTransferProhibited set when the domain name cannot be transferred due to server or client policy.
- serverDeleteProhibited/clientDeleteProhibited set when the domain name cannot be deleted due to server policy or client provisions.
- serverRenewProhibited/clientRenewProhibited set when the domain name is not eligible for renewal.

Each domain object will always have at least one associated status value. Additionally, domain objects support the following status values related to the grace period mapping as per RFC 3915, Section 3.1:

- autoRenewPeriod
- renewPeriod
- transferPeriod
- redemptionPeriod
- pendingRestore

- pendingDelete

The contact object supports the following status values (as described in Section 2.2 of RFC 5733):

- linked (when the object is used in at least one domain name object)
- ok (default status)
- serverUpdateProhibited/clientUpdateProhibited (for server or client policy reasons, modifications to the object are not allowed)
- serverDeleteProhibited/clientDeleteProhibited (for server or client policy reasons removal of the object from the registry is not allowed)

Each contact object will always have at least one associated status value.

The host object supports the following status values (as described in Section 2.3 of RFC 5732):

- linked: Set by the registry when a host is referenced by at least one domain
- ok (default status)
- pendingTransfer: Set on internal host objects when the superordinate domain is pending transfer.
- serverDeleteProhibited/clientDeleteProhibited (for server or client policy reasons removal of the object from the registry is not allowed)
- serverUpdateProhibited/clientUpdateProhibited (for server or client policy reasons, modifications to the object are not allowed)

Each host object will always have at least one associated status value.

6 EPP Server Implementation

The EPP server implementation is based on the Apache HTTP server, with the HTTP protocol handler replaced with a custom, Perl-based EPP handler. This allows for the reuse of Apache's session management, logging and resource allocation functionality. EPP systems based on this software have been deployed in production since 2004. The software has been continuously developed, in order to accommodate policy changes and scalability requirements.

The EPP software variant for the proposed TLD is already available and has already been deployed on prototype systems (with the exception of functionality where specifications are unclear at the time of this writing, i.e. Trademark Clearing House integration).

Since no proprietary extensions are planned, no EPP templates and no EPP extension schemas are provided in response to this question. Schemas and examples of the commands supported are included in the respective RFCs.

7 Resource Planning

The technical resources required for the operation of the EPP server (as part of the SRS) are described in response to questions 32 and 24. For EPP development and evaluation of related issues, the Registry Back-End Operator has a highly skilled research & development team of 5 persons, of which 3 people are intimately familiar with the details of the EPP protocol. They also monitor and contribute to the discussions within the IETF regarding future developments of EPP ("provreg" mailing list).

All technical staff are trained on the day-to-day operations of the EPP service. The

helpdesk team is trained and experienced in troubleshooting EPP support problems with Registrars, and can escalate to the EPP experts or even core developers in case of more complex problems.

26. Whois

Overview

As detailed in Specification 4 "Specification for Registration Data Publication Services" (RDPS), the Registry Operator will operate a fully compliant "Registration Data Directory Service" (RDDS), will provide "Zone File Access" as required and will grant ICANN the required "Bulk Registration Data Access". These services will fulfil the requirements stated in the respective specification, and will also meet or exceed the respective RDDS SLAs as required in Specification 10.

In addition to the requisite WHOIS service, a lightweight variant of the RDDS, a so-called "Domain Availability Interface", based on the "finger" protocol, will be provided. This service will supplement the WHOIS service, and exposes a very limited subset of the information already available via the RDDS, namely, whether or not a certain domain name is available for registration.

Registration Data Directory Services

A WHOIS service will be available via port 43 in compliance with RFC 3912. Additionally a web-based directory service, to be made available at "whois.nic.GMBH will provide a free, publicly accessible, query-based interface which will provide information regarding "Domain Name", "Registrar" and "Nameserver" objects. The data format used for those objects is specified below. It is understood that ICANN reserves the right to require alternative formats and protocols, and upon such specification, such changes will be implemented as soon as reasonably practicable.

Specifically, the WHOIS service fulfils the following requirements:

The server is fully compliant with RFC 3912
Free public query-based access is provided
The services runs on "whois.nic.GMBH" on TCP port 43
Data objects represented by key/value pairs, with multiple key/value pairs with the same key in case of fields with more than one value
Additionally, web-based access on "whois.nic.GMBH is provided
In order to prevent abuse, highly configurable volume access limitations are deployed
The architecture is robust, implements a number of failsafe mechanisms and is in compliance with the RDDS SLA's outlined in Specification 10.

Architecture

The technical architecture of the WHOIS system (servers, switches, routers, etc.) is depicted in Figure Q26-02, and employs the following components:

Connectivity to the internet is handled via the two redundant access routers of the registry system. Each server is connected to each of the two routers, with one connection serving as an active path, and the second path (to the other router)

serving as a failover path in case of failure of the first.
Two virtual machines on physically separate hardware run the frontend Whois/Finger/HTTP daemons.
The WHOIS service on each server operates as part of an active-active cluster. Both servers announce their respective service addresses to the routers via OSPF with the routers distributing traffic between the two frontends by means of OSPF load sharing logic.
Both active instances are connected to the active registry database using persistent database connections to reduce session handling overhead. The frontend servers switch automatically to the registry standby database in the event of a database failover.
In the case where one of the frontend servers fails, the OSPF announcement for that server automatically ceases and traffic is redirected to the remaining active node within a few seconds.
Access is restricted to TCP port 43 (for Whois), TCP port 79 (for Finger) and TCP port 80 (HTTP) using firewall access lists on the routers.
The codebase for the WHOIS and Finger servers was developed in-house using the "C" programming language and is based on state-of-the art design concepts to ensure a robust and stable operation. This software has been actively developed for a number of years and is currently in production at the ".at" and ".no" TLD registries.
The software is also highly configurable, allowing query limits to be set based on source IP address/blocks for both IPv6 and IPv4 addressing formats. It also allows for fine grained control of specific rate-limits on a per network block basis.
The software actively generates access and service statistics for monitoring and management purposes.
The RDDS uses the "live" registry database and as a result updates to the registry database are reflected in real-time to the WHOIS server. However, in the event that the WHOIS load starts to impact the performance of the Registry database, provisions are in place to move the WHOIS server to an alternate read-only replica of the "live" database if necessary.

Access Limitations and Access Restrictions

Access control lists (ACLs) protect the RDDS service hosts against unwanted access but grant public access to the defined services (WHOIS, finger, HTTP).

In addition to this general protection of the service infrastructure, the RDDS must also make provision to address the following scenarios:

Bulk requests from public unknown sources (e.g. to grab data)
High speed / high volume requests from known source addresses (e.g. from registrars)

In order to handle the above scenarios the WHOIS software supports the following configurable service policies:

The number of allowed requests (within a specific time frame) on a per IP address (or per IP subnet) basis, for either IPv4 or IPv6 and with support for a "most specific" matching rule of those entries. This provides the ability to set different limitations for different user groups / network ranges. Violations of those limits are included in the daily WHOIS service reports sent to the operations team.

WHOIS Input Format

The data format complies with the requirements of Specification 4 of the "new gTLD agreement". The definitions below apply to the command line WHOIS interface (port 43) as well as the web interface:

Queries can be issued for domain name, registrar and nameserver objects
Queries that include the argument "registrar" trigger a search for registrar data objects. If the argument is "nameserver", a search for nameserver objects is actioned, while queries without any such prefix trigger a search for a domain or nameserver.
Wildcard searches and substring searches are not supported.
Using the option "-C" ("charset") as part of the command line WHOIS query specifies a character encoding for the protocol. This setting applies to the both the input and output character encoding, and supports the following values: "US-ASCII", "ISO-8859-1" and "UTF-8". The default character set is "UTF-8". On the web interface the character encoding will always be set to UTF-8 with modification of this option not available.
In the case of IDNs, the search string must be in the A-Label format of the domain or nameserver. Searches based on the U-Label format are not supported.

Example queries (including the command line "whois" client itself):

Domain name data: whois -h whois.nic.GMBH example.GMBH
Domain name data (with character set parameter): whois -h whois.nic.GMBH -- -C us-ascii example.GMBH
Registrar data: whois -h whois.nic.GMBH "registrar Example Company"
Nameserver data by name: whois -h whois.nic.GMBH ns1.example.GMBH
Nameserver data by IP address: whois -h whois.nic.GMBH "nameserver 10.0.0.10"

Note: In the case where a host is registered for the origin of a delegated domain, i.e. both domain "example.GMBH" and nameserver "example.GMBH" exist, the query will match and return both the domain name and nameserver data objects.

WHOIS Output Format

The output format of the WHOIS server follows that outlined in Specification 4 of the "new gTLD agreement":

Domain Name Data:

Domain ID: D1234567-TLD
Domain Name: EXAMPLE.GMBH
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Registry Expiry Date: 2010-10-08T00:44:59Z
Sponsoring Registrar: EXAMPLE REGISTRAR LLC
Sponsoring Registrar IANA ID: 5555555
Domain Status: clientDeleteProhibited
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Domain Status: serverUpdateProhibited
Registrant ID: 5372808-GTLD
Registrant Name: EXAMPLE REGISTRANT
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP
Registrant Postal Code: A1A1A1
Registrant Country: EX
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234
Registrant Fax: +1.5555551213

```
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.GMBH
Admin ID: 5372809-GTLD
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: EX
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext:
Admin Email: EMAIL@EXAMPLE.GMBH
Tech ID: 5372811-GTLD
Tech Name: EXAMPLE REGISTRAR TECHNICAL
Tech Organization: EXAMPLE REGISTRAR LLC
Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: EX
Tech Phone: +1.1235551234
Tech Phone Ext: 1234
Tech Fax: +1.5555551213
Tech Fax Ext: 93
Tech Email: EMAIL@EXAMPLE.GMBH
Name Server: NS01.EXAMPLEREGISTRAR.GMBH
Name Server: NS02.EXAMPLEREGISTRAR.GMBH
DNSSEC: Signed
DS Key Tag 1: 54135
Algorithm 1: 5
Digest Type 1: 1
Digest 1: 〈DIGEST〉
DS Key Tag 2: 54135
Algorithm 2: 5
Digest Type 2: 2
Digest 2: 〈DIGEST〉

% Copyright (c) 20XX by NIC.GMBH
% Restricted rights.
% Response generated on: 2011-10-13 11:11:25 UTC
```

Note that the “Domain Name” field will always contain the A-Label format of the domain. In cases where an IDN response is returned (and an appropriate character encoding was requested), the response will contain an additional field, the so-called “Domain U-Label”, containing the U-Label format of the respective Domain, for example:

```
Domain U-Label: exämple.GMBH
```

In the case where data for an unsigned domain is returned, the “DNSSEC” field will contain the value “unsigned” and the other DNSSEC-related fields will be excluded from the response.

```
Registrar Data:
```

```
Registrar Name: Example Registrar, Inc.
Street: 1234 Admiralty Way
City: Marina del Rey
State/Province: CA
Postal Code: 90292
Country: US
Phone Number: +1.3105551212
Fax Number: +1.3105551213
Email: registrar@example.GMBH
Registrar IANA ID: 55566677

% Copyright (c) 20XX by NIC.GMBH
% Restricted rights.
% Response generated on: 2011-10-13 11:11:25 UTC

Nameserver Data:

Server Name: NS1.EXAMPLE.GMBH
IP Address: 192.0.2.123
IP Address: 2001:0DB8::1
Registrar: Example Registrar, Inc.
Registrar IANA ID: 55566677

% Copyright (c) 20XX by NIC.GMBH
% Restricted rights.
% Response generated on: 2011-10-13 11:11:25 UTC
```

Web-based RDDS

In addition to the command line based WHOIS service described above, the Registry Operator will, in line with requirements, provide a web-based WHOIS interface. The web-based interface supports the following classes of users in accordance with stated policies:

The general public (“anonymous access”):
Anonymous users can retrieve a limited amount of responses from the web based interface. To avoid unwanted bulk access and to prevent users from data harvesting the following access restrictions are deployed:
Client limits per day to be set based on source IPv4 and IPv6 addresses or blocks.
CAPTCHAs as a challenge-response test to ensure that the response is generated by a human being.
Registrars and other authenticated users:
Registrars and other approved users are issued with an authentication token that allows them to retrieve a greater number of WHOIS records via the web interface. Users qualifying in principal could for example include ICANN staff, URS or UDRP providers, and will be approved case by case by the registry.

All transactions on the web-based WHOIS are also logged and daily usage reports are sent to operations staff. The web-based WHOIS supports the same object types and query formats as the command line interface above, with the exception of the „-C“ (character set) switch. The contents of a response from the web-based WHOIS service are also identical to the command line service, but may be reformatted and styled using HTML/CSS to aid presentation and display.

Searchable WHOIS

Searchable WHOIS functionality is not provided. This is to prevent bulk data harvesting and further data merging using extensive request combinations and Boolean search techniques. This is done intentionally to comply with data protection laws and privacy obligations.

Any request from legal institutions and law enforcement agencies for information outside of that supplied by any of the WHOIS services is dealt with directly by the legal department of the registry.

As a result there is no future intention to offer a broad search functionality, this applies to both the WHOIS protocol interface (port 43) and the web-based WHOIS interface

Lightweight RDDS Access ("Finger")

In addition to the required WHOIS interface a lightweight domain availability interface is supported. This interface is based on the "Finger" protocol, specified in RFC 1288, and exposes a very limited subset of data (already available in WHOIS), namely whether or not a certain domain name is available for registration. It provides faster response times than the standard WHOIS interface and places less load on the registry systems. The service will be operated accordingly:

Lightweight access based on the "finger" protocol according to RFC 1288
Lightweight access runs on finger.nic.GMBH on port 79
No exposure of any information additional to that already available via the WHOIS RDDS
Query format (command line example): "finger example.GMBH@finger.nic.GMBH"
Response format (example): "example.GMBH IS NOT available"

IPv6 Support

All RDDS services (WHOIS, web-based WHOIS, Finger and bulk data access) fully support IPv6. In summary there is no difference in service quality levels or service responses between IPv4 and IPv6 for these services.

A detailed description of IPv6 support can be found in response to Question 36.

Service Level Compliance

The RDDS service complies with the SLA requirements (as defined in Specification 10) as follows:
Table Q26-01: please see attachment

RDDS Availability

The redundant and resilient architecture of the WHOIS system is described above, and is served by architecture as outlined in response to question 32. It is designed, at a minimum, to meet the required availability levels of 98%. It is understood that a reliable RDDS system is vitally important for TLD operations.

RDDS query RTT

The internal response time of the WHOIS system is significantly below the RDDS query RTT limit of 2000 ms so that it can be expected that for 95% of the queries this SLA requirement will be met. On test installations of the service, the query RTT is less than 500 ms, even in the event of a significant number of concurrent connections.

RDDS update time

Since the WHOIS system queries the "live" registry database, there is no update delay and hence the RDDS update time of 60 minutes for 95% of the updates can be assured.

Zone File Access

In accordance with Section 2 of Specification 4 of the Agreement („Zone File Access"), the Registry Operator will enter into an agreement with any internet user to provide access to download the zone file data and will cooperate as required with Centralized Zone Data Access (CZDA) Providers. This will be facilitated as follows:

A dedicated FTP server will be set up for access to the zone file data. The name of that server will be: berlin.zda.icann.org (pending allocation of that hostname by ICANN zone administrators). The zone file and associated checksum files will be available for download for the previous 3 days. Files will be generated once a day and named according to Section 2.1.3 of the Agreement.
The file format follows exactly the specification which is based on the Master Zone File format defined in RFC 1035, according to Section 2.1.4 of the agreement.
A specific user ID and password has to be assigned for each user to restrict access to accredited users and to prevent unauthorized access. This user has to access the server with this specific user ID to be able to transfer data.
Access will be free of charge but limited to one download per day.
All logins and data transfers are logged, monitored and reported. Access statistics will be available to the registry operator as well as to others if required.

The Registry Operator will also cooperate with ICANN and CZDA Providers as required in Section 2.2 of the agreement. Additional access is granted to ICANN itself (or its designee) and any designated Emergency Operator if required.

Bulk Registration Data Access

As an operator of a Thick Registry, the Registry Operator will operate in compliance with Section 3.2 of Specification 4 of the „new gTLD Agreement" („Exceptional Access to Thick Registration Data") as well as in compliance with Section 3.1 of Specification 4 („Periodic Access to Thin Registration Data"), and will provide ICANN with the required data in the required format.

The data will be provided in conformance with Specification 2 („Escrow") of the Agreement, as required.

Resources

Regarding development of the RDDS interfaces, it shall be noted that most of the work is already complete at the time of this writing (eg. WHOIS and finger daemon are fully deployed and operational for other TLDs). Therefore, only minimal development work is required, and hence within TLD-Box's development team, only a half FTE is necessary (and planned for) for the continuous adaption and maintenance of the RDDS software itself.

For the actual operation of the RDDS interfaces, all technical operations staff members are trained on the various infrastructure and software components of the system, and manpower resources are accounted for in the general Network Operations Center budget.

The research & development team of the Registry Backend Operator is aware of ICANN's

SSAC work regarding WHOIS (eg. http://www.icann.org/en/committees/security/sac051.pdf), and also participates in the IETF's proposed "WEIRDS" working group, in order to stay up-to-date with developments in the fields of domain data related publication services.

The RDDS makes use of virtual machines on the hardware provisioned for the TLD (and described in responses to Question 32 and 24). Therefore, no additional hardware resources are needed, however, the required bandwith in order to provide the RDDS services are accounted for in the general network topology of the Registry System.

27. Registration Life Cycle

Introduction

The domain registration lifecycle of .GMBH follows ICANNs "Life Cycle of a Typical gTLD Domain Name" (http://www.icann.org/en/registrars/gtld-lifecycle.htm) and adds a PENDING CREATE state (pendingCreate state as described in RFC 5731) to allow for manual review of the application. By following this standard model lifecycle, Registrars have only minimal effort in order to become familiar with the registration procedures under the proposed TLD. Figure Q27-01 shows the lifecycle of a domain with the various states. The description below lists EPP status values, DNS status, and typical allowed transactions for each of the domain states. It also describes whether Whois information is available and what information is provided in a finger request (note: for reasons of clarity the transfer process is shown in a separate figure).

Since the registry system supports the Redemption Grace Period (RGP) extensions as specified in RFC 3915, the domain states 'REDEMPTION' and 'PENDING DELETE' refer to the respective RGP states.

Typical Lifecycle of a Registration

A typical domain lifecycle is initiated by a create domain EPP command for an AVAILABLE name. The domain is now in a 'PENDING CREATE' state allowing for manual review of the application. Response to question 20e contains information about Eligibility, Name Selection, Content/Use and Enforcement of the community policies. Whilst in this 'PENDING CREATE' state, domain information cannot be updated. When the application is rejected during manual review, the domain enters the 'PENDING DELETE' state. In case the application is approved, the domain enters the 'REGISTERED' state. Whilst in this state the information associated with a domain may be updated by the respective registrar (using the update domain EPP command). A domain may also be transferred to another registrar (domain transfer, see detailed state diagram below). A domain is always registered for a specific period (maximum 10 years). At any time Registrars can manually renew domains (given that the maximum registration period is not exceeded). The registry system is also supporting an auto-renew option. The auto-renew option can be deactivated on the request of a Registrar (on a per-Registrar basis), but is enabled by default to ensure that domains do not expire unintentionally.

When a domain is deleted by either the 'delete domain' command, or alternatively expires (not manually renewed and auto-renew is disabled for the registrar), the domain first enters the 'REDEMPTION' state. Whilst in this state, a registrar is allowed to restore domains for the respective domain holder in case the non-renewal

was unintentional. When the domain is successfully restored while in the REDEMPTION state (a restore report via EPP is required), the domain enters the 'REGISTERED' state again. Domains which are not restored after 30 days in the 'REDEMPTION' state enter the 'PENDING DELETE' state. Whilst in this state, a domain cannot be restored and will become AVAILABLE for re-registration after a period of 5 days.

Furthermore, additional EPP status values set on a domain may affect the allowed transactions (operations), e.g. status values of serverUpdateProhibited or clientUpdateProhibited, serverTransferProhibited or clientTransferProhibited, serverDeleteProhibited or clientDeleteProhibited and serverRenewProhibited or clientRenewProhibited will prohibit the respective transaction. Such server states are for example used when a domain is LOCKED.

To discourage and to address problems with abusive registrations, the proposed registry will follow policies described in response to question 28.

For domains under dispute, the registry will use the LOCKED status, and will also set appropriate status values on the associated host and contact objects, as required by the specific dispute scenario (e.g. URS). Note that the LOCKED status may also be used to enforce the community policies, as outlined in response to question 20e.

Domain States and Properties

This section describes the individual Domain States, as outlined in figure Q27-01. For each of these states, it is described what the trigger points to reach the status are, whether the domain is included in DNS, which transactions are allowed on the object, whether WHOIS information is available, and what the boolean response for the lightweight RDDS interface (finger) is. Furthermore the EPP (base and RGP) status values set on the domain are listed.

Note that in addition to the commands listed below "check domain" is always possible and the commands "info domain" and "transfer query" are always allowed on existing domain objects, regardless of their status.

Also note that in addition to the EPP status values listed below, the value "inactive" is set for domains without associated host objects.

AVAILABLE:

Trigger points: Initial status of "new" domains, final release of a "PENDING DELETE" domain
in DNS: No
Allowed Transactions: create domain
in WHOIS: No
Finger results: "available"
EPP status values: n⁄a

PENDING CREATE:

Trigger points: "create domain" command
in DNS: No
Allowed Transactions: None
in WHOIS: Yes
Finger results: "unavailable"
EPP status values: pendingCreate, serverTransferProhibited, serverUpdateProhibited, serverRenewProhibited, serverDeleteProhibited, serverHold

REGISTERED:

Trigger points: Approval of domain, Restore Report received, disputes resolved
in DNS: Yes*
Allowed Transactions: update domain, transfer domain (request), delete domain, renew domain
in WHOIS: Yes
Finger results: "unavailable"
EPP status values: serverTransferProhibited (during first 60 days), ok (after the first 60 days if not inactive and no other status value is set)

REDEMPTION:

Trigger points: "delete domain" command, domain expiration, disputes resolved, restore report not received.
in DNS: No
Allowed transactions: restore domain
in WHOIS: Yes
Finger result: "unavailable"
EPP Status values: pendingDelete, serverUpdateProhibited, serverHold, serverTransferProhibited, serverRenewProhibited, rgp:redemptionPeriod

PENDING DELETE:

Trigger points: domain not restored, delete locked domain, reject domain
in DNS: no
Allowed Transactions: none
in WHOIS: Yes
Finger result: "unavailable"
EPP Status values: pendingDelete, serverUpdateProhibited, serverHold, serverTransferProhibited, serverRenewProhibited, rgp:pendingDelete

PENDING RESTORE:

Trigger points: "restore domain" command, dispute resolved
in DNS: Yes*
Allowed transactions: update domain (including delivery of the restore report), delete domain, renew domain.
in WHOIS: Yes
Finger result: "unavailable"
EPP status values: pendingDelete, serverTransferProhibited, rgp:pendingRestore

LOCKED:

Trigger points: Opening of a dispute over the domain name
in DNS: Yes**
Allowed transactions: renew domain
in WHOIS: Yes
Finger result: "unavailable"
EPP status values: serverUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, (serverHold**)

*Note: Domain is only included in the DNS if the domain object is linked to host object(s), and neither serverHold nor clientHold are set on the domain object.

**Note: Depending on the individual dispute case, the Registry may be instructed to

set the serverHold flag on the domain, and subsequently, the name would be excluded from the DNS.

The EPP status values pendingRenew and pendingUpdate are never set on domain objects since there is no human review or third-party action necessary to complete these actions. Furthermore, the RGP status addPeriod is never set for domains since the add grace period does not apply for the proposed TLD.

Transfers

The transfer lifecycle of the proposed gTLDs complies with ICANNs "Policy on Transfer of Registrations between Registrars" (http://www.icann.org/en/transfers/policy-12jul04.htm), specifically to its Section 6 (Registry Requirements). The lifecycle is illustrated in Figure Q27-02.

A transfer request must have valid 'authInfo' in order to be successful. Note that only one transfer request for a domain can be pending at any one time. Transfer requests for a domain name object that is already in the "pending Transfer" state are hence rejected.

Additionally, only domains that have been registered for more than 60 days (counted from the date of the initial registration) can be transferred.

Pending transfers can be either approved or rejected by the currently sponsoring Registrar. After a period of 5 days, any un-actioned requests are auto-approved by the Registry. Pending transfers may also be cancelled by the requesting registrar.

In the "pending Transfer" state, the following transactions on a domain name are not allowed:

transfer (op=request)
delete

(update, renew, and all other transfer sub-commands are allowed). All EPP commands are specified in RFC 5731.

A successful transfer extends the validity period of the transferred domain. The default validity period extension is 1 year but clients may request longer periods in the "transfer op=request" command), between one and 10 years (whole years only; as always, the maximum registration period is capped at 10 years).

Host Objects

The lifecycle of host objects is contained in the response to this question because internal host objects can be affected by transactions on their respective superordinate domain (parent domain). They "follow" the status of their parent domain in order to avoid issues with stale glue records.

Figure Q27-03 shows the lifecycle of internal host objects (comprised of a domain name in the .TLD namespace), and Figure Q27-04 shows the simpler lifecycle of an external host object (comprised of a domain name outside the of .TLD namespace). In Figure Q27-03, bold solid lines indicate states and transactions created by transactions on the host object itself, while dotted lines indicate effects on the internal host object that are created indirectly by transactions/states on the superordinate domain of the host object.

Internal host objects can only be created when the superordinate domain exists.

The description of the individual states of the Host objects is as follows:

AVAILABLE: The host object does not exist in the Registry, and can be created using the "create host" EPP command.
REGISTERED: The host object exists, and can be used in domain names in order to refer to the domain name's nameserver.

Internal hosts additionally follow the states of their respective superordinate domain as follows (Status values in the list below refer to the status of that domain):

REGISTERED (PENDING TRANSFER): The host object will be transferred together with the superordinate domain (in case the transfer is completed successfully).
REDEMPTION: For the redemption period of the superordinate domain, the host object glue will continue to be included in the TLD, even if the superordinate domain is not included in the zone anymore.
PENDING DELETE: The glue record will not be included in the DNS anymore. On final deletion of the host object, all references to this host object will be removed too.

More information regarding this process in order to avoid stale glue records is included in response to Question 28 (Abuse Prevention and Mitigation).

Grace Periods
The following grace periods are supported for domains:

transfer grace period: the transfer grace period is currently 5 calendar days following a successfully completed domain transfer. If a domain is deleted in this timeframe, the sponsoring registrar is credited for the amount billed during the domain transfer. The transfer grace period is terminated when a restore, renew or subsequent domain transfer is performed.
renew grace period: after each renew command, a 5 calendar day long renew grace period starts. When the domain is deleted in this timeframe, the registrar is credited for the corresponding fee and the domain enters REDEMPTION. A deletion, restoration or approved transfer of a domain immediately ends the renew grace period.
auto-renew grace period: every auto-renew is followed by an auto-renew grace period (45 calendar days). If a domain is deleted or transferred within this period the fee for the renewal is refunded to the registrar. However, when a renew command is performed there is no grace period credit any more.

The registry system supports the following pending periods in which certain operations are not allowed:
Redemption Grace Period: consisting of
** Redemption Period: Whilst in this 30 day period, a domain can be restored after a deletion action.
** Pending Restore: in order to successfully restore a domain in the redemption period, a restore report is required. This report has to be submitted within 7 days of this pending restore period. If no restore report is submitted, a new 30 day long redemption period begins.
** Pending Delete: If a domain is deleted and not restored, it is placed into the pending delete period following the redemption period. After 5 days in this period, the domain is finally available for re-registration.
Pending Transfer Period: lasts for a maximum of 5 days after the initial transfer request command. The losing registrar has 5 days to approve or reject the request. The requestor may also cancel the transfer within this period. If no action is taken by the losing or gaining registrar, the registry auto-approves the transfer.

Pending Create: The create domain command was received and the domain is going to be reviewed offline. The Registrar is notified about the outcome (either approved, then the domain enters the 'REGISTERED' sate or rejected, then the domains enters 'PENDING DELETE' state) by queuing a service message.

This registration lifecycle matches the business model of the proposed gTLD. The proposed registry software fully supports this lifecycle and the technical resources needed to run a registry based on the lifecycle as described are readily available.

Resourcing

Three staff members of TLD-Box (the Registry Back-End Operator of the proposed gTLD) are experts in domain name life cycle, and have designed life cycles for the ".at", ".bh" TLD, as well as consulted some other TLDs on their domain life cycle.

All other technical staff members as well as support staff are trained on the operational aspects of the Domain Name Lifecycle.

There are only minor staff and/or infrastructure resources needed for the day to day operations in relation to the domain lifecycle itself (since once developed, the resources to run the lifecycle come from resources operating the EPP servers). In terms of ongoing maintenance, it is expected that about 5 person days per year are required in order to clarify details, corner cases and relations to other business processes of the registry. Those 5 person days are budgeted for in the general maintenance time & resource budget of the registry.

28. Abuse Prevention and Mitigation

1 Overview

Abusive activities during the operation of a gTLD registry system can be categorized as follows:

• Abusive registrations of names under a gTLD.
• Abusive use of a domain name under that gTLD („Malicious Use")
• Abuse of the registration processes, the technical interfaces, infrastructure of the Registry systems and the DNS network itself.

With respect to the first (and also parts of the second) category, ICANN's "RAP" WG (Registration Abuse Policies Working Group) has produced an illustrative categorization of known abuses in their "Registration Abuse Policies Working Group Final Report" (http://gnso.icann.org/issues/rap/rap-wg-final-report-29may10-en.pdf, dated 29 May 2010). The anti-abuse measures of the proposed gTLD registry largely follow the RAPWG's recommendations for the individual abuse scenarios. More details on the individual countermeasures are included below.

Furthermore, the proposed registry also takes into consideration the ICANN Security and Stability Advisory Committee's document "SAC 048" ("SSAC Comment on Orphan Glue Records in the Draft Applicant Guidebook") as well as "SAC 023" ("Is the WHOIS Service a Source for email Addresses for Spammers?").

2 General Provisions against Abuse under gTLD

2.1 Legal Safeguards

To meet the requirements of ICANN to a community-based designation of the application, the registrant has to fulfill certain requirements in terms of eligibility and the .GMBH designation.

This designation of .GMBH to the .GMBH Community will be enforced by specific language in the Registry-Registrar-Agreement that holds gTLD registrars responsible to include the restrictions as outlined above in respective agreements with their gTLD registrants.

The .GMBH Registry will, from time to time in its sole discretion or upon evidence or advice manually conduct continuing or recurring audits of domain names registered to ensure continued compliance with these requirements. Failure to comply will result in a notice providing 20-days to comply. Non-compliance following such a notice period may result in take-down of the relevant domain name, at the discretion of the Registry.

2.2 WHOIS Accuracy Measures

In parallel to auditing domain names for compliance wuth the eligibility requirements as outlined in 2.1, any such domain names will simultaneously also be checked for the accuracy of their WHOIS data.

3 Abuse Contact and Abuse Handling Provisions

The .GMBH registry operator will establish and publish a single abuse point of contact on its website. This contact is responsible for addressing matters requiring expedited attention and for providing a timely response to abuse complaints concerning all names registered in the .GMBH, through all registrars of record, including those involving a reseller.

The contact information for the abuse contact will consist of:

• an email address
• a phone number
• the postal address of the abuse contact (offices of the registry operator)

Communication submitted to the abuse contact will be handled as follows:

• review inbound communication for new abuse requests and⁄or ongoing cases
• treat remaining communication such as spam or non-applicable requests (e.g. for domains in other TLDs) appropriately, e.g. by discarding or rejecting it
• identify registrar of respective domain
• provide a preliminary response to the request’s originator
• approach registrar of record with the abuse case
• track abuse handling measures of registrar
• respond to originator with the outcome

Confirming receipt of communication and forwarding third-party communication is regularly handled during business hours, but after 24 hours at the latest. The initial time frame for the registrar of record to complete its abuse handling measures is 72 hours. Exceptionally and only at a registrar’s request this can be extended by another 24 hours. Details will be specified in the Registrar Accreditation Agreement.

4 Potential Registration Abuse Categories and Countermeasures

As outlined above ICANN's RAPWG has identified a number of potential abuse categories (see chapter 5 of their document). These correspond to the first bullet point of the potential abuses of a Registry as listed in section 1 above ("Abusive Registrations"). The proposed registry system addresses these individual categories as follows:

4.1 Cybersquatting

Abuses from cybersquatting cases in the proposed .GMBH will be addressed by using ICANN's existing and well know Uniform Dispute Resolution Process ("UDRP"). However, registry staff will also closely follow developments regarding Rights Protection Mechanisms within ICANN and will investigate potential paths towards adoption of such processes once they are clearly defined for the .GMBH registry space.

4.2 Front-Running

Even though the RAPWG does not recommend any specific action regarding this issue, the proposed registry will a) treat all logfiles and any other information that reflects user interests in a particular domain name as confidential. Such data and log information will only be available to staff with actual operational requirements to access those files, and b) will include a respective provision in the gTLD's registrar accreditation agreement.

4.3 Gripe Sites; Deceptive and Offensive Domain Names

The gTLD registry will – in accordance with its obligations to the .GMBH Community – develop best practices to restrict the registration of offensive strings. Additionally, it is believed that the existing UDRP, in addition to court decisions (which the registry will obviously be bound by) provides sufficient, independent action against such potentially abusive names.

4.4 Fake Renewal Notices

The registry will not, in line with the RAPWG's recommendations, implement any specific countermeasure within its registry systems and services. As the registry is required to provide accurate and complete WHOIS information for all domain names (which is believed to be the information source for such notices) it is not feasible to implement such measures at this level. It is understood that ICANN continually monitors this issue and will take necessary countermeasures against registrars associated with such practices.

The registry will, however, post warnings on their website about any clearly fraudulent (and clearly illegal) renewal and expiration notices of which its staff becomes aware and will take legal measures against registrars performing such illegal, fraudulent acts.

4.5 Name Spinning

This is considered to be a practice employed mainly by registrars in a legitimate way to offer users more choice and⁄or alternatives should their desired name already be taken. As such, it is believed that it is within the registrar's responsibility to use those techniques in a considered manner. In reality it is not possible for the registry to differentiate between a legitimate domain name request, say one manually entered by a user, and a domain name request that was "spun" by the registrar.

In the event that such name spinning practices could lead to trademark infringements on a domain name, the UDRP allows for appropriate action to be taken against the holder of such a name. This follows the RAPWG's recommendation.

4.6 Pay-Per-Click

In agreement with the RAPWG's position, this is considered to be an indirect and purely web related issue that does not have a direct relationship to the registration of domain names. In most cases, pay-per-click is a legitimate revenue source for domain name owners and web site operators. Any potential misuse of such practices must be out of scope for the Registry and again any trademark cases are expected to be brought using the UDRP.

4.7 Traffic Diversion

In accordance with the RAPWG's position, this is again a web related issue and no specific countermeasures have been implemented within the registry's operations.

4.8 Domain Kiting / Tasting

In order to prevent mass domain kiting / tasting (as it was observable in gTLD and ccTLD registries), the Registry will implement the "Add Grace Period Limits Policy" (http://www.icann.org/en/tlds/agp-policy-17dec08-en.htm), which efficiently removes the financial advantage of domain kiting / tasting and hence significantly reduces the volume of such registrations. All registrars will obviously be treated identically in this respect with no exemptions from that policy.

5 Abusive Use of a Domain Name

Corresponding to the second bullet in the list above ("Abusive Use"), the RAPWG has also provided an analysis in their Final Report. The Registry will apply a policy as outlined below:

5.1 Abuse Policy for gTLD

The intention of .GMBH's Abuse Policy is to take action against the use of a domain name in conjunction with illegal, malicious, fraudulent or otherwise harmful activities on the Internet. Such activities comprise:

• Spam: Spam is generally defined as bulk unsolicited e-mail, but can also occur in instant messaging or mobile environments. Spam may be sent from domains, and spam is used to advertise Web sites.
• Phishing: Phishing is a website fraudulently presenting itself as a trusted site – often as a bank website – in order to deceive Internet users into divulging sensitive information (e.g. online banking credentials, email passwords).
• Pharming: Pharming is a redirection of Internet users to fraudulent websites, predominantly achieved by techniques like DNS hijacking or poisoning.
• Deliberate distribution of Malware: Malware is a piece of software that without the users' consent infiltrates their system to harm it or e.g. use it for bot net activities. Examples are viruses, worms, Trojans or key logger.
• Malicious Fast-Flux hosting: Malicious Fast-Flux hosting is a DNS-based component of bot net activities in particular, to e.g. disguise the location on the Internet of these activities and to harden them against discovery and defense.

Any incoming communication about a potential abuse will be handled according to section 3 of the response to this question. Experts at the Registry Operator will then asses whether there is indeed an abuse at hand in conjunction with a gTLD

domain name and of what kind it is. Subsequently the best method to tackle the issue will be derived from the initial assessment.

The main differences are a) whether the domain name has specifically been registered to commit the malicious activity or if this activity exploits a legitimate use of the domain name and its registrant is fully unaware of it, i.e. its website has been hacked – and b) whether there is a need for immediate action (domain is locked and removed from the delegation) or not (domain is locked only).

5.2 Handling of URS Requests

The registry Operator's handling of Uniform Rapid Suspension (URS) requests is specified in detail in section 1.3 of the response to question #29.

6 Registry Interfaces Abuse

The registry will employ the following countermeasures to protect against abuses of the registry systems and the DNS network itself:

6.1 WHOIS data harvesting

WHOIS access is a critical and vital service provided by any gTLD registry and the Registry will obviously comply with ICANN's requirements for WHOIS access.

However, as indicated in the SSAC's document "Is the WHOIS Service a Source for email Addresses for Spammers?", WHOIS abuse can be considered to be one of the primary means to generate email address lists for the purposes of sending unsolicited email, in particular the practice of mass harvesting information from the WHOIS. It is also believed that the WHOIS is the main source of data for generating fake renewal notices. To protect against harvesting of registration data (and particularly, email addresses), the registry will employ the following countermeasures:

• WHOIS query rate limits: All access to whois data will be query rate limited on a per-IP-address basis (for IPv4) and a per-prefix basis (for IPv6), with a daily limit of 25 WHOIS queries per IP address/prefix. Once this limit is reached, the WHOIS server responds with a relevant notification message instead of the standard WHOIS answer (The query limits may be reviewed and adapted by the Registry operator from time to time). IP-Ranges of accredited registrars (and other IP-ranges, eg. ICANN itself, UDRP and URS service providers etc) will be excluded from those rate limiting measures. This will allow legitimate usage of the service while at the same time make it very difficult to harvest data on a large scale.

• Email/Phone/Fax privacy: The EPP implementation of the "contact" object provides a mechanism that allows a registrar to define whether or not the "email", "phone", and "fax" fields of the contact object shall be publicly disclosed (i.e. "contact:disclose" element). The registry will set these fields to "do not disclose" by default, however, registrars can modify this setting via the normal EPP command stream. When a flag for a certain field is set to "do not disclose", the respective field will be omitted from anonymous WHOIS outputs, providing a minimum level of privacy to registrants. To allow for various business processes, IP Ranges of accredited registrars (and other IP-ranges as needed, eg. ICANN itself, UDRP and URS service providers) will still need to see the full data set, including those fields marked as "do not disclose".

• WHOIS monitoring: The WHOIS service will be monitored in order to identify unusual activity on the interface

The countermeasures above provide a well-balanced compromise between the requirements to provide access to WHOIS data and the basic data protection rights of registrants. More information about the WHOIS service provided by the registry is contained in response to Question 26.

6.2 EPP Interface Abuse

As described in the answers to the SRS, EPP and security questions (Question 24, 25 and 30, respectively), the EPP interfaces of the Registry are heavily firewalled, are only accessible from IP-ranges of accredited registrars and are protected by EPP authentication mechanisms. As such, abuse of those interfaces (such as DDoS, brute-force attacks against username⁄password combinations etc) can only be performed from networks of parties with which the Registry Operator has a legal agreement. Additionally, EPP interfaces are rate-limited at the network layer.

On top of the outlined technical means, usage figures beyond any regular and meaningful traffic patterns that are ongoing or recurring will be investigated by the Registry Operator. A lack of a decent explanation for such non-regular registrar behaviour on the EPP interface might lead to sanctions such as service degradation, interruption or even termination to the extend possible it is provided for in the Registrar Accreditation Agreement.

6.3 DNS Interface Abuse

Public nameservers, hidden masters and the signing infrastructure is configured and firewalled so that they allow NOTIFYs and UPDATEs from the required addresses only. In order to prevent zone walking and load peaks, zone transfers from the DNS infrastructure are disabled.

7 Management and removal of orphan glue records

It is understood, that inline with the SSAC’s comments in http:⁄⁄www.icann.org⁄en⁄committees⁄security⁄sac048.pdf, glue records have a vital function in the correct and normal operation of the DNS but that they can also be used for malicious purposes.

In order to prevent such malicious usage, the registry performs glue record management in accordance with the following policy:

• Provisioning of host objects with glue: In line with the EPP RFCs, glue record (“internal”) host objects can only be provisioned when the superordinate (parent) domain name exists in the registry. Host objects that are not under the TLD managed by the registry (“external hosts”) can never have A or AAAA records
• Deletion of domain with subordinate glue record hosts: When a domain name transitions from a “REGISTERED” to a “REDEMPTION” status (for example, via the EPP “delete domain” command, or via expiration), the domain name itself is removed from the DNS, however any glue records under the deleted domain are kept in the zone temporarily. Other registrars who are affected by a potential impact on DNS service due to the upcoming removal of the host from their domains are notified via the EPP message queue.
• Subsequently, when the domain name transitions from a “REDEMPTION” to a “PENDING DELETE” status, the glue records under the affected domain name are revoked from the DNS, but still exist in the SRS database.
• In the last step of the deletion process (transition from “PENDING DELETE” to “AVAILABLE”), the glue record host objects are deleted together with the domain and are also removed from any other domain name in the registry that still uses those hosts.

This policy effectively prevents misuse of orphan glue records in the registry since the status of a host object always follows the status of the superordinate domain. As a result glue records can never exist for domains that are not in the registry database. Additionally, keeping the glue records in the zone during the redemption period together with notification to Registrars significantly reduces the risk of other domains being impacted and reduces the effort required by a registrar in the event that the domain is subsequently restored.

However, in addition to this procedural policy outlined above, the registry operator will also act on documented evidence that glue records are present and used in connection with malicious activity by subsequently removing such glue records manually.

8 Ressourcing Plan

The Registry operator expects a domain name volume in the first three years of operations of .GMBH as listed in response #46. It will plan staffing needs based on these figures and install abuse response functions which will likely consist of internal and outsourced staff. The planned functions for .GMBH are based on nic.at's experience with the management of abuse complaints. The abuse response staff will be able to swiftly investigate abuse complaints and to react accordingly.

8.1 CERT.at is a department of the backend provider

It is important to note that the Austrian CERT (Computer Security Emergency Response Team, see http://www.cert.at/), staffed with 5 full-time-equivalents is a department within nic.at and shares offices with the registry operations team. Hence, world class security and anti-abuse expertise is committed to be available literally „next door" to the registry operations centre.

29. Rights Protection Mechanisms

Overview

As required by specification 7 of the new gTLD Agreement, the Registry Operator will implement and strictly adhere to any rights protection mechanisms („RPMs") that are mandated by ICANN. All mandated and independently developed RPMs will be included in the Registry-Registrar Agreement for .GMBH. The Registry Operator will implement all required RPMs described in the Trademark Clearinghouse („TMCH") function (once adopted by ICANN) and understands that ICANN may revise such requirements from time to time.

The detailed implementation of the TMCH function is still unspecified to a greater extent.

The Registry Operator will not mandate that owners of applicable intellectual property rights have to use any other trademark information aggregation, notification or validation service in addition to or instead of the ICANN-designated TMCH.

The Registry Operator will comply with PDDRP, RRDRP and URS procedures, and will implement and adhere to the remedies ICANN imposes via those processes.

The Registry Operator will also take reasonable steps to investigate and respond to any reports from law enforcement, governmental and quasi-governmental agencies of illegal conduct under the TLD, and understands that the Registry Operator will not be required to take any action that contradicts applicable law.

Details about the implementation of the various rights protection mechanisms are included below.

Safeguard Against Violation of the TLDs Eligibility Restrictions

To meet the requirements of ICANN to a community-based designation of the application, the registrant must use the .GMBH domain in connection to the Community as defined in Question 20.

The .GMBH Registry will conduct regular continuing validation of domain names registered to ensure continued compliance with these requirements. Failure to comply will result in a notice to comply. Non-compliance following such a notice period may result in take-down of the relevant domain name, at the discretion of the Registry.

The Registry is entitled to lock, cancel, initiate the gTLD-deletion cycle or transfer domain names that do not meet the registration criteria. It will set up a process for any questions and challenges that may arise from registrations. Complainants will be provided a single point of contact via the Registry's website to submit any questions and complaints regarding alleged abuse. The Registry also follows the standard dispute policies as defined in Q 28 and Q 39.

In detail the following measures will be carried out by the Registry to enforce the policies:

- Policies against domain name abuse and an Eligibility Requirements Dispute Resolution Policy (ERDRP)
- Dispute Policy based on local law
- Anti-Abuse Policies

By these policies the Registry is allowed to block, delete or transfer domain names.

UDRP Support

It is understood that ICANN's Uniform Dispute Resolution Process (UDRP) is largely concerned with registrars. Hence, the Registry Operator does not need to implement any specific process in order to support the UDRP specifically. However, the Registry Operator will support registrars in UDRP cases involving domain names under the TLD and will cooperate with approved Dispute Resolution Service Providers in order to assist in their work.

URS Support

The Registry Operator will comply with ICANN's requirements regarding the Uniform Rapid Suspension (URS) process and understands that the following services are required (and will be provided) during the operation of .GMBH:

Contact information: the Registry Operator will provide email and other contact information to accredited URS-DRPs (Dispute Resolution Provider) so that notices and other communication regarding URS cases can be communicated efficiently.

Notice and locking of a domain: Upon receipt of a respective Notice from an accredited URS provider, the Registry Operator will "lock" the affected domain name within 24 hours by means of putting it into the LOCKED status. This means that modifications (including transfers) on the domain name and registration data will be rejected but the name will still resolve in the DNS. The Registry Operator will immediately notify the URS-DRP upon locking the domain.

Remedies: In order for the URS-DRP to implement the Remedy, the Registry Operator will subsequently modify the registration (for example, by changing nameservers to the URS-DRP's own hosts) or remove the LOCKED status on the domain or implement other such measures as instructed by the URS-DRP.

Extend Registration: the Registry Operator will support successful Complainants if they wish to extend the registration period for one year at commercial rates.

The Registry Operator wishes to note that authentication of URS-DRP is a critical issue since Notices and other instructions may be sent via email to the Registry Operator and email itself does not provide any means of authentication. Hence, additional measures such as cryptographically signing such emails will be deemed necessary in order to identify a Notice as authentic and subsequently authorize requests to the Registry Operator.

PDDRP

The Registry Operator agrees to participate in the procedures required by the Post-Delegation Dispute Resolution Procedure (PDDRP) and be bound to all determinations that are the result of said procedures. The process implemented by the Registry Operator for actual complaints will be as follows:

Once a Complaint is received electronically or in paper notice form from the Provider, the Registry Operator will verify the content requirements of the Complaint, according to section 7.2 of the current PDDRP specification (dated Sep 19 2011). The Complaint will be reviewed by legal staff of the Registry Operator.

The Registry Operator will notify the Provider about the receipt of a complaint. If deemed necessary, the Registry Operator will submit papers within 10 days of receipt of the Complaint.

Registry Operator will subsequently follow the process regarding implementation of the remedies, as described in the PDDRP specification.

RRDRP

The Registry Operator agrees to participate in the procedures required by the Registration Restriction Dispute Resolution Policy (RRDRP) and be bound to the determinations that are the result of said procedures, in accordance to Section 2a of Specification 7 of the New gTLD Agreement. The actual administrative steps for handling Complaints based on the RRDRP will be identical, process-wise, to the PDDRP process described above.

Trademark Claims (Clearinghouse)

It is understood that – according to the Trademark Clearinghouse („TMCH") definition

dated Jan 12 2012 – ICANN is going to define a TMCH provider who will in turn supply two primary functions (see Section 1.2 of the document), of which function (ii) ("serving as a database to provide information to new gTLDs") will be directly relevant to the operation of this TLD.

It is also understood that ICANN's work towards the establishment of such a TMCH is still in progress. Therefore, it is not yet possible to describe the actual process and technical interfaces by which the Registry will support the TMCH requirements.

The Registry Operator will, however, implement any reasonable measures and processes that are required by the TMCH function.

Sunrise Services

The .GMBH Registry will perform a single Sunrise phase:

Registration in the "Trademark Clearinghouse" Sunrise

As part of its intended general service, the Registry Operator intends to implement a Sunrise period, where applicants will be validated using the Trademark Clearinghouse services. Eligible are all registrants who meet the eligibility criteria of .GMBH described in Question 20 and whose trademarks were validated by the Trademark Clearinghouse. The Sunrise period has a duration of 30 days; allocation follows the first-come, first-served principle.

The current draft .GMBH Sunrise Policy will be completed and ⁄ or in parts be replaced by the mandatory rules of the ICANN Trademark Clearinghouse as soon as they become available.

1.7.1 - Timing of the phased registration

D(-)180 - information on the registration phase. 3-6 months before the expected approval of the .GMBH, the Registry informs the public, administration, media and associations and chambers of the planned Sunrise and other procurement phases.

D0 - Approval of the .GMBH top-level domain by ICANN

D30 to D60 - Implementation of the Trademark Clearinghouse Sunrise period. During a period of 30 days, the Registry will receive requests for domain registrations via ICANN accredited registrars and conduct a review of the applications received.

D60-D90 – Cooling off period

D90 - Start of the general registration period (Landrush)

1.7.2 Requirements and Restrictions

Those wishing to register their marks in the .GMBH domain during the TMCH Sunrise Phase must own a current trademark or service mark listed in the TMCH. Eligible are all registrants who meet the eligibility criteria of .GMBH described in Question 20.

Notice will be provided to all trademark holders in the TMCH if someone is seeking a Sunrise registration. This notice will be provided to holders of marks in the TMCH that are an Identical Match (as defined in the TMCH) to the name to be registered

during Sunrise.
Sunrise registration will require a minimum term of one year.

An application is only considered complete when the applicant provides the Registry, via a registrar, with at least the following information:

a) the full name of the applicant; where no name of a company or organisation is specified, the individual requesting registration of the domain name is considered the Applicant; if the name of the company or the organisation is specified, then the company or organisation is considered the applicant;
- Address and country of the registered office, central administration or principal place of business of the applicants organization, or
b) the full name, address, and the land of an administrative contact person (natural person);
c) the e-mail addresses of the applicant or his representative and the administrative contact;
d) telephone and fax number by which the applicant or his representative and the administrative contact can be reached;
e) the requested domain;
f) the complete name for which a Prior Right is claimed;
g) the type of Prior Right claimed by the applicant;
h) the country in which the Prior Right claimed is protected.

The information referred to (f) and (h) above is deemed to constitute the legal basis in national or Community law for the claimed Prior Right to the name.

The Domain Name applied must consist of the complete name for which a Prior Right is claimed.
The Registry is entitled to exchange the above information with the Validation Agent(s) (including their agents and subcontractors) in order to effect validation of the rights claimed.

Other Reports

The following will be memorialized and be made binding via the Registry-Registrar and Registrar-Registrant Agreements:

- The registry may reject a registration request or a reservation request, or may delete, revoke, suspend, cancel, or transfer a registration or reservation under the following criteria:
a. to enforce registry policies and ICANN requirements; each as amended from time to time;
b. that is not accompanied by complete and accurate information as required by ICANN requirements and⁄or registry policies or where required information is not updated and⁄or corrected as required by ICANN requirements and⁄or registry policies;
c. to protect the integrity and stability of the registry, its operations, and the TLD system;
d. to comply with any applicable law, regulation, holding, order, or decision issued by a court, administrative authority, or dispute resolution service provider with jurisdiction over the registry;
e. to establish, assert, or defend the legal rights of the registry or a third party or to avoid any civil or criminal liability on the part of the registry and⁄or its affiliates, subsidiaries, officers, directors, representatives, employees, contractors, and stockholders;
f. to correct mistakes made by the registry or any accredited registrar in connection with a registration; or

g. as otherwise provided in the Registry-Registrar Agreement and/or the Registrar-Registrant Agreement.

Dispute-related Technical Functionality in the Registry System

In order to handle any disputes concerning a domain in the .GMBH zone according to the RPMs defined, the Registry Administration Panel (a web-based interface to the SRS to query and manipulate registry data) includes functionality to manually put domains into the "LOCKED" status (see Answer to question 27 - Registration Lifecycle). The dispute related functions are based on more than 12 years of experience in managing disputes under the ".at" TLD and provide the following functionality:

Search for domain names and display WHOIS as well as registrar data

For each domain, the following tasks can be performed:

** Delete the domain immediately (domain immediately enters PENDING DELETE state and thus cannot be restored by a registrar)
** Put the domain into the LOCKED state (which prevents modifications and transfers on the domain name, and also prohibits modifications on the associated registrant contact)
** Add the "serverHold" status to domain names under LOCKED (so that the name is excluded from the DNS, and hence technically disabled)
** Remove the "serverHold" status from a LOCKED domain
** Put domain names in LOCKED state back to their previous state (most commonly, REGISTERED).
** For each action, the system allows users to select one of several "reasons" to be recorded with the action.
** An additional free-form text box allows users to record additional information, such as pointers to external documents, or case numbers.
List all domain names in LOCKED status
Display data, reasons, and additional information of domains in LOCKED state
Display historical data about such cases

Resourcing Plan for Implementation and Ongoing Maintainance

Basic functionality regarding rights protections mechanisms (domain locking, tracking of requests) is already implemented in the registry core system, hence no further resources are needed for this initial implementation.

However, it is understood that resources are necessary to implement further measures that require technical interaction with the registry system, as soon as they are clearly defined (especially the TMCH process and sunrise). The implementation effort cannot be foreseen at the time of writing, hence the concrete resourcing plan for the technical part of the implementation and ongoing maintenance cannot be provided. However, the Registry Operator is aware of the fact that during landrush and sunrise more resources will be allocated to handle the increased load on the day to day operations as well performing necessary changes on the system after completion of sunrise and landrush if instructed by ICANN rules to do so.

Still, the Registry Operator will implement any reasonable measures and processes that are required by ICANN in respect to rights protection and resources will be allocated accordingly to have the functionality available for the operation of the

registry.

30(a). Security Policy: Summary of the security policy for the proposed registry

Registry Policy Framework

The Information Security Management System was developed in accordance with the international standard ISO 27001 and the registry backend operator is currently on the ISO 27001 certification path for the Information Security Management System (ISMS) to be completed before launching the registry. For the secondary datacenter in Salzburg the certification will be completed in 2012 and the primary datacenter in Vienna is already certified – please find ISO 27001 certification document in attachment 30a-06.

Registry Back-end Operator Security Organization

The role of the Chief Information Security Officer (CISO) is defined in the organization operating the registry back-end, and is staffed with an FTE. This person is responsible for the setup, operation and continuous improvement of the Information Security Management System and Business Continuity Management System.

In the organization chart the CISO is located directly below senior management. This role is independent of operational management and directly reports to the upper management of the registry backend operator who in turn reports to the registry operator’s management. The CISO advises the management on all security related issues.

Information Security Management System (ISMS):

The ISO 27001 based ISMS supports and facilitates management in achieving the goals defined in the Corporate Security Policy and Security Standard. The ISMS as shown in diagram Q30a-1 provides the Deming - cycle (plan-do-check-act) in security concerns as referred to in ISO 27001.

The Security Policy Framework and Security Standard have a review cycle of a maximum of 1 year. The CISO is responsible for adhering to this review cycle.

Business Continuity Management System (BCMS)

Please find further details on BCMS in response to question 39.

Corporate Security Policy

The Corporate Security Policy is understood as the commitment by upper management to support and maintain information and IT security.

The main items are:

The overall goal of these activities is to prevent security incidents and to minimize their impact.
Prevention before damage reduction; personal responsibility and awareness before surveillance of employees.
Information security and IT security are important quality metrics for the registry.

Information security and IT security are core competences of the registry.
Safeguarding the integrity and availability of the gTLDs Domain Name System
In the event of a Security incident to minimize any potential damage.

Corporate Security Standard

The Corporate Security Standard, based on ISO 27001, defines the areas of responsibility for information – and IT security:

IT Risk Management
Continuous Improvement Process
Audit Management
IT Asset Management
Information Classification and Processing
IT Change Management
Identity and Access Management
Personal Management
Security Incident Management
IT Project Management
IT Patch and Update Management
Backup and Recovery
Logging and Monitoring
Spam and Antivirus
Mobile Devices
Media Disposal
Network Security
Physical Security
External Suppliers

These areas will be discussed in more detail in the following sections.

* IT Risk Management

Diagram Q30a-2 describes the risk management process in use at the registry.

The evaluation of risks is performed according to 4 different category types:

Finance: assesses any potential financial impact on the registry.
Operating Tasks: assesses the influence on the main business processes or tasks of the registry.
Corporate Image: assesses the effects of reputational damage or loss of trust in the registry.
Compliance: assesses impact of contractual or legal damages.

The risks are evaluated and categorized into the following severity levels:

Critical
High
Medium
Low

The risks are further measured by their estimated frequency of occurrence:

Very high probability: 1 per month or more frequently
High probability: 1 per year
Possible: every 10 years
Highly unlikely: every 100 years

Impossible: risk is not relevant (for example avalanches in Vienna)

The risk assessment is performed using the Delphi technique and involves management, the CISO and the head of IT. Within each category the worst cases are rated as the most important ones.

Aspects of risk management are also used for the vulnerability management.

ISO27001

Domain	Name
6	Organization of information security
6.1	Internal organization
6.2	External parties
12	Information systems acquisition, development and maintenance
12.6	Technical vulnerability management

Continuous Improvement Process

The continuous improvement process is risk-management oriented, and shown in Figure Q30a - 3: Continuous Improvement process.

Regular organizational meetings are set up to trigger the process:

IT security update:
** Participants: Head of IT, CISO
** Topics: Operational tasks
** Frequency: At least every 2 weeks
Security jour fixe:
** Participants: CTO, CISO, optional head of IT
** Topics: Planning, monitoring of projects, tasks, countermeasures
** Frequency: At least every month
Management security jour fixe:
** Participants: CEO, CTO, CISO, optional head of IT
** Topics: Risk management, large scale management decisions

The management review has to take place at least once per year or as needed in the event that a potential risk arises.

Audit Management

The planning of all audit work including technical audits such as penetration tests and vulnerability scans is managed by the CISO.

Different kinds of technical security audits are accomplished:

Regular basis
** Vulnerability scans on systems at operating system level to identify problems in patch management or configuration processes
** Penetration tests are executed by third party security consultants to identify design issues, organizational deficits or other security issues. The focus of the penetration tests is varied every year.
** Web vulnerability scans (OWASP Top 10) are performed against all internal and external websites
Prior to the launch of a new system:
** Penetration testing of all business critical system elements
** Vulnerability scans on the system at an operating system level
** Web vulnerability scan (if the system is web-based)

ISO27001

Domain	Name
6	Organization of information security
6.1	Internal organization
6.2	External parties
15	Compliance
15.1	Compliance with legal requirements
15.2	Compliance with security policies and standards, and technical compliance
15.3	Information systems audit considerations

IT Asset Management

All assets and their lifecycles are fully documented. Assets are categorized as follows:

Physical assets
Software assets
Information assets

ISO27001

Domain	Name
7	Asset Management
7.1	Responsibility for assets
7.2	Information classification
8	Human resource security
8.3	Termination or change of employment

Information Classification

All information is classified into the following categories:

Public: For example data on public websites
Internal: For example general company information
Confidential: For example annual business reports before publication
Highly confidential: For example person specific data, penetration testing reports

The data classification policy defines how to store, transmit and share these different kinds of information.

ISO27001

Domain	Name
7	Asset management
7.1	Responsibility of assets
7.2	Information classification
10	Communications and operations management
10.7	Media handling
10.8	Exchange of information
12	Information systems acquisition, development and maintenance
12.3	Cryptographic controls
15	Compliance
15.1	Compliance with legal requirements

IT Change Management

IT change management ensures that all modifications to IT systems can be reproduced, fulfill the organizational needs and are documented. Changes are categorized into following groups:

Changes without approval
** Below low risk
** Implemented within 1 week
Standard change
** Low risk
** Implemented within 1 month
Emergency change
** If availability of a service is dependent on a specific change
** Has to be done as soon as possible
** Can’t be scheduled any more
** Escalation to management is required

ISO27001

Domain	Name
10	Communications and operations management
10.1	Operational procedures and responsibilities
12	Information systems acquisition, development and maintenance
12.6	Security in development and support processes

Identity and Access Management

All user rights are based on the “least privilege” and “need to know” principle. Roles are used to group the relevant user permissions where appropriate.

User accounts are personal accounts meaning that they identify one specific person. Group or role accounts are non-standard and have to be approved in writing by the CISO.

Administrative accounts have to be approved by the head of IT in writing. There are stronger policies, for example password policies.

External accounts (for third parties) also need written approval by the CISO. These types of accounts are deactivated after 30 days.

External administrative accounts need written approval by the head of IT and the CISO. Such accounts are subject to increased monitoring and logging. These types of accounts are also deactivated after 30 days by default.

If an employee leaves the company, his⁄her account is deactivated immediately.

Inactive accounts are deleted after 60 days.

At least once a year there is a review of the accounts structure and user rights permissions performed by analyzing a sample of accounts.

ISO27001

Domain	Name
11	Access controls
11.1	Business requirement for access control

11.2 User access management
11.3 User responsibility
11.5 Operating system access control
11.6 Application and information access control

Personnel Management

Checklists exist for employee entry and exit activities. Every new employee is added to these lists and registered. All new employees have to prove that they have not been previously prosecuted and do not have a criminal record which means that there are no relevant records in the police records (Strafregisterauszug). Every employee must attend a security awareness course.

Background checks for security personnel

All Computer Emergency Response Team (CERT) members and the CISO are background security checked by the Federal Ministry of Interior (§55 Sicherheitspolizeigesetz).

ISO27001
Domain Name
8 Human resource security
8.1 Prior to employment
8.2 During employment
8.3 Termination or change of employment

Security Incident Management

A sister company of the registry backend operator also operates a CERT. This team consists of one Junior Security Analyst and a minimum of five Senior Security Analysts with at least 5 years and up to 15 years experience in IT Security.

This team also operates the national CERT for the Republic of Austria (CERT.at) and together with the Federal Chancellery of the Republic of Austria, the Austrian Government CERT (GovCERT Austria). It is internationally accredited as a Forum of Incident Response Member (FIRST) and a Trusted Introducer. By achieving these memberships the registry has built an excellent formal and informal information network. As a result the registry is well prepared for the prevention of and response to security incidents.

Figure Q30a – 4 the Security Incident Management Process is described.

Classification for the triage of security incidents

Urgency:

Immediate: Reaction within 1h, invoke crisis organization if necessary
Soon: Reaction within 8h or on the next business day
Normal: Equivalent to a systems change, defined by change management procedures

Impacts:

Critical
High
Middle
Low

ISO27001

Domain	Name
13	Information security incident management
13.1	Reporting information security events and weaknesses
13.2	Management of information security incidents and improvements

IT Project Management

A specific project management methodology has been defined.

ISO27001

Domain	Name
6	Organization of information security
6.2	Internal organization
10	Communications and operations management
10.1	Operational procedures and responsibilities
10.3	System planning and acceptance
12	Information systems acquisition, development and maintenance
12.1	Security requirements of information systems
12.5	Security in development and support processes

IT Patch and Update Management

A formal vulnerability and patch management process has been defined (shown in Figure Q30a - 5: Vulnerability Management).

Patches are classified as:

Critical (remediation within hours)
Non critical (remediation by the next patch day)

All patches are fully tested prior to being deployed.

The effectiveness of the patching process is audited by vulnerability scans and by matching the actual software inventory with vulnerability databases.

Reports are discussed on a regular basis by management in order to guarantee continuous improvement.

ISO27001

Domain	Name
10	Communications and operations management
10.1	Operational procedures and responsibilities
12	Information systems acquisition, development and maintenance
12.5	Security in development and support processes
12.6	Technical Vulnerability Management

Backup and Recovery

A full backup and recovery framework is in place. For details see the answer to question 37.

ISO27001

Domain	Name
10	Communications and operations management
10.5	Back Up

15 Compliance
15.1 Compliance with legal requirements

Logging and Monitoring

A logging and monitoring solution is in operation to identify malicious activities and unauthorized access. All authorized access is also logged.

All servers and systems are time synced using the Network Time Protocol (NTP).

The level of detail of logging:

Varies with expected risks
Requirements of business processes
Requirements of data integrity and confidentiality

Minimum details are

User ID
Date and time
Type of access
Software
Non authorized access
** Not working action
Administrator actions
** System start and stop
** Change of system configuration
** Activation and de-activation of security components
Security components alarms
Error protocol
Security protocol, for example anti virus software

All relevant systems of the gTLD registry are controlled by a host-based intrusion detections system (HIDS). All events are logged on a central device.

The HIDS allows to:

Check of host integrity.
Check of file integrity.
Port monitoring
Programs using specific ports
Process checks
Login⁄logoff

The HIDS and the other log sources are integrated into a central monitoring tool. This tool can trigger certain events.

Analysis of logging and monitoring information is performed continuously to detect security incidents and performed as needed in the event of a security incident.

ISO27001
Domain Name
10 Communications and operations management
10.2 Third party service delivery management
10.10 Monitoring
15 Compliance
15.1 Compliance with legal requirements

Spam and Antivirus

All office systems are protected by anti malware software. Servers are checked on a regular basis, if real time protection is not possible.

ISO27001
Domain Name
10 Communications and operations management
10.4 Protection against malicious and mobile code
10.6 Network security management
13 Information security incident management
13.1 Reporting information security events and weaknesses

Mobile Devices

All smartphones and mobile devices (for example notebooks) must use full hard disk encryption if technically possible. If possible it should be combined with remote wipe functionality.

The actual standard for smartphones are to use Blackberry devices with a corporate policy.

Every loss of a device has to be reported to the IT department as soon as possible.

ISO27001
Domain Name
7 Asset management
7.1 Responsibility for assets
11 Access control
11.7 Mobile computing and teleworking

Media Disposal

Information in paper form must be shredded if it is classified as confidential or higher.

Hard disk drives (HDD) and other storage media are deleted or destroyed in conformance with policy requirements.

For example:

Overwrite HDDs multiple times with random data
Shredder CDs

Media disposal policies apply to all relevant devices, e.g. also HDDs in printer or other media devices.

ISO27001
Domain Name
9 Physical and environmental security
9.2 Equipment security
10 Communications and operations management
10.7 Media handling

Network Security

The aspects of integrity, confidentiality and availability are considered as essential aspects in our network design.

Integrity, confidentiality:

Encryption on network layers between:
** Data centers
** Offices and data centers

Availability

Redundant physical paths via multiple carriers

Access to the network itself is restricted by means of security zone definitions, for example no direct connection is available to the corporate network from visitor meeting rooms etc.

All controls are audited on a regular basis, for example by penetration tests.

ISO27001

Domain	Name
10	Communications and operations management
10.6	Network security management
11	Access control
11.4	Network Access Control
12	Information systems acquisition, development and maintenance
12.3	Cryptographic controls

Physical Security

The physical security risks are again evaluated on an annual basis.

The gTLD systems themselves are operated in two different data centers with state-of the art security provisions in place, e.g. heavily restricted access to data center and locked racks.

For details see answer to question 39.

ISO27001

Domain	Name
9	Physical and environmental security
9.1	Secure areas
9.2	Equipment security

External Suppliers

For external suppliers either the same restrictions as those for internal personnel or further restrictions are applied.

Domain	Name
6	Organization of information security
6.2	External parties
10	Communications and operations management
10.2	Third party service delivery management

Annex B

Common register portal of the German federal states

Federal / state governments
Online services
Announcements

Homepage
Normal search
Advanced search
Login
Register
State info
Information / Help
Website Details
Contact

Change current search
Previous search result

Entity data

Company: Berlin District court **Berlin (Charlottenburg) HRB 124498** – TLDDOT GmbH

Legal status:	Gesellschaft mit beschränkter Haftung
Capital:	25.000,00 EUR
Date of entry:	01/02/2010 (When entering date of entry, wrong data input can occur due to system failures!)
Date of removal:	-
Balance sheet available:	-
Address (subject to correction):	TLDDOT GmbH Akazienstr. 2 10823 Berlin

Print this page . back to top