# التقرير النهائي من
# مجموعة العمل المتخصصة حول خدمات دليل gTLD:
# خدمة دليل
# تسجيل من الجيل التالي (RDS)

### حالة هذه الوثيقة

هذا هو التقرير النهائي المقدم من مجموعة العمل المتخصصة حول خدمات دليل نطاقات gTLD (أو EWG)، يسرد تفاصيل التوصيات المقدمة إلى مجلس إدارة ICANN لخدمات دليل تسجيل من الجيل التالي (RDS) لاستبدال نظام WHOIS الحالي.

## 1. الملخص التنفيذي

هذا هو التقرير النهائي المقدم من مجموعة العمل المتخصصة حول خدمات دليل نطاقات gTLD (أو EWG)، يسرد تفاصيل التوصيات المقدمة إلى رئيس/ المدير التنفيذي لمجلس إدارة ICANN لخدمات دليل تسجيل من الجيل التالي (RDS) لاستبدال نظام WHOIS الحالي.

يمثل هذا التقرير النهائي ذروة فترة مكثفة من العمل قوامهما أكثر من 15 شهرًا أمضت خلالها هذه المجموعة المتنوعة من المتطوعين آلاف الساعات من أعمال البحث المتعمقة، ونظرت في أكثر من 2600 صفحة من التعليقات العامة، والردود على استطلاعات الرأي، وأيضًا نتائج الأبحاث، كما شاركت في 19 عملية تشاور للمجتمع العام، و35 يوم من اجتماعات EWG المباشرة، و42 دعوة لـ EWG، وأكثر من 200 دعوة للفرق الفرعية، مع عدد لا محدود من جلسات جمع التعقيبات بالتعاون مع خبراء خارجيين وأعضاء من المجتمع - كل ذلك من أجل الرد على سؤال بسيط:

**ها هناك بديل عن نظام WHOIS الحالي يخدم مجتمع الإنترنت العالمي بشكل أفضل؟**

نعم، يوجد ذلك. توصي مجموعة EWG بالإجماع بالتخلي عن نموذج WHOIS الحالي الخاص بإعطاء كل مستخدم نفس الوصول العام غير معلوم الهوية بالكامل (غير الدقيق في الكثير من الأحيان) لبيانات تسجيل gTLD.

وعوضًا عن ذلك، توصي مجموعة العمل المتخصصة EWG بتحول في النماذج إلى نظام RDS من الجيل التالي من أجل جمع وتوثيق بيانات التسجيل والكشف عنها للأغراض المصرح بها فقط.

بينما تظل البيانات الأساسية متاحة أمام الجمهور، لا يمكن الوصول والاطلاع على البقية إلى من خلال مقدمي الطلبات المعتمدين الذي يحددون هوياتهم، ويعلون أغراضهم، ويوافقون على تحمل المسئولية عن الاستخدام المناسب لها.

وتصف الصفحات الـ 150 التالية الإسهامات والأبحاث التي أدت بمجموعة EWG إلى تقديم هذه التوصية، ومقترح تفصيلي للحصول على نظام RDS جديد، بالإضافة إلى الاستنتاجات التالية:

- هذه المسألة معقدة للغاية.
- فقد فحصت مجموعة EWG هذه المسألة من واقع مجموعة وجهات النظر وأجرت بحثًا من أجل ضمان أن نظام RDS قابل للتطبيق.
- وعلى الرغم من أن نظام RDS المقترح غير نموذجي، إلا أنه يعكس التسويات البارعة والمتوازنة مع العناصر المتداخلة التي لا يجب فصلها.
- وقد تم تصميم RDS المقترح من أجل التعامل المباشر بطريقة غير مسبوقة مع:
  - مشكلات خصوصية البيانات الصعبة؛
  - تحديات التوثيق ذات البيانات الطويلة والمتردية من حيث الجودة والدقة
  - بالإضافة إلى تحقيق توازن قابل للتطبيق بين الوصول والمساءلة.
- ويجب اعتماد نظام RDS بالكامل. فاعتماد بعض وليس كل مبادئ التصميم الموصى بها هنا يقوض مزايا النظام البيئي بالكامل.

يعكس هذا التقرير النهائي إجماعًا، بما في ذلك التوصيات والمبادئ المقترحة الخاصة به بالنسبة لنظام RDS من الجيل التالي. وهذا الدعم والتأييد جدير بالملاحظة بالنظر إلى النطاق الواسع لوجهات النظر وأصحاب المصلحة المشار إليهم بين أعضاء مجموعة EWG.[1]

علمًا بأن مجموعة عمل المتخصصين EWG على ثقة من أن هذا التقرير النهائي يحقق توجيه مجلس إدارة ICANN للمساعدة في إعادة تحديد الغرض وتوفير بيانات تسجيل gTLD التي ستوفر أساسًا لمساعدة مجتمع ICANN (من خلال منظمة دعم الأسماء العامة، GNSO) في إنشاء سياسة عالمية جديدة لخدمات دليل gTLD.

وفريق EWG على ثقة من أن نظام RDS الموصوف في هذا التقرير النهائي يصف أساسًا أكثر ثباتًا من الموجود حاليًا - أساس يمكن من خلاله لـ GNSO وضع سياسة عالمية جديدة لبيانات تسجيل gTLD من أجل حماية الخصوصية الشخصية وتأكيد أعلى مستوى من الدقة والمساءلة والشفافية بالنسبة لنظام ICANN البيئي الكامل لأعوام قادمة.

وحيث إن مجلس الإدارة، وGNSO، ومجتمع ICANN ينظرون في هذا التقرير النهائي، توصي مجموعة EWG بأن يتم تأطير هذا النظر من خلال الأسئلة التالية:

- هل نظام RDS مفضل على نظام WHOIS الحالي؟
- فإن لم يكن الأمر كذلك، هل يوافق مجتمع ICANN على أن وجود الاستمرار في استخدام نظام WHOIS الحالي، وهل له القدرة على تحقيق احتياجات الإنترنت العالمي المتنامي؟

**الخلفية**

تم تشكيل فريق الخبراء المتخصصين EWG بمعرفة الرئيس التنفيذي لـ ICANN، فادي شحاده، بناء على طلب من مجلس إدارة ICANN، للمساعدة في حل الجمود الذي دام لعشر سنوات داخل مجتمع ICANN حول كيفية استبدال نظام WHOIS الحالي.[2]

ولتجاوز أوجه القصور في نظام WHOIS الذي تحدد من خلال العديد من تقارير ودراسات المجتمع[3]، يتمثل تفويض مجموعة EWG في إعادة النظر وتحديد الغرض من جمع والحفاظ على بيانات تسجيل gTLD، والنظر في كيفية حماية البيانات، واقتراح حل الجيل التالي الذي من شأنه أن يلبي بأفضل حال احتياجات مجتمع الإنترنت العالمي.

ومن خلال البدء بصفحة بيضاء، استعرضت مجموعة EWG افتراضات أساسية حول أغراض واستخدامات، بيانات التسجيل بالإضافة إلى جمعها والحفاظ عليها وتوفيرها. وقد نظرت مجموعة EWG في كل صاحب مصلحة مشارك في خدمات دليل gTLD، مع التعرف على احتياجات الدقة والوصول والخصوصية. وقد نظرت في الأساليب المحتملة في تحقيق تلك الاحتياجات بمزيد من الفاعلية.

---

[1] برجاء الاطلاع على الملحق ي للتعرف على تشكيل فريق EWG وخبرات الأعضاء.

[2] يرجى الرجوع إلى https://www.icann.org/news/announcement-2-2012-12-14-en

[3] يرجى الرجوع إلى الملحق ب للحصول على قائمة بتقارير توثق أوجه القصور في WHOIS.

ولكي تتمكن مجموعة EWG من توجيه المداولات التي تجريها، فقد وضعت بيان أغراض رفيع المستوى، من خلال استخدمه في مطابقة التوصيات الواردة في هذا التقرير مع مهمة ICANN وتصميم نظام لدعم تسجيل أسماء النطاقات والحفاظ عليها تتوفر فيه المواصفات التالية:

- يوفر وصولاً مناسبًا لبيانات التسجيل الدقيقة والموثوقة والموحدة؛
- يحمي خصوصية معلومات المسجل؛
- يوفر آلية معتمدة تقوم بتعريف، وإقرار والحفاظ على القدرة على الاتصال بالمسجلين؛
- يدعم إطار عمل يتناول المشكلات التي تشتمل على المسجلين، بما في ذلك على سبيل المثال لا الحصر: حماية المستهلك، والتحري عن الجرائم الإلكترونية، وحماية الملكية الفكرية
- يوفر بنية تحتية للتعامل مع الاحتياجات المناسبة لإنفاذ القانون.

**المستخدمين والأغراض**

قامت مجموعة EWG بفحص الأغراض الحالية والمحتملة لجمع وتخزين وتوفير بيانات تسجيل gTLD لتوفير مجموعة واسعة ومتنوعة من المستخدمين، والتعرف على مجموعة من حالات استخدام WHOIS الواسعة والتمثيلية الواسعة.


وقد نظرت مجموعة EWG في المجموع الكلي لهذه الحالات الخاصة بالاستخدام بالإضافة إلى الدروس المستفادة منها، فضلاً عن المواد المرجعية وتعقيبات المجتمع، من أجل توجيه مجموعة موحدة من المستخدمين والأغراض المسموح بها والتي يجب تسويتها من خلال RDS وإساءات الاستخدام التي يجب الحيلولة دون حدوثها.

**الأغراض التي يجب تسويتها أو حظرها**

اتساقًا مع مهمة وتفويض EWG، تم فحص سائر هؤلاء المستخدمين للتعرف على تدفقات العمل الحالية والمحتملة في المستقبل بالإضافة إلى أصحاب المصلحة والبيانات المشمولة فيها.

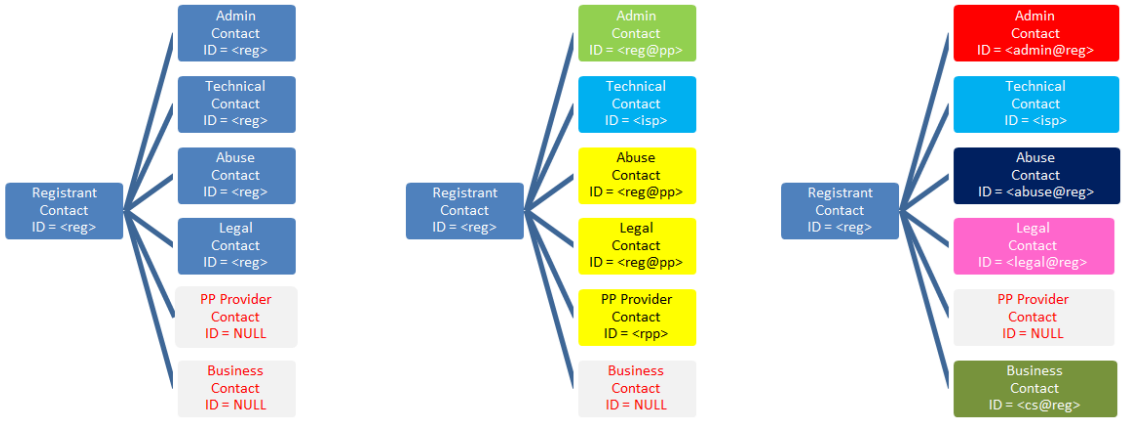
ويجب على بيانات تسجيل أسماء النطاقات - متى ما تم تحليلها - أن تقود عناصر البيانات الإلزامية، والمخاطر ذات الصلة، وقانون الخصوصية ومتضمنات السياسة، وتناول الأسئلة الأخرى التي تم التعرف عليها في هذا التقرير. ويحتوي الجانب الأيمن على تلخيص للأغراض المسموح بها من مجموعة EWG.


وبالنسبة للأغراض المسموح به والمحددة في الوقت الحالي بالإضافة إلى بيانات واتصالات واحتياجات استعلامات التسجيل المرتبطة بها فهي محددة أدناه والمزيد من التفاصيل في القسم الثالث.

| الغرض | يضمن مهام مثل... |
|---|---|
| **التحكم في اسم النطاق** | إنشاء وإدارة ومراقبة اسم النطاق الخاص بالمسجل (DN)، بما في ذلك إنشاء DN، وتحديث المعلومات حول DN، وتحويل DN، وتجديد DN، وحذف DN، والحفاظ على محفظة DN، واكتشاف الاستخدام التدليسي لمعلومات الاتصال الخاصة بالمسجل. |
| **حماية البيانات الشخصية** | تعريف موفر الخصوصية/الوكيل المعتمد أو الجهة المعتمدة لأوراق الاعتماد المحمية الآمنة المرتبطة باسم DN والإبلاغ عن إساءة الاستخدام، أو طلب الكشف، أو حتى الاتصال بهذا الموفر. |
| **حل المشاكل التقنية** | العمل على حل المشكلات الفنية المرتبطة باستخدام أسماء النطاقات، بما في ذلك مشكلات تسليم البريد الإلكتروني، وفشل حل نظام DNS، والمشكلات الوظيفية لمواقع الويب، من خلال الاتصال بفريق العمل الفني المسئول عن التعامل مع هذه المشكلات. |
| **توثيق أسماء النطاقات** | إصدار جهة التوثيق (CA) شهادة X.509 لجهة تم تحديدها من خلال اسم نطاق بحاجة إلى تأكيد أن اسم DN مسجل باسم حامل الشهادة. |
| **الاستخدام الفردي للإنترنت** | تعريف المؤسسة من خلال استخدام اسم نطاق من أجل غرس ثقة العملاء، أو الاتصال بتلك المؤسسة من أجل رفع شكوى للعملاء إليهم أو تقديم شكوى حولهم. |
| **بيع أو شراء أسماء نطاقات شركات الأعمال** | تقديم استعلامات شراء حول اسم DN، والاستحواذ على اسم DN من مسجل آخر، وتمكين بحث العناية الواجبة. |
| **بحث DNS للمصلحة الأكاديمية/العامة** | دراسات بحثية للمصلحة العامة الأكاديمية حول أسماء النطاقات المنشورة في RDS، بما في ذلك المعلومات العامة حول المسجل وجهات الاتصال المعينة، وتاريخ وحالة اسم النطاق، وأسماء النطاقات المسجلة من خلال مسجل محدد. |

| الغرض | يضمن مهام مثل... |
|---|---|
| **إجراءات قانونية** | التحري عن الاستخدام التدليسي المحتمل لاسم أو عنوان المسجل من خلال أسماء نطاقات أخرى، والتحري عن الانتهاكات المحتملة للعلامات التجارية، والاتصال بممثل قانوني لمسجل/مرخص له وذلك قبل اتخاذ إجراء قانوني ومن ثم اتخاذ إجراء قانوني إذا لم يتم التعامل بشكل مرضي مع المسألة. |
| **الإنفاذ النظامي والتعاقدي** | تقصي الجهات الضريبية لشركات الأعمال ذات التواجد على الإنترنت، والتحري عن UDRP، والتحري عن الامتثال التعاقدي، وعمليات تدقيق مستودعات بيانات التسجيل. |
| **التحري الجنائي والحد من إساءة استخدام DNS** | الإبلاغ عن إساءة استخدام شخص ما يمكنه التقي والتعامل مع إساءة الاستخدام هذه، أو الاتصال بالكيانات ذات الصلة باسم نطاق خلال التحري الجنائي غير المتصل بالشبكة. |
| **شفافية DNS** | الاستعلام عن بيانات التسجيل المعلنة للجمهور من خلال المسجلين من أجل تحقيق مجموعة متنوعة وكبيرة من الاحتياجات من أجل إطلاع الجمهور العام عليها. |

لكي يتم توفير وصول مستند إلى الأغراض إلى بيانات التسجيل مع تحسين الاتصال والخصوصية الشخصية، قامت مجموعة EWG بوضع مبادئ للاتصالات المستندة إلى الأغراض (PBC). ومن خلال ما تحصل عليه من دعم بأدوار ومسئوليات محددة، تم تحديد جهات الاتصالات المستندة إلى الأغراض PBC لكافة الأغراض المسموح بها في الحالات التي يلزم فيها إجراء اتصال. وفيما يلي توضيح لثلاثة أمثلة ومزيد من التفاصيل في القسم الثالث و الرابع.




كما قامت مجموعة EWG بتحليل كافة عناصر بيانات التسجيل - بدءًا من البيانات المحددة في اتفاقية RAA لسنة 2013 - من أجل توجيه مجموعة من المبادئ الإرشادية لجمع والإفصاح عن البيانات التي تتناسب تمامًا مع إطار عمل PBC الموصى به، بالإضافة إلى التوصيات المقدمة من أجل تمكين الامتثال لقوانين حماية البيانات. وقد قدمت مجموعة EWG توصيات إضافية لتحديد وتعريف عناصر البيانات الجديدة التي قد يختارها المسجلون وجهات الاتصال للنشر لجعل الاتصال أكثر قوة. وهذه التوصيات مذكورة بالتفصيل في القسم الرابع وهناك أمثلة على ذلك في الملحق هـ.

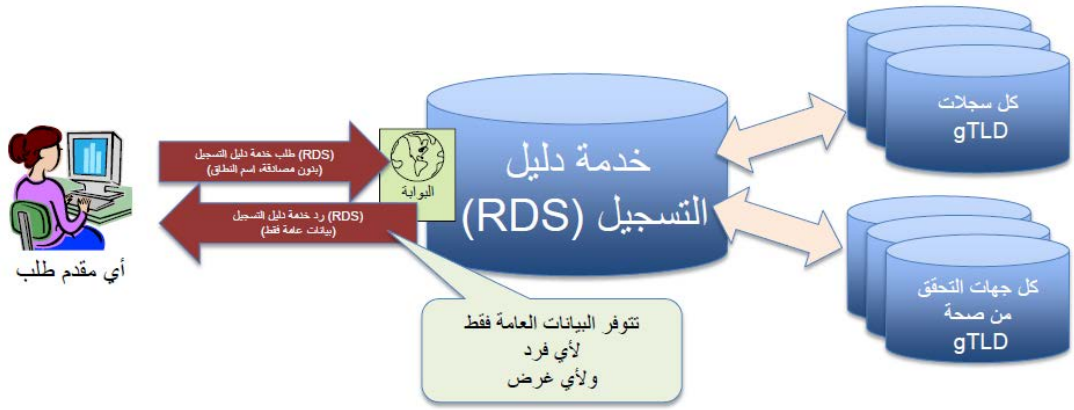
**الوصول الموجه بالأغراض**

يتخذ نظام RDS الموصى به أسلوب السجل النظيف، تاركًا نظام WHOIS الحالي المناسب لجميع الأغراض لصالح أسلوب الوصول الوجه بالأغراض للبيانات الموثقة أملاً في تحسين الخصوصية والدقة والمساءلة. وترى

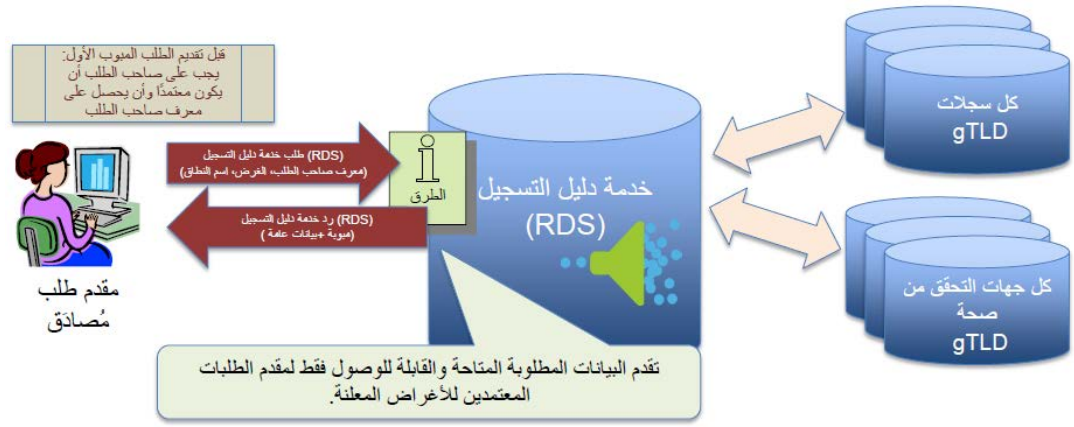
مجموعة EWG أن هذا النموذج الجديد الخاص بالوصول يمكن أن يزيد من المساءلة بالنسبة لجميع الأطراف المشاركة في الإفصاح عن بيانات تسجيل أسماء نطاقات gTLD واستخدامها من خلال:

- تسجيل جميع أنواع الوصول إلى بيانات تسجيل gTLD، بما في ذلك الوصول غير المرخص به إلى عناصر البيانات العامة، من أجل تمكين التعرف على أشكال إساءة الاستخدام والحد منها؛
- وضع بوابة وصول لعناصر البيانات الأكثر حساسية والتي لا تتوفر فقط لمقدمي الطلبات الذين يقدمون طلبات للحصول عليها وتم اعتمادهم للحصول على وصول RDS، في المستوى المناسب لكل مستخدم والغرض المحدد؛
- تدقيق كل من الوصول العام والوصول من خلال بوابة للبيانات من أجل الحد من مستوى إساءة الاستخدام وفرض عقوبات وغير ذلك من التعويضات نظير الاستخدام غير المناسب، بما يتفق مع الأحكام والشروط التي يوافق مقدم الطلب عليها صراحة.

فيما يلي شرح تفصيلي لمبادئ الوصول للبيانات الخاصة بمجموعة EWG، والتي استخدمت كأسس لتوصياتها التفصيلية حول الوصول للبيانات بشكل عام أو من خلال بوابة، في القسم الرابع. ووفقًا لما هو محدد أدناه، لا تزال هناك إمكانية لطلب عناصر البيانات العامة من RDS من خلال أي شخص، سواء كان بتصديق أو بدون تصديق.




كما يمكن أيضًا طلب عناصر البيانات من خلال نظام RDS. وللقيام بذلك، يجب على مقدم الطلب أن يحصل على المصادقة والاعتماد أولاً. وبعد ذلك، يجوز لمقدم الطلب أن يقدم استعلامات معتمدة يطلب فيها عناصر البيانات لغرض محدد.



راجع الملحق هـ للتعرف على توضيح أكثر تفصيلاً لعناصر البيانات المعادة إلى استعلامات البيانات العامة ومن خلال بوابات، وكيف أن الوصول عن طريق بوابة يعتمد على المستخدم والغرض، وكيف يمكن لجهات اعتماد مستخدمي RDS أن تلعب دورًا في توثيق وتدقيق الوصول عن طريق البوابات.

**حماية الخصوصية والبيانات**

من العناصر المحورية بالنسبة لاختصاص مجموعة EWG مسألة كيفية تصميم نظام يعمل على زيادة دقة البيانات التي يتم تجميعها في حين يعرض أيضًا سبل حماية للمسجلين الساعين لحماية خصوصيتهم والحفاظ عليها.

وتدرك مجموعة EWG أن المعلومات الشخصية محمية بموجب قانون حماية البيانات، وحتى في الحالات التي لا تكون فيها قوانين، فإن هناك أسبابًا شرعية للأفراد للسعي لتحقيق أشكال من الحماية العالية لمعلوماتهم الشخصية. بالإضافة إلى ذلك، قد تسعى بعض شركات الأعمال والمؤسسات إلى حماية معلوماتها لأغراض شرعية، كما هو الحال عندما تقوم بالإعداد للبدء في إطلاق خط إنتاج جديد، أو في حالة شركات الأعمال الصغيرة، حيث تفصح معلومات الاتصال عن البيانات الشخصية.

وطبقًا لذلك، قامت مجموعة EWG بصياغة مجموعة من التوصيات من أجل تمكين التوافق الروتيني مع قوانين حماية الخصوصية والبيانات، المذكورة بالتفصيل في القسم السادس. وتغطي هذه المبادئ ما يلي:

- الآليات المستخدمة في تسهيل التجميع الروتيني للبيانات والمتوافق مع الناحية القانونية والنقل بين الجهات الفاعلة داخل النظام البيئي RDS؛
- فقرات العقود القياسية المتوافقة مع قوانين حماية الخصوصية والبيانات والمشفرة في السياسية؛
- "محرك قوانين" لتطبيق قوانين حماية البيانات
- بالإضافة إلى طريقة ارتباط موقع تخزين بيانات RDS بالوصول إلى إنفاذ القوانين.

بالإضافة إلى الخصوصية المقدمة من خلال التوافق مع قوانين حماية البيانات، أوصت RDS أيضًا بمبادئ من أجل استيعاب الاحتياجات الخاصة بالخصوصية من خلال تضمين ما يلي في نظام RDS البيئي:

- خدمة خصوصية/وكالة معتمدة للاستخدام العام
- بالإضافة إلى خدمة أوراق اعتماد محمية وآمنة معتمدة للأشخاص المعرضين للخطر وفي الحالات التي قد يتم فيها رفض حقوق التحدث بحرية أو محاكمة المتحدثين.

كما توصي مجموعة EWG أيضًا بأن تتحرى ICANN عن وضع سياسة خصوصية أحادية ومتوافقة تحكم أنشطة RDS بطريقة شاملة.

وللتعامل مع الحاجة إلى خدمات خصوصية ووكالة أكثر وحدة واعتمادية تتيح الفرصة لقدر أكبر من المساءلة، فقد ضمت مجموعة EWG اتصال خصوصية/وكالة في مبادئ PBC الخاصة بها. كما أوصت بمبادئ خصوصية/وكالة بالإضافة إلى إطار عمل كتعقيب وإضافة إلى مجموعة عمل مشكلات اعتماد خدمات الخصوصية والوكالة لـ GNSO.

وللتعامل مع احتياجات الأفراد والمجموعات الذين يوضحون أنهم سيتعرضون لخطر إذا ما تم التعرف على هويتهم في بيانات التسجيل، توصي مجموعة EWG بإطار عمل أوراق اعتماد محمية وآمنة يمكن لتلك الأطراف من خلالها تقديم طلب بدون تحديد هوياتهم والحصول على أسماء نطاقات مسجلة من خلال استخدام أوراق اعتماد آمنة، يدعمها ضامنون وجهات أخرى معتمدة من أجل توفير حاجز بين الكيانات المعرضة للخطر وأمناء السجلات. وتوصي مجموعة EWG بأن تقوم ICANN بتسهيل تأسيس مجلس إدارة مستقل للمراجعة المعتمدة يعمل على توثيق دعاوى المؤسسات أو الأفراد المعرضين للخطر من أجل اعتماد أوراق الاعتماد (ورفضها عند الضرورة).

**جودة البيانات**

توصي مجموعة EWG بتوثيق أكثر قوة لبيانات المسجل بدلاً مما يقدمه نظام WHOIS الحالي أو التعزيزات التي قد تتحقق من خلال التنفيذ الواسع لاتفاقية RAA لسنة 2013. تشمل التحسينات الأساسية على جودة البيانات ما يلي.

- يجب أن يؤدي توفير جهات اتصال قائمة على الأغراض من خلال المسجلين إلى تحسينات كبيرة على القدرة على الوصول بالنسبة لجهات الاتصال المناسبة لأغراض مختلفة ويوفر حافزًا أمام المسجلين من أجل توفير المعلومات الدقيقة لتلك الأدوار.
- ومن خلال الوصول المتوفر عن طريق بوابات إلى عناصر البيانات الأكثر حساسية، سيكون لدى المسجلين حافز أقل في تقديم بيانات غير دقيقة، ويأتي مع ذلك قدر أكبر من المساءلة من أجل ضمان دقة البيانات.

بالإضافة إلى ذلك، توصي مجموعة EWG بإجراء تطويرين مرتبطين ولكن مستقلين في نفس الوقت:

- التوثيق القياسي لكافة بيانات تسجيل gTLD، من خلال استخدام كل من الفحوصات الدورية والتوثيق في وقت الجمع، مع خيار التوثيق المسبق لقوالب من بيانات الاتصال لإعادة الاستخدام في العديد من تسجيلات أسماء النطاقات، بالإضافة إلى قدرة مستخدمي RDS على الاطلاع على آخر مرة تم فيها توثيق البيانات وإلى أي مستوى
- عملًا بأن دليل جهات الاتصال الموثق مسبقًا والمنفصل من ناحية المفاهيم عن دليل أسماء النطاقات، لتعزيز الجودة والقدرة على إعادة استخدام عناصر البيانات المستخدمة في الاتصال مسجلي أسماء النطاقات والأشخاص أو المؤسسات التي يمكن تحديدها من خلال المسجلين كجهات اتصال PBC لأغراض مختلفة.

يمكن العثور على المبادئ والعمليات التي تسرد هذه التوصيات بالتفصيل في القسم الرابع.

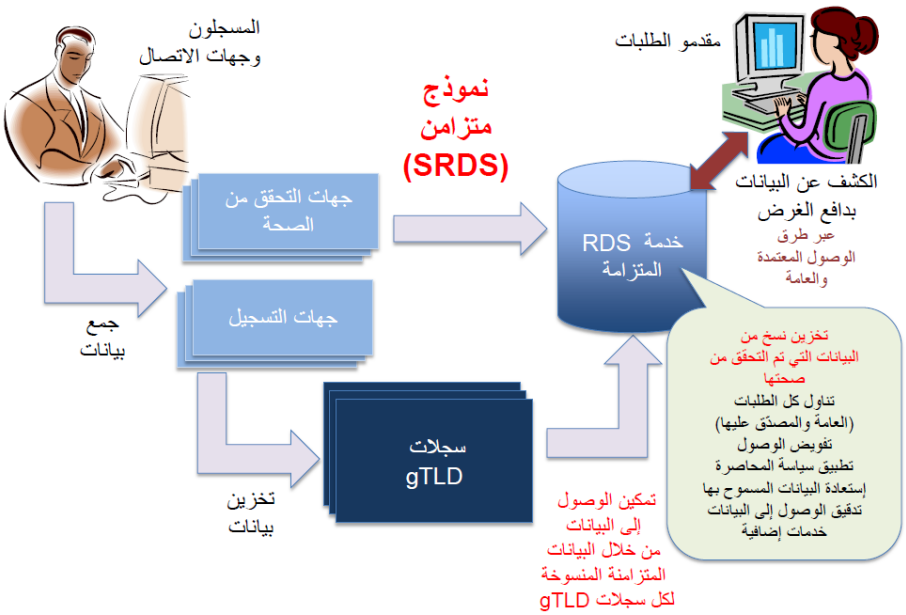
**نماذج التنفيذ**

بالنظر إلى كيفية إدخال هذه المبادئ والتوصيات حيز التنفيذ، استكشفت مجموعة EWG العديد من النماذج البديلة بعمق. وقد تم تقييم كافة النماذج من خلال استخدام مجموعة من معايير متعددة الأوجه وفقًا لما هو محدد في الملحق و. وبعد تحليل قوي، استنتجت مجموعة EWG ما يلي.

- يقوم أمناء السجلات والجهات التابعة لأمناء السجلات في الوقت الحالي بجمع وتخزين معلومات التسجيل من العملاء (المسجلين) التابعين لهم. وهذه العملية موزعة بشكل أساسي. وبالإضافة إلى مواصلة جمع بيانات التسجيل من المسجلين عن طريق أمناء السجلات أو الجهات التابعة لها، تقترح مجموعة EWG جمع بيانات الاتصال من خلال جهات توثيق.
- وهناك العديد من النماذج المحتملة بالنسبة لتخزين معلومات التسجيل عبر كافة نطاقات gTLD. وقد حددت مجموعة EWG العديد من النماذج المحتملة وسلطت الضوء على نموذجين رأت أنهما واعدين أكثر وتوصي المجموعة باختيار واحد منهما من خلال استخدام معايير تقييم.
- ولحماية خصوصية صاحب البيانات، يجب أن تتيح واجهة مركزية لمقدمي الطلبات المناسبين إمكانية الوصول والاطلاع على معلومات التسجيل عبر كافة نطاقات gTLD، بما في ذلك الوصول إلى البيانات العامة غير الموثقة والوصول إلى البيانات عبر البوابات الموثقة.
- ويجب على RDS استخدام RDAP أو EPP (حسب ما يتناسب لكل واجهة) باعتباره بروتوكول الوصول الأساسي للأدلة من أجل الحصول على معلومات التسجيل من مواقع التخزين، مهما كان مكانها.

وقد وضعت مجموعة EWG واختبرت العديد من نماذج النظم البديلة، المذكورة بالتفصيل في الملحق و، بما في ذلك النماذج التي اقترحها مجتمع ICANN. وتختلف النماذج المحتملة من حيث الطريقة التي يتم بها نسخ معلومات التسجيل أو الاستعلام عنها من خلال نظام RDS. وقد فحصت مجموعة EWG كل نموذج عن قرب من أجل تحديد تأثير هذه الاختلافات. وبعد مقارنة هذه النماذج المحتملة، فقد اكتشفت مجموعة EWG أنه، وباستثناء نظام WHOIS الحالي، فإن جميعها قادر على تحقيق مبادئ RDS الموصى بها من مجموعة EWG إلى درجة ما. ومن بينها، فقد ركزت مجموعة EWG على النموذجين الواعدين أكثر لإجراء مزيد من الفحص - النموذج الموحد والنموذج المتزامن (والمعروف في السابق باسم "النموذج التجميعي").

ولإضفاء مزيد من الاستنارة على تحليلها، بدأت مجموعة العمل تحليلاً لتكلفة نموذج التنفيذ أجرته جهة أخرى محايدة (IBM) من أجل الوقوف على المتطلبات والتكاليف المحتملة لهذين النموذجين. استنادًا إلى تحليل EWG المتعمق بالإضافة إلى تقرير تحليل IBM، والذي أثبت أن النموذج الموحد هو الأكثر كلفة بالنسبة لنظام RDS البيئي بالكامل، **فقد أوصت مجموعة EWG في النهائية بنظام RDS المتزامن (SRDS).**




**الخاتمة**

بسبب التفاصيل الموسعة وتعقيد وطول التقرير النهائي، فإن هذا الملخص التنفيذ ليس بمثابة نظرة عامة شاملة ويجب على القراء الرجوع إلى نص هذا التقرير النهائي للحصول على معلومات إضافية.

قدمت مجموعة EWG هذا التقرير النهائي إلى المدير التنفيذي ومجلس إدارة ICANN، ونشرته بشكل عام على الإنترنت، وسوف تعقد العديد من المشاورات العامة في اجتماع ICANN المقرر في يونيو 2014 في مدينة لندن. كما ستجري أيضًا ندوات ويب وفرص أخرى من أجل مناقشة التقرير والرد على الأسئلة حوله مع مجتمع ICANN. والغرض من هذا التقرير النهائي أن يكون أساسًا بالنسبة لعملية وضع السياسات (PDP) الخاصة بـ GNSO المطلوبة من مجلس الإدارة من أجل توفير بيانات تسجيل gTLD والمفاوضات التعاقدية، حسبما يتناسب.

علمًا بأن مجموعة عمل المتخصصين EWG على ثقة من أن هذا التقرير النهائي يحقق توجيه مجلس إدارة ICANN للمساعدة في إعادة تحديد الغرض وتوفير بيانات تسجيل gTLD التي ستوفر أساسًا لمساعدة مجتمع ICANN (من خلال منظمة GNSO) في إنشاء سياسة عالمية جديدة لخدمات دليل gTLD.

## 2. تفويض وغرض ونتائج فريق EWG

### أ. التفويض

تم تشكيل فريق خبراء العمل في خدمات دليل gTLD أو (EWG) بواسطة الرئيس التنفيذي لـ ICANN، فادي شحاده، بناء على طلب من مجلس إدارة ICANN، للمساعدة في حل الجمود الذي دام لعشر سنوات داخل مجتمع ICANN حول كيفية استبدال نظام WHOIS الحالي. وتشير العديد من تقارير ودراسات المجتمع[4] المنشورة خلال هذه الفترة إلى أوجه القصور في النظام الحالي والذي يدعو إلى توفير حل.

يتمثل تفويض واختصاص مجموعة EWG في إعادة النظر وتحديد الغرض من جمع والحفاظ على خدمات مجموعة gTLD، مع الأخذ في الاعتبار كيفية حماية البيانات، واقتراح حل الجيل التالي الذي من شأنه أن يلبي على أفضل نحو احتياجات مجتمع الإنترنت العالمي. بدأت مجموعة EWG باستخدام صفحة بيانات، للتعرف والاستفسار عن افتراضات أساسية حول أغراض واستخدامات، بيانات التسجيل بالإضافة إلى جمعها والحفاظ عليها وتوفيرها. وقد نظرت مجموعة EWG في كل صاحب مصلحة مشارك في خدمات دليل gTLD، مع التعرف على احتياجات الدقة والوصول والخصوصية والأساليب المحتملة في تحقيق هذه الاحتياجات بمزيد من الفاعلية.

### ب. الغرض

للمساعدة على توجيه مجموعة عمل EWG في المداولات التي تقوم بها، وضعت المجموعة بيانًا بالغرض عالي المستوى يتم من خلاله اختبار النتائج والتوصيات التي قدمتها، على النحو التالي:

> دعمًا للمهمة التي تقوم بها ICANN في تنسيق نظام المعرفات الفريدة للإنترنت العالمي، ولضمان التشغيل الآمن والمستقر لنظام المعرفات الفريدة الخاص بالإنترنت، والمعلومات حول أسماء نطاقات gTLD، من الضروري تعزيز الثقة والاطمئنان في الإنترنت لسائر أصحاب المصلحة.
>
> ووفقًا لذلك، من المفضل تصميم نظام لدعم تسجيل والحفاظ على أسماء النطاقات والذي:
>
> - يوفر وصولاً مناسبًا لبيانات التسجيل الدقيقة والموثوقة والموحدة
> - يحمي خصوصية المعلومات الشخصية
> - يوفر آلية معتمدة تقوم بتعريف، وإقرار والحفاظ على القدرة على الاتصال بالمسجلين
> - يدعم إطار عمل يتناول المشكلات التي تشتمل على المسجلين، بما في ذلك على سبيل المثال لا الحصر: حماية المستهلك، والتحري عن الجرائم الإلكترونية، وحماية الملكية الفكرية
> - يوفر بنية تحتية للتعامل مع الاحتياجات المناسبة لإنفاذ القانون

[44] يرجى الرجوع إلى الملحق ب للحصول على قائمة بتقارير توثق أوجه القصور في WHOIS.

### ج. النتائج

في 24 يونيو 2013، قامت EWG بنشر تقريرها الأولي، والأسئلة المتداولة، بالإضافة إلى استبانة على الإنترنت، وبدأت عملية مشاورات موسعة داخل مجتمع ICANN حول توصياتها الأولية. في تقريرها الأولي، خلصت مجموعة عمل المتخصصين EWG إلى وجوب التخلي عن نموذج WHOIS الحالي- والذي يعطي لكل مستخدم نفس الوصول غير معلوم الهوية إلى بيانات تسجيل نطاقات gTLD (غير الدقيق في الغالب). وبدلا من ذلك، توصي EWG بنقلة نوعية يتم من خلالها جمع بيانات تسجيل gTLD، والتحقق من صحتها والإفصاح عنها لأغراض مسموح بها فقط، مع بعض عناصر البيانات التي يمكن الوصول إليها من مقدمي الطلبات المصدق عليهم الذين يتحملون المسئولية بعد ذلك عن الاستخدام المناسب.

وقد توصلت مجموعة EWG إلى أن هذه التوصية بعد النظر الكامل في التقارير السابقة التي تسرد تفاصيل أوجه القصور في نظام WHOIS والعديد من أصحاب المصلحة المختلفين الذين يستخدمون نظام WHOIS الحالي. ولكل مجموعة محددة من المستخدمين، قامت مجموعة EWG بتحليل الأغراض التي حققتها بيانات التسجيل وعناصر البيانات الفردية اللازمة للقيام بذلك. وفي ضوء الاستفادة من هذا التحليل، أوصت مجموعة EWG بمبادئ ومزايا لتوجيه إنشاء خدمة دليل تسجيل (RDS) من الجيل التالي. ولتوضيح الطريقة التي يمكن من خلال تنفيذ هذه المبادئ، نظرت مجموعة EWG أيضًا في العديد من البدائل واقترحت نموذجًا لجمع والإفصاح عن عناصر بيانات تسجيل أسماء النطاقات الدقيقة لأغراض مسموح بها.

وفي 11 نوفمبر 2013، وبعد النظر بعناية في كافة التعليقات والتعقيبات الواردة من مجتمع ICANN، نشرت مجموعة EWG تقريرًا لتحديث الحالة، يركز على رأي فريق EWG بخصوص العديد من المشكلات الأساسية. كما وفر تقرير تحديث الحالة أيضًا قدرًا كبيرًا من التفاصيل حول التحليل الكامن خلف التقرير الأولي، وفقًا لما طلبه المجتمع.

وقد شاركت مجموعة EWG في تحليل تفصيلي للتعقيبات الواردة من كلا هذين التقريرين، مستخدمة في ذلك التعقيبات الواسعة والمتنوعة من المجتمع للرجوع بالفائدة على الأعمال المتواصلة والنواحي وفتح مجالات واختبار وتعديل توصياتها. وبسبب تعقيد المهمة الحالية وأهمية وضع أساس لأي نظام RDS من الجيل التالي وتحقيق فهم ثابت للمزايا والتأثيرات التي قد تنجم عن ذلك، أجرت مجموعة EWG بحثًا في خمسة مجالات: نطاق ccTLD الحالي وممارسات توثيق البيانات التجارية، وممارسات موفري خدمة الخصوصية/الوكيل الحالية، والتعرف على المنظمات ذات القدرة على اعتماد مستخدمي RDS، وتحليل مخاطر/مزايا وتكاليف RDS. أما نتائج هذا البحث، والمنشورة في مارس 2014، فقد تم استخدامها من أجل إجراء مزيد من التعديل على توصيات مجموعة EWG.

وفي هذا السياق، نظرت مجموعة EWG بعناية في الأعمال السابقة على نظام WHOIS، والمستخدمين الحاليين والمحتملين في المستقبل لبيانات تسجيل gTLD وأغراضهم، والتعقيبات والإسهامات من العديد من أصحاب المصلحة المتنوعين في نظام WHOIS الحالي، والممارسات الحالية المرتبطة بتحسينات RDS المقترحة، وتحليل لمخاطر RDS ومزاياه وتكاليفه. وقد تمت الاستفادة بكافة هذه التعقيبات في توصيات مجموعة EWG[5] للحصول على نظام من الجيل التالي، المذكور بالتفصيل في هذا التقرير المقدم إلى مجلس إدارة ICANN والغرض منه أن يكون تعقيبًا وإسهامًا مركزًا في عملية وضع السياسة.

## 3. المستخدمين والأغراض

### أ. المنهجية

تمت توصية مجموعة EWG باتخاذ أسلوب نقي وخالص في جهودها لتحديد الجيل التالي من خدمات دليل التسجيل، بدلاً من اقتراح تحسينات على نظام WHOIS الحالي، والذي يعتبر على نطاق واسع غير مناسب. واتساقًا مع توجيه مجلس الإدارة، بدأت مجموعة EWG تحليلها بفحص الأغراض الحالية والمحتملة لجمع وتخزين وتوفير بيانات تسجيل gTLD لتوفير مجموعة متنوعة بشكل واسع من المستخدمين.

ولتحقيق ذلك، قام أعضاء EWG بصياغة مجموعة موسعة من حالات الاستخدام الفعلي التي تشتمل على نظام WHOIS الحالي، وذلك من خلال تحليل كل منهم لتحديد (1) المستخدمين الراغبين في الوصول للبيانات، و(2) المبرر المنطقي للاحتياج لهذا الوصول، و(3) عناصر البيانات التي يحتاجونها و(4) الأغراض التي تحققها هذه البيانات. كما تم استخدام الحالات أيضًا من أجل تحديد سائر أصحاب المصلحة المشاركين في جمع وتخزين وتوفير بيانات التسجيل، بما يساعد مجموعة EWG على فهم تدفقات العمل الحالية والمحتملة بالإضافة إلى الطريقة التي يمكن من خلالها إرضاء هؤلاء المستخدمين وتحقيق احتياجاتهم بأفضل ما يمكن من خلال خدمة دليل التسجيل RDS من الجيل التالي.

ولم يكن الغرض من حالات الاستخدام هذه أن تكون شاملة، ولكن بالأحرى أن تكون ممثلة للعديد من استخدامات نظام WHOIS الحالي، بما يوضح التنوع الكبير في المستخدمين، والاحتياجات وتدفقات العمل. توجد قائمة بحالات الاستخدام التي تناولها مجموعة EWG بالدراسة في الملحق ج.

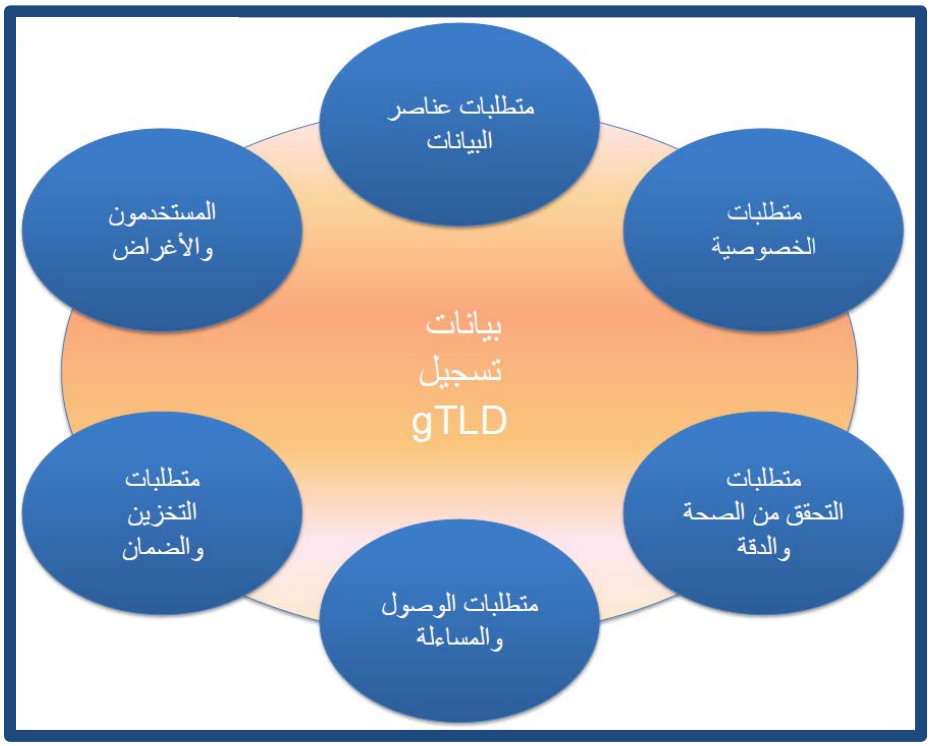
وقد نظرت مجموعة EWG في إجمالي حالات الاستخدام تلك والدروس المستفادة منها من أجل توجيه مجموعة موحدة من أصحاب المصلحة والأغراض المرغوبة التي يجب توفيقها من خلال RDS، بالإضافة إلى مجموعة من حالات إساءة الاستخدام المحتملة والتي يتعين على النظام محاولة إعاقتها (راجع في القسم التالي من هذا التقرير).

---

[5] وعبر هذا التقرير، تستخدم مبادئ EWG المصطلحات التالية، استنادًا إلى التعريفات المحددة في RFC 2119:

- يجب: تعني هذه الكلمة، أو كلمة "يتعين" أو "يلزم" أن التعريف من المطالب المطلقة لهذا التقرير.
- يجب أن لا: تعني هذه العبارة، أو عبارة "لا يجوز" أن التعريف عبارة عن حظر مطلق في هذا التقرير.
- يلزم: هذه الكلمة، أو الصفة "موصى به"، تعني أنه قد تكون هناك أسباب صحيح في ظروف محددة لإغفال بند محدد، إلا أن المتضمنات الكاملة يجب فهمها ووزنها بعناية قبل اختيار مسار مختلف.
- لا يلزم: هذه العبارة، أو العبارة "غير موصى به"، تعني أنه قد تكون هناك أسباب صحيحة في ظروف خاصة عندما يكون هناك سلوك محدد مقبول أو غير مفيد، لكن المتضمنات الكاملة يجب أن تفهم وأن يتم وزن الحالة بعناية قبل تنفيذ أي من أشكال السلوك الموصوفة بهذه الكلمة.

وعلاوة على ذلك، قامت مجموعة EWG باستشارة مواد مرجعية من الأنشطة السابقة ذات الصلة بـ WHOIS، وتعقيبات المجتمع، وحالات الاستخدام في فحص الاحتياجات النوعية في كل من الجوانب الواردة في الشكل 1 أدناه.




**الشكل 1: تحليل الاحتياجات**

واصلت مجموعة EWG عملها من خلال تحليل هذه الأغراض واحتياجات المستخدم من أجل الوصول إلى أقل مجموعة من عناصر البيانات اللازمة لكل غرض، والمخاطر ذات الصلة بجعل هذه البيانات قابلة للوصول، وقانون الخصوص ومتضمنات السياسة الخاص بالقيام بذلك، والأسئلة الإضافية التي تم التقصي عنها في هذا التقرير.

### ب. مستخدمي وأغراض RDS

يسرد الشكل 2 أدناه ملخصًا غير شامل بمستخدمي نظام WHOIS الحالي، بما في ذلك المستخدمين ذوي الأغراض البناءة أو الضارة. واتساقًا مع مهمة وتفويض EWG، تم فحص سائر هؤلاء المستخدمين للتعرف على تدفقات العمل الحالية والمحتملة في المستقبل بالإضافة إلى أصحاب المصلحة والبيانات المشمولة فيها.


**الشكل 2: المستخدمين**

تم في هذا التقرير استخدام اللفظ "مقدم الطلب" للإشارة بشكل عام إلى كل المستخدمين الراغبين في الحصول على بيانات تسجيل gTLD من النظام. ووفقًا لما هو مشروح باستفاضة في هذا التقرير، توصي مجموعة EWG بالتخلي عن نموذج WHOIS الحالي - الذي يعطي لكل مستخدم نفس الوصول العام غير معلوم الهوية لبيانات تسجيل gTLD (غير الدقيقة في الكثير من الأحيان). وبدلا من ذلك، توصي EWG بنقلة نوعية حيث يتم جمع تسجيل بيانات gTLD، والتحقق من صحتها والإفصاح عنها لأغراض مسموح بها فقط، مع بعض عناصر البيانات التي يمكن الوصول إليها من مقدمي الطلبات المصدق عليهم الذين يحاسبون على استخدامهم المناسب.

قامت مجموعة EWG بتحليل حالات الاستخدام الممثلة من أجل وضع القائمة التالية، والتي تلخص أنواع المستخدمين الراغبين في الوصول إلى بيانات تسجيل gTLD، والأساس المنطقي وراء الحاجة إلى الوصول إلى تلك البيانات، والأغراض الكاملة التي تؤديها هذه البيانات. تتوفر مزيد من التفاصيل حول كل مستخدم وغرض واحتياجات البيانات المرتبطة في القسم الثالث (ج)، الأغراض المقرر مواءمتها أو رفضها وأيضًا الملحق د.

| المستخدم | الغرض | مثال على حالات الاستخدام | الأساس المنطقي للوصول إلى بيانات التسجيل |
|---|---|---|---|
| **جميع المسجلين** (على سبيل المثال؛ الأشخاص الطبيعيين، الأشخاص الاعتباريين، موفري خدمات الخصوصية/الوكيل) | التحكم في اسم النطاق | إنشاء حساب تسجيل اسم النطاق | تمكين تسجيل أسماء النطاقات من خلال أي نوع من المسجلين عن طريق إنشاء حساب جديد لدى أمين سجل |
| | | مراقبة تعديل بيانات أسماء النطاقات | التعرف على التعديل العرضي أو غير المستنير أو غير المصرح به لبيانات التسجيل الخاصة بأسماء النطاقات، سواء الحالية أو التاريخية (من خلال استخدام WhoWas). |
| | | إدارة محفظة أسماء النطاقات | تسهيل تحديث كافة بيانات تسجيل أسماء النطاقات (على سبيل المثال، جهات الاتصال المخصصة، والعناوين) للحفاظ على محفظة بأسماء النطاقات |
| | | البدء في نقل أسماء النطاقات | تمكين عملية التحويل التي يقوم بها المسجل لأسماء النطاقات إلى أمين سجل آخر |
| | | حذف أسماء النطاقات | تمكين حذف أسماء النطاقات المنتهية |

| المستخدم | الغرض | مثال على حالات الاستخدام | الأساس المنطقي للوصول إلى بيانات التسجيل |
|---|---|---|---|
| | | تحديث DNS لأسماء النطاقات | تمكين التغيير من جانب المسجل لنظام DNS لأسماء النطاقات |
| | | عمليات تجديد أسماء النطاقات | تمكين تجديد أسماء النطاقات المسجلة من خلال مسجل اسم النطاق |
| | | توثيق عقود أسماء النطاقات | تسهيل التوثيق الأولي والمتواصل لبيانات التسجيل (على سبيل المثال، العقود المخصصة، والعناوين) عن طريق المسجل |
| **مسجلين محميين** (على سبيل المثال، عملاء خدمات الخصوصية/الوكالة الذين يجب الاتصال بهم) | حماية البيانات الشخصية | الاتصال بموفر خدمة الخصوصية/البروكسي | تمكين الاتصال بموفري خدمات الخصوصية أو الوكالة المعتمدين الذين يقدمون خدمات يستخدمها أي مسجل يسعى للحد من الوصول العام للأسماء والعناوين الشخصية |
| | | الاتصال بجهة اعتماد المؤهلات الآمنة | تمكين الاتصال بجهة اعتماد المؤهلات الآمنة التي تعرض خدمات تسجيل يستخدمها أفراد أو مجموعات معرضة لتهديد، من خلال استخدام أدوات الاعتماد آمنة عبر جهة خارجية معتمدة |
| **الفريق الفني للإنترنت** (على سبيل المثال، مديري DNS، ومديري البريد، ومديري الويب وموفري خدمة الإنترنت ISP) | حل المشاكل التقنية | الاتصال بالفريق الفني لأسماء النطاقات | تسهيل الاتصال بالفريق الفني (الأفراد، أو الأدوار أو الكيانات) ممن لهم القدرة على المساعدة في حل المشكلات الفنية أو التشغيلية في أسماء النطاقات (على سبيل المثال حالات تعطل حل DNS، أو مشكلات توصيل البريد الإلكتروني، أو المشكلات الوظيفية في مواقع الويب) |
| **جهات التوثيق** | توثيق أسماء النطاقات | إصدار شهادات أسماء النطاقات | مساعدة هيئات التوثيق (CA) على تحديد المسجل الخاص بأسماء النطاقات بحيث يكون ملتزمًا بشهادة SSL/TLS |
| **مستخدمي الإنترنت الفرديين** (على سبيل المثال، العملاء) | استخدام الإنترنت الفردي | الاتصال الفعلي بالعالم | مساعدة العملاء على الحصول على معلومات الاتصال من غير الإنترنت لمسجل اسم النطاق (على سبيل المثال، عنوان الأعمال) |
| | | حماية المستهلك | توفير وإتاحة آلية خفيضة الوزن للعملاء للاتصال بجهات الاتصال الخاصة بشركات الأعمال المحددة من خلال مسجلي أسماء النطاقات (على سبيل المثال خدمة عملاء موزعي التجزئة عبر الإنترنت) من أجل حل المشكلات سريعًا، دون تدخل LE/OpSec |
| **مستخدمي الإنترنت من شركات الأعمال** (على سبيل المثال، حاملي العلامات التجارية، أو السماسرة، أو الوكلاء) | بيع أو شراء أسماء نطاقات شركات الأعمال | بيع أسماء النطاقات بالوساطة | تمكين العناية الواجبة فيما يتصل بشراء أسماء النطاقات |
| | | مقاصة العلامات التجارية لأسماء النطاقات | تمكين تعريف مسجلي أسماء النطاقات في دعم مخالصة العلامات التجارية (تحليل المخاطر) عند إقرار ماركات جديدة |
| | | الاستحواذ على أسماء النطاقات | تسهيل شراء والاستحواذ على أسماء النطاقات التي تم تسجيلها في السابق من خلال تمكين الاتصال بالمسجل |
| | | الاستعلام عن شراء أسماء النطاقات | تمكين تقرير توافر أسماء النطاقات وجهة الاتصال الحالية للمسجل والمدير (إن وجد) |

| المستخدم | الغرض | مثال على حالات الاستخدام | الأساس المنطقي للوصول إلى بيانات التسجيل |
|---|---|---|---|
| | | السجل التاريخي لتسجيل أسماء النطاقات | توفير سجل بتسجيل أسماء النطاقات للتعرف على المسجلين السابقين والتواريخ من خلال استخدام WhoWas |
| | | أسماء النطاقات لمسجل محدد | تمكين تقرير كافة أسماء النطاقات المسجلة بمعرفة كيان محدد (الاستعلام العكسي) كجزء من توثيق أصول الاندماج/الموافقة |
| **باحثي الإنترنت** | بحث DNS للمصلحة الأكاديمية/العامة | السجل التاريخي لتسجيل أسماء النطاقات | تمكين البحث التاريخي حول تسجيل أسماء النطاقات (WhoWas) خلال أبحاث DNS للمصلحة الأكاديمية/العامة |
| | | أسماء النطاقات لجهة اتصال محددة | تمكين التعرف على هوية كافة النطاقات المسجلة باستخدام اسم محدد أو عنوان أو خادم اسم، أو بيانات تسجيل، إلخ (الاستعلام العكسي) خلال أبحاث DNS للمصلحة الأكاديمية/العامة |
| | | استطلاع مسجل أسماء النطاقات أو جهات الاتصال المخصصة | تمكين استطلاعات مسجلي أسماء النطاقات أو جهات الاتصال المخصصة بها |
| **أصحاب الملكية الفكرية**<br>(على سبيل المثال، حاملي العلامات التجارية، ومالكي العلامات التجارية ومالكي الملكية الفكرية IP) | إجراءات قانونية | اتصال مستخدم اسم النطاق | تمكين الاتصال بالجهة المستخدمة لاسم نطاقات يجري التحري عنه للتعرف على أي انتهاك للعلامة التجارية/الاسم التجاري أو السطو على IP |
| | | محاربة الاستخدام المدلس للبيانات المسجل | تسهيل التعرف والرد على الاستخدام المدلس للبيانات القانونية (على سبيل المثال، العنوان) لأسماء النطاقات التي تخص مسجل آخر من خلال استخدام الاستعلام العكسي أو البيانات الموثقة من خلال الهوية. |
| | | السجل التاريخي لتسجيل أسماء النطاقات | تمكين البحث التاريخي حول تسجيل أسماء النطاقات (WhoWas) خلال بحث انتهاك IP |
| | | أسماء النطاقات لمسجل محدد | تمكين التعرف على هوية كافة النطاقات المسجلة باستخدام اسم أو عنوان محدد (الاستعلام العكسي) من خلال بحث انتهاك IP |
| **محققين غير LEA**<br>(على سبيل المثال، الجهات الضريبية، موفري UDRP، وتوافق ICANN) | الإنفاذ النظامي والتعاقدي | التحري عن الضرائب عن طريق الإنترنت | تسهيل التعرف على جهات الاتصال لأسماء النطاقات المتورطة في البيع عن طريق الإنترنت حسب الجهات الضريبية الوطنية أو التابعة للولاية أو المقاطعة أو الجهات الضريبية المحلية |
| | | إجراءات UDRP | تمكين موفري UDRP من تأكيد هوية المستجيب الفعلي على أسماء النطاقات، وإجراء فحوصات التوافق، وتقرير متطلبات العمليات القانونية والحماية من تغيير ملكية أسماء النطاقات للتملص من النزاعات |
| | | التوافق التعاقدي لنظام RDS البيني | إتاحة الفرصة أمام ICANN لتدقيق الشكاوى والرد عليها حول عدم الامتثال من خلال الجهات المتعاقدة (على سبيل المثال عدم دقة البيانات أو عدم توافرها، وتنفيذ قرار UDRP، وشكاوى التحويل، ومستودعات البيانات واحتجازها) |
| **محققي LEA/OpSec**<br>(على سبيل المثال، وكالات إنفاذ | التحري الجنائي والحد من إساءة استخدام DNS | التحري عن إساءة استخدام أسماء النطاقات | تمكين التحري الفعال والتحري عن الأدلة من خلال فريق LEA/OpSec بالرد على ما يزعم من أسماء نطاقات مسجلة بشكل ضار، بما في ذلك فحص البيانات التاريخية |

| المستخدم | الغرض | مثال على حالات الاستخدام | الأساس المنطقي للوصول إلى بيانات التسجيل |
|---|---|---|---|
| القانون، وفرق الرد على الحوادث) | | التحري عن الأنشطة الجنائية غير المتصلة بالإنترنت | تمكين التحري الفعال والتحري عن الأدلة من خلال فريق LEA/OpSec بالرد على النشاط الجنائي غير المتصل بالإنترنت من خلال توفير بيانات التسجيل التفصيلية و/أو البحث عن أسماء النطاقات المسجلة لمشتبه به (الاستعلام العكسي) |
| | | خدمات السمعة لأسماء النطاقات | تمكين تحليل القوائم البيضاء/السوداء لأسماء النطاقات بمعرفة موفري خدمات السمعة |
| | | التحري عن الأنشطة الجنائية المتصلة بالإنترنت | مساعدة الضحايا أو مستشاريهم القانونيين من التعرف على مسجل اسم النطاق المتورط في أنشطة قد تكون غير قانونية في تمكين مزيد من التقصي بمعرفة LE/OpSec |
| | | إساءة استخدام جهات الاتصال لأسماء النطاقات الضعيفة | المساعدة في تسوية أسماء النطاقات المعرضة للخطر من خلال مساعدة فريق LEA/OpSec على الاتصال بالمسجل أو جهة الاتصال المحددة بإساءة الاستخدام |
| **الجمهور العام** (على سبيل المثال، المدونين، وسائط الإعلام، النشطاء السياسيين) | شفافية DNS | الولوج إلى بيانات التسجيل العامة | تحديد المؤسسة التي تقف "وراء" اسم نطاق، وفقًا لما هو مرغوب بشكل مشترك من خلال مجموعة متنوعة وواسعة من مستخدمي الإنترنت غير الواضح بشكل آخر في حالات الاستخدام الأكثر خصوصية |
| **الأوغاد** (على سبيل المثال، المتورطون في الرسائل غير المرغوبة، DDoS، أو الاحتيال، أو السطو على الهوية، أو قرصنة النطاقات) | أنشطة الإنترنت الضارة | السطو على أسماء النطاقات | جمع بيانات تسجيل النطاقات من أجل الحصول على وصول غير قانوني لحساب المسجل والسطو على اسم (أسماء) النطاقات الخاصة بالمسجل تلك |
| | | تسجيل أسماء النطاقات الضارة | استخدام حساب تسجيل لأسماء النطاقات الحالية/الضعيفة من أجل تسجيل أسماء جديدة لدعم الأنشطة الإجرامية أو التدليسية أو المسيئة |
| | | التنقيب عن بيانات التسجيل للتعرف على الرسائل غير المرغوبة/التدليس | جمع بيانات مسجل اسم النطاق للتعرف على الاستخدام الضار من جانب مرسلي الرسائل غير المرغوبة، والمدلسين وغيرهم من المجرمين (الأوغاد) |

**الجدول 1. مستخدمي وأغراض RDS**

### ج. الأغراض المقرر تسويتها أو حظرها

سعت مجموعة EWG إلى وضع وتحديد الأولويات بالنسبة للأغراض الموضحة أعلاه من أجل التركيز على تطوير حالات الاستخدام وتضييق نطاق الأغراض المسموح بها. وعلى الرغم من ذلك، كان من الصعب تحديد أساس منطقي لتسوية احتياجات بعض المستخدمين الذي يقومون بالوصول إلى نظام WHOIS الحالي اليوم وليس غيرهم، طالما كانت أغراضهم غير ضارة. وقد أدت النتائج إلى حمل مجموعة EWG على التوصية بوجوب تسوية كافة الأغراض المسموح به والمحددة من خلال RDS بطريقة ما، باستثناء أنشطة الإنترنت المعروف أنها ضارة ويجب إعاقتها بشكل فعال. وأوصت مجموعة EWG بالأغراض المسموح بها ومن ثم فإنها ملخصة فيما يلي.


**الشكل 3: الأغراض المسموح بها**

يجب ملاحظة أنه في إطار كل غرض هناك عدد غير محدود من حالات الاستخدام الحالية أو المحتملة في المستقبل. وعلى الرغم من أن EWG لم تحاول تحديد كافة حالات الاستخدام المحتملة، إلا أنها حاولت التعرف على عينة تمثيل أملاً في التعريف القوي بأنواع المستخدمين وأغراضهم في الرغبة في الحصول على بيانات تسجيل gTLD. وعلى الرغم من ذلك، يجب تصميم RDS بحيث تكون له القدرة على تسوية المستخدمين الجدد والأغراض المسموح به والتي قد تظهر بمرور الوقت.

حيث إن مجموعة EWG قامت بتحليل حالات الاستخدام الموضحة في الملحق ج، أضحى من الواضح أن العديد من المستخدمين لديهم احتياجات لنفس عناصر البيانات، لكن من أجل تحقيق أغراض مختلفة. وبعض هذه الاحتياجات مفهومة جيدًا، على سبيل المثال:

- القدرة على تحديد ما إذا كان اسم النطاق قد تم تسجيله أم لا
- القدرة على تحديد الحالة الراهنة لأي نطاق
- القدرة على الاتصال بشخص ما حول اسم النطاق

وعلى الرغم من ذلك، بعض الاحتياجات مشتركة ولم يتم تنفيذها حاليًا من خلال نظام WHOIS الحالي بطريقة متسقة. والأمثلة على ذلك تشمل ما يلي:

- القدرة على تحديد كافة النطاقات المسجلة من خلال جهة محددة (والمشار إليها بشكل عام بلفظ WHOIS العكسية)

- القدرة على تحديد معلومات التسجيل التاريخية الخاصة باسم نطاق (والمشار إليها بشكل عام بلفظ WhoWas)

وقد وضعت مجموعة EWG هذه الاحتياجات المشتركة في الاعتبار عند وضع توصيات RDS المشار إليها بالتفصيل في هذا التقرير. وعلى الرغم من ذلك، حيث إنه من المحتمل إمكانية تحديد مزيد من الاحتياجات المشتركة بمرور الوقت، فإن أي نظام من الجيل التالي يجب تصميمه مع وضع إمكانية التوسع في الاعتبار. علمًا بأن الأغراض المسموح بها المحددة في الوقت الحالي لمجموعة EWG وبيانات التسجيل المرتبطة وجهات الاتصال واحتياجات الاستعلام موضحة باستفاضة أدناه.

| الغرض | التعريف |
|---|---|
| **التحكم في اسم النطاق** | تشمل المهام في نظام هذا الغرض كل من إنشاء وإدارة ومراقبة اسم النطاق الخاص بالمسجل ((DN، بما في ذلك إنشاء DN، وتحديث المعلومات حول DN، وتحويل DN، وتجديد DN، وحذف DN، والحفاظ على محفظة DN، واكتشاف الاستخدام التدليسي لمعلومات الاتصال الخاصة بالمسجل. وهذا يشتمل ضمنًا على أن كل مسجل يجب أن يكون مستخدم RDS معتمد لهذا الغرض، وأن تكون له القدرة على الوصول إلى كافة المعلومات العامة والتي يمكن الوصول إليها عن طريق بوابات في نظام RDS حول اسم النطاق DN الخاص بها، بما في ذلك بيانات الاتصال المحددة المنشورة في نظام RDS لاسم النطاق DN هذا. |
| **حماية البيانات الشخصية** | تشمل المهام في نطاق هذا الغرض تحديد موفر خدمة الخصوصية/البروكسي المعتمد المرتبط باسم DN والإبلاغ عن إساءة الاستخدام، والمطالبة بالكشف عن، أو الاتصال بموفر الخدمة. ولتحقيق هذه المهام، يجب على المستخدم أن يتصل بمصداقية وسهولة بموفر خدمة الخصوصية/البروكسي - على سبيل المثال، من خلال اتباع عنوان URL لإساءة الاستخدام لجهة اتصال PBC الخاصة بموفر خدمة الخصوصية/البروكسي لصفحة تصف عملية الكشف الخاصة بموفر الخدمة أو تسمح للمستخدم تقديم نموذج طلب كشف. |
| **حل المشاكل التقنية** | تشمل المهام في نطاق هذا الغرض العمل على حل المشكلات الفنية المرتبطة باستخدام اسم النطاق، ويشمل ذلك مشكلات إرسال البريد الإلكتروني، وتعطل حل DNS، والمشكلات الوظيفية لمواقع الويب. ولتنفيذ هذه المهام، يحتاج المستخدم للقدرة على الاتصال بفريق العمل الفني المسئول عن التعامل مع هذه المشكلات. (ملاحظة: قد يكون من المفيد تحديد نقاط اتصال متعددة للتعامل مع أنواع المشكلات المختلفة - على سبيل المثال، مسئول البريد لمشكلات البريد الإلكتروني). |
| **توثيق أسماء النطاقات** | تشمل المهام داخل نطاق هذا الغرض قيام جهة توثيق (CA) بإصدار شهادة X.509 لجهة محددة باسم نطاق. لتحقيق هذه المهمة، يتعين على المستخدم تأكيد أن اسم النطاق DN مسجل للجهة المرخصة؛ ويتطلب القيام بذلك الوصول إلى كافة البيانات العامة والمحددة من خلال بوابات حول المسجل. |
| **الاستخدام الفردي للإنترنت** | تشمل المهام داخل نطاق هذا الغرض تعريف المؤسسة من خلال استخدام اسم نطاق من أجل غرس ثقة العملاء، أو الاتصال بتلك المؤسسة من أجل رفع شكوى للعملاء إليهم أو تقديم شكوى حولهم. ولتحقيق هذه المهام، يحتاج المستخدم إلى اسم المؤسسة (يفضل أن تكون موثقة الهوية) وعنوانها القانوني (البريدي)، ويمكنها الاستفادة من اتباع عنوان URL لجهة الاتصال لصفحة تصف المؤسسة وجهات الاتصال الخاصة بخدمة العملاء أو السماح للمستخدم بتقديم استعلام عن خدمة العملاء. |
| **بيع أو شراء أسماء نطاقات شركات الأعمال** | تشمل المهام في نطاق هذا الغرض تقديم استعلامات شراء حول اسم DN، والاستحواذ على اسم DN من مسجل آخر، وتمكين بحث العناية الواجبة. ولتحقيق هذه المهام، يحتاج المستخدم إلى وصول إلى مؤسسة المسجل وعنوان البريد الإلكتروني، وفي بعض الحالات بيانات إضافية عن طريق بوابة - على سبيل المثال، لأداء استعلام عكسي على اسم مسجل أو جهة اتصال من أجل تحديد أسماء النطاقات الأخرى التي ترتبط بها. |

| الغرض | التعريف |
|---|---|
| **بحث DNS للمصلحة الأكاديمية/العامة** | تشمل المهام في نطاق هذا الغرض دراسات بحثية للمصلحة العامة الأكاديمية حول أسماء النطاقات المنشورة في RDS، بما في ذلك المعلومات العامة حول المسجل وجهات الاتصال المعينة، وتاريخ وحالة اسم النطاق، وأسماء النطاقات المسجلة من خلال مسجل محدد (الاستعلام العكسي). لتحقيق هذه المهام، يحتاج المستخدم للقدرة على الوصول إلى كافة البيانات العامة في نظام RDS وفي بعض الحالات قد يحتاج للوصول إلى بيانات عن طريق بوابة من أجل الاستخدام بصيغة مجهّلة الهوية وتجميعية. |
| **إجراءات قانونية** | تشمل المهام في نطاق هذا الغرض التحري عن الاستخدام التدليسي المحتمل لاسم أو عنوان المسجل من خلال أسماء نطاقات أخرى، والتحري عن الانتهاكات المحتملة للعلامات التجارية، والاتصال بممثل قانوني لمسجل/مرخص له وذلك قبل اتخاذ إجراء قانوني ومن ثم اتخاذ إجراء قانوني إذا لم يتم التعامل بشكل مرضي مع المسألة. ولتنفيذ هذه المهام، يحتاج المستخدم للقدرة على الاتصال بالممثل القانونين للمسجل/المرخص له، دون الترحيل عبر موفر خدمة خصوصية/بروكسي معتمد. |
| **الإنفاذ النظامي والتعاقدي** | تشمل المهام في نطاق هذا الغرض تقصي الجهات الضريبية لشركات الأعمال ذات التواجد على الإنترنت، والتحري عن UDRP، والتحري عن الامتثال التعاقدي، وعمليات تدقيق مستودعات بيانات التسجيل. ولتحقيق ذلك، يحتاج المستخدم المعتمد للوصول إلى بعض عناصر بيانات جهة الاتصال وعناصر بيانات DN عبر بوابة، مثل العنوان البريدي ورقم الهاتف، حسب ما يتناسب للغرض المحدد. على سبيل المثال، قد تحتاج WIPO إلى الوصول إلى حل UDRP. |
| **التحري الجنائي والحد من إساءة استخدام DNS** | تشمل المهام في نطاق هذا الغرض الإبلاغ عن إساءة استخدام شخص ما يمكنه التقي والتعامل مع إساءة الاستخدام هذه، أو الاتصال بالكيانات ذات الصلة باسم نطاق خلال التحري الجنائي غير المتصل بالشبكة. ولتحقيق هذه المهام، يحتاج المستخدم المعتمد (مثل وكيل إنفاذ القانون، أو جهة الرد الأولى) للوصول سريعًا وبموثوقية إلى جهة اتصال إساءة الاستخدام المسئولة عن اسم النطاق المرتبط - على سبيل المثال، من خلال اتباع عنوان URL لوصف عملية إبلاغ عن إساءة استخدام أو نموذج تقرير حوادث. |
| **شفافية DNS** | تشمل المهام في إطار هذا الغرض الاستعلام عن بيانات التسجيل المعلنة للجمهور من خلال المسجلين من أجل تحقيق مجموعة متنوعة وكبيرة من حالات الاستخدام حول إطلاع الجمهور العام. ولتحقيق هذه المهام، يحتاج المستخدم لوصول سهل إلى البيانات العامة (والبيانات العامة فقط) التي يمكن توفيرها من خلال RDS. يجب إطلاع المسجلين على أن البيانات العامة الخاصة بتسجيل أسماء النطاقات الخاصة بهم يمكن استخدامها لهذا الغرض "العام"، ويجب أن يقتصر هذا الغرض على البيانات العامة (أي، هذا الغرض لا يسمح بالوصول إلى البيانات عن طريق بوابات). |

**الجدول 2. تعريفات الغرض**

تحتوي الجدول التالي على تلخيص مستفيض لنطاق بيانات التسجيل اللازم لتحقيق هذه الأغراض، بما في ذلك أسماء النطاقات المشاركة، ونوع البيانات اللازمة (بيانات المسجل، وبيانات جهة الاتصال، وبيانات اسم النطاق)، والاستعلامات الإضافية اللازمة.

| الغرض | نطاق الاستعلام | جهة (جهات) الاتصال المطلوبة | بيانات المسجل المطلوبة | بيانات DN | استعلامات أخرى مطلوبة |
|---|---|---|---|---|---|
| **التحكم في اسم النطاق** | اسم النطاق المملوك | وكل | عامة+عن طريق بوابة | نعم | عكسي (البيانات الخاصة) WhoWas (اسم النطاق المملوك) |
| **حماية البيانات الشخصية** | PP DN* | PP | عام | نعم | لا يوجد |
| **حل المشاكل التقنية** | أي DN | فني | عام | نعم | لا يوجد |
| **توثيق أسماء النطاقات** | أي DN | لا يوجد | عامة+عن طريق بوابة | نعم | لا يوجد |
| **مستخدم فردي للإنترنت** | LP DN* | أعمال | عام | لا | لا يوجد |
| **بيع أو شراء أسماء نطاقات شركات الأعمال** | أي DN | مشرف | عام+ معتمد عن طريق بوابة | نعم | عكسي (بيانات معتمدة) WhoWas (أي DN) |
| **بحث DNS للمصلحة الأكاديمية/العامة** | أي DN | وكل | عام+ موافق عليه عن طريق بوابة | نعم | عكسي (بيانات معتمدة) WhoWas (أي DN) |
| **إجراءات قانونية** | أي DN | القسم القانوني | عام+ موافق عليه عن طريق بوابة | نعم | عكسي (بيانات معتمدة) WhoWas (أي DN) |
| **الإنفاذ النظامي والتعاقدي** | أي DN | القسم القانوني | عامة+عن طريق بوابة | نعم | عكسي (أية بيانات) WhoWas (أي اسم النطاق) |
| **التحري الجنائي والحد من إساءة استخدام DNS** | أي DN | الإساءة | عامة+عن طريق بوابة | نعم | عكسي (أية بيانات) WhoWas (أي DN) |
| **شفافية DNS** | أي DN | | عام | نعم | لا يوجد |

**الجدول 3. نطاق بيانات التسجيل اللازمة لكل غرض**

في الجدول 3، يمكن تعريف "بيانات البوابة المعتمدة" بشروط الخدمة التي يمكن لمستخدم RDS المعتمدين تطبيقها عليها، مع مراعاة السياسات المحددة التي تغطي:

- من المؤهل للوصول عبر بوابات
- أسباب شرعية للاحتياج لتلك البيانات
- قيود على استخدام تلك البيانات
- الإشراف المطلوب من أجل ضمان الاستخدام المناسب

هذه الأغراض التي تتطلب "بيانات بوابة معتمدة" بحاجة إلى مزيد من التحليل، بالتشاور مع تلك المجتمعات من مستخدمي RDS، لتحديد الطريقة التي يمكن من خلالها تعريف وتنفيذ وإنفاذ هذه السياسات بشكل معقول، مع موازنة الاحتياجات الخاصة بالمساءلة والخصوصية. وعلى الرغم من ذلك، تم تقديم الأمثلة التالية من أجل توضيح الطريقة التي قد يعمل بها هذا:

- **بحث DNS للمصلحة الأكاديمية/العامة** قد يشتمل على باحث من جامعة معترف بها، مشارك في دراسة محددة لنظام DNS، قام بإحصاء عناصر البيانات عبر البوابة اللازمة والطريقة التي سيتم استخدامها بها، والموافقة على نشر النتائج فقط في شكل مجمع/مجهّل الهوية، مع مراعاة إشراف مجلس مراجعة مستقل (IRB). بعد الحصول على الموافقة على إجراء "بحث DNS للمصلحة العامة"، قد يحق لمستخدمة RDS المعتمد الاطلاع على بعض عناصر بيانات المسجل عبر بوابة أو الاستعلام على عناصر البيانات تلك في استعلام عكسي.
- **بيع/شراء DN** قد يشتمل التحري عن ذلك على مستخدم أعمال، مشارك في معاملة تجارية تتطلب عناية واجبة حول أصول أسماء النطاقات المملوكة لبائع. من خلال المراقبة والإشراف عن طريق هيئة اعتماد (محددة في القسم الرابع (ج)، اعتماد مستخدم RDS)، يمكن لهذا المستخدم الشهادة بأنه ليس فقط مشارك في شراء اسم نطاق، لكن أيضًا بيانات RDS مطلوبة لتمكين العناية الواجبة حول البائع "س" وسوف تستخدم النتائج لهذا الغرض الخاص فقط. بعد الموافقة على استخدام DNS في أداء هذا النوع من العناية الواجبة، قد يكون لمستخدم RDS المعتمد الحق في استخدام الاستعلامات العكسية للبحث عن أسماء النطاقات باستخدام البيانات المعتمدة عبر بوابة والمرتبطة بالبائع "س" وفقًا لما هو موضح بمزيد من التفصيل في الملحق هـ.
- قد يشتمل التحري عن **الإجراءات القانونية** على محامي مرخص مشارك في عمل تحري عن انتهاك العلامات التجارية. من خلال المراقبة والإشراف عن طريق هيئة اعتماد (محددة في القسم الرابع(ج)، اعتماد مستخدم RDS)، يمكن لهذا المستخدم الشهادة بأنه ليس فقط يتحرى عن إجراء قانوني محتمل، إلا أن بيانات RDS يجري طلبها من أجل تمكين التحري عن الجهة "ص" وكافة البيانات الناتجة عن ذلك سوف يتم استخدامه فقط لهذا الغرض المحدود. بعد الموافقة على استخدام DNS في أداء هذا النوع من التحري عن انتهاك العلامات التجارية، قد يكون لمستخدم RDS المعتمد الحق في استخدام الاستعلامات العكسية للبحث عن أسماء النطاقات باستخدام البيانات المعتمدة عبر بوابة والمرتبطة بالجهة "س" وفقًا لما هو موضح بمزيد من التفصيل في الملحق هـ.

ولتوضيح البيانات المشاركة في هذه الأغراض، ودور البيانات المعتمدة عن طريق بوابات، وأشكال الحماية التي يمكن إنفاذها لتحميل المستخدمين المسئولية عن إساءة الاستخدام والحد منها، راجع الملحق هـ، توضيحات الوصول عن طريق بوابات والوصول غير المصادق عليه.

وقد أدى هذا التقصي عن مستخدمي RDS والأغراض المسموح بها إلى حمل مجموعة EWG على صياغة المبادئ التأسيسية التالية لتمكين الوصول المستند إلى الأغراض لبيانات التسجيل:

| رقم. | مبادئ الأغراض المسموح بها |
|---|---|
| .1 | يجب على ICANN أن تضع، وفي مكان واحد، سياسة سهلة الاستخدام تصف الغرض من الاستخدامات المسموح بها لبيانات التسجيل، من أجل إطلاع المسجلين بوضوح عن السبب وراء جمع هذه البيانات والطريقة التي سيتم التعامل بها معها واستخدامها. |
| .2 | كما يجب أن تكون هناك استخدامات محددة مسموح/غير مسموح بها لنظام RDS. |
| .3 | ويجب أن يدعم RDS الأغراض المسموح بها والمحددة، بما في ذلك الاستخدامات التي تشتمل على ما يلي:<br>• تحديد هوية المسجل وجهات الاتصال المخصصة لغرض محدد؛<br>• التواصل مع جهات الاتصال المخصصة لغرض محدد؛<br>• استخدام البيانات التي نشرتها السجلات حول أسماء النطاقات<br>• البحث عن أقسام بيانات التسجيل اللازمة لغرض محدد. |
| .4 | يجب تصميم RDS بحيث تكون له القدرة على تسوية المستخدمين الجدد والأغراض المسموح به والتي قد تظهر بمرور الوقت.<br>• يجب تحديد عملية تقديم الطلبات.<br>• ويجب مراجعة الطلبات في مقابل معايير محددة<br>• وبالنسبة للطلبات التي تجتاز المراجعة فيجب تقييمها واعتمادها بمعرفة مجلس مراجعة من أصحاب مصلحة متعددين وفقًا لما يتقرر من خلال عملية وضع السياسة<br>• يجب إضافة الطلبات المعتمدة إلى سياسة خصوصية RDS ووضع جدول زمني للتنفيذ بصفة دورية (على سبيل المثال، كل ربع سنة، سنويًا) وفقًا لما يتحدد من خلال السياسة<br>ملاحظة: راجع القسم السادس عناصر البيانات للتعرف على عملية لإضافة عناصر بيانات جديدة. |
| .5 | يجب تسوية كافة الأغراض المسموح به والمحددة من خلال RDS بطريقة ما، باستثناء أنشطة الإنترنت المعروف أنها ضارة ويجب إعاقتها بشكل فعال. ويحتوي الجدول 1، مستخدمي وأغراض RDS، على تلخيص للأغراض المسموح بها من مجموعة EWG، والشكل 3، الأغراض المسموح بها. |
| .6 | يجب جمع بيانات تسجيل gTLD والتحقق من صحتها والإفصاح عنها فقط لأغراض مسموح بها فقط، مع إمكانية الاطلاع على بعض عناصر البيانات فقط لمقدمي الطلبات المصدق عليهم على أن يتحملوا بعد ذلك المسئولية عن الاستخدام المناسب. |
| .7 | يجب أن تكون لكل مسجل القدرة على الوصول إلى كافة المعلومات العامة والتي يمكن الوصول إليها عن طريق بوابات والمنشورة في نظام RDS حول اسم النطاق الخاص بها، بما في ذلك بيانات الاتصال المحددة. |

### د. أصحاب المصلحة المشاركين في RDS

توفر القائمة التالية ملخصًا تمثيليًا بمختلف أصحاب المصلحة المشاركين في جمع وتخزين والكشف عن واستخدام بيانات تسجيل gTLD، للأغراض المرتبطة بها. يقوم بعض أصحاب المصلحة بتوفير البيانات (على سبيل المثال؛

المسجلين)، في حين يقوم آخرون بجمع/تخزين البيانات (على سبيل المثال؛ جهات التوثيق وأمناء السجلات، والسجلات) أو الإفصاح عن البيانات (على سبيل المثال موفر خدمة RDS، أو موفري خدمة الخصوصية/الوكالة المعتمدين). وعلى الرغم من ذلك، فإن غالبية أصحاب المصلحة عبارة عن أطراف مشاركين في بدء طلبات الحصول على البيانات (على سبيل المثال، مالكي الماركات التجارية، ووكلائهم) أو الأطراف المحددين، أو المتعاقدين أو حتى المتضررين من البيانات المفصح عنها (على سبيل المثال، جهات اتصال إساءة استخدام أسماء النطاقات). وهذا الملخص من المقرر له توضيح عمق واتساع أصحاب المصلحة الذين يتأثرون أكثر بخدمة RDS. وعلى الرغم من ذلك، وفي أي معاملة محدد تنطوي على بيانات تسجيل، قد يكون هناك أصحاب مصلحة إضافيين لم يتم حصرهم هنا.

| أصحاب المصلحة | الأغراض |
|---|---|
| **إساءة استخدام جهات الاتصال لأسماء النطاقات** | التحري الجنائي والحد من إساءة الاستخدام |
| **الأطراف الأخرى الساعية للاتصال** | الإجراءات القانونية<br>حماية البيانات الشخصية |
| **الباحث** | بحث DNS للمصلحة الأكاديمية/العامة |
| **التزام ICANN** | الإنفاذ التنظيمي/التعاقدي |
| **السجل** | جميع الأغراض |
| **الشخص/الهوية قيد التحري** | الإنفاذ التنظيمي/التعاقدي |
| **الشركة المستحوذة** | بيع أو شراء أسماء نطاقات شركات الأعمال |
| **العملاء المشترين للسلع من مواقع الويب** | مستخدم فردي للإنترنت |
| **المبلّغ عن المشكلة** | حل المشاكل التقنية |
| **المسجل** | جميع الأغراض |
| **الموزع** | التحكم في أسماء النطاقات<br>التحري الجنائي والحد من إساءة الاستخدام |
| **أعضاء هيئة UDRP** | الإنفاذ التنظيمي/التعاقدي |
| **أمين السجل** | بيع أو شراء أسماء نطاقات الأعمال<br>التحكم في أسماء النطاقات<br>بحث أسماء DNS للمصلحة العامة<br>استخدام الإنترنت الفردي<br>الإجراءات القانونية<br>حماية البيانات الشخصية<br>الإنفاذ التنظيمي/التعاقدي<br>حل المشكلات الفنية<br>التحري الجنائي والحد من إساءة الاستخدام |
| **جهات اتصال الأعمال المدرجة** | استخدام الإنترنت الفردي<br>التحكم في أسماء النطاقات<br>بحث DNS للمصلحة الأكاديمية/العامة |
| **جهات اتصال المشرفين المدرجة** | الإنفاذ النظامي/التعاقدي<br>بيع/شراء أسماء النطاقات<br>التحكم في أسماء النطاقات<br>بحث DNS للمصلحة الأكاديمية/العامة |
| **جهات اتصال إساءة الاستخدام المدرجة** | التحري الجنائي والحد من إساءة الاستخدام<br>التحكم في أسماء النطاقات<br>بحث DNS للمصلحة الأكاديمية/العامة |
| **جهات الاتصال الفنية المدرجة** | حل المشكلات الفنية<br>التحكم في أسماء النطاقات<br>بحث DNS للمصلحة الأكاديمية/العامة |
| **جهات الاتصال القانونية المدرجة** | الإجراءات القانونية<br>الإنفاذ النظامي/التعاقدي<br>بحث DNS للمصلحة الأكاديمية/العامة |
| **جهات الاتصال القانونية للمسجل** | الإجراءات القانونية<br>الإنفاذ التنظيمي/التعاقدي |
| **جهة اعتماد المؤهلات الآمنة** | حماية البيانات الشخصية |

| أصحاب المصلحة | الأغراض |
|---|---|
| **جهة الاتصال بموفر خدمة الخصوصية/البروكسي المدرجة** | حماية البيانات الشخصية<br>التحكم في أسماء النطاقات<br>بحث DNS للمصلحة الأكاديمية/العامة |
| **جهة التوثيق** | جميع الأغراض |
| **جهة التوثيق** | توثيق أسماء النطاقات |
| **حامل الاسم التجاري** | الإنفاذ التنظيمي/التعاقدي |
| **خدمات توثيق العناوين** | التحكم في اسم النطاق |
| **دراسة رعاية المنظمات** | بحث أسماء DNS للمصلحة العامة |
| **ضحية التدليس** | إجراءات قانونية |
| **ضحية إساءة الاستخدام** | التحري الجنائي والحد من إساءة الاستخدام |
| **عميل خدمة الخصوصية/الوكالة** | شراء أو بيع أسماء نطاقات شركات الأعمال<br>التحكم في أسماء النطاقات<br>حل المشكلات الفنية<br>الإنفاذ التنظيمي/التعاقدي<br>حماية البيانات الشخصية |
| **فريق إنفاذ القانون** | التحري الجنائي والحد من إساءة الاستخدام<br>الإجراءات القانونية |
| **فريق عمل الوكالة الحكومية** | الإنفاذ التنظيمي/التعاقدي |
| **مالك الاسم التجاري** | بيع أو شراء أسماء نطاقات شركات الأعمال |
| **متلقي المؤهلات الآمنة** | حماية البيانات الشخصية |
| **مجلس مراجعة مستقل (IRB)** | بحث DNS للمصلحة الأكاديمية/العامة |
| **محقق** | مستخدم فردي للإنترنت |
| **مزود استضافة الويب** | حل المشاكل التقنية |
| **مزود الخدمة عبر الإنترنت** | حل المشاكل التقنية |
| **مزود خدمة إدارة الأسماء التجارية** | التحكم في اسم النطاق |
| **مزودو خدمة Op/Sec** | التحري الجنائي والحد من إساءة الاستخدام |
| **مزودو خدمة الإنترنت** | حل المشكلات الفنية<br>التحري الجنائي والحد من إساءة الاستخدام |
| **مستخدمو الإنترنت المطلعين على موقع الويب** | مستخدم فردي للإنترنت |
| **مشتري النطاقات** | بيع أو شراء أسماء نطاقات شركات الأعمال |
| **مقدم الشكوى** | الإنفاذ التنظيمي/التعاقدي |
| **من يحل المشكلة** | حل المشاكل التقنية |
| **موفر RDS** | جميع الأغراض |
| **موفر UDRP** | الإنفاذ التنظيمي/التعاقدي |
| **موفر خدمة الخصوصية/الوكالة** | التحري الجنائي والحد من إساءة الاستخدام<br>بيع أو شراء أسماء نطاقات الأعمال<br>التحكم في أسماء النطاقات<br>بحث أسماء DNS للمصلحة العامة<br>حل المشكلات الفنية<br>الإجراءات القانونية<br>حماية البيانات الشخصية<br>الإنفاذ التنظيمي/التعاقدي<br>حل المشكلات الفنية |
| **هدف الإجراءات القانونية/المدنية** | مستخدم فردي للإنترنت |
| **وسيط النطاقات** | بيع أو شراء أسماء نطاقات شركات الأعمال |
| **وكلاء المسجل** | التحكم في اسم النطاق |
| **وكلاء/محامو الشركة المستحوذة** | بيع أو شراء أسماء نطاقات شركات الأعمال |
| **وكيل ضحية التدليس** | إجراءات قانونية |

**الجدول 4. ملخص تمثيلي لأصحاب المصلحة**

### ه. مبادئ الاتصال المستندة إلى الأغراض

وجود واستخدام أسماء نطاقات الإنترنت داخل النطاقات العامة يؤدي إلى إيجاد تأثيرات خارجية محتملة على الجهات الأخرى في جميع أنحاء العالم. من السلوك المسيء إلى المشكلات الفنية إلى انتهاكات الحقوق ومشكلات أسماء النطاقات الكبيرة والصغيرة، هناك أسباب عدة قد تجعل أي جهة أخرى في أي مكان في العام بحاجة قانونية للاتصال بشخص أو مؤسسة مرتبطة باسم نطاق معين.

وفي نفس الوقت، قد يرغب مسجلو أسماء النطاقات ويكون من حقهم الحصول على الخصوصية (استنادًا إلى اختصاصهم القضائي المحلي). وقد لا يرغبون في الإعلان صراحة عن تفاصيل الاتصال الخاصة بهم. وعلاوة على ذلك، غالبًا لا يكون المسجلون الشخص أو الكيان الأفضل في حل أية مشكلة يتم طرحها من خلال جهة أخرى -- على سبيل المثال، المشكلات ذات الصلة بتكوين DNS لاسم نطاق أو الرد على خلاف يتعلق بعلامة تجارية. ولذلك، فإن تقديم معلومات المسجل وحدها قد لا يكون كافيًا للجهات الأخرى الساعية لحل المشكلات المرتبطة باسم نطاق.

وسوف تتطلب الطبيعة المتنوعة للمشكلات المحتملة ردودًا متباينة - من حيث المحتوى والإطار الزمني - للمشكلات التي غالبًا ما تحل منطقيًا من خلال أشخاص مختلفين و/أو منظمات مرتبطة بنطاق محدد. وبرغم ذلك، وعلى الأقل يجب على أي اسم نطاق أن تكون له جهة اتصال واحدة أو أكثر منشورة أمام الجمهور ودقيقة ويمكن الوصول إليها بحيث يمكنها الرد على الاستعلامات الخارجية وتوفير نقاط مرجعية للردود المسموح بها للجهات الفاعلة الخارجية المتأثرة بوجود أو عمليات أسماء النطاقات.

وقد يكون الالتزام الزمني للرد هدفًا مرغوبًا بالنسبة لصناعة السياسات لأنواع محددة من جهات الاتصال. وعلى الرغم من ذلك، يجب موازنة الهدف في مقابل الأعباء التي قد تنشأ عن متطلبات الرد على الكيانات التي تحقق تلك الأهداف. يجب أن لا يؤدي إدخال الألعاب في النظام، أو الطلبات غير المناسبة أو التحميل المفرط المتعمد لجهات الاتصال إلى أية جزاءات على جهات الاتصال تلك. ومن المرغوب بالنسبة لمقدمي الطلبات أن تكون لديهم عملية لتصعيد الاتصالات الفاشلة بهجة اتصال غير مستجيبة لأغراض محددة (على سبيل المثال؛ التعامل مع مشكلات إساءة الاستخدام، أو الرد على تقديم قضايا UDRP). والعجز عن الرد على هذه العملية ربما يؤدي إلى تعليق و/أو حذف جهة الاتصال تلك وربما اسم (أسماء) النطاقات المتأثرة في عملية مشفرة. وعلى الرغم من ذلك، فإن أهداف السياسة المحددة للتحديد الزمني للردود تتجاوز نطاق هذا التقرير.

| رقم. | مبادئ الاتصال المستندة إلى الأغراض |
|---|---|
| .8 | يجب توفير جهة اتصال واحدة على الأقل مستندة للأغراض (PBC) لكل اسم نطاق مسجل يقوم بالإعلان عن وحدة كافة عناصر البيانات الإلزامية لسائر جهات اتصال PBC الإلزامية. ويجب أن تكون PBC هذه دقيقة من الناحية التركيبية ويمكن الوصول إليها من الناحية التشغيلية لتحقيق احتياجات كل غرض مسموح به مشفر. |
| .9 | وخلال تسجيل أسماء النطاقات، يجب استخدام جهة اتصال المسجل[6] باعتباره معرف PBC الافتراضي لكل غرض. ويجب إطلاع المسجل على كافة الأغراض المسموح بها وأن تعطى له الفرصة لتأسيس معرفات PBC أخرى لكل غرض، بما في ذلك استبدال معرف اتصال المسجل لأي وجميع الأغراض. |

6 ومعرفات جهات الاتصال عبارة عن معرفات مرتبطة بمجموعات بيانات الاتصال من أجل تمكين الاستعادة والتحديث، والمطروحة في القسم الرابع (أ)، عناصر البيانات، والمعرفة في القسم الخامس (د)، إطار العمل التشغيلي لمعرفات الاتصال.

| رقم. | مبادئ الاتصال المستندة إلى الأغراض |
|---|---|
| .10 | وجهة الاتصال المستندة إلى الغرض لا يجب أن تكون بالضرورة هي المسجل، وقد يكون الوصول إلى معلومات المسجل محددة بشكل كبير من خلال بوابة حسب السياسات الأخرى. لاحظ أن أي عنوان PBC لا يمثل بالضرورة شخصًا ولكن بالأحرى نقطة اتصال محددة للعديد من الأغراض. |
| .11 | ولا يجب تنشيط أي اسم نطاق (أي وضعه في نظام DNS العالمي) إلى أن يتم توفير معرف PBC لكل غرض معمول به. وإذا أصبح أي PBC غير صالح للغرض المحدد له، فإن عملية توفر للمسجل القدرة على تحديد جهة اتصال جديدة صالحة، يجب أن تضمن الإشعار والوقت المعقولين لتحديث معرف PBC لكي يحدث. حسب المبدأ رقم 9 أعلاه، يجب استخدام جهة اتصال المسجل باعتباره معرف PBC الافتراضي لكل غرض. والعجز عن توفير معرف PBC صالح يتجاوز هذا الوقت قد يؤدي إلى تعليق و/أو حذف اسم النطاق في عملية مشفرة. (راجع القسم الخامس للتعرف على متطلبات التوثيق). |
| .12 | يمكن توفير معرفات PBC اختياريًا لكل غرض مصرح به، مع متطلبات محددة ومتباينة لعناصر البيانات التي تكون بحاجة إلى تجميع ونشر لكل نوع من PBC من أجل تنفيذ الاحتياجات الخاصة بما يرتبط بذلك من أغراض مسموح بها. |
| .13 | كما يجب وضع عملية وسياسات تمكن جهات الاتصال المحددة من خلال المسجلين من اختيار/عدم اختيار إمكانية نشر معرفات جهات الاتصال الخاصة بهم كمعرفات PBC لأسماء النطاقات، من أجل دعم حقوق الأشخاص والكيانات على قبول أو رفض المسئولية عن العمل في أدوار محددة لتسجيلات نطاقات خاصة. |
| .14 | وأي نظام لتوفير "جهات الاتصال المستندة إلى الغرض" يجب أن يكون مرنًا ويسمح بأغراض جديدة وإمكانية إنشاء أنواع جهات الاتصال ونشرها في RDS. (راجع القسم الثالث (ج) للتعرف على تفاصيل حول إضافة أغراض جديدة). |

**و. أدوار ومسؤوليات جهات الاتصال المستندة إلى الأغراض**

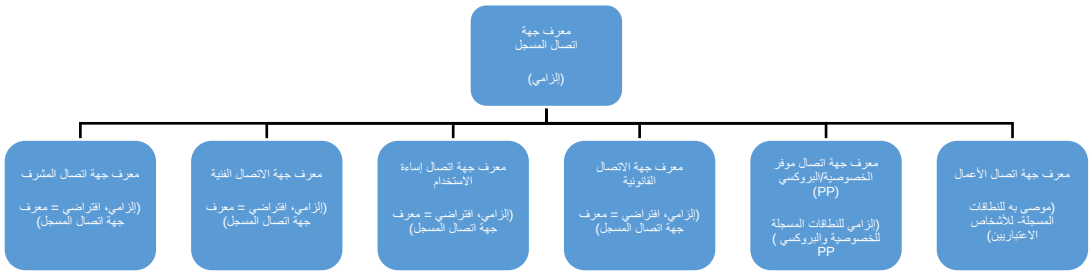
وفقًا لما تم ترخيصه في الشكل 4 وحسب التفاصيل الواردة في الجدول 1، قامت مجموعة EWG بتحليل حالات الاستخدام التمثيلي من أجل تحديد أنواع المستخدمين الراغبين في الوصول إلى بيانات التسجيل لنطاقات gTLD والأغراض المسموح بها في الوقت الحالي التي تحققها تلك البيانات. ولتحقيق وتوفير الوصول المستند إلى الأغراض إلى بيانات التسجيل، فقد تم تحديد كافة الأغراض المسموح بها على جهات PBC. على سبيل المثال:

- ويمكن تخصيص أي جهة اتصال "قانونية" من أجل التعامل مع نزاعات العلامات التجارية أو غيرها من الدعاوى القانونية فيما يخص اسم نطاق. ولتمكين الاتصال من أجل الأغراض المرتبطة، فإن لهذا العنوان PBC مجرد عنوان مادي له القدرة على تلقي الإشعارات القانونية، وعنوان بريد إلكتروني نشط من أجل تلقي الاستعلامات، وهاتف عمل أو رقم فاكس من أجل تلقي الاستعلامات.
- ويمكن تحديد جهة اتصال "إساءة استخدام" من أجل التعامل مع الاستعلامات حول السلوك المسيء المنبعث من نطاق ويتضح في مرور بيانات أو غير ذلك من أنشطة الإنترنت الضارة والحساسة للغاية للوقت. ولتمكين الاتصال من أجل الأغراض المرتبطة، فإن لهذا العنوان PBC يجب أن يكون له قادر على تلقي والرد على الشكاوى الصحيحة بالإضافة إلى رقم هاتف نشط من أجل تلقي الاستعلامات. ويمكن لجهة اتصال PBC أيضًا تضمين الوسائط الاجتماع وعناوين الرسائل الفورية من أجل تسهيل التفاعل في الوقت الفعلي، أو عنوان مادي أو رقم فاكس من أجل تلقي الاستعلامات، بالإضافة إلى عنوان URL منشور يعمل على تسهيل الإبلاغ عن إساءة الاستخدام.

يوصى أيضًا لجهات اتصال PBC تحديد موفر معتمد لخدمة الخصوصية/البروكسي الإدارية والفنية بالإضافة إلى جهات اتصال أعمال. وتتوفر قائمة كاملة بأنواع ومسئوليات PBC في القائمة 5، راجع أيضًا القسم الرابع، مبدأ جمع البيانات رقم 20، للتعرف على احتياجات عناصر البيانات لكل نوع من PBC.

وكما هو موضح في الشكل التالي، توصي مجموعة EWG بأن يتم استخدام المعرف الخاص بالمسجل في حالة عدم توفير جهات اتصال PBC أكثر تحديدًا لاسم نطاق محدد. على سبيل المثال، في حالة تحديد جهات اتصال قانونية لاسم نطاق محدد، فيجب إشعار المسجل بأن الأطراف قد تضطر للاتصال به لهذا الغرض المسموح به وأن تعطى له الفرص على تحديد جهة اتصال PBC من أجل تلقي هذه الطلبات لاسم هذا النطاق.

إذا اختار المسجل عدم تحديد جهة اتصال PBC، فيتم إرسال هذه الطلبات إلى المسجل، من خلال استخدام البيانات المطلوبة لهذا الغرض المرتبط بمعرف جهة اتصال المسجل. وإذا فضل المسجل عدم الإعلان عن عناصر البيانات تلك، فيجوز تسجيل اسم النطاق من خلال استخدام خدمة خصوصية/وكالة معتمدة. راجع القسم الرابع للتعرف على مزيد من النقاش لمبادئ عناصر البيانات وجهات اتصال PBC.




**الشكل 4. أنواع جهات اتصال RDS**

يجب ترميز جميع الأغراض/جهات الاتصال من خلال صناع السياسات من خلال عملية محددة لإضافة أو تغيير أو حذف الأغراض.

ويحتفظ هذا الأسلوب الخاص بـ PBC ببساطة المسجلين باحتياجات جهات الاتصال الأساسية وتعرض تشعبًا للمسجلين ذوي احتياجات الاتصالات الأكثر توسعًا. ولتوضيح هذا المفهوم، أوردنا ثلاثة أمثلة وظيفية مختلفة ونموذجية في نفس الوقت كالتالي:

1. يجوز لأي مسجل أن يحدد بوضوح معرف اتصال المسجل الخاص به باعتباره نقطة الاتصال الوحيدة لاسم النطاق الخاص به. وفي هذه الحالة، فإن استعلامات RDS لكل غرض مسموح به سوف ينتج عنها عناصر بيانات مرخصة عامة أو من خلال بوابات مع معرف اتصال المسجل، وفقًا لما هو مطلوب لكل غرض.

**مثال على سجل DN:**

| | | | | |
|---|---|---|---|---|
| Registrant | Contact | ID | = | <reg> |
| Tech | Contact | ID | = | <reg> |
| Admin | Contact | ID | = | <reg> |
| Abuse | Contact | ID | = | <reg> |
| Legal | Contact | ID | = | <reg> |

2. وأي مسجل يستخدم خدمة **خصوصية** معتمدة (المحددة في القسم السابع) قد تخصص العديد من معرفات الاتصال الفريدة لاسم النطاق الخاص بها، بما في ذلك معرف اتصال موفر الخصوصية/البروكسي (أي؛ موفر خدمة الخصوصية)، ومعرف جهة الاتصال الفنية (على سبيل المثال؛ موفر الاستضافة أو ISP)، والمشرف المقدم من موفر الخدمة، ومعرفات إساءة الاستخدام وجهات الاتصال القانونية. وفي هذا المثال، جهة الاتصال الفنية المحددة مسئولة عن حل كافة المشكلات الفنية المرتبطة باسم النطاق، وجهات اتصال موفر الخصوصية/البروكسي المعتمدة مسئولة عن كافة خدمات الخصوصية المرتبطة باسم النطاق (بما في ذلك مسئول التوجيه، وإساءة الاستخدام ورسائل جهات الاتصال القانونية إلى المسجل).

**مثال على سجل DN:**

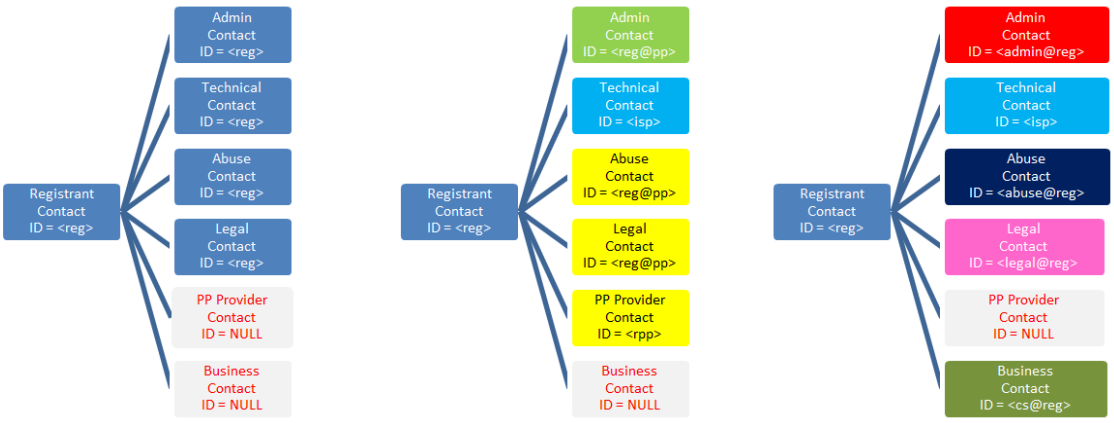
Registrant Contact ID = <reg>
PP Contact ID = <pp>
Tech Contact ID = <isp>
Admin Contact ID = <reg@pp>
Abuse Contact ID = <reg@pp>
Legal Contact ID = <reg@pp>

3. وأي مسجل يختار التعريف الذاتي كشخصية اعتبارية يجوز له توفير العديد من معرفات الاتصال الفريدة لأي اسم نطاق محدد، بما في ذلك معرفات PBC القانونية وإساءة الاستخدام والأعمال والمرتبطة بشكل خاص باسم النطاق المحدد. في هذا المثال، سوف تنتج استعلامات RDS لكل من هذه الأغراض عن عناصر بيانات مرتبطة بمعرف PBC متخصص مقابل، بما يسهل الاتصال المباشر مع الشخص أو الكيان الذي قبل المسئولية عن الدور المحدد. وقد يصبح هذا السيناريو أكثر شيوعًا بمرور الوقت مع استفادة المؤسسات الأكبر من هذا التنوع في تحسين قدرات الاتصال وتقليل سوء الاتصال وإعادة التوجيه.

**مثال على سجل DN:**

Registrant Contact ID = <reg>
Tech Contact ID = <isp>
Admin Contact ID = <admin@reg>
Abuse Contact ID = <abuse@reg>
Legal Contact ID = <legal@reg>
Business Contact ID = <cs@reg>

هذه الأمثلة موضحة بالرسومات في الشكل التالي:




**الشكل 5. مثال على سجلات DN التي تستخدم جهات الاتصال المستندة إلى الأغراض**

يرجى الرجوع إلى القسم الرابع للتعرف على قائمة بجهات اتصال PBC وإلى الملحق د للتعرف على قائمة كاملة بعناصر البيانات المرتبطة بكل غرض مسموح به وكل PBC مرتبط.

تشمل مسئوليات PBC تلقي الطلبات حول اسم هذا النطاق، وتقييم تلك الطلبات، وإقرار الطلب و/أو إشعار المسجل/المرخص له، استنادًا إلى الاتفاقية التعاقدية بين المسجل وPBC.

ويمكن تلخيص المسئوليات المحتملة لكل PBC على النحو التالي:

| نوع PBC | المسؤوليات المحتملة |
|---|---|
| الإشراف | التعامل مع الطلبات ذات الصلة ببيع أو الاستحواذ على اسم نطاق، مثل استعلامات الشراء والتنازلات عن أسماء النطاقات. |
| القسم القانوني | التعامل مع الطلبات حول اسم النطاق هذا من الجهات الضريبية، ومسئولي التحري عن UDRP، ومسئولي التحري عن الامتثال التعاقدي، والممثلين القانونيين. |
| الفني | التعامل مع الطلبات المقدمة حول المشكلات المرتبطة باسم هذا النطاق بالإضافة إلى انتهاكات موقع الويب ومشكلات DNS، ومشكلات تسليم البريد، إلخ. |
| الإساءة | التعامل مع تقارير إساءة استخدام DNS حول اسم هذا النطاق، بالإضافة إلى التصيد والبريد العشوائي، وغير ذلك من أنشطة الإنترنت الضارة. |
| الخصوصية والبروكسي | التعامل مع طلبات الترحيل/الكشف، وتقديم الشكاوى حول إساءة استخدام اسم النطاق بالنيابة عن المسجل/المرخص له، مع الالتزام بتحريات LEA في الأنشطة الجنائية. |
| المشروع | التعامل مع طلبات العملاء الخاصة بالحصول على المعلومات حول شركة أعمال ومعلومات من أجل الاتصال بالشركة من أجل الحصول على مزيد من المعلومات أو حل شكاوى العملاء. |

**الجدول 5. المسئوليات المحتملة لكل من جهات الاتصال المستندة إلى الأغراض**

**للاعتبارات المستقبلية:** قد تكون هناك جهات اتصال PBC متعددة محددة لكل نوع من PBC، بما يسمح للاتصال المباشر مع أفراد محدد ذوي مسئوليات أساسية. على سبيل المثال، للحصول على تواجد كبير على الإنترنت، سيكون من المرغوب تقسم المشكلات الفنية فيما بين مسئول البريد، ومشغل DNS، ومسئول الويب، إلخ. والواجبات التي يتم تأديتها من خلال هذه الجهات المتخصصة سوف يتم تمييزها في خانة يتم نشرها في البيانات العامة من أجل تحديد الغرض الخاص لـ PBC وفقًا لما يحدده المسجل. وقد لا يكون هذا التعقيد مضمونًا في هذا الوقت، لكن لا يجب منعه في المستقبل.

### ز. تفويض استخدام اتصال RDS

وفقًا لم تم وصفه عاليه، يجب أن تحدد تسجيلات أسماء النطاقات الحد الأدنى اللازم على الأقل من جهات اتصال PBC. ويجب أن تكون كافة جهات الاتصال تلك على علم وتوافق على تنفيذ الدور (الأدوار) المحددة لكل اسم نطاق مسجل. وفينا يلي مزيد من التفاصيل حول المبادئ المرتبطة بهذا المفهوم.

| رقم. | مبادئ تفويض استخدام جهات الاتصال المستندة إلى الأغراض |
|---|---|
| 15. | يجب أن تكون الموافقة على كل PBC من اليسير الحصول عليها بطريقة قابلة للتوسعة وفي الوقت الفعلي أو بالقرب من الوقت الفعلي من أجل تجنب تأخير تسجيلات أسماء النطاقات أو تحديثات أسماء النطاقات. |
| 16. | ويجب أن تمنع السياسات والعمليات الاستخدام غير المرخص لجهات اتصال PBC. |

| رقم. | مبادئ تفويض استخدام جهات الاتصال المستندة إلى الأغراض |
|---|---|
| 17. | ويجب أن تكون لـ PBC أو المسجل القدرة على إلغاء الموافقة في وقت لاحق. (راجع القسم الخامس، التوثيق للحصول على التفاصيل). |
| 18. | يجب أن تكون للمسجلين القدرة على تخصيص أنفسهم بسهولة كجهات اتصال PBC لأسماء النطاقات الخاصة بهم دون موافقة طرف خارجي/آخر. |

على سبيل المثال، يقدم المسجل معرف اتصال PBC ورمز استخدام لمرة واحدة يمكن التحقق منه على الفور وتلقائيًا من خلال المحقق المسئول عن هذا المعرف الخاص بجهة الاتصال. وعوضًا عن ذلك، يمكن استخدام نظام للتحقق من البريد الإلكتروني أو الرسائل النصية القصيرة في عملية للحصول على ترخيص جهات الاتصال.

## 4. تحسين المساءلة

يتخذ نظام RDS الموصى به أسلوب السجل النظيف، تاركًا نظام WHOIS الحالي المناسب لجميع الأغراض لصالح أسلوب الوصول الوجه بالأغراض للبيانات الموثقة أملاً في تحسين الخصوصية والدقة والمساءلة.

وترى مجموعة EWG أن هذا نموذجًا للوصول عبر بوابات يمكن أن يزيد من المساءلة بالنسبة لجميع الأطراف المشاركة في الإفصاح عن بيانات تسجيل أسماء نطاقات gTLD واستخدامها. أولاً، يسجل RDS كافة أشكال الوصول إلى بيانات تسجيل gTLD، بما في ذلك الوصول غير المرخص إلى عناصر البيانات العامة، وقيود الوصول من أجل منع التجميع الجماعي للمعلومات. بالإضافة إلى ذلك، فإن الوصول عن طريق بوابات لعناصر البيانات الأكثر حساسية يتاح فقط للمطالبين الذي يتقدمون بطلبات وحصولهم على أوراق اعتماد من أجل توثيق استعلام RDS. وفي النهاية، يقوم RDS بتدقيق كل من الوصول إلى البيانات العامة والبيانات عن طريق بوابات من أجل الحد من إساءة الاستخدام وفرض جزاءات وغيرها من التعويضات للاستخدام غير المناسب. يجوز تطبيق أحكام وشروط مختلفة على أغراض مختلفة. وفي حالة مخالفة مقدمي الطلبات للأحكام والشروط، يتم تطبيق جزاءات.

وقد عبر الكثير من أعضاء مجتمع ICANN على مخاوف حول التخلي التام عن نظام WHOIS العام مجهّل الهوية لصالح نموذج الوصول عن طريق بوابات الموصى به من مجموعة EWG. واقترح البعض بأنه يجب أن تظل جميع بيانات التسجيل عامة بالنسبة لجميع مقدمي الطلبات غير محددي الهوية، في حين اقترح آخرون بجعل قليل من البيانات عامة أو عدم نشر أي من المعلومات على الإطلاق. وأيد البعض مفهوم اعتماد المستخدمين المطالبين بالوصول لأغراض مسموح به، لكن سعوا للحصول على تفاصيل إضافية حول عناصر البيانات المتاحة، وعمليات الاعتماد، والطريقة التي يمكن من خلالها وضع السياسات ذات الصلة وتعديلها بمرور الوقت. وفي حين أنه لا توجد إجابة سهلة تلبي هذه الآراء المتباينة، يحدد هذا القسم بالتفصيل توصيات EWG في هذه النواحي.

### أ. مبادئ عناصر البيانات

توصي مجموعة EWG بالمبادئ التالية من أجل تصنيف عناصر البيانات.

| رقم. | مبادئ عناصر البيانات |
|---|---|
| .19 | يجب أن يستوعب نظام RDS الإفصاح المدفوع بالأغراض لعناصر البيانات. (راجع القسم الثالث للتعرف على قائمة بالأغراض المسموح بها وجهات الاتصال المستندة إلى الأغراض المرتبطة بها (PBC)). |
| .20 | من غير المقرر أن تكون جميع البيانات التي يتم جمعها عامة أمام الجمهور، فيجب أن يعتمد الإفصاح على مقدم الطلب والغرض. |
| .21 | فالوصول العام إلى مجموعة الحد الأدنى من البيانات المحددة يجب أن يتاح، بالإضافة إلى بيانات PBC المنشورة بشكل عام من أجل تسهيل الاتصال لهذا الغرض. |
| .22 | أما عناصر البيانات المقرر لها أن تكون أكثر حساسية (بعد إجراء تقييم المخاطر والتأثيرات) فيجب أن تتوفر لها الحماية من خلال الوصول إليها عن طريق بوابات، استنادًا إلى ما يلي:<br>• تعريف الغرض المسموح به<br>• إفصاح مقدم الطلب/العرض<br>• التدقيق/التوافق من أجل ضمان أن الوصول عن طريق البوابات لا يتم إساءة استخدامه |
| .23 | يجب الإفصاح عن عناصر البيانات المسموح بها فقط للغرض المعلن عنه (أي، تقديم ردود أو البحث عنها من خلال الاستعلامات العكسية أو استعلامات WhoWas). |
| .24 | أما عناصر البيانات الوحيدة التي يجب جمعها فهي تلك العناصر ذات غرض واحد على الأقل مسموح به. |
| .25 | ويجب ربط كل عنصر بيانات بمجموعة من الأغراض المسموح بها.<br>• مجموعة أولية من الاستخدامات المقبولة، والأغراض المسموح به واحتياجات عناصر البيانات فهي محددة من خلال هذا التقرير، (راجع القسم الثالث و الملحق د).<br>• ويجب ربط كل غرض مسموح به بالوصول إلى عناصر البيانات المحدد بشكل واحد بالإضافة إلى سياسات الاستخدام.<br>• كما هو محدد في القسم الثالث، يجب تحديد عملية مراجعة مستمرة من أجل النظر في الأغراض الجديدة المقترحة والتحديث الدوري للأغراض المسموح بها من أجل توضيح الإضافات المعتمدة، وتحديدها على عناصر البيانات الحالية.<br>• يجب تحديد عملية تعريف السياسات من أجل النظر في عناصر البيانات الجديدة المقترحة، وأيضًا متى ما لزم ذلك، تحديث عناصر البيانات المحددة، وتقييدها على الأغراض الحالية المسموح بها. |
| .26 | كما أن قائمة عناصر البيانات المقرر جمعها وتخزينها والإفصاح عنها يجب أن تستند إلى حالات الاستخدام المعروفة (والمشار إليها في هذه الوثيقة) بالإضافة إلى تقييم المخاطر (والمقرر إكمالها قبل تنفيذ RDS). |
| .27 | يجب على سائر السجلات وجهات التوثيق تخزين المجموعة الكاملة لعناصر البيانات التي يقومون بجمعها/توفيرها إلى RDS. (راجع أيضًا القسم السابع، نماذج RDS المحتملة). |

### الخطوة 1: جمع البيانات

يجب جمع البيانات قبل أن يتم الإفصاح عنها انتقائيًا للأغراض المسموح بها. المبادئ التالية موصى بها لتوجيه عملية الجمع في وقت التسجيل:

| رقم. | مبادئ جمع البيانات |
|---|---|
| .28 | دعمًا للمبادئ القانونية المحورية المحددة في القسم السادس، يجب على السجلات وجهات التوثيق توفير الفرصة أمام مسجلي أسماء النطاقات وجهات الاتصال المستندة إلى الغرض، في وقت جمع البيانات، على الموافقة على استخدام البيانات الخاصة بهم للأغراض المسموح بها قبل الإفصاح، بما يتفق مع قوانين حماية البيانات في دوائرهم القضائية. وفي صياغة السياسة، يجب التعامل مع هذا المبدأ في السياق الأوسع لهذه المبادئ القانونية المحورية.[7] |
| .29 | ولتحقيق الاحتياجات الأساسية للتحكم في النطاقات، يجب أن يكون لزامًا على السجلات وأمناء السجلات جمع عناصر البيانات التالية وعلى المسجلين توفيرها وذلك عند تسجيل أي اسم نطاق:<br>أ. اسم النطاق<br>ب. خوادم DNS<br>ج. اسم المسجل<br>د. نوع المسجل<br>يشير إلى نوع الكيان المحدد من خلال اسم المسجل، من أجل الاستخدام في تطبيق متطلبات بيانات التسجيل، على النحو التالي:<br>**غير المعلنة** – يسري بشكل افتراضي في حالة عدم تحديد الخيارات التالية وتتم معاملتها من خلال RDS بطريق مماثلة للشخص الطبيعي.<br>**موفر الخصوصية/البروكسي** – يجب اختياره لأسماء النطاقات المسجلة من خلال استخدام موفر خصوصية/بروكسي معتمد. يجب أيضًا على معرف جهة الاتصال الخاصة بموفر خصوصية/بروكسي معتمد عند اختياره أن يتوفر من أجل تمكين ترحيل/كشف تصعيد الطلب إلى جهة اتصال PBC للخصوصية والبروكسي PP.<br>**الشخص الاعتباري** – يمكن تحديده لأسماء النطاقات المسجلة للكيانات غير الأشخاص الاعتباريين وغير موفري البروكسي. أي معرف لجهة الاتصال الخاصة بجهة اتصال PBC يجب أيضًا توفيره -إذا ما تم اختياره- من أجل تسهيل استعلامات وشكاوى العملاء. (راجع الملاحظة أسفل هذا الجدول).<br>**الشخص الطبيعي** – يمكن تحديده لأسماء النطاقات المسجلة للأشخاص الطبيعيين. لا يجوز تعريف أي من جهة اتصال PBC الخاصة بالخصوصية/البروكسي -إذا ما تم اختيارها- وتتم معاملة اسم المسجل والعناوين كمعلومات شخصية بما يتفق مع قوانين حماية البيانات المعمول بها على الاختصاص القضائي الخاص بصاحب البيانات.<br>هـ. معرف جهة اتصال المسجل<br>أي معرف فريد محدد لكل جهة اتصال مسجل [الاسم+العنوان] خلال عملية التوثيق (راجع القسم الخامس للحصول على تعريف أكثر تفصيلاً لمعرف جهة الاتصال وكيفية إنشاءه من خلال جهة التوثيق واستخدامه لتسجيل DN) |

[7] وقد كان هناك شبه إجماع على دعم هذا النص، مع رفض عضو واحد في مجموعة EWG.

| رقم. | مبادئ جمع البيانات |
|---|---|
| | و. العنوان البريدي للمسجل<br>ويشمل عناصر البيانات التالية: الشارع، المدينة، الولاية/المقاطعة، الرمز البريد، الدولة (حسب ما ينطبق)<br>ز. عنوان البريد الإلكتروني للمسجل<br>ح. هاتف المسجل<br>ويشمل عناصر البيانات التالية: الرقم، والرقم الداخلي (إذا انطبق ذلك) |
| 30. | أ. لتحسين كل من الخصوصية والقدرة على الاتصال للمسجل، يتعين على أمناء السجلات جمع، وعلى المسجلين توفير جهات الاتصال المستندة إلى الغرض (PBC) لكل اسم نطاق مسجل.<br>ب. يجوز للمسجلين اختياريًا تحديد جهات اتصال PBC المتوفرة من خلال الخصوصية/البروكسي أو جهات اتصال PBC المرخصة من جهات أخرى للأغراض المصرح بها المحددة (راجع القسم الثالث).<br>ج. لتحقيق احتياجات الاتصال المرتبطة بكل غرض مسموح به، فإن جهات اتصال PBC التي تم إنشاؤها من خلال جهة توثيق والمرتبطة بعد ذلك باسم نطاق فيجب أن تحقق الحد الأدنى من متطلبات عناصر البيانات الإلزامية التالية:<br>جهة الاتصال الفنية: عنوان البريد الإلكتروني<br>جهة اتصال المشرف: عنوان البريد الإلكتروني للمؤسسة<br>جهات الاتصال القانونية: عنوان البريد الإلكتروني والهاتف والعنوان البريدي للمؤسسة<br>جهة اتصال إساءة الاستخدام: عنوان البريد الإلكتروني ورقم الهاتف<br>جهة اتصال الأعمال[8]: العنوان البريدي للمؤسسة<br>جهة الاتصال بموفر خدمة الخصوصية/البروكسي[9]: المؤسسة، عنوان البريد الإلكتروني، عنوان URL لجهة الاتصال، عنوان URL لإساءة الاستخدام<br>د. وإذا لم يحدد مسجل جهة اتصال PBC لكل غرض مسموح به إلزامي، فإن معرف جهة الاتصال الخاص بالمسجل يجب استخدامها افتراضيًا لجهات اتصال PBC تلك. (لاحظ أن المسجل بإمكانه تجنب ذلك من خلال استخدام خدمة خصوصية/بروكسي معتمدة، أو من خلال تعيين جهات اتصال PBC). في حالة استخدام معرف اتصال المسجل كمعرف PBC، فإن متطلبات الجمع والإفصاح بالنسبة لبيانات المسجل قد تزيد من أجل تحقيق احتياجات عناصر البيانات الإلزامية لـ PBC المحددة أعلاه. |
| 31. | ولتجنب جمع بيانات أكثر من اللازم، فإن كافة البيانات الأخرى المقدمة من المسجل غير المنصوص عليها في المبدأ 29 أو 30 أعلاه والمستخدمة لغرض واحد على الأقل مسموح به يجب أن تجمع اختياريًا وفقًا لتقدير المسجل. ويجب على جهات التوثيق والسجلات وأمناء السجلات السماح بجمع هذه البيانات وتخزينها إذا اختار المسجل ذلك. |

[8] جهة الاتصال إلزامية فقط إذا كان نوع المسجل = شخص اعتباري

[9] جهة الاتصال إلزامية فقط إذا كان نوع المسجل = موفر خدمة الخصوصية والبروكسي

| رقم. | مبادئ جمع البيانات |
|---|---|
| .32 | ولزيادة مستوى استقرار الإنترنت، يجب توفير عناصر البيانات الإلزامية التالية من خلال السجلات وأمناء السجلات إلى RDS:<br>أ. حالة التسجيل<br>ب. حالة العميل (تحدد من خلال أمين السجل)<br>ج. حالة الخادم (تحدد من خلال السجل)<br>د. أمين السجل<br>هـ. الدائرة القضائية لأمين السجل<br>و. الدائرة القضائية للسجل<br>ز. لغة اتفاقية التسجيل<br>ح. تاريخ الإنشاء<br>ط. تاريخ انتهاء أمين السجل<br>ي. تاريخ التحديث<br>ك. عنوان URL لأمين السجل<br>ل. رقم IANA لأمين السجل<br>م. رقم هاتف جهة اتصال إساءة الاستخدام لدى أمين السجل<br>ن. عنوان البريد الإلكتروني لجهة اتصال إساءة الاستخدام لدى أمين السجل<br>ص. عنوان URL لموقع شكاوى مركز معلومات شبكة الإنترنت Internic |
| .33 | بالنسبة لعناصر البيانات المحددة بنطاق TLD، يجب على سجل TLD إنشاء ونشر سياسة لجمع البيانات (متسقة مع هذه المبادئ المحورية) وتحمل المسئولية عن أي توثيق لعناصر البيانات تلك المحددة من خلال TLD. |
| .34 | ويجوز لجهات التوثيق والسجلات وأمناء السجلات جمع أو تخزين أو الإفصاح عن عناصر بيانات إضافية للاستخدام الداخلي التي لم يتم مشاركتها أبدًا مع RDS.[10] |

**ملاحظة:** بعد مناقشة طويلة، لم توصي مجموعة EWG بإضافة **غرض اسم نطاق** كعنصر بيانات. وعوضًا عن ذلك، فقد أوصت مجموعة EWG بمبادئ لإقرار أهداف مرتبطة بالإضافة إلى **جهة اتصال PBC للأعمال** واضحة تمت التوصية بها من أجل النشر عن طريق المسجلين الذين يعرفون أنفسهم بأنهم **أشخاص اعتباريين** يشاركون في نشاط تجاري. وقد يؤدي ذلك إلى العديد من قيام مستخدمي الإنترنت التجاريين الذين ينشرون عناصر البيانات بشكل أكثر وحدة إلى دعم ثقة العملاء، بالإضافة إلى الإقرار بأن المسجلين يحددون في النهاية بأنفسهم هذا التصنيف وقد يكون من المستحيل تقريبًا إنفاذ امتثال قوي على المستوى العالمي حول غرض أسماء النطاقات - التجارية في مقابل غير التجارية.

[10] تشمل الأمثلة عنوان IP المستخدم من خلال العملاء في وقت التسجيل، ورابط لاستخراج طلب للحصول على مفتاح تحويل EPP لاسم نطاق، بالإضافة إلى بيانات السداد المرتبطة بحساب العميل. بيانات استخدام الإنترنت غير محددة في إطار قياس من خلال RDS إلا أنها محددة بالأحرى بشكل خاص من خلال السجلات وأمناء السجلات.

### الخطوة 2: الكشف عن البيانات

بعد جمع البيانات يمكن الإفصاح عنها انتقائيًا للأغراض المسموح بها. المبادئ التالية موصى بها لتوجيه عملية الإفصاح مع تلقي الاستعلامات:

| رقم. | مبادئ الإفصاح عن البيانات |
|---|---|
| .35 | لزيادة مستوى خصوصية المسجل، يجب أن تحدد البيانات المقدمة من خلال المسجل عن طريق بوابات بشكل افتراضي، باستثناء الحالات التي تكون فيها حاجة ملحة للحصول على وصول عام يتجاوز الخطر الناجم.<br>• يمكن للمسجلين اختيار جعل أية بيانات محددة عن طريق بوابات ومقدمة من المسجلين بيانات عامة من خلال الحصول على موافقة مستنيرة. |
| .36 | ولزيادة مستوى استقرار الإنترنت، يجب أن تكون كافة بيانات التسجيل المقدمة من السجل أو أمين السجل دائمًا عامة، باستثناء الحالات التي يؤدي فيها القيام بذلك إلى خطر غير مقبول.<br>• ويمكن للمسجلين اختيار تحويل أي بيانات عامة مقدمة من السجل/أمين السجل إلى بيانات محددة ببوابات، باستثناء ما هو مشار إليها أدناه ليمكن التحكم الأساسي في النطاقات. |
| .37 | ولزيادة مستوى إمكانية الوصول، يجب أن تكون كافة جهات اتصال PBC عامة بشكل افتراضي.<br>• يمكن لحاملي جهات الاتصال[11] اختيار تحويل أي عناصر بيانات PBC محددة ببوابات، باستثناء ما هو محدد لتحقيق الغرض المحدد (المشار إليه بالتفصيل في الجدول 5). |
| .38 | ولتحقيق الاحتياجات الأساسية للتحكم في النطاقات، فإن البيانات التالية المقدمة من المسجل، والتي تعتبر إلزامية لتجميعها وأقل خطرًا في الإفصاح، فيجب أن يتم تضمينها في الحد الأدنى لمجموعة البيانات العامة:<br>أ. اسم النطاق<br>ب. خوادم DNS<br>ج. نوع المسجل<br>د. معرف جهة اتصال المسجل (المحددة أكثر في القسم الخامس)<br>هـ. عنوان البريد الإلكتروني للمسجل<br>و. جهة الاتصال الفنية<br>ز. معرّف جهة اتصال الإشراف<br>ح. معرف جهة الاتصال القانونية<br>ط. جهة اتصال إساءة الاستخدام<br>ي. معرف جهة اتصال موفر الخصوصية/البروكسي<br>(إلزامي فقط إذا كان نوع المسجل = موفر خدمة الخصوصية/البروكسي)<br>ك. معرف جهة اتصال الأعمال<br>(إلزامي فقط إذا كان نوع المسجل = شخص اعتباري) |

[11] حسب القسم الثالث (ز)، تفويض استخدام جهة اتصال RDS، يجب على جهات اتصال RDS المخصصة التصريح باستخدام معرف جهة اتصال في حدود تسجيل اسم النطاق المحدد. ومن خلال القيام بذلك، يوافق حاملو جهات الاتصال أيضًا على الاستخدام العام/المحدد ببوابات لبياناتهم لهذا الغرض. وعلى الرغم من ذلك، إذا لم تحتوي جهة اتصال PBC على عناصر بيانات إلزامية/عامة لتحقيق غرض محدد، فلا يمكن تخصيص جهة اتصال PBC تلك لذلك الغرض في تسجيل اسم نطاق.

| رقم. | مبادئ الإفصاح عن البيانات |
|---|---|
| .39 | لموازنة البساطة وإمكانية الوصول، إذا لم يقم مسجل بتقديم جهة اتصال PBC إلزامية، يجب إشعار المسجل بأن معرّف الاتصال الخاص به أو بها سوف يتم استخدامه كجهة اتصال PBC، وسوف يتم نشر عناصر بيانات المسجل كجهة اتصال فنية لاسم النطاق، وجهة اتصال المشرف، وجهة الاتصال القانونية، وجهة اتصال إساءة الاستخدام. ويمكن للمسجل تجنب هذا الإفصاح من خلال تحديد جهة اتصال PBC واحدة أو أكثر للجهات الأخرى أو من خلال استخدام خدمة خصوصية/بروكسي معتمدة (وفي هذه الحالة يتم توريد تلك العناوين من خلال موفر الخدمة). |
| .40 | بالنسبة لعناصر البيانات المحددة بنطاق TLD، يجب على سجل TLD إنشاء ونشر سياسة للإفصاح عن البيانات (تكون متسقة مع هذه المبادئ المحورية) وتحمل المسئولية عن تعريف الأغراض المسموح بها لأي من عناصر البيانات تلك المحددة من خلال TLD عن طريق بوابات. |

### تصنيفات عناصر البيانات الناتجة

استنادًا إلى هذه المبادئ، يسرد الجدول التالي تفاصيل التصنيف الناتج لكل عنصر في بيانات RDS توصي به مجموعة EWG، من خلال استخدام الملاحظة التالية:

- هل أي عنصر إلزامي (M) أو (O) اختياري في الحصول عليه. ويعني ذلك:

**[1] بالنسبة للبيانات التي يتم تجميعها من المسجلين،** (M) إلزامي وتعني أن البيانات يجب أن تطلب من خلال أمناء السجلات/جهات التوثيق ويتم تقديمها من خلال المسجلين، في حين أن
(O) اختياري وتعني أن البيانات يجب أن تطلب من خلال أمين السجل/جهة التوثيق لكن يمكن أو لا يمكن تقديمها وفقًا لاختيار المسجل، حسب ما ينطبق.

**[2] بالنسبة للبيانات التي يتم تجميعها من حاملي جهات الاتصال المستندة للأغراض،**
(M) إلزامي وتعني أن البيانات يجب أن تطلب من خلال أمناء السجلات/جهات التوثيق ويتم تقديمها من خلال حاملي جهات الاتصال، في حين أن
(O) اختياري وتعني أن البيانات يجب أن تطلب من خلال أمين السجل/جهة التوثيق لكن يمكن أو لا يمكن تقديمها وفقًا لاختيار حامل جهة الاتصال، حسب ما ينطبق

(**R**) موصى به ويعني ذلك أن البيانات يجب طلبها من خلال أمين السجل/جهة التوثيق لكن يجوز أو لا يجوز تقديمها وفقًا لتقدير حامل جهة الاتصال، حسب ما ينطبق، لعكس كل من توصيات الممارسات "الأفضل" و"الجيدة"[12]

**[3] بالنسبة للبيانات التي يتم تقديمها من السجلات وأمناء السجلات إلى RDS،**
(M) إلزامي وتعني أن البيانات يجب أن يتم تقديمها من خلال السجل/أمين السجل، في حين أن
(O) اختياري وتعني أن البيانات يمكن أو لا يمكن تقديمها، حسب ما ينطبق.

[12] تستند أفضل الممارسات الموصى بها لنشر مختلف عناصر بيانات PBC إلى الخبرة التشغيلية لأعضاء EWG. تمثل العناصر الإلزامية حدًا أدنى من المتطلبات التشغيلية لتنفيذ تلك الأغراض. وعلى الرغم من ذلك، من الناحية العملية، إذا كانت هناك طريقة اتصال لغرض محدد (على سبيل المثال، صيغة ويب للإبلاغ عن المشكلات، أو بريد إلكتروني بديل للوصول إلى فريق العمل الفني) إذن تكون هذه الطريقة البديلة مفيدة بشكل كبير وغالبًا ما تكون مفضلة للتعامل مع المشكلات. وسوف يتفاوت ذلك عبر كافة جهات اتصال PBC - على سبيل المثال، أي عنوان بريدي مفيد أكثر لأغراض جهة الاتصال القانونية أو شركة الأعمال وغير مفيدة بشكل كبير في الحل السريع لأغراض إساءة الاستخدام أو جهات الاتصال الفنية. وبذلك، فقد قدمت مجموعة EWG توصيات خاصة لعناصر البيانات في كل نوع من PBC.

- هل أي عنصر (P) عام [يمكن لأي شخص الوصول إليه بتصديق أو بدون تصديق] أو (G) عن طريق بوابات [يمكن الوصول إليه من خلال المستخدمين المرخص لهم فقط، وللأغراض المسموح بها فقط]، وهل يمكن للمسجلين تغيير هذا الإعداد الافتراضي للإفصاح بنعم أو لا (Y/N). ويعني ذلك:

**[4] بالنسبة للبيانات التي يتم جمعها من المسجلين،**
P / N وتعني أن البيانات التي يتم جمعها يجب أن تكون عام ولا يمكن إخفائها،
P / Y وتعني أن أية بيانات يتم جمعها هي عامة بشكل افتراضي لكن يمكن إخفائها من خلال المسجل،
G / Y وتعني أن أية بيانات يتم جمعها تأتي عن طريق بوابة بشكل افتراضي لكن يمكن نشرها عن طريق المسجل، من خلال الحصول على الموافقة المستنيرة.

**[5] بالنسبة للبيانات التي يتم تقديمها من السجلات وأمناء السجلات إلى RDS،**
P / N فتعني أن أية بيانات يتم تقديمها يجب أن تكون عامة ولا يمكن إخفائها، في حين أن
G / N تعني أن أية بيانات يتم تقديمها يجب أن تكون عن طريق بوابة، ولا تندرج أية بيانات في هذه الفئة.

**[6] بالنسبة للبيانات التي يتم جمعها من حاملي جهات الاتصال المستندة إلى الأغراض،**
P / N وتعني أن البيانات التي يتم جمعها يجب أن تكون عام ولا يمكن إخفائها،
P / Y وتعني أن أية بيانات يتم جمعها هي عامة بشكل افتراضي لكن يمكن إخفائها من خلال حامل جهة الاتصال

لاحظ أنه سواء كانت عناصر البيانات المحددة من خلال بوابات يمكن الوصول إليها من خلال مستخدم محدد فإن ذلك يتوقف على الأغراض المسموح بها. عندما يختار مسجل تحويل عنصر محدد ببوابة افتراضيًا إلى عنصر عام، يصبح لكل شخص القدرة على الوصول إليه. وعندما يختار مسجل تحويل عنصر عام بشكل افتراضي إلى عنصر محدد ببوابة، يصبح الوصول إليه عند ذلك محددًا لأغراض مسموح بها.

| البيانات المقدمة من المسجل/ أمين السجل | التجميع إلزامي أو اختياري | الإفصاح افتراضي عام أو عن طريق بوابة | الإفصاح هل يمكن تغييره؟ | ملاحظات<br>راجع [3] تعريف التجميع<br>و[5] تعريف الإفصاح |
|---|---|---|---|---|
| حالة التسجيل | **إلزامي** | **عام** | **لا** | |
| تفويض DNSSEC | **اختياري** | **عام** | **لا** | |
| حالة العميل (أمين السجل) | **إلزامي** | **عام** | **لا** | يحتوي على كافة القيم المعمول بها على اسم النطاق في مستوى أمين السجل: الحذف محظور، التجديد محظور، التنازل محظور |
| حالة الخادم (السجل) | **إلزامي** | **عام** | **لا** | ليست في RAA، كما هو الحال بالنسبة لعالية،<br>لكن في مستوى السجل |
| أمين السجل | **إلزامي** | **عام** | **لا** | |
| الموزع | **اختياري** | **عام** | **لا** | |
| الدائرة القضائية لأمين السجل | **إلزامي** | **عام** | **لا** | ليست في RAA |
| الدائرة القضائية للسجل | **إلزامي** | **عام** | **لا** | ليست في RAA |
| لغة اتفاقية التسجيل | **إلزامي** | **عام** | **لا** | ليست في RAA |
| تاريخ الإنشاء | **إلزامي** | **عام** | **لا** | |
| تاريخ التسجيل الأصلي | **اختياري** | **عام** | **لا** | ليست في RAA |
| تاريخ انتهاء أمين السجل | **إلزامي** | **عام** | **لا** | |
| تاريخ التحديث | **إلزامي** | **عام** | **لا** | |
| عنوان URL لأمين السجل | **إلزامي** | **عام** | **لا** | |
| رقم IANA لأمين السجل | **إلزامي** | **عام** | **لا** | |
| عنوان البريد الإلكتروني لجهة اتصال إساءة الاستخدام لدى أمين السجل | **إلزامي** | **عام** | **لا** | |
| رقم هاتف جهة اتصال إساءة الاستخدام لدى أمين السجل | **إلزامي** | **عام** | **لا** | |
| عنوان URL لموقع شكاوى مركز معلومات شبكة الإنترنت Internic | **إلزامي** | **عام** | **لا** | |

| بيانات المسجل<br>تم جمعها من المسجل | التجميع<br>إلزامي أو<br>اختياري | الإفصاح<br>افتراضي<br>عام أو عن طريق<br>بوابة | الإفصاح<br>هل يمكن<br>تغييره؟ | ملاحظات<br>راجع [1] تعريف التجميع<br>و[4] تعريف الإفصاح |
|---|---|---|---|---|
| اسم النطاق | **إلزامي** | **عام** | **لا** | |
| خوادم DNS | **إلزامي** | **عام** | **لا** | |
| اسم المسجل | **إلزامي** | **عن طريق بوابة** | **نعم** | |
| نوع المسجل | **إلزامي** | **عام** | **لا** | |
| معرف جهة اتصال المسجل | **إلزامي** | **عام** | **لا** | يستبدل معرف المسجل السجل، الصادر من جهة التوثيق في RDS |
| حالة توثيق جهة اتصال المسجل | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| آخر توقيت زمني موثق لجهة اتصال المسجل | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| منظمة المسجل | **اختياري** | **عام** | **نعم** | تجمع عندما يكون نوع المسجل - شخص اعتباري أو موفر وكيل |
| معرّف شركة المسجل (على سبيل المثال، الاسم التجاري، D-U-N-S) | **اختياري** | **عام** | **نعم** | معرفات العالم الواقعي الصادرة إلى شركات الأعمال حسب المصادر مثل Dunn و Bradstreet<br>تجمع عندما يكون<br>نوع المسجل = شخصية اعتبارية<br>ليست في RAA |
| عنوان سكن المسجل | **إلزامي** | **عن طريق بوابة** | **نعم** | |
| مدينة المسجل | **إلزامي** | **عن طريق بوابة** | **نعم** | |
| ولاية/مقاطعة المسجل | **اختياري** | **عن طريق بوابة** | **نعم** | حسب اتفاقية RAA لسنة 2013، تجمع كافة عناصر "الولاية/المقاطعة" متى كان ذلك منطبقًا |
| الرمز البريدي للمسجل | **اختياري** | **عن طريق بوابة** | **نعم** | حسب اتفاقية RAA لسنة 2013، تجمع كافة عناصر "الرمز البريدي" متى كان ذلك منطبقًا |
| الدولة المسجل | **إلزامي** | **عن طريق بوابة** | **نعم** | |
| هاتف + تحويلة المسجل | **إلزامي** | **عن طريق بوابة** | **نعم** | يتم الحصول على التحويلة إذا انطبق ذلك |
| هاتف + تحويلة المسجل البديلة | **اختياري** | **عن طريق بوابة** | **نعم** | خيار جديد، ليس في RAA |
| عنوان البريد الإلكتروني للمسجل | **إلزامي** | **عام** | **لا** | |
| البريد الإلكتروني البديل للمسجل | **اختياري** | **عام** | **نعم** | خيار جديد، ليس في RAA |
| فاكس + تحويلة المسجل | **اختياري** | **عن طريق بوابة** | **نعم** | حسب اتفاقية RAA لسنة 2013، تجمع كافة عناصر "الفاكس" و"تحويلة الفاكس" متى كان ذلك منطبقًا |
| الرسائل النصية SMS للمسجل | **اختياري** | **عن طريق بوابة** | **نعم** | خيار جديد، ليس في RAA |
| الرسائل الفورية IM للمسجل | **اختياري** | **عن طريق بوابة** | **نعم** | خيار جديد، ليس في RAA |
| وسائل التواصل الاجتماعي للمسجل | **اختياري** | **عن طريق بوابة** | **نعم** | خيار جديد، ليس في RAA |
| وسائل التواصل الاجتماعي البديلة للمسجل | **اختياري** | **عن طريق بوابة** | **نعم** | خيار جديد، ليس في RAA |
| عنوان URL لجهة اتصال المسجل | **اختياري** | **عن طريق بوابة** | **نعم** | خيار جديد، ليس في RAA |
| عنان URL لجهة اتصال المسجل | **اختياري** | **عن طريق بوابة** | **نعم** | خيار جديد، ليس في RAA |

| جهات الاتصال المستندة إلى الأغراض جهة اتصال الإداري | التجميع إلزامي/مطلوب/اختياري | الإفصاح افتراضي عام أو عن طريق بوابة | الإفصاح هل يمكن تغييره؟ | ملاحظات راجع [2] تعريف التجميع و[6] تعريف الإفصاح |
|---|---|---|---|---|
| **الأغراض: شراء/بيع DN، التحكم في اسم النطاق، بحث DNS** | | | | |
| معرف جهة اتصال المشرف | **إلزامي** | **عام** | **لا** | |
| معرّف PBC | **إلزامي** | **عام** | **لا** | ليست في RAA |
| حالة توثيق PBC | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| آخر توقيت زمني موثق لجهة PBC | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| اسم PBC | **إلزامي** | **عام** | **لا** | |
| منظمة PBC | **إلزامي** | **عام** | **لا** | |
| عنوان سكن PBC | **مطلوب** | **عام** | **نعم** | |
| مدينة PBC | **مطلوب** | **عام** | **نعم** | |
| ولاية/مقاطعة PBC | **اختياري** | **عام** | **نعم** | |
| الرمز البريدي لـ PBC: | **اختياري** | **عام** | **نعم** | |
| دولة PBC | **إلزامي** | **عام** | **لا** | |
| هاتف + تحويلة PBC | **اختياري** | **عام** | **نعم** | |
| هاتف + تحويلة PBC البديلة | **اختياري** | **عام** | **نعم** | ليست في RAA |
| عنوان البريد الإلكتروني لـ PBC | **إلزامي** | **عام** | **لا** | |
| عنوان البريد الإلكتروني البديل لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| فاكس + تحويلة PBC | **اختياري** | **عام** | **نعم** | |
| الرسائل النصية لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| الرسائل الفورية IM لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| وسائل التواصل الاجتماعي لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| وسائل التواصل الاجتماعي البديلة لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| عنوان URL لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| عنوان URL لإساءة الاستخدام لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |

| جهات الاتصال المستندة إلى الأغراض جهة الاتصال القانونية | التجميع إلزامي/مطلوب /اختياري | الإفصاح افتراضي عام أو عن طريق بوابة | الإفصاح هل يمكن تغييره؟ | ملاحظات راجع [2] تعريف التجميع و[6] تعريف الإفصاح |
|---|---|---|---|---|
| **الأغراض: الإجراءات القانونية، الإنفاذ النظامي/التعاقدي، التحكم في أسماء النطاقات، بحث DNS** | | | | |
| معرف جهة الاتصال القانونية | **إلزامي** | **عام** | **لا** | ليست في RAA |
| معرف PBC | **إلزامي** | **عام** | **لا** | ليست في RAA |
| حالة توثيق PBC | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| آخر توقيت زمني موثق لجهة PBC | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| اسم PBC | **إلزامي** | **عام** | **لا** | |
| منظمة PBC | **إلزامي** | **عام** | **لا** | |
| عنوان سكن PBC | **إلزامي** | **عام** | **لا** | |
| مدينة PBC | **إلزامي** | **عام** | **لا** | |
| ولاية/مقاطعة PBC | **اختياري** | **عام** | **نعم** | |
| الرمز البريدي لـ PBC: | **اختياري** | **عام** | **نعم** | |
| دولة PBC | **إلزامي** | **عام** | **لا** | |
| هاتف + تحويلة PBC | **إلزامي** | **عام** | **لا** | |
| هاتف + تحويلة PBC البديلة | **اختياري** | **عام** | **نعم** | ليست في RAA |
| عنوان البريد الإلكتروني لـ PBC | **إلزامي** | **عام** | **لا** | |
| عنوان البريد الإلكتروني البديل لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| فاكس + تحويلة PBC | **مطلوب** | **عام** | **نعم** | |
| الرسائل النصية لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| الرسائل الفورية IM لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| وسائل التواصل الاجتماعي لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| وسائل التواصل الاجتماعي البديلة لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| عنوان URL لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| عنوان URL لإساءة الاستخدام لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |

| جهات الاتصال المستندة إلى الأغراض جهة الاتصال التقنية | التجميع إلزامي/مطلوب /اختياري | الإفصاح افتراضي عام أو عن طريق بوابة | الإفصاح هل يمكن تغييره؟ | ملاحظات راجع [2] تعريف التجميع و[6] تعريف الإفصاح |
|---|---|---|---|---|
| **الأغراض: حل المشكلات الفنية، التحكم في أسماء النطاقات، بحث DNS** | | | | |
| معرّف جهة الاتصال الفنية | **إلزامي** | **عام** | **لا** | |
| معرّف PBC | **إلزامي** | **عام** | **لا** | ليست في RAA |
| حالة توثيق PBC | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| آخر توقيت زمني موثق لجهة PBC | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| اسم PBC | **مطلوب** | **عام** | **نعم** | |
| منظمة PBC | **مطلوب** | **عام** | **نعم** | |
| عنوان سكن PBC | **مطلوب** | **عام** | **نعم** | |
| مدينة PBC | **مطلوب** | **عام** | **نعم** | |
| ولاية/مقاطعة PBC | **اختياري** | **عام** | **نعم** | |
| الرمز البريدي لـ PBC: | **اختياري** | **عام** | **نعم** | |
| دولة PBC | **إلزامي** | **عام** | **لا** | |
| هاتف + تحويلة PBC | **مطلوب** | **عام** | **نعم** | |
| هاتف + تحويلة PBC البديلة | **مطلوب** | **عام** | **نعم** | ليست في RAA |
| عنوان البريد الإلكتروني لـ PBC | **إلزامي** | **عام** | **لا** | |
| عنوان البريد الإلكتروني البديل لـ PBC | **مطلوب** | **عام** | **نعم** | ليست في RAA |
| فاكس + تحويلة PBC | **اختياري** | **عام** | **نعم** | |
| الرسائل النصية لـ PBC | **مطلوب** | **عام** | **نعم** | ليست في RAA |
| الرسائل الفورية IM لـ PBC | **مطلوب** | **عام** | **نعم** | ليست في RAA |
| وسائل التواصل الاجتماعي لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| وسائل التواصل الاجتماعي البديلة لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| عنوان URL لـ PBC | **مطلوب** | **عام** | **نعم** | ليست في RAA |
| عنوان URL لإساءة الاستخدام لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |

| جهات الاتصال المستندة إلى الأغراض جهة اتصال إساءة الاستخدام | التجميع إلزامي/مطلوب /اختياري | الإفصاح افتراضي عام أو عن طريق بوابة | الإفصاح هل يمكن تغييره؟ | ملاحظات راجع [2] تعريف التجميع و[6] تعريف الإفصاح |
|---|---|---|---|---|
| **الغرض: الحد من إساءة الاستخدام، التحكم في اسم النطاق، بحث DNS** | | | | |
| جهة اتصال إساءة الاستخدام | **إلزامي** | **عام** | **لا** | ليست في RAA |
| معرّف PBC | **إلزامي** | **عام** | **لا** | ليست في RAA |
| حالة توثيق PBC | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| آخر توقيت زمني موثق لجهة PBC | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| اسم PBC | **مطلوب** | **عام** | **نعم** | |
| منظمة PBC | **مطلوب** | **عام** | **نعم** | |
| عنوان سكن PBC | **مطلوب** | **عام** | **نعم** | |
| مدينة PBC | **مطلوب** | **عام** | **نعم** | |
| ولاية/مقاطعة PBC | **اختياري** | **عام** | **نعم** | |
| الرمز البريدي لـ PBC: | **اختياري** | **عام** | **نعم** | |
| دولة PBC | **إلزامي** | **عام** | **لا** | |
| هاتف + تحويلة PBC | **إلزامي** | **عام** | **لا** | |
| هاتف + تحويلة PBC البديلة | **اختياري** | **عام** | **نعم** | ليست في RAA |
| عنوان البريد الإلكتروني لـ PBC | **إلزامي** | **عام** | **لا** | |
| عنوان البريد الإلكتروني البديل لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| فاكس + تحويلة PBC | **اختياري** | **عام** | **نعم** | |
| الرسائل النصية لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| الرسائل الفورية IM لـ PBC | **مطلوب** | **عام** | **نعم** | ليست في RAA |
| وسائل التواصل الاجتماعي لـ PBC | **مطلوب** | **عام** | **نعم** | ليست في RAA |
| وسائل التواصل الاجتماعي البديلة لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| عنوان URL لـ PBC | **مطلوب** | **عام** | **نعم** | ليست في RAA |
| عنوان URL لإساءة الاستخدام لـ PBC | **مطلوب** | **عام** | **نعم** | ليست في RAA |

| جهات الاتصال المستندة إلى الأغراض جهة اتصال موفر الخصوصية/البروكسي (PP) | التجميع إلزامي/مطلوب /اختياري | الإفصاح افتراضي عام أو عن طريق بوابة | الإفصاح هل يمكن تغييره؟ | ملاحظات راجع [2] تعريف التجميع و[6] تعريف الإفصاح |
|---|---|---|---|---|
| **الأغراض: حماية البيانات الشخصية، التحكم في أسماء النطاقات، بحث DNS** | | | | |
| معرف جهة اتصال PP | **إلزامي** | **عام** | **لا** | ليست في RAA |
| معرّف PBC | **إلزامي** | **عام** | **لا** | ليست في RAA |
| حالة توثيق PBC | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| آخر توقيت زمني موثق لجهة PBC | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| اسم PBC | **إلزامي** | **عام** | **لا** | |
| منظمة PBC | **إلزامي** | **عام** | **لا** | |
| عنوان سكن PBC | **إلزامي** | **عام** | **لا** | |
| مدينة PBC | **إلزامي** | **عام** | **لا** | |
| ولاية/مقاطعة PBC | **اختياري** | **عام** | **نعم** | |
| الرمز البريدي لـ PBC: | **اختياري** | **عام** | **نعم** | |
| دولة PBC | **إلزامي** | **عام** | **لا** | |
| هاتف + تحويلة PBC | **إلزامي** | **عام** | **لا** | |
| هاتف + تحويلة PBC البديلة | **اختياري** | **عام** | **نعم** | ليست في RAA |
| عنوان البريد الإلكتروني لـ PBC | **إلزامي** | **عام** | **لا** | |
| عنوان البريد الإلكتروني البديل لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| فاكس + تحويلة PBC | **اختياري** | **عام** | **نعم** | |
| الرسائل النصية لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| الرسائل الفورية IM لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| وسائل التواصل الاجتماعي لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| وسائل التواصل الاجتماعي البديلة لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| عنوان URL لـ PBC | **إلزامي** | **عام** | **لا** | ليست في RAA |
| عنوان URL لإساءة الاستخدام لـ PBC | **إلزامي** | **عام** | **لا** | ليست في RAA |

| جهات الاتصال المستندة إلى الأغراض جهة اتصال الأعمال | التجميع إلزامي/مطلوب /اختياري | الإفصاح افتراضي عام أو عن طريق بوابة | الإفصاح هل يمكن تغييره؟ | ملاحظات راجع [2] تعريف التجميع و[6] تعريف الإفصاح |
|---|---|---|---|---|
| **الأغراض: استخدام الإنترنت الفردي، التحكم في أسماء النطاقات، بحث DNS** | | | | |
| معرف جهة اتصال الأعمال | **إلزامي** | **عام** | **لا** | ليست في RAA |
| معرّف PBC | **إلزامي** | **عام** | **لا** | ليست في RAA |
| حالة توثيق PBC | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| آخر توقيت زمني موثق لجهة PBC | **إلزامي** | **عام** | **لا** | جديد مقدم من جهة التوثيق |
| اسم PBC | **إلزامي** | **عام** | **لا** | |
| منظمة PBC | **إلزامي** | **عام** | **لا** | |
| عنوان سكن PBC | **إلزامي** | **عام** | **لا** | |
| مدينة PBC | **إلزامي** | **عام** | **لا** | |
| ولاية/مقاطعة PBC | **اختياري** | **عام** | **نعم** | |
| الرمز البريدي لـ PBC: | **اختياري** | **عام** | **نعم** | |
| دولة PBC | **إلزامي** | **عام** | **لا** | |
| هاتف + تحويلة PBC | **مطلوب** | **عام** | **نعم** | |
| هاتف + تحويلة PBC البديلة | **اختياري** | **عام** | **نعم** | ليست في RAA |
| عنوان البريد الإلكتروني لـ PBC | **مطلوب** | **عام** | **نعم** | |
| عنوان البريد الإلكتروني البديل لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| فاكس + تحويلة PBC | **اختياري** | **عام** | **نعم** | |
| الرسائل النصية لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| الرسائل الفورية IM لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| وسائل التواصل الاجتماعي لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| وسائل التواصل الاجتماعي البديلة لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |
| عنوان URL لـ PBC | **مطلوب** | **عام** | **نعم** | ليست في RAA |
| عنوان URL لإساءة الاستخدام لـ PBC | **اختياري** | **عام** | **نعم** | ليست في RAA |

تؤكد مجموعة EWG أيضًا على توصيتها بأداء تحليل واسع النطاق للمخاطر/التأثيرات من أجل التأكد من أن هذه التصنيفات المستندة إلى المبادئ تؤدي في حقيقة الأمر إلى تجميع مناسب وإفصاح عن البيانات لأغراض محددة.

### التماشي مع اتفاقية RAA لسنة 2013 وعناصر البيانات الجديدة

لتسهيل النقل والفهم، تمت محاذاة أسماء عناصر البيانات التي أوصت بها مجموعة EWG مع ما تم تحديده في اتفاقية RAA لسنة 2013 متى ما أمكن ذلك (على سبيل المثال تفويض DNSSEC، وتاريخ انتهاء RDS). وعلى الرغم من ذلك، فإن أسماء عناصر البيانات المستخدمة في اتفاقية RAA لسنة 2013 لعناصر بيانات جهات الاتصال فهي غير كافة لكي تعكس مقترح EWG لجهات الاتصال المستندة إلى الأغراض (راجع القسم الثالث). ولتغطية ذلك، قامت مجموعة EWG بتطبيق المخططات التالية:

عندما يشير معرف جهة اتصال مشرف RDS إلى PBC،
RDS PBC Name = RAA Admin Contact Name
RDS PBC Organization = RAA Admin Contact Organization
وكذلك الحال بالنسبة لعناصر بيانات جهات اتصال مشرف RAA الأخرى

عندما يشير معرف جهة الاتصال الفنية الخاصة بـ RDS إلى PBC،
RDS PBC Name = RAA Tech Contact Name
RDS PBC Organization = RAA Tech Contact Organization
وكذلك الحال بالنسبة لعناصر بيانات جهات الاتصال الفنية الأخرى في RAA

ملاحظة: توصي مجموعة EWG بأن تحدد بوابة RDS التعريفات لكل نوع PBC يمكن الوصول إليه بالفعل بالنسبة لمستخدمي RDS (على سبيل المثال، استخدام التعريفات بنظام الأطر المنبثقة عند وضع مؤشر الماوس فوقها) للإشارة بشكل واضح إلى أن PBC محددة من أجل التعامل مع الاستعلامات للأغراض المسموح بها، وأن أي نقطة اتصال يجب أن تتحدد من أجل تغطية تلك الأغراض. يجوز لأمناء السجلات اختيار الحصول على الاستعلامات بأنفسهم (وتخصيص معرف المسجل كجهة اتصال (PBC، وإشراك موفر معتمد للخصوصية/البروكسي من أجل تلقي تلك الاستعلامات (إشراك PP من أجل توفير عناصر البيانات تلك - غالبًا إعادة توجيه العناوين أو عناوين موفر الخدمة)، أو تحديد كيان محدد من أجل تلقي تلك الاستعلامات (على سبيل المثال، موفر خدمة، أو موفر خدمة استضافة، وكيل قانوني، مكتب خدمة العملاء).

كافة عناصر البيانات كما هي محددة في اتفاقية RAA لعام 2013، مع الإضافات التالية:

**الدائرة القضائية لأمين السجل والسجل:** الاختصاص القضائي أو المنطقة التي يعمل فيها أمين السجل أو السجل، وفقًا لما هو محدد في الاتفاقية الموقعة مع ICANN.

**لغة اتفاقية التسجيل:** اللغة التي كتبت بها اتفاقية أمين السجل مع المسجل.

**تاريخ التسجيل الأصلي:** تاريخ تسجيل اسم النطاق هذا للمرة الأولى.[13]

**حالة العميل، حالة الخادم:** من خلال التوسع على قيم حالة العملاء في اتفاقية RAA لسنة 2013، تحتوي عناصر البيانات هذه على قيم حالة أمين السجل (العميل) والسجل(الخادم) المطبقة في الوقت الحالي على اسم النطاق هذا: الحذف محظور، التجديد محظور، التنازل محظور.

**معرف شركة المسجل:** الرقم التجاري في المملكة المتحدة، رقم D-U-N-S، أو غير ذلك من معرفات الشركات الواقعية الفريدة المخصصة للمسجل من خلال دليل أعمال عام. وهذا يتيح إمكانية البحث عن شركة خارج RDS.

**معرف جهة اتصال المسجل:** مقبض فريد مخصص لمجموعة موثقة مسبقًا لبيانات جهة الاتصال المحددة بأنها هذا المسجل لاسم النطاق. راجع القسم الخامس للحصول على معلومات أكثر تفصيلاً حول معرف جهة الاتصال وكيفية إنشائها واستخدامها. ويعمل هذا المعرف على تمكين إعادة استخدام وصيانة بيانات جهة الاتصال داخل RDS.
لاحظ أن نوع المسجل = الخصوصية/البروكسي، ومعرف جهة اتصال المسجل سوف تعكس المعرف الفريد المخصص لهذا الموفر المعتمد للخصوصية/البروكسي.

[13] يختلف هذا الأمر عن تاريخ الإنشاء حيث يسجل تاريخ الإنشاء آخر وقت تم تسجيل اسم النطاق فيه، ومن المحتمل أن يكون اسم النطاق قد تم تسجيله في السابق وتم حذفه بعد ذلك عدة مرات. يشير تاريخ التسجيل الأصلي إلى التاريخ الأول الذي تم فيه تسجيل اسم النطاق على الإطلاق.

**حالة توثيق جهة اتصال المسجل/PBC، آخر إطار زمني موثق لجهة اتصال المسجل/PBC:** تم تحقيق أعلى مستويات التوثيق بالإضافة إلى التاريخ الذي تم التوثيق فيه آخر مرة، وفقًا لما هو محدد بمزيد من التفصيل في القسم الخامس.

**المسجل/SMS لـ IM/PBC/وسائل التواصل:** طرق الاتصال الجديدة التي قد يتم استخدامها اختياريًا من أجل التواصل مع المسجل أو PBC من خلال SMS، أو الرسائل الفورية، أو غير ذلك من أشكال الاتصال عن طريق الوسائط الاجتماعية البديلة.

**المسجل/بريد PBC الإلكتروني البديل، الهاتف البديل، الوسائط الاجتماعية البديلة:** العناوين البديلة الجديدة التي قد يتم استخدامها اختياريًا من أجل التواصل مع المسجل أو PBC في حالة فشل العنوان الأساسي. والغرض من هذه العناصر الجديدة للبيانات هي التعامل مع الاحتياجات الشائعة مثل حل المشكلات الفنية عند تعطل اسم النطاق نفسه وتمكين اتصال أسرع من خلال الهاتف المحمول أو الوسائط الاجتماعية.

**المسجل/عنوان URL لاتصال PBC، عنوان URL لإساءة الاستخدام:** عناصر البيانات الجديدة التي تؤدي اختياريًا إلى صفحات ويب حيث يمكن وضع تعليمات أو سياسات أو نماذج الاتصال أو الإبلاغ عن إساءة الاستخدام من أجل تسهيل مزيد من الاتصال المثمر.

**معرف جهة اتصال PBC:** مقبض فريد مخصص لمجموعة موثقة مسبقًا لبيانات جهة الاتصال المحددة بأنها PBC لاسم هذا النطاق، في الدور المشار إليه من خلال دور جهة الاتصال. معرف جهة اتصال المسجل ومعرف جهة اتصال PBC قد تشير أو لا تشير إلى نفس جهة الاتصال.

**ملاحظة:** تحديات النقل والامتثال المرتبطة بهذه العناصر الجديدة من البيانات يجب النظر فيها قبل تنفيذ أي RDS.

### ب. مبادئ للوصول إلى البيانات غير الموثقة وعن طريق بوابات

توصي مجموعة EWG باتخاذ أسلوب جديد في الوصول إلى بيانات التسجيل، مع التخلي بالكامل عن الوصول مجهّل الهوية عن طريق كل شخص إلى أي شيء لصالح نموذج جديد يضم وصولاً عامًا إلى بعض البيانات ذات الوصول عن طريق بوابات إلى بيانات أخرى. وفيما يلي المبادئ التي تعكس هذه التوصية.

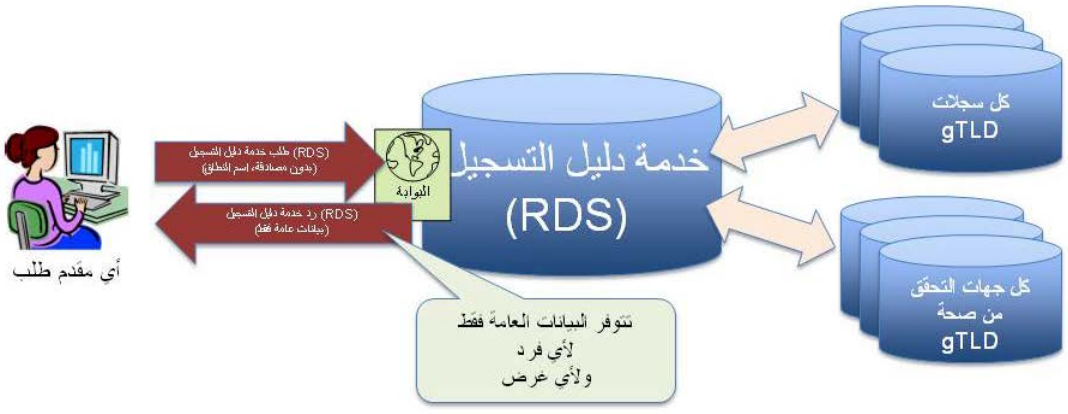
| رقم. | مبادئ الوصول إلى البيانات |
|---|---|
| .41 | حد أدنى من مجموعة عناصر البيانات، على الأقل بما يتوازى مع نظام الخصوصية الأكثر صرامة، يجب أن يكون قابل للوصول من خلال مستخدمي RDS غير الموثقين. |
| .42 | كما يجب دعم مستويات متعددة من الوصول إلى البيانات غير الموثقة، بما يتسق مع الأغراض المسموح بها والمقررة. |
| .43 | كما يجب ربط أوراق اعتماد وصول مستخدم RDS بعملية توثيق قابلة للتدقيق، وفقًا لما هو محدد أكثر في القسم الرابع (ج)، اعتماد مستخدم RDS. |
| .44 | يجب أن لا يكون الوصول على أساس تمييزي (أي يجب أن تؤدي العملية إلى مجال بمستوى الممارسة لسائر مقدمي الطلبات، في نفس الغرض). |

| رقم. | مبادئ الوصول إلى البيانات |
|---|---|
| .45 | لإعاقة إساءة الاستخدام وتعزيز المساءلة:<br>• يجب أن تكون كافة أشكال الوصول إلى عناصر البيانات مستندة إلى غرض محدد؛<br>• الوصول إلى عناصر البيانات عن طريق بوابات يجب أن يكون مقتصرًا على مقدمي الطلبات الموثقين الذين يؤكدون على غرض مسموح به<br>• ويتوجب على مقدمي الطلبات أن تكون لهم القدرة على تقديم الطلبات والحصول على أوراق الاعتماد من أجل استخدام استعلامات الوصول إلى البيانات المعتمدة في المستقبل. |
| .46 | وهناك نوع من الاعتماد يجب تطبيقه على مقدمي الطلبات ذات الوصول عن طريق بوابات:<br>• عند قيام مقدمي الطلبات المعتمدين بالاستعلام عن البيانات، يجب تحديد الغرض الخاص بهم في كل مرة يتم فيها تقديم طلب.<br>• يجوز تطبيق أحكام وشروط مختلفة على الأغراض المختلفة.<br>• وفي حالة مخالفة مقدمي الطلبات المعتمدين للأحكام والشروط، يجب تطبيق الجزاءات. |
| .47 | لرفع معيار حماية بيانات تسجيل gTLD، يجب على كافة استعلامات/ردود RDS استخدام إجراءات تشفير وتوثيق الرسائل المتاحة بشكل عام من أجل حماية سرية وتكامل البيانات المنقولة. |
| .48 | ولتلبية احتياجات مستخدمي RDS الموثقة مع الأغراض المسموح بها، يجب على RDS توفير خدمة استعلام عكسي تعمل على البحث عن عناصر البيانات العامة والمحددة ببوابات لقيمة محددة وتخرج قائمة بكافة أسماء النطاقات التي تشير إلى تلك القيمة. |
| .49 | ولتلبية احتياجات مستخدمي RDS الموثقة مع الأغراض المسموح بها، يجب على RDS توفير خدمة WhoWas تنتج لقطات تاريخية من عناصر البيانات العامة والمحددة ببوابات لأسماء نطاقات محددة، تكون مقتصرة على البيانات التاريخية المتوفرة إلى RDS. |
| .50 | ويجب على RDS دعم الخدمات الابتكارية التي تستغل عناصر بيانات RDS، على النحو التالي.<br>• ويجب أن تكون للجهات الأخرى القدرة على توفير الخدمات الابتكارية الحالية والمستقبلية - بما في ذلك الاستعلامات العكسية وWhoWas - من خلال استخدام عناصر البيانات العامة والتمسك بالأحكام والشروط الخاصة باستخدام بيانات RDS.<br>• وفي حالة قيام هذه الجهات الأخرى بعرض خدمات ابتكارية تشتمل على عناصر بيانات عن طريق بوابات، فيجب اعتماد وتوثيق هذه الجهات الأخرى ومراعاة أحكام وشروط استخدام بيانات RDS. |
| .51 | وكافة عمليات الإفصاح عن عناصر البيانات المحددة ببوابات يجب أن تتم من خلال طرق وصول محددة من خلال RDS (بما في ذلك ما هو مشار إليه أعلاه). وإجمالي مجموعة بيانات RDS لكافة نطاقات gTLD (أو إجمالي مجموعات بيانات السجل لنطاق gTLD واحد) يجب أن لا يتم تصديرها في شكل جماعي للوصول غير الخاضع للرقابة. |

| رقم. | مبادئ الوصول إلى البيانات |
|---|---|
| .52 | وقد تتم عمليات الإفصاح من خلال عرض تفاعلي بالإضافة إلى طرق أخرى لوصول RDS.<br>• ولجعل البيانات أسهل في العثور عليها والوصول إليها بطريق متسقة، يجب عرض نقطة وصول (على سبيل المثال؛ بوابة الويب).<br>• يجب توفير الوصول للبيانات العامة أمام سائر مقدمي الطلبات من خلال طريقة استعلام غير موثقة (على الأقل من خلال موقع ويب آمن).<br>• أما الوصول الآمن المحدد ببوابات للبيانات فيجب أن يتوفر له الدعم من خلال الويب الآمن أو طرق الوصول والتنسيقات الأخرى (على سبيل المثال، ردود xml لـ RDAP، وSMS، والبريد الإلكتروني)، استنادًا إلى مقدم الطلب الموثق والغرض.<br>• ويجب أن تكون لمقدمي الطلبات القدرة على الحصول على بيانات معتمدة من RDS في الوقت الفعلي عند الاحتياج إلى ذلك.<br>• ويجب على RDS استيعاب الأتمتة لعمليات البحث من العيار الثقيل لمختلف حالات الاستخدام والأغراض المسموح بها. |
| .53 | ولكي يكون نظام RDS عالمي بحق، يجب أن تستوعب عرض بيانات التسجيل بلغات متعددة، ومجموعات خطوط وأحرف متعددة، بما في ذلك أسماء النطاقات الدولية (IDN). |
| .54 | ويجب على RDS دعم كافة سياسات الترجمة الصوتية المستقبلية المحددة من خلال GNSO لنطاقات gTLD. |
| .55 | ويجب على RDS تمكين جمع وعرض عناصر بيانات التسجيل باللغات المحلية. |

### توضيح الوصول للبيانات العامة

ووفقًا لما هو موضح في الشكل التالي، لا تزال هناك إمكانية لطلب عناصر البيانات العامة من RDS من خلال أي شخص، سواء كان بتصديق أو بدون تصديق. راجع الملحق هـ للحصول على توضيح أكثر تفصيلاً لعناصر البيانات التي تنتج عن استعلام البيانات العامة غير الموثقة.

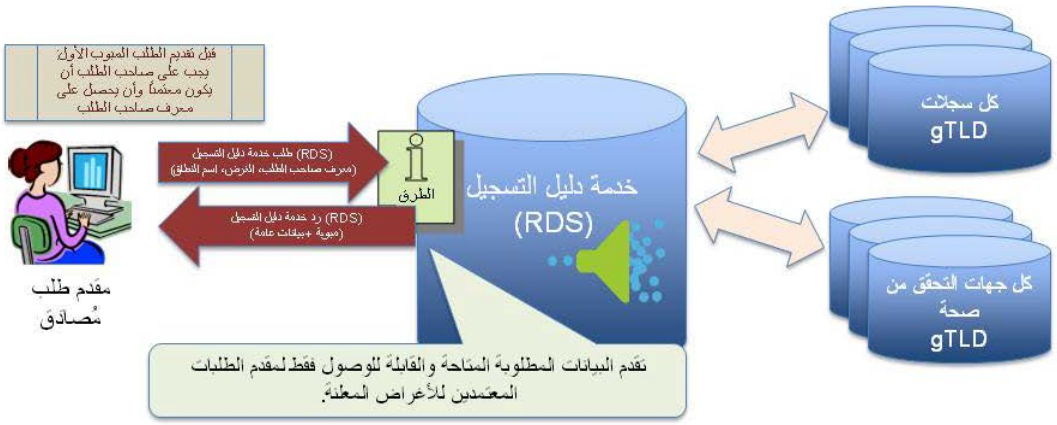



**الشكل 6. الوصول إلى بيانات التسجيل العامة غير الموثقة عن طريق RDS**

الملحق ي يحتوي كذلك على مخططات انسيابية بالإضافة إلى مثال على حالة استخدام لتوضيح الخطوات المشمولة في الوصول إلى عناصر البيانات ذات الصلة.

**توضيح الوصول للبيانات المحددة ببوابات**

وفقًا لما هو موضح في الشكل التالي، يمكن طلب عناصر البيانات المحددة من خلال بوابات عبر نظام RDS. وللقيام بذلك، يجب على مقدم الطلب أن يحصل على المصادقة والاعتماد أولاً. وبعد ذلك، يجوز لمقدم الطلب أن يقدم استعلامات معتمدة يطلب فيها عناصر البيانات لغرض محدد. راجع الملحق هـ للحصول على توضيح أكثر تفصيلاً لعناصر البيانات التي تخرج نتيجة استعلام البيانات غير الموثقة عن طريق بوابات.




**الشكل 7. الوصول إلى بيانات التسجيل المحددة ببوابات عبر RDS**

**البروتوكولات الفنية وطرق الوصول**

قامت مجموعة EWG بفحص ما إذا كانت البروتوكولات الفنية المستخدمة في النظام الحالي لتسجيل النطاقات (مثل EPP[14])، وقيد التطوير في IETF (مثل ما يتم من خلال مجموعة عمل WEIRD)، يمكن أن تدعم خصائص التصميم التي توصي بها مجموعة EWG. وقد شارفت مجموعة عمل WEIRD على الانتهاء من معيار جديد يشار إليه باسم بروتوكول الوصول إلى بيانات التسجيل (RDAP). واعتماد هذه البروتوكولات في النموذج الموصى به من مجموعة EWG قد يؤدي إلى تكاليف نقل أقل لكل من الأطراف المتأثرة.

قامت مجموعة EWG بتحليل ما إذا كانت EPP بإمكانها دعم كل عنصر من عناصر البيانات من المتضمنة في RDS الموصي به أم لا، وما إذا كان بروتوكول RDAP يمكنه دعم المبادئ الخاصة بأوراق اعتماد الوصول التي توصي بها مجموعة EWG أم لا. ويقترح تحليل EWG إمكانية استخدام كل من EPP وRDAP من خلال نظام RDS، بصرف النظر عن أي من النموذجين البديلين يتم اختياره. وعلى الرغم من ذلك، قد يتطلب القيام بذلك بضعة تمديدات أو إضافات أو استخدام "العلامات" RDAP. وهناك تقييم تفصيلي لكل من هذه البروتوكولات مضمن في الملحق ز.

[14] راجع EPP: المعيار رقم 69، طلبات RFC رقم 5730 - 5734

### ج. مبادئ اعتماد مستخدم RDS

وفقًا لما أشرنا في القسم الثالث الأغراض، تتطلب بعض الأغراض الوصول إلى كافة العناصر المحددة من خلال بوابات أو مجموعة فرعية معتمدة من عناصر البيانات المحددة ببوابات. وفقًا لما أشرنا في القسم الرابع (ب)، المبدأ رقم 46، فإن أي غرض يتطلب الحصول على وصول إلى بيانات محددة ببوابات يشترط اعتماد المستخدم. وعلى الرغم من ذلك، لا يتضمن اعتماد المستخدم وصولاً غير محدود للبيانات المحددة من خلال بوابات. فكل أشكال الوصول يجب أن تكون مستندة إلى الغرض، وأن ينتج عنها فقط عناصر البيانات المسموح بها للغرض المحدد.

وتوصي مجموعة EWG، بالنسبة لكل مجتمع لمستخدمي RDS المحددين في القسم الثالث الراغبين في الوصول إلى البيانات المحددة ببوابات لأغراض مسموح بها، يجب التشاور مع خبراء المجتمع من أجل تأكيد أغراض بيانات التسجيل المحددة من خلال EWG، وعناصر البيانات التي يجب أن تكون قابلة للوصول لهذا الغرض، والجهات المعتمدة المحتملة لمستخدمي RDS.

ومن المتحمل أن تقوم العديد من المؤسسات بإبرام عقود مع ICANN من أجل العمل كجهات معتمدة لمستخدمي RDS. وفي حين أن سائر الجهات المعتمدة لمستخدمي RDS يجب أن يسترشد بمجموعة عامة من المبادئ، إلا أن عمليات التنفيذ المتباينة قد تحدث لكل مجتمع لمستخدمي RDS. على سبيل المثال:

**السيناريو 1: جهة الاعتماد منفصلة عن مشغل الاعتماد، في حين تقوم الهيئة باعتماد المستخدمين، إلا أن أي مشغل خارجي يقوم بإدارة وصول المستخدمين المعتمدين إلى نظام RDS**

بالنسبة لمجتمع من مستخدمي RDS مثل مالكي العلامات التجارية، قد تتولى منظمة تعمل في نفس المجال المسئولية عن اعتماد الأعضاء فيها الراغبين في الوصول إلى بيانات محددة ببوابات لأغراض مسموح بها. وقد لا تلعب هيئة الاعتماد هذه أي دور في إدارة حسابات المستخدمين أو توثيق طلبات الوصول التي يتم إرسالها إلى نظام RDS. وبالأحرى، تقوم هيئة الاعتماد بإنشاء قواعد للعضوية، وشروط للخدمة، بالإضافة إلى عمليات لتقديم الطلبات والإنفاذ، إلخ، وذلك لمجتمع محدد من مستخدمي RDS. ويجوز لهيئة الاعتماد بعد ذلك الاتصال بمشغل اعتماد خارجي من أجل إنشاء وإدارة حسابات مستخدم RDS، وإصدار أوراق اعتماد وصول RDS، بالإضافة إلى توثيق طلبات وصول RDS، وتوفير التعامل من المستوى الأول لإساءة الاستخدام، بما في ذلك التعليق المؤقت للحسابات. يقوم مشغل الاعتماد ببساطة بتنفيذ وإنفاذ قواعد الوصول إلى RDS التي تقرها هيئة الاعتماد لمجتمع محدد؛ وأي طعن على تعليق حساب أو نزاعات أخرى سوف يتم تصعيدها إلى هيئة الاعتماد.

**السيناريو 2: هيئة الاعتماد مع مشغل الاعتماد، يمرران طلبات الوصول إلى RDS الموثقة إلى نظام RDS**

بالنسبة لمجتمع من مجتمعات مستخدمي RDS مثل OpSec، قد تقوم مؤسسة عامل في نفس المجال بتولي المسئولية عن اعتماد أعضائها من خلال عملية توثيق (معتمدة) تستخدمها بالفعل من أجل منح المستخدمين وصولاً إلى النظم الأخرى. في هذا المثال، تعمل المؤسسة بصفة جهة اعتماد وفي نفس الوقت مشغل اعتماد، من خلال استغلال نظام حالي مستخدم بالفعل من خلال أعضائها لوثيق ثم تمرير طلبات الوصول عبر بوابات للأغراض المسموح بها إلى نظام RDS. وهنا يتولى مستخدم RDS المسئولية عن الامتثال للأحكام والشروط، ويجب على المؤسسة العاملة في المجال وضع عملية من أجل التعامل مع حالات إساءة استخدام الوصول، وحالات الإيقاف، إلخ، المطبقة على حالات وصول RDS لمستخدم محدد.

**السيناريو 3: هيئة الاعتماد مع مشغل الاعتماد، يمرران طلبات الوصول عن طريق البروكسي إلى نظام RDS بالنيابة عن أعضائهما (أي، نموذج الإنتربول)**

بالنسبة لمجتمع من مجتمعات مستخدمي RDS مثل إنفاذ القانوني، ، قد تقوم مؤسسة منظمة وموثوقة بتولي المسئولية عن اعتماد أعضائها من خلال توثيق (معتمد) تستخدمه بالفعل من أجل منح المستخدمين وصولاً إلى النظم الأخرى. في هذا المثال، تعمل المؤسسة بصفة جهة اعتماد وفي نفس الوقت مشغل اعتماد، من خلال استغلال نظام حالي مستخدم بالفعل من خلال أعضائها لوثيق ثم تمرير طلبات الوصول عبر بوابات بروكسي للأغراض المسموح بها إلى نظام RDS. وهنا تعتبر المؤسسة هي مستخدم RDS وتقبل المسئولية عن إجراءات أعضائها فيما يتعلق بالطلبات الممررة عن طريق بروكسي مع الامتثال للأحكام والشروط. وفي حين أن نظام RDS قد لا يكون على علم بأنشطة مستخدم محدد، يجب على المؤسسة تعيين عملية للتعامل مع حالات إساءة استخدام الوصول، وحالات الإيقاف، إلخ، بطريقة تسمح للمؤسسة تدقيق عمليات وصول مستخدم محدد والتعرف على حالات إساءة الاستخدام.

لتمكين وصول مستخدم RDS المعتمد إلى عناصر البيانات المحددة من خلال بوابات لأغراض مسموح بها، توصي مجموعة EWG بالمبادئ التالية لاعتماد مستخدم RDS.

| رقم. | مبادئ اعتماد مستخدم RDS |
|---|---|
| .56 | الوصول غير المعتمد وغير الموثق إلى البيانات غير المحددة ببوابات (أي العامة) يجب أن يكون ممكناً في الوقت الفعلي. |
| .57 | واعتماد مستخدمي RDS للوصول إلى بيانات RDS لا يجب أن يتم في الوقت الفعلي لكافة حالات الاستخدام و/أو مقدمي الطلبات. |
| .58 | يجب على RDS تطبيق الحد الأدنى فقط من "مخطط الاعتماد" اللازم لتوفير الوصول لمستخدم RDS إلى عناصر البيانات المحددة ببوابات للغرض المحدد.[15] |
| .59 | ولا يجب أن يكون هناك مطلب "للموافقة المسبقة" أو توفير أوراق اعتماد لكل مستخدم محتمل لنظام RDS. ويمكن إنشاء طلب وعملية تنفيذ لكل "نوع" من مستخدمي RDS المعتمدة (أي مجتمع مستخدمي RDS). |
| .60 | الاعتماد لمستخدمي RDS الساعين للوصول إلى بيانات للأغراض المسموح بها يمكن منحها بثلاث طرق.<br>• بدون (أي الوصول غير الموثق للبيانات العامة فقط، كما هو موضح أعلاه).<br>• الاعتماد الذاتي من خلال الشخص/الكيان مقدم طلب الحصول على البيانات، مثل أي نظام يحدد فيها المستخدم ببساطة هويته، بالإضافة إلى البيانات التي يطلبها وسبب ذلك، وبعد ذلك يتم منحه وصولاً إلى هذا المستوى من البيانات. على سبيل المثال، قد ينطبق هذا على المسجلين الراغبين في الوصول إلى بيانات اسم النطاق الخاص بهم لأغراض التحكم في اسم النطاق، حيث يتم ربط الشهادة الذاتية لهم بالتسجيل الفعلي لاسم نطاق، بما يؤهلهم للحصول على أوراق اعتماد للوصول إلى تلك المعلومات في نظام RDS.<br>• الاعتماد من خلال جهة أخرى معتمدة (أي جهة اعتماد مستخدم RDS، راجع المبدأ رقم 64 أدناه). |

[15] على سبيل المثال، هذا الاعتماد لا يجب أن لا يشترط بيانات محلفة متعددة العوامل، ولا يحتاج لأن يعمل كنظام شامل متكامل للحصول على غالبية أنواع البيانات.

| رقم. | مبادئ اعتماد مستخدم RDS |
|---|---|
| .61 | متى ما كان ممكنًا، يجب على أي عملية لاعتماد RDS لجهة أخرى الاستفادة من عمليات الاعتماد الحالية داخل كل مجتمع لمستخدمي RDS المشار إليهم في القسم الثالث كمجتمع بحاجة للحصول على أوراق اعتماد. |
| .62 | ويجب منح هذه العمليات الخاصة باعتماد الجهة الخارجية من خلال الجهة المسئولة عن تنفيذ وإنفاذ سياسة اعتماد مستخدمي RDS (على سبيل المثال ICANN، هيئة لأصحاب المصلحة المتعددين) بالإضافة إلى مراجعتها بصفة دورية. |
| .63 | وأي مؤسسة تعمل كجهة توثيق لمستخدمي RDS يجب أن تكون لديها اتفاقية موقعة مع ICANN و/أو موفر خدمة RDS من أجل عرض هذه العمليات الخاصة بالتوثيق بموجب إرشادات توجيهية متفق عليها، مع وضع إطار عمل للسماح بالعمليات الواجبة، والمساءلة، والأم، والوصول العادل، والالتزام بالقوانين النافذة. |
| .64 | ويمكن لجهات الاعتماد تولي مسئولية واحدة أو كلتا المسئوليتين التاليتين.<br>• ويجوز لهيئة اعتماد مستخدم RDS تحديد وإدارة مجتمع من المستخدمين، بما في ذلك وضع معايير للعضوية، وتحديد متطلبات الاعتماد، وتحديد وإنفاذ الأحكام والشروط الخاصة بها للعضوية.<br>• يجوز لمشغل اعتماد مستخدمي RDS عرض منصة تستخدمها هيئات الاعتماد، بما يوفر وظائف مثل إنشاء حسابات المستخدمين، وإصدار أوراق الاعتماد، والتعليق والإلغاء، وإدارة دورة حياة حساب المستخدمين، والعمليات المرتبطة مثل التعامل مع النزاعات وإنفاذ ToC.<br>يجوز لجهة اعتماد محددة تولي كلتا المسئوليتين، ولكن لا يعتبر هذا شرطًا. |
| .65 | أما جهات الاعتماد الراغبة في المشاركة في التعامل مع طلبات RDS للبيانات بالنيابة عن أعضائهم فيجوز لهم القيام بذلك من خلال طريقتين:<br>• يجوز لجهة الاعتماد توفير وصول عن طريق بروكسي إلى نظام RDS عن طريق نظام التوثيق الخاص بها وقبول المسئولية الكاملة عن الاستخدام المتوافق. على الرغم من تحمل جهة الاعتماد للمسئولين في حالة إساءة الاستخدام، فإن الطلبات التي يتم تمريرها عن طريق بروكسي من خلال جهة الاعتماد بهذه الطريقة يجب توثيقها بطريق تمكن من تدقيق وحل شكاوى إساءة الاستخدام ذات الصلة بوصول المستخدمين الفرديين.<br>• كما يجوز لجهة الاعتماد توفير وصول إلى RDS عن طريق نظام التصديق الخاص بها، لكن مع ترحيل الطلبات المصدق عليها إلى نظام RDS. أما الطلبات المرسلة من خلال جهة الاعتماد بهذه الطريق فيجب أن تحدد بشكل فريد مستخدم RDS، الذي يكون مسئولاً عن الاستخدام المتوافق وسوف يتحمل المسئولية المباشرة في حالة إساءة الاستخدام. |
| .66 | وفقًا لما أشرنا في القسم الرابع (ب)، المبدأ رقم 50، يجب على نظام RDS توفير وصول في الوقت الفعلي لمقدمي الطلبات الحاصلين على أوراق اعتماد من خلال طرق متعددة. ويمكن المصادقة على الطلبات من خلال مشغل الاعتماد المناسب، ويجب على أوراق اعتماد الوصول إلى RDS الصادرة أثناء عملية المصادقة أن تكون مناسبة للاستخدام مع كافة طرق الوصول المحددة.[16] |

[16] كما يجب تحديد وتعريف واجهات المصادقة خلال عملية التنفيذ. على سبيل المثال بالنسبة لبعض طرق الاعتماد، يمكن لنظام RDS استخدام إطار عمل قياس مثل لغة ترميز تأكيد الأمن (SAML) لتمكين المصادقة من خلال مشغل الاعتماد الذي أصدر أوراق الاعتماد تلك.

| رقم. | مبادئ اعتماد مستخدم RDS |
|---|---|
| .67 | ويمكن تعريف أفضل الممارسات لإدارة أوراق الاعتماد، ويجب أن يتوقع من جهات الاعتماد الالتزام بأفضل الممارسات. |
| .68 | ويجب على RDS المطالبة بالحصول على أوراق اعتماد فريد من أجل الوصول المرخص به. |
| .69 | ولا يجب أن يكون وصول RDS المصادق عليه انتقاليًا (أي لا يجوز لمستخدم RDS مصادق عليه مشاركة بيانات محددة ببوابات مع جهات أخرى خارج الاعتماد الخاص به). |
| .70 | ويجب وضع وإنفاذ عملية للإفصاح المسئول عن البيانات المحددة ببوابات لدعم الغرض الأصلي الذي طلبت له. (على سبيل المثال، تمكين مالك IP المتحري عن انتهاك العلامات التجارية من أجل رفع شكوى UDRP، بما يسمح لمستخدم OpSec من التحري عن النشاط الجنائي المحتمل لإشعار إنفاذ القانون). |
| .71 | وأي مؤسسة تسعى للوصول إلى بيانات RDS يمكنها تقديم طلب للحصول على مصادقة مستخدم RDS والحصول على تغطية لجميع الأشخاص المستخدمين لنظام RDS في المؤسسة الخاصة بها من خلال اعتماد واحد.[17] وتتحمل كل من هذه المؤسسات المسئولية عن إدارة الوصول المعتمدة داخل المؤسسة الخاصة بها. كما أن إساءة استخدام النظام من قبل الأعضاء في مؤسسة معتمدة لمستخدمي RDS قد يؤدي إلى عقوبات ضد المؤسسة بالكامل. |
| .72 | قد يحصل مستخدم RDS واحد يلعب أدوارًا مختلفة على العديد من أوراق الاعتماد من أجل الوصول إلى أنواع مختلفة من البيانات لأغراض مختلفة. وعلى الرغم من ذلك، من الموصى به بشدة من منظور إمكانية الاستخدام توفير أوراق اعتماد فردية لكل مستخدم RDS والتي يمكن استخدامها لأغراض متعددة، بالإضافة إلى كل غرض محدد لكل وصول حسب ما هو وارد في القسم الرابع (ب). |
| .73 | يجب استخدام عمليات التدقيق وتحليلات البيانات من أجل تحديد إساءة استخدام النظام وأوراق اعتماد الوصول. |
| .74 | ويجب تحديد عملية طعون من أجل السماح لمستخدمي RDS من دحض ادعاءات إساءة الاستخدام عند السعي لإعادة تنشيط/إعادة إقرار أوراق اعتماد الوصول إلى RDS. |
| .75 | ويجب على كل مسجل الحصول على أوراق اعتماد لكي يتمكن من فحص بيانات الاتصال الخاصة به وفقًا لما هو مخزن من خلال نظام RDS فيما يتعلق بأسماء النطاقات المسجلة له. (راجع القسم الثالث، أغراض التحكم في أسماء النطاق). |
| .76 | كما يجب وضع عملية من أجل إضافة جهات اعتماد إضافيين لمستخدمي RDS تقوم إما بإكمال العمليات الحالية أو تقديم طرق جديدة ابتكارية من أجل توفير اعتماد المستخدمين للأغراض المعتمدة لـ RDS. وهذه الجهات الخاصة باعتماد مستخدم RDS يجب أن تحقق الحد الأدنى من المتطلبات وفقًا لما هو محددة في المبادئ المنصوص عليها في هذه الوثيقة. |

### د. ملخص المزايا الأساسية للمساءلة

يعد تضمين وضم الوصول الموثق لعناصر البيانات المحددة ببوابات جزءًا لا يتجزأ من نظام RDS من الجيل التالي وسوف يعمل على تحسين المساءلة من خلال مطالبة من يقوم بالوصول إلى البيانات الأكثر حساسية بتعريف أنفسهم وتحديد أغراضهم من طلب البيانات. وعلى وجه الخصوص، تشمل المزايا التي قد تنشأ عن اعتماد عناصر البيانات الموصى بها من مجموعة EWG ومبادئ الوصول ما يلي.

[17] والأمر عائد إلى المؤسسة في تأكيد وحدة ونزاهة أي من أوراق الاعتماد الصادرة للوصول إلى RDS.

- إقرار نموذج مدفوع بالأغراض لجمع البيانات والإفصاح عنها من أجل تعزيز المساءلة للكيانات التي تستخدم بيانات التسجيل لأغراض مسموح بها.
- توفير إطار عمل داعم للتوافق مع قوانين حماية البيانات في مختلف الدوائر القضائية.
- وضع طريقة لتوفير المسائلة للأشخاص الذي يصلون إلى البيانات لأغراض متنوعة. كما يوفر هذا دعمًا إضافيًا لمتطلبات حماية/خصوصية البيانات في العديد من الدوائر القضائية ويضمن توازن للمساءلة بين من يطالبون بتوفير بيانات دقيقة ومن يستخدمونها لأغراض معتمدة. ويتناول ذلك عدم إنصاف أساسي مع نظام WHOIS الحالي حيث لا يكون لمقدمي طلبات الحصول على البيانات أي مساءلة عن وصولهم واستخدامهم لبيانات جهات الاتصال.
- تزويد المسجلين وجهات الاتصال بفهم أوضح بالأغراض التي يتم من أجلها جمع البيانات والتحكم التقديري الأكبر حول ماهية المعلومات الشخصية العامة أو المحددة ببوابات.
- تحقيق الاحتياجات العامة لبيانات التسجيل من خلال مجموعة أساسية من البيانات العام، مع تقليل البيانات التي تكون عام بشكل افتراضي وتوثيق من يصلون إلى البيانات المحددة ببوابات.
- زيادة دقة البيانات، بسبب حماية عناصر البيانات الحساسة من الإفصاح العام، بما يؤدي إلى احتمال أكبر في مشاركة بيانات أكثر دقة من المسجلين وجهات اتصال PBC. وباستثناء الاستخدام لأغراض ضارة، عند حماية البيانات من النشر العام، فسوف يوفر أصحاب البيانات غالبًا معلومات أكثر دقة من أجل الحصول على مزايا توفيرها، حيث يتم الحد من خطر كبير ومعلوم.
- تحسين المرونة والكفاءة الإجمالية للاتصال بالنسبة لمستخدمي RDS والمسجلين عن طريق تضمين عناصر بيانات اختيارية جديدة لتسهيل الاتصال عن طريق طرق اتصال جديدة أو بديلة.
- دعم الاستعلامات العكسية أو استعلامات WhoWas من خلال بوابة مركزية لتمكين عمليات البحث عبر كافة تسجيلات نطاقات gTLD، من خلال مستخدمي RDS المعتمدين للأغراض المسموح بها فقط.
- تمكين قدرات الوصول المعزز لتحسين الكفاءة العامة "للنظام".
- توفير الوصول، لكل من غير الموثقين إلى البيانات العامة ومن خلال الوصول عن طريق أوراق الاعتماد إلى البيانات المحددة ببوابات، من أجل الحد من الخلط بين قدرات الوصول، ومستويات الخدمة، والتنسيقات في ردود نظام WHOIS الحالي لنطاقات gTLD، مع السماح بالتنفيذ السهل لاستعلامات RDS من خلال معيار واحد.
- توفير خدمة عالية الجودة والوصول المسئول، بما يسمح بالتخلي عن العديد من تدابير مكافحة إساءة الاستخدام الموزعة عبر النظام البيئي.

ولتحقيق هذه المزايا، فإن تثقيف مستخدمي RDS حول الأغراض المسموح بها والاستخدامات المناسبة للبيانات المستعادة من نظام RDS سيكون بمثابة أمر أساسي. العثور على جهات اعتماد على استعداد لتولي المسئولية عن اعتماد وصول RDS من خلال أعضاء المجتمع قد يكون من الأمور الصعبة. وفي البداية، قد يكون هناك ارتباك بين المستخدمين في تحديد جهة الاعتماد المناسبة، لاسيما بالنسبة للمستخدمين الذين يتعاملون مع RDS لأغراض متعددة. سوف تتطلب استعلامات RDS التلقائية أيضًا تحديث الأدوات. وعلى الرغم من ذلك، فإن هذه الاستثمارات الأولية ضرورية من أجل إنشاء وصول مدفوعة بالأغراض سوف تضع أساسًا قويًا لتحميل مستخدم RDS المسئولية عن الاستخدام المسئول لبيانات التسجيل.

## 5. تحسين جودة البيانات

توصي مجموعة EWG بتوثيق أكثر قوة لبيانات المسجل بدلاً مما يقدمه نظام WHOIS الحالي أو التعزيزات التي قد تتحقق من خلال التنفيذ الواسع لاتفاقية RAA لسنة 2013. أولاً، يجب أن يؤدي توفير جهات اتصال PBC من خلال المسجلين إلى تحسينات كبيرة على القدرة على الوصول بالنسبة لجهات الاتصال المناسبة لأغراض مختلفة ويوفر حافزًا أمام المسجلين من أجل توفير المعلومات الدقيقة لتلك الأدوار. ثانيًا، سوف يؤدي الوصول المتوفر عن طريق بوابات إلى عناصر البيانات الأكثر حساسية سيقلل حافز المسجلين على توفير بيانات غير دقيقة وزيادة مستوى مساءلة المسجلين عن دقة البيانات.

ولتحقيق هذه الأهداف، توصي مجموعة EWG بإجراء تطويرين مرتبطين ولكن مستقلين في نفس الوقت:

- ويجب أن تطبق RDS توثيق معياري لكافة بيانات تسجيل gTLD. وبالإضافة إلى عمليات الفحص الدورية، يجب أن تتم عملية التوثيق في وقت جمع البيانات، مع خيار التوثيق المسبق لمجموعات بيانات الاتصال من أجل إعادة الاستخدام التسجيلات المتعددة لأسماء النطاقات.
- ويجب أن يشتمل النظام البيئي لـ RDS على دليل جهات اتصال موثق مسبقًا ومنفصل من ناحية المفاهيم عن دليل أسماء النطاقات، لتعزيز الجودة والقدرة على إعادة استخدام عناصر البيانات المستخدمة في الاتصال مسجلي أسماء النطاقات والأشخاص أو المؤسسات التي يمكن تحديدها من خلال المسجلين كجهات اتصال PBC لأغراض مختلفة.

يمكن العثور على المبادئ والعمليات التي تسرد هذه التوصيات بالتفصيل أدناه. للحصول على أقصى فائدة، توصي مجموعة EWG بكلى التطويرين، لكنها تشير إلى أن دليل جهات اتصال أمر ممكن بدون توثيق عالي والعكس صحيح.

### أ. دقة البيانات ومبادئ المصادقة

التوثيق المسبق للمسجل أو معلومات الاتصال الأخرى أمر مرغوب من أجل:

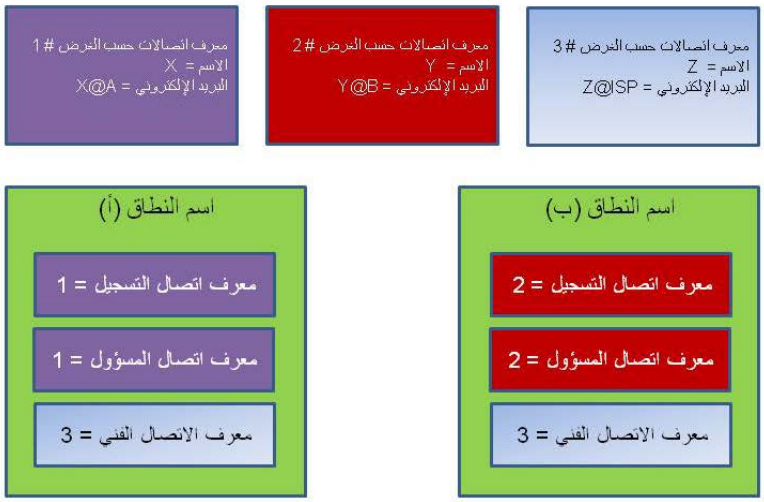
- زيادة دقة معلومات الاتصال من خلال استغلال التوثيق المسبق للتحقق من البيانات قبل الاستخدام لأسماء النطاقات الجديدة وتعزيز البيانات المتسقة عبر كافة التسجيلات (تقليل الأخطاء والتدليس)؛
- تجنب الحاجة إلى توثيق المسجل أو بيانات اتصال PBC الأخرى في كل يقوم فيها المسجل بتسجيل اسم نطاق جديد من خلال أداء عملية التوثيق لمرة واحدة وبعد ذلك إعادة استخدام هذه المجموعة من بيانات الاتصال للعديد من تسجيلات النطاقات (تبسيط العملية وتقليل متطلبات العمل)
- تجنب التأخير في التعامل مع تسجيل النطاقات، حيث إن التوثيق يجب أن يتم في وقت التسجيل.

والعديد من موفري الخدمات، والممثلين القانونيين، والأطراف الخارجية الأخرى غالبًا ما تكون هي نقاط الاتصال الأساسية للعديد من الأدوار (على سبيل المثال الفنية، والفواتير، وإساءة الاستخدام والعملية القانونية) على النطاقات المسجلة من خلال مجموعة كبيرة ومتنوعة من المسجلين (غالبًا مئات إلى مئات الآلاف من النطاقات).

وللسماح بقدر أكبر من الدقة العالية عبر هذه المساحة المتنوعة وسهولة استخدام هذه الاتصالات، من المرغوب توفير آليات من أجل السماح بالاستخدام السهل لجهات الاتصال هذه من خلال العديد من السجلات، على سبيل المثال شركة استضافة الويب التي توفر معرف فريق لـ NOC لجهات الاتصال "الفنية" و"إساءة الاستخدام" للنطاقات الخاضعة لتحكم العملاء. وعلاوة على ذلك، عندما يتعين على مثل هذا الكيان تحديث معلومات الاتصال الخاصة بها بحيث تعكس رقم هاتف/عنوان جديد أو دمج/استحواذ، فيجب أن يكون من السهل تحديث تلك المعلومات

في مكان واحد وأن يتم إظهار وعرض ذلك على كافة النطاقات المرتبطة بتلك المجموعة من بيانات الاتصال (وفقًا لما يتحدد من خلال معرف فريد).

يوضح الشكل التالي نموذجًا يمكن فيه إنشاء جهات الاتصال المستندة إلى الأغراض (PBC)، وربطها بمعرف فريدة (PBC ID)، وبعد ذلك إعادة استخدامها في العديد من تسجيلات أسماء النطاقات. ووفقًا لما هو مذكور بالتفصيل في القسم الثالث، فإن جهات اتصال PBC لا تمثل بالضرورة أشخاص فرديين، ولكن بالأحرى نقاط اتصال منشورة تم إنشاء بشكل صريح من خلال حاملي جهات الاتصال والغرض منها هو تمكين الاتصال للأغراض ذات الصلة بنظام DNS.




ينعكس تحديث معرف الاتصالات حسب الغرض # 3
تلقائيًا في بيانات التسجيل الخاصة
بأسماء النطاقات (أ) و(ب)

| رقم. | مبادئ لمعرفات جهات الاتصال والبيانات المرتبطة بها |
|---|---|
| .77 | يجب أن تكون إدارة جهات الاتصال مجدية وممكنة بشكل منفصل عن إدارة النطاق، بما يسمح بإمكانية انتقال ومساءلة جهة الاتصال بشكل منفصل عن أسماء النطاقات وخضوعها للإدارة من خلال الأفراد أو الكيانات الفعلية المدرجة بموجب جهات الاتصال تلك. |
| .78 | يجب إدارة جهات الاتصال من خلال جهات موثقة تقوم بإدارة قواعد بيانات جهات الاتصال، وتنفيذ أنظمة للتوثيق، بالإضافة إلى الحفاظ على المعلومات في مستوى الصحة لكل من جهة الاتصال وعناصر البيانات الخاصة بها (والتي يمكن الوصول إليها من خلال RDS).[18] |
| .79 | ويمكن ربط سجلات النطاق بمعرفات جهات الاتصال من خلال مسجليهم واعتمادهم من خلال جهات الاتصال المخصصة لأغراض متنوعة مرتبطة باسم نطاق. |
| .80 | ويجب أن تحتوي جهات الاتصال تلك على عناصر بيانات إلزامية. وسيتعين توفير السياسات والإشراف من أجل إدارة هذه العمليات لضمان أن معرفات جهات الاتصال لا تستخدم بدون تفويض جهة الاتصال وتحقيق الحد الأدنى من المعايير. |

[18] ملاحظة: يمكن لأمناء السجلات أن يكونوا ومن المفترض أن يكونوا جهات توثيق معتمدة من أجل توفير خدمات التوثيق لجهات الاتصال المرتبطة بأسماء النطاقات التي يقومون بتسجيلها.

| رقم. | مبادئ لمعرفات جهات الاتصال والبيانات المرتبطة بها |
|---|---|
| .81 | وتخضع إدارة التغيير والتفويض لاستخدام معلومات جهة الاتصال عن طريق حامل جهة الاتصال ويؤثر على كافة النطاقات المرتبطة بجهة اتصال. العمليات والسياسات لضمان الحصول على تنفيذ دقيق وموثوق وفي الوقت المناسب للتغييرات المرغوبة بدون تحميل أعباء على جهات اتصال PBC أو المسجلين فيجب وضعها من أجل دعم هذا النموذج الجديد. |
| .82 | وكل مجموعة فردية من بيانات جهات الاتصال يجب أن يكون لها معرف اتصال يحدد بشكل فريد كل من جهة التوثيق وحامل الاتصال لتمكين استعادة وتحديث بيانات الاتصال المرتبطة. ويجب نشر هذا المعرف الخاص بجهة الاتصال في أي من المعارض العامة لبيانات RDS. |

### ب. عملية التوثيق المسبق

للتعامل مع هذه الاحتياجات، يوصى القيام بعملية التوثيق المسبق التالية:

أ) يقوم كل مقدم طلب بتقديم بيانات الاتصال من خلال جهة توثيق من اختياره (على سبيل المثال، أمين السجل أو السجل أو موفر خدمة إدارة جهات اتصال خارجي).

ب) تتم عملية التوثيق التركيبي والتشغيلي (حسب SAC-058) من خلال جهة التوثيق.

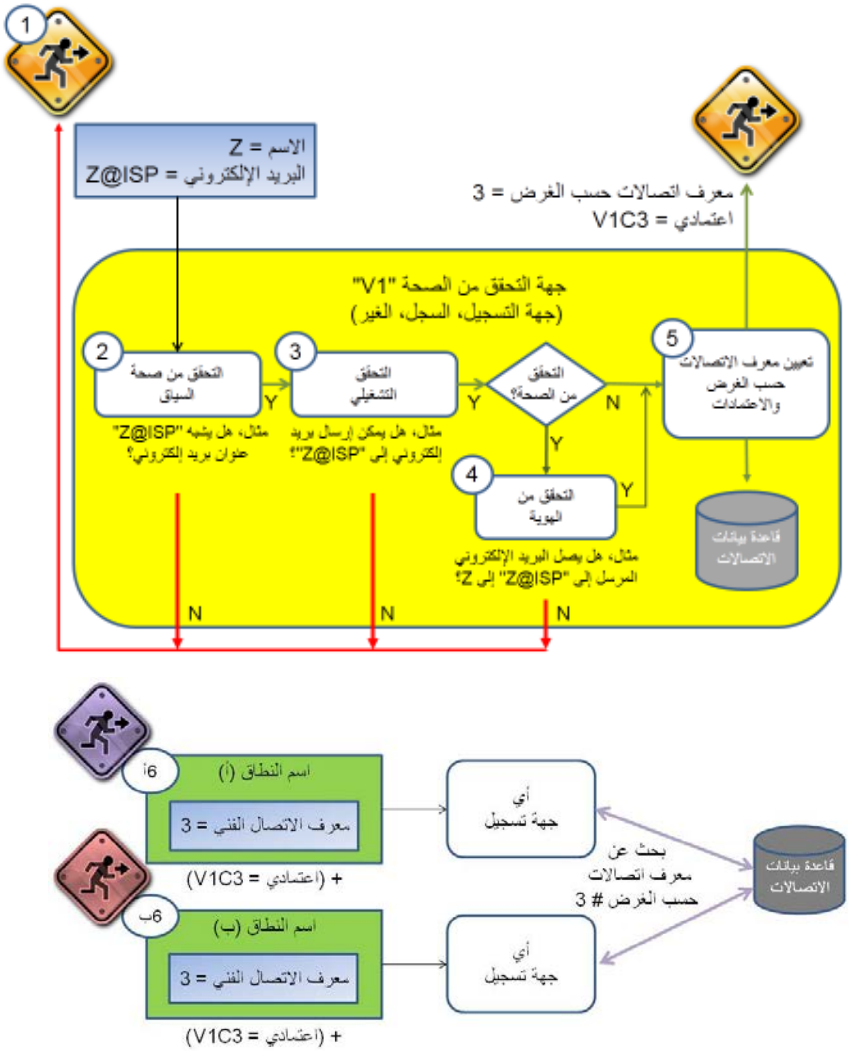
ج) **اختياري**: يمكن تنفيذ توثيق الهوية من خلال جهات التوثيق، من خلال استغلال جهات مثل مكاتب البريد، ومديري ccTLD، وشركات الهواتف، ومكاتب الضريبة، إلخ. لاحظ أن جهات الاتصال التي حقق معايير توثيق الهوية الاختيارية يمكن تخصيصها على هذا النحو في الحالة الخاصة بها من أجل زيادة ثقة المستخدمين، وهو ما يعمل على تسهيل التجارة عبر الإنترنت. لاحظ أيضًا أن هذه الخدمات ذات القيمة المضافة من المتحمل أن تكون لها كلفة مرتبطة بها وقد تتحملها الجهة المطالبة بهذا المستوى الإضافي من التوثيق.

د) وبعد التوثيق التركيبي الناجح وأي من عمليات التوثيق التجريبي المطلوبة، يتم إصدار معرّف لمجموعة بيانات جهات الاتصال (جهة الاتصال) من خلال جهة التوثيق، والتي تحدد بشكل فريد كل من جهة التوثيق وجهة الاتصال من أجل تمكين الاستعادة والتحديث التالي.

ه) وتقوم جهة التوثيق بتخزين بيانات الاتصال في قاعدة البيانات الخاصة بها، وإصدار أوراق الاعتماد (حسب ما ينطبق، من أجل تمكين التحديث في المستقبل لجهات الاتصال)، بالإضافة إلى ترحيل المعرف الفريد إلى مقدم الطلب (والمعروف من الآن فصاعدًا باسم حامل الاتصال).

و) ويقوم حامل الاتصال بتوفير معرف الاتصال هذا إلى المسجلين، والذين يمكنهم بعد ذلك المتابعة إلى أي أمين سجل، وذلك من خلال استخدام هذا المعرف الفريد، لتسجيل أسماء النطاقات من خلال استخدام معرفات الاتصال كجهات اتصال مستندة إلى الأغراض (أي PBC) مخصصة. وفقًا لما هو محدد في القسم الثالث، يجب الاستعانة بعملية توثيق من أجل ضمان موافقة المسجل وجهات الاتصال المعينة على الأغراض التي سوف يقبلها PBC لكل اسم نطاق.

ز) ويمكن تعيين جهات الاتصال الموثقة كجهات اتصال PBC لاسم نطاق (على سبيل المثال؛ مسجل، فني، مشرف، شركة أعمال، إساءة الاستخدام، القانونية، موفر الخصوصية/البروكسي) باتباع المبادئ الخاصة بجهات الاتصال المستندة إلى الأغراض وفقًا لما هو محدد في القسم 3 (هـ).




لاحظ أن كل جهة توثيق تحافظ على قاعدة بيانات جهات الاتصال الخاصة بها. كما يجب توفير هذه البيانات إلى نظام RDS، إلا أن الآلية تتوقف على نموذج RDS وفقًا لما هو محدد في القسم السابع. على سبيل المثال في النموذج المتكامل، يمكن دفع إضافات وتحديثات بيانات الاتصال من خلال EPP إلى RDS. وفي النموذج الفيدرالي، يمكن سحب بيانات الاتصال من خلال RDS في الوقت الفعلي عبر RDAP.

### ج. الدقة، والتدقيق وعملية التصحيح

يوصى بالعمليات التالية لضمان الدقة المتواصلة لبيانات التسجيل وتصحيح بيانات التسجيل غير الدقيقة:

أ) **التصحيح الذاتي**: يستخدم حاملو جهات الاتصال جهة التوثيق من أجل تصحيح/تحديث بياناتهم من خلال استخدام أوراق الاعتماد الصادرة في السابق. وتتدفق المعلومات تلقائيًا إلى كافة النطاقات من خلال استخدام جهة الاتصال الخاصة تلك (وفقًا لما يتحدد من خلال معرفة جهة الاتصال الفريدة).

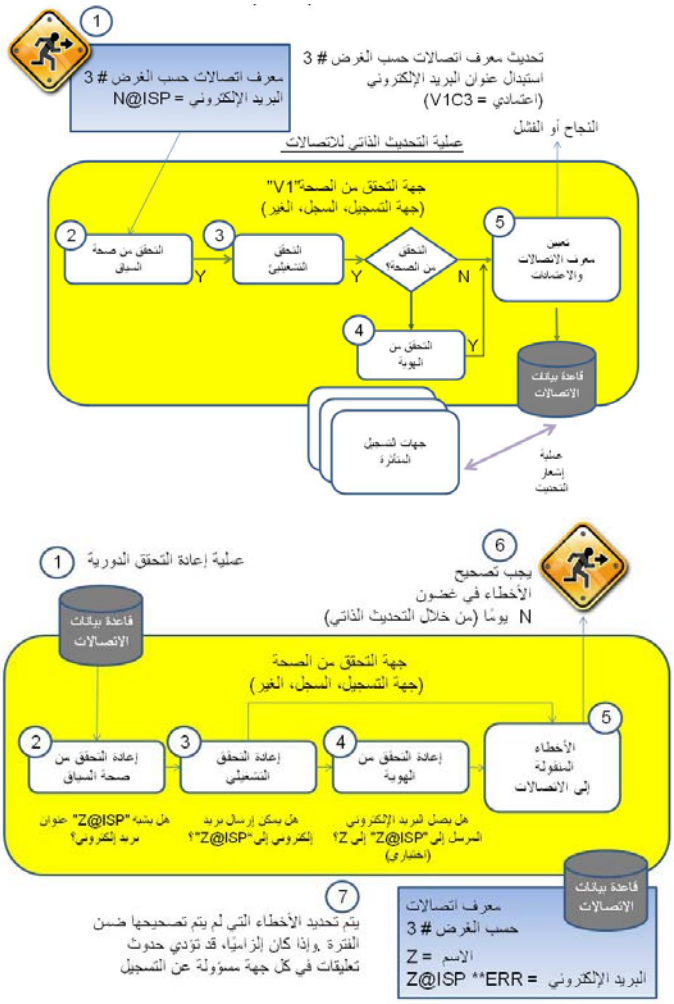
ب) **العملية المراقبة**: تقوم جهات التوثيق بإجراء توثيق تشغيلي واختياري للهوية بشكل دوري على مجموعات جهات الاتصال المدارة من خلال خدمتها. ملاحظة: ولا يجب أن تكون هذه الإجراءات الخاصة بالتوثيق مرهقة بشكل زائد، لكن يمكن أن تنعكس في الحالات المنشورة لأي جهة اتصال (على سبيل المثال، تصبح جهة الاتصال صحيحة من الناحية التشغيلية اعتبارًا من 1 يناير 2016).

ج) وتقوم جهات التوثيق بالإبلاغ عن أية بيانات غير دقيقة يتم اكتشافها إلى حامل الاتصال، بما يوفر فترة محددة من الوقت (على سبيل المثال، 14 يومًا) أمام حامل الاتصال حتى يقوم بتصحيح عدم الدقة. ويجوز إشعار أي من المسجلين أو السجلات أو أمناء السجلات للنطاقات المتأثرة بذلك. ويستخدم حامل جهة الاتصال جهة التوثيق المحددة مسبقًا من أجل تصحيح عدم الدقة من خلال استخدام أوراق الاعتماد الصادرة في السابق.

د) إذا ظلت بيانات التسجيل غير دقيق بعد الموعد النهائي، يتم تمييز البيانات بأنها غير دقيقة. فإذا كانت البيانات المميزة إلزامية بالنسبة لأي PBC تشير في الوقت الحالي إلى معرف جهة اتصال، يتم وضع النطاقات المرتبطة بها في عملية تصحيح تقوم بإشعار المسجل بعدم الدقة وتسمح له بتصحيحها في فترة زمنية منصوص عليها في اتفاقية RAA. وقد يؤدي الإخفاق في التصحيح إلى عقوبات على اسم النطاق والتي قد تشمل التعليق أو الحذف حسب اتفاقية RAA المعمول بها.

ه) وبمجرد استبدال البيانات المميزة ببيانات صحيحة، تتم إزالة العقوبات من النطاقات المتضررة.

و) وفي حالة تقارير الدقة المقدمة من أجل امتثال ICANN، يتم إشعار جهة التوثيق من أجل تكرار التوثيق التركيبي والتشغيلي. وإذا نجحت عملية إعادة التوثيق، يجوز للطرف المقدم لتقرير الدقة اتخاذ إجراءات أخرى حسبما يتناسب مع موقفه (على سبيل المثال، تقديم شكوى UDRP أو تقديم طلب كشف). وفي حالة فشل عملية إعادة التوثيق، يجب إشعار مسجلي جميع أسماء النطاقات المستخدمين لمعرف اتصال غير دقيق واتباع عملية التصحيح العادية الموضحة أعلاه.



### د. إطار العمل التشغيلي لمعرفات الاتصال

يوصى بإطار العمل التالي من أجل إدارة معرفات الاتصال وربطها بمعلومات التسجيل:

أ) يجب أن تكون معرفات الاتصال فريدة عبر كافة جهات التوثيق من أجل ضمان إمكانية نقل معرفات الاتصال وتوفير مخططات تعريفية بين أسماء النطاقات ومعلومات الدليل الضرورية.

ب) معرفات الاتصال التي تعرف كل من الاتصال وجهة التوثيق يجب ربطهما بمجموعات منفصلة من معلومات الاتصال من أجل تمكين الاستعادة والتحديث. تفسير: يقوم معرف جهات اتصال برسم مخطط بمجموعة من بيانات الاتصال تكون قابلة للاستخدام من أجل التعبير عن جهات اتصال أسماء النطاقات المخصصة. والمعلومات التي ينقصها هذا المطلب غير ذات فائدة من الناحية التشغيلية.

ج) ويجب إصدار معرفات جهات الاتصال من خلال جهات توثيق معتمدة. ويجوز لأي كيان تقديم طلب لكي يصبح جهة توثيق، مع مراعاة المعايير المماثلة للمعايير المستخدمة في اعتماد أمناء السجلات. ويجوز لجهات التوثيق المعتمدة ضم أمناء السجلات والسجلات وموفري خدمة التوثيق الخارجيين. المبرر المنطقي: جهة التوثيق عبارة عن وظيفة ضرورية لإنشاء قاعدة بيانات لجهات الاتصال. وقد يتفاوت مستوى التوثيق حسب جهة الاتصال، إلا أن العملية يجب أن تكون متجانسة فيما بين جهات التوثيق من أجل ضمان الدقة والمساءلة لمسجلي النطاقات والجهات التوثيق المخصصة لها.

د) ولكي يتم الربط مع أسماء النطاقات، يجب على أي مسجل أو جهة اتصال PBC مخصصة الحصول على معرف اتصال.

ه) ويجوز تعيين معرفات اتصال للعديد من الأدوار بالنسبة لنطاق واحد أو العديد من النطاقات. على سبيل المثال، يمكن استخدام معرف PBC محدد كمعرف لمسجل بالنسبة لنطاق واحد، وجهة اتصال فنية وإساءة استخدام لنطاقات أخرى.

و) ويمكن إنشاء جهات اتصال وتعديلها في أي وقت، ويشمل ذلك ما هو جزء من عملية تسجيل النطاقات.

### ه. التفاعل مع جهات التوثيق

توصي مجموعة EWG بالمبادئ التالية لتفاعل جهات التوثيق مع حاملي الاتصالات (أي الأطراف التي تنجح في إنشاء مجموعات موثقة وقابلة للاستخدام من بيانات الاتصال).

| رقم. | مبادئ التفاعل بين حاملي جهات الاتصال وجهات التوثيق |
|---|---|
| 83. | بالنسبة لأي معرف اتصال محدد، يجوز لأي حامل لجهة اتصال اختيار أي جهة توثيق[19]. |
| 84. | ويجب وضع سياسات إشراف ومساءلة ذات صلة بإدارة معرفات جهات الاتصال. |
| 85. | ويجب أن تكون لحاملي جهات الاتصال القدرة على تعديل معلومات جهات الاتصال المرتبطة بمعرف الاتصال من خلال إصدار جهة اعتماد. |
| 86. | ويجب على جهات التوثيق استخدام توثيق حامل جهة الاتصال من أجل إيقاف التعديل غير المرخص به لمعلومات جهات الاتصال المرتبطة بأي معرف لجهة اتصال. |

[19] وحسب المبدأ رقم 88، تحدد معرفات الاتصال كل من جهة التوثيق وحامل جهة الاتصال. ويجب تنفيذ ذلك بطريقة تتيح إمكانية النقل معرفات الاتصال فيما بين جهات التوثيق.

| رقم. | مبادئ التفاعل بين حاملي جهات الاتصال وجهات التوثيق |
|---|---|
| .87 | ويجوز لجهات التوثيق عرض مستويات متعددة من توثيق حامل جهة الاتصال، والتي تتراوح من توثيق PIN إلى توثيق من عاملين. ويجب أن تكون لحاملي جهات الاتصال القدرة على اختيار الموفرين استنادًا إلى مخصصات التكلفة/الفائدة المرتبطة بسهولة الاستخدام، والأمن، والتكاليف، والعوامل المنطقية الأخرى للأعمال. |
| .88 | ويجب على جهات التوثيق نشر السياسات الخاصة بها عند التوثيق بطريقة يمكن استغلالها عالميًا من أجل إدارة السمعة. وسوف يشجع ذلك على مستوى أفضل من الدقة والمساءلة لمعلومات الاتصال المدرجة. |
| .89 | ويتعين أن تكون لجهات التوثيق القدرة على توثيق معلومات الاتصال المقدمة باللغة الأصلية لحامل جهة الاتصال. ويجب أن يحسن ذلك من دقة بيانات اللغة الأصلية ودعم إمكانية التوسع بالنسبة لنظام تسجيل أسماء النطاقات إلى بيئة متعددة اللغات. على سبيل المثال، يمكن لأمناء السجلات العمل مع جهات التوثيق في مواقع متنوعة من اجل توفير خدمات توثيق موسعة إلى أعداد كبيرة من المسجلين وجهات اتصال مخصصة دون الحاجة إلى الاستثمار في الأدوات المكلفة من أجل توثيق البيانات بلغات غير معرفة بالنسبة للفرق الخاصة بهم. |

### و. مبادئ توثيق جهات الاتصال

يمكن توثيق بيانات الاتصال في ثلاث مستويات مختلفة: التركيبية والتشغيلية والهوية حسب المعيار SAC 058. توصي مجموعة EWG بمبادئ مستوى التوثيق.

| رقم. | مبادئ توثيق جهات الاتصال |
|---|---|
| .90 | كافة عناصر البيانات المرتبطة بمعرف جهة اتصال يجب توثيقها في مستوى تركيبي. وهذا يمثل مستوى أساسي من التوثيق يجب أن يكون قابل للتنفيذ من خلال جهة تعمل في نفس المجال. |
| .91 | وأية عناصر لبيانات الاتصال الإلزامية المرتبطة بمعرف جهة اتصال بالنسبة لغرض خالص يجب توثيقها على المستوى التشغيلي[20] قبل أن يمكن تضمين هذا المعرف الخاص بالاتصال ببيانات تسجيل اسم نطاق لهذا الغرض. |
| .92 | يجوز لحامل جهة اتصال السعي اختياريًا للحصول على مستويات أعلى من التوثيق (على سبيل المثال، التوثيق الاختياري للهوية)، مع تحمل التكاليف المرتبطة في مقابل المزايا المستحصل عليها (على سبيل المثال ثقة العمل في أسماء النطاقات المسجلة للكيانات ذات الهوية الموثقة)[21]. |
| .93 | بالنظر إلى التكاليف المشمولة في عملية توثيق الهوية الاختيارية، يجب توفير آلية منخفضة التكلفة بالنسبة لحاملي جهات الاتصال غير المتميزة من الناحية الاقتصادية للحصول على توثيق اختياري للهوية. |
| .94 | وللحفاظ على الروابط والسماح بعملية تصحيح، يمكن لأي معرف جهة اتصال الحصول على حالة "غير دقيق" وأن يظل في النظام. |
| .95 | كما يجب تعقب حالة توثيق معرف جهة الاتصال ونشرها حسب ما يتناسب عند الاطلاع على معلومات RDS، بالإضافة إلى أقرب وقت تم فيه تقرير حالة التوثيق. |

[20] برجاء الرجوع إلى SAC 058 و ملخص توثيق بيانات WHOIS لـ ccTLD/نتائج استطلاع التوثيق للتعرف على الطرق الممكنة في تنفيذ التوثيق التشغيلي وممارسات ccTLD الحالية.

[21] على سبيل المثال، يمكن أن يكون توثيق الهوية الاختياري إضافة محددة الأسعار بشكل منفصل أو تضمينها في حزم تسجيل أسماء النطاقات أو عرضها كحافز بالنسبة للعملاء ذوي الأحجام الكبيرة. راجع طلب الحصول على المعلومات حول توثيق بيانات الاتصال ونظم التوثيق للتعرف على أمثلة للخدمات التجارية التي تؤدي هذا التوثيق.

| رقم. | مبادئ توثيق جهات الاتصال |
|---|---|
| .96 | ويجوز للجهات الأخرى تقديم تقارير عدم دقة من أجل رفض حالة توثيق معرف اتصال وفقًا لما هو منصوص عليه في القسم الخامس (ج)، مما يعجل بعملية تصحيح قياسية قد تؤدي إلى تمييز معرف الاتصال برمز "غير دقيق" وعواقب أخرى لأسماء النطاقات التي تستخدم معرفات الاتصال كجهات PBC. |
| .97 | ولا يمكن للنطاقات النشطة أن تحول لها اتصال إلزامي مع حالة "غير دقيق" دون نوع ما من التصحيح. وعلى الرغم من ذلك، يمكن تقرير المخطط في مكان ما. |
| .98 | ويجب التحقق من مستوى عند الحد الأدنى من التوثيق المتقاطع لكافة عناصر بيانات الاتصال المرتبطة بمعرفات الاتصال حيث يسري التوثيق المتقاطع (على سبيل المثال العنوان المادي). |
| .99 | يجب تنفيذ عملية إعادة توثيق بيانات الاتصال بصفة منتظمة من خلال جهة التوثيق المعنية من أجل ضمان دقة البيانات في المستوى المعلن. |
| .100 | وفي حالة تقديم حامل الاتصال عناصر بيانات اختيارية، يجب أن تكون تلك العناصر موثقة من الناحية التركيبية على أقل تقدير. ولا يتم توثيق عناصر البيانات الاختيارية لما هو أبعد من التركيب ما لم تطلب جهة الاتصال وتسدد افتراضًا أي تكلفة مرتبطة بهذا التوثيق. |
| .101 | كما أن مستوى التوثيق المحقق بما يتجاوز التوثيق التركيب لعناصر البيانات التي قد تكون موثقة الهوية من الناحية التشغيلية - أو (اختياريًا) فيجب تسجيلها والاحتفاظ بها بمعرفة جهة التوثيق. على سبيل المثال، يمكن توثيق عناصر مثل البريد الإلكتروني والهاتف والعنوان على المستوى التشغيلي، في حين أن اسم أو اسم مؤسسة لا يمكن توثيقه من الناحية التشغيلية بل يمكن توثيق هويته اختياريًا. |
| .102 | بالإضافة إلى ذلك، يجب على جهة التوثيق تحديد ونشر حالة التوثيق الإجمالية كعنصر لبيانات RDS والتي يتم تحقيقها من خلال كل معرف جهة اتصال. على سبيل المثال، في حالة اجتياز كافة عناصر البيانات الإلزامية التي يمكن توثيقها من الناحية التشغيلية لهذه الفحوصات، فسوف تكون حالة التوثيق الإجمالية لجهة الاتصال "تم التوثيق على المستوى التشغيلي". وفي حالة فشل أي من عناصر البيانات الإلزامية التي يمكن توثيقها من الناحية التشغيلية، فسوف يتم تنزيل رتبة حالة التوثيق الإجمالية لجهة الاتصال إلى "تم التوثيق على المستوى التركيبي". أما إذا اجتازت كافة عناصر البيانات الإلزامية التي يمكن توثيق هويتها لهذا الفحص الاختياري، فسوف تتم ترقية حالة التوثيق الإجمالية لجهة الاتصال إلى "تم توثيق الهوية". ولتعزيز دقة الدقة والاتصاف الكافي، يجب إتاحة وتوفير حالة التوثيق الإجمالية بالنسبة لمستخدمي RDS كأحد عناصر البيانات الموحدة الجديدة لكل جهة اتصال.[22] |
| .103 | بالنسبة لأي عنصر بيانات مر بعملية التوثيق، فإن التمييز الزمني لهذا التوثيق يجب توثيقه أيضًا والاحتفاظ به بمعرفة جهة التوثيق. |
| .104 | والتمييز الزمني لأحدث عمليات التغيير على حالة التوثيق الإجمالية لمعرف اتصال كامل يجب أيضًا أن يتحدد من خلال جهة التوثيق ونشره كعنصر بيانات لـ RDS حسب جهة الاتصال. |

[22] كما نظرت مجموعة EWG أيضًا في مسألة نشر عناصر بيانات RDS من أجل إيصال حالة التوثيق الفردية لكل عنصر من عناصر بيانات الاتصال الفردية (على سبيل المثال حالة عنوان البريد الإلكتروني لـ PBC = تم التوثيق على المستوى التشغيلي، حالة اسم PBC = تم توثيق الهوية). ونشر حالة التقسيم في هذا التقسيم سوف يتطلب بروتوكولاً كبيرًا، وعنصر بيانات بالإضافة إلى طلب عميل / تغييرات في واجهة GUI وما إلى ذلك غير موصى به في الوقت الحالي، لكنه قد يحتاج إلى دراسة مستفيضة.

### ز. قدرة بيانات الاتصال الفريدة

وللتغلب على انتحال الشخصية، والتشهير وإساءة الاستخدام، يجوز لحامل جهة الاتصال تحديد أن تكون بيانات الاتصال الخاصة بهم فريدة ويجب ألا تستخدم من خلال مدعين آخرين من حاملي جهات الاتصال.

أ) وقد تشتمل البيانات الفريدة أيضًا على العديد من العناصر لمجموعة الاتصال، لاسيما عنوان البريد الإلكتروني ورقم الهاتف. تفرد وعدم تكرار العناوين والأسماء قد يكون صعب ضمانه أو مستحيل.

ب) وفي حالة طلب حامل جهة الاتصال لتخصيص بالتفرد، فيجب أن تكون هناك آلية يتم توفيرها لجهات التوثيق الأخرى من أجل مقارنة مجموعة بيانات جهة الاتصال المطلوبة في مقابل بيانات الاتصال الخاصة بحامل الاتصال، من أجل ضمان عدم تعدي مقدمين جدد لمعرف الاتصال (أو حاملي اتصال حاليين يعدلون المعلومات الخاصة بهم) على البيانات المحمية بشكل فريد.[23]

ج) وأية بيانات يتم تخصيصها بأنها فريدة يجب أن تكون موثقة الهوية من أجل الحماية من انتحال الشخصية وأنواع هجوم "رفض الخدمة" (عدم قدرة جهة الاتصال الصحيحة على استخدام بياناتها الصحيحة).

### ح. ملخص المزايا الأساسية لجودة البيانات

إن اعتماد نظم إدارة وتوثيق معرفات جهات الاتصال باعتبارها جزء لا يتجزأ من نظام RDS من الجيل التالي سوف يعمل على تحسين مستوى جودة البيانات من خلال جعل الأمر أكثر صعوبة على المسجلين في إدارة بيانات مغلوطة في نظام RDS والحد من حالات التدليس والسطو على الهوية. وعلى وجه الخصوص، تشمل مزايا اعتماد دقة البيانات الموصى بها من مجموعة EWG ومبادئ التوثيق ما يلي.

- زيادة قدرة الأفراد والمنظمات على التحكم والحفاظ على بيانات الاتصال الخاصة بهم بصرف النظر على المكان الذي يتم استخدامها فيه في النظام البيئي لأسماء النطاقات.
- جعل الأمر أكثر صعوبة على المحتالين في الحصول على أسماء النطاقات، حيث إن كافة جهات الاتصال يجب توثيقها في أقل مستوى عند الإنشاء أو عمليات التحديث. يجب أن تتيح متطلبات اعتماد جهة التوثيق تحديد الهوية والعقوبات على جهات التوثيق المارقة أو المنحلة والتي لا تفي بالمعايير التشغيلية. وفي حالة تحديد المحتالين من خلال تسجيل نطاق واحد، فقد يتم التعرف على النطاقات الأخرى التي يملكها نفس المحتال والحد منها عن طريق جهات اتصال PBC العامة.
- إنشاء بيانات أكثر اتساقًا عبر العديد من أسماء النطاقات المسجلة من خلال مسجل محدد. وفي حين قد يكون هناك بعض التكاليف المباشرة لعملية توثيق جهة اتصال محددة، إلا أن توفير معرف اتصال فردي ومحمول يتيح الفرصة أمام عمليات التسجيل الإضافية غير الخلافية ويجب أن يقلل بشكل كبير من تكليف الصيانة المستقبلية للعديد من المسجلين.
- تحسين القدرة على التعرف على معلومات الاتصال غير الصحيحة بمرور الوقت وتطبيق عمليات تصحيح على المجموعة الكاملة للنطاقات من خلال استخدام معلومات الاتصال تلك. متطلبات لعمليات فحص التوثيق الدورية من خلال جهات التوثيق، أو متى ما تم إجراء عمليات تحديث، فيجب أن تلقي الضوء على مشكلات معلومات الاتصال القديمة وتطبيق كافة التحديثات على كافة تسجيلات أسماء النطاقات المتأثرة من خلال تغيير واحد.

---

[23] وهذا التفرد في الفحص يمكن القيام به بسهولة نسبيًا في نموذج RDS المتزامن، لكنه قد يكون أكثر صعوبة في الأداء في نموذج RDS الفيدرالي.

- التكلفة وتحسينات الكفاءة للنظام البيئي بالكامل. في حين أن طرح تطورات جديدة على نظام التسجيل الإجمالي، يمكن فصل إدارة جهات الاتصال عن غدارة تسجيل النطاقات، بما يسمح بتطبيق التحديثات الكبيرة على النطاقات مع السماح بإمكانية توطين عملية إدارة بيانات الاتصال.
- القدرة بالنسبة لموفر الخدمات على التحديث السلس لتفاصيل الاتصال مع الاضطرار إلى تحديث تسجيلات النطاقات الفردية بالنسبة للنطاقات التي تظهر فيها كجهة اتصال مستندة إلى الأغراض. وفي العديد من مواقف موفري الخدمات، قد يتيح هذا الأمر الفرصة للتحديثات السهلة لآلاف أو حتى ملايين من أسماء النطاقات.
- تقليل مستوى إساءة الاستخدام التي تحدث عن طريق انتحال الشخصية في بيانات التسجيل من خلال توفير توثيق اختياري للهوية. وفي حين أن التوثيق الاختياري للهوية قد يقتضي تكاليف بالنسبة لحامل جهة الاتصال التي تحصل عليه، إلا أن القدرة على تقليص إساءة الاستخدام عبر انتحال الشخصية (السطو على الهوية) يحدث بشكل روتيني من خلال الكيانات ذات المؤهلات الكبيرة، وكبار موفري الخدمات، أو الأفراد ذوي الأهداف الخبيثة، سوف تكون جديرة بالإنفاق.
- كما أن فصل إدارة وتوثيق بيانات الاتصال عن تسجيل/إدارة أسماء النطاقات يعمل عن قرب على محاذاة أصحاب البيانات مع البيانات الخاصة بهم، بما يسمح لتطبيق أسهل لقانون حماية البيانات ذي الصلة حيث يمكن التعرف على أماكن جهات التوثيق في الدوائر القضائية المحلية بالنسبة لحامل جهة الاتصال، بصرف النظر عن أمين السجل أو موقع السجل.
- كما يمكن لجهات التوثيق تقديم الخدمات بلغاتها الأصلية لحاملي جهات الاتصال والمسجلين، بما يعمل على تحسين جودة البيانات ودقتها، وبذلك يقلل من تكلفة التوثيق. وقد يتيح ذلك الفرصة أمام أمناء السجلات على توفير خدمات باللغات التي لا يمكنهم دعمها أو توثيقها بها بسهولة، وذلك من خلال مجموعة موزعة من جهات التوثيق.

## 6. الاعتبارات القانونية والتعاقدية

في العمل الذي قامت به مجموعة EWG، فقد استرشدت ببعض المبادئ القانونية المحورية:

| |
|---|
| يجب أن تكون البيانات الشخصية:<br>• تم التعامل معها من الناحية القانونية، وبشكل منصف وبطريقة شفافة فيما يتعلق بصاحب البيانات،<br>• أن يتم جمعها لأغراض محددة وواضحة وشرعية وأن لا تتم معالجتها بطريقة أخرى غير متوافقة مع تلك الأغراض،<br>• أن تكون ملائمة وذات صلة ومقتصرة على الحد الأدنى المطلوب فيما يتعلق بالأغراض التي تمت معالجتها من أجلها<br>• وأن تكون دقيقة وأن تظل حديثة حسب المطلوب للأغراض المحددة. |
| المعالجة القانونية، بما في ذلك التنازل والإفصاح عنها يمكن تستند - مع مراعاة الاختصاص القضائي المعني - إلى ما يلي:<br>• موافقة صاحب البيانات،<br>• ضرورة تحرير عقد يكون صاحب البيانات طرفًا فيه<br>• ضرورة الامتثال لالتزام قانوني تكون فيه الجهة المتحكمة طرفًا. |
| الحق في الوصول والاطلاع على المعلومات والحق في تصحيح عدم الدقة بالنسبة لصاحب البيانات يجب أن يكون مضمونًا. |

توصي مجموعة EWG بوجوب مراعاة هذه المبادئ والمبادئ الأخرى ذات الصلة الموجودة بشكل عادي في قانون حماية البيانات وذلك عند صياغة السياسات النهائية وعمليات التنفيذ بالنسبة لنظام RDS. بالإضافة إلى ذلك، من المعترف به تمامًا أنه في بعض الاختصاصات القضائية، تمتد حقوق الخصوصية إلى الأشخاص الاعتباريين وإلى الكيانات فيما يتعلق بحرية التعبير وحرية تكوين الجمعيات والانتماء إليها. وتقر مجموعة EWG بكلتا هاتين المجموعتين المنفصلتين من الحقوق، والتي تحظي بالحماية بشكل منفصل ومختلف في جميع أنحاء العالم.

وبالنظر إلى هذا الأساس، قامت مجموعة EWG بتقييم الخيارات وقامت بعد ذلك بصياغة مبادئ RDS للخصوصية وحماية المبادئ، وأيضًا للوصول إلى إنفاذ القوانين. وهذه المبادئ الخاص بمجموعة EWG مطروحة في هذا القسم، وتدعمها المبادئ الخاصة بالامتثال التعاقدي، والمساءلة والتدقيق.

### أ. مبادئ حماية البيانات

تعتبر الممارسات التي يفترض أن تتناول القوانين الوطنية المعمول بها بالنسبة للخصوصية وحماية المستهلك غير متسقة في هذه الآونة. حيث تتطلب بعض القوانين أنه عند تصدير بيانات خارج الاختصاص القضائي للشخص أو للجهة المتعاملة مع البيانات الخاضعة لذلك القانون، تطبيق عمليات حماية مماثلة أو مقابلة لحماية البيانات. فالتوجيه الأوروبي الخاص بحماية البيانات لسنة 1995 لا يجيز نقل البيانات خارج الاختصاص القضائي ما لم يتم تقييم القانون المحلي بأنه "ملائم". وقد سعت العديد من الاختصاصات الأخرى خارج الاتحاد الأوروبي للحصول على أحكام تعاقدية قوية، ولكن في معظم الحالات تشترط القوانين على من يملكون بيانات شخصية عدم تحويلها أو الإفصاح عنها دون الحصول على الموافقة إلا إذا كانت الحماية مضمونة. وقد تستحق المسئولية عند هذه النقطة من التحويل. وفي الوقت الراهن، تعاملت ICANN مع هذا الأمر من خلال السماح بتنازل في عقد RAA إلى أمناء

السجلات الذين يوضحون أنهم يراعون قانون حماية البيانات التي تحذر تخزين البيانات. وليس هذا هو الحكم الوحيد في النظام البيئة لـ ICANN الذي يمثل خطرًا على من يسعون للالتزام بقانون حماية البيانات، لذلك كان هناك اقتراح بأنه يجب فحص الوضع الراهن بعناية. وبالنظر إلى التركيز الذي بذلته مجموعة EWG بالنسبة للمساءلة في الأعمال الخاصة بها، فإن مطلب التحلي بالمساءلة عن حماية البيانات قد تم فحصه.

وفي الوقت الراهن، فإن المطالب الخاصة بوجوب قيام الكيان الذي يحصل على البيانات الشخصية بضمان حماية كافية ومتسقة مع أنواع الحماية المقدمة إلى صاحب البيانات "في الموطن" ويجب تنفيذها على **كل حالة على حدة** استنادًا إلى الكيان المتلقي للبيانات في أي اختصاص قضائي يوفر حماية تشريعية للبيانات أو حماية مناسبة كتلك. وهذا يعني أن الكفاية مضمونة من خلال القانون المعمول به بالنسبة للكيان الذي يتلقى البيانات أو الضمانات الأخرى التي تطبق بما يسمح بأن تكون عملية تحويل البيانات قانونية بموجب القانون المنطبق على صاحب البيانات.

## آليات حماية البيانات

بالنظر إلى الوضع الحالي، تم فحص أربعة خيارات تزايدية لحماية البيانات الشخصية في سائر نواحي النظام البيئي لـ RDS وهي:

(0) عدم القيام بأي شيء؛

(1) طرح آليات لتسهيل التجميع الروتيني للبيانات والمتوافق مع الناحية القانونية والنقل؛

(2) طرح آليات تسعى إلى مواءمة الخصوصية وحماية البيانات في سائر قطاعات النظام البيئي لـ ICANN، من أجل توفير "منصة" أساسية لحماية البيانات والتي تقر أفضل الممارسات المقبولة لسياسة الخصوصية

(3) بالإضافة إلى تقديم هذه السياسة كمجموعة من "القواعد الملزمة للمؤسسات".

**ملاحظة:** خلال هذا القسم، يشير اللفظ "نظام RDS البيئي" إلى كافة الجهات الفاعلة المشار إليها في القسم الثامن (ج) العلاقات التعاقدية والامتثال وأيضًا القسم الثامن (د) المساءلة والتدقيق. ويشمل ذلك ICANN (وهي مؤسسة أمريكية غير ربحية)، وكافة سجلات gTLD وأمناء السجلات (والتي تعمل جميعها كمؤسسات مستقلة قائمة في العديد من الدول) وكافة الكيانات الجديدة المعتمدة التي تقترحها مجموعة EWG في هذه الوثيقة: موفر RDS وجهات التوثيق وجهات الموافقة على أوراق الاعتماد الآمنة والمحمية وجهات اعتماد مستخدم RDS، وتوافق ICANN وأي من الكيانات الأخرى المشاركة في التعامل مع البيانات الخاصة.

### الخيار (0): "عدم القيام بأي شيء"

يؤدي عدم القيام بأي شيء إلى مستوى عال جدًا من التعقيد بسبب الخطر المستمر المتمثل في عدم الالتزام بقانون حماية البيانات وضرورة فحص كل تسجيل من أجل تحديد القانون المعمول به. وسوف تؤدي إلى إيجاد تكاليف باهظة بالنسبة لبعض المشغلين، لاسيما السجلات. وبالنسبة لأمناء السجلات فسوف تمثل تكلفة عالية لمراقبة دقة الحماية المطلوبة من المسجلين والسجلات. وسوف تضيف إمكانية عدم اليقين القانوني لكافة الأطراف، بما في ذلك ICANN وغيرها من أصحاب المصلحة في نظام اسم النطاق. الزيادة في عدد نطاقات gTLD وتنوع مواقع السجلات يؤيد إلى إيجاد تحديات جديدة على صعيد القانون المعمول به والاختصاص القضائي للأنظمة التعاقدية لـ ICANN حيث إنها ترتبط بخصوصية المسجل وحماية العملاء. الفوضى وعدم اليقين والممارسات غير العادلة سوف تتطلب مزيدًا من الجهد من جانب ICANN لضمان الامتثال التعاقدي والحد من المخاطر المحتملة. وتوجد هذه التحديات بشكل مستقل عن المسألة الخاصة بنظام RDS. ومن خلال طرح أكثر من 1000 نطاق gTLD،

أصبحت المسألة أكثر حدة. والأهم من ذلك، فإن لا يمكن ضمان حماية صاحب البيانات بشكل متسق. ويعد إطار عمل للاتساق يعمل على الحد من المخاطر، وتقليل الأعباء، والحد من التعقيد محل اهتمام كل صاحب مصلحة.

**الخيار (1): طرح آليات لتسهيل التجميع الروتيني للبيانات والمتوافق مع الناحية القانونية والنقل**

الخيار الثاني الذي تم النظر فيه هو طرح نظام يعمل على تقييم الخصوصية ذات الصلة وقانون حماية البيانات وطرح التشريع في قائمة بحيث يمكن لأصحاب المصلحة تطبيقه، ويمكن للأفراد معرفة أماكن تواجد البيانات وأي القوانين التي طبقت. ويمكن تطبيق القائمة بشكل تلقائي من خلال RDS عبر "محرك قوانين" وفقًا لما هو محدد في القسم التالي. وإذا عاش أي فرد في بلد به قانون لحماية البيانات، وتم تطبيق هذا القانون خارج البلاد على البيانات الشخصية المنقولة من شخص إلى جهة أخرى (وهي في هذه الحالة أمين السجل) فقد يسري القانون. وإذا كان مكان أمين السجل في بلد انطبقت فيه قوانين حماية البيانات على سائر الأفراد (أي ليس فقط على مواطني هذا البلد) عندئذ ينطبق القانون بالتأكيد. البيانات محل الاهتمام أو في نطاق الأغراض الخاصة بنا هي فقط التي يتم جمعها في RDS[24]. تشفير البيانات حول الدوائر القضائية والتي تسري في النظام البيئي سوف تجعل الحياة أكثر بساطة بالنسبة لأصحاب المصلحة المشاركين، وهو ما يؤكد حقوق حماية البيانات (إذا كان ذلك منطبقًا) بالنسبة للمسجل، وسوف يقلل من مخاطر عدم الامتثال. وعلى الرغم من ذلك، في الدوائر القضائية بدون قانون لحماية البيانات يسري على أعمال تسجيل أسماء النطاقات، أو السجلات أو ICANN وآليات التوافق الخاصة بها، يوفر هذا السيناريو حماية أقل للمسجلين الأفراد. وقد يؤدي ذلك إلى نظام متعدد الطبقات بالنسبة لحقوق الخصوصية، وعدم حصول أي من المسجلين الأفراد على أي شيء وحصول آخرين على كامل حقوق الإنسان ومسار إجرائي مع الإشراف القضائي.

**الخيار (2): طرح آليات تسعى إلى مواءمة حماية البيانات في سائر قطاعات نظام RDS البيئي من أجل توفير "منصة" أساسية لحماية البيانات والتي تعتني بأفضل الممارسات المقبولة لسياسة الخصوصية.**

يمكن صياغة الفقرات التعاقدية من أجل سد أي من الفجوات في حماية الخصوصية (تمت مناقشتها باستفاضة في موضوع التنفيذ)، ويمكن إسناد هذه الفقرات إلى مجموعة حماية الخصوصية المقبولة قبولاً عامًا، والتي قد تشكل الأساس بالنسبة لسياسة خصوصية ICANN. وقد تكون هذه السياسة دقيقة، من خلال إدراج الفقرات ذات الصلة في ملحق. وقد يتيح هذا الأمر إمكانية التحويل غير المقيد للبيانات بين الجهات الفاعلية في نظام RDS البيئي من خلال توفير مستوى من حماية البيانات يكون عالي الكفاءة في حماية الاعتراضات لأسباب الخصوصية الشخصية، وحماية البيانات وحقوق العملاء.

وبالنسبة للآليات الخاصة بتسهيل جمع البيانات المتسق من الناحية القانونية والتحويل في سائر قطاعات نظام RDS البيئي فقد تأخذ أشكالاً مختلفة، لكنها سوف تكون جميعها مستندة إلى سياسة متسقة في حماية البيانات تنطبق على نظام RDS. وسوف تقوم ICANN بإنفاذ هذه السياسة مع سائر أصحاب المصلحة من خلال أحكام تعاقدية، كما هو الحال بالنسبة للسياسات الأخرى.

[24] ولن يجعل هذا الأمر من الحياة أقل تعقيدًا بالنسبة لأمين السجل، والذي يتحكم في الكثير من البيانات الأكثر حساسية، مثل بيانات البنوك، ومعلومات بطاقات الائتمان، وسجلات رعاية العملاء، إلخ، والتي لا يتم تحويلها إلى نظام RDS، وعلى الرغم من ذلك فإن "محرك القوانين" سوف يكون مفيدًا بالتأكيد في بعض المواقف، بالنظر إلى مدى تعقيد نظام gTLD القادم.

**الخيار (3): وبالبناء على البند (2) أعلاه، يمكن وضع السياسة المقدمة كمجموعة من "القوانين الملزمة للشركات"، وفقًا لما يقره منتدى التعاون الاقتصادي لدول آسيا والمحيط الهادئ APEC والاتحاد الأوروبي في قانون حماية الخصوصية/البيانات.**

وسوف يعمل هذا الخيار على تبسيط عمليات نقل البيانات فيما بين الدول الأعضاء وعددها 28 دولية في الاتحاد الأوروبي، حيث إنه يوفر تقريرًا للحماية المناسبة للبيانات لأغراض دول الاتحاد الأوروبي، مع التخلص من الطبيعة المخصصة لقرارات حماية البيانات التي تشير إليها تدفقات البيانات عبر نظام RDS البيئي. وفي حين أن هذا الخيار قد يكون أكثر استهلاكًا للوقت، إلا أنه قد يؤدي إلى تقليل خطر عدم الامتثال وضمان مستوى أفضل من الحماية. كما يمكن أن يوفر إشرافًا مستقلاً لسياسة الخصوصية.

| رقم. | ملخص آليات حماية البيانات التي تم النظر فيها |
|---|---|
| (0) | عدم القيام بأي شيء. |
| (1) | الحد الأدنى للحل عبارة عن<br>أ) تحديد عمليات النقل التي يتوفر ضمان لحماية الخصوصية المناسبة لها بموجب القانون ونشر القائمة المعنية<br>ب) طرح قواعد مشتركة في العقد الخاص بهذه الجهات الفاعلة في نظام RDS البيئي ممن لا تتوفر الحماية القانونية الكافية لعمليات النقل الخاصة بهم، وهو ما يوفر لوظيفة الامتثال منصة واحدة وبسيطة للصيانة. |
| (2) | يمكن صياغة سياسة أساسية في خصوصية ICANN بالنسبة لنظام RDS، وذلك استنادًا إلى أفضل الممارسات القياسية لحماية الخصوصية، كما يمكن صياغة الفقرات التعاقدية القياسية التي تعطي أثرًا لهذه السياسة عبر سائر قطاعات نظام RDS البيئي. كما يمكن تضمين الفقرات القياسية في كافة التعاقدات المبرمة بين ICANN وكافة الجهات الفاعلة في نظام RDS البيئي المشاركين في عمليات نقل البيانات، بما يضمن مستوى عال بما يكفي من حماية البيانات من أجل السماح بالتحويل غير المقيد داخل هذا النظام البيئي. |
| (3) | وبالنظر إلى أن ICANN مؤسسة غير ربحية متعددة الجنسيات، فإن نظام RDS البيئي الكامل الخاضع لسيطرتها يمكن إخضاعه لوثيقة القواعد الملزمة للشركات (BCR)، والتي أثبتت فاعليتها في إتاحة عمليات نقل البيانات عبر جميع أنحاء العالم داخل مؤسسة. وفي هذه الحالة، يصبح النظام البيئي خاضعًا للامتثال. وقد ينظر إلى ICANN على أنها جهة تعمل بصفة "جهة متحكمة في البيانات"، وذلك من أجل استخدام مصطلحات منتدى التعاون الاقتصادي لدول آسيا والمحيط الهادئ APEC والاتحاد الأوروبي، من خلال تحديد السياسة والمتطلبات التعاقدية. |

**التقييم:**

**الخيار (0) عدم القيام بأي شيء.** بالنظر إلى التعقد المتنامي للنظام، والتركيز على الدقة المتزايدة والمساءلة، اعتبر هذا الخيار غير مناسب.

**الخيار (1) آليات تسهيل التجميع الروتيني للبيانات والمتوافق مع الناحية القانونية والنقل.** سوف يكون هذا الخيار أكثر تعقيدًا وأكثر ديناميكية مع تغير القوانين في مختلف الدوائر القضائية، ومن المفترض النظر في مجموعة معقدة من تدفق البيانات داخل النظام البيئي. ووفقًا لما ناقشنا في السابق، يجوز لأي مسجل فرد أن يكون له أمين سجل في

دائرة قضائية مختلفة، واستخدام جهة توثيق في دائرة قضائية ثالثة، والاحتفاظ بالبيانات في سجل في اختصاص قضائي رابع، والاعتماد على موفر RDS في اختصاص قضائي خامس.

**الخيار (2) الفقرات التعاقدية القياسية التي تسعى إلى مواءمة حماية البيانات في جميع قطاعات نظام RDS البيئي.** قد يتطلب هذا الخيار توافقًا مع القوانين المعمول بها لأصحاب المصلحة المحددين، لاسيما المسجلين، وأمناء السجلات والسجلات وICANN. وقد يشتمل ذلك أيضًا على الجهات الفاعلة في نظام RDS البيئي الموصى به في هذا التقرير: جهات التوثيق، وموفر RDS، وجهات اعتماد مستخدم RDS، إلخ.

بالإضافة إلى تفويض الامتثال لقوانين حماية البيانات المحلية، فسوف يحقق هذا الخيار - من خلال سرد العناصر المشتركة المستوحاة من قانون حماية البيانات لكل من منتدى التعاون الاقتصادي لدول آسيا والمحيط الهادئ APEC والاتحاد الأوروبي - الكثير من أجل ضمان الامتثال. ويمكن للفقرات أن تنص على شروط الموافقة، وحقوق الوصول، وسياسات الاحتفاظ، والعناصر الأخرى من خلال (على سبيل المثال) تضمين متطلبات الاتحاد الأوروبي في التعامل مع البيانات القانونية والعناصر المناسبة التي يتم التعامل معها من خلال القواعد الملزمة للشركات. وهذه الفقرات القياسية الواردة في العقود لا تتطلب بالضرورة تفويضًا/مراقبةً من خلال الجهات المعنية بحماية البيانات، باستثناء ما يكون في الدوائر القضائية التي تكون فيها هذه التفويضات إلزامية.

**الخيار (3) (القواعد الملزمة للشركات BCR بالنسبة لنظام RDS البيئي).** بالإضافة إلى تفويض الامتثال لقوانين حماية البيانات المحلية، يمكن لهذا الخيار سرد العناصر المشتركة المستوحاة من قانون حماية البيانات لكل من منتدى التعاون الاقتصادي لدول آسيا والمحيط الهادئ APEC والاتحاد الأوروبي. وكما هو الحال في الخيار (2)، يمكن للفقرات أن تنص على شروط الموافقة، وحقوق الوصول، وسياسات الاحتفاظ، والعناصر الأخرى من خلال (على سبيل المثال) تضمين متطلبات الاتحاد الأوروبي في التعامل مع البيانات القانونية والعناصر المناسبة التي يتم التعامل معها من خلال القواعد الملزمة للشركات. وهذه الفقرات القياسية الواردة في العقود لا تتطلب بالضرورة تفويضًا/مراقبةً من خلال الجهات المعنية بحماية البيانات، باستثناء ما يكون في الدوائر القضائية التي تكون فيها هذه التفويضات إلزامية. وعلى الرغم من ذلك، يجب إجراء تهيئة للقواعد الملزمة للشركات BCR بما يتفق مع مواصفات نظام RDS البيئي. علمًا بأن القواعد الملزمة للشركات BCR أكثر تطبيقًا من الناحية النظرية على كيانات المؤسسات ذات هياكل التحكم التقليدية أكثر منها بالنسبة للنظام البيئي المتصل بشكل واسع مثل ما تتم إدارته من خلال ICANN، لكن هذه هي الحالة بالتأكيد بالنسبة للمؤسسات متعددة الجنسيات التي تقوم بإنفاذ قواعد الخصوصية الملزمة من خلال نفس الأنواع تحديدًا للعقود التي تستخدمها ICANN في اعتماد والتحكم في أصحاب المصلحة التابعين لها.

**وختامًا،** "عدم القيام بأي شيء" لا يعد خيارًا حقيقًا، لاسيما إذا كانت توصيات EWG لتحسين الدقة والمساءلة مقبولة. أما الخيار (1) فسوف يكون معقدًا إلى حد ما من الناحية القانونية ولا يوفر أية حقوق متساوية بالنسبة لسائر المسجلين، في حين أن الخيار (3) يطرح تساؤلات حول مدى المطابقة داخل نظام RDS البيئي (أي هذا القواعد الملزمة للشركات مناسبة أم لا، هل ستكون مقبولة، وما هي المتضمنات بالنسبة لـ ICANN من حيث المسئولية؟).

ومن ثم، توصي مجموعة EWG بالخيار (2) - وضع سياسة من خلال استخدام فقرات تعاقدية قياسية تتم مواءمتها مع قوانين حماية البيانات من أجل تنفيذ المتطلبات الخاصة بالسياسة، والتأكيد من خلال مختلف آليات التدقيق أن هذه الأشكال الخاصة بحماية الخصوصية نافذة من خلال العقود بين كافة الجهات الفاعلية في النظام البيئي لـ RDS المشتمل في التعامل مع المعلومات الشخصية.

**تنفيذ آليات حماية البيانات**

بالنسبة لكافة السيناريوهات سالفة الذكر، تعتبر مسألة تنفيذ RDS ذات صلة - لاسيما فيما يتعلق بتوطين موفر خدمة RDS.

وإذا كان من المقرر لنظام RDS أن يحتوي على بيانات شخصية، فسوف يكون من المناسب إذا تم وضع تلك البيانات في اختصاص قضائي نص على حقوق نافذة لحماية البيانات، من أجل تجنب الأسئلة ذات الصلة بشرعية وقانونية عمليات تحويل البيانات والمسئولية عن اختراق البيانات. وهذه المسألة واضحة إذا كان نظام RDS يحوز على بيانات تقع في نفس المكان الذي تقع فيه الجهة المتعاملة مع البيانات. يجب تطبيق إطار عمل مماثل للدراسة، حتى وإن لم تكن البيانات كائنة في نفس المكان ولكن تم جلبها هناك من أجل المعالجة (على سبيل المثال التوثيق) وإرسالها في أي مكان آخر بعد ذلك. قامت مجموعة EWG بالنظر في ثلاثة خيارات لتنفيذ حماية البيانات:

| رقم. | ملخص عمليات تنفيذ حماية البيانات التي تم النظر فيها |
|---|---|
| (0) | ينطبق خيار "عدم القيام بأي شيء" في حالة عدم أخذ مستوى الحماية القانونية للبيانات المنطبق على توطين نظام RDS في الاعتبار عند القيام بالاختيارات الجغرافية. وقد يؤدي القيام بذلك إلى توطين نظام RDS في دائرة قضائية ذات مستوى منخفض من حيث حماية البيانات. |
| (1) | ويمكن لنظام RDS توفير التصنيف القانوني. وعلى وجه الخصوص، يمكن تمييز عناصر البيانات بما يتفق مع القانون المعمول به بالنسبة لصاحب البيانات (أي، المسجل) والتعامل معها بما يتفق مع ذلك. ولتحقيق هذا التصنيف القانوني، يمكن لنظام RDS تنفيذ "محرك قواعد" يقوم بتطبيق قوانين حماية البيانات المعمول بها على كل عملية تحويل.<br><br>وعلى وجه الخصوص، يشير "محرك القواعد" إلى ميزة يمكن تنفيذها داخل نظام RDS من أجل إدارة (أ) التخزين والمع والمعالجة لمعلومات أسماء النطاقات استنادًا إلى المسجل وجهة الاتصال وأمين السجل والسجل والدوائر القضائية لـ RDS (التي تمثلها عناصر البيانات التالية: المسجل وكود البلد لجهة الاتصال، بالإضافة إلى أمين السجل والدوائر القضائية للسجل)، (ب) قوانين حماية البيانات في الدوائر القضائية المعمول بها، بما يتفق مع سياسة ICANN المحددة مستقبلاً لنظام RDS.<br><br>وهذا الأمر معقد بشكل متأصل، وفقًا لما هو مذكور أعلاه، ومن الصعب إنفاذه إذا كان نظام RDS يعمل في دائرة قضائية ليس بها قانون لحماية البيانات ويوفر وصولاً إلى محكمة. |
| (2) | يتم اختيار توطين نظام RDS بما يتفق مع معيار تحويل البيانات الأكثر سهولة والأقل تعقيدًا. وسوف يتضمن القيام بذلك اختيار موقع (مواقع) لتخزين بيانات RDS حيث ينص قانون حماية البيانات الوطني المعمول به على مستوى عال من الحماية. |

**التقييم:**

**الخيار (0) "عدم القيام بأي شيء"** يحافظ على الوضع الراهن ويزيد من تعقيد العديد من عمليات تحويل البيانات من خلال:

- إعادة التأكيد على عملية تجعل من الصعب، ومن المستحيل من الناحية العملية، احترام أطر العمل القانونية؛
- تحميل أعباء إدارية وقانونية على أمناء السجلات بالإضافة إلى الجهات الفاعلة الأخرى في النظام البيئي، ويشمل ذلك دائرة امتثال ICANN

- بالإضافة إلى أنه يفتقر تمامًا إلى الشفافية بما يتعلق بالقانون المحلي لحماية البيانات وامتثال الخصوصية كما أنه غير قابل للتوسعة.

**الخيار (1) التصنيف القانوني من خلال "محرك قواعد"** عبارة عن خيار ابتكاري، ولكن يجب اختبار جدواه من الناحية الفنية. ومن الناحية القانونية، هناك عدد من الأسئلة المفتوحة، لاسيما فيما يتعلق بالتعريف والقبول القانوني والتنفيذ بالنسبة لهذا النظام.

**الخيار (2) توطين البيانات في دائرة (دوائر) قضائية محددة** يمكن أن يكون حلاً ذكيًا وبسيطًا في توفير مستوى عالٍ جدًا من الحماية لكافة انتقالات البيانات. وعلى الرغم من ذلك، لا يتيح هذا الخيار في حد ذاته قوانين حماية البيانات المحلية لكل صاحب بيانات.

حيث إن الخيار (0) غير مناسب، والاختيار (1) و(2) غير شاملين فيما بينهما، توصي مجموعة EWG بوجوب النظر في كلا الخيارين (1) و(2) في الوقت الحالي كوسيلة لتنفيذ المستوى العالي من حماية البيانات للتأكد من خلال السياسة والفقرات التعاقدية القياسية.

وبعد النظر في حالة هذه الخيارات التي تحيط بسياسات حماية البيانات، والآليات والتنفيذ، وافقت مجموعة EWG على المبادئ التالية:

| رقم. | مبادئ حماية البيانات |
|---|---|
| .105 | يجب اعتماد آليات من أجل تسهيل التجميع الروتيني للبيانات والمتوافق مع الناحية القانونية والنقل بين الجهات الفاعلة داخل النظام البيئي RDS. |
| .106 | فقرات العقود القياسية المتوافقة مع قوانين حماية الخصوصية والبيانات والتي يجب صياغتها في سياسة وإنفاذها من خلال عقود تبرم فيما بين سائر الجهات الفاعلة في نظام RDS البيئي في التعامل مع المعلومات الشخصية. |
| .107 | نظام معلومات من أجل تطبيق قوانين حماية البيانات (أي "محرك قواعد") بالإضافة إلى توطين تخزين بيانات RDS فيجب النظر إليها على اعتبارها وسيلتين في تنفيذ مستوى عال من الحماية اللازمة للبيانات. ويجب ضمان ذلك من خلال فقرات تعاقدية قياسية، والتي تتدفق من خلال سياسة خصوصية منطقية لنظام RDS البيئي. |

**ب. مبادئ الوصول للبيانات من خلال إنفاذ القانون**

على عكس ما هو كائن في حالة حماية البيانات، فإن الحماية القانونية لصاحب البيانات في حالات الوصول عن طريق إنفاذ القانون لا يمكن "تصديرها". وللوصول من خلال إنفاذ القانون، تم النظر في ثلاثة اختيارات.

| رقم. | ملخص خيارات الوصول إلى إنفاذ القانون التي تم النظر فيها |
|---|---|
| (0) | "عدم القيام بأي شيء". يتبع الوصول من خلال إنفاذ القانون القواعد الحالية طالما أن إنفاذ القانون الوطني سيكون له وصول إلى بيانات RDS المخزنة في كل مستودع بيانات في المستوى الوطني المعني. وفي بوابة RDS المركزية، يتم منح الوصول من خلال اتباع القانون المحلي للدولة المضيفة لبوابة RDS. |

| رقم. | ملخص خيارات الوصول إلى إنفاذ القانون التي تم النظر فيها |
|---|---|
| (1) | وفي المستوى المركزي لبوابة RDS، حيث لا تتوفر البيانات أمام الجمهور وفي الحالات التي لا يلزم فيها إجراءات قانونية محددة من إنفاذ القانون بموجب القانون الوطني المعمول به، يجب تخصيص شروط الوصول على نظام RDS وتنفيذه بطريقة من اثنتين:<br>أ) يمكن لكل من اليوروبول والإنتربول تحرير اتفاقية تعاقدية مع نظام RDS من أجل تنفيذ وإنفاذ هذا النظام، والعمل كوسيط نشط في الوقت الفعلي لوصول كافة أشكال إنفاذ القانون وتحمل المسئولية عن الحماية والاستخدام المناسبين للبيانات.<br>ب) يمكن لكل من اليوروبول والإنتربول تحرير اتفاقية تعاقدية مع نظام RDS للعمل كجهات توثيق للمستخدمين بالنسبة لمجتمع إنفاذ القانون، من خلال فحص مقدمي الطلبات لإصدار أوراق اعتماد RDS والتي ستستخدم بعد ذلك من خلال الوكالات الفريدة للوصول إلى بيانات RDS المحددة ببوابات وتحمل المسئولية عن الحماية والاستخدام المناسبين للبيانات. |
| (2) | بالإضافة إلى ذلك، في المستوى المركزي، يمكن إقرار آليات تسمح للوصول إلى بوابة RDS المركزية من خلال إنفاذ القانون، حتى في الحالات التي توجد فيها متطلبات خاصة في العلاقات الثنائية التقليدية والتي يتم التعامل معها من خلال معاهدات المساعدة القانونية المتبادلة (MLAT). تقسم وتوزيع البيانات فيما يتعلق بالقوانين المعمول بها يمكن أن يدعم تأسيس مثل هذه الآلية. |

**التقييم:**

**الخيار (0) ("عدم القيام بأي شيء")** لا يوفر بشكل واضح قيمة إضافية للوصول بالنسبة لإنفاذ القوانين.

**الخيار (2) (معاهدات المساعدة القانونية المتبادلة MLAT)** من غير المتوقع أن يتطلب إتاحة الوصول إلى عناصر البيانات المحددة ببوابات والموصى بها من خلال نظام RDS تفويض قضائي إضافي للوصول إلى إنفاذ القانون. ومن ثم، فإن الخيار (2) لا يجب النظر إليه بأكثر من ذلك.

**الخيار (1) (أسلوب بوابة وصول مستخدم RDS المعتمدة)** تعمل على تسهيل الوصول من خلال إنفاذ القانون. على الرغم من أن كلا المتغيرين (1أ) و(1ب) سيقومان على الهياكل الحالية، فإن المتغير (1أ) (الوصول المعتمدة مع التصنيف من خلال وسيط في الوقت الفعلي) سوف ينبني أيضًا على الآليات الحالية لتعاون إنفاذ القانون وتجنب إنشاء طبقة إضافية من التعقيد. وعلى الرغم من ذلك، فإن القدرة على التعرف على حالات إساءة الاستخدام الفردية المحتملة وتصحيحها يجب التحقق منه رغم ذلك.

المتغير (1أ) مشروحة بمزيد من التفصيل في القسم الرابع (ج)، اعتماد مستخدم RDS، السيناريو رقم 3، والذي يسرد بالتفصيل كيفية قيام جهات التوثيق المحتملة مثل الإنتربول بتوكيل إنفاذ القانون المرخص لطلبات الوصول إلى RDS في حين تعقيد حالات إساءة الاستخدام المحتملة. يرجى الإشارة إلى مبادئ اعتماد مستخدم RDS للتعرف على التوصيات ذات الصلة.

بالإضافة إلى ذلك، بالنسبة للخيار (1) يجب التأكيد على أن الإطار القانوني لإنفاذ القانون الوطني في الدائرة (الدوائر) القضائية التي يتم فيها تخزين بيانات RDS لا تلغي إطار العمل الذي يقره نظام RDS. ومن ثم تعتبر جغرافية توطين RDS ذات أهمية حرجة.

| رقم. | مبادئ الوصول إلى إنفاذ القانون |
|---|---|
| 108. | يجب على نظام RDS تخزين البيانات في الدائرة (الدوائر) القضائية حيث يكون إنفاذ القانون معتمدًا بشكل عام، بصرف النظر عن نموذج التنفيذ. |

### ج. الامتثال ومبادئ العلاقات التعاقدية

توصي مجموعة EWG بمجموعة المبادئ التالية حول العلاقات التعاقدية فيما بين الأطراف داخل نظام RDS البيئي:

| رقم. | مبادئ العلاقات التعاقدية |
|---|---|
| .109 | موفر خدمات خارجي يكون عبارة عن منظمة غير حكومية ذات نطاق عالمي يجب أن تكون هي من تشغل نظام RDS. |
| .110 | ويتوجب على ICANN إبرام عقد مناسب مع موفر خدمات خارجي لخدمات RDS لتمكين التوافر والتدقيق والامتثال. |
| .111 | ويتعين على ICANN إبرام عقود مناسبة مع جهات توثيق، وموفري خدمات الخصوصية/الوكالة، وموفري أوراق الاعتماد المؤمّنين، وغيرهم ممن يمكنهم التعامل مع خدمة RDS (راجع القسم الثالث (ج) المبدأ رقم 1). |
| .112 | ويجب على ICANN تعديل الاتفاقيات الحالية (RAA، واتفاقيات السجل) من أجل استيعاب خدمة RDS والتخلص من المتطلبات القديمة. |
| .113 | ويجب تطبيق نظام RDS على سائر سجلات gTLD، سواء الحالية أو الجديدة. لا يجب السماح بأي رعاية أو إعفاءات خاص. |

### د. مبادئ المساءلة والشفافية

توصي مجموعة EWG بأن تتحمل الجهات الفاعلة في نظام RDS البيئي عن الإجراءات التي يتم اتخاذها مع معلومات التسجيل، على النحو التالي:

| رقم. | مبادئ المساءلة والشفافية |
|---|---|
| .114 | يجب أن تتحمل سائر الكيانات داخل نظام RDS البيئي المسئولية عن واحد أو أكثر من المتطلبات المنصوص عليها في القائمة 6:<br>أ) توفير معلومات تسجيل دقيقة ومعتمدة<br>ب) استخدام المعلومات فقط للأغراض المحددة<br>ج) تأمين المعلومات التي يتم جمعها أو تخزينها أو إرسالها<br>د) توثيق أو إثبات المعلومات عند تجميعها<br>ه) تحديث المعلومات المتوفرة في السابق في الوقت الفعلي<br>و) إنفاذ سياسات خصوصية RDS وشروط الاستخدام (ToU)<br>ز) اكتشاف إساءة استخدام معلومات التسجيل<br>ح) تناول المشكلات وتعقبها<br>ط) الالتزام بسياسات شروط الاستخدام وشروط الأمن المقررة<br>ي) إقرار آليات للتعرف على حصاد بيانات الجهات الأخرى وإنشاء الحسابات التدليسية الجماعية<br>ك) وضع عملية تدقيق وتصحيح مستمرة |

| رقم. | مبادئ المساءلة والشفافية |
|---|---|
| | أصحاب المصلحة التاليين[25] لديهم أدوار مسائلة في نظام RDS البيئي:<br>أ) مستخدمي RDS الساعين للحصول على بيانات (USD) - المشار إليها في القسم الثالث<br>ب) ذوي الحماية<br>ج) أمناء السجل[26]<br>د) السجلات[27]<br>ه) موفر خدمة دليل التسجيل<br>و) ICANN<br>ز) موفرو خدمة الخصوصية/الوكالة<br>ح) جهة اعتماد المؤهلات الآمنة والمحمية<br>ط) جهات التوثيق<br>ي) جهات توثيق مستخدم RDS<br>ك) جهات الاتصال المستندة إلى الأغراض<br>ل) موفرو مخازن البيانات |
| .115 | ويجب أن تحدد خدمة RDS إجراءات من أجل التعامل مع المشكلات حول عدم توافر البيانات، والاستخدام غير المناسب للبيانات، والوصول غير المرخص للبيانات، ومخالفات سياسة الخصوصية، والقيد غير الصحيح للبيانات، على سبيل المثال: عناصر بيانات جهات اتصال إساءة الاستخدام، بالإضافة إلى بوابة للحصول على الشكاوى من مستخدمي RDS الساعين للحصول على بيانات USD والمسجلين. |
| .116 | ويجب على RDS إقرار تصحيحات متصاعدة للبيانات غير الدقيقة، على سبيل المثال: تحذير البريد الإلكتروني، التمييز المرئي للمستخدم/المتصفح حول السجلات، إجراء امتثال ICANN، والمحفزات الجديدة الأخرى من أجل تشجيع الدقة. (راجع القسم الخامس تحسين جودة البيانات للتعرف على متطلبات الدقة). |
| .117 | يجب على RDS إقرار تصحيحات متصاعدة للوصول غير المرخص للبيانات، على سبيل المثال: تحذير البريد الإلكتروني، وتقييد المعدل، والحجب المؤقت، وتعليق الاعتماد، والإنهاء، وغيرها من المعوقات. (راجع القسم الرابع تحسين المساءلة للتعرف على متطلبات الوصول المحدد ببوابات). |
| .118 | يجب على RDS إقرار تصحيحات متصاعدة للاستخدام المناسب للبيانات، على سبيل المثال: تحذير البريد الإلكتروني، وتقييد المعدل، والحجب المؤقت، وتعليق الاعتماد، والإنهاء، وغيرها من العقبات. (راجع القسم الثالث المستخدمين والأغراض للتعرف على الأغراض المسموح بها). |
| .119 | يجب أن يقر نظام RDS آليات تدقيق من أجل التعرف على إساءة استخدام أوراق اعتماد الوصول إلى RDS وانتهاكات شروط الاستخدام، على سبيل المثال: آليات التعرف على أنماط السلوك غير المعتاد. (راجع القسم الرابع تحسين المساءلة لمتطلبات اعتماد مستخدم RDS). |

[25] وتمتد هذه الأدوار والمسئوليات إلى وكلاء أصحاب المصلحة والمتنازل لهم (على سبيل المثال الموزعين)

[26] وفقًا لتعريف http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm

[27] وفقًا لتعريف http://newgtlds.icann.org/en/applicants/agb/agreement-approved-09jan14-en.pdf

| رقم. | مبادئ المساءلة والشفافية |
|---|---|
| .120 | يجب أن يقر نظام RDS آليات تدقيق من أجل التعرف على إساءة استخدام بيانات التسجيل في استخدامات لغير الأغراض المحددة، على سبيل المثال: آليات التعرف على أنماط السلوك غير المعتاد. (راجع القسم الثالث المستخدمين والأغراض). |
| .121 | يجب أن يقر نظام RDS آليات تدقيق من أجل التعرف على إساءة الاستخدام من جانب جهات التوثيق، على سبيل المثال: تدريب جهات التوثيق، والحصول على العينات الدورية العشوائية من البيانات لفحصها من أجل التأكد من التوثيق الصحيح. (راجع القسم الخامس تحسين جودة البيانات). |
| .122 | يجب أن يقر نظام RDS آليات تدقيق من أجل التعرف على إساءة الاستخدام من جانب جهات اعتماد مستخدمي RDS؛ على سبيل المثال: وضع آليات التعرف على أنماط السلوك غير المعتاد. (راجع القسم الرابع تحسين المساءلة للاطلاع على تعريف لأنواع إساءة الاستخدام). |
| .123 | يجب أن يقر نظام RDS آليات تدقيق من أجل التعرف على إساءة الاستخدام من جانب موفري خدمات الخصوصية/البروكسي وجهات الاعتماد الآمنة لأوراق الاعتماد؛ على سبيل المثال: وضع آليات التعرف على أنماط السلوك غير المعتاد. (راجع القسم السادس تحسين خصوصية المسجل للاطلاع على تعريف لأنواع إساءة الاستخدام). |
| .124 | يجب أن يوافق مستخدمو RDS الساعين للحصول على بيانات USD على تدقيق الوصول إلى البيانات، واستخدام وتوفير معلومات الهوية والأغراض الدقيقة في شروط الاستخدام (ToU). |
| .125 | يجب أن يقر نظام RDS عملية للتصحيح، أو التعليق أو الإنهاء لجهات التوثيق إذا لم يتم توثيق البيانات بشكل صحيح، وتخزينها وتأمينها. (راجع القسم الخامس تحسين جودة البيانات للتعرف على متطلبات VR). |
| .126 | يجب أن يقر نظام RDS عملية للتصحيح، أو التعليق أو الإنهاء لجهات اعتماد المؤهلات الآمنة إذا كان الاختبار غير مناسب أو دقيق. (راجع القسم السابع تحسين خصوصية المسجل للتعرف على المتطلبات). |
| .127 | يجب أن يقر نظام RDS عملية للتصحيح، أو التعليق أو الإنهاء لجهات توثيق مستخدم RDS إذا كان مستخدم USD غير معتمد ومخزن ومؤمن بشكل صحيح. (راجع القسم الرابع تحسين المساءلة لمتطلبات جهة اعتماد مستخدم RDS). |
| .128 | يجب على ICANN إقرار سياسات ToS لضمان قيام المسجلين وأمناء السجلات وجهات التوثيق بتوفير بيانات دقيقة وحديثة وفي الوقت المناسب إلى نظام RDS. (راجع القسم السادس الاعتبارات القانونية والتعاقدية لنظام RDS ومتطلبات السجل، لكي تظهر في كل من RIA وRAA). |
| .129 | يجب أن يقر نظام RDS عملية تدقيق للسجلات، وأمناء السجلات وجهات التوثيق بالإضافة إلى عملية إبلاغ إلى ICANN إذا لم يقم المسجل/أمين السجل/جهة التوثيق بتوفير بيانات دقيق ومحدثة وفي الوقت المناسب. (راجع القسم السادس الاعتبارات القانونية والتعاقدية لنظام RDS ومتطلبات السجل، لكي تظهر في كل من RIA وRAA). |
| .130 | يجب على RDS إقرار آليات للتدقيق من أجل ضمان الجودة والوحدة المستمرة للبيانات التي يتم تجميعها من خلال نظام RDS وتوفيرها لدى موفر المستودع. (راجع القسم الثامن مستودع تخزين البيانات والقيد) |

| رقم. | مبادئ المساءلة والشفافية |
|---|---|
| .131 | ويجب على ICANN وضع آليات تدقيق من أجل التعرف على مخالفات أي من ToC من جانب موفر RDS. على سبيل المثال: السماح بالاستخدام غير المرخص للبيانات، لا يرد على الشكاوى فيما يتعلق بإساءة استخدام البيانات، أو إساءة استخدام أوراق الاعتماد أو إساءة استخدام التوثيق. (راجع القسم السادس الاعتبارات القانونية والتعاقدية) |
| .132 | يجب على ICANN وضع عملية للتصحيح أو التعليق أو الإنهاء لموفري خدمات RDS إذا لم يقوموا بأداء المسئوليات التعاقدية. على سبيل المثال: توافر واعتمادية وخصوصية وحقوق الوصول ومتطلبات الأداء. (راجع القسم السادس الاعتبارات القانونية والتعاقدية) |
| .133 | يجب على ICANN تعريف وتمييز التحسينات السنوية المقدمة تجاه تحقيق الأهداف الأساسية لـ RDS: (1) جودة البيانات المحسنة، و(2) المساءلة المحسنة، (3) الخصوصية المحسنة. يجب أن يوضح نظام RDS تقدمًا مستدامًا في كافة النواحي الثلاثة في نفس المعدلات، مع عملية من أجل تحديد وتصحيح المشكلات غير المتوقعة التي تتسبب في تحسن أي جانب ببطء أكثر من الجوانب الأخرى. |

تلخص القائمة التالية كيانات النظام البيئي RDS وأنواع المساءلة ومتطلبات التدقيق التي يجب تطبيقها عليهم، وبالتوسع على المبدأ رقم 114.

| المتطلبات المعمول بها | مستخدم RDS الساعي للحصول على البيانات | المسجل | أمين السجل | السجل | موفر RDS | ICANN | موفر الخصوصية/ البروكسي | جهة اعتماد المؤهلات الأمنية | جهة التوثيق | جهات توثيق مستخدم RDS | جهة الاتصال المستندة إلى الأغراض | موفر مخازن البيانات |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| تقديم معلومات دقيقة/معتمدة | | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | | ✔ | ✔ |
| استخدام الأغراض المخصصة | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | | ✔ |
| المعلومات الآمنة | | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | | ✔ |
| توثيق/مصادقة | | | | | ✔ | | | | ✔ | ✔ | | |
| التحديثات في الوقت الفعلي | | ✔ | ✔ | ✔ | | | ✔ | ✔ | ✔ | | ✔ | |
| تفعيل سياسات الخصوصية | | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | | ✔ |
| اكتشاف إساءة الاستخدام | | | | | ✔ | ✔ | | | | ✔ | | |
| عملية الشكاوى | | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | |
| إعاقة حصاد الجهات الأخرى | | | | ✔ | ✔ | | | | ✔ | | | |
| التدقيق والتصحيح | | | | | ✔ | ✔ | | | | ✔ | | |

**الجدول 6: متطلبات التوافق على كيانات نظام RDS البيئي**

## 7. تحسين خصوصية المسجل

من العناصر المحورية بالنسبة لاختصاص مجموعة EWG مسألة كيفية تصميم نظام يعمل على زيادة دقة البيانات التي يتم تجميعها في حين يعرض أيضًا سبل حماية للمسجلين الساعين لحماية خصوصيتهم والحفاظ عليها. وتدرك مجموعة EWG أن المعلومات الشخصية محمية بموجب قانون حماية البيانات، وحتى في الحالات التي لا تكون فيها قوانين، فإن هناك أسبابًا شرعية للأفراد للسعي لتحقيق أشكال من الحماية العالية لمعلوماتهم الشخصية. بالإضافة إلى ذلك، قد تسعى بعض شركات الأعمال والمؤسسات إلى حماية معلوماتها لأغراض شرعية، كما هو الحال عندما تقوم بالإعداد للبدء في إطلاق خط إنتاج جديد، أو في حالة شركات الأعمال الصغيرة، حيث تفصح معلومات الاتصال عن البيانات الشخصية.

وطبقًا لذلك، توصي مجموعة EWG بالمبادئ الأساسية التالية:

| رقم. | مبادئ الخصوصية |
|---|---|
| .134 | بالإضافة إلى الخصوصية المقدمة من خلال التوافق مع قوانين حماية البيانات، يدب على RDS استيعاب الاحتياجات الخاصة بالخصوصية من خلال تضمين ما يلي:<br>• خدمة خصوصية/بروكسي معتمدة لحماية البيانات الشخصية والالتزام بقانون الخصوصية المحلي<br>• بالإضافة إلى خدمة أوراق اعتماد محمية وآمنة معتمدة للأشخاص المعرضين للخطر وفي الحالات التي قد يتم فيها رفض حقوق التحدث بحرية أو محاكمة المتحدثين. |
| .135 | ويجب أن يكون هناك اعتماد لموفري خدمة الخصوصية/الوكالة وقواعد فيما يتعلق بتوفير واستخدام الخصوصية المعتمدة/خدمات الخصوصية. |
| .136 | وخارج أسماء النطاقات المسجلة عن طريق خدمات الخصوصية/الوكالة المعتمدة، يتوجب على سائر المسجلين تحمل المسئولية عن أسماء النطاقات التي يقومون بتسجيلها. |
| .137 | يجب على ICANN التحري عن تطوير سياسة خصوصية واحدة ومتجانسة تحكم أنشطة RDS بطريقة شاملة، وفقًا لما هو مناقش أدناه. |

بالإضافة إلى قوانين حماية البيانات، توفر قوانين ودساتير الخصوصية الوطنية الأخرى الحماية لحقوق مئات الملايين من مستخدمي الإنترنت في التحدث عبر الإنترنت والتعبير عن وجهات نظرهم بدون تعقب آرائهم بسهولة وعلى الفور بالنسبة لأسمائهم وعناوينهم. وتشمل قوانين الخصوصية هذه إعلان الأمم المتحدة لحقوق الإنسان (المادة 19)[28] والذي يحمي حقوق حرية التعبير والتحدث بحرية، والاحتفاظ بالقدرة وحتى بالتزام المجموعات والمنظمات والأفراد والشركات (مثل شركات الوسائط والصحافة) لمراجعة ونقد وانتقاد ممارسات القيادة وممارسة القيادة وإدارة الدول أو الثقافة أو المجتمع.

قوانين الخصوصية التي تحمل حرية الحديث وحرية التعبير غالبًا ما تدرك الحاجة إلى ممارسة هذه الحقوق بموجب قوانين تفصل أسماء وعناوين المنظمات والمجموعات عن الحديث الذي يصدرونه وقد يكون هذا الأمر حرجًا بالنسبة للحكومات أو المجتمعات أو الجاليات أو الأحياء. وقد يشجع ذلك سوق الأفكار، ويفرض الحاجة إلى الحصول على مجتمعات منفتحة للتواصل بما يفوق السلطة على كبح المتحدثين أو إمكانية إصدار أحكام مسبقة على رسالة لمجرد أن شخصًا لا يروقه مؤيدها.

يمكن لقوانين الخصوصية والحقوق التأسيسية أيضًا حماية حرية تكوين الجمعيات والانتماء إليها، والدين والعرق والأخلاق والمجتمع. ويمكن لها جميعًا أن تمنع حاجة الأفراد أو المؤسسات من الإعلان عن أسمائها أو حتى عناوينها في ممارسة وجهات النظر غير المعروفة أو وجهات نظر الأقلية - لذلك قد لا يتم تعقبها على الفور والاستخفاف بها أو أسوء من ذلك. وفي هذا العقد المتميز بعدم الاستقرار السياسي المتأصل ومعاداة أي وجهات نظر مقابلة، توفر قوانين الخصوصية الحماية لأصوات الأقلية وتحفظ قدرة المتحدثين على الإنترنت على الحث القوي على التغيير والإصلاح.

وفي ثنايا هذا التقرير، هناك إقرار بأنه عند الحديث عن الخصوصية وحماية المعلومات الشخصية، فإننا نعني كل من هذه المجموعات المنفصلة من الحقوق، والتي يتم حمايتها في الغالب من خلال تشريع مختلفة، ويتم ذلك بشكل مختلف حول العالم.

### أ. مبادئ خدمة الخصوصية والبروكسي المعتمدة

في الوقت الحالي هناك خدمات تقدم من أجل تجهيل هوية و/أو عنوان الكيانات التي تستخدم أسماء النطاقات. وتم تطوير هذه بسبب الطبيعة المفتوحة لـ WHOIS. في حين أن هناك العديد من المتغيرات، تحدد اتفاقية اعتماد أمين السجل لعام 2013 خدمتين:

- "خدمة الخصوصية" عبارة عن خدمة يتم من خلال تسجيل أي اسم مسجل للمستخدم المستفيد بصفته حامل الاسم المسجل، ولكن يتم توفير معلومات اتصال بديلة ومعتمدة له من خلال موفر الخصوصية/البروكسي من أجل عرض معلومات اتصال حامل الاسم المسجل في خدمة بيانات التسجيل (WHOIS) أو خدمات مقابلة.
- "خدمة البروكسي" عبارة عن خدمة من خلالها يقوم حامل الاسم المسجل بترخيص استخدام اسم مسجل أو عميل الخصوصية/البروكسي من أجل توفير استخدام عملاء الخصوصية/البروكسي لاستخدام اسم النطاق، ومعلومات اتصال حامل الاسم المسجل يتم عرضه في خدمة بيانات التسجيل (WHOIS) و خدمات مقابلة غير معلومات الاتصال الخاصة بعميل الخصوصية/البروكسي.

في التعريفات، "موفر الخصوصية/البروكسي" أو "موفر الخدمة" هو مزود الخصوصية/البروكسي، ويشمل ذلك أمين السجل والجهات التابعة له، حسب مقتضى الحال. "عميل الخصوصية/البروكسي" يعني، (بغض النظر عن المصطلحات التي يستخدمها موفر خدمة الخصوصية/البروكسي)، المرخص له، أو العملاء، أو المستفيد، أو المتلقي الآخر لخدمات الخصوصية وخدمات البروكسي.

خدمات الخصوصية أو البروكسي الحالية ليست محددة المعايير، فليس لموفري الخدمة أي علاقة تعاقدية مع ICANN، على الرغم من أن اتفاقية RAA لسنة 2013 تطرح مفهوم الاعتماد من جانب ICANN بالإضافة إلى أساس للالتزامات، وفقًا لما هو محدد من خلال مواصفة داخلية. وعلى الرغم من ذلك، بعض موفري الخدمات هم أيضًا أمناء سجلات في نفس الوقت. ويخضع جميع أمناء السجلات لاتفاقية RAA، والتي تنص على ما يلي فيما يتعلق بأسماء النطاقات المسجلة من خلال بروكسي:[29]

3.7.7.3 أي حامل اسم مسجل ينوي ترخيص استخدام اسم نطاق إلى طرف ثالث سيكون رغم هذا حامل الاسم المسجل في السجل، وسيكون مسئولا عن تزويد معلومات الاتصال الخاصة به وتزويد وتحديث المعلومات الدقيقة ومعلومات الاتصال الإدارية الكافية لتسهيل الحل في الوقت المناسب لأية مشكلة قد تنشأ[30] فيما يتعلق بالاسم المسجل. يكون لحامل الاسم المسجل استخدام ترخيص أي اسم مسجل وفقا لهذا الحكم قبول المسؤولية عن الأضرار الناجمة عن الاستخدام الخاطئ للاسم المسجل، ما لم تفصح عن معلومات الاتصال الحالية التي يقدمها المرخص له وهوية المرخص له في غضون سبعة (7) أيام إلى الطرف الذي يقدم لحامل الاسم المسجل أدلة معقولة من ضرر للتنفيذ.

WHOIS بالنسبة لنطاق مسجل اليوم من خلال خدمة بروكسي قد تبدو شيئًا مثل هذا:

Domain Name: EXAMPLE-DOMAIN.COM
Created on: 31-Oct-11
Expires on: 31-Oct-13
Last Updated on: 19-Sep-12

Registrant:
Domains By Proxy, LLC ← Registrant Name = Proxy
DomainsByProxy.com ← Registrant Org = Proxy
14747 N Northsight Blvd Suite 111, PMB 309 ← Registrant Address = Proxy's
Scottsdale, Arizona 85260
United States

Admin Contact: [same for Tech Contact]
Private, Registration
example-domain.com @domainsbyproxy.com ← Email = domain@proxy
Domains By Proxy, LLC ← Name = Proxy
DomainsByProxy.com ← Org = Proxy
14747 N Northsight Blvd Suite 111, PMB 309 ← Address = Proxy's
Scottsdale, Arizona 85260
United States
(480) 624-2599 Fax -- (480) 624-2598 ← Tel/Fax = Proxy's

WHOIS لنطاق تم تسجيله اليوم من خلال استخدام ما يطلق عليه في الوقت الحالي اسم خدمة خصوصية تبدو متشابهة، باستثناء أن اسم المسجل (وفي الغالب أسماء المشرف/جهة الاتصال الفنية) للتعريف المباشر لعميل خدمة الخصوصية، وليس موفر خدمة الخصوصية.

[29] وقد تم اعتماد اتفاقية RAA لسنة 2013 من خلال مجلس إدارة ICANN في 27 يونيو 2013، القسم 3.7.7.3 (المذكور هنا) لم يتم تغييره بشكل كبير عن اتفاقية RAA لسنة 2009، باستثناء إضافة فترة سبعة 7 أيام.

[30] ملاحظة: وتقترح مجموعة EWG بأن تنظر ICANN فيما إذا كانت "أي مشكلة" واسعة بشكل مسهب.

ولا توجد عمليات قياسية مستخدمة من خلال جميع موفري خدمة الخصوصية والبروكسي الحاليين. وعلى الرغم من ذلك، هناك العديد من الاحتياجات المشتركة التي غالبًا ما تكون مدعومة إلى حد ما:

- ترحيل الاتصال إلى عميل خدمة الخصوصية أو البروكسي الحالية - والتي تتم في الغالب من خلال بريد إلكتروني يتم إرساله تلقائيًا إلى عنوان البريد الإلكتروني للمشرف/جهة الاتصال الفنية. ويتوفر الترحيل من خلال العديد من موفري الخدمات ولكن ليس كلهم.
- الكشف عن هوية المرخص له وتفاصيل الاتصال المباشر لعميل البروكسي ردًا على شكوى حول اسم النطاق. العمليات والتوثيق والقدرة على الاستجابة، والإجراءات التي تتم تتفاوت وغالبًا ما تعتمد على علاقات قائمة فيما بين مقدمي الطلبات وموفري الخدمات.
- وكشف النقاب عن هوية المرخص له، بما يجعل تفاصيل الاسم وجهة الاتصال لعميل خدمة البروكسي متوفرة بشكل عام في WHOIS.
- وفي حالة عدم قدرة مقدمي الطلبات على الاتصال بعميل خدمة البروكسي أو الحصول على حل من موفر خدمة البروكسي، فغالبًا ما يلجئون إلى أمين السجل (وهو ما قد يرتبط أو لا يرتبط بموفر خدمة البروكسي).

حالات التقصير في خدمات الخصوصية والبروكسي في الوقت الحالي موثقة بشكل جيد.[31] وللتعامل مع كل من احتياجات مسجل اسم النطاق وصاحب المصلحة للحصول على مزيد خدمات خصوصية وبروكسي أكثر وحدة ومصداقية تتيح مستوى أعلى من المساءلة، توصي مجموعة EWG بالمبادئ التالية:

| رقم. | مبادئ خدمات الخصوصية/البروكسي المعتمدة |
|---|---|
| | **عام** |
| .138 | يجب على ICANN اعتماد موفر خدمة الخصوصية والبروكسي[32]. |
| .139 | وكحد أدنى، يجب أن يستمر برنامج الاعتماد لالتزامات الخصوصية/البروكسي بموجب مواصفة RAA لسنة 2013. |
| | **مبادئ لخدمات الخصوصية المعتمدة** |
| .140 | يجوز للكيانات والأشخاص الطبيعيين تسجيل أسماء النطاقات من خلال استخدام خدمات الخصوصية المعتمدة التي لا تفصح عن تفاصيل اتصال المسجل باستثناء ما يكون في ظروف محددة (على سبيل المثال انتهاك شروط الخدمة، مذكرة استدعاء). |
| .141 | ويجب على ICANN المطالبة بتضمين أحكام خاصة في شروط الخدمة. ويجب أن تشتمل شروط الخدمة على مطالبة موفر الخدمة بمحاولة توفير إشعار في الحالات الخاصة بالتعطل المتوقع. |

[31] راجع **الملحق ب** للتعرف على الدراسات والتقارير التي توثق أوجه القصور في نظام WHOIS بالإضافة إلى خدمات الخصوصية/البروكسي.

[32] وقد قامت منظمة GNSO بتشكيل مجموعة عمل من أجل تطوير السياسات الخاصة باعتماد خدمة الخصوصية/البروكسي. وتوصي مجموعة EWG بأن تقوم RDS بإعادة استخدام أي من الأسس المقررة من خلال مجموعة عمل PPSAI، والتي يتم تعديلها حسب الحاجة من أجل عكس طريق الوصول إلى RDS وعناصر البيانات - الجدير أكثر بالملاحظة، جهات الاتصال المستندة إلى الأغراض المنشورة.

| رقم. | مبادئ خدمات الخصوصية/البروكسي المعتمدة |
|---|---|
| .142 | ويجب أن توفر خدمات الخصوصية المعتمدة لأمين السجل (من خلال استخدام PBC يتم إنشاؤه من خلال جهة توثيق) بتفاصيل دقيقة وموثوقة للاتصال بالنسبة لكافة جهات الاتصال الإلزامية المستندة إلى الأغراض، من أجل الوصول إلى موفر خدمة الخصوصية والكيانات المفوضة بحل المشكلات الفنية والإدارية والمشكلات الأخرى بالنيابة عن المسجل. |
| .143 | ويجب فرض خدمات الخصوصية المعتمدة من أجل ترحيل رسائل البريد الإلكتروني من خلال توجيه عنوان البريد الإلكتروني الخاص بالمسجل إلى المسجل. |
| | **مبادئ لخدمات البروكسي المعتمدة** |
| .144 | يجوز للكيانات والأشخاص الطبيعيين تسجيل أسماء النطاقات من خلال استخدام خدمات البروكسي المعتمدة التي تقوم بتسجيل أسماء النطاقات بالنيابة عن عميل خدمة البروكسي. |
| .145 | يجب على موفر خدمة البروكسي المعتمد تزويد أمين السجل (الذي يستخدم PBC تم إنشاؤه من خلال جهة توثيق) مع اسم المسجل الخاص به وتفاصيل الاتصال، بما في ذلك عنوان البريد الإلكتروني الفريد للتوجيه من أجل الاتصال بالكيان المرخص له تسجيل اسم النطاق بالنيابة عن عميل خدمة البروكسي. |
| .146 | باعتباره مالك الاسم المسجل، يتعين على موفري خدمات البروكسي المعتمدين تولي كافة المسئوليات الاعتيادية للمسجل عن اسم هذا النطاق، بما في ذلك توفير جهات الاتصال الدقيق والمعتمدة والإلزامية المستندة إلى الأغراض وغيرها من بيانات التسجيل. |
| .147 | ويجب أن توفر خدمات البروكسي المعتمدة لأمين السجل (من خلال استخدام PBC يتم إنشاؤه من خلال جهة توثيق) بتفاصيل دقيقة وموثوقة للاتصال بالنسبة لكافة جهات الاتصال الإلزامية المستندة إلى الأغراض، من أجل الوصول إلى موفر خدمة البروكسي والكيانات المفوضة بحل المشكلات الفنية والإدارية والمشكلات الأخرى بالنيابة عن عميل خدمة البروكسي. |
| .148 | ويجب فرض خدمات البروكسي المعتمدة من أجل ترحيل رسائل البريد الإلكتروني الواردة من توجيه عنوان البريد الإلكتروني الخاص بالمسجل وفقًا لما هو مشار إليها بالتفصيل في الملحق ح. |
| .149 | ويجب فرض خدمات البروكسي المعتمدة من أجل الرد على طلبات الكشف في الوقت المناسب وفقًا لما هو موضح في إجراءات التصعيد المشروحة بالتفصيل في الملحق ح. |

### ب. مبادئ اعتماد المؤهلات الآمنة والمحمية

تم الإقرار بأن بعض الأفراد والمجموعات الراغبة في الحفاظ على عدم الإفصاح عن هويتها على الإنترنت، أو على الأقل تجنب إتاحة عنوانها ومعلوماتها الشخصية لمن قد يمثلون تهديدًا بالنسبة لهم، لأن لديهم حاجة مشروعة في الحصول على حماية عالية لخصوصيتهم. وقد تمارس هذه الأطراف حقوقها بموجب قانون الخصوصية حيث يوجد أو استخدام خدمات تسجيل البروكسي. لكن لسوء الحظ لا يمكن أن تكون هذه الآليات آمنة بشكل كاف لمن هم واقعون بحق تحت تهديد. فإذا لم تكن تفاصيل المسجل متوفرة على الإنترنت، فسوف يستهدف من يلاحقون هؤلاء الأفراد أو المجموعات جهات التوثيق، أو أمناء السجلات أو السجلات بطلباتهم للحصول على المعلومات، من خلال استخدام أساليب الهندسة الاجتماعية في الغالب والتي لا يكون لهذه الأطراف الاستعداد الكافي لاكتشافها.

والهدف من عرض أوراق الاعتماد المحمية والآمنة هو توفير التسجيل المجهل الآمن لكل من الأفراد أو المجموعات تحت التهديد. وقد يشتمل ذلك على من يرغب في ممارسة حرية التحدث (والتي تعتبر محمية بشكل واسع)، أو المتحدثون الذين قد يتسبب التعرف عليهم في تهديد على حياتهم أو حياة أسرهم.

وفيما يلي خمسة أمثلة مختلفة:

### 1. الأقليات الدينية

في العديد من الدوائر القضائية هناك أقليات دينية واقعة تحت تهديد من مجموعات في المجتمع الأكبر أو من عناصر في العقيدة الخاصة بهم. وقد يرغبون في الحصول على موقع ويب من أجل توفير معلومات إلى أعضائها، مع الحفاظ في نفس الوقت على السرية فيما يتعلق بمكان وطريقة العمل. على سبيل المثال، جماعة الأقلية اليهودية في رومًا لا تفصح عن عنوانها بسبب تهديدات التفجيرات المتكررة، وعلى الرغم من ذلك تقوم بنشر أوقات الخدمة للأعضاء الذين يعرفون مكانها.

### 2. العنف الأسري

توفر العديد من الدوائر القضائية شكلاً من أشكال تغيير الهوية للأشخاص الذين عانوا من العنف الأسري أو الذين فروا هاربين من المعتدين عليهم. وينطبق هذا الأمر كذلك على من يهربون من مجتمعات وطوائف دينية محددة ومن يخضعون لبرامج حماية الشهود. قد يتعين على الملاجئ الخاصة بالنساء اللاتي يعانين من العنف الأسري الإعلان عن الخدمات التي تقدمها على الإنترنت بالإضافة إلى جهات اتصال آمنة وتوجيهات للضحايا الأصليين من أجل الوصول إلى المنشأة إلخ، وبالنسبة للأفراد والأسر التي قامت بتغيير هويّاتها فقد تكون لديها رغبة مشروعة في إقامة مواقع ويب دون الإفصاح مطلقًا عن عنوانها وهويتها الحقيقية. وتجدر الإشارة إلى أن هناك العديد من الأفراد العاملين لدى الحكومات والذين يعملون بموجب هوية مختلفة لأسباب عديدة، غالبًا ما ترتبط بالأمر القومي وإنفاذ القانون، وهؤلاء الأفراد بحاجة أيضًا إلى حماية معززة في كل من المجال والحياة الخاصة التي يعيشونها.

### 3. الخطاب السياسي

في العديد من الدول حول العالم، قد يهرب حزب معارض أو مرشحين خاسرين بعد أي انتخابات. وقد يرغبون أيضًا في إدارة موقع على الويب حيث يمكنهم توفير تفاصيل حول الأحداث التي تقع في بلدانهم الأم أو القمع الذي يتعرضون له. وقد تقوم الحكومة صاحبة السلطة بملاحقة موقع الويب، مدعية الخيانة العظمى أو جرائم أخرى، بعد توثيق أعمال الإساءة التي تقوم بها والظاهرة على موقع الويب. وهذه من المواقف الصعبة، حيث تتفاوت حقوق حرية التحدث بشكل كبير من دولة إلى أخرى ونادرًا ما تواجه اتهامات الخيانة العظمى. والحق في تسجيل نطاق هو كل ما يجب أن يشغل ICANN وأمناء السجلات المعتمدين منها.

### 4. المجموعات العرقية وغيرها من المجموعات

غالبًا ما تعاني المجموعات العرقية من التضييق والتمييز وقد ترغب في إدارة موقع على الويب حيث توفر معلومات حيوية إلى أعضائها. على سبيل المثال، قد ترغب في إدارة موقع على الويب حيث يمكن للأعضاء نشر حوادث التضييق والتحرش دون خوف من التعرف على هويتهم والانتقام منهم. وقد ترغب مجموعات أخرى غريبة إدارة موقع ويب معلوماتي واعتيادي للغاية للمجتمع الخاص بها، وتخشى على الرغم من ذلك من التعرف على هوية أعضائها بسبب القوانين المقيدة في بلادهم أو الانتقام من جانب لجان الأمن أو جماعات الكراهية. كما أن هناك أمثلة على عمليات الانتقام التي تحدث بحق مشغلي المواقع التي توفر معلومات صحية وغذائية للنساء، ومعلومات حقوق التناسل، إلخ.

### 5. الصحفيين العاملين في الأماكن المعادية

قد تكون هناك حاجة لدى الصحفيين الذين يقوم بنشر الأحبار من الأماكن المعادية أو رغبة في إدارة موقع ويب مع الحفاظ على الأمن والخصوصية التي تحيق بهوياتهم ومعلومات العناوين، بما في ذلك عناوين وهويات من يتعامل معهم ومترجميهم، إلخ.

**التعرف على تقنيات المؤهلات الآمنة**

هناك مؤهلات آمنة متعددين في الأسواق، مثل U-Prove من شركة مايكروسوفت (http://research.microsoft.com/en-us/projects/u-prove/) وIdentity Mixer من شركة IBM (http://researcher.watson.ibm.com/researcher/view_project.php?id=664). وتتيح هذه الأساليب للمتلقي إثبات العديد من الخصائص -- مثل الحصول على التقدير والامتنان من جهة معتمدة، بأنه قد حصل على اعتماد مالي نظير حق أو خدمة معينة ---دون الكشف عن أي من المعلومات الشخصية حول أنفسهم أو إثبات أي من آثار المعاملات التي أتاحت هذه الخصائص أو المؤهلات. والأطراف المرحلة لديها إثبات تشفيري آمن بأن الكيان الذي أصدرت له أوراق اعتماد آمنة قد حصل على الموافقة من الجهة المعتمدة، دون الحاجة إلى معرفة من هم أو كيف يحصلون على هذه الموافقة.

ويمكن استخدام هذه التقنية من أجل إقرار عملية يمكن من خلالها للجهات المعرضة للخطر المشار إليها أعلاه الحصول على اسم نطاق تم تسجيله من خلال استخدام أوراق اعتماد محمية وآمنة. ولا يحصل أمين السجل أو جهة التوثيق على أية معلومات حول ماهية الكيانات المعرضة للخطر تتجاوز العقود المطلوبة وتتحمل المسئولية عن التعامل مع مشكلات DNS. ومن ثم لن تكون لهم القدرة بشكل مشروع على الرد على الطلبات المقدمة للحصول على المعلومات الشخصية أو معلومات العنوان. ومن الواضح، هناك مخاوف حيال التوافق الفني، وإساءة الاستخدام وعمليات التخفيف من هذه المخاطر (والمشار إليها أدناه). أما النقطة الأساسية فهي أنه بالنسبة لأسماء النطاقات المسجلة من خلال استخدام أوراق اعتماد آمنة، فلن يكون أمناء السجلات والسجلات بعد ذلك من يتحمل المخاطر والمسئولية عن تحديد هوية الأفراد المعرضين للخطر أمام المعتدين عليهم.

**المشكلات التشغيلية**

لكي يتم إفراغ المشكلات والمخاطر المرتبطة بمثل هذه الخدمة، قامت مجموعة EWG بالتحري على المواقف المحتملة التالية:

1. مقدم طلب الحصول على المعلومات الراغب في إقرار اسم أو عنوان حقيقي لفرد كما هو مذكور في البند 2 و3 و4 أعلاه، بالنسبة لما تمثله كأغراض مشروعة (ادعاءات إساءة استخدام العلامات التجارية، أو الرغبة في بيع أو شراء اسم نطاق، أو الرغبة في التحري عن سلامة منتج، إلخ). لاحظ أنه في موقع الحياة والموت، يكون أي أمين سجل في موقف صعب عند محاولة تحديد ما إذا كان مقدم الطلب يتصرف بادعاءات باطلة أم لا، ولا يتوقع من فريق العمل فهم نوع التهديدات غير المعروفة التي قد يواجهها الناس، لاسيما في حالات تغيير الهوية.
2. يتقدم مقدم طلب إلى أمين سجل لاسم النطاق (أو جهة توثيق PBC معينة) مدعيًا نوعًا من الأنشطة الجنائية أو التشهيرية ويطالب بإيقاف موقع ويب يستخدم اسم النطاق هذا. وفي هذه الحالات، يتم اتباع شروط الخدمة لكل من أمين السجل وموفر خدمة البروكسي، وربما يؤدي إلى طلب كشف من أجل الحصول على هوية وعنوان المرخص له باسم النطاق. وعلى الرغم من ذلك، بالنسبة لأسماء النطاقات المسجلة التي تستخدم أوراق الاعتماد الآمنة، فإن الكشف الناجح لا يؤدي إلا إلى الجهة المعتمدة التي وافقت على المؤهلات الآمنة. وفي هذه النقطة، تتحمل الجهة المعتمدة المسئولية عن التحري عن إساءة

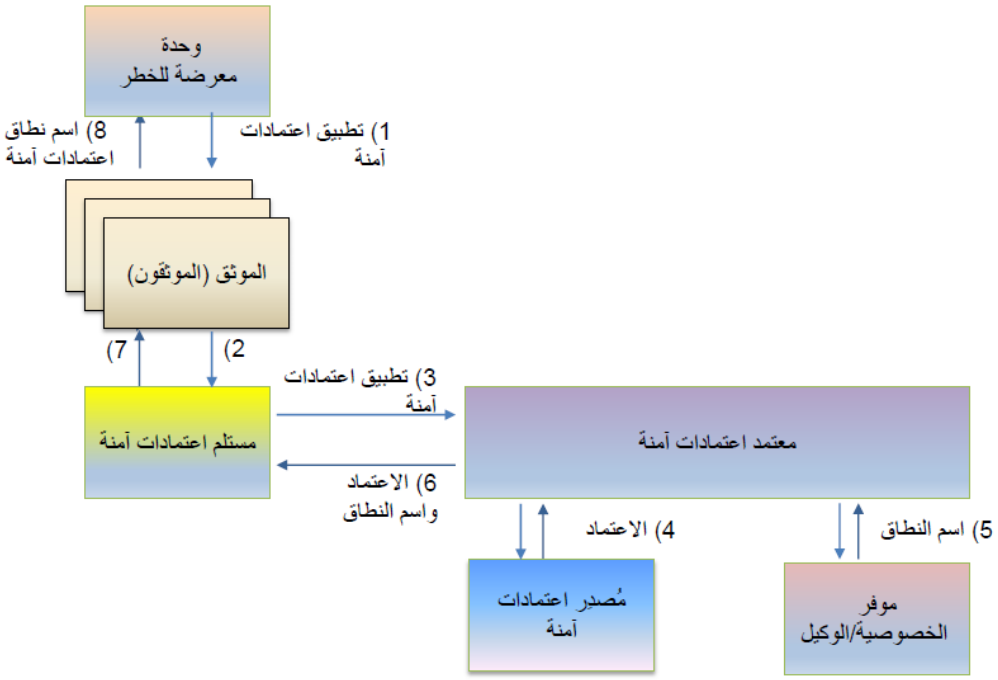
الاستخدام المحتملة لنظام DNS. وفي بعض الحالات، مثل الأنشطة الجنائية، قد يتم منح إيقاف عاجل لمواقع الويب هذه.

3. في الحالات التي تقدم فيها وكالات حكومية ادعاءات تتعلق بالخطاب الديني التي تنشأ عن مستوى من الخيانة أو المسائل الجنائية، قد يتعين على أمناء السجلات على الرغم من ذلك استخدام إيقاف سريع لمواقع الويب التي تستخدم أسماء النطاقات المسجلة بأوراق اعتماد آمنة، وذلك بالاعتماد على القانون ذي الصلة في الولاية القضائية.

وحتى بالنظر إلى هذه القيود، إلا أن أوراق الاعتماد الآمنة توفر مزيدًا من الأمن للكيانات المعرضة للخطر أكثر مما تحظى في الوقت الحالي، وإذا تطلبت RDS الجديدة الحصول على دقة ومساءلة معززة للبيانات، عندئذ يجب توفير خدمة كهذه. ولتحقيق ذلك، يجب توفير الوظائف الأساسية التالية:

1. عملية لوضع معايير لتأهل الكيانات المعرضة لمخاطر من أجل أوراق الاعتماد الآمنة، على أن تبدأ بأمثلة للمستخدم يتم الاستشهاد به وغيرها مما يعتبره مجتمع ICANN مناسبًا من خلال وضع سياسة.
2. نماذج الطلبات والشهادات المطلوبة والنظم المالية، جميعها مع التركيز على التأكيد على أن الهويات الخاصة بالكيانات المعرضة للخطر (وفي بعض الحالات الجهات الضامنة لهم) محمية. وفي أي نظام مجهّل الهوية، تعد هذه واحدة من نقاط الضعف الأساسية.
3. مجلس مراجعة مستقل من أجل تقييم واعتماد الطلبات المقدمة للحصول على أوراق اعتماد آمنة بالإضافة إلى شهادات الأطراف المعتمدة، مثل الحكومات التي حصلت على تغييرات معتمدة على الأسماء، ومنظمات الأمم المتحدة المشاركة في حماية اللاجئين، والروابط الدولية للصحفيين، إلخ.
4. الأطراف المعنية (مثل الأطراف المدرجة في البند 3 أعلاه) الراغبين في ترحيل طلبات الحصول على تأهيل آمن وأسماء النطاقات الناتجة عن ذلك إلى/من مجلس المراجعة المستقل هذا. وهذه الأطراف المعتمدة - المشار إليها فيما يلي هنا بلفظ متلقو أوراق الاعتماد الآمنة - يجب عليهم إثبات حاجة الكيانات المعرضة للمخاطر للتجهيل وقبول المساءلة عن أي من حالات إساءة استخدام DNS المحتملة من جانب أسماء النطاقات المسجلة بأوراق اعتماد آمنة.
5. موفرو خدمة البروكسي المعتمدين ممن لديهم استعداد لقبول المؤهلات الآمنة عند تسجيل أسماء النطاقات المقرر ترخيصها من خلال جهة اعتماد المؤهلات الآمنة، بالإضافة إلى النظم المالية التي يتم السداد من خلالها.
6. السياسات التي تحيط بإجراءات الغلق المتوقعة وغيرها من عمليات تخفيف إساءة استخدام DNS. وقد يشتمل ذلك على مراقبة الأمن المعزز لأسماء النطاقات المسجلة للمؤهلات الآمنة، من أجل التخفيف ضد إساءة استخدام DNS المحتملة وإساءة الاستعمال والمساعدة في حماية أسماء النطاقات من عمليات الهجوم. والأطراف التي تدعي إساءة استخدام DNS يجب أن تطرح قضيتها على مجلس الإدارة الذي اعتمد طلب الكيان المعرض للخطر، وأن جهة اعتماد المؤهلات الآمنة سوف تقوم بتقييم إساءة الاستخدام المزعومة.

ويوضح الشكل التالي علاقات المحتملة بين هذه الأطراف، ومسئولياتهم، وتدفق الاتصال فيما بينهم.




**الشكل 8. نموذج المؤهلات الآمنة والمحمية**

### المخاطر الباقية

لا تحظى أوراق الاعتماد الآمنة باستخدام واسع النطاق بسبب، على سبيل المثال لا الحصر، تعقيد تنفيذها، لاسيما فيما يتعلق بالتسجيل والرفض. وقد قيل بأن كافة الأطراف يتوجب أن تكون مؤهلة لهذا التسجيل، ولكن بالنظر إلى عتبة العمل المطلوبة لإقرار هذه الخدمة وضمان أنها لا تستخدم لأغراض تدليس أو أغراض إجرامية، تعتبر مجموعة EWG هذا الأسلوب غير مناسب. وتوصي مجموعة EWG بوضع مؤهلات أمنة محمية لاستخدام محدود وبعد ضمان أن الكيانات المستفيدة من الخدمة لديها حاجة مشروعة بحق للحصول على تجهيل الهوية.

ومن المعروف أنه بمجرد تسجيل أي اسم نطاق ودخول موقع الويب الذي يستخدمه حيز التشغيل، قد تؤدي أنواع مختلفة من البيانات الكبيرة ومحتوي مرور الإنترنت إلى تعريف هوية مستخدم اسم النطاق. وهذا يتجاوز اهتمامات ICANN، والتي تركز بشكل فردي على مشكلات تسجيل النطاقات وبيانات المرافق التي يتم جمعها، واستخدام والإفصاح عنها من أجل تحقيق الأغراض المحددة في حدود اختصاص ICANN. والمعلومات التي يتم استخراجها من الاستخدام الفعلي لاسم النطاق يجب أن تكون من مسئولية الكيانات التي تتقدم بطلبات للحصول عليها وتستخدم أسماء النطاقات المسجلة بأوراق اعتماد آمنة، قد يكون من المهم توفير معلومات تركز على هذا الخطر. وتنتهي مسئولية ICANN بنظام اسم النطاق نفسه.

| رقم. | مبادئ الحصول على مؤهلات آمنة محمية |
|---|---|
| .150 | يجب أن تكون للأفراد والمجموعات الذين يوضحون أنهم سيتعرضون لخطر القدرة على تقديم طلب بدون تحديد هوياتهم والحصول على أسماء نطاقات مسجلة من خلال استخدام أوراق اعتماد آمنة، يدعمها ضامنون وجهات أخرى معتمدة من أجل توفير حاجز بين الكيانات المعرضة للخطر وأمناء السجلات/جهات التوثيق. |

| رقم. | مبادئ الحصول على مؤهلات آمنة محمية |
|---|---|
| .151 | يجب على ICANN تسهيل تأسيس مجلس إدارة مستقل للمراجعة المعتمدة يعمل على توثيق دعاوى المؤسسات أو الأفراد المعرضين للخطر من أجل اعتماد أوراق الاعتماد (ورفضها عند الضرورة). وهذه المؤسسة - المشار إليها هنا بلفظ جهة اعتماد المؤهلات الآمنة (SCA) - يجوز لها تطوير خدمات أخرى، مثل تثقيف المستخدمين حول المخاطر وممارسات الإنترنت الآمن. |
| .152 | يتعين على ICANN تسهيل تطوير أو ترخيص جهة إصدار أوراق اعتماد تقر بموافقات SCA وتستخرج أوراق الاعتماد الآمنة المقابلة. |
| .153 | ويجب على جهة اعتماد المؤهلات الآمنة استخدام أوراق الاعتماد الصادرة من أجل ترخيص أسماء النطاقات من موفري خدمات البروكسي المعتمدة بطريقة اعتيادية. وسوف تظهر معلومات موفر خدمة البروكسي في نظام RDS. ولن يتم التعرف على أية بيانات حول الكيان المعرض لخطر ويستخدم اسم النطاق المسجل بأوراق الاعتماد الآمنة في نظام RDS، ويجب استخدام نظام ما من السداد غير معروف الهوية أو البروكسي. |
| .154 | يجب على أسماء النطاقات المسجلة باستخدام أوراق الاعتماد الآمنة المحمية اتباع إجراءات الكشف والحل الاعتيادية لموفر خدمة الخصوصية/البروكسي المعتمدة. الفشل من جانب عميل الخصوصية/البروكسي (أي جهة اعتماد المؤهلات الآمنة) في الرد في الوقت المناسب، أو إثبات إساءة استخدام DNS، قد يؤدي إلى إيقاف سريع لأسماء النطاقات المسجلة باستخدام المؤهلات الآمنة. |
| .155 | ومع إقرار أن أسماء النطاقات المسجلة باستخدام المؤهلات الآمنة المحمية قد تكون في حد ذاتها معرضة لخطر الهجوم الإلكتروني، أو أن التحري عن المخالفات سوف يكون صعبًا، فقد يتم النظر في مراقبة أمن عالية لأسماء النطاقات هذه من أجل الحد من المخاطر. |
| .156 | ويجب وضع سياسات وعمليات من أجل الموافقة على طلبات المؤهلات المحمية الآمنة ورفضها.<br>• ويجب أن تسمح عملية الموافقة لصفر أو أكثر من الشهود لتوفير الحماية الكافية لهوية وموقع الكيان المعرض للخطر من متلقي المؤهلات الآمنة المعتمدة التي تقدم الطلب إلى SCA. عدد وهوية الشهود شفاف بالنسبة لنظام RDS، الطرف الوحيد الذي يتعامل مباشرة مع SCA هو متلقي المؤهلات الآمنة.<br>• ويجب أن تتيح عملية الرفض حماية مماثلة لهوية وموقع الأفراد المعرضين لمخاطر مع تعزيز شروط الخدمة للمؤهلات الآمنة. يجب أن تتحمل SCA المسئولية عن التحري عن إساءات استخدام DNS المزعومة والتي تشتمل على مؤهلات آمنة وإنفاذ شروط الخدمة. وفي حال كانت إساءة استخدام DNS خطيرة بما يكفي بحيث تستدعي رفض المؤهلات، تلقي SCA بالمسئولية على متلقي المؤهلات الآمنة. |

### ج. ملخص المزايا الأساسية للخصوصية

من خلال التحسينات التي أدخلت على الدقة والمساءلة، سوف يكون من الأكثر أهمية حماية المواطنين الأفراد، لاسيما المعرضين لخطر. علمًا بأن ضم حماية البيانات، والخصوصية/البروكسي المعتمدين، ومبادئ المؤهلات المحمية الآمنة وآلياتها كجزء لا يتجزأ من RDS من الجيل التالي سوف يؤدي إلى تحسين خصوصية المسجلين وجهات الاتصال.

أما مبادئ حماية البيانات الموصى بها من مجموعة EWG فهي:

- الحماية الموحدة بشكل أكبر للبيانات الشخصية من خلال تطبيق سياسة RDS متجانسة، وتطبيقها بشكل متسق في سائر نواحي النظام البيئي لـ RDS واستخدام "محرك قواعد" لتطبيق القانوني المحلي.
- المطالبة بتسجيل أقل وبيان اتصال لنشرها أو إتاحتها بدون معرفة الهوية.
- الحماية الأفضل للمسجل وبيانات جهة الاتصال ضد إساءة الاستخدام.

والمبادئ التي أوصت بها مجموعة EWG لموفري خدمات الخصوصية/البروكسي المعتمدين كالتالي:

- توفير وضوح أكبر بالنسبة للمسجلين الساعين للحصول على خدمات الخصوصية/البروكسي من خلال وضع إطار اعتماد لموفر الخدمات الذين يعرضون هذه الخدمات.
- المطالبة بالتوثيق لأسماء النطاقات على اعتبار أنها مسجلة من خلال استخدام الخدمات المقدمة من خلال موفر خصوصية/بروكسي معتمد.
- الإشارة بشكل واضح داخل بيانات التسجيل إلى طريقة الاتصال بموفر الخصوصية/البروكسي.
- منع الجهات الأخرى من استخدام معلومات اتصال موفر الخصوصية/البروكسي المعتمدين دون الحصول على تفويض.
- مطالبة موفر معتمد للخصوصية/البروكسي بترحيل البريد الإلكتروني إلى مسجل أساسي والرد على الاستعلامات.
- توفير مزيد توقعات أكثر اتساقًا وتوقعًا لإنفاذ القانون والمبلغين على إساءة الاستخدام من أطراف أخرى ومقدمي طلبات الإفصاح.

أما مبادئ المؤهلات الآمنة المحمية الموصى بها من مجموعة EWG فهي:

- للمرة الأولى، وضع إجراءات من أجل تمكين المجموعات المعرضة لمخاطر والمهمشة للاستفادة من المزايا المتعددة لامتلاك النطاقات الخاصة بهم على الإنترنت.
- حماية من هم بحاجة ملحة لاستخدام الإنترنت لأغراض الحديث بحرية والاتصال داخل المجموعات، وتوفير تصحيحات لإساءة الاستخدام المحتملة.
- التخلص من المسئولية المحتملة من جهات التوثيق وأمناء السجلات، الذي يتحملون اليوم المسئولية عن الكشف عن المعلومات الشخصية الحساسة بشكل كبير من خلال محاولات الهندسة الاجتماعية.
- توفير أمن إضافي حول أسماء النطاقات المسجلة باستخدام أوراق الاعتماد الآمنة والمحمية .
- المطالبة بإيقاف سريع لأوراق الاعتماد الآمنة والمحمية لمواقع الويب المسجلة بها والمشاركة في إساءة استخدام نظام DNS.

## 8. نماذج RDS المحتملة

### أ. مبادئ تصميم النماذج

يوفر هذا التقرير تفاصيل حول النماذج المتعددة البديلة التي تحرت عنها مجموعة EWG، بالإضافة إلى تحليل كيفية تحقيق هذه النماذج للمبادئ الموصى بها من مجموعة EWG. وقد تم تقييم كافة النماذج من خلال استخدام مجموعة من معايير متعددة الأوجه وفقًا لما هو محدد في الملحق و.

وفي إجراء مجموعة EWG للتحليل، فقد طبقت المبادئ التالية للتصميم:

| رقم. | مبادئ تصميم النماذج |
|---|---|
| .157 | **التجميع:** يقوم أمناء السجلات والجهات التابعة لأمناء السجلات في الوقت الحالي بجمع وتخزين معلومات التسجيل من العملاء (المسجلين) التابعين لهم. وهذه العملية موزعة بشكل أساسي. وبالإضافة إلى مواصلة جمع بيانات التسجيل من المسجلين عن طريق أمناء السجلات أو الجهات التابعة لها، تقترح مجموعة EWG جمع بيانات الاتصال من خلال جهات توثيق. |
| .158 | **التخزين:** وهناك العديد من النماذج المحتملة بالنسبة لتخزين معلومات التسجيل عبر كافة نطاقات gTLD. حددت مجموعة EWG العديد من النماذج المحتملة، وركزت على اثنين سوف يكونان واعدين، واختارت نموذج واحد موصى به من خلال تطبيق معايير التقييم الموضحة في المحلق و. |
| .159 | **الوصول:** لحماية خصوصية صاحب البيانات، يجب أن تتيح واجهة مركزية لمقدمي الطلبات المناسبين إمكانية الوصول والاطلاع على معلومات التسجيل عبر كافة نطاقات gTLD، بما في ذلك الوصول من خلال أي شخص إلى البيانات العامة غير الموثقة والوصول إلى البيانات عبر البوابات الموثقة من خلال المستخدمين المعتمدين. |
| .160 | **البروتوكول:** ويجب على RDS استخدام RDAP[33] أو EPP (حسب ما يتناسب لكل واجهة) باعتباره بروتوكول الوصول الأساسي للأدلة من أجل الحصول على معلومات التسجيل من مواقع التخزين، مهما كان مكانها. |

### ب. النماذج المعتبرة

لاختبار نماذج النظام البديلة التي تنظر فيها مجموعة EWG في تقريرها الأولي والنماذج الإضافية المقترحة من خلال مجتمع ICANN، حددت مجموعة EWG في البداية النماذج التي سيتم اختبارها بعمق. يختلف كل نموذج بطرق متعددة، ويشمل ذلك نسخ معلومات التسجيل أو الاستعلام عنها من خلال نظام RDS. وهذه الفروق ملخصة في الجدول التالي[34] وبمزيد من التفصيل في الملحق و.

| النماذج المحتملة | التجميع | التخزين | نسخ | الوصول |
|---|---|---|---|---|
| WHOIS الحالي | RR | RR/Ry | لا يوجد | RR/Ry |
| اتحادي | RR & V | RR/Ry & V | لا يوجد | RDS |
| متزامن * | RR & V | RR/Ry & V | RDS | RDS |
| إقليمي | RR & V | RR/Ry & V | إقليمي | RDS |
| تخلي | RR & V | RR/Ry & V | اختياري | RDS |
| تمرير | RR & V | RR & V | RDS | RDS |

[33] http://tools.ietf.org/html/draft-ietf-weirds-rdap-query-02

[34] مفتاح جدوا مراجعة النماذج: تشير RR إلى أمناء السجلات، وRy إلى السجلات، وV إلى جهات التوثيق

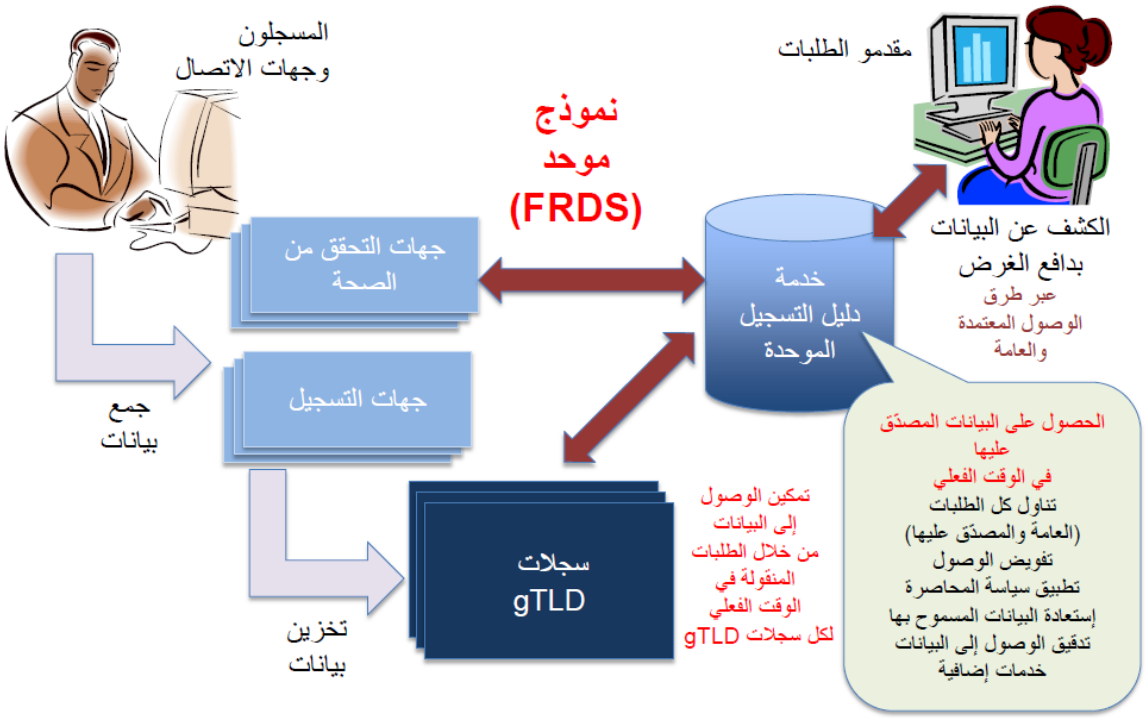
* **ملاحظة:** النموذج المشار إليه في السابق بلفظ **"RDS المجمع (ARDS)"** تمت إعادة تسميته إلى **"RDS المتزامن (SRDS)"** لكي يعكس بشكل أفضل خاصية النموذج في استخدام البيانات التي تستقر في أمكان متعددة بطريقة متسقة ومنسقة. وسوف يتم نشر واستخدام كافة النماذج التي تم تداولها هنا من خلال استخدام أفضل ممارسات الهندسة من أجل تحقيق تحمل الأخطاء، والتوافر العالي، وموازنة الأحمال، بما في ذلك مراكز البيانات المتنوعة على المستوى الجغرافي، والاتصال المتنوع القوي، بالإضافة إلى البنية التحتية الفائضة في كل مركز بيانات.

## ج. النموذج الموصَى به

من بين النماذج المحتملة للنظام المحددة أعلاه، يختلف كل منها من حيث الطريقة التي يتم بها نسخ معلومات التسجيل أو الاستعلام عنها من خلال نظام RDS. وقد فحصت مجموعة EWG عن كثب كل منها من أجل تحديد الطريقة التي يمكن أن تؤثر بهذا على الخصائص المختلفة. وبعد مقارنة هذه النماذج المحتملة، فقد اكتشفت مجموعة EWG أنه، وباستثناء نظام WHOIS الحالي، فإن جميعها قادر على تحقيق مبادئ RDS الموصى بها من مجموعة EWG إلى درجة ما. ومن بينها، فقد ركزت مجموعة EWG على النموذجين الواعدين أكثر لإجراء مزيد من الفحص - النموذج الموحد والنموذج المتزامن (والمعروف في السابق باسم "النموذج التجميعي") -**وأوصت في النهاية بالنموذج المتزامن (SRDS)**.

### النموذج الموحد (صاحب المرتبة الثانية)

يصف هذا النموذج نظام RDS الذي يسحب معلومات التسجيل من مناطق التخزين الموزعة والتي تديرها سجلات كثيفة بالإضافة إلى جهات توثيق، والتي تستخدم جميعها مخطط بيانات عام للبيانات الموحدة. لا يوجد تجميع للبيانات في موقع تخزين واحد، ولكن بالأحرى وصول موحد عام/محدد ببوابات من خلال نظام RDS إلى معلومات التسجيل التي يتم الحصول عليها في الوقت الفعلي من سائر سجلات gTLD (بيانات أسماء النطاقات) وجهات التوثيق (تفاصيل الاتصال).



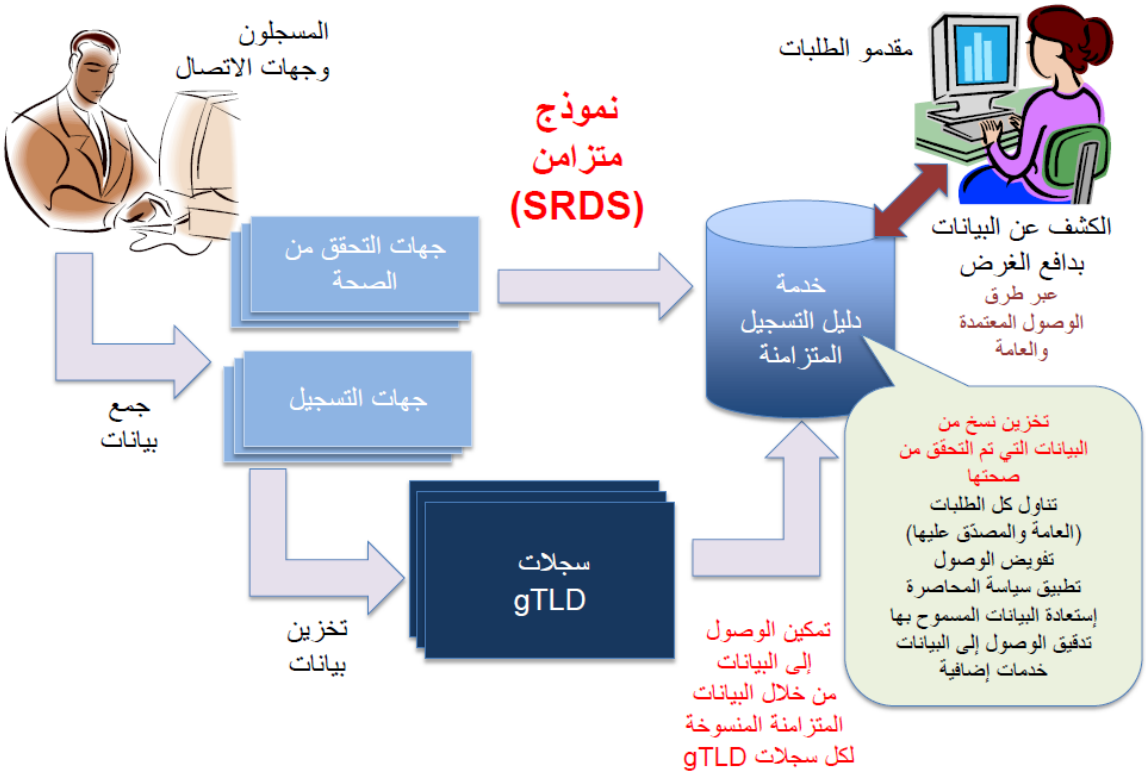
وفي هذا النموذج، يتم سحب البيانات من خلال FRDS من جهات التوثيق والسجلات/أمناء السجلات عن طريق RDAP. كما أن تدفق بيانات الاتصال والتسجيل المرتبطة بهذا النموذج موضح بمزيد من التفصيل في الملحق ط (المخططات الانسيابية لعملية RDS) وموضحة بالتفصيل في الملحق هـ باستخدام أمثلة الاستعلام.

## النموذج المتزامن (SRDS) (الموصى به)

يصف هذا النموذج نظام RDS الذي يقوم - في الوقت الفعلي تقريبًا- بسحب بيانات النسخ الواردة من مناطق التخزين الموزعة والتي يديرها سجلات كثيفة وجهات توثيق في نظام متزامن يقوم بتجميع وتخزين البيانات في بنية موزعة تدار من خلال نظام RDS.

وبموجب هذا النموذج، يعتبر RDS هو المصدر الموثوق للبيانات ويوفر وصولاً معتمدًا وفقًا للوصف السابق. ونتيجة لذلك، سوف ينتقل RDS إلى أبعد من مطلب RAA الحالي (والحاجة الحالية) لتوقيت أمين السجل والسجل للتحديثات. ويمكن للسجلات وأمناء السجلات وجهات التوثيق تزويد العملاء بالوصول إلى البيانات الخاصة بهم، إلا أن كافة الطلبات المقدمة للحصول على البيانات المحددة ببوابات يجب الرد عليها من خلال استعلام RDS. ويأتي هذا النموذج ردًا على توصيات WHOIS السابقة والطلبات الخاصة بتقليل ارتباك العملاء من حيث مكان وكيفية الوصول إلى بيانات التسجيل، بالإضافة إلى تقليل التكلفة ومتطلبات المساءلة بالنسبة لأمناء السجلات والسجلات.

وعلى الرغم من توفير RDS وصولاً إلى البيانات، إلا أن البيانات لا يتم تسجيلها في موقع واحدة ولكن عوضًا عن ذلك في مواقع متعددة، ومتنوعة وكبيرة حسب أفضل ممارسات الهندسة للنظم التي تتطلب تحمل الأخطاء، والتوافر العالي، وموازنة الأحمال. وتواصل السجلات وجهات التوثيق تخزين البيانات الخاصة بها، إلا أن RDS بإمكانية استخدام النسخ المتزامنة من تلك البيانات لمعالجة طلبات الوصول بمزيد من الفاعلية.



وفي هذا النموذج، يتم دفع هذه البيانات إلى SRDS من خلال جهات التوثيق والسجلات/أمناء السجلات عن طريق EPP. كما أن تدفق بيانات الاتصال والتسجيل المرتبطة بهذا النموذج موضح بمزيد من التفصيل في الملحق ط (المخططات الانسيابية لعملية RDS) وموضحة بالتفصيل في الملحق هـ باستخدام أمثلة الاستعلام. فيما يلي وصف لمقارنة نسبية لهذين النموذجين المفضلين لدى مجموعة EWG بعد تطبيق الطريقة المحددة في الملحق و.

- **المتضمنات الأمنية**- يقدم كلا هذين النموذجين نتائج مشابهة عن التقييم في مقابل تأثيرها على الأمن. وبرغم التعليقات العامة التي وردت على النموذج التجميعي (الذي أعيدت تسميته بعد ذلك إلى متزامن) مثل ما هو مقترح في التقرير الأولي والذي مثل خطرًا بسبب نموذج "فشل النقطة الواحدة" من واجهة مركزية، فقد رأت مجموعة EWG أنه غير متباين بالنسبة للأخطار المطروحة حاليًا بسبب سجلات gTLD الكبيرة ومواقع الويب على الإنترنت ذات الحجم الكبير. وتشير أفضل الممارسات الحالية إلى أن النظم الكبيرة المستندة إلى المعلومات تستغل مراكز البيانات المتعددة ، ونظم التخزين الاحتياطي والاستعادة من الكوارث، بالإضافة إلى البنية التحتية المتنوعة على المستوى الجغرافي والفائضة بالكاملة من أجل الحد من هذه المخاطر.

ويتمتع أي نموذج متزامن بفائدة إضافية تتمثل في قدرته المتميزة على تأمين التنفيذ المتسق للأمن بالإضافة إلى إنفاذ السياسات. ومن خلال التشغيل الدقيق لمكونات النظام، فإن النموذج المتزامن المتميز بالبنية التحتية الموزعة التي تدار من خلال مشغل واحد من المحتمل أن تؤدي إلى أسلوب أكثر وحدة في الوصول إلى الأهداف المحددة للأمن مقارنة بالنموذج الموحد. وهذا في جزء منه بسبب أنه في النموذج الموحد، ربما آلاف من السجلات وأمناء السجلات وجهات التوثيق تدير قواعد البيانات الخاصة بها، بمستويات متباينة من خبرات السجل/أمين السجل/جهات التوثيق والاستثمار في ممارسات الأمن.

- **المخاوف التشريعية ومخاوف الخصوصية** – يقدم كلا هذين النموذجين نتائج متشابهة عند تقييم التأثيرات القضائية وتأثيرات الخصوصية. وفي النموذج الموحد، يتم تخزين البيانات والتحكم فيها في مستوى السجل مع الاحتفاظ بنسخ إضافية في مواقع أخرى (وهي بالتحديد، أمين السجل، وجهة التوثيق، ومراكز النسخ الاحتياطي للبيانات المنتشرة في جميع أنحاء العالم).ويقوم النموذج المتزامن بتخزين والتحكم في البيانات في مواقع متعددة منفصلة عن السجلات، مع نسخ إضافية يتم الاحتفاظ بها في مواقع أخرى (أمين السجل، والسجل، ومراكز النسخ الاحتياطي للبيانات المنتشرة في جميع أنحاء العالم). وعند النظر في جميع النماذج التي يجري تقييمها، فالغالبية لم تقم بالتخلص من تحويل البيانات إلى مواقع متعددة، باستثناء "نموذج التمرير"، والذي يتخلص من حاجة السجلات إلى تخزين بيانات جهات الاتصال.

وعلاوة على ذلك، يتيح النموذج المتزامن تطبيقًا أكثر اتساقًا للقواعد من أجل التوافق مع متطلبات الخصوصية المحلية، حيث إنه من الأيسر إدارة القواعد التي يتحكم فيها كيان واحد (مشغل نظام RDS المتزامن) وليس آلاف من المشاركين المحتملين في النموذج الموحد.

- **الاعتماد** – يمكن تطبيق متطلبات الاعتماد في كل من النموذج المتزامن والنموذج الموحد. حيث يمكن لكلا النموذجين مزايا لتعقب وإنفاذ من يسيئون استخدام نظام الاعتماد، على الرغم من أنه قد يكون من الأيسر القيام بذلك عندما تكون قاعدة البيانات مدارة من خلال كيان واحد في نموذج متزامن، مقارنةً بآلاف المشاركين المحتملين في النموذج الموحد. وعلاوة على ذلك، فإن تنفيذ نموذج موحد سيقتضي مصروفات إضافية بالإضافة إلى التزامات تعاقدية تفصيلية، واتفاقيات مستوى الخدمة، بالإضافة إلى إشراف امتثال ICANN لدعم الإنفاذ المتسق وقدرات التدقيق.

- **التشغيل** – يقدم النموذج المتزامن نظم كفاءة في بعض النواحي التشغيلية الأكثر صعوبة في التنفيذ في نموذج موحد. على سبيل المثال، استخدام ونشر بوابة سهلة الاستخدام تعرض بيانات بلغات/نصوص متعددة قد تكون أسهل في النموذج المتزامن، حيث يمكن ترجمة بيانات جهة الاتصال أو ترجمتها صوتيًا في تنسيق أكثر اتساقًا. ولتحقيق نفس المستوى من الاتساق في نموذج موحد، يجب أن تنص الاتفاقيات بوضوح على مواصفات معيارية لكل من الترجمة الصوتية/الترجمة. ويمكن تصميم كلا النموذجين لإتاحة الفرصة أمام عمليات تدقيق جودة البيانات العشوائية، على الرغم من أن ذلك قد يكون أسهل في التنفيذ داخل نظام متزامن.

  تقل مخاوف تأخر البيانات والمزامنة في النموذج الموحد، حيث إن البيانات التي ستعرض سوف تأتي مباشرة من السجل نفسه. وعلى الرغم من ذلك، فإن سحب البيانات من نموذج متزامن يمثل مشكلات من خلال التأخر والتي يمكن التغلب عليها من خلال حمل جهات التوثيق وأمناء السجلات (من خلال السجلات) على الدفع بتحديثات EPP في الوقت الفعلي إلى نظام SRDS (راجع مبدأ الامتثال رقم 108).

- **التنفيذ** – أي نموذج موحد أكثر توحدًا وتماشيًا مع النموذج الموزع لنظام WHOIS الحالي، أكثر من أي نموذج متزامن. وعلى الرغم من ذلك، فإن متطلبات الأداء وقدرات البحث اللازمة لتوفير ميزات قوية توصي بها مجموعة EWG سوف تتطلب مواصفات تفصيلية ومقاييس للأداء تتجاوز إلى حد كبير المقاييس المعروض في نظام WHOIS الحالي. يجب توفير إشراف أكبر على التزام وموارد ICANN من أجل تأكيد أن كافة الأطراف في النظام الموحد يؤدون واجباتهم وفقًا للمستوى المتوقع. وبموجب أي من النموذجين، فإن المشاركين المتأثرين سوف يتوجب عليهم تحديث منصة البرمجيات الخاصة به من أجل التفاعل مع واجهة RDS لتقديم نتائج البحث وبيانات الاتصال اللازمة.

- **التكاليف** – قد يتم تحقيق توفير في التكاليف من جانب كل من أمناء السجلات والسجلات (وأيضًا جهات التوثيق) بموجب النموذج المتزامن من خلال الإعفاء من الأعباء التشغيلية للرد المستمر والدائم على الاستعلامات المعقدة من واجهة RDS (مثل الاستعلامات العكسية) وفقًا لم هو مطلوب بموجب أي نظام موحد. وعلى وجه الخصوص، فإن مقارنة تكاليف النموذج (المذكورة بالتفصيل في الملحق و) توصلت إلى النتائج التالية:

  (1) ومن خلال الافتراضات المستخدمة، فإن نظام RDS الأصلي أكثر كلفة إلى حد ما في نموذج RDS الموحد (FRDS) عنه في نموذج RDS المتزامن (SRDS). وعلى الرغم من ذلك، فإن النموذج الموحد أعلى حساسية بالنسبة لعدد الاستعلامات العكسية. **مع مقدار أعلى من الاستعلامات العكسية، يصبح نموذج FRDS أكثر كلفة إلى حد كبير من نظام SRDS.** على سبيل المثال، مع حمولة بنسبة 3% من الاستعلامات العكسية بدلاً من حمولة 1% من الاستعلامات العكسية، تصبح تكلفة نموذج FRDS أعلى كلفة بنسبة 35% من نموذج SRDS. ومع استعلامات عكسية بنسبة 5%، فإن التكلفة العامة المتوقعة لنموذج FRDS تزيد بحوالي 85%. وهذا من العوامل الهامة في عدم اليقين والخطر المرتبط بنموذج FRDS. حيث يعتقد أن نموذج SRDS أقل حساسية بالنسبة لكمية الاستعلامات العكسية.

  (2) بالإضافة إلى ذلك، **لنموذج FRDS تكلفة أعلى بالنسبة للنظام البيئي بالكامل بسبب [تكلفته الأعلى] وتأثير على مشغلي السجلات**. وفي نموذج FRDS، يجب على كل مشغل سجل تنفيذ ودعم - بموجب اتفاقية SLA - الردود على استعلامات RDAP لنظام RDS في الوقت الفعلي، بما في ذلك الاستعلامات العكسية واستعلامات WhoWas التاريخية. وبالنسبة للاستعلامات الأخيرة، يجب أيضًا الاحتفاظ بالبيانات التاريخية من خلال مشغلي السجلات، بما يزيد من التكاليف أكثر على السجلات. لاحظ أن هذه التكلفة الإضافية حسب السجلات سوف تكون أعلى وتتجاوز تأثير نظام RDS الأصلي فوق التقدير.

(3) وعلاوة على ذلك، **يتطلب نموذج FDRS عمليات تطبيق وجهود أعلى من حيث الدعم والصيانة والاختبار** مقارنة بنموذج SRDS، حيث إن التفاعلات الأعلى مع مشغلي السجلات متوقعة.

يمكن العثور على مزيد من التفاصيل حول تحليل التكلفة لهذا النموذج بالإضافة إلى نطاقه ومنهجيته، ومقاييسه وافتراضاته الأساسية في الملحق و و "تحليل تكلفة نموذج تنفيذ خدمة دليل التسجيل (RDS)[35]" الذي أعدته IBM لـ ICANN في مارس، 2014.

## د. مبادئ تخزين البيانات، ومستودع البيانات والتسجيل

| رقم. | المتطلبات العامة لمستودع وتخزين البيانات وقيدها |
|---|---|
| .161 | يجب تطوير كل من سياسات الموقع، والاحتفاظ والخصوصية الوصول. |
| .162 | يجب أن تتوافق التخزين والمستودع وسياسات التسجيل والتنفيذ مع القوانين المحلية والدولية. |
| | مبادئ التخزين |
| .163 | للحفاظ على النظم الواسعة والتخلص من نقاط الفشل الفردية، يجب أن ترتكز البيانات على مواقع متعددة (أي ، جهة التوثيق وأمين السجل، والسجل، وموفر المستودع، وموفر RDS). |
| .164 | يجب الحفاظ على الاتساق عندما تخرج البيانات في أماكن متعددة. |
| .165 | ويجب أن تحافظ RDS على عناصر البيانات بطريقة آمنة، مع حماية سرية ووحدة عناصر البيانات المعرضة للخطر من الاستخدام أو الإفصاح غير المرخص. |
| .166 | يجب تخزين بيانات المعاملات بشكل لا متناهي من أجل الحفاظ على دقة سجلات تغيير البيانات على مدار الوقت ودعم وظيفة WhoWas، ولكن بما لا يزيد عن الحدود المقررة (إن وجدت) والمطلوبة للامتثال لقوانين حماية البيانات المعمول بها. كما يجب تطهير بيانات الاتصال المقتطعة بشكل دوري، بما يتفق مع القوانين (على سبيل المثال، عام واحد بعد الحل). |
| | مبادئ[36] المستودعات |
| .167 | ويجب إجراء عمليات التدقيق للبيانات المخزنة من أجل اختبار تنسيق، ووحدة، واكتمال البيانات المودعة. |
| .168 | قد يكون التخزين في المستودعات وتدقيقها أسهل من حيث التنسيق مع نموذج RDS المتزامن. |
| .169 | يجب أن تكون بيانات التخزين في المستودعات في حد ذاتها مشفرة ومبهمة بالنسبة للمدققين. |
| .170 | ويجب الاحتفاظ ببيانات المستودع لفترة زمنية متسقة مع المتطلبات المنصوص عليها في اتفاقية اعتماد أمين السجل، واتفاقيات سجل gTLD الفردية، والقوانين المعمول بها في حماية البيانات. وفي الوقت الحالي، سوف يكون هذا طوال مدة نشر رعاية الكيان للبيانات ولمدة عامين إضافيين بعد لك أو مدة أطول إذا اشترط ذلك بموجب اتفاقية سجل gTLD، ولكن بما لا يزيد عن الحد الأقصى الذي يسمح به القانون. |

[35] https://community.icann.org/display/WG/EWG+Public+Research+Page

[36] يشير المستودع إلى النسخ الاحتياطي المشفر للنظام لدى جهة أخرى معتمدة (موفر المستودع) لأغراض الاستعادة في حالات الكوارث، أو تعطل النظام، إلخ. راجع اتفاقية RAA للحصول على تفاصيل أكثر.

| | مبادئ التسجيل |
|---|---|
| .171 | يجب تسجيل استعلامات RDS من أجل توفير سجلات حول كيفية استخدام النظام. |
| .172 | وقد يلزم القيام بعمليات تجميع السجلات من أجل التعرف على عمليات إساءة الاستخدام الموجهة في النظم الموزعة. |
| .173 | كما يجب تسجيل التغييرات من أجل توفير سجل بعناصر البيانات بمرور الوقت. |
| .174 | ويجب أن يكون الوصول إلى سجلات RDS التشغيلية مقتصرًا على الأفراد والكيانات المعتمدة والموثقة والمرخصة ذات الأغراض المحددة و"الحاجة إلى المعرفة". ويجب أن يشتمل ذلك على مشغلين معتمدين لنظام RDS نفسه (من أجل تأكيد التشغيل الصحيح لنظام RDS واكتشاف مشكلاته وحلها) بالإضافة إلى كيانات حماية البيانات المرخصة (من أجل مراقبة امتثال RDS مع تشريعات حماية البيانات). (راجع أيضًا القسم الثامن (ب)، الوصول إلى إنفاذ القانون.) |

## 9. التكاليف والتأثيرات

### أ. مبادئ التكاليف

وفقًا لما هو مشار إليه في الملحق و، طرق لمقارنة النماذج، فقد نظرت مجموعة EWG أيضًا في تكاليف وتأثيرات نظام RDS. حيث تقر مجموعة EWG بأن بعض الجوانب في النموذج الموصى به سوف تفرض تكاليف جديدة، لكنها ترى أيضًا أن العديد من التكاليف الأخرى الخفية التي يتم تكبدها في نظام WHOIS الحالي غير الكفء وغير الدقيق في أغلب الأحيان يمكن الحد منها. وحيث إن نظام RDS الموصى به يوفر خدمات جديدة ومحسنة، فيجب تقييم كل من المزايا والتكاليف. وسوف يوفر الأسلوب الموصى به لصناع السياسات خيارًا للمرة الأولى يتمثل في صياغة طرق لمن يطلبون بيانات تسجيل من النظام من أجل المساهمة بشكل فعال في تشغيل هذا النظام.

إن تكاليف تشغيل نظام WHOIS غير معروفة في الوقت الحالي، لكنها تشمل تكاليف النظام البيئي بالكامل، ليس فقط بالنسبة للسجلات وأمناء السجلات الذين يعرضون خدمات WHOIS. ولا يتعين على أمناء السجلات تقسيم تكاليف WHOIS، وقد تواجههم صعوبات في التمييز بين تكاليف توفير هذه الخدمات بالنسبة لنطاقات gTLD في مقابل نطاقات ccTLD. وتتكبد الجهات الفاعلة الأخرى في النظام البيئي تكاليف نتيجة حالات عدم الكفاءة والقصور في نظام WHOIS الحالي، مثل حاملي العلامات التجارية الذي يسددون نظير خدمات شركات حماية الأسماء التجارية وخدمات WHOIS التجارية في التعرف على حالات سرقة عناوين الإنترنت.

توصي مجموعة EWG بمبادئ التكلفة التالية:

| رقم. | مبادئ التكاليف |
|---|---|
| .175 | الوصول غير المرخص (غير المحدد ببوابات) إلى عناصر البيانات العامة يجب أن يكون مجانيًا. |
| .176 | أما الوصول المرخص (المحدد ببوابات) بموجب إنفاذ القانون من أجل تفويض عناصر البيانات (مع مراعاة العملية الواجبة) قد يخضع لاعتبارات خاصة من حيث التكلفة. |
| .177 | يجب أن يحقق تصميم RDS كفاية التكاليف والتخفيض إلى الحد الأدنى، دون الإخلال بالأهداف الأخرى. |
| .178 | يجب أن تعمل RDS وفق نموذج استعادة التكلفة. |
| .179 | ولتسهيل عملية الانتقال من نظام WHOIS، يجب إنشاء منصة تطوير برمجية لنظام RDS على أن يتم تمويله من خلال ICANN للحد من تكاليف تنفيذ RDS بالنسبة لكل من السجلات/أمناء السجلات وجهات التوثيق وجهات اعتماد مستخدم RDS. |

| رقم. | مبادئ التكاليف |
|---|---|
| 180. | ولا يجب أن يكون توفير هذه المنصة الخاصة بتطوير البرمجيات عبئًا في غير موضعه على مستخدم RDS الآخرين. |

وبدون الدخول إلى تفاصيل التنفيذ النوعية، يمكن مشاركة التكاليف في سائر أنحاء النظام البيئي. وتشمل الأمثلة على النواحي التي يمكن استعادة التكاليف منها فرض رسوم ترخيص متباينة، أو الاعتماد على المستخدم، أو عناصر البيانات التي يتم الوصول إليها، أو الغرض (مثل رسوم الاستخدام التجاري، أو رسوم التسجيل والمشاركة للمستخدمين المتميزين، أو رسوم الدخول الفائق)، أو المطالبة برسوم مقابل الخدمات ذات الصلة (مثل رسوم استخراج أوراق الاعتماد أو رسوم ما قبل التوثيق).

وقد يقدم نظام RDS أيضًا توفيرًا في التكلفة بالنسبة للسجلات وأمناء السجلات الذين لم يعد لزامًا عليهم توفير وصول عام أو استيفاء أوقات الرد من مستوى الخدمة القوية. ويمكن أيضًا تحقيق توفير في التكلفة بالنسبة لمقدمي الطلبات الساعين للحصول على البيانات من خلال الحد من أوجه القصور بسبب الموفرين غير الممتثلين (أمناء السجلات أو السجلات أو جهات التوثيق أو موفري خدمات الخصوصية/البروكسي).

## ب. المزايا مقارنة بنموذج WHOIS الحالي بموجب اتفاقية RAA لسنة 2013

تم توثيق أوجه قصور WHOIS على مدار العقد الماضي من الزمن من خلال العديد من التقارير والدراسات، الموضحة في الملحق ب. تحسينات على نظام WHOIS، وفقًا لما هو موضح في اتفاقية اعتماد أمين السجل الجديدة لعام 2013 (اتفاقية RAA لسنة 2013) والتي جاءت مقترنة بتحسينات أخرى نجمت عن تقييم مجلس إدارة ICANN لتوصيات فريق استعراض WHOIS، وقد تناولت هذه التحسينات بعضًا من أوجه القصور المعروفة في نظام WHOIS.

وعلى الرغم من أن اتفاقية RAA لسنة 2013 قد طرحت العديد من الالتزامات الجديدة، والأكثر ملاحظة منها متطلبات التوثيق والمصادقة من أجل تحسين الدقة، وهناك أوجه قصور أخرى كبيرة لا تزال موجودة. وفيما يلي تلخيص لأوجه القصور هذه، مقسمة إلى قطاعات من هذا التقرير والتي تحتوي على توصيات لتنفيذ مزيد من المزايا.

| عيب WHOIS بموجب اتفاقية RAA لسنة 2013 | تم التعامل معها من خلال RDS في القسم |
|---|---|
| يعمل الوصول العام مجهول الهوية لكافة عناصر البيانات إلى إنشاء بيئة حيث يمكن أن يحدث التنقيب وإساءة الاستخدام، مع القليل من المساءلة أو القدرة على التصحيح | 3 المستخدمين/الأغراض<br>4 تحسين المساءلة<br>6 (د) المساءلة والتدقيق |
| القدرة المحدودة على حماية خصوصية الأفراد | 6 (أ) حماية البيانات<br>7 تحسين مستوى خصوصية المسجل |
| من خلال القدرة المحدودة على ضمان وحدة بيانات التسجيل، يمكن للمسجلين إدراج تفاصيل خاطئة بسهولة، ويشمل ذلك البيانات المملوكة لآخرين | 5 تحسين جودة البيانات<br>5 (و) قدرة بيانات الاتصال الفريدة |
| الافتقار إلى مزايا الأمان | 4 (ب) الوصول غير المرخص والمحدد ببوابات للبيانات<br>4 (ج) اعتماد مستخدم RDS |
| الافتقار إلى قدرات التدقيق | 6(د) المساءلة والتدقيق |

| عيب WHOIS بموجب اتفاقية RAA لسنة 2013 | تم التعامل معها من خلال RDS في القسم |
|---|---|
| | 8 (د) تخزين البيانات والمستودع والتسجيل |
| الوصول غير مرتبط بشكل مباشر بالأغراض المشروعة المحددة | 3 المستخدمين/الأغراض<br>3 (هـ) جهات الاتصال المستندة للأغراض |
| واجهات وردود استعلامات WHOIS غير المتسقة | 4 (ب) الوصول غير المرخص والمحدد ببوابات للبيانات<br>8 نماذج RDS المحتملة |
| عدم وجود دعم أو معايير لعرض بيانات التسجيل الدولية | 4 (ب) الوصول غير الموثق وعن طريق بوابات للبيانات<br>5 (هـ) التفاعل مع جهات التوثيق |
| قدرة محدودة على تطبيق القواعد المختلفة للتوافق مع الأنظمة المختلفة في خصوصية البيانات | 6 (أ) حماية البيانات |
| مستويات دقة غير مقبولة تؤدي إلى أوجه قصور بالنسبة لمن يسعون للتواصل مع المسجلين | 5 تحسين جودة البيانات<br>3 (هـ) جهات الاتصال المستندة إلى الأغراض |
| عمليات الإدارة المرهقة من أجل تحديث جهات الاتصال عبر أسماء النطاقات المتعددة | 5 تحسين جودة البيانات<br>5 (ج) الدقة والتدقيق وعملية التصحيح |
| صعوبات في تعريف والتواصل مع عملاء خدمات الخصوصية والبروكسي | 3 (هـ) جهات الاتصال المستندة إلى الأغراض<br>7 (أ) خدمات الخصوصية/البروكسي الملحق ح نموذج الترحيل والكشف |
| لا يوجد نظام لخدمات الخصوصية أو البروكسي، بما يتجاوز متطلبات اتفاقية RAA لسنة 2013 تسري فقط على أمناء السجلات والجهات التابعة لهم | 7 (أ) خدمات الخصوصية/البروكسي الملحق ح نموذج الترحيل والكشف |

## ج. تقييم المخاطر والتأثير

وفقًا لما أشرنا في القسم الرابع، تحسين المساءلة، توصي مجموعة EWG بأداء تقييم واسع النطاق للمخاطر من أجل تأكيد أن مبادئ RDS الموصى بها تؤدي في حقيقة الأمر إلى الجمع المناسب والإفصاح عن البيانات بالنسبة للأغراض المحددة، بما يحقق التوازن الصحيح بين المخاطر والمزايا.

في 14 مارس، دعت مجموعة EWG كافة الأطراف التي توفر أو تستخدم بيانات تسجيل أسماء نطاقات gTLD للمشاركة في استطلاع مخاطر RDS على الإنترنت، ويشمل ذلك المسجلين وأمناء السجلات والسجلات بالإضافة إلى مجموعة واسعة من الأفراد وشركات الأعمال والمؤسسات الأخرى التي تستهلك بيانات WHOIS اليوم. وقد وفر هذا الاستطلاع للمجيبين عليه الفرصة لإخبار EWG حول المخاطر والمزايا التي قد يحتوي عليها نظام استبدال WHOIS من الجيل التالية بالنسبة لهم.

وقبل الانتهاء من هذا التقرير، قامت EWG بفحص لقطة من المخاطر والمزايا المحددة من خلال هذا الاستعراض على أمل الحد من المخاطر غير المتوقعة وغير الضرورية. وحتى 29 مايو 2014، فقد أدى هذا الإصدار الإنجليزي من الاستطلاع إلى جمع 180 رد جزئي، أكمل منها 100 تقريبًا الاستطلاع بالكامل. أما من أجابوا عن الاستطلاع فقد كانوا من أميركا الشمالية (68%) وأوروبا (35%) وآسيا (20%) وأميركا اللاتينية (14%) وأفريقيا (11%) وأوقيانوسيا (10%) وكانت مقسمة بالتساوي فيما بين من يستخدم ويوفر بيانات التسجيل. وقد ألقت الإجابات الضوء على المخاطر والمزايا الأكثر احتمالاً وتأثيرًا في النواحي التالية: الفنية والتشغيلية والقانونية والمالية والأمن والخصوصية. كما علق حوالي عشرون مشارك على المخاطر التي لا يمكن تفاديها وغير المقبولة وعلى طرق التخلص من المخاطر أو تقليلها.

ولتمكين تعقيب المجتمع الواسع على هذا الموضوع، قررت مجموعة EWG ترك استطلاع مخاطر RDS مفتوحًا حتى يوليو 2014 وإطلاق إصدارات مترجمة. وسوف يتم استخدام الردود للاستفادة بها في مراجعة مجلس إدارة ICANN لهذا التقرير وكتعقيب على التحليل الرسمي المستقبلي للتكاليف، والمخاطر والمزايا لسائر أصحاب المصلحة والتي قد تتأثر باستبدال نظام WHOIS بنظام RDS.[37]

[37] راجع أيضًا تقييم مخاطر DNS (التكرار 1) للتشاور العام لـ ICANN

## 10. الاستنتاج والخطوات التالية

وبعد مطالعة وجهات نظر العديد من أصحاب المصلحة في النظام البيئي الذي يعتمد على بيانات التسجيل، توصي مجموعة EWG بالإجماع بالتخلي عن نموذج WHOIS الحالي - بما يعطي لكل مستخدم نفس الوصول العام مجهول الهوية إلى بيانات تسجيل gTLD - من خلال نظام بديل، تم بناؤه من الألف إلى الياء.

وتؤمن مجموعة EWG بأن المبادئ ونظام RDS من الجيل التالي الموصى به في هذا التقرير النهائي توفر أساسًا أكثر صلابة عن ما هو موجود في الوقت الحالي - أساسًا يمكن من خلاله حماية الخصوصية الشخصية وضمان مستوى أعلى من الدقة والمساءلة والشفافية بالنسبة لنظام ICANN البيئي الكامل لأعوام قادمة. وينبني نظام RDS على التحسينات التي تمت بموجب اتفاقية RAA لسنة 2013 التي تم التفاوض عليها في الوقت الحالي، لكنه يتجاوز بمراحل كبيرة، وفقًا لما هو موضح بمزيد من التفصيل في القسم التاسع (ب).

في حين قد يبدو التقرير النهائي بالنسبة للبعض مسهب في التفاصيل، إلا أنه غير شامل. وكما أوضحنا في الملحق أ، فإن التقرير يتناول كل من الأسئلة المطروحة من جانب مجلس الإدارة. وعلى الرغم من ذلك، لا تزال العديد من المشكلات عالقة للتعامل معها في المستقبل - سواء في عملية وضع السياسة للمتابعة (PDP) أو أي من جهور التنفيذ ذات الصلة.

- **هيئات الاعتماد والسياسات لمجتمعات مستخدمي RDS.** حيث إن بعض مجتمعات المستخدمين قد تحصل على وصول إلى بيانات محددة ببوابات لغرض معتمد، إلا أن السياسات المستخدمة في تحديد من يتأهلون كأعضاء في هذا المجتمع يجب التحقق منها وفحصها خلال مرحلة التنفيذ، وفقًا لما يجب على هيئات الاعتماد والنماذج المناسبة لكل مجتمع.
- **الامتدادات المطلوبة لكل من EPP وRDAP.** وفقًا لما هو محدد في الملحق ز، توصي مجموعة EWG بأن يتم استخدام البروتوكولات المعيارية تلك من أجل دعم احتياجات RDS، لكنها حددت امتدادات معينة تتطلب الدعم الكامل لنموذج RDS الموصى به بالإضافة إلى عناصر البيانات.
- **تقييم الخطر والتأثير.** وفقًا لما تمت مناقشته في القسم التاسع، توصي مجموعة EWG بتنفيذ وإجراء تقييم كامل للمخاطر بالإضافة إلى تحليل للتكلفة/المزايا قبل تنفيذ نظام RDS الموصى به، قد بدأت بالفعل عملية استطلاع من أجل جمع التعقيبات على تلك العملية.
- **سياسة خصوصية RDS.** كما ناقشنا في القسم السابع، توصي مجموعة EWG بصياغة سياسة أساسية في خصوصية ICANN بالنسبة لنظام RDS، وذلك استنادًا إلى أفضل الممارسات القياسية لحماية الخصوصية، كما يمكن صياغة الفقرات التعاقدية القياسية التي تعطي أثرًا لهذه السياسة عبر سائر قطاعات نظام RDS البيئي.
- **الترجمة الصوتية/الترجمة لبيانات جهات الاتصال.** حيث إن هناك عملية وضع السياسة (PDP) جارية في الوقت الحالي حول هذه المسألة، اختارت مجموعة EWG عدم تكرار الجهود لما يتجاوز المبادئ المحددة فيالقسم الرابع (ب)، واقترحت بدلاً من ذلك إمكانية فحص نتيجة عملية PDP الحالية في المستقبل من أجل تحديد كيفية تطبيق أي من السياسات الجديدة على نظام RDS.
- **خدمات الخصوصية والبروكسي.** سوف يتعين النظر في مبادئ EWG ذات الصلة بموفري خدمات الخصوصية/البروكسي المعتمدين بالإضافة إلى الأعمال التي تجري في الوقت الحالي في منظمة GNSO حول هذا الموضوع، من خلال تسوية نتيجة عملية PDP الحالية مع أي تنفيذ لنظام RDS.
- **النظام البيئي لجهة التوثيق.** إنشاء برنامج للتوثيق بالنسبة لجهات التوثيق، والعمليات المستخدمة في توثيق جهات الاتصال بالنسبة للمسجلين وجهات الاتصال الواقعة في جميع أنحاء العالم، بحاجة إلى مزيد من التقصي خلال مرحلة التنفيذ.

يعكس نظام RDS بحرص التسويات البارعة والمتوازنة مع العناصر المتداخلة التي لا يجب فصلها. وقد استفادت هذه التسويات من التعقيبات الواردة من مجموعة EWG في العديد من التعليقات العامة وندوات الويب والمشاورات الواردة على عملها حتى اليوم. ونتيجة لذلك تشجع مجموعة EWG مجلس الإدارة على توجيه التقرير النهائي إلى منظمة GNSO من أجل اعتماده بالكامل. واختيار اعتماد بعض وليس كل هذه المبادئ الخاصة بتصميم RDS تقوض مزايا النظام البيئي بالكامل. كما أن مجموعة EWG متخوفة من أن فحص المكونات على المستوى الفردي قد يؤدي إلى تكرار النزاع والخلاف في المجتمع الذي صاحب المحاولات السابقة إلى تحسين WHOIS.

قدمت مجموعة EWG هذا التقرير النهائي إلى المدير التنفيذي ومجلس إدارة ICANN، ونشرته بشكل عام على الإنترنت، وسوف تعقد العديد من الجلسات في اجتماع ICANN المقرر في يونيو 2014 في مدينة لندن. كما ستجري أيضًا ندوات ويب وفرص أخرى من أجل مناقشة التقرير والرد على أسئلة مجتمع ICANN حوله. والغرض من التقرير النهائي أن يكون أساسًا بالنسبة لعملية وضع السياسات (PDP) الخاصة بـ GNSO المطلوبة من مجلس الإدارة من أجل توفير بيانات تسجيل gTLD والمفاوضات التعاقدية، حسبما يتناسب. وحيث إن مجلس الإدارة ومجتمع ICANN ينظرون في هذا التقرير النهائي، توصي مجموعة EWG بأن يتم تأطير هذا النظر من خلال الأسئلة التالية:

- هل نظام RDS مفضل على نظام WHOIS الحالي؟
- فإن لم يكن الأمر كذلك، هل يوافق مجتمع ICANN على أن وجود الاستمرار في استخدام نظام WHOIS الحالي، وهل له القدرة على تحقيق احتياجات الإنترنت العالمي المتنامي؟

علمًا بأن مجموعة عمل المتخصصين EWG على ثقة من أن هذا التقرير النهائي يحقق توجيه مجلس إدارة ICANN للمساعدة في إعادة تحديد الغرض وتوفير بيانات تسجيل gTLD التي ستوفر أساسًا لمساعدة مجتمع ICANN (من خلال منظمة GNSO) في إنشاء سياسة عالمية جديدة لخدمات دليل gTLD.

## الملحق أ: الرد على أسئلة مجلس الإدارة

اشتمل قرار مجلس الإدارة الذي وجه أعمال مجموعة EWG على مجموعة من الأسئلة المحددة التي يجب الرد عليها أثناء إجراء التحليل الخاص به. يشير هذا الملحق إلى الأقسام في هذا التقرير والتي تتناول مخاوف مجلس الإدارة.

| أسئلة وإرشادات مجلس الإدارة | أقسام التقرير |
|---|---|
| من المقرر لمجموعة EWG تحديد الغرض من:<br>• جمع،<br>• والحفاظ على<br>• وتوفير الوصول إلى بيانات تسجيل gTLD<br>• والنظر في الضمانات الخاصة بحماية البيانات | القسم الثالث، المستخدمين والأغراض<br>القسم السادس، تحسين المساءلة |
| لماذا يتم تجميع القضايا؟ | القسم الثالث، المستخدمين والأغراض<br>القسم السادس (أ) عناصر البيانات |
| ما الغرض الذي سوف تخدمه البيانات؟ | الملحق د، الأغراض واحتياجات البيانات |
| من الذي يقوم بتجميع البيانات؟ | القسم الخامس، تحسين جودة البيانات<br>الملحق ط المخططات الانسيابية لعملية RDS |
| أين يتم تخزين البيانات وما هي المدة التي يجب تخزينها فيها؟ | القسم الثامن، نماذج RDS المحتملة<br>القسم الثامن (د)، تخزين البيانات |
| أين يتم إيداع البيانات وما هي المدة التي يجب إيداعها فيها؟ | القسم الثامن (د) مبادئ تخزين البيانات، ومستودع البيانات والتسجيل |
| من بحاجة إلى البيانات ولماذا؟ | القسم الثالث، المستخدمين والأغراض |
| من الذي يحتاج إلى تسجيل الدخول للوصول إلى البيانات ولماذا؟ | القسم السادس (د)، مبادئ المساءلة والشفافية |
| الوصول العام إلى تفاصيل حول تسجيل اسم النطاق؟ | القسم الرابع (ب) الوصول غير الموثق وعن طريق بوابات للبيانات<br>القسم السادس (أ) عناصر البيانات<br>القسم السابع، تحسين مستوى خصوصية المسجل |
| وصول إنفاذ القانون إلى تفاصيل حول تسجيل اسم النطاق؟ | القسم الثالث، المستخدمين والأغراض<br>القسم السادس (ب)، مبادئ الوصول للبيانات من خلال إنفاذ القانون |
| وصول صاحب الملكية الفكرية إلى تفاصيل حول تسجيل اسم النطاق؟ | القسم الثالث، المستخدمين والأغراض |
| وصول ممارس الأمن إلى تفاصيل حول تسجيل اسم النطاق؟ | القسم الثالث، المستخدمين والأغراض |
| ما القيم التي يحققها الجمهور بالوصول إلى بيانات التسجيل؟ | القسم الثاني (ب)، الغرض<br>القسم الثالث، المستخدمين والأغراض |
| من بين بيانات التسجيل المتاحة، ما الذي يحتاج الجهور إلى الوصول إليه منها؟ | القسم السادس (أ) عناصر البيانات |
| هل بروتوكول WHOIS هو الاختيار الأفضل بالنسبة لتوفير هذا الوصول؟ | القسم الرابع (ب) الوصول غير الموثق وعن طريق بوابات للبيانات<br>الملحق ز، قدرة بروتوكول EPP وRDAP على دعم RDS |
| الأمن | |
| ما الذي يمثل الحاجة المشروعة لإنفاذ القانون؟ | القسم الثالث، المستخدمين والأغراض<br>القسم السادس (ب)، مبادئ الوصول للبيانات من خلال إنفاذ القانون |

| أسئلة وإرشادات مجلس الإدارة | أقسام التقرير |
|---|---|
| كيف يتم تحديد وكيل إنفاذ القانون؟ | القسم الرابع (ج) مبادئ اعتماد مستخدم RDS<br>القسم السادس (ب)، مبادئ الوصول للبيانات من خلال إنفاذ القانون |
| ما هي بيانات التسجيل وإلى أي مستوى من الدقة تتألف الهوية الحقيقية للطرف المسئول؟ | القسم الخامس، تحسين جودة البيانات<br>القسم السادس (أ) عناصر البيانات<br>القسم السابع (ب) المؤهلات الآمنة المحمية |
| ما هي بيانات التسجيل وإلى أي مستوى من الدقة تتألف المعلومات ذات القيمة بالنسبة لوكيل إنفاذ القوانين الذي يبحث عن الهوية الحقيقية للطرف المسئول؟ | القسم الثالث، المستخدمين والأغراض<br>الملحق د، الأغراض واحتياجات البيانات |
| هل بروتوكول WHOIS هو الاختيار الأفضل بالنسبة لتوفير هذا؟ | القسم الرابع (ب) الوصول غير الموثق وعن طريق بوابات للبيانات<br>الملحق ز، قدرة بروتوكول EPP وRDAP على دعم RDS |
| أصحاب الملكية الفكرية | |
| هل الوصول إلى بيانات تسجيل اسم النطاق المرغوب متسق مع الوصول الذي يحظى به أصحاب الملكية الفكرية للأنواع المماثلة من البيانات في الصناعات الأخرى؟ | القسم الثالث، المستخدمين والأغراض<br>القسم الرابع (ج) مبادئ اعتماد مستخدم RDS |
| كيف يمكن تحديد صاحب الملكية الفكرية؟ | القسم الرابع (ج) مبادئ اعتماد مستخدم RDS |
| من بين كافة بيانات التسجيل المتاحة، ما الذي يتعين على صاحب الملكية الفكرية الوصول إليه منها؟ | القسم الثالث، المستخدمين والأغراض<br>الملحق د، الأغراض واحتياجات البيانات |
| ما بيانات التسجيل المناسبة التي يمكن توفيرها؟ | القسم السادس (أ) عناصر البيانات |
| هل بروتوكول WHOIS هو الطريقة المناسبة للوصول؟ | القسم الرابع (ب) الوصول غير الموثق وعن طريق بوابات للبيانات<br>الملحق ز، قدرة بروتوكول EPP وRDAP على دعم RDS |

## الملحق ب: دراسات تقييم قصور WHOIS

- تقرير SSAC - SAC 051
- تقرير SSAC - SAC 054
- تقرير SSAC - SAC 055
- مبادئ WHOIS لدى GAC
- التقرير النهائي لفريق مراجعة سياسة WHOIS
- مسودة إجراءات ICANN للتعامل مع تضارب WHOIS مع قانون الخصوصية
- قائمة متطلبات خدمة WHOIS – التقرير النهائي
- التقرير الأولي لقوة عمل WHOIS رقم 2 (لسنة 2009)
- التقرير النهائي لقوة العمل حول خدمات WHOIS (لسنة 2007)
- دراسة تقييم الحلول لتقديم وعرض بيانات الاتصال المدوّلة
- التقرير النهائي لـ WHOIS الكثيفة من GNSO
- تقرير بيني من مجموعة EWG حول بيانات التسجيل الدولية
- مراجعة إجراءات ICANN للتعامل مع تضارب Whois مع قانون الخصوصية
- دراسات WHOIS لمنظمة GNSO ويشمل ذلك
  - دراسة دقة معلومات اتصال تسجيل WHOIS
  - دراسة حول سيادة أسماء النطاقات المسجلة باستخدام خدمة خصوصية أو بروكسي بين أعلى 5 نطاقات gTLD
  - دراسات إساءة استخدام WHOIS
  - دراسة تحديد هوية مسجل WHOIS
  - دراسة إساءة استخدام خدمات الخصوصية والبروكسي لـ WHOIS
  - دراسة جدوى لكشف وترحيل وكيل/خصوصية WHOIS + الملاحق

## الملحق ج: أمثلة على حالات الاستخدام

وفقًا لما هو مذكور بالتفصيل في القسم الثالث، قامت مجموعة EWG بتحليل حالات الاستخدام الفعلية التي تشتمل على نظام WHOIS الحالي من أجل التعرف على المستخدمين الراغبين في الوصول إلى بيانات gTLD، وأغراضهم وراء القيام بذلك وأصحاب المصلحة والبيانات المشمولة في ذلك. وقد تناولت مجموعة EWG بالدراسة قائمة من حالات الاستخدام التمثيلية كما هو موضح أدناه.

| الغرض | مثال على حالات الاستخدام |
|---|---|
| التحكم في اسم النطاق | إنشاء حساب تسجيل اسم نطاق |
| | مراقبة تعديل بيانات أسماء النطاقات |
| | إدارة محفظة أسماء النطاقات |
| | البدء في نقل أسماء النطاقات |
| | حذف أسماء النطاقات |
| | تحديثات DNS لأسماء النطاقات |
| | عمليات تجديد أسماء النطاقات |
| | توثيق عقود أسماء النطاقات |
| حماية البيانات الشخصية | الاتصال بموفر خدمة الخصوصية/البروكسي |
| | الاتصال بجهة اعتماد المؤهلات الآمنة |
| حل المشاكل التقنية | الاتصال بالفريق الفني لأسماء النطاقات |
| توثيق أسماء النطاقات | إصدار شهادات أسماء النطاقات |
| مستخدم فردي للإنترنت | الاتصال الفعلي بالعالم |
| | حماية المستهلك |
| بيع أو شراء أسماء نطاقات شركات الأعمال | بيع أسماء النطاقات بالوساطة |
| | مقاصة العلامات التجارية لأسماء النطاقات |
| | الاستحواذ على أسماء النطاقات |
| | الاستعلام عن شراء أسماء النطاقات |
| | السجل التاريخي لتسجيل أسماء النطاقات |
| | أسماء النطاقات لمسجل محدد |
| بحث أسماء النطاقات للمصلحة الأكاديمية/العامة | السجل التاريخي لتسجيل أسماء النطاقات |
| | أسماء النطاقات لجهة اتصال محددة |
| | استطلاع مسجل أسماء النطاقات أو جهات الاتصال المخصصة |
| إجراءات قانونية | اتصال مستخدم اسم النطاق |
| | محاربة الاستخدام المدلس للبيانات المسجل |
| | السجل التاريخي لمسجل اسم النطاق |
| | أسماء النطاقات لجهة اتصال محددة |

| الغرض | مثال على حالات الاستخدام |
|---|---|
| الإنفاذ النظامي والتعاقدي | التحري عن الضرائب عن طريق الإنترنت |
| | إجراءات UDRP |
| | التوافق التعاقدي لنظام RDS البيئي |
| التحري الجنائي والحد من إساءة استخدام DNS | التحري عن إساءة استخدام أسماء النطاقات |
| | التحري عن الأنشطة الجنائية غير المتصلة بالإنترنت |
| | خدمات السمعة لأسماء النطاقات |
| | التحري عن الأنشطة الجنائية المتصلة بالإنترنت |
| | إساءة استخدام جهات الاتصال لأسماء النطاقات الضعيفة |
| شفافية DNS | الولوج إلى بيانات التسجيل العامة |
| أنشطة الإنترنت الضارة | السطو على أسماء النطاقات |
| | تسجيل أسماء النطاقات الضارة |
| | التنقيب عن بيانات التسجيل للتعرف على الرسائل غير المرغوبة/التدليس |

**الجدول 7. مثال على حالات الاستخدام**

لتوضيح منهجية مجموعة EWG، تم إيراد حالة استخدام واحدة أدناه. راجع القسم الثالث للتعرف على أوصاف إضافية لكل حالة استخدام مرتبطة بمستخدمي RDS واحتياجات البيانات.

**حل المشكلة الفنية - الاتصال بالفريق الفني لأسماء النطاقات**

**الهدف/السيناريو رقم 1**

شخص يعاني من مشكلة تشغيلية أو فنية في اسم نطاق مسجل. ويود أن يعرف ما إذا كان هناك شخص يمكنه الاتصال به من أجل حل المشكلة في الوقت الفعلي أو بالقرب من الوقت الفعلي، لذلك فإنه يستخدم RDS من أجل تحديد شخص أو دور أو كيان مناسب يمتلك القدرة على حل المشكلة. تشمل قائمة غير كاملة بالأمثلة على المشكلات الفنية مشكلات إرسال البريد الإلكتروني ومشكلات التسليم، ومشكلات حل DNS، والمشكلات الوظيفية لموقع الويب.

**حالة استخدام التنسيق الموجز**

**حالات الاستخدام:** تحديد شخص أو دور أو كيان يمكنه المساعدة في حل المشكلات الفنية في اسم نطاق.

**حالات الاستخدام الأساسية:** يقوم شخص بالوصول إلى نظام RDS من أجل الحصول على معلومات الاتصال المرتبطة بأسماء النطاقات المسجلة بموجب نطاق TLD أو نطاقات TLD. يقدم الشخص اسم نطاق إلى RDS من أجل التعامل معه. ويعيد RDS المعلومات المرتبطة مع اسم النطاق الذي يحدد شخصًا أو دورًا أو كيانًا يمكن الاتصال به من أجل حل المشكلات الفنية.

**حالة استخدام التنسيق العرضي**

**العنوان:** تحديد شخص أو دور أو كيان يمكنه حل المشكلات الفنية في اسم نطاق.

**الجهة الفاعلة الرئيسية:** شخص يعاني من مشكلة فنية في اسم نطاق مسجل.

**أصحاب مصالح آخرون:** مشغل نظام RDS؛ شخص أو دور أو كيان مرتبط باسم النطاق المسجل الذي يمكنه حل المشكلات الفنية؛ مسجل (قد يهتم بالتعرف على المشكلات التشغيلية)؛ جهة توثيق (ربما يكون قد أصدر معرف اتصال إلى جهة الاتصال الفنية)؛ أمين سجل أو موفر استضافة (قد يوفر خدمة تشغيلية)؛ موفر خدمة خصوصية/بروكسي معتمد (يمكنه المساعدة في التوصل إلى الشخص، أو الدور، أو الكيان المرتبط باسم النطاق الذي يمكنه حل المشكلات الفنية).

**المجال:** التفاعل مع RDS

**المستوى:** مهمة المستخدم

**عناصر البيانات:** عناصر البيانات التي تتيح الاتصال في الوقت الفعلي أو قرب الفعلي هي الأكثر فائدة في سياق حالة الاستخدام هذه. وهذه تشمل عنوان بريد إلكتروني، وعنوان مراسلة فورية، ورقم هاتف، و/أو مؤشر يحدد طريقة الاتصال المفضلة المحددة من جانب المسجل. القسم 4 من RFC 2142 يصف التوصيات الخاصة بعناوين بريد @abuse، و@noc، و@security من أجل "توفير المسار لكل من العملاء والموفرين وغيرهم ممن يعانون من صعوبات في خدمة الإنترنت للمؤسسة"، لكن من المهم ملاحظة أن الطبيعة العامة لهذه العناوين غالبًا ما تجعلها جذابة لمرسلي الرسائل العشوائية غير المرغوبة عن طريق البريد الإلكتروني.

**القصة:** شخص (مقدم طلب) يمر بمشكلات فنية مع اسم نطاق مسجل يقوم بالوصول إلى RDS من أجل الحصول على معلومات حول أسماء النطاقات المسجلة بموجب نطاق TLD أو نطاقات TLD. ويمكن الوصول إلى RDS من خلال أي موقع ويب أو بعض الوسائل الأخرى الخاصة بالتعامل الإلكتروني.

يقوم مقدم الطلب بتقديم اسم نطاق مسجل إلى النظام من أجل المعالجة.

ويتعامل نظام RDS مع الطلب فإما أن يقدم تقريرًا بحالات الأخطاء أو يواصل الاستعلام عن بيانات تسجيل gTLD من أجل استعادة المعلومات المرتبطة بأي شخص أو دور أو كيان تم تحديده في السابق على أنه مصدر للمساعدة في حل المشكلات الفنية بالنسبة لاسم النطاق المعني.

فإما أن يقدم نظام RDS معلومات التسجيل المرتبطة باسم النطاق أو حالة خطأ تمت مصادفتها أثناء استعادة البيانات.

**الشكل 9. مثال على حالة الاستخدام**

## الملحق د: أغراض واحتياجات البيانات

قامت مجموعة EWG بتحليل حالات استخدام من أجل التعرف على المستخدمين الراغبين في الوصول إلى بيانات gTLD، وأغراضهم وراء القيام بذلك وأصحاب المصلحة والبيانات المشمولة في ذلك. ويلخص الجدول التالي عناصر بيانات RDS الموصى بها في القسم الرابع والمرسومة من أجل الأغراض المسموح بها والمحددة في القسم الثالث. راجع القسم الرابع للتعرف على توصيات التجميع والإفصاح لكل عنصر للبيانات.

| عنصر البيانات | الأغراض |
|---|---|
| اسم النطاق | وكل |
| خوادم DNS | التحكم في اسم النطاق<br>حل المشاكل التقنية<br>توثيق أسماء النطاقات<br>بيع/شراء أسماء نطاقات شركات الأعمال<br>بحث DNS للمصلحة الأكاديمية/العامة<br>الإنفاذ التنظيمي/التعاقدي<br>التحري الجنائي/الحد من إساءة استخدام DNS |
| اسم المسجل و/أو المؤسسة<br>نوع المسجل<br>معرف جهة اتصال المسجل<br>حالة توثيق جهة اتصال المسجل<br>آخر توقيت زمني حديث لجهة اتصال المسجل | وكل |
| معرف شركة المسجل | التحكم في اسم النطاق<br>توثيق أسماء النطاقات<br>مستخدم فردي للإنترنت<br>بيع/شراء أسماء نطاقات شركات الأعمال<br>إجراءات قانونية<br>بحث DNS للمصلحة الأكاديمية/العامة<br>الإنفاذ التنظيمي/التعاقدي<br>التحري الجنائي/الحد من إساءة استخدام DNS<br>شفافية DNS |

| عنصر البيانات | الأغراض |
|---|---|
| العنوان البريدي للمسجل، ويشمل:<br>عنوان سكن المسجل<br>مدينة المسجل<br>ولاية/مقاطعة المسجل<br>الرمز البريدي للمسجل<br>الدولة المسجل | التحكم في اسم النطاق<br>توثيق أسماء النطاقات<br>بيع/شراء أسماء نطاقات شركات الأعمال *<br>بحث DNS للمصلحة الأكاديمية/العامة *<br>إجراءات قانونية*<br>الإنفاذ التنظيمي/التعاقدي<br>التحري الجنائي/الحد من إساءة استخدام DNS |
| هاتف + تحويلة المسجل<br>هاتف + تحويلة المسجل البديلة | التحكم في اسم النطاق<br>حل المشاكل التقنية<br>توثيق أسماء النطاقات<br>بيع/شراء أسماء نطاقات شركات الأعمال *<br>بحث DNS للمصلحة الأكاديمية/العامة *<br>إجراءات قانونية*<br>الإنفاذ التنظيمي/التعاقدي<br>التحري الجنائي/الحد من إساءة استخدام DNS |
| عنوان البريد الإلكتروني للمسجل<br>البريد الإلكتروني البديل للمسجل | وكل |
| فاكس + تحويلة المسجل | التحكم في اسم النطاق<br>توثيق أسماء النطاقات<br>بيع/شراء أسماء نطاقات شركات الأعمال *<br>بحث DNS للمصلحة الأكاديمية/العامة *<br>إجراءات قانونية*<br>الإنفاذ التنظيمي/التعاقدي |
| يمكن لمسجلي طرق الاتصال الجديدة اختيار نشر:<br>الرسائل النصية SMS للمسجل<br>الرسائل الفورية IM للمسجل<br>وسائل التواصل الاجتماعي للمسجل<br>وسائل التواصل الاجتماعي البديلة للمسجل<br>عنوان URL لجهة اتصال المسجل<br>عنوان URL لإساءة استخدام المسجل | يمكن أن يكون مفيدًا لكل غرض مسموح به كبديل لعنوان البريد الإلكتروني للمسجل |
| معرف جهة اتصال المشرف<br>عناصر بيانات اتصال المشرف | التحكم في اسم النطاق<br>توثيق أسماء النطاقات<br>بيع/شراء أسماء نطاقات شركات الأعمال<br>بحث DNS للمصلحة الأكاديمية/العامة<br>شفافية DNS |
| معرف جهة الاتصال القانونية<br>عناصر بيانات الاتصال القانونية | التحكم في اسم النطاق<br>توثيق أسماء النطاقات<br>بحث DNS للمصلحة الأكاديمية/العامة<br>إجراءات قانونية<br>الإنفاذ التنظيمي/التعاقدي<br>شفافية DNS |
| جهة الاتصال الفنية<br>عناصر بيانات الاتصال الفنية | التحكم في اسم النطاق<br>حل المشاكل التقنية<br>توثيق أسماء النطاقات<br>بحث DNS للمصلحة الأكاديمية/العامة<br>شفافية DNS |
| جهة اتصال إساءة الاستخدام<br>عناصر بيانات اتصال إساءة الاستخدام | التحكم في اسم النطاق<br>توثيق أسماء النطاقات<br>بحث DNS للمصلحة الأكاديمية/العامة<br>التحري الجنائي/الحد من إساءة استخدام DNS<br>شفافية DNS |

| عنصر البيانات | الأغراض |
|---|---|
| معرف جهة اتصال الخصوصية/البروكسي<br>عناصر بيانات اتصال موفر الخصوصية/البروكسي | التحكم في اسم النطاق<br>حماية البيانات الشخصية<br>توثيق أسماء النطاقات<br>بحث DNS للمصلحة الأكاديمية/العامة<br>شفافية DNS |
| معرف جهة اتصال الأعمال<br>عناصر بيانات اتصال الأعمال | التحكم في اسم النطاق<br>توثيق أسماء النطاقات<br>مستخدم فردي للإنترنت<br>بحث DNS للمصلحة الأكاديمية/العامة<br>شفافية DNS |
| تفويض DNSSEC | التحكم في اسم النطاق<br>بحث DNS للمصلحة الأكاديمية/العامة |
| حالة التسجيل<br>حالة العميل (أمين السجل)<br>حالة الخادم (السجل) | التحكم في اسم النطاق<br>بيع/شراء أسماء نطاقات شركات الأعمال<br>بحث DNS للمصلحة الأكاديمية/العامة<br>الإنفاذ التنظيمي/التعاقدي<br>التحري الجنائي/الحد من إساءة استخدام DNS |
| أمين السجل<br>الموزع<br>عنوان URL لأمين السجل<br>رقم IANA لأمين السجل<br>عنوان البريد الإلكتروني لجهة اتصال إساءة الاستخدام لدى أمين السجل<br>رقم هاتف جهة اتصال إساءة الاستخدام لدى أمين السجل<br>عنوان URL لموقع شكاوى مركز معلومات شبكة الإنترنت Internic | التحكم في اسم النطاق<br>بيع/شراء أسماء نطاقات شركات الأعمال<br>بحث DNS للمصلحة الأكاديمية/العامة<br>الإنفاذ التنظيمي/التعاقدي<br>التحري الجنائي/الحد من إساءة استخدام DNS<br>شفافية DNS |
| الدائرة القضائية لأمين السجل<br>الدائرة القضائية للسجل<br>لغة اتفاقية التسجيل | الكل |
| تاريخ التسجيل الأصلي | التحكم في اسم النطاق<br>بيع/شراء أسماء نطاقات شركات الأعمال<br>بحث DNS للمصلحة الأكاديمية/العامة<br>الإنفاذ التنظيمي/التعاقدي |
| تاريخ الإنشاء<br>تاريخ التحديث<br>تاريخ انتهاء أمين السجل | التحكم في اسم النطاق<br>بيع/شراء أسماء نطاقات شركات الأعمال<br>بحث DNS للمصلحة الأكاديمية/العامة<br>الإنفاذ التنظيمي/التعاقدي<br>التحري الجنائي/الحد من إساءة استخدام DNS |

ملاحظة: الوصول إلى عناصر بيانات المسجل المطلوبة في بعض الأحيان حسب الأغراض والمميزة بعلامة * أعلاها موافقة الرغبة في المعرفة، راجع القسم الثالث للتعرف على مناقشة "البيانات المعتمدة المحددة ببوابات".

## الملحق هـ: توضيح الوصول للبيانات المحددة ببوابات وغير المرخصة

يعمل سجل بيانات التسجيل التالي على تمديد مثال WHOIS في اتفاقية RAA لسنة 2013 بحيث يعكس مبادئ RDS الموصى بها في جمع والإفصاح عن البيانات.

العناصر الرمادية اختيارية التحديد، أما البقية فإلزامية.
**العناصر العريضة دائمًا ما تكون معلومات عامة**; والبقية ربما تكون محددة ببوابات، وفقًا لاختيار صاحب جهة الاتصال.

| | |
|---|---|
| مقدمة من السجل أو أمين السجل | **حالة التسجيل: x** |
| | **DNSSEC تفويض: signedDelegation** |
| | **حالة العميل: DeleteProhibited, RenewProhibited, TransferProhibited** |
| | **حالة الخادم: DeleteProhibited, RenewProhibited, TransferProhibited** |
| | **أمين السجل: EXAMPLE REGISTRAR LLC** |
| | **بائع التجزئة: EXAMPLE RESELLER** |
| | **الدائرة القضائية لأمين السجل: EXAMPLE JURISDICTION** |
| | **الدائرة القضائية للسجل: EXAMPLE JURISDICTION** |
| | **لغة اتفاقية التسجيل: ENGLISH** |
| | **تاريخ الإنشاء: 2000-10-08T00:45:00Z** |
| | **تاريخ التسجيل الأصلي: 2000-10-08T00:45:00Z** |
| | **تاريخ انتهاء تسجيل أمين السجل: 2010-10-08T00: 44:59 Z** |
| | **تحديث التسجيل: 2009-05-29T20:13:00Z** |
| | **عنوان URL لأمين السجل: http://www.example-registrar.tld** |
| | **رقم IANA لأمين السجل: 5555555** |
| | **المسجل شكوى اتصل بنا البريد الإلكتروني: email@registrar.tld** |
| | **المسجل شكوى اتصل بنا الهاتف: +1.1235551234** |
| | **عنوان URL لموقع شكاوى مركز معلومات شبكة الإنترنت /Internic: http://wdprs.internic.net** |
| يتم جمعها من المسجل | **اسم النطاق: EXAMPLE.TLD** |
| | **خادم الاسم: NS01.EXAMPLE-REGISTRAR.TLD** |
| | اسم المسجل: EXAMPLE REGISTRANT |
| | **نوع المسجل: LEGAL PERSON** |
| | **معرف اتصال المسجل: xxxx-xxxx** (يصدر من جهة التوثيق المعتمدة من RDS) |
| | **حالة توثيق جهة اتصال المسجل (من جهة التوثيق)** |
| | **آخر توقيت زمني موثق لجهة اتصال المسجل (من جهة التوثيق)** |
| | منظمة المسجل: EXAMPLE ORGANIZATION |
| | معرف شركة المسجل: D-U-N-S #12345 (issued by Dunn and Bradstreet) |
| | **البريد الإلكتروني للمسجل: EMAIL@EXAMPLE.TLD** |
| | البريد الإلكتروني البديل للمسجل: EXAMPLE@OTHERDN.TLD |

| | |
|---|---|
| | شارع المسجل: EXAMPLE STREET 123<br>مدينة المسجل: ANYTOWN |
| | دولة/مقاطعة المسجل: AP<br>الرمز البريدي للمسجل: A1A1A1 |
| | **دولة المسجل**: AA<br>هاتف المسجل: 1.5555551212+<br>تحويلة هاتف المسجل: 1234 |
| | الهاتف البديل للمسجل: <cellnumber><br>تحويلة الهاتف البديلة للمسجل: 1234<br>فاكس المسجل: 1.5555551213+<br>تحويلة فاكس المسجل: 4321<br>الرسائل النصية للمسجل: <textingnumber><br>الرسائل الفورية IM للمسجل: <IMhandle><br>وسائل التواصل الاجتماعي للمسجل: <SMhandle><br>وسائل التواصل الاجتماعي البديلة للمسجل: <OtherSMhandle><br>عنوان URL لجهة اتصال المسجل: <link to contact me form or instructions><br>عنوان URL لجهة اتصال المسجل: <link to abuse report form or instructions> |
| يجب على المسجل نشر جهات الاتصال المستندة إلى الأغراض لأنواع PBC الإلزامية | **معرف اتصال المشرف: xxxx-xxxx**<br>**(يتبعه تفاصيل اتصال PBC للمشرف*)** |
| | **معرف الاتصال الفنية: xxxx-xxxx**<br>**(يتبعه تفاصيل اتصال PBC الفنية*)** |
| | **معرف الاتصال القانوني: xxxx-xxxx**<br>**(يتبعه تفاصيل اتصال PBC القانونية*)** |
| | **معرف اتصال إساءة الاستخدام: xxxx-xxxx**<br>**(يتبعه تفاصيل اتصال PBC لإساءة الاستخدام*)** |
| | معرف اتصال الأعمال: xxxx-xxxx (فقط إذا كان نوع المسجل = شخصية اعتبارية)<br>(يتبعه تفاصيل اتصال PBC للأعمال*) |
| | معرف اتصال الخصوصية: xxxx-xxxx (فقط إذا كان نوع المسجل = موفر خصوصية/بروكسي)<br>(يتبعه تفاصيل اتصال PBC لموفر الخصوصية/البروكسي*) |

المفتاح: العناصر الرمادية اختيارية/شرطية التحديد، أما البقية فإلزامية.

* العناصر العريضة دائمًا ما تكون معلومات عامة; والبقية ربما تكون محددة ببوابات، وفقًا لاختيار صاحب جهة الاتصال.

عناصر بيانات PBC ليست موضحة هنا بالكامل.

**مثال رقم 1: الاستعلام العام غير الموثق لأغراض حل المشكلات الفنية**

1) يقدم المستخدم استعلام RDS غير موثق
(DN = MerchantZ.gtld, Purpose = Tech Issue Resolution, Data = All)

2) يقوم RDS بتقييم الاستعلام:
بدون توثيق لأن الاستعلام غير موثق
بدون تفويض، لذلك، تم منح الوصول إلى البيانات العامة
الوصول مقيد على البيانات العامة المطلوبة لحل المشكلة الفنية --
أي كافة البيانات العامة المطلوبة لاسم النطاق بالإضافة إلى جهة الاتصال الفنية

3) نظام RDS يستعيد عناصر البيانات المطلوبة:
تتم استعادة بيانات MerchantZ.gtld من ذاكرة RDS المؤقتة (المتزامنة) أو أن السجل (الموحد) يقدم فقط عناصر بيانات عامة يتم تحديدها لهذا الغرض، ويشمل ذلك

Registrant Contact ID = 12345
Registrant Type = Legal Person
Registrant Organization = MerchantZ, Inc.[38]
Tech Contact ID = 67890

تتم استعادة معرف الاتصال الفني [67890] من ذاكرة RDS المؤقتة أو جهة التوثيق، من خلال الحصول فقط على عناصر البيانات العامة التي يتم نشرها صراحة من خلال هذا الاتصال لهذا الغرض ويشمل ذلك

PBC ID = 67890

PBC Name= <name of entity responsible for resolving <technical issues for domain name MerchantZ.gtld>

PBC Email Address= <mandatory email address of entity responsible for resolving technical issues for domain name <MerchantZ.gtld>

PBC Alt Email Address= <recommended alternative email address of entity responsible for resolving technical issues <for this DN>

PBC Phone Number = <recommended phone number of <entity responsible for resolving technical issues for this DN>

PBC Contact_URL= <recommended contact link published by <entity responsible for resolving technical issues for this DN>

any optional public data elements published by this entity>>

[38] يتم جمع معلومات منظمة المسجل من المسجلين الذين يحددون نوع المسجل على شخصية اعتبارية أو موفر خدمة خصوصية/بروكسي معتمدة؛ وقد تغيب إذا كان نوع المسجل محدد افتراضيًا على غير موضح

4) يقدم نظام RDS حالة خطأ أو رد ناجح على المستخدم. على سبيل المثال:

| |
|---|
| اسم النطاق: MerchantZ.gtld<br>Registration Status: x<br>Client Status: DeleteProhibited, RenewProhibited, TransferProhibited<br>Server Status: DeleteProhibited, RenewProhibited, TransferProhibited<br>Registrar: EXAMPLE REGISTRAR LLC<br>Registrar Jurisdiction: EXAMPLE JURISDICTION<br>Registry Jurisdiction: EXAMPLE JURISDICTION<br>Registration Agreement Language: ENGLISH<br>Creation Date: 2000-10-08T00:45:00Z<br>Registrar Registration Expiration Date: 2010-10-08T00:44:59Z<br>Updated Date: 2009-05-29T20:13:00Z<br>http://www.example-registrar.tldRegistrar URL:<br>Registrar IANA Number: 5555555<br>Registrar Abuse Contact Email: email@registrar.tld<br>Registrar Abuse Contact Phone: +1.1235551234<br>/URL of the Internic Complaint Site:http://wdprs.internic.net |
| Name Server: NS01.EXAMPLE-REGISTRAR.TLD<br>Registrant Contact ID = 12345<br>Registrant Type = Legal Person<br>Registrant Organization = MerchantZ, Inc.<br>Registrant Email = 12345@MerchantZ.gtld<br>Registrant Contact Validation Status = Operationally-Validated<br>Registrant Contact Last Validated Timestamp = x<br>Other Optional Public Data Elements published by Registrant for this ><br><DN |
| Tech Contact ID = 67890<br>PBC ID = 67890<br>BC Validation Status = Operationally-Validated<br>PBC Last Validated Timestamp = x<br>PBC Name: EXAMPLE TECHNICIAN<br>SuperbHostingServices.gtld@67890 = PBC Email<br>PBC Alt Email = SuperbHostingServices@OtherDN.gtld<br>BC Phone Number =+1.1235567890<br>PBC Contact_URL=TechSupport@SuperbHostingServices.gtld<br><Optional Public Data Elements published by this PBC> |

**مثال رقم 2: الاستعلام الموثق عن طريق بوابات لأغراض حل المشكلات الفنية**

1) يقدم المستخدم استعلام RDS موثق
(DN = PersonY.gtld, Purpose = Tech Issue Resolution, Data = All)

2) يقوم RDS بتقييم الاستعلام:
- إذا كانت "A" موثقة، يتم اعتماد الاستعلام عن طريق بوابات
- إذا كان "A" عبارة عن ISP معتمد، يتم منح الوصول لأغراض حل المشكلة الفنية
- الوصول مقيد على البيانات العامة+المحددة ببوابات المطلوبة لحل المشكلة الفنية --
- الوصول مقيد على البيانات العامة+المحددة ببوابات المطلوبة لحل المشكلة الفنية --
أي كافة البيانات العامة+المحددة ببوابات والمطلوبة لهذا الغرض بالإضافة إلى جهة الاتصال الفنية

3) نظام RDS يستعيد عناصر البيانات المطلوبة:
تتم استعادة بيانات PersonY.gtld من ذاكرة RDS المؤقتة (المتزامنة) أو أن السجل (الموحد) يحصل على عناصر بيانات عامة+محددة ببوابات يتم تحديدها لهذا الغرض، ويشمل ذلك

Registrant Contact ID = 12345
Registrant Type = Undeclared
any optional public or gated data elements published by this >
<Registrant – for example, if Registrant chooses, his/her name
Tech Contact ID = 67890[39]

تتم استعادة معرف الاتصال الفني [67890] من ذاكرة RDS المؤقتة أو جهة التوثيق، من خلال الحصول على عناصر بيانات عامة+محددة ببوابات يتم نشرها صراحة من خلال هذا الاتصال لهذا الغرض ويشمل ذلك

PBC ID = 67890

PBC Email Address = <mandatory email address of entity responsible for resolving technical issues for domain name <PersonY.gtld>

PBC Alt Email Address = <recommended alternative email address of entity responsible for resolving technical issues <for this DN>

PBC Phone Number = <recommended phone number of <entity responsible for resolving technical issues for this DN

PBC Contact_URL = <recommended contact link published by entity responsible for resolving technical issues for this <DN>

any optional public or gated data elements published by >
<this entity – for example, SMS Number

[39] إذا لم يقدم المسجل أي معرفات اتصال خلال تسجيل DN، فيجب إشعار المسجل بأن العناوين الخاصة بالمسجل سوف يتم نشرها كعنوان PBC أولي ويتم إعطاؤه الفرصة للموافقة من أجل توفير معرف PBC أولي آخر (على سبيل المثال، معرف اتصال موفر الخصوصية)، أو إلغاء التسجيل.

4) يقدم نظام RDS حالة خطأ أو رد ناجح على المستخدم. على سبيل المثال:

| |
|---|
| اسم النطاق: PersonY.gtld<br>Registration Status: x<br>Client Status: DeleteProhibited, RenewProhibited, TransferProhibited<br>حالة الخادم: DeleteProhibited, RenewProhibited, TransferProhibited<br>Registrar: EXAMPLE REGISTRAR LLC<br>Registrar Jurisdiction: EXAMPLE JURISDICTION<br>Registry Jurisdiction: EXAMPLE JURISDICTION<br>Registration Agreement Language: ENGLISH<br>Creation Date: 2000-10-08T00:45:00Z<br>Registrar Registration Expiration Date: 2010-10-08T00:44:59Z<br>Updated Date: 2009-05-29T20:13:00Z<br>Registrar URL: http://www.example-registrar.tld<br>Registrar IANA Number: 5555555<br>Registrar Abuse Contact Email: email@registrar.tld<br>Registrar Abuse Contact Phone: +1.1235551234<br>/URL of the Internic Complaint Site:http://wdprs.internic.net |
| خادم الاسم: NS01.EXAMPLE-REGISTRAR.TLD<br>Registrant Contact ID = 12345<br>Registrant Type = Undeclared<br>Registrant Email = 12345@PersonY.gtld<br>Registrant Contact Validation Status = Operationally-Validated<br>Registrant Contact Last Validated Timestamp =x<br>Other Optional Public or Gated Data Elements published by Registrant ><br>for DN, such as Registrant Name or Registrant SMS or Registrant<br>< Contact_URL |
| Tech Contact ID = 67890<br>PBC ID = 67890<br>BC Validation Status = Operationally-Validated<br>PBC Last Validated Timestamp = x<br>PBC Name: EXAMPLE TECHNICIAN<br>SuperbHostingServices.gtld@67890 = PBC Email<br>PBC Alt Email = SuperbHostingServices@OtherDN.gtld<br>BC Phone Number =+1.1235567890<br>PBC Contact_URL=TechSupport@SuperbHostingServices.gtld<br><Optional Public or Gated Data Elements published by this PBC> |

**مثال رقم 3: الاستعلامات المعتمدة للبيانات المحددة ببوابات لأغراض شراء/بيع أسماء النطاقات أو الإجراءات القانونية**

التحري عن الانتهاكات المعتمدة للعلامات التجارية موضع أدناه، ولكن تسري نفس نقاط وخطوات البداية على شراء أسماء النطاقات، والاندماج/الاستحواذ، والعديد من عمليات التقصي الأخرى داخل هذه الأغراض والأغراض الأخرى.

**الخطوة 1)** يقوم مستخدم RDS بتسجيل الدخول إلى هيئة اعتماد (والمعرفة بلفظ القسم الرابع (ج)، اعتماد مستخدم RDS) والإقرار بأن الهدف الخاصة به ليس فقط إجراء قانوني، ولكن أيضًا يتم الحصول على البيانات من أجل التقصي عن الانتهاكات المحتملة للعلامات التجارية من خلال الجهة "س". ويوفر المستخدم معلومات الاسم والاتصال الخاصة بالفرد/المؤسسة موضوع الاهتمام. استعلامات RDS لهذا الغرض محدودة بالأساس على بيانات التسجيل المرتبطة بهذه الجهة.

**الخطوة 2)** ويجوز لمستخدم RDS بعد ذلك أداء استعلام عكسي على القيم المعروفة بالفعل حول الجهة، بالبحث في RDS للحصول على قائمة بأسماء النطاقات التي تحتوي على قيم محددة:

- اسم/مؤسسة المسجل و/أو PBC
- الهاتف/الهاتف البديل للمسجل و/أو PBC
- العناوين البريدية للمسجل و/أو PBC
- البريد الإلكتروني/البريد الإلكتروني البديل للمسجل و/أو PBC

يجوز تحديد بعض من عناصر هذه البيانات عن طريق بوابات. يقوم الاستعلام العكسي بالبحث على عناصر البيانات هذه المحددة ببوابات والمعتمدة، لكن فقط لقيمة محددة وغرض محدد، وفقًا لما هو موضع بالتفصيل في الشهادة.

**الخطوة 3)** بالنظر إلى قائمة من أسماء النطاقات قيد التحري عن ما يمكن اعتباره مشاركة في عملية انتهاك للعلامات التجارية قيد التحري، يمكن لمستخدم RDS الآن أداء استعلامات RDS على أسماء النطاقات هذه من أجل الحصول على البيانات المطلوبة لتقييم الحالات، لاسيما:

- معرف جهة الاتصال
- تواريخ التسجيل
- الدائرة القضائية لأمين السجل
- الدائرة القضائية للسجل
- دولة المسجل (الاختصاص القضائي للمسجل)
- مؤسسة المسجل
- معرف شركة المسجل

وقد تتم المطالبة بنفس هذه المعلومات في استعلامات WhoWas لأسماء النطاقات هذه. في هذه الخطوة، تكون كافة عناصر البيانات عامة إلا عنصر واحد؛ والبيانات الوحيدة المحددة ببوابات هي دولة المسجل.

**الخطوة 4)** وبالتوصل إلى أن هذه الإجراء الإضافي أمر مناسب، يجوز لمستخدم RDS إجراء استعلام RDS من أجل استعادة معرف الاتصال القانوني العام المنشور بالإضافة إلى بيانات الاتصال المرتبطة (بما في ذلك اسم/مؤسسة، وهاتف PBC وعنوانه البريدي). يمكن استخدام النتائج في محاولة الاتصال بجهة الاتصال القانونية المعينة للمسجل، أو يمكن استخدام من أجل رفع قضية، من خلال جلب دعوى UDRP، أو اتخاذ أية إجراءات أخرى قانونية.

**الخطوة 5)** إذا رفضت جهة الاتصال القانونية المسئولية عن اسم النطاق، فقد تكون بيانات الاتصال الكاملة للمسجل مطلوبة من أجل اتخاذ إجراء قانوني. وقد يكون غالبية هذه البيانات معروفة في الخطوة 1، ولم يتم الحصول عليها من RDS. وعلى الرغم من ذلك، قد تكون هناك بعض الفجوات التي يجب ملأها عند هذه النقطة.

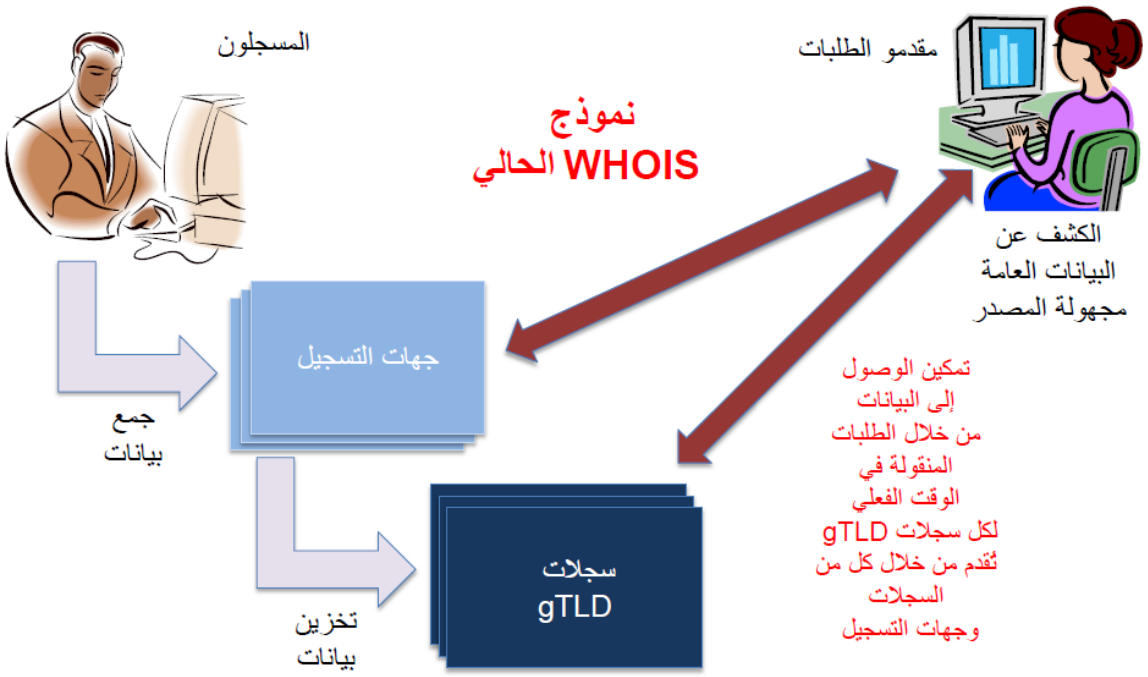
يوضح هذا المثال تفاعلات RDS التي قد تشتمل على تحقيقات وإجراءات قانونية محتملة فيما يتعلق بانتهاك العلامات التجارية. وعلى الرغم من ذلك فإن مجموعة مماثلة من الخطوات قد تتم في أنواع أخرى من الإجراءات القانونية وعند التحري عن أصول أسماء النطاقات خلال عملية شراء/بيع. وفي الحالات التي تنطوي على بيانات محددة ببوابات ومعتمدة، يجب على جهة الاعتماد تحمل المسئولية عن تدقيق الوصول من أجل اكتشاف الطلبات التي قد تتجاوز النطاق الضيق المؤكد ولاتخاذ خطوات من أجل الحيلولة دون إساءة الاستخدام وإنفاذ الشروط التعاقدية. والحصول على شهادة مستخدم RDS على الملف سوف تساعد جهة الاعتماد على تدقيق الوصول وتحري إساءة الاستخدام المحتملة. وسوف تعمل أيضًا كعائق أمام محاولات التصيد.

## الملحق و: نماذج النظم التي تمت دراستها والمنهجيات

بالإضافة إلى النماذج التي وصفت في السابق في نماذج RDS المحتملة، فقد تناولت مجموعة EWG البدائل التالية بالدراسة لكنها توصلت إلى أن كل منها أقل إمكانية من حيث التطبيق عن النموذجين الموحد والمتزامن، للأسباب الملخصة أدناه.

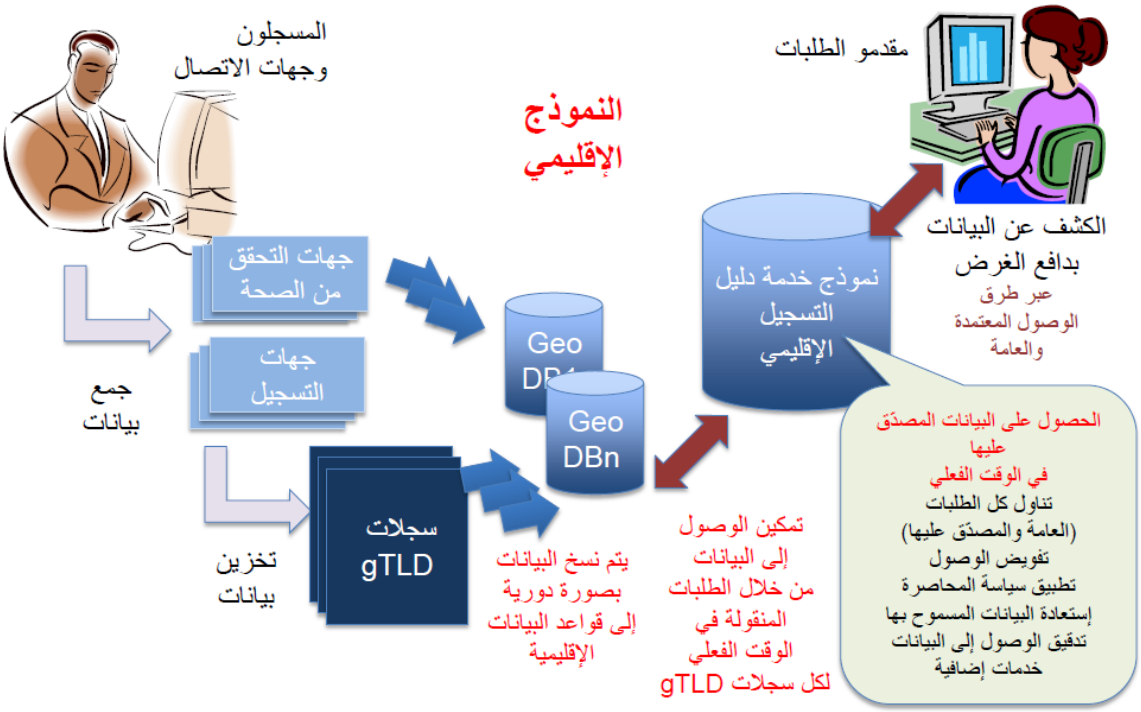
### WHOIS الحالي

ويصف هذا النموذج الأسلوب المستقل الموزع بالكامل المستخدم من خلال نظام WHOIS الحالي، مع قيام كل سجل وأمين سجل بعرض خدمات WHOIS الخاصة به بدون تكامل عبر كافة نطاقات gTLD. على الرغم من إمكانية بناء بوابة مركزية من المقرر أن تمكن من الوصول إلى WHOIS عبر كافة نطاقات gTLD، إلا أن كل سيظل يوفر التخزين والوصول الخاص به والمدار بشكل مستقل، سواء بشكل مباشر (كثيف) أو من خلال التفويض إلى أمناء السجلات (نحيل).



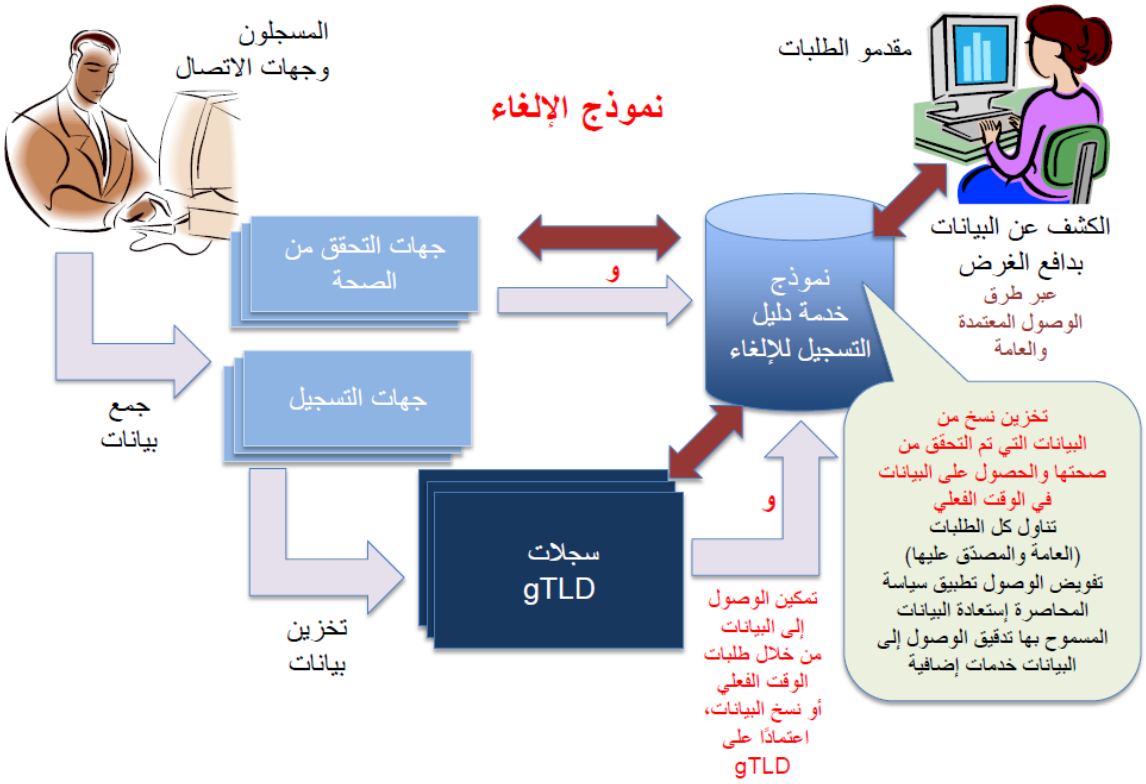
## النموذج الإقليمي

يصف هذا النموذج نظام RDS الذي ينسخ بصفة دورية البيانات من مناطق التخزين الموزعة والتي يديرها السجلات وجهات التوثيق في مناطق التخزين الإقليمية الواقعة حول العالم. وتواصل السجلات وجهات التوثيق تخزين البيانات، إلا أن النسخ الإقليمية من هذه البيانات يمكن استخدامها من خلال RDS من أجل التعامل مع طلبات الوصول بمزيد من الفاعلية. وتتم إدارة مناطق التخزين الإقليمية من خلال نظام RDS إلا أنها تخضع لقوانين الاختصاص القضائي الذي يقع فيه كل منها.



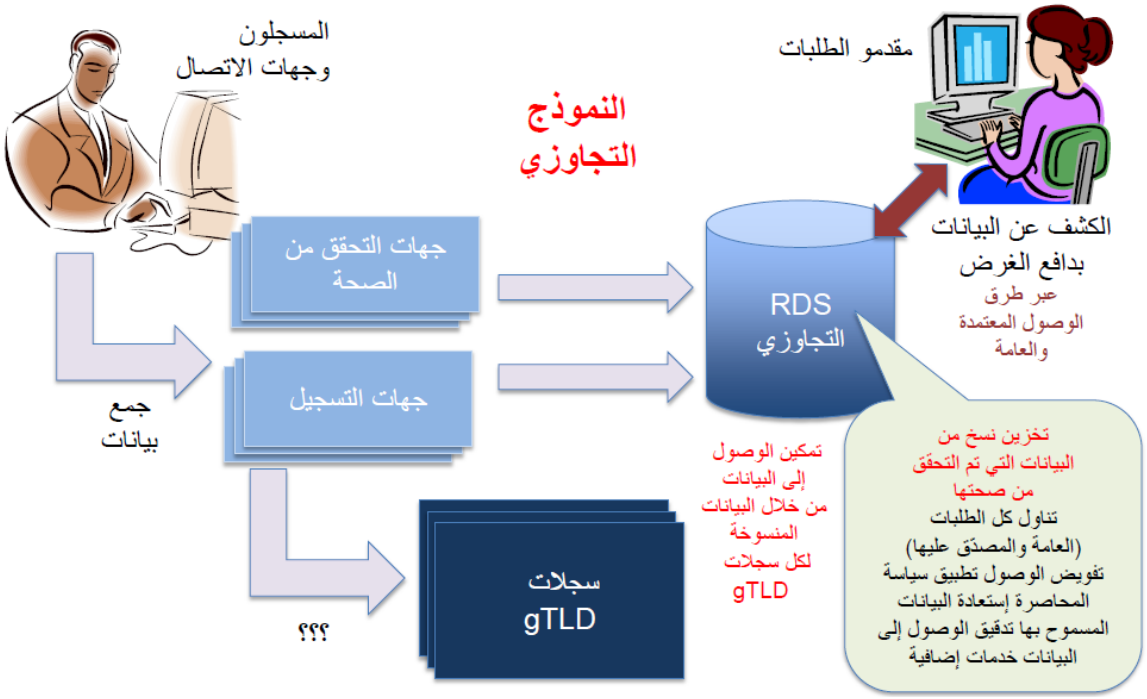
## نموذج عدم الاختيار

يصف هذا النموذج نظام RDS الذي ينسخ بصفة دورية البيانات من مناطق التخزين الموزعة والتي يديرها السجلات في مخزن متزامن تديره RDS. وبموجب هذا النموذج، يمكن لأي سجل اختيار التخزين المتزامن طالما يوافق على توفير البنية التحتية الضرورية من أجل التعامل مع الاستعلامات الكبيرة اللازمة بموجب توافر وأداء اتفاقيات مستوى الخدمة (SLA).



## نموذج التمرير

يصف هذا النموذج نظام RDS الذي ينسخ بصفة دورية البيانات من مناطق التخزين الموزعة والتي يديرها أمناء السجلات في مخزن متزامن تديره RDS. وبموجب هذا النموذج، يتم تمرير السجلات باعتبارها مصدرًا لمعلومات التسجيل، وعوضًا عن ذلك، فإن استعلامات خدمات RDS التي تستخدم بيانات التسجيل المتزامن تنسخ بشكل مباشر من المصادر الموثوقة.



### المنهجية المتبعة في مقارنة نماذج النظم

تداولت مجموعة EWG التكاليف الحالية ونواحي اختراق الأمن المتأصلة في نظام WHOIS الحالي، والتي تم التعامل مع العديد منها في التقارير المدرجة في الملحق ب والتي توثق أوجه القصور في نظام WHOIS. وقد تمت مقارنة التكاليف ونواحي الاختراق في نظام WHOIS الحالي وتمت مضاهاتها مع النماذج المحتملة. بالإضافة إلى ذلك، قامت مجموعة EWG بمقارنة مزايا وعيوب الأمن في كل من النماذج الممكنة في مقابل المعايير التالية:

#### التبعات الأمنية

- **نقطة فشل واحدة:** مع الأخذ في الاعتبار استخدام الهيكل الموزع وموفر الخدمة الأساسي، ما مدى اختراق النموذج بالنسبة لأي فشل نظام واحد؟ هل يمنع فشل أي نظام بشكل مؤقت من الوصول إلى كافة المعلومات أو معلومات التسجيل فقط؟ **ملاحظة:** يجب استخدام التصميم السليم لقواعد البيانات والممارسات السليم للتشغيل من أجل توفير الوفرة الداخلية والنسخ الاحتياطي للبيانات، بحيث يكون ذلك فقط حول توافر البيانات خلال الفشل.
- **عرضة لإساءة الاستخدام الداخلي:** ما مدى اختراق النموذج بالنسبة للإساءة الداخلية لوصول الإداريين/المشغلين إلى معلومات التسجيل المخزنة من خلال أو تمر عبر أي من النظم التي تمثل النموذج؟ هل يمكن أن تؤدي إساءة الاستخدام الداخلية إلى وصول غير مرخص إلى كافة أو بعض البيانات؟ ما مدى سهولة تطبيق عناصر التحكم من أجل اكتشاف/التعرف على إساءة الاستخدام الداخلية؟
- **عرضة للهجوم الخارجي:** ما مدى اختراق النموذج بالنسبة للهجوم الداخلي في مقابل أي نظام يمثل النموذج؟ هل يمكن أن يؤدي الهجوم الخارجي إلى اختراق الخصوصية لكل أو بعض المسجلين؟ ما مدى سهولة تطبيق عناصر التحكم من أجل اكتشاف/التعرف على الهجوم الخارجي؟
- **الاتساق الأمني:** ما مدى اختراق النموذج بالنسبة لتنفيذ الأمن غير المتسق وإنفاذ السياسات؟ هل من المحتمل تحقيق أهداف الأمن بشكل موحد من خلال سائر الجهات الفاعلة في مكونات التشغيل الخاصة بالنظام؟ أم أن الأمن سيتأثر للغاية بالاختلافات في خبرات السجلات/أمناء السجلات/جهات التوثيق والاستثمار؟

#### الاختصاص القضائي وتبعات الخصوصية

- **تخزين البيانات في الاختصاصات القضائية المحلية:** هل يسمح النموذج بتخزين معلومات التسجيل في اختصاص واحد أو عدة اختصاصات قضائية؟ إلى أي مدى يمكن للمسجلين أو أمناء السجلات/جهات التوثيق اختيار تخزين معلومات التسجيل في اختصاص قضائي مع قوانين حماية البيانات التي تكون متوافقة مع الاختصاص القضائي المحلي للمسجل؟
- **يمكن من عرض تطبيق القوانين المحلية:** هل يسمح النموذج بالوصول إلى معلومات التسجيل بطريقة متوافقة مع عدة اختصاصات قضائية؟ إلى أي مدى يمكن لنظام RDS تطبيق قوانين حماية البيانات في الاختصاص القضائي أو منطقة المسجل على معلومات التسجيل التي يتم الوصول إليها من خلال نظام RDS؟
- **يتيح التوافق مع القوانين المحلية لحماية البيانات:** هل يساعد النموذج أو يعوق امتثال أمناء السجلات والسجلات لقوانين حماية البيانات المحلية التي تسري عليهم؟ ما مدى الصعوبة التي يفرضها النموذج في الحصول على الإعفاءات اللازمة لتمكين الامتثال؟ كيف يمكن ضمان الالتزام بالإجراءات القانونية اللازمة من خلال القانون المحلي للمسجل؟

### الاعتماد

- **يمكّن اعتماد مقدم الطلب:** هل يسمح النموذج للمستخدمين الراغبين في الوصول المدفوع بالأغراض إلى البيانات المحددة ببوابة تقديم طلبات للحصول على الاعتماد، أو الفحص أو تلقي أوراق اعتماد الوصول، واستخدامها من أجل الحصول على الوصول المرخص إلى البيانات؟ إلى أي مدى يساعد هذا النموذج أو يعيق التطبيق الموحد والقوي لعملية اعتماد مقدم الطلب تلك؟

  **التوثيق:** هل يجعل منه أمرًا أكثر سهولة؟ هل يجعل منه أمرًا أقل كلفة؟ هل يعجل أي نظام من أوراق الاعتماد الآمنة أسهل أو أرخص؟

- **تعقب/تجريم مقدمي الطلبات:** إلى أي مدى من الكفاءة والمصداقية يمكن للنموذج تسجيل طلبات الوصول إلى البيانات والردود لأغراض التعرف على إساءة استخدام الوصول المعتمد (أي الإجراءات التي تخالف أحكام وشروط الوصول)؟ إلى أي مدى يساعد النموذج أو يعيق إجراءات إنفاذ الامتثال (على سبيل المثال العقوبات المطبقة على المستخدمين غير المتوافقين من أجل إعادة إساءة الاستخدام في المستقبل)؟

- **التدقيق:** هل يمكن النموذج من تدقيق طلبات الوصول إلى البيانات والردود والعمليات ذات الصلة، من أجل تقييم كفاءة عملية الاعتماد والوصول المرخص للبيانات؟

### التشغيل

- **بوابة سهلة الاستخدام:** هل يسمح النموذج بالتقديم سهل الاستخدام لمعلومات التسجيل المعروضة من خلال بوابة ويب أو المقدمة ردًا على استعلامات البروتوكولات؟ إلى أي مدى يدعم النموذج مبادئ التدويل والعولمة (على سبيل المثال، دعم مجموعات الحروف المحلية، وترجمة الردود)؟ إلى أي مدى يعمل النموذج على تسهيل العرض المتسق عبر كافة نطاقات gTLD؟

- **عمليات التدقيق العشوائية للبيانات/تقارير الدقة:** هل يدعم النموذج عمليات التدقيق الدورية للدقة بالإضافة إلى الإبلاغ عن الدقة عبر كافة نطاقات gTLD؟ إلى أي مدى يعمل النموذج على تسهيل التعرف الكفء والمتسق والتحديث لمعلومات التسجيل غير الدقيقة والإنفاذ الموحد لسياسات الدقة؟

- **تأخر البيانات (الأداء):** هل يحتوي النموذج على صعوبات في التعامل مع البيانات التي من المحتمل أن تخل بمستوى الأداء ولا يمكن التعامل معها من خلال تنفيذ منصة قابل للتوسع؟ ما هو الحجم النسبي لأوجه القصور تلك (مقارنة بالنماذج الأخرى) لتحقيق سرعة التعامل مع الطلبات والتأخيرات الوارد من المستخدمين الذين يستعلمون عن معلومات التسجيل؟

- **مزامنة البيانات:** هل يتطلب النموذج مزامنة البيانات المنسوخة من أي نظام مع النظام الأخرى؟ ما مدى توسع هذه الاحتياجات الخاصة بمزامنة البيانات وما مدى الصعوبة التي يكون عليها أي نقص مؤقت في المزامنة (مقارنة بالنماذج الأخرى)؟

- **وصول المسجل إلى البيانات الخاصة به:** هل يدعم النموذج أو يمنع وصول المسجل إلى بيانات التسجيل الخاصة به/بها؟

- **متطلبات التخزين والمستودعات:** هل يقدم النموذج مناطق متعددة للتخزين تعمل على زيادة عدد أو تعقيد تخزين البيانات ومتطلبات المستودع؟

- **يمكّن تدابير الاعتماد المسبق:** هل يدعم النموذج التوثيق المسبق لمعلومات المسجل وجهات الاتصال المستندة إلى الأغراض عبر كافة نطاقات gTLD؟ إلى أي مدى يعمل النموذج على تسهيل إنشاء والحفاظ بكفاءة واتساق على معلومات الاتصال الموثقة من قبل والإنفاذ الموحد لأي من سياسات التفرد ذات الصلة؟

### التنفيذ

- **البنية التحتية المعقدة:** هل النموذج أقل تعقيدًا على الإطلاق، مقارنة بالنماذج الأخرى؟ على سبيل المثال، النموذج الأكثر تعقيدًا (الأضعف) قد يحتوي على العديد من الأنظمة والواجهات التي تتطلب استثمارًا أوليًا وصيانة مستمرة.
- **سهولة التنفيذ:** هل من المحتمل أن يكون النموذج أسهل في التنفيذ، مقارنة بالنماذج الأخرى؟ على سبيل المثال، النموذج الأكثر صعوبة (الأضعف) قد يتطلب تغييرات بالنسبة لنظم أكثر.
- **سهولة الانتقال:** هل يعمل النموذج على تسهيل الانتقال السلس من نظام WHOIS الحالي إلى نظام RDS من الجيل التالي، مقارنة بالنماذج الأخرى؟ فهنا النموذج الأضعف هو الذي يجعل من الصعب على المستخدمين وأمناء السجلات والسجلات الانتقال من العمليات الحالية.

### التكلفة

- **تقليل تكاليف تشغيل WHOIS لكل من أمين السجل والسجل:** هل من المحتمل أن يؤدي النموذج إلى تخفيض في تكاليف التشغيل والصيانة المستمرة بالنسبة لأمناء السجلات والسجلات، مقارنة بنظام WHOIS الحالي؟ وهنا، فإن أي نموذج يعمل على تقليل التكلفة هو الأقوى.
- **خفض تكلفة التنفيذ:** هل يتطلب النموذج استثمار أولي أعلى أم أقل على الإجمال في البنية التحية الجديدة/المعدلة وعملياتها، مقارنة بالنماذج الأخرى؟ هنا، يعتبر النموذج ذي تكاليف التنفيذ الإجمالية الأقل هو الأقوى.
- **الاستعلام العكسي وWhoWas التاريخية:** هل يتطلب النموذج استثمارًا إضافية من أجل استيعاب الاستعلام العكسي وأبحاث WhoWas التاريخية من خلال مقدمي الطلبات المعتمدين؟ في هذا المثال، فإن النموذج الذي يطالب بتكلفة إجمالية أقل لتحقيق هذه الخدمات يعتبر هو الأقوى.

### حالات الاستخدام

مقارنة قدرة هذه النماذج المحتملة على دعم سائر المستخدمين والأغراض المحددة في التقرير الأولى، بما في ذلك (على سبيل المثال لا الحصر) حالات استخدام gTLD التالية:

- الاستحواذ على أسماء النطاقات
- سجل تسجيل أسماء النطاقات (بما في ذلك تعقب تاريخ التسجيل لأي من أسماء النطاقات (WhoWas))
- أسماء النطاقات لمسجل محدد (ويشمل ذلك العثور على كل اسم نطاق مسجل حسب المسجل المحدد (استعلام RDS العكسي))
- إجراءات UDRP
- التحري عن إساءة استخدام أسماء النطاقات
- اكتشاف أنشطة الإنترنت الضارة

### تحليل تكلفة النموذج

للتعرف على جدوى التنفيذ والتكاليف المرتبطة بنموذج SRDS وFRDS، أسندت ICANN إلى IBM مهمة وضع تحليل تفصيلي يرتكز على فروق التكلفة بين هذه النماذج المحتملة للتنفيذ. وقدمت IBM تقريرًا نهائيًا تحت اسم "تحليل تكلفة نموذج تنفيذ خدمة دليل التسجيل (RDS)[40]". مقتطف من نتائج شركة IBM، مأخوذ من التقرير الخاص بهم، وتم نسخه وإيراده هنا للرجوع إليه.

[40] https://community.icann.org/display/WG/EWG+Public+Research+Page

**المنهج**

خلال فبراير/مارس 2014، تم إجراء تحليل تكلفة للميزانية، لمقارنة تحقيق تنفيذ النموذج المتزامن[41] والموحد لـ RDS. وتم استخدم أسلوب مرحلي:

- الخطوة 1: جمع المتطلبات الأساسية لكل نموذج من نماذج التنفيذ.
- الخطوة 2: تعريف والموافقة على الافتراضات الكمية التي تقدمها ICANN والمستندة بشكل كبير إلى تقارير استعلام WHOIS الشهرية التي تقدمها سجلات gTLD. كما أن استخدام هذه الافتراضات في الحصول على حمولة العمل للنظام المتوقع وتعريف حول أساسي رفيع المستوى يضع الأساس لكلا نموذجي التنفيذ.
- الخطوة 3: إنشاء نموذج تكلفة وأداء تحديد تكلفة الميزانيات لكل من هذه المخططات الأساسية للحلول.
- الخطوة 4: صياغة النتائج.

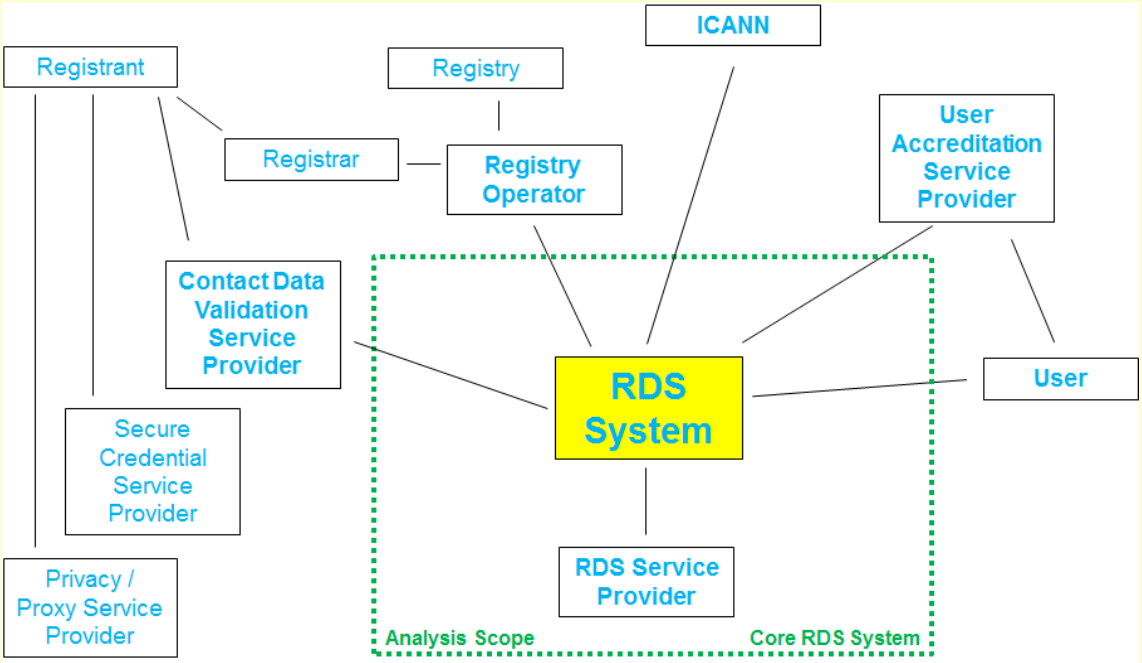
**نقاط البدء في المشاركة**

- إنشاء تقييم تكلفة للميزانية بالنسبة لموفر الخدمة/نظام RDS". تكاليف مشغل السجل غير مقدرة.
- تم إنشاء نموذج وتقييم لتكلفة الخدمات المدارة. أي، تحمل الإعداد والعمليات المستمرة لخدمة RDS مدارة وتقدير التكاليف ذات الصلة.
- ولأغراض مقارنة التكاليف، يستند كل من الحل والتكاليف بشكل كبير إلى محفظة IBM (لاسيما اكتتاب SoftLayer IaasS من IBM)، وذلك من خلال استخدام مكونات حلول من جهات أخرى فقط في حالة عدم وجود بديل في محفظة IBM.
- وتتم عمليات تقدير التكاليف للمطلب الأساسي/مخطط الحل فقط، وليس للمتغيرات، ولا يتم إجراء تحليل محرك تكلفة تفصيلي.

[41] للتوازي مع التقرير النهائي لـ EWG، يشير هذا الملخص إلى نظام RDS المتزامن (SRDS)، النموذج المشار إليه في تقارير EWG السابقة بلفظ RDS المجمعة (ARDS).

**نطاق ومقاييس تحليل التكلفة**

كان تركيز تحليل التكلفة منصبًا على "نظام RDS الأساسي" وفقًا لم هو موضح أدناه




.

حالات الاستخدام الأصلية من أجل الدعم في كل من النماذج (المتزامنة والموحدة) متى ما تم تحديدها.

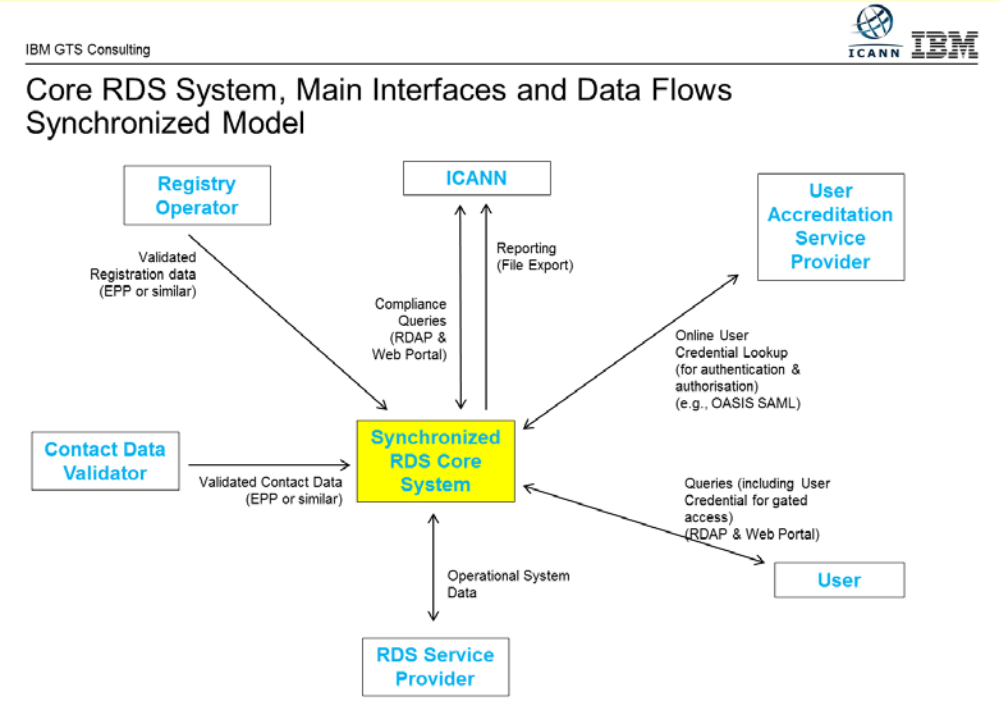
بالإضافة إلى ذلك، تم تعريف الافتراضات الكمية الأساسية:

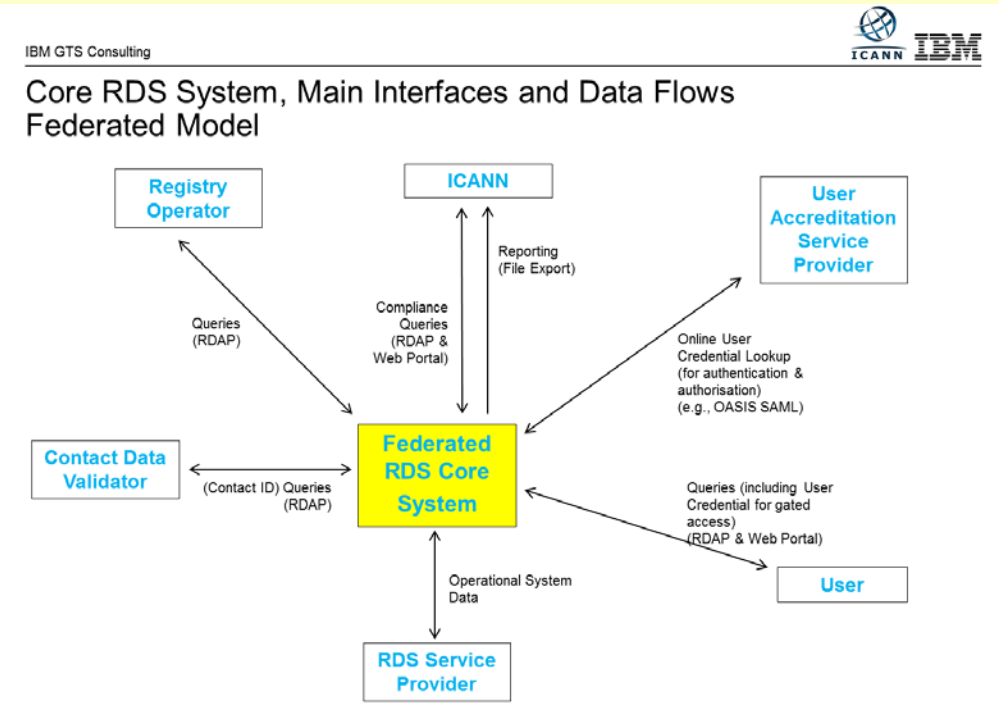
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| YEARLY GROWTH RATE | 22% | nr of DN records added in a year, assumed to include the growth in the nr of gTLDs | | | | | |
| Nr of DN RECORDS, YEARLY UPDATE RATE | 100% | nr of DN records updated in a year | | | | | |
| | | start yr1 (2015) | start yr2 (2016) | start yr3 (2017) | start yr4 (2018) | start yr5 (2019) | end yr 5 (2020) |
| Nr of gTLDs | | 2000 | 3000 | 4000 | 5000 | 6000 | 7000 |
| growth rate | | | 50% | 33% | 25% | 20% | 17% |
| | December 2013, ICANN input | start yr1 (2015) | start yr2 (2016) | start yr3 (2017) | start yr4 (2018) | start yr5 (2019) | end yr 5 (2020) |
| NR OF DOMAIN NAMES | 151.196.101 | 184.459.243 | 225.040.277 | 274.549.138 | 334.949.948 | 408.638.936 | 498.539.502 |
| NR OF QUERIES/MONTH | 9.031.522.529 | 11.018.457.485 | 13.442.518.132 | 16.399.872.121 | 20.007.843.988 | 24.409.569.665 | 29.779.674.992 |
| AVERAGE NR OF QUERIES/SEC | 3.484 | 4.251 | 5.186 | 6.327 | 7.719 | 9.417 | 11.489 |
| NR OF QUERIES/PEAK SEC | | 42.509 | 51.862 | 63.271 | 77.191 | 94.173 | 114.891 |
| AVERAGE NR OF QUERIES/HOUR | 12.543.781 | 15.303.413 | 18.670.164 | 22.777.600 | 27.788.672 | 33.902.180 | 41.360.660 |
| NR OF QUERIES IN PEAK HOUR | 25.087.563 | 30.606.826 | 37.340.328 | 45.555.200 | 55.577.344 | 67.804.360 | 82.721.319 |
| USER VISITS IN PEAK HOUR | 16.892.292 | 20.608.596 | 25.142.488 | 30.673.835 | 37.422.079 | 45.654.936 | 55.699.022 |
| CONCURRENT VISITS IN PEAK HOUR | 563.076 | 686.953 | 838.083 | 1.022.461 | 1.247.403 | 1.521.831 | 1.856.634 |
| NEW VISITS IN PEAK SEC | | 28.623 | 34.920 | 42.603 | 51.975 | 63.410 | 77.360 |

| | |
|---|---|
| % of reverse queries | 1,0% |

## نماذج تنفيذ RDS

تم اشتقاق نماذج التنفيذ التالية من التقارير الأولية وتقارير تحديد الحالة لـ EWG لأغراض تحليل التكلفة:



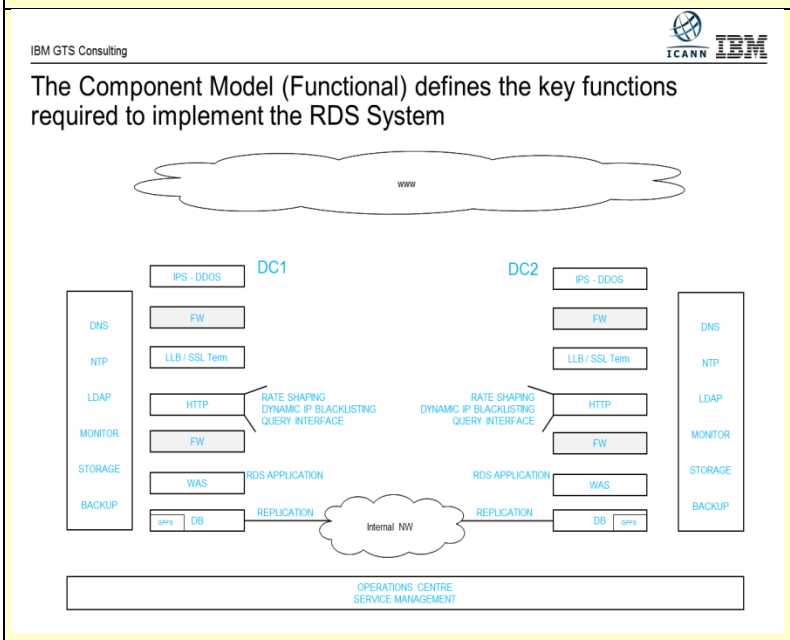



## مكونات RDS الوظيفية

تم إنشاء نموذج المكونات التالية لأغراض تحليل التكلفة، والذي يضم كافة الوظائف الأساسية اللازمة لتنفيذ نظام RDS. تم استخدام افتراضات أفضل الممارسات للنظم القياسية عند تحديد تكلفة كل من نظام SRDS وFRDS، مثل تكرار نظام RDS الأساسي وقاعدة البيانات عبر مركزي بيانات متنوعين على جغرافيًا، مع موازنة الحمولة والتحويل وضمان الوفرة والتوافر، وIPS لتحريف DDoS. ويجب أن يفهم أن هذه المكونات الوظيفية تسري على كلا نموذجي التنفيذ.

**المكونات الوظيفية:**

- موازنة/توجيه حمولة Inter-DC
- تخفيف IPS DDoS
- موازنة وSSL لحمولة Inter-DC
- خادم (HTTP) للويب
- خادم تطبيق الويب (WAS)
- عقدة مدير WAS
- نظام تخزين قواعد البيانات (DB)
- نظام عضو DB
- خادم تخزين
- مراقبة النظم
- DNS
- NTP
- LDSP
- مخزن Syslog
- خادم نسخ احتياطي
- خادم تخزين احتياطي
- نظام وكيل نسخ DB
- تحديد نطاقات الشبكة، جدار الحماية/IPS
- الإنترنت واتصال DC




على سبيل المثال، تم تولي إعداد مكون من مركز بيانات ثنائي لنظام RDS الأساس في كل من نموذج SRDS وFRDS، من خلال استخدام تصميم نشط-نشط حيث تكون لكل نظام RDS أساسي القدرة على التعامل مع 50% من الحمولة القصوى. ولم يشتمل هذا التحليل الخاص بالتكلفة على تجميع التوافر العالي داخل كل مركز بيانات؛ بل يمكن إضافة ذلك بدون تغيير التكاليف النسبية لكلا نموذجي RDS.

### تقديرات التكاليف (التي تتولي 1% من الاستعلامات العكسية)

التكلفة الملخصة أدناه لا تمثل بأي حال من الأحوال مقترح تنفيذ IBM. وقد تم إنشاء التكلفة من أجل الغرض الوحيد والأوحد المقرر استخدامه والنظر فيها كجزء من تحليل تكاليف الميزانية في مقارنة كلا نموذجي تنفيذ RDS. استنادًا إلى التعقيبات الكمية الأساسية، فإن متطلبات حمولة العمل ومخطط الحل المحدد أعلاه، فقد تم تقدير التكلفة لكل اسم نطاق لكل عام بالنسبة **لنظامي FRDS وSRDS الأساسيين فقط** على النحو التالي:

تقدير تكلفة ميزانية SRDS

| | | | | | |
|---|---|---|---|---|---|
| € 0,0183 | average cost/domain/year | | | | |
| cost per domain name | | | | | |
| yr1 | yr2 | yr3 | yr4 | yr5 | |
| € 0,041 | € 0,023 | € 0,017 | € 0,020 | € 0,019 | |

تقدير تكلفة ميزانية FRDS

| | | | | | |
|---|---|---|---|---|---|
| € 0,0173 | average cost/domain/year | | | | |
| cost per domain name | | | | | |
| yr1 | yr2 | yr3 | yr4 | yr5 | |
| € 0,041 | € 0,018 | € 0,017 | € 0,021 | € 0,017 | |

تم تحليل الفروق في التكلفة لأبعد من ذلك مقارنتها على النحو التالي:

## FRDS – SRDS Budgetary Cost Estimate Differences

| | | | | | |
|---|---|---|---|---|---|
| **SETUP COSTS** | | **5,9%** | | 10,5% | |
| **INFRASTRUCTURE SETUP COSTS** | ARCHITECTURE & DESIGN | **1,5%** | 0,2% | 15,6% | 0,0% |
| | PROVISION & CONFIGURE | | 1,2% | | 19,2% |
| | INFRASTRUCTURE TESTING | | 0,1% | | 18,4% |
| **APPLICATION SETUP COSTS** | ANALYSIS, DESIGN, CODE, UNIT TEST | **1,2%** | 1,2% | 0,0% | 0,0% |
| **TESTING** | INTEGRATION TESTING & DEPLOYMENT | **1,7%** | 0,8% | 7,8% | 0,0% |
| | E2E SYSTEM TESTING | | 0,2% | | 38,2% |
| | PERFORMANCE | | 0,2% | | 33,3% |
| | SECURITY (ETHICAL HACK) | | 0,5% | | 0,0% |
| **TRANSITION TO BAU** | TRANSITION TO BAU | **0,6%** | 0,5% | 26,6% | 37,7% |
| | SERVICE DESK SETUP | | 0,1% | | 0,0% |
| **MANAGEMENT** | PROJECT MANAGEMENT | **0,9%** | 0,9% | 13,4% | 13,4% |

The FRDS model implies a higher computing power requirement (more systems required to handle the envisaged load) in the web and web application server layer.

Due to a higher amount of systems to interface with in an on-line manner when handling queries, the FRDS model is estimated to involve more testing effort

## FRDS – SRDS Budgetary Cost Estimate Differences

| COST MODEL FRDS | | SHARE IN TOTAL | | DIFFERENCE WITH ARDS | |
|---|---|---|---|---|---|
| | | 100,0% | | -5,4% | |
| **RUN COSTS** | | 94,1% | | -6,3% | |
| **INFRASTRUCTURE COSTS** | PUBLIC NW | **30,5%** | 8,1% | -22,4% | -55,9% |
| | DC NW, GLB, LLB, IPS/DDOS | | 5,7% | | 10,7% |
| | HTTP SERVERS | | 2,2% | | 236,0% |
| | WAS SERVERS | | 3,7% | | 218,5% |
| | DB SERVERS | | 2,2% | | -52,0% |
| | STORAGE | | 6,3% | | -3,8% |
| | BACKUP | | 1,9% | | -19,0% |
| | GENERIC SYSTEMS | | 0,3% | | 0,0% |
| **SW LICENCE & MAINTENANCE COSTS** | DB | **32,7%** | 13,7% | -17,5% | -59,5% |
| | WAS | | 18,8% | | 234,6% |
| | BACKUP | | 0,3% | | 0,0% |
| **OPERATIONS AND MANAGEMENT COSTS** | INFRA OPERATIONS & MAINTENANCE | **30,9%** | 19,4% | 44,0% | 63,6% |
| | APPLICATION OPERATIONS | | 2,6% | | 20,0% |
| | APPLICATION MAINTENANCE | | 1,3% | | 27,3% |
| | SERVICE GOVERNANCE | | 5,2% | | 0,0% |
| | SERVICE DESK | | 2,4% | | 100,0% |

The Public NW cost is lower in the FRDS case due to the IBM SoftLayer NW charging model: incoming traffic is free; per server 20 TB/month outgoing traffic is free, i.e. you get a total free outgoing volume of #servers x 20 TB per month. As the number of servers increases in the FRDS model, the total amount of free TB outgoing NW volume/month increases.

The FDRS model implies a higher NW throughput requirement. Impact on Firewall and Intrusion Prevention Component.

The FRDS model implies a higher computing power requirement in the web and web application server layer.

The FRDS model implies less storage and backup storage capacity as less data is stored centrally.

The DB compute requirement is estimated to be higher in the SRDS model.

Due to a higher amount of systems to interface with in an on-line manner when handling queries, the FRDS model is estimated to involve a higher application operations, support & maintenance release testing workload

**النتائج الرئيسية**

ومن خلال الافتراضات المستخدمة، فإن نظام RDS الأصلي أكثر كلفة إلى حد ما في نموذج RDS الموحد (FRDS) عنه في نموذج RDS المتزامن (SRDS).

نموذج FRDS حساس للغاية بالنسبة للتنوعات في حمولة الاستعلام العكسي. مع مقدار أعلى من الاستعلامات العكسية، يصبح نموذج FRDS أكثر كلفة إلى حد كبير: مع حمولة بنسبة 3% من الاستعلامات العكسية بدلاً من حمولة 1% من الاستعلامات العكسية، يتم تقدير تكلفة نموذج FRDS لتزيد لما يقرب من 35%. وهذا من العوامل الهامة في عدم اليقين والخطر المرتبط بنموذج FRDS. حيث يعتقد على العكس من نموذج SRDS أنه أقل حساسية بالنسبة لكمية الاستعلامات العكسية.

ومن المتوقع أن يتطلب نموذج FDRS عمليات تطبيق أعلى، ودعم وصيانة وجهود اختبار أعلى مع توقع مزيد من التفاعلات مع مشغلي السجلات.

بالإضافة إلى ذلك، لنموذج FRDS تأثير أكبر على مشغلي السجلات. وفي نموذج FRDS، سوف يتعين على كل مشغل سجل تنفيذ الدعم - بموجب اتفاقية SLA - للاستعلامات على الإنترنت، بما في ذلك الاستعلامات العكسية والاستعلامات التاريخية (المعروفة أيضًا باسم WhoWas). وبالنسبة للاستعلامات الأخيرة، يجب الاحتفاظ بالبيانات التاريخية من خلال مشغلي السجلات.

## الملحق ز :قدرة بروتوكول EPP و RDAPعلى دعمRDS

| عنصر البيانات | دعم EPP للتجميع | دعم EPP للوصول |
|---|---|---|
| اسم النطاق | نعم | نعم |
| حالة التسجيل | نعم | نعم |
| خوادم DNS | نعم | نعم |
| تفويض DNSSEC | نعم | نعم |
| حالة العميل | نعم | نعم |
| حالة الخادم | نعم | نعم |
| أمين السجل | نعم | نعم |
| الموزع | نعم | نعم |
| الدائرة القضائية لأمين السجل | لا | لا |
| الدائرة القضائية للسجل | لا | لا |
| لغة اتفاقية التسجيل | لا | نعم |
| تاريخ الإنشاء | نعم | نعم |
| تاريخ التسجيل الأصلي | نعم | نعم |
| تاريخ انتهاء أمين السجل | نعم | نعم |
| نوع المسجل | لا | نعم* |
| اسم PBC | نعم | نعم |
| معرّف PBC | نعم | نعم |
| حالة توثيق PBC | لا | لا |
| آخر توقيت زمني موثق لجهة PBC | لا | لا |
| منظمة PBC | نعم | نعم |
| عنوان سكن PBC | نعم | نعم |
| مدينة PBC | نعم | نعم |
| ولاية/مقاطعة PBC | نعم | نعم |
| الرمز البريدي لـ PBC: | نعم | نعم |
| دولة PBC | نعم | نعم |
| عنوان البريد الإلكتروني لـ PBC | نعم | نعم |
| عنوان البريد الإلكتروني البديل لـ PBC | لا | نعم |
| هاتف + تحويلة PBC | نعم | نعم |
| هاتف + تحويلة PBC البديلة | لا | نعم |
| فاكس + تحويلة PBC | نعم | نعم |
| الرسائل النصية لـ PBC | لا | نعم |
| الرسائل الفورية IM لـ PBC | لا | نعم |
| وسائل التواصل الاجتماعي لـ PBC، الوسائط الاجتماعية البديلة | لا | نعم |
| جهة اتصال PBC وعنوان URL لإساءة الاستخدام | لا | نعم |
| تاريخ التحديث | نعم | نعم |
| اسم المسجل | نعم | نعم |
| معرف جهة اتصال المسجل | نعم | نعم |
| حالة توثيق جهة اتصال المسجل | لا | لا |

| عنصر البيانات | دعم EPP للتجميع | دعم EPP للوصول |
|---|---|---|
| آخر توقيت زمني موثق لجهة اتصال المسجل | لا | لا |
| منظمة المسجل | نعم | نعم |
| معرف شركة المسجل | نعم | نعم |
| عنوان سكن المسجل | نعم | نعم |
| مدينة المسجل | نعم | نعم |
| ولاية/مقاطعة المسجل | نعم | نعم |
| الرمز البريدي للمسجل | نعم | نعم |
| الدولة المسجل | نعم | نعم |
| هاتف + تحويلة المسجل | نعم | نعم |
| فاكس + تحويلة المسجل | نعم | نعم |
| البريد الإلكتروني للمسجل، عنوان البريد الإلكتروني البديل | نعم | نعم |
| الرسائل النصية SMS للمسجل | لا | نعم |
| الرسائل الفورية IM للمسجل | لا | نعم |
| وسائل التواصل الاجتماعي للمسجل، الوسائط الاجتماعية البديلة | لا | نعم |
| جهة اتصال المسجل وعنوان URL لإساءة الاستخدام | لا | نعم |
| عنوان URL لأمين السجل | لا | نعم |
| رقم IANA لأمين السجل | لا | نعم* |
| عنوان البريد الإلكتروني لجهة اتصال إساءة الاستخدام لدى أمين السجل | لا | نعم |
| رقم هاتف جهة اتصال إساءة الاستخدام لدى أمين السجل | لا | نعم |
| عنوان URL لموقع شكاوى مركز معلومات شبكة الإنترنت Internic | لا | نعم |

*عناصر البيانات هذه غير محددة بوضوح في RDAP. ويمكن الحصول عليها من خلال استخدام حقول "العلامات" أو تمديد بروتوكول.

تمديدات و/أو إضافات البروتوكولات

**الدائرة القضائية لأمين السجل والسجل**: يجب إضافتها إلى EPP أو استمدادها من معلومات موقع أمين السجل الحالي. يمكن الحصول عليها من خلال استخدام "علامات" كيان RDAP أو من خلال تمديد بروتوكول.

**لغة اتفاقية التسجيل:** يجب إضافتها إلى EPP عن طريق تمديد بروتوكول.

**نوع المسجل:** يجب إضافتها إلى EPP عن طريق تمديد بروتوكول.

**حالة توثيق المسجل/PBC، الموعد الزمني لآخر توثيق، عنوان البريد الإلكتروني البديل + التحويلة، SMS، وIM، والوسائط الاجتماعية، والوسائط الاجتماعية البديلة، وعنوان URL للاتصال وعنوان URL لإساءة الاستخدام:** يجب إضافتها إلى EPP عن طريق تمديد بروتوكول. ويمكن لـ RDAP التعامل مع معرفات الوسائط الاجتماعية، لكن يجب وضع مواصفة من أجل تحديد التنسيق الخاص بكل المعرفات.

**نوع الاتصال:** الأنواع المتاحة في الوقت الحالي هي "المشرف" و"الفواتير" و"الفني". أما أنواع الاتصال الإضافية فتقتضي امتدادًا إلى RDAP.

**الغرض المحدد في استعلام RDAP:** يجب إضافتها إلى RDAP عن طريق تمديد بروتوكول.

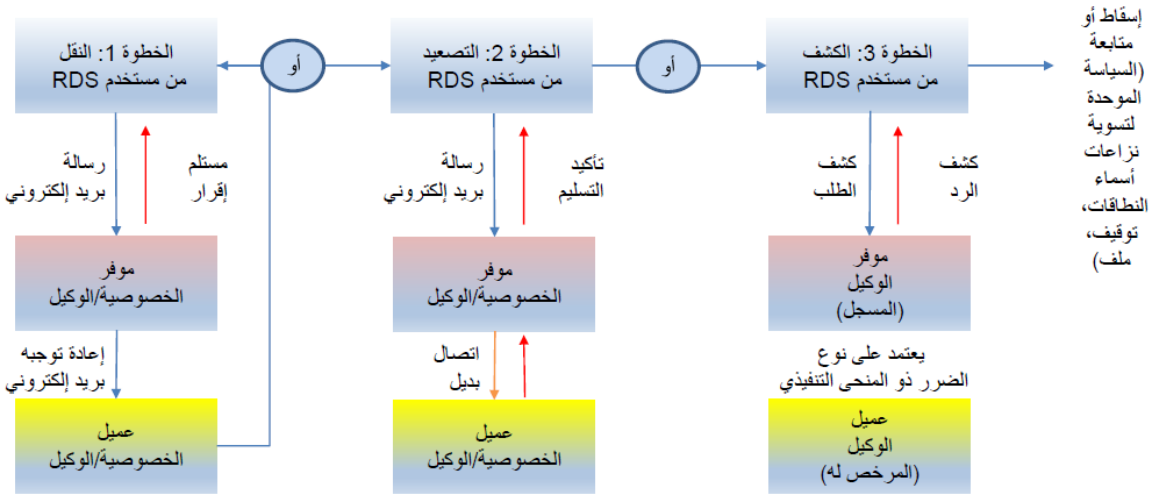
**مستوى الوصول في EPP:** يشمل EPP آلية بسيطة في جمع وتمرير تفضيلات الإفصاح عن عناصر اتصال المسجل من أمين السجل والسجل، حيث يمكن الاستفادة منها في سلوك رد RDAP. وعلى الرغم من ذلك، فإن هذه الآلية غير مقسمة بما يكفي للتعرف التفضيلات في مستوى كل عنصر من البيانات الفردية. ومن ثم يجب توفير امتداد EPP و/أو مخطط للاتصال من أجل الإشارة إلى اختيار المسجل أو جهة الاتصال لإلغاء تفاصيل الإفصاح لكل عنصر بيانات (على سبيل المثال، اختيار نشر عنصر محدد ببوابات بشكل افتراضي).

## الملحق ح: نموذج ومبادئ للترحيل والكشف

وفقًا لما هو موضح في القسم السادس (ب)، توصي مجموعة EWG بمطالبة خدمات الخصوصية والبروكسي المعتمدة من ترحيل كل البريد الإلكتروني من خلال إعادة توجيه عنوان البريد الإلكتروني. والهدف هو تزويد عملاء الخصوصية/البروكسي المعتمدين ومستخدمي RDS ممن قد يرغبون في الاتصال بهم بمسار اتصالات قياسي ومتوفر دائمًا وفي الوقت الفعلي تقريبًا.

بالإضافة إلى ذلك، توصي مجموعة EWG بمطالبة خدمات البروكسي المعتمدة بالرد للكشف عن الطلبات في الوقت المناسب (فيما يلي مزيد من التفاصيل). والهدف هو تزويد المستخدمين الذين يعانون من مشكلات خطيرة في النطاقات المسجلة من خلال البروكسي بعملية قياسية ذات كفاءة ومتوفرة دائمًا لتحقيق حل فعال للمشكلات.

وعند تحليل هذه الاحتياجات الخاصة بالمستخدمين، أوضحت مجموعة EWG نقصًا آخر في الممارسات الحالية: غياب طريقة تصعيد متوفرة دائمًا وفعالة عند فشل الاتصال. ويقفز العديد من المستخدمين سريعًا إلى الكشف لأنه ليست أمامهم مسارات أخرى. وتوصي مجموعة EWG بتقديم عملية تصعيد قد تكون أقل كلفة بالنسبة لجميع الأطراف وتقلل عدد المشكلات التي قد تؤدي إلى طلبات كشف أكثر كلفة واستهلاكاً للوقت. وهذه العملية ذات الخطوات الثلاثة موضحة أدناه:




### الخطوة 1: الترحيل

أ) يطلب مستخدم RDS بيانات الاتصال لنطاق، لاستعادة:

- معرف اتصال المسجل (أي عميل الخصوصية أو معرف اتصال موفر الخصوصية)
- معرفات جهات الاتصال لسائر جهات الاتصال المستندة إلى الأغراض (PBC) وعناوين PBC المنشورة (بما في ذلك عناوين البريد الإلكتروني)
- إشارة إلى أن تسجيل النطاق قد تم من خلال خدمة الخصوصية/البروكسي
- اسم وعنوان موفر خدمة البروكسي أو الخصوصية، يتم توفيره جهة اتصال PBC لموفر خدمة الخصوصية/البروكسي، والتي تشمل عناوين URL لنماذج تصعيد الترحيل والكشف.

ب) مستخدم RDS، بالإشارة إلى أن هذا عبارة عن تسجيل معتمدة للخصوصية/البروكسي، ومحاولة مراسلة عملية الخصوصية/البروكسي بالبريد الإلكتروني على عنوان التوجيه. قد يسمح الموفرون اختياريًا للعملاء توفير مزيد من عناوين التوجيه (على سبيل المثال الهاتف أو SMS أو البريد العادي).

ج) يجب مطالبة موفر الخصوصية/البروكسي المعتمد بتوجيه والاعتراف باستلام رسالة مرحلة (على سبيل المثال؛ إقرار البريد الإلكتروني لكافة الرسائل الواردة لعنوان البريد الإلكتروني الخاص بالتوجيه). قد يتم إعادة إقرار سالب لحالات الخطأ (على سبيل المثال؛ عدم وجود صندوق الوارد)؛ واعترافات إلى نفس المرسل قد تكون مقتصرة على عتبة من أجل عرقلة إساءة استخدام الترحيل.

د) مستخدم RDS الذي يتلقى الإقرار لديه الآن تأكيد بأن الرسائل تم ترحيلها إلى عميل الخصوصية/البروكسي. وعلى الرغم من ذلك، يجوز للعميل اختيار عدم الرد أو يجوز له إهمال الرسائل المرحلة دون قراءتها (على سبيل المثال المعاملة كرسائل غير مرغوبة).

### الخطوة 2: التصعيد

يمل مستخدم RDS من الانتظار من أجل عميل الخصوصية/البروكسي المعتمد للرد واتخاذ قرار بتصعيد اتصال المحاولة السابقة من خلال:

أ) زيارة موقع الويب الخاص بخدمة الخصوصية أو البروكسي المعتمدة والمحددة في الخطوة 1 وتعبئة نموذج تصعيد تحتوي على:

- هوية مستخدم RDS (إعادة الاستخدام المتحملة لأوراق اعتماد استعلام RDS)
- سبب مستخدم RDS للاتصال (قد يكون قائمة منسدلة من الأسباب المحددة)
- اسم النطاق المسجل بالخصوصية/البروكسي
- رسالة محملة يتم ترحيلها إلى العميل (ربما تكون مشفرة؟)
- الطابع الزمني للمرة الأولى التي تمت فيها محاولة الترحيل

ب) يجب مطالبة موفر الخصوصية/البروكسي المعتمد بمحاولة الاتصال بالعميل مباشرة، ربما من خلال استخدام معلومات الاتصال و/أو الطرق غير القابلة للوصول إلى مستخدم RDS، وإعادة "تأكيد تسليم" في غضون عدد *[42] يوم. وهنا مرة أخرى، تتم إعادة تأكيدات سالبة لحالات الخطأ (على سبيل المثال، المستخدم غير المرخص، أو انتهاء المهلة) وعمليات التقديم يمكن تسجيلها وتقييدها بعتبة من أجل الحد من إساءة الاستخدام.

ج) مستخدم RDS الذي يتلقى المعلومات الآن قام بتوثيق دليل بأن الرسالة تم إيصالها إلى عميل الخصوصية/البروكسي. ولا يزال بإمكان العميل اختيار عدم الرد، إلا أن التصعيد يجب أن يساعد في التغلب على حالات فشل الاتصال الأساسي دون الحاجة إلى كشف.

[42] * قد يعتمد انتهاء المهلة على الهوية الموثقة والسبب المحدد للاتصال. على سبيل المثال، 1 يوم لإنفاذ القانون/OpSec للتحري عن الجرائم/إساءة الاستخدام؛ 7 أيام لتحري مالكي العلامات التجارية عن انتهاكات العلامات التجارية، و7 أيام لعملاء الإنترنت الذين يحاولون الوصول إلى التجار عبر الإنترنت.

### الخطوة 3: الكشف (يسري فقط على النطاقات المسجلة من خلال بروكسي)

تنتهي مهلة مستخدم RDS في الانتظار من أجل عميل البروكسي المعتمد (المرخص له) للرد واتخاذ قرار بأن المشكلة كبيرة بما يكفي لإقامة إجراءات جنائية أو مدنية من خلال:

أ) زيارة موقع الويب أو الاتصال أو مراسلة موفر خدمة البروكسي المعتمد والمحددة في الخطوة 1 وتقديم طلب كشف يحتوي على:

- هوية مستخدم RDS

سبب مستخدم RDS للاتصال (مقتصرة بشكل ضيق على الأضرار الإجرائية)

- اسم النطاق المسجل من خلال موفر البروكسي
- توثيق الضرر (معلومات تسجيل العلامات التجارية، وادعاءات إساءة الاستخدام)
- الطابع الزمني لوقت محاولة الترحيل/التصعيد (رقم الحالة من التصعيد؟)

ب) يجب مطالبة موفر البروكسي المعتمد التحري واتخاذ إجراءات مناسبة (راجع د)، لتقدم "رد كشف" في غضون عدد *[43] يوم. يمكن تسجيل وتقييم طلبات الكشف على الأضرار الإجرائية المدعاة من خلال مستخدمي RDS بموقف،[44] للحد من إساءة الاستخدام.

ج) يمكن لموفر البروكسي المعتمد، بالنظر إلى الوثائق التي يمكن من خلالها تقييم الحالة، القيام بما يلي:

- إشعار وتحويل النطاق إلى عميل (أي قطع خدمة البروكسي)
- التعليق المؤقت للنطاق خلال التحريات الجنائية
- الكشف للمستخدم عن هوية/اتصال المرخص له المشاركة في النشاط غير المشروع
- رفض الكشف - التأكيد الإيجابي لمسئولية البروكسي على الاستخدام الإضافية للنطاق

يجب وضع سياسة هنا من أجل تفصيل ما يمثل الوثائق الكافية والأوقات التي يجب فيها إشعار المرخص له. بالإضافة إلى ذلك، يجب أن تكون هناك سياسات واضحة فيما يتعلق بتأثير القانون المحلي والعوامل التي يجب النظر فيها. يحدث كل ما سبق اليوم، بدون أي إشراف، أو إرشاد من سياسة أو عواقب لرفض/إغفال الكشف.

د) مستخدم RDS الذي يتلقى رد الكشف الآن قد حصل على المعلومات المطلوبة لإهمال الأمر أو ملاحقة إجراء قانوني/مدني. على سبيل المثال، قد يؤدي انتهاك العلامات التجارية إلى تقديم قضية UDRP، في حين قد يؤدي التحري الجنائي لإنفاذ القانون إلى اعتقال المشبه به. وإذا تم رفض الكشف (أو لم يتم الحصول على الرد في الوقت المناسب)، يمكن لمستخدم RDS الآن أيضًا اختيار ملاحقة إجراءات قانونية/مدنية ضد البروكسي المعتمد.

لاحظ أن العمليات المشار إليها أعلاه لا تتناول الحالات التي يجب فيها "إماطة اللثام" عن تسجيل بروكسي أو خصوصية للجمهور العام بلا من "الكشف عنها" لمقدم الطلب.

---

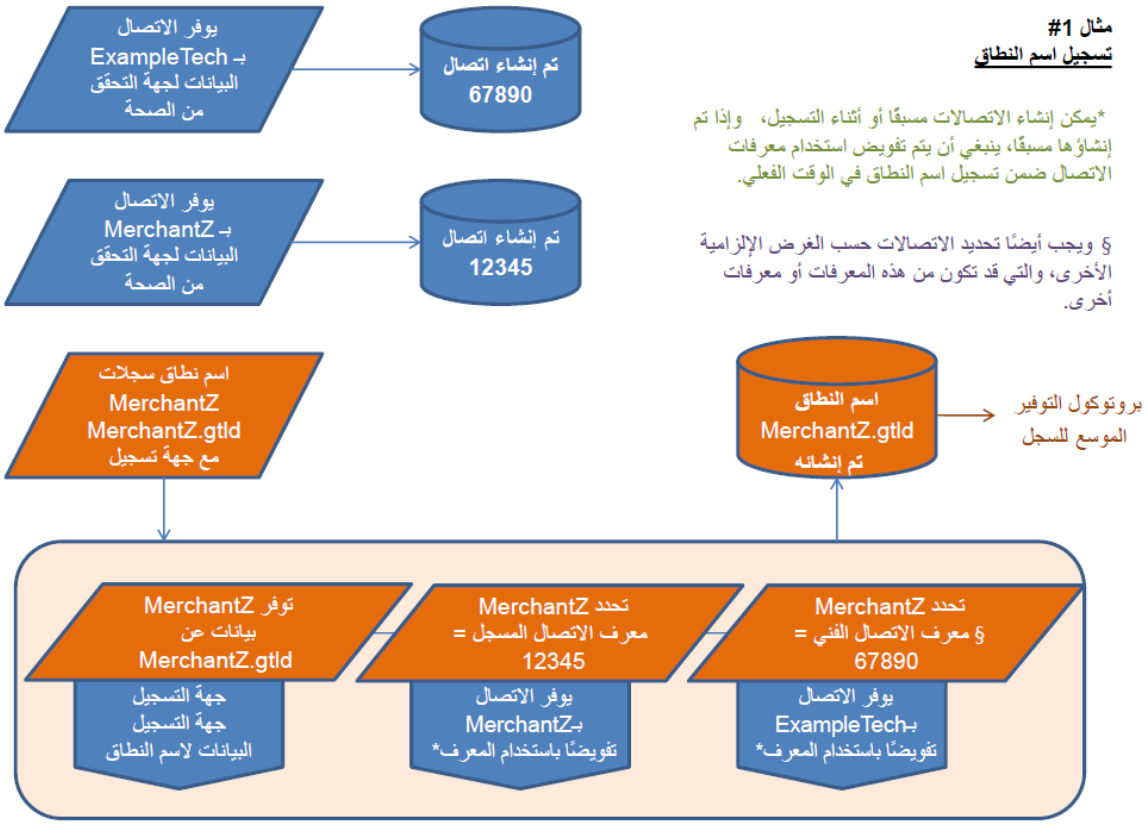
[43] * قد يعتمد انتهاء المهلة على مقدم الطلب والسبب المحدد للاتصال. قد ينتقل إنفاذ القانون مباشرة إلى الخطوة 3 (الكشف) للتحريات الحساسة من ناحية الوقت. والأطر الزمنية والجهود للخطوة 2 يجب أن تكون منخفضة بما يكفي لعدم تشجيع الآخرين عن القفز مباشرة إلى الخطوة 3.

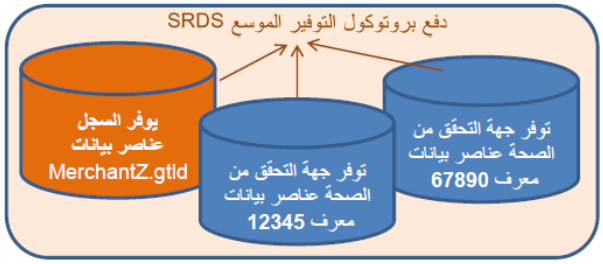
[44] ** أي مستخدم يطالب بكشف يجب أن يوضح أنه (أو يمثل) طرفًا يعاني من ضرر إجرائي. على سبيل المثال، حاملي الماركات العالمية أو وكلائهم المدعين انتهاكات العلامات التجارية قد يثبتون ملكيتهم لاسم (أسماء) نطاقات مشابهة للنطاق المسجل لدى البروكسي. ويجب التفكير مليًا لتحديد أنواع المستخدمين لأنواع الأضرار. راجع قائمة GoDaddy لنموذج شكاوى النطاقات المسجلة من خلال بروكسي كمثال.

ويجب إعادة تعديل هذه النماذج والعمليات المقترحة من خلال مجموعة عمل GNSO PPSAI، استنادًا إلى نظرها في احتياجات مجتمع ICANN والاستنارة بأفضل الممارسات من خلال ردود على استطلاع EWG على الإنترنت لموفري خدمة الخصوصية والبروكسي.

## الملحق ط: المخططات الانسيابية لعملية RDS

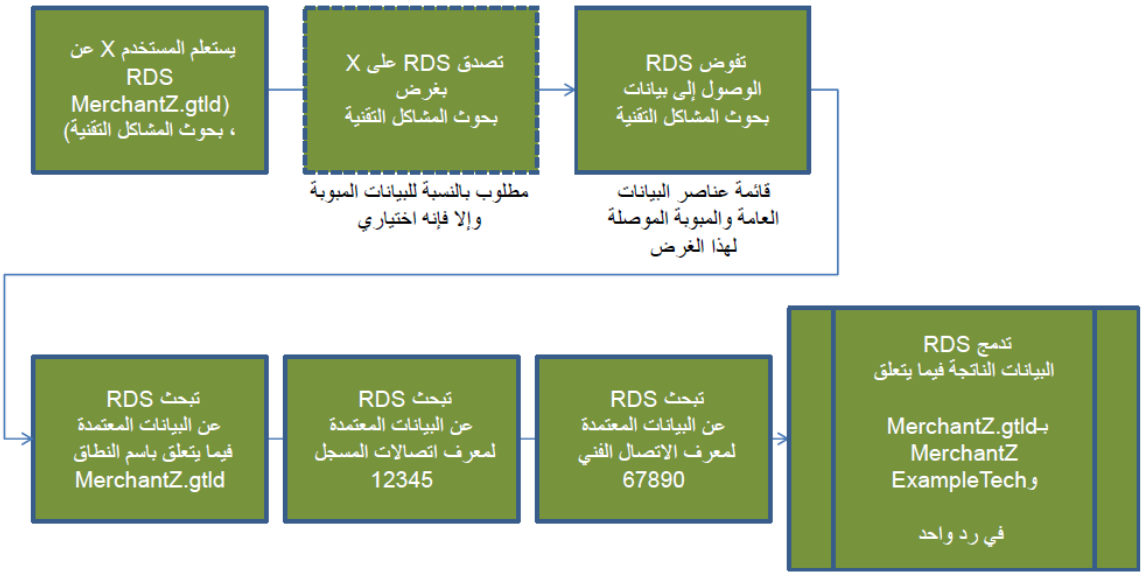
توضح المخططات الانسيابية التالية تدفقات البيانات الأساسية بين عوامل النظام البيئي لـ RDS خلال تسجيل أسماء النطاقات واستعلام مقدمي الطلبات عن RDS للمعلومات على معلومات حول أسماء النطاقات من أجل حل مشكلات فنية.



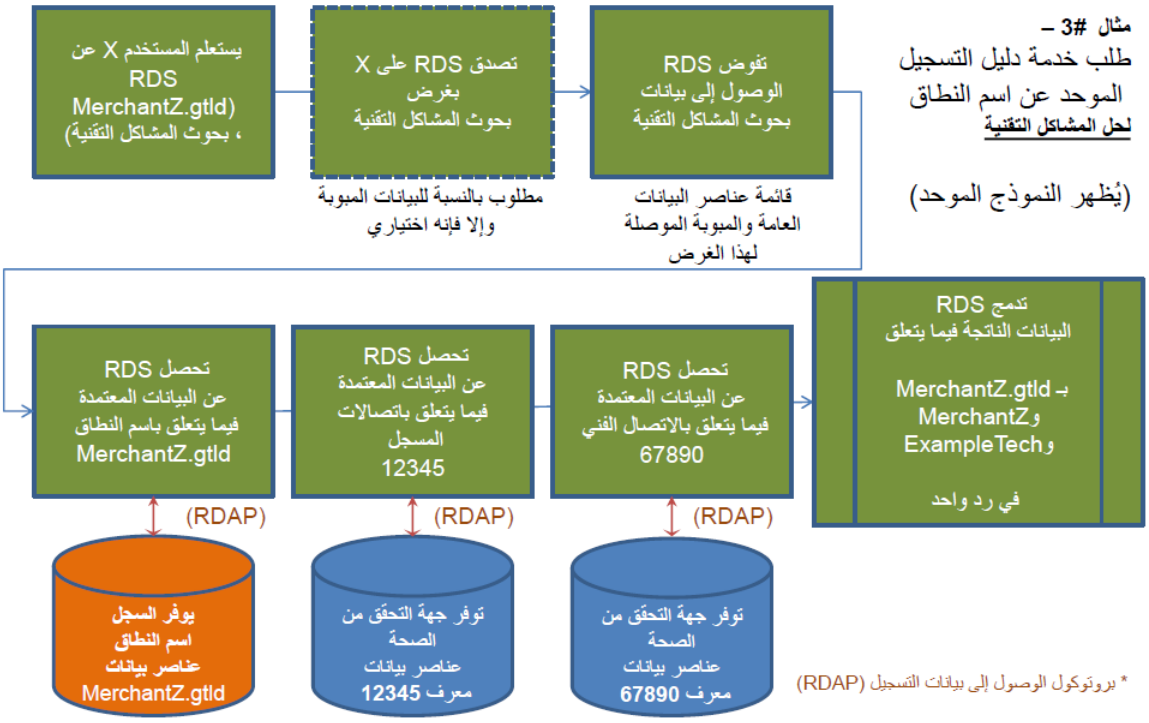



مثال #2 –
خدمات تسجيل دليل الاستعلام عن اسم النطاق
**لحل المشاكل التقنية**

**(تُظهر النموذج المتزامن)**




ولتسهيل مقارنة النماذج، تم تكرار نفس هذا المثال أدناه لـ FRDS.




**مثال #3 –**
طلب خدمة دليل التسجيل الموحد عن اسم النطاق
**لحل المشاكل التقنية**

(يُظهر النموذج الموحد)

* بروتوكول الوصول إلى بيانات التسجيل (RDAP)

# الملحق ي: حول مجموعة EWG

## عملية الاختيار والرؤية

عند تشكيل مجموعة EWG، اعتمد مجلس إدارة ICANN أسلوبًا جديدًا في حل المشكلات الصعبة التي أصيبت بالتأزم والانقسام في الماضي. وقد قام مجلس الإدارة بتجميع الأفراد الذين يمثلون مجموعة واسعة من وجهات النظر وأصحاب المصلحة على أمل أنه بمشاركة خبراتهم يمكنهم تحقيق النجاح حيث فشل الآخرون. من خلال تقديم هذا التقرير النهائي وما يحتوي عليه من 180 مبدأ مؤيد بالإجماع، فقد تجسدت بالفعل رؤية مجلس الإدارة.

وقد تم اختيار أعضاء مجموعة EWG بعناية بمساعدة منسق مخضرم ومحايد، جون فرانسوا باريل. فقد تم اختياره بسبب خبراته في تطوير المعايير في صناعة إلكترونيات العملاء. وقد تم فحص عشرات مقدمي طلبات EWG استنادًا إلى معايير متعددة، ويشمل ذلك مهارات القيادة، والخبرات، والتنوع الجغرافي، وبناء الإجماع، والقدرة على الإبداع، وفي بعض الحالات، الحيادية. وكان هناك شعور بأن الأفراد من خارج مجتمع ICANN يمكنهم جلب وجهات نظر جديدة، واحدة ليست قديمة بسبب المحاولات الماضية للتعامل مع مشكلة WHOIS.

## تشكيل مجموعة EWG

يتألف أعضاء EWG من أفراد، ومنسقي مجلس إدارة وفريق عمل من كل من أستراليا وكندا والصين والاتحاد الأوروبي وأيرلندا وجامايكا ونيجيريا والنرويج وسويسرا والمملكة المتحدة والولايات المتحدة. وقد أثبت التنوع الجغرافي جدواه في فهم العديد من التحديات الخاصة بالولايات القضائية والمرتبطة بأعمال EWG.

ومن بين أعضاء EWG كان المقاولون المخضرمون والقادة العالميون (أجايي، وعلا-بيتيلا، ونيلون، وراسموسن، وشاه). الخبرة التجميعية في موازنة المخاطر ونموذج حل المشكلات الموجه بالنتائج قد مهد الطريق للوصول إلى إجماع مبكر فيما بيت فريق EWG.

وبسبب أن تفويض EWG قد اشتمل على فحص سياسة عامة، لاسيما مشكلات الخصوصية، فإن الخبرات الخاصة في القطاع الحكومية كانت أساسية في نجاحها. وقد ساهم كل من بيرين ونيبيل بخبرات من المنظور الكندي والأوروبي، مؤكدين على أن هذه المشكلات كانت في صدارة تصميم النظام من الجيل التالي. ومن المهم أنه خلال مداولات مجموعة EWG، في أهيب بها وحاولت التفكير في التطورات الأخيرة في التشريعات الخاصة بحماية البيانات في الاتحاد الأوروبي.

ومن الجوانب الحيوية الأخرى في أعمال EWG ما اشتمل على تأكيد أن توصياتها كانت قابلة للتنفيذ بشكل معقول في نظام DNS البيئي الحالي. الخبرات من أمين سجل gTLD (نيلون)، وسجل gTLD (Hollenbeck-.com و .net)، وأعضاء نطاقات ccTLD أي (cn-Jian.، وuk-Nanayakkara.، وng- Ajayi. و au-. Disspain) ألقوا الضوء على مشكلات مثل أساليب التوثيق، وتسجيلات الخصوصية/البروكسي، والتوافق مع البروتوكولات مثل EPP وRDAP الجديد الذي يجري تطويره في IETF، بالإضافة إلى تضمين مفاهيم مثل "الوصول عن طريق بوابات" من أجل عرض عناصر البيانات الحساسة.

تم فحص مشكلات الأمن والاستقرار، مع التركيز على رؤية الأعضاء الحاليين والسابقين في SSAC (كروكر وراسموسن)، بما يسهم في فهمهم الواسع لاحتياجات إنفاذ القانون في التغلب على إساءة الاستخدام الضارة المشمولة في DNS.

إن تصميم نظام جديد أمر مستحيل دون النظر في احتياجات العديد من المستخدمين لنظام RDS من الجيل التالي. وقد اشتملت مجموعة EWG على أعضاء ذوي معرفة متعمقة بمشكلات الملكية الفكرية (كواجوشي، وفايرا، وشاه) والتي تعتمد بشكل كبير على نظام WHOIS الحالي في التغلب على سرقة عناوين الإنترنت، والتدليس والغش عبر الإنترنت، بالإضافة إلى وجهات النظر المشتركة من خلال المستخدمين النهائيين (ساميول وفيفر). وقد ساعدت وجهات النظر المتنوعة هذه على ضمان أن الأغراض المشروعة لوصول RDS إلى بيانات التسجيل يمكن مواءمتها، مع الحد في نفس الوقت من أوجه القصور وإساءة الاستخدام في عمليات التسجيل الحالية متى ما كان ذلك ممكنًا.

ولإكمال مجموعة EWG، فقد أحضر أعضاء فريق ICANN (ميتشل وميلام) وجهة نظر تنفيذية بالإضافة إلى معرفة بالإطار التعاقدي لـ ICANN. كما قدم استشاري (فيفر) أيضًا بيانات من دراسات WHOIS التنفيذية لـ GNSO على مدار الأعوام الخمسة الماضية لمساعدة EWG في صياغة توصيات مستندة إلى حقائق.

**منهجية العمل**

بدأت مجموعة EWG عملها بسلسلة من المعارف بأنشطة الآخرين الموجهة لبناء الألفة والثقة والأكثر أهمية، شعور بالانتماء إلى فريق. وقد وضعت مجموعة EWG مجموعة من قيم الفريق من أجل التغلب على أية عوائق في التعرف على الحلول الابتكارية لهذه المشكلة المعقدة. وهي كما يلي:

- على هذا الفريق كأفراد
- التحدث بحرية
- عدم الرجوع إلى الوسائط الاجتماعية
- الأمانة الفكرية
- التنظيم الذاتي في المجال
- التصميم الجديد
- الاستعانة بالحقائق الثابتة (التكنولوجيا والحكومات)

وقد ساعدت هذه القيم على توجيه EWG إلى التسويات الضرورية من أجل تصميم نظام RDS وتقديم مبادئي موضحة في هذا التقرير النهائي.

للحصول على مزيد من المعلومات والسير الذاتية لأعضاء EWG، برجاء مراجعة هذا الإعلان.