RDS USER ACCREDITATION
RFI RESPONSE SUMMARY

Between 7 February and 10 March 2014, the Expert Working Group (EWG) on Next Generation Registration Directory Services (RDS) invited organizations that currently issue system access credentials to authorized members of their own community, using defined acceptance criteria, to respond to a Request for Information (RFI).

Through this RFI, the EWG wished to identify organizations already issuing credentials to communities identified as gTLD registration data users, hoping to build upon existing membership or credentialing processes to fulfill **RDS User Accreditation** needs.

A summary of RFI responses received from three (3) organizations is provided herein.

RFI Respondents

RFI submissions were received from three (3) organizations:

- **Universal Postal Union (UPU) Postal Technology Center (PTC) Addressing Unit (ADU)**, a specialized agency of the UN, with 192 member countries, 170 EMS and 150 Telematics cooperative members, and POST*CODE DataBase licensees, including government and law enforcement agencies.
- **Canadian Internet Registration Authority (CIRA),** the official registry of the .CA domain, issuing domain names to verified Canadian citizens, corporations, and trademark owners, plus 2 types of credentialed access.
- **Digicert, Inc**., a verification and credentialing company that offers federated and other identity solutions to control access to varying levels of sensitive information, for clients ranging from government entities, academia, and Fortune 500 companies to small e-commerce operations.

Experience of Respondents

The RFI asked Respondents to describe their overall experience with (a) identifying and enroll community members on a regional or global scale, (b) handling enrollment requests, (c) managing user accounts, (d) scaling quickly, (e) communicating in multiple languages, (f) understanding data protection and audit needs, and (g) understanding their community's domain registration needs and purposes.

DigiCert and UPU support communities with global membership, while CIRA is focused on Canadian membership. All three manage multiple communities, based on established criteria:

- **CIRA** requires that .CA domain registrants have a connection to Canada ("presence") through one of 18 categories, including Canadian citizenship, residence, and corporation. Additionally, CIRA issues and manages access credentials for two more restricted communities: CIRA Members that participate in policy making discussions, and CIRA Registrars that allow the registration of .CA domain names. CIRA Members must certify their presence before receiving username/password access to policy making discussions. Approximately 190 CIRA Registrars may identify individual staff authorized to request Registry Lock changes.

- The **UPU** manages several global communities, including national Posts (member country designated operators), restricted unions and cooperatives composed of those operators, .post Registrants, and businesses and software vendors with licensed access to the UPU's Universal POST*CODE DataBase. The process and criteria for enrollment varies across these communities, as

do the credentials and rights that members receive upon acceptance. For example, new UPU member country requests must be approved by existing member countries and contribute to union expenses on a sliding scale. Direct Marketing Advisory Board Members include both member country-designated operators and private-sector companies and associations that pay membership fees, based on their country's contribution fee.

- **DigiCert** verifies more the 1000,000 applicants annually, providing identification and access services to the education, research, and medical communities, government entities, and others that need efficient access control mechanisms. Credentials are provided to members of each community in accordance with community-driven criteria and authentication mechanisms. For example, education and research communities control access using X.509 certificates, while healthcare communities use SAML-based authentication for access to prescription data.

Individual RFI responses provided further detail about community definitions, acceptance criteria, scalability, language support, and understanding of data protection and audit requirements. Enrollment and account management practices are further explored later in this summary.

RDS User Communities

The RFI asked Respondents to describe their existing relationships with RDS user communities; responses are summarized in the Table 1 below. Specifically, "■" indicates that the Respondent claimed to currently enroll and issue credentials to members of that community, while "☐" indicates that the Respondent described some other type of existing relationship with that community.

RDS User Community	CIRA	UPU	DigiCert
Natural Person Registrants	■	☐	■
Legal Person Registrants	■	■	■
Proxy Service Providers			■
Protected Registrants			■
Internet Technical Staff	■	☐	■
On-Line Service Providers		■	■
Individual Internet Users		☐	
Business Internet Users		☐	☐
Internet Researchers		☐	☐
Intellectual Property Owners	■	☐	■
Law Enforcement Agencies		■	☐
OpSec Investigators		■	☐
Other Investigators		☐	☐

Table 1: Community Coverage

Note that the above summary required some interpretation and may not fully reflect each Respondent's relationships or intent; please refer to individual RFI responses for further detail.

Additionally, the fact that a Respondent now issues credentials to members of a community does not imply they are the ONLY organization to do so. For example, both CIRA and UPU register domain names to legal persons, albeit under different TLDs.

Finally, although all Respondents demonstrated experience working with some subset of RDS user communities, it is unclear that any Respondent would be able to determine the *registration data needs and purposes* for those communities. All Respondents described community-defined rules which they enforced; this suggests that communities might need to *define their own* RDS needs and purposes, to be enforced by RDS Accreditors.

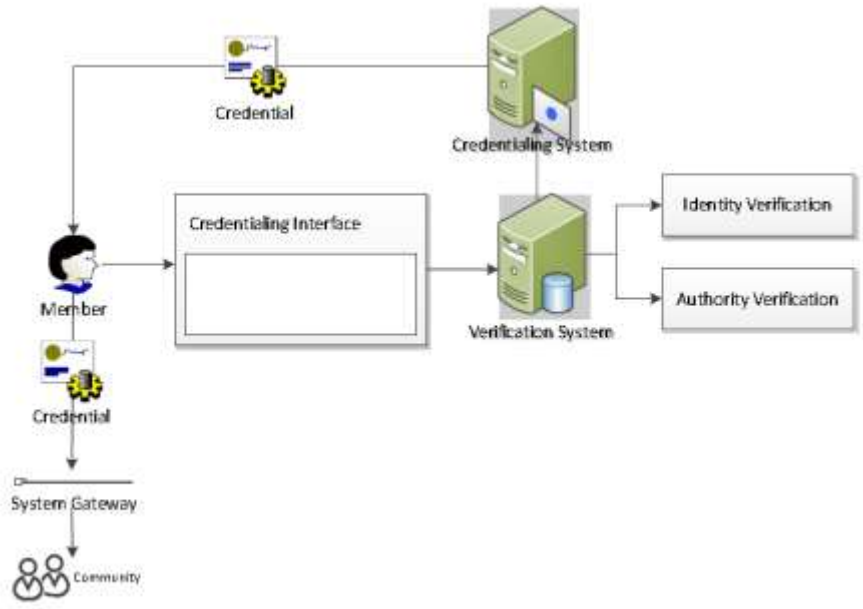
Membership Criteria and Enrollment Processes

The RFI asked Respondents to detail membership criteria and enrollment processes, including requirements, fees, terms and conditions, application form, review/approval, acceptance criteria, identify validation/verification, credentials issued, access rights granted, specified purposes, typical delay, reasons for rejection, and dispute process (if any).

As might be expected, membership requirements, fees, and terms and conditions varied by community. However, processes used by Respondents to add communities, enroll members, check criteria, verify identities, and issue credentials often applied to several communities. For example:

Communities and members wishing to subscribe to DigiCert's credentialing services apply online or through an account representative. For supported communities, DigiCert will establish, by mutual agreement, a set list of criteria required for community member participation. Typically, criteria includes verification of each community member's identity, such as name and address, and authorization to participate, such as having the appropriate licensure or proof of acceptance from the member's sponsoring organization.

Once the community establishes a formal relationship with DigiCert, DigiCert provides the community with an online interface and API that community members may use to obtain community-specific credentials. After receiving an application for participation, DigiCert's verification engine evaluates the applicant's request using the community selected criteria. If successfully verified, the appropriate credential, such as a digital certificate, SAML assertion, or OTP token, is issued by a credentialing system. The approved member can the present the credential to the community's secure systems to gain access to sensitive data and participate in community activities. An example is shown below:



Similarly, CIRA described an overall process consisting of Qualification, Verification, Monitoring, and Training, customized as appropriate to the type of entity and the access requested:

> A single citizen registering a domain name needs to do nothing more than assert presence, but those registrants who seek to be voting members of CIRA are required to offer multi-factor support [for their qualification claim].
>
> Self-qualifying can work at the broadest levels and the least sensitive layers of information, but as data becomes more sensitive and access requires more stringent qualification, persistent review is necessary. There will need to be layers of verification to match the level and purpose of the access. And, whether individual or company, if CIRA's persistent monitoring discovers a reason to challenge standing, the necessary level of documentation increases…
>
> The combination of self-certification and persistent monitoring is designed to add speed to the designation, registration, and use of .CA domain names while providing a check on bad behavior. A dedicated team reviews registrations on an on-going basis. A second team performs the same function with regard to CIRA's registrar relationships… The combination of technology and people is the best solution.

UPU enrollment processes appeared to be less automated, perhaps as a consequence of the UPU's role as a special agency of the UN and the diverse, formally-organized communities involved. For example:

> When adding a new member to a UPU body, the identity of the delegate is verified by country members and the International Bureau. When adding a new user for access to a software solution, the applicant's identity is verified by cooperative members and the International Bureau…For cooperative membership, credentials depend on the software solution to be accessed.

Nonetheless, all three Respondents described relatively speedy enrollment processes:

- **UPU:** "From milliseconds to minutes, depending on investigation needs; longer delay possible."
- **CIRA:** "Deviations from eligibility requirements [are detected by persistent monitoring that] occurs post-registration – it does not delay the activation of the domain name."
- **DigiCert:** "Credentials for community members are usually approved within minutes, but the delay depends on the level of assurance and responsiveness of the applicant…Even the highest assurance credentialing typically takes less than an hour to verify and issue."

DigiCert was the only Respondent to detail a dispute process, as follows:

> Applications are rejected if they do not meet the criteria specified by the community of interest. Examples include if the applicant lacks the appropriate licensure, the applicant submits a fraudulent application, or if the applicant cannot be satisfactorily verified.
>
> Rejected applications may appeal the rejection, which initiates a manual review…If the rejection remains after the appeal process, the rejected applicant can appeal to the community representative for further consideration. If permitted by the community, the community representative may authorize issuance of the credential regardless of the rejection.

User Account Management Practices

The RFI asked Respondents to detail user account management practices, including data and credentials associated with user accounts and processes for update, suspension, revocation, termination, ToC enforcement, and dispute.

DigiCert described its user account management process as follows:

> User accounts are used to manage credentials, including replacing lost credentials, canceling compromised credentials, and requesting upgrade credentials. Members can use accounts to review and update information used in issuing the credential.
>
> Passwords and usernames are retrieved using standard online password reset mechanism where a password reset link is emailed to the account on file. If two-factor authentication is required and the second factor is hardware, the account user can request a new token…sent to the verified address.
>
> Accounts are suspended, revoked, or terminated if the terms of user are violated or if the applicant is no longer permitted to participate in the designated community. Accounts are also suspended if the credentials required to access the account expire… A user may terminate their account at any time by providing notice to DigiCert.

With regard to ToC enforcement and remediation, CIRA described its on-going Monitoring process, conducted by a dedicated team involving nearly 20 percent of CIRA employees. According to CIRA:

> Registrations are subject to a persistent check that validates [the registrant's self-declared Canadian presence claim.] By way of example:
>
> - A personal Registrant who has claimed Canadian citizenship will be asked for documentation to substantiate their claim such as a Canadian passport or birth certificate.
> - A corporate Registrant who has claimed Canadian Corporation will be asked to produce its Certificate of Status.
> - A Registrant who has claimed the Canadian trademark category will be asked to produce evidence of its Canadian registered trademark.
>
> The persistent monitoring has a primary focus on deviations from eligibility requirements… Domain names found to be registered outside the parameters of presence will be withdrawn from Registrants.

DigiCert's process for auditing ToC compliance and remediating violations is more general-purpose, enforcing ToCs that vary by level of assurance but always require provision of accurate data, update to reflect changes, and reasonable assistance in investigating and curing compromise. For example, DigiCert described its process to remediate detected or reported ToC violations:

> DigiCert has an email that is monitored 24/7 where community members, administrators, law enforcement agencies, and other interested parties may submit ToC violations. DigiCert investigates all reported violations immediately and may suspend account access while an investigation is pending. Credentials are usually revoked within 24 hours of a confirmed breach of the ToC.
>
> Except for emergency situations, prior notice of the revocation is sent to the email address listed in the [community's] master account to ensure the community representative is aware of the action. DigiCert [also] permits community administrators responsible for enforcing ToC violations to revoked credentials issued to community members through the master account.

DigiCert maintains and utilizes a scoring system to flag account requests that present a higher risk of fraud. This scoring system evaluates the risk of the request compared to the level of identity verification required. High risk accounts receive addition monitoring for ToC violations.

User Recognition and Federated Authentication

The RFI asked Respondents to describe any partnerships they might have involving mutual user recognition and federated authentication for system/data access.

The UPU described a number of partner organizations, including several with whom data or information is exchanged. However, for reasons of confidentiality, no description of federated authentication and access was provided.

DigiCert noted that it is cross-certified with the *Federal Bridge Certification Authority* (*FBCA*) through a contractual relationship whereby cross certificates issued by either CA (DigiCert or FBCA) can be used for federated authentication and access.

Potential for Building on Existing Processes to Accredit RDS Users

Finally the RFI asked Respondents to discuss their existing processes might be leveraged to accredit RDS users, including (a) vetting RDS user applications (b) confirming RDS user identity (c) determining legitimate need to access data (d) reuse of access credentials, and/or (e) reuse of enforcement and compliance processes.

All three Respondents saw opportunities to build on their existing processes and systems to help fulfill RDS User Accreditation needs. For example:

- **CIRA** cited its long history in managing a "gated community" of registrants and registrars as a solid platform for supporting the RDS goal of providing gated access to registration data.
- The **UPU** noted that its regional support centers and close coordination with designated postal operators in 192 member countries could play a role in confirming RDS user identity. For example, it might be possible to use the UPU's PostID framework to check the email and telephone number of a user applying for RDS access, or to use the postal network for contact data investigations.
- **DigiCert** noted that it would be able to provide various levels of assurance in confirming RDS user identities, ranging from purely automated to manual high assurance verification. DigiCert further suggested that a separate credentialing account be available for RDS access, noting "Whether existing credentials could or should be reused for RDS access depends on the desires of individual community members and how ICANN establishes assurance levels."

Individual RFI responses provided additional discussion of opportunities and each Respondent's rationale for why their organization is well suited to help meet RDS User Accreditation Needs.

NOTE: Unless otherwise stated, RFI responses should be treated as confidential, not for publication.