# EPP and RDAP Status Values

## Introduction

In the domain management landscape, EPP and RDAP status values are indispensable tools for enforcing registry policies, managing domain lifecycles, and safeguarding against unauthorized actions. The registry system leverages these protocols to provide a robust framework for domain registration and management. This document delves into the specific EPP and RDAP status values implemented in the registry system, highlighting their roles in maintaining domain integrity and security. Whether it's preventing unauthorized transfers, managing grace periods, or handling abusive registrations, these statuses are critical for ensuring the smooth operation of domain names within the DNS ecosystem.

## EPP Status Values

EPP status values are critical for controlling the state and operations of domain names. They are used by registries and registrars to enforce policies, manage domain lifecycles, and prevent unauthorized actions. Here are the key EPP status values implemented in the registry system:

1. Client and Server Prohibitions:
    - clientDeleteProhibited / serverDeleteProhibited: These statuses prevent the deletion of a domain name. They are essential for protecting domains from accidental or unauthorized deletions. The `clientDeleteProhibited` status is set by the registrar, while the `serverDeleteProhibited` status is set by the registry. These statuses ensure that a domain remains active and secure, especially when it is involved in legal disputes or has significant business value.
    - clientTransferProhibited / serverTransferProhibited: These statuses prevent the transfer of a domain name to another registrar. They are crucial for maintaining domain ownership and preventing unauthorized transfers. The `clientTransferProhibited` status is applied by the registrar, while the `serverTransferProhibited` status is enforced by the registry. These statuses are often used during the initial registration period or when a domain is involved in a dispute.
    - clientUpdateProhibited / serverUpdateProhibited: These statuses prevent any updates to the domain's configuration. They are used to lock the domain's settings, ensuring that no unauthorized changes are made. The `clientUpdateProhibited` status is set by the registrar, while the `serverUpdateProhibited` status is applied by the registry. These statuses are useful for domains that require a high level of security and stability.
1. Hold Statuses:
    - clientHold / serverHold: These statuses indicate that the domain is not included in the DNS, rendering it inactive. The `clientHold` status is applied by the registrar, while the `serverHold` status is enforced by the registry. These statuses are often used for domains involved in abuse or policy violations, effectively suspending their operation until the issues are resolved.
1. Pending Statuses:

- pendingCreate / pendingDelete / pendingTransfer / pendingUpdate: These statuses indicate that a request to create, delete, transfer, or update the domain is in progress. They are used to track the status of domain operations and ensure that they are completed successfully. These statuses are temporary and are removed once the operation is finalized.

1. Redemption and Grace Periods:
   - redemptionPeriod: This status indicates that the domain is in a grace period after expiration, allowing the original registrant to restore it. The redemption period typically lasts for 30 days, during which the domain is not included in the DNS. This status provides a safety net for registrants who may have missed the renewal deadline.
   - addPeriod / renewPeriod / transferPeriod: These statuses indicate various grace periods following domain creation, renewal, or transfer. They provide registrants with a window of time to cancel the operation without incurring additional fees. These periods are essential for managing domain lifecycles and ensuring that registrants have the flexibility to make changes as needed.

# RDAP Status Values

RDAP status values provide a standardized way to represent the state of domain names and other Internet resources. They are used to convey information about the status of a domain and its eligibility for certain operations. Here are the key RDAP status values implemented in the registry system:

1. Active / Inactive:
   - active: This status indicates that the domain is operational and included in the DNS. It signifies that the domain is functioning as expected and is accessible to users.
   - inactive: This status indicates that the domain is not included in the DNS, similar to EPP hold statuses. It is used for domains that are not currently operational, either due to policy violations or pending actions.
1. Prohibited Actions:
   - delete prohibited / renew prohibited / transfer prohibited / update prohibited: These statuses correspond to EPP prohibitions, indicating disallowed actions. They are used to enforce policies and prevent unauthorized operations on the domain.
1. Pending Actions:
   - pending create / pending delete / pending transfer / pending update: These statuses reflect EPP pending statuses, indicating ongoing operations. They provide visibility into the status of domain requests and ensure that they are processed in a timely manner.
1. Grace Periods:
   - add period / auto renew period / redemption period / renew period / transfer period: These statuses are similar to EPP grace periods, indicating various windows of time during which certain actions can be taken. They provide registrants with the flexibility to manage their domains effectively.

# Abusive Registrations

Domains considered abusive may have specific statuses applied to restrict their operation. These statuses are used to prevent the misuse of domain names and ensure compliance with registry and registrar policies. Here are some of the key statuses used for managing abusive registrations:

- serverHold: This status is used for domains identified as abusive, preventing DNS resolution. It effectively suspends the domain's operation, making it inaccessible to users. This status is applied by the registry and is often used in cases of spam, phishing, or other malicious activities.
- clientHold: This status is applied by registrars to suspend domains suspected of abuse. It is used to prevent the domain from being included in the DNS, effectively rendering it inactive. This status is often used as a temporary measure while investigations are conducted.
- serverDeleteProhibited / serverTransferProhibited / serverUpdateProhibited: These statuses are used to lock down domains involved in abuse, preventing deletion, transfer, or updates. They are applied by the registry and are used to maintain control over domains that pose a risk to the DNS ecosystem.

# Conclusion

EPP and RDAP status values play a vital role in managing domain names and ensuring the security and stability of the DNS. By implementing these statuses, the registry system provides registries and registrars with the tools they need to enforce policies, manage domain lifecycles, and prevent unauthorized actions. These statuses are essential for maintaining the integrity of the DNS and protecting against abusive registrations. Through the use of EPP and RDAP, the registry system≠≠= ensures that domain management is both efficient and secure, providing a robust platform for handling domain registrations.