Domain Connect 2.0

Version 2.0 Revision 37 Dec-8-2017 DRAFT

Contents

1 Introduction and Background

GoDaddy recently implemented a feature called Domain Connect that simplified how Service Providers configured domains hosted at GoDaddy (the DNS Provider). This made the end to end experience considerably easier for the end user.

Based on learnings from this implementation, an improved and more general version of this protocol was created. This document describes Domain Connect 2.0 and is shared with the intent of it becoming an open standard that can be utilized by multiple DNS Providers and Service Providers to simplify this interaction across the internet.

1.1 Terminology

Service Providers refers to entities that provide products and services attached to domain names. Examples include web hosting providers (such as Wix or SquareSpace), email Service Providers (such as Microsoft or Google) and potentially even hardware manufacturers with DNS-enabled devices like home routers or automation controls (such as Linksys, Nest, and Philips).

DNS Providers refers to entities that provide DNS services such as registrars (such as GoDaddy or 1and1) or standalone DNS services (like CloudFlare).

Customer/User refers to the end-user of these services.

Templates/Service Templates refers to a file that describes a set of changes to DNS and domain functionality to enable a specific service.

Root Domain refers to a registered domain (e.g. example.com or example.co.uk) or a delegated zone in DNS.

Sub Domain refers to a sub-domain of a root domain (e.g. sub.example.com or sub.example.co.uk).

1.2 Problem Statement

Configuring a service at a Service Provider to work with a domain has historically been a complex task that is difficult for users.

Typically a customer would try to configure their service by entering their domain name with the Service Provider. The Service Provider then used a number of techniques with mixed reliability to discover the DNS Provider. This might include DNS queries for nameservers, queries to whois, and mapping tables to figure out the registrar or company running DNS.

Once the Service Provider discovered the DNS Provider, they typically gave the customer instructions for proper configuration of DNS. This might include help text, screen shots, or even links to the appropriate tools.

Discovery of the DNS Provider in this manner is unreliable, and providing instructions to users would present a number of technologies (DNS record types, TTLs, Hostnames, etc.) and processes they didn't understand. These instructions authored by the Service Provider often quickly become out of date, further confusing the issue for users.

1.3 Goals

The goal of this specification is to create a system where Service Providers can easily enable their applications/services to work with the domain names of their customers. This includes both discovery of the DNS Provider and subsequent modification of DNS.

The system will be implemented using simple web based interactions and standard authentication protocols. The creation and modification of DNS settings will be done through the application of templates instead of direct manipulation of individual DNS records.

1.4 Templates

Templates are core to this proposal, as they describe a service owned by a Service Provider and contain all of the information necessary to enable and operate/maintain a service.

The individual records may be identified by a groupId. This allows for the application of templates in different stages. For example, an email provider might first set a TXT record to verify the domain, and later set an MX record to configure email delivery. While done separately, both changes are fundamentally part of the same service.

It is important that templates be constrained to an individual service, as later removal of a template would remove all associated records.

Templates can also contain variable portions, as often values of data in the template change based on the implementation and/or user of the Service Provider (e.g. the IP address of a service, a customer id, etc.).

Configuration and onboarding of templates between the DNS Provider and the Service Provider is seen as a manual process. The template is defined by the Service Provider and given to the DNS Provider. Future versions of this specification may allow for an independent repository of templates. For now the templates are all published at http://domainconnect.org

By basing the protocol on templates instead of DNS Records, several advantages are achieved. The DNS Provider has very explicit knowledge and control of the settings being changed to enable a service. And the system is more secure as templates are tightly controlled and contained.

1.5 Summary

- Connect can make changes to DNS based on a service template and avoid exposing DNS to customers and Service Providers.
- Connect can have arbitrary parameters for known variables with values that change per user and not confuse users with their meanings or functionality.
- Connect is easy for customers with a simple confirmation dialog flow.
- For more complex integrations, Connect has an OAuth based implementation to provide an acceptable level of security, but allowing for the Service Provider to call an API to apply a template at a later time.

2 Protocol Overview and End User Flows

To attach a domain name to a service provided by a Service Provider, the customer would first enter their domain name.

Instead of relying on examination of the nameservers and mapping these to DNS Providers, DNS Provider discovery would be handled through simple records in DNS and an API. The Service Provider can query for a specific record in the zone to determine a REST endpoint to initiate the protocol. A Domain Connect compliant DNS Provider would return information about that domain and how to configure it using Domain Connect.

For the application of the changes to DNS, there are two use cases. The first is a synchronous web flow, and the second is an asynchronous flow using OAuth and an API.

It should be noted that a DNS Provider may choose to only implement one of the flows. As a matter of practice many Service Providers are based on the synchronous flow, with only a handful of them based on the asynchronous OAuth flow. So many DNS providers may opt to only implement the synchronous flow.

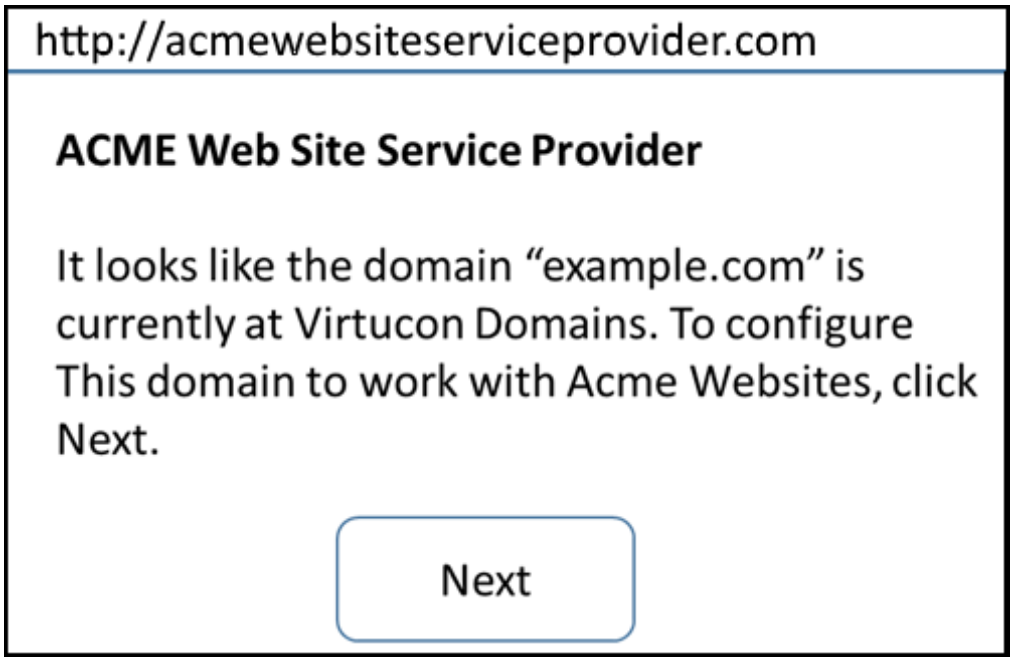
It should also be noted that individual services may work with the synchronous flow only, the asynchronous flow only, or with both.

2.1 The Synchronous Flow

This flow is tailored for the Service Provider that requires a one time and synchronous change to DNS.

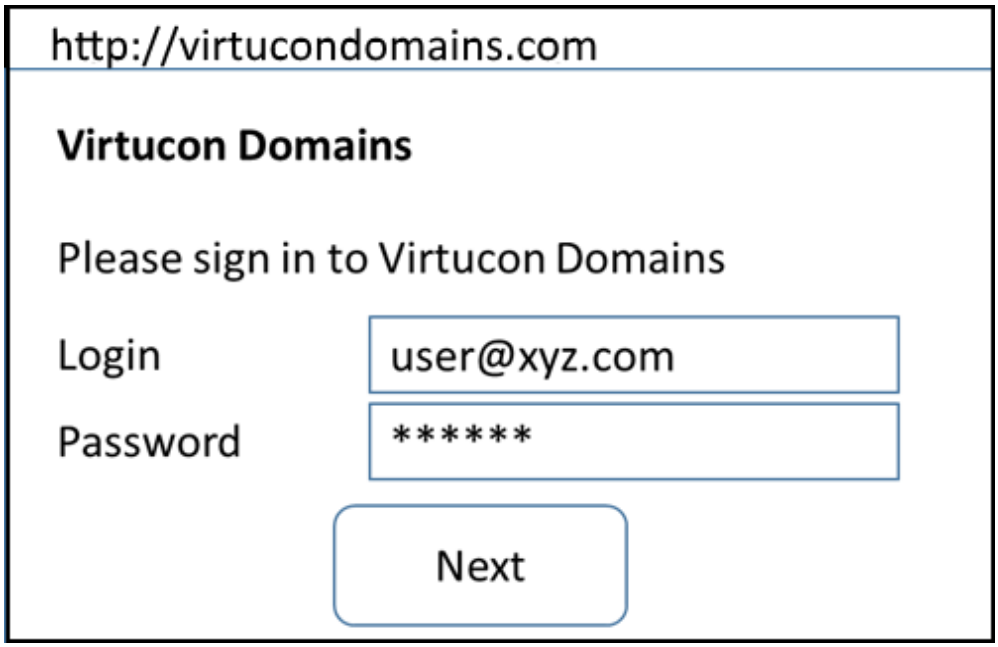
The user would first enter their domain name at the Service Provider website.

After the Service Provider determines the DNS Provider, the Service Provider might display a link to the user indicating that they can "Connect their Domain" to the service.

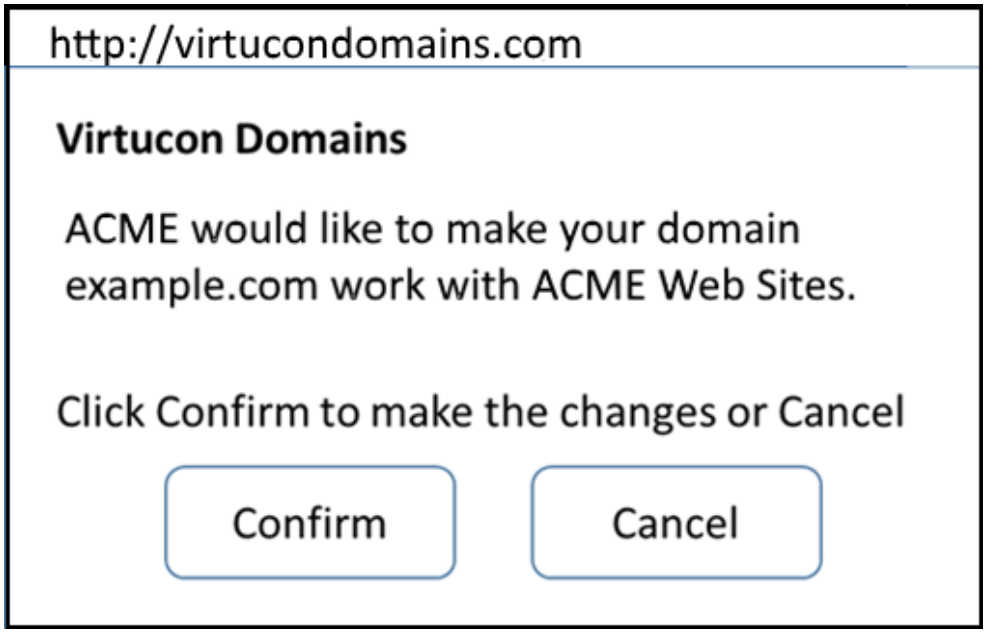


After clicking the link, the user is directed to a browser window on the DNS Provider's site. This is typically done in another tab or in a new browser window, but can also be an in place navigation with a return url. This link would pass the domain name being modified, the service provider and template being enabled, and any additional parameters needed to configure the service.

Once at the DNS Provider site, the user would be asked to authenticate if necessary.



After authenticating at the DNS Provider, the DNS Provider would verify the domain name is owned by the user. The DNS Provider would also verify other parameters passed in are valid and would prompt the user to give consent for making the change to DNS. The DNS Provider could also warn the user of services that would be disabled by applying this change to DNS.



Assuming the user grants this consent, the DNS changes would be applied.
Upon successful application of the DNS changes, if invoked in a pop-up window or tab the browser window would be closed. If in place the user would be redirected back to the service provider.

2.2 The Asynchronous Flow

The asynchronous OAuth flow is tailored for the Service Provider that wishes to make changes to DNS asynchronously with respect to the user interaction, or wishes to make multiple or additional changes to DNS over time.

The OAuth based authentication and authorization flow begins similarly to the web based synchronous flow. The Service Provider determines the DNS Provider and links to a consent dialog at the DNS Provider. Once at the DNS Provider the user signs in, the ownership of the domain is verified, and consent is granted.

Instead of applying the DNS changes on user consent, OAuth access is granted to the Service Provider. An OAuth access code is generated and handed back to the Service Provider. The Service Provider then requests an access (bearer) token.

The permission granted in the OAuth token is a right for the Service Provider to apply a requested template (or templates) to the specific domain (and its subdomains) owned by a specific user.

The Service Provider would later call the OAuth API to apply a template using the access token. This is a simple API that allows the application or removal of a template given authorization.
Additional parameters are expected to be passed as name/value pairs on the query string of each API call.

3 DNS Provider Discovery

In order to facilitate discovery of the DNS Provider from a domain name, a domain will contain a record in DNS.

This record will be a simple TXT record containing a URL used as a prefix for calling a discovery API. This record will be named *_domainconnect*.

An example of the contents of this record might contain:

```
domainconnect.virtucondomains.com
```

As a practical matter of implementation, the DNS Provider need not contain a copy of this data in each and every zone. Instead, the DNS Provider needs simply to respond to the DNS query for the *_domainconnect* TXT record with the appropriate data.

How this is implemented is up to the DNS Provider.

For example, the DNS Provider may not store the data inside a TXT record for the domain, opting instead to put a CNAME in the zone and have the TXT record in the target of the CNAME. Another DNS Provider might simply respond with the appropriate records without having the data in each zone.

Once the URL prefix is discovered, it is used by the Service Provider to determine the additional settings for using Domain Connect on this domain at the DNS Provider. This is done by calling a REST API.

```
GET
https://{_domainconnect}/v2/{domain}/settings
```

This will return a JSON structure containing the settings to use for Domain Connect on the domain name (passed in on the path) at the DNS Provider. This JSON structure will contain the following fields.

Field	Key	Type	Description
Provider Id	providerId	String	Unique identifier for the DNS Provider. Typically, the domain name (e.g. virtucom.com).
Provider Name	providerName	String	The name of the DNS Provider.
Provider Display Name	providerDisplayName	String	The name of the DNS Provider that should be displayed by the Service Provider. Note: This might change for some DNS Providers that white label their infrastructure.
UX URL Prefix for Synchronous Flows	urlSyncUX	String	The URL Prefix for linking to the UX of Domain Connect for the synchronous flow at the DNS Provider. If not returned, the DNS Provider is not supporting the synchronous flow on this domain.
UX URL Prefix for Asynchronous Flows	urlAsyncUX	String	The URL Prefix for linking to the UX elements of Domain Connect for the asynchronous flow at the DNS Provider. If not

			returned, the DNS Provider is not supporting the asynchronous flow on this domain.
API URL Prefix	urlAPI	String	This is the URL Prefix for the REST API
Width of Window	width	Number	This is the desired width of the window for granting consent when navigated in a popup. Default value is 750px.
Height of Window	height	Number	This is the desired height of the window for granting consent when navigated in a popup. Default value is 750px.

As an example, the JSON returned by this call might contain.

```
{
        "providerId":          "vicrucomdomains.com",
        "providerName":        "Virtucon Domains",
        "providerDisplayName": "Virtucon Domains",
        "urlSyncUX":           "https://domainconnect.virtucondomains.com",
        "urlAsyncUX":          "https://domainconnect.virtucondomains.com",
        "urlAPI":              "https://api.domainconnect.virtucondomains.com",
        "width":               750,
        "height":              750
}
```

Discovery should work on the root domain (zone) only.

It should be noted that it is possible a zone returns a value for the _domainconnect TXT record query, but that a subsequent call for the JSON fails. For example, a zone may errantly have a value for this record. Or a DNS Provider may decide to place the record in all zones, even for some where Domain Connect isn't enabled.

4 Domain Connect Details

4.1 Endpoints

The Domain Connect contains endpoints returned in the JSON during discovery are in the form of URLs.

The first set of endpoints are for the UX that the Service Provider links to. These are for the synchronous flow where the user can click link to grant consent for and to configure the domain, and for the asynchronous OAuth flow where the user can click to grant consent for OAuth access.

The second set of endpoints are for the API endpoints via REST.

All endpoints begin with a root URL for the DNS Provider such as:

```
https://connect.dnsprovider.com
```

They may also include any prefix at the discretion of the DNS Provider. For example:

```
https://connect.dnsprovider.com/api
```

The root URLs for the UX endpoints and the API endpoints are returned in the JSON payload during DNS Provider discovery.

4.2 Synchronous Flow

4.2.1 Query Supported Template

```
GET
{urlAPI}/v2/domainTemplates/providers/{providerId}/services/{serviceId}
```

This URL can be used by the Service Provider to determine if the DNS Provider supports a specific template through the synchronous flow.

Returning a status of 200 without a body indicates the template is supported. Returning a status of 404 indicates the template is not supported.

4.2.2 Apply Template

```
GET
{urlSyncUX}/v2/domainTemplates/providers/{providerId}/services/{serviceId}/apply?[prope
rties]
```

This is the URL used to ask for consent and to apply a template to a domain. It is called from the Service Provider to start the Domain Connect Protocol.

This URL can be called in two ways.The first is through a new browser tab or in a popup browser window. The DNS Provider would sign the user in if necessary, verify domain ownership, and ask for confirmation before application of the template. After application of the template, the DNS Provider would automatically close the browser tab or window.

The second is in the current browser tab/window. As above the DNS Provider would sign the user in if necessary, verify domain ownership, and ask for confirmation before application of the template. After application of the template (or cancellation by the user), the DNS Provider would redirect the browser to a return URL (redirect_uri).

The return_uri must be in a domain specified in syncRedirectDomain in the template.

Several parameters may be appended to the end of this return_uri.

- State

  If a state parameter is passed in on the query string, this will be passed back as state= on the return_uri

- Error

  If authorization could not be obtained or an error has occurred, the parametner error= will be appended. For consistency with the ascynronous OAuth flows the valid values for the error parameter will be as specified in OAuth 2.0 RFC 6749 (4.1.2.1. Error Response - "error" parameter). Valid values are: invalid_request, unauthorized_client, access_denied, unsupported_response_type, invalid_scope, server_error, and temporarilly_unavailable.

- Error Description

  When an error occurs, an optional error description containing a developer focused error description may be returned at the discretion of the DNS Provider.

  Most errors are due to configuration or usage problems. But under normal operation the access_denied error can be returned for a number of reasons. For example, the user may not have access to the account that owns the domain. Even if they do and successfully sign-in, the account or the domain may be suspended.

  It is unlikely that the DNS Provider would want to leak this information to the Service Provider, and as such the description may be vague.

  There is one piece of information that may be interesting to communicate to the Service Provider. This is when the end user decides to cancel the operation. Should the DNS Provider wish to communicate this to the Service Provider, when the error=access_denied the error_description can contain the prefix “user_cancel”. Again, this is left to the discretion of the DNS Provider.

It is also strongly recommended that the DNS Provider warn the user of existing settings that would change and/or services that would be disrupted as part of

applying this template. The fidelity of this warning is left to the DNS Provider. The only requirement is that after application of the template the new service is enabled.

More details on recommendations for conflict detection are outlined below in the section 6 on Templates.

Parameters/properties passed to this URL include:

Property	Key	Description
Domain	domain	This parameter contains the domain name being configured. This is the root domain, typically the registered domain or delegated zone.
Host	host	This is an optional host name of the sub domain. If left blank, the template is being applied to the root domain. Otherwise the template is applied to the sub domain within the domain.
Redirect URI	redirect_uri	The location to direct the client browser to upon successful authorization, or upon error. The parameter is optional, and if omitted the DNS Provider will close the browser window upon completion. It must be scoped to the syncRedirectDomain from the template.
State	state	OPTIONAL but recommended. This is a random, unique string passed along to prevent CSRF. It will be returned as a parameter when redirecting to the redirect_uri described above.
Name/Value Pairs	Any key that will be used as a replacement for the "% surrounded" value(s) in a template.	Any variable fields consumed by this template. The name portion of this API call corresponds to the variable(s) specified in the template and the value corresponds to the value that should be used when applying the template.
Group Id	groupId	This OPTIONAL parameter specifies the group of changes from the template to apply. If no group is specified, all groups are applied. Multiple groups can be specified in comma delimited format.
Provider Name	providerName	This OPTIONAL parameter specifies the provider name for display in the UX. It allows for application of a template for a service that is sold through different companies. Not all templates allow for this capability. See Shared Templates below.
Signature	sig	An OPTIONAL signature of the query string. See Security Considerations section below.
Key	key	An OPTIONAL value containing the host in DNS where the public key for the signature can be obtained. The domain for this host is in the template in syncPubKeyDomain.

An example query string is below:

```
GET https://web-
connect.dnsprovider.com/v2/domainTemplates/providers/coolprovider.com/services/hos
ting/apply?www=192.168.42.42&m=192.168.42.43&domain=example.com
```

This call indicates that the Service Provider wishes to connect the domain example.com to the service using the template identified by the composite key of the provider (coolprovider.com) and the service owned by them (hosting). In this example, there are two variables in this template, "www" and "m" which both require values (in this case each requires an IP address). These variables are passed as name/value pairs.

4.2.3 Security Considerations

By applying a template with parameters, there is a security consideration that must be taken into account.

Consider an email template where the IP address of the MX record is passed in through a variable. A bad actor could generate a URL with a malicious IP and phish the user. If an end user is convinced to click on this link, they would land on the DNS Provider site to confirm the change. To the user, this would appear to be a valid request to configure the domain. Yet the IP would be hijacking the service.

Not all templates have this problem. But when they do, there are two options.

One option would be to not enable the synchronous flow and use asynchronous OAuth. While this can be controlled with the syncBlock value from the template, as will be seen below OAuth has both a higher implementation burden and requires onboarding between each Service and DNS Provider.

The second option would be to digitally sign the query string. The signature will be appended as an additional query string parameter, properly URL encoded and of the form:

```
sig=NLOQQm6ikGC2FlFvFZqIFNCZqlaC4B%2FQDwS6iCwIElMWhXMgRnRE17zhLtdLFieWkyqKa4I%2FOo
FaAgd%2FAl%2ByzDd3sM2X1JVF5ELjTlj84jZ4KOEIdnbgkEeO%2FTkYRrPkwcmcHMwc4RuX%2Fqio8vKY
xJaKLKeVGpUNSKo7zkq3XIRgyxoLSRKxmlSTHFAz4LvYXPWo6SHDoVcRvElWj18Um13sSXuX4KhtOLym2y
ImHpboEi4m2Ziigc%2BNHZE0VvHUR7wZgDaB01z8hFm5ATF%2B8swjandMRf2Lr4Syv4qTxMNT61r62EWF
kt5t9nhxMgss6z4pfDVFZ3vYwSJDGuRpEQ%3D%3D
```

The Service Provider can generate this signature using a private key. The DNS Provider can then verify the signature using the public key.

The public key will be placed in a TXT DNS Record in a domain specified in the template. To allow for key rotation, the host name of the TXT record will be appended as another variable on the query string of the form:

```
key=_dcpubkeyv1
```

This example indicates that the public key can be found by doing a DNS query for a TXT record called _dcpubkeyv1 in the domain specified in the syncPubKeyDomain from the template.

Since the public key may be greater than 255 characters, multiple TXT records may exist for the DNS TXT query. For a public key of:

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1dCqv7JEzUOfbhWKB9mTRsv3O9Vzy1Tz3UQlID
GpnVrTPBJDQTXUhxUMREEOBKo+rOjHZqfYnSmlkgu1dnBEO8bsELQL8GjS4zsjdA53gRk2SDxuzcB4fK+N
CDfnRHut5nG0S3U4cq4DuGrMDFVBwxH1duTsqDNgIOOfNTsFcWSVXoSSTqCCMGbj8Vt51umDhWQAj06lf5
0qP2/jMNs2G+KTlk3dBHx3wtqYLvdcop1Tk5xBD64BPJ9uwm8KlDNHe+8O+cC9j04Ji8B2K0/PzAj90xnb
8XJy/EM124hpT9lMgpHKBUvdeurJYweC6oP41gsTf5LrpjnyIy9j5FHPCQIDAQAB
```

There would be several TXT records. The records would be of the form:

- `p=1,a=RS256,t=x509,d=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1dCqv7JEzUOfbhWKB 9mTRsv3O9Vzy1Tz3UQlIDGpnVrTPBJDQTXUhxUMREEOBKo+rOjHZqfYnSmlkgu1dn`
- `p=2,a=RS256,t=x509,d=BEO8bsELQL8GjS4zsjdA53gRk2SDxuzcB4fK+NCDfnRHut5nG0S3U4cq4DuGr MDFVBwxH1duTsqDNgIOOfNTsFcWSVXoSSTqCCMGbj8Vt51umDhWQAj06lf5`
- `p=3,a=RS256,t=x509,d=NCDfnRHut5nG0S3U4cq4DuGrMDFVBwxH1duTsqDNgIOOfNTsFcWSVXoSSTqCC MGbj8Vt51umDhWQAj06lf50qP2/jMNs2G+KTlk3dBHx3wtqYLvdcop1Tk5xBD64BPJ9`
- `p=4,a=RS256,t=x509,d=uwm8KlDNHe+8O+cC9j04Ji8B2K0/PzAj90xnb8XJy/EM124hpT9lMgpHKBUvd eurJYweC6oP41gsTf5LrpjnyIy9j5FHPCQIDAQAB`

Here the public key is broken into four records in DNS, and the data also indicates that the signing algorithm is an RSA Signature with SHA-256 using an x509 certificate. The value for “a” if omitted will be assumed to be RS256, and for “t” will be assumed to be x509.

It should be noted that the above data was generated for a query string:

```
a=1&b=2&ip=10.10.10.10&domain=foobar.com
```

Support for signing the query string and verification is optional. Not all services require this level of security. Presence of the syncPubKeyDomain in the template indicates that the template requires signature verification.

The digital signature will be generated on the full query string excluding the sig and key parameters. The values of each query string value will be properly URL Encoded before the signature is generated.

4.2.1 Shared Templates

Most services are enabled and sold by the same company. However, some Service Providers have a reseller channel. This allows the service to be provided by the Service Provider, but sold through third party resellers. It is often this third party reseller that configures the service.

While each reseller could enable Domain Connect, this is inefficient for the DNS Providers. Enabling a single template that is shared by multiple resellers would be more ideal.

To facilitate this, the ability to pass in the name of the reseller in the synchronous flow is provided for some templates. This allows the DNS Provider to display the name of the reseller in the confirmation user experience.

As an example, the message can now read "(Reseller) XYZ would like to make your domain example.com work with ACME Websites."

In this example, ACME Websites is a service provided by ACME but resold through XYZ.

This should only work for templates that have set the "shared" attribute to true.

4.2.2 Verification of Changes

There are circumstances where the Service Provider may wish to verify that the template was successfully applied. Without domain connect, this typically involved the Service Provider querying DNS to see if the changes to DNS had been made.

This same technique works with Domain Connect, and if necessary can be triggered either manually on the Service Provider site or automatically upon page/window activation in the browser when the browser window for the DNS Provider is closed.

When the redirect_uri is used and an error is not present in the URI, the Service Provider can assume the changes were correctly applied and will be published into DNS. It should be noted that that due to the nature of DNS the changes may not be immediately visible due to the latency of DNS based on the TTL.

4.3 Asynchronous Flow: OAuth

Using the OAuth flow is a more advanced use case needed by Service Providers that have more complex configurations that may require multiple steps and/or are asynchronous from the user's interaction.

Details of an OAuth implementation are beyond the scope of this specification. Instead, an overview of how OAuth is used by Domain Connect is given here.

4.3.1 OAuth Flow: Setup

Service providers wishing to use the OAuth flow must register as an OAuth client with the DNS provider. This is envisioned as a manual process.

To register, the Service Provider would provide (in addition to their template) any parameters necessary for the DNS Providers OAuth implementation. This includes valid URLs and Domains for redirects upon success or errors.

The OAuth specification gives several options for the registration of return uris, including the registration of fully qualified uris, partial uris, or no uris. For Domain Connect to work consistently across providers, it is recommended that the client

register one more more host names to be validated with against a fully qualified uri passed into the call for getting an authorization code.

In return, the DNS provider will give the Service Provider a client id and secret which will be used when requesting tokens. It is also recommended that the client id is the same as the providerId.

4.3.2 OAuth Flow: Getting an Authorization Code

```
GET
{urlAsyncUX}/v2/domainTemplates/providers/{providerId}
```

To initiate the OAuth flow the Service Provider would link to the DNS Provider to gain consent.

This endpoint is similar to the synchronous flow described above, and will handle authenticating the user, verification of domain ownership, and asking for the user's permission to allow the Service Provider to make the specified changes to the domain on their behalf. Similarly the DNS Provider will often want to warn the user that (eventual) application of a template might change existing records and/or disrupt existing services attached to the domain.

While the variables for the applied template would be provided later, the values of some variables are necessary to determine conflicts. As such, any variables impacting conflicting records needs to be provided in the consent flow. Today this includes variables in hosts, and variables in the data portion for certain TXT records. As conflict resolution evolves, this list may grow.

The protocol allows for the Service Provider to gain consent for the application of multiple templates (specified in the scope parameter) applied to multiple domains/sub-domains (specified in the domain and host parameter). If conflict detection is implemented by the DNS Provider, they should account for all permutations.

The scope parameter is a space separated list of the templates (as per the OAuth protocol). The host parameter is an optional comma separated list of hosts. A blank entry for the host implies the template can be applied to the root domain. For example:

Query String	Description
scope=t1+t2&domain=example.com	Templates "t1" and "t2" can be applied to example.com
scope=t1+t2&domain=example.com&host=sub1,sub2	Templates "t1" and "t2" can be applied to sub1.example.com or sub2.example.com

scope=t1+t2&domain=example.com&host=sub1,	Templates “t1” and “t2” can be applied to example.com or sub1.example.com

Upon successful authorization/verification/consent from the user, the DNS Provider will direct the end user’s browser to the redirect URI. The authorization code will be appended to this URI as a query parameter of “code”.

Similar to the synchronous flow, upon error the DNS provider will append an error code as query parameter “error”. These errors are also from the OAuth 2.0 RFC 6749 (4.1.2.1. Error Response - "error" parameter). Valid values include: invalid_request, unauthorized_client, access_denied, unsupported_response_type, invalid_scope, server_error, and temorarilly_unavailable. An optional error_description suitable for developers can also be returned at the discretion of the DNS Provider. The same considerations as in the synchronous flow apply here.

The state value passed into the consent will be passed back on the query string as “state=”.

The following table describes the values to be included in the query string parameters for the request for the OAuth consent flow.

Property	Key	Description
Domain	domain	This parameter contains the domain name being configured. This is the root domain, typically the registered domain or delegated zone.
Host	host	This is an optional list of comma separated host names upon which the template may be applied. An empty string implies the root.
Client Id	client_id	This is the client id that was provided by the DNS provider to the service provider during registration. It is recommended that this be the same as the providerId in the template.
Redirect URI	redirect_uri	The location to direct the client’s browser upon successful authorization, or upon error. Validation of the redirect_uri will be done by verifying the host (domain) name matches registered hosts as part of onboarding.
Response type	response_type	OPTIONAL. If included should be the string ‘code’ to indicate an authorization code is being requested.
Scope	scope	The OAuth scope corresponds to the requested templates. This is list of space separated serviceIds.
State	state	OPTIONAL but recommended. This is a random, unique string passed along to prevent

		CSRF. It will be returned as a parameter when redirecting to the redirect_url described above.
Name/Value Pairs	Any key that will be used as a replacement for the "% surrounded" value(s) in a template required for conflict detection.	Required for fields that impact the conflict detection. This includes variables used in hosts and data in TXT records.

4.3.3 OAuth Flow: Requesting an Access Token

```
POST
{urlAPI}/v2/oauth/access_token
```

Once authorization has been granted the Service Provider must use the Authorization Code provided to request an Access Token. The OAuth specification recommends that the Authorization Token be a short lived token, and a reasonable recommended setting is ten minutes. As such this exchange needs to be completed before that time has expired or the process will need to be repeated.

This token exchange is done via a server to server API call from the Service Provider to the DNS Provider.

The Access Token granted will also have a longer lifespan, but also can expire. To get a new access token, the Refresh Token is used.

The request for the access token is done via a POST to a well-known path of the urlAPI from the JSON. However, care must be taken here because a secret is sent with this POST. A malicious user could return false JSON information in their domain, allowing them to hijack this request. When called they could steal the server secret.

Instead of using the urlAPI from a runtime query, the Service Provider should maintain a table mapping the DNS Provider to the proper URL. This will involve storage of the urlAPI per DNS Provider, but can sit alongside the secret that is stored per DNS Provider.

The following table describes the POST parameters to be included in the request for the access token.

Property	Key	Description
Authorization Code/Refresh Code	code	The authorization code that was provided in the previous step when the customer accepted the authorization request, or the refresh_token for a subsequent access token.
Redirect URI	redirect_uri	This is required if a redirect_uri is passed to request the authorization code. When included, it needs to be the same redirect_uri provided in this step.
Grant type	grant_type	The type of code in the request. Usually the string 'authorization_code' or 'refresh_token'

Client ID	client_id	This is the client id that was provided by the DNS provider, to the Service Provider during registration
Client Secret	client_secret	The secret provided to the Service Provider during registration

Upon successful token exchange, the DNS Provider will return a response with 4 properties in the body of the response.

Property	Description
access_token	The access token to be used when making API requests
token_type	Always the string "bearer"
expires_in	The number of seconds until the access_token expires
refresh_token	The token that can be used to request new access tokens when this one has expired.

4.3.4 OAuth Flow: Making Requests with Access Tokens

Once the Service Provider has the access token, they can call the DNS Provider's API to make change to DNS on the domain by applying and removing authorized templates. These templates can be applied to the root domain or to any sub-domain of the root domain authorized.

All calls to this API pass the access token in the Authorization Header of the request to the call to the API. More details can be found in the OAuth specifications, but as an example:

```
GET /resource/1 HTTP/1.1
Host: example.com
Authorization: Bearer mF_9.B5f-4.1JqM
```

While the calls below do not have the same security consideration of passing the secret, it is recommend that the urlAPI be from a stored value vs. the runtime query for these as well.

4.3.5 OAuth Flow: Apply Template to Domain.

```
POST
{urlAPI}/v2/domainTemplates/providers/{providerId}/services/{serviceId}/apply?[properti
es]
```

The primary function of the API is to apply a template to a customer domain.

While the providerId is implied in the authorization, this is on the path for consistency with the synchronous flows and other APIs. If not matching what was authorized, an error would be returned.

When applying a template to a domain, it is possible that a conflict may exist with previous settings. While it is recommended that conflicts be detected when the user

grants consent, because OAuth is asynchronous it is possible that a new conflict was introduced by the user.

While it is up to the DNS Provider to determine what constitutes a conflict (see section on Conflicts below), when one is detected calling this API should return an error. This error will enumerate the conflicting records in a format described below.

Because the user isn't present at the time of this error, it is up the Service Provider to determine how to handle this error. Some providers may decide to notify the user. Others may decide to apply their template anyway using the "force" parameter. This parameter will bypass error checks for conflicts, and after the call the service will be in its desired state.

Calls to apply a template via OAuth require the following parameters:

Property	Key	Description
Domain	domain	This contains the root domain name being configured. It must match the domain that was authorized in the token.
Host	host	This is the host name of the sub domain of the root domain. If omitted or left blank, the template is being applied to the root domain.
Name/Value Pairs	Any key that will be used as a replacement for the "% surrounded" value(s) in a template.	Any variable fields consumed by this template. The name portion of this API call corresponds to the variable(s) specified in the record and the value corresponds to the value that should be used when applying the template as per the implementation notes.
Group ID	groupId	This OPTIONAL parameter specifies the group of changes in the template to apply. If omitted, all changes are applied. This can also be a comma separated list of groupIds.
Force	force	This OPTIONAL parameter specifies that the template should be applied independently of any conflicts that may exist on the domain. This can be a value of 0 or 1.

An example call is below. In this example, it is contemplated that there are two variables in this template, "www" and "m" which both require values (in this case each requires an IP address). These variables are passed as name/value pairs.

```
POST
https://connect.dnsprovider.com/v2/domainTemplates/providers/coolprovider.com/serv
ices/hosting/apply?www=192.168.42.42&m=192.168.42.43&force=1
```

The API must validate the access token, and that the domain belongs to the customer and is represented by the token being presented. Any errors with variables, conflicting templates, or problems with the state of the domain are returned and returned; otherwise the template is applied.

Results of this call can include information indicating success or an error. Errors will be 400 status codes, with the following codes defined.

Status	Response	Description
Success	20*	A response of an http status code of 204 indicates that call was successful and the template applied. Note that any 200 level code should be considered a success.
Unauthorized	401	A response of a 401 indicates that caller is not authorized to make this call. This can be because the token was revoked, or other access issues.
Error	400, 404, 422	This indicates something wrong with the request itself, such as bad parameters.
Failed	409	This indicates that the call was good, and the caller authorized, but the change could not be applied due to a conflicting template. Errors due to conflicts will only be returned when force is not equal to 1.

When a 409 is returned, the body of the response will contain details of the error. This will be JSON containing the error code, a message suitable for developers, and an array of tuples containing the conflicting records type, host, and data element.

As an example:

```
{
     "code": "409",
     "message": "Conflicting records",
     "records": [
             {
                     "type": "CNAME",
                     "host": "www",
                     "data": "@"
             },
             {
                     "type": "A",
                     "host": "@",
                     "data": "random ip"
             }
     ]
}
```

In this example, the Service Provider tried to apply a new hosting template. The domain had an existing service applied for hosting.

4.3.6 OAuth Flow: Revert Template

This call reverts the application of a specific template from a domain.

```
POST
{urlAPI}/v2/domainTemplates/providers/{providerId}/services/{serviceId}/revert?dom
ain={domain}&host={host}
```

This API allows the removal of a template from a customer domain/host using an OAuth request.

The provider and service name in the authorization token must match the values in the URL.

This call must validate that the template requested exists and has been applied to the domain by the Service Provider, or a warning must be returned that the call would have no effect.

An example query string might look like:

```
POST
https://connect.dnsprovider.com/v2/domainTemplates/providers/coolprovider.com/services/hosting/revert?domain=example.com
```

Response codes Success, Authorization, and Errors are identical to above.

4.3.7 OAuth Flow: Revoking access

Like all OAuth flows, the user can revoke the access at any time using UX at the DNS Provider site. As such the Service Provider needs to be aware that their access to the API may be denied.

5 Domain Connect Objects and Templates

5.1 Template Versioning

Templates are not versioned. Instead, if a breaking change is made to a template it is recommended that a new template be created. While on the surface versioning looks appealing, the reality is that the settings in a template rarely change. This is because a successful service will have many customers with settings in their DNS, some applied by templates using this protocol, and some manually applied. As such changes to the template need to be done in a manner that accounts for existing customers.

For some template changes such as the addition of a new record, the template is largely backward compatible. With the caveats that the template would need to be on-boarded with the DNS Providers and that only new applications of the template would have the change.

5.2 Template Definition

A template is defined as a standard JSON data structure containing the following data:

Data Element	Type	Key	Description
Service Provider Id	String	providerId	The unique identifier of the Service Provider that created this template. This is used in the URLs to identify the Service Provider. To ensure non-

			coordinated uniqueness, it is recommended that this be the domain name of the Service Provider.
Service Provider Name	String	providerName	The name of the Service Provider. This may be displayed to the user on the DNS Provider consent UX.
Service Id	String	serviceId	The name or identifier of the template. This is used in URLs to identify the template. It is also used in the scope parameter for OAuth. It should not contain space characters.
Service Name	String	serviceName	The friendly name of this service. This may be displayed to the user.
Logo	String	logoUrl	A graphical logo for use in any web-based flow. This is a URL to a graphical logo sufficient for retrieval.
Description	Text	description	A textual description of what this template attempts to do. This is meant to assist integrators, and therefore should not be displayed to the user.
Synchronous Block	Boolean	syncBlock	Indicates that the synchronous protocol should not be enabled for this template. The default for this is false.
Shared	Boolean	shared	Indicates that the template is shared and the provider name can be passed in on the query string. The default for this is false.
Synchronous Public Key Domain	String	synchPubKeyDomain	When present, indicates that calls to apply a template synchronously will be digitally signed. This element contains the domain name for querying the TXT record from DNS that contains the public key information.
Synchronous Redirect Domain	String	syncRedirectDomain	(optional) When present, this is the domain name for which redirects must be sent to with the response for the configuration. The domain from the providerId is also allowed.
Template Records	Array of Template Records	records	A list of records for the template.

5.3 Template Record

Each template record is an entry that contains a type and several optional parameters based on the value.

For all entries of a record other than “type” and “groupId”, the value can contain variables denoted by %<variable name>%. These are the values substituted at runtime when writing into DNS.

It should be noted that as a best practice, the variable should be equal to the portion of the values in the template that change as little as possible.

For example, say a Service Provider requires a CNAME of one of three values for their users: s01.example.com, s02.example.com, and s03.example.com.

The value in the template could simply contain %servercluster%, and the fully qualified string passed in. Alternatively, the value in the template could contain s%var%.example.com. By placing more fixed data into the template, the data is more constrained.

Each record will contain the following elements.

Data Element	Type	Key	Description
Type	enum	type	Describes the type of record in DNS, or the operation impacting DNS. Valid values include: A, AAAA, CNAME, MX, TXT, SRV, NS, APEXCNAME, REDIR301, or REDIR 302 For each type, additional fields would be required. A: host, pointsTo, TTL AAAA: host, pointsTo, TTL CNAME: host, pointsTo, TTL TXT: host, data, TTL MX: host, pointsTo, priority, TTL SRV: name, target, protocol, service, priority, weight, port, TTL
Group Id	String	grouping	This OPTIONAL parameter identifies the group the record belongs to when applying changes.
Host	String	host	The host for A, AAAA, CNAME, TXT, and MX values. This is the hostname in DNS.
Points To	String	pointsTo	The pointsTo location for A, AAAA, CNAME, and MX records.
TTL	Int	ttl	This is the time-to-live for the record in DNS. Valid for A, AAAA, CNAME, TXT, MX, and SRV records
Data	String	data	This is the data for a TXT record in DNS
Priority	Int	priority	This is the priority for an MX or SRV record in DNS.
Weight	Int	weight	This is the weight for the SRV record
Port	Int	port	This is the port for the SRV record
Protocol	String	protocol	This is the protocol for the SRV record
Service	String	services	This is the protocol for the SRV record

6 Template Considerations

6.1 Disclosure of Changes and Conflicts

It is left to the DNS Provider to determine what is disclosed to the user regarding changes being made to DNS and of potential conflicts. This can happen at multiple points in time.

For the synchronous flow this happens when the template is being applied.

For the asynchronous flow this happens when permissions are granted to make changes to DNS on the user's behalf (OAuth). Detection of conflicts also happens when the API is called to apply the template in the form of an error response code when the "force" parameter is not set to 1.

For disclosure of changes being made to DNS, one DNS Provider may decide to simply tell the user the name of the service being enabled. Another may decide to display the records being/that will be set. And another may progressively display both.

The template can also conflict with existing records and other templates already applied on the domain. Some DNS Providers may simply overwrite changed records without warning. Others may warn the users of the records that will change. And others may implement logic to further remove any the existing templates that overlap with the new template *. Again this may be progressively displayed.

* As an example, example, consider a template that set two records in DNS (recordA and recordB). Next consider applying a new template that overlaps with the first template (recordB and recordC). If the DNS Provider removes conflicting templates when applying new ones, upon application of the second template the first template would be removed. This would result in recordA being cleared, and only recordB and recordC being set.

Manual changes made by the user at the DNS Provider may also have appropriate warnings in place to prevent unwanted changes as well; with overrides being possible and removal of conflicting templates.

It is ultimately left to the DNS Provider to determine the amount of disclosure and/or conflict detection. The only requirement is that after a template is applied the new service is enabled. However, a reasonable set of recommendations would consist of:

- The consent UX should inform the customer of the service that will be enabled. Should the customer want to know the specifics, the DNS Provider could provide a "show details" link to the user. This could display to them the specific records that are being set in DNS.

- If there are conflicts, either at the template or record level, the consent UX should warn the user about these conflicts. For templates this would be services that would be disabled. For records this would be records that would be overwritten. This could be progressively disclosed

Note: When applying the same template, DNS Providers should not detect the conflict. Instead the first template would be removed and the new instance applied. For most templates this is a benign operation. Unless the template contains variables in host names. For consideration of this, see the section below.

6.2 Record Types and Conflicts

A proposed handling of records and conflicts is as follows (if not otherwise specified, conflicts occur if the records have the same name):

- Replace records of the same type for A, AAAA, MX, CNAME, APEXCNAME, SRV. If the template specifies an A or AAAA, the respective AAAA or A record should be removed to avoid IPv4 and IPv6 pointing to different services
- Append to the existing records of the same type for TXT
    - An exception exists for records of unique nature like SPF or DKIM which should be replaced
- Replace any record for CNAME
- Remove any CNAME record existing at the same or parent level to any records added by the template

6.3 Template Scope

An individual template is scoped to the set of records applied to a fully qualified domain. This includes the root domain and the host or sub-domain.

As an example, applying a template on domain=example.com&host=sub1 and later applying the template on domain=example.com&host=sub2 will be treated as two distinct templates. Should a conflict be detected later while applying a template with the records set into “sub2.example.com”, only the records set with this template would be removed.

6.4 Variables and Host Considerations

Templates do allow for variables in a host name. However, these should be used sparingly.

As an example, consider setting up hosting for a site. But instead of applying the template to a sub-domain, the name of the sub-domain is placed as a variable in the template.

Such a template might contain an A record of the form:

```
{
        “type”:  “A”,
        “host”: “%var%”,
        “pointsTo”: “2.2.2.2”,
        “ttl”: 1800
}
```

This template could be applied on the domain example.com with a variable for “sub”, “sub1”, “sub2”, etc.

However, application of this template would be at the domain level for “example.com”. Re-application of this template would remove all records previously set by the template.

So application of this template on “example.com” with the var=sub would result in the A record for sub.example.com to the value 2.2.2.2. But later applying the template on “example.com” with the var=sub2 would first remove the old template, and set the new one. Sub.example.com would be removed, and sub2.example.com would be set to the value 2.2.2.2.

While removing variables in host entries entirely from the specification would prevent this type of problem from occurring, there are some templates that utilize CNAME values containing user identification for validation of domain ownership. For practical purposes these values do not conflict with other services or sub-domains being configured and are seen as reasonable.

As such, variables remain applicable to the host name but for very limited circumstances.

6.5 Repository and Integrity

This template format is intended largely for documentation and communication between the DNS Providers and Service Providers, and there are no codified endpoints for creation or modification of these objects. Instead, Domain Connect references a template by ID.

As such, DNS Providers may or may not use templates in this format in their internal implementations.

However, by defining a standard template format it is believed it will make it easier for Service Providers to share their configuration across DNS Providers. Further revisions of this specification may include a repository for publishing and consuming these templates. For now templates are maintained at http://domainconnect.org

Implementers are responsible for data integrity and should use the record type field to validate that variable input meets the criteria for each different data type.

Hard-coded host names are the responsibility of the DNS Provider to protect. That is, DNS Providers are responsible for ensuring that host names do not interfere with known values (such as m. or www. or mail.) or internal names that provide critical functionality that is outside the scope of this specification.

7 Extensions/Exclusions

Additional record types and/or extensions to records in the template can be implemented on a per DNS Provider basis. However, care should be taken when defining extensions so as to not conflict with other protocols and standards. Certain record names are reserved for use in DNS for protocols like DNSSEC (DNSKEY, RRSIG) at the registry level.

Defining these optional extensions in an open manner as part of this specification is highly recommended. The following are the initial optional extensions a DNS Provider/Service Provider may support.

7.1.1 APEXCNAME

Some Service Providers desire the behavior of a CNAME record, but in the apex record. This would allow for an A Record at the root of the domain but dynamically determined at runtime.

The recommended record type for DNS Providers that wish to support this is an APEXCNAME record. Additional fields included with this record would include pointsTo and TTL.

Defining a standard for such functionality in DNS is beyond the scope of this specification. But for DNS Providers that support this functionality, using the same record type name across DNS Providers allows template reuse.

7.1.2 Redirection

Some Service Providers desire a redirection service associated with the A Record. A typical example is a service that requires a redirect of the domain (e.g. example.com) to the www variant (www.example.com). The www would often contain a CNAME.

Since implementation of a redirection service is typically simple, it is recommended that service providers implement redirection on their own. But for DNS Providers that have a redirection service, supporting simple templates with this functionality may be desired.

While technically not a “record” in DNS, when supporting this optional functionality it is recommended that this be implemented using two new record types.

REDIR301 and REDIR302 would implement 301 and 302 redirects respectively. Associated with this record would be a single field called the “target”, containing the target domain of the redirect.

Setting a REDIR301 or REDIR302 will internally set an A Record on the domain.

7.1.3 Nameservers

Several service providers have asked for functionality supporting an update to the nameserver records at the registrar associated with the domain.
When implementing this, two records should be provided. NS1 and NS2, each containing a pointsTo argument.

It will be noted that a nameserver update would require that the DNS Provider is the registrar. This is not always the case.

This functionality is again deemed as optional and up to the DNS Provider to determine if they will support this.

7.1.4 DS (DNSSEC)

Requests have also been made to allow for updates to the DS record for DNSSEC. This record is required at the registry to enable DNSSEC, but can only be written by the registrar.

For DNS Providers that support this record, the record type should be DS. Values will be keyTag, algorithm, digestType, and digest.

Again it should be noted that a DS update would require that the DNS Provider is the registrar, and is again deemed as optional and up to the DNS Provider to determine if they will support.

8 Example Templates

Example Template

```
{
        "providerId": "example.com",
        “providerName”: “Example Web Hosting”,
        "serviceId": "hosting",
        “serviceName”: “Wordpress by example.com”,
        “logoUrl”: “https://www.example.com/images/billthecat.jpg”,
        “description”: “This connects your domain to our super cool web hosting”,
        “launchURL” : https://www.example.com/connectlaunch,
        "records": [
                {
                        “groupId” : “service”,
                        “type”: “A”,
                        “host”: “www”,
                        “pointsTo”: “%var1%”,
                        “ttl”: “%var2%”
                },
                {
                        “groupId” : “service”,
                        “type”: “A”,
```

```
                "host": "m",
                "pointsTo": "%var3%",
                "ttl": "%var2%"
        },
        {
                "groupId" : "service",
                "type": "CNAME",
                "host": "webmail",
                "pointsTo: "%var4%",
                "ttl": "%var2%"
        },
        {
                "groupId" : "verification",
                "type": "TXT",
                "host": "example",
                "data: "%var5%",
                "ttl": "%var2%"
        }

    ]

}
```

Example Records: Single static host record

Consider a template for setting a single host record. The records section of the template would have a single record of type "A" and could have a value of:

```
    [{
            "type": "A",
            "host": "www",
            "pointsTo": "192.168.1.1",
            "ttl":  600
    }]
```

This would have no variable substitution and the application of this template to a domain would simply set the host name "www" to the IP address "192.168.1.1"

Example Records: Single variable host record for A

In the case of a template for setting a single host record from a variable, the template would have a single record of type "A" and could have a value of:

```
    [{
            "type": "A",
            "host": "@",
            "pointsTo": "192.168.1.%srv%",
            "ttl":  600
    }]
```

A query string with a key/value pair of

```
srv=2
```

would cause the application of this template to a domain to set the host name for the apex A record to the IP address "192.168.1.2" with a TTL of 600

Example: DNS Zone merging

Consider a following DNS Zone before a template application:

```
$ORIGIN test-domain.com.
@       3600    IN      SOA     ns11.acme.net. support.acme.net. 2017050817 7200
1800 1209600 3600
@       3600    IN      NS      ns11.acme.net.
@       3600    IN      NS      ns12.acme.net.
@       3600    IN      A       1.1.1.1
@       3600    IN      A       1.1.1.2
@       3600    IN      AAAA    2001:db8:1234:0000:0000:0000:0000:0000
@       3600    IN      AAAA    2001:db8:1234:0000:0000:0000:0000:0001
@       3600    IN      MX      10 mx1.acme.net.
@       3600    IN      MX      10 mx2.acme.net.
@       3600    IN      TXT     "v=spf1 a include: spf.acme.com ~all"
www     3600    IN      CNAME   other.host.com.
```

Now application of the following template:

```
[
        {
            "type":"A",
            "host":"@",
            "pointsTo":"2.2.2.2",
            "ttl":"1800"
        },
        {
                "type":"A",
                "host":"www",
                "pointsTo":"2.2.2.2",
                "ttl":"1800"
        },
        {
                "type":"TXT",
                "host":"@",
                "data":"\"v=spf1 a include: spf.hoster.com ~all\"",
                "ttl":"1800"
        }
]
```

The following DNS Zone shall be generated after the template is applied:

```
$ORIGIN test-domain.com.
@       3600    IN      SOA     ns11.acme.net. support.acme.net. 2017050920 7200
1800 1209600 3600
@       3600    IN      NS      ns11.acme.net.
@       3600    IN      NS      ns12.acme.net.
@       1800    IN      A       2.2.2.2
@       3600    IN      MX      10 mx1.acme.net.
@       3600    IN      MX      10 mx2.acme.net.
@       1800    IN      TXT     "v=spf1 a include: spf.hoster.com ~all"
www     1800    IN      A       2.2.2.2
```