GlobalSign ACME Implementation Guide

May 2024

Table of Contents

Overview **3**

Getting Started **3**

Atlas Onboarding Process 3

ACME Client Selection 5

External Account Binding 5

Certificate Management **5**

Domain Validation and Certificate Issuance 6

HTTP Validation 6

DNS Validation 6

Domain Reuse Period 6

Other Domain Validation Methods 7

Domain Validation for Subdomains 7

CSR Signature Algorithm 7

Revoke a Certificate 7

Renew a Certificate 7

Account Management **8**

Update Your Contact Email 8

Deactivate Your Account 8

Account Key Rollover 8

Technical Addendum **9**

Certbot on NGINX 9

Domain Validation Using DNS CNAME Records 9

1. Update your DNS 9
2. Validate a Domain 10

ACME Directory Objects 10

Change Log

Version	Change
January 2022	First publication, featuring information about the GlobalSign ACME DV service and how it integrates with GlobalSign's PKI Platform Atlas. This version included a few FAQs
February 2022	• Added a technical addendum with information on how to do domain validation via DNS CNAME records, and how to use Certbot with NGINX. • Added more FAQs
July 2022	• Moved the FAQ to a dedicated Support website • Minor copy updates
March 2023	Added information about GlobalSign's new ACME OV service
December 2023	• Added information about new functionality that enables a user to change the email address associated with their ACME client account • Added information about new functionality that enables a user to deactivate their ACME client account
February 2024	• Added information about the hash algorithm that is used by our service for issuing certificates • Added an ACME Directory Objects section to the Technical Addendum
May 2024	• Added information on the implementation of the ACME Key Change endpoint according to RFC 8555 • Updated the subdomain verification process to incorporate a new backend logic change that bypasses subdomain verification if the parent domain already has a valid, active domain claim against it.

Overview

The ACME (Automated Certificate Management Environment) protocol is designed to automate certificate issuance, provisioning, renewal, and revocation processes by providing a framework for CAs to communicate with ACME clients installed on customer endpoints. Initially the protocol was designed by the Internet Security Research Group (ISRG) for its free public CA, Let's Encrypt. It has since been published as an internet standard (RFC 8555) and is available for use and adoption by anyone.

ACME is an extensible framework for automating certificate issuance and domain validation procedures. ACME allows users to conduct certificate management actions using a set of JavaScript Object Notation (JSON) messages carried over HTTPS. Issuance using ACME resembles a traditional CA's issuance process, in which a user creates an account, requests a certificate, and proves control of the domain(s) in that certificate for the CA to issue the requested certificate.

In GlobalSign's ACME service, customers set up an account on the GlobalSign Atlas platform and validate their organization information. You will need to link the ACME client with your Atlas account using ACME External Account Binding (EAB). Once EAB is completed, ACME is used to automatically request and issue CA/Browser Forum-compliant public-trust TLS certificates from Atlas without having to interface with the Atlas portal or APIs.

Getting Started

Atlas Onboarding Process

To begin, create an account on the GlobalSign Atlas portal.

1. Go to https://atlas.globalsign.com/register to register for an Atlas account. Once you create a username and password, you will receive an email to validate that account.
2. Open the email and click the link to validate your email address.
3. Login to Atlas with your username and password. You will be prompted to enter some business information.
4. At this point, please contact your GlobalSign Account Manager and provide them with your email address. Your Account Manager will prepare a quote for a TLS ACME service, and you will receive a notification when your quote is ready to review on your Atlas portal dashboard.
5. Review the quote, select the payment type, click-agree to the quote and Terms & Conditions, and then click **Place Order**.

6. Create an ACME Identity Profile. This is the object that all domains will be linked to. You may want to create one identity for testing or QA purposes and one for production use, which will keep the domains separate from each other.
    a. From the Atlas portal dashboard, navigate to **Identity Profiles**.
    b. Click **Request an Identity**.
    c. Select the relevant identity profile type - i.e., ACME (DV)
    d. Enter a friendly name for the identity profile.
    e. If you are a Service Provider, you will be asked to provide further details on the end customer's identity information.
    f. Click **Request this Identity** and then return to the portal dashboard.

    If you requested an ACME OV identity it will take 1-3 business days for our Vetting agents to process your request. You can check the status of your request in the Atlas portal. ACME DV identities are automatically validated.
7. Generate your API credentials and obtain the MAC key (also known as HMAC) so you can perform EAB with your ACME client. These credentials are used to bind your ACME client to your Atlas account.
    a. From the Atlas portal dashboard, navigate to **Access Credentials > API Credentials**.
    b. Click **Generate an API Credential**.
    c. Select how you will receive your credentials. We recommend using the **View and Copy** method.
    d. Select the ACME service with which these credentials will be used. Note the service will only appear after you have accepted the quote (step 5).
    e. Select the identity you created above.
    f. Enter a familiar name for these credentials (lower case only) to identify them later.
    g. Return to the API Credentials page and click **Request an ACME MAC** on the card for the credentials you just created.
    h. For EAB you will need the ACME MAC and the Key ID (which is the same as your API Key). Copy these values and store the MAC key in a secure location. The MAC key is valid for 30 days and up to 1000 uses. This will be your only chance to copy and save your MAC key.
    i. If you want to obtain a new MAC key to supersede your prior one, go to the API credentials page and select the three dots icon on your ACME credentials card and then click **Manage MAC Key**. From there you can request a new MAC which will be valid for 30 days and 1000 uses. This will immediately disable your prior MAC. Existing bound ACME clients will

continue to work, but you will not be able to use the MAC for new EAB actions.

ACME Client Selection

Select your preferred ACME client. Certbot is recommended, and the instructions in this guide are written for that client. Make sure you have the latest version installed on your web server before continuing.

External Account Binding

The final step is to register your GlobalSign Atlas account with your ACME client. With Certbot, this is typically done in the same command used to request a certificate and validate a domain.

You'll need the following to do EAB:

- MAC Key and Key ID from the API credentials page
- ACME URL: https://emea.acme.atlas.globalsign.com/directory

Regarding the MAC key:

- The MAC key is a shared secret between the customer and the GlobalSign ACME service which permits customers to bind their specific ACME account key to their Atlas account (and more precisely, to an API credential within the customer account).
- In order to reduce the risk of MAC key compromise or abuse, each MAC key can be used for a maximum of 30 days and up to 1000 times.
- In the event that the MAC key is inadvertently disclosed or compromised, you can create a new MAC key which disables the prior one. This does not disable ACME clients that may have used the compromised MAC key. If you need to disable an affected client, you will want to get new API credentials and MAC, re-install ACME clients with the new MAC bound to the new API Credential, and then revoke that API Credential.
- Once a MAC key has expired or been used 1000 times, you must obtain a new MAC before you can bind more ACME clients to your account.
- The validity and remaining uses are available on the API credential card in the Atlas portal.

Certificate Management

GlobalSign ACME issues CA/Browser Forum-compliant TLS certificates. Using Certbot, with one simple command you can register your GlobalSign Atlas account with your ACME client, validate the certificate domain, and request a certificate.

Please note that we rotate all of our ACME ICAs every quarter, so your ACME client should

always use the provided ICA(s) when configuring the web server. Please see this support article for more information.

Domain Validation and Certificate Issuance

HTTP Validation

The HTTP domain validation method (http-01) relies on the ACME agent placing a random value at a specific location on the target website. Certbot does HTTP validation by default. Use the following code sample when registering your GlobalSign Atlas account with Certbot and requesting a certificate using the HTTP validation method.

```
certbot certonly --webroot -w <YOUR DOMAIN ROOT FOLDER ADDRESS> -d
<YOURDOMAIN.COM> -n --agree-tos --eab-kid <YOUR-API-KEY> --eab-hmac-key
<YOUR-MAC-KEY> -m <YOUR@EMAIL.COM> --server
https://emea.acme.atlas.globalsign.com/directory
```

If your Atlas account has already been registered in your Certbot client then you can use the following code sample to request a certificate using the HTTP validation method.

```
certbot certonly --webroot -w <YOUR DOMAIN ROOT FOLDER ADDRESS> -d
<YOURDOMAIN.COM> --server
https://emea.acme.atlas.globalsign.com/directory
```

According to the CA/Browser Forum baseline requirements you cannot use the HTTP validation method to validate a wildcard SAN, you must instead use the DNS validation method.

If you wish to issue a certificate via CSR, please generate a CSR with a SHA-256 hashing algorithm.

DNS Validation

The DNS validation method (dns-01) requests the GlobalSign ACME server to check the DNS TXT record on your website. When you make this request, you will receive a token which must be uploaded to your website's DNS TXT record.

Certbot automatically selects the HTTP validation method for all domain validations, so you need to specify in this command to use the DNS validation method. The command used will depend on the way your ACME client is configured, for more information please visit https://eff-certbot.readthedocs.io/en/stable/using.html#dns-plugins.

Domain Reuse Period

Domains validated via ACME can be reused for 365 days before they need to be

revalidated.

Other Domain Validation Methods

The GlobalSign Atlas platform additionally supports the email domain validation method, which can be used to validate domains to a specific identity profile and then subsequently used by ACME. For more information, refer to our Atlas Certificate Management API guide.

Domain Validation for Subdomains

GlobalSign's ACME service is configured so that if you have successfully verified control of a parent domain, you may request certificates for any subdomains of that parent domain without having to individually validate those subdomains as well. For example, if you have successfully validated www.example.com, then if you submit a certificate request for www.shop.example.com, GlobalSign will automatically bypass the domain validation step since the parent domain has already been verified. This logic has been implemented for parent domains that have been validated with a validation method that can be used for wildcards and subdomains.

CSR Signature Algorithm

GlobalSign's ACME service is configured so that we will only issue certificates with either an RSA or ECC signature using a SHA-256 signature hash algorithm. The expectation is that your ACME agent will generate the CSR for you, so you will not have to create and submit a valid CSR. If you encounter an error that points to the CSR, it might be because the agent is submitting one that is being blocked by our service. Check the CSR and confirm it is using a SHA-256-based signature algorithm. If it isn't, you may need to configure your agent to submit one or generate your own CSR and instruct the agent to use it.

Revoke a Certificate

Use the following code sample when revoking a certificate from the GlobalSign ACME server. When revoking a certificate, you can specify the reason for the revocation by using the reason flag.

```
certbot revoke --cert-name <YOUR DOMAIN> --reason unspecified
```

Renew a Certificate

According to the Certbot documentation, certificate autorenewal often comes preconfigured at installation by periodically running a scheduled task `certbot renew`. If you have manually requested a certificate, you will need to manually configure certificate autorenewals. More information about how Certbot handles automatic and manual renewals can be found here: https://eff-certbot.readthedocs.io/en/latest/using.html#renewing-certificates

Account Management

Update Your Contact Email

You can change the email address(es) associated with your ACME client's account by providing it with the updated address(es). This will ensure the GlobalSign ACME server has the most up-to-date information to contact the client for issues related to the account. This action will not affect any other aspects of the account.

```
certbot update_account --email <UPDATED.EMAIL@EXAMPLE.COM>
```

Deactivate Your Account

You can use your ACME client to deactivate your ACME client's account. You may wish to do this when the account key is compromised or has been decommissioned. A deactivated account can no longer request certificate issuance or access resources related to the account, such as orders or authorizations. Any pending operations authorized by the account's key will be cancelled (e.g., certificate orders). Certificates issued by the account will not be revoked.

There is no way to reactivate a deactivated account, you must create a new one and do a fresh EAB again.

```
certbot unregister
```

Account Key Rollover

If you want to change the public key that is associated with your client ACME account, to recover from a key compromise or proactively mitigate the impact of an unnoticed key compromise, you may do so with the GlobalSign endpoint `https://emea.acme.atlas.globalsign.com/key-change`. The request sent to the server needs to contain signatures by both the old and new keys. The signature by the new key covers the account URL and the old key, signifying a request by the new key holder to take over the account from the old key holder. The signature by the old key covers this request and its signature, and indicates the old key holder's assent to the rollover request.

When this action is complete, no further changes will be made to your account. You will not need to perform EAB or other authentication actions afterward. This change will not impact any pending certificate orders or authorizations. This action may be preferred over deactivating your account and making a new one, and reestablishing EAB.

Not all ACME clients support this action (such as, Certbot). You will have to research to see if your client of choice supports this feature. If you decide to use a custom client, please refer to the ACME RFC for guidance on implementation.

Technical Addendum

Certbot on NGINX

The following configuration must be added to the default HTTP config if the server has already been configured (which is present in 90% of circumstances) so that the HTTP ACME challenge does not do a vanilla 301 redirect to the corresponding HTTPS page:

```
server {
    listen 80 default_server;
    server_name _;
```

One way to approach this to allow configuration across all servers by using the `cli.ini` Certbot file to load parameters rather than adding them to the command as switches. The file might contain lines like:

```
agree-tos = true
email = example@example.com
eab-kid =
eab-hmac-key =
server = https://emea.acme.atlas.globalsign.com/directory
```

Domain Validation Using DNS CNAME Records

A Canonical Name (CNAME) record is a type of resource record in the Domain Name System (DNS) which maps one domain name (an alias) to another (the CNAME). You can, for example, point ftp.example.com and www.example.com to the DNS entry for example.com, which in turn has an A record which points to the IP address. If the IP address ever changes, you only have to record the change in one place within the network: in the DNS A record for example.com.

CNAME records are handled specially in the DNS and have several restrictions on their use. When a DNS resolver encounters a CNAME record while looking for a regular resource record, it will restart the query using the CNAME instead of the original name. (If the resolver is specifically told to look for CNAME records, the CNAME is returned, rather than restarting the query.) The CNAME that a CNAME record points to can be anywhere in the DNS, whether local or on a remote server in a different DNS zone.

1. Update your DNS

For each domain you want to verify using CNAME, you need to create a subdomain CNAME record that begins with an underscore character (“_”). For example, if you want to verify example.com, you need to create a CNAME for “_acme-challange.example.com.”

The CNAME should point to the place you intend to put a DNS TXT record with the verification token. For this example, let’s use “verify-example.com.”

2. Validate a Domain

When you verify example.com, "_acme-challange.example.com" as the Authorization Domain Name (ADN - the place you want GlobalSign to look for the token) in the API call. The API will see that there is a CNAME record to "verify-example.com," so GlobalSign will look there for the DNS TXT record. You don't need to modify the example.com DNS in the process of this domain validation.

1. Using the Atlas API, request a domain to be verified: POST /claims/domains/{domain}
2. Receive the token for the validation.
3. Update your DNS to add a TXT record to "verify-example.com" with the token (it's OK if there are a few there already).

   Note: Since this is a different domain name (and different DNS login credentials) than the ones to your production DNS, this validation method is secure because no one can change your production DNS domain names.
4. Using the Atlas API, POST /claims/domains/{claimID}/dns with the ADN of "_acme-challange.example.com."
5. GlobalSign knows this is a valid ADN because of the logic you built previously (can approve domains using a CNAME in a subdomain beginning with "_"). GlobalSign will find the CNAME and then will check for the TXT record at "verify-example.com."
6. When the valid TXT record is found at verify-example.com, the domain validation is approved.

You may then delete the TXT record you created.

ACME Directory Objects

GlobalSign supports the following directory URLs and other account management functions according to the ACME RFC.

Field	Description
newNonce	Request a new nonce
newAccount	Request a new account
onlyReturnExisting	A client can look up an account URL based on an account key
contact	A client can modify the contact details of an existing account
externalAccountBinding	An ACME account securely binds itself to a CA account for dedicated certificate management
deactivated	Deactivate an ACME account
newOrder	Request a new (certificate) order
newAuthz	Request a new authorization
revokeCert	Revoke a certificate
keyChange	Change the public key that is associated with an account