GlobalSign ACME Implementation Guide

Document Version 1.5

Table of Contents

Overview

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

ACME is an extensible framework for automating certificate issuance and domain validation procedures. ACME allows users to request 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 integration with ACME, 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 revoke CA/Browser Forum-compliant SSL/TLS certificates from Atlas without having to interface with the Atlas portal or APIs.

Getting Started

Atlas Onboarding Process

To get things started, you will need to 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 the following your name and other business information.
4. At this point, please contact your GlobalSign Account Manager and provide them your email address which they can use to look up your new Atlas account. Your Account Manager will prepare a quote for a TLS ACME service, and you will receive a notification when your quote is ready to view on your Atlas dashboard.
5. Review the quote, select the payment type **Invoice only**, 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. After accepting a quote, you will be prompted to create an Identity Profile
    b. Click on **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 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.
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. Each GlobalSign product has its own credentials.
    a. From the 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 accept the quote.
    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 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, the customer can create a new MAC key which disables the prior one. This does not disable ACME clients that may have used the inadvertently disclosed MAC key. If you need to do that, then 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 SSL/TLS certificates and private certificates off of our IntranetSSL private root CA. 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 CAs 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 in one command.

```
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
```

If you want to validate a wildcard SAN, then you must use the DNS method since the HTTP method is prohibited from being used for issuance of wildcard certificates per the CA/Browser Forum baseline requirements.

If you wish to issue a certificate via CSR, please generate a CSR with a SHA-256, SHA-384, or SHA-512 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 supports several other domain validation methods which can be used to validate domains to the specified identity profile and then subsequently used by ACME. For more information, refer to our Atlas API guide.

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

You can set up automatic renewals for certificates that are about to expire using the following code sample. Include the complete set of subject domains for the certificate using `-d` flags. You may also want to include the `-n` or `--noninteractive` flag to allow Certbot to run without requesting user prompts, which is useful when running the command from cron. For more information on using this command please visit https://certbot.eff.org/docs/using.html

```
certbot certonly -n -d <YOUR DOMAIN>
```

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 easy configuration across all servers is use 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.

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. Let's use "verify-example.com."

Validate a Domain

When you want to verify example.com you specify "_acme-challange.example.com" as the Authorization Domain Name (ADN) in the API call (the place you want GlobalSign to look

for the token). 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 didn’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: As noted above, 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 to /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. The valid TXT record is found at verify-example.com, and the domain validation is approved.

You may then delete the TXT record you created.