About Signatures of API Requests

- EN
- FR

The signing process is used to add authentication information to the requests sent to 3DS OUTSCALE in order to ensure their integrity and authenticity.

The creation of signatures is based on the Hash-based Message Authentication Code (HMAC) protocol, a mechanism for message authentication codes which involves cryptographic hash functions.

When you create requests to 3DS OUTSCALE manually, you need to sign your requests yourself. However, you do not need to sign your requests when you use tools such as the OUTSCALE Command Line Interface (OSC CLI), the AWS Command Line Interface (AWS CLI), or a Software Development Kit (SDK). These tools sign requests automatically with the access key that you specify when you configure them. For more information about OSC CLI and AWS CLI, see respectively Installing and Configuring OSC CLI and Installing and Configuring AWS CLI.

Related Pages

- Creating a Canonical Request
- Creating a String to Sign
- Calculating a Signature
- Adding a Signature to Your API Request

General Information

The signing process makes requests more secure as it provides the following:

- Identity verification of the requester: The signature used to authenticate the request is created from an access key, which enables you to check the identity of the person who sends the request. For more information about access keys, see About Access Keys.
- In-transit data protection: To prevent a request from being tampered with while in transit, some of its elements are used to calculate a hash of the request. The result of this hash, which is the signature, is included in the request. When 3DS OUTSCALE receives your request, it uses the same information to recalculate the signature and matches it against yours. If the signatures match, 3DS OUTSCALE processes your request. Otherwise, your request is denied.
- Protection against replay attacks: In general, a request must reach 3DS OUTSCALE within five minutes of the timestamp specified in the request. Otherwise, your request is denied.

To sign a request, you first need to use a cryptographic hash function (HMAC) to calculate a hash of the request. You then need to use the value of this hash, your secret key and other information to calculate another hash whose result is the signature. Finally, you add the signature to the request, either in the HTTP `Authorization` header or as a value in the query string. In that last case, the signature is part of the URL, which becomes a pre-signed URL. For more information about the creation process of a signature, see the Creation of a Signature section below.

3DS OUTSCALE supports both Signature Version 2 and Signature Version 4. However, we recommend using Signature Version 4 for all OUTSCALE services.

Creation of a Signature

A signature is calculated as follows:

1. Creation of a canonical request:
   Before you can sign the request, you need to arrange it in a standard format, also called canonical format. Using a canonical format is necessary because 3DS OUTSCALE uses this same format to recalculate the signature. For more information, see Creating a Canonical Request.

2. Creation of a string to a sign from the canonical request and other information:
   The information contained in the canonical request needs to be concatenated into a single string to sign. For more information, see Creating a String to Sign.

3. Creation of a signature from a signing key and the string to sign:
   The signing key, which is created from your access key, and the string to sign are hashed with a cryptographic hash function. The result is the signature. For more information, see Calculating a Signature.

4. Insertion of the signature into the request, either in a header or as a parameter in the query string:
   The signature must be added to the request to turn it into a signed request. For more information, see Adding a Signature to Your API Request.

After 3DS OUTSCALE receives the request, it recalculates the signature with the same information and the same hash function you used to sign your request. If the signature calculated by 3DS OUTSCALE matches yours, 3DS OUTSCALE processes the request. Otherwise, 3DS OUTSCALE denies the request.

AWS™ and **Amazon Web Services**™ are trademarks of Amazon Technologies, Inc or its affiliates in the United States and/or other countries.