http-signatures-php Documentation

Liam Dennehy

Aug 18, 2019

Contents:

PHP implementation of Signing HTTP Messages draft IETF specification, allowing cryptographic signing and verifying of PHP PSR-7 messages.

Version 10.x of this library implements all features of requirements of version 10 of the RFC.

CHAPTER 1

Quickstart

This page provides a quick introduction to HTTP Signatures PHP library and introductory examples.

If you have not already installed HTTP Signatures PHP library head over to the *Installation* page.

A reference signing client and verifying server are included that will actually exchange messages over HTTP. To see the library in actions, head over the the Reference Implementation Guide in the file REFERENCE.md.

1.1 Signing a message

Once you have a PSR-7 message ready to send, create a Context with:

- your chosen algorithm
- the list of headers to include in the signature
- the key you will use to sign the message

For these examples we will sign the method + URI (indicated by `(request-target)`) and the `Content-Type` header. This provides a very basic level of protection, and you should consider the headers you sign in your application carefully. These may also be specified by the verifier (most often a server hosting an API or web service).

Note also that this does not apply only to HTTP requests sent by a client. Servers can add a signature to responses that the client can verify.

1.1.1 Shared Secret Context (HMAC)

This type of signature uses a secret key known to you and the verifier.

```
$signingContext = new \HttpSignatures\Context([
  'keys' => ['key12' => file_get_contents('/path/to/secret-key')],
  'algorithm' => 'hmac-sha256',
  'headers' => ['(request-target)', 'Date'],
]);
```

1.1.2 Private Key Context (RSA)

This type of signature uses a private key known only to you, which can be verified using a public key that is known to anyone who wants to verify the message.

The key file is assumed to be an unencrypted private key in PEM format.

```
$signingContext = new \HttpSignatures\Context([
  'keys' => ['key12' => file_get_contents('/path/to/privatekey.pem')],
  'algorithm' => 'rsa-sha256',
  'headers' => ['(request-target)', 'Date']
]);
```

1.1.3 Signing the Message:

With your PSR-7 compliant message in `$message`:

```
$signingContext->signer()->sign($message);
```

Now `$message` contains the `Signature` header:

```
print $message->getHeader('Signature')[0];
// keyId="key12",algorithm="<yourAlgorithm>",headers="...",signature="..."
```

There is a similar function to add the `Authorization: Signature` header:

```
$signingContext->signer()->authorize($message);

print $message->getHeader('Authorization')[0];
// Signature keyId="key12",algorithm="<yourAlgorithm>",headers="...",signature="..."
```

1.1.4 Adding a Digest header while signing

Include a `Digest` header automatically when signing to also protect the payload (body) of the message in addition to the request-target and headers:

```
$signingContext->signer()->signWithDigest($message);

$message->headers->getHeader('Digest')[0];
// SHA-256=<base64SHA256Digest>
```

1.2 Verifying a Signed Message

Most parameters are derived from the Signature in the signed message, so the Context can be created with fewer parameters.

It is probably most useful to create a Context with multilpe keys/certificates. the signature verifier will look up the key using the keyId attribute of the Signature header and use that to validate the signature.

1.2.1 Verifying a HMAC signed message

A message signed with an hmac signature is verified using the same key as the one used to sign the original message. Since multiple signatures may come from multiple keys, the verifier can take an array of known keys and will match the id of the key provided with the `keyId` parameter in the received message header.

```
$verifier = new \HttpSignatures\Verifier([
  'key300' => 'some-other-secret',
  'key12' => 'your-secret-here'
]);

$verifier->isSigned($message); // true or false
// OR
$verifier->isAuthorized($message); // true or false
```

1.2.2 Verifying a RSA signed message

An RSA signature is verified using the certificate associated with the Private Key that created the message. Create a context by importing the X.509 PEM format certificates in place of the 'secret':

```
$verifier = new \HttpSignatures\Verifier([
  'key12' => file_get_contents('/path/to/certificate'),
  'key87' => $someOtherCertificate
]);

$verifier->isSigned($message); // true or false
// OR
$verifier->isAuthorized($message); // true or false
```

1.2.3 Verifying a message digest

To confirm the body has a valid digest header and the header is a valid digest of the message body, use the `$verifier` from above:

```
$verifier->isValidDigest($message); // true or false
```

An all-in-one validation that the signature includes the digest, and the digest is valid for the message body:

```
$verifier->isSignedWithDigest($message); // true or false
// OR
$verifier->isAuthorizedWithDigest($message); // true or false
```

1.3 Symfony compatibility

Symfony requests normalize query strings which means the resulting request target can be incorrect. See https://github.com/symfony/psr-http-message-bridge/pull/30

When creating PSR-7 requests you use *withRequestTarget* to ensure the request target is correct. For example

```
use Symfony\Bridge\PsrHttpMessage\Factory\DiactorosFactory;
use Symfony\Component\HttpFoundation\Request;

```

(continues on next page)

(continued from previous page)

```
$symfonyRequest = Request::create('/foo?b=1&a=2');
$psrRequest = (new DiactorosFactory())
      ->createRequest($symfonyRequest)
      ->withRequestTarget($symfonyRequest->getRequestUri());
```

CHAPTER 2

The HTTP Signature

This section is based on the definitions and descriptions in Signing HTTP Messages IETF draft RFC version 10.

Table of Contents

2.1 Signature Line

```
keyId="abc123",algorithm="rsa-sha256",headers="(request-target) date",signature=
↪"base64string"
```

The Signature line is the component of a signature header that describes the parameters of how a message was signed as well as the actual digital signature.

These parameters together should provide any verifier with the information required to prove the validity of a signature against the HTTP message it accompanies.

The parameters of the Signature Line are described here

2.1.1 keyId

As desribed in the draft RFC, the `keyId` parameter is used by the verifier to look up the key that can be used to verify the provided signature.

- In the HMAC case these are the same key - the shared secret.
- In the RSA or EC case, this is the public component of the key.

Note that the RFC is not specific about the meaning of the parameter's value. This could be a fingerprint of the certificate containing the key, the e-mail address of the signer, or even no value at all if the verifier can determine which key to use by another means entirely e.g. if the key/certificate is provided in a dedicated header.

The value of `keyId` must therefore be agreed before the message is transmitted - either by agreeing an explicit value, or the format of the value acceptable to the verifier if it not distinct. This is typically found in the API documentation for the resource.

2.1.2 algorithm

The `algorithm` parameter informs the verifier which hash algorithm was used to generate the hash signed by the signature ("hash" algorithm), and which cryptographic algorithm was used to sign that resulting hash ("signature algorithm").

The hash algorithm cannot be deduced simply by looking at the key and signature, so must be provided in this parameter.

However the verifier should not rely on the signature algorithm part of the `algorithm` parameter alone to determine which signature algorithm to use. Rather the "metadata" (e.g. which elliptic curve algorithm the key is designed for) associated with the key should be relied on separate from the signed message.

This arises as some types of keys can be used in multiple modes, and selecting the wrong mode for verification may introduce security issues.

In any case the signer and verifier should agree which hash and signature algorithms are acceptable for a given request/response.

2.1.3 headers

The `headers` parameter is a space-delimited list of the headers that are included in the signature itself. These headers are specified in lowercase, and let the verifier know which order to place the headers in when the signature is verified - so this order cannot be altered.

The signer and verifier(s) need to agree on which headers should be included in any signature, especially if there are minimum headers that must be included and any that are forbidden.

If this parameter is missing from a provided signature line, then the default value "`date`" is used to verify the signature.

2.1.4 signature

The `signature` parameter is simply a base64-encoded string representing the raw digital signature (which is likely encoded with unprintable characters).

The verifier can use this string, along with the other parameters and headers in the HTTP message, to verify the contents of the message (specifically the message's *headers*) have not been altered since the signer generated the signature.

2.2 Headers

2.2.1 Authorization header

```
Authorization: Signature <signatureline>
```

The `Authorization` header is described in **RFC 7235#section-4.2** and provides a way for a HTTP client to "authenticate itself with an origin server". This gives a hint that the header is used almost exclusively by a client when talking to a server.

The first parameter of an `Authorization` header is the authorization type, of which many have been defined. When the type is `Signature`, the server will expect the next parameters to be a *Signature Line* according to the specifications of https://tools.ietf.org/html/draft-cavage-http-signatures

Since this header is involved primarily with authenticating a client to a server, this header is not typically used to protect the content of a message, and is not useful in a HTTP Response.

2.2.2 Signature header

```
Signature: <signatureline>
```

The `Signature` header is a new HTTP header proposed in https://tools.ietf.org/html/draft-cavage-http-signatures.

The value of the header is simply the *Signature Line*.

This header is more versatile than the `Authorization` header as it can be used:

- by both the client *and* server (HTTP request and HTTP respnse respectively)
- to prove the identity of the signer (similar to the `Authorization` header in `Signature` mode
- in addition to an `Authorization` header when needed

2.2.3 Digest header

```
Digest: SHA-256=<base64string>
```

The `Digest` header is a base64-encoded representation of the hash of the message payload (aka body). It is defined in **RFC 3230**. Note that this library has only rudimentary support for this specification e.g. can only include a single digest value while the RFC requires support for multiple digests.

Including the `Digest` header in the signature's *signature* allows the integrity of the payload to be included in the signature itself.

When the message has no payload - e.g. a GET request, or a reponse with code *202* - the digest is calculated on the empty string `''`.

CHAPTER 3

API Reference

Table of Contents

3.1 Class: Context

```
new Context($contextArgs)
```

The Context class is the base of all signing and verification actions.

$contextArgs is an associative array of parameters for the context. The following keys are recognised:

Key Name	Type	Description
`keys`	Array of keys	An array of shared secret, public or private key objects
`algorithm`	blah	blah
`headers`	blah	blah

CHAPTER 4

Usage

Add liamdennehy/http-signatures-php to your `composer.json`. Full instructions can be found in *Installation*

To quickly see how a message is signed, take a look in *Signing a message* in the Quickstart guide.

CHAPTER 5

Requirements

1. PHP 5.6 (PHP >7.0 recommended)
2. Composer for full autoloading of class loading
3. Understanding of PSR-7 HTTP message handling

5.1 Installation

The recommended way to install http-signatures-php is with Composer. Composer is a dependency management tool for PHP that allows you to declare the dependencies your project needs and installs them into your project.

```
# Install Composer
curl -sS https://getcomposer.org/installer | php
```

You can add http-signatures-php as a dependency using the `composer.phar` CLI:

```
php composer.phar require liamdennehy/http-signatures-php
```

Alternatively, you can specify http-signatures-php as a dependency in your project's existing `composer.json` file:

```
{
  "require": {
     "liamdennehy/http-signatures-php": "~6.0"
  }
}
```

After installing, you need to require Composer's autoloader in your project to be able to locate the library within PHP:

```
require __DIR__ . '/vendor/autoload.php';
```

You can find out more on how to install Composer, configure autoloading, and other best-practices for defining dependencies at getcomposer.org.

CHAPTER 6

Contributing

Pull Requests are welcome, as are issue reports if you encounter any problems.

CHAPTER 7

License

Index

R