Signing

Signing XML documents with XAdES: the options of the signed properties, the references of the data objects and the options of the signature

Anonymous · 09/11/2026

Signing

`XadesSigner::sign()` signs a document with XAdES. It writes the `QualifyingProperties` of the signature in an `Object` of the signature, adds to the signature a reference to the `SignedProperties` (so the signature signs them) and gives the rest of the work to `derafu/signature`.

```
$signed = $signer->sign($xml, $certificate, $options);
```

`$xml` is a string or an `XmlDocumentInterface`, `$certificate` is the certificate of the signer (`derafu/certificate`) and `$options` is an array (or an `OptionsInterface`) that is valid only for that signature: what is not given has its default value and nothing is kept for the next signature.

A signature that does not say what it signs signs the whole document. To sign an element, give its `Id` in the options of the signature (see **The Signature**).

Options

Option	Default	
`version`	The default of the registry	Version of XAdES (`1.3.2` or `1.3.2-201601`).
`signature_id`	`xades-signature-1`	`Id` of the signature, that the properties have as their target.
`signed_properties_id`	`<signature_id>-signed-properties`	`Id` of the `SignedProperties`.
`qualifying_properties_id`	none	`Id` of the `QualifyingProperties`.
`signing_time`	The time of the clock	A date (a text or a `DateTimeInterface`). It is written in UTC.
`certificate_digest_algorithm`	`sha256`	Algorithm of the digest of the certificate of the signer.

Option	Default	
`certificate_chain`	`false`	Also writes the certificates of the chain of the signer in the properties, and includes them in the `KeyInfo`.
`signature_policy`	none	`'implied'` or an array (see below).
`signature_production_place`	none	An array (see below).
`signer_role`	none	An array (see below).
`data_object_formats`	`[]`	A list of arrays (see below).
`commitment_type_indications`	`[]`	A list of arrays (see below).
`signature`	`[]`	The options of the signature, for `derafu/signature`.

The identifiers start with a letter or an underscore, and have only letters, numbers, underscores, hyphens and dots. An option that is not in the table, or has a value that is not valid, is an `XadesException` that says which one.

The signing time comes from a PSR-20 clock (`Psr\Clock\ClockInterface`, the third argument of the constructor: `SystemClock` of `derafu/date` by default), so a test can fix it with a `FixedClock`.

Signature Policy

```
['signature_policy' => 'implied']

['signature_policy' => [
    'identifier' => 'urn:oid:1.2.3.4',
    'identifier_qualifier' => 'OIDAsURN',          // Or OIDAsURI.
    'description' => 'My policy',
    'documentation_references' => ['https://example.com/policy.pdf'],
    'document' => $policyText,                      // Its digest is calculated, or:
    // 'digest' => base64 of the digest,
    'digest_algorithm' => 'sha256',
    'transforms' => ['http://www.w3.org/TR/2001/REC-xml-c14n-20010315'],
    'qualifiers' => [
        'https://example.com/policy',               // A URI.
        ['user_notice' => ['organization' => 'Org', 'numbers' => [1, 2], 'text' =>
'Read it']],
    ],
]]
```

`identifier` is required, and one of `document` or `digest` (not both).

Place of the Signature

```
['signature_production_place' => [
    'city' => 'Santiago',
    'street_address' => 'Calle 1',      // Only in 1.3.2-201601.
    'state_or_province' => 'RM',
    'postal_code' => '8320000',
    'country_name' => 'Chile',
]]
```

At least one field is required.

Role of the Signer

```
['signer_role' => [
    'claimed_roles' => ['Manager', ['xml' => '<r:Role xmlns:r="urn:r">x</r:Role>']],
    'certified_roles' => [$base64OfAnAttributeCertificate, ['certificate' => $base64,
'id' => 'attr-1', 'encoding' => 'DER']],
    'signed_assertions' => [['xml' => '<a:Assertion xmlns:a="urn:a"/>']],   // Only in
1.3.2-201601.
]]
```

A claimed role, a signed assertion or a qualifier is a text, or an array with its `xml`: the XML has to be well formed, and the prefixes that it uses have to be declared in it. At least one role is required.

Data Objects

`data_object_formats` says how the data that the signature signs are, and `commitment_type_indications` what the signer commits to with each one:

```
[
    'data_object_formats' => [[
        'reference' => '#ref-a',
        'description' => 'The document',
        'mime_type' => 'text/xml',
        'encoding' => 'UTF-8',
        'object_identifier' => ['identifier' => 'urn:oid:1.9'],
    ]],
    'commitment_type_indications' => [[
        'type' => ['identifier' => 'http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin'],
        'object_references' => ['#ref-a'],     // Without them, it is of all the
signed data.
        'qualifiers' => ['text'],
    ]],
    'signature' => ['references' => [['uri' => '#A', 'id' => 'ref-a']]],
```

```
]
```

The reference of a data object is `#` and the **`Id` of a `Reference` of the signature** (not its `URI`), so the `Reference` has to be given with that `id` in the `references` of the signature. If it is not there, the signer refuses to sign.

An identifier of an object (`type`, `object_identifier`, the identifier of a policy) is an array with its `identifier` and, optionally, a `qualifier` (`OIDAsURI` or `OIDAsURN`), a `description` and `documentation_references`.

The Signature

The option `signature` has the options of `derafu/signature` (see its generator): the reference, the algorithms, the place of the signature, other references and other objects. The signer chooses what is not given:

- `signature_prefix`: `ds`.
- `digest_algorithm`: `sha256`.
- `signature_algorithm`: by the key of the certificate: RSA, ECDSA or DSA with SHA-256.
- `include_certificate_chain`: the value of `certificate_chain`.

The `Id` of the signature is `signature_id` of the options of XAdES: if the options of the signature have another one, it is an error. The objects and the references that are given are kept, and the ones of XAdES are added at the end.

```
$signed = $signer->sign($xml, $certificate, [
    'signature' => [
        'reference' => 'A',                          // Signs the element with Id="A".
        'digest_algorithm' => 'sha512',
    ],
]);
```

Options for `derafu/signature`

When the signature is made by another way, `options()` gives what has to be added to its options: the `Id` of the signature, the `Object` with the properties and the reference to them.

```
$xades = $signer->options($certificate, ['signature_policy' => 'implied']);
// ['signature_id' => ..., 'objects' => [['xml' => ...]], 'references' => [[...]]]
```

Last updated on 09/11/2026