Introduction

XAdES-B-B electronic signatures in PHP, local and without network: sign XML documents with the signed properties of ETSI and validate them, over derafu/signature

Anonymous · 09/11/2026

XAdES Signatures



Derafu XAdES signs XML documents with XAdES (XML Advanced Electronic Signatures, ETSI), and validates the signatures that have its properties. It works at the level **B-B** (basic): everything that a signature needs to be checked by who receives it, locally and without network.

The XML signature itself (canonicalization, digests, signature value, `KeyInfo`) is made and validated by `derafu/signature`, that knows nothing about XAdES. This package adds what is of XAdES: the `QualifyingProperties` that the signature carries in an `Object`, the reference that makes the signature sign them, and the checks that the properties follow what XAdES requires.

Features

- **Two versions of XAdES**, chosen by an identifier: `1.3.2` (the default) and `1.3.2-201601`. See **Versions**.
- **Every optional signed property of B-B**: the signing time, the certificate of the signer, the signature policy, the place of the signature, the role of the signer, the format of the signed data and the commitments of the signer. See **Signing**.
- **Validation of the properties**: besides the validity of each signature, the validator reports what the properties do not follow of XAdES, one issue for each thing, including the errors against the official schemas of ETSI. See **Validation**.
- **Checked against other implementations**: what the package signs is verified by `xmlsec1` and by `signxml`, and what they sign is validated by the package. The properties are valid against the official XSDs of ETSI. See **Development**.

What the package does not do: the levels above B-B (time-stamps, the data of revocation and archive), the elements that time-stamp the signed data (`AllDataObjectsTimeStamp` and `IndividualDataObjectsTimeStamp`) and the counter signatures. They need a time-stamping authority or the status of the certificates, that is, network.

Installation

```
composer require derafu/xades
```

Basic Usage

```
use Derafu\Certificate\Service\CertificateLoader;
use Derafu\Signature\Service\SignatureGenerator;
use Derafu\Signature\Service\SignatureValidator;
use Derafu\Xades\Service\XadesSigner;
use Derafu\Xades\Service\XadesValidator;
use Derafu\Xml\Service\XmlDecoder;
use Derafu\Xml\Service\XmlEncoder;
use Derafu\Xml\Service\XmlService;
use Derafu\Xml\Service\XmlValidator;

$xmlService = new XmlService(new XmlEncoder(), new XmlDecoder(), new XmlValidator());
$generator = new SignatureGenerator($xmlService);

$signer = new XadesSigner($generator);
$validator = new XadesValidator(new SignatureValidator($generator, $xmlService));

$certificate = (new CertificateLoader())->loadFromFile('/path/to/certificate.p12',
'password');

// The signature of the whole document, with the properties of XAdES.
$signed = $signer->sign('<Root><Doc Id="A"/></Root>', $certificate);

$report = $validator->validate($signed);
if ($report->isValid()) {
    echo 'The signature is valid and follows XAdES.';
}
```

Services

Class	Interface	What it does
`XadesSigner`	`XadesSignerInterface`	Signs a document with XAdES, or gives the options that `derafu/signature` needs to do it.
`XadesValidator`	`XadesValidatorInterface`	Validates the signatures of a document and checks their XAdES properties.
`VersionRegistry`	`VersionRegistryInterface`	Has the versions of XAdES that the package supports.

The package has its configuration for `symfony/dependency-injection` in `resources/config/xades-`

`services.yaml`. The application imports the configuration of `derafu/signature` and of `derafu/date` (the clock that gives the signing time), that the services need.

Last updated on 09/11/2026