

Certificate Loader

How to load a certificate from a PKCS#12 file or data, from an array, from its keys or from only the certificate, and what fails when the input is not valid

Anonymous · 17/10/2026

CertificateLoader Class

The `CertificateLoader` creates a `Certificate` from the different forms in which a certificate is found. The result is always a `CertificateInterface`.

```
use Derafu\Certificate\Service\CertificateLoader;  
  
$loader = new CertificateLoader();
```

Loading

Method	Loads from
<code>loadFromFile(\$filepath, \$password)</code>	A PKCS#12 file.
<code>loadFromData(\$data, \$password)</code>	The content of a PKCS#12 file.
<code>loadFromArray(\$data)</code>	An array with the certificate, the private key and, optionally, the chain.
<code>loadFromKeys(\$certificate, \$privateKey, \$chain = [])</code>	The certificate and the private key, as text.
<code>loadFromCertificate(\$certificate, \$chain = [])</code>	Only the certificate: there is no private key.

```
$certificate = $loader->loadFromFile('/path/to/certificate.p12', 'password');  
  
$certificate = $loader->loadFromArray([  
    'cert' => $certificatePem,  
    'pkey' => $privateKeyPem,  
    'chain' => [$intermediateCaPem],  
]);
```

The keys can be given with or without the PEM header and footer: the loader adds them if they are missing.

The Array

`loadFromArray()` accepts these indexes (the second name of each pair is an alias):

- `cert` or `certificate`: the certificate (required).
- `pkey` or `privateKey`: the private key (required).
- `chain` or `extracerts`: the intermediate CA certificates (optional). `extracerts` is the index that `openssl_pkcs12_read()` gives, so its result can be passed as it is.

The Trust Chain

When a PKCS#12 bundles the intermediate CA certificates, they are kept in the certificate:

`getCertificateChain()` gives them and `getCertificateBundle()` gives the certificate followed by the chain.

A Certificate without Private Key

`loadFromCertificate()` is for when only the public part is needed, for example to verify. The certificate that it gives has `getKeys()['pkey']` as `null`, and `getPrivateKey()` throws a `CertificateException`. Everything that is read from the certificate (data, modulus, exponent, validity) works.

When It Fails

The loader throws a `CertificateException` when:

- The file can not be read, or its content can not be read.
- The PKCS#12 can not be read: it is not a PKCS#12 or the password is wrong. The errors of OpenSSL are in `getErrors()`, as translatable messages, and the ones that are known are explained and translated (for example, `MAC verification failed in PKCS12, certificate or password is incorrect (Error #11800071)`).
- The array has no certificate or no private key.
- In the array, the certificate or the private key is not text, or the chain is not an array of texts.

See [Exceptions](#).

Last updated on 17/10/2026