

**NAME**

PKCS12\_parse - parse a PKCS#12 structure

**SYNOPSIS**

```
#include <openssl/pkcs12.h>
```

```
int PKCS12_parse(PKCS12 *p12, const char *pass, EVP_PKEY **pkey, X509 **cert,  
STACK_OF(X509) **ca);
```

**DESCRIPTION**

**PKCS12\_parse()** parses a PKCS12 structure.

**p12** is the **PKCS12** structure to parse. **pass** is the passphrase to use. If successful the private key will be written to **\*pkey**, the corresponding certificate to **\*cert** and any additional certificates to **\*ca**.

**NOTES**

Each of the parameters **pkey**, **cert**, and **ca** can be NULL in which case the private key, the corresponding certificate, or the additional certificates, respectively, will be discarded. If any of **pkey** and **cert** is non-NULL the variable it points to is initialized. If **ca** is non-NULL and **\*ca** is NULL a new STACK will be allocated. If **ca** is non-NULL and **\*ca** is a valid STACK then additional certificates are appended in the given order to **\*ca**.

The **friendlyName** and **localKeyID** attributes (if present) on each certificate will be stored in the **alias** and **keyid** attributes of the **X509** structure.

The parameter **pass** is interpreted as a string in the UTF-8 encoding. If it is not valid UTF-8, then it is assumed to be ISO8859-1 instead.

In particular, this means that passwords in the locale character set (or code page on Windows) must potentially be converted to UTF-8 before use. This may include passwords from local text files, or input from the terminal or command line. Refer to the documentation of **UI\_OpenSSL(3)**, for example.

**RETURN VALUES**

**PKCS12\_parse()** returns 1 for success and zero if an error occurred.

The error can be obtained from **ERR\_get\_error(3)**

**BUGS**

Only a single private key and corresponding certificate is returned by this function. More complex PKCS#12 files with multiple private keys will only return the first match.

Only **friendlyName** and **localKeyID** attributes are currently stored in certificates. Other attributes are discarded.

Attributes currently cannot be stored in the private key **EVP\_PKEY** structure.

## SEE ALSO

**d2i\_PKCS12(3)**, **passphrase-encoding(7)**

## COPYRIGHT

Copyright 2002-2020 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <<https://www.openssl.org/source/license.html>>.