

---

# PKCS #9: Selected Attribute Types

An RSA Laboratories Technical Note

Version 1.1

Revised November 1, 1993\*

## 1. Scope

This standard defines selected attribute types for use in PKCS #6 extended certificates, PKCS #7 digitally signed messages, PKCS #8 private-key information, and PKCS #10 certificate-signing requests.

## 2. References

PKCS #6	RSA Laboratories. <i>PKCS #6: Extended-Certificate Syntax Standard</i> . November 1993.	Version 1.5,
PKCS #7	RSA Laboratories. <i>PKCS #7: Cryptographic Message Syntax Standard</i> . November 1993.	Version 1.5,
PKCS #8	RSA Laboratories. <i>PKCS #8: Private-Key Information Syntax Standard</i> . November 1993.	Version 1.2,
PKCS #10	RSA Laboratories. <i>PKCS #10: Certification Request Syntax Standard</i> . November 1993.	Version 1.0,
X.208	CCITT. <i>Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1)</i> . 1988.	
X.402	CCITT. <i>Recommendation X.402: Message Handling Systems—Overall Architecture</i> . 1988.	
X.509	CCITT. <i>Recommendation X.509: The Directory—Authentication Framework</i> .	1988.
X.520	CCITT. <i>Recommendation X.520: The Directory—Selected Attribute Types</i> .	1988.

---

\*Supersedes June 3, 1991 version, which was also published as NIST/OSI Implementors' Workshop document SEC-SIG-91-24. PKCS documents are available by electronic mail to <pkcs@rsa.com>.

Copyright © 1991–1993 RSA Laboratories, a division of RSA Data Security, Inc. License to copy this document is granted provided that it is identified as "RSA Data Security, Inc. Public-Key Cryptography Standards (PKCS)" in all material mentioning or referencing this document.

003-903024-110-000-000

DIS 10646      ISO/IEC JTC 1. *DIS 10646-1.2: Information Technology—Universal Multiple-Octet Coded Character Set (UCS)—Part 1: Architecture and Basic Multilingual Plane*.  
February 1992.

### 3. Definitions

For the purposes of this standard, the following definitions apply.

**ASN.1:** Abstract Syntax Notation One, as defined in X.208.

**Attributes:** A type that specifies a set of attributes. Each attribute contains an attribute type (specified by object identifier) and one or more attribute values. Some attribute types are restricted in their definition to have a single value; others may have multiple values. This type is defined in PKCS #6, #7, #8, and #10.

**CertificationRequestInfo:** A type that specifies a subject name, a public key, and a set of attributes. This type is defined in PKCS #10.

**ExtendedCertificate:** A type that consists of an X.509 public-key certificate and a set of attributes, collectively signed by the issuer of the X.509 public-key certificate. This type is defined in PKCS #6.

**ContentInfo:** A type that specifies content exchanged between entities. The `contentType` field, which has type `OBJECT IDENTIFIER`, specifies the content type, and the `content` field, which has type `ANY DEFINED BY contentType`, contains the content value. This type is defined in PKCS #7.

**PrivateKeyInfo:** A type that specifies a private key and a set of extended attributes. This type is defined in PKCS #8.

**SignerInfo:** A type that specifies per-signer information in the signed-data content type, including a set of attributes authenticated by the signer, and a set of attributes not authenticated by the signer. This type is defined in PKCS #7.

**DER:** Distinguished Encoding Rules for ASN.1, as defined in X.509, Section 8.7.

**UCS:** Universal Multiple-Octet Coded Character Set, as defined in DIS 10646.

### 4. Symbols and abbreviations

No symbols or abbreviations are defined in this standard.

<b>X.520 Attribute Types</b>	
businessCategory	preferredDeliveryMethod
commonName	presentationAddress
countryName	registeredAddress
description	roleOccupant
destinationIndicator	serialNumber
facsimileTelephoneNumber	stateOrProvinceName
iSDNAddress	streetAddress
localityName	supportedApplicationContext
member	surname
objectClass	telephoneNumber
organizationName	teletexTerminalIdentifier
physicalDeliveryOfficeName	telexNumber
postalAddress	title
postalCode	x121Address
postOfficeBox	
<b>X.402 Attribute Types</b>	
mhs-or-address	

**Table 1.** X.520 and X.402 attribute types useful in PKCS #6 extended certificates.

## 5. General overview

The following sections specify new attribute types and object identifiers. This standard exports the various object identifiers.

New attribute types that are useful in PKCS #6 extended certificates are electronic-mail address, unstructured name, and unstructured address. The attributes would be used in the `attributes` field of a `CertificateWithAttributes` value.

New attribute types that are useful in PKCS #7 digitally signed messages are content type, message digest, signing time, and countersignature. The attributes would be used in the `authenticatedAttributes` and `unauthenticatedAttributes` fields of a `SignerInfo` value.

No new attribute types that are useful in PKCS #8 private-key information are given.

New attribute types that are useful in PKCS #10 certification requests are challenge password and extended-certificate attributes. The attributes would be used in the `attributes` field of a `CertificationRequestInfo` value.

**Note.** The X.520 and X.402 attributes types in Table 1, and probably several others, might also be helpful in PKCS #6 and PKCS #10.

## 6. Attribute types

This standard defines nine new attribute types: electronic-mail address, unstructured name, content type, message digest, signing time, countersignature, challenge password, and extended-certificate attributes.

### 6.1 Electronic-mail address

The electronic-mail address attribute type specifies the electronic-mail address or addresses of the subject of a certificate as an unstructured ASCII string. The interpretation of electronic-mail addresses is intended to be specified by the issuer of the certificate; no particular interpretation is required. The electronic-mail address attribute type is intended for PKCS #6 extended certificates.

Electronic-mail address attribute values have ASN.1 type `EmailAddress`:

```
EmailAddress ::= IA5String
```

An electronic-mail address attribute can have multiple attribute values.

**Note.** It is likely that other standards bodies overseeing electronic-mail systems will register electronic-mail address attribute types specific to their system. The electronic-mail address attribute type is intended as a short-term substitute for those specific attribute types.

### 6.2 Unstructured name

The unstructured-name attribute type specifies the name or names of the subject of a certificate as an unstructured ASCII string. The interpretation of the names is intended to be specified by the issuer of the certificate; no particular interpretation is required. The unstructured-name attribute type is intended for PKCS #6 extended certificates.

Unstructured-name attribute values have ASN.1 type `UnstructuredName`:

```
UnstructuredName ::= IA5String
```

An unstructured-name attribute can have multiple attribute values.

**Note.** It is expected that if UCS becomes an ASN.1 type (e.g., `UNIVERSAL STRING`), `UnstructuredName` will become a `CHOICE` type:

```
UnstructuredName ::= CHOICE {  
    IA5String, UNIVERSAL STRING }
```

### 6.3 Content type

The content-type attribute type specifies the content type of the `ContentInfo` value being signed in PKCS #7 digitally signed data. The content-type attribute type is required if there are any PKCS #7 authenticated attributes.

Content-type attribute values have ASN.1 type `ContentType`:

```
ContentType ::= OBJECT IDENTIFIER
```

A content-type attribute must have a single attribute value.

### 6.4 Message digest

The message-digest attribute type specifies the message digest of the contents octets of the DER encoding of the content field of the `ContentInfo` value being signed in PKCS #7 digitally signed data, where the message digest is computed under the signer's message digest algorithm. The message-digest attribute type is required if there are any PKCS #7 authenticated attributes.

Message-digest attribute values have ASN.1 type `MessageDigest`:

```
MessageDigest ::= OCTET STRING
```

A message-digest attribute must have a single attribute value.

### 6.5 Signing time

The signing-time attribute type specifies the time at which the signer (purportedly) performed the signing process. The signing-time attribute type is intended for PKCS #7 digitally signed data.

Signing-time attribute values have ASN.1 type `SigningTime`:

```
SigningTime ::= UTCTime
```

A signing-time attribute must have a single attribute value.

**Note.** No requirement is imposed concerning the correctness of the signing time, and acceptance of a purported signing time is a matter of a recipient's discretion. It is expected, however, that some signers, such as time-stamp servers, will be trusted implicitly.

## 6.6 Countersignature

The countersignature attribute type specifies one or more signatures on the contents octets of the DER encoding of the `encryptedDigest` field of a `SignerInfo` value in PKCS #7 digitally signed data. Thus, the countersignature attribute type countersigns (signs in serial) another signature. The countersignature attribute must be an unauthenticated PKCS #7 attribute; it cannot be an authenticated attribute.

Countersignature attribute values have ASN.1 type `Countersignature`:

`Countersignature ::= SignerInfo`

Countersignature values have the same meaning as `SignerInfo` values for ordinary signatures (see Section 9 of PKCS #7), except that:

1. The `authenticatedAttributes` field must contain a message-digest attribute if it contains any other attributes, but need not contain a content-type attribute, as there is no content type for countersignatures.
2. The input to the message-digesting process is the contents octets of the DER encoding of the `encryptedDigest` field of the `SignerInfo` value with which the attribute is associated.

A countersignature attribute can have multiple attribute values.

### Notes.

1. The fact that a countersignature is computed on a signature (encrypted digest) means that the countersigning process need not know the original content input to the signing process. This has advantages both in efficiency and in confidentiality.
2. A countersignature, since it has type `SignerInfo`, can itself contain a countersignature attribute. Thus it is possible to construct arbitrarily long series of countersignatures.

## 6.7 Challenge password

The challenge-password attribute type specifies a password by which an entity may request certificate revocation. The interpretation of the password is intended to be specified by the issuer of the certificate; no particular

interpretation is required. The challenge-password attribute type is intended for PKCS #10 certification requests.

Challenge-password attribute values have ASN.1 type ChallengePassword:

```
ChallengePassword ::= CHOICE {
    PrintableString, T61String }
```

A challenge-password attribute must have a single attribute value.

**Note.** It is expected that if UCS becomes an ASN.1 type (e.g., UNIVERSAL STRING), ChallengePassword will become a CHOICE type:

```
ChallengePassword ::= CHOICE {
    PrintableString, T61String, UNIVERSAL STRING }
```

### 6.8 Unstructured address

The unstructured-address attribute type specifies the address or addresses of the subject of a certificate as an unstructured ASCII or T.61 string. The interpretation of the addresses is intended to be specified by the issuer of the certificate; no particular interpretation is required. A likely interpretation is as an alternative to the X.520 postalAddress attribute type. The unstructured-address attribute type is intended for PKCS #6 extended certificates and PKCS #10 certification requests.

Unstructured-address attribute values have ASN.1 type UnstructuredAddress:

```
UnstructuredAddress ::= CHOICE {
    PrintableString, T61String }
```

An unstructured-address attribute can have multiple attribute values.

**Note.** T.61's newline character (hexadecimal code 0d) is recommended as a line separator in multi-line addresses.

It is expected that if UCS becomes an ASN.1 type (e.g., UNIVERSAL STRING), UnstructuredAddress will become a CHOICE type:

```
UnstructuredAddress ::= CHOICE {
    PrintableString, T61String, UNIVERSAL STRING }
```

## 6.9 Extended-certificate attributes

The extended-certificate-attributes attribute type specifies a set of attributes for a PKCS #6 extended certificate in a PKCS #10 certification request. (The value of the extended-certificate-attributes attribute becomes the attributes field of the requested PKCS #6 extended certificate.)

Extended-certificate-attributes attribute values have ASN.1 type ExtendedCertificateAttributes:

```
ExtendedCertificateAttributes ::= Attributes
```

An extended-certificate-attributes attribute must have a single attribute value. (That value is a set, which itself may contain multiple values, but there must only be one set.)

## 7. Object identifiers

This standard defines 10 object identifiers: pkcs-9, emailAddress, unstructuredName, contentType, messageDigest, signingTime, countersignature, challengePassword, unstructuredAddress, and extendedCertificateAttributes.

The object identifier pkcs-9 identifies this standard.

```
pkcs-9 OBJECT IDENTIFIER ::=
  { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 9 }
```

The object identifiers emailAddress, unstructuredName, contentType, messageDigest, signingTime, countersignature, challengePassword, unstructuredAddress, and extendedCertificateAttributes identify, respectively, the electronic-mail address, unstructured-name, content-type, message-digest, signing-time, countersignature, challenge-password, unstructured-address and extended-certificate-attributes attribute types.

```
emailAddress OBJECT IDENTIFIER ::= { pkcs-9 1 }
unstructuredName OBJECT IDENTIFIER ::= { pkcs-9 2 }
contentType OBJECT IDENTIFIER ::= { pkcs-9 3 }
messageDigest OBJECT IDENTIFIER ::= { pkcs-9 4 }
signingTime OBJECT IDENTIFIER ::= { pkcs-9 5 }
countersignature OBJECT IDENTIFIER ::= { pkcs-9 6 }
challengePassword OBJECT IDENTIFIER ::= { pkcs-9 7 }
unstructuredAddress OBJECT IDENTIFIER ::= { pkcs-9 8 }
```



```
extendedCertificateAttributes OBJECT IDENTIFIER ::=
    { pkcs-9 9 }
```

The object identifiers are intended to be used in the `attributeType` field of a value of type `Attribute`. The `attributeValue` field of that type, which has the syntax SET OF ANY, would have ASN.1 type SET OF `EmailAddress`, `UnstructuredName`, `ContentType`, `MessageDigest`, `SigningTime`, `Countersignature`, `ChallengePassword`, `UnstructuredAddress`, and `ExtendedCertificateAttributes`, respectively.

The `content-type`, `message-digest`, `signing-time`, `challenge-password` and `extended-certificate-attributes` attributes must have a single attribute value. All other attributes can have multiple attribute values.

## Revision history

### Version 1.0

Version 1.0 is part of the June 3, 1991 initial public release of PKCS. Version 1.0 was published as NIST/OSI Implementors' Workshop document SEC-SIG-91-24.

### Version 1.1

Version 1.1 incorporates several editorial changes, including updates to the references and the addition of a revision history. The following substantive changes were made:

- Section 6: Challenge-password, unstructured-address, and extended-certificate-attributes attribute types are added.
- Section 7: challengePassword, unstructuredAddress, and extendedCertificateAttributes object identifiers are added.

## Author's address

RSA Laboratories  
100 Marine Parkway  
Redwood City, CA 94065 USA

(415) 595-7703  
(415) 595-4126 (fax)  
pkcs-editor@rsa.com