PKCS #9:
Selected Attribute Types

RSA Data Security, Inc.
Redwood City, CA

June 3, 1991

Version 1.0

1. Scope

This standard defines selected attribute types for use in extended certificates [1], digitally signed messages [2], and private key information [3].

2. References

[1] RSA Data Security, Inc. *PKCS #6: Extended-Certificate Syntax Standard.* Version 1.4, June 1991.

[2] RSA Data Security, Inc. *PKCS #7: Cryptographic Message Syntax Standard.* Version 1.4, June 1991.

[3] RSA Data Security, Inc. *PKCS #8: Private-Key Information Syntax Standard.* Version 1.1, June 1991.

[4] CCITT. *Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1).* 1988.

[5] CCITT. *Recommendation X.509: The Directory—Authentication Framework.* 1988.

[6] CCITT. *Recommendation X.520: The Directory—Selected Attribute Types.* 1988.

[7] CCITT. *Recommendation X.402: Message Handling Systems—Overall Architecture.* 1988.

[8] Andrew Pollack. Universal computer code due. *New York Times*, February 20, 1991, pages D1, D5.

3. Definitions

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

ASN.1: Abstract Syntax Notation One, as defined in X.208 [4].

`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 three of the PKCS standards [1–3].

`ExtendedCertificate`: A type that consists of an X.509 public-key certificate [5] and a set of attributes, collectively signed by the issuer of the X.509 public-key certificate. This type is defined in PKCS #6 [1]. The `attributes` field, which has type `Attributes`, contains the attributes.

`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 [2].

`PrivateKeyInfo`: A type that specifies a private key and extended attributes. The `attributes` field, which has type `Attributes`, contains the extended attributes. This type is defined in PKCS #8 [3].

`SignerInfo`: A type that specifies per-signer information in the signed-data content type. The `authenticatedAttributes` field, which has type `Attributes`, contains a set of attributes authenticated by the signer, the `encryptedDigest` field contains the signer's signature, and the `unauthenticatedAttributes` field, which has type `Attributes`, contains a set of attributes not authenticated by the signer. This type is defined in PKCS #7 [2].

DER: Distinguished Encoding Rules for ASN.1, as defined in X.509 [5], Section 8.7.

4. Symbols and abbreviations

No symbols or abbreviations are defined in this standard.

5. General overview

The next three sections specify attribute types for PKCS #6, #7 and #8. The sections also list attribute types defined elsewhere that may be useful in those standards.

The object identifier for this standard is `pkcs-9`:

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

6. PKCS #6 attribute types

This section defines attribute types for PKCS #6 (Extended-Certificate Syntax Standard).

Attributes in PKCS #6 are used in the `attributes` field of the `CertificateWith-Attributes` type to represent extra information that is input to the certification process along with an ordinary X.509 certificate.

Two attribute types are defined: electronic-mail address and unstructured name.

Note. Several attribute types defined in X.520 [6] and X.402 [7] might also be useful in PKCS #6 in providing additional information about the subject of a certificate. Attributes that might have an application include the following:

X.520 attribute types:

```
businessCategory                commonName
countryName                     description
destinationIndicator            facsimileTelephoneNumber
iSDNAddress                     localityName
member                          objectClass
organizationName                physicalDeliveryOfficeName
postalAddress                   postalCode
postOfficeBox                   preferredDeliveryMethod
presentationAddress             registeredAddress
roleOccupant                    serialNumber
stateOrProvinceName             streetAddress
supportedApplicationContext     surname
telephoneNumber                 teletexTerminalIdentifier
telexNumber                     title
x121Address
```

X.402 attribute types:

```
mhs-or-address
```

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 has object identifier `emailAddress` and electronic-mail address attribute values have ASN.1 type `EmailAddress`:

```
emailAddress OBJECT IDENTIFIER ::= { pkcs-9 1 }

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 has object identifier `unstructuredName` and unstructured-name attribute values have ASN.1 type `UnstructuredName`:

```
unstructuredName OBJECT IDENTIFIER ::= { pkcs-9 2 }

UnstructuredName ::= IA5String
```

An unstructured-name attribute can have multiple attribute values.

Note. It is expected that if Unicode [8] receives a universal ASN.1 type, `UnstructuredName` will become a `CHOICE` type:

```
UnstructuredName ::= CHOICE { IA5String, Unicode }
```

7. PKCS #7 attribute types

This section defines attribute types for PKCS #7 (Cryptographic Message Syntax Standard).

Attributes in PKCS #7 are used in the `authenticatedAttributes` and `unauthenticatedAttributes` fields of a `SignerInfo` value. In the first field, the attributes represent extra information that is input to the signature process along with the content being signed. In the second field, the attributes represent extra information that is associated with the signature, but is not input to the signature process.

Four attribute types are defined: content type, message digest, signing time, and countersignature.

7.1 Content type

The content-type attribute type specifies the content type of the `ContentInfo` value being signed.

The `authenticatedAttributes` field of a `SignerInfo` value must contain a content-type attribute if it contains any other attribute.

The content-type attribute type has object identifier `contentType` and content-type attribute values have ASN.1 type `ContentType`:

```
contentType OBJECT IDENTIFIER ::= { pkcs-9 3 }

ContentType ::= OBJECT IDENTIFIER
```

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

7.2 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, where the message digest is computed under the signer's message digest algorithm.

The `authenticatedAttributes` field of a `SignerInfo` value must contain a message-digest attribute if it contains any other attribute.

The message-digest attribute type has object identifier `messageDigest` and message-digest attribute values have ASN.1 type `MessageDigest`:

```
messageDigest OBJECT IDENTIFIER ::= { pkcs-9 4 }

MessageDigest ::= OCTET STRING
```

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

7.3 Signing time

The signing-time attribute type specifies the time at which the signer (purportedly) performed the signing process.

The signing-time attribute type has object identifier `signingTime` and signing-time attribute values have ASN.1 type `SigningTime`:

```
signingTime OBJECT IDENTIFIER ::= { pkcs-9 5 }
```

```
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.

7.4 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. Thus, the countersignature attribute type countersigns (signs in serial) another signature.

The countersignature attribute must be an unauthenticated attribute; it cannot be an authenticated attribute.

The countersignature attribute type has object identifier `countersignature` and countersignature attribute values have ASN.1 type `Countersignature`:

```
countersignature OBJECT IDENTIFIER ::= { pkcs-9 6 }

Countersignature ::= SignerInfo
```

`Countersignature` values have the same meaning as `SignerInfo` values for ordinary signatures (see Section 8 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.

8. PKCS #8 attribute types

This section defines attribute types for PKCS #8 (Private-Key Information Syntax Standard).

Attributes in PKCS #8 are used in the `attributes` field of the `PrivateKeyInfo` type.

No attribute types are currently defined.