PKCS #5 v2.0 Amendment 1:
XML Schema for Password-Based Cryptography

FINAL DRAFT

RSA, The Security Division of EMC

13 October 2006

TABLE OF CONTENTS

1 Introduction

1.1 Scope

This document provides an XML schema for the functions and schemes defined in PKCS #5 Version 2.0 [1].

1.2 Background

PKCS #5 Version 2.0 defines a number of functions and schemes related to password-based cryptography. To make use of these constructs in an interoperable manner, PKCS #5 v2.0 provides an ASN.1 module containing object identifiers identifying the defined algorithms and ASN.1 type definitions for their parameters. This enables the exchange of PKCS #5-derived data in ASN.1-oriented environments.

An XML schema containing syntactical definitions of functions and schemes defined in PKCS #5 v2.0 is useful in web service-oriented contexts which make use of XML but do not make use of ASN.1 As an example, a need for such definitions arise when data is encrypted with keys that are derived from pass-phrases using constructs from PKCS #5 v2.0 and sent using WS-Security [2]. This document provides identifiers for the algorithms defined in PKCS #5 v2.0 as well as XML type definitions for their parameters.

1.3 Document organization

The organization of this document is as follows:

- Section 1 is an introduction.
- Section 2 defines acronyms and notation used in this document.
- Section 3 describes the XML schema for PKCS #5 v2.0.
- Appendix A contains the XML schema
- Appendix B contains some examples.
- Appendices C, D, and E cover intellectual property issues, give references to other publications and standards, and provide general information about the Public Key Cryptography Specifications.

2 Acronyms and notation

2.1 Acronyms

ASN.1	Abstract Syntax Notation One
URI	Uniform Resource Identifier
XML	Extensible Markup Language

2.2 Notation

XML elements are written in brackets and bold Helvetica: **<element>**. XML attributes are written in italics and bold Helvetica: ***attribute***. XML types are written in bold Helvetica: **xmlType**. ASN.1 types are written in Courier: `ASN1Type`.

3 XML definitions for PKCS #5 v2.0

3.1 Function and scheme identifiers

The following identifiers shall be used to identify the algorithms defined in [1] :

PBKDF2: **http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-5#pbkdf2**

PBES2: **http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-5#pbes2**

PBMAC1: **http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-5#pbmac1**

3.2 Algorithm parameter types

3.2.1 Background

The XML Encryption Recommendation [3] states: “Any … additional parameters to an algorithm appear as content elements within the [xenc:EncryptionMethodType] element. Such parameter child elements have descriptive element names, which are frequently algorithm specific, and SHOULD be in the same namespace as … an algorithm specific namespace.” Similarly, the XML Digital Signature Recommendation [4] states: “Explicit additional parameters to an algorithm appear as content elements within the algorithm role element. Such parameter elements have a descriptive element name, which is frequently algorithm specific, and MUST be in … an algorithm specific namespace.” This document follows these recommendations by defining explicit parameters for the identified algorithms in the same namespace as the algorithms themselves, using descriptive element names.

3.2.2 The AlgorithmIdentifierType type

The **AlgorithmIdentifierType** corresponds to the `AlgorithmIdentifier` type of [1] and carries the algorithm identifier in the ***Algorithm*** attribute. Algorithms shall be identified using a URI. Algorithm-specific parameters are carried in the **<Parameters>** element, when applicable.

```
<xs:complexType name="AlgorithmIdentifierType">
        <xs:sequence>
            <xs:element name="Parameters" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="Algorithm"/>
</xs:complexType>
```

3.2.3 The PBKDF2ParameterType type

This type corresponds to the `PBKDF2-params` type from [1] and carries parameters associated with the PBKDF2 function. Child elements of this type have the same names and the same meaning as the corresponding components of the `PBKDF-params` type.

```
<xs:complexType name="PBKDF2ParameterType">
        <xs:sequence>
            <xs:element name="Salt">
                <xs:complexType>
                    <xs:choice>
                      <xs:element name="Specified" type="xs:base64Binary"/>
                      <xs:element name="OtherSource" type="SaltAlgorithmIdentifierType"/>
                    </xs:choice>
                </xs:complexType>
            </xs:element>
            <xs:element name="IterationCount" type="xs:positiveInteger"/>
            <xs:element name="KeyLength" type="xs:positiveInteger"/>
            <xs:element name="PRF" type="PRFAlgorithmIdentifierType"/>
        </xs:sequence>
</xs:complexType>
```

3.2.4 The PBES2ParameterType type

This type corresponds to the `PBES2-params` type from [1] and carries parameters associated with the PBES2 encryption scheme. Child elements of this type have the same names and the same meaning as the corresponding components of the `PBES2-params` type.

```
<xs:complexType name="PBES2ParameterType">
        <xs:sequence>
            <xs:element name="KeyDerivationFunc" type="AlgorithmIdentifierType"/>
            <xs:element name="EncryptionScheme" type="xenc:EncryptionMethodType"/>
        </xs:sequence>
</xs:complexType>
```

3.2.5 The PBMAC1ParameterType type

This type corresponds to the PBMAC1-params type from [] and carries parameters associated with the PBMAC1 message authentication scheme. Child elements of this type have the same names and the same meaning as the corresponding components of the `PBMAC1-params` type.

```
<xs:complexType name="PBMAC1ParameterType">
        <xs:sequence>
            <xs:element name="KeyDerivationFunc" type="AlgorithmIdentifierType"/>
            <xs:element name="MessageAuthScheme" type="ds:SignatureMethodType"/>
        </xs:sequence>
</xs:complexType>
```

3.3 Elements for use with XML Encryption and XML Digital Signatures

The following elements are to be used e.g. in instances of the XML Encryption **xenc:EncryptionMethodType** or instances of the XML Digital Signature [4] **ds:SignatureMethodType**:

The **<PBKDF2-params>** element shall be used in instances of the **xenc:EncryptionMethodType** when the ***Algorithm*** attribute of that type identifies the PBKDF2 key derivation function.

The **<PBES2-params>** element shall be used in instances of the **xenc:EncryptionMethodType** when the ***Algorithm*** attribute of that type identifies the PBES2 encryption scheme.

The **<PBMAC1-params>** element shall be used in instances of the **ds:SignatureMethodType** when the ***Algorithm*** attribute of that type identifies the PBMAC1 message authentication scheme.

```
<xs:element name="PBKDF2-params" type="PBKDF2ParameterType"/>

<xs:element name="PBES2-params"  type="PBES2ParameterType"/>

<xs:element name="PBMAC1-params" type="PBMAC1ParameterType"/>
```

A. XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Schema file for PKCS #5 v2.0 -->
<!-- $Revision: 1.4 $ $Date: 2006/10/12 15:47:50 $ -->

<!-- Copyright (c) RSA, The Security Division of EMC 2006. All rights reserved. -->
<!-- License to copy and use this schema file is granted provided that
     it is identified as "RSA Public Key Cryptography
     Standard #5 (PKCS #5): Password-based Encryption Version 2.0"
     in all material mentioning or referencing it.

     RSA makes no representations concerning either the
     merchantability of this schema or the suitability of this schema
     for any particular purpose. It is provided "as is" without
     express or implied warranty of any kind.
-->

<xs:schema
  targetNamespace="http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-5v2-0#"
  xmlns="http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-5v2-0#"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">

  <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
   schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-
schema.xsd"/>

  <xs:import namespace="http://www.w3.org/2001/04/xmlenc#"
   schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd"/>

<!-- Basic types -->
<xs:complexType name="AlgorithmIdentifierType">
  <xs:sequence>
    <xs:element name="Parameters" minOccurs="0"/>
  </xs:sequence>
  <xs:attribute name="Algorithm"/>
</xs:complexType>

<xs:complexType name="SaltAlgorithmIdentifierType">
  <xs:complexContent>
    <xs:restriction base="AlgorithmIdentifierType">
      <xs:attribute name="Algorithm" type="xs:anyURI"
      default="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="PRFAlgorithmIdentifierType">
  <xs:complexContent>
    <xs:restriction base="AlgorithmIdentifierType">
      <xs:attribute name="Algorithm" type="xs:anyURI"
      default="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="PBKDF2ParameterType">
```

```
  <xs:sequence>
    <xs:element name="Salt">
      <xs:complexType>
        <xs:choice>
          <xs:element name="Specified" type="xs:base64Binary"/>
          <xs:element name="OtherSource" type="SaltAlgorithmIdentifierType"/>
        </xs:choice>
      </xs:complexType>
    </xs:element>
    <xs:element name="IterationCount" type="xs:positiveInteger"/>
    <xs:element name="KeyLength" type="xs:positiveInteger"/>
    <xs:element name="PRF" type="PRFAlgorithmIdentifierType"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="PBES2ParameterType">
  <xs:sequence>
    <xs:element name="KeyDerivationFunc" type="AlgorithmIdentifierType"/>
    <xs:element name="EncryptionScheme" type="xenc:EncryptionMethodType"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="PBMAC1ParameterType">
  <xs:sequence>
    <xs:element name="KeyDerivationFunc" type="AlgorithmIdentifierType"/>
    <xs:element name="MessageAuthScheme" type="ds:SignatureMethodType"/>
  </xs:sequence>
</xs:complexType>

<!-- Exports -->
<xs:element name="PBKDF2-params" type="PBKDF2ParameterType"/>
<xs:element name="PBES2-params"  type="PBES2ParameterType"/>
<xs:element name="PBMAC1-params" type="PBMAC1ParameterType"/>
</xs:schema>
```

B. Examples

The following is an example of an **<xenc:EncryptedKey>** element using the constructs defined herein:

```
<xenc:EncryptedKey
  xmlns:pkcs-5="http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-5v2-0#"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  Type="http://www.some-key-type.com">
  <xenc:EncryptionMethod
    Algorithm="http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-5#pbes2">
    <pkcs-5:PBES2-params>
      <KeyDerivationFunc
        Algorithm="http://www.rsasecurity.com/rsalabs/pkcs/schemas/pkcs-5#pbkdf2">
        <Parameters xsi:type="pkcs-5:PBKDF2ParameterType">
          <Salt>
            <Specified>32113435</Specified>
          </Salt>
          <IterationCount>1024</IterationCount>
          <KeyLength>128</KeyLength>
          <PRF/>
        </Parameters>
      </KeyDerivationFunc>
```

```
   <EncryptionScheme Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128-cbc">
   </EncryptionScheme>
  </pkcs-5:PBES2-params>
 </xenc:EncryptionMethod>
 <ds:KeyInfo>
  <ds:KeyName>Passphrase1</ds:KeyName>
 </ds:KeyInfo>
 <xenc:CipherData>
  <xenc:CipherValue>qwertyuiopasqwdftroewdsw</xenc:CipherValue>
 </xenc:CipherData>
 <xenc:CarriedKeyName>43212093</xenc:CarriedKeyName>
</xenc:EncryptedKey>
```

C. Intellectual property considerations

RSA makes no patent claims on the general constructions described in this document, although specific underlying techniques may be covered.

Copyright © 2006 RSA, The Security Division of EMC. All rights reserved. License to copy this document and furnish the copies to others is granted provided that the above copyright notice is included on all such copies. This document should be identified as "RSA Public-Key Cryptography Standards (PKCS)" in all material mentioning or referencing this document.

RSA is a registered trademark of RSA, The Security Division of EMC, in the United States and/or other countries. The names of other products or services mentioned may be the trademarks of their respective owners.

This document and the information contained herein are provided on an "AS IS" basis and RSA DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. RSA makes no representations regarding intellectual property claims by other parties. Such determination is the responsibility of the user.

D. References

[1] RSA Laboratories, *PKCS #5: Password-Based Cryptography Standard*. Version 2.0, March 1999. URL: ftp://ftp.rsasecurity.com/pub/pkcs/

[2] OASIS, "*Web Services Security: SOAP Message Security*." Version 1.1, February 2006. URL: http://tinyurl.com/knnxm

[3] World Wide Web Consortium, "*XML Encryption Syntax and Processing*." W3C Recommendation, December 2002. URL: http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[4] World Wide Web Consortium, "*XML Signature Syntax and Processing*." W3C Recommendation, February 2002. URL: http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

E. About PKCS

The *Public Key Cryptography Standards* are documents produced by RSA in cooperation with secure systems developers for the purpose of simplifying integration and management of accelerating the deployment of public-key cryptography and strong authentication technology into secure applications, and to enhance the user experience of these technologies.

RSA plans further development of the PKCS series through mailing list discussions and occasional workshops, and suggestions for improvement are welcome. Results may also be submitted to standards forums. For more information, contact:

PKCS Editor
RSA, The Security Division of EMC
174 Middlesex Turnpike
Bedford, MA 01730 USA
pkcss-editor@rsasecurity.com
http://www.rsasecurity.com/rsalabs/