XML Encryption, XML Signature, and Derived Keys: Suggestion For a Minor Addition

Magnus Nyström
RSA
RSA Laboratories PKCS #5 deals with “password-based cryptography”
- i.e., how to derive keys from shared secrets such as passwords
- These keys are then used for encryption or message authentication

PKCS #5 syntax originally in ASN.1
- Natural for use with S/MIME, etc.

XML syntax published in 2007
PKCS #5 XML Syntax (snippet)

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

For use in xenc:EncryptionMethod
•  <xenc:EncryptionMethod
    Algorithm = rsa.com../pkcs-5#pbes2)
  <pkcs-5:PBES2-params>
    <KeyDerivationFunc
      Algorithm="http://www.rsasecurity.com/.../pkcs-5#pbkdf2">
        ...
    </KeyDerivationFunc>
    <EncryptionScheme
      Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc">
      
    </EncryptionScheme>
  </pkcs-5:PBES2-params></xenc:EncryptionMethod>
```
What’s Missing?

- An ability to inform a recipient that she should use a key derived from a known pass-phrase (or other shared secret) for *multiple* encrypted data (or authenticated data) instances
  - A single encrypted (authenticated) data works with current approach (PBES2/PBMAC1)
  - WS-I also recommends forward cross-referencing in this case

- It was felt this should be an extension to XML Enc/ XML Dsig rather than PKCS
  - Too generic – Derived Key

- The current gap causes some issues – e.g. in IETF KEYPROV that leverages PKCS #5
  - Had to define their own Derived Key key type
One (out of many!) Possible Way to Do It

- Modeled after `<xenc:EncryptedKeyType>`
- `<element name="DerivedKey" type="xmlsec:DerivedKeyType"/>`
- `<complexType name="DerivedKeyType">
  <sequence>
    <element name="KeyDerivationMethod"
      type="xmlsec:KeyDerivationMethodType" minOccurs="0"/>
    <element ref="xenc:ReferenceList" minOccurs="0"/>
    <element name="CarriedKeyName" type="string" minOccurs="0"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
  <attribute name="Type" type="anyURI" use="optional"/>
</complexType>"
There are use cases for a “Derived Key” key type

They are not currently covered by XML Enc, XML Dsig (or by PKCS #5)

XML Security Group could be a natural place to introduce this

Would like to contribute in this area of work

Happy to take on editing responsibility in this regard