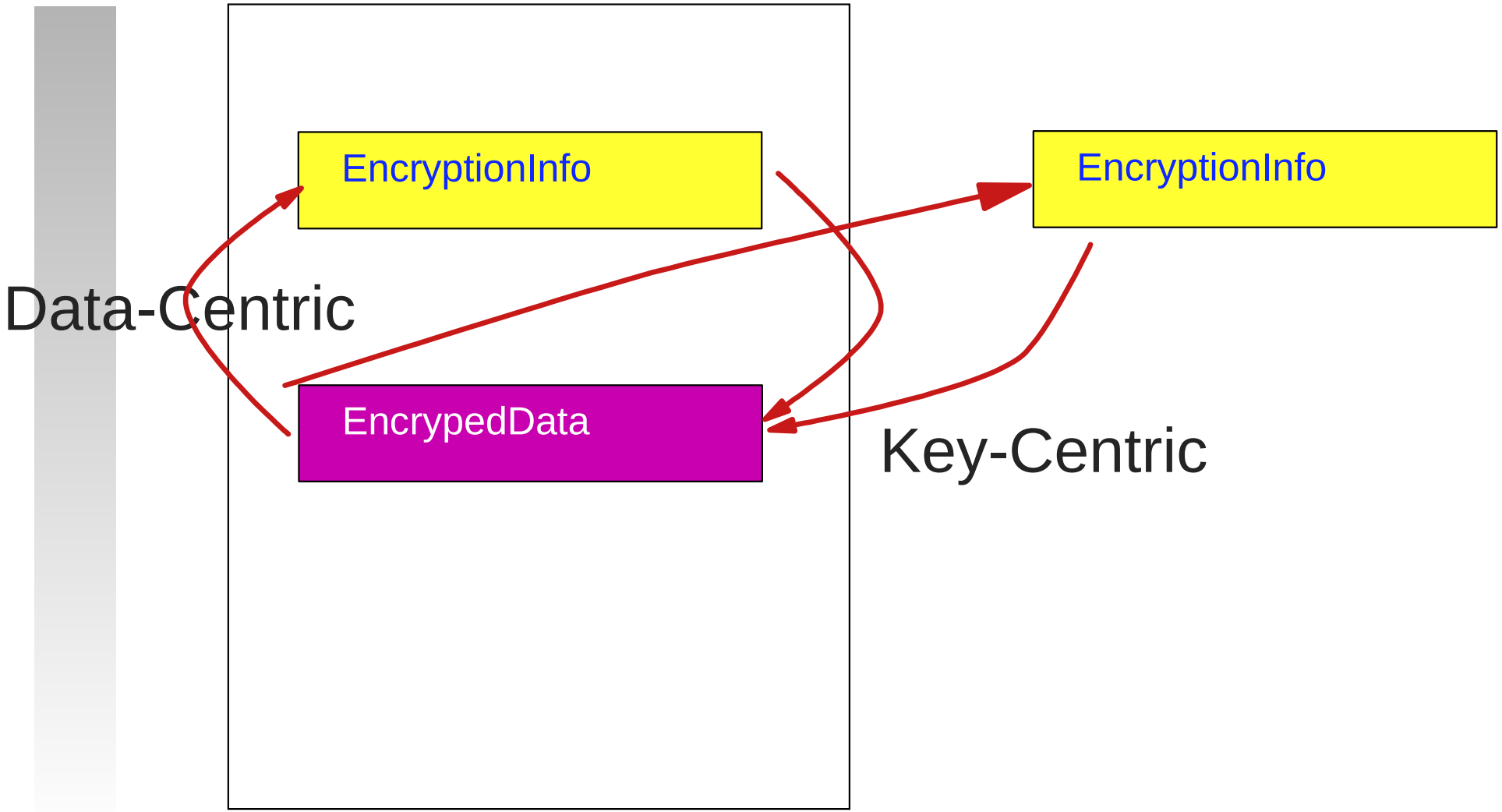
Proposal:
Syntax for Keying Information & Encryption Algorithm

Hiroshi Maruyama
Tokyo Research Laboratory
IBM Research

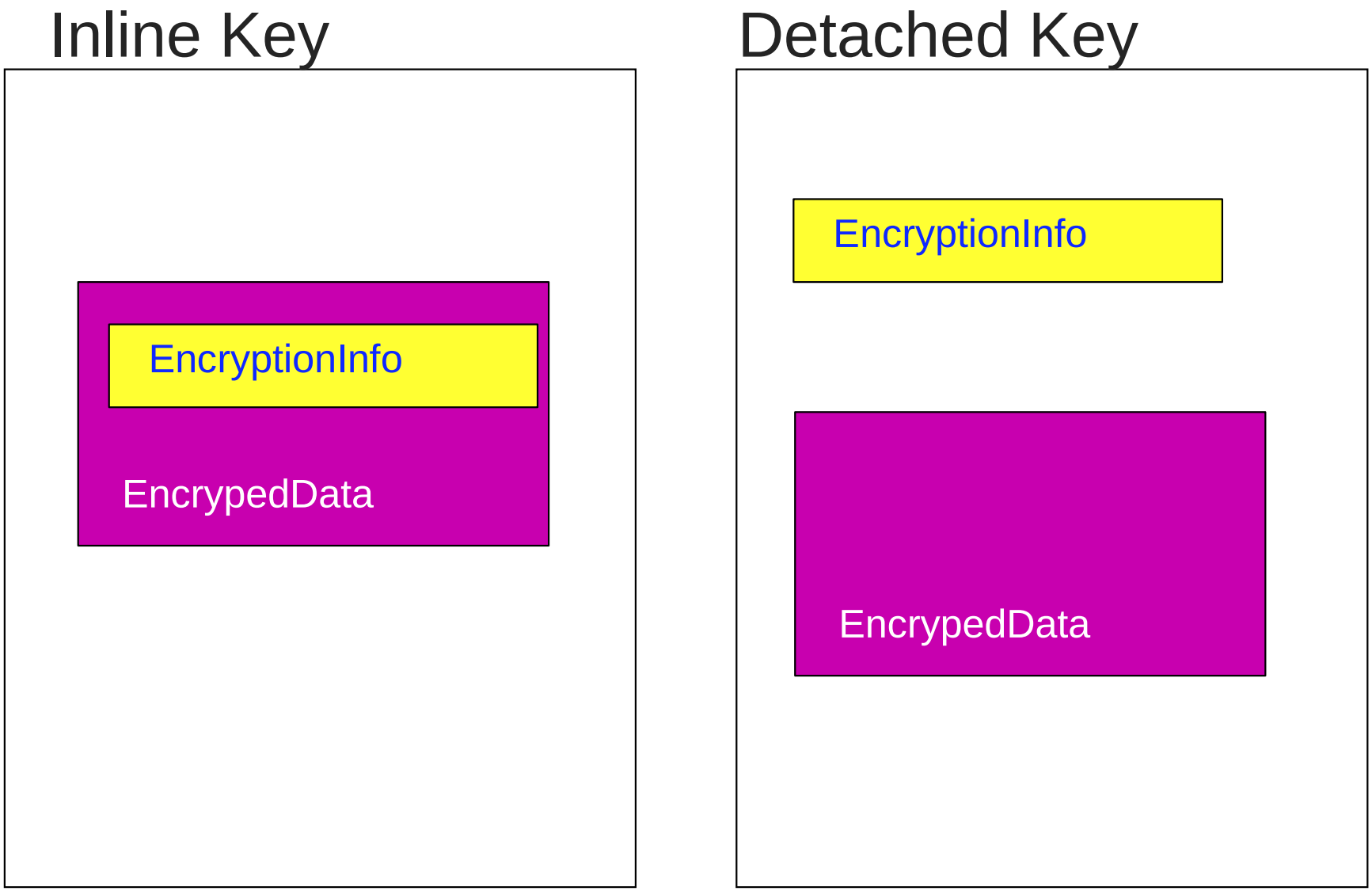
Introduction

- Focused on EncryptionInfo (DecryptionInfo)
- Design principles:
  - Alignment with XML Signature (i.e., reuse of KeyInfo!)
  - Reuse of content-encryption mechanism for key-encryption
- Design assumptions on Node Encryption
  - Node substitution model:
    - An item is encrypted into an element, with which the item is replaced
    - Encrypted node is well-formed
    - InfoSet preserve
  - Encryption keys represented as elements or text strings
  - Either inline key (<EncryptionInfo> in <EncryptedData>) or detached key
  - Key-centric processing and Data-centric processing

Data-Centric vs Key-Centric



Inline Key vs Detached Key



Syntax Overview

```
<EncryptionInfo xmlns="http://www.w3.org/2000/10/xmlenc" (Id=)?>
   (EncryptionMethod (Algorithm=))        for encryption algorithm
   (EncryptionPropertyList)?              for meta-information
   <ReferenceList>
      (Reference (URI=)? (XPath=)?)+      for reference to encrypted data
   </ReferenceList>?
   (KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#")
</EncryptionInfo>                         for encryption key
```

Example 1: Base case

```
[01] <EncryptionInfo xmlns="http://www.w3.org/2000/10/xmlenc"
                          Id="encryptionInfo23">
[02]   <EncryptionMethod Algorithm="http://.../xmlenc#des-cbc-pkcs5padding"/>
[03]   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
[04]     <KeyValue>MC0CFFrV...</KeyValue>
[05]   </KeyInfo>
[06] </EncryptionInfo>
```

Example 2: Use of Key Name (shared symmetric key)

```
[01] <EncryptionInfo xmlns="http://www.w3.org/2000/10/xmlenc"
                          Id="encryptionInfo23">
[02]   <EncryptionMethod Algorithm="http://.../xmlenc#des-cbc-pkcs5padding"/>
[03]   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
[04]     <KeyName>1234</KeyName>
[05]   </KeyInfo>
[06] </EncryptionInfo>
```

Example 2: Use of Manifest Enabling Key-centric Processing

```
[01] <EncryptionInfo xmlns="http://www.w3.org/2000/10/xmlenc">
[02]   <EncryptionMethod Algorithm="http://.../xmlenc#des-cbc-pkcs5padding"/>
[03]   <ReferenceList>
[04]     <Reference URI="#encryptedData11"/>
[05]   </ReferenceList>
[06]   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
[07]     <KeyName>1234</KeyName>
[08]   </KeyInfo>
[09] </EncryptionInfo>
```

Example 3:
Using Key Transport (1/3)

```
[01] <EncryptionInfo xmlns="http://www.w3.org/2000/10/xmlenc"
                          Id="encryptionInfo23">
[02]   <EncryptionMethod Algorithm="http://.../xmlenc#des-cbc-pkcs5padding"/>
[03]   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
[04]     <KeyValue>MC0CFFrV...</KeyValue>
[05]   </KeyInfo>
[06] </EncryptionInfo>
```

This is to be encrypted
by recipient's public key

Example 3:
Using Key Transport (2/3)

```
[01] <EncryptionInfo xmlns="http://www.w3.org/2000/10/xmlenc" Id="encryptionInfo23">
[02]   <EncryptionMethod Algorithm="http://.../xmlenc#des-cbc-pkcs5padding"/>
[03]   <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
[04a]   <ds:KeyValue>
[04b]     <EncryptedData URI="#encryptionInfo27">k0xFFH56...</EncryptedData>
[04c]   </ds:KeyValue>
[05]   </ds:KeyInfo>
[06] </EncryptionInfo>

[07] <EncryptionInfo xmlns="http://www.w3.org/2000/10/xmlenc" Id="encryptionInfo27">
[08]   <EncryptionMethod Algorithm="http://www.w3.org/2000/10/xmlenc#rsa"/>
[09]   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
[10]     <X509Data>...</X509Data>
[11]   </KeyInfo>
[12] </EncryptionInfo>
```

Example 3:
Inline EncryptionInfo

```
[01] <EncryptionInfo xmlns="http://www.w3.org/2000/10/xmlenc" Id="encryptionInfo23">
[02]   <EncryptionMethod Algorithm="http://.../xmlenc#des-cbc-pkcs5padding"/>
[03]   <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
[04a]   <ds:KeyValue>
[04b]     <EncryptedData>
[04c]       <EncryptionInfo>
[04d]         <EncryptionMethod Algorithm="http://www.w3.org/2000/10/xmlenc#rsa"/>
[04e]         <ds:KeyInfo>
[04f]           <ds:X509Data>...</ds:X509Data>
[04g]         </ds:KeyInfo>
[04h]       </EncryptionInfo>
[04i]       <CipherText>k0xFFH56...</CipherText>
[04j]     </EncryptedData>
[04k]   </ds:KeyValue>
[05]   </ds:KeyInfo>
[06] </EncryptionInfo>
```

Example 5: Including Meta-Information

```
[01] <EncryptionInfo xmlns="http://www.w3.org/2000/10/xmlenc" Id="encryptionInfo23">
[02]   <EncryptionMethod Algorithm="http://.../xmlenc#des-cbc-pkcs5padding"/>
[03]   <EncryptionPropertyList>
[04]     <EncryptionProperty>
[05]       <timestamp xmlns="http://www.ietf.org/rfcxxxx.txt">
[06]         <date>20001027</date>
[07]         <time>192030</time>
[08]       </timestamp>
[09]     </EncryptionProperty>
[10]   </EncryptionPropertyList>
[11]   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
[12]     <KeyName>1234</KeyName>
[13]   </KeyInfo>
[14] </EncryptionInfo>
```

Discussions

- What data model is suitable for XML Encryption and <EncryptionInfo> and which should be adopted?
- What should be added to (or deleted from) <EncryptionInfo>?
- How should <EncryptionInfo> and <EncryptedData> reference each other?
- Any other algorithms?
- Interaction with Signature

Use of "Decrypt" Transform

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod
      Algorithm="http://www.w3.org/TR/2000/WD-xml-c14n-20001011">
    </ds:CanonicalizationMethod>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
    <ds:Reference URI="#Body">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/10/xmlenc#decrypt">
          <xenc:Reference
            xmlns:xenc="http://www.w3.org/2000/10/xmlenc"
            URI="#encData1"/>
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>MC0CFFrVLtRlk=...</ds:SignatureValue>
</ds:Signature>
```

Need to know about encryption before signature