古今東西
XML署名フォーマット

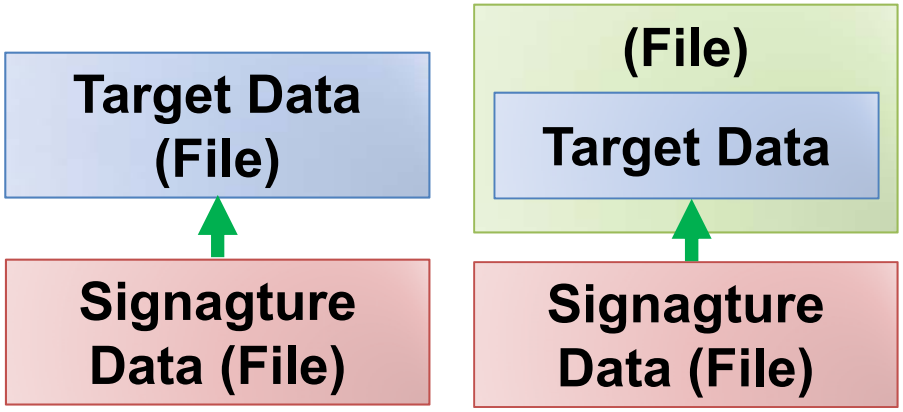
～電子申請/署名コンテナの書式を読み解く～

有限会社ラング・エッジ
宮地 直人（miyachi@langedge.jp）

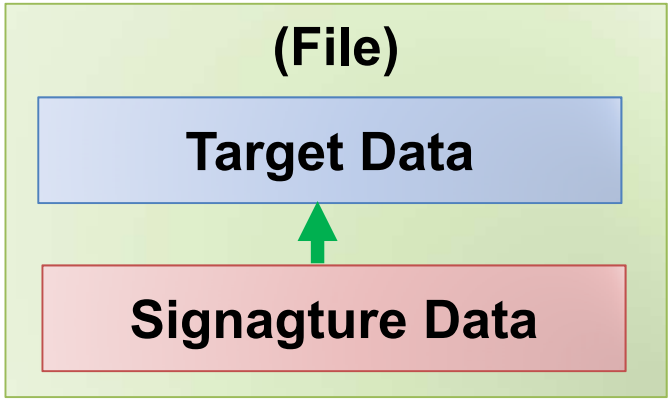
２０１７年5月２２日

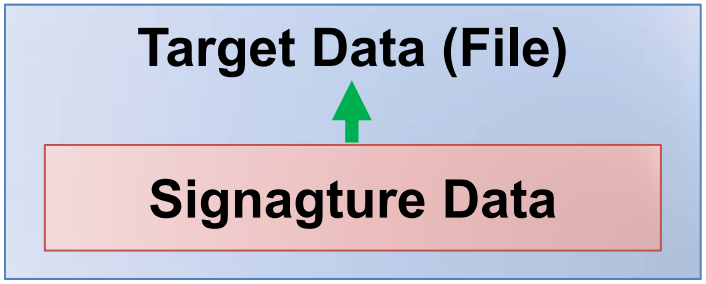
基本1：XML署名の参照方式（Reference種別）

外部Detached と 外部部分署名



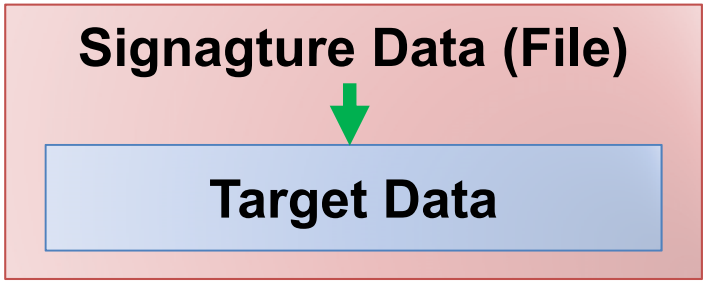
内部Detached（内部部分署名）





Enveloped（外包）

※ 署名値計算時に署名部を省く



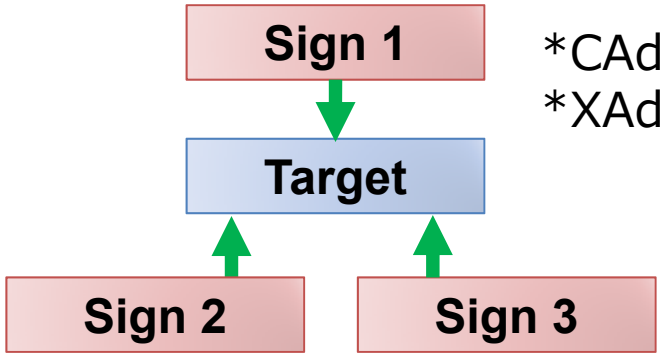
Enveloping（内包）

※ 対象をds:Objectとして埋め込む

基本2：複数署名の種類（パターンの一例です）

並列署名

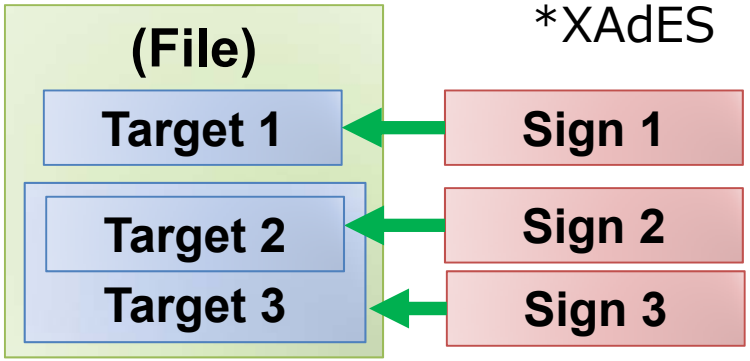
並列署名（Parallel Signatures）



*CAdES
*XAdES

部分署名（Partial Signatures）

*XAdES

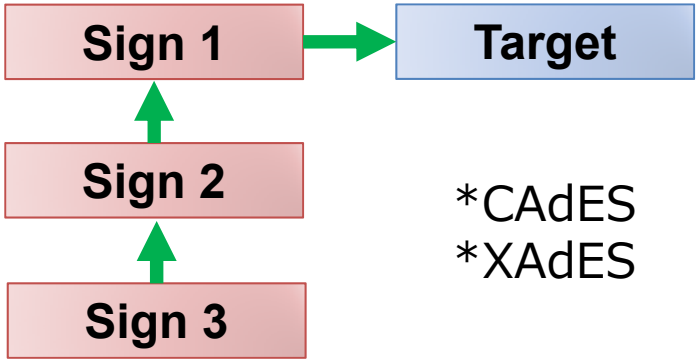


直列署名

シリアル署名（Serial Signatures）

*PAdES

カウンタ署名（Counter Signatures）



*CAdES
*XAdES

基本3：XML署名の利点（注：個人的意見です :-）

利点その１：

複数の参照方式を混在指定可能

例えば、Envelopedと、外部Detachedを、一度に指定した利用で両方（本体＋外部）を守れる。

利点その２：

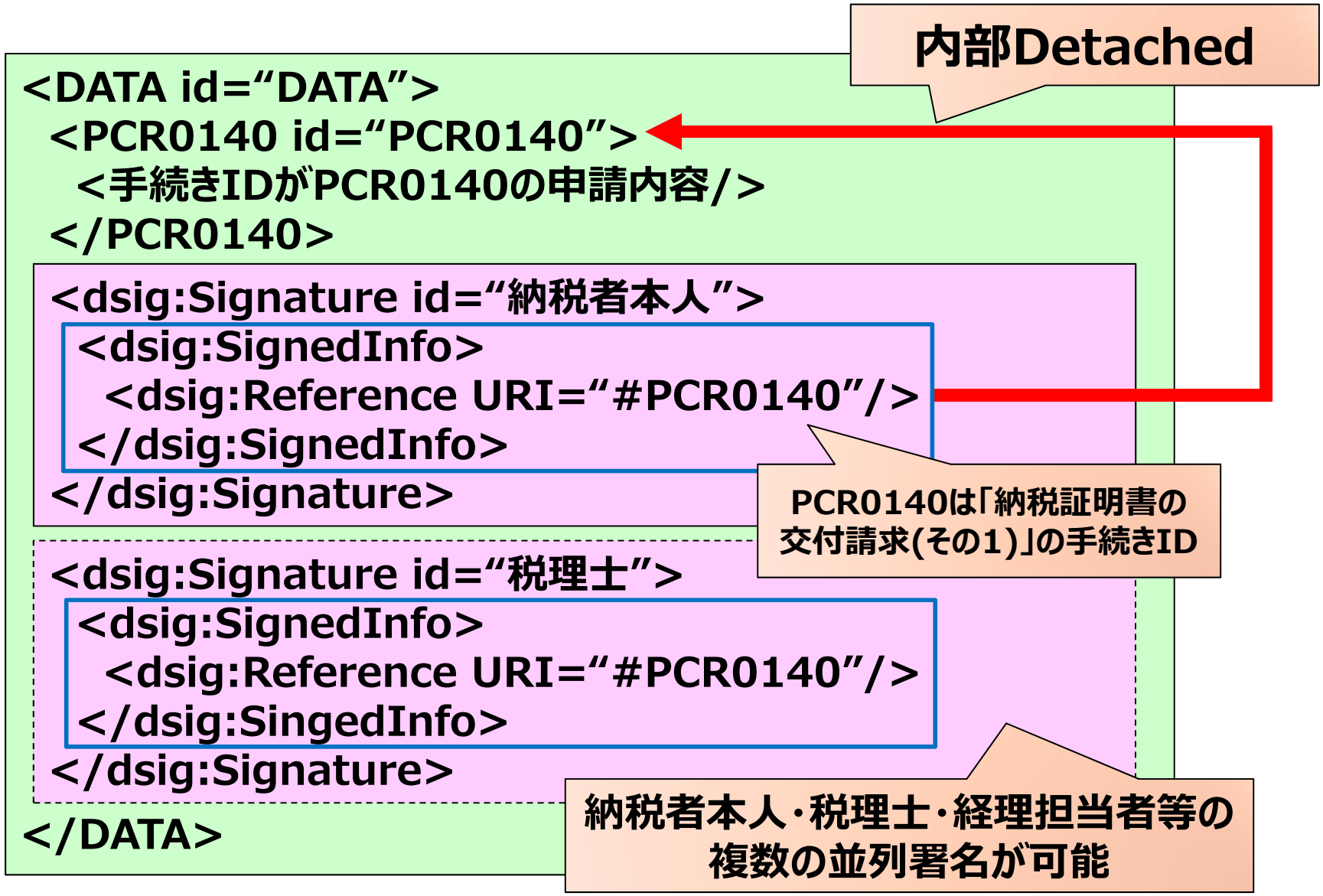
色々な複数署名方式に対応可能

更に混在も可能、例えば並列署名と部分署名の混在。

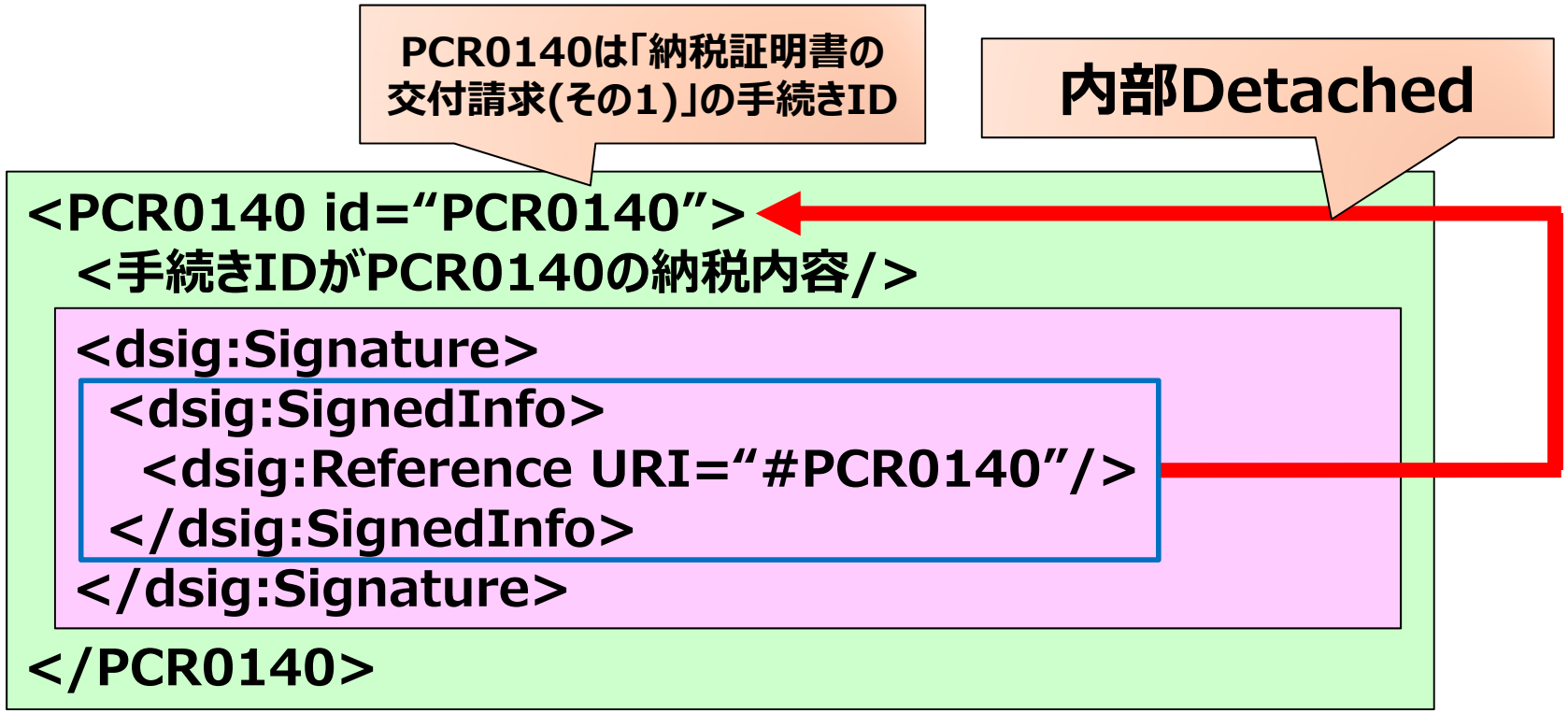
利点その３：

Java/.NETで機能が標準利用可能

e-Tax 送信データ (電子申請)



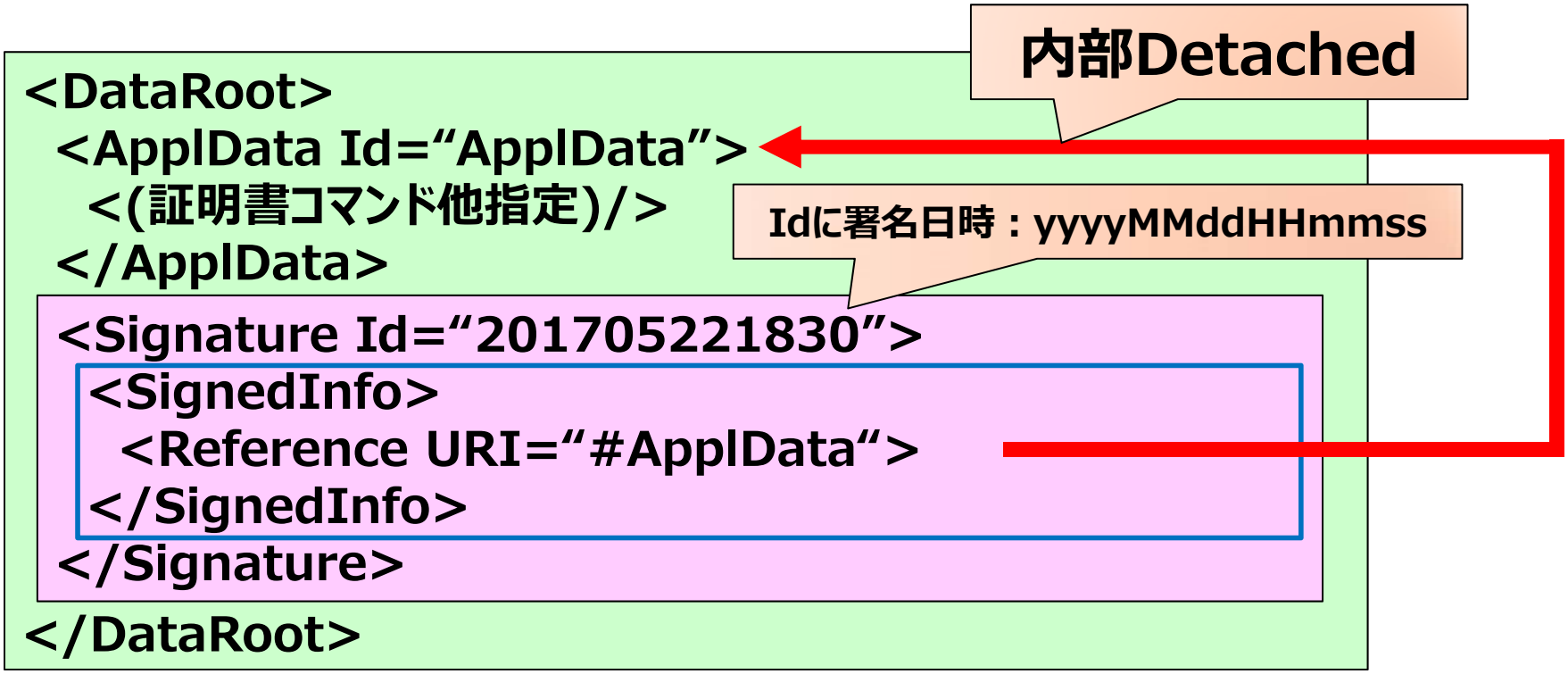
e-Tax 電子納税証明書



考察：

内部Detachedになっているけど、形式としては Enveloped（外包）の方が良いかも。

e-Gov API認証用の電子署名（証明書管理）



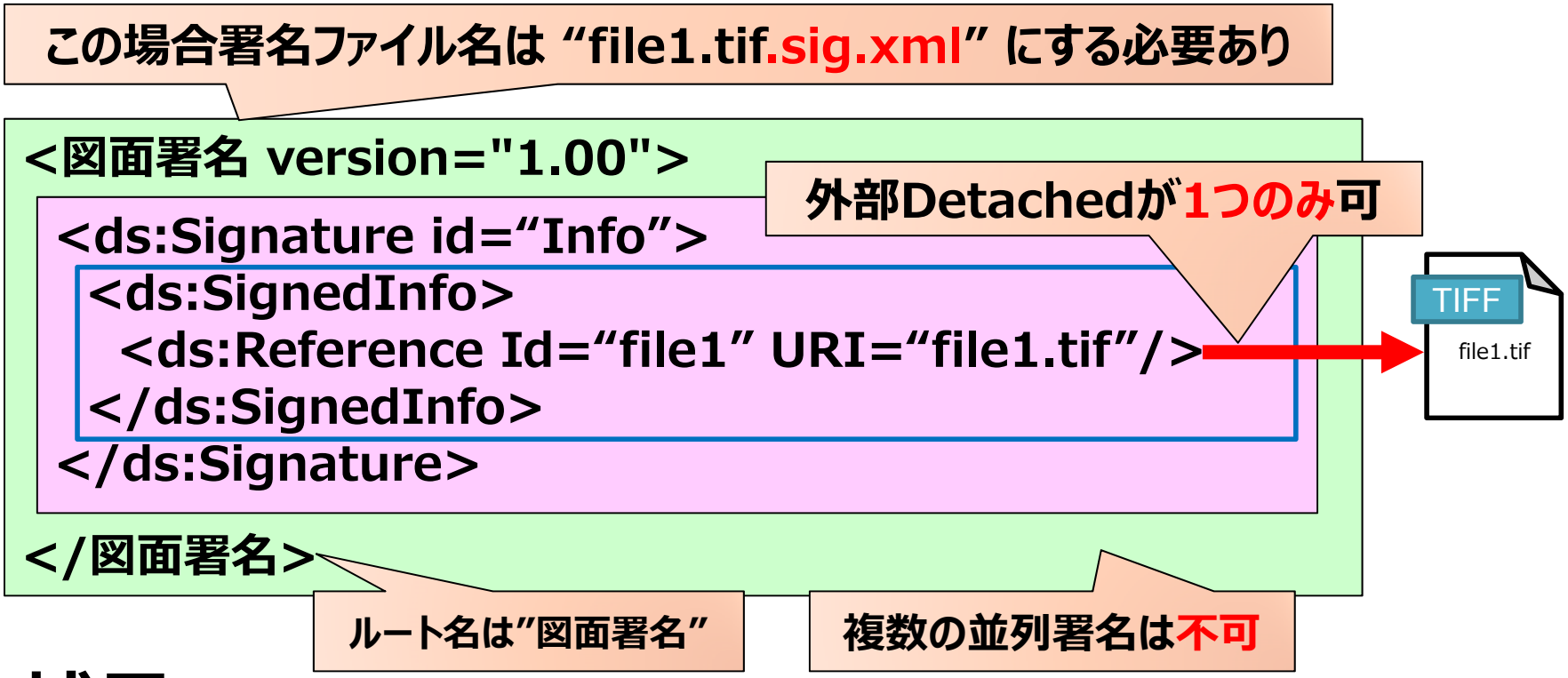
コマンド例：利用時UserIDのみ、AddX509Certificate/X509Certificate/DelX509Certificate

補足：

RESTfulな外部連携API利用時に必要

一括申請はZIP化した独自コンテナ形式（後述）

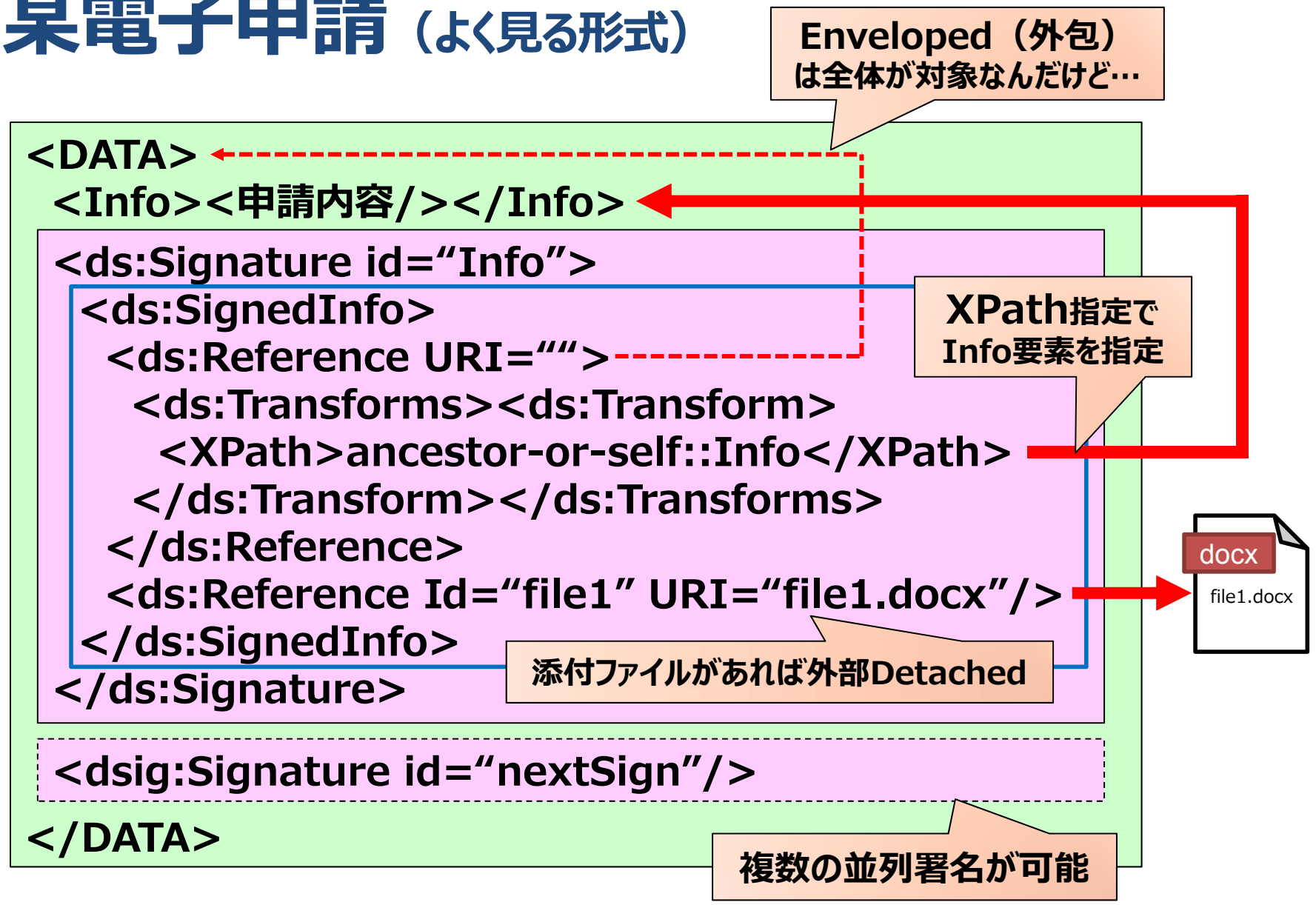
土地所在図等の図面署名（不動産登記規則第73条第1項）



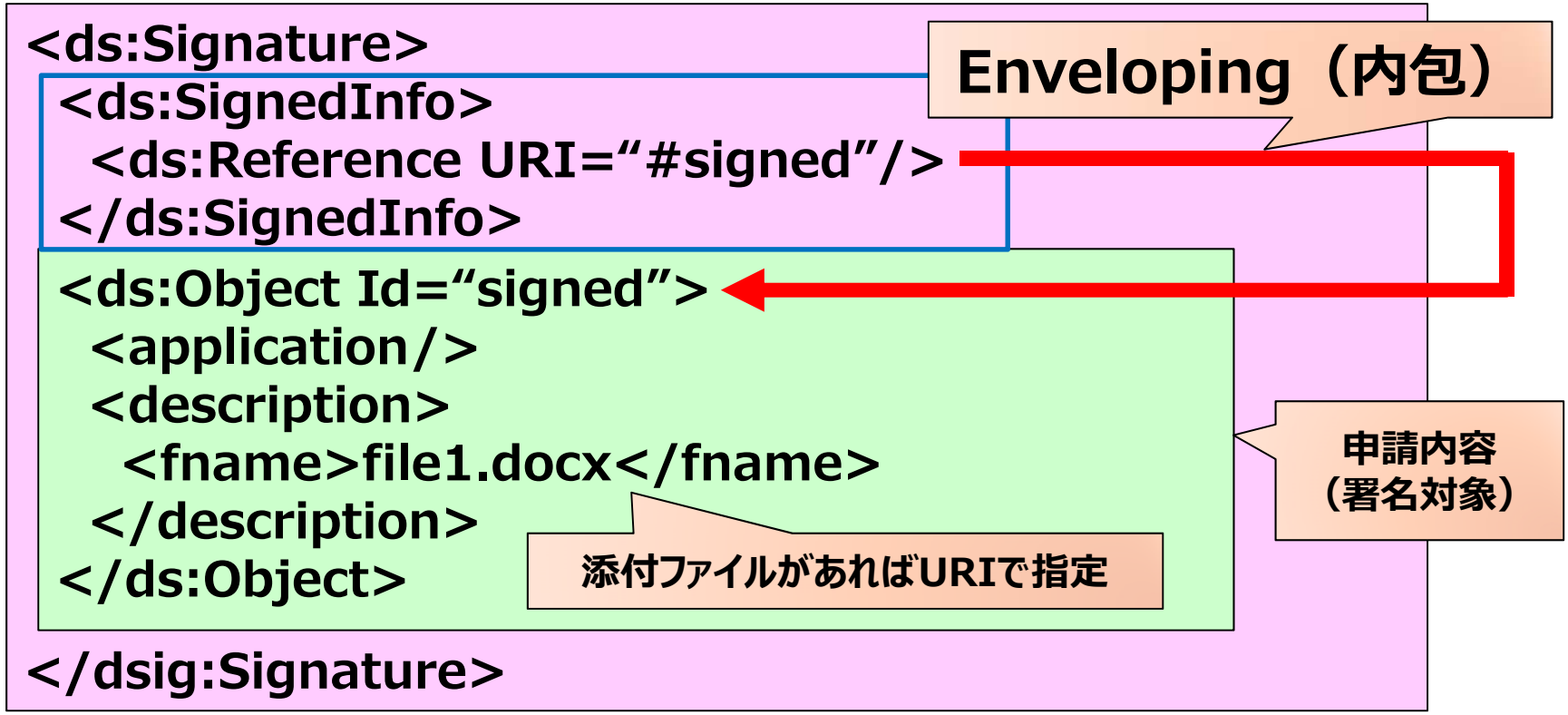
補足：

外部Detachedが1つだけ可能、署名対象が複数ある場合には複数の署名ファイルを用意。SHA-2署名受け付けて貰えるが記載は無い…

某電子申請（よく見る形式）



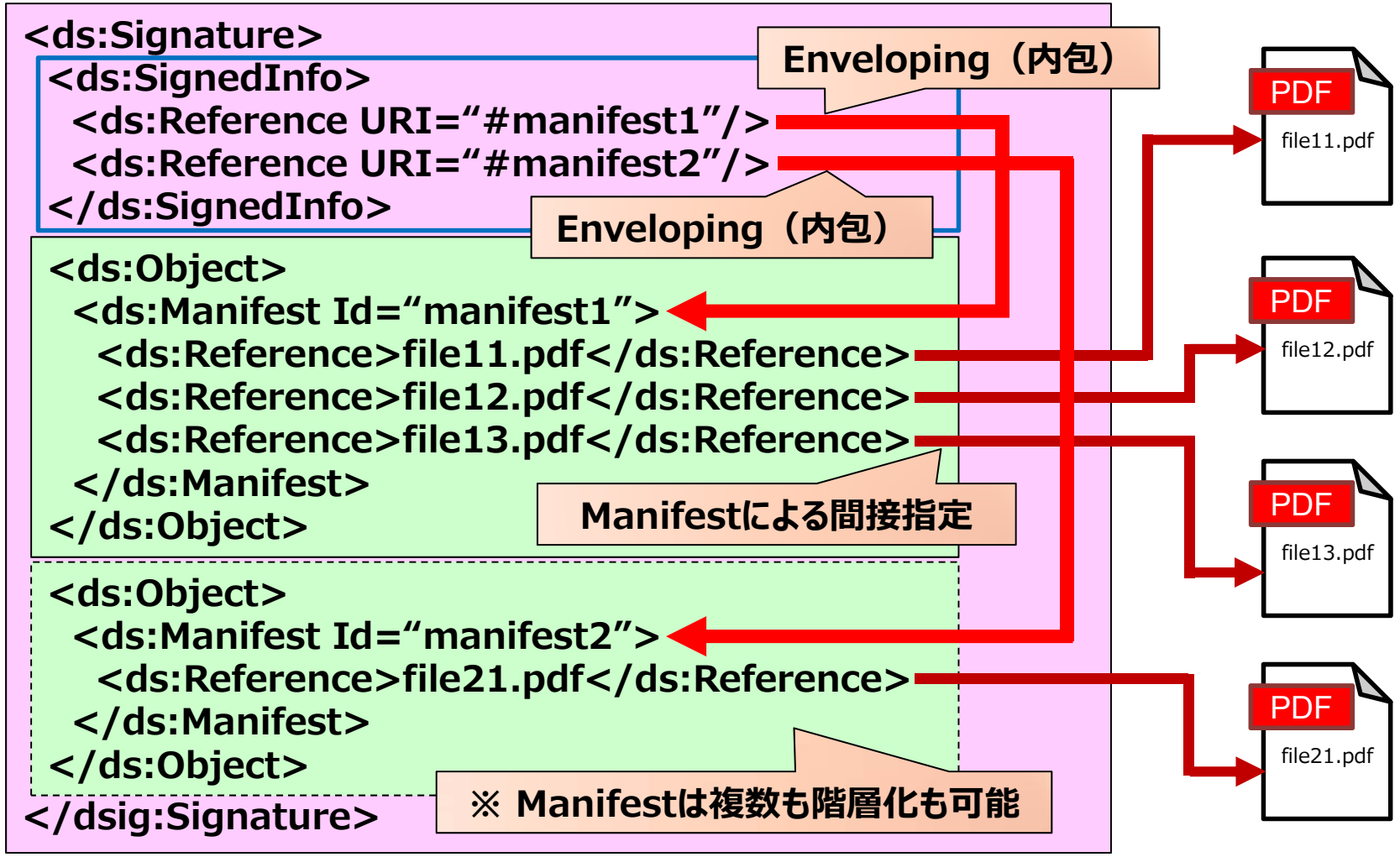
某地方自治体の電子申請



考察：

添付ファイルが外部Detachedなら守れるけど、
添付ファイルは重要では無いとの考え方もあり。

とある文書の大量一括保存



補足：Manifest長期署名延長は注意点あり。

電子処方箋（複数署名：追記署名型）

EnvelopedとXPathでも同じ参照の指定は可能

```
<EPD>
 <Document Id="Doc0123">
  <Prescription>
   <PrescriptionDocument Id="PD4567">
    <!-- HL7 CDA R2 -->
   </PrescriptionDocument>
   <PrescriptionSign>
    <Signature>
     <Reference URI="#PD4567"/>
    </Signature>
   </PrescriptionSign>
  </Prescription>
  <Dispensing>
   <DispensingDocument>
    <!-- HL7 CDA R2 -->
   </DispensingDocument>
  </Dispensing>
 </Document>
 <DocmentSign>
  <Signature>
   <Reference URI="#Doc0123"/>
  </Signature>
 </DocmentSign>
</EPD>
```

処方箋

内部Detached

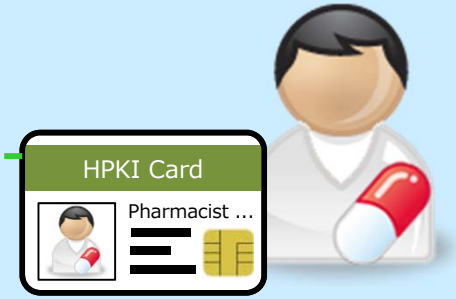
調剤結果

医師の処方箋と電子署名を含む

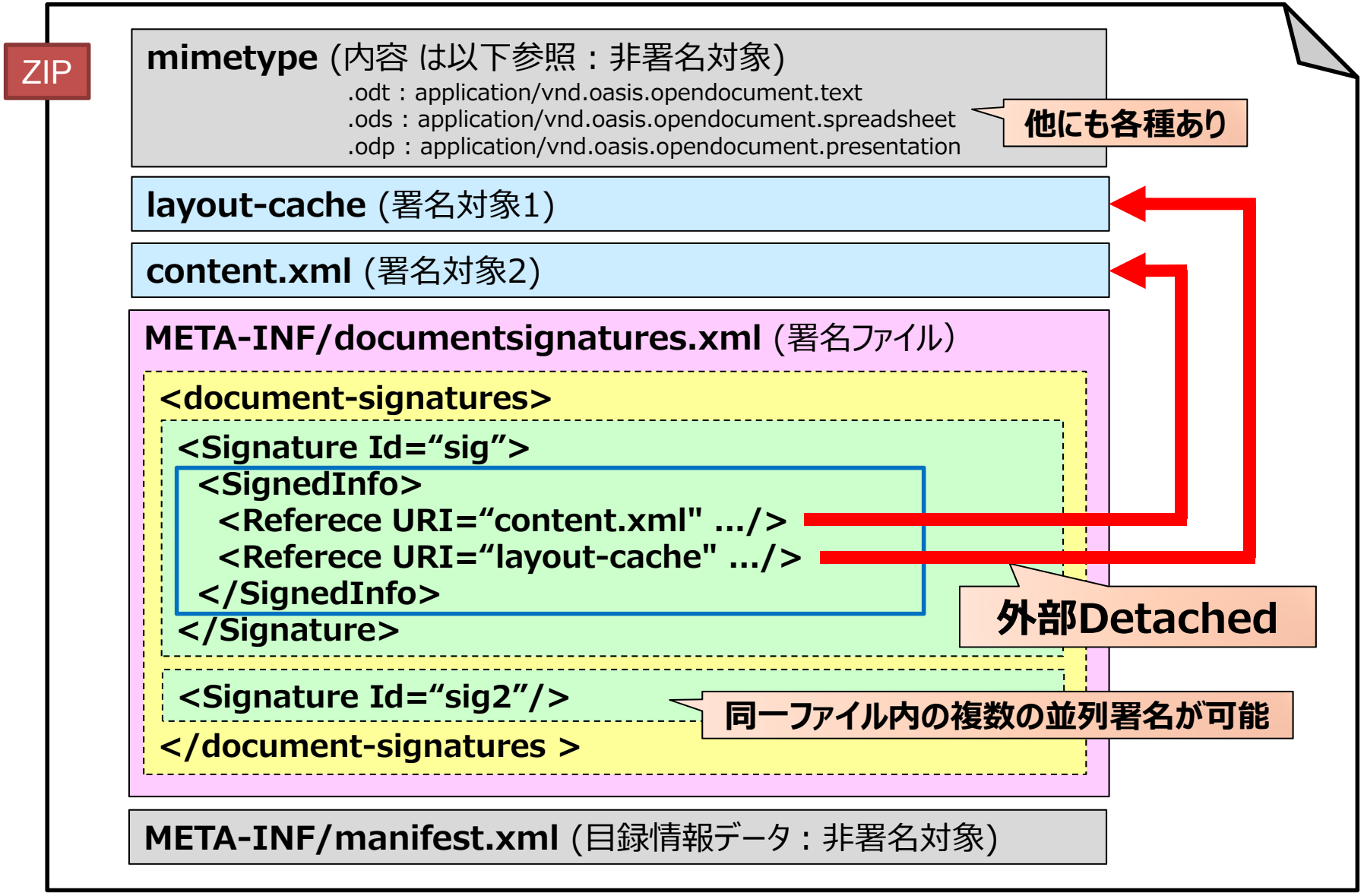
内部Detached

医師

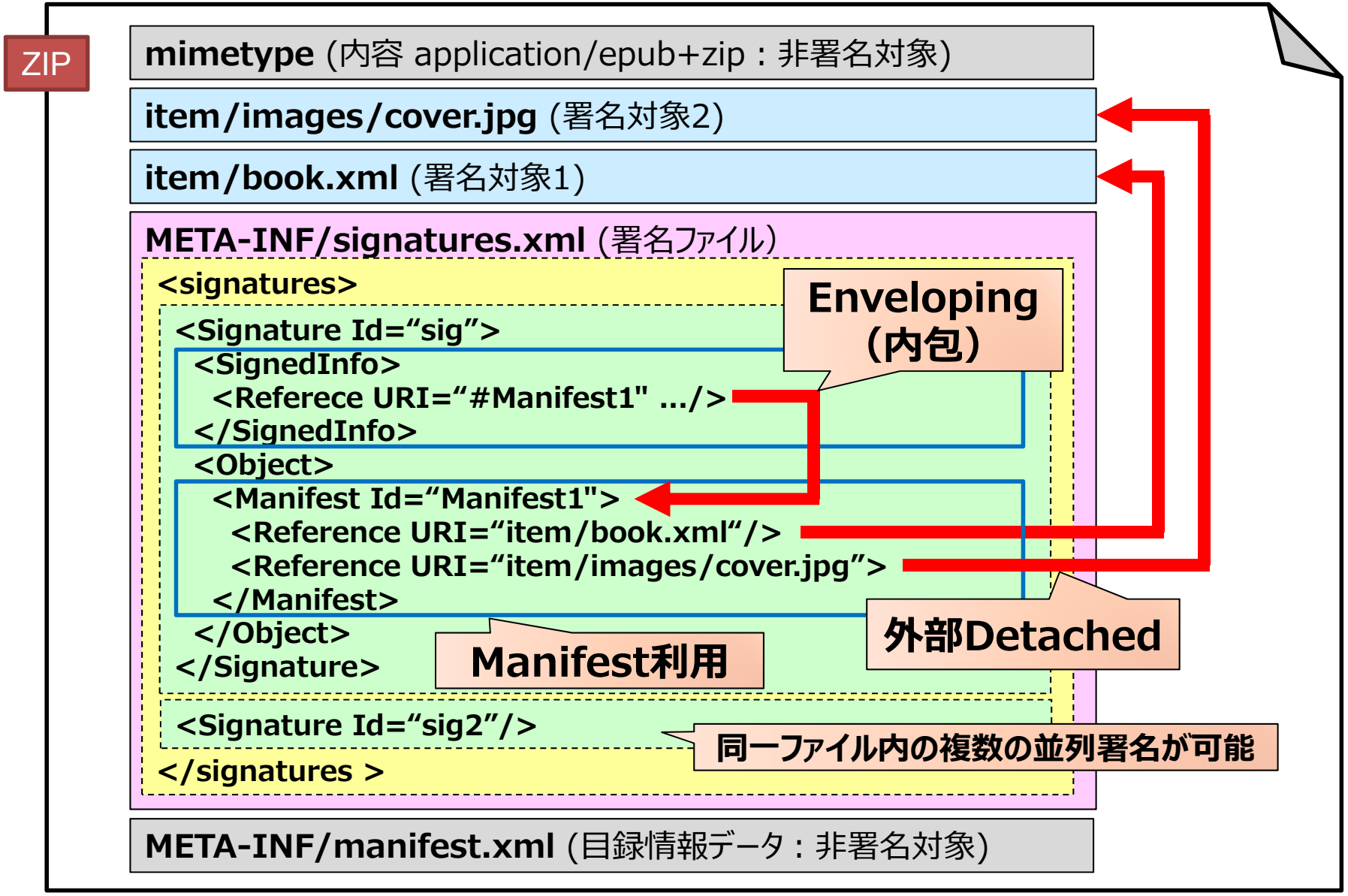
薬剤師



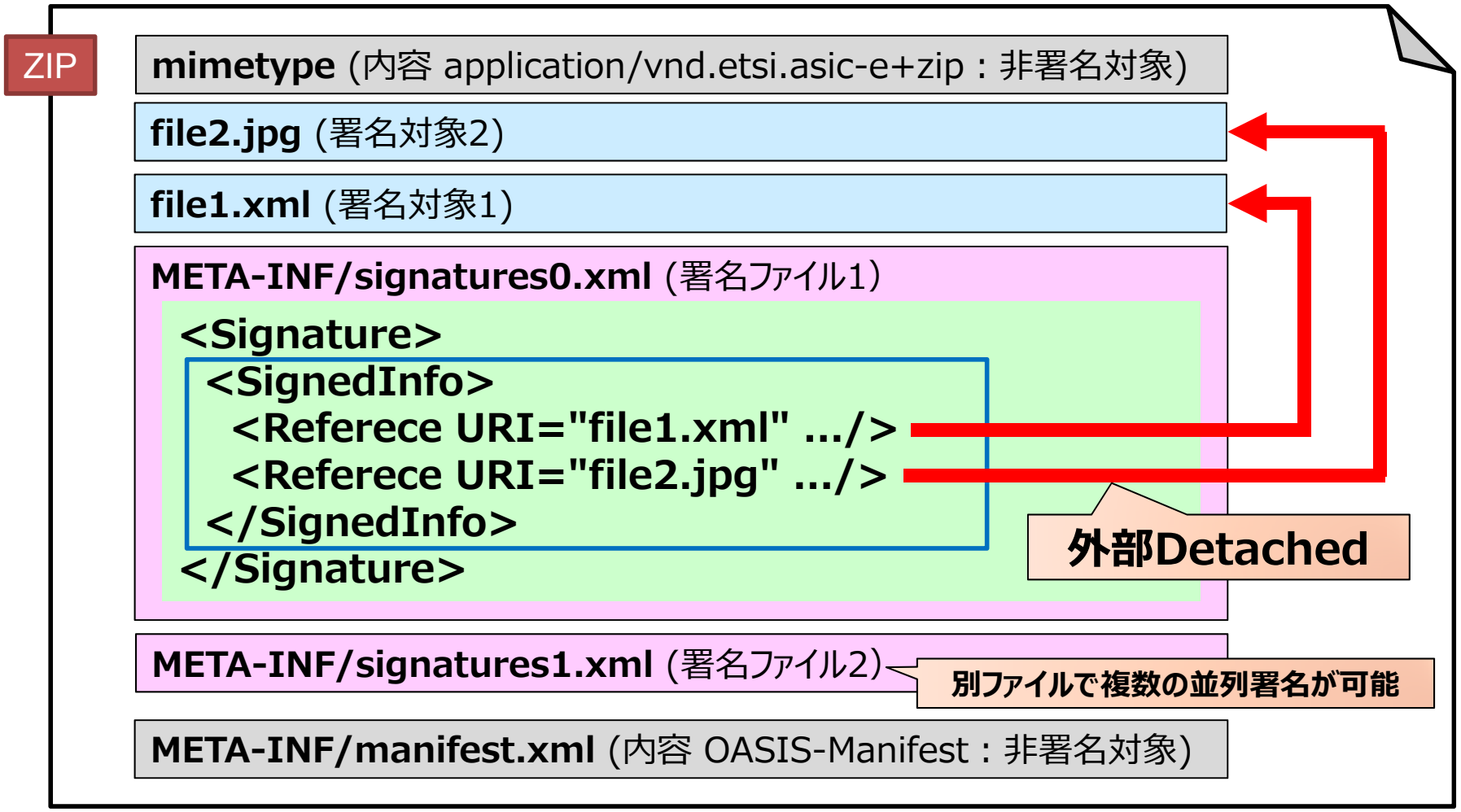
ODF (OASIS /OpenDocument Format - ISO/IEC 26300)



OCF (IDPF - EPUB Open Container Format)

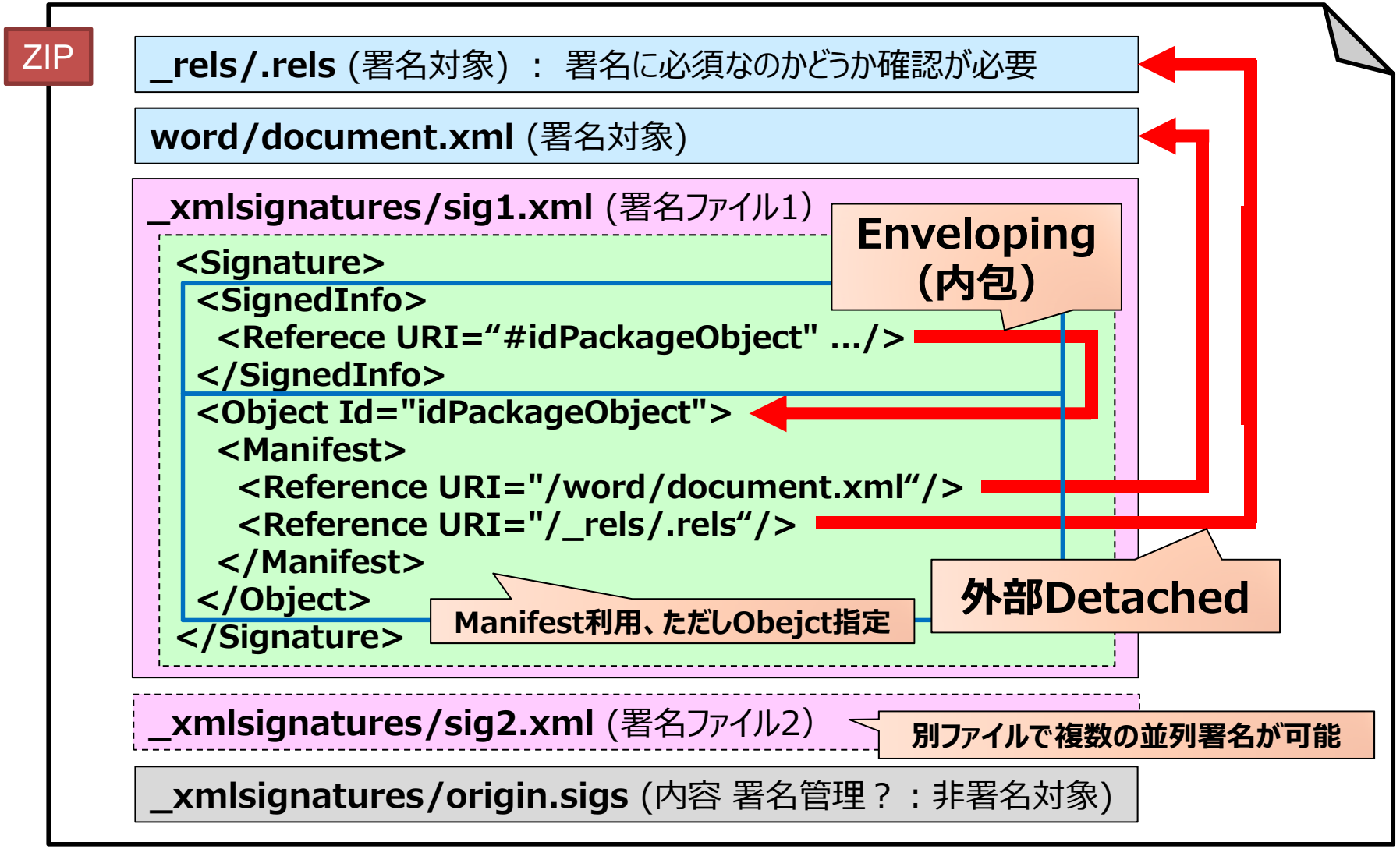


ETSI ASiC-E / Estonia他 BDOC



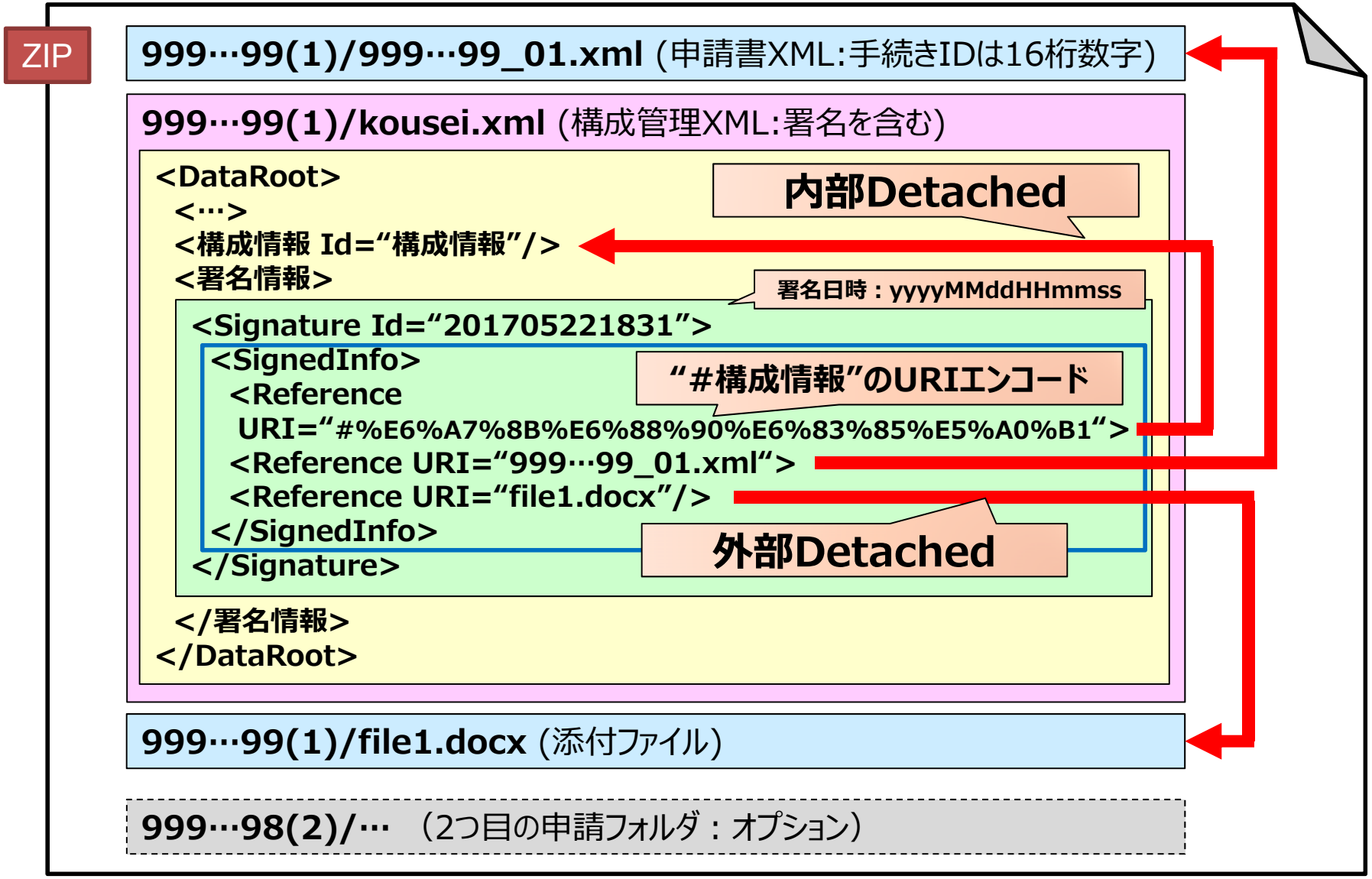
※ XML署名では無くXAdESが必要だが、欧州のEN仕様に従う必要あり。
※ XAdES以外に、CAdESやタイムスタンプも利用可能。

OPC (OOXML/Open Packaging Conventions - ISO/IEC 29500-2)



※ OPCはJTC1 SC34にてより汎用化（例：Manifestオプション化）予定。

e-Gov 一括申請（電子申請：署名が必要な場合）



XML署名参照方式の（個人的）感想

Detached：最も良く使われる基本参照

内部・外部共に良く使われている。
署名対象が明確で分かりやすい。

Enveloped：対象＞署名 の場合

単独XML情報に署名をする場合に多い。

Enveloping：署名＞対象 の場合（少ない）

Manifestを埋め込み時には利用。

Manifest：間接指定で時々使われる

署名検証は早いが、長期署名時に面倒あり…
うまく使えれば便利。

おまけ：米国の署名戦線異常あり？

“Electronic Signatures in Global and National Commerce (ESIGN) Act”
2000年に連邦レベルに合格した法律。

“Uniform Electronic Transactions Act (UETA)” ESIGNのベースになった法律
UETAは米47州/コロンビア特別区/プエルトリコ/米領バージン諸島が採択した法律。

ESIGN/UETAの基本要求:

1. 署名する意図が明白でなければならない。
2. 署名は記録と関連/連携していなければならない。
3. 電子取引するためには、はっきりした同意が必要である。
4. 記録へのアクセスが可能でなければならない。
5. 文書をむやみに変更をしないこと。

デジタル署名は要件に入っていない

※ ETSI ESI と 米国政府が共同で電子署名のワークショップを開催
"US Government and European Union Workshop on Digital Signatures!"
2017年3月8日にワシントンDCで開催、内容は Federal Public Key Infrastructure (FPKI) 等
https://www.eventbrite.com/e/digital-signatures-us-government-and-european-union-workshop-tickets-31538125382

※ DocuSignが本人確認問題で裁判に負けたとのブログ情報あり
“US Court Rejects DocuSign E-Signatures as method to provide Digital Authorization”
一部抜粋：「DocuSignは法的環境におけるe-verificationの信頼できる出典であるかと疑われているからです。」
つまり技術の問題では無く署名者の本人性の推定の問題か？PKIのようなインフラを使う必要があると言うことか？
なおブログを書いているのはPKIベンダーなので本当に正しいことを言っているのか確認は必要と考えている。
https://www.cryptomathic.com/news-events/blog/us-court-rejects-docusign-e-signatures-as-method-to-provide-digital-authorization