XML コンテンツの暗号化と復号

トランスポート層での暗号化を提供する SSL/TSL の暗号化とは異なり、XML での暗号化はメッセージ レベルで機能します。これにはいくつかの利点がありますが、そのひとつは、メッセージの特定の部分を暗号化できることです。この場合、メッセージのそれ以外の部分を人の読めるテキストのまま残すことができます。もうひとつの利点は、メッセージが宛先に到達したあとでも暗号化されたままであることです。こうすると、実際に必要になる時点まで保護しておくことができます。

送信 XML コンテンツの暗号化

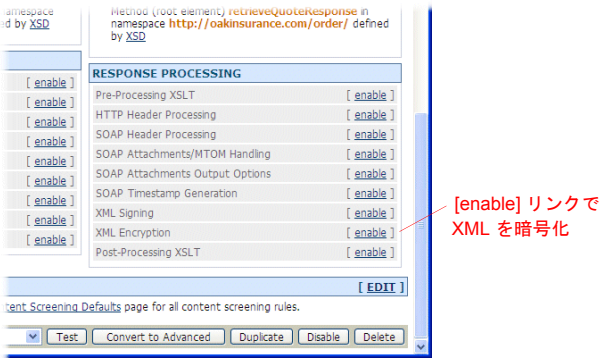
メッセージ コンテンツを暗号化するには、受信者の公開鍵を使用する必要があります（受信者がそのコンテンツを復号するには、対応する秘密鍵を必要とします）。

実際に XML 暗号化機能を利用するために最初に必要なことは、ユーザの証明書の読み込みです。ポリシーに入れるパートナーの公開鍵がこの証明書に含まれています。別の方法として、ACE XML Gateway は 受信要求の XML シグニチャに含まれている公開鍵でもメッセージを暗号化できます。この例では架空の Beagle Partners, Inc. の公開証明書を使用します。

メッセージの暗号化をセットアップする手順は次のとおりです。

1. ルーティング ブラウザで retrieveQuote サービス プロキシをクリックします。
2. **Response Message Specification** の下に見える **XML Encryption** の横の [enable] リンクをクリックします。

図 18-1　送信応答の暗号化



3. **XML Encryption** ページで **Transport with Public Key** の証明書リソース、beagle.cer を選択します。この証明書をまだアップロードしていない場合は、次の手順で行ってください。
   a. オプション メニューの横の **[Upload]** ボタンをクリックします。
   b. ポリシー内のリソースにつける名前を入力します。
   c. URL 欄には次の URL を入力してください。

      http://example.reactivity.com/pki/client/beagle.cer

   次のオプションの値はデフォルトのままでかまいません：**[For SOAP Role]**、**[Encryption Algorithm]**、**[Transport Cipher]**、**[Encryption Type]**

   実際には、要求を受け取るアプリケーションの都合により、これらのオプションをカスタマイズする必要があるかもしれません。
4. **[Element specified by these XPaths]** オプションを選択し、[XPath] 欄に次の値を入力します。

   ```
   //*[local-name()='price']
   ```

   応答メッセージのうち、`price` エレメントのみが暗号化されます。
5. **[Save Changes]** をクリックします。
6. retrieveQuote サービスにアクセス コントロールを設定している場合は、簡単にするため、この時点で公開アクセスにリセットします。それにより、イベント ログの中から暗号化に関連するイベントを見つけやすくなります。

   公開アクセスに設定するには、設定ページの最下部にある **[Edit Access Control]** リンクをクリックし、アクセス レベルとして **[Public]** を選択します。

   また、デフォルト（非暗号化ポート 80）設定に戻す必要があるかもしれません。ポートを変更するには、そのサービス プロキシに対するユーザ インターフェイスの設定を修正します。以前に説明した方法に従ってください。
7. 変更を保存したら、必ずポリシーを導入してください。

これで XML 暗号化のテストが可能になりました。

暗号化のテスト

メッセージの暗号化設定を終えたら、WFetch からサービスへメッセージを送信します。WFetch の設定は、再びデフォルトのポートと非同期認証を使用するように設定し直してください。次の例に類似したメッセージが応答として表示されます。

図 18-2　暗号化されている応答

この応答にはいくつか注意点があります。

- 暗号化されたデータを記述しているメッセージには WSSE セキュリティヘッダが追加されています。
- このヘッダに含まれているのは、暗号化された次のエレメントを識別する参照宣言です。
  `<DataReference URI="#RXFIDIXHYOTE"/>`
- 暗号化された `price` エレメントへの DataReference ポイント。暗号化されて次のように表示されます。

```
<EncryptedData
  Type="http://www.w3.org/2001/04/xmlenc#Element"
  Id="RXFIDIXHYOTE">
 <EncryptionMethod
    Algorithm="http://www.w3.org/2001/04/xmlenc#
      tripledes-cbc"/>
 <CipherData>
   <CipherValue>wuZ36uMfv7cqJvL2G/NI=</CipherValue>
 </CipherData>
</EncryptedData>
```

暗号化された応答に現れる設定オプションの結果に注意してください。インターフェイスにおける他のオプションについても自由にテストを行い、応答に現れる結果を確認してください。たとえば、**[Encrypt Element]** の選択肢として **[encrypt only the contents of the specified elements]** を試したり、XPath 行を設定に追加して、暗号化するエレメントを追加してください。

注： メッセージの表示形式を改善するには、WFetch ではなく、メッセージ トラフィック ログのウィンドウで応答メッセージを開きます。

設定変更をテストすると、ACE XML Gateway により、複雑な技術が簡単に実行できます。XML 暗号化だけでなく、XML シグニチャ、SAML、UsernameToken など、他の Web Service 技術についても同様のことが言えます。

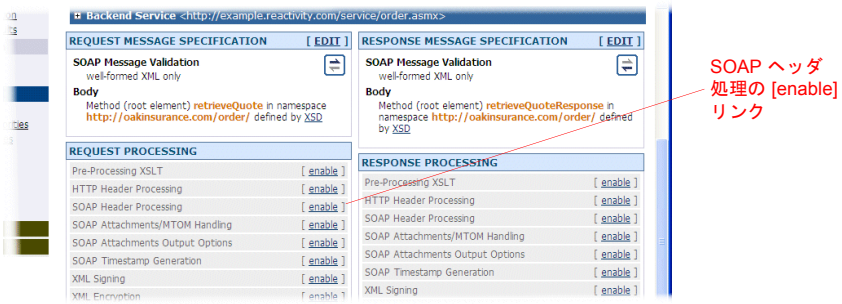
受信 XML コンテンツの復号

暗号化したコンテンツは、暗号化で使用した公開鍵に組み合わせる秘密鍵で復号する必要があります。これは、メッセージを送信した相手が ACE XML Gateway の公開鍵を持っていることが前提です。そのためコンテンツの復号設定では、復号に使用する鍵として ACE XML Gateway の秘密鍵を指定することになります。

サービス プロキシ上でメッセージ復号を設定する手順は次のとおりです。

1. ルーティング ブラウザ上で、暗号化したメッセージを発行するサービス プロキシをクリックします。
2. サービス プロキシ情報ページで、**Request Message Specification** 項目の **SOAP Header Processing** の横の **[enable]** リンクをクリックします。

図 18-3　受信要求の復号



3. 最初のチェックボックス **[Process header elements for SOAP Role]** にチェックを入れます。ドロップダウン メニューのオプションは `[no role]` のまま残します。

4. `WSS:XML Decryption` ヘッダの下にある **[Enable XML decryption using the selected keys]** にチェックを入れます。

   このオプションを有効化すると、暗号化された SOAP エレメントを ACE XML Gateway に復号できますが、リストに記載された鍵に限ります。

5. 復号に使用する秘密鍵を選択します（必要であれば **[Upload]** ボタンを利用して PKCS#12 形式の証明書 / 鍵ペアをアップロードできます）。

[Save Changes] を実行すると、設定の概要がサービス プロキシ情報ページの **Request Processing** エリアに表示されます。この変更を有効にするために必ずポリシー導入を行ってください。