デジタル署名の作成と照合

XML シグニチャを利用することにより、XML データの信頼性と完全性を保証することができます。つまり、データが特定の送信元から届き、シグニチャの生成以降に改変されていないことが保証できます。

ACE XML Gateway を利用すると、XML 暗号化のメッセージ処理への組み込みが簡単に行えます。送信メッセージの XML シグニチャの生成と、受信メッセージのシグニチャ確認をセットアップできます。

ACE XML Gateway は XML シグニチャを生成するために、秘密鍵を使用して指定コンテンツのダイジェストを作成します。その対象はメッセージの一部でも全体でもかまいません。XML シグニチャは、受信者が ACE XML Gateway の公開鍵を使用して処理します。公開鍵を使ってダイジェストを復号できれば、受信者は、公開鍵と対となる（ACE XML Gateway の）秘密鍵の持ち主によってそのメッセージが生成されたことを確認できます。同様に、シグニチャ照合を設定するには、送信者の公開鍵を使用します。

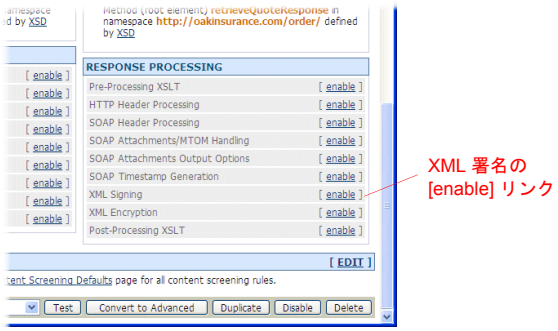
これから説明する手順は送信応答のコンテンツに署名する方法です。ここでは、サンプル リソース用 Web サイトに収容されているリソース ファイルを使用して署名の設定を行います。リソースを入手していない場合は、example.reactivity.com から入手してください。

応答メッセージへの署名

送信応答の XML 署名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 Signing** の横の [enable] リンクをクリックします。

図 19-1　送信応答への署名



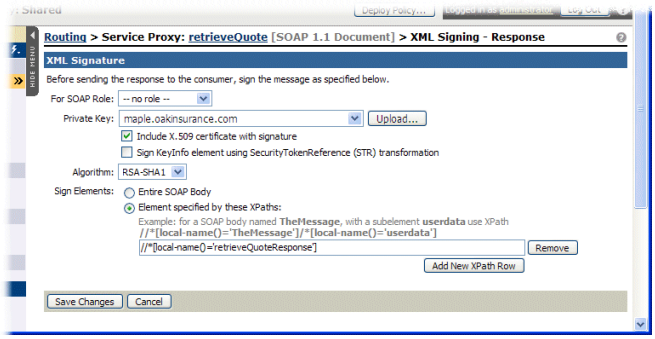
3. **XML Signature** ページ で **[Private Key]** オプションの横の **[Upload]** ボタンをクリックします。
4. **Upload Public/Private Keypair Resource** ウィンドウで名前を入力します。リソースはポリシーの中で使われるので、意味のわかる名前（`maple keypair` など）をつけます。
5. ファイル選択ウィンドウで **[Browse]** をクリックしてから、`maple.p12` ファイルを探して選択します。
6. パスワードとして `swordfish` と入力します。
7. **[Upload]** ボタンをクリックします。
8. **Private Key** メニューでそのリソースが選択されていることを確認します。

   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]**、**[Include X.509 certificate with signature]**（有効化されていること）、**[Algorithm]**
9. **[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()='retrieveQuoteResponse']
   ```

   この設定は、署名を行った応答エレメント全体に対して有効です。

図 19-2　XML シグニチャの設定



10. **[Save Changes]** をクリックし、ポリシーを導入します。

以上の手順で、特定のエレメントに署名が行われました。実際にはほとんどの場合、SOAP メッセージ本文全体に署名が行われます。また、メッセージの安全性と完全性を保証するため、通常 XML シグニチャと XML 暗号化が一緒に使用されます。

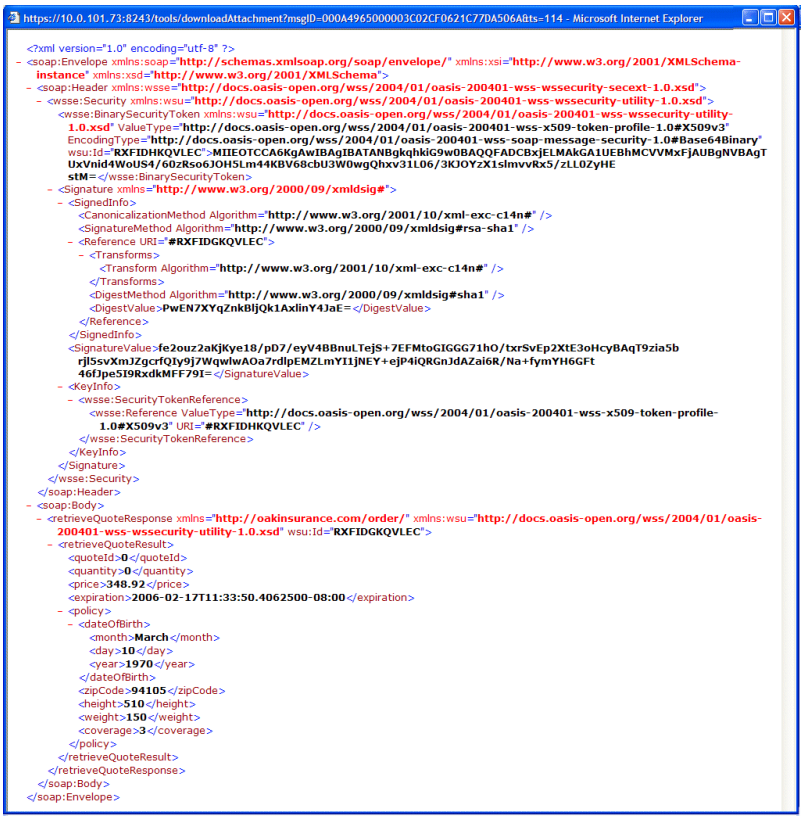
XML シグニチャのテスト

メッセージの XML 署名を設定したら、WFetch からサービスへメッセージを送信します。結果は WFetch の出力表示ウィンドウに現れますが、メッセージをよりわかりやすく表示するには、次の手順でメッセージ トラフィック ログとして開きます。

1. 操作メニューで **[Message Traffic Log]** リンクをクリックします。
2. メッセージ エントリを表示するために **[req/resp pair]** リンクをクリックします。
3. **[Logged Message Content]** ウィンドウの **[Outgoing Response Attributes]** エリアで **[text/xml]** リンクをクリックします。

   次のようなウィンドウが表示されます。

図 19-3　署名されている応答



この応答の中で、次の部分に注意してください。

- Signatureエレメントが WSSE セキュリティ ヘッダに表示されています。図 19-3 では前の操作で設定した暗号化部分が省略されていますが、暗号化を有効に設定してあれば、Signature エレメントがセキュリティ ヘッダの中で EncryptedKey エレメントとともに表示されます。
- この図では BinarySecurityToken エレメントのコンテンツが省かれていますが、実際のテストでは非常に長いものになります。
- retrieveQuoteResponse エレメントには新しい属性がいくつか加わっています。wsu:Id 属性値は Reference エレメントの URI 値の対象としてのエレメントを示しています。

これらの機能により、受信したアプリケーションは署名付きエレメントに格納された情報の有効性と完全性を確認できます。