XML Consortium

～ 第8回 XMLコンソーシアムDay ～

セキュリティ部会活動中間報告

Digital Signature Serviceを用いた、アプリケーション試作に向けて

2006年12月12日

XMLコンソーシアム セキュリティ部会

岡村 和英（株式会社ネット・タイム）

アジェンダ

- OASIS Digital Signature Service
  - DSSとは？
  - Core仕様
  - プロファイル
- アプリケーション試作に向けて
  - 活動の状況報告

Digital Signature Service

- 電子署名／署名検証サービスのためのインターフェースを規定
  - XMLを用いた要求／応答ﾒｯｾｰｼﾞ
  - XML-SignatureまたはCMS（RFC3369）による署名形式に対応
  - X.509 PKI TSP(RFC3161)を模した、XML形式のﾀｲﾑｽﾀﾝﾌﾟ
  - PGPなどの他の署名形式、ﾀｲﾑｽﾀﾝﾌﾟ形式にも拡張可能
  - 様々な用途に応じたﾌﾟﾛﾌｧｲﾙの提供
- OASIS DSS TCにて策定中

  2006/10/03～2006/12/02にﾊﾟﾌﾞﾘｯｸﾚﾋﾞｭｰを実施

DSSの用途

- 企業での署名サーバとしての利用
  - 組織ﾌﾟﾚｽﾘﾘｰｽや配布ﾌﾟﾛｸﾞﾗﾑに対する署名の付与。
    - ■個別社員ではなく、組織としての署名の作成
  - 署名ﾘｸｴｽﾄの中央管理、監査、ｱｰｶｲﾌﾞ。
    - ■いつ、誰の要求でどのﾒｯｾｰｼﾞに署名を行ったのか

仕様書構成

- 概要
  - Digital Signature Service Overview
- コア仕様
  - Digital Signature Serivce Core Protocols, Elements, and Bindings
- プロファイル
  - XML Timestamping Profile
  - Asynchronous Processing Abstract Profile
  - Abstract Code-Signing Profile
  - J2ME Code-Signing Profile
  - Entity Seal Profile
  - Electronic PostMark (EPM) Profile
  - German Signature Law Profile
  - Advanced Electronic Signature（AdES）Profiles
  - Signature Gateway Profile

コア仕様概略

- メッセージ形式の定義
  - 署名プロトコル（SignRequest / SignResponse）
  - 検証プロトコル（VerifyRequest / VerifyResponse）
  - XMLタイムスタンプ（TimeStamp）
- メッセージ送受信方法の定義
  - HTTP POST Transport Binding
  - SOAP 1.2 Transport Binding
  - TLS Security Binding
    - TLS X.509 Server Authentication
    - TLS X.509 Mutual Authentication
    - TLS SRP Authentication
    - TLS SRP and X.509 Server Authentication

プロファイルとは？

- DSSコア仕様に基づき、
- 利用目的に応じて、
  - どのバインディング方式を用いるべきか
  - 親仕様を拡張するための要素／属性
  - 親仕様に対する制限事項
    - 必須となる要素／属性
    - 使用できない要素／属性
    - 要素／属性の値として何を指定可能か
  - どういう処理プロセスを用いるか

  を規定。

プロファイル概略 (1)

- XML Timestamping Profile
  - RFC3161 Timestampの生成と検証。
  - HTTP POST ＋ TLS X.509 Server AuthN
  - SignRequest
    - OptionalInputs
      - RenewTimestamp　既存のタイムスタンプの有効期限を延長する。
- Asynchronous Processing Abstract Profile
  - 非同期通信による署名／検証サービスの為のメカニズムを提供。
- Abstract Code-Signing Profile
  - ソフトウェアプログラムに対する署名を行うための抽象プロファイル。
- J2ME Code-Signing Profile
  - MIDP 2.0アプリケーションに対する署名の付与。

プロファイル概略 (2)

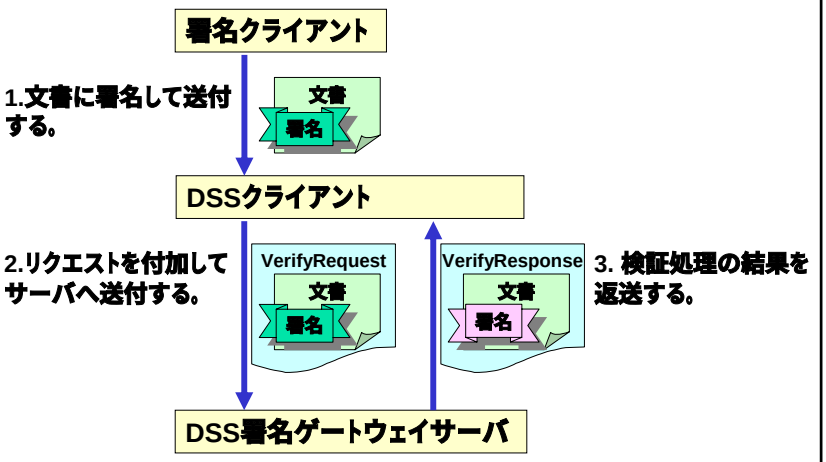
- Entity Seal Profile
  - 指定された電子データが所定の時間に存在していたことを示す「シール」の生成と検証。
- Electronic PostMark (EPM) Profile
  - UPU (万国郵便連合) の支持に基づく、電子消印
- German Signature Law Profile
  - 独デジタル署名法 (SigG／SigV) に準ずる、電子署名の生成と検証。
- Advanced Electronic Signature (AdES) Profiles
  - XAdESおよびETSI TS 101 733(Electronic signature formats and Signature Policies)に定義されるような、高度な電子署名の生成と検証。

プロファイル概略 (3)

- Signature Gateway Profile
  - 署名検証プロトコルのみを取り扱う。
    - SignatureRequestおよびSignatureResponseは扱わない。
  - ユースケース。
    1. 署名者が署名用の証明書を使って署名を生成する。
    2. 署名を直接受領者に送付する代わりに、署名ゲートウェイへ送付する。
       - 受領者が署名者の署名を 1) 理解できない / 2) 信頼しない かもしれないので。
       - 署名ゲートウェイは署名者と受領者の双方から信頼されている。
    3. 署名ゲートウェイが受領者の検証可能な新しい署名を生成。
       - 現在の署名を検証し、新しい署名を生成する。
  - 2つの実装モデル (Deployment Model) を定義。
    - Request-Response実装モデル
    - In-Line実装モデル

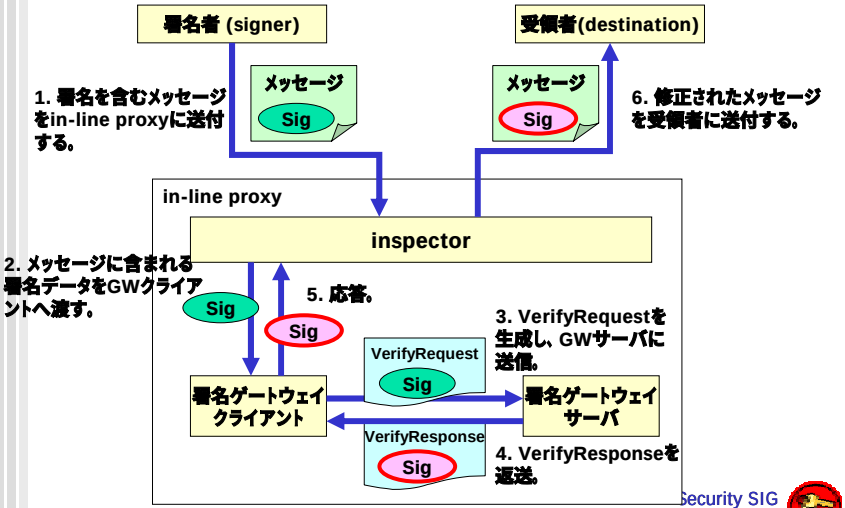
Signature Gateway Profile

- Request-Response実装モデル



Signature Gateway Profile

- In-Line実装モデル



アプリケーション試作の検討

- シナリオ
- 実装方針
- スケジュール

アプリケーションシナリオ

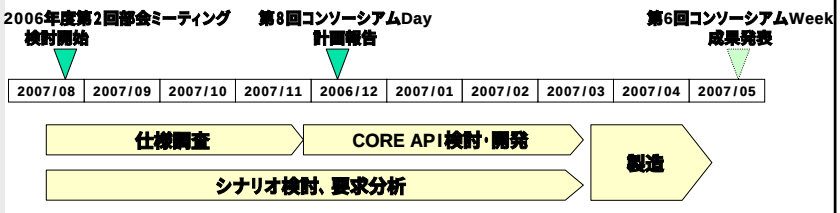
- 利用シーン（ビジネスシナリオ）が想像しやすい形で、
- DSSのメリットをわかりやすく伝える。

模索中

試作にあたっての方針

- 実現機能
  - 署名対象
    - 最初はDocumentHashだけを対象とする。
    - 単一署名のみをサポート。
  - 署名形式
    - XML-DSigのみ。CMSは対象外。
  - 署名オプション
    - タイムスタンプ付き署名は実現したい。
  - メッセージバインディング
    - HTTP POST
- シナリオ
  - クライアントとしてWebブラウザが用いられると望ましい。
  - ＸＭＬデータとしての結果ではなく、ユーザ側の視点で実感可能なわかりやすいアウトプットが欲しい。
- 実装手段
  - Java用API
    - JAXB 2.0を用いてJava/XMLバインディングを行なう。
    - テストケース（テスト用データ）の作成方法を確立すること。

大雑把な開発スケジュール



- 来年3月くらいまでかけてシナリオ検討
- CORE APIについても並行して検討、開発
- 3月からWeekに向けて一気に作る！

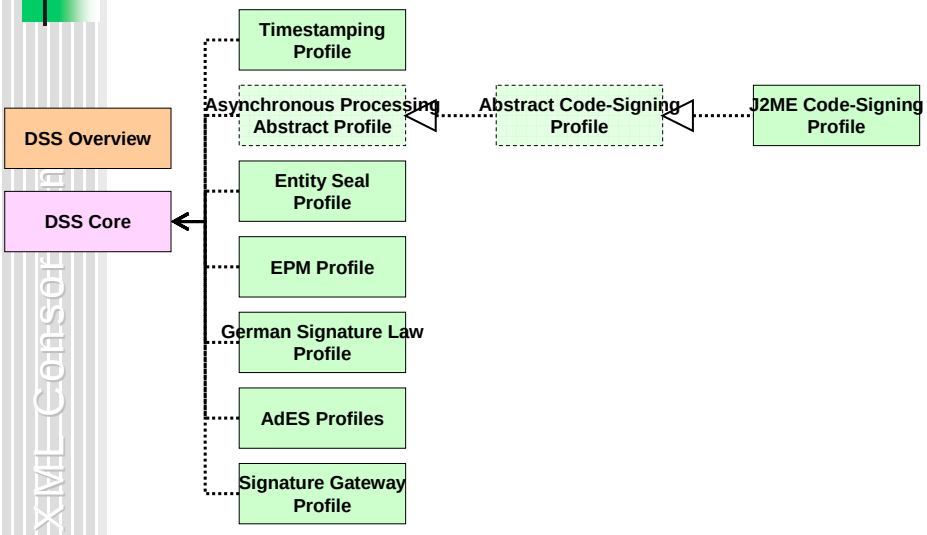
まとめ

- DSS
  - 署名と検証をWebサービス化。
  - 署名やタイムスタンプを中央管理し、監査可能に。
  - 信頼の出来る代理サーバを用いることで、署名の上書きや検証を代行。
  - 組織としての署名を実現。
- アプリケーション試作
  - まだ検討を始めたばかり。
  - 実際にプログラムを書く人が殆どいません、

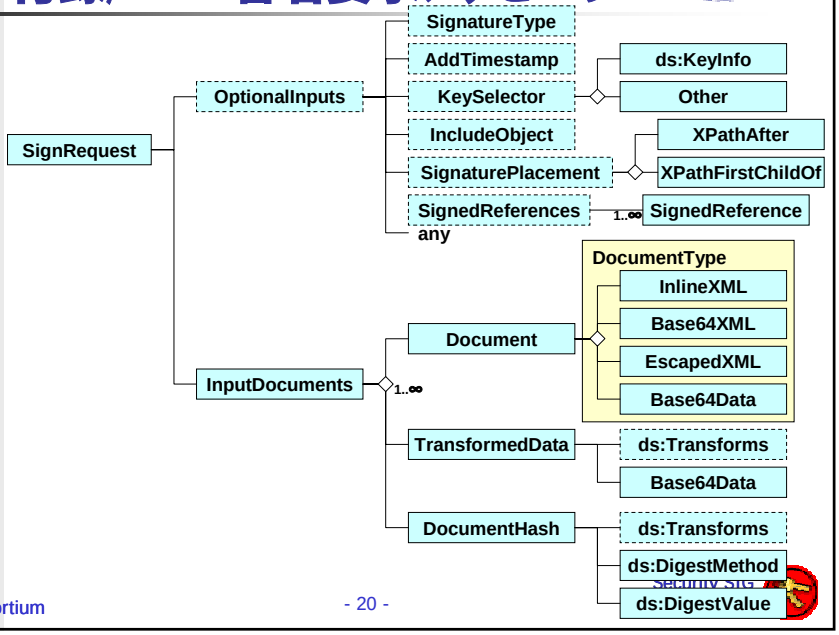
協力して頂ける方、大歓迎！

付録

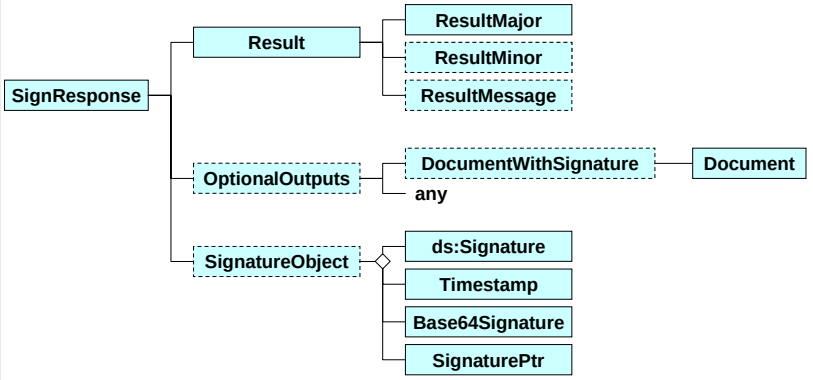
付録) DSS各仕様の関係



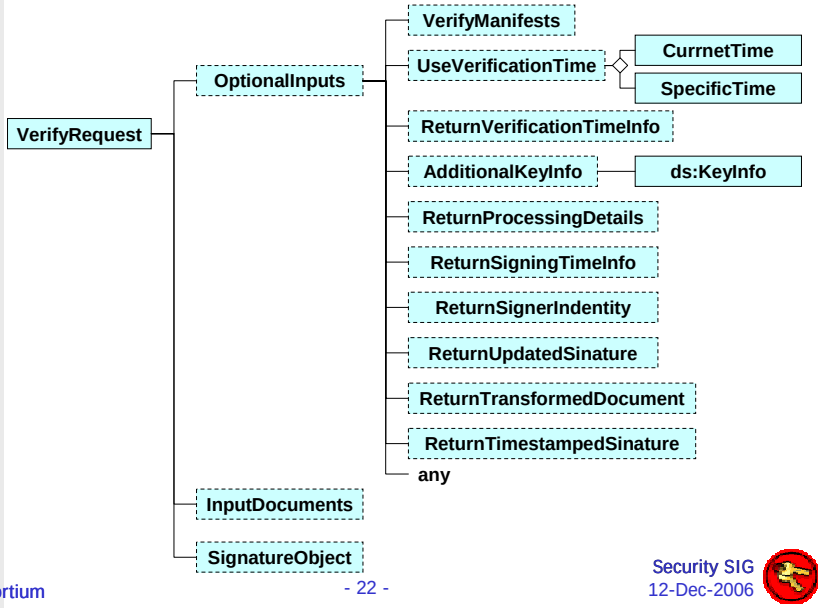
付録) DSS署名要求メッセージ



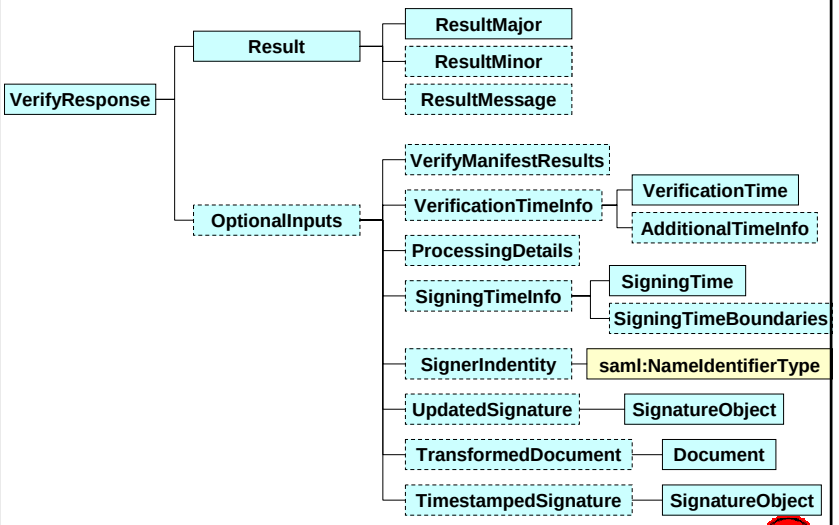
付録) DSS署名応答メッセージ



付録) DSS検証要求メッセージ



付録) DSS検証応答メッセージ



付録) DSSタイムタイムスタンプ