Entrust® Securing Digital Identities & Information

ECom


# 長期署名フォーマットの欧州実証実験
## ETSI Remote XAdES/CAdES Plugtests の結果報告

NPO日本ネットワークセキュリティ協会:JNSA PKI Day 2009
2009年6月24日 (木) 11:25～12:15

欧州通信規格協会 (ETSI) STF351 メンバー
エントラストジャパン株式会社　漆嶌 賢二

# 本日のアジェンダ

- 本題に入る前に
  - ETSIとは？
  - そもそも、長期署名フォーマット(CAdES/XAdES)とは？
- ETSI XAdES/CAdESリモートテスト
  - テスト概要
  - テスト環境
  - テスト実施の流れ
  - テスト結果
- ETSI STF351 (実験の企画,準備,運営のタスクフォース)
- プラグテストテスト所感
- 長期署名フォーマット関連の標準化動向

# 本題に入る前に（1）
# ETSIとは

# Entrust：ETSI とは

- ETSIとはEuropean Telecommunications Standards Institute：欧州通信規格協会
- 1988年に設立された欧州委員会（EC）に正式に認められた標準化団体
- 本部はフランス・ソフィアアンチポリス（仏のシリコンバレー）
- 欧州標準化委員会（CEN）と連携している
- 主な策定標準に長期署名などの電子署名関連、携帯電話の3G、道路交通情報システム（ITS）などがある
- 電子署名はTC ESI（電子署名基盤技術委員会）で策定
- 次世代電子商取引推進協議会（ECOM）はTC ESIのアソシエートメンバ（＝議決権が無い）
- 積極的に各標準のプラグテストイベントを実施している

# 本題に入る前に（2）
# 長期署名フォーマットCAdES/XAdESとは？

# Entrust® 従来署名の問題点と長期署名フォーマット

2つの問題点

## 従来の署名

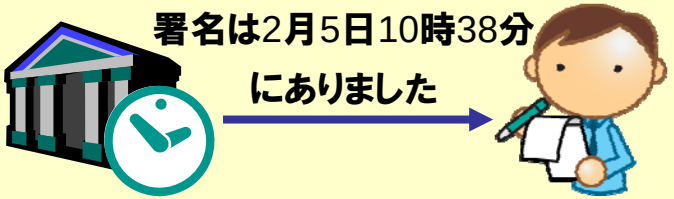

署名がICカードを落とした
前か後か信用できない

法的「証拠」にならない


将来スーパーコンピューター
により暗号が破られる

解決

## 長期署名フォーマット




署名にデジタルタイムスタンプを付け
第三者が署名の存在時刻を保証

技術的に立証可能な署名


署名と検証情報を最強の暗号でくるんで
改ざんから保護し、且つ証明書,CRLの遺失防止

# Entrust CAdES/XAdES長期署名フォーマットとは？

## 一言で言えば

CMS (PKCS#7) 署名やXML署名と互換性のある拡張フォーマット

## さらに何を追加できるか？ (署名者の属性とタイムスタンプ)

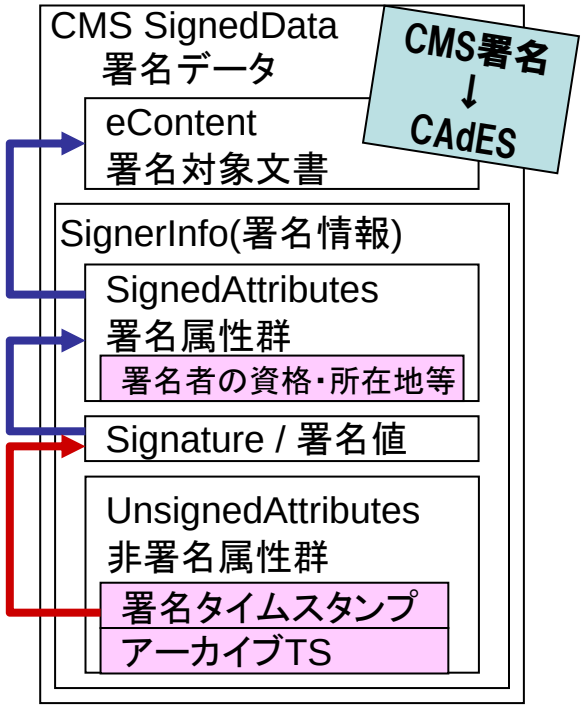
- 署名者の資格・署名意図・所在などを示す補足の属性情報
- カウンタ署名(上司承認・同意)
- 信頼できる署名した時刻(証明書の失効の前か？)
- 証明書検証情報(証明書チェーン、CRL、OCSPレスポンス)
- 2～3年以上の署名データ保護(アーカイビング)

## できること・特徴

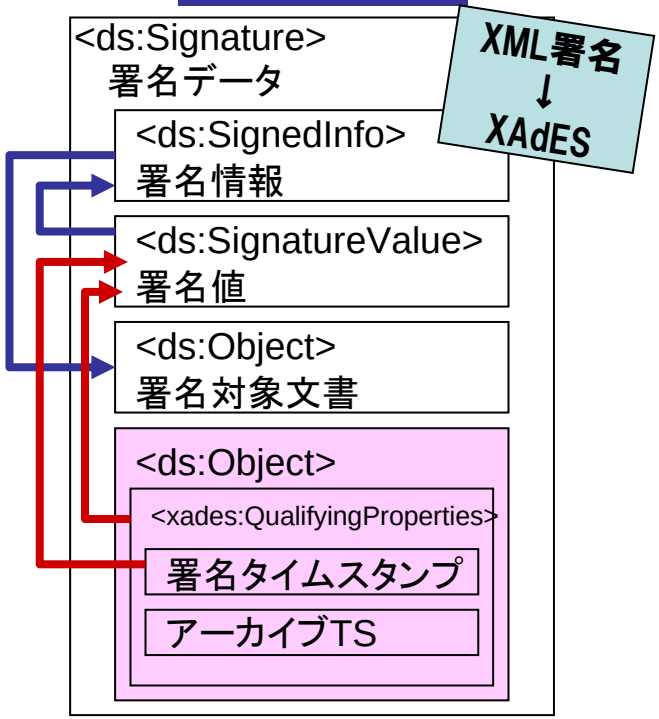
- 署名した人がどんな属性の人か詳細なプロフィールを示せる
- 署名が証明書が有効であった時にされたものか厳密に保証できる
- 改ざんしやすいデジタルデータを長期に渡り保管できる
- 欧州やブラジルでは法的に有効な電子署名の要件になっている
- 日本でもe文書法や保健医療分野で使われている
- 日本では長期署名フォーマットのプロファイルがJISになり、ISO化も

# Entrust CAdES/XAdESとはCMS署名,XML署名の拡張

## S/MIME,PDF署名で使うCMS署名




## XML署名




【CMS署名,XML署名の問題点】
・本人性を示す証明書が有効であったときに署名されたものかわからない
・将来、暗号アルゴリズムが破られた際に正しかったかどうかわからない

単に基本の署名にタイムスタンプ要素を追加するだけで問題を解決

【メリット】
・元となるCMS署名、XML署名の検証ツールで、大筋は検証できる。
・追加された要素に対してのみ、別途検証すればよい。

# Entrust：長期署名フォーマットはオプション属性が付与可能

| | |
|---|---|
| SigningCertificate | 署名者証明書を特定する参照情報 |
| SignerLocation | 署名者の所在地 |
| SignerAttributes | 署名者の職位・所属・資格 |
| CommitmentType | 署名の意図（原本作成,承認,配信記録など） |
| SigningTime | 署名者が主張する署名時刻 |
| SignaturePolicy | 署名ポリシ（送受信者の署名の生成・検証方法の取り決め） |
| SignatureTimeStamp | 第三者が保証する署名時刻（=署名タイムスタンプ） |
| CompleteCertificateRefs | 署名者証明書検証パスの証明書参照情報群 |
| CompleteRevocationRefs | 署名者証明書検証パスの失効参照情報群 |
| X Type1 TimeStamp | 署名値、署名タイムスタンプ、検証参照情報のタイムスタンプ |
| X Type2 TimeStamp | 検証参照情報のタイムスタンプ |
| ArchiveTimeStamp | 全ての情報の保管（アーカイブ）に使うタイムスタンプ |
| | 、、、、他 |

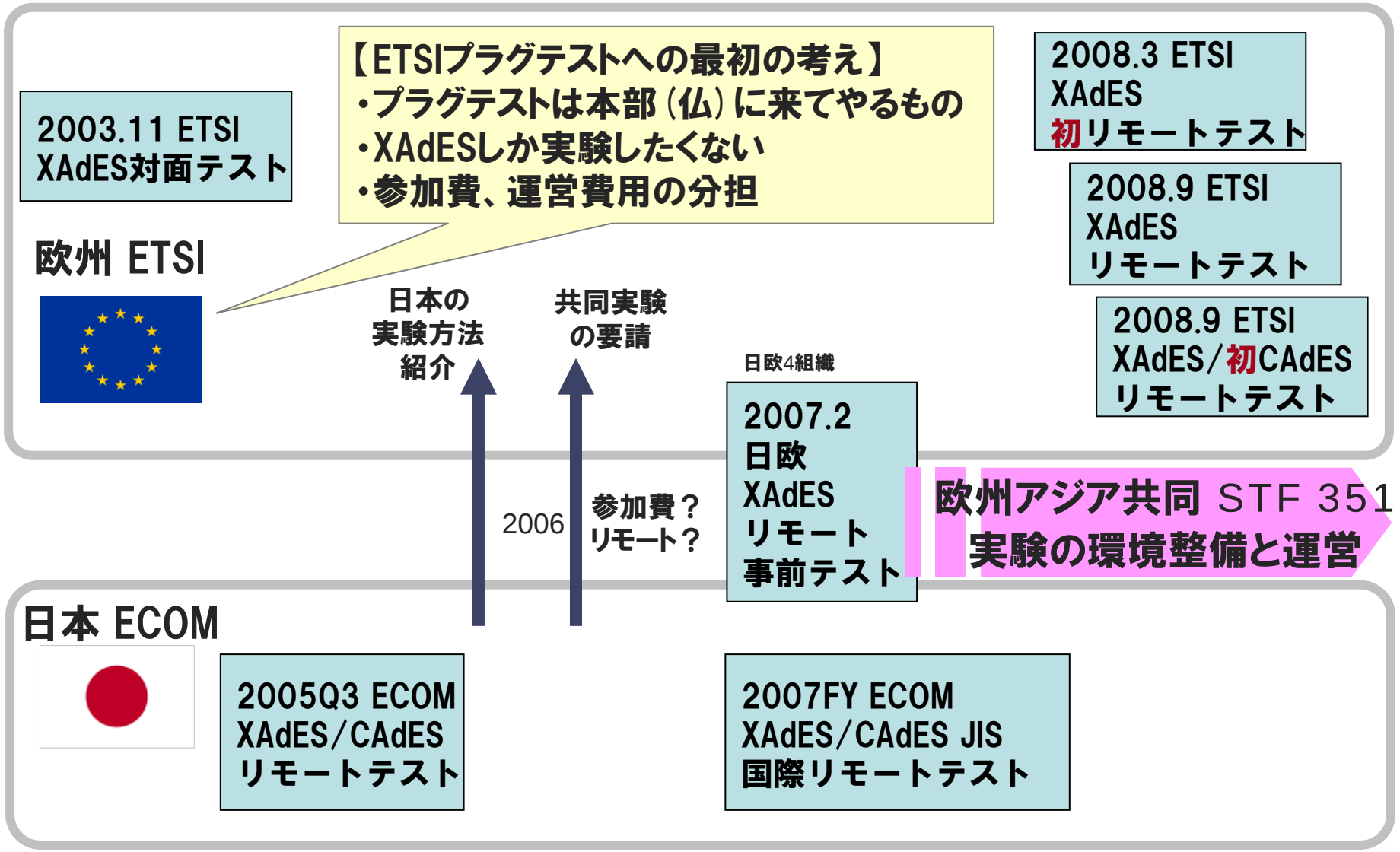
# ETSI CAdES/XAdES リモートテスト
# (1) 概要

# Entrust Se ETSI AdES Plugtest（2008年3月・9月、2009年2月）

- 実施内容
  ECOMテストと同じリモートテスト
  - 共通データ標準準拠性テスト
  - 生成・検証相互運用性テスト
  - 電話会議・自己紹介・製品紹介
- 実験期間は2週間程度
- インターネットと電話会議によりリモートで実験に参加できる（実験方式は日本提案）
- 日本から実験方式、実験企画・運営に貢献


http://www.etsi.org/plugtests/XAdES/XAdES.htm

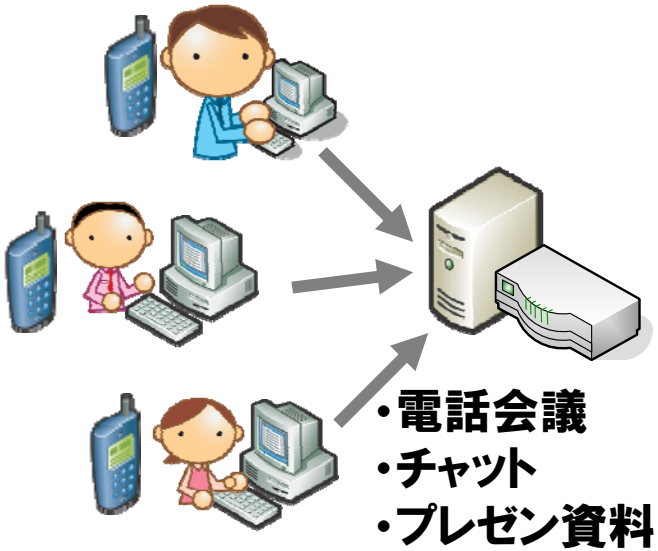
# Entrust CAdES/XAdESプラグテストの歴史



# Entrust® リモートテストとは？

ETSI初

**いちいちETSI本部（フランス）に集わなくても**
**インターネットと電話会議でどこからでも参加できるテスト**



- 電話会議
- チャット
- プレゼン資料
- メーリングリスト

による説明会・情報交換

テストケース閲覧

証明書発行

署名生成

生成した署名のアップ

他参加者署名のDL

署名検証

検証結果ファイルのアップ

- ポータル
- CA+OCSP
- タイムスタンプ局
- テスト結果管理

**メリット**

- （欧州への）出張費がかからなくて助かる
- 仕事の合間に適当にテスト（署名生成・検証）ができる
- 時間的な拘束が少ない（時差もそれほど気にならない）

# Entrust® ETSI Remote XAdES/CAdES Plugtests概要（1/3）

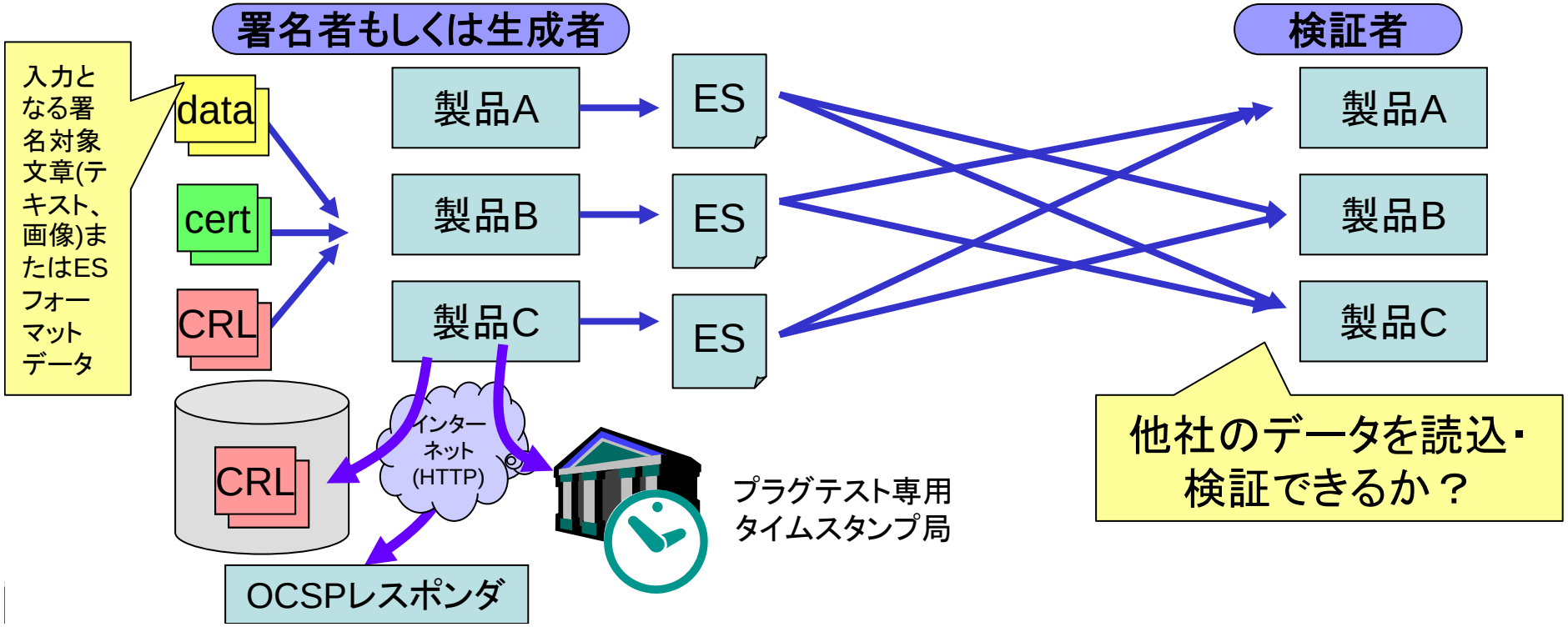
| テスト | 1st Remote XAdES | 2nd Remote XAdES | 3rd RemoteX/CAdES |
|---|---|---|---|
| 時期 | 2008年3月 | 2008年9月 | 2009年2月 |
| 期間 | 1週間 | 1週間 | 2週間 |
| 参加 | 10ヶ国26組織（亜1） | 11ヶ国20組織（亜4） | 12ヶ国17組織（亜4） |
| 参加費 | 359ユーロ（VAT込） | 598ユーロ（VAT込） | 598ユーロ（VAT込） |
| X生成 | 34 (B12,E2,T1,C2,X4,L4,A9) | 34 (B12,E2,T1,C2,X4,L4,A9) | 35 (B12,E2,T1,C3,X4,L4,A9) |
| X失敗系 | 13 (B13) | 20 (B3,E1,T3,C0,X4,L6,A3) | 26 (B4,E1,T3,C1,X4,L8,A5) |
| C生成 | — | — | 34 (B12,E2,T1,C2,X4,L4,A9) |
| C失敗系 | — | — | 19 (B2,E2,T3,C0,X3,L6,A3) |
| 備考 | 初のリモートテスト<br>署名者鍵は共通 | STF351発足後初<br>まともな失敗系検証テスト<br>参加者毎の署名者鍵 | 初のCAdESテスト<br>まともな属性証明書使用テスト |

・※為替レート 当時 1ユーロ=170円ぐらい（2009.06現在137円ぐらい）参加費は5～10万円程度

# Generation and Cross-verification Tests
# (署名データ生成・検証相互運用性テスト)

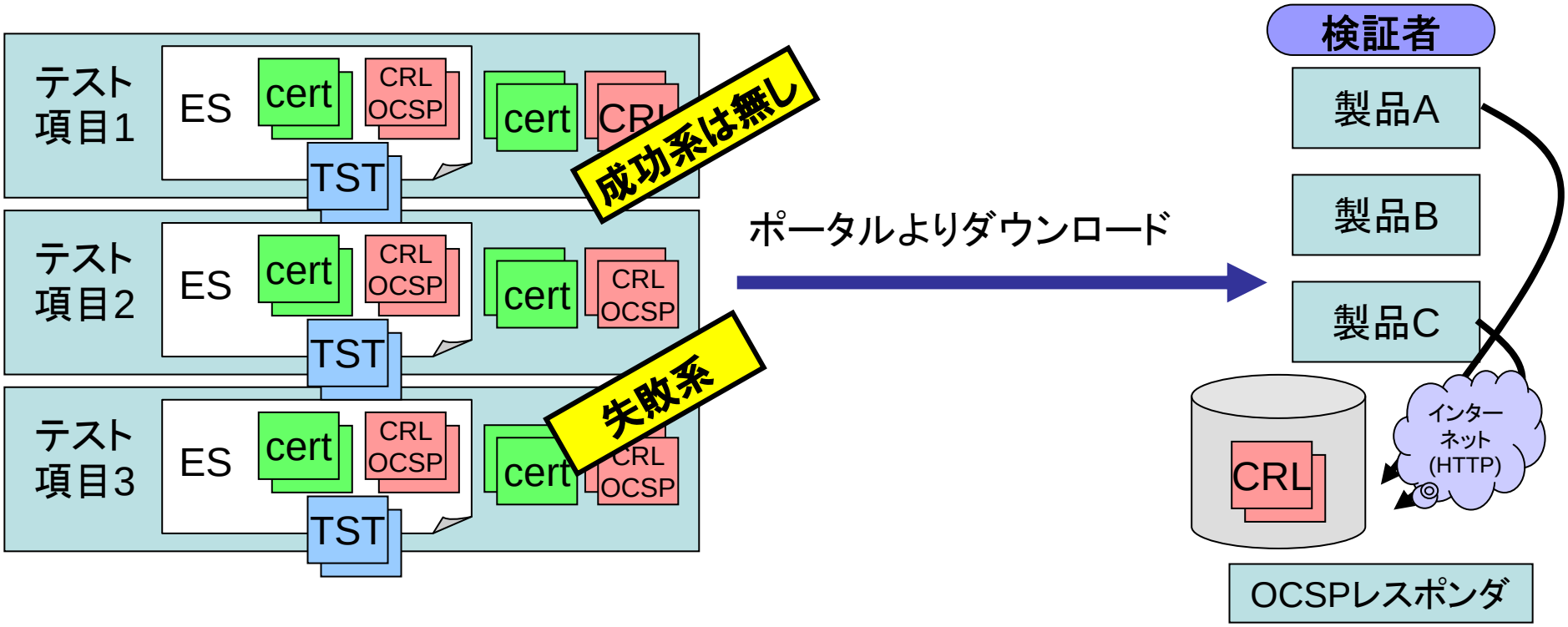
Entrust®

| | |
|---|---|
| 目的 | ・他社実装が生成した有効なCAdES/XAdESフォーマットのデータが相互に読み取り、検証できることを確認 |
| 内容 | 指定した証明書、CRL、タイムスタンプサービスを用いて各実装により有効であるようなCAdES/XAdESフォーマット(BES, EPES, T, C, X, XL, A)を生成する。各実装において読込み、他社の生成したデータが有効である事を検証する。 |



# Only-verification Tests
# 検証機能の標準準拠性テスト

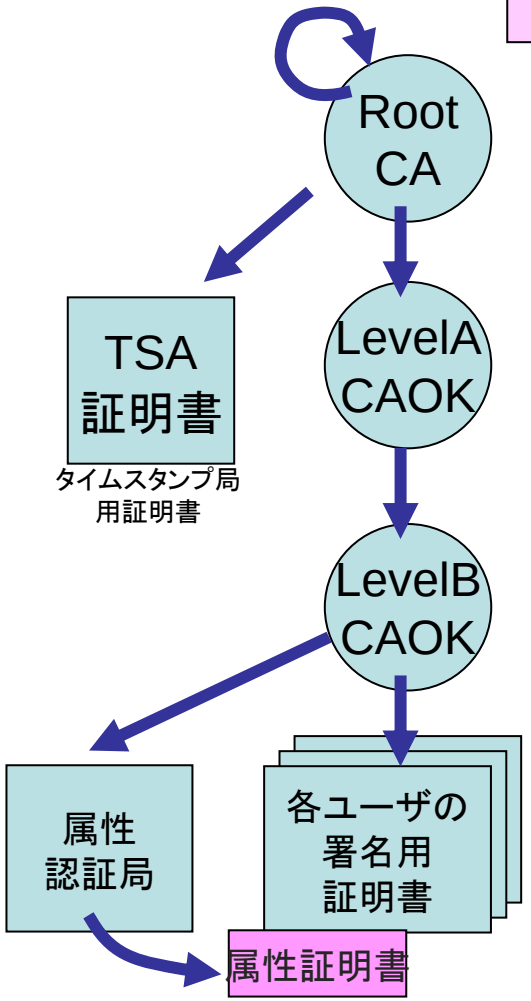
| | |
|---|---|
| 目的 | ・実装されている長期署名フォーマットの検証機能の確認 |
| 内容 | ETSIが作成したESフォーマットのデータ（BES, EPES, T, C, X, XL, A）、検証情報、設定情報のセットをテスト対象として、各社製品で有効性を検証する。期待値は無効のみ。 |



# テスト環境

# Entrust テスト用認証局（CA）の信頼モデル

- **プラグテスト専用のプライベート**CA
- **厳密な階層モデル**(strict hierarchy model)
- **属性証明書**V2**の発行**




自己署名ルート証明書 (プライベート、5年物)
CN=RootCAOK,OU=Plugtest,O=ETSI,STREET=STF-351 2008-2009,C=FR

サブCA証明書 (3年物)
CN=LevelACAOK,OU=Plugtest,O=ETSI,STREET=STF-351 2008-2009,C=FR

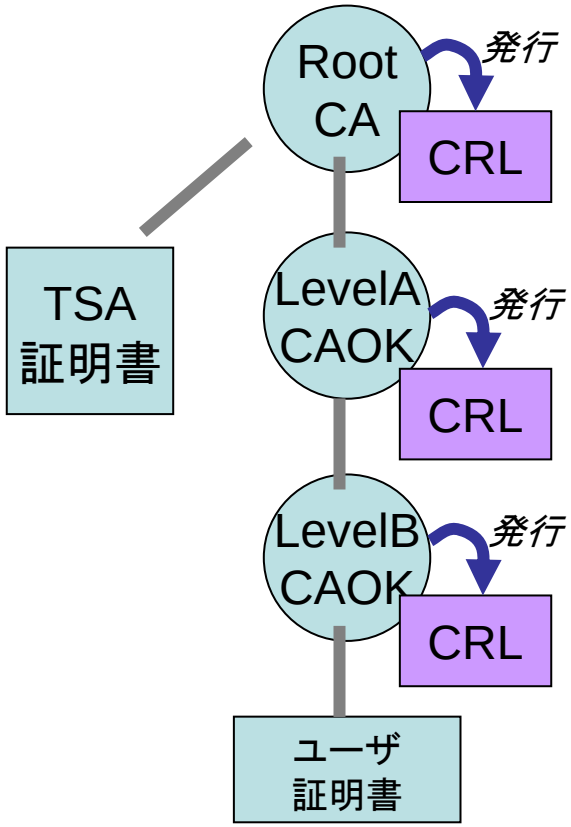
サブCA証明書 (3年物)
CN=LevelBCAOK,OU=Plugtest,O=ETSI,STREET=STF-351 2008-2009,C=FR

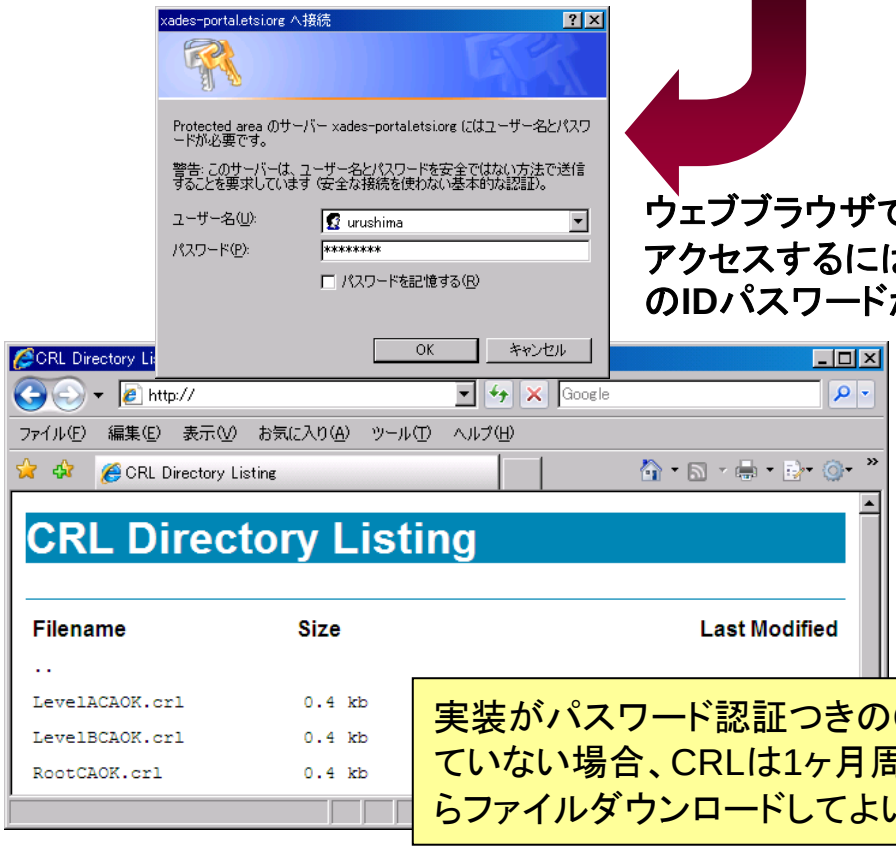
・相互生成検証テスト用の実験参加者の署名用証明書(3年物)
・検証テスト用の証明書 (成功系、失敗系を含む)

・証明書プロファイルは特に特殊なものはない
・一点、OCSPのために機関情報アクセス(AIA)拡張があることだけ

# Entrust テスト用認証局（CA）の証明書失効リスト（CRL）

- **ごく一般的な結合**CRL(FullCRL)**のみです**
- CRL**のプロファイルは一般的で**reasonCode**のエントリ拡張があります**
- CRL**の定期発行周期は全**CA**共通で「**1ヶ月**」です。**
- **従って、猶予期間**(grace period)**に配慮した実装の場合注意が必要です**
- **テスト実施期間中に**CRL**が発行されないよう長さや時期を調整予定です**
- CRL**はHTTPにより配布されますが、そのURLはベーシック認証が必要です**



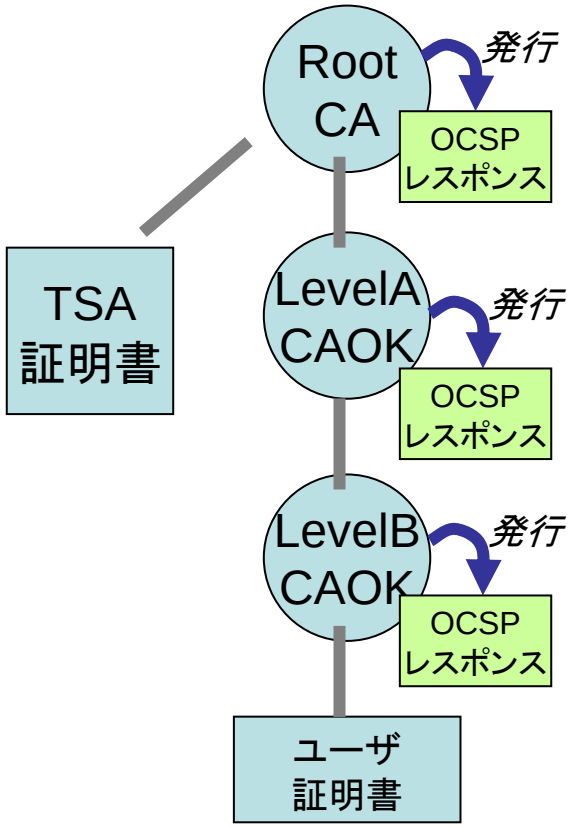




**ウェブブラウザでCRL配布点にアクセスするにはポータルサイトのIDパスワードが必要**

実装がパスワード認証つきのCRLの取得に対応していない場合、CRLは1ヶ月周期なのでブラウザからファイルダウンロードしてよい

# Entrust テスト用認証局のOCSPレスポンダ

- ETSIではECOMには無かったOCSPのテストを行います
- OCSPレスポンダのURLは証明書のAIA拡張に記載されています
- OCSPレスポンダのURLはベーシック認証が必要です
- OCSPの発行モデルは「Direct Model」です
- 即ちOCSPレスポンスは発行するCAの鍵で直接署名されています

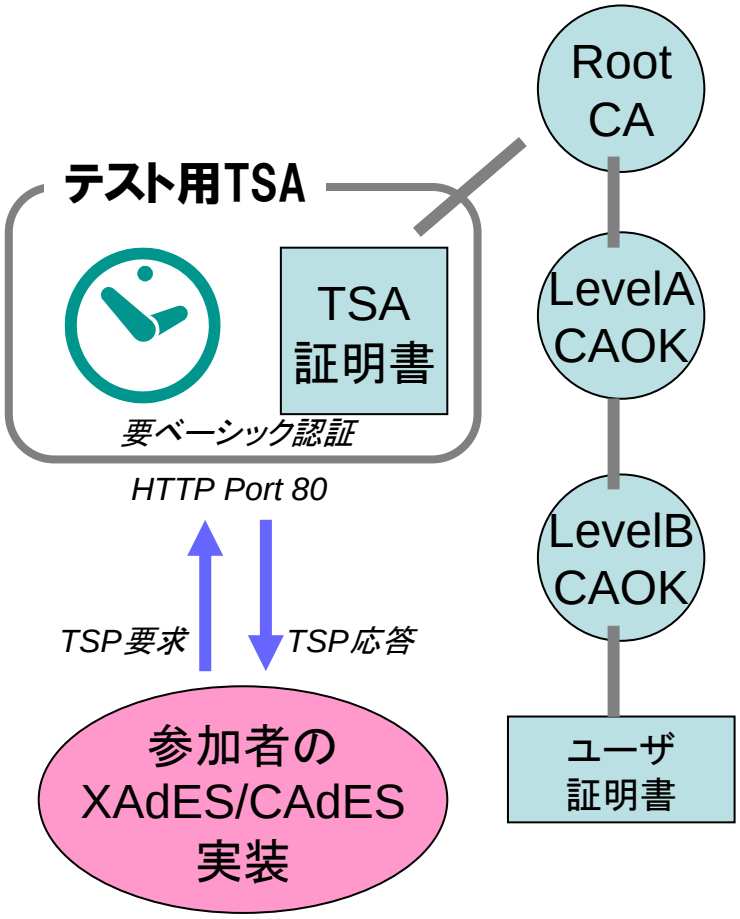



参加者の実装のOCSPの取得がベーシック認証に対応していない場合

参加者の固定IPアドレスによりアクセス制限を行い、認証無しでアクセスできるようにした

# Entrust® テスト用タイムスタンプ局

- RFC 3161**ベースの**HTTP**によるテスト専用タイムスタンプサービス**
- TSP**接続にはベーシック認証が必要です**
- **日本国内の認定時刻認証事業者と異なり**
  genTime**は秒単位です(ミリ秒、マイクロ秒等含まれません)**




参加者の実装のTSPの接続がベーシック認証に対応していない場合

参加者の固定IPアドレスによりアクセス制限を行い、認証無しでアクセスできるようした

# テスト実施の流れ

# テスト実施のフロー

各国の
実験参加者

テストケース閲覧

証明書発行

署名生成

生成した署名のアップ

他参加者署名のDL

署名検証

検証結果ファイルのアップ

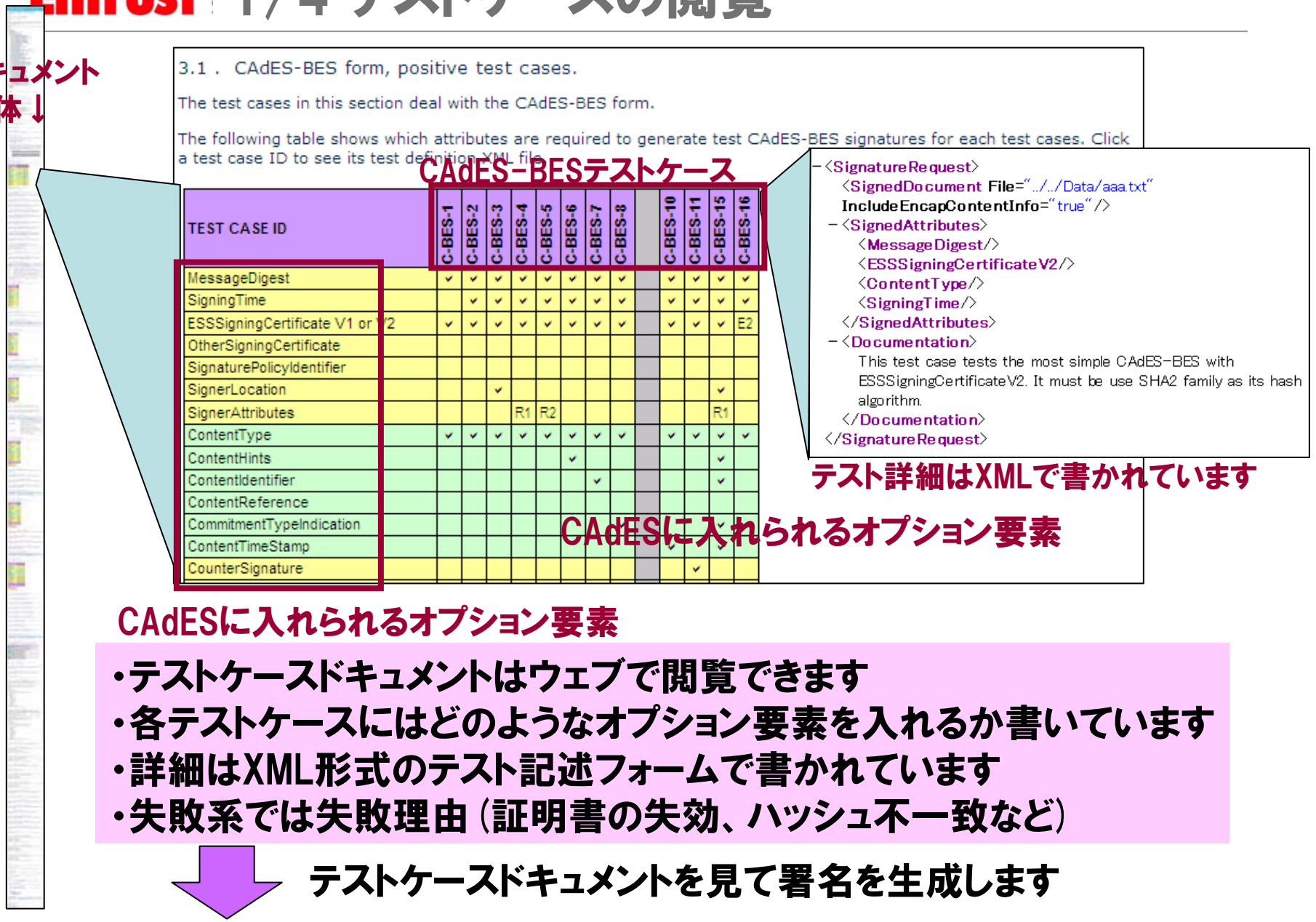
検証結果集計の閲覧

ETSI X/CAdES
テスト用サーバー
(VMWare)

- ポータル
- CA+OCSP
- タイムスタンプ局
- テスト結果管理
  システム

# Entrust 1/4 テストケースの閲覧

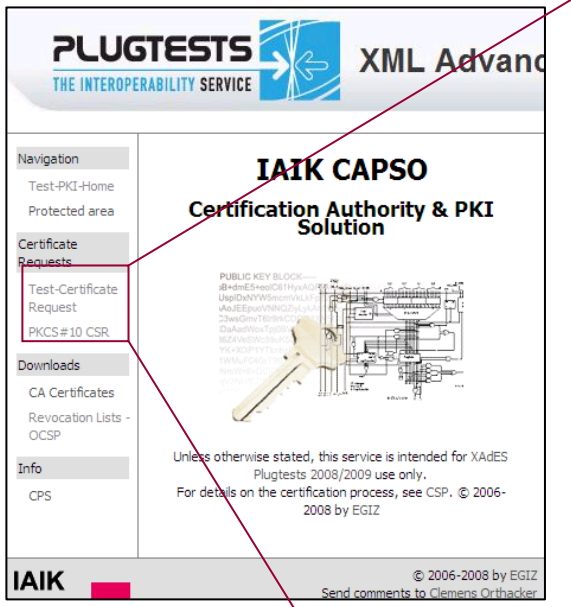
ドキュメント
全体↓




- テストケースドキュメントはウェブで閲覧できます
- 各テストケースにはどのようなオプション要素を入れるか書いています
- 詳細はXML形式のテスト記述フォームで書かれています
- 失敗系では失敗理由（証明書の失効、ハッシュ不一致など）

テストケースドキュメントを見て署名を生成します

# Entrust 2/4 参加者の署名用証明書の発行




ポータルサイトよりCAのページの証明書発行のリンクをクリック

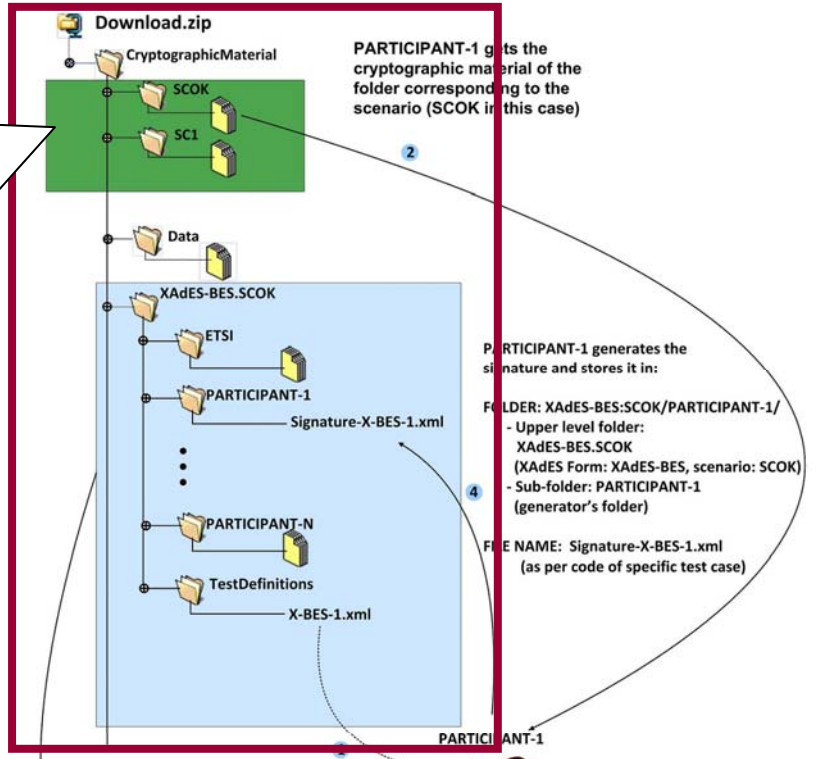

証明書発行に必要な項目を記入します

連絡先メールアドレスに証明書発行のURLが届くので、このリンクを開くとWindows証明書ストアに発行された証明書が格納されます

JavaなどWindows CryptoAPI以外の環境で使う場合にはPKCS#12ファイルとしてエクスポートして使います

# Entrust® 3/4 生成した署名・他参加者署名検証結果のアップロード

- 指定されたフォルダ階層をコピーしておきます
- 署名ファイルを置きます
- 検証結果ファイルを置きます
- ZIPアーカイブで固めます
- ポータルにアップロードします




# Entrust 4/4 検証結果の集計 (1)

**他参加者による署名の検証結果はアップロードされる度に自動集計され、結果一覧をポータルで見られます**

Signer company: ENT

The following table shows the verification results for the signatures of ENT in case of XAdES-BES.SCOK.

| Verifiers → TestCases ↓ | | | | | | | | | | | | | | | | ENT | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X-BES-1.xml | S:N | S:V | S:V | S:N | S:V | S:V | S:V | S:N | S:V | S:V | S:N | S:V | S:N | S:N | S:V | S:V | S:V | S:N |
| X-BES-2.xml | S:N | S:V | S:V | S:N | S:V | S:V | S:V | S:N | S:V | S:V | S:N | S:V | S:N | S:N | S:V | S:V | S:V | S:N |
| X-BES-3.xml | S:N | S:N | S:V | S:N | S:V | S:V | S:V | S:N | S:V | S:V | S:N | S:V | S:N | S:N | S:V | S:V | S:V | S:N |
| X-BES-4.xml | S:N | S:N | S:V | S:N | S:V | S:V | S:V | S:N | S:V | S:V | S:N | S:V | S:N | S:N | S:V | S:V | S:V | S:N |
| X-BES-5.xml | S:N | S:N | S:V | S:N | S:V | S:V | S:V | S:N | S:N | S:N | S:N | S:V | S:N | S:N | S:V | S:V | S:N | S:N |
| X-BES-6.xml | S:N | S:N | S:V | S:N | S:V | S:V | S:V | S:N | S:N | S:V | S:N | S:V | S:N | S:N | S:V | S:V | S:V | S:N |
| X-BES-7.xml | S:N | S:N | S:V | S:N | S:V | S:V | S:V | S:N | S:N | S:V | S:N | S:V | S:N | S:N | S:V | S:V | S:V | S:N |
| X-BES-8.xml | S:N | S:N | S:V | S:N | S:V | S:V | S:V | S:N | S:N | S:N | S:N | S:V | S:N | S:N | S:V | S:V | S:V | S:N |
| X-BES-9.xml | S:N | S:N | S:V | S:N | S:V | S:V | S:V | S:N | S:N | S:V | S:N | S:V | S:N | S:N | S:V | S:V | S:V | S:N |
| X-BES-10.xml | S:N | S:N | S:V | S:N | S:V | S:V | S:V | S:N | S:N | S:V | S:N | S:V | S:N | S:N | S:V | S:V | S:V | S:N |
| X-BES-11.xml | S:N | S:N | S:N | S:N | S:V | S:V | S:V | S:N | S:N | S:V | S:N | S:V | S:N | S:N | S:V | S:V | S:V | S:N |
| X-BES-15.xml | S:N | S:N | S:N | S:N | S:V | S:V | S:V | S:N | S:N | S:V | S:N | S:V | S:N | S:N | S:V | S:V | S:V | S:N |

# Entrust® 4/4 検証結果の集計 (2)

Signer company

**相手側検証でエラーが出ると以下のように赤く表示されます**

The following table shows the verification results for the signatures of UPC in case of XAdES-BES.SCOK.

| Verifiers → TestCases ↓ | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X-BES-1.xml | S:N | S:V | S:V | S:N | S:V | S:V | S:V | S:N | S:V | S:V | S:N | S:V | S:N | S:N | S:V | S:V | S:V | S:N |
| X-BES-8.xml | S:N | S:N | S:V | S:N | S:V | S:V | S:V | S:N | S:N | S:V | S:N | S:V | S:N | S:N | S:F | S:V | S:V | S:N |
| X-BES-9.xml | S:N | S:N | S:F | S:N | S:V | S:V | S:V | S:N | S:N | S:V | S:N | S:V | S:N | S:N | S:I | S:F | S:V | S:N |
| X-BES-10.xml | S:N | S:N | S:F | S:N | S:V | S:V | S:V | S:N | S:N | S:V | S:N | S:V | S:N | S:N | S:F | S:F | S:V | S:N |
| X-BES-11.xml | S:N | S:N | S:N | S:N | S:V | S:V | S:V | S:N | S:N | S:N | S:N | S:V | S:N | | | S:V | S:V | S:N |
| X-BES-15.xml | S:N | S:N | S:N | S:N | S:V | S:V | S:V | S:N | S:N | S:V | S:N | | | | | S:V | S:V | S:N |

**クリックすれば失敗理由・ログなど表示される**

<Failed>
schema validation error. Id attribute can't be used in CertifiedRole.
</Failed>

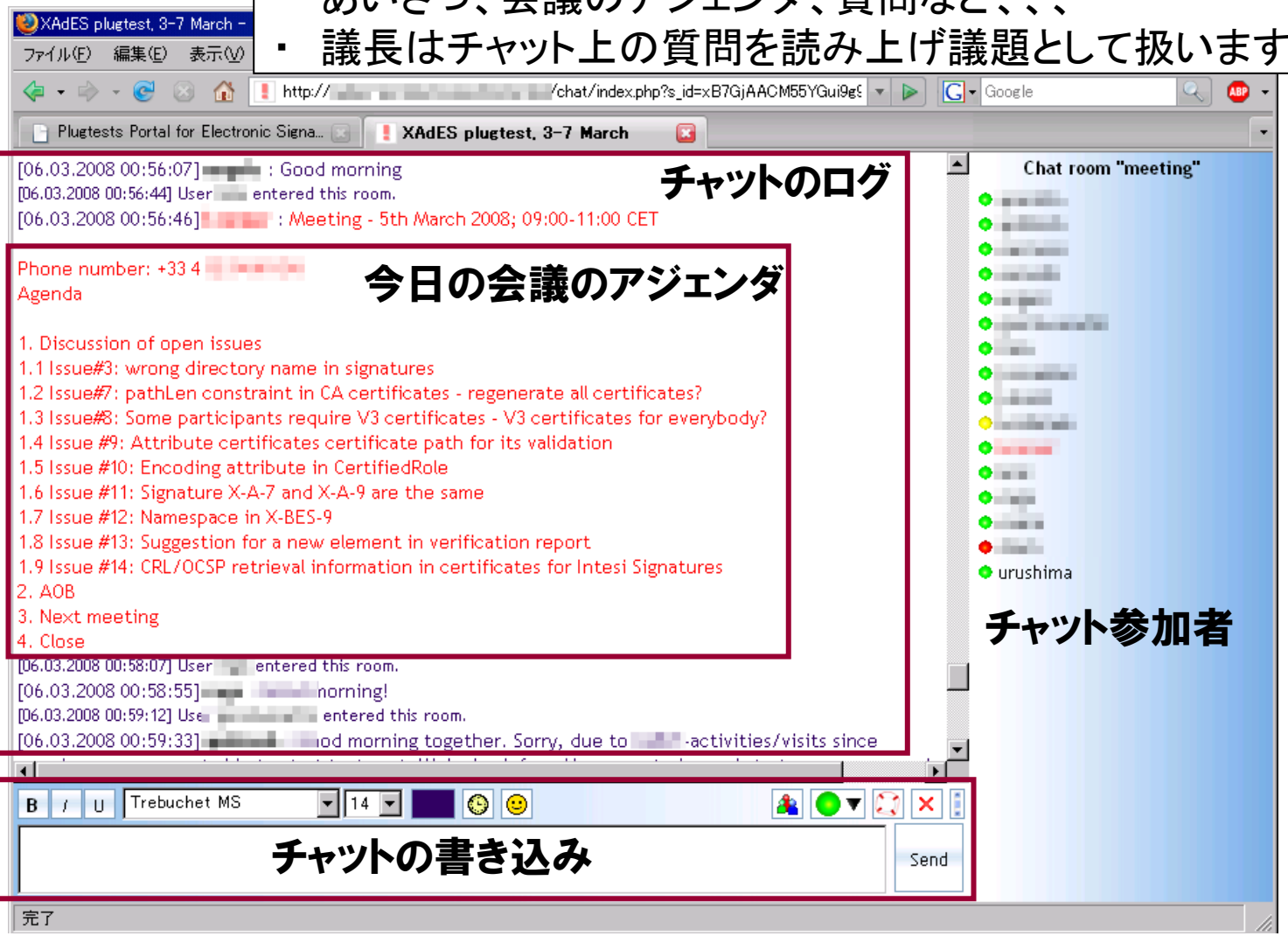
**署名検証に失敗した場合、赤色で表示される**
**真面目に検証していない実装は緑色にすることもあります、、、**

# Entrust リモートテストの通信連絡手段

| | |
|---|---|
| 電話会議 | 初回オリエンテーションで参加者自己紹介とテスト方法の説明。あとはテスト期間中１～２回、事務局からのアナウンスと質疑応答、問題点の指摘など行います。 |
| チャット | 電話会議を補助するために使います。参加者の数十名の電話会議なので、議長が話すのが殆どのため、質問、コメントなどはチャットで行うことが多く、書き込めばこれを議長が取り上げてくれます。 |
| メールリスト | 通常のアナウンスやテスト仕様、テスト環境、相手の署名の問題点の指摘などあれば基本的にメールリストで行います。 |
| ウェブポータル | 署名や署名生成に必要なデータ、検証結果のダウンロード・アップロードはウェブポータルを使います。 |

# Entrust: 電話会議を補助するチャット

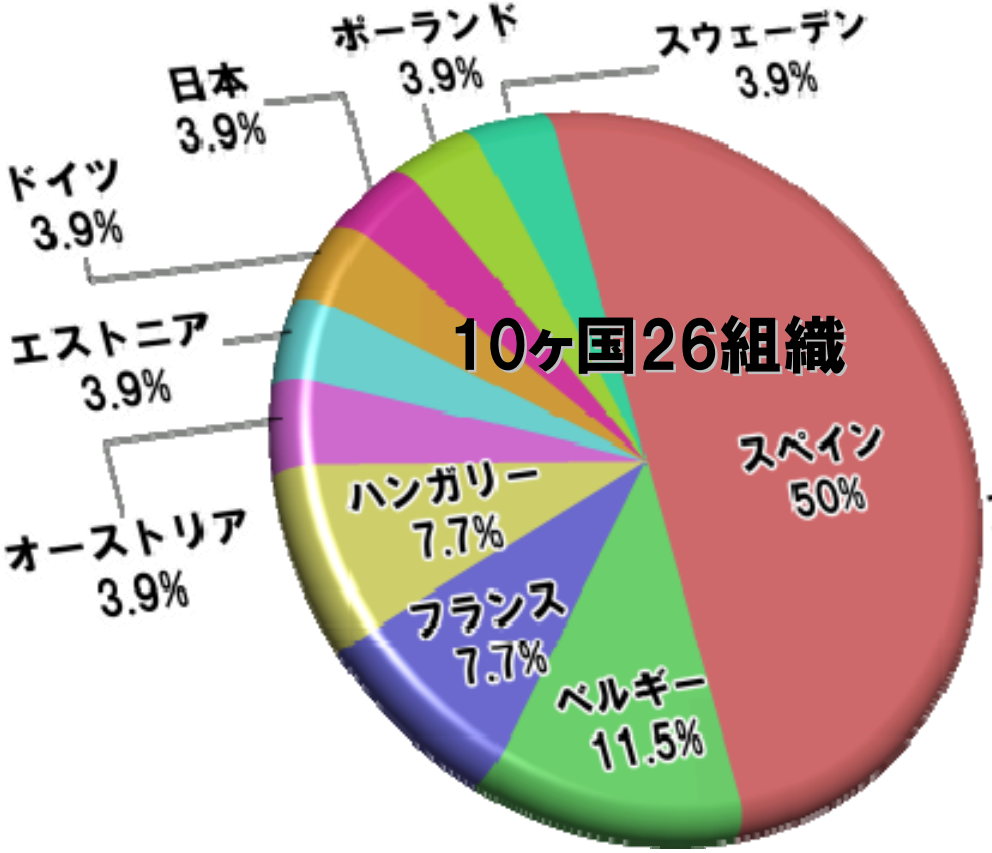
- 電話会議の際の対話を補助するためにチャットを使います
- ウェブブラウザでポータルサイトから開けます
- あいさつ、会議のアジェンダ、質問など、、、
- 議長はチャット上の質問を読み上げ議題として扱います



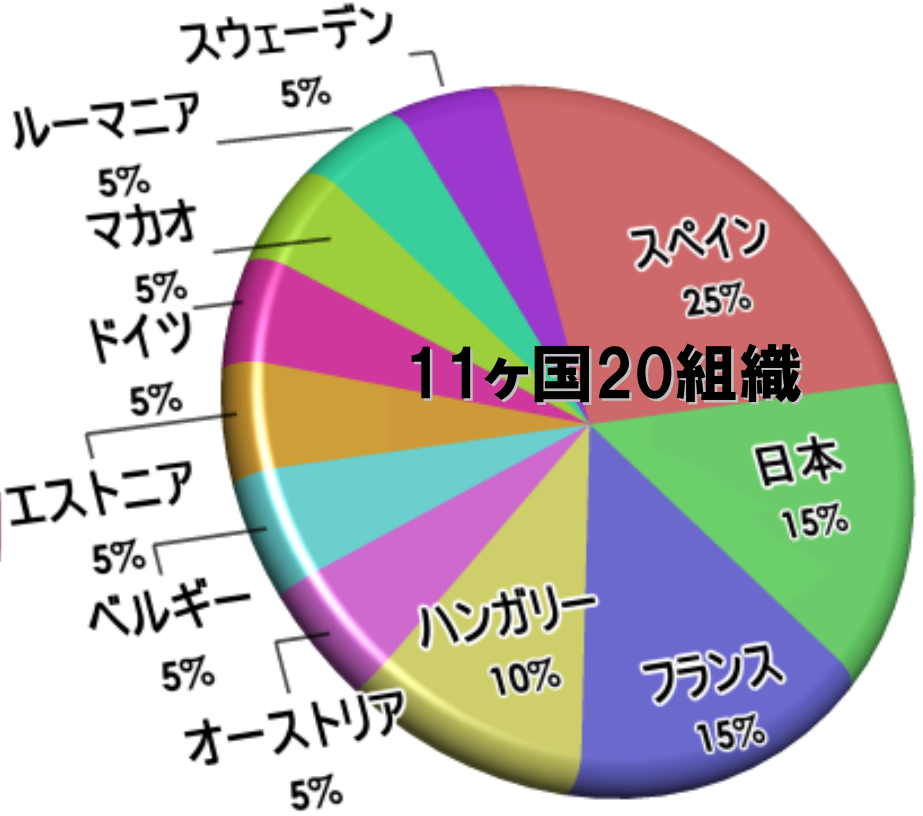
# テスト結果

# ETSI Remote XAdES/CAdES Plugtests概要（1/3）

## 第一回テスト（'08.3）

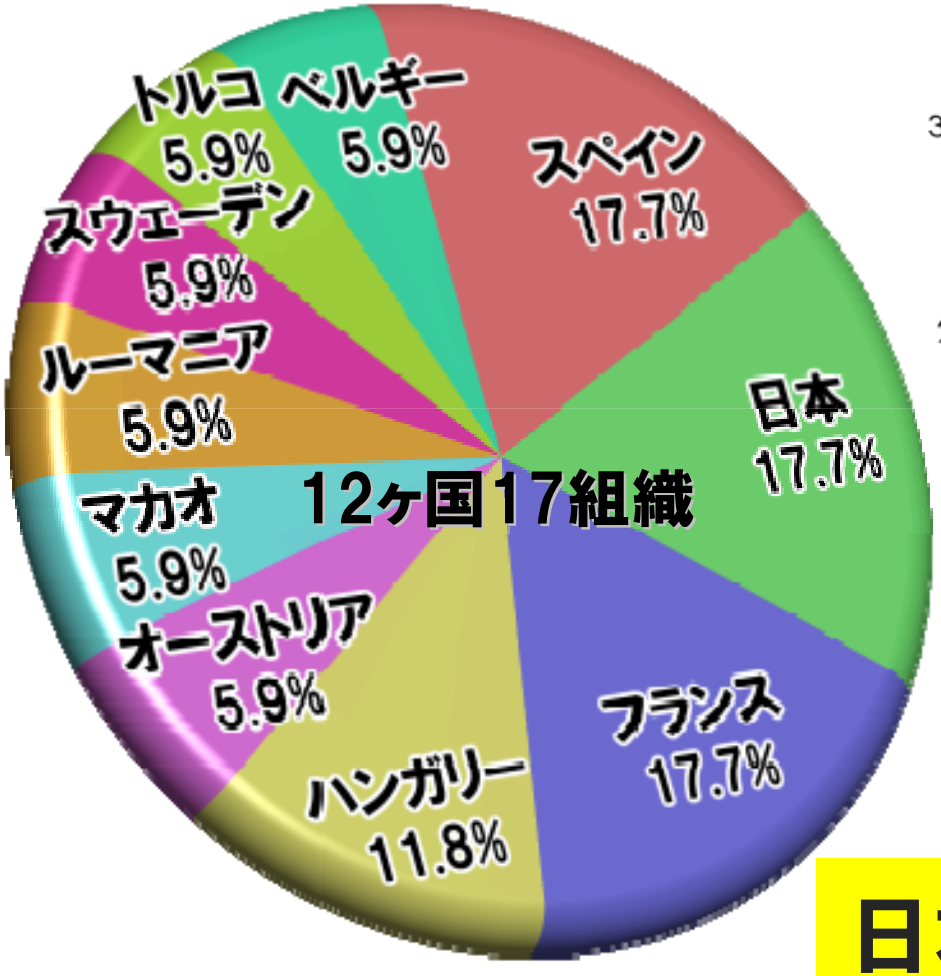



## 第二回テスト（'08.9）

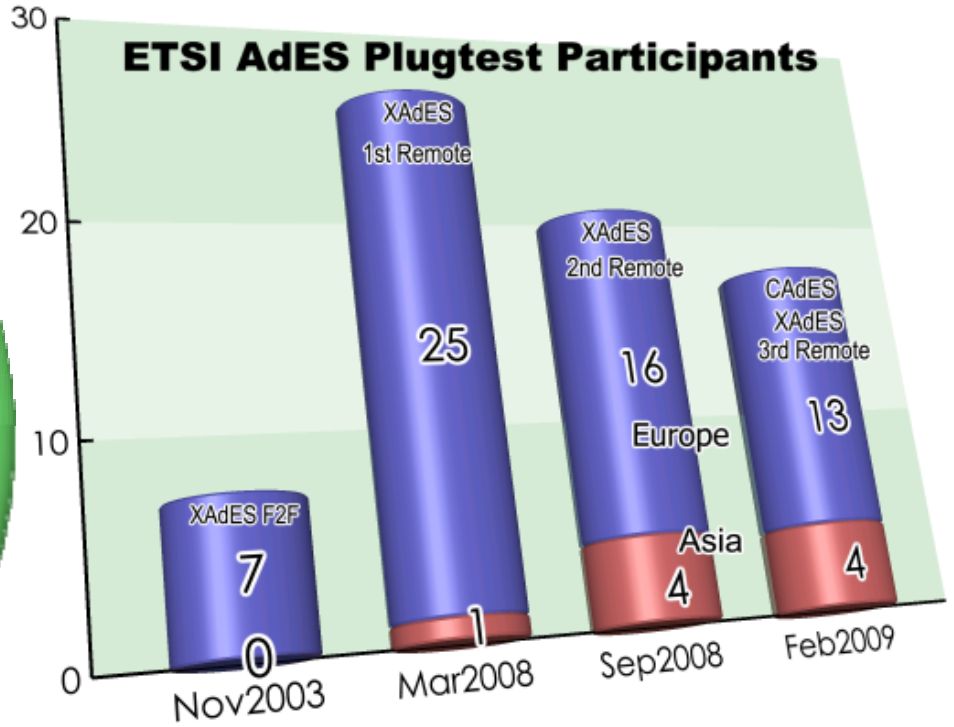


# ETSI Remote XAdES/CAdES Plugtests概要 (2/3)

## 第三回テスト ('09.2)




## 参加国推移

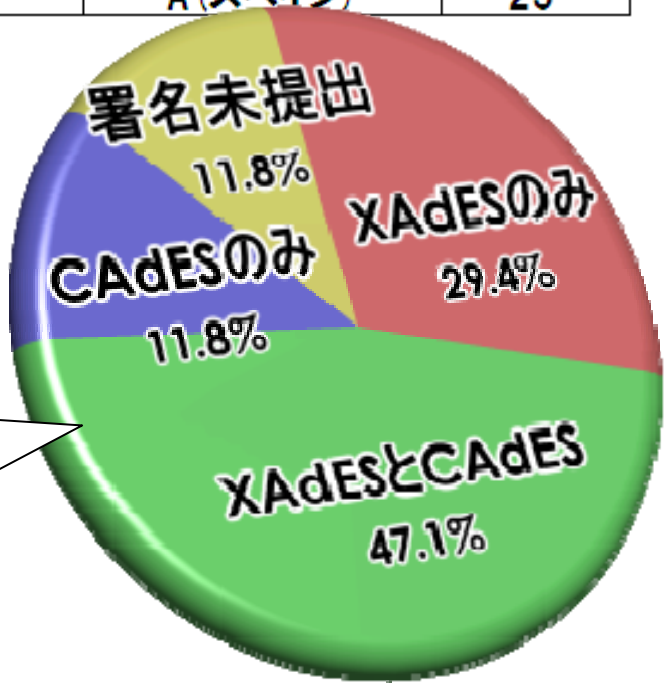



**日本から累計5組織が参加**

# Entrust テスト結果と傾向

| ランキング | XAdES | 実装率% | CAdES | 実装率% | 総合 | 実装率% |
|---|---|---|---|---|---|---|
| 1 | エントラスト（日本） | 100 | エントラスト（日本） | 100 | エントラスト（日本） | 100 |
| 2 | P（ハンガリー） | 97 | C2（フランス） | 94 | C2（フランス） | 88 |
| 3 | U（スペイン） | 94 | S1（日本） | 82 | U（スペイン） | 72 |
| 4 | I（オーストリア） | 91 | S2（スペイン） | 53 | S2（スペイン） | 55 |
| 5 | C2（フランス） | 83 | U（スペイン） | 50 | P（ハンガリー） | 49 |
| 6 | F（ベルギー） | 77 | T1（トルコ） | 32 | I（オーストリア） | 46 |
| 7 | S2（スペイン） | 57 | M2（ハンガリー） | 18 | S1（日本） | 41 |
| 8 | M2（ハンガリー） | 37 | A（スペイン） | 15 | F（ベルギー） | 39 |
| 9 | A（スペイン） | 34 | C1（ルーマニア） | 6 | M2（ハンガリー） | 28 |
| 10 | O（フランス） | 31 | T2（スウェーデン） | 6 | A（スペイン） | 25 |

- **やはりXAdESは欧州では実装が充実している**
- CAdESは**初欧州テストにしては頑張っている**
- **日本の参加企業も頑張っている**




- **初回テストにしてはCAdESは充実していた**
- **思ったほどCAdESが無いというわけではない**
- XAdESと**CAdESの双方を実装する企業が多い**

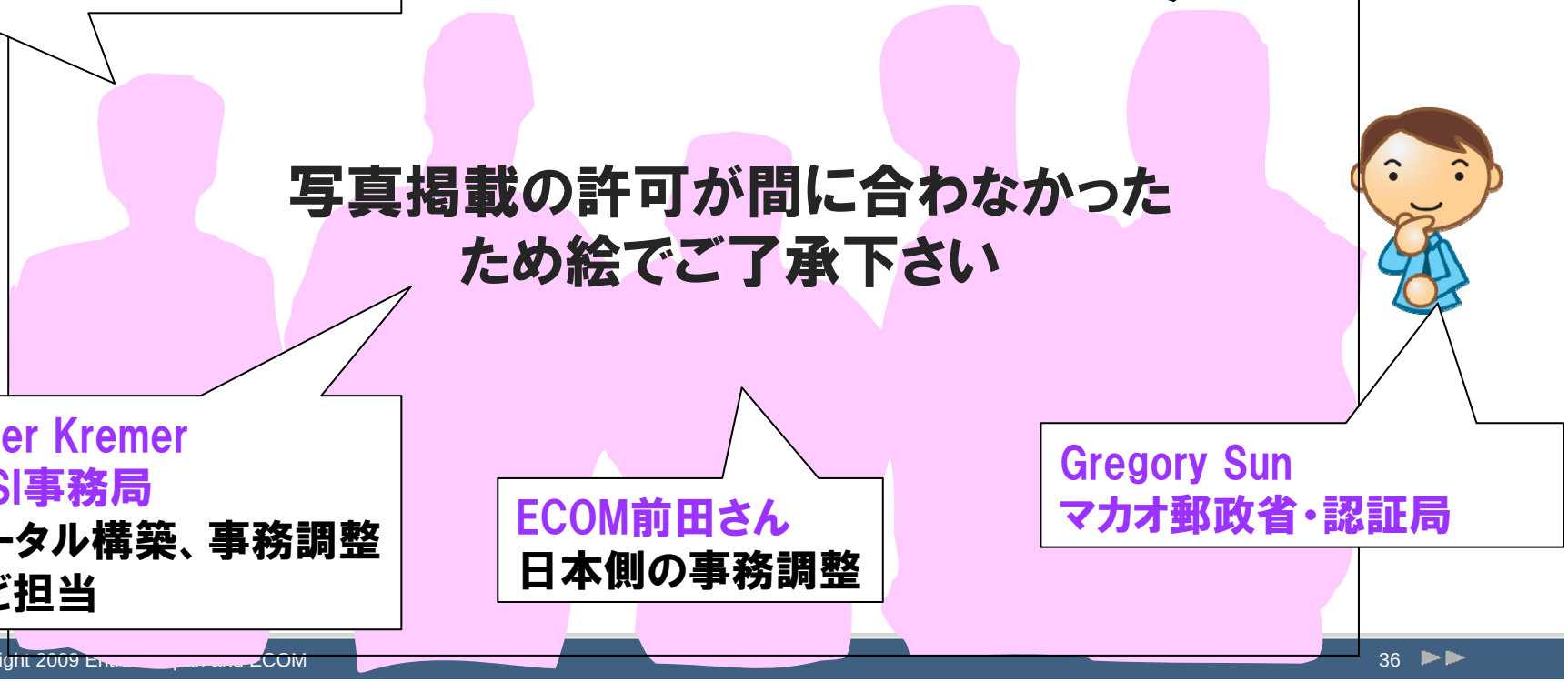
# ETSI STF351
# プラグテストの企画、実験運営、環境整備を行うタスクフォース

# Entrust ETSI STF-351(1)

STF351リーダー
Juan Carlos Cruellas教授
スペイン カタロニア工科大
XAdESテスト全般を担当
XAdES, OASIS-DSSX
などのエディタ
村上春樹のファン・お刺身
好き

エントラスト 漆嶌
リモート方式の企画
CAdES全般設計
XAdES失敗系のテスト
データ生成等を担当

Konrad Lanz
オーストリア IAIK, ASIT
ポータル, CA, TSA, OCSP
構築
XAdESテスト設計
W3C XMLDSIG, OASIS
DSSX, XAdES
エディタ



写真掲載の許可が間に合わなかった
ため絵でご了承下さい



Peter Kremer
ETSI事務局
ポータル構築、事務調整
など担当

ECOM前田さん
日本側の事務調整

Gregory Sun
マカオ郵政省・認証局

# ETSI STF-351 (2)

- ETSI Specialist Task Force 351
  - Interoperability framework for XAdES
  - http://portal.etsi.org/stfs/STF_HomePages/STF351/STF351.asp
  - 2008年度3回のAdESのプラグテスト企画,準備,運営,サポート
  - eEurope, 欧州委員会 (EC) で承認された活動 (要レポート)
- 活動
  - 実施期間:2008年4月～2009年3月
  - プラグテストの企画・テストケース設計・テストデータ生成
  - ポータルサイトの構築・テストのチュートリアル・サポート
  - ほぼ週一回の電話会議 (+Skypeチャット)
  - 2回の対面会議 (2008年8月東京、2009年2月バルセロナ)
  - メーリングリスト・FTPサイトでのドキュメント共有
  - セミナーの実施 (2008年8月東京、2009年1月フランスETSI本部)

# プラグテスト所感

# ETSIの長期署名は標準化サイクルがうまくまわっている


- 標準の不明瞭・曖昧な箇所が相互運用実験により露呈する
- 実装からの標準へのフィードバック
- ただ実験参加者の意見をそのまま取り入れるのは危険
- 実験参加者は過去の経緯を知らないし標準化の専門家ではない。

# ETSIとECOMとのテストの意識の違い

| | ETSIテスト | ECOMテスト |
|---|---|---|
| 誰のため？ | 標準化のエディタ<br>実験参加組織 | 実験参加組織 |
| 主目的 | ① 標準の改訂・改良が主目的<br>② XAdESだけでよい | ① 実験参加組織の満足（問題の修正,テスト参加／合格表明,高相互運用性）<br>②長期署名フォーマットおよびJISプロファイルの国内普及<br>③ CAdESとXAdES双方の普及 |
| 検証テスト | 失敗系のみで、実装者しかテスト結果を活用できない。テストケースが成熟してない。時間もリソースも無かった。 | ブラックボックステストを目標とし、成功系、失敗系を含み、実装者はもちろん、製品を購入するユーザが機能を具備するか判定できる。 |

# 検証テストのブラックボックステスト

**実装の中身を知らなくても当該の機能があるかどうか判定できるテスト**

**例えばSHA-256のMessageDigest属性を扱えるか判定するには**

| テストケース | 期待値 | 結果 |
|---|---|---|
| SHA-1のMessageDigestが署名対象と一致 | 有効 | 有効 |
| SHA-1のMessageDigestが署名対象と不一致 | 無効 | 無効 |
| SHA256のMessageDigestが署名対象と一致 | 有効 | 有効 |
| SHA256のMessageDigestが署名対象と不一致 | 無効 | 無効 |

**これら全てが期待値と一致するなら「機能を具備する」と言える**
**テストを自動で流すだけで、どのような機能を持つか自動判定できる**

# 関連技術の標準化動向

# 長期署名フォーマットに関係する標準化の動向

2009年
6月現在

- CAdES 1.8.1 ドラフト（CMS形式の長期署名フォーマット）
- XAdES 1.4.1 ドラフト（XML形式の長期署名フォーマット）
- JIS長期署名フォーマットプロファイルのISO提案
  - 2008.11にTC154（電子商取引）でNWI提案したが5月投票で積極参加がわずか1カ国不足。あきらめず継続して調整する国内合意。
- RFC 3161bis ドラフト（タイムスタンププロトコルの改訂）
- PDF長期署名フォーマット

# 本日のまとめ

# 本日のまとめ

- ETSIで昨年度3回行われた長期署名の相互運用テストの報告
  - テスト概要
  - テスト環境
  - テスト手順
  - テスト結果
- 相互運用テストの運営、企画、環境整備を行うタスクフォース
  - STF351の紹介と活動概要
- プラグテストの所感
- 長期署名関連の標準の動向

# ご清聴ありがとうございました

# 参考リンク

- ETSI XAdES/CAdES Interoperability Tests
  - http://xades-portal.etsi.org/pub/index.shtml
  - http://www.etsi.org/plugtests/XAdES2/html/XAdES2.htm
- ETSI Specialist Task Force 351 (ETSI専門家タスクフォース351)
  - STF-351: Interoperability framework for XAdES
  - http://portal.etsi.org/stfs/STF_HomePages/STF351/STF351.asp
- ECOM長期署名フォーマットプラグテスト
  - http://www.ecom.jp/LongTermStorage/index.html
- ETSI Top Page
  - http://www.etsi.org/WebSite/homepage.aspx
- RFC 5126 CAdES
  - http://tools.ietf.org/html/rfc5126
- W3C Note XAdES
  - http://www.w3.org/TR/XAdES/ (古い v1.1.1)