

電子署名をめぐる国内外の最新動向 (2)

- Trust Application Service Providers 関連技術 -

2014. 3. 13

NTTセキュアプラットフォーム研究所

石本 英隆

◆電子署名を利用した、Trust Application Service Providers(TASP : アプリケーションサービス提供者)について紹介

(1) EUのパイロットプロジェクト

PEPPOL, SPOCS, STORK, epSOS, e-CODEX

(2) 基盤となるETSI仕様他関連技術

eDelivery, eDocument, MIDB, eSafe...,
Registered eMail, Data Preservation

Trust Application Service Providers (TSAP) **JNSA**

定義:(TR 119 500 4.1節より)

“A Trust Application Service Provider (TASP) operates a value added Trust Service offering value added services applying electronic signatures that relies on the generation/validation of electronic signatures in normal operation.”

**電子署名を用いて、信頼される付加価値
サービスを提供するプロバイダ**

①データの「信頼できる」配送サービス:

“e-delivery” service

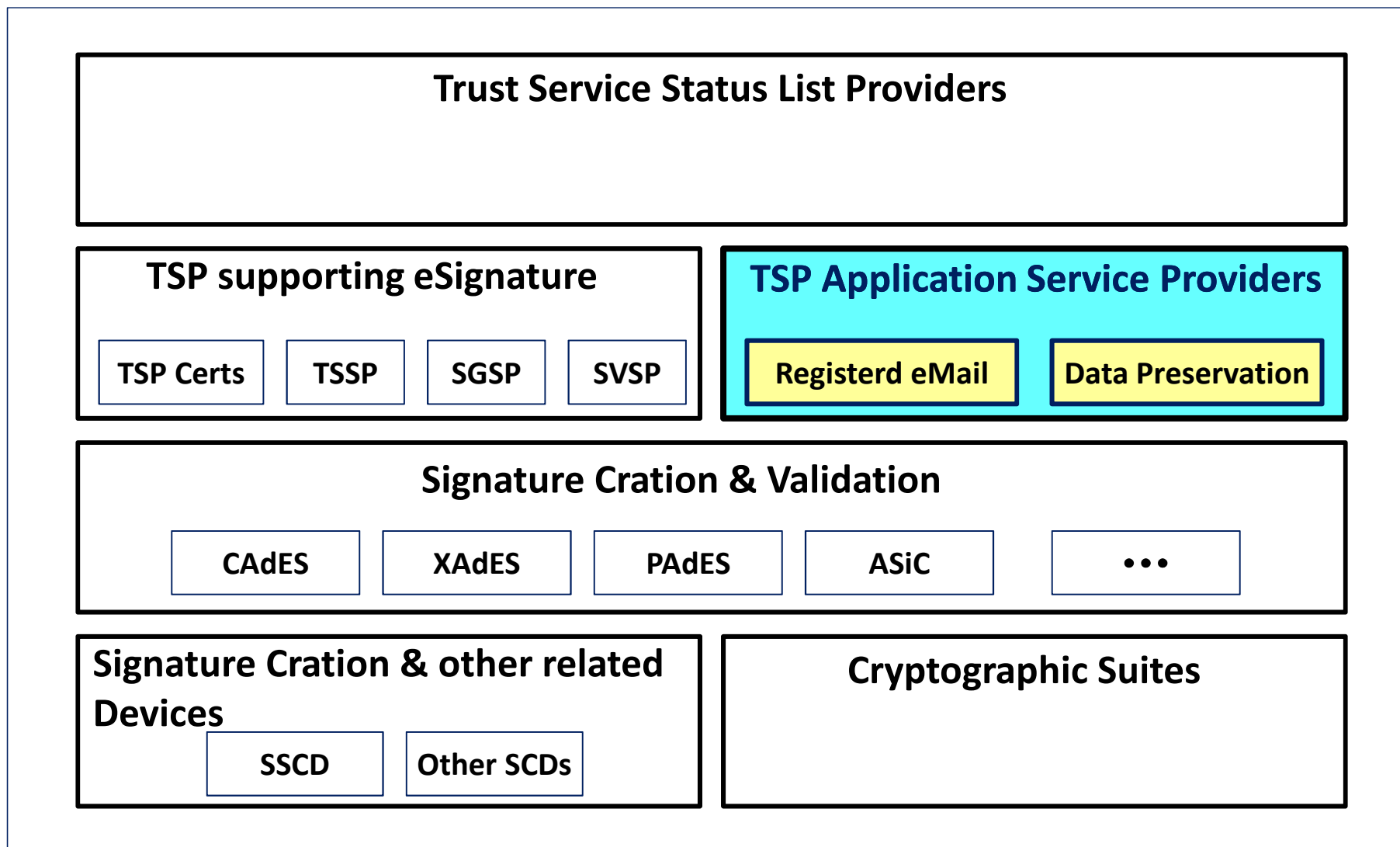
②データの「信頼できる」保存サービス:

Long term storage service

TASPの位置付け(署名関連フレームワーク)



ETSI , CEN, ETSI SR 001 604「Rationalised Framework for Electronic Signature Standardisation」より



TASP関連規格体系



1. ガイダンス	TR 119 500 適用されるべき規格の選定に関するガイダンス	Draft
	SR 019 530 e-Delivery サービスに関する要件	未
2. ポリシーとセキュリティ要件	EN 319 511 Registered eMailのサービス提供者向け要件	未
	EN 319 521 Data Preservationのサービス提供者向け要件	未
3. 技術仕様	EN 319 512 Registered eMail技術仕様 (概説,論理アーキテクチャ,管理証跡,msgフォーマット,トランスポート,相互運用性)	未
	EN 319 522 Data Preservation技術仕様 (電子署名,TST利用に関する規定)	未
ベース規格: TR 102 640 Registered eMail、TR 101 533 Data Preservation		済
4. 適合性評価	EN 319 513 Registered eMail 提供者の適合性評価基準	未
	EN 319 523 Data Preservation 提供者の適合性評価基準	未
5. 評価検査実施	TS 119 504 技術適合性と相互運用性試験に関する要件	未
	TS 119 514 相互運用性評価用テストスイート	未

http://www.buildconnectgrow.eu/

JNSA

ITCを活用したEUの経済成長戦略
“Build, Connect, Grow”



欧州のElectronic Delivery関連プロジェクト

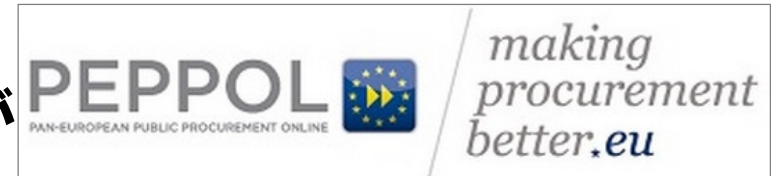
European Large Scale Pilots (LSPs)



- **PEPPOL** (Pan-European Public eProcurement On-Line)
EU内公共事業の電子調達システム基盤
- **SPOCS** (Simple Procedures Online for Cross-border Services)
大規模ポータルサイト基盤(SSO,ワンストップ)
- **STORK** (Secure idenTity acrOss boRders linKed)
eID相互運用基盤
- **epSOS**(eHealth)
医療記録相互運用基盤
- **e-CODEX** (e-Justice Communication via Online Data Exchange)
法的情報のデータ交換用基盤

PEPPOL (Pan-European Public eProcurement On-Line) **JNSA**

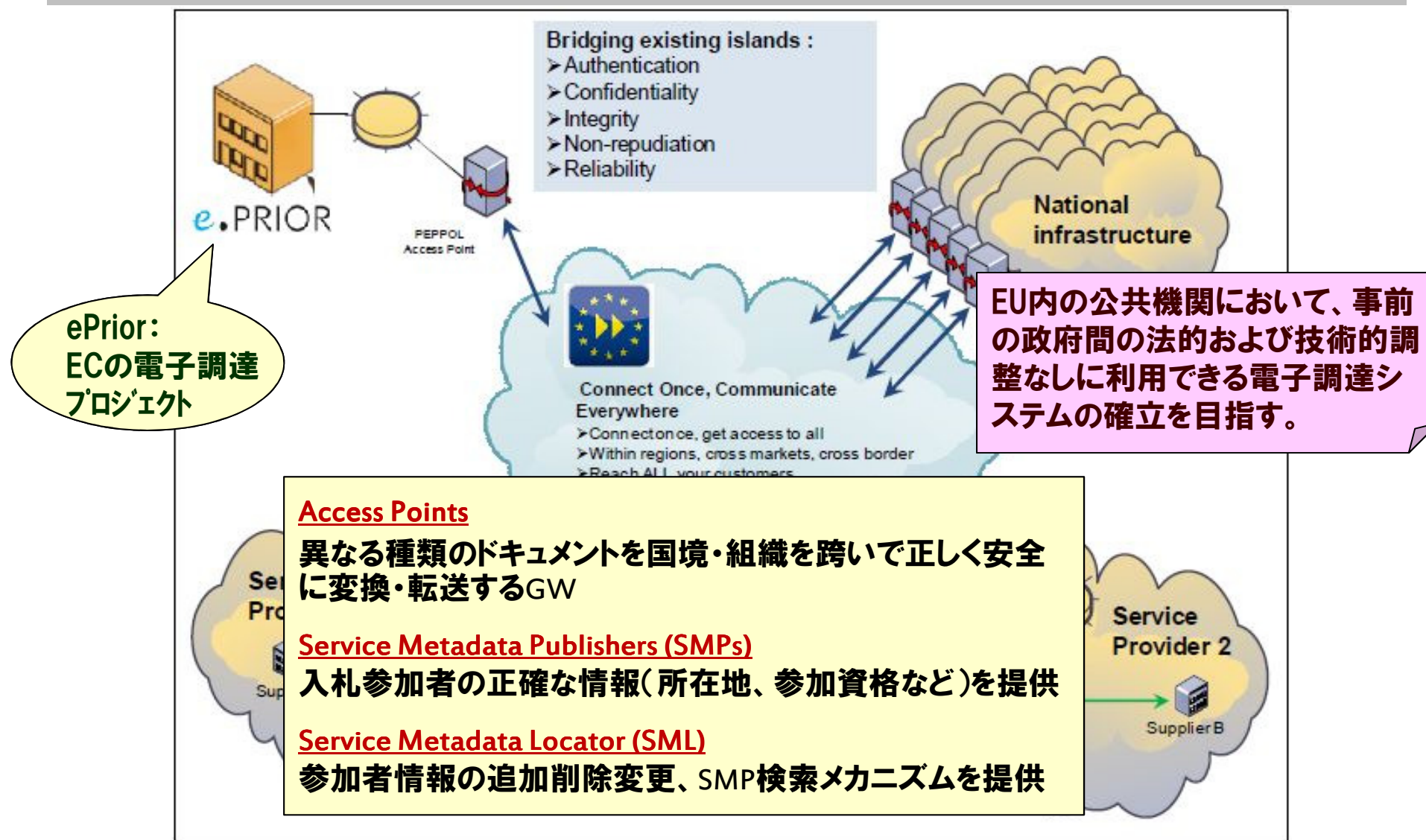
- EU内電子調達システム基盤の確立を目的として、ECとPEPPOLコンソーシアムが立ち上げたプロジェクト。2008年開始。
- EU内の政府間で実現可能な標準仕様を開発。2012年9月に非営利団体(OpenPEPPOL)へ移行。



BIS(Business Interoperability Specifications)

- ビジネスプロセスの標準化([common eProcurement processes](#))
 - 電文フォーマットの統一(注文書、請求書、カタログ)
[eCatalogue](#), [eOrders](#), [eInvoices](#) 等のドキュメントフォーマット
 - 信頼できるメッセージ転送手段([e-Delivery](#))
 - 電子署名の相互運用性確保
ドキュメントコンテナ仕様([Virtual Company Dossier](#))
- 実証実験で相互運用性を評価。官民の団体が参加

PEPPOL Procurement model



https://joinup.ec.europa.eu/svn/peppol/PEPPOL_EIA/1-ICT_Architecture/1-ICT-Transport_Infrastructure/12-ICT-Framework/ICT-Transport-ICT_FactSheet-100.pdf

SPOCS (Simple Procedures Online for Cross-border Services) **JNSA**

- **ビジネス国外展開時の登録・登記サービス。**
(審査、認可、管理手続き等)

ECが設立. 16カ国参加. 2009.5～2012.6



EUサービス指令(**Services Directive 2006/123/EC**):

- **他国での起業やサービス開始のための手続きオンライン化の
2009までの達成を各国に義務付け。**

“Points of Single Contact”(PSC): ワンストップポータル

- **構成要素(SPOCS building blocks)**

Syndication, eDocuments, eDelivery, eSafe, eServices

技術資料: <http://www.eu-spocs-starterkit.eu/index.php/documents#b611>

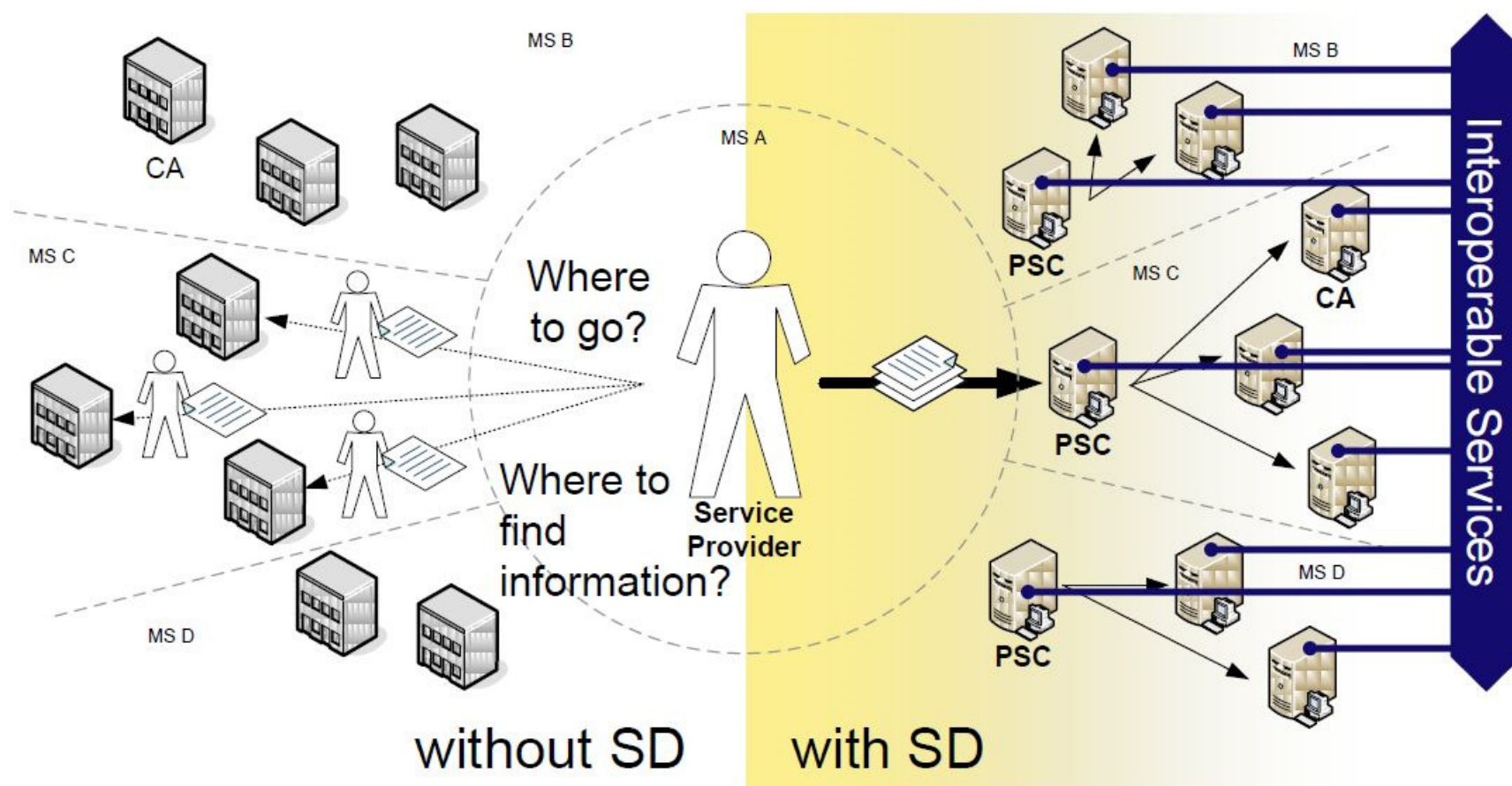
- **パイロットプロジェクト例**

旅行代理店、不動産、建築業者など

(Austria, Germany, Greece, Italy, Poland, Lithuania, Portugal, Slovenia の8カ国)

“Points of Single Contact”(PSC) **JNSA**

Today → **Services Directive** → SP  CS



www.cegd.eu/public/files/eeeGovDays_Kustor2.pdf

STORK(Secure idenTity acrOss boRders linKed)



- EU各国のeIDの相互運用基盤. EUが設立.
2008.6～2011.6. 現在も **STORK2.0**
として継続中. 19カ国参加.
- 主なプロジェクト

STORK

- eID相互認証サービス
- Safer Chat
- 留学(就学選択)
- eDelivery
- 住所変更
- ECAS(EC Authentication Service)

STORK2.0

- eLearning / 学位証明
- eBanking
- Business / eHealth 関連公共サービス





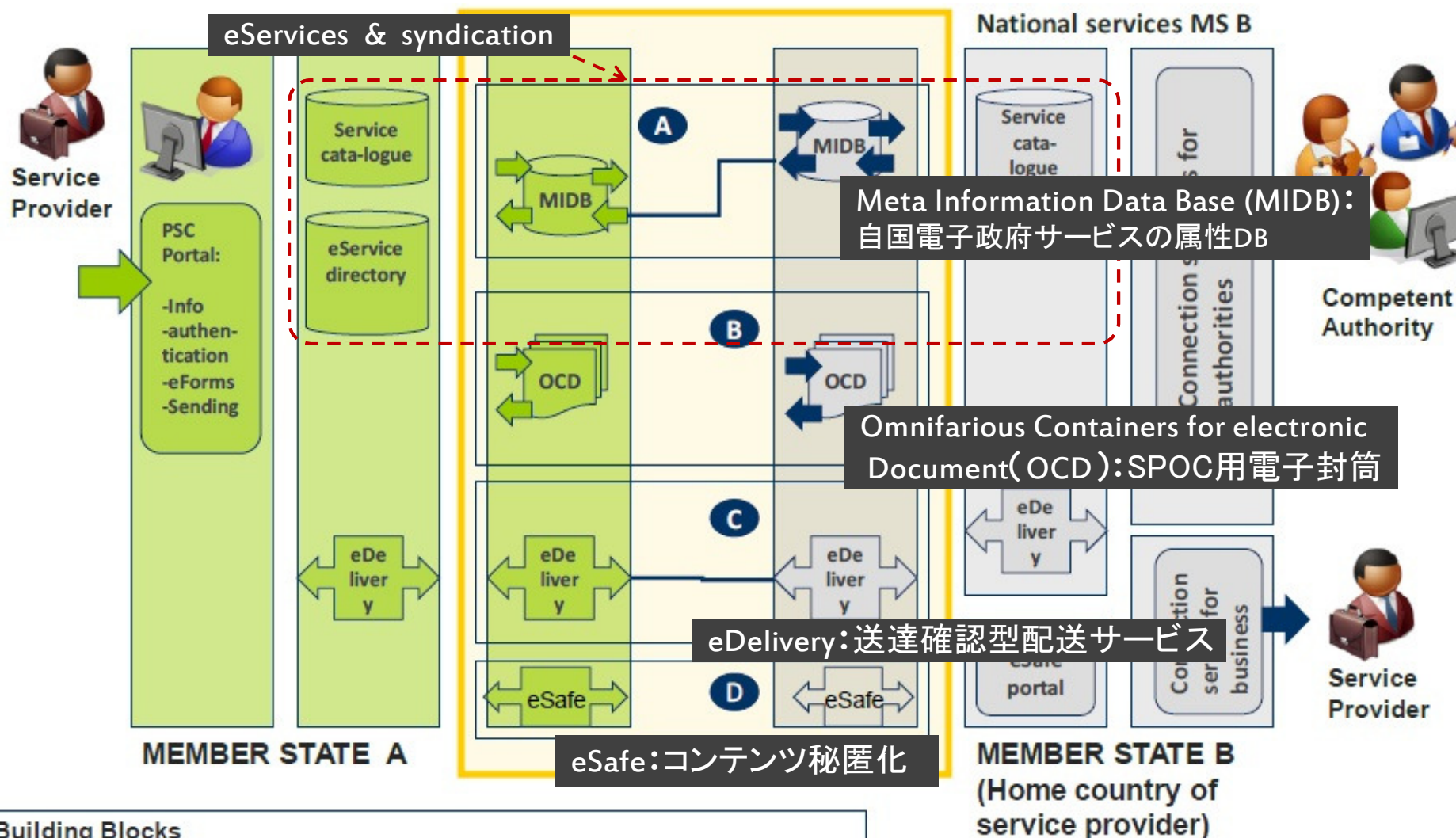
- **医療記録の相互運用基盤**
2008.1～2014.7(継続中)
25カ国が参加(44組織)
- **他国の医療機関からの自国の医療情報へのアクセスを可能とすることで、旅行中の医療機関受診に際しての医療ミスの防止と迅速な処置を実現.**
- **eDelivery技術の活用**
- **提供サービス**
 - Patient Summary: 患者の医療情報の安全な提供
 - ePrescription: 電子処方箋

- **法的情報の流通基盤**
2013.1～2013.12
25カ国が参加(44組織)



- **eDelivery技術の活用**
- **提供サービス**
 - 電子支払(European Payment Order)
 - 少額支払(Small Claims: 2000€未満の罰金支払)
 - 裁判記録情報の流通
 - 電子逮捕令状
 - 罰金請求の相互承認(他国での罰金刑支払い追跡管理)

SPOCS building blocks

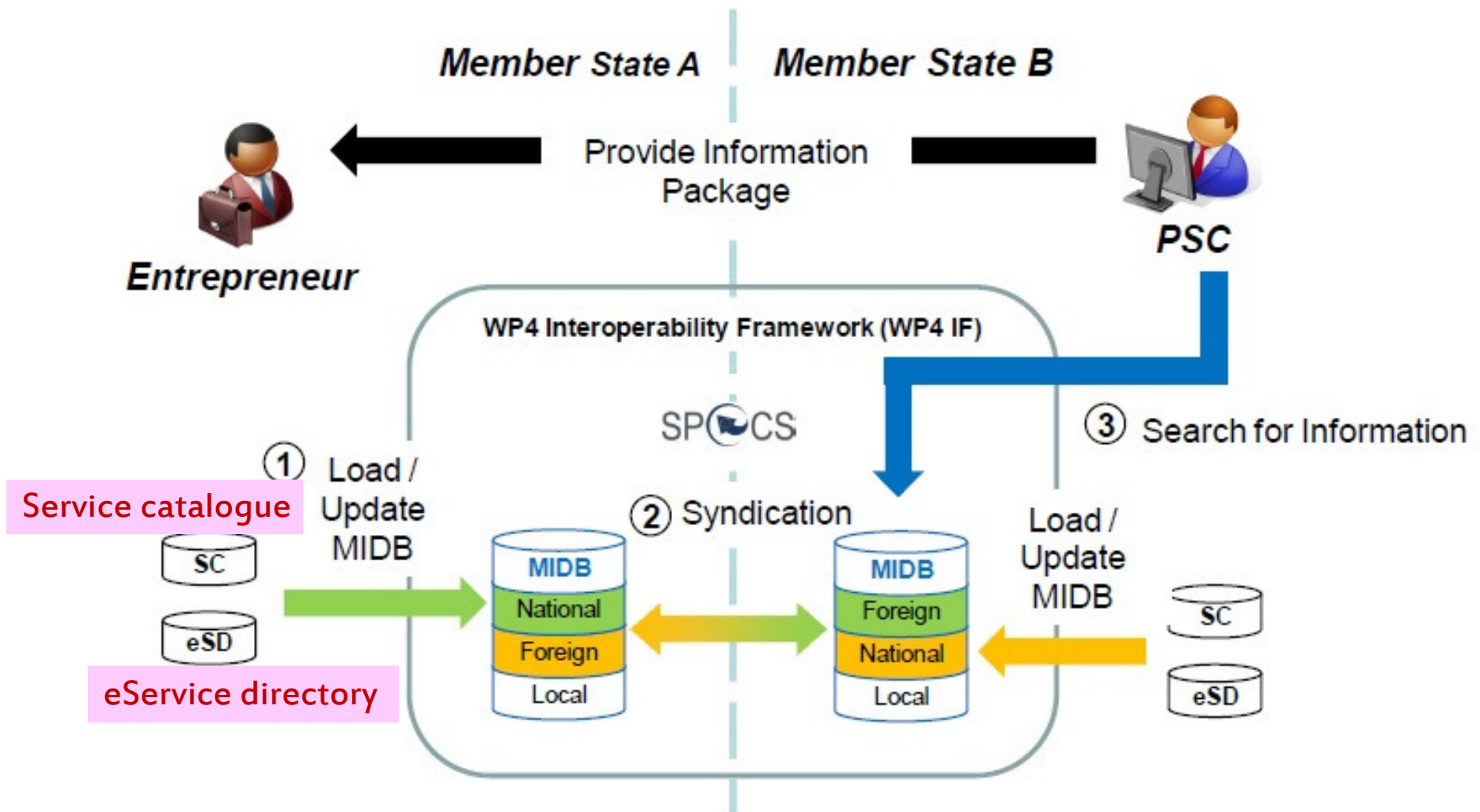


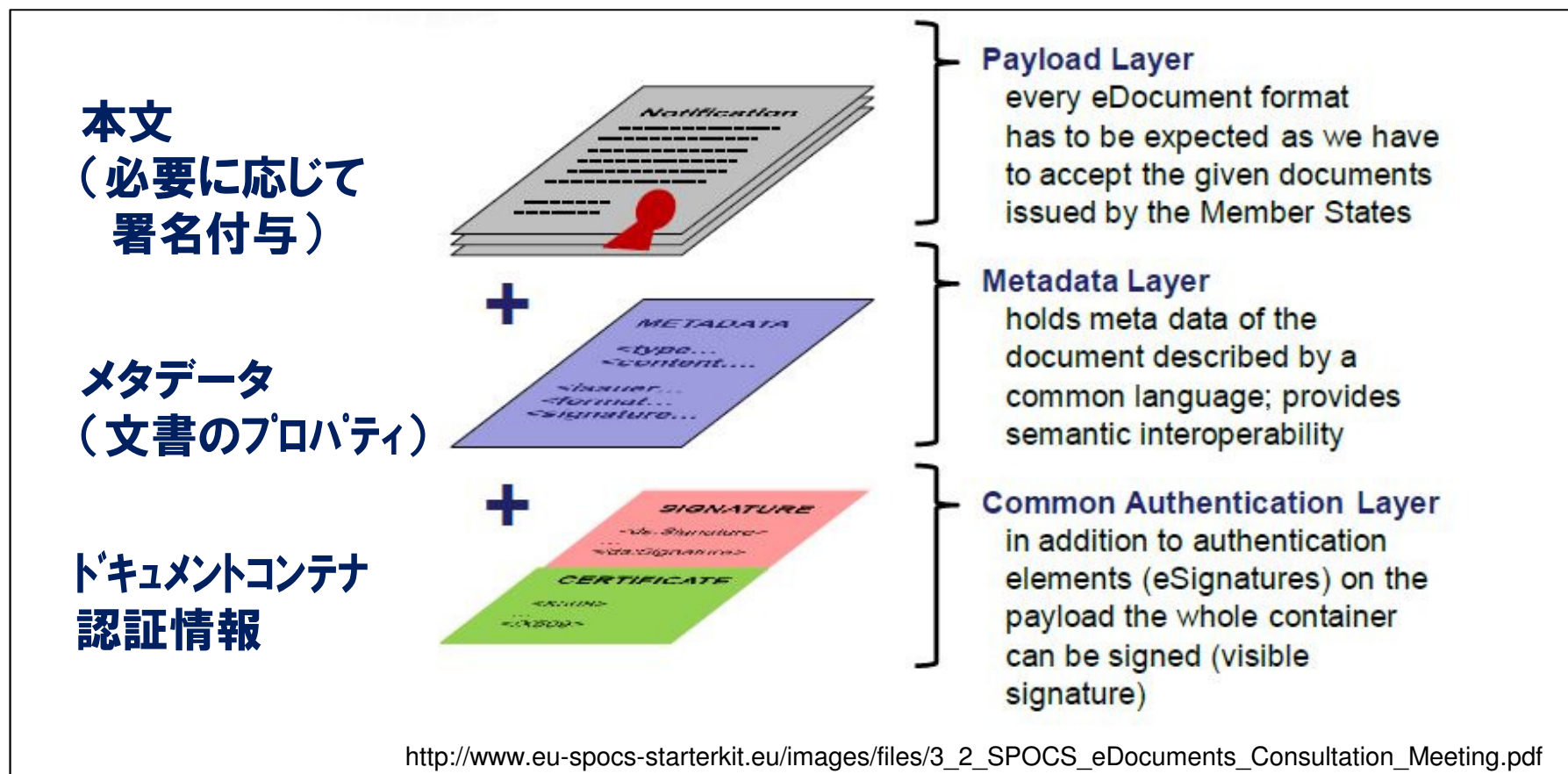
Building Blocks
A = eServices & Syndication
B = eDocuments

C = eDelivery
D = eSafe

http://www.eu-spocs-starterkit.eu/images/files/SPOCS_CM_June12_BB_v1_0_Final.pdf

eServices & syndication



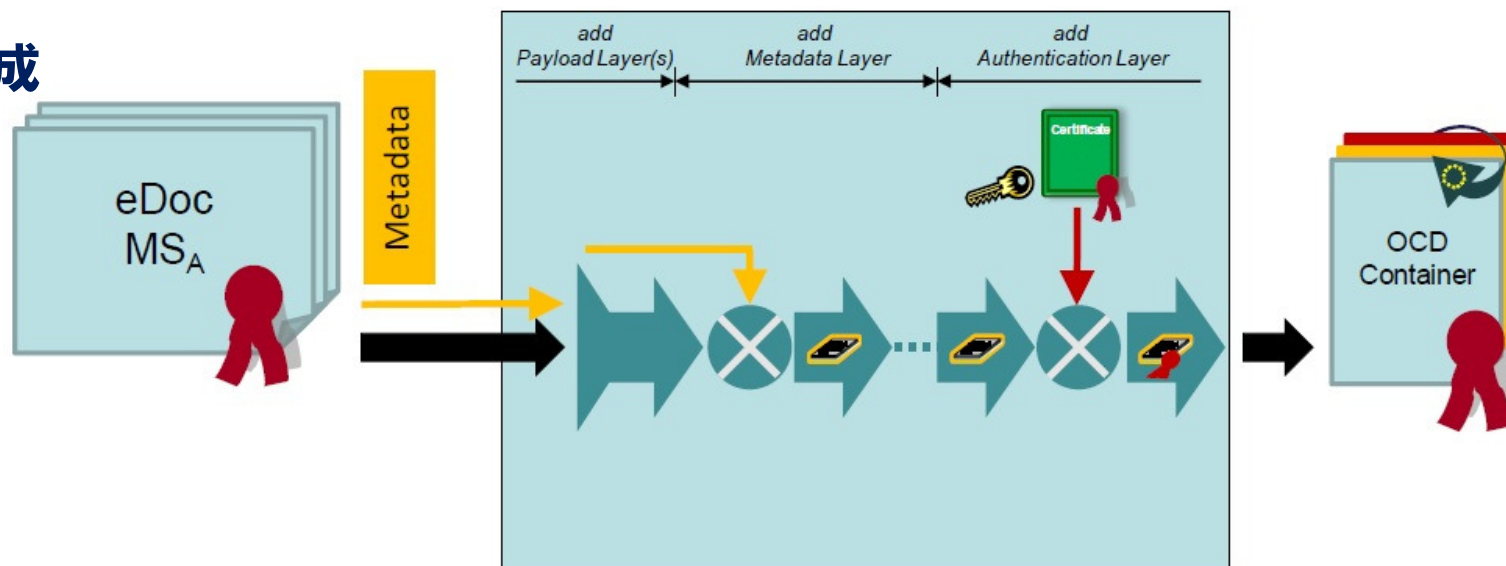


ZIP based ODC container :バックオフィス向け → **ASiC (TS 102 918)**
PDF based OCD container:国民向け → **規格化検討中**

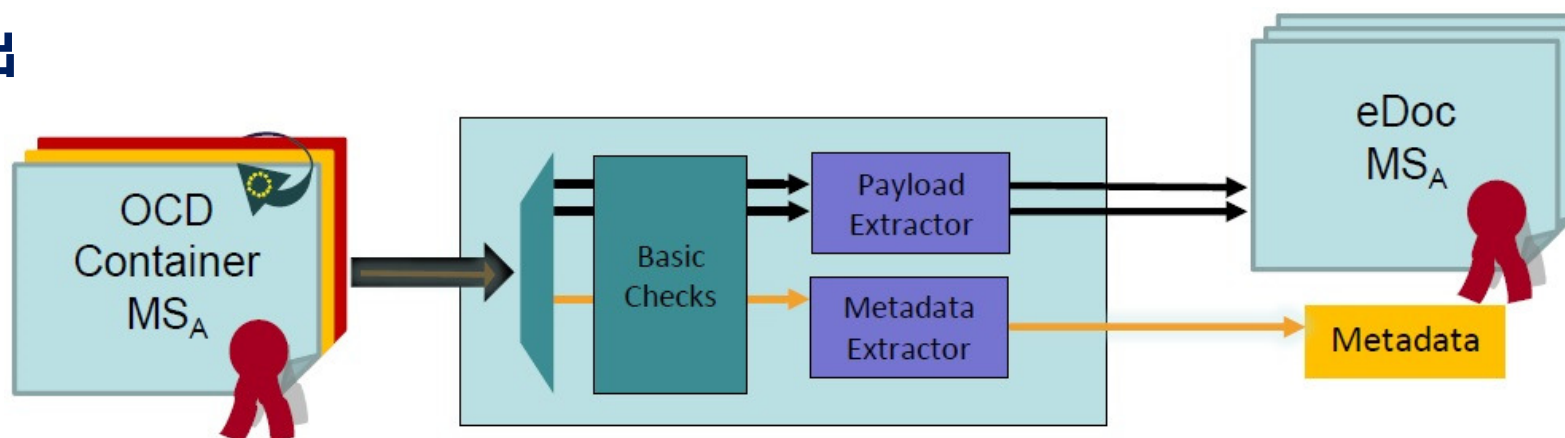
eDocuments 生成・抽出サービス



生成

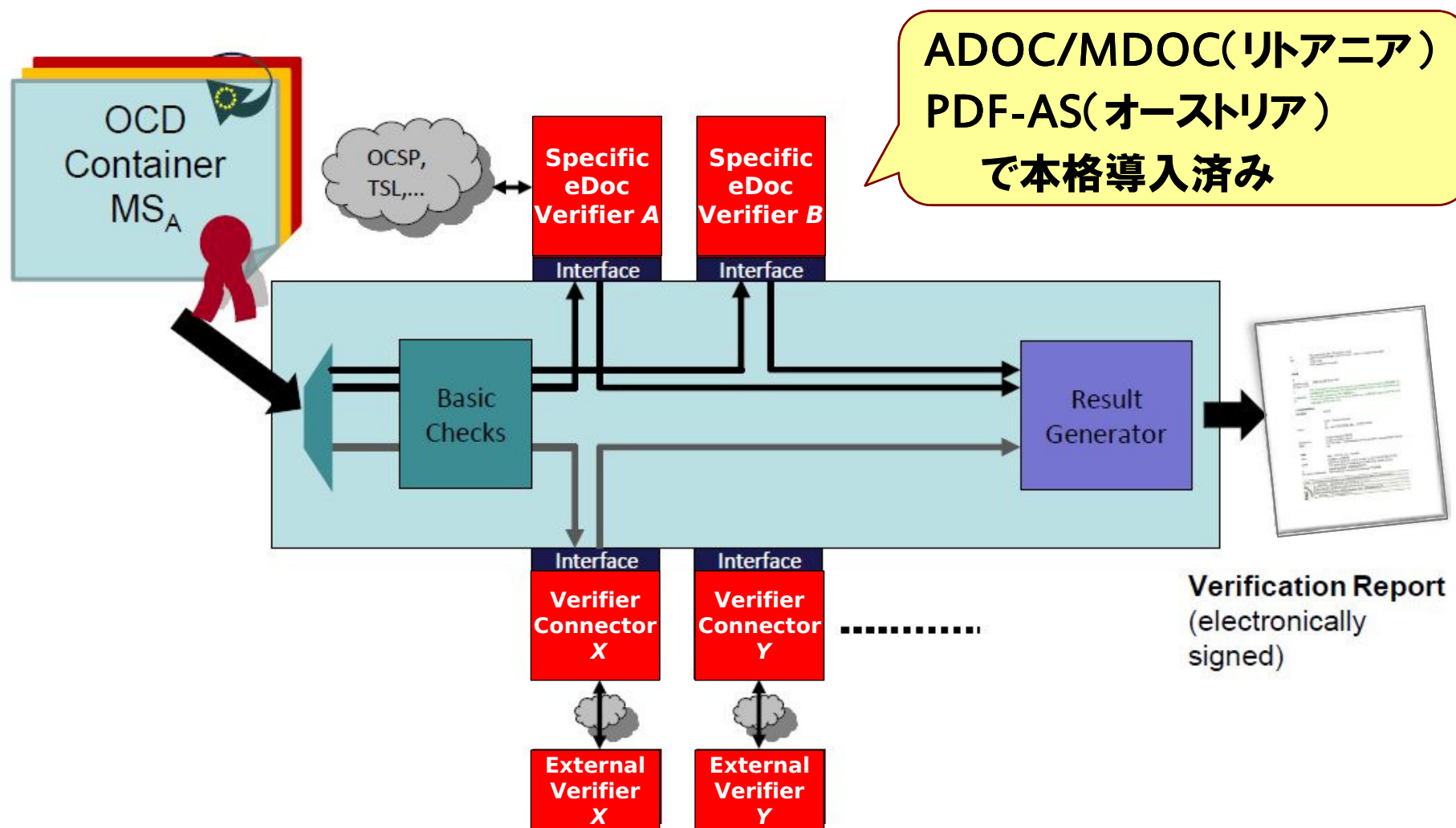


抽出



http://www.eu-spocs-starterkit.eu/images/files/3_2_SPOCS_eDocuments_Consultation_Meeting.pdf

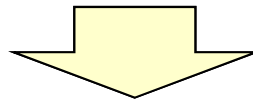
eDocuments 検証サービス



http://www.eu-spocs-starterkit.eu/images/files/3_2_SPOCS_eDocuments_Consultation_Meeting.pdf

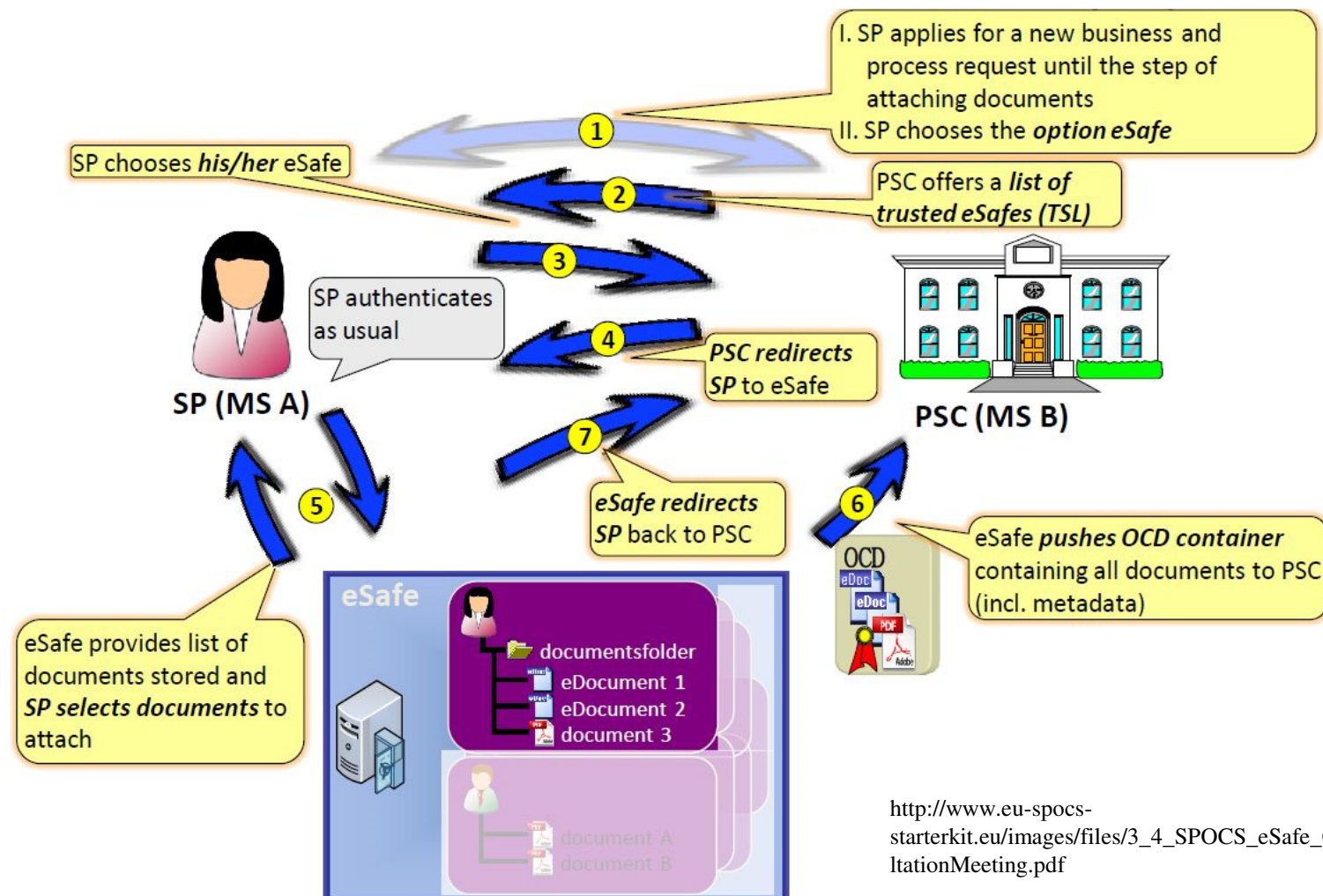
- 各国のeDeliveryシステムを活用した、セキュアなcross borderの証跡記録付き配送サービス。
- PEPPOLでは、相互接続部分の方式を規定

- SOAP(1.2) / WS-* profiling
- Standard body structures for mapping/carrying payload and related metadata
"normalized" Msg; to some extent XML structuring of RFC 5233 eMail format
- Cross border end entity authentication via SAML
Ready to use PEPS (STORK) issued token in the future
- Open to connect to PEPPOL's BusDox concept "Universal Identifier Scheme"
- Adoption of ETSI TS 102 640 (REM evidences)
Traceability/ receipting of delivery, provability of communication



ETSI TS 102 640-6-3 REM-MD SOAP Binding Profile (2011年6月)

・電子ドキュメントの安全な受信、送信、蓄積サービス (認証／署名、暗号化／eDocumentの生成、転送)



http://www.eu-spocs-starterkit.eu/images/files/3_4_SPOCS_eSafe_ConsultationMeeting.pdf

ご清聴ありがとうございました。

