



欧州の動向-電子署名指令から eIDAS規則へ

2015/4/10

株式会社コスモス・コーポレーション

ITセキュリティ部 濱口 総志



自己紹介

株式会社コスモス・コーポレーション

製品安全／EMC／医療機器評価・認証

TUViT GmbHの日本代理店

ETSI認証／データセンタ監査／コモンクライテリア評価／調査

一般財団法人 日本情報経済社会推進協会

客員研究員

東京工科大学 手塚 悟 研究室

COSMOS



eIDAS規則と電子署名指令

eIDAS規則:

Regulation (EU) No910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

2012年6月草案公開 → 2014年8月発効

電子署名指令:

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

COSMOS



eIDAS規則 –背景（序文より抜粋）

- (1) オンライン環境において信頼を構築することは、経済発展の鍵となる。信頼の欠如、特に法的確実性の欠如は、消費者や企業または行政が取引を電子取引上で行うことや、新たなサービスを導入することを躊躇させることになる。
- (2) 本規制は、市民、企業、行政間の安全な電子取引の共通基盤を提供することにより欧州域内市場の電子取引における信頼を強化し、それにより連合国におけるオンラインサービス、電子ビジネス、電子取引の効率を高めようとするものである。
- (3) 欧州議会及び理事会指令1999/93/ECは、安全で、信頼でき、かつ使いやすい電子取引の包括的な国境やセクターを超えた枠組みの提供以外の電子署名についてを対象としている。本規制はこの指令の利点を強化し、拡大するものである。

COSMOS



(4)「A Digital Agenda for Europe (欧州デジタルアジェンダ)」と題した2010年8月26日の欧州委員会コミュニケーションでは、デジタル市場の分裂、相互運用性の欠如、そしてサイバー犯罪の増加を、デジタル経済の良好な循環にとって大きな障害となるものとして認定した。

委員会はさらに、2010年の「Dismantling the obstacles to EU citizens' rights (EU市民に対する障害の排除)」と題したEU市民活動レポートにおいて、連合市民がデジタル単一市場や国境を越えたデジタルサービスの恩恵を受けることの妨げとなっている問題を解決することの必要性について強調した。



eIDAS規則 –背景（序文より抜粋）

- (5) 2011年2月4日及び2011年10月23日の結論文書では、欧州理事会は委員会に対し、安全な電子識別及び認証の促進に特別な注意を払いながら国境を越えたオンラインサービスの利用を促進することにより、2015年までにデジタル単一市場を創設し、デジタル経済の鍵となる分野を飛躍的に進歩させ、完全一体型のデジタル単一市場を促進するよう要請した。
- (6) 2011年5月27日の結論文書では、理事会は委員会に対し、電子識別、電子文書、電子署名、電子配達サービスなどの国境を越えた成功の鍵となるものの相互認証と、欧州連合における相互運用性のある電子政府サービスに対する適切な条件を策定することにより、デジタル単一市場に寄与するよう要請した。



電子署名指令

目的:

- 電子署名の利用の促進及び、法的効力の承認
- 電子署名及び認証事業者の法的枠組みの整備による、域内市場の活性化

<指令>

指令でかけられている内容の実現の為に、加盟国に指令に沿った国内法の整備を求めるもの

つまり、上記目的を実現する為に、加盟国が独自に国内法を制定する

COSMOS



- 監督システム
 - Supervision vs Notification
 - 監査規格？ ETSI TS 101 456?
- トラストリスト
 - フォーマット、xml?
- 適格電子署名
 - 自国の電子署名のみ受け入れ
 - 法人への適格証明書の発行

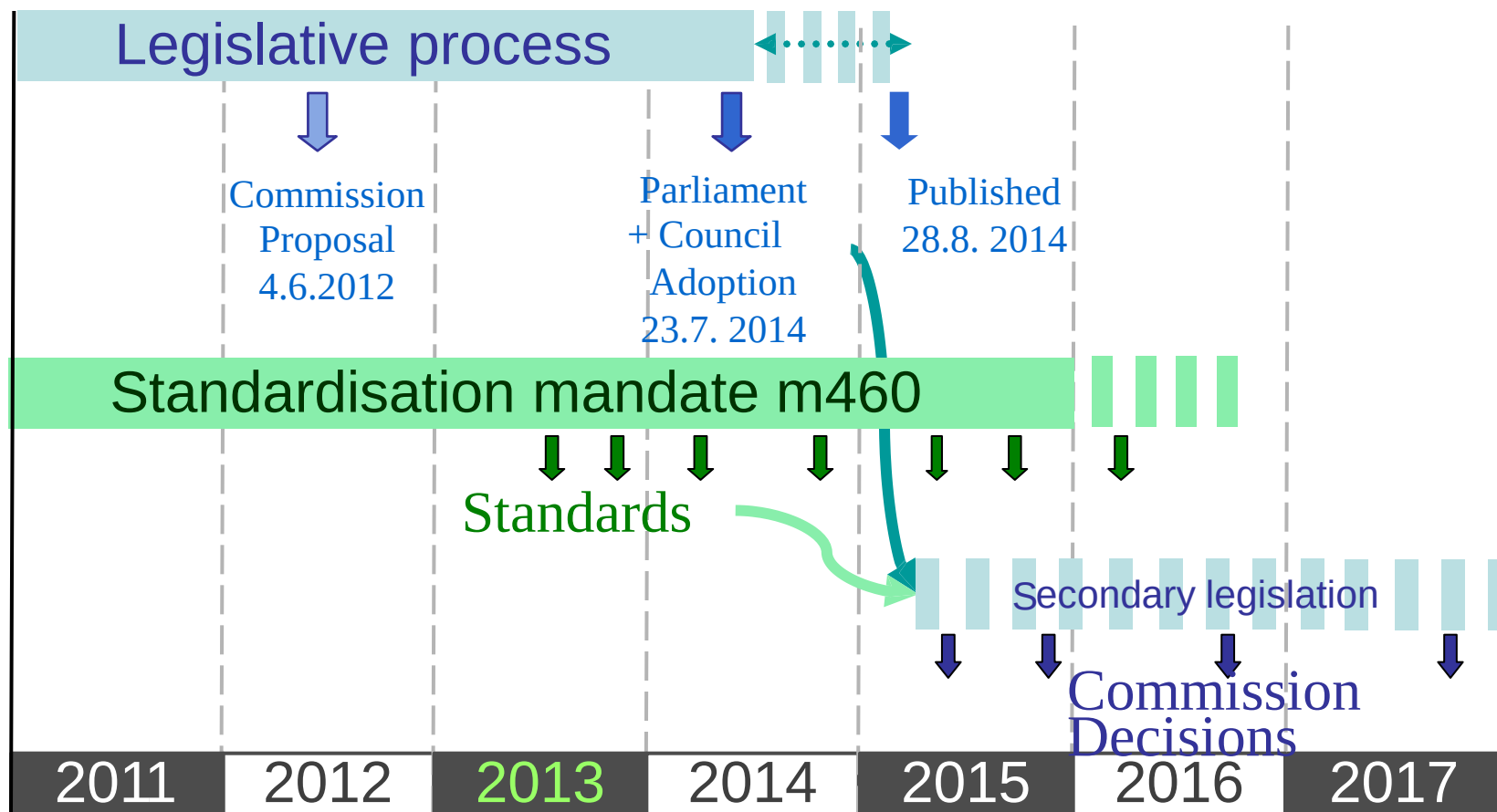


電子署名指令とeIDAS規則

	電子署名指令	eIDAS規則
目的	電子署名の利用促進と、法的承認への寄与 特定認証サービスに関する法的枠組みを構築することで、EU域内市場の適切な機能を確保	eIDとトラストサービスの適切なセキュリティレベルの実現による域内市場の適切な機能を保証 eIDの相互認証の為の条件を定め、また、トラストサービスの法的枠組みを確立する
範囲	電子署名	eID及びTS
効力	指令に基づいて加盟国が法整備	加盟国に直接適応



eIDAS タイムフレーム





電子署名とeID(電子認証)

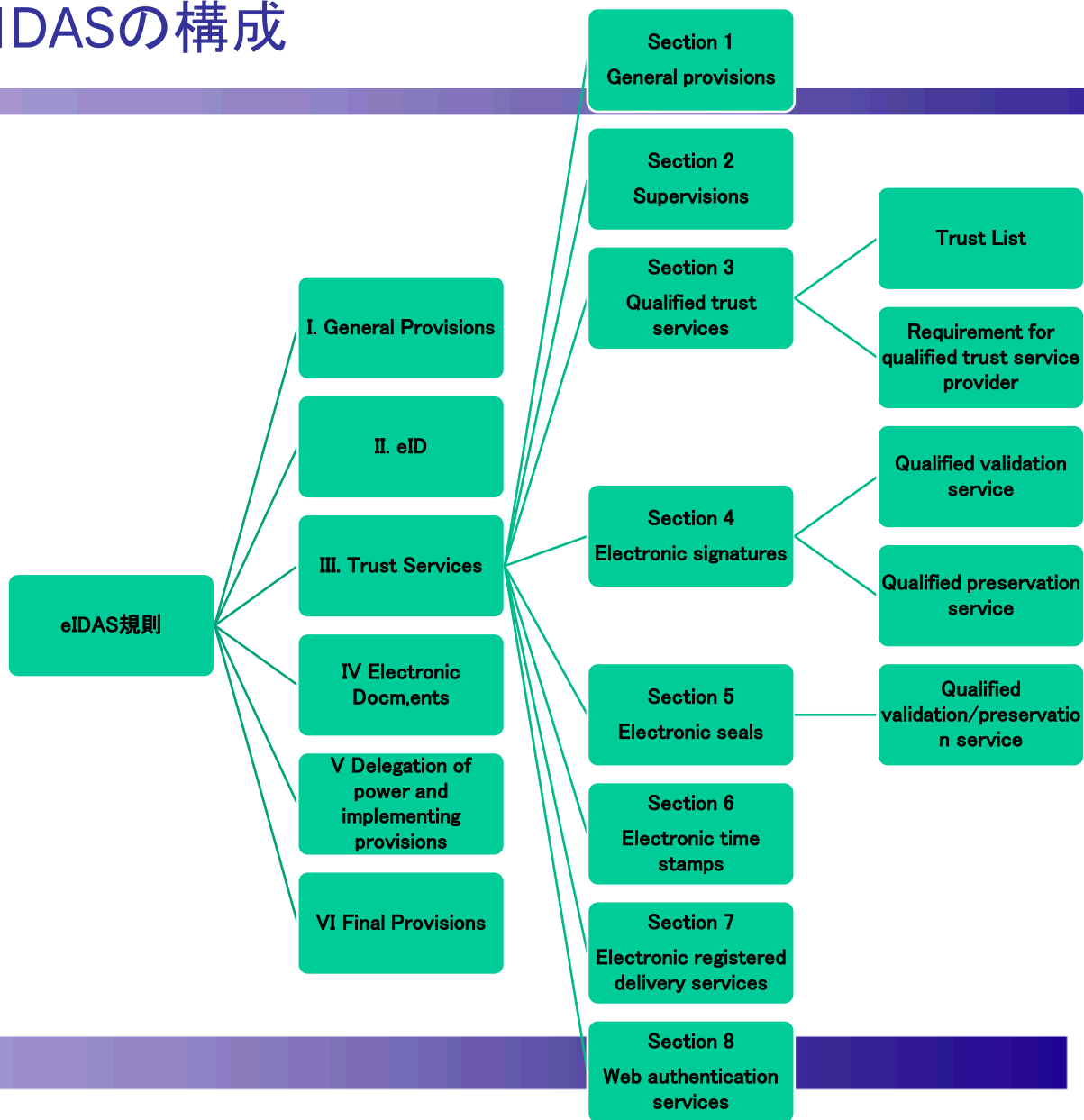
	電子署名	eID(認証)
用途	法的拘束力を伴う取引（契約書へ署名 等	ID認証, オンラインでの本人確認
比較対象	手書き署名と同等	旅券や免許証等による本人確認と同等
検証者	誰でも検証可能	限定された第三者が検証可能
検証可能期間	暗号強度によるが, 後からでも, 何度でも検証可能	認証時一度のみ

電子署名と認証は技術的に大きな差異はないが、制度として大きく異なり、紙の世界で署名が必要とされている部分で認証が署名に代ることはない。

COSMOS



eIDASの構成



COSMOS

eID＝オンラインで本人確認を実現できるID (e.g ドイツ新国民IDカード (Der Neue Personalausweis) のeID機能)

- 電子認証の保証レベル
 - Low
 - Substantial
 - High





eIDの相互承認の条件

1. 加盟国からEU委員会へ事前の通知によってEU委員会
が公開するeIDスキームのリストへの掲載
2. 電子認証を提供するeIDの保証レベルがSubstantial(十
分)あるいはHigh(高い)である
3. 公共サービスの要求する保証レベルがSubstantialある
いはHighである。
4. eIDの保証レベルが、公共サービスの要求する保証レベ
ルと同等あるいは、より高いレベルである。

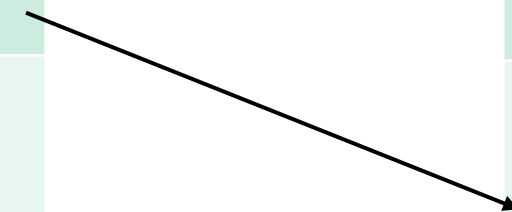


II. eIDの相互承認の条件（例）



スキーム	LoA
eID	High
公共サービスが求める 認証の保証 レベル	High

スキーム	LoA
eID	Substantial
公共サービスが求める 認証の保証 レベル	Substantial





＜法的有効性＞

適格証明書を使わない電子署名の法的有効性は否定されない。適格証明書を使った電子署名は手書き署名と同等とみなす。これはEU域内であれば、他国の署名であっても同等である。

＜公的セクターにおける扱い＞

公的セクターで、電子署名を要求する場合、適格電子署名を受け入れなければならない。また、適格電子署名より高いセキュリティレベルを要求してはならない。



定義:

「電子シール」とは、電子データに添付又は論理的に関係している電子形式のデータであり、元の電子データの起源と完全性を保証するものをいう

法的有効性:

適格電子シールは、電子シールがリンクするデータの完全性及びデータの起源の正確性を推定することが出来るものとする。

	電子シール	電子署名
定義	「電子シール」とは、電子データに添付又は論理的に関係している電子形式のデータであり、元の電子データの起源と完全性を保証するものをいう	「電子署名」と、電子データに添付されている又は論理的に関係している電子形式のデータであり、署名者が署名として使うものをいう *署名者=自然人(定義9参照)
証明書の定義	「電子シール証明書」とは、電子シール検証データと法人を関連付け、その法人名称を確認する電子証明書という	「電子署名証明書」とは、電子署名検証データと自然人を関連付け、少なくともその人物氏名、又は仮名を確認する



法的有効性について

eIDAS規則では、電子署名の法的有効性について、手書き署名と同等と規定している。

手書き署名の法的有効性や、実際（電子でない）のシールの法的有効性は、加盟国の国内法に依存する。

序文(49): 本規則は、電子署名が、電子形式であること、あるいは適格電子署名の要求を満たしていないことが理由で法的効果を拒否されるべきではないという原則を確立する。ただし、**適格電子署名が自筆署名と同等の法的効力をもたせるべきであるという本規則で規定される要求事項を除き、電子署名の法的効果を定義するのは国内法である。**

序文(59): 電子シールは電子文書が法人により発行されたことの証拠となり、文書の発行元と完全性を保証するものである。

COSMOS



電子シールの使用例

1. 請求書
2. 電子契約
3. 認証局 (CRL, subCA)
4. ソフトウェアコード



タイムスタンプ

<定義>

「電子タイムスタンプ」とは、電子形式のデータで、他の電子データを特定の時間と結びつける事により、元のデータがその時間に存在していた証拠を確立するものをいう;

<法的有効性>

タイムスタンプはその法的有効性を否定されない。適格タイムスタンプはその時刻の正確性と、データの完全性に関する推定を享有する。

ある加盟国で発行された適格電子タイムスタンプは、他の全て加盟国で適格電子タイムスタンプとして認められるものとする。

COSMOS



電子登録配送サービス (e Registered Delivery)

<定義>

「電子登録配布サービス」とは、電子手段により第三者間でデータを送信することを可能にし、データの送受信の証拠を含む送信されたデータの取扱に関する証拠を提供し、送信されたデータの損失、破損や窃盗、損害、又は不正な変更のリスクから守るものをいう;

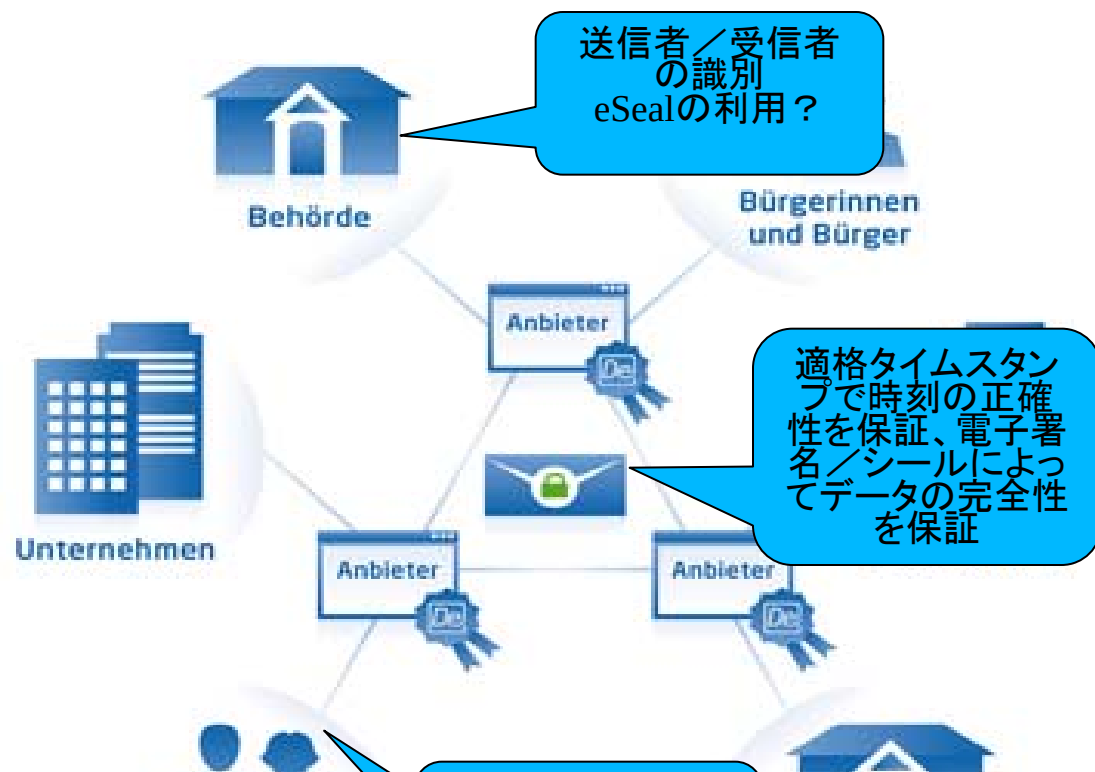
<法的有効性>

適格電子登録配布サービスを利用して送受信されたデータは、識別された送信者により送信、識別されたデータの宛先で受信されるデータの完全性と、適格電子登録配布サービスで示されたデータの送受信の日時の正確性を、法的に推定することが出来るものとする。

COSMOS



e.g. De-Mail



ドイツでは2011年5月にDe-Mail法（De-Mail Act）が発効され政府機関と市民や民間企業間のセキュアな電子通信の要求事項が定められた

現在、ドイツ連邦情セキュリティ庁（BSI）よりDe-Mailサービス事業者としての認定を受けサービスを提供している事業者は、1&1 De-Mail GmbH, Mentana Claimsoft GmbH, T-systems International GmbH及びTelecom Deutschland GmbHの4社である。

このようにオンラインで、実際の世界（紙での世界）と同等な仕組みを構築し、市民が安心して利用できるようにするためには、タイムスタンプや、電子シールの法的枠組みを整備する必要がある。



<定義>

「検証」と、電子署名又シールが有効であるかを照合及び確認するプロセスをいう。「検証データ」と、電子署名又電子シール検証に使用されるデータをいう

適格検証サービスプロバイダの先進電子署名又は、先進電子シールを利用した、自動的な検証プロセスの結果の受領を可能にするサービス



適格保存サービス

<定義>

適格電子署名の適格保存サービス は技術的有効期間 を超える適格電子署名の信頼性延長を可能にする手順及び技術を利用するQTSP みが提供することができる。

COSMOS



<定義>

「ウェブ認証証明書」とは、ウェブサイトを確認し、ウェブサイトと証明書が発行された自然人又は法人を結びつける証明書をいう

ウェブサイトをサポートする偽りでない合法的な実体があることを、ウェブサイト訪問者が確信できる手段を提供する。このようなサービスは、認証を受けたウェブサイトに対してユーザが信頼するようになることで、オンラインで取引を行ううえで信頼や信用構築に寄与する。

- 所謂SSLサーバ証明書を発行するサービス



監督機関と監査スキーム

■ 監督

- 加盟国は、その国内の監督機関を指定しなければならない。他の加盟国の監督機関を指定することも可能（要Agreement）
- 監督機関には、必要な権力と、適切なリソースが与えられる。
- 監督機関の役割は；
- TSP及びQTSPの監督
- 詳細はImplementing Actで規定する。

■ QTSPの監督

- 適合性調査機関から少なくとも2年毎に自費で監査を受けなければならない。
- 監督機関はいつでも自ら或いは、適合性調査機関を利用して、QTSPを監査できる。
- 監督機関がQTSPに不適合を改善するよう要求し、そのQTSPが改善を実行しない場合は、監督機関が指定する期間内で、不適合の具体的な程度、期間及び影響を考慮し、適格トラストサービスプロバイダ及び適格トラストサービスプロバイダが提供するサービスから適格の地位を取り消すことができる。

COSMOS



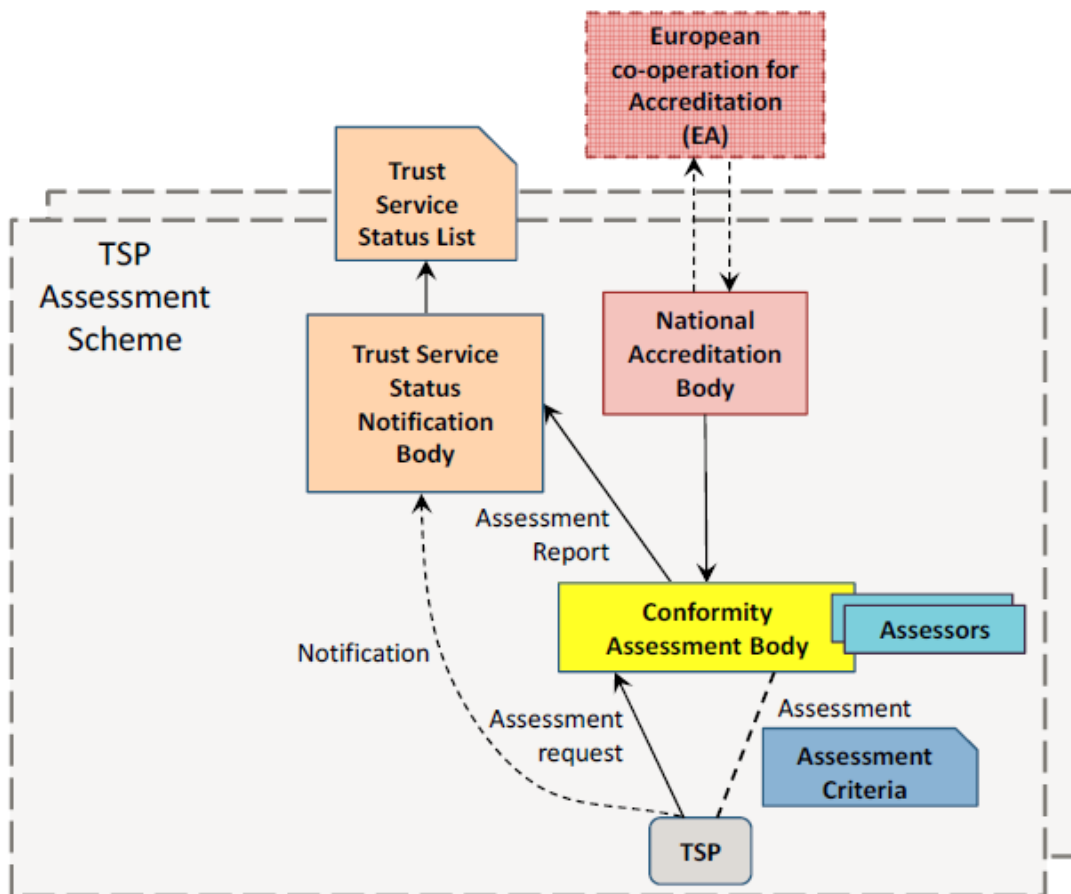
QTSPへの要求事項

- 適格証明書を発行する際、適格トラストサービスプロバイダは、適切な手段と国家法に基づき、適格証明書発行の対象となる自然人または法人の身元及び、該当する場合はその属性を証明するものとする
 - 登録プロセス
 - 物理的確認
 - eIDを使用する場合、保証レベルsubstantial or high
 - 適格電子署名、適格電子シール
 - 国家レベルで認められたその他認証方法（適合性調査機関による確認が必要）
 - 失効
 - 適時、但しいかなる場合も24時間以内
 - セキュリティ対策と専門性
- 必要な専門知識、信頼性、経験、資格を有し、セキュリティ及び個人情報保護法に関する適切なトレーニングを受けたスタッフ又は委託先を雇用し、欧州または国際的な基準に沿った運用及び管理手順を適用すること
詳細はImplementing Actで規定

COSMOS



監督機関と監査スキーム



出典: EN 319 403 TSP Conformity Assessment

COSMOS



トラストリスト

加盟各国は、電子署名あるいは電子シールされたトラストリスト(QTSP リスト)を自動処理可能な形で公開し、維持しなければならない

議会は、電子署名あるいは電子シールされた加盟国トラストリストリストを自動処理可能な形で公開し、維持しなければならない



TSL-XML.xml

COSMOS



EU トラストマーク



e-Mark U Trust Competition



The three finalists have now been selected.

Now it is your time to **vote**.

Help us select the **winner** of the e-Mark U Trust Competition.



Vote on
bit.ly/eMarkUtrust



Digital Agenda for
Europe

Ranking



B – EUSAFE – 432 votes



A – ELSE – 227 votes



C – Noblesse Oblige – 154 votes

COSMOS



■ International aspects

EU域外の国のトラストサービスについては、その国あるいは国際機関との合意の下でのみ、EU域内のトラストサービスと同等とみなす。

■ 罰則

加盟国は、本規則の違反者に適用される罰則についての規則(rule)を制定すること。課せられる罰則は、効果的で相応なものであり、抑止効果のあるものであること。



発効日と猶予期間

本規則は、以下を除き、2016年7月1日から適用される：

第 8(3)、9(5)、12(2)から(9)、17(8)、19(4)、20(4)、21(4)、22(5)、23(3)、24(5)、
27(4)(5)、28(6)、29(2)、30(3)(4)、31(3)、32(3)、33(2)、34(2)、37(4)(5)、
38(6)、42(2)、44(2)、45(2)、47及び48条は、2014年9月17日より適用される。

第7条、8条(1)、(2)、9条、10条、11条、12条(1)は、第8条(3)と12条(8)の実施法令
の適用の日より適用される。

第6条は、第8条(3)と12条(8)の実施法令の適用の日より3年後に適用される。

トラストサービス関連 → 2016年7月1日から
eIDの相互承認 → 実施法の3年後
その他 → すでに適用されている

COSMOS



Implementing ActとDelegated Act

規則ではその規則の下位法である実施法と委任法により、規則の詳細を定めることができる。

実施法とは、規則で規定されている内容に対して加盟国全体で統一された実施を実現するための下位法であり、例えば、規則で定められている要求事項の技術的適合性に関して、現存する技術規格への参照が行われる。

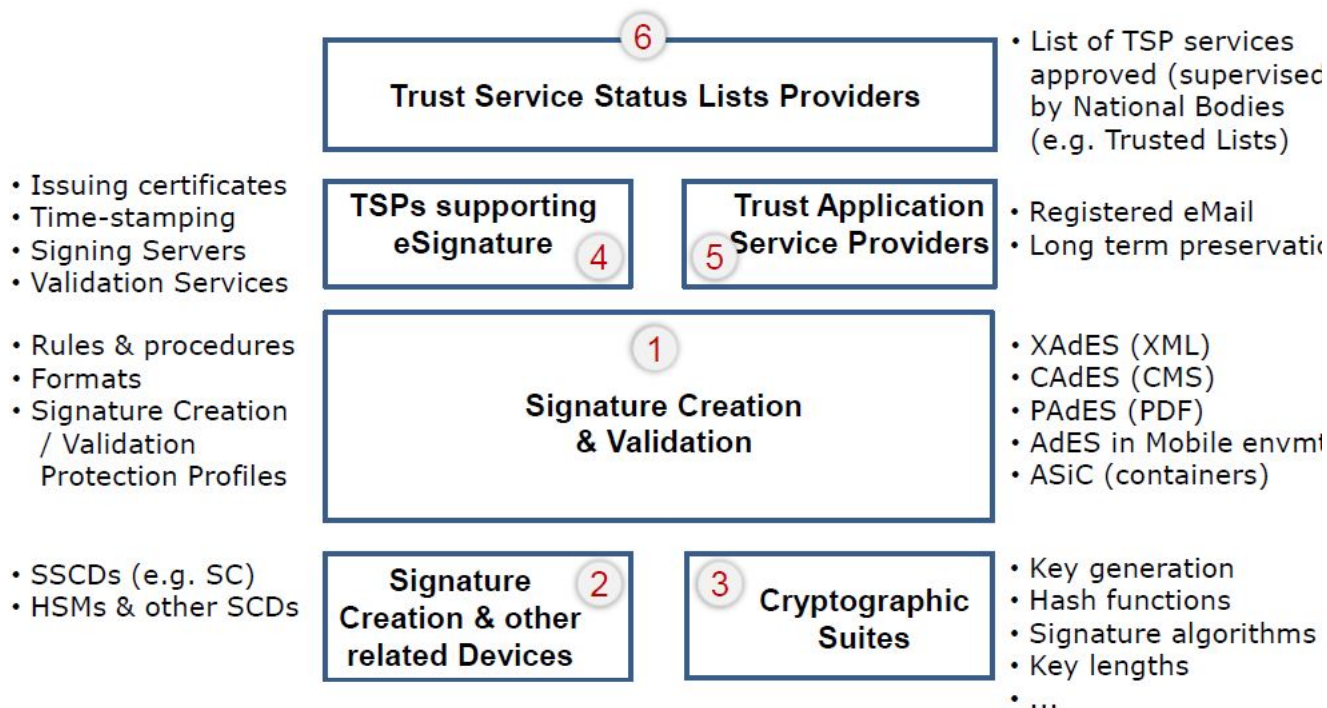
委任法とは、規則に対して重要でない部分について修正する為の下位法である。

COSMOS





Standardization mandate m460





ETSI TS → ETSI EN

ETSI TSから ETSI ENへの 移行

Technical Specification (TS)

TS 119 403

TS 101 456

TS 102 042

TS 102 023

European Norm (EN)

General Policy
Requirements

319 401

Requirements
for Conformity
Assessments

319 403
(ISO/IEC 17065)

General CA
Requirements

319 411-1

Qualified Certs

319 411-2

Pub. Key Certs

319 411-3

Time Stamps

319 421

eIDAS: HOW IT WILL BENEFIT YOUR BUSINESS ?



PAYING TAX



SIGNING CONTRACTS



TENDERS



INVOICING



A SWEDISH COMPANY WANTS TO PARTICIPATE IN
A PUBLIC CALL FOR TENDER IN CROATIA

BEFORE

Danger of **UNCERTIFIED WEBSITE**



WEBSITE
AUTHENTICATION

The Swedish SME **IS NOT
AUTHENTICATED** might be fake



E-ID
AUTHENTICATION

EXCHANGE OF PHYSICAL DOCUMENTS...



NOW



CREATION OF THE E-DOCUMENT



Confirmed time of submission
e-Acknowledgement of receipts

E-REGISTERED
DELIVERY



LESS DOCUMENT STORAGE



LESS TIME

1 - 2 WEEKS



HOURS - FEW DAYS

LOWER COST

€ 50 - 100



€ 10 - 20



Source: European Commission



ec.europa.eu/digital-agenda/en/trust-services-and-eid



European
Commission

出典 : <http://ec.europa.eu/digital-agenda/en/news/eidas-infographic>

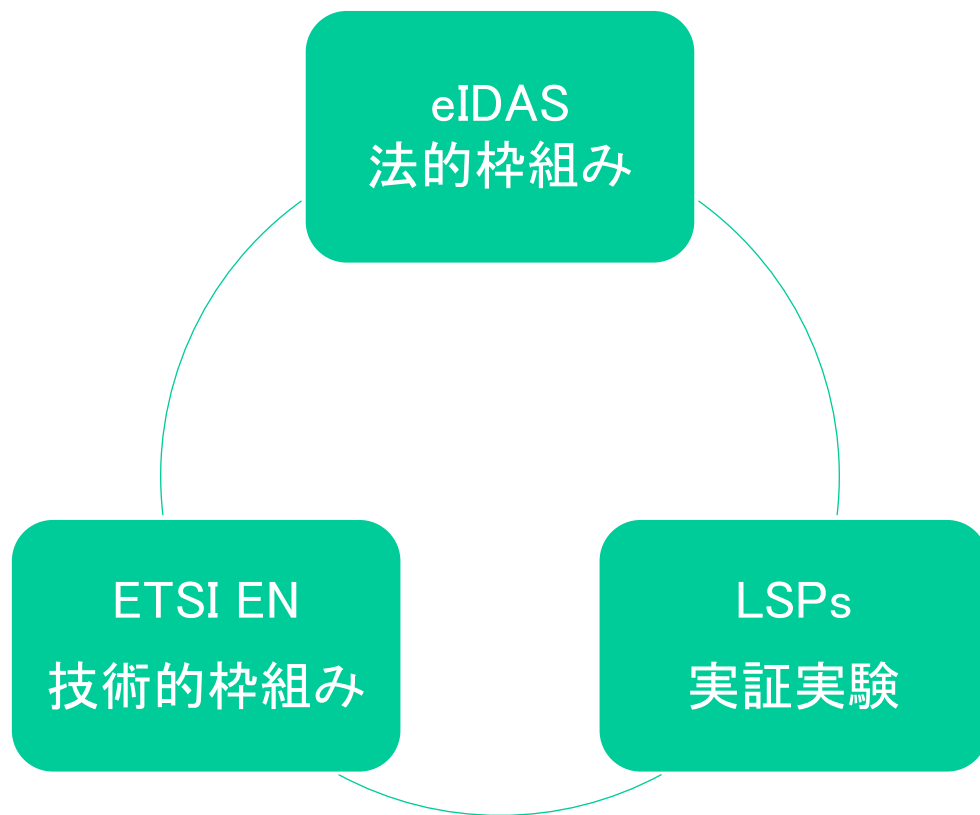
GOSMOS



- LSPs (Large Scale Pilot)
 - PEPPOL (€ 30.8M)
 - 電子調達相互運用性
 - STORK (€26M)
 - eID相互運用性
 - STORK 2.0 (€18.7M)
 - eID相互運用性
 - epsos (€23M)
 - 電子処方箋
- eIDAS token



欧州の取り組み





- 市民はeIDの国境を越えたセキュアな認証によって、外国の大学への出願から電子健康情報へアクセスといった、市民の権利を最大限利用することができる
- 外国へ移住する際の手続きをオンラインで
- 企業、外国へ案件に対して、オンラインで入札可能に・・・スピードとコスト面で多大なメリット
- ユーザ名＋パスワードからeID認証へ・・・セキュリティ向上
- 政府系サービスもより市民にとって使いやすいものに



- 欧州のサービス事業者は法適合のトラストサービスを提供できるようになり、国際競争力が上がる。
- 欧州では法適合のトラストサービスが要求され、欧州以外のトラストサービスが選択されにくくなる。
- 欧州技術仕様のデファクト化？



ご清聴ありがとうございました

ご質問等御座いましたら、

コスモス・コーポレーション

ITセキュリティ課

濱口 総志

s.hamaguchi@cosmos-corp.com

までご連絡ください。

* eIDASの全訳を3月中に公開予定です。

COSMOS