欧州委員会

数字| DG CNECT
欧州施設の接続

CEFeDeliveryビルディングブロック

バージョン 1.00

セキュリティ管理

eIDAS（Q）ERDSとCEFeDeliveryのリンク

特定の契約番号257フレームワーク契約番号D
I / 07171 –ロット2

ドキュメントのステータス：

状態
最後の

ドキュメント承認者：

名前	役割
Joao Rodrigues Frade	CEFeDeliveryプロジェクトおよびアーキテクチャオフィス

ドキュメントレビューア：

名前	役割
フィリペベアト	PwCEUサービス
Dusko Karaklajic	PwCEUサービス
エイドリアン・フェリアル	CEFeDeliveryテクニカルオフィスCEFeDeliveryテクニカルオフィスCEFeDeliveryテクニカルオフィ
イオアナ・ドラガサヌ	
マールテンダニエルズ	
マルコフェルナンデス-ゴンザレス	
スザンヌウィガード	数字（ISA）

変更の概要：

バージョン 日付		によって作成された	変更の簡単な説明
0.01	2016-05-04 PwC	EUサービス	トラストゾーンの定義最終レビ
1.00	2017-02-27欧州	委員会	ユー

目次

A 文書のアプローチと目的

このドキュメントは、読者がコネクティングヨーロッパファシリティ（CEF）のeDeliveryビルディングブロックとeIDAS規制に精通していることを前提としています。これらのトピックに精通していない読者は、以下を参照することをお勧めします。

- eDeliveryの紹介ドキュメント[1]は、その技術仕様、ソフトウェア、およびサービスについて学習します。
- 国内市場での電子取引のための電子識別および信頼サービスに関するeIDAS規則（規則（EU）N°910/2014）[2]。
- eIDASの特定の規定を実装する方法に関するENISA [3]による技術ガイドライン。

このドキュメントでは、動的検出なしで、つまりサービスメタデータパブリッシャー（SMP）とサービスメタデータロケーター（SML）なしでAS4メッセージングプロトコルを使用するeDeliveryのメッセージ交換ユースケースに適用可能なセキュリティ制御と推奨事項について説明します。このドキュメントでさらに詳しく説明するように、メッセージ交換のユースケースは、eIDAS規制に基づく信頼サービスであるElectronic Registered Delivery Service（ERDS）と密接に関連しています。

eIDAS規則[2]は次のように定義しています **E** レクトロニック **R** egistered **D** 配達 **S** ervice（ERDS）は、電子的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明を含む、送信されたデータの処理に関連する証拠を提供し、送信されたデータをリスクから保護するサービスとして紛失、盗難、損傷、または不正な変更。

eIDASに基づく他のすべてのトラストサービスと同様に、ERDSは、資格のないトラストサービスプロバイダー（TSP）または資格のあるTSP（QTSP）によって提供されます。TSPはERDSを提供しますが、QTSPはQualified ERDS（QERDS）を提供します。これは、資格のないTSPは、軽いタッチと事後の事後監督活動の対象となるだけであり、QTSPは、国の監督機関による事前および事後の要件/義務の両方の対象となるためです。これらのより厳しい要件の結果として、QTSPのみが国内の信頼できるリストの一部であり、EUの信頼マークを利用できます。規則の第43条に規定されているように、適格および非適格のERDSは、法的手続きの証拠として非差別条項の恩恵を受けますが、QERDSのみが「*データの整合性、特定された送信者によるそのデータの送信、特定された宛先によるその受信、およびQERDSによって示される送信と受信の日時の正確性*」。QERDS要件は、規則の第44条に指定されています。次の章では、eDeliveryがこれらのテクノロジーに中立な要件とどのように連携しているかを示します。このドキュメントは、TSPがeDeliveryが資格を取得するのにどのように役立つか（つまりQTSP）を理解するための良い出発点ですが、eDeliveryを単独で使用しても、資格のあるステータスが付与または保証されるわけではありません。この決定は国の監督機関によってのみ行うことができることを強調する価値があります。このドキュメントの主な内容には、次の情報が含まれています。

- メッセージ交換のセキュリティ制御の説明eDeliveryのユースケース、特にAS4プロファイルに埋め込まれた制御の説明[1] e-SENS大規模パイロット内で作成されました。
- QERDS要件のeDeliveryのセキュリティ管理へのマッピング。
- eDeliveryを使用する予定の企業および公的機関向けの一連の推奨事項
  QERDSを提供するQTPSPになるプロセスを潜在的に通過すること。

[1] http://wiki.ds.unipi.gr/display/ESENS/PR+-+AS4

このドキュメントは、ERDSまたは同様のサービスの提供にeDeliveryビルディングブロックを使用することを意図している、公的または私的を問わず、あらゆる組織を対象としています。次の図は、このドキュメントの目的、対象読者、および主な成果をまとめたものです。

目的

eIDAS規制からQERDS要件を抽出します。

eDeliveryのセキュリティ管理を理解し、それらをQERDS要件にマッピングします。

おそらくQTSPとしてeDeliveryを使用するときに実装するセキュリティ制御のリストを提案し、推奨します。

観客

政策担当者 eDeliveryメッセージングインフラストラクチャを必要とするEU全体または国内のポリシーの展開に関与します。

ITアーキテクト（主にセキュリティエキスパート）eDeliveryビルディングブロックのAS4プロファイルを実装するeDeliveryメッセージングインフラストラクチャの設計と運用に関与します。

サービスプロバイダー（TSPおよびQTSP） eDeliveryの実装と展開に関与します。

出力

A **QERDS要件のリスト** eIDAS規制から抽出（ **第2章** ）

A **セキュリティ管理の世論調査** QERDS要件への対応（ **第3章** ）

A **推奨事項のセット** eDeliveryビルディングブロックを使用するときに実装するセキュリティ制御の例（ **第4章** ）

図1。 このドキュメントの目的、対象者、および出力の要約

G 損失

これで使用される重要な用語 資料 表1に定義されています。eDeliveryビルディングブロックで使用される主要な頭字語は、CEF用語集 CEFデジタルシングルWebポータル：

表1。 セキュリティ管理と推奨事項の重要な用語

期間	説明
アクセス・ポイント	CEF eDeliveryのアクセスポイント（AP）は、e-SENSプロファイル[4]に従ってAS4メッセージ交換プロトコルを実装します。これにより、標準化された相互運用可能で安全で信頼性の高いデータ交換が保証されます。詳細については、CEFデジタルポータル[5]を参照してください。
AS4	eDeliveryのAS4プロファイルは、OASISのAS4仕様に基づいてe-SENSによって定義されたAS4使用プロファイル/実装ガイドラインであり、それ自体がOASIS ebXMLメッセージングサービスバージョン3.0のプロファイルであり、OASISのさまざまなWebサービス仕様に基づいています。
バックエンドシステム	eDeliveryのコンテキストでは、バックエンドシステムは、eDeliveryを介して交換されるドキュメントとデータの発信元である、企業および行政によって使用されるITシステムを表します。そのためには、バックエンドシステムを直接またはコネクタコンポーネントを介してeDeliveryアクセスポイントに接続する必要があります。
ビジネスドメインの所有者	このコンテキストでは、eDeliveryを使用するプロジェクトの所有者を表します。これらは通常、特定のポリシードメイン内の1つ以上のアクセスポイント（AP）の恩恵を受ける企業および行政機関です。彼らは通常、eDeliveryを使用して、ドメイン内でデータやドキュメントを交換するための安全なメッセージングインフラストラクチャを作成します。
CEFeDelivery	eDeliveryビルディングブロックは、相互運用性、安全性、信頼性、信頼性の高い方法で、行政が他の行政、企業、市民と（通常はWebポータルを介して）電子データやドキュメントを交換するのに役立ちます。
コネクタ	eDeliveryのコネクタコンポーネントは、バックエンドシステムによって実装されたシステムとアクセスポイント間の相互運用性と統合を容易にするオプションのコンポーネントです。
電子シール	eIDAS規則によれば、「電子シールとは、電子形式のデータを意味し、電子形式の他のデータに添付または論理的に関連付けられて、後者の起源と完全性を保証します」。電子シールは、電子文書が法人によって発行された証拠として機能し、文書の出所と完全性の確実性を保証する必要があります。高度な電子シールとは、第36条の要件を満たす電子シールを意味します。資格のあるステータスの場合、電子シールは、資格のある電子シール作成デバイスによって作成され、電子シールの資格のある証明書に基づく高度な電子シールである必要があります。
電子署名	eIDAS規則によれば、「電子署名とは、電子形式の他のデータに添付または論理的に関連付けられ、署名者が署名するために使用する電子形式のデータを意味します」。証明書に依存する場合、後者は自然人に発行されます。高度電子署名とは、記事の要件を満たす電子署名を意味します 26.資格のあるステータスの場合、電子署名は、資格のある電子署名作成デバイスによって作成され、電子署名の資格のある証明書に基づく高度な電子署名である必要があります。eIDAS規則の第3条（36）によると、ERDSは、電子的手段によって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明を含む、送信されたデータの処理に関する証拠を提供するサービスです。送信されたデータを紛失、盗難、損傷、または不正な変更のリスクから保護します。eIDAS規則の第3条（33）によると、「電子タイムスタンプ」とは、電子形式の他のデータを特定の時間にバインドする電子形式のデータを意味し、後者のデータがその時点で存在したという証拠を確立します。
電子登録配達サービス（ERDS）	
電子タイムスタンプ	

	第42条に定められた要件を満たすスタンプ。
e-SENS	電子SimpleEuropean Networked Services（e-SENS）は、EU全体の行政間のデジタル相互作用を促進するために、共通の構成要素に基づいた技術ソリューションを統合、改善、および拡張することを目的とした大規模なパイロットプロジェクトです。
FTP	ファイル転送プロトコル（FTP）は、コンピューターネットワークを使用して異なるエンドシステム間でファイルを転送するために使用される標準のネットワークプロトコルです。
JMS	Java Messaging Serviceは、Java EEアプリケーションコンポーネントがメッセージを作成、送信、受信、および読み取ることを可能にするメッセージング標準です。
メッセージの暗号化	メッセージの暗号化は、機密保持を目的として、プレーンテキストメッセージを暗号文に変換するプロセスです。メッセージの暗号化は、暗号化と復号化に同じキーが使用される対称キーアルゴリズム、または暗号化と復号化に異なるキーが使用される非対称キーアルゴリズム（秘密キーと公開キーのペアが使用される）を使用して計算できます[6]。 。
メッセージング層のセキュリティ	メッセージングレイヤーセキュリティは、AS4メッセージ交換プロトコルを使用して転送されるメッセージ（ドキュメント、電子メール、ファイルなど）のセキュリティを考慮します。
組織	このドキュメントのコンテキストでは、組織とは、特定のポリシードメイン内の1つ以上のアクセスポイントを運用または利用する企業および行政を指します。組織は、資格のないまたは資格のある電子登録配信サービスを提供または恩恵を受ける場合があります。
PMode	PMode（処理モード）は、サービス品質、送信モード、およびエラー処理に関して、AS4メッセージ（ユーザーメッセージや信号メッセージなど）がアクセスポイントのペア間でどのように交換されるかを決定するパラメータのコレクションです。
ポリシードメイン	ポリシードメインは通常、eJusticeドメインやeHealthドメインなどのドメインのビジネスオーナーであるDGJusticeやDGSANTEなど、欧州委員会の総局にリンクされています。ポリシードメインはeDeliveryを使用して、データとドキュメントを交換するための安全なメッセージングインフラストラクチャを作成します。
行政	eIDAS規則によれば、行政とは、州、地域または地方自治体、公法に準拠する機関、または1つまたは複数のそのような機関によって形成される協会、または公法に準拠する1つまたは複数の機関、またはそのような任務の下で行動するとき、公共サービスを提供するそれらの当局、団体または協会の少なくとも1つ。eIDAS規則によれば、第3条（37）「適格電子登録配達サービス」とは、第44条に定められた要件（「適格電子登録配達サービスの要件」）を
認定された電子登録配送サービス（QERDS）	満たす電子登録配達サービスを意味します。
認定信託サービスプロバイダー（QTSP）	eIDAS規則によれば、第3条（20）「適格信託サービスプロバイダー」とは、第3条（20）に定められた要件に従って、1つ以上の適格信託サービスを提供し、監督機関から適格ステータスを付与される信託サービスプロバイダーを意味します。 24（「資格のある信託サービスプロバイダーの要件。
セキュリティ管理	ISO 27001 [7]によると、統制とは、情報セキュリティリスクを変更または管理するための保護手段および対策として使用される管理、管理、技術、または法的方法です。このドキュメントでは、セキュリティ管理策は、機密性と整合性を確保し、その結果、eIDAS規制から抽出されたセキュリティ要件に対処するために導入される技術メカニズムを表しています。
セキュリティドメイン	セキュリティドメインは、eDeliveryfourcornerモデルのさまざまな通信領域の責任エンティティによって実装および管理される一連のセキュリティ制御です。
サービスプロバイダー	サービスプロバイダーとは、eDeliveryを統合および実装するサービスを提供する自然人または法人を意味します。
トランスポート層のセキュリティ	トランスポート層セキュリティは、エンドシステムまたはホスト間でデータを透過的に転送するプロトコルのセキュリティを定義し、ホストからホストへの通信への完全なデータ転送を保証します。
信頼	信頼とは、ある組織が2番目のエンティティに依存して、一連のアクションを実行したり、一連のサブジェクトやスコープについて一連のアサーションを作成したりすることをいとわないという特徴です）[6]。
信託サービス	eIDAS規則によれば、「信託サービス」とは、報酬のために通常提供される電子サービスを意味し、以下で構成されます。

	a。 電子署名、電子シールまたは電子タイムスタンプ、電子登録配信サービスおよびそれらのサービスに関連する証明書の作成、検証、および妥当性確認、または b。 Webサイト認証用の証明書の作成、検証、および妥当性確認。または c。 これらのサービスに関連する電子署名、シール、または証明書の保存
トラストサービスプロバイダー（TSP）	eIDAS規則の第3条（19）によると、TSPとは、適格または非適格のTSPとして1つ以上の信頼サービスを提供する自然人または法人を意味します。

C 文書で使用されている発明

これで使用される適格および非適格ステータスに関する規則 資料 表2に定義されています。

表2。 使用される規則の説明

コンベンション	説明
ERDS	ERDSが認定されていない場合に使用されます。
QERDS	ERDSが適格なステータスを保持している場合に使用されます。
（Q）ERDS	ERDSが認定されているかどうかに関係なく使用されます。
TSP	TSPが修飾されていない場合に使用されます。
QTSP	TSPが認定ステータスを保持している場合に使用されます。
（Q）TSP	TSPが認定されているかどうかに関係なく使用されます。

R 参照

[1]「ConnectingEuropeファシリティ、eDeliveryビルディングブロックの概要」[オンライン]。利用可能：
https://ec.europa.eu/cefdigital/wiki/x/5gBfAQ。

[2]「eIDAS規制」[オンライン]。利用可能：http：//eur-lex.europa.eu/legal-
content / EN / TXT / PDF / ? uri = CELEX：32014R0910＆rid = 2。

[3] ENISA、「eIDASを実装するためのガイドライン」[オンライン]。利用可能：https：//www.enisa.europa.eu/topics/trust-
サービス/ガイドライン/。

[4]「e-SENSAS4プロファイル」、[オンライン]。利用可能：https：//ec.europa.eu/cefdigital/wiki/x/AwFfAQ。

[5]「CEFeDeliveryアクセスポイント」[オンライン]。利用可能：https：//ec.europa.eu/cefdigital/wiki/display/
CEFDIGITAL / Access + Point + software

[6]「OASISトラスト」[オンライン]。利用可能：http：//docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html。

[7]「ISO / IEC27001」、[オンライン]。利用可能：http：//www.iso27001security.com/html/27001.html。

[8]「CEFデジタルポータル-eDelivery」[オンライン]。利用可能：https：//ec.europa.eu/cefdigital/wiki/x/nwBfAQ。

[9]「ENISAアルゴリズムとキーサイズ」[オンライン]。利用可能：
https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report。

[10]「BSI技術ガイドライン」[オンライン]。利用可能：
https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TechnicalGuidelines_node.html。

[11]「TLSプロトコル」[オンライン]。利用可能：https：//tools.ietf.org/html/rfc5246。

[12] ENISA、「電子IDおよびトラストサービスプロバイダーの分野における標準化」[オンライン]。
利用可能：https：//www.enisa.europa.eu/publications/standards-eidas。

[13]「CEFeDeliveryPKIサービス」[オンライン]。利用可能：https：//ec.europa.eu/cefdigital/wiki/display/
CEFDIGITAL / PKI +サービス

[14] ETSI、「電子署名およびインフラストラクチャ（ESI）; 署名の標準化のためのフレームワーク：
概要」[オンライン]。利用可能：
http://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.01.01_60/tr_119000v010101p.pdf。

1.1。 私 はじめに

コネクティングヨーロッパファシリティ（CEF）のeDeliveryビルディングブロックにより、企業と行政（以下「組織」と呼びます）は、相互運用性、安全性、信頼性、信頼性の高い方法で電子データとドキュメントをデジタル形式で交換できます[8]、他の組織と（そして間接的に市民と）。eDeliveryビルディングブロックは、e-SENSプロファイル/実装ガイドラインで定義されたガイドラインに従ってAS4メッセージングプロトコルを実装するアクセスポイントの使用を規定しています。アクセスポイントは、（Q）TSPによって運用およびサービスとして提供され、異種システムがインターネット上で安全な方法で相互に対話できるようにします。このドキュメントでは、AS4アクセスポイントを介してシステムを相互接続し、第3条（36）のElectronic Registered Delivery Services（以下「ERDS」と呼びます）の定義に従ってデータを送信するときに、組織が実施するセキュリティ管理策のリストを推奨しています。 eIDAS規則の（EU）N°910/2014。このドキュメントで推奨されているセキュリティ管理策は、eIDAS規則の第44条の要件に従って、適格ERDS（以下「QERDS」と呼びます）の提供を容易にします。これらの技術的に中立な要件への準拠により、ドキュメントとデータが国境を越えてデジタル形式で交換される場合の一般的な法的効果が可能になります[2]。推奨されるセキュリティ管理策は、適格なステータスを付与または保証しません。

1.1。四隅モデル

ほとんどのeDeliveryメッセージングインフラストラクチャは、図2に示すように、4コーナーモデルと呼ばれる単純なメッセージングトポロジに基づいています。これは、コーナー1の元の送信者（C1）とコーナー4の最終受信者（C4）の間で情報が交換されることを意味します。 ）アクセスポイント、コーナー2と3（C2とC3）をそれぞれ経由します。これらのアクセスポイントは、同じメッセージ交換プロトコルと実装ガイドラインを実装しているため、相互運用可能です。

つまり、e-SENSプロファイル[4]で定義されているAS4メッセージプロトコル。より詳細には、図2は、C1とC4を運用する組織がC2とC3によって提供される（Q）ERDSを使用するeDeliveryビルディングブロックのメッセージ交換のユースケースを示しています。どちらも（Q）TSP（または同等のもの）です。

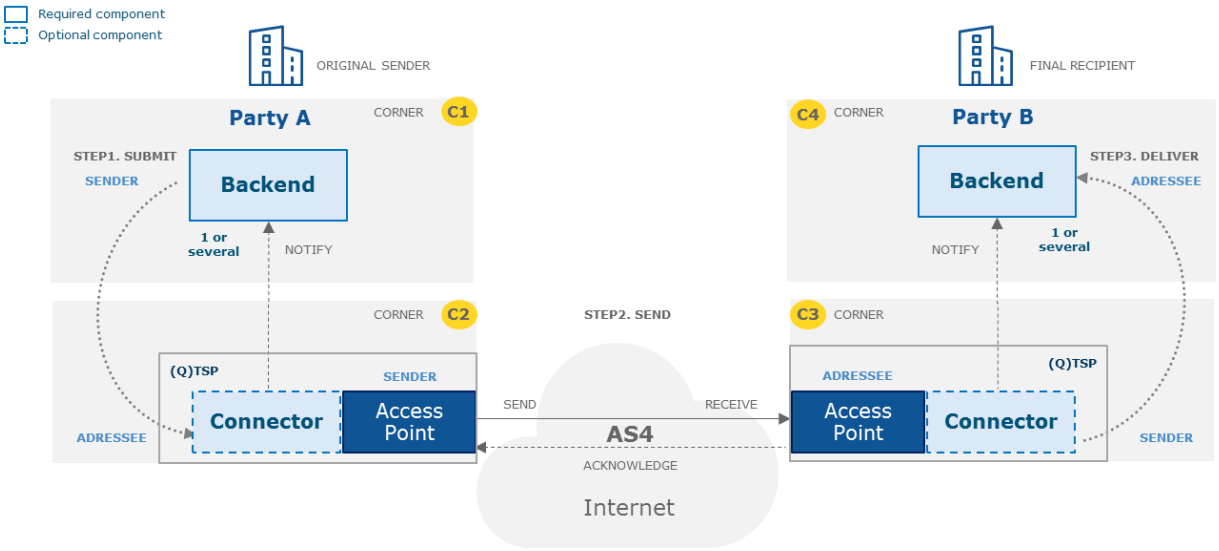

図2 eDeliveryの4コーナーモデル

4コーナーモデルの要素は次のとおりです。

- ザ· **元の送信者（C1）**そしてその **最終受信者（C4）**。これらのコーナーは両方とも組織であり、すなわち、法人（企業および行政）。これらの組織はITシステム（以下、**バックエンドシステム）**（Q）ERDSに接続します。バックエンドシステムは、エンタープライズリソースプランニングシステム、ドキュメント管理システム、ケース管理システム、ベースレジストリシステム、ポータルなど、どのタイプでもかまいません。バックエンドシステムは（Q）の外部にあるため、ERDS、自然人/エンドユーザーを認証するために使用される認証メカニズムは、これらのシステムに任されています。これは、4コーナーモデルでは次のことを意味します。

  - o **C1** メッセージの元の送信者です。したがって、C1の **バックエンド** システムが生成し、**提出する**（Q）ERDSの送信者の役割（C2）を果たしているアクセスポイントへのメッセージ。

  - o **C4** メッセージの宛先です。したがって、C4の **バックエンド** システムプロセスと メッセージを消費します **配信**（Q）ERDSのレシーバーの役割（C3）を実行するアクセスポイントによって。

  バックエンドシステムは、任意のテクノロジ（JMS、FTP、ポーリング、Webサービスなど）を使用して、アクセスポイントとの間で情報を送受信できることを明確にすることが重要です。[C1とC2経由の（Q）ERDS]と[C4とC3経由の（Q）ERDS]の間で使用される認証メカニズムの選択は、（Q）TSPに任されています。これらの（Q）TSPは、（Q）ERDS要件に準拠する技術ソリューションを使用する必要があります。メッセージ自体は、任意の形式（XML、JSON、PDF、バイナリデータなど）でパッケージ化できます。

- ザ· **送信側アクセスポイント（C2）**そしてその **受信機アクセスポイント（C4）**は、e-SENSAS4プロファイル[4]に従ったAS4メッセージ交換プロトコルの実装です。これらのコーナーは、メッセージの送信者（C1）とメッセージの受信者（C4）の間で安全で信頼性の高いデータ交換を保証します。これらのコーナーは、（Q）ERDSの境界です。2つ以上の（Q）TSP間でデータが転送される場合、C2とC3の両方がQERDS要件に準拠していれば、ERDSサービス、つまりQERDSが認定されます。また、バックエンドシステムとアクセスポイント間の統合を容易にするためにコネクタを配置できることにも注意してください。

読者は、CEFデジタルポータル[8]にアクセスして、上記の要素について詳しく知ることができます。

1.2。eDeliveryビルディングブロックの範囲

以下の表に要約されているように、4コーナーモデルで交換されるデータは、複数の通信レイヤー間で転送されます。eDeliveryビルディングブロックは、主にメッセージングおよびトランスポート通信レイヤーに焦点を当てており、他のレイヤーに対して中立です。

表3。 通信層

レイヤー	役割
アプリケーション層 （範囲外）	エンドユーザーとバックエンドシステム間の相互作用を担当します。
メッセージングおよびトランスポート層	電子データ、ドキュメント、バイナリファイルなどのメッセージをパッケージ化および転送する機能的および手続き的な手段とともにプロトコルを提供します。eDeliveryは、e-SENSプロファイル[4]に従ってAS4メッセージプロトコルを使用します。
ネットワーク層 （範囲外）	通常、このレイヤーはパブリックインターネットです。これは、ネットワークノード間でメッセージシーケンスを転送する機能的および手続き的な手段に貢献します。

通信層に加えて、4コーナーモデルに存在するセキュリティ制御を区切るために、3つのセキュリティドメインが定義されています。eDeliveryビルディングブロックは、主にクロスパーティセキュリティドメインに焦点を当てており、他のドメインに対して中立です。したがって、このセキュリティドメインはAS4メッセージングプロトコルと緊密にリンクされています[4]。

表4。 セキュリティドメイン

セキュリティドメイン	役割
クロスパーティセキュリティ（C2-C3）	アクセスポイント間の情報交換の保護に重点を置いています。
内部セキュリティ（C1-C2およびC3-C4）	バックエンドシステムとアクセスポイント間の情報交換の保護に重点を置いています。
エンドツーエンドセキュリティ（C1-C4）	元の送信者（C1）と最終的な受信者（C4）の間の情報交換の保護に重点を置いています。このドメインに含まれるのは、クロスパーティセキュリティドメインと内部セキュリティドメインで行われた選択の集約の結果です。

上記の結果として、図3は、eDeliveryビルディングブロックの範囲、つまりクロスパーティセキュリティドメインとメッセージングおよびトランスポート層を示しています。このスコープは、（Q）ERDSスコープに合わせて調整されます。

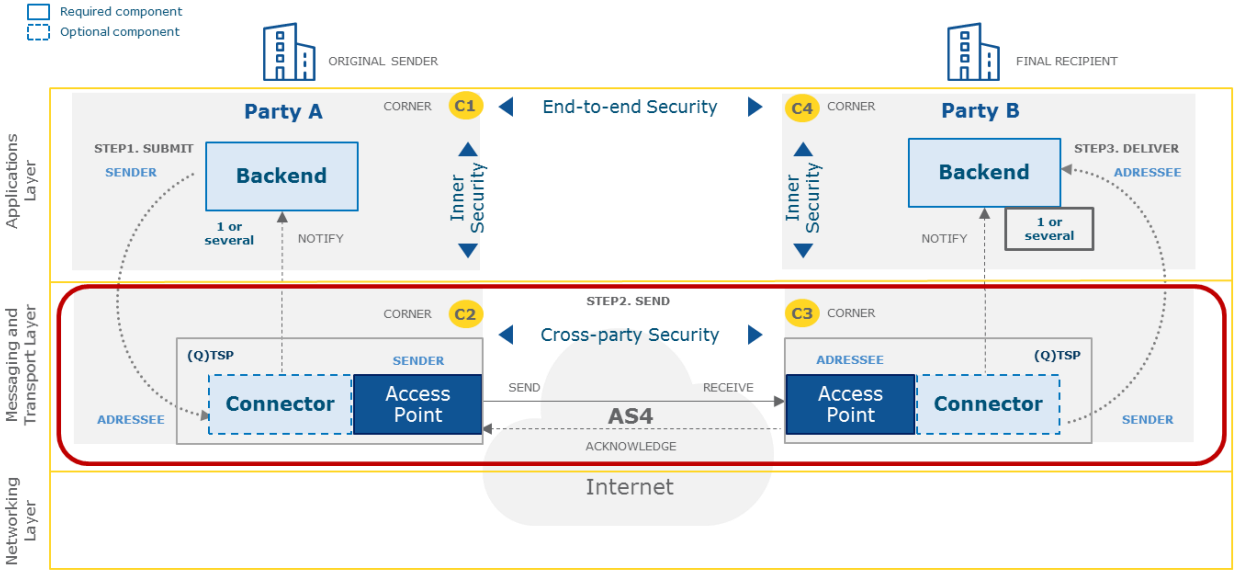

図3。 4コーナーのeDeliveryインフラストラクチャの通信レイヤーとセキュリティドメイン

各セキュリティドメインに推奨される一連のセキュリティ制御については、このドキュメントのセクション4で説明しています。各ドメインの詳細については、付録Iを参照してください。

2.2。 QERDS 要件

QERDS要件は、eIDAS規則の第44条で、テクノロジーに中立な方法で指定されています。表5[2]以下に、QERDS要件がeDeliveryの4コーナーモデルのさまざまなセキュリティドメインにどのように関連しているか、およびそれらの要件のどれに適用されるかを示します。

表5。 eIDAS規制からのQERDS要件の要約

QERDS 要件	eIDASリファレンス	CEFeDeliveryのセキュリティを目的とした解釈	ドメイン
REQ1： メッセージ **誠実さ**	第3条（36） 第19条 第24条 第44条、 *（d）データの送受信は高度な電子機器によって保護されています データが検出できないほど変更される可能性を排除するような方法での、資格のある信託サービスプロバイダーの署名または高度な電子シール。* *（e）データの送信または受信の目的で必要なデータの変更は、データの送信者および受信者に明確に示されます。*	メッセージは、送信中の不正および不正な操作から保護する必要があります。 これは、高度な電子署名/シールを介して保証する必要があります。	端から端まで セキュリティ（C1-C4）
REQ2： メッセージ **守秘義務**	第5条 第19条 第24条	メッセージは送信中に暗号化する必要があります。	端から端まで セキュリティ（C1-C4）
REQ3：送信者 **識別**	第24条 第44条 *（b）送信者の識別を高いレベルの信頼性で保証します。*	送信者の身元は、高レベルの 認証プロセスおよび/または高度電子署名/シールの使用による信頼。	内部セキュリティ （C1-C2）[3]
REQ4： **宛先** **識別**	第24条 第44条 *（c）データを配信する前に、宛先の識別を確実にします。*	宛先のIDは、メッセージを配信する前に、認証プロセスおよび/または高度な方法で確認する必要があります。 電子署名/シール。	内部セキュリティ （C3-C4）[4]
REQ5：時間- **参照**	第44条 *（f）データの送信、受信、および変更の日時は、適格な電子タイムスタンプで示されます。*	メッセージを送受信する日時は、高度な電子署名/シールによって保証された修飾された電子タイムスタンプを介して示される必要があります。	クロスバーティ セキュリティ（C2-C3）
REQ6：の証明 **送受信**	第3条（36）「…データの送受信の証拠を含む、送信されたデータの取り扱いに関連する証拠を提供する…」	メッセージの送信者と受信者には、メッセージの送受信の証拠を提供する必要があります。これは、を介して送信/配信の日時にリンクする必要があります タイムスタンプまたは修飾ステータスの修飾電子タイムスタンプ。	クロスバーティ セキュリティ（C2-C3）

[2] eIDAS規則の範囲内の要件の詳細は、付録IIに示されています。

[3][4] 技術的には、送信者の識別はC1-C2間で実行され、受信者の識別はC3-C4間で実行されます。法的に、両方の当事者（C2およびC3）は、両方の要件を満たすことに関与しています。第44条（1）（a）および第44条（1）eIDAS規則の2番目のサブパラグラフによる。QERDSは、第44条（1）（b）から（f）のそれぞれを満たす複数の資格のある信託サービスプロバイダーによって提供されます。言い換えれば、資格のある各信託サービスプロバイダーは、送信者と受信者を識別することを監督機関に証明する必要があります。複数の資格のあるトラストサービスプロバイダーのコンテキストでは、直接行うことはできませんが、他の資格のあるトラストサービスプロバイダーによって行われた識別に依存して（そしてSBに説明して）（逆に）行うことができます。

図4は、表5で説明されているQERDS要件を4コーナーモデルのコーナーにマップし、eDeliveryビルディングブロックがeIDAS規制の第44条をどのように促進するかを示しています。

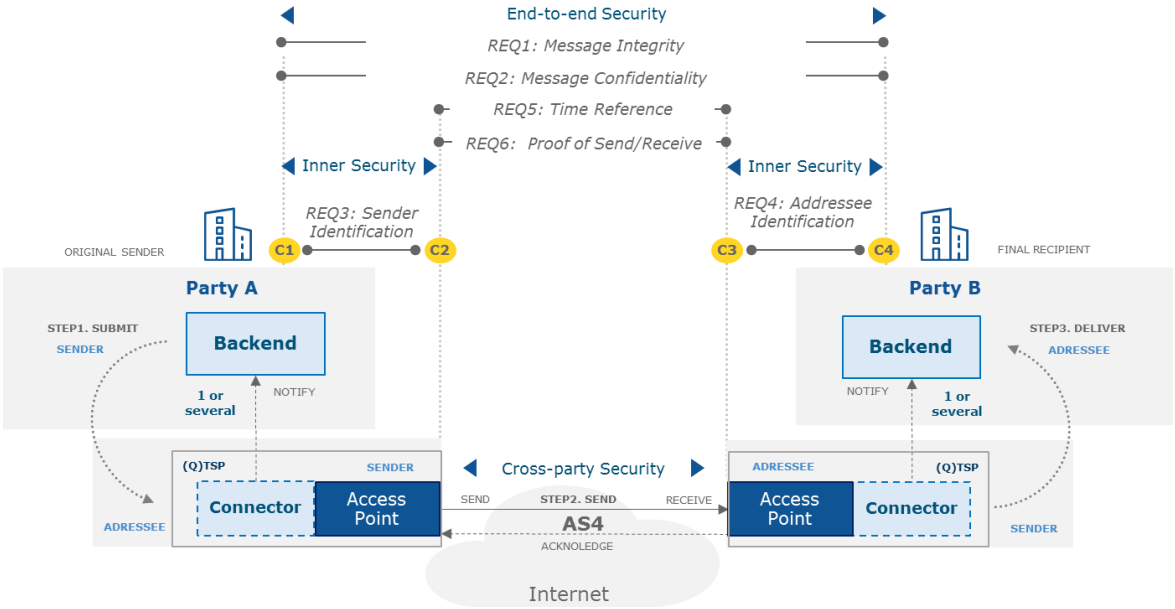

図4。 4コーナーモデルに適用されるeIDASのQERDS要件

表5に記載されている要件に加えて、サービスが2つ以上の組織によって提供されている場合は、第44条に従って「 *ポイント（a）から（f）の要件は、資格のあるすべての信託サービスプロバイダーに適用されるものとします。*

3.3。 S ECURITY CONTROLS

セキュリティ管理は、各セキュリティドメインでeDeliveryのメッセージ交換のユースケースを保護するために導入される技術メカニズムを表しています。これらのセキュリティ制御は、e-SENS AS4プロファイル（eDelivery C2-C3で使用）およびENISA [9]およびBSI [10]のベストプラクティスドキュメントから派生しました。このドキュメントには、次の2種類のセキュリティ制御があります。

- **規範的統制：** eIDAS規制の要件に対応するために必要な管理を示します。
- **非規範的統制：** このドキュメントの作成者による分析によれば、eIDAS規制の要件に対応するために必要ではないが、セキュリティを強化するために導入する必要がある推奨される管理を示します。

次の表に、セキュリティドメインごとのセキュリティ制御の種類について簡単に説明します。資格のあるステータスを付与するのはEU加盟国の監督機関次第であることを強調することが重要です。したがって、監督当局が異なる一連の統制を適用する可能性があるため、このリストは決して網羅的または完全なものではありません。

表6。 4コーナーモデルのセキュリティドメイン

セキュリティドメイン	責任者	一目でわかるセキュリティ管理の種類
C2-C3（クロスパーティ）セキュリティ	（Q）TSP	C2とC3の間の交換を保護するための主に規範的なセキュリティ制御のセット。これらのコントロールは、e-SENSAS4プロファイルに基づいて定義されています。したがって、これらはデフォルトで実装され、eDelivery仕様の対象となります。このセキュリティドメインの詳細については、セクション4.1を参照してください。
C1-C2（内部）セキュリティ **C3-C4（内部）セキュリティ**	ビジネスの送信 ドメイン所有者 受入事業 ドメイン所有者	バックエンドシステムとアクセスポイント間の交換を保護するために実装された一連のセキュリティ制御。これらのセキュリティ制御は、eDeliveryを使用する、または使用する予定のバックエンドシステム（C1およびC4）を担当する組織が実装および管理する必要があります。セクション4.2では、このセキュリティドメインに実装する必要があるコントロールのリストを推奨しています。
C1-C4（エンドツーエンド）セキュリティ	すべての集約 その他	C1とC4の間の交換を保護するために導入された一連のセキュリティ制御。このドメインは、クロスパーティおよび内部セキュリティドメインのセキュリティを集約したものであるため、両方のドメインでセキュリティ制御を実施する必要があります。セクション4.3では、このセキュリティドメインに実装する必要のあるコントロールについて説明します。

表7は、セクション2のQERDS要件にリンクされたセキュリティ管理とそれぞれの法的意味を示しています。資格のあるステータスを付与するプロセスについては、TSPは各国の監督機関を参照する必要があることに注意してください。信頼できるリストはTSPの認定ステータスを示しているため、単独で、またはPKIや相互キー交換などの他の信頼モデルと組み合わせて、コーナー間の信頼をブートストラップするために使用できます。信頼モデルの選択は、ドメインのニーズとリスク分析を考慮して行う必要があります。

このドキュメントで使用されている電子署名/シールは、eIDAS規制およびeSignature指令（指令1999/93 / EC）で定義されている高度電子署名/シールの形式です。高度な電子署名/シールは、資格のある証明書に基づいている必要があり、安全な署名/シール作成デバイスによって作成されるため、より高いセキュリティと信頼性が保証されます。高度な署名/シールを認定するには、認定された署名/シール作成デバイスで作成する必要があります。署名/シールの認定ステータスは、完全性と正確性、およびより高いセキュリティと信頼レベルの法的効果を提供します。

表7。 セキュリティ管理の概要[5]

セキュリティ管理	QERDS 要件	法的意味
CTR1： トランスポート層セキュリティプロトコル（TLS） トランスポート層セキュリティ（TLS）プロトコルは、ホスト間で暗号化メカニズムを適用することにより、メッセージの信頼性と整合性を提供します。サーバー（宛先）認証が必要であり、サーバー証明書を使用して達成されます。これにより、クライアント（送信者）は、TCP接続が適切なサーバーでセットアップされていることを確認できます。送信者（クライアント）の識別はオプションであり、構成可能なクライアント認証を通じて追加で実現できます。[6]さまざまなメカニズムの使用： • *相互認証（双方向TLS）：* これは、クライアント（送信者）のデジタル証明書を使用して行われ、サーバー（受信者）が接続しているクライアント（送信者）を確認できるようにします。相互証明書交換は、PKIや信頼リストなどの信頼モデルに依存しています。 • *基本認証：* クライアント（送信者）は、ユーザー名/パスワードを使用してサーバー（宛先）への認証を行います。この場合、安全なストレージ、十分な複雑さ、定期的な更新など、適切なパスワード管理をクライアントが保証する必要があります。 TLSは、ENISAセキュリティ[9]およびBSI [10]のガイドラインに従う必要があります。現在のバージョンは1.2です[11]。	**REQ1：** メッセージ **REQ2：** メッセージ **REQ3：** 送信者 **REQ4：** 宛先	**欧州一般データ保護規制（GDPR）。** 適用可能な場合の 守秘義務 識別 識別
CTR2： メッセージの暗号化 メッセージの暗号化により、メッセージの機密性が確保されるため、機密性の正しい受信者のみが保護されます。 メッセージはそれにアクセスできます。メッセージ暗号化プロトコルは、ENISAセキュリティに従う必要があります[9]およびBSI [10]ガイドライン。	**REQ2：** メッセージ	**欧州一般データ保護規制（GDPR）、** 適用性。
CTR3： メッセージの電子シール 電子形式のデータ。電子形式の他のデータに添付されているか、論理的に関連付けられており、後者の起源と整合性を保証します。技術的な観点から、電子シールは メッセージの整合性、および発信元のID。その法的効力はeIDASによって定義されています 規制、第35条。 *（1）「電子シールは、電子形式である、または適格な電子シールの要件を満たしていないという理由だけで、法的手続きの証拠としての法的効力および許容性を否定されないものとします。」* *（2）「認定された電子シールは、データの完全性と、認定された電子シールがリンクされているデータの出所の正確性の推定を享受するものとします。」* 高度な電子シールの場合、要件はeIDAS規則の第36条で定義され、標準アルゴリズムと暗号スイートはeIDとTSPのENISA標準化[12]で定義され、ETSI TR 119 000 [14]に従います。	**REQ1：** メッセージ **REQ3：** 送信者 識別	**不適格：** データの整合性と発信元、つまりデータの認証を保証します。 **認定済み：** eIDAS規則、第35条。「認定された電子シールは、データの完全性と、認定された電子シールがリンクされているデータの出所の正確性の推定を享受するものとします」 **両方とも：** 訴訟手続きにおける無差別
CTR4 ：証拠の電子シール メッセージが送信され、目的の受信者に配信されたことを示すメッセージの送信者への証拠として機能します。	**REQ6：** の証明 送受信	
CTR5： 電子タイムスタンプ 電子形式の他のデータを特定の時間にバインドする電子形式のデータは、後者のデータがその時点で存在したという証拠を確立します。その法的効力は、eIDAS規則の第41条で定義されています。 *（1）「電子タイムスタンプは、電子形式である、または適格な電子タイムスタンプの要件を満たしていないという理由のみで、法的手続きの証拠としての法的効力および許容性を否定されないものとします。」* *（2）「適格な電子タイムスタンプは、それが示す日付と時刻の正確さ、および日付と時刻がバインドされているデータの整合性の推定を享受するものとします。」* 適格なタイムスタンプ要件は、eIDAS規制の第42条で定義されていますが、標準アルゴリズムと暗号スイートは、eIDとTSPのENISA標準化[11]で定義されており、ETSI TR 119 000 [14]に従います。	**REQ5：** 時間- 参照	**不適格：** 特定の時間にデータの存在を確立します。つまり、データの日付と時刻を確認します。 **認定済み：** eIDAS規則、第41条。「適格な電子タイムスタンプは、それが示す日付と時刻の正確さ、および日付と時刻がバインドされているデータの整合性の推定を享受するものとします。」 **両方とも：** 訴訟手続きにおける無差別
CTR6： メッセージの電子署名 電子形式の整合性の他のデータに添付または論理的に関連付けられ、署名者が署名するために使用する電子形式のデータ。その法的効力は、eIDAS規則のArticleによって定義されています。 25。 *（1）「電子署名は、法的効力および法的証拠としての許容性を否定してはならない。* *電子形式である、または資格のある電子署名の要件を満たしていないという理由だけで手続きを行います。」* *（2）「適格な電子署名は、手書きの署名と同等の法的効力を有するものとします」* 高度電子署名要件はeIDAS規則の第26条で定義されていますが、標準アルゴリズムと暗号スイートはeIDとTSPのENISA標準化[12]で定義されており、ETSI TR 119 000 [14]に従います。	**REQ1：** メッセージ **REQ3：** 送信者 識別	**不適格：** 自然人が署名するために使用します。言い換えれば、明示的な同意（または署名者が特定のトランザクションに対して持つ可能性のあるその他の機能的同等性） **認定済み：** eIDAS規則、第25条。「適格な電子署名は、手書きの署名と同等の法的効力を有するものとします」 **両方とも：** 訴訟手続きにおける無差別

[5] セキュリティ管理策のリストは網羅的ではなく、特定のアルゴリズムを示唆していません。そのため、読者はENISA [10]、BSI [11]などのベストプラクティスガイドライン、および定義されたとおりに使用できる標準の例のリストを参照しています。 eIDおよびTSPのENISA標準化[13]、eIDASを実装するENISAガイドライン[3]およびETSI TR 119 000 [15]。

[6] 認証は、単一または複数のオーセンティケーターに基づくデジタルIDの信頼性を確立するために使用されるプロセスであり、エンティティの知識（ユーザー名/パスワード）、所有（デジタル証明書やトークンなど）、または固有性（バイオメトリクスなど）に基づくことができます。

4.4。 R 推奨事項

このセクションでは、4コーナーモデルのセキュリティドメインのそれぞれに導入する規範的および非規範的なセキュリティ管理策の推奨事項を示します。セキュリティ管理、技術的および法的意味のより詳細な説明は、付録Iにあります。

4.1。クロスパーティセキュリティ（C2-C3）

このセクションでは、QERDS要件を満たすために、eDeliveryアクセスポイントによってクロスパーティセキュリティドメインにデフォルトで実装されているセキュリティ制御について説明します。図5は、C2とC3の間のこれらの規範的なセキュリティ制御を黄色で示しています。これらのコントロールは、e-SENSAS4プロファイルで規定されています。

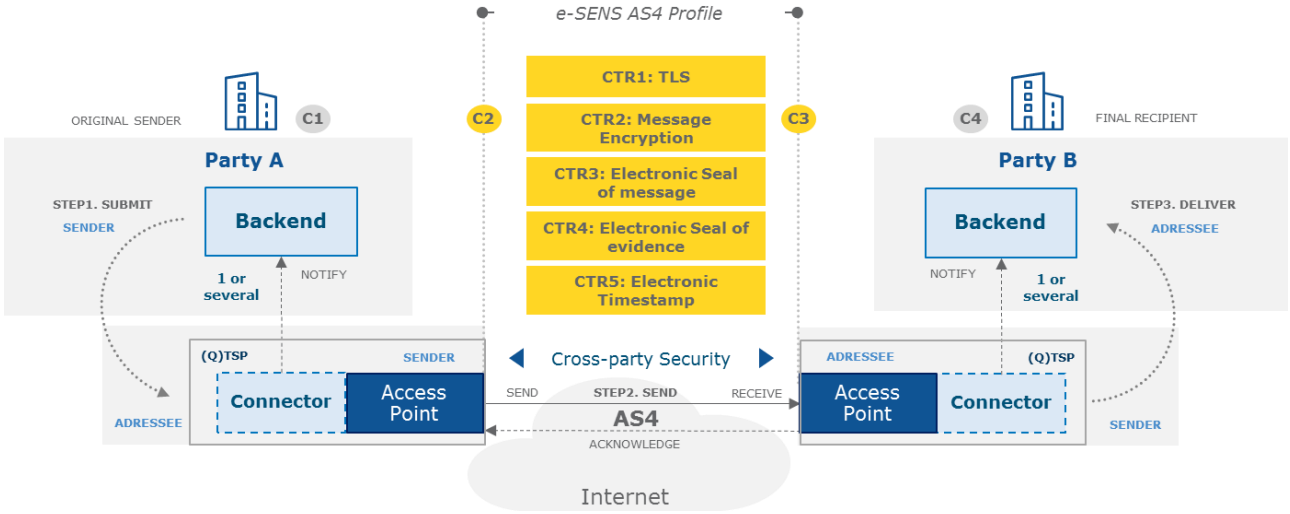

図5。 クロスパーティセキュリティドメインで実装された（黄色の）セキュリティ制御

表8は、クロスパーティセキュリティドメイン（C2-C3）の規範的なセキュリティ管理の概要と、QERDS要件へのマッピングを示しています。表は次のとおりです。

- バツ アクセスポイントにデフォルトで実装されている規範的なセキュリティ制御用。この場合、セルはグレー表示され、e-SENS AS4プロファイル（C2-C3）に従ってeDeliveryビルディングブロックでこれらのコントロールがデフォルトで使用可能であることを示します。
- O アクセスポイントのPModeパラメータを介してオプションで構成可能な非規範的なセキュリティ制御用。

このドメインのセキュリティ管理の技術的および法的意味は、付録I.1に記載されています。

表8。 クロスパーティドメインのセキュリティ管理[7]

	C2 – C3						説明
	REQ1	REQ2	REQ3	REQ4	REQ5	REQ6	
CTR1：トランスポート層セキュリティプロトコル（TLS）	バツ	バツ	O	バツ			TLSは、C2-C3間のメッセージの機密性と整合性を保証するため、REQ1、REQ2、およびREQ4を満たします。REQ3は現在オプションであり、AS4プロファイルで定義されているように、相互認証（セクション2に示す）を介してアクセスポイントの設定で定義できます。TLSは、メッセージがC2とC3に暫定的に格納されている間ではなく、C2-C3間のメッセージ転送中にREQ1とREQ2が満たされることを保証することに注意してください。
CTR2：メッセージ暗号化		バツ					メッセージはC2からC3によって暗号化（CTR2）されます。これにより、C3のみがメッセージを開くことができることが保証され、REQ2が保証されます。
CTR3：メッセージの電子シール	バツ		バツ				REQ1とREQ3を満たすために、C2はメッセージに電子シールを適用します。これにより、C3はメッセージの整合性と送信者を確認できます。（高度な）電子シールがメッセージに添付されているため、C2の公開証明書を使用して、任意のエンティティがいつでも確認でき、送信者（C2）からの否認防止が保証されます。
CTR4：証拠の電子シール						バツ	REQ6を満たすために、受信側のアクセスポイント（C3）は、メッセージの受信に電子シールを適用します。この領収書は、リクエストに応じて利用できるように保存されます。これにより、受信者（C£）からの否認防止が保証されるだけでなく、「その」メッセージを受信したことも保証されます。
CTR5：電子タイムスタンプ					バツ		REQ5（非適格）を満たすために、eDeliveryアクセスポイント（C2およびC3）は、タイムスタンプを使用して送信時刻を証明し、タイムスタンプを受信時刻に使用します。適格なタイムスタンプの場合、日付の正確さは協定世界時に基づいており、QTSPの高度な電子シールを使用して署名されている必要があります（第42条）。

伝説：

REQ1：メッセージの整合性	REQ4：宛先の識別	□：適用できません
REQ2：メッセージの機密性	REQ5：時間参照	バツ：デフォルトの規範的統制
REQ3：送信者の識別	REQ6：プルーフ送信/受信	O：非規範的管理

4.2。内部セキュリティ（C1-C2、C3-C4）

このセクションでは、バックエンドシステムを4コーナーモデルのアクセスポイントに接続するためにC1およびC4が実装する必要のあるセキュリティ制御のリストを推奨します。図6に示すように、それらの数は最小限に抑えられています。この図は、推奨されるセキュリティ管理策にリンクされているQERDS要件も示しています。

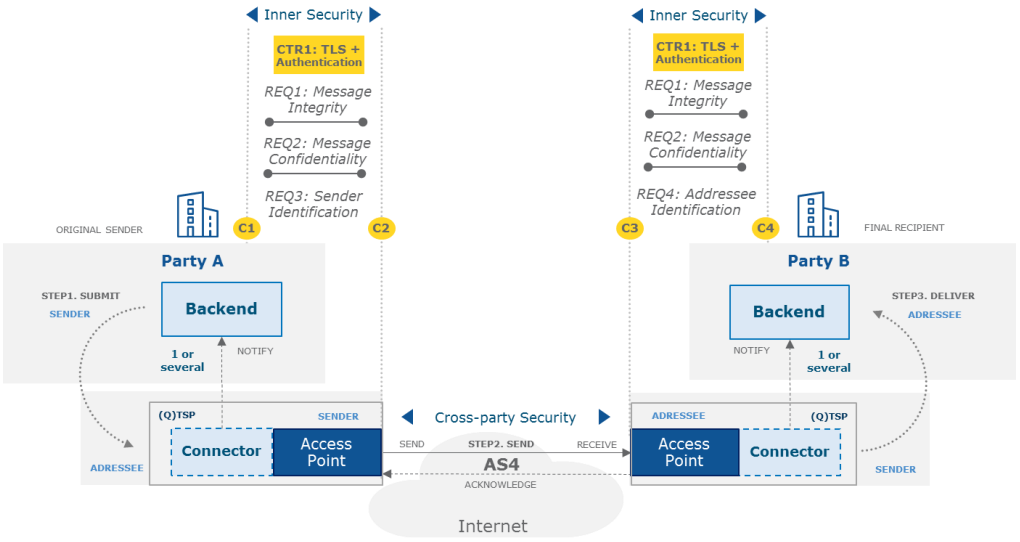

図6。 内部セキュリティドメインに推奨されるセキュリティ制御（黄色）

[7] 認証は、eIDAS規則の第3条（5）で、「自然人または法人の電子識別、または電子形式のデータの出所と完全性を確認できる電子プロセス」として定義されており、REQ4を表します。 C2とC3の間は、電子シール（CTR3）を使用して満たされます。属性またはアクセス制御リストによる組織のアクセス権の定義は、アクセスポイントレベルで構成可能であり、（Q）TSPによってPMode構成で指定されます。アクセス制御は非規範的な制御を表すため、アクセス権は表6に示されていません。

表9は、バックエンドシステムをeDeliveryアクセスポイントに接続するときに組織が実施する必要のある最小限のセキュリティ制御の概要を示しています。このセキュリティドメインは **C1-C2** そして **C3-C4**。 ザ· バツ このドメインの規範的なセキュリティ管理を表します。この場合、追加の非規範的統制はありません（ O ）。 REQ5（時間参照）およびREQ6（送信/受信の証明）はC2およびC3によって実装されるため、このドメインには存在しないことに注意してください。それでも、アクセスポイントによって生成された証拠は、要求に応じてC1およびC4で利用できるようになる必要があります。このドメインのセキュリティ管理の技術的および法的意味は、付録I.2に記載されています。

表9。 内部セキュリティドメインのセキュリティ管理

	C1 – C2				C3 – C4				説明
	REQ1	REQ2	REQ3	REQ4	REQ1	REQ2	REQ3	REQ4	
CTR1：輸送 レイヤーセキュリティ プロトコル（TLS） クライアントと **認証**	バツ	バツ	バツ		バツ	バツ		バツ	TLSは、C1-C2とC3-C4の間のメッセージの機密性と整合性を保証します。C1-C2間のTLSは、TLSがクライアント認証を追加する場合（つまり、C2とC3にそれぞれ接続する場合はC1とC4）、REQ1とREQ2も満たします。これは、基本認証（ユーザー名/パスワードなど）または双方向TLS（相互認証）を使用して実行できます。同じことがC3-C4間のTLSセッションにも当てはまります。TLSは、メッセージがC2とC3に暫定的に保存されている間ではなく、C1-C2とC3-C4の間のメッセージ転送中にREQ1とREQ2が満たされることを保証することに注意してください。

伝説

REQ1：メッセージの整合性	REQ4：宛先の識別	バツ ：規範的統制
REQ2：メッセージの機密性	REQ5：時間参照	O ：非規範的統制
REQ3：送信者の識別	REQ6：送信/受信の証明	

4.3。エンドツーエンドセキュリティ（C1-C4）

このドメインは、C1およびC4（内部セキュリティ）を運用する組織によって実施されるセキュリティ制御と、eDeliveryアクセスポイント（C2およびC3（クロスパーティセキュリティドメイン））によって実装される制御の集合体で構成されます。その結果、図7は、エンドツーエンドのセキュリティが推移的に達成されることを示しています。

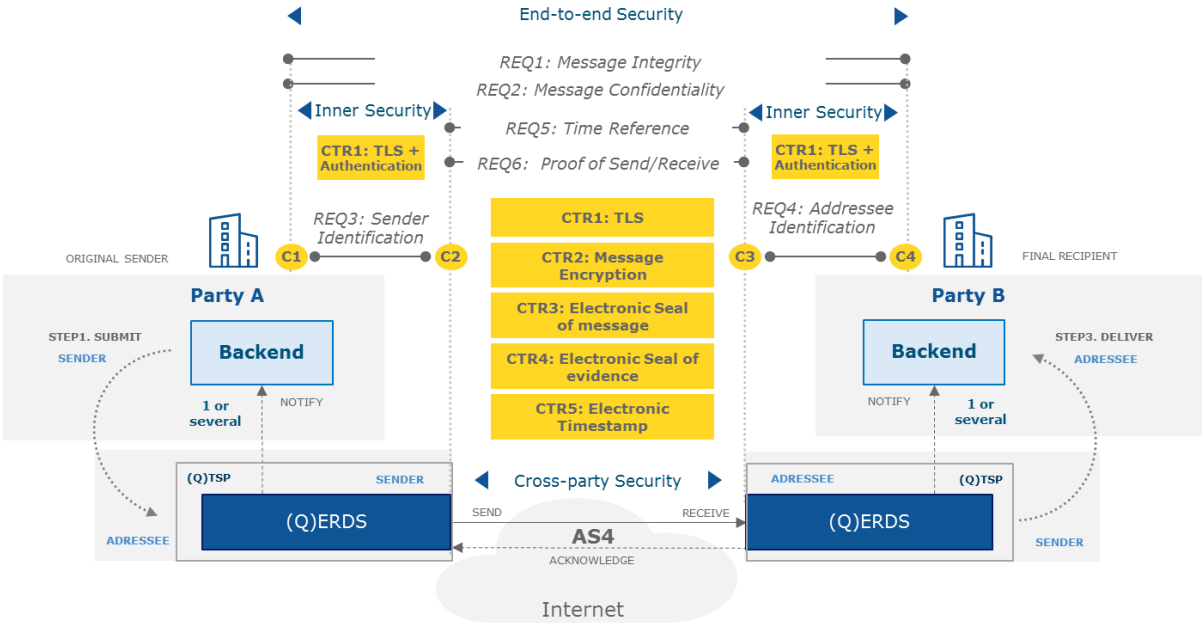

図7。 エンドツーエンドのセキュリティドメインに推奨されるセキュリティ制御（黄色）

eIDAS規則のERDS定義によれば、ERDSは、送信されたデータの処理に関連する証拠を提供します（第3条（36））。さらに、第24条（2）（h）に記載されているように、証拠を記録および提供するための信頼サービスを提供するのは（Q）TSPの責任です。したがって、このドキュメント（REQ6）に記載されている法的証拠は、（Q）TSP（つまり、C2とC3の操作）によって、要求に応じて元の送信者（C1）と最終受信者（C4）に提供されます。

エンドツーエンドのセキュリティドメインには、元の送信者（C1）から最終的な受信者（C4）までのセキュリティが必要です。どちらも、QERDS要件に準拠するアクセスポイント（C2〜C3）と通信します。表10は、エンドツーエンドのセキュリティ（C1-C4）を実現するために必要な規範的および非規範的なセキュリティ管理策をまとめたものです。 **推移的に。** この表には、それぞれのQERDS要件へのマッピングも示されています。前の章と同様に、 バツ は、要件を満たすために必要なセキュリティコントロールを示し、灰色のセルは、e-SENSAS4プロファイルに従ってeDeliveryビルディングブロックでデフォルトで使用できるコントロールを示します。eDeliveryメッセージングインフラストラクチャの機密性と整合性のレベルをさらに強化するために、組織は追加の非規範的なセキュリティ制御を実装できます（これらは O ）。これらは、ビジネスニーズとセキュリティポリシーに従って選択する必要があります。エンドツーエンドセキュリティドメインの詳細については、付録I.3を参照してください。

表10。 C1およびC4をeDeliveryに接続するためのエンドツーエンドセキュリティドメインの推奨セキュリティ制御

	C1			C2 – C3						C4			説明
	REQ1	REQ2	REQ3	REQ1	REQ2	REQ3	REQ4	REQ5	REQ6	REQ1	REQ2	REQ4	
CTR1：輸送 レイヤーセキュリティプロトコル（TLS）と**認証**	バツ	バツ	バツ	バツ	バツ					バツ	バツ	バツ	TLSは、C1-C2とC3-C4の間など、コーナー間のメッセージの機密性と整合性を保証します。特に、TLSはC1-C2およびC3-C4のREQ1およびREQ2を満たしています。 元の送信者（C1）と最終受信者（C4）の識別は、それぞれC2とC3の責任です。したがって、REQ3はC1-C2間で、REQ4はC3-C4間で、認証付きTLS（双方向TLSまたは基本認証）によって満たされます。自然人/エンドユーザーの認証に使用される認証メカニズムは、バックエンドシステム（つまり、C1およびC4）に任されています。
CTR2：メッセージ**暗号化**		O			バツ								REQ2を満たすために、C2はC3（CTR2）のメッセージを暗号化します。オプションで、C1はC4を暗号化して、パスC1〜C4全体（転送、ストレージ、処理）でREQ2が満たされるようにすることができます。
CTR3：電子シール メッセージの	O		O	バツ		バツ							REQ1とREQ3を満たすために、C2はメッセージヘッダーとペイロードに電子シールを適用し、C3はメッセージの整合性と送信者を検証します。オプションで、C1はメッセージペイロードを封印して、C2（REQ3）に対して自身を識別し、REQ1が満たされていることを確認できます（この可能性の詳細については、付録I.3の拡張セキュリティシナリオを参照してください）。
CTR4：電子シール **証拠の**									バツ				（Q）TSPとしてREQ6、C2、およびC3を満たすには、各メッセージの送受信と日時（電子タイムスタンプとして）に電子シールを適用し、それを保存して、C1およびC4への要求に応じて利用できるようにします。
CTR5：電子 タイムスタンプ								バツ					REQ5を満たすために推奨される構成は、C2とC3が（修飾された）タイムスタンプを使用して、メッセージの送受信時刻を証明することです。適格なタイムスタンプの場合、日付の正確さは協定世界時に基づいており、QTSPの高度な電子シールを使用して署名されている必要があります（第42条）。
CTR6：電子 **署名**	O		O										CTR6は、C2（REQ3）に対する自然人の識別、およびC4までのREQ1の実行に使用できます。（この可能性の詳細については、付録の拡張セキュリティシナリオを参照してください。 I.3）。

伝説：

REQ1：メッセージの整合性	REQ4：宛先の識別	□：適用できません
REQ2：メッセージの機密性	REQ5：時間参照	バツ：デフォルトの規範的統制
REQ3：送信者の識別	REQ6：証明の送信/受信	バツ：実装される規範的な制御
		O：非規範的統制

5.5。 S UMMARY AND C 結論

eIDAS規則は、（Q）ERDSの共通の参照を提供し、ヨーロッパ全体で共通の法的効力を持ちます。eDeliveryビルディングブロックは、メッセージングおよびトランスポート層に一連のセキュリティ制御を導入することにより、eIDAS規制の（Q）ERDS要件への対応を容易にします。

このドキュメントでは、eIDAS規制の要件の概要と、元の送信者から最終の受信者にメッセージを安全に交換するためにこれらの要件を満たすのに役立つ推奨セキュリティ制御のリストを提供しました。さらに、eDeliveryによって実装されるセキュリティ制御、およびeDeliveryメッセージングインフラストラクチャを介して接続する、または接続する予定の組織が実施することを推奨するセキュリティ制御のリストについても説明しました。

ドキュメントで説明されているように、内部セキュリティドメインでのセキュリティ制御の実装は、（Q）ERDSを使用する組織（つまり、企業および行政）の全責任です。このドキュメントに記載されているセキュリティ管理策の実装は、「適格」ステータスを保証するものではないことに注意することが重要です。（Q）TSPにそれを付与するのはEU加盟国の監督機関次第です[2]。

6.6。 C 連絡先情報

CEFサポートチーム

メール：CEF-EDELIVERY-SUPPORT@ec.europa.eu

電話：+32 2 299 09 09

- **標準サービス：午前8時から午後6時（通常のEC営業日）**
- **スタンバイサービス*：午後6時から午前8時（コミッションと祝日、週末）**

** 重大かつ緊急のインシデントの場合のみ、電話のみ*

付録I。 S ECURITYドメイン詳細な説明

このセクションでは、eDeliveryビルディングブロックに実装されているセキュリティ制御について説明し、組織がeDeliveryへの信頼できる接続を実行するためのセキュリティガイドラインをいくつか示します。

このドキュメントで使用されている電子署名/シールは、高度な電子署名/シールの形式であるため、認定された証明書に基づいており、安全な署名/シール作成デバイスによって作成されます。認定ステータスは、より高いセキュリティレベルと法的サポートを提供しますが、認定ステータスは、適合性評価機関の認定時に監督機関によってのみ提供されます。[8.8]。

I.1。C ロス海支隊（ C2-C3 ）S ECURITY DOMAIN

このセクションでは、eDeliveryビルディングブロックに実装されている標準的なセキュリティ制御と、図8に示すアクセスポイント間の通信フローについて詳しく説明します。

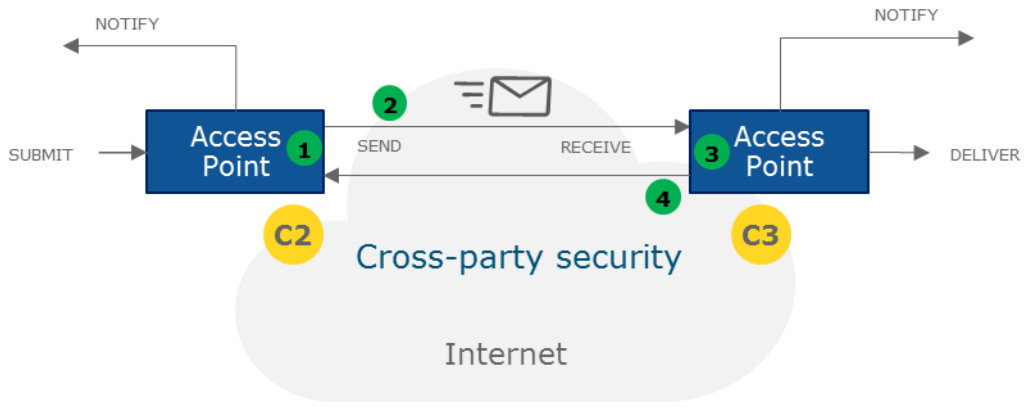

図8。 クロスパーティセキュリティ（C2-C3 ）

eDeliveryコンポーネントは、トランスポートおよびメッセージング層でe-SENS AS4プロファイルに準拠したいくつかのセキュリティ制御を使用することにより、C2とC3の間のセキュリティを確保します。

C2（送信者）とC3（受信者）間のメッセージ交換は、次の4つのステップで説明されます（図8）。

1.1。 アクセスポイント（C2）は、SOAPで構成されるAS4メッセージを作成します **ヘッダー、SOAP本体、および1つ以上のペイロード（** 図9に示すように、受信者としてC3を使用した添付ファイル）。暗号化され、電子的に封印されたコンテンツが添付ファイルに含まれます。電子シールは、C2の秘密鍵を持つRSA-SHA256暗号スイートを使用して実行されます。コンテンツの暗号化には、GCM認証動作モードでのAES対称暗号化が、RSAOAEPを使用してC3の公開鍵で暗号化されたランダムに生成された鍵で使用されます。さらに、メッセージID、元の送信者、最終的な受信者情報などのメッセージメタデータの詳細を含むヘッダーもC2によって封印されます。電子シールダイジェスト

[8] 適合性評価機関は、規則（EC）765/2008に基づくeIDAS規則に対してQTSP / QTSの状態を評価します。適合性評価機関は、加盟国の国家認定機関によって認定されています。

ヘッダーとコンテンツペイロードの暗号化情報はWS-Securityヘッダーに含まれますが、SOAP本体はe-SENSAS4プロファイルで説明されているように空で送信されます。

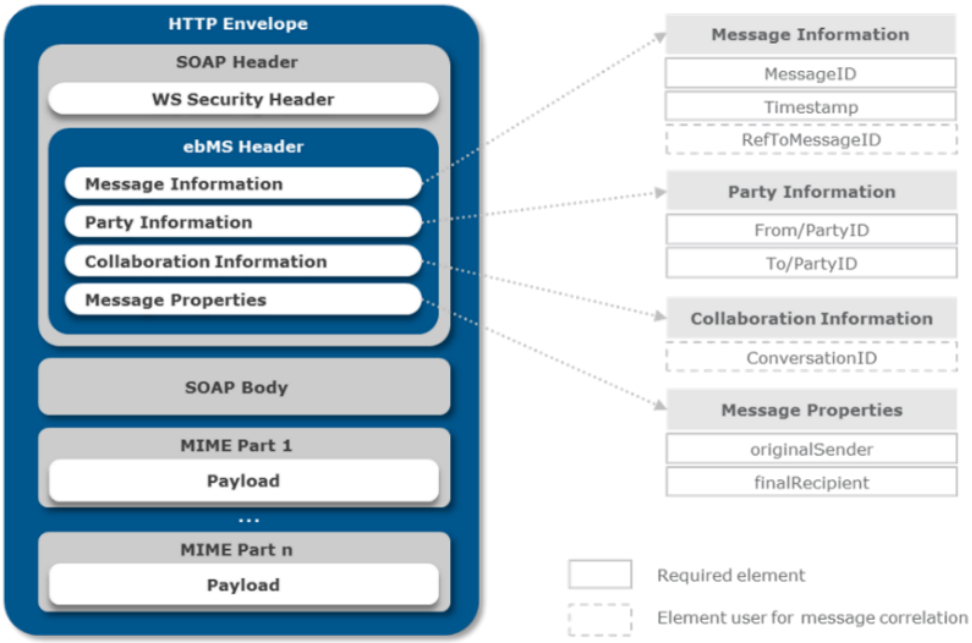

図9。 e-SENS AS4 eDeliveryメッセージ構造（SOAPエンベロープ）

2.2。メッセージはTLS接続を介して送信され、トランスポート層でメッセージの機密性と信頼性を提供します。TLS接続の確立中に、C2（送信者）はC3のデジタル証明書を使用してC3（宛先）を識別しますが、C2はオプションで（PMode設定で構成可能）相互認証を使用して識別されます。メッセージはメッセージング層で安全であるため、TLSの使用は冗長であることがわかりますが、セキュリティの層が追加され、メッセージ転送の感度レベルに応じてパフォーマンスに影響を与えます。TLS暗号スイートは構成可能であり、TLSの将来の使用に推奨される暗号スイートはENISAガイドライン[9]に従う必要があります。

3. C3は、秘密鍵を使用してメッセージを復号化し、C2のデジタル証明書（公開鍵）に従ってメッセージの整合性と信頼性を検証します。これにより、C2がメッセージの送信者であり、通信中にメッセージが改ざんされていないことがC3に保証されます。デジタル証明書の交換とC2およびC3の信頼モデルは、eDeliveryPKIサービスで定義されています[13]。

4.受信と検証の際、C3は受信したメッセージ情報に基づいて証拠の受信を生成し、電子証明書を使用してそれを封印し、受信の証拠としてC2に送信します。C2はメッセージがC3によって受信されたことを確認できるため、電子シールは証拠の完全性と信頼性を提供します。

表11に、C2とC3の間のクロスパーティセキュリティドメインで実装されたセキュリティ制御の概要を、eIDAS規制に基づくセキュリティ要件へのマッピング、および技術的（セキュリティ）および法的意味とともに示します。

表11。アクセスポイントの送信（C2）とアクセスポイントの受信（C3）の間の、クロスパーティセキュリティドメインでのセキュリティ制御の技術的および法的意味。

セキュリティコントロール	説明	要件	含意	
			テクニカル	法的
CTR1：輸送層セキュリティ（TLS）	ENISAセキュリティ[9]およびBSIに従って、トランスポート層セキュリティ（TLS 1.2 [11]）プロトコルが使用されます[10]ガイドライン。C2は、トランスポート層での整合性メッセージの機密性と信頼性のために、C3とのTLS接続を確立します。送信者（C2）IDは次のように提供されます。 • 相互認証：これは、C2のデジタル証明書（TLS / SSL証明書）を使用して行われ、C3がC2を識別できるようにします。認定ステータスの場合は、認定証明書を使用する必要があります。	REQ1：C2⟷C3間で送信されるメッセージのメッセージの信頼性。 REQ 2：メッセージC2からC3の間で送信されるメッセージの機密性。守秘義務 REQ3：送信者識別 REQ4：宛先宛先（C3）は、識別を使用して送信者（C2）によって識別されます。	双方向TLSが使用されている場合、送信者（C2）は、Webサイト認証証明書（マシン間またはTLS証明書）を使用して宛先（C3）によって識別されます。 メッセージ送信前のWebサイト認証証明書（マシン間またはTSL証明書）。これは*オプション* PMode設定で構成する必要があります。	適用可能な場合は、欧州の一般データ保護規則（GDPR）。
CTR2：メッセージ暗号化	C2は、ランダム秘密鍵を使用してAES-GCMを使用してメッセージのペイロードを暗号化し、RSA-OAEPを使用してC3の公開鍵を使用してランダム鍵を暗号化します。メッセージ暗号化は、W3CXML暗号化を使用したWS-Securityに従います。対称暗号化に使用される暗号スイートはAES GCMモードであり、非対称暗号化に使用される暗号スイートはRSA-OAEPです。これは、ENISAセキュリティ[9]およびBSI [10]のガイドラインに従っています。	REQ2：メッセージ	メッセージペイロードは、宛先の機密性のためにC2によって暗号化されます C3。これにより、宛先C3のみが適用を開くことができることが保証されます。送信、保存、および処理中のメッセージ。	欧州の一般データ保護規則（GDPR）、
CTR3：電子のシールメッセージ	メッセージには電子シールが貼られています。C2は、整合性保護を保証する独自の秘密鍵を使用して、メッセージヘッダーとペイロードに電子シールを適用します。シールは、メッセージペイロードとヘッダーの発信元の信頼性と否認防止のためにC2の公開鍵を使用してC3によって検証されます。 電子シーリングは、W3CXML署名を使用したWS-Securityに従います。使用されている暗号スイートはRSASHA256です。高度なシールに関するその他の推奨規格は、eIDおよびTSPのENISA標準化[11]に記載されており、ETSI TR 119 000 [14]に従います。	REQ1：メッセージ誠実さ REQ3：送信者識別	メッセージのペイロードとヘッダーは電子的に封印されており、送信、保存、および処理。これにより、C3はメッセージペイロードを確認できます 送信者はC2です。電子シールが付いているので メッセージ、それは保持している任意のエンティティによっていつでも確認できます C2公開証明書と同じ信頼ドメイン内。	**不適格：** データの整合性と発信元、つまりデータの認証を保証します。 **認定済み：** eIDAS規則、第35条。「資格のある電子シールとヘッダーは改ざんされていないものとし、メッセージデータの整合性と正確性の推定をお楽しみください 認定された電子シールがリンクされているデータの出所。」 **両方とも：** 法的手続きにおける無差別。
CTR4：電子のシール証拠	領収書には電子シールが貼られています。C 2からのメッセージの受信および検証時に、ＲＥＱ６：Ｃ３の証明は、メッセージ（例えば、メッセージ）に基づいて証拠受信を生成する。 新しいタイムスタンプと受信メッセージへの参照を含む識別子、タイムスタンプ、および送信者メタデータ）は、電子シールを適用し、シールされた証拠をC2に返します。レシートは、最初のメッセージに対する「シグナル」メッセージ応答としてC2に自動的に送信されます。 CTR3と同様に、電子シーリングはW3CXML署名を使用したWS-Securityに従います。（CTR3を参照）	識別情報	C3が正しいメッセージと否認防止を受信したことをC2に保証します。シールは、送信、保管、および処理中に確認できます。	
CTR5：電子タイムスタンプ	メタデータ（システム）タイムスタンプはWS-Securityヘッダーに配置され、整合性保護のために電子的にシールされます。現在使用されているタイムスタンプはシステムクロックに依存しているため、修飾されません。適格なタイムスタンプについては、監督機関からの承認後に追加の措置を講じる必要があります。高度なタイムスタンプに関するその他の推奨標準は、eIDおよびTSPのENISA標準化[11]に記載されています。	REQ5：時間-参照	応答証拠受信のタイムスタンプは、メッセージが特定の時間にC3によって処理されたことを保証します。一方、元のAS4メッセージのタイムスタンプは、メッセージが特定の時間にC2によって送信されたことを保証します。	**不適格：** 特定の時間にデータの存在を確立します。つまり、データの日付と時刻を確認します。 **認定済み：** eIDAS規則、第41条。「適格な電子タイムスタンプは、それが示す日付と時刻の正確さ、および日付と時刻がバインドされているデータの整合性の推定を享受するものとします。」 **両方とも：** 訴訟手続きにおける無差別

[9] eIDAS規則によって定義され、推進されているすべての法的効果は、EU-28内のすべての加盟国に適用されます。

I.2。私 NNER（ C1-C2、C3-C4 ）S ECURITY DOMAIN

このセクションでは、ERDS要件に従ってバックエンドシステムとアクセスポイント間の通信を保護するために、バックエンドシステムを運用している組織が内部セキュリティドメインに実装する規範的なセキュリティ制御について詳しく説明します。

ERDS要件に準拠するために、バックエンドシステムを制御する組織は、TLSを実装して、メッセージの機密性と整合性、および接続コーナー（C1とC2、またはC3とC4）の認証を保証することをお勧めします。

TLSの使用に関連する技術的および法的な影響は、接続コーナーごとに表12に示されています。

I.3。E ND-TO-END（ C1-C4 ）S ECURITY DOMAIN

通信C1-C4は、元の送信者と最終受信者の間のバックエンド（C1）からバックエンド（C4）への通信を具体化します。次の3つのシナリオは、eDeliveryの利害関係者によって特定されています。 **デフォルト** eDeliveryビルディングブロックの一般的な使用法を表すシナリオ。C2とC3は（Q）TSPを表します。

1.委任シナリオ（ **デフォルト** ）、 元の送信者C1を運用している組織
C2システムに接続しますが、メッセージのセキュリティ（シーリングや暗号化など）をC2に委任します。シーリングは、C1が元の送信者として識別されている間に、C2の証明書からの資格情報を使用して実行されます。

2.拡張委任シナリオ。元の送信者C1を管理している組織が、C1に発行されたデジタル証明書でメッセージを封印する権利をC2に委任します。この場合の法的側面は、C1とC2を運営する組織間で契約上取り扱われます。

3.3。通信組織（元の送信者C1と最終受信者C4）が、メッセージのさまざまな機密レベルとビジネス要件に応じて、メッセージの署名/封印やメッセージの暗号化などのセキュリティ制御の重要な部分を担当する拡張セキュリティシナリオ。したがって、組織は、電子シール/署名（CTR3およびCTR4）を使用して、追加の非規範的なセキュリティ制御を実装します。このシナリオでは、相互運用可能な方法でメッセージ交換を中継するために、C1とC4、およびC2-C3間の相互信頼が必要です。

表12に、セキュリティ管理策、それらが満たす要件、およびそれらの技術的および法的意味の詳細な説明を示します。

I.3.1。D エレゲーションシナリオ

委任シナリオ（デフォルト）は、図10に示すように、元の送信者C1に対応する組織が（Q）TSPを表す通信パートナーC2にメッセージ処理権限を明示的に委任するシナリオを考慮します。この場合、C2はメタデータ内の元の送信者C1への参照を保持しながら、独自のデジタル証明書（つまり、対応する秘密鍵）を持つメッセージ。受信者側では、C4はメタデータを介してメッセージの元の送信者がC1であることを確認でき、C3はC2が証明書を使用してメッセージをデジタルで封印したことを確認できます。

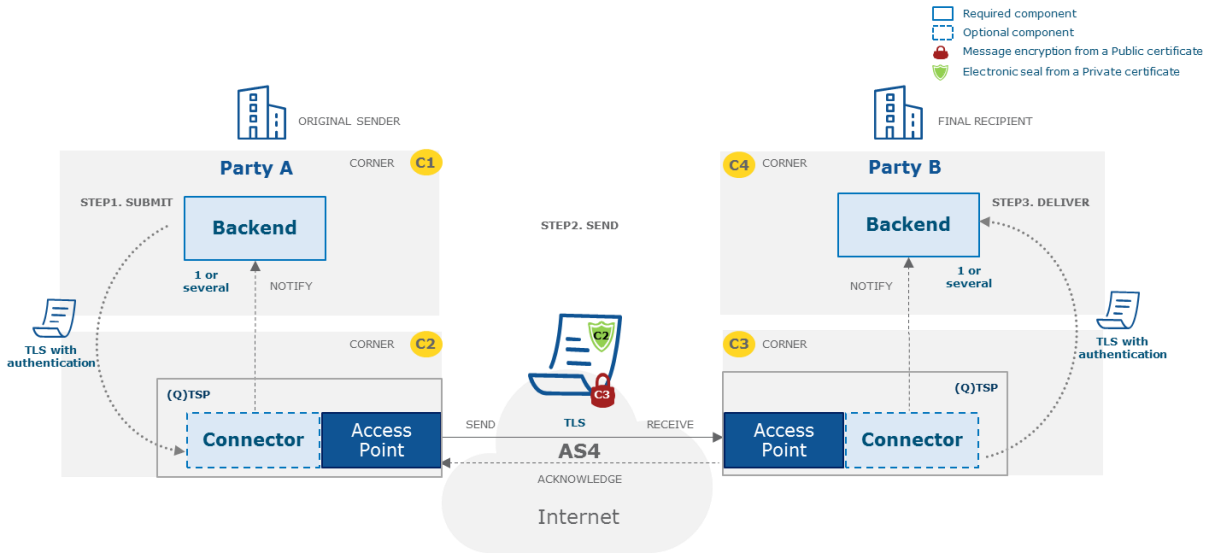

図10。 4コーナーモデルでのeDelivery委任シナリオ（つまり、デフォルトシナリオ）

このシナリオを実装するには、C2はメッセージを封印する前にC1を認証する必要があります。表10に示すように、eDeliveryビルディングブロックによって提供される既存のセキュリティ制御に加えて、TLSプロトコルをC1-C2とC3-C4の間に実装する必要があります。C1からC4への認証は、C2 –C3によって提供される信頼できるサービスによって実行されます。

メッセージはC2によって封印されているため、電子封印に関連する法的意味（表12）は、C2を操作する法人に関連しています。

注意：このケースには、セキュリティへの影響がいくつか含まれています。TLSはC1とC2の間の転送中のメッセージを保護しますが、メッセージがC2によって保存および処理されるときは保護しないため、処理中にメッセージが改ざんされるリスクを軽減するために、C2を運用する組織が追加の組織および技術的対策を講じる必要がありますその環境で。さらに、（Q）TSPアクセスポイントは、特定のPKIまたは相互信頼を介して、たとえば信頼リストを使用するなど、同じ信頼モデルの下で行う必要があります。このシナリオに関連する法的側面は、C1とC2を運営する組織間で契約上処理する必要があります。

I.3.2。E XTENDED DELEGATION SCENARIO

委任シナリオと同様に、このシナリオは、図11に示すように、ビジネスエンティティ（元の送信者C1）がメッセージ処理を通信パートナー（C2）に委任するときに発生します。ただし、この特定のシナリオでは、C2はデジタルも保存および保持します。 C1の証明書と関連する秘密鍵。したがって、これを使用してメッセージを電子的に封印します。このようにして、C1は、受信側によるメッセージの処理、転送、および保存中に、元の送信者として識別できます。このシナリオは、C1とC2が同じ組織および法人に属している場合に、最終的にはより適切になります。いずれにせよ、このシナリオに関連する法的側面は、C1とC2を運営する組織間で契約上処理する必要があります。

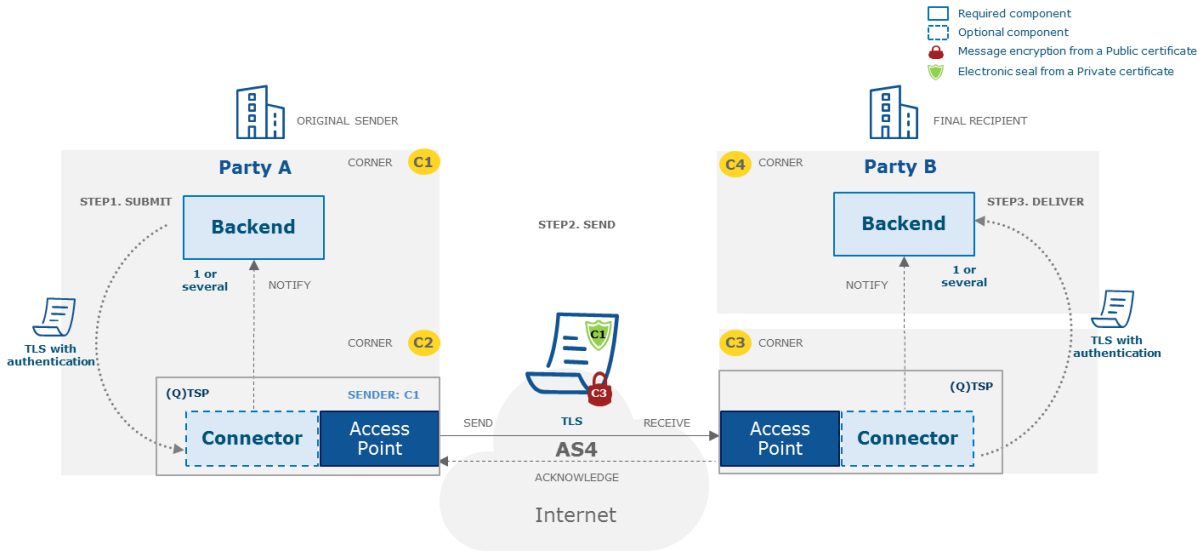

図11。 4コーナーモデルでのeDelivery拡張委任シナリオ

メッセージはC2によってC1として封印されるため、電子封印に関連する法的意味（表12）は、C1を操作する法人に関連しています。

注意。 このケースには、セキュリティへの影響が含まれています。C2はC1のデジタル証明書を保持しているため、C2がメッセージを改ざんするリスクを軽減するために、C1を運用している組織が追加の組織および技術的対策を講じる必要があります。実際、メッセージはC1のデジタル証明書を使用してC2によって封印されているため、このようなシナリオの法的影響は、C1とC2の間の契約上の合意によって対処する必要があります。 **このシナリオは、C1とC2が同じ組織および法人である場合に適しています。**

I.3.3。E XTENDED SECURITY SCENARIO

特定のビジネスニーズとセキュリティポリシーに応じて、バックエンドシステムを担当する組織は、さまざまな構成を実行し、追加のセキュリティ制御を実装できます。このシナリオ（図12に示されている）は、C1とC4が機密性の高いデータを交換し、必要なセキュリティ手段と機能を備えている場合に適しています。

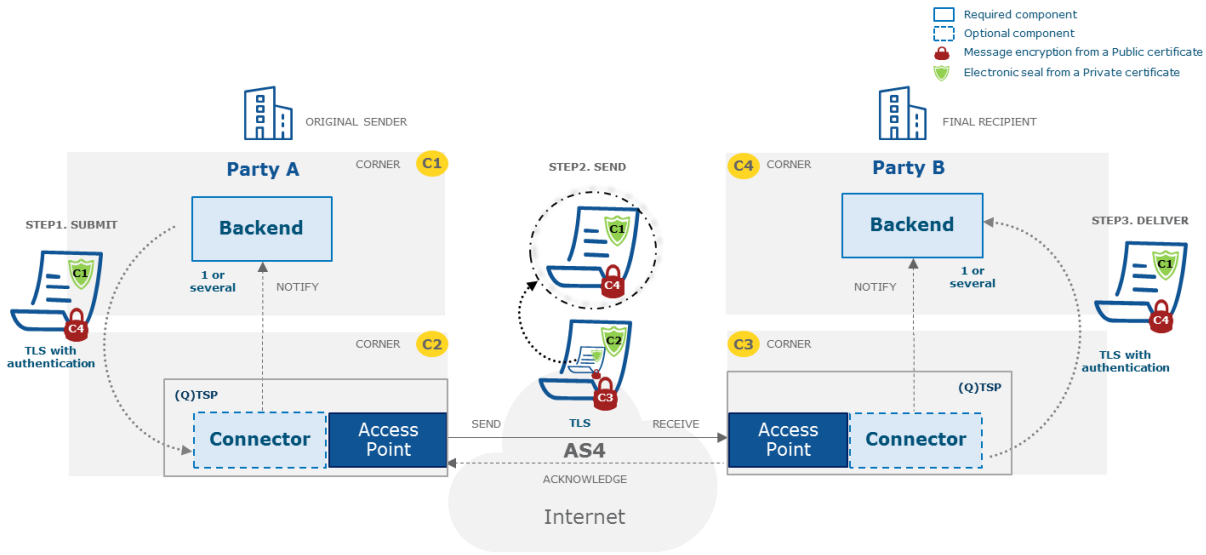

図12。 4コーナーモデルでのeDelivery拡張セキュリティシナリオ

このシナリオでは、C1とC4が技術的および法的責任を負い、適切なセキュリティ制御を実装して、さまざまなドメインのセキュリティを保証します。たとえば、図12に示すように、元の送信者（C1）は、電子シールまたは署名をメッセージに適用することを選択できます。これにより、最終的な受信者（C4）は、C1の公開デジタル証明書を使用してメッセージを検証できます。さらに、C1は（C4の公開デジタル証明書を使用して）メッセージを暗号化して、C1からC4へのメッセージの機密性を高め、セキュリティの層を追加することができます。どちらの場合も、C1とC4は、交換されたメッセージを正しく検証および暗号化するために相互にデジタル証明書を交換する必要があり、同じ信頼モデル（特定のPKI、信頼リスト、または相互信頼）の下にあります。通常、このシナリオに従う組織は、機密情報、場合によっては機密情報を交換する前に、必要なセキュリティ規定に同意し、メッセージのセキュリティを完全に制御する必要があります。このシナリオに関連する法的側面は、C1とC2を運営する組織間で契約上処理する必要があります。

エンドツーエンドドメインでこのシナリオに適用した場合のセキュリティ管理策の技術的および法的意味を表10にまとめています。

注意。 通信組織は信頼を確立し、メッセージの検証と暗号化に必要な安全なデジタル証明書交換を実行する必要があるため、このケースにはセキュリティへの影響が含まれています。さまざまな信頼モデルを使用して、信頼リストの使用や特定のPKIを介した、デジタル証明書の安全で信頼できる相互交換を保証できます。また、これらの組織は、eIDAS規制に準拠するかどうかについて全責任を負います。

表12。 エンドツーエンド（および内部）でのセキュリティ管理の技術的および法的意味 **S** 元の送信者（C1）と最終受信者（C4）の間の正確なドメイン

セキュリティ管理	説明	要件	含意	
			テクニカル	法的
CTR1：トランスポート層セキュリティ（TLS）と認証 *C1からC2へ（およびC3からC4）*	ENISAセキュリティ[9]およびBSI [10]ガイドラインに従ったトランスポート層セキュリティ（TLS 1.2 [11]）プロトコルは、C1とC2の間のメッセージの送信を保護します。送信者（C1）の識別については、組織は次の2つのオプションを選択できます（同じことがC4ー C3にも当てはまります） • *相互認証：* これは、C1のデジタル証明書（TLS / SSL証明書）を使用して行われ、C2がC1を識別できるようにします。認定ステータスの場合は、認定証明書を使用する必要があります。 • *基本認証：* C1は、たとえば、ユーザー名とパスワードの組み合わせを使用して、IDC2を認証します。この場合、安全なストレージ、十分な複雑さ、定期的な更新など、適切なパスワード管理をC1で保証する必要があります。ために	REQ1：メッセージ誠実さ	C1からC2、およびC3からC4に送信されるメッセージの信頼性。	適用可能な場合は、欧州の一般データ保護規則（GDPR）。
		REQ2：メッセージ守秘義務	C1からC2、およびC3からC4に送信されるメッセージの機密性。	
		REQ3：送信者識別	送信者（C1）は、Webサイト認証証明書（マシンツーマシンまたはTSL / SSL証明書）を使用してC2によって識別されるか、メッセージ送信の前に基本認証によって識別されます。C3およびC4についても同様です。	
		REQ4：宛先識別	宛先（C4）は、メッセージ送信の前にWebサイト認証証明書（マシン間またはTSL / SSL証明書）を使用してC3によって識別されます。	
CTR2：メッセージ暗号化 *C1とC4から*	のために *拡張セキュリティシナリオ：* 元の送信者C1は、メッセージのペイロードをREQ2に暗号化します。メッセージの最終受信者C4は、ENISAセキュリティ[9]およびBSIに従う必要がある暗号化メカニズムを使用します。 [10]ガイドラインeIDおよびTSPのENISA標準化。	守秘義務	メッセージペイロードは、最終受信者C4の元の送信者C1によって暗号化されます。これにより、メッセージの送信、保存、および処理中に、最終受信者C4のみがメッセージを開くことができることが保証されます。したがって、アクセス権のないコンポーネント（C2やC3など）は開くことができません メッセージのペイロードを読み取ります。	適用可能な場合は、欧州の一般データ保護規則（GDPR）。
CTR3：電子シールメッセージの *C1による*	のために *拡張セキュリティシナリオ：* メッセージには電子シールを貼付する必要があります。元のREQ1：メッセージ送信者C1は、デジタルを使用してメッセージヘッダーとペイロードに電子シールを適用する必要があります 法人に発行された証明書。次に、メッセージペイロードとヘッダーの信頼性と否認防止のためにC1の公開鍵を使用して、C2、C3、およびC4によってシールを検証できます。 電子シールアルゴリズムと暗号スイートは、ENISAセキュリティ[9]およびBSI [10]のガイドラインに従う必要があります。高度なシールの推奨規格は、eIDおよびTSPのENISA標準化[11]に記載されており、ETSI TR 119 000 [14]に従います。	誠実さ	メッセージのペイロードとヘッダーは電子的に封印されています。これにより、最終受信者（C4）およびその他のコンポーネント（C2またはC3）は、メッセージのペイロードとヘッダーが改ざんされておらず、メッセージの元の送信者がC1であることを確認できます。メッセージには電子シールが貼られているので、いつでも確認できます。したがって、電子シールは、メッセージの送信、保存、および処理中に、送信者としてのC1の信頼性を保証します。	**不適格：** データの整合性と出所を保証します。 言い換えれば、データの認証 **認定済み：** eIDAS規則、第35条。「認定された電子シールは、データの完全性と、認定された電子シールがリンクされているデータの出所の正確性の推定を享受するものとします。」 **両方とも：** 訴訟手続きにおける無差別
		REQ3：送信者識別		
CTR6：電子署名 *C1による*	のために *拡張セキュリティシナリオ：* 電子署名はC1を自然人と見なします 個人のデジタル証明書を使用してメッセージに電子的に署名します。技術的にはElectronicIntegrityシールと同様ですが、これには、法人ではなく自然人に発行されるデジタル証明書を使用する必要があります（ElectronicSeal）。したがって、これはC1によるメッセージに適用する必要があります。高度なシールの推奨規格は、eIDおよびTSPのENISA標準化[11]に記載されており、ETSI TR 119 000 [14]に従います。	REQ1：メッセージ	技術的な観点からは、CTR3と同じ効果：メッセージの電子シール。	**不適格：** 自然人が署名するために使用します。言い換えれば、明示的な同意（または署名が特定のトランザクションに対して持つ可能性のあるその他の機能的同等性） **認定済み：** eIDAS規則、第25条。「適格な電子署名は、手書きの署名と同等の法的効力を有するものとします」 **両方とも：** 訴訟手続きにおける無差別
		REQ3：送信者識別		
CTR5：電子時間切手（認定済み） *C1による*	のために *拡張セキュリティシナリオ：* 修飾された電子タイムスタンプは、元の送信者C1がメッセージを送信した瞬間、および最後の受信者C4がメッセージの時間参照に電子シールを適用することにより、メッセージを取得した時点で作成する必要があります。デフォルトシナリオでREQ5を満たすための推奨設定：C2は（修飾された）タイムスタンプを使用して送信時間を証明します。C2とC3が（Q）TSPである場合、C3はレシートに（修飾された）タイムスタンプを使用します。 電子タイムスタンプアルゴリズムは、ENISAセキュリティ[9]およびBSI [10]のガイドラインに従う必要があります。高度なシールに関するその他の推奨規格は、eIDおよびTSPのENISA標準化[11]に記載されており、ETSI TR 119 000 [14]に従います。	REQ5：時間参照	メッセージが特定の時間に作成、処理、および送信されたことをC1およびC4に保証します。	**不適格：** 特定の時間にデータの存在を確立します。つまり、データの日付と時刻を確認します。 **認定済み：** eIDAS規則、第41条。「適格な電子タイムスタンプは、それが示す日付と時刻の正確さ、および日付と時刻がバインドされているデータの整合性の推定を享受するものとします。」 **両方とも：** 訴訟手続きにおける無差別

付録II。 E IDAS 規制- R 必要条件

このセクションは2つの部分に分かれています。1つ目は、信託サービスプロバイダーに適用される一般規定に対応し、2つ目は、電子登録配信サービスに固有の要件に対応します。

eDeliveryを使用して適格または非適格の信頼サービスを提供することを意図しているサービスプロバイダーは、eIDAS規制によって義務付けられている要件の完全なリストに準拠する必要があります。適格信託サービスの開始の要件については、読者は規則の第21条を参照してください。

このセクションの残りの部分では、eDeliveryの範囲内でeIDAS規制に準拠する一般的な要件の概要を示します。

II.1。 G 一般規定

第5条（データ処理および保護）、パラグラフ1：

1.個人データの処理は、指令95/46 / ECに従って実行されるものとします。

注意： DIGITは、eDeliveryの情報ライフサイクルを文書化し、個人の処理が規則（EC）No 45/2001に準拠していることを確認することにより、データ保護とプライバシー分析を実行する必要があります。

eDeliveryメッセージングインフラストラクチャを使用する各サービスプロバイダーは、該当する法律に従ってデータ保護とプライバシー分析を実行する必要があります。出発点として、DIGITが提供するeDeliveryメッセージングの情報ライフサイクルを使用できます。

第12条（障害者のアクセシビリティ）

可能であれば、提供される信託サービスおよびそれらのサービスの提供に使用されるエンドユーザー製品は、障害者が利用できるようにするものとします。

リサイタル29

理事会決定2010/48 / EC（1）によって承認された障害者の権利に関する国連条約、特に条約の第9条に基づく義務に沿って、障害者は信託サービスを利用できるべきであり、これらのサービスの提供に他の消費者と平等に使用されるエンドユーザー製品。したがって、可能であれば、提供される信託サービスおよびそれらのサービスの提供に使用されるエンドユーザー製品は、障害者が利用できるようにする必要があります。実現可能性の評価には、とりわけ、技術的および経済的考慮事項を含める必要があります。

注意： いずれにせよ、eDeliveryアクセスポイントを実装するトラストサービスプロバイダーは、 *障害者の権利に関する国連条約。*

第13条（立証責任および立証責任）、パラグラフ2：

信託サービス提供者が提供するサービスの利用制限について事前にお客様に正式に通知し、第三者にその制限を認める場合、信託サービス提供者は、指定された制限を超えるサービスの利用により生じた損害について責任を負わないものとします。 。

注意： いずれにせよ、eDeliveryアクセスポイントを実装しているサービスプロバイダーは **単独で責任を負う**
サービスの使用に関する制限について顧客に通知するため。

第19条 (信託サービス提供者に適用されるセキュリティ要件)

適格および非適格の信託サービスプロバイダーは、提供する信託サービスのセキュリティにもたらされるリスクを管理するために、適切な技術的および組織的措置を講じるものとします。最新の技術開発を考慮して、これらの措置は、 ***セキュリティのレベルは、リスクの程度に見合ったものです。*** *特に、セキュリティインシデントの影響を防止および最小化し、そのようなインシデントの悪影響を利害関係者に通知するための対策を講じる必要があります。*

注意 ： 適切なセキュリティ対策を決定するために、サービスプロバイダーは、DIGITが提供するeDeliveryの情報セキュリティリスク評価を、提供するサービスの「全体的な」リスク評価の開始点として使用できます。

第24条 (資格のある信託サービス提供者の要件) 、パラグラフ2 次のアイテムを含みます：

適格な信託サービスを提供する適格な信託サービスプロバイダーは、以下を行うものとします。

e) 変更から保護され、それらによってサポートされるプロセスの技術的なセキュリティと信頼性を確保する、信頼できるシステムと製品を使用する。

f) 信頼できるシステムを使用して、提供されたデータを検証可能な形式で保存し、次のようにします。

a。それらは、データが関係する人の同意が得られた場合にのみ、検索のために公に利用可能です。

b。保存されたデータを入力および変更できるのは、許可された人だけです。

c。データの信頼性を確認できます。

g) データの偽造や盗難に対して適切な措置を講じます。

h) 資格のある信託サービスプロバイダーの活動が停止した後を含め、適切な期間、記録し、アクセス可能な状態を維持します。これには、特に法的証拠を提供する目的で、資格のある信託サービスプロバイダーが発行および受信したデータに関するすべての関連情報が含まれます。手続きおよびサービスの継続性を確保するため。このような記録は電子的に行うことができます。

注意 ： トラストサービスプロバイダーは、該当する法律で定義されている期間、これらの記録を保持する責任を単独で負います。

i) 指令95/46 / ECに従って個人データの合法的な処理を確保する。

II.2。R 電子登録配信に直接関連する要件

eIDAS規則では、電子登録配信を次のように定義しています。 *「電子的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明を含む、送信されたデータの処理に関連する証拠を提供し、送信されたデータを* ***紛失、盗難、損傷、または不正な変更のリスク*** 」（第3条（36））。

第44条（資格のある電子登録配達サービスの要件）：

a）それらは1つ以上の資格のある信託サービスプロバイダーによって提供されます。

注意 ：(適格）信託サービスプロバイダーは **単独で責任を負う** 資格のあるステータスを付与するためのすべての要件を確実に満たすため。

b）送信者の識別を高いレベルの信頼性で保証します。

注意： エンドユーザー **認証** 資格のある電子登録配達サービスのプロバイダーが対処する必要があります。

c）データを配信する前に、宛先を確実に識別します。

d） *データの送受信は、高度電子署名または*
データが検出できないほど変更される可能性を排除するような方法での、資格のある信託サービスプロバイダーの高度な電子シール。

注意： エンドツーエンドの信頼およびエンド参加者による署名の生成/検証は、資格のあるトラストサービスプロバイダーの責任であり、eDeliveryDSIの範囲外です。

e）データの送信または受信の目的で必要なデータの変更は、データの送信者および受信者に明確に示されます。

f）データの送信、受信、および変更の日時は、適格な電子タイムスタンプで示されます。

2つ以上の適格な信託サービスプロバイダー間でデータが転送される場合、ポイント（a）から（f）の要件は、すべての適格な信託サービスプロバイダーに適用されるものとします。」

IAS2プロジェクト、 二次立法へのインプットを提供するものは、プライバシー保護の機密性を強調します。

「特に行動や好みを開示する可能性のある取引関連情報の販売および再販売に関して、プライバシーに配慮した情報の処理に注意を払う必要があります」

付録III。 E- SENS C OMPARISONマッピング

次の表（表13）は、e-SENS AS4の機能と制御の間の、このドキュメントに示されているERDS要件とセキュリティ制御へのマッピングをまとめたものです。

表13。 ERDS要件とセキュリティ制御を使用したe-SENSAS4プロファイル機能のマッピング

機能性	e-SENSAS4プロファイル	セキュリティ管理	ERDS要件
トランスポート層の整合性、送信者認証、レシーバー認証とメッセージ守秘義務（非持続的）	• トランスポート層（SSL / TLS）セキュリティ	• 基本認証または相互認証を使用したTLS（CTR1）	• メッセージの整合性（REQ1） • メッセージの機密性（REQ2） • 送信者識別（REQ3） • 宛先の識別（REQ4）
メッセージの識別	• ebMS3 MessageId	• 電子シール（CTR3） • 電子署名（CTR5） • 電子タイムスタンプ（CTR5）	• メッセージの整合性（REQ1）
メッセージの相関関係	• ebMS3 RefToMessageIdおよびConversationId	• NA	• NA
メッセージのタイムスタンプ	• ebMS3タイムスタンプとWS-Security タイムスタンプ	• 電子タイムスタンプ（CTR5）	• 時間参照（REQ5）
パーティの識別	• ebMS3.0の「From」および「To」パーティ識別子。	• 電子シール（CTR3） • 電子署名（CTR6）	• 宛先の識別（REQ4）
否認防止	• WS-Security1.1を使用XML署名	• 電子シール（CTR3） • 電子署名（CTR6） • 電子タイムスタンプ（CTR5）	• メッセージの整合性（REQ1） • 送受信の証明（REQ6）
メッセージの機密性	• WS-Security1.1を使用XML暗号化	• TLS（CTR1） • メッセージの暗号化（CTR2）	• メッセージの機密性（REQ2）
否認防止領収書	• 署名されたレシート信号メッセージ	• 電子シール（CTR3） • 電子署名（CTR6） • 電子タイムスタンプ（CTR5）	• メッセージの整合性（REQ1） • 送受信の証明（REQ6）
信頼できるメッセージ	• AS4レセプションの認識機能軽量、相互運用可能な信頼性メッセージング	• 電子シール（CTR3） • 電子署名（CTR6） • 電子タイムスタンプ（CTR5）	• メッセージの整合性（REQ1） • 送受信の証明（REQ6）