資料10－2

FUJITSU
shaping tomorrow with you

欧州におけるeシール用証明書を発行する認証局の設備の基準、秘密鍵の保護環境

2021年3月5日
富士通株式会社

目次

- EUにおける認証局側の設備（HSM）の基準
- EUにおけるユーザ側のeシール生成装置の基準
- EUにおける設備の管理に係る基準
- まとめ
- 欧州におけるTSPのセキュリティ要件及びQTSPの要件[参考資料]

EUにおける認証局側の設備（HSM）の基準

FUJITSU

- EN319 411-1,2では以下の通り規定されている。

eシールのレベル	ポリシーレベル	設備(HSM)の基準	コメント
適格eシール	QCP-l-qscd	TSPの鍵ペア生成は、以下のいずれかに該当する信頼できるシステムである安全な暗号化装置で行うこと。 a) ETSI EN319 411-1を満たすST或いはPPを前提とし、**ISO/IEC 15408、または同等の国内または国際的に認められた IT セキュリティの評価基準によって EAL4以上**であると保証されている。あるいは b)**ISO/IEC 19790又はFIPS PUB 140-2 レベル3** で示されている要件を満たしている。 *ISO/IEC 15408を満たすデバイスが一般的に利用可能になることで、ISO/IEC 19790やFIPS 140-2レベル3はもはや受け入れられなくなると予期されている。	ポリシーレベルによるHSMの基準に違いはないが、第三者監査が義務づけられているのはQCP-l, QCP-l-qscdだけであり、その他の先進eシールについては任意での確認となる。 欧州では、FIPS PUB 140-2からISO/IEC 15408（コモンクライテリア）評価／認証取得製品への移行を促している。
先進eシール	QCP-l, NCP+, NCP		
	LCP		

EUにおけるユーザ側のeシール生成装置の基準

FUJITSU

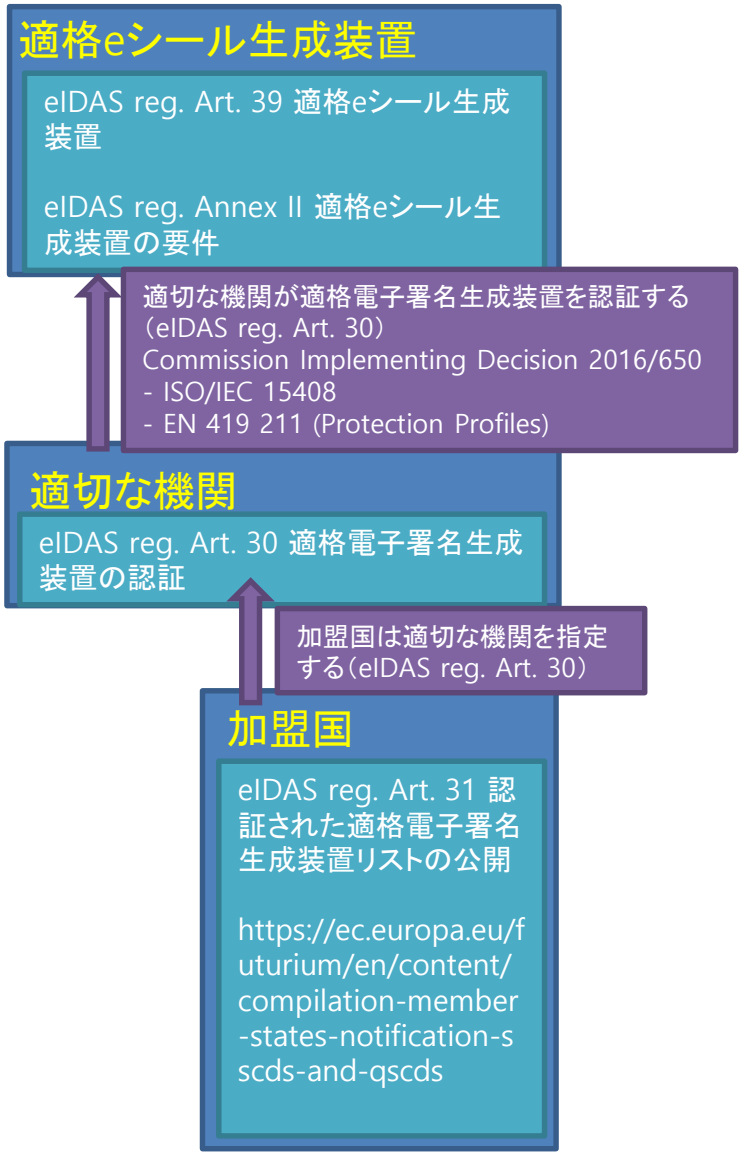
eシールのレベル	ポリシーレベル	生成装置の基準	加入者（法人）に対する秘密鍵の管理要求	コメント
適格eシール	QCP-l-qscd	TSPが準備した装置であるか否かにかかわらず、その装置が**QSCD**として認証されていることを検証すること。	（NCP,LCPの要件に加えて）TSPはデジタル署名が**QSCDによってのみ生成**され、**秘密鍵が法人の管理の下使用され、且つeシールの為のみに使用されることを義務付け**ること。	委員会実施決定2016/650によってQSCDの評価／認証方法についてはISO/IEC15408（コモンクライテリア）評価及びプロテクションプロファイルが採用されている。 加盟国は認証取得QSCDについてリストを公開している。 https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds
先進eシール	QCP-l	-	（NCP,LCPの要件に加えて）TSPは**秘密鍵が法人の管理の下使用され、且つeシールの為のみに使用されることを義務付け**ること。	-
	NCP+	安全な暗号装置の使用。 -安全な発行（準備、保管、配送） -安全なディアクティベーション及びアクティベーション -アクティベーションデータは安全に準備と配送	（NCP,LCPの要件に加えて）TSPは秘密鍵を、安全な暗号化装置内でのみ使用することを義務付けること。	安全な暗号装置に関する明確な基準は無いものの、第三者監査の観点ではコモンクライテリア認証取得製品の利用及び、ガイダンスに従った運用によって、安全な発行が確認されている。
	NCP、LCP	-	使用制限内での秘密鍵の利用、秘密鍵の不正使用禁止、危殆化及び変更に関する通知等	-

eIDAS規則における適格性認定が必要なポリシー

法的要件を除いたベストプラクティス

（参考）ISO/IEC 15408 コモンクライテリア

［第6回検討会 コスモス・コーポレイション提出資料より内容抜粋］



- ISO/IEC 15408 コモンクライテリア

IT製品やシステムがセキュリティの観点で適切に設計され、正しく実装されていることを評価する為の国際規格。

セキュリティ評価のフレームワークであり、満たさなければならないセキュリティ要件そのものは規定していない。
世界20か国以上の政府調達基準として採用されている。

- プロテクションプロファイル

IT製品やシステムが満たすべき要求仕様を調達者の視点で定めたもの。

- 評価保証レベル（EAL）

セキュリティ保証要件のパッケージであり、EAL1～7の7段階ある。
保証要件＝実際の評価作業

https://www.ipa.go.jp/security/jisec/cc/documents/CCPART3V3.1R5-J1.0.pdf

（参考）ISO/IEC 15408 コモンクライテリア

［第6回検討会 コスモス・コーポレイション提出資料より内容抜粋］

適格eシール生成装置

eIDAS reg. Art. 39 適格eシール生成装置

eIDAS reg. Annex II 適格eシール生成装置の要件

適切な機関が適格電子署名生成装置を認証する（eIDAS reg. Art. 30）
Commission Implementing Decision 2016/650
- ISO/IEC 15408
- EN 419 211 (Protection Profiles)

適切な機関

eIDAS reg. Art. 30 適格電子署名生成装置の認証

加盟国は適切な機関を指定する（eIDAS reg. Art. 30）

加盟国

eIDAS reg. Art. 31 認証された適格電子署名生成装置リストの公開

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

EN 419 211 プロテクションプロファイル
EAL4+(AVA_VAN.5, ALC_DVS.2)

保証クラス	保証ファミリ	評価保証レベル別の保証コンポーネント						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
開発	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
ガイダンス文書	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
ライフサイクルサポート	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
セキュリティターゲット評価	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
テスト	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
脆弱性評定	AVA_VAN	1	2	2	3	4	5	5

https://www.ipa.go.jp/security/jisec/cc/documents/CCPART3V3.1R5-J1.0.pdf

EUにおける設備の管理に係る基準

- EN 319 401, 411-1,2の要求範囲は以下の通り規定されている。

EN 319 401

大項目	中項目	小項目
リスクアセスメント	-	-
ポリシー及び運用	トラストサービス運用規定	
	契約条件	
	情報セキュリティポリシー	
TSP の管理及び運営	内部組織	組織の信頼性、職務分掌
	人的資源	
	資産管理	一般要件、メディアの取り扱い
	アクセスコントロール	
	暗号管理	
	物理的セキュリティ及び環境セキュリティ	
	運用セキュリティ	
	ネットワークセキュリティ	
	インシデント管理	
	証拠の収集	
	事業継続マネジメント	
	TSPの終了及び終了計画	
	コンプライアンス	

EN 319 411-1,2

大項目	中項目	小項目
-	-	-
CP, CPSに関する一般規定	CPSの要件	
	証明書ポリシーの名称及び識別	
	PKIの関係者	認証局、加入者及びサブジェクト、その他
	証明書の使用	
TSP の運用	公開及び保管の責任	
	識別及び認証	ネーミング、初回身元確認、リキーの識別と認証、失効リクエストの識別と認証
	証明書のライフサイクル運用要件	証明書申請、申請プロセス、証明書発行、証明書の受領、鍵ペア及び証明書の使用、証明書更新、リキー、証明書の変更, 失効及び停止、証明書ステータスサービス、加入の終了、鍵供託及び回復
	施設、管理、及び運用管理	**一般、物理セキュリティ管理、手順管理、人員管理、監査ログ、記録の保管、鍵の切り替え、危殆化及び災害復旧、認証局又は登録局の業務停止**
	技術的セキュリティ管理策	**鍵ペアの生成及び組み込み、秘密鍵の保護及び暗号モジュールの技術管理、鍵ペア管理のその他の側面、アクティベーションデータ、コンピュータセキュリティ管理、ライフサイクルセキュリティ管理、ネットワークセキュリティ管理、タイムスタンプ**
	証明書、CRL及びOCSPプロファイル	証明書プロファイル、CRLプロファイル、OCSPプロファイル
	適合性の監査及びその他の評価	
	その他の事業及び法的事項	料金、財政的責任、事業情報の機密性、個人情報のプライバシー、知的財産権、表明と保証、保証の拒否、責任の制限、賠償、有効期間及び解除、個別通知及び関係者との連絡、、改正、紛争処理手続き、準拠法、適用法、雑則
	その他の規定	組織的規定
		追加試験
		障害
		条件

まとめ

- 認証局側のHSMは現状FIPS140-2のレベル3も認められているが、将来的にはISO/IEC15408評価/認証取得製品を採用する方向にシフト
- QSCDもISO/IEC15408ベースの評価がされるが、CC認証とは別の加盟国による認証が必要
- ユーザ環境における秘密鍵の管理規定については、法人内複数人での秘密鍵の使用を禁じる要求はなく、秘密鍵があくまでも法人の管理下であることを求めている。
- TSP、QTSP共にセキュリティ要件が課されているが、監督機関による事前監督の対象となっているのはQTSPだけである。
- eIDAS規則と技術基準（EN319 401,411-1,-2）の間の明確な紐づきとなる実施法令は未整備

［参考］欧州におけるTSPのセキュリティ要件

FUJITSU

eシールのレベル	eIDAS規則が求めるセキュリティ要件	コメント
適格eシール 先進eシール	第19条 トラストサービスプロバイダに適用されるセキュリティ要件 1.適格・非適格トラストサービスプロバイダは、自身が提供するトラストサービスのセキュリティを脅かすリスクを管理する技術的、組織的な適切な措置をとらなければならない。これらの措置は、最新の技術開発を考慮して、セキュリティレベルがリスクの度合いに対し適正であることを保証すること。特に、対策はセキュリティインシデントの影響を回避及び最小限に抑えるものであり、このようなインシデントの影響について関係者に情報を提供すること。 2.適格・非適格トラストサービスプロバイダは、提供するトラストサービスやそこで管理する個人情報に重大な影響を及ぼすセキュリティ違反や完全性の喪失が発生した場合、不当な遅延なく、それに気付いた時より24時間以内に、監督機関と、必要に応じて、情報セキュリティに関する管轄機関や情報保護機関等の関連機関に通知すること。 セキュリティ違反や完全性の喪失が、トラストサービスが提供された自然人または法人に不利に影響するであろう場合、トラストサービスプロバイダは、不当な遅延なく、セキュリティ違反又は完全性の喪失を自然人又は法人にも通知すること。 必要に応じて、特に二か国以上の加盟国に関係するセキュリティ違反や完全性の喪失が発生した場合には、通知された監督機関は関連する他加盟国の監督機関及び欧州ネットワーク・情報セキュリティ機関（ENISA）に報告すること。 4.委員会は、実施法令の手段により、: (a)1項で言及される手段を更に特定する；及び (b)2項の目的の為に適用する締め切りを含めた形式・手続きを定義する。 それらの実施法令は、第48条(2)に言及される検査手順に従って採用されること。	4項で示されている、TSPのセキュリティ要件に関する実施法令については現在のところ施行されておらず、ETSIの技術基準と本要件の間の明確な紐づきは、法律上与えられていない。 *実施法令とはeIDAS規則の法的要件を既存の技術基準の指定等によって特定する法令である。

［参考］欧州におけるQTSPの要件

eシールのレベル	eIDAS規則が求めるQTSPの要件	コメント
適格eシール	第24条 適格トラストサービスプロバイダの要件 **[証明書発行対象の身元確認]** 1. トラストサービスに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、適切な手段により国内法に従い、適格証明書が発行される自然人または法人のアイデンティティ及び、該当する場合はその属性を検証すること。 前述の小項にある情報は、適格トラストサービスプロバイダにより、直接又は国内法に従い委任された第三者により検証されること: (a)自然人又は法人の権限を与えられた代表者の物理的存在により;又は (b)遠隔で、適格証明書の発行に先立ち、電子識別手段の利用により、自然人又は法人の権限を与えられた代表者の物理的存在が保証され、保証レベル「十分(substantial)」又は「高(high)」に関する第8条に規定された要件を遵守する;又は (c)(a)、(b)に準拠して発行された適格電子署名又は、適格eシールの証明書の手段により;又は (d)物理的存在を同等に保証する国家レベルで認められたその他識別方法を使用して、同等の保証は、適合性評価機関により確認される必要がある。 それらの実施法令は、第48条(2)に言及される検査手順に従って採用されること。	第9回検討会で報告した身元確認に関する要件と同じである。 以下の4つの身元確認方法が求められている。 ①対面での身元確認 ②eIDによる身元確認 ③デジタル署名（適格電子署名或いは適格eシール） ④対面での身元確認と同等の方式と認められる方法

［参考］欧州におけるQTSPの要件

FUJITSU

eシールのレベル	eIDAS規則が求めるQTSPの要件	コメント
適格eシール	2. 適格トラストサービスを提供する適格トラストサービスプロバイダは以下を実施すること: (a)適格トラストサービスの提供におけるいかなる変更、及びこれらの行動の停止の意思を監督機関へ連絡する; (b)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規則に関する適切なトレーニングを受けたスタッフ、又は該当する場合は委託先を雇用し、欧州または国際的な基準に沿った管理手順を適用すること; (c)第13条による損害に対する責任のリスクに関して、国内法に従い、十分な財源の維持、及び/または適切な債務保険を取得する; (d)適格トラストサービスの利用を検討する人物に対し、契約締結前に、明確で包括的な方法で、そのサービスの使用の限度を含めた明確な条件を連絡する; (e)変更に対して保護された信頼できるシステムと製品を使用し、それらにサポートされるプロセスの技術的セキュリティと信頼性を保証する; (f)信頼できるシステムを利用して、以下が可能となるように提供されたデータを検証可能な形式で保管する: (i)情報が関係する人物の同意が得られる場合のみ検索の為に公的に利用可能である、 (ii)権限保持者のみが保管データへの入力及び変更が可能である、 (iii)データの真正性が確認可能である;	(a) QTSPのサービスの変更については監督機関への連絡が必要 (b) 要員の教育及び資格管理 (c) 損害保険と財源維持 (d) サービス利用者に対する責任限度の表示 (e) セキュリティ製品の利用 (f) データの保管、完全性保護及びアクセスコントロール

［参考］欧州におけるQTSPの要件

FUJITSU

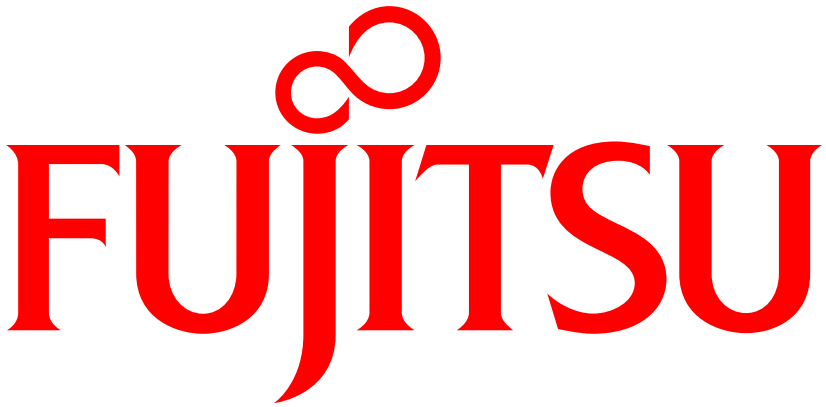
eシールのレベル	eIDAS規則が求めるQTSPの要件	コメント
適格eシール	2. 適格トラストサービスを提供する適格トラストサービスプロバイダは以下を実施すること: (g)データの偽造及び盗難に対して適切な処置を取る; (h)適格トラストサービスプロバイダにより発行または受信されるデータに関するすべての関連情報を、特に法的手続きの証拠提供とサービスの継続を保証する目的で、適格トラストサービスプロバイダが業務を停止した後を含めて、適切な期間、記録・アクセス可能にする。記録は電子的に行うことができる; (i)第17条(4)の(i)のもと、監督機関によって検証された規定に従ったサービスの継続を保証する為の最新の終了計画を持つ; (j)指令95/46/ECに従った個人情報の法的処理を保証する; (k)適格トラストサービスプロバイダが発行する適格証明書の場合、証明書データベースを確立、更新を続ける。	(g) データへのセキュリティ管理 (h) 記録の保管及び証拠の提供 (i)廃業に関する規定 (j)指令95/46/ECはGDPRによって上書きされており、GDPRに従った個人情報の扱いが求められている (k)証明書のデータベースの維持

［参考］欧州におけるQTSPの要件

FUJITSU

eシールのレベル	eIDAS規則が求めるQTSPの要件	コメント
適格eシール	3. 適格証明書を発行する適格トラストサービスプロバイダは、証明書を廃止することを決定した場合、適時、ただしいかなる場合も要求を受けてから24時間以内に、証明書の失効を証明書データベースに登録し、証明書の失効状況を公開すること。失効は、その公開と同時に有効となること。 4. 3項に関しては、適格証明書を発行する適格トラストサービスプロバイダは、発行する適格証明書の有効性、又は失効状況に関する情報をいかなる依拠当事者にも提供すること。この情報は、少なくとも証明書毎で、いつでも、信頼でき、無料で効果的な自動化された方法により、証明書の有効期間を越えて利用可能でなければならない。 5. 委員会は、実施法令の手段により、本条の2項 (e)、(f)の要件に準拠する信頼できるシステムと製品の基準の参照番号を確立することができる。本条で定められた要件に適合することは、信頼できるシステム及び製品がこれらの基準を満たしていることの推定となること。それらの実施法令は、第48条(2)に言及される検査手順に従って採用されること。	3. 失効要求から24時間以内の失効及びCRL等の更新 4. CRL、OCSP等による証明書ステータスの公開 5. 実施法令は定められていない

19条、24条の要件についてはそれぞれ19条4項及び24条5項において実施法令で特定の技術基準を指定することが示唆されているが、現在まで技術基準は指定されていない。EN 319 401及びEN 319411-1,2は欧州規格(European Norm)として発行されており各EU加盟国において国内標準として採用されており、実質的にこのEN 319 401及びEN 319 411-1及び2が、eIDAS規則24条への適合性を評価する為の技術基準となっている。



shaping tomorrow with you