※ 資料は 2023 年 1 月現在の文案に基づいており、外部要求の変更等を受けて文案をさらに更新する可能性があることをご了承ください。

GlobalSign
Certification Practice Statement
(認証業務運用規程)

本書は、GlobalSign Certification Practice Statement を日本語に翻訳したものであり、言語の違いにより、原文の意味合いを完全に訳することができない場合があります。英語の原本と本書の間で、解釈に不一致がある場合は、英語の原本が優先されます。

Date: March 2023

Version: v.9.1X

目次

修正履歴 8

前提確認事項 11

1. はじめに 12

1.1. 概要 13
1.1.1. 証明書名称 15
1.2. 文書名と識別 17
1.3. PKI における関係者 26
1.3.1. 認証局 26
1.3.2. 登録局(RA) 26
1.3.3. 利用者 28
1.3.4. 依拠当事者 28
1.3.5. その他の関係者 28
1.4. 証明書の使用方法 28
1.4.1. 適切な証明書の使用方法 29
1.4.2. 禁止されている証明書の用途 31
1.5. ポリシー管理 31
1.5.1. 文書を管理する組織 31
1.5.2. 問い合わせ窓口 32
1.5.3. CPS がポリシーに適合しているかを判断する担当者 32
1.5.4. CPS 承認手続き 32
1.6. 定義と略語 32

2. 公開とリポジトリの責任 39

2.1. リポジトリ 39
2.2. 証明書情報の公開 40
2.3. 公開の時期及び頻度 40
2.4. リポジトリへのアクセス管理 40

3. 識別と認証 41

3.1. 名称 41
3.1.1. 名称の種類 41
3.1.2. 意味のある名称である必要性 41
3.1.3. 利用者の匿名又は仮名の使用 41
3.1.4. 様々な形式の名称の解釈方法 41
3.1.5. 名前の一意性 41
3.1.6. 商標の認知、認証、役割 42
3.2. 初回の身元情報の十分性検証 42
3.2.1. 秘密鍵の所有を証明する方法 42
3.2.2. 組織の識別情報の認証 42
3.2.3. 個人の身元情報の認証 44
3.2.4. 検証されない利用者情報 48
3.2.5. 権限の十分性検証 49
3.2.6. 相互運用のための基準 50
3.2.7. ドメイン名の認証 50
3.2.8. IP アドレスの認証 51
3.2.9. 電子メールアドレスの認証 51
3.3. 鍵更新申請時における識別及び認証 51

3.3.1. 定期的な Re-key における識別及び認証 51
3.3.2. 失効後の Re-key における識別及び認証 52
3.4. 失効申請における識別及び認証 52

4. 証明書のライフサイクルに対する運用上の要求事項 52

4.1. 証明書申請 52
4.1.1. 証明書の申請者 52
4.1.2. 登録手続きとそこで負うべき責任 52
4.2. 証明書申請手続き 53
4.2.1. 識別及び認証の実施 53
4.2.2. 証明書申請の承認又は却下 53
4.2.3. 証明書の申請処理に要する期間 54
4.3. 証明書の発行 54
4.3.1. 証明書発行時における認証局の業務 54
4.3.2. 認証局から利用者への証明書の発行に関する通知 54
4.3.3. 利用者への NAESB 用証明書の発行に関する通知 54
4.4. 証明書の受領 54
4.4.1. 証明書の受領とみなされる行為 54
4.4.2. 認証局による証明書の公開 55
4.4.3. 認証局からその他のエンティティへの証明書の発行に関する通知 55
4.5. 鍵ペアと証明書の利用 55
4.5.1. 利用者による鍵ペアと証明書の利用 55
4.5.2. 依拠当事者による公開鍵と証明書の利用 55
4.6. 証明書の更新 55
4.6.1. 証明書更新の条件 56
4.6.2. 更新の申請者 56
4.6.3. 証明書更新申請の処理 56
4.6.4. 利用者への新しい証明書の発行に関する通知 56
4.6.5. 更新された証明書の受領とみなされる行為 56
4.6.6. 認証局による更新された証明書の公開 56
4.6.7. 認証局からその他のエンティティへの証明書の発行に関する通知 56
4.7. 証明書の RE-KEY 56
4.7.1. 証明書の Re-key の条件 56
4.7.2. 新しい公開鍵を含む証明書の申請者 56
4.7.3. 証明書 Re-key 申請の処理 56
4.7.4. 利用者への新しい証明書の発行に関する通知 56
4.7.5. Re-key された証明書の受領とみなされる行為 56
4.7.6. 認証局による Re-key された証明書の公開 56
4.7.7. 認証局からその他のエンティティへの証明書の発行に関する通知 57
4.8. 証明書記載情報の修正 57
4.8.1. 証明書記載情報の修正の条件 57
4.8.2. 証明書記載情報の修正の申請者 57
4.8.3. 証明書記載情報の修正申請の処理 57
4.8.4. 利用者への新しい証明書の発行に関する通知 57
4.8.5. 記載情報の修正された証明書の受領とみなされる行為 57
4.8.6. 認証局による記載情報の修正された証明書の公開 57
4.8.7. 認証局からその他のエンティティへの証明書の発行に関する通知 57
4.9. 証明書の失効、効力の一時停止 57
4.9.1. 失効の条件 57
4.9.2. 失効の申請者 59
4.9.3. 失効申請の処理手続き 59
4.9.4. 失効申請までの猶予期間 60
4.9.5. 認証局が失効申請を処理すべき期間 60

4.9.6. 失効情報確認に関する依拠当事者への要求事項 60
4.9.7. CRL の発行頻度 60
4.9.8. CRL の最大通信待機時間 61
4.9.9. オンラインでの失効情報の確認 61
4.9.10. オンラインでの失効情報の確認の要件 61
4.9.11. その他の方法による失効情報の提供 61
4.9.12. 認証局の鍵の危殆化に伴う特別な要件 61
4.9.13. 証明書の効力の一時停止を行う条件 62
4.9.14. 証明書の効力の一時停止の要求者 62
4.9.15. 証明書の効力の一時停止手続き 62
4.9.16. 証明書の効力の一時停止期限 62
4.10.証明書ステータス情報サービス 62
4.10.1. 運用上の特徴 62
4.10.2. サービスを利用できる時間 62
4.10.3. 運用上の特性 63
4.11.利用の終了 63
4.12.キーエスクローとリカバリー 63
4.12.1. キーエスクローとリカバリーのポリシーと手続き 63
4.12.2. 鍵カプセル化とリカバリーのポリシーと手続き 63

5. 施設、経営及び運用上の管理 63

5.1. 物理的管理 63
5.1.1. 所在地及び建物 63
5.1.2. 物理的アクセス 64
5.1.3. 電源及び空調 64
5.1.4. 水漏れ 64
5.1.5. 火災安全及び保護 64
5.1.6. メディア ストレージ(記憶媒体) 64
5.1.7. 廃棄処理 64
5.1.8. オフサイトバックアップ 64
5.2. 手続き的管理 64
5.2.1. 信頼された役割 64
5.2.2. タスク毎に必要な人員数 64
5.2.3. 各役割の識別及び認証 64
5.2.4. 職務分掌を要する役割 65
5.3. 人員コントロール 65
5.3.1. 資格、経験及び許可条件 65
5.3.2. バックグラウンドチェック手続き 65
5.3.3. 研修要件 65
5.3.4. 再研修の頻度及び条件 66
5.3.5. 職務のローテーション頻度及び条件 66
5.3.6. 不正行為に対する処罰 66
5.3.7. 個別契約者の要件 66
5.3.8. 個人に付与された文書について 66
5.4. 監査ログの手続き 66
5.4.1. 記録されるイベントの種類 66
5.4.2. ログ処理の頻度 67
5.4.3. 監査ログの保有期間 67
5.4.4. 監査ログの保護 67
5.4.5. 監査ログバックアップ手続き 67
5.4.6. 監査ログ収集システム 67
5.4.7. イベント発生要因の対象への通知 67
5.4.8. 脆弱性の評価 67

5.5. アーカイブ対象記録 68
5.5.1. アーカイブ対象記録の種類 68
5.5.2. アーカイブの保有期間 68
5.5.3. アーカイブの保護 68
5.5.4. アーカイブバックアップの手続き 68
5.5.5. データのタイムスタンプについての要件 68
5.5.6. アーカイブ収集システム(組織内又は組織外) 68
5.5.7. アーカイブ情報の取得と検証の手続き 68
5.6. 鍵交換 69
5.7. 危殆化及び災害からの復旧 69
5.7.1. インシデント及び危殆化に対する対応手続き 69
5.7.2. コンピューティング資産、ソフトウェア、又はデータが損壊した場合 69
5.7.3. 秘密鍵が危殆化した際の手続き 69
5.7.4. 失効ステータスの可用性 69
5.7.5. 災害後の事業継続能力 69
5.8. 認証局又は RA の稼動終了 70
5.8.1. 業務を引き継ぐ認証局 70

6. 技術的セキュリティ管理 70

6.1. 鍵ペア生成及びインストール 70
6.1.1. 鍵ペア生成 70
6.1.2. 利用者への秘密鍵配布 71
6.1.3. 証明書発行者へ公開鍵の配布 71
6.1.4. 認証局から依拠当事者への公開鍵配布 71
6.1.5. 鍵のサイズ 71
6.1.6. 公開鍵パラメーター生成及び品質検査 73
6.1.7. 鍵の使用目的(X.509 v3 鍵使用フィールドにおいて) 73
6.2. 秘密鍵保護及び暗号化モジュール技術管理 73
6.2.1. 暗号化モジュールの基準及び管理 73
6.2.2. 秘密鍵(m 中の n) 複数の人員による管理 73
6.2.3. 第三者への秘密鍵の預託 73
6.2.4. 秘密鍵のバックアップ 73
6.2.5. 秘密鍵のアーカイブ 73
6.2.6. 暗号モジュール間の秘密鍵移行 73
6.2.7. 暗号モジュールにおける秘密鍵の保存 74
6.2.8. 秘密鍵のアクティブ化方法 74
6.2.9. 秘密鍵の非アクティブ化方法 74
6.2.10. 秘密鍵の破棄方法 74
6.2.11. 暗号モジュール 評価 74
6.3. 鍵ペア管理におけるその他の側面 74
6.3.1. 公開鍵のアーカイブ 74
6.3.2. 証明書の操作可能期間及び鍵ペアの使用期間 74
6.4. アクティベーションデータ 75
6.4.1. アクティベーションデータの生成及びインストール 75
6.4.2. アクティベーションデータの保護 75
6.4.3. その他のアクティベーションデータの要素 75
6.5. コンピュータ セキュリティ コントロール 75
6.5.1. 特定のコンピュータ セキュリティ技術条件 75
6.5.2. コンピュータ セキュリティの評価 76
6.6. ライフサイクル 技術管理 76
6.6.1. システム開発管理 76
6.6.2. セキュリティ マネージメント コントロール 76
6.6.3. ライフサイクル セキュリティ コントロール 76

6.7. ネットワーク セキュリティ コントロール 76
6.8. タイムスタンプ 77
6.8.1. PDF 署名タイムスタンピングサービス 77
6.8.2. コードサイニング及び EV コードサイニングタイムスタンピングサービス 77

7. 証明書、CRL、及び OCSP のプロファイル 77

7.1 証明書プロファイル 77
7.1.1. バージョン番号 77
7.1.2. 証明書拡張 77
7.1.3. アルゴリズム識別子 77
7.1.4. 名前形式 77
7.1.5. 名前制約 78
7.1.6. 証明書ポリシー識別子 78
7.1.7. ポリシー制約拡張の使用 78
7.1.8. ポリシー修飾子の構文と意味 78
7.1.9. クリティカルな証明書ポリシー拡張についての解釈方法 78
7.1.10. シリアル番号 78
7.1.11. 適格証明書に関する特則 78
7.2 CRL プロファイル 79
7.2.1. バージョン番号 79
7.2.2. CRL 及び CRL エントリ拡張子 79
7.3 OCSP プロファイル 79
7.3.1. バージョン番号 79
7.3.2. OCSP 拡張 80

8. 準拠性監査及びその他の評価 80

8.1. 評価の頻度及び状況 80
8.2. 評価者の身元及び能力 80
8.3. 評価者と被評価者の関係 81
8.4. 評価対象項目 81
8.5. 結果が不備である場合の対応 81
8.6. 結果についての連絡 81
8.7. 自己監査 81

9. その他ビジネス及び法的事項 81

9.1. 料金 81
9.1.1. 証明書発行及び更新料金 81
9.1.2. 証明書アクセス料金 81
9.1.3. 失効情報アクセスに関する料金 82
9.1.4. その他サービスの料金 82
9.1.5. 返金ポリシー 82
9.2. 財務上の責任 82
9.2.1. 保険の適用範囲 82
9.2.2. その他資産 82
9.2.3. エンドエンティティに対する保険若しくは保証 82
9.3. 業務情報の機密性 82
9.3.1. 機密情報の範囲 82
9.3.2. 機密情報の範囲外に属する情報 82
9.3.3. 機密情報保護の責任 82
9.4. 個人情報保護 83
9.4.1. 保護計画 83
9.4.2. 個人情報として取り扱われる情報 83
9.4.3. 個人情報とみなされない情報 83
9.4.4. 個人情報保護の責任 83

9.4.5. 個人情報使用についての通知及び同意 83
9.4.6. 法的又は管理処理に従う開示 83
9.4.7. その他情報開示の場合 83
9.5. 知的財産権 83
9.6. 表明保証 83
9.6.1. 認証局の表明保証 83
9.6.2. 登録局(RA)の表明保証 85
9.6.3. 利用者の表明保証 86
9.6.4. 依拠当事者の表明保証 87
9.6.5. その他関係者の表明保証 88
9.7. 保証の免責事項 88
9.8. 責任制限 88
9.9. 補償 88
9.9.1. GlobalSign による補償 88
9.9.2. 利用者による補償 88
9.9.3. 依拠当事者による補償 88
9.10. 期間及び終了 89
9.10.1. 期間 89
9.10.2. 終了 89
9.10.3. 終了の効果と存続 89
9.11. 関係者への個別通知及び伝達 89
9.12. 改正条項 89
9.12.1. 改正手続き 89
9.12.2. 通知方法及び期間 89
9.12.3. OID(オブジェクト識別子)を変更しなければならない場合 89
9.13. 紛争解決に関する規定 89
9.14. 準拠法 90
9.15. 適用法の遵守 90
9.16. 雑則 90
9.16.1. 包括的合意 90
9.16.2. 譲渡 90
9.16.3. 分離条項 90
9.16.4. 執行 (弁護士費用及び権利放棄) 90
9.16.5. 不可抗力 91
9.17. その他の規定 91
9.17.1. CA チェーニング契約書 91
9.17.2. PKI 審査 91
9.17.3. 利用者 CA の導入 91
9.17.4. 継続的要件及び監査 92

修正履歴

Version	Release Date	Status & Description
V5.0 V5.5	10/07/05 19/06/07	Various changes leading up to a rewrite to support Extended Validation
V5.6	25/06/07	Final modification for EV Issue 1.0
V6.0	17/12/07	Major Release supporting new Certificate life cycle solutions
V6.1	20/05/08	Administrative update/ clarifications
V6.2	13/10/08	Administrative update/ clarifications
V6.3	16/12/08	Administrative update/ clarifications
V6.4	11/02/09	Administrative update/clarifications
V6.5	12/05/09	Administrative update/clarifications
V6.6	03/02/10	Administrative update
V6.7	12/05/10	Administrative update/clarifications
V7.0	22/03/12	Administrative update – Inclusion of additional WebTrust 2.0 and CA/B Forum Baseline Requirements for issuance of SSL Certificates
V7.1	29/03/12	Addition of support for NAESB and incorporation of the AlphaSSL product range
V7.2	07/06/12	Additional CA/B Forum Baseline Requirements
V7.3	01/07/12	Final CA/B Forum Baseline Requirements
V7.4	03/15/13	Extended validity period of Personal Sign, Administrative updates/clarifications Modification to NAESB Certificates incorporating WEQ-012 v 3.0 updates
V7.5	03/31/13	Statement of compliance to CA/Browser Forum Baseline Requirements, EPKI specification update
V7.6	03/07/14	Modified validity period for timestamping Certificate Added Certificate Data in the scope of archive Administrative updates/clarifications
V7.7	04/25/14	Modified availability requirement and maximum process time for revocation Administrative update/clarifications
V7.8	02/09/14	Modifications to enhance the description of domain validation processes, highlighted by public review.
V7.9	02/25/15	Modified maximum validity period of Code Signing certificate. GlobalSign's new R6 root and readability enhancements to cover new AATL offerings
V8.0	08/20/15	Support for IntranetSSL, Hosted Root™, alternative OIDs and Publication of all Subordinate CAs which are non-constrained.
V8.1	05/02/16	Annual Review Modified NAESB EIR requirements to reflect non WEQ energy participants requirements
V8.2	06/16/16	Adding R7 and R8 Root certificates
V8.3	08/11/16	Clarification on Certificate Transparency Adding Test CA OID
V8.4	01/17/17	CA/B Forum Ballot 173 Removal of Root R2 & R4 Addition of Minimum Requirements for Code Signing Certificates

V8.5	08/07/17	Updates for AATL Digital Signing Service Added CAA record checking requirement Annual update/review to fix bugs
V8.6	15/12/17	Updates related to Annual BR assessment
V8.7	03/04/18	Max SSL validity set to 825 days Specified that GlobalSign no longer generates keys for SSL certificates Updates for NAESB identify requirements
V8.8	06/15/18	Updates for Qualified Certificates Removed Method #5 to comply with BR domain validation practices.
V8.9	10/11/2018	Updates to revocation timelines in accordance with CABF Ballot SC6 Made a variety of definition/acronym updates for clarification
V9.0	03/12/19	Updated roles requiring separation of duties Added new ICAs for AATL and Timestamping Added new Email Domain Validation methods and definitions Added new Phone Domain Validation methods and definitions Added new IoT policy OIDs
V9.1	05/30/2019	Added new GlobalSign R46/E46 Root Certificates Added new Private Client Certificate Policy OID Support for Qualified Timestamping and Qualified Web Authentication Certificates Changed “re-key” definition to match WebTrust
V9.2	09/25/2019	Removed references to NAESB High Assurance certificates Removed “any other” method for IP Address approval
V9.3	03/31/2020	Added non-TLS roots Updated address in section 1.5 Added more detail to AATL Individual/Organization vetting requirements Added new Timestamping Token OID Added advanced electronic signature/seal (or higher) as an alternative means to confirm authority following COVID-19 emergency Added notification period for subscribers regarding expiration of certificates Added new CABF code signing requirements
V9.4	07/07/2020	Support for qualified certificates (non-QSCD) and QSCD managed by GlobalSign. Max SSL validity set to 397 days. Removed code signing certificates for individuals. Added hierarchy validation approach for eIDAS. Updates for uniqueness of Names.
V9.5	09/30/2020	Disclosure of Registration / Incorporating Agency. Added S/MIME and Client Authentication certificate products and OIDs. Added revocation at GlobalSign’s discretion. Updates to revocation reasons. Removal of Root R7, R8.
V9.6	12/29/2021	Updates for UK trust services Revision of revocation requirements

		Revision of OIDs Updates for ballots SC28, SC30, SC31, SC33 Grammatical updates, language consistency, RFCs Relying party liability for PSD2 certificates Root inclusion feedback Specification of KeyPurposeIds
V9.7	03/30/2021	Updates for UK trust services Clarification on max validity Including affiliated entities Added Timestamping Root E46 Revision of OIDs, including LRA OIDs Clarified non-verified subscriber information Grammatical updates, language consistency Updates to operational periods and key pair usage periods
V9.8	30/09/2021	Updates for ballots SC42, SC48 Clarification of reuse periods Added support for ACME domain validation method Added OID for UK eIDAS Qualified Timestamping Revised OID description for JCAN
V9.9	30/11/2021	Updates for ballot SC45 Revision of OIDs Update of Certificate and CRL validity Updates to Private Key management Grammatical updates, language consistency
V9.10	15/03/2022	Updates for Apple Root Program Updates for ballots SC51, CSC12 Revision of OIDs Updates to Qualified validation procedures Removed ExpiredCertsOnCrl extension for Qualified certificates Update of key management practices for Qualified certificates Clarification of operational and validity period Grammatical updates, language consistency
V9.11	30/08/2022	Updates for OU deprecation (ballot SC47) Updates for Mozilla Root Store Policy 2.8 Improved definition of certificate lifecycle events, including re-key, modification, renewal and re-issue Updates to CRL/OCSP sections for clarity and ETSI requirements Including video verification for a set of products Improved structure of domain, IP and email address validation and CAA validation. Grammatical updates, language consistency

前提確認事項

1. はじめに

本「Certificate Practice Statement (認証業務運用規程)」(以下、「本 CPS」という)は、GlobalSign NV/SA 及び関連会社(以下、「GlobalSign」という) が提供する製品及びサービスに適用する。本 CPS は、電子証明書の発行と、証明書の有効性チェックサービスを含むライフサイクル管理を主に取り扱う。また、GlobalSign は、タイムスタンプ等の追加サービスも提供する。本 CPS は、1.5 項「ポリシー管理」に規定する通り、適宜更新される。本 CPS の最新版は GlobalSign グループ会社のリポジトリ(https://www.globalsign.com/repository)に公開される。(依拠当事者及び利用者に対し CPS の理解を補助するために、本 CPS の翻訳が提供されることがある。但し、言語によって内容の不一致がある場合、英語版が適用・引用される。)

本 CPS は、「共通のセキュリティに関する要求事項を持つ特定の団体若しくはアプリケーション類にデジタル証明書を発行するための手続き」を定めるものである。本 CPS は 2003 年 11 月に Internet Engineering Task Force(以下、「IETF」という)が発行した RFC 3647 に定められた構成に従って記述する。(RFC 3647 の発行に伴い RFC 2527 は廃止されている。)この RFC は、電子署名と証明書の管理における標準的な業務手続きについて記述した公式の手引きである。本 CPS において、章・節などは RFC 3647 の構成に準拠して設けているが、そこで扱うべき内容が GlobalSign のサービスでは実装されていない事項に関するものである場合には、「規定なし」と記述している。RFC 3647 の書式に合わせることで、他のサードパーティ認証局との比較照合を可能にし、相互運用性を高める。また、証明書に記載された情報を信頼し依拠する者(以下、「依拠当事者」という)は、本 CPS を参照することで、認証業務手続きをあらかじめ知ることができる。

本 CPS は以下の要求事項に準拠することを目的とする。

- Browsers' root programs
- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003
- North American Energy Standards Board (NAESB) Accreditation Requirements for Authorized Certificate Authorities
- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security
- WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL
- WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements
- Regulation (EU) No 910/2014 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
- The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019)
- The Electronic Identification and Trust Services for Electronic Transactions Regulation 2016 (2016 No.696))
- JIPDEC Trusted Service Registration Requirements

本 CPS は、現時点における以下の外部要求事項に準拠する:

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (以下「Baseline Requirements」)
- CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (以下「EV ガイドライン」)
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/B Forum Baseline Requirements for Code Signing (以下「Baseline Requirements for Code Signing」)

http://www.cabforum.org で公開される。 本文書及び上記外部要求の間に不一致があった場合、外部要求事項が本文書に優先して適用される。

本 CPS は、GlobalSign が発行する証明書のライフサイクル期間中において GlobalSign が採用する技術、手続き、及び要員に関するポリシーを規定している。

本 CPS は、様々な種類の証明書を発行する GlobalSign への要求事項を記述しており、どのルート認証局にチェーニングされるかは中間証明書の選択、若しくはプラットフォームやクライアント側で使用される、又は提供されている相互認証証明書によって異なる。

本 CPS は、本 CPS に基づいて認証局が提供する認証サービスを利用する利用者、及び依拠し、又は依拠しようとする依拠当事者に適用される。

利用者については、利用契約(以下、利用約款による場合を含む)に同意することにより本 CPS が発効し、利用者を拘束する。依拠当事者については、本 CPS に基づき発行された証明書に依拠することにより、本 CPS が依拠当事者を拘束する。加えて、利用者は利用契約により、本 CPS が依拠当事者に効力を発することを依拠当事者に告知するよう求められている。

本 CPS は英文版を原本とする。英文原本の版及びその他の言語に訳された版の間にて内容に不一致がある場合、英文版の規定が優先適用される。

1.1. 概要

本 CPS は GlobalSign が発行する証明書階層全てに適用されるものであり、その目的は GlobalSign が採用する証明書管理の実務手続きを説明し、GlobalSign が規定する要件並びに上述の業界標準の要件の双方に準拠して電子証明書が発行されていることを証することである。eIDAS 規則 (Regulation (EU)N910/2014) (以下、「eIDAS」という) 及び eIDAS (英国の法律) と電子取引の電子識別及びトラストサービスに関する規則 2016 (以下、「UK eIDAS」という) は、認証及び否認防止の目的で使用される電子署名を承認した。これに基づき、GlobalSign はそのサービスの提供にあたり同法の適用される項の規定の範囲で業務を行っている。英国向けのトラストサービスは、GlobalSign の関連会社である GMO GlobalSign LTD.が運営し、同社を通じて提供される。

本 CPS の狙いは GlobalSign による認証サービスと中間 CA 証明書、クライアント証明書、サーバ証明書、その他の目的のためのエンドエンティティ証明書の証明書ライフサイクル管理を文書化することである。本 CPS が取り扱う証明書タイプは以下の通り。

PersonalSign 1	保証のレベルが低い個人向け証明書
PersonalSign 2	保証のレベルが中程度の個人向け証明書
PersonalSign 2 Pro	保証のレベルが中程度で、所属する職業・組織の情報を含む、個人向け証明書
PersonalSign 2 Pro DepartmentSign	保証のレベルが中程度で、所属する職業・組織の情報・役職の情報を含む、機械、デバイス、部署、又は役職向けの証明書
PersonalSign 3 Pro	保証のレベルが高く、所属する職業・組織の情報を含む、個人向け認証証明書
PersonalSign Partners	PersonalSign 2 Pro 又は PersonalSign 2 Pro DepartmentSign を発行するトラストアンカーとして構築されるプライベート認証局
IntranetSSL	パブリックな GlobalSign のルートにつながらない、ウェブサーバを認証する証明書
DomainSSL	ウェブサーバを認証する証明書
AlphaSSL	ウェブサーバを認証する証明書
OrganizationSSL & ICPEdu	ウェブサーバを認証する証明書
Extended Validation SSL [1]	ウェブサーバを認証する証明書
GlobalSign Timestamping	時刻情報の発行元を認証する証明書

[1] この証明書は EV ガイドライン及び Baseline Requirements for Code Signing に従って発行・管理される。その他の証明書については、CA/B Forum の Baseline Requirements に従って発行・管理され、その中でもし指定されていれば、1.2 項で詳述する通り、CA/B Forum ポリシーOID（識別子）を証明書内に記載する。

AATL	ハードウェアにインストールされ、Adobe AATL 及び Microsoft Office 文書に中程度の保証を提供する証明書
Code Signing [2]	データオブジェクトを認証する証明書
Extended Validation Code Signing[1]	データオブジェクトを認証する証明書
North American Energy Standard Board (NAESB) Authorized CA Certificates	北米エネルギー規格委員会の指定を受け権限を与えられた認証局が発行する、保証レベルが最小限、低、中何れかの、個人、役職、サーバ、又はデバイス向けの証明書
Hosted Root	GlobalSign が、ユーザの代わりにルート CA の秘密鍵及び証明書を維持、管理し、また、そのルートがルートストアに搭載される時まで相互認証証明書を提供するために用いるサービス。 当該ユーザはその期間内に当該ユーザの名前で WebTrust 監査を通すこととなる。
Qualified Certificates for Electronic Signatures	電子署名を提供するために用いられる、eIDAS/UK eIDAS に準拠する適格証明書
Qualified Certificates for Electronic Seals	e シールを提供するために用いられる、eIDAS/UK eIDAS に準拠する適格証明書
Qualified Web Authentication Certificates	Web 上での認証(SSL)に用いられる、eIDAS/UK eIDAS に準拠する適格証明書
Certificates for Qualified Timestamping	eIDAS に準拠する適格タイムスタンプに署名するために用いられる証明書
S/MIME	メールの正当性及び送信者を認証するための証明書
JCAN Certificates	JIPDEC トラステッド・サービス登録基準に従って発行される証明書

GlobalSign 証明書は、以下の何れの目的にも使用することができる。

- 取引の際、手書きの署名の代わりに電子署名を使用する
- サーバその他のデバイスを含むウェブリソースを認証する
- コード、文書その他のデータオブジェクトに電子的に署名する
- データを暗号化する

本 CPS では、GlobalSign の証明書のライフサイクル、使用、当該証明書への依拠、及び管理などに関与する全てのエンティティの役割、責任、実務を明らかにする。実務、サービスレベル、義務と責任を記述する本 CPS の条項は GlobalSign、GlobalSign 登録局(以下、「GlobalSign RA」という)、利用者、依拠当事者など関与する全てのエンティティに適用される。また条項によっては認証サービスプロバイダ、アプリケーションプロバイダなど、上述以外のエンティティにも適用される。

GlobalSign 証明書ポリシー(以下、「GlobalSign CP」という)は本 CPS を補完する。GlobalSign CP の目的は「順守すべきこと」を明らかにすることであり、そのために様々な GlobalSign の製品・サービスに関する業務ルールの枠組みを定めている。

本 CPS は「認証局が証明書ポリシーに準拠する方法」を定めており、GlobalSign がその証明書を生成し管理するにあたって採用するプロセス、手続き、条件などについて詳述し、エンドユーザにこの情報を提供する。また、GlobalSign CP、本 CPS の他に、以下のような事項に関する別のポリシー文書も規定している。

- 事業継続計画・災害復旧計画
- セキュリティポリシー
- 人的ポリシー
- 鍵管理ポリシー
- 登録手続き

[2] この証明書は Baseline Requirements for Code Signing に従って発行・管理される。

その他の関連文書には以下のものがある。

- GlobalSign から提供される保障に関する事項を取り扱う GlobalSign ワランティーポリシー
- 個人情報保護に関する GlobalSign プライバシーポリシー
- GlobalSign のルート証明書の信頼対象を取り扱う GlobalSign CP

GlobalSign の発行する証明書の利用者、依拠当事者は、GlobalSign が発行する証明書を信頼するため、また GlobalSign の活動について情報を得るために、本 CPS を参照すべきである。階層全体の証明書チェーンの信頼性を確認することも重要であり、これにはルート CA 証明書、その他のあらゆるオペレーショナル・ルートの証明書が含まれる。これらは、本 CPS における GlobalSign の表明に基づき、その信頼性が確認される。適格証明書については、関連する EU 又は UK eIDAS トラステッドリスト内に登録されている GlobalSign のトラストアンカーまでチェーンしているかどうか、証明書階層に対する十分性の検証を完遂しなければならない。

適用可能な GlobalSign の全てのポリシーは権限ある第三者から監査を受けており、これらのポリシーは WebTrust シールを付与した GlobalSign のウェブサイトで公開されている。追加情報は要求を受けて提供する。

1.1.1. 証明書名称

本 CPS に基づき管理される GlobalSign ルート CA 証明書の名称は以下の通り。

GlobalSign Public Root CA Certificates
GlobalSign Public Root CA Certificates

- GlobalSign Root CA – R1 with fingerprint EBD41040E4BB3EC742C9E381D31EF2A41A48B6685C96E7CEF3C1DF6CD4331C99
- GlobalSign Root CA – R3 with fingerprint CBB522D7B7F127AD6A0113865BDF1CD4102E7D0759AF635A7CF4720DC963C53B
- GlobalSign Root CA – R5 with fingerprint 179FBC148A3DD00FD24EA13458CC43BFA7F59C8182D783A513F6EBEC100C8924
- GlobalSign Root CA – R6 with fingerprint 2CABEAFE37D06CA22ABA7391C0033D25982952C453647349763A3AB5AD6CCF69
- GlobalSign Root CA – R46 with fingerprint 4FA3126D8D3A11D1C4855A4F807CBAD6CF919D3A5A88B03BEA2C6372D93C40C9
- GlobalSign Root CA – E46 with fingerprint CBB9C44D84B8043E1050EA31A69F514955D7BFD2E2C6B49301019AD61D9F5058

GlobalSign は、これらのルート証明書が、電子証明書に対応可能なハードウェア／ソフトウェアプラットフォーム及び関連暗号サービスへ搭載されるよう、積極的に働きかけを行っている。GlobalSignは、可能な場合にはプラットフォームプロバイダと契約を締結し、ルート証明書の効果的なライフサイクル管理を行っている。同時に、GlobalSign はプラットフォームプロバイダが自己の裁量により、契約上の義務を負わずに GlobalSing CA ルート証明書を搭載することも積極的に奨励している。尚、GlobalSign Root CA - R2 及び GlobalSign Root CA - R4 は GlobalSign の所有から外れた。

GlobalSign Public Non-TLS Root CA Certificates

- GlobalSign Client Authentication Root R45 with fingerprint 165C7E810BD37C1D57CE9849ACCD500E5CB01EEA37DC550DB07E598AAD2474A8
- GlobalSign Client Authentication Root E45 with fingerprint 8B0F0FAA2C00FE0532A8A54E7BC5FD139C1922C4F10F0B16E10FB8BE1A634964
- GlobalSign Code Signing Root R45 with fingerprint 7B9D553E1C92CB6E8803E137F4F287D4363757F5D44B37D52F9FCA22FB97DF86
- GlobalSign Code Signing Root E45 with fingerprint 26C6C5FD4928FD57A8A4C5724FDD279745869C60C338E262FFE901C31BD1DB2B
- GlobalSign Document Signing Root R45 with fingerprint 38BE6C7EEB4547D82B9287F243AF32A9DEEB5DC5C9A87A0056F938D91B456A5A
- GlobalSign Document Signing Root E45 with fingerprint F86973BDD0514735E10C1190D0345BF89C77E1C4ADBD3F65963B803FD3C9E1FF
- GlobalSign Secure Mail Root R45 with fingerprint 319AF0A7729E6F89269C131EA6A3A16FCD86389FDCAB3C47A4A675C161A3F974
- GlobalSign Secure Mail Root E45 with fingerprint 5CBF6FB81FD417EA4128CD6F8172A3C9402094F74AB2ED3A06B4405D04F30B19
- GlobalSign Timestamping Root R45 with fingerprint 2BCBBFD66282C680491C8CD7735FDBBAB7A8079B127BEC60C535976834399AF7
- GlobalSign Timestamping Root E46 with fingerprint 4774674B94B78F5CCBEF89FDDEBDABBD894A71B55576B8CC5E6876BA3EAB4538

- GlobalSign IoT Root R60 with fingerprint 319AF0A7729E6F89269C131EA6A3A16FCD86389FDCAB3C47A4A675C161A3F974
- GlobalSign IoT Root E60 with fingerprint 5CBF6FB81FD417EA4128CD6F8172A3C9402094F74AB2ED3A06B4405D04F30B19

上記のルート証明書は TLS 以外の用途に構築され、WebTrust の要求事項を基に監査を受けたパブリック証明書であり、GlobalSign の様々なサービス提供にかなうものとなっている。これらのルート証明書を、GlobalSign の使用事例及び該当する安全性の標準に倣い、証明書及び関連する暗号化サービスを支えるハードウェア及びソフトウェアのプラットフォームへ組み入れることを、GlobalSign は推奨している。ルート証明書のライフサイクル管理を効果的に行うことができるよう保証するため、可能であれば、GlobalSign はプラットフォームのプロバイダと契約・約款を締結する。しかし、GlobalSign はプラットフォームのプロバイダに対し、自由裁量にて契約上の義務なく GlobalSign のルート証明書を組み入れることも推奨している。

GlobalSign Non-public Root CA Certificates

- GlobalSign Non-Public Root CA – R1 with fingerprint 8D2EEFC79397F86BD4DB5B16A84144156D7EE352B57DE36B2C4FC738081DF9C9
- GlobalSign Non-Public Root CA – R2 with fingerprint 24FD17248F3B76F82AF2FD9C57D60F3EF60551508EE98DC460FD3A67866ECCEA
- GlobalSign Non-Public Root CA – R3 with fingerprint A3BB9A2462E728818A6D30548BD3950B8C8DAE1B63FC89FE66E10BB7BAB5725A
- GlobalSign Trusted Platform Module Root CA with fingerprint F27BF02C6E00C73D915EEB6A6A2F5FBF0C31AE0393149E6B5C31E41B113841C3
- GlobalSign Trusted Platform Module ECC Root CA with fingerprint 5A8C7B5EB888CFCE9322068E80E82B28B554FFEB7FDC9638DCB3763077401D26

1.1.1.1. 下位発行 CA 証明書の公表

ブラウザのルートプログラムは、(nameConstraints 及び拡張鍵用途への制約を通して)技術的に制約されていない全ての下位 CA が公表されることを要求している。パブリックルート証明書に直接的又は経由する形でチェーンする、現時点で利用されている全ての下位 CA 証明書を Common CA Database (CCADB)に列挙する。SHA1 の指数、有効期限、及びダウンロード及び点検を可能にするためのリンクも併記する。失効されずにいる全ての引退した CA 証明書は、適用されるルートプログラムで要求されているように、バグレポートや電子メールを介してルートプログラムに半年毎に報告される。失効した下位 CA 証明書も、同様に報告される。報告の時期は、定期的な失効の場合は失効から短期間のうち、セキュリティ上の懸念によって失効された場合は失効直後である。

Trusted Root とは GlobalSign のサービスで、第三者が保有する CA を中間 CA を介して GlobalSign ルート証明書の 1 つにチェーンできるようにすることである。Trusted Root のエンドエンティティ証明書は、当該第三者の CPS の対象となるため、本 CPS の適用範囲外とする。

TrustedRoot TPM とは、第三者が運用する発行 CA を上記の GlobalSign Trusted Platform Module のルート証明書の 1 つにチェーンさせるという、GlobalSign のサービスであり、当該サービスにおけるエンドエンティティ証明書は本 CPS の対象外である。

電子証明書により、エンティティは電子的取引の際、他の取引参加者に自己の身元を証明したり、データに電子的に署名したりすることができる。GlobalSign は、電子証明書を使用する利用者(サブジェクト)がその公開鍵を持つことを審査し確認する。電子証明書を受領するプロセスには、ユーザの識別、名前確認、認証、登録などと共に、電子証明書の発行、失効、有効期限満了といった証明書を管理するための手続きが含まれる。電子証明書の発行プロセスを通じて利用者が使用する公開鍵を限定することによって、証明書のユーザが本人であることを証明する。GlobalSign が提供する電子証明書は、否認防止、暗号化、認証に使用することができる。しかしながら、ワランティーポリシー又は証明書が使用されるアプリケーションの制約を受けて、証明書を特定のビジネス、契約、取引のレベルでのみ使用するよう限定されることがある。

1.2. 文書名と識別

本書は GlobalSign CPS である。

GlobalSign NV/SA(GlobalSign)のオブジェクト識別子(以下、「OID」という)は、ISO (1)、識別された組織 (3)、DoD (6)、インターネット (1)、民間 (4)、企業 (1)、GlobalSign (4146)である。
GlobalSign は本 CPS が対象とする様々な証明書、文書に対し、次の OID を付与する。

Category	OID	Description
TLS	**1.3.6.1.4.1.4146.10.1**	**TLS Policies Arc**
	1.3.6.1.4.1.4146.10.1.1	Extended Validation TLS Policy
	1.3.6.1.4.1.4146.10.1.2	Organization Validation TLS Policy
	1.3.6.1.4.1.4146.10.1.3	Domain Validation TLS Policy
Authentication	**1.3.6.1.4.1.4146.10.2**	**Authentication Policies Arc**
	1.3.6.1.4.1.4146.10.2.1	Extended Validation Auth Policy
	1.3.6.1.4.1.4146.10.2.2	Organization Validation Auth Policy
	1.3.6.1.4.1.4146.10.2.3	Domain Validation Auth Policy
	1.3.6.1.4.1.4146.10.2.4	Individual Validation Auth Policy
S/MIME	**1.3.6.1.4.1.4146.10.3**	**S/MIME Policies Arc**
	1.3.6.1.4.1.4146.10.3.1	Organization Validation S/MIME Policy
	1.3.6.1.4.1.4146.10.3.2	Sponsored Validation S/MIME Policy
	1.3.6.1.4.1.4146.10.3.3	Mailbox Validation S/MIME Policy
	1.3.6.1.4.1.4146.10.3.4	Individual Validation S/MIME Policy
	1.3.6.1.4.1.4146.1.40.70	Client Certificates Policy (Email Protection)

Category	OID	Description
Code Signing	**1.3.6.1.4.1.4146.10.4**	**Code Signing Policies Arc**
	1.3.6.1.4.1.4146.10.4.1	Extended Validation Code Signing Policy
	1.3.6.1.4.1.4146.10.4.2	Organization Validation Code Signing Policy
Document Signing	**1.3.6.1.4.1.4146.10.5**	**Document Signing Policies Arc**

Category	OID	Description	Private Key
Qualified	**1.3.6.1.4.1.4146.1.40.36**	**eIDAS Qualified Certificates - QSCD**	
	1.3.6.1.4.1.4146.1.40.36.1	Qualified Certificates for Electronic Signatures	Private key on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.36.2	Qualified Certificates for Electronic Seals	Private key on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.38	**eIDAS Qualified Certificates – Remote QSCD**	
	1.3.6.1.4.1.4146.1.40.38.1	Qualified Certificates for Electronic Signatures	Private key on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.40.38.2	Qualified Certificates for Electronic Seals	Private key on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.40.41	**eIDAS Qualified Certificates – Remote Non QSCD**	
	1.3.6.1.4.1.4146.1.40.41.1	Qualified Certificates for Electronic Signatures	Private key not on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.40.41.2	Qualified Certificates for Electronic Seals	Private key not on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.40.37	**eIDAS Qualified Certificates – Non QSCD**	
	1.3.6.1.4.1.4146.1.40.37.1	Qualified Certificates for Electronic Signatures	Private key not on QSCD

Category	OID	Description	Private Key
			Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.37.2	Qualified Certificates for Electronic Seals	Private key not on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.37.3	Qualified Certificates for Electronic Seals - PSD2	Private key not on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.40.40	**eIDAS Qualified Certificates for Website Authentication (QWAC)**	
	1.3.6.1.4.1.4146.1.40.40.1	Qualified Certificates for Website Authentication (QWAC)	
	1.3.6.1.4.1.4146.1.40.40.2	Qualified Certificates for Website Authentication (QWAC) – PSD2	
	1.3.6.1.4.1.4146.1.40.39	**Qualified Certificates for Authentication**	
	1.3.6.1.4.1.4146.1.40.39.1	Qualified Certificates for Authentication (Natural Persons)	
	1.3.6.1.4.1.4146.1.40.39.2	Qualified Certificates for Authentication (Legal Persons)	
	1.3.6.1.4.1.4146.1.44.36	**UK eIDAS Qualified Certificates – QSCD**	
	1.3.6.1.4.1.4146.1.44.36.1	Qualified Certificates for Electronic Signatures	Private key on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.44.36.2	Qualified Certificates for Electronic Seals	Private key on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.44.38	**UK eIDAS Qualified Certificates – Remote QSCD**	
	1.3.6.1.4.1.4146.1.44.38.1	Qualified Certificates for Electronic Signatures	Private key on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.44.38.2	Qualified Certificates for Electronic Seals	Private key on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.40.41	**UK eIDAS Qualified Certificates – Remote Non QSCD**	
	1.3.6.1.4.1.4146.1.40.41.1	Qualified Certificates for Electronic Signatures	Private key not on QSCD

Category	OID	Description	Private Key
			Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.40.41.2	Qualified Certificates for Electronic Seals	Private key not on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.44.37	**UK eIDAS Qualified Certificates – Non QSCD**	
	1.3.6.1.4.1.4146.1.44.37.1	Qualified Certificates for Electronic Signatures	Private key not on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.44.37.2	Qualified Certificates for Electronic Seals	Private key not on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.44.37.3	Qualified Certificates for Electronic Seals - PSD2	Private key not on QSCD Managed by Subscriber
	1.3.6.1.4.1.4146.1.44.39	**UK Qualified Certificates for Authentication**	
	1.3.6.1.4.1.4146.1.44.39.1	Qualified Certificates for Authentication (Natural Persons)	
	1.3.6.1.4.1.4146.1.44.39.2	Qualified Certificates for Authentication (Legal Persons)	
	1.3.6.1.4.1.4146.1.44.40	**UK eIDAS Qualified Certificates for Website Authentication (QWAC)**	
	1.3.6.1.4.1.4146.1.44.40.1	Qualified Certificates for Website Authentication (QWAC)	
	1.3.6.1.4.1.4146.1.44.40.2	Qualified Certificates for Website Authentication (QWAC) – PSD2	

Category	OID	Description
Registration Authorities	1.3.6.1.4.1.4146.1.45.1	LRA for Qualified certificates
	1.3.6.1.4.1.4146.1.45.2	External RA for Qualified certificates
Timestamping	1.3.6.1.4.1.4146.1.30	Timestamping Certificates Policy

	1.3.6.1.4.1.4146.1.31	Timestamping Certificates Policy – AATL
	1.3.6.1.4.1.4146.1.32	Timestamping Certificate Policy – Certificates for Qualified Time stamping (QTS) under eIDAS regulation
	1.3.6.1.4.1.4146.1.33	Timestamping Certificate Policy – Certificates for Qualified Time stamping (QTS) under UK eIDAS regulation
	1.3.6.1.4.1.4146.1.34	Hosted Timestamping Certificates Policy
	1.3.6.1.4.1.4146.1.35	Hosted Timestamping Certificates Policy – AATL
	1.3.6.1.4.1.4146.2	Policy by which the timestamping services operated by GlobalSign incorporates the time into IETF RFC 3161 responses
	1.3.6.1.4.1.4146.2.2	Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 1 (SHA1)
	1.3.6.1.4.1.4146.2.3	Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2)
	1.3.6.1.4.1.4146.2.3.1	Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2) with R6 CA hierarchy
	1.3.6.1.4.1.4146.2.3.1.1	Trusted Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2) with R6 CA hierarchy
	1.3.6.1.4.1.4146.2.3.1.2	CodeSign Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2) with R6 CA hierarchy
	1.3.6.1.4.1.4146.2.4	Policy by which the time-stamping services operated by GlobalSign incorporate the time into IETF RFC 3161 responses specifically for extended validation code signing services

	1.3.6.1.4.1.4146.2.6	JP Accredited Timestamping Tokens - AATL
	1.3.6.1.4.1.4146.2.7	JP Accredited Timestamping Tokens - non-AATL
Other Certificate Policies	1.3.6.1.4.1.4146.1.40	Non-Generic use Certificates Policy
	1.3.6.1.4.1.4146.1.40.20	Japan Certificate Authority Network (JCAN) Issuing CA Policy
	1.3.6.1.4.1.4146.1.40.20.1	Japan Certificate Authority Network (JCAN) Basic certificate policy
	1.3.6.1.4.1.4146.1.40.20.2	Japan Certificate Authority Network (JCAN) Advanced certificate policy
	1.3.6.1.4.1.4146.1.40.30	GlobalSign AATL Certificates Policy
	1.3.6.1.4.1.4146.1.40.30.2	GlobalSign AATL Certificates Policy (Class 2)
	1.3.6.1.4.1.4146.1.80	Retail Industry Electronic Data Interchange Client Certificate Policy
	1.3.6.1.4.1.4146.1.81	Retail Industry Electronic Data Interchange Server Certificate Policy
	1.3.6.1.4.1.4146.1.90	Trusted Root TPM Policy
	1.3.6.1.4.1.4146.1.95	Online Certificate Status Protocol Policy
	1.3.6.1.4.1.4146.3	GlobalSign's documents (such as Certificate Policy (CP) and Certification Practice Statement (CPS))
	1.3.6.1.4.1.4146.4	GlobalSign-specific certificate extensions Internet of Things (IoT)
	1.3.6.1.4.1.4146.5	GlobalSign Time Assessment policies
	1.3.6.1.4.1.4146.5.1	GlobalSign Japan Accredited Time Assessment Service Policy
CA Chaining and Cross Signing	1.3.6.1.4.1.4146.1.60	CA Chaining Policy – Trusted Root and Hosted Root
	1.3.6.1.4.1.4146.1.60.1	CA Chaining Policy – Trusted Root (Baseline Requirements Compatible)

Private hierarchy	1.3.6.1.4.1.4146.11.1	Private Hierarchy Certificate Policy Arc
	1.3.6.1.4.1.4146.11.1.1	Non-public Certificate Policy Arc
	1.3.6.1.4.1.4146.11.1.1.1	IntranetSSL
	1.3.6.1.4.1.4146.11.1.1.2	IntranetSMIME
	1.3.6.1.4.1.4146.11.1.1.3	Demo Certificates Policy (Private GlobalSign Hierarchy) – Should not be trusted as it may not contain accurate information. This is to be used for testing and integration purposes.
	1.3.6.1.4.1.4146.11.1.2	Private GlobalSign Internal Certificate Policy Arc
	1.3.6.1.4.1.4146.11.1.3	Private Customer Internal Certificate Policy Arc

Legacy OIDs
以下の OID はレガシーとしてマークされており、該当する場合は上の表に示された新しい階層に置き換えられる。

Category		**OID**	**Description**
TLS		1.3.6.1.4.1.4146.1.1	Extended Validation Certificates Policy – SSL - Legacy
		1.3.6.1.4.1.4146.1.1.1	Qualified Certificates under eIDAS Regulation – Qualified Web Authentication Certificates (QWAC) - Legacy
		1.3.6.1.4.1.4146.1.1.2	Qualified Certificates under eIDAS Regulation – Qualified Web Authentication Certificates (QWAC) – PSD2 - Legacy
		1.3.6.1.4.1.4146.1.2	Extended Validation Certificates Policy – Code Signing - Legacy
		1.3.6.1.4.1.4146.1.10	Domain Validation Certificates Policy - Legacy
		1.3.6.1.4.1.4146.1.10.10	Domain Validation Certificates Policy – AlphaSSL - Legacy
		1.3.6.1.4.1.4146.1.20	Organization Validation Certificates Policy - Legacy

Category		OID	Description
		1.3.6.1.4.1.4146.1.25	IntranetSSL Validation Certificates Policy - Legacy
Qualified		1.3.6.1.4.1.4146.1.40.35	eIDAS Qualified Certificates (Generic) - Legacy
		1.3.6.1.4.1.4146.1.40.35.1	Qualified Certificates for Electronic Seals (Legal Persons with QSCD) - managed by Subscriber - Legacy
		1.3.6.1.4.1.4146.1.40.35.1.1	Qualified Certificates for Electronic Seals (Legal Persons) - PSD2 - Legacy
		1.3.6.1.4.1.4146.1.40.35.2	Qualified Certificates for Electronic Signatures (Natural Persons with QSCD) - managed by Subscriber – Legacy
Code signing		1.3.6.1.4.1.4146.1.50	Code Signing Certificates Policy (Certificates issued by GlobalSign containing 1.3.6.1.4.1.4146.1.50 are issued and managed in accordance with the Baseline Requirements for Code Signing)
Authentication		1.3.6.1.4.1.4146.1.40.60	Client Certificates Policy (Client Authentication)
Client certificates		1.3.6.1.4.1.4146.1.40.10	Client Certificates Policy (EPKI – Enterprise PKI - Legacy)
		1.3.6.1.4.1.4146.1.40.40	Client Certificates Policy (EPKI for private CAs - Legacy)
		1.3.6.1.4.1.4146.1.40.50	Client Certificates Policy (Private Hierarchy - AEG - Legacy)
Others		1.3.6.1.4.1.4146.1.26	Test Certificate Policy –Should not be trusted as it may not contain accurate information. This is to be used for testing and integration purposes. (Legacy)
		1.3.6.1.4.1.4146.1.70	High Volume CA Policy
		1.3.6.1.4.1.4146.1.100	Internet of Things Device Certificates Policy (legacy)

Community OIDs

該当するコミュニティの要件に準拠する証明書には、以下の追加の識別子の何れかが含まれる。

Community	OID	Description
CA/Browser Forum	2.23.140.1.1	Extended Validation Certificate Policy
	2.23.140.1.2.1	Domain Validation Certificates Policy
	2.23.140.1.2.2	Organization Validation Certificates Policy
	2.23.140.1.3	EV Code Signing Certificates Policy
	2.23.140.1.4.1	Code Signing Minimum Requirements Policy
	2.23.140.1.4.2	Code Signing Minimum Requirements Timestamping Policy
ETSI	0.4.0.194112.1.0	QCP-n: certificate policy for EU qualified certificates issued to natural persons
	0.4.0.194112.1.1	QCP-l: certificate policy for EU qualified certificates issued to legal persons
	0.4.0.194112.1.2	QCP-n-qscd: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD
	0.4.0.194112.1.3	QCP-l-qscd: certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD
	0.4.0.194112.1.4	QCP-w: certificate for EU qualified website certificate issued to a natural or a legal person and linking the website to that person
NAESB	2.16.840.1.114505.1.12.1.2	NAESB Rudimentary Assurance
	2.16.840.1.114505.1.12.2.2	NAESB Basic Assurance
	2.16.840.1.114505.1.12.3.2	NAESB Medium Assurance

1.3. PKI における関係者

1.3.1. 認証局

GlobalSign は本 CPS に基づき証明書を発行する認証局である。GlobalSign は、認証局として、証明書のライフサイクル管理にまつわる業務を行う。この業務には、利用者の登録、及び証明書の発行、更新、交付、失効などが含まれる。GlobalSign は、証明書のステータス情報を、証明書失効リスト（CRL）配布ポイントの形式で示されるレポジトリ及び/又はオンライン証明書ステータスプロトコル（OCSP）レスポンダを使用して提供する。この認証局は、下位発行 CA の登録局（RA）からの依頼に基づき証明書を発行する役割を示す意味で「発行局」又は「GlobalSign」の名で呼ばれることがある。

GlobalSign の PACOM1 – CA Governance Policy Authority は、GlobalSign の経営チーム、及び GlobalSign の取締役会で承認されたメンバーで構成されており、GlobalSign の証明書階層に含まれる全ての電子証明書の CPS を維持管理する責任を負う。GlobalSign の Policy Authority は、全ての証明書のライフサイクル管理に関する最終権限を有する。この証明書には、ルート証明書及び TrustedRoot の発行 CA を含む GlobalSign 証明書階層を構成する下位発行 CA の証明書などが含まれる。

GlobalSign はタイムスタンプ局(以下、「TSA」という)でもあり、特定の日時にデータが存在したことを証明する。GlobalSign は TSA サービスを適宜外部に委託し、日時・時刻に関係する正確性検証業務を独自に行うことを許可する。

GlobalSign は、そのルート証明書の下で発行される証明書の管理サービスを安定的に提供する。このサービスは、特定のアプリケーションで利用可能である、ないし必要となる、証明書の発行、失効、ステータスの正確性検証などを含むがこれに限定しない。GlobalSign は、当該認証局の下位 CA、発行 CA の下で発行される全てのタイプの証明書に向け、オンライン登録システム、及びいくつかの API を提供管理する。

証明書のライフサイクル管理に関する業務のいくつかは、GlobalSign RA に委任され、この業務は GlobalSign とのサービス契約に基づき遂行される。

1.3.2. 登録局(RA)

登録局（RA）は証明書の申請者を識別及び認証することに加えて、証明書の失効、更新及び Re-key の要求を受理し、それを転送したりする。

GlobalSign はこの RA 業務を行うことができる組織であり、この場合には以下の各業務に責任をもって当たる。

- 証明書申請を受理し、評価し、当該証明書申請の登録を承認又は却下する。
- 利用者を証明書サービスへ登録する。
- (要求された証明書タイプに応じた)利用者の識別を促進するシステムを提供する。
- 公証された、又は他の形で認められた文書を使用して申請者の申請を評価及び認証を行う。
- 申請の承認後、多要素認証のプロセスに基づいて証明書の発行を要求する。
- GlobalSign の、関連する下位発行 CA、或いは下位のパートナー発行 CA からの要求を受け証明書失効手続きを取る。

GlobalSign と契約を締結したサードパーティが独自の RA を運営し、証明書の発行を行うことがある。この際、サードパーティは、本 CPS が定める全ての要求事項並びに CA/B Forum かつ/又はブラウザのルートプログラムが推奨する付加的な基準を組み込む契約条項に準拠しなければならない。RA は、その内部ポリシーに基づき、より厳格な審査手続きを取ることがある。

ドメインの承認、或いは SSL 及び S/MIME 証明書のサブジェクトフィールドに含まれる IP アドレス又は電子メールアドレスのコントロール又は認証は委任されない。

特定のタイプの証明書を発行するにあたり、RA はサードパーティ認証局が発行した証明書、又はサードパーティの運営するデータベースや情報源などに依拠することがある。パスポートや eID といった国家が発行した個人の証明書、運転免許証等が該当する。RA がサードパーティ認証局発行の証明書に依拠している場合、RA はそうしたサードパーティの CPS を参照し、サードパーティによる十分性検証の方法及び依拠当事者の義務を確認しなければならない。

EPKI(マネージド PKI)及び MSSL (SSL マネージドサービス)の場合、事前審査された上で GlobalSign のシステムに設定された情報によって証明書の発行が制限される。これらの RA をエンタープライズ RA という。

GlobalSign は、そのエンタープライズ RA が属する組織からの証明書申請を検証するために、エンタープライズ RA を指定することができる。EPKI(マネージド PKI)及びマネージド SSL(マネージド SSL) が利用するエンタープライズ

RA では、事前審査の上 GlobalSign のシステムに登録された利用者の組織情報に従って、証明書の発行が制限される。エンタープライズ RA が組織を代表するためには、以下の要件が GlobalSign によって検証される。

1. 要求された FQDN は、エンタープライズ RA の検証済みドメイン名内にあり、
2. 証明書申請に FQDN 以外のタイプのサブジェクト名が含まれている場合、GlobalSign は、その名前が委任された企業又は委任された企業の関連会社の名前であること、又は委任された企業が名前付きサブジェクトの代理人であることを確認する。

1.3.2.1 EV SSL 証明書・EV Code Signing 証明書に関する RA 特有の要求事項

EV SSL 証明書・EV コードサイニング証明書の発行にあたっては、GlobalSign は各 RA 又は委託先に対し、EV ガイドライン及び該当する場合は Baseline Requirements for Code Signing の全ての適用要件に準拠し、必要な手続きを取ることを義務付ける。

EV ガイドラインの条項に基づき、GlobalSign は、特定の有効な EV 証明書のサブジェクトに対し、契約に基づいて RA としての機能を果たし、また GlobalSign が当該のオリジナルの EV 証明書に記載されたドメインの第三レベル或いはそれ以上のレベルのドメイン名に対して追加の証明書(これをエンタープライズ EV 証明書という。) を発行することを許可することがある。この場合、サブジェクトはエンタープライズ RA とみなされ、第三階層以上の EV 証明書をエンタープライズ RA 又はエンタープライズ RA が所有する又は直接支配する企業以外のサブジェクトに対し発行することを認証局に許可してはならないものとする。GlobalSign はこの要件を、システムを通じ機械的に強制する。

GlobalSign は EV ガイドライン 11.12 項の最終相互相関関係並びにデューディリジェンス要件の履行をエンタープライズ RA に委任しない。

1.3.2.2 適格証明書に関する RA 特有の要求事項

GlobalSign は、LRA 又は外部の RA として活動するサードパーティに身元証明及び証明書ライフサイクル のイベントを委任することができる。GlobalSign は、適用される規制、法律、業界標準、ポリシーに RA が準拠していることを保証するものとする。

LRA 及び外部の RA に対しては、GlobalSign と当該 RA との間で、少なくとも以下の項目を含む、委任された活動に関する契約が存在するものとする。

- RA が関連する規制、法律、業界標準及びポリシーを遵守する義務。
- GlobalSign と RA 間の責任分掌。
- GlobalSign の委任を取り消す能力
- GlobalSign の監査権限により、RA が関連規制、法律、業界標準及びポリシーを遵守していることを監督する。

1.3.2.2.1 LRA

<u>サブジェクト</u>

身元証明の対象は、LRA、その親会社、子会社、又は関連するグループ組織に雇用される従業員（自然人）に限定される。

<u>委任された活動</u>

LRA への委任は、個々の主体の身元証明と認証、および証明書要求と失効を含む証明書ライフサイクルイベントに限定される。

<u>コンプライアンス</u>

GlobalSign は、LRA が適用される規制、法律、業界標準、ポリシーに準拠することを保証するために、適切な手段を適用するものとする。

1.3.2.2.2 外部の RA

<u>サブジェクト</u>

対象者は個人（自然人）及び/又は組織（法人）である。

<u>委任された活動</u>

委任される活動には、加入者（及び/又はサブジェクト）の身元証明、要求の認証、要求及び失効を含む証明書のライフサイクルイベントなどが含まれる場合がある。

<u>監査</u>

関連する規制、法律、業界標準、ポリシーへの準拠を保証するために、外部 RA は以下を行うものとする。

- GlobalSign の監査の一環として監査を受ける、又は
- 適合性評価機関又は同等の機関からの監査報告書を提出すること。

1.3.2.2.3 JCAN LRA

JCAN LRAs は、LRA 向け JIPDEC トラステッド・サービス（JTS）登録基準をもとに JIPDEC による外部審査の対象となる。JCAN LRA は GlobalSign より登録を受ける前に、当審査に合格しなければならない。

JCAN LRA はアイデンティティへの審査、鍵管理を含む、証明書のライフサイクル管理に携わる。

1.3.3. 利用者

利用者とは、取引、通信、デジタル署名の使用のため証明書を申請し受領した法人又は自然人をいう。
証明書のサブジェクトとは、証明書に名前を記載される当事者をいう。この文脈における利用者とは、証明書のサブジェクトであると同時に GlobalSign と契約を締結し証明書の発行を受けるエンティティである。身元の正確性検証及び証明書の発行を受ける前の利用者を申請者という。

法人は、当該法人が公表する付随定款の見直し、役員の任命、官報又は同様の公式な政府刊行物又はその他の Qualified Independent Information Source (QIIS)や Qualified Independent Information Source (QGIS)などのサードパーティデータベースに基づき、組織情報の検証が行われる。自営業を営むサブジェクトは居住国の管轄当局が発行する商業登録証明に基づき組織情報の検証が行われる。

全ての利用者は、証明書のオンライン申請を行う際に説明される要求事項に従い、さらなる信用証明情報の提出が必要となる。

GlobalSign が発行するエンドエンティティ証明書の利用者には、GlobalSign のネットワーク資源にアクセスする必要がある日常業務に携わる従業員、代理人が含まれる。利用者は鍵ペアの生成を行い証明書を保管する署名生成デバイスの運用上又は法的な所有者である場合もある。

利用者である組織は、GlobalSign が当該利用者に GlobalSign 証明書サービスを使用するアプリケーションの範囲内において、特定の機能を果たす権限を与えるサービス契約又はその他の既存の契約関係を GlobalSign と締結していることが求められる。GlobalSign と利用申請を行うエンドエンティティの間で締結された契約に基づいてのみ、利用者である組織に証明書が発行される。

1.3.4. 依拠当事者

電子証明書の有効性を検証するにあたり、依拠当事者は GlobalSign が提供する失効情報を CRL 配布点若しくは OCSP レスポンダを通じて参照しなければならない。

Adobe は Acrobat® 9.12 以上の製品で AATL プラットフォームを提供している。これにより、文書の受領者は、認証された PDF 文書が本物であることをより確実に保証される。ここでの文書の受領者は、Adobe 製品でこの機能をサポートするプラットフォームを使用し、認証された PDF 文書になされた利用者の署名を検証する依拠当事者である。ベストプラクティスは、文書を認証しようとする作成者が、署名する PDF に証明書ステータス情報と適切なタイムスタンプを含めることである。依拠当事者は適切な Adobe PDF リーダーのバージョンを使用してこうした情報を検証することができる。

1.3.5. その他の関係者

その他の関係者には、ブリッジ認証局、PKI コミュニティ内において信頼される発行 CA を相互認証する認証局などを含む。

1.4. 証明書の使用方法

証明書は、事業体が電子取引を行う際、その他の関係者に身元を証明することを可能にする。証明書は、ID カードの電子上の代替物として商業環境で使用される。

1.4.1. 適切な証明書の使用方法

エンドエンティティ証明書は Key Usage 及び Extended Key Usage の値によって、その使用方法を制限される。GlobalSign が発行する証明書は以下のような機能を必要とするパブリックドメインでの通信で使用することができる。

- **否認防止:**当事者は、取引を行ったこと、電子メッセージを送信したことを否認することができない。
- **認証:**あるエンティティに対し、別のエンティティが主張する人物(組織・物)であることを証明する。
- **機密性(秘匿性):**あるエンティティに対し、明確に受信者として意図された相手以外には誰もデータを読み取ることができないことを保証する。
- **完全性:**あるエンティティに対し、送信者から受信者に送られる間、及び送信された時刻から受信された時刻までの間に、データが(意図的に又は意図せず)変更が加えられていないことを保証する。

デジタル署名:デジタル(電子)署名は電子フォーム、電子文書、又は電子メールなどデジタル署名に対応する特定の取引にのみ使用することができる。証明書は、証明書内の公開鍵と一致する秘密鍵によって作成されたデジタル署名を検証するために使用され、従って、証明書をサポートするアプリケーションという用途でのみ使用される。デジタル署名に使用できる証明書の種類は以下の通り。

- **PersonalSign 2:** 取引への否認防止(中程度の保証レベル)
- **PersonalSign 2 Pro:** 組織内の担当者として取引を行う当事者による取引への否認防止(中程度の保証レベル)
- **AATL:** 組織内の担当者として取引を行う当事者による取引への否認防止(中程度のハードウェアレベルの保証)。(証明書の特異性をかんがみ、証明書を暗号化に使用することは推奨されない。)
- **適格証明書:** 個人(eIDAS 適格電子署名証明書)及び法人(eIDAS 適格 e シール証明書)による署名への否認防止

認証(ユーザ):ユーザ認証証明書は、ウェブサイトその他のオンラインデータへのアクセス、電子メールなど、電子的な認証を必要とする通信に使用することができる。証明書の認証機能は、公開鍵に結合された利用者の識別など、証明書の固有の特性に関するテストの組合せの結果である場合が多い。「デジタル署名」という用語は、権限認証の機能を記述するために、利用者が証明書内の公開鍵に一致する秘密鍵に対する所有権を証明することができる方法、という意味で使われることが多い。

- **PersonalSign 2:** 自然人及び電子メールアドレスの実在を認証する(中程度の保証レベル)
- **PersonalSign 2 Pro:** 組織内の自然人又は組織内の役職名、或いは機械、装置、部署を認証する(中程度の保証レベル)。オプションで、電子メールアドレスの実在を認証することも可能。
- **PersonalSign 3 Pro:** 組織内の自然人を認証する(高い保証レベル)
- **NAESB Rudimentary:** NIST SP800-63A Digital Identity Guidelines : Enrollment and Identity Proofing, Section 4.3 “Identity Proofing Assuarance Level 1 に記載されている内容を認証する
- **NAESB Basic:** **Authentication as prescribed in the Baseline Requirements** の **Section 3.2.3 Authentication of Individual Identity** に記載されている内容を認証する。上記の Basic Level と同等の手段で申請者の身元を確認した事業主は、LRA になることを選択し、申請者の身元証明を、会社が発行した写真 ID の検査又は LRA の安全なオンラインプロセスを介して直接行うことができる。企業が発行した写真 ID 又はオンラインプロセスは、政府が発行した写真 ID で作成する必要がある。
- **NAESB Medium:** EV ガイドライン 11.2.2 項:許容される正確性の検証方法(4) 主たる個人に規定されている内容を認証する

認証 (デバイス及びオブジェクト):デバイス認証証明書は、ウェブサイトその他ソフトウェアオブジェクトをはじめとするオンラインリソースを、電子的な認証を必要とする通信に使用することができる。証明書の権限の認証機能は、しばしば、公開鍵に紐づけされた機器(Web サーバ)の識別など、証明書の固有のプロパティに関するテストの組合せの結果である。
権限認証の機能を記述するために、「デジタル署名」という用語が使用されることが多い。これは、例えば、Web サーバが、証明書内に記載されているドメイン名が証明書の公開鍵に一致する秘密鍵の所有権があることを証明することができる方法であるためである。

- **DomainSSL:** ドメイン名とウェブサービスの認証、通信の暗号化
- **AlphaSSL:** ドメイン名とウェブサービスの認証、通信の暗号化

- **OrganizationSSL:** リモートドメイン名、リモートドメイン名と関連づけられる組織名とウェブサービスの認証、通信の暗号化
- **ICPEdu:** リモートドメイン名、リモートドメイン名と関連づけられる組織名とウェブサービスの認証、通信の暗号化
- **Extended Validation SSL:** ドメイン名、ドメイン名と関連づけられる組織名とウェブサービスの認証、通信の暗号化
- **Code Signing:** 法人、法的エンティティとそのデータオブジェクトの認証
- **EV Code Signing:** 法人、法的エンティティとそのデータオブジェクトの認証
- **Time Stamping:** 組織内での日付・時刻に関連するサービスの認証
- **PersonalSign(全種):** 組織に関連づけられるデバイスやマシンの認証
- **NAESB Rudimentary:** NIST SP800-63A Digital Identity Guidelines の Enrollment and Identity Proofing, Section 4.3 Identity Proofing Assurance Level I に記載されている内容を認証する
- **NAESB Basic:** Baseline Requirements の Section 3.2.3 Authentication of Individual Identity に記載されている内容を認証する
- **NAESB Medium:** EV ガイドライン 11.2.2 項:許容される正確性の検証方法(4) 主たる個人に規定されている内容を認証する

保証レベル:利用者は、依拠当事者に提示することを希望するアイデンティティにおいて保証レベルを選択する必要がある。たとえば、あまり知られていないブランド名を使用する利用者は EV SSL 証明書を使用して積極的に自らの身元を依拠当事者に保証すべきであり、閉じられたコミュニティ内でよく知られた URL 又は特定の通信サーバを用いる場合には低い保証レベルを選択できる。

- **低い保証レベル:** Class 1 証明書は、認証された識別情報が証明書内に記載されないため、本人確認には適していない。本証明書は、否認防止をサポートしない。
- **中程度の保証レベル:** Class 2 証明書は、一定のリスクを伴う組織間、組織内、及び商業的取引を暗号化するのに適した、個人及び組織用の証明書である。
- **高い保証レベル:** Class 3 証明書は、Class 1・Class 2 証明書に比較してサブジェクトの識別情報について高いレベルの保証を提供する、個人又は組織に発行される証明書である。
- **高い保証レベル(EV):** EV 証明書は EV ガイドラインに準拠して GlobalSign が発行する Class 3 証明書である。
- **NAESB Rudimentary:** 最も低い保証レベルを提供する。このレベルの主な目的は署名された情報の完全性を保証するために使用される。このレベルは悪意のある行動をとることが少ないと考えられる環境にて使用するのが適切である。このレベルは認証を必要とする取引には適していない。また、一般的に機密性を必要とする取引には適していないが、より高い認証レベルの証明書が使用できない場合は、このレベルの証明書を使用してもよい。
- **NAESB Basic:** データ漏えいにつながるリスクがあるがその影響が大きくないと考えられる環境において、基礎レベルの保証を提供するのに適している。この環境はプライベート情報にアクセスするが、悪意のあるアクセスが行われる可能性は高くない環境を含む。尚、この保証レベルでは悪意を持ったユーザはいないと想定している。
- **NAESB Medium:** このレベルはデータ漏えいにつながるリスクが中程度にある環境に適している。この環境は大きな金銭的価値がある取引や不正のリスク、又は不正アクセスの可能性が大きい環境においてプライベート情報にアクセスすることを含む。

機密性:タイムスタンプ及びコードサイニング用の証明書を除く全てのタイプの証明書は、電子証明書による通信の機密を保全する目的で使用することができる。機密情報にはビジネス上の通信、個人的な通信、個人情報、プライバシーなどがある。

北米エネルギー規格委員会(以下、「NAESB」という) の PKI において発行された証明書はビジネスプラクティススタンダード WEQ-001、WEQ-002、WEQ-003、WEQ-004、WEQ-005 における取引に使用することができる。また、双方の合意がある場合はその他の取引にも使用することができる。NAESB Wholesale Electric Quardrant Busiess Practice Standards WEQ-012(“NAESB WEQ PKI Standards”)に基づいて発行された証明書は以下の使用方法を禁ずる。

- データが危殆化若しくは偽装された場合、懲役を受ける可能性があるデータの転送 及び
- 連邦法において違法とみなされるデータの転送

本 CPS に記載のない証明書のその他の使用方法:
証明書の利用に際し、一つの証明書内に電子署名（否認防止）と認証（デジタル署名）の機能が同時に存在することが可能である。上記の用語は IETF、及び EU 指令 1999/93/EC（電子署名におけるコミュニティフレームワーク）及び eIDAS 規則 (Regulation (EU)N910/2013) (eIDAS) 又は eIDAS (英国の法律) と 電子取引の電子識別及びトラストサービスに関する規則 2016 の法的枠組みにおいて異なる定義をされることがある。

JCAN 証明書の種類は下記のとおり。

(a) JCAN アドバンスト
JCAN アドバンストは、LRA から自然人に対し発行される。LRA は、公的な根拠資料に基づくデータベースで自然人を確認する。 サブジェクトの CN は実名又は PS 名である。

(b) JCAN ベーシック
JCAN(ベーシック)証明書は公式文書のない次の実体に発行される:
• 当該組織の内部サブジェクト(メンバー、それらの役割名、組織名、メールアドレス; オブジェクトの名前,識別子);
• 当該組織の外部サブジェクト(パートナー、それらの役割名、組織名、メールアドレス; オブジェクトの名前、識別子)
注）パートナーは、契約関係、グループ会社、会員、委員会の構成員、或いは客員、学生、信頼できる書類で認証した人、クレジットカードを登録した人等

JCAN 証明書に記載するサブジェクト CN は以下である。
• メンバー又はパートナー名（実名又は PS 名）
• 役割名
• 会社、団体、部門、チーム、グループ等の組織名
• メールアドレス
• 文書名、サーバ名、ID、コード等の識別子

(c)アクセス認証用証明書
アクセス認証用証明書は、LRA に発行される証明書である。 アクセス認証用証明書は、JCAN 証明書の発行/失効時に「JCAN 証明書発行サービスサイト」 へのアクセスに用いる。 アクセス認証用証明書は、JCAN 認証局以外の CA から発行してもよい。

(d) テスト証明書
JCAN 認証局の稼働確認を目的に、 JCAN 認証局はテスト証明書を発行する。

1.4.2. 禁止されている証明書の用途

証明書は証明書エクステンションの Key Usage 及び Extended Key Usage を用いて、その使用方法を制限される。このエクステンションと合致しない目的で証明書を使用することは認められていない。通信において、GlobalSign のワランティーポリシーに示された信頼性の限度を超えた方法で証明書を使用することは認められていない。

本 CPS に準拠して発行された証明書は、そのサブジェクトが信頼できること、信頼できる事業を行っていること、証明書がインストールされた機器に瑕疵、マルウェア、ウィルスがないことなどを保証するものではない。コードサイニング証明書は、署名されたコードにバグや脆弱性がないことを保証するものではない。

本 CPS に準拠して発行された証明書は、以下の目的に使用してはならない。

- フェイルセーフ機能を必要とするあらゆるアプリケーション
- 安全上の危険(例：人的又は環境に対するリスク)を起こしうる用途又は仕組・構造。
- 法により禁じられている場合。
- 適格 e シール証明書は法人によってのみ使用されなければならない一方、適格電子署名証明書は自然人によってのみ使用されなければならない。
- NAESB WEQ-PKI に準拠して発行された証明書は以下の目的で使用してはならない。
  - 危殆化や改ざんが起きた場合投獄され得るような通信やデータ伝送
  - 連邦法において違法とみなされる通信やデータ伝送

1.5. ポリシー管理

1.5.1. 文書を管理する組織

発行 CA が認定スキームに準拠しているかどうかの情報を得たい場合、又はその他本 CPS に関する問い合わせは、以下に送付すること。

PACOM1 – CA Governance GlobalSign NV
Diestsevest 14,
3000 Leuven,
Belgium
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909
Email: policy-authority@globalsign.com

1.5.2. 問い合わせ窓口

質問全般

GlobalSign NV/SA
attn. Legal Practices,
Diestsevest 14,
3000 Leuven, Belgium
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909
Email: legal@globalsign.com
URL: www.globalsign.com

証明書問題報告
マルウェア対策団体、利用者、依拠当事者、アプリケーション・ソフトウェア・サプライヤー、及び他の第三者は、秘密鍵の危殆化の可能性、証明書の不正使用、疑義のあるコードへの署名に用いられている証明書、乗っ取り攻撃、又は他の種類の不正、セキュリティの侵害、証明書の誤発行、不適切な行為等について、又、証明書に関連するその他事項については、report-abuse@globalsign.com 宛てに電子メールで報告することができる。
GlobalSign は、これらの要求に応じ、当該証明書を失効することで対応することが可能である。また、調査の結果、失効しない場合もある。この意思決定のために GlobalSign はセクション 4.9.5 に記載されている調査を実施する。

1.5.3. CPS がポリシーに適合しているかを判断する担当者

適格な監査人から受領するアドバイスに基づき GlobalSign CP の適格性、適用可能性や本 CPS の準拠性を判断するのは、PAOM1-CA Governance である。

本 CPS の信頼性を維持・促進し、認定基準及び法的要件により的確に対応するため、PACOM1 – CA Governance は最低でも本 CPS を年次でレビューし、適宜又は状況に応じ、ポリシーを改訂し更新する。更新されたポリシーは、すでに発行済の証明書、及び発行予定の証明書に対し、本 CPS の公表に伴って拘束力を持つ。

1.5.4. CPS 承認手続き

本 CPS の変更は、PACOM1 – CA Governance によってレビュー・承認される。更新された本 CPS は、整合性をチェックするために、GlobalSign CP に対してレビューされる。GlobalSign CP の変更も必要に応じて追加される。ポリシーの更新が PACOM1 – CA Governance に承認されると、本 CPS の新バージョンが GlobalSign のオンラインリポジトリ(https://www.globalsign.com/repository)において公開される。

新バージョンは、前のバージョンの本 CPS に準拠して発行された証明書の利用者と依拠当事者を含む全ての当事者を拘束する。

1.6. 定義と略語

本契約において使用されているが定義されていない語句は、Baseline Requirements、EV ガイドライン、Baseline Requirements for Code Signing、及び/又は eIDAS 規則 又は UK eIDAS 規則において定義されるものとする。

Adobe Approved Trust List (AATL): 文書署名用証明書に関し Adobe PDF Reader version 9.0 より搭載されている、Adobe Root CA Policy Authority によって作成された、CA のトラストストア

関連企業: あるエンティティ、機関、部門、行政小区、政府機関の直接的支配下で運営されるエンティティなどが支配下におくか、これらの支配下におかれるか又は共通支配下にある企業、パートナー、ジョイントベンチャーその他のエンティティ

マルウェア対策団体: 疑義のあるコードに関する情報提供及び/又はマルウェアの防止、検知、又は除去に用いられるソフトを開発する団体

申請者: 証明書の申請をする、又は更新しようとする自然人又は法人。証明書が発行されれば、申請者は利用者と呼ばれる。デバイス自体が証明書の申請データを送信している場合であっても、証明書に名称の記載されたデバイスを管理運用するエンティティがこの証明書の申請者である。

アプリケーションソフトウェアサプライヤー: ルート証明書を搭載し証明書を表示・使用するブラウザ、その他証明書に依拠するソフトウェアの提供者

認証状: サブジェクトの身元情報が正確であることを表明する文書

認証用ドメイン名: 特定の FQDN を証明書に記載するための認証を得るために使用される FQDNのこと。CA は DNS の CNAME ルックアップから返された FQDN をドメイン十分性検証の目的で FQDN として使用できる。ワイルドカード・ドメイン名が証明書に含まれる場合、CAはワイルドカード・ドメイン名の最も左側の部分から「*.」を削除して、対応する FQDN を得なければならない。認証機関は、ベースドメイン名に出会うまで、FQDN のドメインラベルを左から右に 0 個以上プルーニングし、プルーニングによって得られた値（ベースドメイン名そのものを含む）のいずれかをドメイン検証の目的で使用することができる。

認証局: 公開鍵インフラストラクチャ(PKI) - WEQ-012 の北米エネルギー標準化委員会(NAESB) 事業手続き基準の全ての規定に準拠する認証局

ベースドメイン名 : 申請された FQDN のうち、レジストリ管理下又は公開されたサフィックスの左側にある最初のドメイン名ノードに、レジストリ管理下又は公開されたサフィックスを加えた部分（例:「example.co.uk」又は「example.com」）。トップレベルドメインのノードが、レジストリ契約に ICANN 仕様 13 を持つ gTLD である FQDN の場合、その gTLD 自体をベースドメイン名として使用することができる。

事業体: EV ガイドラインで定義されている民間組織、政府機関、非営利組織ではない組織。例としては、一般的なパートナー、非法人組織、個人企業などが挙げられるが、これらに限定されない

証明書: デジタル署名によってある公開鍵とある識別情報とを紐づける電子文書

Certificate Authority Authorization (CAA): CAA レコードは、どの証明書局がドメインに対して証明書を発行できるかを指定するために使用される。

証明書受益者: 本証明書の利用契約又は利用条件の当事者である利用者、アプリケーションソフトウェアサプライヤーにより配布されるソフトウェアにルート証明書を含めるために GlobalSign が契約を締結した全てのアプリケーションソフトウェアサプライヤー、及び有効な証明書に合理的に依拠する全ての依拠当事者。

証明書データ: 認証局が保持、管理、又はアクセス権限を有する(申請者その他から入手する)証明書申請及び付随データ

証明書管理手続き: 認証局が証明書データを検証し、証明書を発行し、リポジトリを管理し、証明書を失効する際に使用する、鍵、ソフトウェア、ハードウェアに関連するプロセス、実務、手続き

証明書ポリシー: 共通のセキュリティ要件を持つ特定のコミュニティ内若しくは公開鍵基盤において、ある証明書が使用できるかどうかを示す一連のルール

証明書問題報告: 証明書の危殆化の疑い、不正使用、その他の不正行為、危殆化、不正使用、証明書に関連する不適当行為に関する申し立て

証明書申請: 証明書の発行を要求するために行われる Baseline Requirements 10 項に規定される情報の伝達

証明書失効リスト: 証明書を発行した認証局が作成しデジタル署名した、定期的に更新されるタイムスタンプ付きの失効した証明書の一覧

認証局: 証明書の生成、発行、失効、管理に責任を負う組織。この用語は、ルート認証局、下位認証局のどちらを表す場合にも使用される。

認証業務運用規程: 証明書を生成、発行、管理、使用する際の運用方法の枠組みを規定する複数の文書の一つ

Common CA Database (CCADB): パブリックに信頼されたルート及び中間 CA 証明書の全てが一覧になっている、Mozilla によって運営されているレポジトリ

危殆化: 機密情報が管理できなくなる事態を引き起こすセキュリティポリシー違反。

適合性評価機関: 規則(EC) No. 765/2008 第 2 条第 13 項に定義される機関であって、同規則に従って適格トラストサービスプロバイダの適合性、また、当該プロバイダが提供するトラストサービスの適合性評価を実施する権限を有すると認定されている機関。

国: 国際連合の加盟国、又は少なくとも二つの国連加盟国が主権国家として認めた地理的地域

相互認証証明書:2 つのルート認証局がトラスト関係を構築するために使用する証明書

DCF77:ドイツの長波長信号と標準周波数無線局。

電子署名:メッセージを非対称暗号方式とハッシュ関数を用いてエンコードすること。オリジナルメッセージと署名者の公開鍵を所有する人物が、署名者の公開鍵と対になる秘密鍵を使用してエンコードが行われたこと、及びオリジナルメッセージがエンコード後に書き換えられたかどうかを正確に判断することができる。

DNS CAA Email Contact: Baseline Requirements の Appendix B.1.1 に定義されている電子メールアドレス

DNS TXT Record Email Contact: Baseline Requirements の Appendix B.2.1 に定義されている電子メールアドレス

DNS TXT Record Phone Contact: Baseline Requirements の Appendix B.2.2 に定義されている電子メールアドレス

Domain Contact: Base Domain Name の WHOIS 又は DNS SOA のレコードに記載されている、或いはドメイン名の登録事業者へのダイレクトコンタクトを通して取得された、ドメイン名の登録者、技術担当者、或いは管理契約(又は ccTLD における同等のもの)。

ドメインラベル:RFC 8499 (http://tools.ietf.org/html/rfc8499)より。“ドメイン名の一部を構成する、0 個以上のオクテットに順序をつけて並べたもの。グラフ理論を使用すると、ラベルとは、あり得るドメイン名 全てのグラフの一部に含まれる一つのノードを特定するものという定義となる。”

ドメイン名:ドメインネームシステムでノードに割り当てられた 1 つ又は複数のドメインラベルの順序付きリスト。

ドメイン名システム(Domain Name System, DNS):ドメイン名を IP アドレスに変換するインターネットサービス。

ドメイン名空間:ひとつのドメインネームシステム内においてある単一の下位ノードに与えられ得るあらゆるドメイン名全て

ドメイン名の登録者:「ドメイン名の所有者」とも呼ばれるが、より正確にはレジストラに登録された人物又はエンティティで、ドメイン名の使用について管理権限を有し、WHOIS やレジストラに「登録者」として登録されている自然人又は法人を指す。

ドメイン名のレジストラ:以下に列挙する者の援助又は契約に基づきドメイン名の登録業務を行う人物又はエンティティをいう。(1)Internet Corporation for Assigned Names and Numbers(ICANN)又は(2)各国のドメイン名管理当局（登記所）、又は(3)Network Information Center(その関連会社、請負業者、委託業者、承継人、譲受人を含む)

eIDAS 規則 (“eIDAS”):欧州議会及び理事会の規則(EU)第 910/2014 号。2014 年 7 月 23 日、欧州内市場における電子取引の電子識別及びトラストサービスに関する規則。指令 1999/93/EC を廃止する。

e シール:電子形式のデータであって、電子形式で他のデータに添付されているか、又は論理的に関連付けられているものであって、他のデータの出所及び完全性を確保するためのもの

デジタル署名:電子形式のデータであって、電子形式で他のデータに添付され又は論理的に関連付けられ、かつ、署名者が署名するために使用するもの

エンタープライズ PKI (EPKI):Microsoft Windows が信頼するデジタル ID、Adobe Approved Trust List のライフサイクル全体を管理するための、発行、再発行、更新、及び失効を含む、組織向けの製品サービス

エンタープライズ RA:認証局から証明書の発行権限を付与されているところの、認証局の関連会社ではない組織或いはその子会社の従業員又は代理人をいう。エンタープライズ RA は、パートナーや顧客、或いは関連会社、それら当該組織との交流を望むところの対象者に対するクライアント認証の権限を有する。

有効期限:証明書の有効期間の終わりを定義する証明書内の日付で、この日を境に証明書が無効となる。

Fully-Qualified Domain Name（完全修飾ドメイン名、FQDN）:インターネットドメインネームシステム内の全ての上位ノードのドメインラベルを含むドメイン名のこと。

GlobalSign Certificate Center(GCC):顧客とパートナーが GlobalSign から証明書を購入、管理するクラウドベースの証明書管理システム

全地球測位システム（GPS）:現在位置、ナビゲーション、タイミング(PNT)サービスをユーザに提供する米国運用のシステム。

政府が承認した形式の ID:地方自治体が発行する身分証明書の物理的又は電子的形態、又は、地方自治体が自己の公的目的のために個人の身分証明書を検証するために受諾する身分証明書の形態。

政府機関: 政府が運営する法的機関、省、支部、その他同様の国又は行政小区内の構成単位(たとえば州、県、市、郡など)

ハッシュ(SHA1、SHA256 など): あるビット単位を別の(通常、より小さい)ビット単位に置き換えるアルゴリズムで、以下のような特徴を持つ。

- あるメッセージに対し、同じメッセージをインプットとして使用してアルゴリズムを実行した場合、毎回同じ結果が得られる
- アルゴリズムを用いて生成された結果から計算して元のメッセージを復元することは不可能である
- 二つの異なるメッセージから同じアルゴリズムを用いて同じハッシュ結果を生成することは不可能である

ハードウェアセキュリティモジュール(HSM): デジタル署名及びサーバアプリケーションが重要な鍵へアクセスする際に強固な認証を行う機能など、デジタル鍵の管理と暗号化処理を行うセキュアな暗号プロセッサの一種

参照により組み込む: 組み込むとの明示により、ある文書を別の文書の一部とみなすこと。その際、当該文書の全文を読者が入手できるようにし、また別の文書の一部とすることを明記する。組み込まれた文書は、組み込む文書と同様の効力を有する。

設立機関: 民間機関にあっては、法人設立機関であって、法的存在を登録する政府機関。(例えば、設立証書を発行する政府機関)政府機関の場合、政府機関の法的存在を確立する法律、規則又は法令を制定する機関。

個人: 自然人

Internal Name(内部名称): 証明書のコモンネーム又は Subject Alternative Names フィールドに含まれる文字列(IP アドレスではない)で、 IANA のルートゾーンデータベースに登録されているトップレベルドメインで終わらないため、証明書発行時にパブリック DNS 内で グローバルに一意であることが確認できないもの。

国際化ドメイン名(IDN): 少なくとも 1 つの言語固有のスクリプト又はアルファベット文字を含み、ASCII 文字列のみを受け入れる DNS で使用するためにピュニコードでエンコードされるインターネットドメイン名。

IP アドレス: インターネットプロトコルを用いる機器に付与される、32 ビット又は 128 ビットの表示。

IP アドレス割当先: IP アドレス登録機関にて、(複数の)IP アドレス使用について管理権限を持つ主体として登録されている、(複数の)個人又は(複数の)エンティティ。

IP アドレス登録機関: The Internet Assigned Numbers Authority (IANA) 又は 地域インターネットレジストリ (RIPE, APNIC, ARIN, AfriNIC, LACNIC)。

発行局: 証明書を発行する認証局。ルート認証局であることも、下位認証局であることもある

JCAN 認証局: JCAN 認証局は、JIPDEC による JIPDEC トラステッド・サービス登録(認証局)の基準に係る審査に合格した CA であり、パブリックルート CA のサブ CA である。

JTS 登録の基準: JIPDEC による JIPDEC トラステッド・サービス登録制度の基準

JCAN LRA: 利用者の代表として JIPDEC による JIPDEC トラステッド・サービス登録の基準 (LRA)に係る審査に合格した LRA であり、JCAN 証明書ポリシー及び業務運用規程の下、JCAN 証明書に記載する DN の真正性の審査と利用者の本人確認を行い、証明書ライフサイクルマネ ージメント(発行、失効)を行う。

設立の管轄: 民間機関の場合は、適当な政府機関又は組織(例えば、法人化された場所)への申請(又はその行為)により、当該機関の法的存在が設立された国及び(該当する場合は)州又は地域。政府機関の場合、当該機関の法的存在が法律により創設された国及び(該当する場合)州又は省。

鍵の危殆化: 秘密鍵に対する権限を持たない人物に秘密鍵が漏えいした場合、権限を持たない人物による秘密鍵へのアクセスがあった場合、権限を持たない人物が秘密鍵の値を探し当てることが技術的に可能であった場合に、秘密鍵が危殆化したと称する。

鍵ペア: 秘密鍵と、その対になる公開鍵

法人: 団体、企業、パートナーシップ、自営業、信託、政府機関、その他ある国の法制度において法的地位を有するエンティティ

アクセス認証用証明書: アクセス認証用証明書は、LRA が指名する人に、GlobalSign より発行される LRA 操作責任者 用の電子証明書である。 この証明書は JCAN 証明書の発行など証明書管理サービスへのアクセスを認証するために用 いる。

北米エネルギー規格委員会(NAESB)認証局認定要件: NAESB に認定認証局として認可を受けるために認証局が準拠すべき技術的・管理要件

公開鍵基盤(PKI)のための NAESB 事業手続き基準 WEQ-012(「NAESB 事業手続き基準」): NAESB PKI 規格に準拠するために、認証局、それらの認証局によって発行された証明書、及びそれらの証明書を使用する最終エンティティによって満たされなければならない最低限の要件を定義する。

ネットワーク・タイム・プロトコル (NTP): パケット交換可変遅延データネットワーク上のコンピュータシステム間のクロック同期のためのネットワーク化プロトコル。

オブジェクト識別子(OID): ISO 規格において特定のオブジェクト又はオブジェクトクラスに付与された英数字から成る一意の識別子

OCSP レスポンダ: 証明書ステータス確認要求を処理するためリポジトリにアクセスする認証局の監督下で運営されるオンラインサーバ。オンライン証明書ステータスプロトコルの項も参照のこと。

オンライン証明書ステータスプロトコル(OCSP): 証明書に依拠するソフトウェアが証明書のステータスをオンラインで確認するためのプロトコル。OCSP レスポンダの項も参照のこと。

Payment Services Directive (PSD2): 全 EU 及び EAC 域内の決済サービス及び決済サービスプロバイダを規制する EU 指令 2015/2366

事業所の所在地: 申請者の業務を行う施設(工場、店舗、倉庫等)の所在地

秘密鍵: 鍵ペアの一方で、鍵ペアの所有者が秘密裏に保管し、デジタル署名の生成や公開鍵を用いて暗号化された電子データやファイルを復号するのに用いる。

民間団体: 非政府の法人(所有権が非公開であるか公開であるかを問わない)であって、その存在が、設立機関への申請(又はその行為)又は設立管轄権における同等のものによって創出されたもの。

PSD2 証明書: PSD2 特定の属性を含む適格証明書

PSD2 特定の属性: PSD2 証明書に特定の属性は以下の通り:

- 所轄官庁(National Competent Authority, NCA)より発行されている認証番号。若しくは、国家又はヨーロッパのレベルで認識されている登録番号、或いは信用機関への登録に含まれる法人識別子。
- 決済サービスプロバイダの一つ以上の役割
- 所轄官庁の名前 (NCAName) 及び固有の識別子 (NCAId).

公開鍵: 鍵ペアの一方で、対になる秘密鍵の所有者によって公開される鍵をいい、その秘密鍵の所有者が生成したデジタル署名を依拠当事者が検証する際、或いは対になる秘密鍵を用いてのみ復号が可能な暗号化データを生成するために使用するものをいう。

公開鍵基盤(PKI): 公開鍵暗号方式に基づき、証明書と鍵を信頼できる手法によって生成、発行、管理、使用するためのハードウェア、ソフトウェア、関係者、手続き、ルール、ポリシー、義務などを含む体制全般

パブリックに信頼される証明書: 広く普及するソフトウェアに搭載されるトラストアンカーであるルート証明書にチェーンされている事実をもって信頼を享受する証明書

適格監査人: 8.2 項(評価者の身元/能力) の要件を満たす自然人又は法人。

適格証明書: eIDAS/UK eIDAS 規則で定義された資格要件を満たす証明書。

eIDAS 適格 e シール証明書: 適格なトラストサービスプロバイダによって発行され、eIDAS/UK eIDAS 規則の付属書 III に定める要件を満たす e シールの証明書。

eIDAS 適格電子署名証明書: 適格トラストサービスプロバイダによって発行され、eIDAS/UK eIDAS 規則の付属書 I に定める要件を満たす電子署名の証明書。

適格 e シール: 適格 e シール作成装置によって作成され、適格 e シール証明書に基づく高度な e シール。

適格電子署名: 適格電子署名作成装置によって作成され、かつ、適格電子署名証明書に基づく高度な電子署名。

適格政府情報源: 政府機関によって維持されるデータベース。

適格国税情報源:民間組織、事業体又は個人に関する税務情報を具体的に記載した適格な政府情報源。

適格独立情報源:定期的に更新され、最新の公的に利用可能なデータベースであって、それが参照される情報を正確に提供することを目的として設計され、一般的に信頼できる情報源として認識されているもの。

適格電子署名/e シール作成装置(QSCD):電子署名/e シール作成装置であって、eIDAS 規則の付属書 II に規定される要件を満たすもの。

適格タイムスタンピング (QTS):eIDAS/UK eIDAS 規則 42 条に準拠するタイムスタンプを提供すること

適格トラストサービスプロバイダ(QTSP):eIDAS/UK eIDAS 規則に定義されている監督機関から適格性を認められた 1 つ以上のトラストサービスを提供する自然人又は法人

QWAC 証明書(QWAC):eIDAS/UK eIDAS 規則 45 条に符合する eIDAS 適格 SSL サーバ証明書

登録ドメイン名:レジストラに登録されたドメイン名

登録局(RA):証明書のサブジェクトの識別及び認証に責任を負う法人であり、認証局ではないため、証明書を発行したり、証明書に署名したりすることはない。登録局は証明書の申請手続き、失効手続きをサポートする。「登録局」が役割、機能を説明する場合、必ずしも独立した組織を指すとは限らず、認証局の一部であることもある。

依拠当事者:有効な証明書に依拠する自然人又は法人。アプリケーションソフトウェアサプライヤーは、単に当該サプライヤーが配布するソフトウェアがある証明書に関する情報を表示するというだけでは、依拠当事者とはみなされない。

レポジトリ:証明書ポリシーや認証業務運用規程など一般に公開される PKI 上の文書、及び CRL 又は OCSP レスポンスの形式によって配布される証明書ステータス情報などを含むオンラインデータベース

予約済み IP アドレス:以下の IANA レジストリのいずれかのエントリのアドレスブロックに含まれる IPv4 又は IPv6 のアドレス。

https://www.iana.org/assignments/iana‐ipv4‐special‐registry/iana‐ipv4‐special‐registry.xhtml
https://www.iana.org/assignments/iana‐ipv6‐special‐registry/iana‐ipv6‐special‐registry.xhtml

ルート認証局:アプリケーションソフトウェアサプライヤーが配布するソフトウェアに搭載されるルート証明書を発行するトップ階層にある認証局で、下位認証局の証明書を発行する。

ルート証明書:ルート認証局が発行し自己署名した証明書。ルート認証局の下位認証局に発行した証明書の正確性検証をするために使用される。

SSL 証明書:インターネット経由にてアクセス可能なサーバを認証する用途の証明書

サブジェクト:証明書にサブジェクトとして記載される自然人、デバイス、システム、部門、法人など。サブジェクトがデバイス又はシステムの場合、それは利用者の管理運営下になければならない。

サブジェクト識別情報:証明書のサブジェクトを識別するための情報。これには、subjectAltName エクステンションや commonName フィールドに記載されるドメイン名を含まない。

下位 CA:その証明書がルート認証局又は別の下位認証局に署名された認証局

利用者:証明書の発行を受ける自然人又は法人で、利用契約により法的に拘束される。

利用契約:認証局と申請者又は利用者との間で締結される契約で、当事者の権利義務を規定するもの

監督機関:加盟国の領域内に設立された適格なトラストサービス提供者を監督し、必要に応じて、加盟国の領域内に設立された非適格なトラストサービス提供者に関して行動をとる任務を負う機関。詳細は eIDAS 第 17 条に記載されている。

乗っ取り攻撃: 詐欺、窃盗、サブジェクトの代理人による意図的な悪意ある行為、又は他の違法行為をとおし、署名サービス又はコードサイニング証明書の秘密鍵を危殆化させる攻撃。

技術的に制約された下位 CA 証明書: 下位 CA が利用者証明書又は追加の下位 CA 証明書を発行できる範囲を制限するために、拡張キー使用と名前の制限を組み合わせて設定する下位 CA 証明書

利用条件:申請者又は利用者が認証局の関連会社である場合に、Baseline Requirements の要求事項に従い発行された証明書に関してこれを保管・使用する際に準拠すべき条項。

第三者検証者: 国内法に基づき、以下のいずれかの行為を行う能力を有し、権限を有する個人又は法人。
1. 自然人又は法人の特定の属性の検証を含む、申請者に関する事実上の主張に対する意見を述べること
2. 文書への署名の実行を認証すること。例えば、公務員、公証人、公認会計士、又は弁護士などが挙げられる。

TPM(Trusted Platform Module) : Trusted Computing Group が規定する暗号デバイス (https://www.trustedcomputinggroup.org/specs/TPM)

信頼される第三者:政府が承認した ID の書式に基づいて、個人の本人確認に使用される安全なプロセスを有するか、又はそのサービス自体が、政府が承認した ID の書式を生成するとみなされるサービスプロバイダ。

信頼できるシステム:侵入や不正使用から合理的に保護されており、適正なレベルの可用性と信頼性があり、正確に動作し、意図された機能の実行に適しており、セキュリティポリシーを厳格に適用するコンピュータ、ソフトウェア、手続きなど。

UK eIDAS 規則:eIDAS (英国の法律) と電子取引の電子識別及びトラストサービスに関する規則 2016

有効な証明書:RFC 5280 で規定される十分性の検証手続きの結果、有効であると認められた証明書。

審査要員: 当 CPS に規定される情報の正確性検証業務を行う担当者。

有効期間:証明書が発行された日から有効期限までの期間。

認証局向け WebTrust プログラム:AICPA・CICA により提供されるその時点で最新の認証局向けの WebTrust プログラム

WebTrust 保証シール:認証局向け WebTrust プログラムにおいて準拠性を証明するもの。

ワイルドカード証明書:証明書の Subject Alternative Names にワイルドカード・ドメイン名を 1 つ以上含む証明書。

ワイルドカード・ドメイン名: "*."(U+002A ASTERISK, U+002E FULL STOP)で始まる文字列の直後に FQDN を付加したもの。

WHOIS Lookup: RFC3912 で定義されたプロトコル、RFC7482 で定義されたレジストリデータアクセスプロトコル、又は HTTPS ウェブサイトを介してドメイン名登録官又はレジストリオペレータから直接検索される情報。

X.400: 電子メールのための ITU-T(国際電気通信連合-T)の規格。

X.500: ディレクトリサービスのための ITU-T(International Telecommunications Union-T)の規格。

X.509:国際電気通信連合電気通信標準化部門(ITU-T)が規定する電子証明書の規格

AATL	Adobe Approved Trust List
AICPA	米国公認会計士協会
API	アプリケーション・プログラム・インタフェース
ARL	発行局失効リスト (エンドエンティティ失効リストではなく)
CA	認証局
CAA	Certificate Authority Authorization
CCADB	Common CA Database
ccTLD	国別コードトップレベルドメイン
CICA	カナダ公認会計士協会
CP	証明書ポリシー
CPS	認証業務運用規程
CRL	証明書失効リスト
DBA	事業名
DNS	ドメインネームシステム
EIR	Electric Industry Registry
EKU	拡張鍵
EPKI	エンタープライズ PKI
ETSI	欧州電気通信標準化機構
EV	Extended Validation
FIPS	(米国政府)連邦情報処理標準

FQDN	完全修飾ドメイン名
GCC	GlobalSign Certificate Center
GPS	Global Positioning System
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICPEdu	Infraestrutura de Chaves Públicas para Ensino e Pesquisa
IETF	インターネット技術タスクフォース
ISO	国際標準化機構(International Organization for Standardization)
ITU	国際電気通信連合
LRA	ローカル登録局
NAESB	北米エネルギー規格委員会
NCA	所轄官庁(National Competent Authority)
NIST	(米国政府)アメリカ国立標準技術研究所
NTP	ネットワーク・タイム・プロトコル
OCSP	オンライン証明書ステータスプロトコル
OID	オブジェクト識別子
PKI	公開鍵基盤
PSP	決済サービスプロバイダ
QGIS	Qualified Government Information Source
QGTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
RA	登録局
RFC	リクエスト・フォー・コメンツ
S/MIME	セキュア MIME(多目的インターネットメール拡張)
SSCD	安全な署名生成装置
SSL	セキュア・ソケット・レイヤー
TLD	トップレベルドメイン
TLS	トランスポートレイヤー・セキュリティ
VAT	付加価値税

2. 公開とリポジトリの責任

2.1. リポジトリ

GlobalSign はリポジトリにおいて、全ての CA 証明書、相互認証証明書、発行した証明書についての失効情報、CP、CPS、依拠当事者規約、利用契約を公開する。GlobalSign は、発行した証明書についての失効情報及びルート証明書をリポジトリで常時供覧に付し、これらの情報の可用性について、最低 99%を保証する。また、計画的なダウンタイムに関しても 0.5%を超えないものとする。

GlobalSign は証明書のステータス情報を提供する際、一般にアクセス可能なディレクトリにおいて提出された情報を公開する。

GlobalSign はセキュリティ管理、業務の手続き、及び社内セキュリティポリシーといった、機密性の高い文書については公開しない。但しこれらの文書は、GlobalSign で WebTrust 又は ETSI の監査が実施される際、必要に応じて適格監査人に提供される。

GlobalSign 及びそのグループ会社は、本 CPS の翻訳版及びそれを公開するウェブサイト、その他の文書を、販売活動の目的で提供する。しかしながら、GlobalSign のリポジトリは https://www.globalsign.com/repository 及び https://www.globalsign.com/en/company/corporate-policies であり、言語によって何らかの不一致がある場合は、英語版を優先して解釈・適用する。

2.2. 証明書情報の公開

GlobalSign は CP、CPS、利用契約、依拠当事者規約を https://www.globalsign.com/repository に公開する。CP 及び CPS は、RFC 3647 で要求される全ての項目を含み、RFC 3647 に従って構成されている。CRL はオンラインリポジトリで公開する。CRL には、有効期限が満了しておらず、有効であり、かつ失効された全ての証明書が、種類及び証明書チェーン内の証明書の位置に応じて掲載されている。

GlobalSign は、アプリケーションソフトウェアサプライヤーがパブリックに信頼される各ルート証明書にチェーンする利用者証明書で、自社のソフトウェアをテストできるテストページを運用している。
以下は、(i)有効期間内、(ii)失効済、(iii)有効期限切れの証明書のテストページである。

ルート R1:
https://valid.r1.roots.globalsign.com
https://revoked.r1.roots.globalsign.com
https://expired.r1.roots.globalsign.com

ルート R3:
https://valid.r3.roots.globalsign.com
https://revoked.r3.roots.globalsign.com
https://expired.r3.roots.globalsign.com

ルート R5:
https://valid.r5.roots.globalsign.com
https://revoked.r5.roots.globalsign.com
https://expired.r5.roots.globalsign.com

ルート R6
https://valid.r6.roots.globalsign.com
https://revoked.r6.roots.globalsign.com
https://expired.r6.roots.globalsign.com

ルート R46
https://valid.r46.roots.globalsign.com
https://revoked.r46.roots.globalsign.com
https://expired.r46.roots.globalsign.com

ルート E46
https://valid.e46.roots.globalsign.com
https://revoked.e46.roots.globalsign.com
https://expired.e46.roots.globalsign.com

2.3. 公開の時期及び頻度

CA 証明書は発行後すぐにサポートページからアクセス可能なリポジトリに公開する。

GlobalSign は、GlobalSign の認証局(CA)の運用が正確で透明性が高く、先述の「前提確認事項」に記載されている外部要求事項に準拠するように、少なくとも年 1 回、CP 及び CPS を見直し、適切な変更を行う。GlobalSign は CA/B Forum が行う決議及び要求事項の更新を注視し、それらの更新事項を GlobalSign の業務に適時反映する。GlobalSign CP、本 CPS、利用契約、依拠当事者契約の新版及び改訂版は、PACOM1 - CA Governance により、タイムスタンプ付きの Adobe AATL PDF 署名証明書を用いてデジタル署名された後、7 日以内に公表されるものとする。

2.4. リポジトリへのアクセス管理

GlobalSign は、読取のみ可能な形で公開リポジトリを公開している。
そのために、権限のない人物によるリポジトリの内容への追記、消去、又は改変を防ぐ論理的及び物理的セキュリティ対策が実施されている。

3. 識別と認証

GlobalSign は RA の役割を担い、証明書の申請者の身元情報及びその他の属性情報を認証し、これら情報を証明書に入れる前に、真正であることを審査・認証する。

証明書申請者は、他者の知的財産権を侵害する名称を証明書内で使用してはならない。GlobalSign は、申請者が申請に含まれる名称の知的財産権を有する者であるかを検証せず、またドメイン名、商標、サービスマークの所有に関連する紛争について、調停、仲裁、その他の方法で解決に関与しない。GlobalSign は、証明書申請者に対しなんらの義務を負うことなく、係る紛争を理由として申請を却下する権利を有する。

GlobalSign RA は、証明書の失効を申請する者について、係る権利を有する者であることを認証する。

3.1. 名称

3.1.1. 名称の種類

GlobalSign が発行する証明書に含まれるサブジェクト識別名は、X.500「名称」、RFC 822「名称」、及び X.400「名称」に規定される要求事項に準拠している。識別名は、名前空間において一意であることを担保し、誤解を招くものを含まない。しかしながら、DV TLS、OV TLS や IntranetSSL Common Names といったいくつかの証明書は、発行する証明書に RFC 2460(IPv6)又は RFC 791(IPv4)に規定される IP アドレスを記載することがある。

ワイルドカード SSL 証明書では、ワイルドカードを示すアスタリスク(*)を、CN 又は SAN に入れる最初の文字として、ドメイン名に含んで発行する。この証明書を発行するに先立って、GlobalSign はレジストリ管理下のドメイン名又は「パブリック・サフィックス」の直前に、ワイルドカード文字(アスタリスク)が CN 又は SAN に挿入されていないか(たとえば、「*.com」や、「*.co.uk」など。詳しくは RFC 6454 の 8.2 章を参照のこと)を判定するためのベストプラクティスを遂行する。証明書を申請するドメイン名空間が利用者に所有又は管理されていない場合、GlobalSign は前述のようなワイルドカード SSL 証明書の申請を却下する。

JCAN 認証局は、 JCAN 認証局の領域内において利用者に割り当てられた識別名の唯一 性を保証する。また、サブジェクトの OrganizationUnitName1 の唯一性を保証する。

3.1.2. 意味のある名称である必要性

GlobalSign の製品が、役職名や部署名を記載すること、さらに DN に OU のフィールドを含むことを許可している場合には、一般的な DN 要素を持つ証明書の中から依拠当事者が特定の証明書を識別することを可能にするために、付加的な固有の要素が DN の OU フィールドに設定されることがある。

3.1.3. 利用者の匿名又は仮名の使用

GlobalSign は、ポリシーにおいて禁じられていない場合、及び名前空間における一意性が担保される場合、匿名又は仮名 (「かめい」、(Pseudonym)) のエンドエンティティ証明書を発行することがある。GlobalSign は法の求めるところにより、利用者の身元情報を開示する権利を有する。証明書の国際ドメインネーム(IDN)の要求は、追加の手動レビューを受けることとなる。デコードされたホスト名は、フィッシングや他の不正な使用の危険性を低減するために、追加のレビューを受けることとなる。デコードされたホスト名は、以前に却下された証明書申請や失効された証明書と照合される可能性がある。GlobalSign は、リスク低減基準に基づいて申請を拒否することができる。例えば、フィッシング又はその他の不正使用の危険性がある名称、Google Safe Browsing List に掲載されている名称、又は Anti-Phishing Working Group が管理するデータベースに掲載されている名称などがそれに該当する。

3.1.4. 様々な形式の名称の解釈方法

証明書内の識別名の記載にあたっては、X.500 規格及び ASN.1 の構文を使用する。統一資源識別子(URI)及び HTTP 構文において X.500 に規定される証明書内の識別名を解釈する方法については、RFC 2253 及び RFC 2616 を参照のこと。

3.1.5. 名前の一意性

GlobalSign は証明書内のサブジェクト名の一意性を以下の通り担保する。下記にある「Class」の定義については、3.2.3 項を参照。

- **PersonalSign1 Certificates:** 電子メールアドレスのみ (Class 1)
- **PersonalSign Certificaets:** 電子メールアドレス及び個人名。並びに、パスポートを発行した国名(Class2)又は個人が GlobalSign (Class 2)へ提供する同等の身分証明

- **PersonalSign Pro Certificates:** 組織名及び、場合によっては組織の州及び地域と関連付けられた電子メールアドレス(証明書に含まれる場合)。並びに、個人名又は部署名及び、場合によっては部門名(Class 2)。
- **PersonalSign 3 Pro Certificates:** 組織の名称・州かつ/又は地域及び、パスポート上、又は個人がGlobalSign 又は信頼された第三者(Class 3)に提出する同等の身分証明上の個人名と対応した電子メールアドレス
- **Code Signing Certificates:** 組織の名称・州かつ/又は地域 (Class2)
- **EV Code Signing Certificates:** 組織名、事業分類、法人格が登録された管轄地、登録番号、及び地理上の住所(Class3)
- **SSL Certificates (Non EV types):** 組織の名称・州かつ/又は地域に対応し、ICANN により認められたドメイン名の最小単位を commonName に記載
- **SSL Certificates (EV):** 組織名、事業分類、法人格が登録された管轄地、登録番号、及び地理上の住所に対応し、ICANN により認められたドメイン名の最小単位を commonName に記載
- **Time Stamping Certificates:** 組織の名称・州かつ/又は地域、電子メールアドレス(Class 2)を付加することもある
- **NAESB Rudimentary:** 電子メールアドレスのみ(Class 1)
- **NAESB Basic、Medium A:** 組織の名称及び住所、加えて個人名又は部門名と対応した電子メールアドレス(証明書の subjectDN に含まれる場合)。
- **AATL Certificates:** 組織の名称と州かつ/又は地域、又は個人名と州かつ/又は地域で、任意の電子メール・アドレス(クラス 2)を持つ、従業員、代理人、請負業者、取引先、又は顧客の何れかとして組織に所属する個人の名前。
- **Qualified Certificates:** 個人名と居住地の州及び所在地(組織名なし)、又は組織の名称と組織の州かつ/又は所在地(eIDAS 適格電子署名証明書)、又は組織の名称と識別子及び住所(eIDAS 適格 e シール証明書)(Class3)。
- **S/MIME Certificates:** 固有のメールアドレスに組織名及び、州かつ/又は所在地に加え、組織と関連する個人名又は部署名を紐づけたもの(Class2)
- **JCAN Certificates:** 一意のメールアドレス(証明書に記載される場合)で、組織名と紐づけられる。任意で組織が登録されている州、地域、および組織に所属する個人名または部署名、任意で組織単位(Class2)とも紐づけられる。

3.1.6. 商標の認知、認証、役割

利用者は、他のエンティティの知的財産権を侵害する内容を含む証明書を申請してはならない。特に別段の定めのない限り、GlobalSign は申請者が商標の所有権を有するかどうかを検証しない。しかしながら、GlobalSign は係争中の商標権を含む証明書を失効する権利を留保する。

3.2. 初回の身元情報の十分性検証

GlobalSign は、認証局のチェーニングサービスなどの利用を申し込む法人・個人の申請者の身元情報を識別するために必要な連絡、調査などにおいて、あらゆる法的手続きを用いる。

GlobalSign は、初回の身元情報の十分性検証の結果、真正と認められた身元識別情報を、事後に別の情報及び新規に検証した情報と組み合わせ、別の製品を提供する際にも使用することができる。GlobalSign Certificate Center (GCC)アカウントにログインが可能であることをもって、検証済の情報に依拠して証明書の発行ないしサービスの提供を受ける権利を有することを確認する。GCC アカウントは、3.3.1 項の正確性の再検証要件がその GCC アカウント保有者によって遵守されているという条件のもと、過去に審査された再申請者についての情報を再利用できるかどうかを認証するために使用される。

3.2.1. 秘密鍵の所有を証明する方法

(規定なし)

3.2.2. 組織の識別情報の認証

GlobalSign は、GlobalSign が加盟する様々なルートプログラム、並びに Baseline Requirements、EV ガイドライン及び Baseline Requirements for Code Signing の要求事項に準拠するよう、定期的にレビューされるよう社内ポリシー及び手続きを定めている。十分性検証ポリシー及び手続き文書は、WebTrust Program for CAs の Principle 6 の基準を満たす PACOM5 - Subscriber Validation (1.5.1 項の主なポリシー機関の下位機関)の管理下にある。

GlobalSign が組織のアイデンティティを検証する方法は、通常は全製品・サービスの種類において一貫しているが、以下にあげる、より一般的に使用されている QGIS 手法で認証ができない場合には、あらかじめ容認された方法に従った代替手段を使用することがある。

組織情報を含む全ての証明書について、申請者は、組織名及び登録の又は商業上の住所の提出を求められる。組織の識別情報を含む全ての証明書について、GlobalSign は法的実在性、識別情報、法的名称、仮名(該当する場合)、法的形式(設立の管轄区域における要請又は法的名称の一部に含まれる場合)、要求された組織の住所及び信頼できる通信手段を認証する。EV 証明書では、GlobalSign はさらに物理的な実在、運営上の実在、及び追加の十分性検証を行う必要がある場合には、信頼できる通信手段を検証する。

これらの情報は、以下の何れかの十分性の検証方法を用いて認証することができる。

- 申請者の管轄の政府機関（QTIS 又は QGIS、法人設立機関又は登録機関を含む）、又は申請者が政府機関と名乗っている場合は申請者より上位の政府機関 (設立機関又は登記機関、及び QTIS を含む、QGIS)への確認
- QIIS
- 認証済みの弁護士意見書又は会計士意見書
- 申請者からの独立した確認書

加えて、EV 証明書以外の証明書については、 GlobalSign は以下の信頼できるデータソースの何れかを用いて申請者の情報の十分性を検証することがある。

- 会計士、弁護士、政府関係者、又はその他の信頼できる第三者によって書かれた、対象情報が正しいことを証明する書簡。
- GlobalSign が合理的に正確かつ信頼できると判断した文書、一般的には公共料金の請求書、銀行取引明細、クレジットカード明細、政府発行の税務文書、その他 GlobalSign が正確であり信頼に足ると判断した証明書類。これらの文書は、営利企業や政府の間で信頼できると認められており、申請者が証明書を取得する以外の目的で第三者が作成したものである。
- 申請者が証明書を取得する以外の目的で第三者が作成した第三者データベース。このデータベースは、商業界や政府の間で信頼できると一般的に認識されており、情報を検証するために使用され、定期的に更新される。この第三者のデータベースは、その信頼性、正確性及び変更や改ざんへの耐性について GlobalSign が評価する。

これらの十分性の検証方法は、業界標準に基づいて使用される。全ての十分性の検証方法が全ての状況で受け入れられるわけではなく、また、全ての種類の情報に使用できるわけではない。

GlobalSign は自社ウェブサイトのレポジトリにおいて「十分性検証資料(Validation Resources)」として、設立機関又は登記機関の一覧を公開している。

申請者が組織を代表して証明書を申請する権限を有するかについては、以下、3.2.5 項に従って検証する。

3.2.2.1. LRA の認証

ePKI 及びマネージド SSL サービスで使用するアカウントについては、GlobalSign は、認証済の組織情報をプロファイルとして設定する。権限が付与されていると認証を受けたアカウント管理者が、LRA の業務を担当し、証明書を申請する申請組織に属する個人、ないし組織が所有又は管理下におくサブドメインの認証を行う。(LRA は契約に基づき個々の認可を行う権限を有するが、対象全ドメインは全て、事前に、本 CPS 及び CA/B Forum の基本要件に従い事前に許諾されたところの上位レベルドメインを有することが要件となる。)

3.2.2.2. 役職情報を含む証明書の認証(DepartmentSign)

GlobalSign は、機械や装置や組織の部署、或いは役職に対する証明書を発行するにあたって、認証局に代わって業務を担当する RA、又は発行 CA・RA との契約に基づき義務を負う LRA に、それら機械や装置や組織の部署、或いは組織内の役職名及び組織の事業を正確かつ正しい方法で認証させなければならない。

3.2.2.3. 適格証明書

GlobalSign は以下の通り、組織情報を含む適格証明書を 3 種類発行する。

- eIDAS 適格 e シール証明書(組織情報を証明)
- eIDAS 適格電子署名証明書(個人が組織に所属することを証明)
- eIDAS 適格 SSL サーバ証明書（QWAC 証明書）

組織情報を含む全ての適格証明書について、申請者は、法人の正式名称(法的形式を含む)及び事業所の物理的な所在地の住所を示すことが求められる。

GlobalSign は、以下を参照して、法的存在と住所を確認する。
- Qualified Government Information Source に掲載されている公式の政府記録、又は
- 組織の法的設立、法的存在又は法的認知を有する管轄区域の政府機関により確認、若しくは提供される文書
- Qualified Government Information Source により提供される記録

さらに、GlobalSign は、以下を参照して住所を検証することができる。
- 検証された弁護士意見書又は会計士意見書
- 当該組織の有効な適格 e シールを用いて署名された物理的所在地の証明

その証明の記載事項は、適格証明書の内容と一致していなければならない

適格証明書には、組織の正式名称、ビジネス上の名義(商号又は取引における名義)も含めることができる。GlobalSign は、組織が、事業所管轄区域において、ビジネス上の名義を含む名称を適切な政府機関に登録したこと、及び当該登録が引き続き有効であることを確認する。

本人が組織に所属していることを主張する証明書に関して、GlobalSign は、下記の事項に基づいて、本人の所属を確認する。
- 機関が提供する確認であって、検証された伝達方法を用いて取得したもの
- 組織からの独立した確認
- 検証された弁護士意見書又は検証された会計士意見書
- 組織の有効な適格 e シールによって署名された証明
- 権限が付与されていると認証を受けたアカウント管理者が LRA の余地を埋めるため取得した証明

組織の同一性を主張する適格証明書及び QWAC 証明書については、GlobalSign は、組織の権限を付与された代表者の同一性及び権限を検証する。

GlobalSign は、下記事項を参考に、権限を与えられた代表者の権限を確認する。
- Qualified Government Information Source が提供する公式の政府記録
- 組織の法的設立、法的存在又は法的認知を有する管轄区域の政府機関により確認、若しくは提供される文書
- Qualified Government Information Source により提供される記録
- 検証された弁護士意見書又は会計士意見書
- 組織の有効な適格 e シールを用いて署名された証明(その証明の記載事項は、適格証明書の内容と一致していなければならない)

GlobalSign は、セクション 3.2.3 に従って、授権された代表者の身元を確認する。

GlobalSign は、関連会社又はこれらの関連会社と関係があることが特定されている個人のために、証明書を購入することがある。GlobalSign の関連会社としては、親会社及び子会社、及び GlobalSign と同一の親会社を持つその他の企業がある。
GlobalSign は PSD2 の特有の属性について、国立の監督当局から提供された情報を用いて属性を検証する。これには、国立の登録局等の所轄官庁、ヨーロッパ銀行の登録局、及び所轄官庁からの認証された通信が含まれるが、これに限定されない。

GlobalSign は新たに発行された証明書に記載の所轄官庁への通知に用いられる新しい電子メールアドレスを通知された場合、その電子メールアドレスに証明書の 16 桁のシリアルナンバー、サブジェクトの識別名、証明書発行者の識別名、証明書の有効期間、失効申請の連絡先、指示、証明書ファイルのコピーなどの情報を平文で送信する。

3.2.3. 個人の身元情報の認証

GlobalSign は個人に発行する証明書のクラスに応じて、以下の通り認証する。

3.2.3.1. Class 1

申請者は証明書に記載する電子メールアドレス又はドメイン名に対する管理権限を証明する。GlobalSign は、申請者が GlobalSign のサービスを申請・登録する際に提示する可能性があるその他の情報/属性を認証しない。この認証方法は DV 証明書に適用される。

DV 証明書 について、申請者は、証明書に記載される予定である全てのドメイン名に対する管理権限を証明することが要求される。

3.2.3.2. Class 2

申請者は、証明書申請に含まれている場合、証明書に記載する電子メールアドレスやドメイン名といった、特定の身元属性に対する管理権限を証明する。この認証方法は OV 証明書に適用される。

OV 証明書について、申請者は、証明書に記載される予定である全てのドメイン名に対する管理権限を証明することが要求される。

申請者はまた、政府機関発行の有効な身分証(運転免許証、軍人身分証明書、その他同様のもの)又は写真付き ID カードの判読可能なコピーの提出を求められる可能性がある。また、政府機関発行以外の身分証、写真付き ID カードの提出を求められることもある。GlobalSign は証明書申請に含まれる名前と身分証に記載される名前、及び国、州、その他の住所の情報が一致することなど、適切なレベルで本人確認が行われることを担保する。GlobalSign は、身分証の写しに記載される名前が証明書申請に含まれる名前と一致すること、及び国名、州名、居住地などの他のサブジェクト情報が正しいことを、合理的なレベルで保証する。

GlobalSign は申請者の本人識別情報を以下の何れか一つの方法によって認証することができる。

1. 申請者の電話番号を信頼できる情報源から入手し、電話によるチャレンジ・レスポンスを求める。
2. 申請者の FAX 番号を信頼できる情報源から入手し、FAX によるチャレンジ・レスポンスを求める。
3. 申請者の電子メールアドレスを信頼できる情報源から入手し、電子メールアドレスによるチャレンジ・レスポンスを求める。
4. 申請者の住所を信頼できる情報源から入手し、郵便によるチャレンジ・レスポンスを求める。
5. (管轄地域の法令上、文書への署名として使用が許可されている場合、) 書面にて受領した申請にて印影を確認する。

AATL に対しては、以下の何れか一つの方法によって認証することができる。その他の Class 2 の商材に対しても有効である。

1. 正当な公証人、又は信頼できる第三者機関から、政府が承認した形式の ID に基づき個人の身元が検証されている旨の証明を受ける。
2. 組織に所属する個人の場合、GlobalSign は少なくとも当人固有の生体認証の1要素を含む、履行済の申告(指紋又は手書きの署名など)を取得する。このアイデンティティを保有する個人について、電子証明書に記載されている組織の代表権限を保有する者は、この個人を目視したこと、当個人の写真付き ID を照合したこと、そして証明書申請内のアイデンティティに関する情報が照合された写真付き ID のものと一致していることを確認する。これらの文書の正当性については、Qualified Independent Information Source 又は a Qualified Government Information Source 上の連絡先から当代表者に連絡することで、GlobalSign が直接確認をとる。当代表者の保有する組織の代表権限については、GlobalSign が EV ガイドラインに従って確認する。
3. 組織に属する個人の場合、承認された LRA に証言を依頼する可能性がある。マネージド PKI 又はマネージド SSL のプロファイルを通して Class 2 の証明書申請があった場合、3.2.3.5 項を参照。
4. 政府が承認した形式の ID の正確性検証に基づいて、組織が自身のエンドユーザの身元を検証し、組織がこれらの正確性検証についてセキュアで監査可能な証跡を維持していることを、組織から証明してもらうこと。
5. 適格証明書について行う個人への正確性検証に沿った、その他の正確性検証方法。

AATL については、GlobalSign は、映像ベースの面談又は同等の保証を有する方法によって、個人の身元確認と、政府が認めた形式の ID の検証を実施することができる。

GlobalSign は、申請者にさらに情報を提出することが求めることがある。また同じレベルの信頼性を担保する上記以外の方法を採用することもある。

証明書申請に電子メールアドレスが含まれる場合、GlobalSign 又は LRA はその電子メールアドレスの真正性及び所有者を検証しなければならない。

3.2.3.3. Class3

EV コードサイニング証明書について、申請者は証明書に記載する電子メールアドレスに対する管理権限を証明することが要求される。

EV SSL 証明書について、申請者は証明書に記載される予定である全てのドメイン名に対する管理権限を証明する。

申請者は政府機関発行の有効な身分証(運転免許証、軍人身分証明書、又はその他同様のもの)又は写真付き ID カードの判読可能なコピーを提出する。付加的に、政府機関発行以外の身分証、写真付き ID カードの提出を求められることもある。GlobalSign 又は信頼される第三者は、身分証の写しに記載される名前が証明書申請に含まれる名前と一致すること、及び国名、州名、居住地などの他のサブジェクト情報が正しいことを、合理的なレベルで保証する。

政府発行の国の身分証明書又は写真 ID の写しの提出が現地の法律又は規則により禁止されている場合、GlobalSign は、申請者の身元を認証するために代替手段を用いなければならない。この場合、GlobalSign は、本人確認を行う権限を有する信頼できる第三者から証明又は文書を受け取るものとする。

「信頼される第三者」とは、関連する規則及び規制に準拠して本人確認サービスを提供し、当該規則及び規制に準拠していることを第三者により証明される事業体を意味する。

PersonalSign 3 Pro の申請においては、申請者のアイデンティティを確立するために、申請者との面会が必須である。これには公証人又は信頼できる第三者による、申請者に対面しその写真付き身分証を検証したという証言及び、申請情報が正確であるという証言が求められる。 GlobalSign は、映像ベースの面談又は同等の保証を有する方法によって、個人の身元確認と、政府が認めた形式の ID の検証を実施することができる。

申請者はまた、電子証明書に含まれることになる電子メールアドレスを管理していることを証明するよう求められる。
GlobalSign はまた、EV ガイドライン及び Baseline Requirements for Code Signing に準拠した申請者との信頼できる通信方法として GlobalSign によって検証された信頼できる伝達手段を用いて、証明書のサブジェクトになる団体を代表する申請者の権限を認証する。

申請者又は申請者の属する組織は、さらに情報を提出することが求められることがある。また同じレベルの信頼性を担保する上記以外の方法を採用することもある。

3.2.3.4. 適格証明書

GlobalSign は、以下の方法を用い、eIDAS の第 24.1 項に従って、個々の利用者のアイデンティティを検証する。

- 対面による本人確認
- 電子的な識別手段の使用
- 適格電子署名の使用
- ビデオによる正確性検証

3.2.3.4.1. 対面による正確性検証

対面による正確性検証においては、利用者が物理的に存在している必要があり、以下の文書の提出が必要である。

- 政府発行写真付き ID
- 署名されたパーソナル・ステートメント

個人の肖像を写真付き ID と比較し、写真付き ID のセキュリティ機能を検査する。パーソナル・ステートメントの署名は、写真付き ID の署名と比較される。
この正確性検証は、第三者検証者により実施される場合がある。

申請者の同一性を確認するため、又は証明書に含まれる名前以外の情報を検証するために、追加の二次的証拠が必要な場合がある。

3.2.3.4.2. リモート環境での電子的な識別手段の使用

GlobalSign は電子的な方法で個人の身元の検証を行うこともある。
全ての電子的な識別手段は、eIDAS 規則第 8 条に定める「実質的」又は「高水準」の保証水準を有する。また、発行に先立ち、本人の物理的存在が保証される。

1. 通知された電子的な識別スキームについては、保証水準は、加盟国から欧州委員会への通知によって決定される。
2. 通知されていない電子的な識別手段については、保証水準は欧州委員会によって記述された要件に従って決定される。適合性評価機関による審査の後、GlobalSign は、本項に定めている電子的な識別手段を受け入れる前に、審査結果を監督機関に提出し、許可を受ける。

3.2.3.4.3. 適格電子署名

GlobalSign は、利用者の有効な適格電子署名を個人のパーソナル・ステートメントに使用して、適格電子署名を作成するために使用される証明書に含まれる申請者の身元及び追加属性を確認する。これらの証明書は eIDAS 第 24.1 項(a) 又は (b)に従って発行されなければならない。

3.2.3.4.4. ビデオによる正確性検証

GlobalSign は、ビデオ検証を使用することができる。利用者は、対面証明と同様に、以下の文書を提供することが求められる。

- 政府発行写真付き ID
- (電子的に)署名されたパーソナル・ステートメント

申請者の同一性を確認するため、又は証明書に含まれる名前以外の情報を検証するために、追加の二次的な証拠文書を必要とする場合がある。

個人の肖像を写真付き ID と比較し写真付き ID のセキュリティ機能を検査する。この方式では、利用者がインターネット対応機器、ウェブカメラ又は他のビデオ機器、マイク及びサウンドシステムを利用できることを前提とする。

3.2.3.5. ローカル登録局認証

組織アカウントはローカル登録局（以下「LRA」）と考えることができるが、GlobalSign は、このアカウントに対し、認証済の組織情報をプロファイルとして設定する。こうしたアカウント内の証明書はプロファイルの情報を利用する。LRA 組織は証明書を申請する申請組織に属する個々を認証する契約上の義務を負う。

3.2.3.6. 北米エネルギー規格委員会（NAESB）向け証明書

北米エネルギー規格委員会（以下「NAESB」）向け証明書申請については、関連会社による利用者証明書の組織情報の真正性を確認するために、組織名、住所、及び組織が存在することの証明文書を含まなければならない。GlobalSign 若しくは RA は、申請者の真正性及び申請者の当該組織における申請権限の有無も含めて、情報の検証をしなければならない。WEQ-012 の申請のために証明書を利用している利用者は、法的な事業識別情報を登録する義務があり、NAESB の EIR に登録され、利用者申請時や発行時に使用するための「エンティティコード」を確保しなければならない。WEQ-012 の申請以外の目的で、エネルギー産業内で使用される証明書を発行する場合、ACA は、NAESB EIR 内で利用者登録を必要とする WEQ-012-1.9.1、WEQ-012-1.3.3 及び WEQ-012-1.4.3 の規定を除き、NAESB WEQ-012 Public Key Infrastructure Business Practice Standards and Models の規定に準拠しなければならない。

GlobalSign は RA 運用を自社で実施するか、提供するマネージドサービスの一つを通して、RA 運用/機能の一部若しくは全てを別の法人に外部委託することを選ぶことが可能である。どちらの場合においても RA 運用/機能を行う組織は身元証明、監査、ログ保存、利用者情報の保護、データ保存やその他 CP 及び NAESB 要件及び NAESB Business Practice Standards に RA が実施すると定められている手続きを実施しなければならない。社内で RA 運用/機能を実施する場合、認証局に課せられた責務として、全ての RA 運用/機能に係る RA インフラ及び手続きは上記要件に準拠しなければならない。NAESB 認定認証局及び/又は委任されたエンティティは、RA 運用/機能を行う全ての当事者が NAESB 認定認証局要件を理解し、同意していることを保証しなければならない。

GlobalSign、及び/又は関連する RA は申請者の身元情報が GlobalSign の CP/CPS に記載されたプロセスにより審査されることを保証しなければならない。審査プロセスは証明書レベルにより異なり、NAESB Accredition Specification に記載されなければならない。尚、文書及び審査要件は保証レベルにより異なる。

身元情報を証明する手続き要件は以下の通り行う。

NIST Assurance Level	NAESB Assurance Level
レベル 1	Rudimentary 最小限
レベル 2	Basic 低度
レベル 3	Medium 中程度

GlobalSign 又は指定された RA(マネージド PKI の場合)は、申請者により提供された識別情報を全て、section 2.2.2: Authentication of Subscribers of the “NAESB Accreditation Requirements for Authorized Certification Authorities にて説明されている、Identity Proofing Process (IPP) Method に従って審査しなければならない。

3.2.3.7 JCAN 証明書におけるサブジェクトの確認

サブジェクトの登録に使用される情報は、以下に示した書類、コピー、データベース、データ （パートナーの所属組織が証明書記載事項を管理していることを示したもの）である。 当該情報及び発行の記録（本人確認資料、同意書等）は、当該組織の他部門で保管されている場 合を除き、紙又はデータとして保管される。 当審査記録を再利用することはできない。

(1) JCAN Advanced

JCAN 証明書の各申請ごとに、以下のいずれかの信頼できる書類又はそのコピー/データベース（人事台帳等）でサブジェクトの確認を行う。
· 住民票の写し
· マイナンバーカード(個人番号カード)
· 地方税特別徴収税額決定通知書
· 雇用保険被保険者
· 住民税
· 扶養控除
· 保険料控除情報
· 保険証、運転免許証、パスポート等の有効期間がある公的証明書を根拠資料
· 信頼できるデジタル証明書

1. CommonName に名前（実名又は PS 名）を記載する場合、上記信頼できる書類又はそのコピー/データベースで当該名の確認を行う。
2. OrganizationUnitName2 and/or CommonName に組織名を記載する場合、以下のいずれかの信頼できる書類又はそのコピー/データベースで当該組織名の確認を行う。
· 信頼されるデータベース
· 上記信頼できる書類
3. rfc822Name に Email アドレスを記載する場合、Email アドレスが当該組織に登録されていることをセクション 3.2.4 の通り GlobalSign とともに確認を行う。

(2) JCAN Basic

JCAN 証明書の各申請ごとに、 LRA は次の 1 つ以上の書類、そのコピー、データベース、データ（パートナーの所属組織が証明書記載事項（組織名、名前、Email アドレス、オブジェクト）を管理していることを示したもの）で「サブジェクトの属性」の確認を行う：

1. CommonName に名前（実名又は PS 名）を記載する場合
· 社員証、学生証等
· 組織が発行する在籍証明書
· 信頼されるデータベース
· 有効で失効されていないクレジットカード
· JCAN アドバンストに示す信頼できる書類
注）PS 名の確認は不要
2. OrganizationUnitName2 and/or CommonName に組織名を記載する場合
· 信頼されるデータベース
· JCAN アドバンストに示す信頼できる書類
3. OrganizationUnitName2 and/or CommonName にオブジェクトの名前、識別子を記載する場合
· パートナーの所属組織が当該オブジェクトを管理していることを示した電子文書
4. rfc822Name に Email アドレスを記載する場合
· パートナーの所属組織が当該 Email アドレスを管理していることを示した電子文書

3.2.4. 検証されない利用者情報

SSL 証明書又はコードサイニング証明書の Subject:OrganizationalUnitName フィールドが、特定の自然人や法人を指す名称、事業名、商号、住所、所在地、又はその他のテキストを含む場合を除き、GlobalSign は Subject:OrganizationalUnitName フィールドを検証しない。

- 証明書に記載されている名称、事業名、商号、住所、所在地を明確に示していない場合、或いはテキストが特定の自然人や法人を指していない場合、例えば「マーケティング」のような一般的な名称の場合又は

デバイスの実際のシリアル番号など、GlobalSign はこの項目が本項に記載されている検証されていない利用者情報として扱われることを免責する。

業界標準により許可されている場合、検証されていない利用者の情報の所在地として、SerialNumber をサブジェクトとして利用することができる。

Intranet SSL/TLS の証明書に限っては、GlobalSign は申請者の希望により、インターナルネットワーク内で使用されるドメイン名、非公開ドメイン名、ホスト名、RFC 1918 に規定される IP アドレスなどを、証明書の SubjectAlternativeName フィールドに記載する。

GlobalSign は EPKI サービスを通じ、エンドユーザ、ロール、デバイスに対し、クライアント認証、文書署名、セキュアメッセ ージに最も一般的に使用される証明書を提供する。ローカル登録局は、デバイス名、役割、名前の検証を行うことが契約上義務付けられている。

3.2.5. 権限の十分性検証

PersonalSign1 Certificate	チャレンジ・レスポンス方式を用いて申請者が証明書に記載される電子メールアドレスを管理していることを検証する。
PersonalSignDemo Certificate	申請者が証明書に記載される電子メールアドレスを管理していることで正確性検証をする。
PersonalSign2 Certificate	信頼できる方法による申請者個人との連絡を通じた検証に加え、証明書に記載された電子メールアドレスを管理していることで正確性検証をする。
NAESB Certificate	3.2.3.5 項の規定に従い、信頼できる方法による申請組織又は個人との連絡を通じた検証に加え、申請者が証明書に記載される電子メールアドレスを管理していることで正確性検証をする。
PersonalSign2 Pro	申請者個人との信頼できる連絡手段を通し正確性検証をすると同時に、必要に応じ、証明書に記載される電子メールアドレスをその申請者が管理していることの正確性検証をする。マネージド PKI アカウントにより発行された証明書は、プロファイル設定時に、LRA の権限者を検証する。
PersonalSign2 Department Certificates	申請者個人との信頼できる連絡手段を通し正確性検証をすると同時に、必要に応じ、証明書に記載される電子メールアドレスをその申請者が管理していることの正確性検証をする。マネージド PKI アカウントにより発行された証明書は、プロファイル設定時に、LRA の権限者をが検証する。
PersonalSign3 Certificate	申請組織との信頼できる連絡手段を通し、申請者が組織を代表して証明書を申請する権限を有することの正確性検証をする。申請者の身元証明のため、申請者が RA 担当者と面会して身分証を提示することが必須である他、証明書に記載される電子メールアドレスをその申請者が管理していることの正確性検証をする。
S/MIME Certificates	申請者組織又は個人との信頼できる連絡手段を通し正確性検証をすると同時に、証明書に記載されるメールアドレスをその申請者が管理していることの正確性検証をする。
Code Signing Certificates	申請組織又は個人との信頼できる連絡手段を通し検証すると同時に、オプションとして証明書に記載される可能性がある電子メールアドレスをその申請者が管理していることの正確性検証をする。
EV Code Signing Certificates	EV ガイドライン及び Baseline Requirements for Code Signing の規定に従い、契約署名者及び証明書承認者の権限を検証する。
DV/AlphaSSL Certificates	3.2.7 項に規定されている十分性の検証方法の一つを使用し、申請者がドメイン名を保有又は管理していることの十分性を検証する。
OV SSL & ICPEdu Certificates	3.2.7 項に規定されている方法を通し、申請組織又は個人との信頼できる手段による意思確認を通し正確性検証をすると同時に、必要に応じ、証明書に記載されるドメイン名を申請者が保有又は管理していることの正確性検証をする。マネージド SSL アカウントによって発行された証明書は、プロファイル設定時に、その権限を有する LRA が検証する。
EV SSL Certificates	EV ガイドラインに従い、契約署名者及び証明書承認者の権限の正確性検証をする。同時に、3.2.7 項に規定されている方法を通し、申請者がドメイン名を保有又は管理していることを検証する。マネージド SSL アカウントによって発行された証明書は、プロファイル設定時に、その権限を有する LRA が検証する。
Timestamping Certificates	組織の申請者との信頼できる連絡手段を通し正確性検証をする

AATL	申請組織又は個人との信頼できる連絡手段を通し検証すると同時に、電子メールアドレスを証明書に記載する要求があった場合、申請者が電子メールアドレスを管理していることを検証する。マネージド PKI アカウントにより発行された証明書の場合、LRA の権限はプロファイル設定時に検証される。
TrustedRoot	組織の申請者との信頼できる連絡手段を通し正確性検証をする。トップレベルドメイン/サブドメイン、又は 3.2.7 項で説明されているドメイン名といった、Name Constraints（名前の制限）に含まれる可能性がある全要素の正確性検証をする。
Qualified Website Authentication Certificates	3.2.7 項に記載の方法によって申請者のドメイン名に対する所有権又は管理権限を検証し、またこれに加えて 3.2.2.3 項に記載の方法による契約書署名者/証明書承認者及び正式な代表者の権限を検証する。
Qualified Certificate for Electronic Seal	3.2.2.3 項に記載の方法に従って、契約署名者かつ証明書承認者、及び認証された代表者の権限の正確性検証をする。
Qualified Certificate for Electronic Signature	3.2.3.4 項に記載の方法によって、個人の申請者による申請について権限の正確性検証をする。
JCAN 証明書	組織の申請者との信頼できる連絡手段を通し検証をする。

申請組織とコミュニケーションをとるうえで依拠しうる手段に代わって、GloalSign は以下の何れかの方法によって申請組織の権限を確認することができる:

- 組織名及びその関連会社(親会社、支社、関連会社等)の組織名を含む、高度な(又はそれ以上の水準の) e シール。
- 組織名及びその関連会社(親会社、支社、関連会社等)の組織名を含む、高度な(又はそれ以上の水準の)電子署名。この場合、GlobalSign は、証明書に記載された組織の従業員又は代理人であることが適切に確認されていることを検証する。
- 確認された組織の従業員又は代理人の高度な（又はそれ以上の）電子署名。

3.2.6. 相互運用のための基準

2.1 項に準じる。

3.2.7. ドメイン名の認証

全ての SSL 証明書について、以下の何れか一つの方法によって、申請された FQDN の申請者（申請者の親会社、子会社又は関連企業を含み、これらを合わせて「申請者」という）が同 FQDN を所有ないし管理していることを認証する:

1. 乱数をドメインの連絡先に電子メールで送信し、確認した相手からその乱数を用いた返答を受信する審査を通し、申請された FQDN が申請者の管理下にあることを確認する。(BR section 3.2.2.4.2) 又は
2. ドメイン連絡先に架電し、申請者からの FQDN の十分性検証要求についての応答を得る審査を通し、申請された FQDN が申請者の管理下にあることを確認する。(BR section 3.2.2.4.3) 尚、当該方法は 2019 年 3 月 31 日をもって用いられることはなくなる。又は
3. ローカル部分に'admin', 'administrator', 'webmaster', 'hostmaster', 又は'postmaster'を追加し、その直後に@、そのあとに認証用ドメイン名が続く電子メールアドレスに対し、乱数を送信したあと、その乱数を用いた返答を受信する審査を通し、申請された FQDN が申請者の管理下にあることを確認する。(BR section 3.2.2.4.4)
4. 認証用ドメイン名上にある DNS CNAME 又は TXT レコード内に乱数が存在することを確認する審査を通し、申請された FQDN が申請者の管理下にあることを確認する。(BR section 3.2.2.4.7)
5. DNS CAA の宛先になっているメールアドレスに任意の値を送信する審査を通し、申請された FQDN が申請者の管理下にあることを確認する。GlobalSign は、RFC 8659 Section 3 に規定されている検索アルゴリズムを用い、関係する CAA Resource Record Set を必ず確認するものとする。(BR section 3.2.2.4.13)
6. 任意の値(BR section 3.2.2.4.14)を電子メールにて DNS TXT Record Email Contact へ送信し、その任意の値を用いて確認の返信を受けることで、申請された FQDN が申請者の管理下にあることを確認する。
7. ドメイン管理者の電話番号に電話し、申請者が行った FQDN の十分性検証の要求を確認する返答を受けることで、申請された FQDN(BR section 3.2.2.4.15)が申請者の管理下にあることを確認する。
8. DNS TXT レコードの電話連絡先の電話番号に電話し、ADN 検証を確認する返答を受けることで、申請された FQDN が申請者の管理下にあることを確認する。(BR section 3.2.2.4.16): 又は、

9. 認可されたポート番号を介した HTTP/HTTPS 経由でアクセス可能な認証用ドメイン名を含む"/well-known/pki-validation"ディレクトリ下にあるファイル内に、乱数が存在することを確認する審査を通し、申請された FQDN が申請者の管理下にあることを確認する。(BR section 3.2.2.4.18) 又は、
10. RFC 8555 の 8.3 項で定義された ACME HTTP チャレンジ方法を用いて FQDN のドメイン制御を検証することを通し、申請された FQDN が申請者の管理下にあることを確認する。(BR section 3.2.2.4.19)

GlobalSign は、上記の 9 番目 (BR 3.2.2.4.18) 及び 10 番目 (BR 3.2.2.4.19) の方法を除き、ワイルドカード FQDN の検証に上記の方法を使用する。9 番目 (BR 3.2.2.4.18) 及び 10 番目 (BR 3.2.2.4.19) の方法では、以下のリダイレクトがサポートされる。

3.2.7.1. CAA レコード

GlobalSign は、ドメインの CAA レコードに対して、パブリックに信頼された SSL 証明書のサーバ FQDN を検証する。GlobalSign の CAA 発行者ドメインは「globalsign.com」である。発行権限のある認証局(CA)として globalsign.com を掲載していない CAA レコードが存在する場合、GlobalSign は証明書を発行しない。
GlobalSign は、

- CAA レコードをキャッシュし、最大 8 時間再利用する
- 発行及び、issuewild CAA タグの発行に対応する
- 処理は行うが、iodef プロパティタグには作用しない(つまり、GlobalSign は、CAA iodef レコードに指定された連絡先に、そのような発行要求のレポートを送信しない)
- 追加のプロパティタグは対応していない

3.2.8. IP アドレスの認証

GlobalSign は、申請者が IP アドレスを管理又は使用する権利を有することを確認するために、以下の方法を使用する。

1. 認可されたポート番号を介した HTTP/HTTPS 経由でアクセス可能な、"/well-known/pki-validation"ディレクトリ下にあるファイル内に、乱数が存在することを確認する審査を通し、申請された IP アドレスが申請者の管理下にあることを確認する。(BR 3.2.2.5.1 項)
2. 乱数を IP アドレスの連絡先に電子メールで送信し、確認した相手からその乱数を用いた返答を受信する審査を通し、申請された IP アドレスが申請者の管理下にあることを確認する。(BR 3.2.2.5.2 項) 又は、
3. IP アドレスの逆引きを行い、3.2.7.1 (BR 3.2.2.5.3 項)内の何れかの方法により、検索結果のドメイン名が申請者の管理下にあることを確認する。又は、
4. IP アドレス割当先の電話番号に電話し、申請者が行った IP アドレスの十分性検証の要求を確認する返答を受けることで、申請された IP アドレスが申請者の管理下にあることを確認する。(BR section 3.2.2.5.5)

3.2.9. 電子メールアドレスの認証

GlobalSign は、申請者が電子メールアドレスを管理又は使用する権利を有することを確認するために、以下の方法を使用する。

1. 申請者に乱数を含む URL を電子メールアドレスに送信し、その乱数を用いた確認の返信を受けることで、申請された電子メールアドレスが申請者の管理下にあることを確認する。又は、
2. 3.2.7 項に記載の何れかのドメインの十分性の検証方法を用い、申請者が FQDN を管理又は使用する権利を保有することを確認する。検証されると、エンタープライズ RA は、その FQDN の下でアドレス指定された正確な電子メールを含む証明書を発行することができる。

3.3. 鍵更新申請時における識別及び認証

GlobalSign は、利用者の証明書について、有効期限が満了する前に、鍵更新(以下、「Re-key」という)申請に対応する。

JCAN 証明書においては Re-key は該当しない。

3.3.1. 定期的な Re-key における識別及び認証

Re-key に対応する製品では、Re-key 申請の認証は、証明書の初回発行時に提供された認証メカニズム、又はそれと同等のものに基づいて行われる。

申請の識別は、4.2.1 項に規定される再利用条件の対象となる。証明書に記載される情報が何らかの理由で変更された場合、追加の十分性検証を実施しなければならない。

3.3.2. 失効後の Re-key における識別及び認証

証明書の失効後に定期的に設定されている再発行には対応しない。証明書失効後の再発行のために、利用者は初回の証明書発行時と同じ十分性検証を受けなければならない。

3.4. 失効申請における識別及び認証

RA は、全ての失効申請について、認証する。利用者からの失効申請は、ユーザ名・パスワードによる認証、証明書に記載されたドメイン名や電子メールアドレスなどが要求者の所有するものであることの確認、ネットワークを経由しない方法で検証済の特定の情報を用いて認証を行うなどの適切なチャレンジ・レスポンス方式があった場合に認められる。

GlobalSign は本 CPS かつ/又は利用契約の規定に従い、利用者を代理して失効手続きを取ることがある

4. 証明書のライフサイクルに対する運用上の要求事項

4.1. 証明書申請

4.1.1. 証明書の申請者

GlobalSign は、証明書の申請を承認しない個人又はエンティティのブロックリストを独自に作成する。加えて、GlobalSign がサービスを提供する国・地域の管轄政府当局が発行する、又は国際的に認知された取引禁止対象者リストなどの外部情報源に依拠して、証明書を発行しない申請者を選別する。
GlobalSign は、その事業所の所在国の法律が取引を禁じる対象者に証明書を発行しない。
EV ガイドラインは、EV SSL 又は EV コードサイニング証明書発行のための規則を規定する。申請者は、GlobalSign の提供するサービスの内容に応じて、適切な形式の証明書申請を提出し、並びに電子的に、又はその他の事前に承認された形式の利用契約に同意しなければならない。

証明書申請は以下の何れかの方法で提出できる。

- **オンライン申請:** Web インターフェース(https セッション)による申請。証明書申請者は、GlobalSign が規定する手続きに従い安全な方法で申請を送信する。GlobalSign と直接契約をする顧客の多くはこの方法を使用する。このために使用するアカウントを GCC、すなわち GlobalSign Certificate Centre と呼び、このアカウントへのログインには適切な強度のユーザ名とパスワードを使用する。GCC アカウントでは、証明書のライフサイクルを管理することができる。このアカウントは、マネージド SSL サービス顧客用、マネージド PKI サービス顧客用、直接取引顧客用、パートナー用、リセラー用に別けられる。
- **API:** API を利用する申請者は、GlobalSign に適切な形式の証明書申請を送信するにあたり、API (Application Programming Interface)を使用することができる。API を通じてデータを送信する際には、適切な強度のユーザ名とパスワードが求められる。GlobalSign は、他に利用制限をかけない場合には、申請者の送信元 IP アドレスをデータに含めることを求めることができる。提供するアカウントは、API 用に別けられる。
- **マニュアル申請:** タイムスタンプ証明書の発行、又は GCC アカウントで申込みが可能な上限数を超えた SubjectAlternativeName を証明書に記載することを希望する申請者は、直接電子メールによって、又はネットワークを経由しない方法で申請情報の検証を受けるよう申し込むことができる。

4.1.2. 登録手続きとそこで負うべき責任

GlobalSign は、依拠当事者に申請者の本人識別情報を提示する全てのタイプの証明書について、その情報の真正性を十分に検証するシステム、手続きを採用している。申請者は、必要な正確性検証を行えるよう、GlobalSign 及び RA に対し情報を提出しなければならない。GlobalSign 及び RA は、申請者が申請手続きにおいて GlobalSign Privacy Policy に準拠し、情報を提出する際の通信の秘密を保護し、当該情報を安全に保管する。

申請にあたっては以下の手続きを踏むことになるが、鍵の生成は十分性検証が終わってから行われる場合もあり、必ずしもこの順番では行われない。

- 適切に安全なプラットフォームにおいて、鍵ペアを生成する
- 適切に安全なツールを用いて証明書署名要求(CSR)を生成する
- 証明書の種類に応じた申請と必要な申請情報を提出する
- 利用契約又はその他の約款に同意する
- 料金を支払う

4.2. 証明書申請手続き

4.2.1. 識別及び認証の実施

GlobalSign は、本 CPS の規定に従い、本人識別情報を十分に認証するシステム、手続きを採用している。

初回の身元情報の検証は、GlobalSign の検証チームが 3.2 項の規定に準拠して実施する、又は RA が契約に基づいて実施する。ファックス、電子メールで GlobalSign に提出された申請者の情報は、GCC アカウント、又はパートナーから GlobalSign 提供の API 経由で提出された情報と共に、安全に保管される。初回以降の証明書申請については、ユーザ名・パスワードの単一要素による認証か、又は電子証明書とユーザ名・パスワードの多要素による認証の何れかを用いて権限を検証する。

以下の条件を満たす場合、GlobalSign は、3.2 項で説明された文書及びデータを使用して証明書情報を検証するか、又は以前の十分性検証の内容を再利用することができる。

- GlobalSign が 3.2 項に規定された情報源からデータ又は文書を入手したか、証明書を発行する 825 日前までに十分性検証を完了したこと。
- SSL 証明書については、Baseline Requirement 3.2.2.4 項 及び 3.2.2.5 項に基づくドメイン名及び IP アドレスの十分性検証において、再利用されるデータ、文書、又は完了した十分性検証は、証明書を発行する 398 日前までに入手しなければならない。
- EV SSL 証明書及び EV Code Signing 証明書については、GlobalSign が 3.2 項に規定された情報源からデータ又は文書を入手したか、証明書を発行する 398 日前までに十分性検証を完了したこと。ただし、11.14.2 項に基づく EV 証明書の再発行と、EV ガイドラインのセクション 11.14.1 項で別途許可されている場合を除く。

JCAN 証明書において、審査書類及び審査情報は再利用されない。

顧客は、製品が対応している場合、証明書の交換または「再発行」を申請することができる。

証明書に記載されたサブジェクト名の情報が何らかの理由で変更された場合、ここに記載された手順を再度実行する必要がある。

4.2.2. 証明書申請の承認又は却下

GlobalSign は、何れかの項目について検証を完了することができない場合、証明書申請を却下する。

本 CPS の手順に従い、全ての十分性の検証手順が正常に完了すると仮定した場合、GlobalSign は、一般的に、証明書申請を承認するものとする。GlobalSign は、以下の理由により、申請を却下することができる。

- GlobalSign は、証明書申請を承認することが GlobalSign のブランドを傷つける可能性があると判断した場合、それを却下することができる。
- GlobalSign は、過去に証明書申請を却下した、或いは利用契約に違反した申請者からの証明書申請を却下することができる。

GlobalSign は、証明書申請が却下された理由を申請者に説明する義務を負わない。

EV 証明書、適格証明書、及びコードサイニング証明書については、十分性検証チームの 2 名が証明書申請を承認しなければならない。GlobalSign は各国で事業を行っているが、GlobalSign が社内で処理できない言語の申請については、当該言語で申請を処理し、文書を翻訳することのできる、適切に研修と経験を積んだ外部の RA に事前審査手続きを委託することができる。
GlobalSign は、パブリックに信頼されている SSL 証明書を Internal Names や予約済み IP アドレスに発行しない。

4.2.3. 証明書の申請処理に要する期間

GlobalSign は、証明書申請を検証し処理するために必要とされる全ての適切な手続きを行う。GlobalSign の支配の及ばない理由によって問題が生じた場合には、GlobalSign は申請者に適切に情報を伝達する。

EV 証明書については、GlobalSign は、契約書署名者に利用契約への同意を求める前に、全ての提出された情報が正しいかどうか、検証を行う。

以下は、証明書申請の処理、及び証明書の発行までに必要な時間の概算である。

- PersonalSign1 証明書: およそ 1 分
- PersonalSign2 証明書: およそ 24～48 営業時間
- PersonalSign2 Pro 証明書: およそ 36～72 営業時間
- NAESB 証明書: およそ 24～48 営業時間
- PersonalSign3 Pro 証明書: およそ 48～72 営業時間
- Code Signing 証明書: およそ 24～48 営業時間
- EV Code Signing 証明書: およそ 48～96 営業時間
- DV SSL 証明書: およそ [3] 1～5 分
- AlphaSSL 証明書: およそ [3] 1～5 分
- OV SSL 証明書及び ICPEdu 証明書: およそ 24～48 営業時間
- EV SSL 証明書: およそ 48～96 営業時間
- 適格証明書:およそ 48～96 営業時間
- Time Stamping 証明書: およそ 5～10 営業日
- AATL 証明書: およそ 24～48 営業時間
- Trusted Root: 6～12 週間(テスト、及びオフラインのキーセレモニーの予定調整を含む)
- S/MIME 証明書: およそ 48~72 営業時間

4.3. 証明書の発行

4.3.1. 証明書発行時における認証局の業務

GlobalSign ルート CA による証明書発行は、GlobalSign から認可された信頼された役割のメンバーが直接コマンドを発行することで、ルート CA が証明書に署名をする。

GlobalSign は、証明書発行の直接的な要因となり得る RA アカウントについて、多要素認証が行われている事を確認する。これは、GlobalSign が直接運営する RA に限らず、契約に基づいて運営される RA も同じである。RA は、CA に提出された全ての情報の十分性検証をし、改ざん、不正使用されないようこれらの情報を保護する。

4.3.2. 認証局から利用者への証明書の発行に関する通知

GlobalSign 又は RA は、登録手続きの際に連絡先として提示された電子メールアドレス、又は同様の連絡先を通じて、証明書の発行を利用者又は申請者に通知する。この通知を行う電子メールには、申請された証明書のワークフローにより、証明書そのものを添付している場合、若しくはダウンロードするための URL を記載している場合がある。

4.3.3. 利用者への NAESB 用証明書の発行に関する通知

申請者の識別及び認証手続きが問題なく完了した場合、GlobalSign は証明書を発行し、申請者に通知し、申請者に証明書を提供しなければならない。

4.4. 証明書の受領

4.4.1. 証明書の受領とみなされる行為

GlobalSign は、利用者に対し、電子証明書に記載された情報が正しいことを確認するまでは、当該証明書を使用しないよう通知する。利用者が、このような通知を含む GlobalSign からの電子メールを受信後 7 日以内に GlobalSign に連絡をしない場合、この電子証明書は受領されたものとみなす。

---

[3] DV・Alpha SSL 証明書の申請におけるドメイン名の所有又は管理権限の検証にあたって、潜在リスクが高いとみなされた場合には、OV SSL 証明書の申請に近い検証手続きを取ることがある。

4.4.2. 認証局による証明書の公開

GlobalSign による証明書の公開は、利用者に証明書を交付することにより実施し、また、1 つ以上の Certificate Transparency ログに公開することもできる。加えて、マネージド PKI サービスの顧客に対しては、GlobalSign は LDAP のようなディレクトリを通じて証明書を公開することがある。

4.4.3. 認証局からその他のエンティティへの証明書の発行に関する通知

RA、LRA、パートナー/リセラー、GlobalSign 及びその他のエンティティは、最初の証明書情報の登録に関与していれば、発行について通知を受けることができる。

4.5. 鍵ペアと証明書の利用

4.5.1. 利用者による鍵ペアと証明書の利用

利用者は、秘密鍵が第三者に開示されることのないよう保護しなければならない。GlobalSign は、利用者の秘密鍵の保護義務を規定する利用契約を利用者との間で締結する。秘密鍵は、対になる公開鍵を含む証明書の Key Usage 及び Extended Key Usage フィールドに指定される用途以外に使用してはならない。

認証された公開鍵に関連する秘密鍵が QSCD に格納される適格証明書については、利用者鍵は認められた 適格署名作成装置(QSCD)内で生成・格納されなければならない。

コードサイニング証明書については、利用者の秘密鍵は、FIPS 140-2 レベル 2 又は Common Criteria EAL 4+ の要件を満たす暗号モジュール内、或いは鍵ペアを生成・保護し TPM 鍵認証により利用者の秘密鍵保護を証明することができる Trusted Platform Module（TPM）内で、生成、保管、使用しなければならない。

EV コードサイニング証明書については、利用者の秘密鍵は、FIPS 140-2 レベル 2 又は Common Criteria EAL 4+ の要件を満たすか超える暗号モジュール内で、生成、保管、使用しなければならない。

秘密鍵のバックアップが可能な場合、利用者は、稼働中の秘密鍵と同レベルの注意及び保護を行わなければならない。秘密鍵の有効期限が終了した時点で、利用者は秘密鍵及びバックアップのために分割された全てのフラグメントを安全に削除しなければならない。

GlobalSign のデジタル署名サービスの場合、利用者の同意を得て、GlobalSign は、短期間証明書及び対応する秘密鍵を、要件準拠した HSM 又は QSCD 内でホスト、保管、管理するものとする。

4.5.2. 依拠当事者による公開鍵と証明書の利用

GlobalSign は、CRL や OCSP など証明書の有効性を検証するサービスによる確認を必要とするなど、依拠当事者が電子証明書の情報に依拠する際の条件を本 CPS に規定する。GlobalSign は利用者に対し依拠当事者規約を提供し、その内容を依拠当事者に提示しなければならない。依拠当事者は、GlobalSign からの証明書に依拠する前に、この依拠当事者規約を受諾し、これに従わなければならない。依拠当事者は、この規約に記載された情報をリスク評価のために確認しなければならず、証明書に記載の情報又はそこで提示されるあらゆる保証を信頼し依拠する前にリスク評価を行うことに全責任を負う。

依拠当事者が使用するソフトウェアは、ポリシーと Key Usage の解釈の際のベストプラクティスなどを含め、X.509 規格に準拠したものでなければならない。

4.6. 証明書の更新

証明書の更新とは、利用者又は他の関係者の公開鍵やその他の情報を変更せずに、古い証明書の有効期間終了後に新しい有効期限が設定されている証明書を発行することである。

証明書の更新申請は、利用者又は他の関係者の公開鍵、或いは証明書内のその他の情報が異なる場合、新規証明書要求として処理される。

JCAN 証明書において、証明書の更新は該当しない。

4.6.1. 証明書更新の条件

証明書の更新が可能な製品において、証明書の更新は、利用者、利用者の委任を受けた代理人、または発行局の独自の判断による申請を受けて行うことができる。
証明書の更新は、元の証明書が失効されていない場合にのみ行われるものとする。

4.6.2. 更新の申請者

証明書更新申請は利用者又は利用者の委任を受けた代理人が提出しなければならない。

4.6.3. 証明書更新申請の処理

GlobalSign は証明書更新申請を処理するにあたり、証明書更新申請を利用者又は利用者の委任を受けた代理人と検証しなければならない。
証明書更新申請は新規の証明書申請として処理される。

4.6.4. 利用者への新しい証明書の発行に関する通知

4.3.2 項に準じる。

4.6.5. 更新された証明書の受領とみなされる行為

4.4.1 項に準じる。

4.6.6. 認証局による更新された証明書の公開

4.4.2 項に準じる。

4.6.7. 認証局からその他のエンティティへの証明書の発行に関する通知

(規定なし)

4.7. 証明書の Re-key

証明書の Re-key とは、有効期間や証明書のその他の情報を変更することなく、異なる公開鍵で新しい証明書を発行することである。
Re-key 申請は、有効期間又はその他の情報が変更した場合、新しい証明書の申請として処理される。

JCAN 証明書において、証明書の Re-key は該当しない。

4.7.1. 証明書の Re-key の条件

Re-key が可能な商材において、証明書の Re-key は、利用者、利用者の委任を受けた代理人、又は発行 CA の独自の判断による申請を受けて実施する。
証明書の Re-key は、証明書の秘密鍵が危殆化した際にも申請できる。

4.7.2. 新しい公開鍵を含む証明書の申請者

Re-key 申請は利用者又は利用者の委任を受けた代理人が提出しなければならない。

4.7.3. 証明書 Re-key 申請の処理

GlobalSign は Re-key 申請を処理するにあたり、当申請を利用者又は利用者の委任を受けた代理人と検証しなければならない。
Re-key 申請は新規の証明書申請として処理される。

4.7.4. 利用者への新しい証明書の発行に関する通知

4.3.2 項に準じる。

4.7.5. Re-key された証明書の受領とみなされる行為

4.4.1 項に準じる。

4.7.6. 認証局による Re-key された証明書の公開

4.4.2 項に準じる。

4.7.7. 認証局からその他のエンティティへの証明書の発行に関する通知

(規定なし)

4.8. 証明書記載情報の修正

証明書記載情報の修正とは、利用者公開鍵以外の証明書内の情報の変更に伴い、新たな証明書を発行することである。
証明書記載情報の修正申請は、有効期間が変更した又は利用者公開鍵が異なる場合、新しい証明書の申請として処理される。

JCAN 証明書において、証明書記載情報の修正は該当しない。

4.8.1. 証明書記載情報の修正の条件

証明書記載情報の修正が可能な製品において、証明書記載情報の修正は、利用者、利用者の委任を受けた代理人、又は発行 CA の独自の判断による申請を受けて実施する。

4.8.2. 証明書記載情報の修正の申請者

証明書記載情報修正の申請は利用者又は利用者の委任を受けた代理人が提出しなければならない。

4.8.3. 証明書記載情報の修正申請の処理

GlobalSign は Re-key 申請を処理するにあたり、当申請を利用者又は利用者の委任を受けた代理人と検証しなければならない。
証明書記載情報修正は新規の証明書申請として処理される。

4.8.4. 利用者への新しい証明書の発行に関する通知

4.3.2 項に準じる。

4.8.5. 記載情報の修正された証明書の受領とみなされる行為

4.4.1 項に準じる。

4.8.6. 認証局による記載情報の修正された証明書の公開

4.4.2 項に準じる。

4.8.7. 認証局からその他のエンティティへの証明書の発行に関する通知

(規定なし)

4.9. 証明書の失効、効力の一時停止

4.9.1. 失効の条件

GlobalSign は、失効の手続きを取る前に、失効申請の権限を検証する。

GlobalSign 及び JCAN LRA は自己の裁量によって証明書を失効することができる。

利用者証明書の失効は以下の条件に該当する場合、24 時間以内に行われる。

1. 利用者が証明書の失効を希望する旨を書面で(証明書を発行した RA に)申請した場合。
2. 利用者が元の証明書申請が承認されておらず、遡及的に承認を付与していないことを通知した場合。
3. (証明書の公開鍵と対になる)利用者の秘密鍵が危殆化したという合理的な証拠を取得した場合。
4. 証明書の公開鍵に基づいて利用者の秘密鍵を容易に計算できる、実証済み又は証明された方法を認識している場合。(例えば、Debian の脆弱な鍵など https://wiki.debian.org/SSLkeys を参照)。
5. ドメインの承認或いは証明書内の FQDN 又は IP アドレスへのコントロールについて十分性検証をする際、依拠すべきではない証拠を取得した場合。
6. 通知の受領或いはその他の手段によって、利用者又はサブジェクトの事業機能の予期せぬ終了を認識した場合。

7. PSD2 証明書について、その PSP より認証又は登録されている所轄官庁から正式な失効申請を受領した場合(又はそうした所轄官庁からの失効申請を認証する場合)。失効の正当理由としては、PSP の権限が失効された際や、証明書に含まれる PSP の役割が失効された際が挙げられる。

利用者の証明書の失効は、24 時間以内に実施されるべきであり、以下の 1 つ以上の状況が発生した場合、5 日以内に実施される。

1. 証明書は、6.1.5 項及び 6.1.6 項に規定されているように、Baseline Requirements のアルゴリズムの種類及び鍵長についての要件にもはや準拠していない場合。
2. 証明書が不正使用されたことを示す証拠を取得する場合。
3. 利用者が利用約款に規定された重要な義務に対し違反をした旨、通知を受ける又は認識する場合。
4. GlobalSign が、本証明書における FQDN 又は IP アドレスの使用がもはや法的に許可されていないことを示す状況(例えば、裁判所又は仲裁人がドメイン名を使用するドメイン名登録者の権利を取り消した場合、ドメイン名登録者と申請者との間におけるライセンス契約若しくはサービス契約が終了した場合、又はドメイン名登録者がドメイン名を更新しなかった場合)を認識する。
5. GlobalSign が、ワイルドカード証明書が、不正に誤解を招く下位 FQDN を認証するために使用されたことを認識する。
6. 証明書に含まれる情報に重大な変更があった際、その旨通知を受けた、またその他の方法で知った場合。
7. 証明書が Baseline Requirements 又は GlobalSign の CP 又は CPS に従って発行されたものではないことを認識した場合。
8. 証明書に記載される情報の何れかが正確でないと判断する場合。
9. CRL/OCSP レポジトリの維持管理を継続することに合意することなく、Baseline Requirements に従った証明書を発行する権利が満了する、失効する或いは破棄された場合。
10. GlobalSign の CP 及び/又は CPS により失効が要求された場合。
11. 利用者の秘密鍵を危険にさらす実証済み又は証明された方法を認識している場合、又は、秘密鍵の生成に使用された特定の方法に欠陥があるという明確な証拠がある場合。
12. 証明書の形式又は技術的様式が、アプリケーションソフトウェアサプライヤー又は依拠当事者に容認できないリスクをもたらす場合(例えば、CA/B Forum は、利用されていない暗号/署名アルゴリズム又は鍵のサイズが容認できない危険性を示し、そのような証明書は、所与の期間内に CA によって失効、置き換えがなされるべきであると判断する可能性がある)。
13. 証明書に記載された電子メールアドレスの使用が法的に許可されていないことを示す通知を受け取るか、又は、その他の方法で知った場合。
14. 証明書を発行する際に使用された CA の秘密鍵が漏洩した疑いがある場合。
15. 何らかの理由で業務を停止し、他の認証局(CA)に証明書の失効を委託しない場合。
16. 現行版の Mozilla Root Store Policy に違反する形で証明書が発行された場合。

利用者の証明書の失効は、次に掲げる事情があるときは、商業上合理的な期間内に行うこととする。

1. 利用者又は組織の管理者が、証明書のライフサイクルを管理する GCC アカウントを通じて証明書の失効を申請する。
2. 利用者が、RA 又は GlobalSign のサポートチームへ、認証済み申請を通じて失効を申請する。
3. 利用者が禁止対象者としてブロックリストに追加されたこと、又は、法域の法律に基づき禁止された地域から営業していることの通知を受領するか、又は、発見する。
4. 利用者による当該費用の未払い
5. 証明書の失効申請を受けたとき。
6. 証明書が再発行された場合、GlobalSign は、以前に発行された証明書を取り消すことができる。
7. 一定のライセンス契約に基づき、ライセンス契約の満了又は終了後、証明書を取り消すことができる。
8. 継続的な証明書の利用が証明書発行者又は第三者の事業に対して有害になりうるかの判断を行う。証明書の利用方法が証明書発行者又は第三者の事業の評価へ悪影響を与えるか考慮する際は、とりわけ、受け付ける苦情の性質及び件数、苦情の素性、関連法令、及び、告発された利用者による証明書の有害な利用をはじめとした要素を考慮する。
9. Microsoft は、専らその裁量で、証明書の用途ないし属性情報が Trusted Root Program の趣旨に反していると認定した場合、GlobalSign に連絡し、証明書の失効を要求する。GlobalSign は、本証明書を失効するか、又は Microsoft の要求を受領後 24 時間以内に Microsoft に例外を申請する。Microsoft は、専らその裁量で、提出物を確認し、例外を許可又は拒否するか、最終決定を GlobalSign に通知する。Microsoft が例外を認めない場合、GlobalSign は、例外が拒否されてから 24 時間以内に本証明書を失効させる。
10. 利用者の死亡。

下位 CA 証明書の失効は、次の場合 7 日以内に行う。

1. 下位 CA が、下位 CA 証明書又は本 CPS の 1.5.2 条に詳細が記載されている権限を提供する GlobalSign 事業体に対し、GlobalSign が本証明書の失効を申請していることを書面で要求する。
2. 利用者が、元の証明書申請が承認されておらず、遡及的に承認を付与していないことを GlobalSign に通知する。
3. GlobalSign が、証明書内の公開鍵に対応する下位 CA の秘密鍵が危殆化した、又は、6.1.5 項及び 6.1.6 項に規定されているように、Baseline Requirements のアルゴリズムの種類及び鍵のサイズの要件をもはや満たさないという合理的な証拠を取得する。
4. GlobalSign が、証明書が不正使用されたことを示す証拠を取得する。
5. GlobalSign が、証明書が Baseline Requirements 又は GlobalSign CP 若しくは本 CPS に従って発行されていないこと、又は下位 CA が Baseline Requirements 若しくは GlobalSign CP 若しくは本 CPS を遵守していないことを発見した。
6. GlobalSign が、証明書に表示される情報の何れかが不正確であるか、誤解を招く恐れがあると判断する。
7. 発行 CA 又は下位 CA が、何らかの理由で業務を停止し、他の CA 証明書の失効を委託していない。
8. 発行 CA が、CRL/OCSP レポジトリを維持し続けるための調整をしていない限り、Baseline Requirements に基づき証明書を発行する CA 又は下位 CA の証明書発行権利は、満了するか、取り消されるか、又は終了する。
9. 発行 CA の CP 及び/又は CPS により失効が要求される。
10. 証明書の技術的な内容又は書式が、アプリケーションソフトウェアサプライヤー又は依拠当事者に、許容できないリスクをもたらす(例えば、推奨されない暗号/署名アルゴリズム又は鍵のサイズが容認できないリスクをもたらし、そのような証明書が一定の期間内に CA によって取り消され、置き換えられるべきであると、CA/B Forum が判断する可能性がある場合)。

利用者が失効を要求する場合、該当する失効理由を提供しなければならない。

- Unspecified：以下の理由コードが失効要求に該当しない場合、利用者は「unspecified」以外の理由コードを提示してはならない。
- keyCompromise：証明書の秘密鍵が危殆化したと信じるに足る理由がある場合。（例：権限のない者が証明書の秘密鍵にアクセスした場合）
- cessationOfOperation：証明書に含まれる全てのドメイン名を所有しなくなったとき、又はウェブサイトを閉鎖するため、証明書を使用しなくなったとき。
- affiliationChanged：証明書に含まれる組織名などの組織情報が変更されたとき。
- Supersed：既存の証明書を置き換えるために、新しい証明書を申請したとき。

利用者により失効事由が明記されていない場合、Unspecified が理由コードとして用いられる。

Trusted RootCA に関して、GlobalSign は、Trusted RootCA が、もはや両当事者間の合意の契約上の期間及び条件を満たさない場合、発行 CA を失効させることができる。

4.9.2. 失効の申請者

GlobalSign 及びその RA は、失効申請が権限を有すると検証できた場合に申請を承認することとなる。失効申請は、利用者本人又は証明書に記載された組織から提出された場合、受理される。利用者、依拠当事者、アプリケーションソフトウェアサプライヤー、及びその他第三者は、Certificate Problem Reports を提出して、証明書を失効する合理的な理由が疑われる場合、GlobalSign に通知することができる。加えて PSD2 証明書においては、失効申請が PSP を認証又は登録した NCA（所轄官庁）から行われうる。GlobalSign は発行した証明書を自己の裁量で失効する権利を有し、これには相互認証する認証局に発行された証明書を含む。

4.9.3. 失効申請の処理手続き

失効申請の持つ性質と効率化の観点から、GlobalSign は失効申請を要求し、認証するための自動化されたメカニズムを提供する。主な方法は、GCC アカウントを通じて発行した証明書の失効申請を行う方法がある。次に代替方法として、ファックス、郵便、電話などを通じて、ネットワークを経由せずに失効を要求することができる。また、GCC アカウントが提供されない利用者については、証明書のサブジェクト識別名に関連する一つ以上の要素に対する管理権限を実証する方法で、失効申請権限を検証することもできる。S/MIME 証明書については、電子メールアドレスの管理権限の検証をもって代替とすることが可能である。
GlobalSign 及び RA は、失効申請を記録し、その情報源を認証する。要求が真正であり承認された場合には、適切な失効手続きを取る。

利用者、依拠当事者、アプリケーションソフトウェアサプライヤー、及びその他第三者は、report-abuse@globalsign.com に証明書の問題報告を提出することができる。GlobalSign は、この申請に対応して失効する場合及び、しない場合がある。この意思決定の GlobalSign による判断基準は、4.9.5 項を参照すること。

失効された場合、証明書のシリアル番号、失効日、失効時刻が CRL に記載される。理由コードを含むこともある。CRL は本 CPS に準拠して発行される。

4.9.4. 失効申請までの猶予期間

SSL 証明書及びコードサイニング証明書について、GlobalSign は失効申請までの猶予期間を認めていない。危殆化の疑いがある場合、脆弱な鍵を使用した場合、発行を受けた証明書に記載された情報に不正確な内容が含まれていた場合などに、利用者が失効を要求する前に必要な対策を取るための時間を指す。利用者、GlobalSign の何れかが、何らかの理由により失効を処理できない場合、リスク分析を行い、記録する。

利用者は 48 時間以内に GlobalSign に鍵の漏洩を通知する。

4.9.5. 認証局が失効申請を処理すべき期間

エンドエンティティ証明書の失効申請については、GCC アカウントを通じて送信された失効申請、及び GlobalSign が失効手続きを開始したものの何れであっても、受理から 24 時間以内に処理されなければならない。

TrustedRoot サービスについては、GlobalSign は失効申請を危殆化の事実の確認後 24 時間以内に処理し、認証局失効リスト(以下、「ARL」という)を生成後 12 時間以内に発行する。

GlobalSign は、優先順位の高い Certificate Problem Report に 24 時間 365 日社内で対応できる体制を整えており、必要に応じて、そのような申し立てを法執行機関に転送し、また、そのような申し立ての対象である証明書を失効する。GlobalSign は、Certificate Problem Report を受領してから 24 時間以内に、証明書の危殆化又は不正使用が疑われる場合の捜査手続きを開始する。

GlobalSign は、少なくとも以下の基準に基づいて、失効又はその他の措置が正当化されるかどうかを決定する。

申し立ての問題の性質
特定の証明書又は利用者に関して受け取った報告の件数
申し立てを行っている主体、及び
関連規則

4.9.6. 失効情報確認に関する依拠当事者への要求事項

証明書に記載された情報を信頼し依拠する前に、依拠当事者は、証明書が適正な目的のために使用されていること、証明書が有効であることを確認しなければならず、これを怠った場合には、全ての保証は無効となる。

依拠当事者は依拠しようとする証明書がチェーンされる全ての階層の証明書について、CRL 又は OCSP の情報を参照すべきであり、またこのチェーンが完全であることを検証すべきである。これには、認証局鍵識別子(以下、「AKI」という)及びサブジェクト鍵識別子(以下、「SKI」という)の十分性検証を含む。適格証明書の場合、証明書チェーンの十分性検証は、EU のトラストリスト内の GlobalSign トラストアンカーまで正常に実施されなければならない。

CRL は一定の時間枠で発行されるため、失効直後から次の CRL 生成までの間に OCSP と CRL が同じステータスを返さない期間があり得ることに、依拠当事者は注意すべきである。CRL と OCSP の間に差異が生じた場合、OCSP が最も正確であると推定されるべきである。

GlobalSign は、依拠当事者が失効情報の検証を容易に行えるよう URL を証明書に記載する。

4.9.7. CRL の発行頻度

各 CRL には、発行される CRL 毎に単調に増加する連続した番号が含まれる。

GlobalSign が CRL を終了させるか発行局を失効させることを決定した、又は必要がある場合、GlobalSign は nextUpdate フィールドの値が「99991231235959Z」である最後の CRL を発行し、対応する CRL 配布ポイントで公表するものとする。GlobalSign は、CRL の範囲内の全ての証明書が期限切れ又は失効するまで、最後の CRL を発行しない。最後の CRL は CA 証明書の有効期限が切れるまで利用可能となり、この間 CRL の完全性を保つものとする。

利用者証明書のステータスについて:
CA が CRL を発行する場合、CRL は少なくとも 7 日毎(適格証明書及び JCAN 証明書は 24 時間毎)に更新、再発行され、nextUpdate フィールドの値は、thisUpdate フィールドの値から 10 日を超えてはならない。

下位 CA 証明書のステータスについて:

下位 CA 証明書に CDP が含まれている場合、CRL は、(i) 少なくとも 3 か月に 1 回、(ii) 下位 CA 証明書の失効後 24 時間以内に更新、再発行され、nextUpdate フィールドの値は、thisUpdate フィールドの値より 12 ヵ月を超えてはならない。

4.9.8. CRL の最大通信待機時間

nocheck 型の拡張子を含む。CRL は生成後、商業的に合理的な期間内にレポジトリに投稿される。

4.9.9. オンラインでの失効情報の確認

GlobalSign は、CRL の他、OCSP レスポンダにより失効情報を提供する場合、通常のネットワーク環境においては、OCSP による応答までの待機時間は 10 秒を超えない。

GlobalSign OCSP 応答は、RFC6960 及び/又は RFC5019 に準拠している。
OCSP 応答は、失効ステータスが確認されている証明書を発行した CA によって署名された証明書を持つ OCSP レスポンダによって署名される。OCSP 署名証明書は、RFC6960 によって定義されるように、id-pkix-ocsp-nocheck 型の拡張子を含む。

4.9.10. オンラインでの失効情報の確認の要件

利用者証明書のステータスについて:

1. OCSP レスポンスの有効期間は、8 時間以上とする。
2. OCSP レスポンスの有効期限は 10 日以下とする。
3. 有効期間が 16 時間未満の OCSP レスポンスについては、GlobalSign は有効期間の半分が経過するより前に、OCSP を介して提供される情報を更新するものとする。
4. 有効期間が 16 時間以上の OCSP レスポンスについては、GlobalSign は OCSP を介して提供される情報を、少なくとも nextUpdate の 8 時間前から thisUpdate の 4 日後までに更新するものとする。

下位 CA 証明書のステータスについて:

- GlobalSign は、OCSP レスポンダを通じて提供される情報を、少なくとも(i) 12 か月毎、及び(ii) 下位 CA 証明書を失効した後 24 時間以内に更新する。

発行されていない証明書のステータスのリクエストを受け取った OCSP レスポンダは、そのような証明書に対して「有効」と応答しない。

7.1.5 項に従った技術的な制約をされていない CA の OCSP レスポンダは、このような証明書に対して「有効」と応答しない。

GlobalSign は、OCSP リクエストに次のデータを含めるよう要求する:

- プロトコルバージョン
- サービス要求
- 対象証明書識別子

4.9.11. その他の方法による失効情報の提供

(規定なし)

4.9.12. 認証局の鍵の危殆化に伴う特別な要件

GlobalSign 及びその RA は、その秘密鍵が危殆化した恐れがあるときには、合理的な方法をもって利用者にその旨の通知をする。これには、脆弱性が発見された場合、及び GlobalSign が自己の裁量により鍵の危殆化の疑いがあると判断した場合などが含まれる。鍵の危殆化に疑いの余地がない場合、GlobalSign は発行 CA の証明書、エンドエンティティ証明書などを 24 時間以内に失効し、CRL をオンラインで 30 分以内に、及び ARL を 12 時間以内に発行する。

当事者は、鍵の危殆化を証明するために以下の方法を用いることができる。:

- 秘密鍵で作成、署名された CSR ファイルの提出。その CSR ファイルは以下のいずれかを含む必要がある。
  - GlobalSign が報告者に提供した特定の文字列。又は
  - 危殆化を明示する文字列。
- 危殆化を検証するうえでの参照先となる、脆弱性及び/又はセキュリティインシデントに関する情報や解説資料の提供
- 秘密鍵を抽出する方法を含む、侵害された秘密鍵を含むバイナリの提出

GlobalSign は他の要求を分析し、新しい提出方法が受け入れられる場合には、それに応じて 本 CPS を更新する。

4.9.13. 証明書の効力の一時停止を行う条件

マネージド PKI の顧客には証明書の一時停止が認められている。
証明書の効力の一時停止は、マネージド PKI 管理者がクライアント証明書を一時的に無効にしたい場合に使用できる。
そのような状況には、証明書の一時的な紛失や利用者団体からの一時的な休職などが含まれる。
証明書を永久的に無効にする証明書の失効とは異なり、証明書の効力の一時停止状態は、マネージド PKI 管理者が証明書を再有効化することができる。

SSL 証明書、適格証明書、コードサイニング証明書、タイムスタンプ及び JCAN 証明書は証明書の一時停止に対応していない。

4.9.14. 証明書の効力の一時停止の要求者

マネージド PKI 管理者は、GCC を通じて証明書の効力の一時停止及び解除を申請することができる。
GCC から申請されていない証明書の効力の一時停止は、GlobalSign では処理されない。

4.9.15. 証明書の効力の一時停止手続き

マネージド PKI 管理者は、GCC で証明書の一時停止を申請することができる。
申請が GCC で提出された後、同情報は、一時停止申請を処理するために、RA 及び CA と同期される。
証明書の一時停止は、「certificateHoldd」の理由コードで CRL に追加される

4.9.16. 証明書の効力の一時停止期限

証明書の一時停止は、証明書の有効期限まで継続することができる。

4.10. 証明書ステータス情報サービス

4.10.1. 運用上の特徴

GlobalSign は証明書のステータス情報を、CRL 配布ポイント及び OCSP レスポンダを通じて公開する。失効履歴は、CRL のファイルサイズ管理を効率化するために、証明書の有効期間満了後に削除することができるが、コードサイニング 証明書（有効期間満了後 10 年経過したもののみ）は例外である。

他の種類の証明書の場合、GlobalSign は、失効された証明書の有効期限が過ぎるまで、CRL 又は OCSP 上の失効履歴を削除しない。

GlobalSign は有効期限前の月(主に 30 日前及び 7 日前)に、利用中の証明書の有効期限について顧客へメールで通知する。

適格証明書については、失効状態が遡及しない。

ルートプログラムまたは CA/B Forum の要求により、GlobalSign は RevocationDate フィールドを使用して証明書の失効を遡及することができる。これは、RFC5280 に記載されている invalidityDate フィールドを使用するベストプラクティスの例外となる。

GlobalSign は コードサイニング証明書を過去に遡って失効させることができる。GlobalSign がコードサイニング証明書を過去に遡って失効させる場合、GlobalSign は RFC 5280 に記載されるベストプラクティスの例外として、CSBR 勧告に従い、CRL において invalidityDate ではなく revocationDate を使用するものとする。

4.10.2. サービスを利用できる時間

GlobalSign は、通常の動作条件下で 10 秒以下の応答時間を提供するのに充分なリソースを使用して、CRL 及び OCSP 機能を動作させ、維持する。
GlobalSign は、GlobalSign が発行する全ての有効証明書のステータスを自動的に確認するために、アプリケーションソフトウェアが使用できるオンラインレポジトリを 24 時間 365 日維持している。

GlobalSign は、優先順位の高い Certificate Problem Report に 24 時間 365 日社内で対応する体制を整えており、必要に応じて、そのような申し立てを法執行機関に転送し、そのような申し立ての対象である証明書を失効する。

システム障害、サービスダウン、またはその他の GlobalSign の管理下にないその他の要因により、GlobalSign はこの情報サービスが 48 時間を越えて利用できないことがないようにすることを目指します。

4.10.3. 運用上の特性

(規定なし)

4.11. 利用の終了

利用者は、証明書の失効又は証明書の有効期限を迎えることにより、証明書の利用を終了することができる。Trusted Root については、Trusted Root の利用者と GlobalSign の契約を終了させる手段として GlobalSign が証明書を失効する場合を除き、証明書の有効期間中全期間にわたり、Trusted Root の利用者と GlobalSign の契約が有効でなければならない。

4.12. キーエスクローとリカバリー

4.12.1. キーエスクローとリカバリーのポリシーと手続き

認証局の秘密鍵は預託(エスクロー)されてはならない。GlobalSign は利用者に対してもキーエスクローサービスを提供しない。

4.12.2. 鍵カプセル化とリカバリーのポリシーと手続き

(規定なし)

5. 施設、経営及び運用上の管理

GlobalSign の証明書管理プロセスには下記を必ず含むものとする。

1. 物理的なセキュリティ及び環境面の管理
2. 構成管理、信頼できるコードの完全性保守、及びマルウェアの検知/防止を含むシステムの完全性管理。
3. ポートの制限や IP アドレスフィルタリングを含むネットワークのセキュリティ及びファイアウォールの管理
4. ユーザ管理、信頼された役割の任務の区別、教育、認識、トレーニング、及び
5. 個人の説明責任を全うするための論理的アクセス制御、アクティビティログ記録、及び無活動時のタイムアウト。

GlobalSign のセキュリティプログラムは下記内容の年次のリスク評価を含む。

1. 証明書のデータ又は証明書の管理プロセスの不正アクセス、開示、悪用、改ざん、又は破壊につながる可能性のある予測可能な社内外の脅威を特定する。
2. 証明書データ及び証明書管理プロセスの機密性を考慮し、上記の脅威について、発現する可能性と潜在的な損害を評価する。
3. GlobalSIgn がそのような脅威に対抗するために制定している規程、手順書、情報システム、技術、及び他の取り決めの十分性を評価する。

GlobalSign は上記の目的を達成し、リスク評価で特定されたリスクの管理及び対策を行うため、リスク評価に基づき証明書データ及び証明書の管理プロセスの機密性に応じて設計されたセキュリティ手順、手段、及び製品からなるセキュリティ計画を開発、実施、及び維持している。

セキュリティ計画には、証明書データ及び証明書の管理プロセスの機密性に適した運営、組織、技術、及び物理的なセキュリティ対策が含まれる。セキュリティ計画はまた、利用可能な技術及び特定の措置を実施する費用を考慮に入れ、セキュリティ違反により生じる可能性のある危害及び保護されるべきデータの性質に適した合理的なレベルのセキュリティ対策を実施する。

5.1. 物理的管理

GlobalSign は、証明書発行に使用及び管理されるシステムにおいて、物理的なアクセス管理、自然災害からの保護、火災安全要因、ライフラインの停止(例:電源、電話など)、施設の故障、水漏れ、盗難に対する安全対策、破壊及び不法侵入や、災害対策などに対応する物理的かつ環境的セキュリティポリシーを持つものとする。
損失、損害、又は資産に対する損害、及び営業妨害、情報(データ)・データ処理施設の盗難を防ぐための管理対策を導入する。

5.1.1. 所在地及び建物

GlobalSign は、安全なデータセンター内に位置している。データセンターはコンクリート及びスチール製の専用施設である。

5.1.2. 物理的アクセス

GlobalSign は、生体認証型スキャナ及びカードアクセスシステムによる建物のセキュリティが万全な安全なデータセンター内で稼働している。閉回路の TV（CCTV）による監視及びデジタル録音が 1 日 24 時間年中無休で稼働している。資格を有する警備員が施設の安全を物理的に保護し、安全検査をクリアした関係者のみが敷地内の立ち入りを許可されている。

5.1.3. 電源及び空調

GlobalSign は、冗長な電力供給及び冷房設備を備えた安全なデータセンター内で稼働している。万が一電源が停止した場合には、UPS 及び電源発電機への障害迂回が実行される。

5.1.4. 水漏れ

GlobalSign は、水漏れから保護されている。地面から離れた階の、一段高い床の上に設置されている他、水漏れを検知する警報システムが設けられ、データセンター内の職員は万が一水漏れがあった場合に備え待機している。

5.1.5. 火災安全及び保護

GlobalSign は、火災検知・消防システムを備えたセキュアなデータセンター内にて運営する。

5.1.6. メディア　ストレージ(記憶媒体)

バックアップメディアは敷地外に保管されており、火災や水害から物理的に保護されている。

5.1.7. 廃棄処理

GlobalSign は情報の格納に使用された、全てのメディアが放出若しくは廃棄される前に、一般的に許容される方法において機密解除若しくは破壊されていることを保証するものとする。

5.1.8. オフサイトバックアップ

5.5 項の規定による。

5.2. 手続き的管理

5.2.1. 信頼された役割

GlobalSign は、審査要員を含む全てのオペレーター及び管理者が信頼された役割の範囲内で稼動していることを保証するものとする。
信頼された役割とは利益相反が不可能なものであり、如何なる人物も単独で CA システムのセキュリティを破ることができないように権限分散される。

信頼された役割は以下を含む。(但しこれに限定するものではない)

- 開発者：認証局システムの開発に対する責任がある
- セキュリティオフィサー又は情報セキュリティ長：認証局のセキュリティ実践導入の運営に対する全体的な責任
- 審査要員：適切な登録局システムを用いて証明書に含まれるデータの信頼性及び完全性を検証する責任があり、証明書の生成/失効/停止を承認する
- インフラシステムエンジニア：証明書のライフサイクル管理に使用される認証局システムのインストール、設定及び保守を許可されている
- インフラオペレーター：日常的な認証局システムの操作に責任を持つ。システムバックアップ/復旧、CA システムのアーカイブ及び監査ログの閲覧/保守管理を許可されている
- 監査人：アーカイブ及び監査ログの閲覧を許可されている
- 認証局起動データ保有者：認証局ハードウェアセキュリティモジュール操作に必要である、認証局起動データの保有を許可されている

5.2.2. タスク毎に必要な人員数

認証局の秘密鍵は信頼された役割に就いている人員のみによって、少なくとも 2 名体制で物理的に安全な環境でバックアップ、保管、復旧されている。

5.2.3. 各役割の識別及び認証

信頼された役割に指名する前に、GlobalSign は該当者の身元調査を行うものとする。
先に述べた各役割は、認証局をサポートするために適切な人物が適切な役割を所有していることを保証するために識別及び認証が行われている。

5.2.4. 職務分掌を要する役割

GlobalSign は、認証局設備にて（論理的）、或いは手続き的な方法にて、又はその両方の手段の組み合わせで、役割の分離を強制するものとする。個別の認証局担当者は上記の 5.2.1 項に定義される役割に指定される。

職務分掌が要求される業務には以下のものがある：

- 証明書の生成、失効、及び停止の承認者（審査要員）
- CA システムのインストール、構成、及び維持管理を行う者（インフラシステムエンジニア）
- CA のセキュリティ関連の活動について全面的な管理責任を負う者（セキュリティオフィサー）
- 暗号鍵ライフサイクル管理に関する職務を担う者（鍵コンポーネントの監督者など）（CA アクティベーションデータ保有者）
- CA システムの開発者（開発者）
- CA のシステム監査者（インフラオペレーター、監査人）

5.3. 人員コントロール

5.3.1. 資格、経験及び許可条件

従業員、代理人、又は独立した請負業者に関係なく、証明書の管理プロセスに従事する前に、GlobalSign はその者の身元及び信頼性を確認する。
GlobalSign は、職務権限に適切であり、また提示されたサービスに対して必要な専門知識、経験及び資格を所有する人員を雇用するものとする。
GlobalSign の人員は、正式なトレーニング及び教育、実地経験又はその両方の組み合わせを通して、専門知識、経験及び資格の要件を、満たすものとする。
5.2.1 項にて規定される、信頼された役割及び責任は、職務記述書中で文書化されるものとする。
GlobalSign の人員(臨時社員及び正社員の両者を含む)は、職務分掌及び権限の最小化という視点に立ち、職務、アクセスレベル、身元調査、従業員教育、(職務やセキュリティに対する)意識度などに基づく役職の機密性を明確にする職務表を有するものとする。信頼された役割には、GlobalSign の職員が正式に任命されている。

5.3.2. バックグラウンドチェック手続き

GlobalSign の信頼された役割に従事する全人員について、認証局運営の公平さを損なう恐れのある利益の相反はない。GlobalSign は、役職の適合性に影響するような重罪或いはその他犯罪で有罪判決を受けた人物を、信頼された役割に指名しないものとする。雇用された法域で上記のような調査が許可されているという条件のもと、必要な確認が全て終了し、結果が分析されるまでは、人員は信頼された機能にアクセスできないものとする。信頼された役割に従事する人員は全員、忠誠心、信頼性及び完全性に基づいて選ばれるものとし、法律で許可されている地域に関しては身元調査に従うものとする。

GlobalSign が行ったバックグラウンドチェックによって明らかになった情報を使用する如何なる場合も、その人物が雇用された法域の該当する法律に準拠しなければならない。

5.3.3. 研修要件

GlobalSign は、情報の正確性検証業務を行う全ての人員に、公開鍵基盤の知識、認証、また審査のポリシーや手順（認証局の CP 及び CPS を含む）、情報の正確性検証プロセスにおける一般的な脅威（フィッシングや他のソーシャルエンジニアリングの方策を含む）、及び Baseline Requirements に関する技能研修を実施している。

GlobalSign は上記研修の受講記録を保持しており、審査要員に任命された人員が該当業務を十分に遂行できるような技能水準を維持していることを保証する。

GlobalSign は審査要員にある業務の遂行を許可する前に、その人員が業務遂行に必要な技能を有していることを文書化するものとする。

GlobalSign は審査要員全員に対し、認証局が提供している Baseline Requirements に記載の情報の正確性検証要件に関する試験の合格を必須としている。

5.3.4. 再研修の頻度及び条件

信頼された役割に任命されている全ての人員はその信頼された役割に関連する GlobalSign の年次の研修及び業務遂行プログラムと同じレベルの技能を保持しているものとする。

運用に顕著な変更が出る場合は研修(認知/周知徹底のための)計画を作成し、またこの計画の実行は文書化されるものとする。

GlobalSign は全従業員に対し、少なくとも年に一度情報セキュリティ及びプライバシー研修を実施するものとする。

5.3.5. 職務のローテーション頻度及び条件

GlobalSign は、従業員の如何なる変更も、サービス効率又はシステムの安全性に影響するものではないことを保証するものとする。

5.3.6. 不正行為に対する処罰

運用処理に関して GlobalSign CP、本 CPS、又は認証局関連の運用手順が定める規定及びポリシーに違反した人物に対しては、適切な懲罰的処罰が課せられる。

5.3.7. 個別契約者の要件

GlobalSign に雇用される個人契約者は認証局の正規従業員と同様の処理、手続き、審査、セキュリティコントロール及びトレーニングに従わなければならないものとする。

5.3.8. 個人に付与された文書について

GlobalSign は本 CPS、該当する CP、関連する法規、ポリシー又は契約書をその従業員に対して入手可能な状態にするものとする。その他の技術的、運用的及び管理文書(例:管理マニュアル、ユーザマニュアル等)については、信頼された役割に従事する者に対し、職務遂行の目的で提供されるものとする。
全人員について、トレーニング受講の有無及び、受講済みトレーニングのレベルを識別したうえで、文書化の作業が維持継続される。

5.4. 監査ログの手続き

5.4.1. 記録されるイベントの種類

監査ログファイルは、認証局のセキュリティ及びサービスに関する全てのイベントに関して作成される。セキュリティ監査ログファイルは可能な限り、自動的に生成されるものとする。これが困難な場合は、記録帳、紙媒体又はその他の物理的メカニズムが使用される。コンプライアンス監査の期間中は、電子及び非電子に拘わらず全てのセキュリティ監査記録が再取得及び入手可能な状態になるものとする。
GlobalSign は、認証局のサービスにおいて信頼された役割を担う者が行なう如何なる行為の透明性を証明するため、証明書ライフサイクルに関する全ての事項を記録するものとする。少なくとも、各監査記録は下記の要素を含むものとする。(自動又は手動の記録)

- イベントの種類
- イベントの発生した日時
- 該当する場合、そのイベントの成功又は不成功
- イベントを生じた物又はオペレーターの識別
- イベントの目標とされた物の識別
- イベントの原因

GlobalSign 及び RA は証明書申請を処理し、証明書を発行するために取られた措置の詳細を記録する。これには、証明書申請時に生成された全ての情報及び受領した文書、日時、及び関係する人員が含まれる。GlobalSign はこれらの記録を、「はじめに」に規定された関連する CA 監査スキームに準拠していることを証明するものとして、適格監査人に提供するものとする。

GlobalSign は少なくとも下記のイベントを記録する:
下記を含む CA 証明書と鍵のライフサイクルに関するイベント:

- 鍵の生成、バックアップ、保管、復旧、アーカイブ、及び破壊
- 証明書申請、更新、鍵更新申請、及び失効
- 証明書申請の承認又は却下
- 暗号装置のライフサイクル管理に関わるイベント、及び
- CRL 及び OCSP エントリの生成
- 新しい証明書プロファイルの導入及び現行の証明書プロファイルの破棄

下記を含む利用者の証明書ライフサイクル管理に関わるイベント

- 証明書申請、更新、鍵更新申請、一時停止及び失効
- 本 CPS で規定された全ての正確性検証活動
- 証明書申請の承認又は却下証明書の発行、及び
- OCSP レスポンスへの署名

下記を含む、セキュリティ関連のイベント:

- PKI システムのアクセス試行の結果(成功・不成功を含む)
- PKI 及びセキュリティシステムでの操作
- セキュリティプロファイルの変更
- 証明書システムのソフトウェアのインストール、アップデート及び削除
- システムのクラッシュ、ハードウェアの故障、またその他異常事態
- ファイアウォール及びルーターの稼動内容
- 認証局施設への入退室

5.4.2. ログ処理の頻度

監査ログは定期的に悪意ある行為の証拠を確認するためレビューされており、また重要な作業後にも確認されている。

5.4.3. 監査ログの保有期間

GlobalSign は生成された監査ログを少なくとも 10 年分は保有するものとする。GlobalSign はこれらの監査ログを必要に応じて正規の監査人に提供する。

5.4.4. 監査ログの保護

全ての保有期間中において、監査ログは削除又は破壊(長期にわたり使用する媒体への移行を除く)されない方法で記録されるものとする。

監査ログは変更を防ぎ改ざんを検知できることと共に、権限を付与された信頼された個人によるアクセスによってのみ、完全性、信頼性及び機密性に影響なくデータの操作が可能であることが保証される状態でなければならない。

イベントの記録には、記録の生成日から保存期間の終了日までの間、イベント及びその実行の間において信頼関係があることを証明するため、安全な運用をされているタイムスタンプが必要となる。

5.4.5. 監査ログバックアップ手続き

監査ログ及び監査概要は安全な場所(例:耐火性の金庫)に、信頼された役割に任命された人員の下、情報発生源となる機器とは分離された状態でバックアップされなければならない。
バックアップされた監査ログはその原本と同様に保護されるものとする。

5.4.6. 監査ログ収集システム

監査ログの処理はシステムの起動時に開始され、またシステムの終了時にのみ終了する。監査ログ収集システムは収集されたデータの信頼性及び可用性を保証するものである。監査ログ収集システムは必要に応じてデータの機密性を保護する。万が一監査での収集物を処理中に問題が発生した場合、GlobalSign は問題が解決するまでの間、当該認証局の運用を停止するかどうか判断し、GlobalSign の影響を受ける情報資産所有者に通知する義務がある。

5.4.7. イベント発生要因の対象への通知

(規定なし)

5.4.8. 脆弱性の評価

GlobalSign は下記内容の年次リスク評価を実施する:

1. 証明書のデータ又は証明書の管理プロセスの不正アクセス、開示、悪用、改ざん、又は破壊につながる可能性のある予測可能な社内外の脅威を特定する。
2. 証明書データ及び証明書管理プロセスの機密性を考慮し、上記の脅威の可能性と潜在的な損害を評価する。

3. GlobalSIgn がそのような脅威に対抗するために制定している規程、手順書、情報システム、技術、及び他の取り決めの十分性を評価する。

また、GlobalSign は証明書の発行、製品及びサービスに関する GlobalSign の全資産に対して、脆弱性評価及び侵入テストを定期的に実施するものとする。当評価は、証明書発行処理に対する不正アクセス、改ざん、変更又は破壊を導き出す要因となる内部及び外部の脅威に重点をおくものとする。

5.5. アーカイブ対象記録

5.5.1. アーカイブ対象記録の種類

GlobalSign 及び RA は、署名の有効性並びに CA システムの適切な運用およびセキュリティを確立するために十分な詳細が含まれる記録をアーカイブするものとする。

API 接続する LRA は、JCAN 証明書発行に係るログ情報を信頼性のあ る方法で保持する。

5.5.2. アーカイブの保有期間

GlobalSign は証明書申請、正確性検証、全証明書及び失効に関する全文書、並びに CA システムのセキュリティに関する文書類を少なくとも、証明書の種類に応じて WebTrust 及び/又は eIDAS 又は UK eIDAS の要求事項に定められた保有期間内は保有するものとする。

保有期間は、GlobalSign との契約で別段の定めがない限り、当該文書に基づく証明書が有効でなくなってから 10 年である。

LRA は、サブジェクトの登録に使用される情報を、有効期限切れ後、又は失効後、少なくとも 7 年間保持する。 API 接続する LRA は、JCAN 証明書発行に係るログ情報を、少なくとも 1 年間保持する。

5.5.3. アーカイブの保護

保存が必要とされる期間中、アーカイブは削除若しくは破棄(長期にわたり使用する媒体への移行を除く)されない方法で作成されるともものとする。アーカイブの保護は、データの完全性、正当性、及び機密性を変更することなく、許可された信頼できるアクセスのみが操作を行なえることを証明するものとする。原本メディアがデータを必要な期間中保存できない場合は、定期的に新規メディアへアーカイブデータを移行するメカニズムがアーカイブ側により定義されるものとする。

5.5.4. アーカイブバックアップの手続き

アーカイブバックアップは GlobalSign のオンラインシステム上、或いはオフラインのシステム上に作成される。オンラインバックアップは週毎に複製され、この複製版はオリジナルのオンラインシステムとは別の場所に格納される。この複製版には、当該媒体の耐火金庫による保管を要する。
キーセレモニーの最後にはオフラインのバックアップを取り(キーセレモニーの手順に沿って作成された暗号生成物は別で保管されるため除く)、これをキーセレモニーから 30 日以内にオフサイトの場所にて保管するものとする

5.5.5. データのタイムスタンプについての要件

データのタイムスタンプに、タイムスタンプサービスが使用されている場合、6.8 項に定義される条件に準拠しなければならない。タイムスタンプの方法に拘わらず、全てのログにはイベントの発生時刻データが明示されている必要がある。

5.5.6. アーカイブ収集システム(組織内又は組織外)

アーカイブ収集システムは、5 項に定義されるセキュリティ条件に従うものとする。

5.5.7. アーカイブ情報の取得と検証の手続き

GlobalSign のアーカイブ情報を保存するメディアは、作成にあたり確認される。定期的に、アーカイブ情報の統計サンプルにてデータの継続的な完全性、及び可読性が検証される。
許可された GlobalSign の機器、信頼された役割及びその他許可された人員のみがアーカイブへのアクセスを認められる。アーカイブ情報の入手及び検証の依頼がある場合、信頼された役割のオペレーター(内部監査人、プロセスを統括しているマネージャー、及びセキュリティオフィサー)によって調整される。
訴訟の際に認証の証拠を提供する目的又は監査対応のために必要ならば、保管された記録は開示される。

5.6. 鍵交換

GlobalSign は、6.3.2 項に従って定期的に発行 CA の鍵データを交換する場合がある。
また、ベストプラクティスに準拠すべく証明書のサブジェクト情報及び証明書プロファイルも変更される可能性がある。
以前、利用者の証明書を署名していた秘密鍵は全利用者の証明書が期限切れとなるまで維持されるものとする。

5.7. 危殆化及び災害からの復旧

5.7.1. インシデント及び危殆化に対する対応手続き

GlobalSign は、インシデント対応計画及び災害復旧計画を有している。GlobalSign は、災害・セキュリティの問題、又は事業上の失敗の際にアプリケーションソフトウェアサプライヤー、利用者、また、依拠当事者を合理的に保護すべく設計された、事業継続性及び災害復旧手順を文書化している。
GlobalSign は利用者、依拠当事者、またアプリケーションソフトウェアのサプライヤーに事業継続計画を公開しないが、必要に応じて GlobalSign の監査人には事業計画及びセキュリティ計画を提出する。
GlobalSign は、これらの手順を年 1 回テストし、レビューした上で更新する。事業計画には次の内容を含む:

1. 計画を実行する条件
2. 緊急時の手順
3. 業務の代替手順
4. 再開の手順
5. 計画の保守スケジュール
6. 認知度及び教育の要件
7. 個人の責任
8. 目標復旧時間（RTO）
9. 危機管理計画の定期的な検査
10. 重要な事業プロセスの中断又は障害時に CA の事業運営をタイミング良く保持又は復旧するための GlobalSign の計画
11. 重要な暗号データ(すなわち、安全な暗号機器やそのアクティベーションデータ)を別の場所に保管するための要件
12. 許容可能なシステム停止時間及び復旧時間を構成するもの
13. 重要な事業情報及びソフトウェアのバックアップの頻度
14. CA の本拠地から復旧施設までの距離
15. 災害後の期間中、本拠地又は遠隔地で安全な環境を復元する前に、その施設を可能な限り保護するための手順

5.7.2. コンピューティング資産、ソフトウェア、又はデータが損壊した場合

万一何れの設備が損壊又は操作不能な状態で、しかしながら署名鍵が損壊していない場合、GlobalSign の事業継続計画に基づき証明書の状態情報の生成を優先し、可能限り早急に再構築されるものとする。

5.7.3. 秘密鍵が危殆化した際の手続き

GlobalSign CA の秘密鍵が危殆化、紛失、破壊、又は危惧化されたと疑われる場合、

- GlobalSign は問題の調査後、GlobalSign 証明書を失効すべきかを判断する。もし GlobalSign を失効すべきと判断した場合:
  - 証明書を発行された全利用者へ可能な限り最短のタイミングで通達する
  - 新規 GlobalSign の鍵ペアを生成又は既存の他の認証局階層を代替として使用して新規利用者の証明書を作成する。

5.7.4. 失効ステータスの可用性

失効ステータス情報は、CA 鍵が危殆化した場合に、公的にアクセス可能な場所で提供され、維持されるものとする。(証明書のステータス情報に関するサービスを GMO インターネットの他のグループ会社に移転する場合等が該当する。)

5.7.5. 災害後の事業継続能力

5.7.1 項に明記されるように、災害復旧計画は事業継続について取り決めている。証明書状態情報システムは 24 時間 365 日を通して利用可能な状態に展開されるものとする。

5.8. 認証局又は RA の稼動終了

発行 CA 又は RA の稼働を終了する必要がある場合には、その終了による影響は、一般的な状況に基づいて判断し、可能な限り最小限にとどめるものとし、また該当の発行 CA 又は RA との契約内容に従う。GlobalSign は、そのデジタル証明書の発行及び管理業務の全部又は一部を終了する場合には、その終了の手順を明示する。その手順は少なくとも次の内容を含む:

- 認証局の終了のために生じる混乱を可能な限り最小限にとどめることを保証すること
- 認証局のアーカイブされたデータが保存されることを保証すること
- 認証局の終了に関する通知が利用者、承認された依拠当事者、アプリケーションソフトウェアプロバイダ、その他 GlobalSign の証明書ライフサイクルに利害関係を有する者に対して速やかに行われることを保証すること
- 認証局の終了後も一定の期間内は証明書の失効情報に関するサービスが引き続き提供及び維持される旨を保証すること。(証明書のステータス情報に関するサービスを GMO インターネットの他のグループ会社に移転する場合等が該当する。)
- 発行 CA で発行された全てのデジタル証明書を認証局の終了の時点で失効させるための手続が維持されることを保証すること
- eIDAS/UK eIDAS 適合性評価機関を含む、全監査人への通知
- ベルギーの eIDAS 監督機関(経済・中小企業・自営業者・エネルギー省)に通知すること
- 英国の UK eIDAS 監督機関(情報コミッショナーズオフィス)に通知すること
- 準拠法及び関連規則に従い、その他の関連する政府機関及び認証機関に通知すること

5.8.1. 業務を引き継ぐ認証局

実利的かつ合理的な範囲において、後任の認証局は、終了する前任の認証局と同じ権利義務を負うべきである。
後任の認証局は、前任の認証局の業務終了によりその鍵とデジタル証明書が失効した全ての利用者に対して、各サービスプロバイダ又は利用者の行う新しいデジタル証明書の申請に基づいて、初回の登録と識別及び認証要件の具備を条件として、新規のサービスプロバイダ契約又は証明書保有者契約を締結したうえで、新たに鍵とデジタル証明書を発行するものとする。

6. 技術的セキュリティ管理

6.1. 鍵ペア生成及びインストール

6.1.1. 鍵ペア生成

6.1.1.1. CA 鍵ペア生成

GlobalSign はルート CA の鍵ペアに対し下記の管理を行う:

1. 鍵生成のスクリプトを作成し、それに従う
2. 正規の監査人がルート CA 鍵ペア生成プロセスに立ち会うか、ルート CA 鍵ペア生成プロセス全体のビデオを記録する。
3. 正規の監査人が、鍵生成及び証明書生成プロセス中に GlobalSign がキーセレモニーのスクリプトに従い、鍵ペアの完全性及び機密性を確保するために使用されるコントロールを遵守した旨の報告書を発行する。

その他 CA の鍵ペアに対しては、下記の管理を行う:

1. CP 及び/又は CPS の 5.1 項及び 5.2.2 項に記載されている通り物理的に安全な環境で鍵を生成する
2. 複数の人員による管理及び知識分割という原則の下、信頼された役割に従事する人員が CA の鍵を生成する
3. CA の CP 及び/又は CPS に開示されているように、該当の技術的及び事業要件を満たす暗号モジュール内で CA 鍵を生成する
4. CA 鍵生成に係る作業をログとして記録する
5. CP 及び/又は CPS、また(該当する場合)鍵生成スクリプトに記載された手順に準拠して秘密鍵が生成及び保護されているという合理的保証を実現するための有効的なコントロールを維持する

6.1.1.2. 利用者の鍵ペア生成

GlobalSign によって生成された利用者鍵については、6.1.5 項及び 6.1.6 項に規定されている鍵生成アルゴリズム及び鍵のサイズを使用して、FIPS 140-2(又は同等の)に準拠した安全な暗号装置において鍵生成が行われる。
GlobalSign は、証明書申請に既知の弱い秘密鍵が含まれている場合、証明書申請を受け付けないこととする。

コードサイニング証明書に使用される鍵は、安全なハードウェアトークンで生成されなければならない。

秘密鍵がサブジェクトに代わって GlobalSign 又はサードパーティによって生成される適格証明書の場合、秘密鍵は GlobalSign 又はサードパーティによって保持され、安全に保管されなければならない。デバイスがサブジェクトに代わって第三者によって管理される場合、GlobalSign は、当該第三者が資格認定の観点から適切な要件を満たしていることを検証しなければならない。

QCP-n 又は QCP-l ポリシーに準拠して発行された適格証明書については、安全な暗号化装置はオプションである。

認証された公開鍵に関連する秘密鍵が QSCD に存在する適格証明書については、利用者鍵が生成され、認められた適格署名作成装置(QSCD)内に格納される。QSCD の認証ステータスは監視され、変更があれば失効を含む適切な措置を講じる。

JCAN 証明書を申請するために、利用者による秘密鍵の生成は行わない。JCAN 証明書発行の申請に紐づけられている秘密鍵は、各申請毎に新規で生成されたものでなく てはならない。

6.1.2. 利用者への秘密鍵配布

GlobalSign はパブリックに信頼される SSL 又はコードサイニング証明書用の秘密鍵は生成しない。

利用者の代理として秘密鍵を生成する GlobalSign は、鍵生成の工程から利用者への証明書発行過程において、十分なセキュリティが保たれている時にのみ、それを担うことができる。

パブリックに信頼されない SSL 証明書に関しては、秘密鍵及び証明書を含む、最短 16 文字のパスワードで暗号化された PKCS#12 (.pfx)ファイルを使用することで、上記の条件を満たす。証明書の申請時に最低 8 文字の文字列がシステムにより生成され、利用者に提供された上で利用者が最低 8 文字の文字列を指定する。SMIME 証明書に関しては、秘密鍵及び証明書を含む、利用者が選択した最低 12 文字のパスワードで暗号化された PKCS#12(.pfx)ファイルを使用することで上記の条件を満たす。

適格証明書については、秘密鍵はサブジェクトに代わって GlobalSign 又はサードパーティによって管理され る場合がある。秘密鍵がサブジェクトに代わって管理される場合、GlobalSign は、サブジェクトがその秘密鍵を単独で制御(又はサブジェクトが法人の場合、「制御」)できることを保証するものとする。サードパーティによって管理されている鍵については、GlobalSign は、サードパーティが単独で制御することを保証するものとする。

秘密鍵が QSCD 上に存在する適格証明書について、GlobalSign 又はサードパーティがサブジェクトのために QSCD を管理する場合、秘密鍵は QSCD 内を除いて署名のために使用されてはならないものとする。サブジェクトの秘密鍵ペアは、それぞれ電子署名又は e シールにのみ使用されなければならない。

適格証明書については、GlobalSign が利用者に代わって秘密鍵を管理する場合のみ、GlobalSign は秘密鍵 を生成する。

GlobalSign は適切な RNG 又は PRNG を介して、全ての公開鍵/秘密鍵の完全性及び鍵素材の乱数性を保証する。万が一秘密鍵が認可されていない人物又は利用者と関連のない組織に付与されたことが検出、又は疑われた場合、GlobalSign は、付与された秘密鍵に対応する公開鍵を含む全ての証明書を失効させる。

6.1.3. 証明書発行者へ公開鍵の配布

GlobalSign は、RA から伝送される経路が保護されており、その根源についての真正性と完全性が適切に検証された公開鍵のみを受け入れる。

6.1.4. 認証局から依拠当事者への公開鍵配布

GlobalSign は依拠当事者へ公開鍵を配布するにあたり、鍵のすり替えを防ぐため、相応の方法で請け負うことを保証するも のとする。商業ブラウザ及びプラットフォームオペレーターは、ルートストア及び OS にルート証明書公開鍵を組み込むことが推奨されている。利用者からの発行 CA の公開鍵は、一連の証明書又は GlobalSign が操作するレポジトリを介して配布され、AIA(認証機関アクセス情報)を通じて発行済み証明書のプロファイル内で参照される。発行 CA の公開鍵は、証明書のチェーン又は GlobalSign が運営するレポジトリを介して利用者から配布され、AIA(認証機関アクセス情報)を通じて発行済み証明書のプロファイル内で参照される。

6.1.5. 鍵のサイズ

GlobalSign は、米国国立標準技術研究所(NIST)の特別刊行物 800-133 改訂 2(2020 年) -暗号鍵生成のための勧告-ルート認証局、発行 CA、及び利用者用の鍵ペアの選択において推奨されるタイムライン及びベストプラクティス

について-に準拠している。また GlobalSign の直接管理下にない、信頼されたルートプログラムに属する下位認証局も同様のベストプラクティスを実行することが契約上義務付けられているものとする。
GlobalSign は、以下の鍵のサイズ/ハッシュ値からルート証明書、発行 CA の証明書、エンドエンティティ証明書、並びに CRL/OSCP 証明書のステータスレスポンダを選択する。これらの選択肢は Baseline Requirements 及び EV ガイドラインに準拠している。

証明書はアルゴリズムの種類、及び鍵長について下記の要件を満たさなければならない。

ルート CA 証明書

	有効期間が 2010 年 12 月 31 日以前より開始する	有効期間が 2010 年 12 月 31 日より後に開始する
ダイジェストアルゴリズム	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-256, SHA-384 or SHA- 512
RSA の最低モジュールサイズ（ビット）	2048 [4]	2048
楕円曲線	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521

Subordinate 証明書

	有効期間が 2010 年 12 月 31 日以前より開始し、2013 年 12 月 31 日以前に終了する。	有効期間は 2010 年 12 月 31 日より後に開始し、2013 年 12 月 31 日より後に終了する。
ダイジェストアルゴリズム	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1 [5], SHA-256, SHA-384 or SHA-512
RSA の最低モジュールサイズ（ビット）	1024	2048
楕円曲線	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521

利用者の証明書

ダイジェストアルゴリズム	SHA-1 [6], SHA-256, SHA-384 or SHA- 512
RSA の最低モジュールサイズ（ビット）	2048
楕円曲線	NIST P-256, P-384, or P-521
RSASSA-PSS [7]	

2017 年 7 月 1 日以降、AATL の下位認証局を発行する新しいルート CA 証明書の最小鍵サイズは、RSA 3072 ビット又は ECC NIST P-384 である。

2021 年 1 月 1 日以降、コードサイニング及びタイムスタンプ証明書を発行する新しいルート CA 証明書及び下位 CA 証明書の最小鍵サイズは、RSA 3072 ビット又は ECC NIST P-256 である。

[4] RSA 鍵のモジュールサイズ（ビット）は 8 で割り切れるものでなければならない。2048 ビット未満の RSA 鍵のサイズを有する 2010 年 12 月 31 日以前に発行されたルート CA 証明書は、依然として、本要件に従って発行された利用者の証明書に対するトラストアンカーとしての役割を果たす。
[5] SHA-1 は、IntranetSSL SSL 下位認証局の証明書に使用される場合があるが、こうした CA 証明書がパブリックに信頼されるルートにチェーンすることはない。
[6] SHA-1 は、IntranetSSL 利用者認証局の証明書に使用される場合があるが、こうした CA 証明書がパブリックに信頼されるルートにチェーンすることはない。
[7] RSASSA-PSS は、7.1.3 項で定義された基準に従って、PersonalSign 証明書用の RSA 鍵と併用可能。

2021 年 6 月 1 日以降、新しい Code Signing 及び Timestamping 用利用者証明書の最小鍵サイズは、 RSA 3072-bit 又は ECC NIST P-256 である。

6.1.6. 公開鍵パラメーター生成及び品質検査

GlobalSign は FIPS 186 の規定に従い鍵を生成し、また利用者から提示される鍵の適合性を適切な技術を用いて検証するものとする。既知の脆弱な鍵は検証され、また提出時に拒否される。GlobalSign は、品質検査に関し Baseline Requirements の 6.1.6 項を参照するものとする。

6.1.7. 鍵の使用目的(X.509 v3 鍵使用フィールドにおいて)

GlobalSign は、申請で提案されるフィールドに従い、証明書における鍵の用途を、X.509 v3 の v3 鍵使用フィールドにより設定するものとする。(7.1 項を参照)

ルート証明書に紐づく秘密鍵は、以下の場合を除き、証明書に署名する用途では用いられない。

1. ルート CA 自身を表すための、自己署名証明書
2. 下位認証局及び相互認証証明書
3. OCSP からのレスポンスの正確性検証をする証明書

6.2. 秘密鍵保護及び暗号化モジュール技術管理

GlobalSign は、証明書の不正発行を防止するために、物理的及び論理的な対策を実装している。上記に明記された検証済みシステム又は装置以外の CA 秘密鍵の保護は、物理セキュリティ、暗号化、又は両方の組み合わせで構成され、CA 秘密鍵の公開を防ぐ方法で実装されなければならない。GlobalSign は、暗号化された鍵又は鍵部分の残存寿命中、暗号解読攻撃に耐えることができる最先端のアルゴリズム及び鍵長を用いて、その秘密鍵を暗号化する。

6.2.1. 暗号化モジュールの基準及び管理

GlobalSign は証明書及び GlobalSign が管理している下位 CA 鍵ペアを生成している CRL の署名、又は OCSP のレスポンスを生成する全システムにおいて、少なくとも FIPS140-2 レベル 3 の暗号保護を使用していることを保証するものとする。GlobalSign は利用者に対して、FIPS140-2 レベル 2 若しくはそれ以上のシステムを秘密鍵の保護に使用することを要求、また利用者が保護を保証するために当該システム若しくは適切なメカニズムを使用することに合意の上で責任を持つことを定める。GlobalSign が使用している適切なメカニズムとは、申請プロセスの一環として既知の FIPS に準拠したハードウェアプラットフォームに接続された適切な CSP(暗号化サービスプロバイダ)に限定することである。

6.2.2. 秘密鍵(m 中の n) 複数の人員による管理

GlobalSign は、信頼された役割において職務を担う複数人員の管理の下、文書化された手順に従い、認証局の秘密鍵を暗号化操作のために管理(認証局アクティベーションデータを使用)するものとする。この秘密鍵の複数人員による管理に携わる信頼された役割は、強力に認証される。(例:PIN コード付きトークン)

6.2.3. 第三者への秘密鍵の預託

GlobalSign は、如何なる者に対しても秘密鍵を第三者預託するものではない。

6.2.4. 秘密鍵のバックアップ

GlobalSign は災害時事業継続のために必要な場合、ルート及び下位層の秘密鍵を原本の秘密鍵と同様に複数人員の管理下の元バックアップを行なうものとする。

GlobalSign は、サブジェクトに代わって GlobalSign が管理する QSCD に秘密鍵が存在する場合にのみ、適格証明書の利用者秘密鍵のバックアップを実行する。 バックアップメカニズムは、プライマリロケーションと同じセキュリティ制御で秘密鍵を複製する。

6.2.5. 秘密鍵のアーカイブ

GlobalSign は利用者の秘密鍵のアーカイブを行なわず、秘密鍵の生成過程で鍵が存在していた可能性のある一時的な記憶場所からも削除されることを保証する。

6.2.6. 暗号モジュール間の秘密鍵移行

GlobalSign CA の秘密鍵は、ハードウェアセキュリティモジュールにおいて生成、アクティブ化、及び保存されている。秘密鍵がハードウェアセキュリティモジュールの外(保存若しくは移行のため)にある場合は、暗号化されていることが必須となる。秘密鍵は、暗号モジュール外の環境にて、一般テキスト状態で存在しては絶対にならない。

万が一、下位認証局の秘密鍵が許可されていない人物又は利用者と関連のない組織に付与されたことを GlobalSign が認識した場合、GlobalSign は付与された秘密鍵に対応する公開鍵を含む全ての証明書を失効させる。

6.2.7. 暗号モジュールにおける秘密鍵の保存

GlobalSign は少なくとも FIPS140-2 レベル 3 若しくはそれ以上のデバイスにおいてルート CA 又は下位 CA の秘密鍵を保存するものとする。

6.2.8. 秘密鍵のアクティブ化方法

GlobalSign はハードウェアセキュリティモジュールの製造元が提供する仕様説明書に従い、秘密鍵をアクティブ化する責任を有する。利用者は、利用契約又は利用約款に示される条件に従い、秘密鍵を保護する責任を有する。

6.2.9. 秘密鍵の非アクティブ化方法

GlobalSign はアクティブ化されたハードウェアセキュリティモジュールを放置せず、また不正アクセスが可能な状況にしないことを保証するものとする。GlobalSign の暗号モジュールがオンラインかつ操作可能な間、認証された RA から要求された証明書の発行と、CRL/OCSP の署名にのみ使用される。認証局が運営停止となる際、その秘密鍵はハードウェアセキュリティモジュールから削除される。

6.2.10. 秘密鍵の破棄方法

GlobalSign CA の秘密鍵は、不必要となった時点若しくは対応する証明書が期限切れ又は失効した際に、信任された 2 名以上の人員による複数人管理のもと破棄される。秘密鍵を破棄するにあたり GlobalSign は秘密鍵の如何なる部分も推定されないよう、HSM 内の関連する認証局の秘密アクティベーションデータ全てを破棄する。鍵を破棄する手順は文書化し、関連する記録をアーカイブする。

GlobalSign が GCC で生成した利用者の秘密鍵は PKCS#12 形式で保管され、鍵生成から 30 日経過した時点で自動的に GCC から消去される。

6.2.11. 暗号モジュール 評価

6.2.1 項を参照

6.3. 鍵ペア管理におけるその他の側面

6.3.1. 公開鍵のアーカイブ

GlobalSign は証明書の公開鍵をアーカイブしなければならない。

6.3.2. 証明書の操作可能期間及び鍵ペアの使用期間

証明書は最長で下記に述べる有効期間を持つものとする。

種類	鍵ペアの使用期間	最長証明期間
ルート証明書 [8]	規定なし	28 年
TPM ルート証明書	30 年	41 年
パブリックな下位認証局/発行 CA	規定なし	18 年
Trusted Root	規定なし	11 年
PersonalSign 証明書	規定なし	39 か月
Code Signing 証明書	規定なし	39 か月
EV Code Signing 証明書	規定なし	39 か月
AATL エンドエンティティ証明書	規定なし	39 か月

[8] *RSA によって 2003 年以前に生成された 2048 の鍵については、ハードウェア、ルートストア、及び OS における鍵長の制限のため用途が制限されており、 利用可能年数を 25 年としている。*

eIDAS 適格 e シール証明書、eIDAS 適格電子署名証明書	規定なし	39 か月
DV SSL 証明書	規定なし	397(398)日[9]
AlphaSSL 証明書	規定なし	397(398)日
OV SSL & ICPEdu 証明書	規定なし	397(398)日
EV SSL 証明書	規定なし	397(398)日
eIDAS 適格 SSL サーバ証明書	規定なし	397(398)日
イントラネット SSL	規定なし	5 年
EV SSL 証明書	規定なし	27 か月
Timestamping 証明書	15 か月	11 年
NAESB 証明書	2 年	2 年
JCAN Certificates	825 日	825 日
Private Key Archival\Key Recovery Agent Certificates	規定なし	5 年

鍵ペアの使用期間は、最大で証明書と同じ有効期間に設定することができる。

特定の CA によって署名された証明書は、その CA 証明書の有効期間満了前又は終了日までに有効期間が終了しなければならない。

GlobalSign 証明書は、最長有効期間に関し Baseline Requirements に準拠している。利用者の証明書がそれよりも短い有効期間の場合は、期限が切れた後に元々の有効期間まで再発行が可能となる。

2022 年 4 月 1 日をもって、 id-kp-emailProtection EKU を含むエンドエンティティ証明書の最長有効期間は 1185 日となる。

6.4. アクティベーションデータ

6.4.1. アクティベーションデータの生成及びインストール

GlobalSign CA の秘密鍵をアクティブ化するために使用される、GlobalSign のアクティベーションデータの生成及び使用はキーセレモニー(6.1.1 項を参照)中に行なわれるものとする。アクティベーションデータは適切な HSM(ハードウェアセキュリティモジュール)により自動的に生成、又は同じニーズを満たすような方法で生成される。その後、信頼された役割を担う鍵の持分所有者に配布されるものとする。配布方法においては、アクティベーションデータの機密性及び完全性が保持されなければならない。

6.4.2. アクティベーションデータの保護

発行 CA のアクティベーションデータは、暗号化及び物理的なアクセス管理の仕組みを介して漏洩から保護されなければならない。GlobalSign のアクティベーションデータはスマートカードに格納されなければならない。

6.4.3. その他のアクティベーションデータの要素

GlobalSign のアクティベーションデータの保持は、信頼された役割に従事する GlobalSign の人員に限定しなければならない。

6.5. コンピュータ セキュリティ コントロール

6.5.1. 特定のコンピュータ セキュリティ技術条件

下記のコンピュータ セキュリティ機能は OS、又は OS、ソフトウェア及び物理的防御の組み合わせの何れかにより提供されなければならない。GlobalSign の PKI 構成は下記の機能を必ず含むものとする。

---

9 *有効期間が notBefore から notAfter を含めない期間までと定義される場合は 397 日。notBefore から notAfter を含める期間までと定義される場合は 398 日。*

- 信頼された役割に対しログイン時に認証を要求
- 最低限の権限を付与した任意のアクセスコントロールを提供
- セキュリティ監査能力を提供(完全性が保護されていること)
- 対象物の再利用を禁止
- 強固なパスワードポリシーの使用を要求
- セッション中の通信に対して暗号法の使用を要求
- 識別及び認証には、信頼されたパスを要求
- 不正コードから保護する手段を提供
- ソフトウェア及びファームウェアの完全性を保持する手段を提供
- 処理に対してドメインの分離、様々なシステム及びプロセスの分割を提供する
- OS に対して自己防御を提供する

直接的に証明書発行が可能なアカウントに対し、GlobalSign は多要素認証を実行する。

6.5.2. コンピュータ セキュリティの評価

（規定なし）

6.6. ライフサイクル 技術管理

6.6.1. システム開発管理

GlobalSign におけるシステム開発管理は以下の通り。

- 正式かつ書面化された開発方法にて設計並びに開発されたソフトウェアを使用しなければならない
- 全てのハードウェアは、供給の適合性、及び改ざんの証拠がないことを保証するために試運転の過程で検査されるものとする。入手したハードウェア及びソフトウェアは、どの特定の部品においても改ざんされうる可能性を低減する方法で購入されたものであること。(例：購入時に機器が無作為に選択されたものであることを確認するなど)
- 開発されたハードウェア及びソフトウェアが管理された環境において開発され、開発プロセスが定義された上で文書化されていること。この条件は商業的に流通するハードウェア及びソフトウェアには適用されない
- これらのハードウェア及びソフトウェアで行なう業務は認証局の業務に限定される。認証局の運営に関係のないアプリケーション、ハードウェアデバイス、ネットワーク接続又はインストールされたソフトウェアは存在しない。
- 正しい管理方法により不正なソフトウェアの機器への搭載を防いでいる。認証局の業務を行なうのに必要なアプリケーションのみが機器にインストールされ、ローカルポリシーにより認可されたソースから入手される。GlobalSign のハードウェア及びソフトウェアは、最初の使用時及びその後定期的に不正コードの検知のためにスキャンされる。
- ハードウェア及びソフトウェアの更新版は、元の機器と同様の条件で購入又は開発され、また信頼され教育を受けた人員によって、定められる条件に基づきインストールされる。

6.6.2. セキュリティ マネージメント コントロール

GlobalSign システムの設定は、何れの変更及び更新と同様に文書化され、GlobalSign の管理者により管理されるものとする。GlobalSign のソフトウェア又は設定に対する不正な変更を検知するための仕組みを持つ。正式な設定管理技法が GlobalSign システムの導入及び稼働中の保守において使用されている。最初に GlobalSign のソフトウェアが起動される際、業者から納入された通りであり、変更がなされていないか、更に使用目的のバージョンであるかの確認がなされる。

6.6.3. ライフサイクル セキュリティ コントロール

GlobalSign は、評価・認証されたソフトウェア及びハードウェアの信頼度を保持するため、保守スキームを継続的に維持管理する。

6.7. ネットワーク セキュリティ コントロール

GlobalSign の PKI 構成は、これらがサービスへの妨害(停止)や侵入攻撃から守られていることを保証するため、適切なセキュリティ対応が導入されるものとする。このような対応策には、ガードの使用、ファイアウォール及びルーターのフィルタリングを含む。使用されていないネットワークポート及びサービスは遮断する。PKI 機器がホストされているネットワークを保護する目的で使用される何れの境界コントロールデバイスも、同じネットワーク上のその他機器においてその他サービスが有効化されていたとしても、PKI 機器に必要なサービス以外は全て拒否する。

6.8. タイムスタンプ

GlobalSign の全コンポーネント定期的に信頼できるタイムサービスとの同期を行う。GlobalSign は 1 つの GPS ソース及び 3 つの非認証の NTP ソースのクロックを、正確な時刻を確立するために使用する。

- CA 証明書の初期検証時刻
- CA 証明書の失効
- CRL の掲示
- 利用者のエンドエンティティ証明書の発行

システム時刻の保守には電子的又は手動的手続きが適用される。時計の調整は監査対象イベントとなる。

6.8.1. PDF 署名タイムスタンピングサービス

PDF 署名証明書のデジタル ID によって作成される全てのデジタル署名には、RFC3161 に準拠し、GlobalSign ルート証明書にチェーンされたタイムスタンプ局(TSA)によって発行されたタイムスタンプを含むことができる。当該 TSA の証明書は FIPS140-2 レベル 3 かそれ以上の HSM に格納されなければならない。

6.8.2. コードサイニング及び EV コードサイニングタイムスタンピングサービス

コードサイニング又は EV コードサイニングよって作成される全てのデジタル署名には、RFC3161 に準拠し、GlobalSign ルート CA にチェーンされたタイムスタンプ局(TSA)によって発行されたタイムスタンプを含むことができる。当該 TSA の証明書は FIPS140-2 レベル 3 かそれ以上の HSM に格納されなければならない。

7. 証明書、CRL、及び OCSP のプロファイル

7.1 証明書プロファイル

7.1.1. バージョン番号

GlobalSign は、X.509 バージョン 3 に従ってデジタル証明書を発行するものとする。

7.1.2. 証明書拡張

GlobalSign は、RFC5280 及び現在の Baseline Requirements の 7.1.2.1 から 7.1.2.5 項を含む適用可能なベストプラクティスに従い、証明書を発行するものとする。ただし、本書に記載されている場合を除く。名前の制限(NameConstraints)が設定された場合、依拠当事者を不要なリスクから守るために、重要度(クリティカリティ)についてはベストプラクティスに従って設定される。

下位認証機関及びエンドエンティティ証明書は、証明書の使用目的を説明する KeyPurposeId(s) を含む Extended Key Usage エクステンションを含む。KeyPurposeId 及び ExtendedKeyUsage は、パブリックに信頼されるエンドエンティティ証明書には含まれない。

7.1.3. アルゴリズム識別子

GlobalSign は、下記の OID に示されるアルゴリズムで証明書を発行するものとする。

SHA1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}
SHA256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
SHA384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
SHA512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 13}

ECDSAWithSHA256	{iso(1) member‐body(2) us(840) ansi‐X9‐62 (10045) signatures(4) ecdsa‐with‐SHA2(3) 2 }
ECDSAWithSHA384	{iso(1) member‐body(2) us(840) ansi‐X9‐62 (10045) signatures(4) ecdsa‐with‐SHA2(3) 3 }
ECDSAWithSHA512	{iso(1) member‐body(2) us(840) ansi‐X9‐62 (10045) signatures(4) ecdsa‐with‐SHA2(3) 4 }
RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsassa-pss(10)}

*パブリックに信頼されたエンドエンティティ証明書の署名には使用しない。

7.1.4. 名前形式

GlobalSign は、RFC5280 に従う名前形式及び Baseline Requirements の 7.1.4 項に準拠して証明書を発行する。SSL 証明書の場合、commonName フィールドが存在する場合、このフィールドには、証明書の subjectAltName エクステンションに含まれる値の 1 つである単一の IP アドレス又は FQDN が含まれる。

パブリックに信頼される SSL 証明書では、2022 年 9 月 1 日以降に発行される証明書には Subject organizationalUnitName フィールドは含まれない。

7.1.5. 名前制約

GlobalSign は必要に応じて名前の制限(NameConstraints)を適用して下位 CA 証明書を発行し、また TrustedRoot プログラムの一部として必要な場合にはそれを重要度として設定する。下位認証局に名前の制限(NameConstraints)が設定されていない場合、その CA は本 CPS の 8.0 項に記載されている全面監査の対象に含まれなければならない。

GlobalSign の名前の制限(NameConstraints)は、次の方法を使用する。

- 証明書が id-kp-serverAuth extended key usage を含む場合は、Baseline Requirements バージョン 1.3 以降の 7.1.5 項に記載の通り dNSName、iPAddress、及び DirectoryName に制限をかけなければならない。
- 証明書が id-kp-emailProtection extended key usage を含む場合、Baseline Requirements の 3.2.2.4 項に従い所有権を認証された各名前のうち、最低 1 つは permittedSubtrees に属すという rfc822Name に制限がかかった X.509v3 拡張子の名前の制限(NameConstraints)を含まなければならない。
- GlobalSign は Baseline Requirements の 7.1.5 項に従い、id-kp-emailProtection extended key usage の証明書にも dNSName、iPAddress、及び DirectoryName に名前の制限(NameConstraints)をかけることも可能である。

7.1.6. 証明書ポリシー識別子

GlobalSign は Baseline Requirements の 7.1.6 項に従う。

7.1.7. ポリシー制約拡張の使用

(規定なし)

7.1.8. ポリシー修飾子の構文と意味

GlobalSign は、依拠当事者がそれを受け入れ可能かどうかを判断できるように、ポリシー修飾子と適切なテキストを含めることができる形でデジタル証明書を発行する。

7.1.9. クリティカルな証明書ポリシー拡張についての解釈方法

(規定なし)

7.1.10. シリアル番号

各発行 CA は、CSPRNG からの最低 64 ビットのアウトプットを含む、0 以上の連番でない独自の(発行者サブジェクト識別名及び CA 証明書シリアル番号内のコンテクスト)証明書シリアル番号を含む証明書を発行しなければならない。
TLS 証明書では RFC5280 の例外として、TLS 事前証明書と証明書は同一の serialNumber 値を共有する。

7.1.11. 適格証明書に関する特則

適格証明書は、ETSI EN 319 412 及び ETSI TS 119 495 の該当するプロファイル要件を満たすように設定されている。

7.1.11.1. eIDAS 適格電子署名証明書

eIDAS 適格電子署名証明書には次の適格命令文が含まれる。

- id-etsi-qcs-QcCompliance
- id-etsi-qct-esign

認証された公開鍵に関連する秘密鍵が QSCD に存在する場合は、「id-etsi-qcs-QcSSCD」が含まれる。

UK eIDAS に基づき発行される適格電子署名証明書には、値が GB に設定された「id-etsi-qcs-QcCClegislation」が含まれる。

7.1.11.2. eIDAS 適格 e シール証明書

eIDAS 適格 e シール証明書には次の適格命令文が含まれる。

- id-etsi-qcs-QcCompliance

- id-etsi-qct-eseal

認証された公開鍵に関連する秘密鍵が QSCD に存在する場合は、「id-etsi-qcs-QcSSCD」が含まれる。

PSD2 で使用するために発行された適格 e シール証明書には、「id-etsi-psd2-qcStatement」が含まれる。

UK eIDAS に基づき発行される適格 e シール証明書には、値が GB に設定された「id-etsi-qcs-QcCClegislation」が含まれる。

7.1.11.3. eIDAS 適格 SSL サーバ証明書

eIDAS 適格 SSL サーバ証明書には次の適格命令文が含まれる。

- id-etsi-qcs-QcCompliance
- id-etsi-qct-web

PSD2 で使用するために発行された適格 SSL サーバ証明書には、「id-etsi-psd2-qcStatement」が含まれる。

UK eIDAS に基づき発行される適格 SSL サーバ証明書には、値が GB に設定された「id-etsi-qcs-QcCClegislation」が含まれる。

7.2 CRL プロファイル

7.2.1. バージョン番号

GlobalSign は RFC5280 に従い、バージョン 2 の CRL を発行するものとする。失効リストは以下のフィールドを含む。

- 発行者 GlobalSign XXX 等(製品による)
- 有効開始日 日付及び時間
- NextUpdate 日付及び時間
- 署名アルゴリズム sha256RSA 等(製品による)
- 署名ハッシュアルゴリズム sha256 等(製品による)
- シリアル番号 失効された証明書のシリアル番号
- 失効日 失効日

7.2.2. CRL 及び CRL エントリ拡張子

CRL は、以下の拡張子(エクステンション)を含む。

- CRL 番号 連続する番号
- 認証局鍵識別子 チェーン/十分性検証の要件のための発行 CA の発行者鍵識別子 (Authority Key Identifier)

以下の拡張子を含む。

- ReasonCode 証明書の失効理由についての識別子

当拡張子は、相互認証証明書を含む、ルート CA の証明書又はサブ CA の証明書の CRL エントリに含まれている。当拡張子に含まれる値は、keyCompromise (1), affiliationChanged (3), superseded (4), cessationOfOperation (5), privilegeWithdrawn (9)である。

当拡張子は、利用者のエンドエンティティ証明書の CRL エントリに含めることができる。当拡張子に含まれる値は、keyCompromise (1), affiliationChanged (3), superseded (4), cessationOfOperation (5), certificateHold (6), privilegeWithdrawn (9) である。

7.3 OCSP プロファイル

GlobalSign は、RFC6960 又は 5019 に従いオンライン証明書ステータスプロトコル(OCSP)レスポンダを提供し、OCSP レスポンダ URL を通じて AIA 拡張子内でこれをハイライトする。

7.3.1. バージョン番号

GlobalSign は以下のフィールドを含むバージョン 1 の OCSP レスポンスを発行する。

- レスポンダ ID レスポンダの公開鍵の SHA-1 ハッシュ
- 生成時間 OCSP レスポンスが署名された時間
- 証明書ステータス 問い合わせを受けた証明書のステータス(有効/失効済み/不明)

- ThisUpdate/NextUpdate　レスポンスの推奨有効期間
- 署名アルゴリズム　SHA256 RSA 等(商材により異なる)
- 署名　レスポンダにより生成された署名
- 証明書　OCSP レスポンダの証明書

OCSP リクエストは下記のデータを含む必要がある:
- プロトコルのバージョン
- サービスリクエスト
- ターゲット証明書の識別子

以下のフィールドを含む:
- revocationReason　証明書の失効理由についての識別子

当フィールドは、相互認証証明書を含む、ルート CA の証明書又はサブ CA の証明書の OCSP レスポンダに含まれ、証明書が失効した際に利用者のエンドエンティティ証明書に含めることができる。CRLReason は CRL に利用が許可されている値を含むことを示し、詳細は 7.2.2 項に記載されている。

7.3.2. OCSP 拡張

(規定なし)

8. 準拠性監査及びその他の評価

本 CPS に記載される手続きは、1.0 項に記載された要求事項に準拠するように設計されており、GlobalSign 運用が関与する複数の垂直的 PKI 業界に対する PKI 標準のうち、現状で適用可能な部分について網羅している。

8.1. 評価の頻度及び状況

GlobalSign は、資格を有する監査人を介して、1.0 項で規定される WebTrust/eIDAS/UK eIDAS への準拠を、WebTrust の場合は 1 年に 1 度、eIDAS/UK eIDAS の場合は 2 年に 1 度継続的に評価するものとする。

dNSNameConstraints の制約を受けない Trusted Root CA は、適用される WebTrust に準拠しているかどうか監査される。

JTS 審査においては、JCAN 認証局 は、年に 1 回以上、本サービスが、本 CPS の要件、標準、手続、及びサービスレベルに適合していることを保証するために、準拠性監査を受諾する。JCAN LRA への認定を申請している組織は、GlobalSign より組織として登録される前に、JTS 審査に合格しなければならない。JCAN LRA は内部監査を実施し、少なくとも年に 1 度再審査を受け、要件及び当 CP への準拠性を証明しなければならない。

8.2. 評価者の身元及び能力

GlobalSign の監査は、下記の要件と能力を有する公認監査人によって行われる。
- 監査対象からの独立性
- 8.0 項に記載される的確な監査に明記される条件において、監査を遂行できる能力
- 公開鍵基盤技術、情報セキュリティツール及び技術、IT 及びセキュリティ監査、更に第三者を認証する機能について審査するにあたり、熟練した人員を雇用している
- 資格、認定、認可を有するもの、又は監査スキームに基づいた監査人の能力条件を満たすと評価される者
- 法律、公的規定又は職種倫理規定により認定されている者
- 政府内監査機関の場合を除き、業務上の責任/過失・不備に対する、少なくとも 100 万米ドル($1,000,000)を填補限度額とする保険を保持する。

eDAS は、ETSI EN 319 403 に定められた EN ISO/IEC 17065、特に、eIDAS 規則(EU)No 910/2014 に定義された要件に基づいて、欧州連合加盟国の認定機関により認定された適合性評価機関により監査が実施される。

UK eIDAS では、ETSI EN 319 403 でプロファイリングされた EN ISO/IEC 17065 に基づいて認定された適合性評価機関が、特に UK eIDAS（eIDAS (英国の法律) と 電子取引の電子識別及びトラストサービスに関する規則 2016）で定義された要件に照らして監査を行う。

JTS 審査において、JIPDEC から LRA に対する審査は、関連する経験を有する担当者より実施される。

8.3. 評価者と被評価者の関係

GlobalSign は、GlobalSign とは完全に無関係の独立性を有する監査人若しくは評価者を選択する。

監査人は、被監査部門の業務から独立した立場にあるものとする。 LRA の内部監査人は、被監査部門の業務から独立した立場にあるものとする。

8.4. 評価対象項目

監査は、1.0 項に記載される、評価のための監査スキームの要件を満たさなければならない。これらの要件は、監査スキームの変更に伴って更新される可能性がある。更新された監査スキームは、それが採用された次年度から GlobalSign に対して適用可能となる。

8.5. 結果が不備である場合の対応

GlobalSign 及び技術的制約を受けないクロスサインされた外部 CA は共に、監査法人によって準拠性についての問題を提示された場合には、不備を排除するための適切な是正計画を作成しなければならない。CP 及び CPS によって定められたポリシーや手続きに対して直接影響を与える是正計画については、Policy Authority に上程するものとする。

8.6. 結果についての連絡

監査結果は、ポリシー委員会に報告され、その後の是正計画を通じて、不備の分析及び解決が行われる。当該結果は、法律、規則又は契約により、結果の写しを入手する権利を有するその他の適当な事業体にも提供することができる。GlobalSign の WebTrust 監査報告書は以下を参照：
https://www.globalsign.com/en/repository/

8.7. 自己監査

GlobalSign は、発行された証明書のうち、少なくとも 3%(EV SSL 証明書及び EV コードサイニング証明書については 6%)の無作為に選択された証明書に対して、少なくとも四半期毎に自己監査を実施することにより、CP、CPS、及び「確認事項」の項に明記されたその他外部要件の準拠性を監視し、サービス品質を厳格に管理する。

9. その他ビジネス及び法的事項

9.1. 料金

9.1.1. 証明書発行及び更新料金

GlobalSign は証明書の発行及び更新に対して料金を請求できるものとする。また GlobalSign は、再発行に対しては料金を請求しない。料金及びそれに関連する約款は、申し込みの過程の WEB インターフェース及び GlobalSign の複数の言語の WEB サイト上にある営業・マーケティング資料を通じて、申請者に対して明確に提示されるものとする。

JCAN 証明書において、更新及び再発行は証明書のライフサイクルに該当しない。

9.1.2. 証明書アクセス料金

GlobalSign は発行済み証明書を格納するデータベースへのアクセスに対して、料金請求できるものとする。

9.1.3. 失効情報アクセスに関する料金

非常に多数の依拠当事者を有する利用者で、かつ、GlobalSign の証明書ステータス管理設備の負荷軽減のための技術である“OCSP ステープリング”や、それに類する対策を採用しようとしない利用者に対しては、発行 CA は負荷処理のための追加料金を請求できるものとする。

9.1.4. その他サービスの料金

GlobalSign はタイムスタンピングなどのその他追加サービスに対しては、これを請求できるものとする。

9.1.5. 返金ポリシー

GlobalSign と直接の関係を有し、GlobalSign に直接注文した証明書を使用する顧客で、利用者が発行された証明書に完全に満足していない場合、利用者は証明書が発行されてから 7 日以内に返金を要求することができる。返金は、GlobalSign が負担する手数料を差し引いた額となる。

9.2. 財務上の責任

9.2.1. 保険の適用範囲

GlobalSign NV/SA は、少なくとも 200 万米ドル($2,000,000)上限ポリシーの一般賠償責任保険を、また業務過誤や専門職業人賠償責任保険については、少なくとも 500 万米ドル($5,000,000)上限ポリシーの保険を保有するものとする。発行 CA の保有する保険のカバー範囲は、(1)EV 証明書の発行及び維持における行動、過失、不備、意図的ではない契約違反や不履行に対する損害請求、(2)如何なる第三者の所有権の侵害（コピーライト、特許、及び商標の侵害を除く）、プライバシーの侵害、及び広告侵害により生じた損害に対する請求、である。
保険会社は、現行版の最良の保険ガイド（又は格付け対象企業を会員とする企業団体）において評価が A- よりも上の評価を受けた会社であり、ここを通じて保険が提供されるものとする。

9.2.2. その他資産

(規定なし)

9.2.3. エンドエンティティに対する保険若しくは保証

GlobalSign は利用者に対して GlobalSign の Web サイト https://www.globalsign.com/en/company/corporate-policies 上のワランティーポリシーを提示するものとする。

9.3. 業務情報の機密性

9.3.1. 機密情報の範囲

以下の項目は機密情報として定義され、審査要員やシステム管理者を含む GlobalSign スタッフによる相当な配慮と注意の対象となる。

- 9.4 項に記載される個人情報
- CA 及び RA システムの監査ログ
- 6.4 項で記載される、CA の秘密鍵を活性化するための活性化データ
- 災害復旧計画と事業継続計画を含む GlobalSign の内部的なビジネスプロセス文書
- 8.0 項で記載される独立した監査人からの監査報告書

9.3.2. 機密情報の範囲外に属する情報

本 CPS において機密情報であると定義されない情報は、公開情報とみなされる。証明書のステータス情報及び証明書そのものは公開情報とみなされる。

9.3.3. 機密情報保護の責任

GlobalSign は、従業員、代理人、及び契約社員に対する研修と契約等の実施によって、機密情報を保護するものとする。

9.4. 個人情報保護

9.4.1. 保護計画

GlobalSign は、GlobalSign の Web サイト https://www.globalsign.com/repository 上で公開されるプライバシーポリシーに従い、個人情報を保護するものとする。

9.4.2. 個人情報として取り扱われる情報

GlobalSign は申請者から受領する、通常証明書に記載されない全ての情報を個人情報として取り扱う。この条件は、申し込みが受領され、デジタル証明書が発行された申請者及び、申し込みが却下された申請者にも適用される。GlobalSign は、全ての RA 及び審査スタッフと、個人情報に対してアクセスが必要な全ての従業員に対して、履行するべき注意義務に関して定期的にトレーニングを行う。

9.4.3. 個人情報とみなされない情報

証明書のステータス情報及び全ての証明書の内容は個人情報ではないとみなされる。

9.4.4. 個人情報保護の責任

GlobalSign は個人情報保護規定に従って、紙媒体又はデジタル形式に拘わらず、受領した個人情報を安全に保存する責任を有する。如何なる個人情報のバックアップも、適切なバックアップメディアに対し、その情報が移行される際は、暗号化されなければならない。プライバシーポリシーは、GlobalSign の Web サイト https://www.globalsign.com/repository 上で公開される

9.4.5. 個人情報使用についての通知及び同意

申し込み及び登録処理中に、申請者から受領した個人情報は、非公開情報であるとみなされ、このような情報の使用に関しては、申請者から許可を得る必要がある。GlobalSign は、GlobalSign が提供する製品又はサービスの十分性検証プロセスに利用する追加情報を第三者から入手するために必要な許可を含め、利用約款に必要な同意を盛り込むこととする。

9.4.6. 法的又は管理処理に従う開示

GlobalSign は、法令により開示要求があった場合には、申請者又は利用者に対して通知することなく個人情報を開示することが可能である。

9.4.7. その他情報開示の場合

(規定なし)

9.5. 知的財産権

GlobalSign は第三者の知的財産権を、故意に損なわないものとする。公開鍵及び秘密鍵はこれを正当に保持する利用者の財産である。GlobalSign は証明書の所有権を保持するものではあるが、その証明書が完全な形で複製・配布されるという条件と引き換えに、この証明書の複製・配布を利用者に非独占的かつ無償で許諾するものである。GlobalSign® 及び GlobalSign のロゴは、GMO グローバルサイン株式会社(GMO GlobalSign K.K.)の登録商標である。

9.6. 表明保証

9.6.1. 認証局の表明保証

GlobalSign は、CPS 及び該当する利用契約をもって、利用者及び依拠当事者に対し、発行済み証明書の使用に関する法的条件を告知する。GlobalSign、RA、利用者を含む全ての関係者は、自己の秘密鍵の完全性について保証する。何れの関係者も、万一秘密鍵の危殆化が発生したと疑われる場合は、直ちに該当する RA へ通知するものとする。

GlobalSign は証明書受益者に対して、証明書が有効である間、GlobalSign が証明書の発行と管理において、以下の内容を含む、CP と CPS に準拠していることを表明及び保証する:

- **ドメイン名或いは IP アドレスの使用権：** 証明書発行時点において、GlobalSign が
  (i) 証明書のサブジェクトフィールド或いはサブジェクト別名フィールドに格納されるドメイン名及び IP アドレスの使用権或いは管理権限を申請者が有している(或いはドメイン名のみの場合、使用権或いは管理権限を有する者からそれらの権利や管理を委譲されている)ことを検証する手続きを実施していること
  (ii) 証明書を発行する際、定められた手続きに従っていること
  (iii) それらの手続きが GlobalSign CP や本 CPS に明確に記述されていること(3.2 項を参照のこと)
- **証明書の承認：** 証明書発行の時点において、GlobalSign が
  (i) サブジェクトが証明書の発行を承認しており、申請代行者がサブジェクトに代わって証明書の発行を要求することを承認されていることを検証する手続きを実施していること
  (ii) 証明書を発行する際、定められた手続きに従っていること
  (iii) それらの手続きが GlobalSign CP や本 CPS に明確に記述されていること(3.2.5 項を参照のこと)
- **情報の正確性：** 証明書発行の時点において、GlobalSign が
  (i) 証明書に格納される全ての情報(但し organizationalUnitName 属性と subject:serialNumber (EV 証明書以外の場合)を除く)の事実性及び正確性を検証する手続きを実施していること
  (ii) 証明書を発行する際、定められた手続きに従っていること
  (iii) それらの手続きが GlobalSign CP や本 CPS に明確に記述されていること(3.2.3 及び 3.2.4 項を参照のこと)
- **誤解を招く情報がない：** 証明書発行の時点において、GlobalSign が
  (i) 証明書のサブジェクトの organizationalUnitName に誤解を招くような情報が含まれる可能性を低減するための手続きを実施していること
  (ii) 証明書を発行する際、定められた手続きに従っていること
  (iii) それらの手続きが GlobalSign CP や本 CPS に明確に記述されていること(3.2.3 及び 3.2.4 項を参照のこと)
- **申請者の身元：** 証明書がサブジェクトの身元情報を含む場合、GlobalSign が
  (i) 申請者の身元情報を検証するための手続きを実施していること。また、コードサイニング証明書に対しては、この手続きが少なくとも Baseline Requirements for Code Signing の 11 章の要求事項を充足すること。
  (ii) 証明書を発行する際、定められた手続きに従っていること
  (iii) それらの手続きが GlobalSign CP や本 CPS に明確に記述されていること(3.2.3 及び 3.2.4 項を参照のこと)
- **利用契約：** GlobalSign と利用者が関連会社でない場合、利用者と CA とは、(該当する場合)Baseline Requirements を満たす適法かつ強制力のある利用契約にて位置づけられていること。或いは、両者が関連会社の関係ならば、申請代行者は当使用条件(4.5.1 項を参照)を認め、受諾すること
- **ステータス：** GlobalSign は全ての有期間中の証明書のステータス(有効か失効されたか)に関する現在の情報を 24 時間 365 日公的にアクセス可能な状態に維持すること。コードサイニング証明書については、Baseline Requirements for Code Signing の規定に従い、GlobalSign がリポジトリを維持管理すること。
- **失効：** GlobalSign は(該当する場合)、Baseline Requirements、EV ガイドライン、及び/又は Baseline Requirements for Code Signing にて定義された何れの失効要件に該当する証明書についても失効すること (4.9.1 項を参照のこと) 。

コードサイニング証明書について：

- **コンプライアンス：** コードサイニング証明書については、GlobalSign が各コードサイニング証明書の発行及びその PKI の運用において、Baseline Requirements for Code Signing 及び該当する証明書ポリシー、認証業務運用規程を遵守していること。
- **鍵の保護：** コードサイニング証明書については、GlobalSign は発行時に、コードサイニング証明書に関連する秘密鍵を安全に保管し、誤用を防止する方法に関する文書を利用者に提供したことを、表明するものとする。

さらに、GlobalSign は、NAESB 証明書の証明書受益者に対し、証明書が有効な間、GlobalSign が証明書の発行及び管理において CP 及び CPS に準拠していることを表明し、保証する。

- NAESB WEQ-PKI Standards に基づき、証明書を発行、また管理すること
- 利用者を識別及び証明書を発行する際、NAESB WEQ-PKI Standards の全要件に従っていること
- RA が証明書において検証した事項において、RA が知り得ているところの、或いは当然知り得るはずの虚偽表示がないこと
- 申請者から提供された情報が、正しく証明書に記載されていること
- 証明書が NAESB WEQ-PKI Standards の不可欠な要件を満たしていること

上記の保証に代えて、GlobalSign は、本証明書が有効である間、証明書の発行及び管理、並びに EV SSL 証明書及び EV コードサイニング証明書に含まれる情報の正確性の検証において、GlobalSign が本ガイドライン及び CPS に従っていることを、EV SSL 証明書及び EV コードサイニング証明書の受益者に対して表明し、保証する。

- **法的存在:** GlobalSign は、証明書が発行された日現在、当該証明書に記名されているサブジェクトが設立又は登記管轄区域内で有効な団体又は事業体として法的に存在することを、そのサブジェクトの設立又は登記管轄区域内の設立又は登記機関と確認する。
- **識別**: GlobalSign は、証明書が発行された日現在、証明書に記名されているサブジェクトの正式名称が、サブジェクトの設立又は登記管轄区域における設立又は登記機関の公式記録に記されている名称と一致していること、及び仮名が含まれている場合、その仮名がその事業所の管轄区域において、サブジェクトにより適切に登録されていることを確認する。
- **ドメイン名を使用する権利:** EV 証明書についてのみ、GlobalSign は、証明書が発行された日現在、証明書に記名されているサブジェクトが、証明書に記載された全てのドメイン名を使用する権利を有することを確認するために、合理的に必要な全ての措置を講じる。
- **EV 証明書の発行許可確認:** GlobalSign は、証明書に記名されているサブジェクトが証明書の発行を許可したことを確認するために、合理的に必要な全ての措置を講じる。
- **情報の正確性:** GlobalSign は、証明書が発行された日現在、証明書内の全ての情報が正確であることを検証するために合理的に必要な全ての措置を講じる。
- **利用契約:** 証明書に記名されているサブジェクトは、法的に有効かつ強制力のある利用契約を、該当ガイドラインの要件を満たす CA と締結する、又は、関連会社の場合、申請者の代表者は、利用条件を確認、同意する。
- **ステータス:** GlobalSign は、EV ガイドライン及び/又は Baseline Requirements for Code Signing(該当する場合)の要件に従い、年中オンラインアクセス可能なレポジトリにおいては、証明書の有効又は失効のステータスに関する最新の情報を維持する。
- **失効:** GlobalSign は、EV ガイドライン及び Baseline Requirements for Code Signing の要件に従い、EV ガイドライン及び Baseline Requirements for Code Signing に明記された失効理由の何れかに基づき、証明書を失効する。

9.6.2. 登録局(RA)の表明保証

RA は以下を保証する。

- 発行手続きが本 CPS 及び関連する CP に準拠していること
- GlobalSign に対して提供する情報が、誤解を招く、或いは虚偽のものを含まない
- RA によって提供される全ての翻訳された資料が正確であること

JCAN LRA は、JCAN 証明書ポリシーの下、JCAN 証明書に記載する DN の真正性の審査と利用者の 本人認証を行い、証明書のライフサイクルマネジメントを行う。 JCAN LRA の義務は、以下の通りで ある。

1.全般
· JTS 登録(LRA)の基準 へ準拠する。
· 利用者に利用者の義務を通知する。
· 利用者の同意の記録を保管する。
· リポジトリに公開される情報を取得し、利用者に必要な情報を周知する。特に、GlobalSign から通知を受けた場合等は速やかに行う。
· LRA 業務に従事する者は、不正な発行及び開示を行わない旨を宣言している。

2.証明書発行
· サブジェクトの OrganizationUnitName2、CommonName の唯一性を保証する。
· LRA が PIN を生成した場合、LRA は PKCS#12 形式証明書及び対応する PIN をセキュアに利用者に配付する。
· LRA が PKCS#12 形式証明書及び PIN をバックアップする場合、セキュアに管理する。
· JCAN 証明書の発行後、LRA は、発行の記録（本人確認資料、同意書等）を保管する。

3.証明書失効
· 退職、脱退、廃棄等によりサブジェクト/使用者が当該組織と無関係になった場合、JCAN 証明書を速やかに失効する。
· 利用者が本 CPS 及び/又は LRA の規則の義務に違反した場合、JCAN 証明書を速やかに失効する。
· JCAN 証明書に誤り又は虚偽が記載されている場合、JCAN 証明書を速やかに失効する。
· 被災、アクセス認証用証明書の危殆化等で秘密鍵が危殆化した場合、JCAN 証明書を速やかに失効する。
· LRA がその他の理由で失効を決定した場合、JCAN 証明書を速やかに失効する。

9.6.3. 利用者の表明保証

利用者及び申請者は下記の項目を保証する。

- **情報の正確性:** 利用者は、証明書の発行に関連して、証明書申請及び GlobalSign の要求に基づき、常に正確かつ完全な情報を GlobalSign に提供する。
- **秘密鍵の保護:** 申請者は、要求された証明書及び関連するアクティベーションデータ又はデバイス(例えば、パスワードやトークン)に含まれる秘密鍵の管理、機密性の保持、適切な保護のために、あらゆる合理的な措置を講じるものとする。
- **証明書の受諾:** 利用者は、証明書の内容の正確性を見直し、検証するものとする。
- **証明書の使用:** 利用者は、証明書に記載されている「subjectAltName」でアクセス可能なサーバにのみ SSL 証明書をインストールするものとし、適用される全ての法律、また、利用契約や利用条件に従い、証明書を使用する。
- **報告及び失効:** 利用者は、(a) 証明書に含まれる公開鍵に対応する利用者の秘密鍵の実際、又は疑わしい誤用及び危殆化がある場合、その証明書の失効を速やかに要求し、その証明書と、対応する秘密鍵の使用を中止する;及び(b) 証明書内の情報が不正確になった場合、証明書の失効を速やかに要求し、その使用を中止する。
- **証明書の使用終了:** 利用者は、当該証明書の失効と同時に、証明書の公開鍵に対応する秘密鍵の使用を速やかに中止するものとする;及び、
- **対応:** 利用者は、危殆化又は証明書の誤用に関する GlobalSign からの指示に対しては、48 時間以内に対応するものとする。

- **確認及び了解:** 申請者が利用契約又は利用条件の諸条件に違反した場合、又はフィッシング攻撃、詐欺、マルウェアの配布などの犯罪行為に証明書が使用されていることを GlobalSign が発見した場合、申請者は GlobalSign が直ちに証明書を失効する権利を有することを認識し、了解する。

9.6.3.1. 北米エネルギー規定委員会(NAESB)利用者

WEQ-012 の申請に証明書を使用する Business Practice Standard WEQ-012 v 3.0 に加入するエンドエンティティは NAESB EIR に登録し、電気再販業務に従事することが許可されていることを提示しなければならない。また、NAESB WEQ PKI Standards に定められた認証方法を利用したアプリケーションにアクセスする必要があるが、卸電気業者の資格を持たないエンティティや組織(規制当局、大学、コンサルティング会社等)も NAESB EIR に登録する必要がある。
登録されたエンドエンティティ及びそのユーザコミュニティは、これらの NAESB WEQ PKI Standards に定められたエンドエンティティの義務を全て果たす必要がある。
各利用者組織は NAESB WEQ PKI Standards に定められている以下の義務について理解していることを、GlobalSign を通じて示さなければならない。
各利用者組織は以下の NAESB WEQ PKI Standards の項目を確認し、同意していることを認証局に対して証明しなければならない。

(i) エンドエンティティが、電気業界が以下の目的で安全なプライベート電気通信を必要としていることに同意していること。
  - 機密性:意図した受信者以外にデータが読み取られることがないという保証
  - 認証:エンティティが主張する存在(組織、個人)が正確であるという保証
  - 完全性:通信前後、若しくは過去から現在までの間に(意図的に、又は意図せずに)データが改ざんされていないという保証
  - 否認防止:取引先が、取引を行ったこと、或は電子メールの送信を行ったことについて、あとからそれを否認することをできなくすること。

エンドエンティティが、電気再販業界が公開鍵暗号方式(公開鍵証明書を利用し、個人やコンピュータシステムをエンティティに紐づけること)を利用することについて同意していること。

(ii) エンドエンティティが利用する認証局の CPS を、認証局の認める業界標準を踏まえた上でエンドエンティティが評価していること。

該当する場合、エンドエンティティは法的な事業識別情報を登録し、NAESB の EIR に登録され、利用者申請時や発行時に使用するための「エンティティコード」を確保しなければならない。

また、エンドエンティティは以下の要件にも準拠しなければならない。

- 自分の秘密鍵を他者からのアクセスから保護すること
- 該当する場合、NAESB EIR を通し、GlobalSign を認定認証局として選んだエンティティを識別すること

- GlobalSign がエンドエンティティに安全な電子通信を提供するのに使用される証明書を発行するために必要な本 CPS に規定されている通り、全ての同意書及び契約書に準拠すること
- 証明書申請手続き、申請者身元証明/正確性検証、及び証明書管理手続き等、本 CPS に規定されている全ての義務に準拠すること。
- PKI 証明書管理プログラムがあり、プログラムに参加する全ての従業員がトレーニングを受けること、また、当該プログラムへ準拠していることを確認すること。PKI 証明書管理プログラムは以下を含むが、それに限定されない。
    - 証明書秘密鍵セキュリティ及び運用ポリシー
    - 証明書失効ポリシー
- 利用者の種類を識別し(個人、役職、デバイス、若しくはアプリケーション等)、完全かつ正確な情報を証明書申請の際に提供すること

9.6.3.2 JCAN 証明書の利用者

利用者の義務は以下の通りである。

- LRA（利用者の代表）が PIN を生成した場合、PKCS#12 形式証明書及び PIN をバック アップすることに同意する。

9.6.4. 依拠当事者の表明保証

依拠当事者は、証明書に依拠する前に、依拠当事者規約を受諾し、依拠当事者規約及び本 CPS に基づいて行動しなければならない。

発行 CA の証明書を参照（依拠）する依拠当事者は下記の項目を保証する。

- 証明書を使用する技術的能力を有している
- 発行 CA 及び依拠当事者に関連する諸条件についての通知を受領する
- 正しい証明書パスの十分性検証手続きに従って発行局から発行された、証明書ステータス情報（例：CRL 又は OCSP）を使用して発行 CA の証明書を検証する
- 正確かつ最新版の十分性検証手続きにより、証明書の全情報が検証される場合にのみ、発行 CA の証明書を信頼する
- 妥当であると判断される状況においてのみ、発行 CA の証明書に依拠する
- 依拠当事者が、秘密鍵が危殆化した可能性を察知した場合、適切な RA に直ちに通知する
  依拠当事者が当該証明書に依拠することに妥当性があると判断した場合、その義務事項として下記が発生する。
- 依拠当事者に提示される現状の失効ステータス情報を使用して、認証局の証明書の有効又は失効を検証する
- 証明書若しくは本 CPS にて依拠当事者に示された、証明書の使用に関する全ての制限事項について注意を払う
- アプリケーションコンテキストによって提示されるその他のポリシー或いは規約と同様、発行 CA の証明書中の規定に関しても十分な注意を払う

依拠当事者は、証明書が使用されているアプリケーションの状況等を勘案して、その状況において証明書に依拠することが妥当であるかどうかを常に確認しなければならない。

9.6.4.1. 北米エネルギー規定委員会（NAESB）の依拠当事者

依拠当事者の責任については、以下の定め以外にも、これらの NAESB WEQ PKI Standards を用いた各 NAESB 要件の中に定めなければならない。

- 証明書が認定認証局である GlobalSign により発行されていること
- 認定認証局である NAESB 用 GlobalSign 発行 CA の証明書の十分性検証及び信頼チェーンの全てが損なわれておらず、有効であるということ
- 証明書が有効かつ失効されていないこと
- 証明書が NAESB 保証レベルの Object 識別子の一つに基づいて発行されていること

9.6.4.2. 適格証明書の依拠当事者

決済サービス指令（EU）2015/2366、又はオープンバンキングに基づく適格証明書の場合、依拠当事者は、依拠当事者及び証明書主体に適用される法律を考慮しなければならない。依拠当事者は、証明書に含まれる少なくとも以下の情報を考慮しなければならない。

- 管轄当局
- 決済サービスプロバイダ又は金融機関

LRA OID 1.3.6.1.4.1.4146.1.45.1 を含む適格証明書については、自然人が当該組織に所属するか否かを考慮しなければならない。

9.6.5. その他関係者の表明保証

(規定なし)

9.7. 保証の免責事項

法律又は本契約にそれを禁止する規定がある場合を除き、GlobalSign は、商品性及び特定目的への適合性の保証を含む全ての保証を放棄する。

9.8. 責任制限

GlobalSign は、Baseline Requirements 及び本 CPS に従い、証明書を発行、及び管理する。その場合、これらに正確に準拠している限りにおいては、当該証明書の使用又は依拠の結果として発生した損失に関し、利用者、依拠当事者又は第三者に対する如何なる責任も負わないものとする。特例的に発生した場合でも、GlobalSign の利用者、依拠当事者又は第三者に対する責任は、一証明書当たり 1,000 ドル($1,000)を超えないものとする。 但し、EV 証明書又は EV コードサイニング証明書については 1 証明書当たり 2,000 ドル($2,000)を限度額とする。

但し、本限度額は、GlobalSign 保証ポリシーの規定範囲を超えた場合についての損害賠償に限定される。あくまで保証ポリシーに基づき支払われる金額は、同ポリシーの限度額に従うものとする。

如何なる場合においても、GlobalSign は、間接的、偶発的、特別な、又は派生的な損害、或いは利益の損失、データの損失に関して責任を負わないものとする。また、本 CPS により提供又は企図されている証明書、デジタル署名、又はその他の取引又はサービスの使用、頒布、依拠、ライセンス、行使又は不行使に起因する、又は関連するところの間接的、偶発的、又は派生的な損害についても責任を負わないものとする。

9.9. 補償

9.9.1. GlobalSign による補償

GlobalSign は、アプリケーションソフトサプライヤー(ブラウザベンダー等)に対し、当 CA 発行の EV SSL 証明書、或いは EV コードサイニング証明書に関連して被ったところの如何なるクレーム、損害、或いは損失に対し、その訴因、法的根拠に拘わらず、これを防御し、補償し、免責しなければならない。
但し、これらサプライヤーが(1)有効かつ信頼性のあるEV証明書を、(誤って)無効或いは信頼性欠如と表示してあった場合、また逆に(2)(ⅰ)期限終了の証明書、(ⅱ)失効された証明書、などについて失効情報がオンラインで確認可能な状況でありながら(誤って) これを信頼性ありと表示したような場合は除く。

9.9.2. 利用者による補償

利用者は、法律の許す範囲で、GlobalSign、GlobalSign のパートナー、及びトラステッドルートの企業、またそれらの役員、幹部、従業員、代理人、そして請負業者らに対して、以下の事由に起因するあらゆる損失、損害、或いは出費、またこれらに関連する弁護士費用を補償するものとする。

(i) 利用者による虚偽、不作為、それらが意図的であれそうでないものであれ。
(ii) 利用者の利用契約への違反、また本 CPS 或いは適用法への違反。
(iii) 利用者の責に帰するべき、証明書或いは秘密鍵のセキュリティ侵害、或いは許諾された範囲外の使用。
(iv) 利用者の、証明書或いは秘密鍵の誤用。

9.9.3. 依拠当事者による補償

依拠当事者は、法律の許す範囲で、GlobalSign、GlobalSign のパートナー、及び相互認証の企業、またそれらの役員、幹部、従業員、代理人、そして請負業者らに対して、以下の事由に起因するあらゆる損失、損害、或いは出費、またこれらに関連する弁護士費用を補償するものとする。

(i) 依拠当時者による依拠当事者用契約書への違反、また本 CPS 或いは適用法への違反。
(ii) 依拠当時者による、証明書への不合理な依拠。
(iii) 依拠当時者による、使用前の証明書ステータスの確認ミス。

9.9.4 JCAN LRA による補償

JCAN LRA は、 JCAN 証明書及び JIPDEC トラステッド・サービス登録お申込書に定めた要件に関 連して JCAN 認証局 が被った損害を補償し、法律の許す範囲で、クレーム、異議及び訴訟等に 起因するあらゆる損失、損害或いは出費、またこれらに関する弁護士費用を JCAN 認証局及び その業務上の協力関係者 に補償するものとする。

9.10. 期間及び終了

9.10.1. 期間

本 CPS は、GlobalSign によりそのウェブサイト又はレポジトリにおいて、無効である旨の通知が為されるまでの期間有効である。

9.10.2. 終了

通知された変更は、指定されたバージョンに適切に反映される。当変更はその通知から 30 日後に適用されるものとする。

9.10.3. 終了の効果と存続

GlobalSign は、本 CPS の終了に関する条件及びその影響については、適切なレポジトリを介して通知するものとする。

9.11. 関係者への個別通知及び伝達

GlobalSign は、本 CPS に関してデジタル署名されたメッセージ又は紙媒体を用いた通知を受け入れる。GlobalSign からの有効かつデジタル署名された受領通知があった時点で、通知の送信者はその伝達が有効であったとみなされるものとする。送信者はこの受領通知を 20 営業日以内に必ず受領できるものとする。また書面による場合は、配達証明付きの配送サービスにより発送されるか、若しくは書留郵便、郵便料金前払い、配達証明付郵便を必須として、差出人宛てに書面通知するものとする。GlobalSign への個別の連絡は、legal@globalsign.com 宛、又は本 CPS の 1.5.2 項に指定される GlobalSign のあて先に送付されるものとする。

9.12. 改正条項

9.12.1. 改正手続き

本 CPS は少なくとも年に一度は見直されるが、より頻繁に見直されることもある。全ての変更は、挿入される前に GlobalSign CA Governance Policy Authority により確認、承認される。本 CPS に対する変更があった場合は、適宜そのバージョン番号にて明確化する。

9.12.2. 通知方法及び期間

GlobalSign は、本 CPS に関する主要な又は重要な変更が為された際には、改定版の CPS が承認されるまでの一定の期間、その変更の件をウェブサイトに掲載するものとする。

適格証明書については、PACOM1 - CA Governance Policy Authority により、本 CPS の変更が、サブジェクト、利用者、依拠当事者によるサービスの受諾に影響を及ぼす可能性のある重大な変更であるとみなされた場合、GlobalSign はリポジトリ上に 7 日間の期限付き通知を提供するものとする。

GlobalSign は、本 CPS に関する主要な又は重要な変更が為された際には、JIPDEC へ通知する。

9.12.3. OID(オブジェクト識別子)を変更しなければならない場合

(規定なし)

9.13. 紛争解決に関する規定

審決を含む何らかの紛争解決手段、或いはこれの代替システム (小規模裁判、調停、拘束力のある専門家の助言、共同監視及び通常の専門家による助言などによる方法を例外なく含む)に進む前に、申立当事者はその紛争解決策を模索するため、当該紛争について GlobalSign へ通知することに同意するものとする。

紛争の通知を受けた GlobalSign は、GlobalSign 経営陣にその紛争をどのように取り扱うべきかを助言するための紛争協議会を召集する。紛争協議会は、紛争の通知を受領してから 20 営業日以内に召集されるものとする。紛争協議会は、法律顧問、データ保護責任者、GlobalSign 運営経営陣の者及びセキュリティオフィサー(セキュリティ最高責任者)により構成される。法律顧問又はデータ保護責任者の何れかが会議の議長を務める。その解決策に関して、紛争協議会は GlobalSign 上層経営陣に対し解決方法を提案する。次いで GlobalSign 経営陣は、提案された当該解決方法について申立当事者に伝達・提案するものとする。

万一、 GlobalSign CP に従い最初の通知がなされた後、紛争が 20 営業日以内に解決しない場合、ベルギー国裁判所法典の 1676 から 1723 項に従い、関係当事者は紛争を仲裁へと進める。
仲裁人は、各当事者が夫々1 名の委員を提案、また双方が 1 名を第三者から選出することで、全 3 名の仲裁人から構成される。仲裁の場所は、ベルギー国 Leuven となり、必要となる費用は調停委員が決定するものとする。

9.14. 準拠法

本 CPS は、ベルギー国法に基づき、この支配を受け、また解釈される。この法律の選択は、居住地や、GlobalSign 証明書や他の製品及びサービスの使用地に関係なく、本 CPS の解釈の一律性を確実にするためのものである。また、GlobalSign が、プロバイダ、供給業者、受益者又はその他の役割を担う GlobalSign 製品及びサービスに関し、本 CPS が適用され、又は黙示的・明示的に引用されるところの GlobalSign の業務又は契約関係の全てに対して、ベルギー国法は、適用される。

GlobalSign のパートナー、利用者及び依拠当事者を含む各当事者は、ベルギー国、Leuven の地方裁判所の管轄権に変更不能の条件にて従うものとする。

9.15. 適用法の遵守

GlobalSign は、適用法としてベルギー国法を遵守する。特定の GlobalSign パブリック証明書の管理をする製品及びサービスに使用される特定のタイプのソフトウェアの輸出には、何らかの公的認可又は民間機関の認可を必要とすることがある。各当事者は(GlobalSign、利用者及び依拠当事者を含む)、ベルギーにおいて該当する輸出法及び輸出規制に従うことに同意する。

9.16. 雑則

9.16.1. 包括的合意

GlobalSign は、全ての証明書発行に携わる RA に対し、本 CPS 及び全ての適用可能な業界ガイドラインに従うことを、契約上の義務として要求する。如何なる第三者も、同様の合意を強制するような依頼若しくは訴訟を起こすことはできない。

9.16.2. 譲渡

本 CPS に基づき業務を行なう事業者は、自身が持つ権利又は義務を、GlobalSign からの事前の書面承認を得ずして譲渡することはできない。

9.16.3. 分離条項

本 CPS は、その責任の制限の項目を含む何れかの規定が無効であるか、或いは法的強制力が失効となった場合であっても、本 CPS の他の条項は尚有効であり、当事者間の本来の意図に沿った方法で解釈されるものとする。
有限責任を規定する本 CPS の各条項は、分離可能であり、如何なるその他の規定からも独立したものであることを意図しており、そしてまた、この原則に沿って施行されるものとする。

9.16.4. 執行 (弁護士費用及び権利放棄)

GlobalSign は、ある当事者の行為に起因する損害、損失、費用に対する補償及び弁護士費用をその当事者に求めることができる。GlobalSign が本 CPS の何れかの規定の執行を行わなかった場合でも、それはその後の同規程の執行、又はその他の規定の執行を放棄するということを意味するものではない。如何なる権利放棄も、書面に明記され、また GlobalSign の署名がある場合に有効となる。

9.16.5. 不可抗力

GlobalSign は、政府機関の行為、戦争、暴動、妨害破壊行為、通商禁止、火災、洪水、ストライキ又はその他の行為、輸送の中断又は遅延、通信又は第三者サービスの中断又は遅延などを含む GlobalSign の合理的な制御の及ばない状況に起因又は関連する如何なる損失、費用、経費、責任、損害又は請求に対しても、責任を負わないものとする。

9.17. その他の規定

GlobalSign の TrustedRoot 認証局チェーニングサービスに加入したいと望む第三者発行 CA は、本 CPS 及びその全条件を厳守しなければならない。これは、多くの法的、及び手続的管理によって実施され、また検証される。また年度毎の監査により検証されるものとする。
この管理には以下を含むが、これだけに限定されるものではない。

- TrustedRoot 利用者及び GlobalSign 間における認証局チェーニング契約書を締結すること
- TrustedRoot 利用者の提出及び発行、また GlobalSign 及び/又は GlobalSign の監査人による審査、及びこれを受入れること
- TrustedRoot 利用者による PKI インフラ確認書の提出、及び GlobalSign 及び/又は GlobalSign 監査人を受入れること

9.17.1. CA チェーニング契約書

CA チェーニング契約書は、下記の契約上強制力を有する規定及び条件を含む。

- 利用者法人及びその子会社（50%以上の株式支配権所有）からの TrustedRoot に限定して使用すること
- 非商業的利用に限定：発行された証明書は自身の利用、従業員及び既存のビジネス用途及び処理において利用者と提携する第三者の利用に限定すること
- エンドエンティティ証明書種類（S/MIME, SSL クライアント証明書）への制限を行うこと
- GlobalSign により審査及び受諾された CPS を提出すること
- 本 CPS に準拠すること
- 業界標準に遵守する、物理的、人員、ネットワーク、倫理的及び運用管理についての PKI 評価文書を提出すること
- CA 及びサブ CA の秘密鍵管理において、FIPS140-2 レベル 3 又は相当の暗号化モジュールを使用すること
- 相互認証署名を禁止すること
- 米国輸出規定に基づき、発行済み証明書への輸出管理を実施すること
- GlobalSign 及び/又はその監査人による年一度の監査を受諾すること
- CA 環境への変更により、PKI 評価及び CPS の報告内容と異なる場合は継続的に GlobalSign へ通知すること
- GlobalSign が GlobalSign レポジトリにおいて、（チェーニング系列 CA として）当利用者 CA のことを公開する場合があることを了解すること

GlobalSign 及び/又はその監査人により、Trusted Root 利用者が CA チェーニング契約に違反したと判断した場合、GlobalSign は下位 CA 証明書を取り消すことができる。

9.17.2. PKI 審査

TrustedRoot 利用契約の施行は、GlobalSign 及び/又はその監査人による、利用者側 PKI に対する審査の受入れ、及びその審査に基づくものである。この審査は、利用者の CA 階層及びセキュリティ対応策を記録するものである。この審査には下記の項目を含むが、それだけに限定するものではない。

- 論理的セキュリティ対応が導入されている－人事事項かつ職務分掌及び二重制御も網羅されていること
- 物理的セキュリティ対応策が導入されていること
- ネットワークセキュリティ対応策が導入されていること
- CA 階層が導入されていること
- HSM（ハードウェア セキュリティ モジュール）の種類及びシリアル番号

9.17.3. 利用者 CA の導入

GlobalSign は、利用者 CA のテスト署名を GlobalSign のテスト CA と連動して行なうことを必須事項としてこれを実施する。GlobalSign のテスト CA は GlobalSign のルート証明書を複製するが、これはテスト目的であると識別され

（テスト CA 対 CA）、また第三者アプリケーションに装填されるものではない。テスト署名が成功した場合のみ、利用者 CA は GlobalSign ルート CA から署名される。

9.17.4. 継続的要件及び監査

利用者は常に、その義務に忠実でなければならない。利用者は、前 9.17.2 項に記載された各項目の如何なる変更についても GlobalSign 及び/又はその監査人に報告する継続的な義務を有する。GlobalSign は、WebTrust（ウェブトラスト）の CA 監査の一部として、その資格を有する監査人に対し、上記の要求条件について年に一度の監査を行うよう指示し、加えてコンプライアンス向上のため、ウェブサイトのスキャンサービスを提供する独立した外部の団体から、公開され利用可能なドメインの一覧を取得する。

（以下空白）