GlobalSign Certificate Policy
(証明書ポリシー)

本書は、GlobalSign Certificate Policy 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: August 21, 2023

Version: v7.1

Legal-JP

デジタル署名者 : Legal-JP
日付 : 2024.01.09 11:32:21 +09'00'

目次

文書変更履歴

バージョン	公開日	変更概要
v 7.0	2023 年 3 月 28 日	• PSD2 証明書の名称を "オープンバンキング"に変更。 • CA/B フォーラム投票 CSC-13 と CSC-17 のための更新。 • OID の改訂。 • 本 CP に電子署名を付与して公開する要件を削除。 • "サブジェクトの一意性 "の明確化。 • 通知及び失効プロセスにおける役割として RA を包含。 • 監査ログ及びアーカイブに関する箇所の見直し。 • 秘密鍵保護及び暗号化モジュール技術管理に関する箇所の見直し。 • 短期証明書の失効制限の明確化。 • 文法的な更新、用語の統一。
v 7.1	2023 年 8 月 21 日	• Baseline Requirements for S/MIME に関する更新。 • Baseline Requirements for TLS (v2.0.0) に関する更新。 • 失効事由及び失効ステータスの変更に関する更新。 • 登録局 (RA) 及び Enterprise RA に対する見直し。 • 表明保証に関する見直し。 • 短期証明書の失効に関する制限についての明確化。 • 文言の修正・訂正。

前提確認事項

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。

1.0 はじめに

本証明書ポリシー(以下、「本 CP」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 CP 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 CP 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 CP 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本 CP の理解を補助するために、本 CP 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)

CP は、「共通のセキュリティ要件を持つ特定の集団及び/又はアプリケーションのクラスへの電子証明書の適用範囲を示す、一連の規則」である。本 CP 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 CP 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。付加的な情報を記載する必要がある場合には、標準的な構成に小項目を加えてそこに記述している。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。

本 CP 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
- WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates
- 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))

本 CP は、現時点における以下の CA/B Forum の要件に準拠する：

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (以下「Baseline Requirements for TLS」)
- 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」)
- CA/Browser Forum Baseline Requirements for S/MIME （以下「Baseline Requirements for S/MIME」）[1]

CA/B Forum の要件は http://www.cabforum.org で公開される。本文書及び上記要件の間に不一致があった場合、上記要件が本文書に優先して適用される。

本 CP は、以下に限らないが、証明書のライフサイクル管理のための業界内のベストプラクティスを充足するために要求される、技術的要件、セキュリティ手順、要員及び訓練の必要性といった、ポリシー及び手続きの分野に対応する。本 CP は、GlobalSign が発行するルート証明書、第三者の下位/発行 CA へのチェーニングサービスを含む、全ての証明書に適用される。ルート証明書は、ルート証明書自身を管理する同じエ

[1] 2023 年 9 月 1 日より有効

ンティティによって直接的に制御されるよう想定されているか、制御されないかもしれない 1 つ以上の下位 CA の作成を通して証明書階層を管理するために使われる。

本 CP は、本 CP 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。

本 CP 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 CP は、GlobalSign が、自身のシステムから直接発行する全証明書階層に適用される。
本 CP の目的は、ルート証明書及び発行 CA の管理に関し GlobalSign が採用する管理手続きを説明し、上述の業界標準の要件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。さらに、eIDAS 規則(規則(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、権限の認証又は否認防止の目的で使用される電子署名の認知を定めているが、この点に関し、GlobalSign はサービスの提供にあたり、本法の該当条項の射程の範囲内で運営を行っている。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 CP は、本 CP に基づき発行される証明書のライフサイクルに関わる全ての主体の目的、役割、責任及び手続きを定める。いわば、「遵守すべきこと」を記述することで、商品サービスに対する運営上の規則の枠組みを設定している。

GlobalSign の Certificate Practice Statement(以下「CPS」という)は本 CP を補完し、「認証局がどのように CP に準拠するか」記述する。CPS は、エンドユーザに、発行 CA (すなわち、利用者に証明書を提供する事業体)がそのような証明書を作成し管理する際に使用するプロセス、手順、及び全般的な状況の概要を提供する。

GlobalSign は、本 CP 及び CPS に加え、以下のような問題に対処するポリシーを別途文書化して保持する。

- 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

さらに、他の関連文書には、以下のものが含まれる：

- 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

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 CP に基づき管理される GlobalSign ルート CA 証明書は以下の通り：

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 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 36E80B78775DDA9D0BAC964AC29D5A5EC4F3684E0C74445E954A191C2939B8E0
- GlobalSign IoT Root E60 with fingerprint 43ED443C1F0CD46C9914B4272C24DC42CF6FE62B4AAB37585878A26D882AE4CB

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(又は利用)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 Non-Public Root R43 with fingerprint D6273949002299CC84DA84984EAF3F20F4B09CC2A7B241DFD4B361A8432460EB
- GlobalSign Trusted Platform Module Root CA with fingerprint F27BF02C6E00C73D915EEB6A6A2F5FBF0C31AE0393149E6B5C31E41B113841C3
- GlobalSign Trusted Platform Module ECC Root CA with fingerprint 5A8C7B5EB888CFCE9322068E80E82B28B554FFEB7FDC9638DCB3763077401D26

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当該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 nv/sa の所有から外れた。

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、データにデジタル署名をしたりすることができる。認証局は、電子証明書により利用者及びその秘密鍵の関連性を認証する。

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。本ポリシーに従い、GlobalSign が、証明書の発行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。
このインスタンスのエンティティには、エンドユーザ又は他の認証局が含まれる可能性がある。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。

GlobalSign は、本 CP に関するコメントを、1.5 項ポリシー管理に記載されている住所宛に受理する。

1.2 文書名と識別

本文書は GlobalSign 証明書ポリシーである。 .

GlobalSign NV/SA 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 CP が対象とする様々な証明書、文書に対し、次の OID を管理・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)
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

Category	OID	Description
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
	1.3.6.1.4.1.4146.1.40.37	**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 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 - Open Banking	Private key not 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
	1.3.6.1.4.1.4146.1.40.39	**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)	
	1.3.6.1.4.1.4146.1.40.39.3	Qualified Certificates for Website Authentication (QWAC)	
	1.3.6.1.4.1.4146.1.40.39.4	Qualified Certificates for Website Authentication (QWAC) – Open Banking	
	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
	1.3.6.1.4.1.4146.1.44.36	**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
	1.3.6.1.4.1.4146.1.44.37	**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 - Open Banking	Private key not 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
	1.3.6.1.4.1.4146.1.44.39	**UK eIDAS 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) – Open Banking	
	1.3.6.1.4.1.4146.1.44.41	**UK eIDAS Qualified Certificates – Remote Non QSCD**	
	1.3.6.1.4.1.4146.1.44.41.1	Qualified Certificates for Electronic Signatures	Private key not on QSCD Managed on behalf of Subscriber
	1.3.6.1.4.1.4146.1.44.41.2	Qualified Certificates for Electronic Seals	Private key not on QSCD Managed on behalf of Subscriber

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
	1.3.6.1.4.1.4146.2.1	CDS Timestamp Test Policy
	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	RFC3161 Timestamp Test Policy ECC
	1.3.6.1.4.1.4146.2.5	Qualified Timestamping Tokens for eIDAS
	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

	1.3.6.1.4.1.4146.1.40.30	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
	1.3.6.1.4.1.4146.1.95	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
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	Shared Customer Certificates Arc
	1.3.6.1.4.1.4146.11.1.1.1	IntranetSSL
	1.3.6.1.4.1.4146.11.1.1.2	IntranetS/MIME
	1.3.6.1.4.1.4146.11.1.1.3	Demo Certificates Policy – 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	GlobalSign Internal Certificates
	1.3.6.1.4.1.4146.11.1.3	Customer Branded Certificates

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) – Open Banking - 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
	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) - Open Banking - 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
	1.3.6.1.4.1.4146.40.40.1	Qualified Certificates for Website Authentication (QWAC) – Legacy
	1.3.6.1.4.1.4146.40.40.2	Qualified Certificates for Website Authentication (QWAC) – Open Banking - 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)

Category	OID	Description
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
	2.23.140.1.5.1.1	S/MIME Mailbox-validated Legacy Certificate Policy
	2.23.140.1.5.1.2	S/MIME Mailbox-validated Multipurpose Certificate Policy
	2.23.140.1.5.1.3	S/MIME Mailbox-validated Strict Certificate Policy
	2.23.140.1.5.2.1	S/MIME Organization-validated Legacy Certificate Policy
	2.23.140.1.5.2.2	S/MIME Organization-validated Multipurpose Certificate Policy
	2.23.140.1.5.2.3	S/MIME Organization-validated Strict Certificate Policy
	2.23.140.1.5.3.1	S/MIME Sponsor-validated Legacy Certificate Policy
	2.23.140.1.5.3.2	S/MIME Sponsor-validated Multipurpose Certificate Policy
	2.23.140.1.5.3.3	S/MIME Sponsor-validated Strict Certificate Policy
	2.23.140.1.5.4.1	S/MIME Individual-validated Legacy Certificate Policy
	2.23.140.1.5.4.2	S/MIME Individual-validated Multipurpose Certificate Policy
	2.23.140.1.5.4.3	S/MIME Individual-validated Strict Certificate 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

Community	OID	Description
	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 (「発行 CA」)

認証局の第一の責務は公開鍵基盤（以下、「PKI」という）に関する機能、すなわち証明書のライフサイクル管理、利用者登録、及び証明書の発行、更新、交付、失効などに関する業務を遂行することである。証明書のステータス情報は、証明書失効リスト（以下、「CRL」という。）の配布ポイント又はオンライン証明書ステータスプロトコル（以下、「OCSP」という）レスポンダの形式で、リポジトリを通じて、公開される。この認証局は、GlobalSign が直接又は間接的に管理する下位 CA の登録局（以下、「RA」という）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「発行 CA」の名で呼ばれることがある。

GlobalSign の 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 の証明書階層にチェーンされる全ての電子証明書の証明書ポリシーの維持管理に責任を負う。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 GlobalSign CA 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。

以下、参照しやすくするため、本 CP に基づき証明書を発行する全ての認証局（GlobalSign を含む）を全て「発行 CA」と称する。

発行 CA は、発行される証明書の管理サービスを安定的に提供する。依拠当事者が失効された証明書についての情報を確実に知ることができるよう、適切な情報開示が必要である。発行 CA は、証明書のステータス情報を、電子証明書のプロパティ内に記載の通り、CRL の配布ポイント又は OCSP レスポンダの形式で、リポジトリを通じて提供する。

1.3.2 登録局(RA)

発行 CA は RA 業務を行うことができる組織であり、発行 CA 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とる。

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。

発行 CA は、証明書に適用される規制、法律、業界標準、ポリシーによって許可された条件下で、身元証明及び証明書のライフサイクルイベントをサードパーティへ委任することができる。該当する場合、当委任は CA/B Forum の要件に従って実施しなければならない。

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 CP が定める全ての要求事項並びに CA/B Forum が推奨する付加的な基準を参照により組み込む契約条項を遵守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。

発行 CA 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十分性検証するために、エンタープライズ RA を指定することができる。エンタープライズ RA において、利用者の組織は認証及び事前定義され、システム構成によって制約されるものとする。

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。

1.3.3 利用者

発行 CA の利用者は、発行 CA が管理する証明書階層からエンドエンティティ証明書の発行を直接的に受ける、又は、独自の PKI 階層から証明書を発行することができる発行 CA から証明書の発行を受けようとするサードパーティである。利用者は、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。個人はあるタイプの証明書の発行を受けることができない。

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発行 CA 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。

エンドエンティティ利用者は、以下のような者をいう：

- 利用者の証明書に記載された公開鍵と対になる秘密鍵について最終権限を有する。利用者は証明書のサブジェクトである場合も、そうでない場合（たとえば、組織が使用するファイアウォール、ルーター、サーバ、その他のデバイスに対し機械名、役職名を掲載して発行される証明書など）もある。

1.3.4 依拠当事者

証明書の有効性を検証するために、依拠当事者は常に CRL 配布ポイント又は OCSP レスポンダの様式により GlobalSign の失効情報を参照する必要がある。

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の使用方法は証明書エクステンションの Key Usage 及び Extended Key Usage の値により制限される。

証明書を許可されていない方法で使用した場合には、GlobalSign は利用者及びその依拠当事者になんら保証を行わない可能性がある。

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 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。

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 CP 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のために使用されてはならない
    - 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
    - 連邦法において違法とみなされるデータの転送

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 CP に関する問い合わせは、以下に送付すること。

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

1.5.2 問合せ窓口

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

電子証明書の問題報告
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、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、又は証明書に関連する他の事項は、report-abuse@globalsign.com にメールで報告することとする。

GlobalSign は、この要求に応じて当該証明書を失効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 は第 4.9.5 項に記載されている調査を実施する。

1.5.3 CP がポリシーに適合しているかを判断する担当者

eIDAS における適格監査人から受領するアドバイスに基づき本 CP の適格性、適用可能性や CPS の本 CP への準拠性を判断するのは、PACOM1 – CA Governance である。

本 CP 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 は少なくとも年次で CP をレビューし、適宜又は状況に応じてポリシーを改訂し更新するべきである。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 CP の公表に伴って拘束力を持つ。

1.5.4 CP 承認手続き

CP の更新は PACOM1 – CA Governance により確認・承認される。CP の更新が PACOM1 – CA Governance に承認されると、CP の新バージョンが GlobalSign のリポジトリ（https://www.globalsign.com/repository）において公開される。

更新されたバージョンは、その告示が行われると共に、前のバージョンの CP 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文言は、CA/B Forum の要件及び 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、或い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、申請者は利用者と称される。デバイスに対して発行される証明書の場合、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：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：サブジェクトの情報が正確であることを表明する文書

認定認証局（Authorized Certification Authority、ACA）：NAESB Business Practice Standard for Public Key Infrastructure (PKI) – WEQ-012 の全規定を遵守する CA

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

CA/B Forum の要件： CA/Browser Forum が発行する、証明書の発行及び管理に関する一連の文書。

- CA/Browser Forum Baseeline Requirements for the Issuance and Management of Publicly-Trusted Certificates,
- CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates,
- CA/Browser Forum Network and Certificate System Security Requirements,
- CA/Browser Forum Baseeline Requirements for Code Signing, 及び
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates

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、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

電子証明書の問題報告：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

証明書失効リスト：証明書を発行した認証局が作成し電子署名した、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 により運営されている証明書リポジトリ。

危殆化：機微情報を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。

デジタル署名：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: The Baseline Requirements for TLS 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: The Baseline Requirements for TLS 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: The Baseline Requirements for TLS 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。

レジストラ：Internet Corporation for Assigned Names and Numbers（ICANN）又は各国のドメイン名管理当局・レジストリ、又はNetwork Information Center（その関連会社、契約業者、委託業者、承継人、譲受人を含む）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

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本人確認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

電子署名：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。

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)サービスを利用者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十分性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、言語特有のスクリプト又はアルファベット文字を含み、ASCII 文字列のみを許容する 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 CA：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

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

北米エネルギー規格委員会(NAESB)認証局認定要件：NAESB から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。

オープンバンキング証明書： オープンバンキング属性情報を含む適格証明書

オープンバンキング属性情報：オープンバンキング証明書に特有の属性情報で以下のものがある。

- 所轄官庁より発行されている場合は認証番号、或いは国家又はヨーロッパ水準にて認識されている登録番号又は金融機関の登録に含まれる法人番号
- 決済サービスプロバイダ(PSP)の役割
- 所轄官庁の名称(NCAName)及び独自の識別子 (NCAId).

決済サービス指令(Payment Services Directive, PSD2): 全 EU 及び EAC 域内の支払サービス及び支払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：申請者が事業を行う施設(工場、店舗、倉庫等)の場所

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。

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。

公開鍵暗号基盤(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た証明書：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

仮名 (Pseudonym): 特定の目的のために個人が想定する仮のアイデンティティ。匿名のアイデンティティとは異なり、仮名は個人の実際の身元と連携させることができる。

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 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電子シール。

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 条に準拠したタイムスタンプの提供。

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 条に準拠する 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は、単に当該サプライヤ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。

リポジトリ：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 レジストリの何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である場合、これらは利用者による管理、運営下にある。

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。

S/MIME 証明書：電子メールの署名、検証、暗号化、復号に使用することを目的とする証明書。id-kp-emailProtection（OID：1.3.6.1.5.5.7.3.4）の Extended Key Usage（EKU）を用い、かつ subjectAltName エクステンションに id-on-SmtpUTF8Mailbox タイプの rfc822Name 又は otherName を含む証明書。

S/MIME BR 証明書： Baseline Requirements for S/MIME のポリシーに準拠する S/MIME 証明書。

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。

技術的制限を受ける下位 CA の証明書：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。

利用規約：申請者又は利用者が認証局の関連会社である場合に、本文書のTLSの要求事項に従い発行された証明書を保管・使用する際に準拠すべき条項

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 (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

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：本文書のTLSの要求事項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ー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
GPS	Global Positioning System
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
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
WEQ	Wholesale Electric Quadrant

2.0　公開とリポジトリの責任

2.1　リポジトリ

発行 CA 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、証明書ポリシー、CPS、依拠当事者規約、利用契約を公開する。発行 CA 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。

発行 CA 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ことを、発行 CA 証明書の発行、使用、管理に携わる全ての当事者に対し、ここに通知する。

発行 CA 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、機密性及び/又は機微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。

発行 CA は、本 CP 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 の法的拘束力を有する公開リポジトリは 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、英文版の規定が優先適用される。

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 の全ての要求事項を含み、RFC 3647 に従って構成されるものとする。

2.3　公開の時期及び頻度

CA は、適用される CA/B Forum の要件の最新版について、実施方法を詳述した証明書ポリシー及び/又は認証業務運用規程（CP 及び/又は CPS）を、少なくとも 365 日毎に策定、実施、施行、及び 更新するものとする。CA は、その CP 及び/又は CPS を少なくとも 365 日毎に見直し、更新するものとし、文書に他の変更がない場合でも、バージョン番号を更新し、日付入りの変更履歴を追加するものとする。

2.4　リポジトリへのアクセス管理

発行 CA は、読み取りのみ可能な形でリポジトリを公開するものとする。

3.0　識別と認証

発行CAは申請者の身元情報とその他の属性情報が真正であるかを認証するための手続きを文書化して保管する。

発行CAは、承認された手続き及び基準を用いて、証明書階層にチェーンされることを希望する者（チェーンされることを希望する下位CA、RA、エンタープライズ登録局、エンドエンティティ利用者など）からの申請を受け付ける。

発行 CA は本 CP に従い、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

利用者の識別を行うにあたり、発行 CA は、サブジェクトに割り当てられる名称の種類を含む名称・識別規則（X.500「識別名」、RFC 822「名称」、及び X.400「名称」など）に準拠する。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んではならない。RFC 2460（IPv6）又は RFC 791（IPv4）に規定される IP アドレスが記載されることがある。

S/MIME BR 証明書において、個人に発行される証明書の subject:commonName がメールボックス・アドレスを含まない場合、第 7.1.4.2.2 項(a)に記載の通り、個人名又は仮名として指定される。複数の単語からなる名前は認められる。ハイフンで結合された名は、1 つの名とみなされる。複数の名を持つサブジェクトは、

1 つ又は複数の名を任意の順序で選択することができる。サブジェクトは、各国の慣行に従って、姓と名の順序を選択することができる。認証局は、現地の慣行に従って、個人名の一般的なバリエーションや略称を認めることがある。

3.1.2 意味のある名称である必要性

発行 CA は、可能な場合、識別名を使用して証明書のサブジェクトと発行者の名称を区別する。

S/MIME BR 証明書の場合、個人名は、本人確認書類又はエンタープライズ RA の記録で検証されるサブジェクトの名前を、意味を持って表現したものでなければならない。

3.1.3 利用者の匿名又は仮名の使用

発行 CA は、証明書に適用されるポリシーにおいて禁じられていない場合、及び名称管理体系における一意性が担保される場合、エンドエンティティ証明書に匿名又は仮名（「かめい」、 (Pseudonym)）の使用を許可することがある。

S/MIME BR 証明書の場合、subject:pseudonym 属性の使用は、Baseline Requirements for S/MIME の第 3.1.3 項に従うものとする。

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。

3.1.4 様々な形式の名称の解釈方法

S/MIME BR 証明書の場合、Baseline Requirements for S/MIME の第 3.1.4 項に従って、様々な名称形式を 解釈するものとする。

3.1.5 名前の一意性

（規定なし）

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、本 CP は申請者が商標を使用する権利を有するかどうかの検証を必須としない。しがしながら、発行 CA は、紛争に関連性のある証明書ついては如何なるものであれ、その申請を拒否すること、或いはこの失効を要求することができる。

3.2 初回の身元情報の十分性検証

発行 CA は、証明書を申請する、或いは認証局のチェーンサービスなどの利用を申し込む、法人又は個人の申請者の身元情報の検証のために必要な情報のやりとり、調査などにおいて、あらゆる法的手続きを用いる。

発行 CA は、初回の身元情報の十分性検証の結果、真正と認められたサブジェクト識別名その他の身元識別情報を、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。申請が却下された申請者の以前に検証された情報を認証するためには、第 3.3.1 項の正確性の再検証要件が遵守されていることを条件に、適切なチャレンジ・レスポンス方式のアカウント認証によって行われなければならない。

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

組織の識別情報を含む全ての証明書について、申請者は組織名、及び登記された（又は事業を営む）住所を提示しなければならない。組織の法的実在性、正式名称、(申請又は設立管轄における正式名称の一部に含まれている場合は)登記形態、及び組織が提示した住所は検証されねばならず、その検証に用いられた方法は CPS 内に記述されねばならない。

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、3.2.5 項に従って検証する。

3.2.2.1. LRA の認証

LRA の概念を持ったアカウントについては、認証済の組織情報をプロファイルとして発行 CA、RA に設定することがある。権限が付与されていることの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 CP 及び該当する CA/B Forum の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. 機械、装置、組織及び役割に基づく証明書の認証（DepartmentSign）

発行 CA 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. S/MIME BR 証明書

S/MIME BR 証明書の場合、Baseline Requirements for S/MIME の第 3.2.3 項に従い、組織のアイデンティティを認証するものとする。

3.2.2.4. 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(個人の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、組織の正式名称(法的形式を含む)及びサブジェクトの事業所の物理的な所在地の住所を示ことが求められる。

GlobalSign は以下を参照し、法的存在及び住所を検証する：

- Qualified Government Information Sources 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 Independent Information Source により提供される記録

さらに、GlobalSign は以下を参照し、住所を検証する可能性がある：

- 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

各種証明事項の情報は、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検証する。

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
- LRA の業務対応において、適切な認証を受けたアカウント管理者によって取得された証明

組織及び QWAC 証明書の同一性を主張する適格証明書については、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検証された会計士意見書

- 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、第 3.2.3 項に従って、授権された代表者の身元を確認する。
GlobalSign はオープンバンキング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 桁のシリアル番号、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

発行 CA 又は RA 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の証明が要求される。発行 CA 又は RA には、その他の提示情報を検証することは求められない。

3.2.3.2. Class 2

申請者は、申請上要求されている場合、申請に含まれる一定のアイデンティティ属性(証明書が関係する電子メールアドレスやドメイン名など)の管理を実証する必要がある。

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を提出することができる。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 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. 信頼できる情報源からの電話番号を使用し、申請者に電話によるチャレンジ・レスポンスを行う。
2. 信頼できる情報源からの FAX 番号を使用し、申請者に対して FAX によるチャレンジ・レスポンスを行う。
3. 信頼できる送信元からの電子メールアドレスを使用し、申請者に対して電子メールによるチャレンジ・レスポンスを行う。
4. 信頼できる情報源から得た住所を使用し、申請者に対して郵送によるチャレンジ・レスポンスを行う。
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可能性がある。これらの方法は、その他の Class 2 の商材においても有効である。

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、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. 組織に所属する個人の場合、GlobalSign は承認されたローカル RA の証明に依拠することができる。ePKI 又は MSSL プロファイルを介して要求される Class 2 の証明書については、3.2.3.5 を参照のこと。

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十分性検証し、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

GlobalSign は申請者に対して、更なる情報を要求することができる。同等のレベルの信頼性を実証するために、他の情報及び/又は方法を利用してもよい。

電子メールアドレスが証明書の申請に記載される場合、GlobalSign 又は LRA はその電子メールアドレスの所有の正当性について検証しなければならない。

3.2.3.3. Class 3

EV コードサイニング証明書について、申請者は、証明書に記載される全ての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求められる。

EV SSL 証明書について、申請者は、証明書に記載され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求められる。

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、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。発行 CA 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。

PersonalSign 3 Pro において、公証人又は信頼できる第三者は、その機会に及び国が発行する写真付き身分証を検証したこと、申請情報が正確であることを証言するため、申請者と面会する。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。

発行 CA 及び RA には、EV ガイドライン及び Baseline Requirements for Code Signing に従い、申請者との信頼できるコミュニケーション手段として GlobalSign が検証した信頼できる伝達方法を用い、申請者の保有する、証明書のサブジェクトとして記載されることを希望している組織を代表する権限を認証することが求められる。

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. S/MIME BR 証明書

S/MIME BR 証明書の場合、CA は、Baseline Requirements for S/MIME の第 3.2.4 項に従って、個人の身元を認証するものとする。

3.2.3.5. 適格証明書

個々の利用者のアイデンティティを正確性検証するには、eIDAS /UK eIDAS 規則の第 24.1 項に従って実施されなければならない。：

3.2.3.6. ローカル登録局認証

ローカル登録局の構想を認める組織アカウントでは、発行 CA 及び RA は、認証された組織の詳細をプロファイルの形式で設定することができる。これらのアカウントで発行される証明書には、プロファイルに記載されたデータフィールドが入力される。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。

3.2.3.7. 北米エネルギー企画委員会（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、認定認証局は、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、RA 運用/機能の一部若しくは全てを ePKI 経由で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 認定認証局要件及び NAESB Business Practices 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。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
Level 1	Rudimentary (最小限)
Level 2	Basic (低度)
Level 3	Medium (中程度)

GlobalSign 又は委託された 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。

3.2.4. 検証されない利用者情報

発行 CA は、証明書のサブジェクト識別名に記載される情報、或いはその CPS か発行する証明書そのものに記載する規定において除外される製品又はサービス固有の項目以外の、全ての情報を十分性検証する。Intranet SSL 証明書に限っては、発行 CA は、申請者が提供する SubjectAlternativeName に含まれる内部又は非公開の DNS 名、ホスト名、RFC 1918 の IP アドレスなどの情報に依拠することができる。

コードサイニング証明書については、認証局は、申請者が自己申告の情報をサブジェクトの所属名（organizationalUnitName）フィールドに記載できない申請手続きを採用しなければならない。

S/MIME BR 証明書の場合、Baseline Requirements for S/MIME に従って検証されていない利用者情報は、証明書に含まれないものとする。

3.2.5. 権限の十分性検証

PersonalSign1 Certificates	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で正確性検証をする。
PersonalSign Demo Certificates	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 Certificates	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 Certificates	信頼できる方法による申請組織又は申請者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。(3.2.3.5 項を参照)
PersonalSign2 Pro	申請者個人の正確性検証、及び必要に応じて申請者がメールアドレスを管理していることの正確性検証をする。 さらに、申請代表者が、証明書の発行又は失効を申請する権限、又はこれらの役割を他者に割り当てる権限を有することを正確性検証する。ePKI アカウントを通じて発行される証明書については、プロファイルの設定時に申請代表者のエンタープライズ RA としての権限が正確性検証される。

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。
PersonalSign3 Certificates	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ほか、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。 さらに、申請者代表が、証明書の発行又は失効を申請する権限、又はこれらの役割を他者に割り当てる権限を有することを正確性検証する。EPKI アカウントを通じて発行される証明書については、プロファイルの設定時に申請代表者のエンタープライズ RA としての権限が正確性検証される。
S/MIME BR Certificates	Baseline Requirements for S/MIME に従った十分性検証をする。
Code Signing Certificates	Code Signing Minimum Requirements の規定に従い、申請組織及び申請者個人の正確性検証する。
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の正確性検証する。
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 Certificates	3.2.7 項に規定されている方法により、申請組織又は申請者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 ガイドラインの規定に従い、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 and CDS	申請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、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、その権限を有する LRA が検証する。
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 項に規定されている方法に従い、契約署名者が証明書の承認者かつ権限者であることの正確性検証をする。
Qualified Certificate for Electronic Signature	3.2.2.4 項に規定されている方法に従い、個人の申請者からの申請について権限の正確性検証をする。

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、GlobalSign は以下の何れかの方法によって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(又はそれ以上の水準の)電子署名又は e シール
- 在籍を確認されている従業員又は当組織の代理人の高度(又はそれ以上の水準の)電子署名又は e シール

3.2.6. 相互運用のための基準

発行 CA は、認証局が信頼関係の確立を手配した、又は受け入れたことを条件として（すなわち相互認証証明書の発行にあたって）、 認証局を サブジェクトとする全ての相互認証証明書を開示しなければならないものとする。

3.2.7. ドメイン名の認証

Baseline Requirements for TSL 第 3.2.2.4 項の記載事項に従った方法により、全ての SSL 証明書について、申請された FQDN 及び IP アドレスが当該申請者の保有又は管理下にあることを検証しなければならない。その方法の詳細を CPS に記載されなければならない。

GlobalSign は、ドメインの CAA レコードと照合したパブリックに信頼された SSL 証明書における各サーバの FQDN を十分性検証しなければならない。GlobalSign の発行ドメインは"globalsign.com"である。CAA レコードが globalsign.com を公証された CA として記載していない場合、GlobalSign は証明書を発行することができない。

申請者は更に情報を要求することができ、同等の信頼性を得るために他の情報及び/又は方法を利用することもできる。

3.2.8. IP アドレスの認証

Baseline Requirements for TLS 第 3.2.2.4 項の記載事項に従った方法により、全ての SSL 証明書について、申請された FQDN 及び IP アドレスが当該申請者の保有又は管理下にあることを、検証しなければならない。その方法の詳細は CPS に記載しなければならない。

申請者に更なる情報を要求し、同等の信頼性を得るために他の情報及び/又は方法を利用することもできる。

3.2.9. メールボックスに対する管理権限についての十分性検証

全ての S/MIME 証明書について、申請された全てのメールアドレスを申請者が所有していることを、Baseline Requirements for S/MIME の 第 3.2.2 項に従って検証しなければならない。

3.3 鍵更新申請時における識別及び認証

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

3.3.1 定期的な Re-key における識別及び認証

全ての Re-key 申請は、発行 CA により認証されなければならない。証明書に記載された情報が何らかの形で変更された場合、追加の十分性検証を行わなければならない。

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

発行 CA 又は RA は全ての失効申請に対して認証する。利用者からの失効申請は、ユーザ名及びパスワードによるアカウントへのログイン、又は証明書に組み込まれた固有の要素を所有していることの証明といった、適切なチャレンジ・レスポンスがあった場合に認められる。

発行 CA はまた、該当する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。失効理由としては、利用契約への違反や、該当する料金の未払いなどがある。

4.0　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

発行 CA は、証明書の申請を受諾しない個人又はエンティティのリストを独自に作成する。このブロックリストは、過去の取引履歴、或いはその他の情報源に基づいて作成される。加えて、発行 CA 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。

4.1.2　登録手続きとそこで負うべき責任

証明書の発行に先立ち、認証局は、該当する CA/B Forum の要件に従い、証明書申請並びに、利用契約書及び/又は利用規約への同意を受領するものとする。

発行 CA 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、手続きを採用するものとする。申請者は、必要な正確性検証を行えるよう、発行 CA 及び RA に対し情報を提出しなければならない。発行 CA 及び RA は、申請者が申請手続きにおいて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。

4.2　証明書申請手続き

4.2.1.　識別及び認証の実施

発行 CA は、CPS に準拠し、本人識別情報の真正性を十分に検証するシステム、手続きを採用するものとする。初回の身元情報の十分性検証は、発行 CA の検証チーム又は契約している RA が本 CP3.2 項の規定内容に沿って実施する。手続きに伴い行われる連絡の結果得られた情報は、提出された申請者の情報と共に、安全に保管される。

第 6.3.2 項は、利用者証明書の有効期間を制限する。

CA は、適用される CA/B Forum の要件に従い、完了した十分性検証及び/又はその裏付けとなる証拠を再利用することができる。

初回以降の証明書申請については、単一要素による認証(利用者名かつパスワード)又は多要素認証(ユーザ名/パスワードと紐づけられた証明書)を用いて権限を検証する。

4.2.2.　証明書申請の認可又は却下

発行 CA は、何れかの項目について十分性の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。適切なベストプラクティスの手続きを経て全ての十分性の検証手続きが完了した場合には、発行 CA は通常、証明書申請を承認する。 発行 CA は以下に挙げるような理由があれば、申請を却下することができるものとする。 :

- 申請を受領する際に GlobalSign のブランドが損傷される可能性がある。
- 以前に申請を却下されたか、又は以前に利用契約の条項に違反した申請者からの証明書。

発行 CA は、申請を却下した理由を申請者に説明する義務を負わない。

発行 CA は、パブリックに信頼された SSL 証明書を Internal Names 又は予約済み IP アドレスに対して発行してはならない。

4.2.3.　証明書の申請処理に要する期間

発行 CA は、証明書の申請を処理し評価するために、全ての合理的な方法が使用されることを保証するものとする。

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 が証明書を発行するには、GlobalSign の信頼された役割にある正式なメンバーが、ルート CA が証明書署名の業務を行うために、意図的に直接命令を発行することが必要である。

発行 CA は、RA から証明書の発行を承認する旨の連絡を受け取る機能を有するシステムのアカウントに対し、多要素の認証を行う。発行 CA が直接運営する RA、及び契約に基づいて運営される RA は、認証局に送信される全ての情報が確実に十分性検証され真正性を担保されていることを保証する。

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

発行 CA 又は RA は、登録手続きの際に提示された合理的で適切な連絡先を通じて、証明書の発行を利用者に通知する。

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

発行 CA 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。これが実のない規定とならないよう、発行 CA は、電子証明書が受領されたものとみなされるまでの期間を設定することができる。

4.4.2.　認証局による証明書の公開

発行 CA は、利用者に証明書を交付することにより、又は Certificate Transparency Log といったしかるべきリポジトリにおいて、証明書を公開することができる。

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。発行 CA 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しなければならない。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 QSCD 内で生成・格納されなければならない。

非 EV コードサイニング証明書のうち 2023 年 4 月 23 日以前に発行されたものについては、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 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のうち 2023 年 4 月 23 日以前に発行されたものについては、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。
2023 年 4 月 24 日より、EV 及び非 EV コードサイニング証明書の利用者秘密鍵は、少なくとも FIPS140-2 レベル 2 又は Common Criteria EAL 4+ に適合していると認定されたユニット設計フォームファクタのハードウェア暗号モジュールで生成及び保護されなければならない。

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 は、GlobalSign のデジタル署名サービスにおいて、利用者の同意を得て、短期間のみ利用された証明書とそれに対応する秘密鍵を、要件準拠した HSM 又は QSCD 内でホスト、保護、管理する。

第 9.6.3 項の 2 及び 4 を参照。

4.5.2. 依拠当事者による公開鍵と証明書の利用

発行CAは、CRLやOCSPなど証明書の有効性を検証する適切な方法を通じた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、そのCPSに規定しなければならない。発行CA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、発行CA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。

4.6.1. 証明書更新の条件

証明書の更新は、利用者、利用者の委任を受けた代理人、又は発行 CA の独自の判断により行われる。
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

発行 CA は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。

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。

4.7.1. 証明書の Re-key の条件

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

発行 CA 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。

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。

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

発行 CA 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。

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

認証局は、失効の手続きを取る前に、失効申請の権限を検証しなければならない。

認証局は自己の裁量によって証明書を失効することができる。

認証局は次の条件の何れかに該当するときは、利用者証明書を 24 時間以内に失効する：

1. 利用者が証明書の失効を希望する旨を書面で(証明書の発行 CA 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発行 CA に通知した場合。

3. 認証局 が(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. 認証局が、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. 認証局が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. 発行 CA が、ドメイン管理権限又は証明書に含まれるメールボックスに関するメールボックス管理権限へ実施された正確性検証に依拠すべきではないという証拠を取得した場合。
7. 認証局が、利用者又は サブジェクトの契約又は事業機能の予期せぬ終了について通知を受けるか、又はその他の方法で認識した場合。
8. オープンバンキング証明書について、発行 CA が 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。

認証局は、利用者の証明書を 24 時間以内に失効するものとし、以下のうち 1 つ以上の状況が発生した場合、5 日以内に実施しなければならない。

1. 証明書が、6.1.5 項及び 6.1.6 項に規定されているように、該当する CA/B Forum の要件にあるアルゴリズムの種類及び鍵長にもはや準拠していない。
2. 認証局 が、証明書が不正使用されたことを示す証拠を取得する。
3. 認証局が、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。
4. 認証局が、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. 認証局が、証明書に記載されるメールアドレス又は FQDN の使用が法的に許可されなくなったことを示す状況（例えば、裁判所又は仲裁人がメールアドレス又はドメイン名を使用する権利を取り消した、利用者間との関連するライセンス契約又はサービス契約が終了した、若しくはアカウント所有者がメールアドレス又はドメイン名の有効な状態を維持しなかった、等）を認識する。
6. 認証局が、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。
7. 認証局が、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。
8. 認証局が、証明書が該当する CA/B Forum の要件又は発行 CA 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する。
9. 認証局が、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。
10. 発行 CA が CRL/OCSP リ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、発行 CA が該当する CA/B Forum の要件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。
11. 本 CP 及び/又は CPS により失効が要求された場合。
12. 認証局 が、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。
13. 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、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)。
14. 証明書を発行する際に使用された 発行 CA の秘密鍵が漏洩した疑いがある場合。
15. 発行 CA が、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。
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アカウントを通じて証明書の失効を申請する。
2. 利用者は、発行 CA のサポートチーム又は発行 CA の登録当局へ、認証済み申請を通じて失効を申請する。
3. 発行 CA が、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 GlobalSign の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、受領又は認識する。

4. 利用者による当該費用の未払い
5. 証明書のキャンセル申請を受けたとき。
6. 証明書が再発行された場合に、発行 CA が以前に発行された証明書を失効させることができる。
7. 一定のライセンス契約に基づき、発行 CA は、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. 発行 CA は、本証明書の継続使用が GlobalSign 又は第三者の事業に有害になりうるかの判断を行う。証明書の利用が第三者の事業又は評判に悪影響を及ぼすかどうかを検討する際、GlobalSign はとりわけ、受領した苦情の性質及び件数、苦情申立人の身元、有効な関連法規、及び利用者による有害とされる使用への対応を検討する。
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 の要請を受領後 24 時間以内に Microsoft に例外を申請する。Microsoft は、提出物を確認し、専らその裁量で、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 が失効を書面で申請する。
2. 利用者が、元の証明書リクエスト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発行 CA に通知する。
3. 発行 CA 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、該当する CA/B Forum の要件にある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. 発行 CA 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. 発行 CA が、証明書が該当する CA/B Forum の要件又は CP 若しくは CPS に従って発行されていないこと、又は下位 CA が該当する CA/B Forum の要件又は CP 若しくは CPS を遵守していないことを発見した。
6. 発行 CA 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 リポジトリを維持し続けるための調整をしていない限り、該当する CA/B Forum の要件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)。

他の発行CAを相互認証する発行CAは、相互認証した発行CAが両当事者間で締結された契約条項に適合しない場合、相手の発行CAを失効することが可能である。

4.9.2. 失効の申請者

利用者、RA、又は発行 CA は失効プロセスを開始することができる。
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、及び他の第三者は、証明書を取り消す合理的な理由が疑われる場合、その旨を発行 CA に知らせる電子証明書の問題報告を提出することができる。

発行 CA 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。

加えてオープンバンキング証明書においては、失効申請が PSP を認証又は登録した所轄官庁から行われうる。

4.9.3. 失効申請の処理手続き

第項認証局は、利用者が自己の証明書の失効を要求するためのプロセスを提供するものとする。このプロセスは、認証局の CP 及び/又は CPS に記載されるものとする。認証局は、失効申請及び電子証明書の問題報告の受付及び対応を 24 時間 365 日継続的に行うものとする。

認証局は、秘密鍵危殆化の疑い、証明書の不正使用、又はその他の種類の詐欺、危殆化、不正使用、不適切な行為、或いは証明書に関連するその他の問題を報告するための、明確な方法を提供するものとする。認証局は、容易にアクセス可能なオンライン上の手段及びその CPS の第 1.5.2 項において、その方法を公開するものとする。

4.9.4. 失効申請までの猶予期間

SSL サーバ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設けない。

その他の証明書について、失効申請までの猶予期間とは、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。発行 CA は、利用者に最大 48 時間の猶予を与えることができるが、これを過ぎると発行 CA は利用者の証明書を失効する、或いはその他利用者を代理した適切な手続きを取ることができる。

4.9.5. 認証局が失効申請を処理すべき期間

発行CAは、電子証明書の問題報告を受けた後24時間以内にCertificate Problem Reportの調査を開始する。

エンドエンティティ証明書の失効申請については、アカウントを通じて送信された失効申請、及び発行CAが失効手続きを開始したものの何れであっても、受理から最大でも30分以内に処理されなければならない。

他の発行 CA の証明書を相互認証する CA 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）をキーセレモニー後 12 時間以内に発行する。

発行 CA 及び RA は、Report Abuse を通した報告を通じて、優先度が高い電子証明書の問題報告に内部的に対応する能力を 24 時間 365 日維持し、必要に応じて、当該苦情を法執行権限に転送し、及び/又は当該苦情の対象である証明書を取り消すものとする。発行 CA 及び RA は、報告の受領後 24 時間以内に、疑わしい鍵の危殆化又は証明書の誤用に対する調査手続きを開始するものとする。

発行 CA 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:

1. 申し立ての問題の性質
2. 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
3. 苦情を申し立てている主体、及び
4. 関連規則

適格証明書の場合、実際の失効ステータスは、失効決定後 60 分以内に全ての失効過程を通じて公開/利用可能となり、決して復元しない。

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を十分性検証し、各証明書が有効であることを保証しなければならない。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十分性検証すべきである。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。発行 CA は、依拠当事者が失効情報の検証を容易に行えるよう、該当する URL を証明書に記載することがある。

適格証明書の場合、証明書チェーンの十分性検証は、EU 又は UK eIDAS のトラストリスト内の 発行 CA の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。

4.9.7. CRL の発行頻度

全ての発行 CA は、CRL の発行頻度については、該当する CA/B Forum の要件及び eIDAS 規則に準拠しなければならない。

CRL が提供され、CA が CRL の終了を決定、又は要求される場合、CA 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 配布ポイントで公開するものとする。CA 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 を発行してはならず、少なくとも CPS で指定された期間、最後の CRL の完全性及び可用性を維持するものとする。

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 の証明書に CDP (CRL 配布ポイント)が含まれている場合、CRL は、(i) 少なくとも 12 か月に 1 回、及び、(ii) 下位 CA の証明書を失効した後、24 時間以内に更新、再発行され、nextUpdate のフィールドの値は、thisUpdate のフィールドの値に加えて 12 か月を超えてはならない。

4.9.8. CRL の最大通信待機時間

CRL は生成後、商業的に合理的な期間内にリ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

発行 CA は、CRL の他に 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、OCSP による応答までの待機時間が 10 秒を超えないよう管理する。

発行 CA の OCSP 応答は、RFC6960 及び又は RFC5019 に準拠している。OCSP 応答は、OCSP 応答者によって署名されるものとし、その証明書は、その失効ステータスがチェックされている証明書を発行した CA によって署名される。OCSP 署名証明書は、RFC6960 で定義されるタイプ id-pkix-ocsp-nocheck の拡張を含まなければならない。

4.9.10. オンラインでの失効情報の確認の要件

認証局が運営する OCSP レスポンダは、RFC 6960 及び RFC 5019 に記載されている HTTP の GET メソッドをサポートしなければならない。

OCSP レスポンスの有効期間は、thisUpdate フィールドと nextUpdate フィールドの時間差である。
差異の計算においては、うるう秒を無視して、3,600 秒の差異は 1 時間に、86,400 秒の差異は 1 日に相当するものとする。

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間は、10 日以下とする。
3. 有効期間が 16 時間未満の OCSP レスポンスの場合、認証局は nextUpdate の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 レスポンスの場合、認証局は OCSP を介して提供される情報を、nextUpdate の少なくとも 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:
認証局は、OCSP レスポンダを通じて提供される情報を(i) 少なくとも 12 か月に 1 回、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。

OCSP レスポンダは、シリアル番号のステータスが「unused」の証明書についてリクエストを受け取った場合、証明書に対して「good」と応答しない。
7.1.5 項に従って認証局が技術的に制約されていない場合、OCSP レスポンダは、このようなリクエストに対して「good」と応答しない。

認証局は、セキュリティ対応手順の一環として、「unused」のシリアル番号のリクエストについて OCSP レスポンダを監視するものとする。

OCSP リクエスト内の証明書シリアル番号は、以下の 3 つのオプションの何れかである：

1. 発行 CA が、その証明書のサブジェクトに関連する現在又は過去の鍵を使用して、そのシリアル番号の証明書を発行した場合、「assigned」。
2. 当該シリアル番号の Precertificate [RFC6962] が以下の機関より発行されている場合、「reserved」。
   - 発行 CA
   - 発行 CA に関連する Precertificate 署名用証明書。
3. 上記何れの条件も満たさない場合、「unused」。

4.9.11. その他の方法による失効情報の提供

利用者証明書が高トラフィック FQDN の場合、発行 CA は[RFC4366]に従って、その OCSP 応答を分配するためにステープルに依存することを選択することができる。この場合、発行 CA は、利用者が TLS ハンドシェイクで証明書の OCSP レスポンスを「ステープル」することを保証するものとする。発行 CA は、利用契約を通じて、又は CA が実施する技術的検討手段によって、この要求事項を利用者に対して契約上執行するものとする。

4.9.12. 認証局の鍵の危殆化に伴う特別な要件

発行 CA 及び 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、及び発行 CA 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、発行 CA 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、更新した CRL をオンラインで 30 分以内に発行する。

4.9.13. 証明書の効力の一時停止を行う条件

証明書の効力の一時停止はクライアント証明書にのみ認められる。証明書の効力の一時停止は、他のタイプのエンドエンティティ証明書には許可されない。証明書の効力の一時停止は、SSL 証明書及び適格証明書には厳しく禁じられている。

4.9.14. 証明書の効力の一時停止の要求者

発行 CA 及び RA は、認証済みの一時停止要求を受領するものとする。利用者又は証明書指定の関連機関から停止要求を受けた場合は、停止を許可する。発行 CA はまた、他のクロス署名発行 CA に発行される証明書を含む証明書を自らの判断で停止することができる。

4.9.15. 証明書の効力の一時停止手続き

一時停止要求の性質と効率上の必要性により、発行 CA 及び RA は、例えば一時停止要求された証明書を発行したアカウントを介す等して、一時停止要求を要求し認証するための自動機能を提供することがある。また、自動一時停止機能が不可能な場合、RA は手動のバックアッププロセスを提供することがある。発行 CA 及び RA は、一時停止要求を記録し、送信元を認証し、要求が真正でありかつ承認されている場合、証明書を一時停止するために適切な措置を講じる。一旦中断したら、CRL の理由を示すコードである「certificateHold」を含め、証明書のシリアル番号と日時が適切な CRL に追加される。CRL は、直ちに公表される場合もあれば、認証業務運用規程(CPS)に定義されている通りに公表される場合もある。

4.9.16. 証明書の効力の一時停止期限

証明書の効力の一時停止期限には制限がない。

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

発行 CA 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、発行 CA 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。

ルートプログラム又は CA/B Forum の要求により、発行 CA 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。

4.10.2. サービスを利用できる時間

発行 CA は証明書ステータス情報を 24 時間 365 日提供する。この際、付加的にキャッシュされた情報を含むコンテンツ配信ネットワークを通じたクラウドサービスを使用することがある。最優先にある電子証明書の問題報告に対し社内にて応答できる能力を 24 時間 365 日維持することとし、適切である場合は、法令の執行機関への準拠し、かつ/又はそうした訴えを受けている証明書を失効する。

4.10.3. 運用上の特性

（規定なし）

4.11 利用の終了

利用者は、証明書サービスの利用を、証明書を失効すること、又は有効期限を満了することで終了することができる。発行 CA がエンドエンティティに証明書を発行する下位 CA との契約を締結している場合、両当事者間の契約は証明書の有効期限中は継続されなければならず、契約を終了させる場合には証明書を失効させなければならない。

4.12 キーエスクロー及びリカバリー

4.12.1 キーエスクロー及びリカバリーの、ポリシー及び手続き

認証局の秘密鍵は預託されてはならない。利用者に対してキーエスクローサービスを提供する発行 CA は、利用者の秘密鍵を預託してよい。預託された秘密鍵は、オリジナルの秘密鍵と少なくとも同じセキュリティレベルで保管しなければならない。

4.12.1.1 S/MIME BR

認証局は、自身の CP 及び/又は CPS に規定されるとおりに、利用者の秘密鍵を預託することができる。

認証局は、利用者の秘密鍵が預託された場合、その旨を利用者に通知するものとする。預託された秘密鍵は、暗号化された形式で保管されるものとする。認証局は、エスクローされた秘密鍵を不正な開示から保護するものとする。

認証局は、自身の CP 及び/又は CPS が許可する状況下においてのみ、利用者の秘密鍵を回復するものとする。

4.12.2 鍵カプセル化及びリカバリーの、ポリシー及び手続き

（規定なし）

5.0 施設、経営、及び運用上の管理

認証局は、以下を目的とした包括的なセキュリティ計画を策定、実施、及び維持するものとする：

1. 証明書データ及び証明書管理プロセスの機密性、完全性、及び可用性を保護すること
2. 証明書データ及び証明書管理プロセスの機密性、完全性、及び可用性に対する予期される脅威又は危険から保護すること
3. 証明書データ又は証明書管理プロセスへの不正又は違法なアクセス、使用、開示、改ざん、又は破壊から保護すること
4. 証明書データ又は証明書管理プロセスの偶発的な紛失、破壊、又は損傷から保護すること、及び、
5. 法律により認証局へ適用されるその他全てのセキュリティ要件に準拠すること。

証明書管理プロセスには以下を含むものとする：

1. 物理的環境面のセキュリティ
2. 構成管理、信頼されるコードの完全性維持、マルウェアの検知/防止を含むシステム完全性管理
3. ポート制限及び IP アドレスフィルタリングを含む、ネットワークセキュリティ及びファイアウォール管理
4. ユーザ管理（信任された役割の割り当て、教育、意識向上、訓練を含む）、及び、
5. 個人の行動責任について説明根拠を提供する、論理的アクセス制限、アクティビティログ、及び不活性タイムアウト。

認証局のセキュリティ・プログラムには、年次リスク評価を含むものとする：

1. 証明書データ又は証明書管理プロセスに関し、不正アクセス、開示、誤用、改ざん、又は破壊に至る可能性のある、予見可能な内部及び外部の脅威を特定する
2. 証明書データ及び証明書管理プロセスの機微性を考慮し、これらの脅威の可能性及び潜在的損害を評価する、及び、
3. 認証局が係る脅威に対抗するために導入しているポリシー、手続き、情報システム、技術、及びその他の取り決めの十分性を評価する。

リスク評価に基づき、認証局は、証明書データ及び証明書管理プロセスの機微性に応じて、上記に定める目的を達成し、リスク評価中に特定されたリスクを管理及び制御するために設計されたセキュリティ手続、手段、及び製品から成るセキュリティ計画を策定、実施、維持するものとする。セキュリティ計画には、証明

書データ及び証明書管理プロセスの機微性に見合った管理的、組織的、 技術的、物理的な保護手段を含めるものとする。また、セキュリティ計画は、その時点で利用可能な技術及び特定の措置を実施するための費用を考慮し、セキュリティ侵害によって生じる可能性のある損害及び保護されるデータの性質に適した合理的なレベルのセキュリティを実施するものとする。

5.1 物理的管理

発行CA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ものとする。

5.1.1 所在地及び建物

発行CAは、重要かつ機微な情報を処理する設備が適切なセキュリティ障壁及び入管管理体制を持つ安全な場所に設置されていることを保証するものとする。
これらは不正アクセス、損害、妨害から物理的に保護されるべきであり、またその保護とはリスク分析計画に明記のリスクに対応するものとする。

5.1.2 物理的アクセス

発行CA、証明書ライフサイクル管理に使用される設備が、不正アクセスがシステム又はデータに対してもたらす損害から物理的に保護された環境で運用されていることを保証するものとする。
物理的保護域に不承認者が立入る際は、常に承認された従業員が同行するものとする。
物理的な保護とは、認証局オペレーションを搭載するシステムの周囲に明確に定義されたセキュリティ境界（例；物理的な障壁など）を設置することで達成されるものとする。
この境界区域内においては、認証局資産の如何なる部分もその他組織の構成と共用されるものではない。

5.1.3 電源及び空調

発行 CA は、電力供給及び空調設備が認証局システムの運用を補助するのに十分なものであることを保証するものとする。

5.1.4 水漏れ

発行 CA は、認証局システムが水漏れから保護されていることを保証するものとする。

5.1.5 火災安全及び保護

発行 CA は、消防システムにより認証局システムが保護されていることを保証するものとする。

5.1.6 メディア ストレージ(記憶媒体)

発行CAは、使用される何れのメディア（記憶媒体）も損害、盗難及び不正アクセスから保護され、安全に使用されていることを保証するものとする。
メディアの管理処理は一定期間、メディア本体の老朽化・劣化に対して保護されるべきであり、また記録の保持が必要とする。全てのメディアは情報資産分類スキームの条件に沿って安全に使用され、また機微情報を格納するメディアが必要とされなくなった際は、安全に破棄されなければならないものとする。

5.1.7 廃棄処理

発行 CA 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

発行CAは、証明書発行システムの完全バックアップは、システム停止時にシステムを復旧するために適切なものであり、定期的に作成されていることを保証するものとする。（この期間はCPSにて定義されなければならない）重要な業務情報及びソフトウェアのバックアップ用コピーは定期的に作成されなければならない。災害又はメディア停止に伴い、全ての重要な営業情報及びソフトウェアが復旧できるように適切なバックアップ設備が提供されなければならない。
事業継続計画の条件を満たしていることを保証するため、個々のシステムのバックアップ調整は定期的にテストされるものとする。

少なくとも、1 つはシステムの完全なるバックアップコピーがオフサイト（証明書発行設備とは離れた場所）に格納されていなければならない。バックアップについても、通常の施設と同様に物理的・手続き上の管理が為された場所に格納されるものとする。

5.2 手続き的管理

5.2.1 信頼された役割

発行CA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害の対立が発生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）：

GlobalSign は、GlobalSign の関連会社又はこれらの関連会社と(下請として)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、GlobalSign の親会社及び子会社、及び GlobalSign と同一の親会社を持つその他の企業がある。

- 開発：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(鍵のコンポーネント監視等)
- 管理者：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：認証局システムのインストール、設定及び保守に加え、認証局システムアーカイブ及び監査ログの閲覧及び保守に責任がある
- インフラオペレーター：日常的な認証局システムの操作及びバックアップ・復旧に責任がある
- キーマネージャー：暗号化に用いられる鍵のライフサイクル管理機能(鍵のコンポーネント監視等)に責任がある

5.2.2 タスク毎に必要な人員数

発行 CA は、CPS 内でタスク毎に必要となる人員数を明確に強調して記載するものとする。この目的は、如何なる悪意ある行為も結託する必要が生じるため、全認証局サービス（鍵ペア生成、証明書生成、及び失効）への信頼を保証することとなる。他者間管理が必要な場合、少なくとも関係者の内一人は管理者となる。全ての関係者は先に 5.2.1 項に定義された信頼された役割である事が求められる。

5.2.3 役割毎の識別及び認証

信頼された役割に指名する前に、発行 CA 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 責任の分離を要する役割

発行 CA は、認証局設備、手続き的、又はその両方の意味で、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

発行 CA は、人員が証明書管理プロセスに従事する前に、従業員、代理人、又は契約社員としてのアイデンティティを検証することとする。

発行CA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必要人数雇用するものとする。 発行CAの者は、正式な研修、教育、実地経験又はその何れか2つ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。 発行CAのCPSの中で指定される、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。発行CAの人員(一時的・永続的の両者)は、業務及び最小特権の分離の視点、職務及びアクセスレベル、バックグラウンドチェック、従業員教育に基づいた(職務やセキュリティに対する)理解度に基づく役職の機微性を考慮の上定義された職務記述書を有するものとする。発行CAの人員は、セキュリティ責任者である上級管理職によって信頼された役割に正式に指名されるものとする。職務記述書は技術及び経験の必要条件を含んでいる。管理者の人員は、電子署名テクノロジーでの実務又は研修経験を有し、またセキュリティ業務責任を担う人員のセキュリティ処置、及び情報セキュリティでの経験、リスク評価における経験など十分に管理機能を遂行出来る者が採用されるものとする。

5.3.2 バックグラウンドチェック手続き

発行CAの全信頼された役割に従事する者は、認証局運営の公平を不利にするような矛盾する利益を持たない者とする。発行CAは、役職に対して適正に影響すると思われる重罪或いはその他犯罪に前科を持つ人物を、信頼された役割に指名しないものとする。
人員が雇用される法域で許可されている場合には、全ての必要な確認がなされ、その結果の分析が終わるまでは、人員は信頼済みの機能にアクセスしない。 信頼された役割に従事する人員は全員、忠実、信頼性及び健全性に基づいて選ばれるものとし、バックグラウンドチェックに従うものとする。

発行CA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の利用は如何なる場合も、その人員が雇用される法域の該当の法令に準拠するものとする。

5.3.3 研修要件

認証局は、情報の正確性検証業務を行う全ての人員に、公開鍵基盤の基本的な知識、認証、また審査のポリシーや手順（認証局の証明書ポリシー及び認証業運用規程を含む）、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するものとする。

認証局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レベルを維持していることを保証するものとする。

認証局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スキルを有していることを文書化するものとする。

認証局は審査要員全員に対し、CA/B Forum の要件に記載の情報の正確性検証要件に関する、認証局が提供する試験への合格を必須としている。

5.3.4 再研修の頻度及び要件

信頼された役割に任命されている全ての人員は、GlobalSign 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、少なくとも年次の情報セキュリティ研修を含む研修（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。

5.3.5 職務のローテーション頻度及び順序

発行 CA は、従業員に関わる如何なる変更も、システムのサービス効率又は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、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

認証局は、証明書の発行に携わる委任された第三者が 5.3.3 項のいう研修・技能要件を満たし、5.4.1 項のいう文書保管及び監査ログ要件を充足していることを、検証するものとする。

5.3.8 個人に付与された文書について

発行CAは本CP、該当するCPS、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

発行 CA 及び各委任された第三者は、その証明書システム、証明書管理システム、ルート CA システム、及び委任された第三者のシステムについて、セキュリティに関するイベントを記録するものとする。発行 CA 及び各委任された第三者は、証明書申請を処理し証明書を発行するにあたり、証明書申請に関連して生成された 全ての情報及び受領した文書、日時及び関係者を含む、処理に関連するイベントを記録するものとする。発行 CA は、これらの記録をその適格監査人が入手できるようにするものとする。

発行 CA は少なくとも以下のイベントを記録するものとする。

1. CA 証明書及び CA 鍵のライフサイクルイベント（以下を含む）
   i. 鍵の生成、バックアップ、保管、回復、アーカイブ、及び破棄
   ii. 証明書申請、更新、re-key 申請、及び失効
   iii. 証明書申請の承認及び却下
   iv. 暗号化デバイスのライフサイクル管理イベント
   v. 証明書失効リストの生成
   vi. OCSP レスポンスの署名、及び
   vii. 新しい証明書プロファイルの導入及び既存の証明書プロファイルの廃止

2. 利用者証明書のライフサイクル管理イベント（以下を含む）
   i. 証明書申請、更新、re-key 申請、及び失効
   ii. 本証明書ポリシーに規定される全ての検証活動
   iii. 証明書要求の承認及び却下
   iv. 証明書の発行
   v. 証明書失効リストの生成、及び
   vi. OCSP レスポンスの署名

3. セキュリティに関するイベント（以下を含む）

   i. PKI システムへのアクセスの試みが成功した場合及び失敗した場合
   ii. 実行された PKI 及びセキュリティシステムの動作
   iii. セキュリティプロファイルの変更
   iv. 証明書システム上のソフトウェアのインストール、更新、及び削除
   v. システムクラッシュ、ハードウェア障害、及びその他の異常
   vi. ファイアウォール及びルータの動作、及び
   vii. CA 施設への入退室

ログ記録は、以下の要素を含むものとする。

1. イベントの日付と時間。
2. ジャーナルレコードを記録する人員のアイデンティティ、及び
3. イベントについての説明

5.4.2 ログ処理の頻度

（規定なし）

5.4.3 監査ログの保有期間

発行 CA 及び各委任された第三者は、以下の記録を少なくとも 2 年間は保持するものとする。

1. CA 証明書及び CA 鍵のライフサイクル管理イベント記録（第 5.4.1 項(1)に規定されるもの）は、以下の何れかが発生した後に保存される。
   i. CA 秘密鍵の破棄。
   ii. CA フィールドが true に設定された X.509v3 basicConstraints エクステンションを有し、かつ CA 秘密鍵に対応する共通の公開鍵を共有する証明書一式における、最上位の CA 証明書の失効又は期限切れ。
2. 利用者証明書の有効期間終了後の、利用者証明書ライフサイクル管理イベント記録（第 5.4.1 項 (2)に規定されるもの）。
3. イベント発生後のセキュリティイベント記録（第 5.4.1 項(3)に規定されるもの）。

5.4.4 監査ログの保護

全ての保有期間中において、発生イベントは削除又は破壊（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なければならない。

イベントは、データの完全性、真正性及び機密性に変更を加えることなく、信頼された役割の人員によってのみ、そのプロファイルに関する操作が可能であることが保証される状態で記録されなければならない。

イベントは、改変防止できかつ改ざんを検知できる状態で保護されなければならない。

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

監査ログは安全な場所(例：耐火性の金庫)に、信頼された役割の人員により、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、発行 CA 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

発行 CA 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微性を考慮し、上記の脅威の可能性と潜在的な損害を評価する。
3. 発行 CA 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、発行 CA は証明書の発行、製品及びサービスに関する認証局 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

発行CA及び各委任された第三者は、（5.4.1 項に規定されるとおり）全ての監査ログを保存するものとする。

さらに、発行CA及び各委任された第三者はアーカイブを作成するものとする。

1. 証明書システム、証明書管理システム、ルートCAシステム、及び委任された第三者のシステムに関するセキュリティ文書
2. 証明書申請及び証明書の検証、発行、失効に関連する文書。

5.5.2 アーカイブの保有期間

発行 CA は監査ログ（5.4.1 項に規定するとおり）及び記録（5.5.1 項に規定するとおり）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しなければならない。

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、信頼された役割の人員のみが操作を行なえることを証明するものとする。一定期間、原本メディアがデータを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 手続き

（規定なし）

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、5.3 項に定義されるセキュリティ条件に準拠しなければならない。

5.5.7 アーカイブ情報の取得と検証の手続き

（規定なし）

5.6 鍵交換

発行 CA は 6.3.2 項に伴い、発行 CA の鍵データを定期的に交換する場合がある。証明書のサブジェクト情報についても変更され、また証明書プロファイルも新たなベストプラクティスを守るべく、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応する手続き

発行CAは、コンピューティング資産、ソフトウェア又はデータの損壊・損失など、サービスの運営を妨げる、又は損なう事象の発生時に取るべき手段を解説した事業継続計画を構築するものとする。発行CAは、ビジネスリスクを評価するためのするリスクアセスメントの実施、災害復旧計画から導き出される必須のセキュリティ要件及びオペレーション手続きの決定を行う。このリスク分析は常時見直し、また必要あれば修正（脅威の進化、脆弱性の発展など）される。この事業継続は8項で述べるように、災害発生及び復旧計画後に、何が最初に保全されるオペレーションであるかを検証するため、監査処理の対象範囲となる。
発行CAで信頼された役割及びオペレーションに従事する人員は、事業の核心部にあるオペレーションについて、災害復旧計画に規定された手続きに則してオペレーションするために特別に訓練される。

万一、発行CAがハッキング又はその他攻撃の可能性と思われる行為を発見した場合、その実態及び被害の程度を知るための調査を行なうものとする。 若しくは発行CAにより、認証局又はRAのシステムをリビルド（再構築）する必要性、いくつかの証明書が失効するのみの場合、そして（又は）被害によるCA階層の宣言が必要な場合の判断を行なうために、それぞれの被害の範囲を査定するものとする。 認証局の災害復旧計画はどのサービスが維持されるべきかを明確化するものとする。（例えば、失効及び証明書のステータス情報）

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

万一何れかの設備が損壊又は操作不能な状態で、しかしながら秘密鍵が損壊していない場合、発行 CA 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、可能な限り早急に再構築されるものとする。

5.7.3 発行 CA の秘密鍵が危殆化した際の手続き

発行 CA の署名鍵が損壊、紛失した、又は破壊された、又は破損されたと考えられる場合：

- 発行 CA は問題の調査の後、発行 CA 証明書を失効すべきかを判断する。その場合、
    - 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。
    - 新規発行 CA の鍵ペアを生成又は既存の他の CA 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 災害後の事業継続能力

5.7.1 項に明記されるように、災害事業復旧計画は事業継続について取り決めている。証明書ステータス情報システムは 24 時間 365 日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。発行 CA は、その電子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：

- 発行 CA 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
- 発行 CA 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。(例えば、証明書ステータス情報を他の GMO インターネットのグループ会社に伝達する場合等がある。)
- 発行 CA で発行された全ての電子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 適合性評価機関をはじめ全ての監査人に通知すること
- 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、後任の発行 CA は、終了する前任の発行 CA と同じ権利義務を負うべきである。

6.0 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、発行 CA 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に記録する
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

発行CAは物理的に安全な環境において、信頼された役割に従事している、少なくとも二名の管理下で、全ての発行鍵ペアを生成するものとする。 外部の立会人（理想としては通常日常的に監査を行なう独立監査人）が立会うか、或いはセレモニー全工程がビデオ録画されなければならない。発行CAの鍵生成は、少なくともFIPS140－2 レベル3を満たすデバイスで行なわれるものとする。

発行 CA は、既知の脆弱な秘密鍵を用いて証明書が申請された場合、その申請を却下するものとする。

6.1.1.2 利用者の鍵ペア生成

発行CAが生成した利用者鍵の場合、鍵生成は、第 6.1.5 項及び第 6.1.6 項に規定される鍵生成アルゴリズム及び 鍵サイズを使用して、FIPS 140-2 （又はそれと同等）に準拠した安全な暗号デバイスで実行しなければならない。該当する場合、利用者鍵はCA/B Forumの要件及びeIDAS規制へ準拠して生成されなければならない。

コードサイニング証明書に使用される鍵は、少なくとも FIPS140-2 レベル 2 又は Common Criteria EAL 4+ に適合していると認定されたユニット設計フォームファクタのハードウェア暗号モジュー ル上で生成されなければならない。

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、利用者の鍵は認定された QSCD内で生成及び保管しなければならない。発行CAは QSCD の認証ステータスを監視し、QSCD の認証ステータスに変化があった場合は失効を含む適切な措置を講じるものとする。

6.1.2 利用者への秘密鍵配布

利用者の代理として秘密鍵を生成する発行 CA 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。公開鍵/プライベート鍵生成に関する暗号アルゴリズム(暗号化、符号、暗号ハッシュ、RNG、PRNG など)は FIPS によって承認され、公開鍵/プライベート鍵生成アルゴリズムも FIPS 186-4 で規定されている。

該当する場合、認証局は関連する CA/B Forum の要件の 6.1.2 項に従って、利用者へ秘密鍵を配布するものとする。

6.1.3 証明書発行者への公開鍵配布

発行CAは、RAからの送付中は保護され、またRAがその起点の確実性及び完全性を適切に検証した場合にのみ、公開鍵を受け付けるものとする。

6.1.4 認証局から依拠当事者への公開鍵配布

発行 CA 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。これには、商業ブラウザ及びプラットフォームオペレーターと協力し、ルートストア及び OS にルート証明書公開鍵を組み込む作業を行う場合がある。また、発行 CA の公開鍵は、証明書のチェーン又は発行 CA が運営するリ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（SP）800-133改訂2 (2020)- 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。

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/OCSP 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 CA/B Forum の要件に準拠している。

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 [2]	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。	有効期間が 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 [3], 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 [4], 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 [5]	

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。

2021 年 6 月 1 日以降、新しい Code Signing 及び Code Signing 向け 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。

[2] 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。
[3] 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。
[4] 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。
[5] 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。

6.1.6　公開鍵パラメーター生成及び品質検査

発行 CA は FIPS186 の定めに従い鍵ペアを生成し、また利用者から提示される公開鍵が適切であるか、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。該当する場合、CA/B Forum の要件に従って鍵ペア生成及び品質検査を実施するものとする。

6.1.7　鍵の使用目的(X.509 v3 鍵使用フィールドにおいて)

発行 CA は、申請で提案されるフィールドにしたがい、証明書における鍵の用途を、X.509 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 CA 及び相互認証の証明書
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

発行 CA 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。発行 CA 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

発行CAは証明書、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。
発行CAは利用者に対して、特定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。

6.2.2　秘密鍵(m 中の n) 複数の人員による管理

発行CAは、信頼された役割において職務を担う複数の人員による管理の下、秘密鍵を暗号化操作のためにアクティブに（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コード及びトークン）

6.2.3　第三者への秘密鍵の預託

発行 CA 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

発行 CA は原本の秘密鍵と同様に複数人員の管理下の CA 秘密鍵のバックアップを行なうものとする。

6.2.5　秘密鍵のアーカイブ

発行 CA 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。

パブリックに信頼される証明書を発行する下位 CA の場合、下位 CA 以外の当事者は、下位 CA の承認なしに下位 CA の秘密鍵をアーカイブしてはならない。

6.2.6　暗号モジュール間の秘密鍵移行

発行 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(保存又は移行のため) 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、CA 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発行 CA が認識した場合、発行 CA 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

発行 CA は 6.2.1 項の要件を満たすデバイスに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

発行 CA 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、利用契約及び利用に関する合意書に示される責務に従って、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

発行 CA 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。発行 CA のハードウェアセキュリティモジュールがオンラインかつ操作可能な間、認証済み RA から証明書及び CRL/OCSP へ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なければならない。

6.2.10 秘密鍵の破棄方法

発行 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破棄される。秘密鍵を破棄するにあたり発行 CA 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。

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

発行 CA 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	鍵ペア使用期間	最長の有効期間
Root Certificates[6]	規定なし	28 年
TPM Root Certificates	30 年	41 年
Publicly Trusted Sub-CAs/Issuer CAs	規定なし	18 年
PersonalSign Certificates	規定なし	39 か月
Code Signing Certificates	規定なし	39 か月
EV Code Signing Certificates	規定なし	39 か月
S/MIME BR strict and multipurpose Certificates	規定なし	825 日
S/MIME BR legacy Certificates	規定なし	1185 日
AATL End Entity Certificates	規定なし	39 か月
Qualified Certificate for Electronic Signatures and Seals	規定なし	39 か月
DV SSL Certificates	規定なし	398 日
AlphaSSL Certificates	規定なし	398 日
OV SSL Certificates	規定なし	398 日
EV SSL Certificates	規定なし	398 日
Qualified Website Authentication Certificates	規定なし	398 日
Intranet SSL	規定なし	5 年
Timestamping Certificates	15 か月	11 年
NAESB Certificates	2 年	2 年
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 証明書の有効期間終了までに有効期間が終了しなければならない。

---

[6] *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。*

計算上、1 日は 86,400 秒として計測される。端数秒及び/又はうるう秒を含め、これを超える時間は、追加の 1 日を表すものとする。このような調整を考慮するため、利用者証明書は、デフォルトで許容される最大時間で発行されるべきではない。

発行 CA 証明書は、最長有効期間に関し CA/B Forum の要件に準拠しなければならないため、それに従って証明書の有効期間を短縮する場合がある。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。
現行又は将来の CA/B Forum の要件が、証明書が最初に発行された時点では実施されていなかった証明書発行に対して認証権限に要件を課す場合、特に再発行の申請がなされた場合においては、利用者が最大の有効期間を享受できないことがある。
例：ある証明書の種類について識別及び認証に対する追加要件が含まれる場合、又は最大の有効期間が短縮される場合。

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

発行 CA の秘密鍵をアクティブ化するために使用される、発行 CA 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され、また信頼された役割を担う持分所有者に配布されなければならないものとする。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、暗号及び物理的なアクセス管理の仕組みを介した漏洩から保護されなければならない。発行 CA 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

発行 CA 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発行 CA 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、或いは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。発行CAのPKI構成は下記の機能を必ず含むものとする。

- 信頼された役割に対する認証済みログインを要求
- 最小限の権限と共に、任意のアクセスコントロールを提供する
- 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する
- 強固なパスワードを使用する方針を要求する
- セッション中のコミュニケーションに対して暗号使用を要求する
- 識別及び認証には、信頼済みパスを要求する
- 悪意あるコードを防止する手段を提供する
- ソフトウェア及びファームウェアの統合性を維持する手段を提供する
- 処理に対してドメインを分離し、システム及びプロセスを区分する
- OSに対して自己防御を提供する

証明書発行を直接的に引き起こすことのできるアカウントについては、発行 CA は、多要素認証を実施するものとする。

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

発行 CA 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。
- 入手したハードウェア及びソフトウェアは、どんな特殊なコンポーネントが意図的に混入される可能性を低減する方法において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）
- 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、その開発プロセスが定義・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。
- 全てのハードウェアは、購入場所から運用場所まで一連の継続した責任体制を保証できる、管理された方法を介して配送又は配布されなければならない。
- 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。認証局の運営に属さ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可能となる。発行 CA 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は定期的に不正コード探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 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

発行CA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、発行CAのCA管理者により管理されるものとする。発行CA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発行CA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。最初に発行CA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

発行 CA 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維持するため、保守スキームを継続的に監視する。

6.7 ネットワーク セキュリティ コントロール

発行 CA 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。このようなセキュリティ対応策には、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。

当項を以て、CA/B Forum の Network and Certificate System Security Requirements を参照により組み込む。

6.8 タイムスタンプ

全ての発行CAのコンポーネントは常時原子時計又はネットワーク タイム プロトコル（NTP）のような時刻サービスと同期するものとする。信頼できる時刻の提供に専門の権威（タイム スタンピング オーソリティ等）が使用される可能性も有る。タイムサービス由来の時刻は以下の時刻を構成するのに使われるものとする。

- 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。時刻の調整は監査対象イベントとなる。

7.0 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

認証局は、2.2 項、6.1.5 項、及び 6.1.6 項に規定の技術要件へ準拠するものとする。
認証局は、CSPRNG からの最低 64 ビットのアウトプットを含む、0 よりも大きく 2^159 未満である、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。

7.1.1 バージョン番号

証明書の形式は、X.509 バージョン 3 に従うものとする。

7.1.2 証明書の内容と拡張

認証局は以下の通り、RFC5280 及び現在の CA/B Forum の要件に従うものとする。

証明書の種類	要求事項	該当箇所
TLS	Baseline Requirements for TLS	7.1.2
EV TLS	EV Guidelines	9
Code Signing and EV Code Signing	Baseline Requirements for Code Signing	7.1.2
S/MIME BR	Baseline Requirements for S/MIME	7.1.2

例外については、当 CP 又は当 CP を実施する CPS へ記載することができる。

7.1.3 アルゴリズム識別子

発行 CA は、下記の OID（管理情報識別子）に示されるアルゴリズムでデジタル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。

発行 CA は、該当する CA/B Forum の要件の 7.1.3 項に従い、署名アルゴリズム及びエンコードを用いるものとする。

7.1.4 名前形式

発行 CA は、RFC5280 に従う名前形式及び該当する CA/B Forum の要件の 7.1.4 項に準拠して証明書を発行する。

7.1.5 名前制約

認証局は、該当する CA/B Forum の要件の 7.1.5 項に準拠するものとする。

7.1.6 証明書ポリシー識別子

認証局は、以下の要件を適用するものとする。

証明書の種類	要求事項	該当箇所
TLS	Baseline Requirements for TLS	7.1.6
EV TLS	EV Guidelines	9.3.2
Code Signing and EV Code Signing	Baseline Requirements for Code Signing	7.1.6
S/MIME BR	Baseline Requirements for S/MIME	7.1.6

注：2023 年 9 月 1 日以降、S/MIME に関する Baseline Requirements の適用範囲にある全ての S/MIME 証明書は、当要件への準拠を表明するために、S/MIME BR ポリシー識別子を含めなければならない。2023 年 9 月 1 日以前より、S/MIME BR ポリシー識別子を含めることができる。

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

認証局は、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　適格証明書に関する特則

適格証明書を発行する認証局は、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ものとする。

7.2　CRL プロファイル

7.2.1　バージョン番号

発行 CA は RFC5280 に従い、バージョン 2 の CRL を発行するものとする。

7.2.2　CRL 及び CRL エントリ拡張子

認証局は、該当する CA/B Forum の要件の 7.2.2 項に従うものとする。

7.3　OCSP プロファイル

認証局は、該当する CA/B Forum の要件の 7.3 項に従うものとする。
発行 CA は、RFC2560 又は 5019 に従い、OCSP のレスポンダを提供するものとする。

7.3.1　バージョン番号

（規定なし）

7.3.2　OCSP 拡張

（規定なし）

8.0　準拠性監査及びその他の評価

認証局は如何なる時においても、

1. 自己が事業を営む全ての法域において、自己の事業及び自己が発行する証明書に適用される全ての法律に従って、証明書を発行し、PKI を運営するものとする。
2. 証明書の種類に適用される要件に準拠するものとする。
3. 本項に定める監査要件に準拠するものとする。
4. 当該法域の法律によって証明書の発行に関して認可が要求される場合、当該法域において 認証局としての認可を取得しているものとする。

8.1 評価の頻度及び状況

認証局は、該当する CA/B Forum の要件の 8.1 項及び、該当する eIDAS/UK eIDAS 規制の要件に従うものとする。

8.2 評価者の身元及び能力

CAへの監査は公認監査人により行なわれるものとする。公認監査人とは、以下の条件及び技能を総合的に有する自然人、法人、又は複数の自然人若しくは法人を意味する。

1. 監査対象からの独立性を有する者
2. 適格監査スキーム(8.4項を参照)に明記される条件において、監査を遂行できる能力を有する者
3. PKI 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者
4. (何らかの ETSI 標準に従って実施される監査において、) ISO 17065に従って認証されている、且つ ETSI EN 319 403 又は ETSI EN 319 403-1に規定の要件を適用している者
5. (WebTrust 標準に従って実施される監査において、) CPA Canada より WebTrust に関して認可されている者
6. 法律、公的規定又は職業倫理規定により認定されている者
7. 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者

eIDAS 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ものとする。

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ものとする。

8.3 評価者と被評価者との関係

発行 CA は、発行 CA 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しなければならない。

8.4 評価対象項目

監査は、評価が作成された監査スキームの定める条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。

8.5 結果が不備である場合の対応

準拠性に不備があると提示された場合、相互認証発行 CA を含む、技術制約を受けない発行 CA は何れも同様に、外部の監査人によって作成される適切な修正計画により不備を除去するために対応しなければならない。

8.6 結果についての連絡

認証局は、該当する CA/B Forum の要件の 8.6 項に従うものとする。

監査結果は、分析及び是正措置による不備の解消のために、GlobalSign Policy Authority に報告されなければならない。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

認証局は、該当する CA/B Forum の要件の 8.7 項に従うものとする。

認証局は、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、

発行 CA の 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。

8.8　委任された第三者へのレビュー

8.4 項に規定される基準を満たす年次監査を受ける委任された第三者、エンタープライズ RA、及び技術的制限のある下位認証局を除き、認証局は、委任された第三者の業務及び手続が、該当する CA/B Forum の要件並びに関連する CP 及び/又は CPS に準拠していることを確認するものとする。認証局は、被委任当事者の義務を文書化し、被委任当事者がこれらの義務を遵守していることを、少なくとも年 1 回モニタリングするものとする。

9.0　その他ビジネス及び法的事項

9.1　料金

9.1.1　証明書発行や更新料金

発行 CA 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。また発行 CA は、Re-key についても同様に請求できるものとする。料金及び関連する情報、条件は申請者に対して明確に提示されるものとする。

9.1.2　証明書アクセス料金

発行 CA 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、発行 CA 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

発行 CA 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

発行 CA は利用者に対し、返金ポリシーを提案できる。返金ポリシーの行使を選択する利用者は、その選択時点で全ての発行済み証明書を失効していなければならない。

9.2　財務上の責任

9.2.1　保険の適用範囲

名称制約が課されていない場合の発行CAに関しては、少なくとも200万米ドル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又は保証

発行 CA は利用者に対して保証ポリシーを提供することができる。

9.3 業務情報の機密性

9.3.1 機密情報の範囲

発行 CA は、CPS において機密情報の範囲を定義づけるものとする。

9.3.2 機密情報の範囲外に属する情報

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

発行 CA は機密情報を保護するものとする。発行 CA は従業員、代理人、及び契約社員に対する研修と契約によって、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

認証局はデータ保護の実践に関する情報を提供するプライバシーポリシーを公表するものとする。当プライバシーポリシーは、認証局がどのように個人情報を収集、利用、共有、保存、及び消去又は保持するか、並びにプライバシーの権利を行使するにあたっての連絡先を提示する。

9.4.2 個人情報として取り扱われる情報

認証局又は RA は、証明書の内容として公開されていない個人に関する全ての個人情報を、 個人情報として扱うものとする。これには、仮名とサブジェクト個人の実際の身元を結びつける情報が含まれる。

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

認証局又は RA は、適切な保護措置及び合理的な程度の注意をもって、個人情報を保護するものとする。認証局又は RA は、認証局又は RA に代わって個人情報を取り扱うサービスプロバイダにも、同水準の保護を要求するものとする。

9.4.5 個人情報使用についての通知及び同意

証明書の発行及び管理に関連するサービス提供以外の目的で個人情報を利用する前に、 認証局又は RA は、サブジェクトの個人に適切な通知を行い、必要な同意を得るものとする。
認証局又は RA に代わって個人情報を取り扱うサービスプロバイダに対しても、同水準の手続を要求するものとする。

9.4.6 法的又は管理処理に従う開示

認証局は、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

発行 CA 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それを正当に保持するところの利用者の財産権に属する。発行 CA 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。

9.6 表明保証

9.6.1 認証局の表明保証

証明書を発行することにより、認証局は以下の証明書受益者に対してここに記載される保証を行うものとする：

1. 証明書の利用約款又は利用規約の当事者である利用者。
2. ルート認証局がそのルート認証局証明書を当該アプリケーションソフトウェアサプライヤが配布するソフトウェアに含める契約を締結している全てのアプリケーションソフトウェアサプライヤ、及び
3. 有効な証明書に合理的に依拠する全ての依拠当事者。

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

証明書の保証においては、以下をはじめとする CA/B Forum の要件にある項目を、具体的に記載するものとする。

証明書の種類	要求事項	該当箇所
TLS	Baseline Requirements for TLS	9.6.1
EV TLS	EV Guidelines	7.1
Code Signing and EV Code Signing	Baseline Requirements for Code Signing	9.6.1
S/MIME BR	Baseline Requirements for S/MIME	9.6.1

9.6.1.1. NAESBE（北米エネルギー規格委員会）証明書に対する認証局の表明保証

NAESB WEQ-PKI（NAESB 認証局ルール）は、NAESB 発行 CA が以下の項目を保証することを要求している：

- NAESB Business Practice Standardsに基づき、証明書を発行、また管理すること
- 利用者の識別、及び証明書発行の際、NAESB Business Practice Standardsの全要件に従っている
- 証明書において検証した事項において、RAが知得した、或いは当然知られるであろう誤記や誤りがないこと
- 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 Business Practice Standardsの不可欠要件を満たしていること

9.6.2 RA の表明保証

認証局は全 RA に対し、当該 RA が本 CP 及び関連する CPS に準拠するよう要求するものとする。RA は、当 CPS 又は RA 契約書内に、さらに付加的な表明事項を含めることができるものとする。。

9.6.3 利用者の表明保証

認証局は、利用契約又は利用規約の一部として、申請者に対し、認証局及び証明書受益者の利益のために、本項に記載される約束及び保証を行うことを要求するものとする。

認証局は、証明書の発行に先立ち、認証局及び証明書受益者の利益のために、申請者から以下の何れかを取得するものとする：
1. 申請者が認証局との利用契約に同意すること
2. 申請者が利用規約に同意すること

認証局は、各利用契約又は利用規約が申請者に対して法的拘束力があることを保証するプロセスを導入するものとする。何れの場合も、証明書申請に基づき発行される証明書に利用契約を適用しなければならない。認証局は、係る契約が法的拘束力を有すると判断した場合に限り、電子的又は「クリックスルー」契約を使用することができる。各証明書申請に個別の契約書を使用することも、将来の複数の証明書申請及びその結果生じる証明書について単一の契約を使用することもできる。但し、認証局が申請者に発行する各証明書には、利用契約又は利用規約が明確に適用されることを条件とする。

利用契約又は利用規約には、申請者自身 (又は、再委託やホスティングサービスの関係にある申請者の代表者若しくは代理人) に対して、以下の CA/B Forum の要件の義務及び保証を課す規定が含まれていなければならない。

証明書の種類	要求事項	該当箇所
TLS	Baseline Requirements for TLS	9.6.3
EV TLS	EV Guidelines	7.2
Code Signing and EV Code Signing	Baseline Requirements for Code Signing	9.6.3

S/MIME BR	Baseline Requirements for S/MIME	9.6.3

9.6.3.1 NAESB（北米エネルギー規定委員会）の利用者

NAESB WEQ PKI Standard に加入する利用者は 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 Standard 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、電気再販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、NAESB WEQ PKI Standard に定められたエンドエンティティの責任を全て果たす必要がある。

各利用者組織は NAESB WEQ PKI Standard に定められている以下の責任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 WEQ-012 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。

- 利用者は、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。
- 利用者は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。
- 利用者が利用する認証局のCPSを認証局の認める業界標準に照らして評価していること。

利用者は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。

利用者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 を介して、利用者自らが GlobalSign を正式な認定認証局として選択したことに相違ないことを明らかにすること。
- GlobalSign がエンドエンティティに安全な電子通信を提供するために必要な GlobalSign の CPS に規定されている通り、GlobalSign との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 CP において GlobalSign が要求し、規定す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手続き
    - 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

9.6.4 依拠当事者の表明保証

(規定なし)

9.6.5 その他の関係者の表明保証

コードサイニング証明書及び EV コードサイニング証明書については、認証局は、各署名サービスが疑わしいコードに署名したことを (手段を問わず) 認識した場合、認証局に通知することを各署名サービスに契約上義務付けなければならない。
署名サービスの秘密鍵又は秘密鍵の有効化データが危殆化した場合、又は危殆化したと思われる場合、影響を受ける証明書の失効を要求し、認証局に直ちに通知するよう署名サービスに要求しなければならない。

認証局は、署名サービスからの要求があった場合、又は署名サービスが秘密鍵の危殆化を確認した後 24 時間以内に認証局に通知しなかったと認証局が判断した場合、影響を受ける証明書を失効しなければならない。

署名サービスは、以下の事項に関して利用者の約束を得なければならない：
1. 当該署名サービスは、利用約款/利用規約、該当する CA/B Forum の要件、及び全ての適用法に準拠する、認可された目的のみに使用すること。
2. 疑わしいコードが含まれていることを知りながら、コード署名のためにソフトウェアを提出しないこと。
3. コード署名のために署名サービスに提出されたコードに疑わしいコードが含まれていることが発見された場合、（どのような方法であれ）署名サービスに通知すること。

9.7 保証の免責事項

発行 CA は以下については保証しないことを CPS において明言するものとする。

- 証明書に含まれる、検証不能な情報箇所の正確性。但し、本 CP 内の以下の条項、及びワランティーポリシーにおいて関連製品の説明に規定があり、これに該当する場合を除く。
- 無料の、テスト配布の、又はデモ用の証明書に含まれる如何なる情報の正確性、真正性、完全性又は一致性。

9.8 責任制限

委任された業務については、認証局及び委任された第三者の間において、以下のように契約上の責任を割り当てることができるものとする。但し認証局は、業務が委任されていない場合と同様に、適用される要件に従って、全ての委任された第三者による履行に対する全責任を負うものとする。

認証局が、適用される要件並びにその CP 及び/又は CPS に準拠して証明書を発行及び管理している場合、認証局はその CP 及び/又は CPS に明記されている以上の証明書の使用又は依拠の結果被ったいかなる損害についても、証明書受益者又はその他の第三者に対して責任を否認することができる。

認証局が、適用される要件並びにその CP 及び/又は CPS に準拠して証明書を発行又は管理していなかった場合、認証局は、請求を理由づける事実又は関係する法理論に拘わらず、係る証明書の、認証局が望む適切な手段による使用又は依拠の結果被った全てのクレーム、損失又は損害について、利用者及び依拠当事者に対する責任を制限するよう求めることができる。認証局が、適用される要件又はその CP 及び/又は CPS に準拠して発行又は管理されていない証明書に対する責任を制限することを選択した場合、認証局は、認証局の CP 及び/又は CPS に責任制限を記載するものとする。

認証局は、以下の CA/B Forum の要件にある責任制限に従うものとする：

証明書の種類	要求事項	該当箇所
TLS	Baseline Requirements for TLS	9.8
EV TLS	EV Guidelines	18
Code Signing and EV Code Signing	Baseline Requirements for Code Signing	9.8
S/MIME BR	Baseline Requirements for S/MIME	9.8

認証局の全責任は、その CPS に規定されるワランティーポリシー及び制限事項に従って制限されるものとする。

9.9 補償

利用者及び依拠当事者に対する認証局の責任の制限に拘わらず、認証局は、ルート認証局証明書の配布に同意したアプリケーションソフトウェアサプライヤが、適用される CA/B Forum の要件に基づく認証局の義務又は潜在的な責任、或いは証明書の発行若しくは維持、又は依拠当事者若しくはその他による証明書の信頼に起因して存在しうる認証局の義務又は潜在的な責任を引き受けないことを理解し、これを認めるものとする。従って、認証局が政府機関である場合を除き、認証局は、認証局が発行した証明書に関連してアプリケーションソフトウェアサプライヤが被った全てのクレーム、損害、及び損失について、請求を理由づける事実や法理論に拘わらず、各アプリケーションソフトウェアサプライヤを防御、補償、及び免責するものとす

る。但し、認証局が発行した証明書に関連して当該アプリケーションソフトウェア供給者が被ったクレーム、損害、損失が、当該アプリケーションソフトウェア供給者のソフトウェアが、有効な証明書を信頼できないものとして表示したこと、又は(1)有効期限が満了した証明書、若しくは(2)失効した証明書（但し、失効ステータスが認証局からオンラインで現在入手可能であり、アプリケーションソフトウェアが当該ステータスを確認しなかったか、失効ステータスの表示を無視した場合に限る）を信頼できるものとして表示したことに直接起因するものである場合には、当該クレーム、損害、損失は適用されない。

9.9.1 発行者 CA による補償

発行 CA の補償責任は、CPS、関連利用契約、又は第三者受益者に対する責任を含むところの依拠当事者規約において定められなければならない。

9.9.2 利用者による補償

発行 CA は、利用者による補償責任について、 CPS、及び関連利用契約の中にその関連規定を明記するものとする。

9.9.3 依拠当事者による補償

発行 CA は、依拠当事者による補償責任について、CPS の中にその関連規定を明記するものとする。

9.10 期間及び終了

9.10.1 期間

本 CP は、GlobalSign によりそのウェブサイト又はリポジトリにおいて、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。変更内容は、公表された時点で直ちに有効となる。

9.10.3 終了の効果と存続

発行 CA は、本 CP の終了に関する条件及びその影響については、適切なリポジトリを介して伝達するものとする。

9.11 関係者への個別通知及び伝達

GlobalSign は、本 CP 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こととする。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 CP 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 365 日毎に見直されるが、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 Policy Authority により確認、承認される。
本 CP 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

発行 CA は、本 CP 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 CP 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。

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勧告等の方法は全て該当する）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に努め、当該紛争点について GlobalSign へ通知することに同意するものとする。

紛争の通知の受領後、GlobalSign は GlobalSign の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 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、本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 CP 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 CP 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 の製品及びサービスに関し、本 CP 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、ベルギー国法が適用される。

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 CA、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

発行 CA は、全ての証明書発行に携わる RA に対し、本 CP 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 CP 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 CP の、責任の制限に関する条項も含むところの何れかの条項が、無効、或いは法的強制力が失効となった場合であっても、本 CP 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 CP の各条項は、分離可能であり、如何なるその他の条項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(弁護士の費用及び権利放棄)

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 CP の何れかの規定の執行を行わなかった場合でも、GlobalSign はそ

の後の同規定の執行、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 の合理的な管理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は、その責任を負わないものとする。

9.17 その他の規定

（規定なし）

（以下空白）