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

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

Date: April, 2019

Version: v.9.1

Legal-JP

電子署名者 : Legal-JP
日付 : 2020.02.17 18:00:33 +09'00'

目次

修正履歴

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

V8.4	01/17/17	Giichi Ishii Carolyn Oldenburg Lila Kee	CA/B Forum Ballot 173 Removal of Root R2 & R4 Addition of Minimum Requirements for Code Signing Certificates
V8.5	08/07/17	Giichi Ishii Carolyn Oldenburg Lila Kee Doug Beattie	Updates for AATL Digital Signing Service Added CAA record checking requirement Annual update/review to fix bugs
V8.6	15/12/17	Giichi Ishii Carolyn Oldenburg Lila Kee Doug Beattie Simon Labram	Updates related to Annual BR assessment
V8.7	03/04/18	Doug Beattie Lila Kee	Max SSL validity set to 825 days Specified that GlobalSign no longer generates keys for SSL certificates Updates for NAESB identify requirements
V8.8	06/15/18	Various authors	Updates for Qualified Certificates Removed Method #5 to comply with BR domain validation practices.
V8.9	10/11/2018	Giichi Ishii Arvid Vermote Doug Beattie Carolyn Oldenburg	Updates to revocation timelines in accordance with CABF Ballot SC6 Made a variety of definition/acronym updates for clarification
V9.0	03/12/19	Arvid Vermote Paul Brown Jun Hosoi Doug Beattie Carolyn Oldenburg	Updated roles requiring separation of duties Added new ICAs for AATL and Timestamping Added new Email Domain Validation methods and definitions Added new Phone Domain Validation methods and definitions Added new IoT policy OIDs
V9.1		Arvid Vermote Paul Brown Jun Hosoi Doug Beattie Carolyn Oldenburg	Added new GlobalSign R46/E46 Root Certificates Added new Private Client Certificate Policy OID Support for Qualified Time Stamping and Qualified Web Authentication Certificates Changed “re-key” definition to match WebTrust

前提確認事項

本 GlobalSign CPS は、以下に準拠する：

- 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

本 GlobalSign CPS は、現時点における以下の外部要求事項に準拠する：

- AICPA/CICA, WebTrust 2.1 Program for Certification Authorities
- AICPA/CICA, WebTrust for Certification Authorities – Extended Validation Audit Criteria
- CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
- CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates
- CA/B Forum Network and Certificate System Security Requirements
- CA/B Forum EV Code Signing Certificate Guidelines
- Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at https://aka.ms/csbr.
- Browsers’ Root programs

本文書及び上記外部要求の間に不一致があった場合、外部要求事項が本文書に優先して適用される。
GlobalSign®及び GlobalSign のロゴは、GMO グローバルサイン株式会社(GlobalSign K.K.)の登録商標である。

1. はじめに

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

本 CPS は、「共通のセキュリティに関する要求事項を持つ特定の団体もしくはアプリケーション類にデジタル証明書を発行するための手続き」を定めるものである。本 CPS は 2003 年 11 月に Internet Engineering Task Force(以下、「IETF」という)が発行した RFC 3647 に定められた構成に従って記述する。(RFC 3647 の発行に伴い RFC 2527 は廃止されている。)この RFC は、電子署名と証明書の管理における標準的な業務手続きについて記述した公式の手引きである。本 CPS において、章・節などは RFC 3647 の構成に準拠して設けているが、そこで扱うべき内容が GlobalSign nv/sa 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。GlobalSign は、URL の www.cabforum.org.に公開している「Publicly-Trusted Certificates」の中にある発行と管理の規定に関して、CA ブラウザフォーラム（以下「CA/B Forum」）の CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (the “Baseline Requirements”), the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (the “EV Guidelines”), CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates (the “EV Code Signing Guidelines”)の最新版に準拠するものとする。もし本 CPS の解釈と Baseline Requirements の最新版の解釈との間に不一致があった場合は、Baseline Requirements を優先するものとする。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。また、証明書に記載された情報を信頼し依拠する者(以下、「依拠当事者」という)は、本 CPS を参照することで、認証業務手続きをあらかじめ知ることができる。本 CPS が準拠するその他の規格は前提確認事項の項に記載されている。

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

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

本 CPS は最終であり、GlobalSign nv/sa (所在地：Martelarenlaan 38, 3010 Leuven、VAT 登録番号：BE 0459.134.256、商業登記番号：BE 0.459.134.256 RPR Leuven の会社法人。以下、「GlobalSign」という)と、本 CPS に基づいて認証局が提供する認証サービスを利用する利用者、及び依拠し、又は依拠しようとする依拠当事者を拘束する。

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

1.1. 概要

本 CPS は GlobalSign が発行する証明書階層全てに適用されるものであり、その目的は GlobalSign が採用する証明書管理の実務手続きを説明し、GlobalSign が規定する要件並びに上述の業界標準の要件の双方に準拠して電子証明書が発行されていることを証することである。eIDAS Regulation (Regulation (EU)N910/2014) は、認証及び否認防止の目的で使用される電子署名を承認した。これに基づき、GlobalSign はそのサービスの提供にあたり同法の適用される項の規定の範囲で業務を行っている。本 CPS

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

PersonalSign 1	保証のレベルが低い個人向け証明書
PersonalSign 2	保証のレベルが中程度の個人向け証明書
PersonalSign 2 Pro	保証のレベルが中程度で所属する職業・組織の情報を含む個人向け証明書
PersonalSign 2 Pro DepartmentSign	保証のレベルが中程度で、機械、装置、部署、或いは所属する職業・組織の情報・役職の情報を含む個人向けの証明書
PersonalSign 3 Pro	保証のレベルが高く、所属する職業・組織の情報を含む個人向け証明書
PersonalSign Partners	PersonalSign 2 Pro、或いは PersonalSign 2 Pro DepartmentSign を発行するトラストアンカーとして顧客の注文に応じて構築されるプライベート認証局
Noble Energy	保証のレベルが中程度で、所属する職業・組織の情報を含む、機器、装置、部署又は役職の証明書
IntranetSSL	パブリックな GlobalSign のルートにつながらない、ウェブサーバを認証する証明書
DomainSSL	ウェブサーバを認証する証明書
AlphaSSL	ウェブサーバを認証する証明書
OrganizationSSL & ICPEdu	ウェブサーバを認証する証明書
ExtendedSSL [1]	ウェブサーバを認証する証明書
GlobalSign Timestamping	時刻情報の発行元を認証する証明書
AATL	ハードウェアにインストールされ、Adobe AATL 及び Microsoft Office 文書に中程度の保証を提供する個人向け証明書
Code Signing [2]	データオブジェクトを認証する証明書
Extended Validation Code Signing [1]	データオブジェクトを認証する証明書
North American Energy Standard Board (NAESB) Authorized CA Certificates	北米エネルギー規格委員会の指定を受け権限を与えられた認証局が発行する、保証レベルが最小限、低、中、高いずれかの個人、役職、サーバ、もしくはデバイス証明書
PDF Signing for Adobe CDS [3]	Adobe Root CA にチェーンされ、保証レベルが中程度のハードウェアに搭載された証明書であり、所属する企業組織の情報を含む場合がある
PersonalSign for Adobe CDS	Adobe PDF で作成された文書に署名することを目的に、組織内の自然人(個人)に所属する企業組織の情報を含まず発行される証明書

[1] この証明書は CA/B Forum の EV ガイドライン及び EV Code Signing のガイドラインに従って発行・管理される。 その他の証明書については、CA/B Forum の Baseline Requirements に従って発行・管理され、その中でもし指定されていれば、1.2 項で詳述する通り、CA/B Forum ポリシーOID（識別子）を証明書内に記載する。
[2] この証明書は CA Security Council の Code Signing のガイドラインに従って発行・管理される。
[3] この証明書は、Adobe Systems 社証明書ポリシー(http://www.adobe.com/misc/pdfs/Adobe_CDS_CP.pdf)に従って発行・管理される。

PersonalSign Pro for Adobe CDS	Adobe PDF で作成された文書に署名することを目的に、所属する企業組織の情報を含み発行される個人向け証明書
DepartmentSign for Adobe CDS	Adobe PDF で作成された文書に署名することを目的に、所属する企業組織の情報・役職の情報を含む証明書
Trusted Root/Intermediate signing for Adobe/AATL	GlobalSign の認証局チェーンに組み込むための中間 CA 認証局
Timestamping for Adobe CDS	時刻情報の発行元を認証する証明書
Test Digital Certificate for Adobe CDS	ハードウェアの保証を要しないテストもしくはデモを目的とした証明書
Hosted Root	GlobalSign が、ユーザの代わりにルート CA の秘密鍵及び証明書を維持、管理し、また、そのルートがルートストアに搭載される時までクロス証明書を提供するために用いるサービス。 当該ユーザはその期間内に当該ユーザの名前で WebTrust 監査を通すこととなる。
Qualified Certificates for Electronic Signatures	電子署名を提供するために用いられる、eIDAS に準拠する適格証明書
Qualified Certificates for Electronic Seals	e シールを提供するために用いられる、eIDAS に準拠する適格証明書
Qualified Web Authentication Certificates	Web 上での認証(SSL)に用いられる、eIDAS に準拠する適格証明書
Certificates for Qualified Time Stamping	eIDAS に準拠する適格タイムスタンプに署名するために用いられる証明書

GlobalSign 証明書は、以下のいずれの目的にも使用することができる。

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

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

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

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

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

その他の関連文書には以下のものがある。

- GlobalSign から提供される保障に関する事項を取り扱う GlobalSign ワランティーポリシー
- 個人情報保護に関する GlobalSign プライバシーポリシー

- GlobalSign のルート証明書の信頼対象を取り扱う GlobalSign CP

GlobalSign の発行する証明書の利用者、依拠当事者は、GlobalSign が発行する証明書を信頼するため、また GlobalSign の活動について情報を得るために、本 CPS を参照すべきである。階層全体の証明書チェーンの信頼性を確認することも重要であり、これにはルート CA 証明書、その他のあらゆるオペレーショナル・ルートの証明書が含まれる。本 CPS における GlobalSign の表明にもとづき信頼性を確認すること。

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

1.1.1. 証明書名称

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

GlobalSign パブリックルート証明書
- GlobalSign Root CA – R1 (シリアル番号：040000000001154b5ac394)
- GlobalSign Root CA – R3 (シリアル番号：0400000000121585308a2)
- GlobalSign Root CA – R5 (シリアル番号：605949e0262ebb55f90a778a71f94ad86c)
- GlobalSign Root CA – R6 (シリアル番号：45e6bb038333c3856548e6ff4551)
- GlobalSign Root CA – R7 (シリアル番号：481b6a06a6233b90a629e6d722d5)
- GlobalSign Root CA – R8 (シリアル番号：481b6a09f4f960713afe81cc86dd)
- GlobalSign Root CA – R46 (シリアル番号：11d2bbb9d723189e405f0a9d2dd0df2567d1)
- GlobalSign Root CA – E46 (シリアル番号：11d2bbba336ed4bce62468c50d841d98e843)

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

非パブリックのルート証明書
- GlobalSign Non-Public Root CA – R1 (シリアル番号：467437789376ad2301cdf9ba9e1d)
- GlobalSign Non-Public Root CA – R3 (シリアル番号：4674377c0fba34f6f1c3dcb75d3f)

1.1.1.1. 下位発行認証局証明書の公表

ブラウザのルートプログラムは、(nameConstraints 及び拡張鍵用途への制約を通して)技術的に制約されていない全ての下位 CA が公表されることを要求している。パブリックルート CA 証明書(R1, R3, R5, R6, R7, R8, R46, E46)に直接的又は経由する形でチェーンする、現時点で利用されている全ての下位 CA 証明書を Common CA Database (CCADB)に列挙する。SHA1 の指数、有効期限、及びダウンロード及び点検を可能にする為のリンクも併記する。失効されずにいる全ての利用されていない証明書は、適用されるルートプログラムで要求されているように、バグレポートや電子メールを介してルートプログラムに半年ごとに報告される。失効した下位認証機関(CA)証明書も、同様に報告される。報告の時期は、定期的な失効の場合は失効から短期間のうち、セキュリティ上の懸念によって失効された場合は失効直後である。

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

- GlobalSign Trusted Platform Module Root CA (シリアル番号：040000000000120190919AE)
- GlobalSign Trusted Platform Module ECC Root CA (シリアル番号：45dc9c8c1515db59d0464b9d79e9) [4]

[4] R1, R3, R5, R6, R7, R8, R46, E46 及び TPM/TPM ECC のルートは、集合的に「GlobalSign ルート証明書」と称呼される。

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

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

1.2. 文書名称と識別子

本書は GlobalSign CPS である。

GlobalSign nv/sa(GlobalSign)のオブジェクト識別子(以下、「OID」という)は、ISO (1)、識別された組織(2)、DoD (3)、インターネット (4)、民間 (5)、企業 (1)、GlobalSign nv/sa (4146)、すなわち 1.3.6.1.4.1.4146 である。GlobalSign は本 CPS が対象とするさまざまな証明書、文書に対し、次の OID を付与する。

Extended Validation	
1.3.6.1.4.1.4146.1.1	Extended Validation Certificate Policy – SSL
1.3.6.1.4.1.4146.1.1.1	Qualified Certificates under eIDAS Regulation – Qualified Web Authentication Certificates (QWAC)
1.3.6.1.4.1.4146.1.1.2	Qualified Certificates under eIDAS Regulation – Qualified Web Authentication Certificates (QWAC) – PSD2
1.3.6.1.4.1.4146.1.2	Extended Validation Certificate Policy – Code Signing
Domain Validation	
1.3.6.1.4.1.4146.1.10	Domain Validation Certificate Policy
1.3.6.1.4.1.4146.1.10.10	Domain Validation Certificate Policy – AlphaSSL
Organization Validation	
1.3.6.1.4.1.4146.1.20	Organization Validation Certificate Policy
Intranet Validation	
1.3.6.1.4.1.4146.1.25	IntranetSSL Validation Certificate Policy
Timestamping	
1.3.6.1.4.1.4146.1.30	Timestamping Certificate Policy
1.3.6.1.4.1.4146.1.31	Timestamping Certificate Policy – AATL
1.3.6.1.4.1.4146.1.32	Time Stamping Certificate Policy – Certificates for Qualified Time Stamping (QTS) under eIDAS regulation
Client Certificates	
1.3.6.1.4.1.4146.1.40	Client Certificate Policy (Generic)
1.3.6.1.4.1.4146.1.40.10	Client Certificate Policy (EPKI – Enterprise PKI)
1.3.6.1.4.1.4146.1.40.20	Client Certificate Policy (JCAN – Japan CA Network)
1.3.6.1.4.1.4146.1.40.30	Client Certificate Policy (AATL)
1.3.6.1.4.1.4146.1.40.40	Client Certificate Policy (EPKI for private CAs)
1.3.6.1.4.1.4146.1.40.50	Client Certificates Private Hierarchy
Qualified Certificates under eIDAS	
1.3.6.1.4.1.4146.1.40.35	eIDAS Qualified Certificate (Generic)
1.3.6.1.4.1.4146.1.40.35.1	Qualified Certificates for Electronic Seals (Legal Persons)
1.3.6.1.4.1.4146.1.40.35.1.1	Qualified Certificates for Electronic Seals (Legal Persons) - PSD2
1.3.6.1.4.1.4146.1.40.35.2	Qualified Certificates for Electronic Signatures (Natural Persons)

上記の識別子に加え、これらの識別子に加え、itu-t(0)、識別された組織(4)、etsi(0)、その他の証明書ポリシー(2042)、ポリシー識別子(1)、ncpplus(2)に準拠する全ての証明書は、以下の追加識別子を含む:

0.4.0.194112.1.2 QCP-n-qscd: QSCD 内に保管され、公開鍵及びそれに紐づく秘密鍵を保持する自然人に発行された、 EU 適格証明書の証明書ポリシー(1.3.6.1.4.1.4146.1.40.35.2 と紐づく)
0.4.0.194112.1.3 QCP-l-qscd: QSCD 内に保管され、公開鍵及びそれに紐づく秘密鍵を用いて法人に発行された、 EU 適格証明書の証明書ポリシー(1.3.6.1.4.1.4146.1.40.35.1 と紐づく)

Code Signing	
2.23.140.1.4.1	Code Signing Minimum Requirements
1.3.6.1.4.1.4146.1.50	Code Signing Certificates Policy

上記 OID を含む GlobalSign が発行した証明書は、Code Signing Minimum Requirement に従って発行・管理される。

CA チェーンとクロス署名

1.3.6.1.4.1.4146.1.60	CA Chaining Policy – Trusted Root and Hosted Root
1.3.6.1.4.1.4146.1.60.1	CA Chaining Policy – Trusted Root (Baseline Requirements Compatible)

その他

1.3.6.1.4.1.4146.1.26	Test Certificate Policy – 正確な情報を含んでいない可能性があるため、信用すべきではない。テスト証明書は証明書のテストとインテグレーションのために使用される。
1.3.6.1.4.1.4146.1.70	High Volume CA Policy
1.3.6.1.4.1.4146.1.80	Retail Industry Electronic Data Interchange Client Certificate Policy
1.3.6.1.4.1.4146.1.81	Retail Industry Electronic Data Interchange Server Certificate Policy
1.3.6.1.4.1.4146.1.90	Trusted Root TPM Policy
1.3.6.1.4.1.4146.1.95	Online Certificate Status Protocol Policy

Internet of Things (IoT)

1.3.6.1.4.1.4146.1.100	Internet of Things Device Certificates Policy

上記の識別子に加えて、NAESB Business Practice Standards に準拠する全ての証明書には、以下の識別子のうち 1 つが追加で含まれる。

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
2.16.840.1.114505.1.12.4.2	NAESB High Assurance

上記の識別子に加えて、Baseline Requirements に準拠する全ての証明書には、以下の識別子を含む。

2.23.140.1.1	Extended Validation Certificate Policy
2.23.140.1.2.1	Domain Validation Certificate Policy
2.23.140.1.2.2	Organization Validation Certificate Policy

1.3. PKI における関係者

1.3.1. 認証局

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

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

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

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

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

1.3.2. 登録局(RA)

登録局（RA）は証明書の申請者を識別及び認証することに加えて、証明書の失効、再発行及び更新（Re-key と呼ぶこともある）の要求を受理し、それを転送したりする。GlobalSign はこの RA 業務を行うことができる組織であり、この場合には以下の各業務に責任をもって当たる。

- 証明書申請を受理し、評価し、当該証明書申請の登録を承認又は却下する。
- 利用者を証明書サービスへ登録する。
- (要求された証明書タイプに応じた)利用者の本人確認を行う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チェックし、本人確認を行う。
- 申請の承認後、多要素認証のプロセスに基づいて証明書の発行を要求する。
- GlobalSign の、関連する下位発行 CA、或いは下位のパートナー発行 CA からの要求を受け証明書失効手続きを取る。

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

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は、依拠当事者には、そうしたサードパーティの CPS を参照し、追加の情報を確認することを助言する。

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

GlobalSign は、そのエンタープライズ RA が属する組織からの証明書申請を検証するために、エンタープライズ RA を指定することができる。EPKI(マネージド PKI)及びマネージド SSL(マネージド SSL) が利用するエンタープライズ RA では、事前審査の上 GlobalSign のシステムに登録された利用者の組織情報に従って、証明書の発行が制限される。エンタープライズ RA が組織を代表するためには、以下の要件が GlobalSign によって検証される。

1. 要求された FQDN は、エンタープライズ RA の検証済みドメイン名内にあり、

2. 証明書リクエストに FQDN 以外のタイプのサブジェクト名が含まれている場合、GlobalSign は、その名前が委任された企業又は委任された企業の関連会社の名前であること、又は委任された企業が名前付きサブジェクトの代理人であることを確認する。

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

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

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

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

1.3.2.2 適格証明書に関する RA 特有の要求事項

RA が eIDAS Regulation の要求事項によって認証されるという条件の下で、GlobalSign は、組織の識別情報の検証及び個人の身元証明の双方を RA に委任することができる。

当該条件は以下の場合に充足されると考えられる。

- 委任された RA が、GlobalSign の CP・CPS 上の適格証明書の電子署名における審査について記載されている章に従うことで、利用者情報が適切に認証されているか確認する監査に合格する。
    - GlobalSign は、前回サンプルがとられた直後に委任されたローカル登録局によって審査された、少なくとも 1 つ以上又は１％以上の適格証明書を任意に抽出し、四半期ごとに監査することを通し、CP・CPS をそのローカル登録局が遵守しているか監視しなければならない。
- RA は GlobalSign に、eIDAS 準拠を査定するレポートと同等の監査レポートを提出する。eIDAS 準拠を査定するレポートは GlobalSign に受領される前に、(eIDAS の規則が規定する)Conformity Assessment Body によって確認される。その評価の際、Conformity Assessment Body は以下を考慮する。
    - RA に関する eIDAS の要求事項と同等であるかどうか
    - 監査の範囲及び結論

ほとんどの組織は従業員、代理店、また請負業者の本人確認を行うこととなる。これらの組織は GlobalSign の RA として従業員、代理店、また請負業者に対し本人確認を行う。この場合、GlobalSign 及び当該組織の契約により、GlobalSign は従業員の本人確認の手続きに対するセキュリティ査定を行うこととなる。こうした特定の類型の RA を用いて発行された証明書には、組織情報が記載されており、雇用目的によってのみ使用することができる。

1.3.3. 利用者

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

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

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

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

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

1.3.4. 依拠当事者

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

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

1.3.5. その他の関係者

その他の関係者には、ブリッジ認証局、PKI コミュニティ内において信頼される発行 CA を相互認証する認証局などを含む。たとえば GlobalSign のルート証明書 R1, R3, R5, R6 は Microsoft Code Verification Root に相互認証されており、GlobalSign をサブジェクトに記載し、Windows10 におけるサポートを含む、カーネルモードドライバを提供している。この相互認証証明書におけるサブジェクト名は、以下の通り、GlobalSign である。

尚、R1 へのクロス証明書は、Microsoft のウェブサイトからもダウンロードが可能である。どのクロス証明書がどの製品サービスに適しているか、詳細は GlobalSign のサポートページに掲載されている。

R1 に対する Microsoft Code Signing クロス証明書

-----BEGIN CERTIFICATE-----
MIIFJjCCAw6gAwIBAgIKYSkVJwAAAAAAKjANBgkqhkiG9w0BAQUFADB/MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHUmVkbW9uZDEe
MBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9uMSkwJwYDVQQDEyBNaWNyb3Nv
ZnQgQ29kZSBWZXJpZmljYXRpb24gUm9vdDAeFw0xMTA0MTUxOTU1MDhaFw0yMTA0
MTUyMDA1MDhaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52
LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxTaWduIFJvb3Qg
Q0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZjc6j40+Kfvvx
i4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavpxy0Sy6scTHAH
oT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz8kHp1Wrjsok6Vjk4
bwY8iGlbKk3Fp1S4bInMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdGsnUOhugZitVt
bNV4FpWi6cgKOOvyJBNPc1STE4U6G7weNLWLBYy5d4ux2x8gkasJU26Qzns3dLlw
R5EiUWMWea6xrkEmCMgZK9FGqkjWZCrXgzT/LCrBbBlDSgeF59N89iFo7+ryUp9/
k5DPAgMBAAGjgcswgcgwEQYDVR0gBAowCDAGBgRVHSAAMAsGA1UdDwQEAwIBhjAP
BgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRge2YaRQ2XyolQL30EzTSo//z9SzAf
BgNVHSMEGDAWgBRi+wohW39DbhHaCVRQa/XSlnHxnjBVBgNVHR8ETjBMMEqgSKBG
hkRodHRwOi8vY3JsLm1pY3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9NaWNy
b3NvZnRDb2RlVmVyaWZSb290LmNybDANBgkqhkiG9w0BAQUFAAOCAgEAX/jQZXRq
gcamylsDtpFK6Eu97yuhQvDvtKWtzTOJ7AuVhaxiUBEIqljSWqCDEOWmM3ryWvLF
/nh88JyD3xkK2XOWAC3WLM3pFNQdneg/PBp295BO+wE1CmyTE6DDVutnoOTRepbe
wmfxkPgKe/UyG5TsX3UfjRs02mxYp8stJ54iJrfJqjDMB3e4NuOCAbU5PMyN2adf
fyOzh3/bV5iRi9fOJSDjnWRP3Yf3K2hJAxjgpd98X2hkTTaDjUeB8ungqGmr+nsW
PAWkSeqIMBkKbHMFUXjf1B3dOtR/LeROVL6DQx56dDO0pOvXcHO8KgKYiWbu9ryP
dJN44ykCWlpD4ljOfM+aytI2iTviX9omBU7I1OcskQ4Xl8W+7osTESMjKU/6g9BQ
9rr61T2zFz30/wNKoyXc5nVh0fo1CGvWJ0TQaLeNReDrhSzIoV1hRHQWDllYrtK1
7qW81tcHarYpeP2XZ2fdjU8XlE/S7QyvlyQ3w6Kcgdpr4UO2V3tM7L95Exnnn+hE
6UeBt15wHpH4PdF7J/ULcFZDSAXdqS+rhhAdCxLjGtBMbnXe1kWzC3SIh5NcVkpB
Apr3rreZ2LZ/iPoR8kV89NcbkcAc8aD71AgKQRoUKs706zRIbmaHntVLejl/uw49
OGHPc1cG5BIGa9lrUwjNcBjCLU+XRpG8qfA=
-----END CERTIFICATE-----

R3 に対する Microsoft Code Signing クロス証明書

-----BEGIN CERTIFICATE-----
MIIFKTCCAxGgAwIBAgITMwAAADtqwB4rIeYV3AAAAAAAOzANBgkqhkiG9w0BAQUF
ADB/MQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMH
UmVkbW9uZDEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9uMSkwJwYDVQQD
EyBNaWNyb3NvZnQgQ29kZSBWZXJpZmljYXRpb24gUm9vdDAeFw0xNTA2MDQxNzQ3
NTNaFw0yNTA2MDQxNzQ3NTNaMEwxEzARBgNVBAoTCkdsb2JhbFNpZ24xIDAeBgNV
BAsTF0dsb2JhbFNpZ24gUm9vdCBDQSAtIFIzMRMwEQYDVQQDEwpHbG9iYWxTaWdu
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzCV2kHkGeCIW9cCDtoTK
KJ79BXYRxa2IcvxGAkPHsoqdBF8kyy5L4WCCRuFSqwyBR3Bs3WTR6/Usow+CPQwr
rpfXthSGEHm7OxOAd4wI4UnSamIvH176lmjfiSeVOJ8G1z7JyyZZDXPesMjpJg6D
FcbvW4vSBGDKSaYo9mk79svIKJHlnYphVzesdBTcdOA67nIvLpz70Lu/9T0A4QYz
6IIrrlOmOhZzjN1BDiA6wLSnoemyT5AuMmDpV8u5BJJoaOU4JmB1sp93/5EU764g
SfytQBVI0QIxYRleuJfvrXe3ZJp6v1/BE++bYvsNbOBUaRapA9pu6YOTcXbGaYWC
FwIDAQABo4HQMIHNMBMGA1UdJQQMMAoGCCsGAQUFBwMDMBIGA1UdEwEB/wQIMAYB
Af8CAQEwCwYDVR0PBAQDAgGGMB0GA1UdDgQWBBSP8Et/qC5FJK5NUPpjmove4t0b
vDAfBgNVHSMEGDAWgBRi+wohW39DbhHaCVRQa/XSlnHxnjBVBgNVHR8ETjBMMEqg
SKBGhkRodHRwOi8vY3JsLm1pY3Jvc29mdC5jb20vcGtpL2NybC9wcm9kdWN0cy9N
aWNyb3NvZnRDb2RlVmVyaWZSb290LmNybDANBgkqhkiG9w0BAQUFAAOCAgEAYAKs
DgkNtGp9WQytZkUKGA9epyVcFPbTWs+dXjvHevwAX25AKy3hzm92qzyr2flFz3eQ
UuohlzrSXT5XunPsAHV3onVFdMdiJrBUutXJydps7Wby/4sXsnlZyoBUZdqWyhHe
KrvD1D03/Ob9y5KGbrmtTRto4EfZsIY0IxzaHd1uVO3LDuF61U2yoavO2nEvoj4I
BKwqU9cT2TxuM4ynt7k1r6VZ3zBf6j7od3Ej+PnpHtviFANqiu9kwXvgXVbg5PLI
TODX7wfT1iD63mUZmKfGcStdlK7pyQuRV4aQzN6f1DwZlQQ+/VwrpPw5lY+oh4ey
W8qAT8MWOPUOsO3Xyvb8d0R32ErInZ//MBeY1xLVkN3lOmbg8SyXR5m2Dw5W2ptB
DcNL1fBonMqlhlyGZhLyO4ME/0btLWTUVpUrfnmdAYMTGNVovZHO3Yb7CKCrDEVk
w9EmNF5WomxMaQyLY8qEGHrFc6uzUq6N3OIrA2d9hioSb2hPZIF1LYXluOyABZur
OWnuHzFqair7Nb1jqsXuZdPWlqQ+mZMevu47bGRsrs0UCvzYjCCjHPhif6TAfR8s
fzpQwCaTljecj6UTY7Rz2BarJ0h+qv7rD0h/KZieO0mRkPCPPrrcnyaBnXNmMacn

tuSpTQTl6lMxwPqTSoed/Eph4GOirE+I9MV4H2U=
-----END CERTIFICATE-----

R5 に対する Microsoft Code Signing クロス証明書

-----BEGIN CERTIFICATE-----
MIIEfzCCAmegAwIBAgITMwAAADxDRdim0Drf5AAAAAAAPDANBgkqhkiG9w0BAQUF
ADB/MQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMH
UmVkbW9uZDEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9uMSkwJwYDVQQD
EyBNaWNyb3NvZnQgQ29kZSBWZXJpZmljYXRpb24gUm9vdDAeFw0xNTA2MDQxNzQ3
NTRaFw0yNTA2MDQxNzQ3NTRaMFAxEzARBgNVBAoTCkdsb2JhbFNpZ24xJDAiBgNV
BAsTG0dsb2JhbFNpZ24gRUNDIFJvb3QgQ0EgLSBSNTETMBEGA1UEAxMKR2xvYmFs
U2lnbjB2MBAGByqGSM49AgEGBSuBBAAiA2IABEdFDpb7fV2/6TnRIfifC7bVex6S
OkhZHPBiMS3Aeij+Gqdcs7bMl+dF1Fj60XdtQ6LAh2U0Ch963es8M6HFnU2kb0GV
OH/JHoTr0Z5JkoeUhww6hUpmn51Zk02XYQaGSqOB0DCBzTATBgNVHSUEDDAKBggr
BgEFBQcDAzASBgNVHRMBAf8ECDAGAQH/AgEBMAsGA1UdDwQEAwIBhjAdBgNVHQ4E
FgQUPeYpSJvqB8ohREom3m7e0oPQn1kwHwYDVR0jBBgwFoAUYvsKIVt/Q24R2glU
UGv10pZx8Z4wVQYDVR0fBE4wTDBKoEigRoZEaHR0cDovL2NybC5taWNyb3NvZnQu
Y29tL3BraS9jcmwvcHJvZHVjdHMvTWljcm9zb2Z0Q29kZVZlcmlmUm9vdC5jcmww
DQYJKoZIhvcNAQEFBQADggIBAEAHoOGyvU9GfLBcmnCnTFGXBNCEJiW3f3ENX+9L
/fsgNlPL3XsnL8/tzNvS8GccIxAPMjsOwaEX2wZuImSq3J9SqVhOksgovkDR0lTp
jd7PPz9s65rvnGfEWa2BE3vRCiDSBvGtA/EnSdodZKS7RFlfMNoke2oS5E1oKpl1
OeTmZTnZv4Ww76WcOrIpY1+or2/ci9z9J8fGETyVVZb2t6yaBN3lMVo7yR9JyNjv
WaOtC19QKW28YGaci9zg9JmRaWXQ6eOOX2o+tZaO5mwtdqqHls4StRPb44f4MPtK
k8Jw9IjcLcagpFelYDJTLtKFHmDwdTd1go7DJjZixaiCugqBiEJ3NFXq9EzX4lIa
6kdWw26haxtVLmG23DTfPlqWahlB2joMeJtLIirh4Jk2PS4viF69PRAb54m1bIYx
EiUPuw07tzXowHh+e5vvwnLCFvaas6w6pILcPYJ0MOvB2/EAji6GcpVGtmnMBEiG
/sSbLq7V+FhN9h8g/RipSZDpW0G760Rr1gInXQZyvaFpVO9kfV1DSnCDC+aVzZbO
3NoFAEJV4p3SnAnQJ3J7SqdBIV5hMGhxFeuGWV/fQL0jkvG162LS+PRwAccvhSVV
i69OcMgjPcqUeg6QQ8ikJ7+wl27BSD/cTD9Rj0DtVRN/G5VxgBLF2gEFNgmOemup
DwgW
-----END CERTIFICATE-----

R6 に対する Microsoft Code Signing クロス証明書

-----BEGIN CERTIFICATE-----
MIIGKTCCBBGgAwIBAgITMwAAAD3vOO4dp2hzYQAAAAAAPTANBgkqhkiG9w0BAQUF
ADB/MQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMH
UmVkbW9uZDEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9uMSkwJwYDVQQD
EyBNaWNyb3NvZnQgQ29kZSBWZXJpZmljYXRpb24gUm9vdDAeFw0xNTA2MDQxNzQ3
NTRaFw0yNTA2MDQxNzQ3NTRaMEwxEzARBgNVBAoTCkdsb2JhbFNpZ24xIDAeBgNV
BAsTF0dsb2JhbFNpZ24gUm9vdCBDQSAtIFI2MRMwEQYDVQQDEwpHbG9iYWxTaWdu
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAlQfoc8pm+ewUyns89w0I
8bRFCyyCtEjG61s8roO4QZIzFKRvf+kqzMawiGvFtonRxrL/FM5RFCHsSt0bWsbW
h+5NOhUG7WRmC5KAykTec5RO86eJf094YwjIElBtQmYvTbl5KE1SGooagLcZgQ5+
xIq8ZEwhHENo1z08isWyZtWQmrcxBsW+4m0yBqYe+bnrqqO4v76CY1DQ8BiJ3+QP
efXqoh8q0nAue+e8k7ttU+JIfIwQBzj/ZrJ3YX7g6ow8qrSk9vOVShIHbf2MsonP
0KBhd8hYdLDUIzr3XTrKotudCd5dRC2Q8YHNV5L6frxQBGM032uTGL5rNrI55Kwk
Nrfw77YcE1eTtt6y+OKFt3OiuDWqRfLgnTahb1SK8XJWbi6IxVFCRBWU7qPFOJab
Tk5aC0fzBjZJdzC8cTflpuwhCHX85mEWP3fV2ZGXhAps1AJNdMAU7f05+4PyXhSh
BLAL6f7uj+FuC7IIs2FmCWqxBjpllInA8DX9ydoojRoRh3CBCqiadR2eOoYFAJ7b
gNYl+dwFnidZTHY5W+r5paHYgw/R/98wEfmFzzNI9cptZBQselhP00sIScWVZBpj
Dnk99bOMylitnEJFeW4OhxlcVLFltr+Mm9wT6Q1vuC7cZ27JixG1hBSKABlwg3mR
l5HUGie/Nx4yB9gUYzwoTK8CAwEAAaOB0DCBzTATBgNVHSUEDDAKBggrBgEFBQcD
AzASBgNVHRMBAf8ECDAGAQH/AgEBMAsGA1UdDwQEAwIBhjAdBgNVHQ4EFgQUrmwF
o5MT4qLn4tcc1sfwf8hnU6AwHwYDVR0jBBgwFoAUYvsKIVt/Q24R2glUUGv10pZx
8Z4wVQYDVR0fBE4wTDBKoEigRoZEaHR0cDovL2NybC5taWNyb3NvZnQuY29tL3Br
aS9jcmwvcHJvZHVjdHMvTWljcm9zb2Z0Q29kZVZlcmlmUm9vdC5jcmwwDQYJKoZI
hvcNAQEFBQADggIBAKxHC181ziPmhqUOo5FlccJjaiLqIaHvwyvfWNnkaH8oYTpz
4VpkWA1Jf0ULvL875Lt/mS6Nl5Lt1RuOscQQdLqCgJdYThdbvDmBrX6SfZUd0r98
qIKXuRq2rSLhzLNrN6y//W8B94iVIT2AfuyJOTrMKHhiFOAkWqnclj/4kzV+fJVr
DStpFYhXanXKm9h+IVzsY//VuTDqei1aubVRcTXqWKRzn0keTlVTOKekfzSatpif
JFmtbjyvssL1hMH0ga/BtxLUp6c7Ls7vRV9qB3ZwT9jafhbD1qQgqc/X2S7H+eQr
cfhQ+EIAK2YiZLjvGX3zyRppuYzPiVjD9NFV6XcUf352AcB/pRZYXp4bMLniLK+a
LvksFG/g+e8+97kIUWmlintUe9ivQdnPeFEC/5AVHZaKfdAJOp9oqB/3WRbK+Cq4
Q3+3nb/5JiNVmAeDYoKOMXtAO0q5PWHL3ilBCQPtXcQ/bdShoPCfTHrWy7iO7m7K
BGrLFeHbxQucW10YbRAWnQ4s3Z5qMvFStcFAV+QUOofwEUrqJASZ0/Rvy7RrmHev

X8PKasM+CInaQiZxdsBCZ3il8hK2sEZTFhtxCzJ9p8dgu/K7SB0oEgfyL2+4NRAv
vMRAolNctIQjPS5g5RSPTvoyXMvKxPubaC+3MhDsftQoo/yCeHAsMY+Rw3T6
-----END CERTIFICATE-----

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、本人確認用のカードの電子上の代替物として商業環境で使用される。

1.4.1. 適切な証明書の使用方法

エンドエンティティ証明書は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。GlobalSign が発行する証明書は以下のような機能を必要とするパブリックドメインでの通信で使用することができる。

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

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

- **PersonalSign 2：** 取引への否認防止(中程度の保証レベル)
- **PersonalSign 2/3 Pro：** 組織内の担当者として取引を行う当事者による取引への否認防止(中程度の保証レベル)
- **Noble Energy:** 組織内の担当者として取引を行う当事者による取引への否認防止(中程度のハードウェアレベルの保証)
- **AATL：** 組織内の担当者として取引を行う当事者による取引への否認防止(中程度のハードウェアレベルの保証)。(Adobe 証明書ポリシーで規定される通り、キーエスクロー(鍵の預託)サービスの提供ができないこと及び証明書の唯一性をかんがみ、証明書を暗号化に使用することは推奨されない。)
- **適格証明書：** 個人(電子署名用の適格証明書)及び法人(e シール用の適格証明書)による署名への否認防止

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

- **PersonalSign 2：** 自然人及び電子メールアドレスの実在を認証する(中程度の保証レベル)
- **PersonalSign 2 Pro：** 組織内の自然人又は組織内の役職名、或いは機械、装置、部署を認証する(中程度の保証レベル)。オプションで、電子メールアドレスの実在を認証することも可能。
- **Noble Enrgy：** 自然人又は組織内の自然人、或いは機械、装置、部署、又は組織内の役職名を認証する(中程度の保証レベル)オプションで、電子メールアドレスの実在を認証することも可能。
- **PersonalSign 3 Pro：** 組織内の自然人を認証する(高い保証レベル)
- **NAESB Rudimentary：** NIST SP800-63A Digital Identity Guidelines：Enrollment and Identity Proofing, Section 4.3 “Identity Proofing Assuarance Level 1 に記載されている内容を認証する

- **NAESB Basic：** **Authentication as prescribed in CA/Browser Forum Baseline Requirements for the issuance and management of Publically Trusted Certificates** の **Section 3.2.3 Authentication of Individual Identity** に記載されている内容を認証する。上記の Basic Level と同等の手段で申請者の身元を確認した事業主は、LRA になることを選択し、申請者の身元証明を、会社が発行した写真 ID の検査又は LRA の安全なオンラインプロセスを介して直接行うことができる。企業が発行した写真 ID 又はオンラインプロセスは、政府が発行した写真 ID で作成する必要がある。
- **NAESB Medium：** Extended Validation Certificate の発行及び管理に関する CA/B Forum ガイドライン第 11.2.2 章:許容される検証方法(4) 主たる個人に規定されている内容を認証する
- **NAESB High：** Extended Validation Certificate の発行及び管理に関する CA/B Forum NIST SP800-63A Digital Identity Guideline の第 4.5 項 Identity Assuarance Level 3 に規定されている内容の認証、登録及び身分証明

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

- **DomainSSL：** ドメイン名とウェブサービスの認証、通信の暗号化
- **AlphaSSL：** ドメイン名とウェブサービスの認証、通信の暗号化
- **OrganizationSSL：** リモートドメイン名、リモートドメイン名と関連づけられる組織名とウェブサービスの認証、通信の暗号化
- **ICPEdu：** リモートドメイン名、リモートドメイン名と関連づけられる組織名とウェブサービスの認証、通信の暗号化
- **ExtendedSSL：** ドメイン名、ドメイン名と関連づけられる組織名とウェブサービスの認証、通信の暗号化
- **Code Signing：** 法人、法的エンティティとそのデータオブジェクトの認証
- **EV Code Signing：** 法人、法的エンティティとそのデータオブジェクトの認証
- **Time Stamping：** 組織内での日付・時刻に関連するサービスの認証
- **PersonalSign(全種)：** 組織に関連づけられるデバイスやマシンの認証
- **NAESB Rudimentary：** NIST SP800-63A Digital Identity Guidelines の Enrollment and Identity Proofing, Section 4.3 Identity Proofing Assurance Level I に記載されている内容を認証する
- **NAESB Basic：** CA/Browser Forum Baseline Requirements for the issuance and Management of Publically Trusted Certificates の Section 3.2.3 Authentication of Individual Identity に記載されている内容を認証する
- **NAESB Medium：** Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates の Chapter 11.2.2 Acceptable Method of Verification (4) Principal Individual に記載されている内容を認証する
- **NAESB High：** Authentication as prescribed in NIST SP800-63 A Digital identify Guidelines の Enrollment and Identity Proofing. Section 4.5 Identity Assurance Level 3 に記載されている内容を認証する

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

- **低い保証レベル:** Class 1 証明書は、認証された本人確認情報が証明書内に記載されないため、本人確認には適していない。本証明書は、否認防止をサポートしない。
- **中程度の保証レベル:** Class 2 証明書は、一定のリスクを伴う組織間、組織内、及び商業的取引を暗号化するのに適した、個人及び組織用の証明書である。

- **高い保証レベル:** Class 3 証明書は、Class 1・Class 2 証明書に比較してサブジェクトの本人確認情報について高いレベルの保証を提供する、個人又は組織に発行される証明書である。
- **高い保証レベル(EV):** EV 証明書は EV ガイドラインに準拠して GlobalSign が発行する Class 3 証明書である。
- **NAESB Rudimentary:** 最も低い保証レベルを提供する。このレベルの主な目的は署名された情報の完全性を保証するために使用される。このレベルは悪意のある行動をとることが少ないと考えられる環境にて使用するのが適切である。このレベルは認証を必要とする取引には適していない。また、一般的に機密性を必要とする取引には適していないが、より高い認証レベルの証明書が使用できない場合は、このレベルの証明書を使用してもよい。
- **NAESB Basic:** データ漏えいにつながるリスクがあるがその影響が大きくないと考えられる環境において、基礎レベルの保証を提供するのに適している。この環境はプライベート情報にアクセスするが、悪意のあるアクセスが行われる可能性は高くない環境を含む。尚、この保証レベルでは悪意を持ったユーザはいないと想定している。
- **NAESB Medium:** このレベルはデータ漏えいにつながるリスクが中程度にある環境に適している。この環境は大きな金銭的価値がある取引や不正のリスク、又は不正アクセスの可能性が大きい環境においてプライベート情報にアクセスすることを含む。
- **NAESB High:** このレベルはデータに対する脅威が大きい環境、又はセキュリティサービスの不備があった場合の影響が高い環境のために残されている。

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

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

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

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

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 のワランティーポリシーに示された信頼性の限度を超えた方法で証明書を使用することは認められていない。

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

本 CPS に準拠して発行された証明書は、以下の目的に使用してはならない。

- 以下に挙げるような、フェイルセーフ機能を必要とする用途。
  - 原子力設備の運用
  - 航空管制システム
  - 航空機ナビゲーションシステム
  - 兵器誘導システム
  - その他、誤動作・機能不全が人の怪我や死、又は環境被害をもたらす可能性があるシステム

- 又は、法により禁じられている場合。
- e シールは法人によってのみ使用されなければならない一方、電子署名用の証明書は自然人によってのみ使用されなければならない。
- NAESB WEQ-PKI に準拠して発行された証明書は以下の目的で使用してはならない。
  - 危殆化や改ざんが起きた場合投獄され得るような通信やデータ伝送
  - 連邦法において違法とみなされる通信やデータ伝送

1.5. ポリシー管理

1.5.1. 文書を管理する組織

発行 CA が認定スキームに準拠しているかどうかの情報を得たい場合、又はその他本 CPS に関する問い合わせは、以下に送付すること。
PACOM1 – CA Governance GlobalSign NV
Martelarenlaan 38,
3010 Leuven,
Belgium
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909

1.5.2. 問い合わせ窓口

質問全般

GlobalSign NV
attn. Legal Practices,
Martelarenlaan 38,
3010 Leuven,
Belgium
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909
Email: legal@globalsign.com
URL: www.globalsign.com

証明書問題報告

利用者、依拠当事者、アプリケーション・ソフトウェア・サプライヤー、及び他の第三者は、秘密鍵の危殆化の可能性、証明書の不正使用、又は他の種類の不正、セキュリティの侵害、証明書の誤発行、不適切な行為等について、又、証明書に関連するその他事項については、report-abuse@globalsign.com 宛てに電子メールで報告することができる。

GlobalSign は、これらの要求に応じ、当該証明書を失効することで対応することが可能である。また、調査の結果、失効しない場合もある。この意思決定のために GlobalSign はセクション 4.9.5 に記載されている調査を実施する。

1.5.3. 認証業務運用規程がポリシーに適合しているかを判断する担当者

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

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

1.5.4. 認証業務運用規程承認手続き

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

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

1.6. 定義と略語

本契約において使用されているが定義されていない語句は、Baseline Requirements、EV ガイドライン、EVCodeSigning ガイドライン、CodeSigning 証明書に関する最低要件、及び eIDAS 規則において定義されるものとする。

Adobe Approved Trust List (AATL) : Adobe PDF Reader version 9.0 以降に搭載されている Adobe Root CA Policy Authority が生成する文書署名認証局のトラストストア

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

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、自然人又は法人は利用者と呼ばれる。デバイス自体が証明書の申請データを送信している場合であっても、証明書に名称の記載されたデバイスを管理運用するエンティティがこの証明書の申請者である。

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

認証状：サブジェクトの身元情報が正確であることを表明する文書

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

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

ドキュメント認証サービス(CDS)：Adobe PDF バージョン 6.0 以上に実装された Adobe Root CA Policy Authority が作成した文書署名アーキテクチャ

証明書：デジタル署名によってある公開鍵とある本人確認情報との間を紐づける電子文書

証明書権限(CAA)：CAA レコードは、どの証明書機関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、GlobalSign がアプリケーションソフトウェアサプライヤーにより配布されるソフトウェアにルート証明書を含める契約を締結した全てのアプリケーションソフトウェアサプライヤー、及び有効な証明書に合理的に依拠する全ての依拠当事者。

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

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

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

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

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

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

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

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

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

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

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

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

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

DCF77:ドイツの長波長信号と標準周波数無線局。

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

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

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

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

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

ドメイン名：ドメインネームシステムにおいて単一のノードに与えられた名称

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

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

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

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

eIDAS 規則：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

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

エンタープライズ PKI (EPKI)：Microsoft Windows が信頼するデジタル ID、Adobe Approved Trust List、Adobe Certified Document Services 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。

完全修飾ドメイン名：ドメインネームシステム内の上位ノードに与えられる名前を含むドメイン名

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

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

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

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

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

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

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

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

国際化ドメイン名(IDN)：少なくとも 1 つの言語固有のスクリプト又はアルファベット文字を含み、ASCII 文字列のみを受け入れる DNS で使用するためにプ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。

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

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への秘密鍵の漏えいが技術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 に認定認証局として認可を受けるために認証局が準拠すべき技術的・管理要件

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

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

オブジェクト識別子(OID)：ISO 規格において特定のオブジェクト又はオブジェクトクラスに付与された英数字から成る唯一の識別子

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

Payment Services Directive (PSD2)：全 EU 及び EAC 域内の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：申請者の業務を行う施設(工場、小売店、倉庫等)の所在地

秘密鍵：鍵ペアの一方で、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化するのに用いる。

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

PSD2 証明書：PSD2 特定の属性を含む適格証明書

PSD2 特定の属性：PSD2 証明書に特定の属性は以下の通り：

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

公開鍵：鍵ペアの一方で、対になる秘密鍵の所有者が公開する。対になる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復号化することができるようメッセージを暗号化する際に使用する。

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

一般に信頼される証明書：広く普及するソフトウェアに搭載されるトラストアンカーであるルート証明書にチェーンされている事実をもって信頼を享受する証明書

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

適格証明書：eIDAS 規則で定義された資格要件を満たす証明書。

e シールの適格証明書：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 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。

電子署名の適格証明書：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 e シール。

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

適格政府情報源：政府機関によって維持されるデータベース。

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

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

適格電子署名作成装置(QSCD)：電子署名作成装置であって、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 規則 42 条に準拠するタイムスタンプを提供すること

適格トラストサービスプロバイダ(QTSP)：EU加盟国の国内監督機関により、eIDAS規則に定義されている資格を有するトラストサービスを提供する(サブセットの)ことを認められている自然人又は法人。

QWAC 証明書(QWAC)：eIDAS 規則 45 条に符合する適格 SSL 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本人確認と認証に責任を負う法人であり、認証局ではないため、証明書を発行したり、証明書に署名したりすることはない。登録局は証明書の申請手続き、失効手続きをサポートする。「登録局」が役割、機能を説明する場合、必ずしも独立した組織を指すとは限らず、認証局の一部であることもある。

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

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

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

ルート証明書：ルート認証局が発行し自己署名した証明書。ルート認証局の下位認証局に発行した証明書を検証するために使用される。

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。サブジェクトは利用者であるか、利用者が管理、運営するデバイスである。

サブジェクト本人確認情報：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。

下位認証局：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。

技術的に制約された下位 CA 証明書:下位 CA 証明書が利用者又は追加の下位 CA 証明書を発行できる範囲を制限するために、拡張キー使用設定と名前の制限設定の組み合わせを使用する下位 CA 証明書。

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

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。

有効な証明書：RFC 5280 で規定される検証手続きの結果有効であると認められた証明書。

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。

審査員：Baseline Requirements に規定される情報の検証業務を行う担当者。

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：サブジェクトとして、完全修飾ドメイン名の一番左の欄がアスタリスク(*)で示されたものを記載する証明書。

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

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

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

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

AATL	Adobe Approved Trust List

AICPA	米国公認会計士協会
API	アプリケーション・プログラム・インタフェース
ARL	発行局失効リスト (エンドエンティティ失効リストではなく)
CA	認証局
CAA	Certificate Authority Authorization
CCADB	Common CA Database
ccTLD	国別コードトップレベルドメイン
CICA	カナダ公認会計士協会
CP	証明書ポリシー
CPS	認証業務運用規程
CRL	証明書失効リスト
DBA	事業名
DNS	ドメインネームシステム
EIR	Electric Industry Registry
EKU	拡張鍵
EPKI	エンタープライズ PKI
ETSI	欧州電気通信標準化機構
EV	Extended Validation
FIPS	(米国政府)連邦情報処理標準
FQDN	完全修飾ドメイン名
GCC	GlobalSign Certificate Center
GPS	Global Positioning System
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICPEdu	A Infraestrutura de Chaves Públicas para Ensino e Pesquisa
IETF	インターネット技術タスクフォース
ISO	国際標準化機構(International Organization for Standardization)
ITU	国際電気通信連合
LRA	ローカル登録局
NCA	所轄官庁(National Competent Authority)
NAESB	北米エネルギー規格委員会
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	支払サービスプロバイダ
QGIS	Qualified Government Information Source
QGTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source

RA	登録局
RFC	リクエスト・フォー・コメンツ
S/MIME	セキュア MIME(多目的インターネットメール拡張)
SSCD	安全な署名生成装置
SSL	セキュア・ソケット・レイヤー
TLD	トップレベルドメイン
TLS	トランスポートレイヤー・セキュリティ
VAT	付加価値税

2. 公開とリポジトリの責任

2.1. リポジトリ

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

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

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

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

2.2. 証明書情報の公開

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

- 現在のバージョンの CA/Browser Forum Baseline Requirements for the issuance and management of Publicly-Trusted Certificate (以下「Baseline Requirements」という)
- the CA/Browser Forum Guidelines for the Extended Validation Certificate(以下「EV Guidelines」)
- the CA/Browser Forum Guidelines for the Extended Validation CodeSigning Certificate(以下「EV Code Signing Guidelines」)wwwww.cabforum.org に公開されている。
- the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (以下「Code Signing Minimum Requirements」) published at https://aka.ms/csbr に公開されている。
- GlobalSign のルート証明書を組み込んでいる、その他のルートストアポリシー/プログラム

本文書の解釈と Baseline Requirements との間に矛盾が生じた場合、Baseline Requirements を優先して解釈・適用する。Baseline Requirements と Mozilla Root Store ポリシーの解釈に相違が生じた場合、Mozilla Root Store ポリシーを優先して解釈・適用する。この CP が準拠するその他の規格については、先述の「前提確認事項」を参照。

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

ルート R1:

https://valid.r1.roots.globalsign.com
https://revoked.r1.roots.globalsign.com
https://expired.r1.roots.globalsign.com

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

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

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

ルート R7
https://valid.r7.roots.globalsign.com
https://revoked.r7.roots.globalsign.com
https://expired.r7.roots.globalsign.com

ルート R8
https://valid.r8.roots.globalsign.com
https://revoked.r8.roots.globalsign.com
https://expired.r8.roots.globalsign.com

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

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

2.3. 公開の時期及び頻度

CA 証明書は発行後すぐにサポートページからアクセス可能なリポジトリに公開する。エンドエンティティ証明書の CRL は 24 時間ごとに更新され、7 日間にわたり有効である。CA 証明書の CRL は少なくとも 3 か月ごとに更新し、また証明書が失効された際には 24 時間以内に更新される。それぞれの CRL には、更新ごとに 1 つずつ増加する連続した番号を付与する。

GlobalSign は、GlobalSign の認証局(CA)の運用が正確で透明性が高く、先述の「前提確認事項」に記載されている外部要求事項に準拠するように、少なくとも年 1 回、CP 及び CPS を見直し、適切な変更を行う。GlobalSign は、CA/B Forum の投票及び Baseline Requirements の更新を綿密に監視し、GlobalSign のオペレーションの更新を即時に実施する。CP、本 CPS、利用契約、依拠当事者契約の新版及び改訂版は、Policy Authority により、タイムスタンプ付きの Adobe AATL PDF 署名証明書を用いてデジタル署名された後、7 日以内に公表されるものとする。

2.4. リポジトリへのアクセス管理

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

3. 本人確認と認証

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

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

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

3.1. 名称

3.1.1. 名称の種類

GlobalSign が発行する証明書に含まれるサブジェクト識別名は、X.500「名称」、RFC 822「名称」、及び X.400「名称」に規定される要求事項に準拠している。コモンネームは、名前空間において唯一であることを担保し、誤解を招くものを含まない。しかしながら、IntranetSSL Common Names といったいくつかの証明書や GlobalSign は、発行する証明書に RFC 2460(IPv6)又は RFC 791(IPv4)に規定される IP アドレスを記載することがある。

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

3.1.2. 意味のある名称である必要性

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

3.1.3. 利用者の匿名又は Pseudonym の使用

GlobalSign は、ポリシーにおいて禁じられていない場合、及び名前空間における唯一性が担保される場合、匿名又はペンネーム (Pseudonym)のエンドエンティティ証明書を発行することがある。GlobalSign は法の求めるところにより、利用者の本人確認情報を開示する権利を有する。証明書の国際ドメインネーム(IDN)の要求は、追加の手動レビューを受けることとなる。デコードされたホスト名は、フィッシングや他の不正な使用の危険性を低減するために、追加のレビューを受けることとなる。デコードされたホスト名は、以前に拒絶された証明書申請や失効された証明書と照合される可能性がある。GlobalSign は、リスク低減基準に基づいて申請を拒否することができる。例えば、フィッシング又はその他の不正使用の危険性がある名称、Google Safe Browsing List に掲載されている名称、又は Anti-Phishing Working Group が管理するデータベースに掲載されている名称などがそれに該当する。

3.1.4. さまざまな形式の名称の解釈方法

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

3.1.5. 名前の唯一性

GlobalSign は証明書内のサブジェクト名の唯一性を以下の通り担保する。下記にある「Class」の定義については、3.2.3 項を参照。

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

- **PersonalSign Pro Certificates：** 組織名及び、場合によっては組織の州及び地域と関連付けられた電子メールアドレス(証明書に含まれる場合)。並びに、個人名又は部署名及び、場合によっては部門名(Class 2)。
- **PersonalSign 3 Pro Certificates:** 組織名・組織の住所及び、パスポート上、又は個人が GlobalSign 又は信頼された第三者(Class 3)に提出する同等の身分証明上の個人名と対応した電子メールアドレス
- **Noble Energy Certificates:** 組織名及び住所、加えて個人名又は部門名と対応した電子メールアドレス(証明書の subjectDN に含まれる場合)。
- **Code Signing Certificates：** 組織名と住所、個人名と住所、電子メールアドレスを付加することもある
- **EV Code Signing Certificates:** 組織名、事業分類、法人格が登録された管轄地、登録番号、及び地理上の住所(Class3)
- **SSL Certificates (Non EV types)：** 組織名及び住所に対応し、ICANN により認められたドメイン名の最小単位を commonName に記載
- **SSL Certificates (EV)：** 組織名、事業分類、法人格が登録された管轄地、登録番号、及び地理上の住所に対応し、ICANN により認められたドメイン名の最小単位を commonName に記載
- **Time Stamping Certificates：** 組織名と住所、電子メールアドレス(Class 2)を付加することもある
- **NAESB Rudimentary：** 電子メールアドレスのみ(Class 1)
- **NAESB Basic、Medium、High：** 組織名及び住所、加えて個人名又は部門名と対応した電子メールアドレス(証明書の subjectDN に含まれる場合)。
- **AATL Certificates：** 組織のみ、又は組織に所属する従業員、代理人、請負業者、取引先、又は顧客のいずれかとしての個人の名前と組み合わされた、最低限 Class2 の中レベルを保証する 証明書
- **Trusted Root Inc. AATL & CDS：** SSL 証明書を発行できる下位 CA のために、Subject Naming の基本要件に従う。他の全てのタイプについて、サブジェクト名称は、意味のある CA 名と組織の名前とアドレスを結合する Class 2 手続きに従う。
- **Qualified Certificates：** 住所の詳細又は組織名、組織名、及び関連個人名(適格電子署名の適格証明書)又は組織名と住所(e シールの適格証明書)(Class 3)。

3.1.6. 商標の認知、認証、役割

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

3.2. 初回の本人確認情報の検証

GlobalSign は、認証局のチェーニングサービスなどの利用を申し込む法人・個人の申請者の本人確認のために必要な連絡、調査などにおいて、あらゆる法的手続きを用いる。

GlobalSign は、初回の審査において検証の結果、真正と認められた本人確認情報を、事後に別の情報及び新規に審査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。GlobalSign Certificate Center (GCC)アカウントにログインが可能であることをもって、検証済の情報に依拠して証明書の発行ないしサービスの提供を受ける権利を有することを確認する。GCC アカウントは、3.3.1 項の再審査要件がその GCC アカウント保有者によって遵守されているという条件のもと、過去に審査された再申請者についての情報を再利用できるかどうかを認証するために使用される。

3.2.1. 秘密鍵の所有を証明する方法

利用者は、PKCS#10 形式の CSR(証明書署名要求)又は SPKAC(Signed Public Key and Challenge)形式のデータフォーマットで、登録した公開鍵と対になる秘密鍵の所有を証明しなければならない。

GlobalSign はその TrustedRoot サービスの下で、GlobalSign 証明書階層にチェーンされることを希望する発行 CA の申請を受領するが、一次評価を受け、GlobalSign との個別契約を締結した後、発行 CA も秘密鍵の所有を証明しなければならない。認証局チェーニングサービスの利用においては、(本人確認情報の検証を

受けた)申請組織と GlobalSign との間で契約が締結されていれば、発行 CA を代表する利用者が RA に赴いて審査を受けることは必須としない。

適格 証明書を利用する際は、利用者の秘密鍵は 認証済の Qualified Signature Creation Device (QSCD)の中で生成・保管されねばならない。QSCDの認証ステータスは監視され、変更があれば適切な措置が取られねばならない。

3.2.2. 組織の識別情報の認証

GlobalSign は、GlobalSign が加盟する様々なルートプログラム、並びに Baseline Requirements、EV ガイドライン及び EVCodeSigning ガイドラインの要求事項に準拠するよう、定期的にレビューされるよう社内ポリシー及び手続きを定めている。これらのポリシー及び手続き文書は、WebTrust 2.1 の Principle 6 の基準を満たす PACOM5 - Subscriber Validation (第 1.5.1 項の主なポリシー機関の下位機関)の管理下にある。
GlobalSign が組織のアイデンティティを検証する方法は、通常は全製品・サービスの種類において一貫しているが、以下にあげる、より一般的に使用されている QGIS 手法で認証ができない場合には、あらかじめ容認された方法に従った代替手段を使用することがある。
組織情報を含む全ての証明書について、申請者は、組織名及び登録の又は商業上の住所の提出を求められる。全ての証明書について、法的存在、法的名称、仮名(該当する場合)、法的形式(設立の管轄区域における要請又は法的名称の一部に含まれる場合)及び提出を要請された組織の住所が、以下のいずれかの方法で確認される。

- 申請者、又は申請者自身が政府機関と名乗っている場合、申請者より上位の政府機関を管轄する政府機関(QGIS)への確認
- 定期的に更新されており、GlobalSign が正確であり信頼に足ると判断した第三者データベースの情報を用いた確認
- 会計士、弁護士、政府機関担当者、裁判官、又はその他サブジェクトの身元情報の検証者として通例信頼できるとみなされる第三者が、この情報が正確であることを証した認証状
- 政府公認の納税情報

上記の方法の他、GlobalSign は申請者の(本人確認情報ではなく)住所を公共料金の請求書、銀行取引明細、クレジットカード明細、政府発行の税務書類、その他 GlobalSign が正確であり信頼に足ると判断した証明書類に基づいて検証することがある。尚、この方法は EV には認められていないため、EV においては除外する。

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

3.2.2.1. LRA の認証

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

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

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

3.2.2.3. 適格証明書

GlobalSign は以下の通り、組織情報を含む適格証明書を 2 種類発行する。

- e シールの適格証明書(組織情報を証明)
- 電子署名の適格証明書(個人が組織に所属することを証明)
- QWAC 証明書

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

GlobalSign は、以下を参照して、法的存在と住所を確認する。

- Qualified Government Information Source に掲載されている公式の政府記録、又は

- 組織の法的設立、法的存在又は法的認知を有する管轄区域の政府機関により確認、もしくは提供される文書
- Qualified Government Information Source により提供される記録

さらに、GlobalSign は、以下を参照して住所を検証することができる。
- 検証された法的見解又は会計士の書簡
- 当該組織の有効な適格 e シールを用いて署名された物理的所在地の証明(その証明の記載事項は、適格証明書の内容と一致していなければならない)

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

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

組織の同一性を主張する適格証明書及び QWAC 証明書については、GlobalSign は、組織の権限を付与された代理人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、もしくは提供される文書
- Qualified Government Information Source により提供される記録
- 組織の有効な適格 e シールを用いて署名された証明(その証明の記載事項は、適格証明書の内容と一致していなければならない)

GlobalSign は、セクション 3.2.3 に従って、授権された代表者の身元を確認する。
GlobalSign は特定の属性について、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正式な伝達により提供されている情報をもとに評価する

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、GlobalSign は平文にて以下を含む証明書情報をその電子メールアドレスに送信する。
- 証明書の 16 桁のシリアル番号
- 証明書利用者の識別名
- 証明書発行者の識別名
- 証明書の有効期間
- 連絡先情報
- 失効情報
- 証明書ファイルのコピー

3.2.3. 個人の本人確認情報の認証

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

3.2.3.1. Class 1

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

3.2.3.2. Class 2

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

申請者はまた、政府機関発行の有効な身分証(運転免許証、軍人身分証明書、その他同様のもの)又は写真付き ID カードの判読可能なコピーの提出を求められる可能性がある。また、政府機関発行以外の身分証、写

真付き ID カードの提出を求められることもある。GlobalSign は証明書申請に含まれる名前と身分証に記載される名前、及び国、州、その他の住所の情報が一致することなど、適切なレベルで本人確認が行われることを担保する。

GlobalSign は申請者の本人確認情報を以下のいずれか一つの方法によって認証する可能性がある。

- 申請者の電話番号を信頼できる情報源から入手し、電話によるチャレンジ・レスポンスを求める
- 申請者の FAX 番号を信頼できる情報源から入手し、FAX によるチャレンジ・レスポンスを求める
- 申請者の電子メールアドレスを信頼できる情報源から入手し、電子メールアドレスによるチャレンジ・レスポンスを求める
- 申請者の住所を信頼できる情報源から入手し、郵便によるチャレンジ・レスポンスを求める
- 政府の認めている形式の ID をもとに、公証人又は信頼できる第三者から、個人の身元情報を検証したという証言を得る
- 組織に属する個人の場合、承認された LRA に証言を依頼する可能性がある。マネージド PKI 又はマネージド SSL のプロファイルを通して Class 2 の証明書の注文があった場合、3.2.3.4 項を参照。
- 政府の認めている形式の ID をもとに、利用者自身のエンドユーザの身元情報を検証するために利用者から証言を得る。利用者はこれらの情報が保護された状態で、審査状況を追跡することができる。
- 申請者の印影(その法的文書への押印を認めた管轄地方行政機関のもの)が、書面による申請に付与されている

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

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

3.2.3.3. Class3

EV Code Signing について、申請者は証明書に記載する電子メールアドレスに対する管理権限を証明する。

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

申請者は政府機関発行の有効な身分証(運転免許証、軍人身分証明書、又はその他同様のもの)又は写真付き ID カードの判読可能なコピーを提出する。付加的に、政府機関発行以外の身分証、写真付き ID カードの提出を求められることもある。GlobalSign 又は信頼される第三者は、証明書申請に含まれる名前と身分証に記載される名前、及び国、州、その他の住所の情報が一致することなど、適切なレベルで本人確認が行われることを担保する。

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

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

PersonalSign 3 Pro の申請において、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。この手続きは、PersonalSign 3 Pro の発行においては必須である。

GlobalSign はまた、EV ガイドライン及び EV CodeSigning ガイドラインに準拠した申請者との信頼できる通信方法として GlobalSign によって検証された信頼できる伝達手段を用いて、証明書のサブジェクトになる団体を代表する申請者の権限を認証する。

- 申請者の属する組織の電話番号を信頼できる情報源から入手し、電話によるチャレンジ・レスポンスを求める
- 申請者の属する組織の住所を信頼できる情報源から入手し、郵便によるチャレンジ・レスポンスを求める

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

3.2.3.4. 適格証明書

GlobalSign は、以下の方法に従って、個々の利用者の識別を認証する。

- 本人確認
- 電子上の本人確認の使用
- 適格電子署名の使用
- ビデオ検証

- **3.2.3.4.1. 本人確認**

利用者が物理的に存在している必要があり、以下の文書の提出が必要である。

- 政府発行写真付き ID
- 署名されたパーソナル・ステートメント
- 二つの二次証拠書類

個人の肖像を写真付き ID と比較し、写真付き ID のセキュリティ機能を検査する。パーソナル・ステートメントの署名は、写真付き ID の署名と比較される。

この検証を実行できるエンティティ:

- 認証局(CA)
- 登録局(RA)
- 役人又は第三者検証者
- ローカル登録局 - 組織(個人の組織への所属性を示す適格証明書の場合。その従業員、請負業者、代理人の本人確認)

- **3.2.3.4.2. 遠隔本人確認**

GlobalSign は本人確認に遠隔地から電子的な方法で本人確認を行うこともある。
全ての電子本人確認手段は、eIDAS 規則第 8 条に定める「実質的」又は「高水準」の保証水準を有する。また、発行に先立ち、本人の身体的存在が保証される。

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

自然人の物理的存在は、電子本人確認手段に利用される認証要素のカテゴリーを確認することによって確保することができる。GlobalSign は、以下の権限の認証要因を物理的存在の証明として受け入れている。

- 少なくとも 1 つの固有の要素
- 以下の各カテゴリーのうち 1 つ以上の、複数の要素
    - 保有に基づくもの(「保有に基づく認証要素」とは、サブジェクトが保有していることを証明するために必要な認証要素をいう)。
    - 知識に基づくもの(「知識に基づく認証要素」とは、サブジェクトが知識を有していることを証明するために必要とされる認証要素を意味する。)

この検証を実行できるエンティティ:

- 認証局(CA)
- 登録局(RA)

- **3.2.3.4.3. 適格証明書**

GlobalSign は、利用者の有効な適格電子署名を個人のパーソナル・ステートメントに使用して、適格電子署名を作成するために使用される証明書に含まれる申請者の身元及び追加属性を確認する。

以下のいずれかの条件が満たされた場合、GlobalSign は上記のようにする。

- 発行 CA にかかわらず、適格電子署名の作成に用いられる適格証明書が、高度な保証レベルを有すると通知された電子本人確認スキームの一部としてとして発行された場合
- 適格証明書が新規証明書の発行前 825 日以内に直接本人確認をした後に GlobalSign により発行された場合

この検証を実行できるエンティティ:

- 認証局(CA)
- 登録局(RA)

- **3.2.3.4.4. ビデオ検証**

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

- 政府発行写真付き ID
- (電子的に)署名されたパーソナル・ステートメント
- 二つの二次証拠書類

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

この検証を実行できるエンティティ:

- 認証局(CA)
- 登録局(RA)

- **3.2.3.5. ローカル登録局認証**

マネージド PKI 及びマネージドマネージド SSL アカウントを含む事前審査済み組織アカウントはローカル登録局（以下「LRA」）と考えることができるが、GlobalSign は、このアカウントに対し、認証済の組織情報をプロファイルとして設定する。こうしたアカウント内の証明書はプロファイルの情報を利用する。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々の認証を行う。

3.2.3.6. 北米エネルギー規格委員会（NAESB）向け証明書

北米エネルギー規格委員会（以下「NAESB」）向け証明書申請については、関連会社による利用者証明書の組織情報の真正性を確認するために、組織名、住所、及び組織が存在することの証明文書を含まなければならない。GlobalSign もしくは 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、情報の審査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、法的所在地を登録し、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「利用者コード」を確保しなければならない。WEQ-012 の申請以外の目的で、エネルギー産業内で使用される証明書を発行する場合、ACA は、NAESB EIR 内で利用者登録を必要とする WEQ-012-1.9.1、WEQ-012-1.3.3 及び WEQ-012-1.4.3 の規定を除き、NAESB WEQ-012 Public Key Infrastructure Business Practice Standards and Models の規定に準拠しなければならない。

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

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

本人確認の要件は以下の通り行う。

NIST Assurance Level	**NAESB Assurance Level**
レベル 1	Rudimentary 最小限
レベル 2	Basic 低度
レベル 3	Medium 中程度
レベル 4	High 高度

GlobalSign 又は指定された RA(マネージド PKI の場合)は、申請者により提供された本人確認情報を全て、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

GlobalSign は、証明書のサブジェクト識別名に記載される情報のうち、CPS の本章における規定において除外される項目以外の全てを検証する。GlobalSign は、サブジェクトの所属名(organizationalUnitName)フィールド又はシリアル番号(non-EV/Qualified Certificates)を使用して、依拠当事者に検証されていない利用者情報に対し本人確認を行い、また、免責事項・告知などの情報を提供する。個人の場合は、個人の名前と合わせて携帯電話番号なども個人を特定する情報として検証する。

- GlobalSign が自然人や法人の名称、事業名、商号、住所、所在地、その他を明確に識別することができる全てのタイプの証明書では、GlobalSign はこれらの情報を検証し、免責事項の告知を記載しない。
- GlobalSign が明確に検証できない全ての証明書の種類、例えば、「マーケティング」のような一般的な用語については、GlobalSign は本 CPS に記載されるように、検証されていない利用者情報として分類し、いかなる免責事項も省略する。Intranet SSL/TLS の証明書に限っては、GlobalSign は、申請者の希望により、インターナルネットワーク内で使用されるドメイン名、非公開ドメイン名、ホスト名、RFC 1918 に規定される IP アドレスなどを、証明書の SubjectAlternativeName フィールドに記載する。

SSL/TLS 用の証明書、及び Code Signing 証明書については、GlobalSign 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する。

GlobalSign は、マネージド PKI サービス、エンドユーザ、役職、機器に対し、クライアント認証、文書署名、及び S/MIME の用途で使用されることが多い証明書を提供する。LRA は、契約に基づき機器の名称や役職、又は名称を検証する義務を負う。サブジェクトの所属名(organizationalUnitName)又は commonName フィールドに記載の情報が LRA によって検証済であることを示すために、ポリシー OID(1.3.6.1.4.1.4146.1.40.10)を記載する。

3.2.5. 権限の認証

PersonalSign1 Certificate	チャレンジ・レスポンス方式を用いて申請者が証明書に記載される電子メールアドレスを管理していることを検証する。
PersonalSignDemo Certificate	申請者が証明書に記載される電子メールアドレスを管理していることを検証する。
PersonalSign2 Certificate	信頼できる方法による申請者個人との連絡を通じた検証に加え、証明書に記載された電子メールアドレスを管理していることを検証する。
Noble Energy Certificate	申請組織又は個人との信頼できる手段による意思確認を通し検証すると同時に、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を検証する。
NAESB Certificate	3.2.3.5 項の規定に従い、信頼できる方法による申請組織又は個人との連絡を通じた検証に加え、申請者が証明書に記載される電子メールアドレスを管理していることを検証する。
PersonalSign2 Pro	申請者個人との信頼できる連絡手段を通し検証すると同時に、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を検証する。マネージド PKI アカウントにより発行された証明書は、プロファイル設定時に、LRA の権限者を検証する。
PersonalSign2 Department Certificates	申請者個人との信頼できる連絡手段を通し検証すると同時に、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を検証する。マネージド PKI アカウントにより発行された証明書は、プロファイル設定時に、LRA の権限者をが検証する。
PersonalSign3 Certificate	申請組織との信頼できる連絡手段を通し、申請者が組織を代表して証明書を申請する権限を有することを検証する。申請者の身元証明のため、申請者が RA 担当者と面会して身分証を提示することが必須である他、証明書に記載される電子メールアドレスをその申請者が管理していることを検証する。

Code Signing Certificates	申請組織又は個人との信頼できる連絡手段を通し検証すると同時に、オプションとして証明書に記載される可能性がある電子メールアドレスをその申請者が管理していることを検証する。
EV Code Signing Certificates	EV ガイドライン及び EV Code Signing 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を検証する。
DV/AlphaSSL Certificates	3.2.7 項に規定されている認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を検証する。
OV SSL & ICPEdu Certificates	3.2.7 項に規定されている方法を通し、申請組織又は個人との信頼できる手段による意思確認を通し検証すると同時に、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。
EV SSL Certificates	EV ガイドラインに従い、契約署名者及び証明書承認者の権限を検証する。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検証する
AATL 及び CDS	申請組織又は個人との信頼できる連絡手段を通し検証すると同時に、電子メールアドレスを証明書に記載する要求があった場合、申請者が電子メールアドレスを管理していることを検証する。マネージド PKI アカウントにより発行された証明書は、プロファイル設定時に、その権限を有する LRA が検証する。
TrustedRoot	組織の申請者との信頼できる連絡手段を通し検証する。トップレベルドメイン/サブドメイン、又は 3.2.7 項で説明されているドメイン名といった、Name Constraints（名前の制限）に含まれる可能性がある全要素を検証する。
Qualified Website Authentication Certificates	3.2.2.3 項に記載の方法に従うと同時に、3.2.2.3 項に記載の方法によってドメイン名の所有又は管理を検証することで、契約署名者又は証明書承認者、及び認証された代理人の権限を検証する。
Qualified Certificate for Electronic Seal	3.2.2.3 項に記載の方法に従って、契約署名者かつ証明書承認者、及び認証された代理人の権限を検証する。
Qualified Certificate for Electronic Signature	3.2.3.4 項に記載の方法によって、個人の申請者による申請について権限を検証する。

3.2.6. 相互運用のための基準

2.1 項に準じる。

3.2.7. ドメイン名の認証

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

1. 乱数をドメインの連絡先に電子メールで送信し、確認した相手からその乱数を用いた返答を受信する審査を通し、申請された FQDN が申請者の管理下にあることを確認する。(BR section 3.2.2.4.2)　又は
2. ドメイン連絡先に架電し、申請者からの FQDN 検証要求についての応答を得る審査を通し、申請された FQDN が申請者の管理下にあることを確認する。(BR section 3.2.2.4.3)　尚、当該方法は 2019 年 3 月 31 日をもって用いられることはなくなる。又は
3. ローカル部分に'admin', 'administrator', 'webmaster', 'hostmaster', 又は'postmaster'を追加し、その直後に@、そのあとに認証済のドメイン名が続く電子メールアドレスに対し、乱数を送信したあと、その乱数を用いた返答を受信する審査を通し、申請された FQDN が申請者の管理下にあることを確認する。(BR section 3.2.2.4.4)
4. 認可されたポート番号を介した HTTP/HTTPS 経由でアクセス可能な認証ドメイン名を含む"/well-known/pki-validation"ディレクトリ下にあるファイル内に、乱数が存在することを確認する審査を通し、申請された FQDN が申請者の管理下にあることを確認する。(BR section 3.2.2.4.6)
5. 認証済のドメイン名上にある DNSTXT レコード内に乱数が存在することを確認する審査を通し、申請された FQDN が申請者の管理下にあることを確認する。(BR section 3.2.2.4.7)
6. 任意の値(BR section 3.2.2.4.13)を電子メールにて DNS CAA Email Contact へ送信し、その任意の値を用いて確認の返信を受けることで、申請された FQDN が申請者の管理下にあることを確認する。

7. 任意の値(BR section 3.2.2.4.14)を電子メールにて DNS TXT Record Email Contact へ送信し、その任意の値を用いて確認の返信を受けることで、申請された FQDN が申請者の管理下にあることを確認する。
8. ドメイン管理者(ドメインの登録者)の電話番号に電話し、申請者が行った FQDN 検証の要求を確認する返答を受けることで、申請された FQDN(BR section 3.2.2.4.15)が申請者の管理下にあることを確認する。
9. DNS TXT Record Phone Contact の電話番号に電話し、ADN 検証を確認する返答を受けることで、申請された FQDN が申請者の管理下にあることを確認する。各通話においては複数の ADN を確認することが可能であり、各 ADN(BR section 3.2.2.4.16)について確認の返答を得るために DNS TXT Record Phone Contact が用いられる。

GlobalSign は、Wildcard FQDN の検証に上記の方法 1～9 を使用する。

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

1. IP アドレスを含む Uniform Resource Identifier によって識別されたウェブページ上の情報を、合意に立脚して変更する審査を通し、IP アドレスが申請者の実質的な管理下にあることを確認する。又は、
2. Internet Assignment Numbers Authority (IANA)又は Regional Internet Registory (RIPE、APNIC、ARINIC、ARINIC、LACNIC)から IP アドレス割り当ての文書を入手すること。又は、
3. reverse - IP アドレスの検索を行い、結果と検出された生じるドメイン名に対する制御を検証すること。又は、
4. 電子メールアドレス又は IANA もしくは類似のレポジトリに記載された電話情報に基づく電子メールによるチャレンジを行うこと。又は、
5. 申請者が要求した IP アドレスに対し申請者が保有する所有権を IP アドレスの認証方法が確証しているという証拠を、認証局が文書化して管理・保管している場合、その他の確認方法を用いる。

3.2.8. 電子メールアドレスの認証

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

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

3.3. 鍵更新申請時における本人確認と認証

GlobalSign は、利用者の証明書について、有効期限が満了する前の鍵の更新(以下、「Re-key」という)申請に対応する。GlobalSign は、証明書のライフサイクル期間における再発行要求にも対応する。再発行は、Re-key の一種の形態であり、Re-key との違いは、再発行を受けた証明書の有効期限が元の証明書と同じとなる点である。GCC においては、Re-key は「更新」と呼ばれている。

3.3.1. 定期的な Re-key とその際の本人確認と権限の認証

- **PersonalSign1 証明書：** ユーザ名・パスワードによる 9 年ごとの再検証が必要
- **PersonalSign2 証明書：** 9 年ごとに本人確認情報の再検証が必要であり、ユーザ名・パスワードによる認証又はその時点で有効期限が満了していない、かつ失効していない証明書を用いたクライアント認証が求められる
- **Noble Energy Certificates：** ユーザ名・パスワードによる 9 年ごとの再検証が必要。又は、現時点で有効期限内かつ失効前の証明書に用いたクライアント認証が必要。
- **PersonalSign3 証明書：** ユーザ名・パスワードによる 6 年ごとの再検証が必要
- **Code Signing 証明書：** ユーザ名・パスワードによる 825 日ごとの再検証が必要
- **EV Code Signing 証明書：** EV ガイドラインや EV Code Signing ガイドラインに従った本人確認情報の再検証が必要であり、ユーザ名・パスワードによる認証が求められる
- **DV SSL 証明書：** ユーザ名・パスワードによる 825 日ごとの再検証が必要
- **OV SSL 証明書：** ユーザ名・パスワードによる 825 日ごとの再検証が必要

- **EV SSL 証明書：** EV ガイドラインに従った本人確認情報の再検証が必要であり、ユーザ名・パスワードによる認証が求められる
- **Time Stamping 証明書：** 取り扱わない
- **CA for AATL 証明書：** ユーザ名・パスワードによる 6 年ごとの再検証が必要
- **PDFSigning 証明書：** Adobe CDS のものは取り扱わない
- **TrustedRoot：** 取り扱わない
- **Alpha SSL：** 取り扱わない
- **NAESB 証明書：** 以下のテーブルに基づいて本人確認が必要

保証レベル	本人確認要件
Rudimentary	有効期限が満了する前の秘密鍵を保持すること。
Basic	有効期限が満了する前の秘密鍵を保持すること。但し、最低 5 年に 1 度は初期登録時と同様のプロセスを実施し、本人確認情報を再検証が必要となる。
Medium	有効期限が満了する前の秘密鍵を保持すること。但し、最低 3 年に 1 度は初期登録時と同様のプロセスを実施し、本人確認情報を再検証が必要となる。
High	有効期限が満了する前の秘密鍵を保持すること。但し、最低年次で初期登録時と同様のプロセスを実施し、本人確認情報を再検証が必要となる。

- **適格 e シール**： ユーザ名・パスワードによる 13 か月毎の再検証が必要
- **適格電子署名：** ユーザ名・パスワードによる 13 か月毎の再検証が必要
- **適格証明書：** EV のガイドラインに別途指定がある場合を除き、ユーザ名・パスワードによる 13 か月毎の再検証が必要

3.3.2. 失効後の再発行とその際の本人確認と権限の認証

証明書の失効後、新しい証明書を発行する場合、利用者は本 CPS の説明する初期登録時と同様のプロセスを実施する必要がある。

3.3.3. 証明書情報変更の際の本人確認の再検証と再認証

証明書内のサブジェクト情報が変更となった場合は、CP/CPS に定められている識別情報の確認手続きを再度実施し、認証された情報を含む新しい証明書を発行すること。

GlobalSign は上記の有効期限を越えた利用を許可しないため、追加の認証を行うことなく証明書の再発行に対応することはない。

3.3.4. 失効後の Re-key とその際の本人確認と権限の認証

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審査を受けなければならない。

3.4. 失効申請における本人確認と権限の認証

GlobalSign は、失効申請について、要求者の権限を検証する。GlobalSign は、失効申請を行う要求者に対して、ユーザ名・パスワードによる認証、証明書に記載されたドメイン名や電子メールアドレスなどが要求者の所有するものであることの確認、ネットワークを経由しない方法で検証済の特定の情報を用いて本人確認を行うなどのチャレンジ・レスポンス方式を用いて、その権限を検証する。

- **PersonalSign1 証明書：** ユーザ名・パスワードによる認証又はオフラインでの検証
- **PersonalSign2/Pro 証明書：** ユーザ名・パスワードによる認証又はオフラインでの検証
- **Noble Energy** ユーザ名・パスワードによる認証又はオフラインでの検証
- **NAESB 証明書：** ユーザ名・パスワードによる認証又はオフラインでの検証
- **PersonalSign3 Pro 証明書：** ユーザ名・パスワードによる認証又はオフラインでの検証

- **Code Signing 証明書：** ユーザ名・パスワードによる認証又はオフラインでの検証
- **EV Code Signing 証明書：** EV ガイドラインに準拠する
- **DV SSL 証明書：** ユーザ名・パスワードによる認証、オフラインでの検証又は OneClickSSL 機能によるドメインの管理権限の検証
- **AlphaSSL 証明書：** オフラインでの検証又は OneClickSSL 機能によるドメインの管理権限の検証
- **OV SSL 証明書 & ICPEdu Certificates：**ユーザ名・パスワードによる認証又はオフラインでの検証
- **EV SSL 証明書：** EV ガイドラインに準拠する
- **Time Stamping 証明書：** オフラインでの検証
- **CA for AATL 証明書：** ユーザ名・パスワードによる認証又はオフラインでの検証
- **PDF Signing for Adobe CDS 証明書：**ユーザ名・パスワードによる認証又はオフラインでの検証
- **TrustedRoot：** オフラインでの検証
- **適格 証明書：** ユーザ名・パスワードによる認証又はオフラインでの検証

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

4. 証明書のライフサイクルに対する運用上の要求事項

4.1. 証明書申請

4.1.1. 証明書の申請者

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

証明書申請は以下のいずれかの方法で提出できる。

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

4.1.2. 登録手続きとそこで負うべき責任

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

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

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

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

(1) GlobalSign が 2018 年 3 月 1 日以前に、第 3.2 項に規定された情報源からデータ又は文書を入手したか、又は証明書を発行する 39 ヶ月前までに検証を完了したこと。
(2) GlobalSign が 2018 年 3 月 1 日以降に、第 3.2 項に規定された情報源からデータ又は文書を入手したか、証明書を発行する 825 日前までに検証を完了したこと。

4.2. 証明書申請手続き

4.2.1. 本人確認と認証の実施

GlobalSign は、本 CPS の規定に従い、本人確認情報の真正性を十分に検証するシステム、手続きを採用している。初回の本人確認は、GlobalSign の検証チーム又は契約している RA が 3.2 項の規定に準拠して実施する。ファックス、電子メールで GlobalSign に提出された申請者の情報は、GCC アカウント、又はパートナーから GlobalSign 提供の API 経由で提出された情報と共に、安全に保管される。初回以降の証明書申請については、ユーザ名・パスワードの単一要素による認証か、又は電子証明書とユーザ名・パスワードの多要素による認証のいずれかを用いて権限を検証する。

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

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

CAA チェックは、名前制約 CA を使用して SSL 証明書を発行する GlobalSign Trusted Root の顧客には必須ではない。

4.2.2. 証明書申請の承認又は却下

GlobalSign は、いずれかの項目について検証を完了することができない場合、証明書申請を却下する。
本 CPS の手順に従い、全ての検証手順が正常に完了すると仮定した場合、GlobalSign は、一般的に、証明書申請を承認するものとする。GlobalSign は、以下の理由により、申請を却下することができる。

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

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

EV 証明書、適格証明書、及び Code Signing 証明書については、検証チームの 2 名が証明書申請を承認しなければならない。GlobalSign は各国で事業を行っているが、GlobalSign が社内で処理できない言語の申請については、当該言語で申請を処理し、文書を翻訳することのできる、適切に研修と経験を積んだ外部の RA に事前審査手続きを委託することができる。

4.2.3. 証明書の申請処理に要する期間

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

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

以下は、証明書申請の処理、及び証明書の発行までに必要な時間の概算である。

- PersonalSign1 証明書： およそ 1 分
- PersonalSign2 証明書： およそ 24～48 営業時間
- PersonalSign2 Pro 証明書： およそ 36～72 営業時間
- Noble Energy 証明書： およそ 1 分（LRA のみ）
- NAESB 証明書： およそ 24～48 営業時間
- PersonalSign3 Pro 証明書： およそ 48～72 営業時間
- Code Signing 証明書： およそ 24～48 営業時間
- EV Code Signing 証明書： およそ 48～96 営業時間
- DV SSL 証明書： およそ [4] 1～5 分
- AlphaSSL 証明書： およそ [4] 1～5 分
- OV SSL 証明書及び ICPEdu 証明書： およそ 24～48 営業時間
- EV SSL 証明書： およそ 48～96 営業時間
- 適格証明書：およそ 48～96 営業時間
- Time Stamping 証明書： およそ 5～10 営業日
- AATL 証明書： およそ 24～48 営業時間
- CDS 証明書： およそ 24～48 営業時間
- Trusted Root： 6～12 週間(テスト、及びオフラインのキーセレモニーの予定調整を含む)

4.3. 証明書の発行

4.3.1. 証明書発行時における認証局の業務

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

GlobalSign は、証明書発行の直接的な要因となり得る RA アカウントについて、多要素認証が行われている事を確認する。これは、GlobalSign が直接運営する RA に限らず、契約に基づいて運営される RA も同じである。エンタープライズ RA、LRA については、CA と直接的な通信を行なわないため、多要素の認証は必須ではない。RA は、CA に提出された全ての情報を検証し、改ざん、不正使用されないようこれらの情報を保護する。

4.3.2. 認証局から利用者への証明書の発行に関する通知

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

4.3.3. 利用者への NAESB 用証明書の発行に関する通知

申請者の本人確認及び権限の検証の結果、証明書が発行できると判断され次第、GlobalSign は証明書を発行し、申請者に通知し、申請者に証明書を提供する。

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

4.4. 証明書の受領

4.4.1. 証明書の受領とみなされる行為

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

4.4.2. 認証局による証明書の公開

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

4.4.3. 認証局からその他のエンティティへの証明書の発行に関する通知

RA、LRA、パートナー又は代理店は、利用者の登録手続きに関与した場合、当該利用者への証明書の発行が通知される。

4.5. 鍵ペアと証明書の利用

4.5.1. 利用者による鍵ペアと証明書の利用

利用者は、秘密鍵が第三者に開示されることのないよう保護しなければならない。GlobalSign は、利用者の秘密鍵の保護義務を規定する利用契約を利用者との間で締結する。秘密鍵は、対になる公開鍵を含む証明書の Key Usage 及び Extended Key Usage フィールドに指定される用途以外に使用してはならない。秘密鍵のバックアップを保持する場合には、オリジナルの秘密鍵と同様に保護しなければならない。秘密鍵の有効期間が経過した際には、利用者はバックアップファイルも含め、全ての鍵を安全に消去しなければならない。

GlobalSign のデジタル署名サービスの場合、及び利用者の同意を得て、GlobalSign は、短期間証明書及び対応する秘密鍵を保護し、管理するものとする。

4.5.2. 依拠当事者による公開鍵と証明書の利用

GlobalSign は、CRL や OCSP など証明書の有効性を検証するサービスによる確認を必要とするなど、依拠当事者が電子証明書の情報に依拠する際の条件を本 CPS に規定する。GlobalSign は、利用者の証明書に依拠するにあたり利用者が依拠当事者に提示すべき条件を規定した依拠当事者規約を、利用者に対し提供する。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

4.6.1. 証明書更新の条件

証明書の更新とは、従前に発行を受けた証明書と同一の情報を記載し、同じ公開鍵(再発行されるべき NAESB 証明書のものを除く)を含む、有効期限の異なる証明書を新たに発行することである。

GlobalSign は、以下の製品・サービスについて、証明書の更新を取り扱う。

- PersonalSign1 証明書： GCC アカウントで更新を取り扱う
- PersonalSign2 証明書： GCC アカウントで更新を取り扱う
- PersonalSign2 Pro 証明書： GCC アカウントで更新を取り扱う
- Nobel Energy 証明書： GCC アカウントで更新を取り扱う
- PersonalSign3 Pro 証明書： GCC アカウントで更新を取り扱う
- Code Signing 証明書： GCC アカウントで更新を取り扱う
- EV Code Signing 証明書： GCC アカウントで更新を取り扱う
- DV SSL 証明書： GCC アカウントで更新を取り扱う
- AlphaSSL 証明書： GCC アカウントで更新を取り扱う
- OV SSL 及び ICPEdu 証明書： GCC アカウントで更新を取り扱う

- EV SSL 証明書： GCC アカウントで更新を取り扱う
- Time Stamping 証明書： マニュアル手続きで更新に対応
- NAESB 証明書： GCC アカウントで更新を取り扱う
- AATL 及び CDS 証明書： GCC アカウントで更新を取り扱う
- 適格 証明書：GCC アカウントで更新を取り扱う
- Managed SSL(マネージド SSL)： サービスに付帯して提供するシステムに再発行機能が搭載されている
- Enterpris マネージド PKI(マネージド PKI)： サービスに付帯して提供するシステムに再発行機能が搭載されている
- Trusted Root： マニュアル手続きで更新に対応

GlobalSign は、以下の条件下で再発行を行う。

- オリジナルの証明書が失効されていないこと
- オリジナルの証明書に記載される公開鍵がなんらかの理由でブラックリストに登録されていないこと
- 証明書に記載されている全ての情報が正しく、改めて検証が必要でないこと

GlobalSign は、(上記の制約条件に基づき)すでに更新済又は Re-key 済の証明書を再更新又は再 Re-key することができる。オリジナルの証明書は更新後に失効してよいが、同じオリジナルの証明書を再度更新、Re-key してはならず、また記載情報を変更してはならない。

4.6.2. 更新の申請者

GlobalSign は、GCC アカウントのログイン認証など、オリジナルの証明書のライフサイクルを管理するアカウントにおける適切なチャレンジ・レスポンスを経て、オリジナルの証明書の利用者が承諾した更新申請を受理する。ITEF の RFC の規定では、更新申請において証明書署名要求(CSR)は必須ではないが、GlobalSign では、「更新」という用語を、同一の公開鍵を使用するものの技術的観点からは Re-key となる手続きを指して使用している。

4.6.3. 証明書更新申請の処理

GlobalSign は証明書更新申請に対し、追加的に情報の提出を求めることがある。

4.6.4. 利用者への新しい証明書の発行に関する通知

4.3.2 項に準じる。

4.6.5. 更新された証明書の受領とみなされる行為

4.4.1 項に準じる。

4.6.6. 認証局による更新された証明書の公開

4.4.2 項に準じる。

4.6.7. 認証局からその他のエンティティへの証明書の発行に関する通知

(規定なし)

4.7. 証明書の Re-key

4.7.1. 証明書の Re-key の条件

証明書の Re-key とは、利用者が古い証明書を代替するために、以下の条件に基づいた新しい証明書を取得するためのプロセスである：

- 従前に発行を受けた証明書と同一の情報(アイデンティティ、ドメイン等)を記載している
- 従前に発行を受けた証明書と同一の有効期限に設定されている
- 従前に発行を受けた証明書のものとは異なる新しい公開鍵を含む

証明書の再発行とは、証明書の有効期限の前に、同一の有効期限で証明書を Re-key した場合、かつ新しい証明書が従前に発行を受けた証明書と同一の有効期限を設定されている場合を指す。

GlobalSign は、以下の製品・サービスについて、証明書の Re-key 又は再発行を取り扱う。

- PersonalSign1 証明書： GCC アカウントで Re-key・再発行を取り扱う
- PersonalSign2 証明書： GCC アカウントで Re-key・再発行を取り扱う
- PersonalSign2 Pro 証明書： GCC アカウントで Re-key・再発行を取り扱う
- Nobel Energy 証明書：GCC アカウントで Re-key・再発行を取り扱う
- PersonalSign3 Pro 証明書： GCC アカウントで Re-key・再発行を取り扱う
- Code Signing 証明書： GCC アカウントで Re-key・再発行を取り扱う
- EV Code Signing 証明書： GCC アカウントで Re-key・再発行を取り扱う
- DV SSL 証明書： GCC アカウントで Re-key・再発行を取り扱う
- AlphaSSL 証明書： GCC アカウントで Re-key・再発行を取り扱う
- OV SSL 及び ICPEdu 証明書： GCC アカウントで Re-key・再発行を取り扱う
- EV SSL 証明書： GCC アカウントで Re-key・再発行を取り扱う
- Time Stamping 証明書： マニュアル手続きで Re-key・再発行に対応
- NAESB Certificates GCC アカウントで Re-key・再発行を取り扱う
- AATL 及び CDS 証明書： GCC アカウントで Re-key・再発行を取り扱う
- 適格証明書：GCC アカウントで Re-key・再発行を取り扱う
- Managed SSL(マネージド SSL)： サービスに付帯して提供するシステムに再発行機能が搭載されている
- Enterpris マネージド PKI(マネージド PKI)： サービスに付帯して提供するシステムに再発行機能が搭載されている
- Trusted Root： マニュアル手続きで Re-key・再発行に対応

GlobalSign は、以下の条件下で Re-key を行う。

- オリジナルの証明書が失効されていないこと
- 新しい証明書に記載される公開鍵がなんらかの理由でブラックリストに登録されていないこと
- 証明書に記載されている全ての情報が正しく、新規に、或いは改めて検証が必要でないこと

GlobalSign は、(上記の制約に基づき)すでに更新済又は Re-key 済の証明書を再 Re-key することができる。オリジナルの証明書は Re-key 後に失効してよいが、同じオリジナル証明書を再度更新、Re-key してはならず、また記載情報を変更してはならない。

4.7.2. 新しい公開鍵を含む証明書の申請者

GlobalSign は、オリジナルの証明書のライフサイクルを管理するアカウントにおける適切なチャレンジ・レスポンスによる認証を経て、オリジナルの証明書の利用者又は利用者を代理して鍵管理の責任を負う組織担当者が承諾した Re-key 申請を受理する。Re-key 申請において証明書署名要求(CSR)は必須であり、これには新しい公開鍵情報を含めなければならない。

4.7.3. 証明書 Re-key 申請の処理

GlobalSign は証明書 Re-key 又は再発行申請を処理するにあたり、追加的に情報の提出を求めることがある。過去に情報を検証してから年数が経過している場合、利用者の本人確認情報を再検証する。再発行の申請では、チャレンジ・レスポンス方式による権限の検証を行うことができる。

4.7.4. 利用者への新しい証明書の発行に関する通知

4.3.2 項に準じる。

4.7.5. Re-key された証明書の受領とみなされる行為

4.4.1 項に準じる。

4.7.6. 認証局による Re-key された証明書の公開

4.4.2 項に準じる。

4.7.7. 認証局からその他のエンティティへの証明書の発行に関する通知

(規定なし)

4.8. 証明書記載情報の修正

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とは、従前に発行を受けた証明書と異なる情報を含む証明書を新たに発行することである。新しい情報を記載した証明書は、従前の証明書と同じ公開鍵を含む場合もあれば、異なる公開鍵を含むこともある。また、有効期限も同じである場合もあれば、異なる場合もある。

- GlobalSign は、情報修正を、新規の証明書発行として取り扱う
- GlobalSign は、過去に更新又は Re-key された証明書の情報を修正して発行することができる。オリジナルの証明書は情報修正後に失効してよいが、同じオリジナル証明書を再度更新、Re-key してはならず、また記載情報を変更してはならない

4.8.2. 証明書記載情報の修正の申請者

4.1 項に準じる。

4.8.3. 証明書記載情報の修正申請の処理

4.2 項に準じる。

4.8.4. 利用者への新しい証明書の発行に関する通知

4.3.2 項に準じる。

4.8.5. 記載情報の修正された証明書の受領とみなされる行為

4.4.1 項に準じる。

4.8.6. 認証局による記載情報の修正された証明書の公開

4.4.2 項に準じる。

4.8.7. 認証局からその他のエンティティへの証明書の発行に関する通知

(規定なし)

4.9. 証明書の失効、効力の一時停止

4.9.1. 失効の条件

証明書の失効とは、CRL にシリアル番号と失効日時を記載し、それにより当該証明書をブラックリスト化する手続きをいう。CRL は失効される証明書に署名したものと同じ秘密鍵を使用してデジタル署名される。CRL へのシリアル番号を記載することにより、依拠当事者はこの電子証明書のライフサイクルが終了していることを確認することができる。GlobalSign は CRL のファイルサイズを適切に管理するため、Code Signing 証明書 (失効から 10 年が経過したもの)を除き、有効期限の到来した失効された証明書については、リストから消去することができる。GlobalSign は、失効の手続きを取る前に、失効申請者の権限を検証する。

利用者証明書の失効は以下の条件に該当する場合、24 時間以内に行われる。

1. 利用者が証明書の失効を希望する旨を書面で(証明書を発行した GlobalSign 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 GlobalSign に通知した場合。
3. GlobalSign 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. GlobalSign が通知の受領或いはその他の手段によって、利用者に利用規約又は約款上の重大な義務違反があったこと、かつ/又は利用者、利用規約、或いは事業機能の予期せぬ終了を認識した場合。
5. ドメイン認証或いは証明書内の FQDN 又は IP アドレスへの管理について検証する際、依拠すべきではない証拠を取得した場合。
6. PSD2 証明書について、その PSP より認証または登録されている所轄官庁から正式な失効申請を受領した場合(又はそうした所轄官庁からの失効申請を認証する場合)。失効の正当理由としては、PSP の権限が失効された際や、証明書に含まれる PSP の役割が失効された際が挙げられる。

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

1. 証明書は、6.1.5 項及び 6.1.6 項に規定されているように、Baseline Requirements のアルゴリズムの種類及び鍵長についての要件にもはや準拠していない。
2. GlobalSign は、証明書が不正使用されたことを示す証拠を取得する。
3. GlobalSign は、ドメイン認証又は証明書内の Fully-Qualified Domain Name 又は IP Address の管理の真正性を信頼すべきではないという証拠を取得する。
4. GlobalSign は、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もしくはサービス契約が終了した場合、又はドメイン名登録者がドメイン名を更新しなかった場合)を認識する。
5. GlobalSign は、ワイルドカード証明書が、不正に誤解を招く下位 FQDN を認証するために使用されたことを認識する。
6. GlobalSign 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。
7. GlobalSign は、証明書が Baseline Requirements 又は GlobalSign の CP 又は CPS に従って発行されたものではないことを認識した。
8. GlobalSign が、証明書に記載される情報のいずれかが正確でないか、誤解を招く恐れがあると判断する。
9. GlobalSign 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。
10. GlobalSign が CRL/OCSP レポジトリの維持管理を継続することに合意することなく、GlobalSign が Baseline Requirements に従った証明書を発行する権利が満了する、失効する或いは破棄された場合
11. GlobalSign の CP 及び/又は CPS により失効が要求された場合
12. 証明書の形式の技術的様式が、アプリケーションソフトウェアサプライヤー又は依拠当事者に容認できないリスクをもたらす(例えば、CA/B Forum は、利用されていない暗号/署名アルゴリズム又は鍵のサイズが容認できない危険性を示し、そのような証明書は、所与の期間内に CA によって失効、置き換えがなされるべきであると判断する可能性がある)。
13. GlobalSign が、利用者の秘密鍵を危殆化する実証済又は証明済の方法、公開鍵に基づいて簡単に計算できる方法(Debian weakey、http://wiki.debian.org/SSLkeys など)を認識した場合。又は秘密鍵を生成するために使用された方法に欠陥があることを示す明確な証拠がある場合。

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

1. 利用者又は組織の管理者が、証明書のライフサイクルを管理する GCC アカウントを通じて証明書の失効を申請する。
2. 利用者は、GlobalSign のサポートチーム又は GlobalSign の登録局へ、認証済み申請を通じて失効を申請する。
3. GlobalSign は、利用者が禁止対象者としてブラ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するか、又は、発見する。
4. 利用者による当該費用の未払い
5. 証明書の失効申請を受けたとき。
6. 証明書が再発行された場合、GlobalSign は、以前に発行された証明書を取り消すことができる。
7. 一定のライセンス契約に基づき、GlobalSign 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。GlobalSign は、本証明書の継続使用が GlobalSign 又は第三者の事業に悪影響を及ぼすと判断する。証明書の利用が GlobalSign 又は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。
8. 告発された、利用者による証明書の有害な利用
9. Microsoft は、専らその裁量で、Code Signing 又は EV Code Signing 証明書を、偽名を含むか、又はマルウェア又は不要なソフトウェアの促進に使用されていると認定した場合、Microsoft は、GlobalSign に連絡し、証明書の失効を要求する。GlobalSign は、商業的に合理的な期間内に本証明書を執行するか、又は Microsoft の要請を受領後 2 営業日以内に Microsoft に例外を申請する。Microsoft は、独自の裁量で、例外を許可又は拒否することができる。Microsoft が例外を認めない場合、GlobalSign は、2 営業日を超えない商業上合理的な期間内に本証明書を失効させる。
10. Microsoft が専らその裁量により、マルウェア又は望ましくないソフトウェアの販売促進に SSL 証明書が使用されていることを特定した場合、Microsoft は、GlobalSign に連絡し、証明書の失効を要求する。GlobalSign は、商業的に合理的な期間内に本証明書を失効するか、又は Microsoft の要請を受領後 2 営業日以内に Microsoft に例外を申請する。Microsoft は、独自の裁量で、例外を許可又は拒否することができる。Microsoft が例外を認めない場合、GlobalSign は、2 営業日を超えない商業上合理的な期間内に本証明書を失効させる。
11. 利用者の死

下位認証局(CA)証明書の失効は、次の場合 7 日以内に行う。

1. 下位 CA は、下位 CA 証明書又は本 CPS の第 1.5.2 条に詳細が記載されている権限を提供する GlobalSign 事業体に対し、GlobalSign が本証明書の失効を申請素ていることを書面で要求する。
2. 利用者は、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 GlobalSign に通知する。
3. GlobalSign は、証明書内の公開鍵に対応する下位 CA の秘密鍵が危殆化した、又は、6.1.5 項及び 6.1.6 項に規定されているように、Baseline Requirements のアルゴリズムの種類及び鍵のサイズの要件をもはや満たさないという合理的な証拠を取得する。
4. GlobalSign は、証明書が不正使用されたことを示す証拠を取得する。
5. GlobalSign は、証明書が Baseline Requirements 又は CP もしくは CPS に従って発行されていないこと、又は下位認証局が Baseline Requirements もしくは CP もしくは CPS を遵守していないことを発見した。
6. GlobalSign は、証明書に表示される情報のいず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 は、何らかの理由で業務を停止し、他の CA 証明書の失効を委託していない。
8. 発行 CA が、CRL/OCSP レポジトリを維持し続けるための調整をしていない限り、Baseline Requirements に基づき証明書を発行する CA 又は下位 CA の証明書発行権利は、満了するか、取り消されるか、又は終了する。
9. 発行 CA の CP 及び/又は CPS により失効が要求される。

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

4.9.2. 失効申請者

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

4.9.3. 失効申請の処理手続き

失効申請の持つ性質と効率化の観点から、GlobalSign はシステムを通じて失効申請者の本人確認を行う。第一に、GCC アカウントを通じて発行した証明書の失効申請を行う方法がある。次に代替方法として、フォックス、郵便、電話などを通じて、ネットワークを経由せずに失効を要求することができる。この場合、GCC アカウントを通じて共有される非公開情報に基づいて、失効申請者の本人確認を行う。また、GCC アカウントが提供されない利用者については、証明書のサブジェクト識別名に関連する一つ以上の要素に対する管理権限を実証する方法で、失効申請権限を検証することもできる。SSL/TLS 証明書については、OneClickSSL 機能によるドメインの管理権限の検証をもって代替とすることが可能である。S/MIME 証明書については、電子メールアドレスの管理権限の検証をもって代替とすることが可能である。
GlobalSign 及び RA は、失効申請の記録を残し、要求者の本人確認を行い、要求者の権限が確認された場合には適切な失効手続きを取る。

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

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

4.9.4. 失効申請までの猶予期間

SSL 証明書及び Code Signing 証明書について、GlobalSign は失効申請までの猶予期間を認めていない。
危殆化の疑いがある場合、脆弱な鍵を使用した場合、発行を受けた証明書に記載された情報に不正確な内容が含まれていた場合などに、利用者が失効を要求する前に必要な対策を取るための時間を指す。利用者は 48 時間の猶予を与えられるが、これを過ぎると GlobalSign は利用者の証明書を失効することができる。利用者、GlobalSign のいずれかが、何らかの理由により失効を処理できない場合、リスク分析を行い、記録する。

4.9.5. 認証局が失効申請を処理すべき期間

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

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

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

GlobalSign は、少なくとも以下の基準に基づいて、失効又はその他の措置が正当化されるかどうかを決定する。
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. 申し立てを行っている主体、及び
4. 関連規則

4.9.6. 失効情報確認に関する依拠当事者への要求事項

証明書に記載された情報を信頼し依拠する前に、依拠当事者は、証明書が適正な目的のために使用されていること、証明書が有効であることを確認しなければならない。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り、IETF の X.509 規格に準拠していることを検証すべきである。これには、認証局鍵識別子(以下、「AKI」という)及びサブジェクト鍵識別子(以下、「SKI」という)の検証を含む。GlobalSign は、依拠当事者が失効情報の検証を容易に行えるよう、以下の URL を証明書に記載する。

- http://crl.globalsign.net
- http://crl.globalsign.com/
- http://crl.globalsign.com/gs/
- http://ocsp.globalsign.com
- http://ocsp2.globalsign.com
- http://crl2.alphassl.com/gs/
- http://crl.alphassl.com/

PDF 署名証明書については、依拠当事者は Adobe ルート CRL も検証することが必要である。この CRL は本 CPS の規定の範囲ではないが、次の URL で参照することができる。http://crl.adobe.com/cds.crl

4.9.7. CRL の発行頻度

エンドエンティティ証明書に CDP(CRL 配布点)が含まれている場合、その CRL は少なくとも 7 日ごと(適格証明書の CRL に対して 24 時間ごと)に更新され、nextUpdate フィールドの値は、thisUpdate フィールドの値から 10 日以内である。

CA 証明書に CDP が含まれている場合、その CDP は、少なくとも 12 ヵ月に 1 回、下位 CA 証明書の失効後 24 時間以内に更新され、nextUpdate フィールドの値は、thisUpdate フィールドの値より 12 ヵ月以内である。

適格証明書については、失効が決定された時点から 60 分以内に全ての失効メカニズムを通して失効ステータスの実態が公表される。そのステータスが遡及することはない。

4.9.8. CRL の最大通信待機時間

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

4.9.9. オンラインでの失効情報の確認

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

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

4.9.10. オンラインでの失効情報の確認の要件

依拠当事者は失効情報を確認しなければならず、これを怠った場合には、全ての保証は無効となる。

利用者証明書のステータスについては:
- GlobalSign は、OCSP を通じて提供される情報を少なくとも 4 日ごとに更新する。このサービスからの OCSP 応答は、有効期限 10 日を超えないものとする。

下位 CA 証明書のステータスについては:
- GlobalSign は、OCSP を通じて提供される情報を、少なくとも(i) 12 ヶ月ごと、及び(ii) 下位 CA 証明書を失効した後 24 時間以内に更新する。

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

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

GlobalSign は、OCSP リクエストに次のデータを含めるよう要求する：
- プロトコルバージョン
- サービス要求
- 対象証明書識別子

4.9.11. その他の方法による失効情報の提供

全ての SSL 証明書には、OCSP URL を含むものとする。

4.9.12. 認証局の鍵の危殆化に伴う特別な要件

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

4.9.13. 証明書の効力の一時停止を行う条件

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

適格証明書には証明書の一時停止は対応していない。

4.9.14. 証明書の効力の一時停止の要求者

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

4.9.15. 証明書の効力の一時停止手続き

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

4.9.16. 証明書の効力の一時停止期限

証明書の一時停止は、証明書の有効期限まで継続することができる。

4.10. 証明書ステータス情報サービス

4.10.1. 運用上の特徴

GlobalSign は証明書のステータス情報を、CRL 配布ポイント及び OCSP レスポンダを通じて公開する。
Code Signing 証明書及び cRLDistributionPoints 拡張子を含む適格証明書では、GlobalSign は、失効した証明書の有効期限から 10 年が経過するまで、CRL 又は OCSP の失効履歴を削除しない。他の種類の証明書の場合、GlobalSign は、失効された証明書の有効期限が過ぎるまで、CRL 又は OCSP 上の失効履歴を削除しない。

4.10.2. サービスを利用できる時間

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

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

4.10.3. 運用上の特性

(規定なし)

4.11. 利用の終了

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

4.12. キーエスクローとリカバリー

4.12.1. キーエスクローとリカバリーのポリシーと手続き

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

4.12.2. 鍵カプセル化とリカバリーのポリシーと手続き

(規定なし)

5. 施設、経営及び運用上の管理

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

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

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

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

5.1. 物理的管理

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

5.1.1. 所在地及び建物

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

5.1.2. 物理的アクセス

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

5.1.3. 電源及び空調

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

5.1.4. 水漏れ

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

5.1.5. 火災安全及び保護

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

5.1.6. メディア　ストレージ(記憶媒体)

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

5.1.7. 廃棄物

GlobalSign は情報の格納に使用された、全てのメディアが放出も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も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

GlobalSign はクリティカルなデータを敷地外にて定期的にバックアップする。バックアップされたデータは敷地外の物理的にセキュアな場所にて保管される。

5.2. 手続き的管理

5.2.1. 信頼された役割

GlobalSign は、審査要員を含む全てのオペレーター及び管理者が信頼された役割の範囲内で稼動していることを保証するものとする。
信頼された役割とは利益相反が不可能なものであり、いかなる人物も単独で 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。

GlobalSign は、関連会社又はこれらの関連会社と関係があることが特定されている個人のために、証明書を購入することがある。GlobalSign の関連会社としては、親会社および子会社、及び GlobalSign と同一の親会社を持つその他の企業がある。

信頼された役割は以下を含む。(但しこれに限定するものではない)

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

5.2.2. タスク毎に必要な人員数

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

5.2.3. 各役割の本人確認及び認証

信頼された役割に指名する前に、GlobalSign は該当者の身元調査を行うものとする。
先に述べた各役割は、認証局をサポートする為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為に本人確認及び認証が行われている。

5.2.4. 職務分掌を要する役割

GlobalSign は、認証局設備、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
- CA システムのインストール、構成、及び維持管理を行う者
- 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
- 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 システムの開発者

5.3. 人員コントロール

5.3.1. 資格、経験及び許可条件

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

5.3.2. バックグラウンドチェック手続き

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

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

5.3.3. 研修要件

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

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

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

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

5.3.4. 再研修の頻度及び条件

信頼された役割に任命されている全ての人員は 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。

信頼された役割の責任を負う者は、GlobalSign 又は RA における変更点について、適用される場合は認識しているものとする。運用に顕著な変更が出る場合は研修（認知/周知徹底のための）計画が作成され、またこの計画の実行は文書化されるものとする。

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

5.3.5. 職務のローテーション頻度及び条件

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

5.3.6. 不正行為に対する処罰

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

5.3.7. 個別契約者の要件

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

5.3.8. 個人に付与された書類について

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

5.4. 監査ログの手続き

5.4.1. 記録されるイベントの種類

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

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

GlobalSign は証明書申請を処理し、証明書を発行するために取られた措置の詳細を記録する。これには、証明書申請時に生成された全ての情報及び受領した書類、日時、及び関係する人員が含まれる。GlobalSign はこれらの記録を、「はじめに」に規定される関連する CA 監査要件に CA が準拠していることを証明するものとして、正規の監査人が利用できるようにする。

GlobalSign は少なくとも下記のイベントを記録する：
下記を含む認証局の鍵のライフサイクル管理に関わるイベント：

- 鍵の生成、バックアップ、保管、復旧、アーカイブ、及び破壊
- 暗号装置のライフサイクル管理に関わるイベント、及び
- CA システムの機器設定

下記を含む、CA 及び利用者の証明書ライフサイクル管理に関わるイベント

- （成功/失敗に関わらず）証明書申請、更新、鍵の再設定、失効
- 失効及び有効期限切れの証明書を含む全証明書
- 本 CPS で規定された全ての審査活動
- 審査時の電話掛けの日時、電話番号、通話相手のお客様、及び結果
- 証明書申請の合否
- 証明書の発行、及び
- 証明書への読み書きが失敗した場合を含む CRL 及び OCSP エントリ及び CRL のディレクトリの生成、また実際の CRL

下記を含む、セキュリティ関連のイベント：

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

5.4.2. ログ処理の頻度

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

5.4.3. 監査ログの保有期間

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

5.4.4. 監査ログの保護

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

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

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

5.4.5. 監査ログバックアップ手続き

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

5.4.6. 監査ログ収集システム(内部 vs.外部)

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

5.4.7. イベント発生要因の対象への通知

(規定なし)

5.4.8. 脆弱性の査定

GlobalSign は下記内容の年次リスク評価を実施する：

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

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

5.5. アーカイブ対象記録

5.5.1. アーカイブ対象記録の種類

GlobalSign 及び RA は、署名及び認証局システムの正当な運用の正当性を証明するために十分な詳細が含まれる記録をアーカイブするものとする。

5.5.2. アーカイブの保有期間

GlobalSign は証明書の発注、認証、全証明書及び失効に関する全書類を、その書類に関する証明書の有効期限が切れてから少なくとも 10 年間保持するものとする。

5.5.3. アーカイブの保有

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

5.5.4. アーカイブ　バックアップ　手続き

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

5.5.5. データのタイムスタンプについての条件

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関わらず、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(内部又は外部)

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

5.5.7. 取得手続き及びアーカイブ情報の検証

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

5.6. 鍵交換

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

5.7. 危殆化及び災害からの復旧

5.7.1. 事故及び危殆化に対する対応手続き

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

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

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

万一いずれの設備が損壊又は操作不能な状態で、しかしながら署名鍵が損壊していない場合、GlobalSign の事業継続計画に基づき証明書の状態情報の生成を優先し、可能限り早急に再構築されるものとする。

5.7.3. エンティティの秘密鍵が危殆化した際の手続き

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

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

5.7.4. 災害後の事業継続能力

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

5.8. 認証局又は RA の稼動終了

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

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

5.8.1. 業務を引き継ぐ認証局

業務を引き継ぐ認証局は、認証局の業務終了によりその鍵とデジタル証明書が失効した全ての下位のサービスプロバイダと利用者に対して、各サービスプロバイダ又は利用者の行う新しいデジタル証明書の申請に基づいて、初回の登録と本人確認及び審査要件の具備を条件として、新規のサービスプロバイダ契約又は証明書保有者契約を締結したうえで、新たに鍵とデジタル証明書を発行するものとする。

6. 技術的セキュリティ管理

6.1. 鍵ペア生成及びインストール

6.1.1. 鍵ペア生成

6.1.1.1 CA 鍵生成

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 がキーセレモニーに従い、鍵ペアの完全性及び機密性を確保するために使用されるコントロールを遵守した旨の報告書を発行する。

その他 CA の鍵ペアに対しては、下記の管理を行う：

1. CP 及び/又は CPS の 5.1 項及び 5.2.2 項に記載されている通り物理的に安全な環境で鍵を生成する

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

6.1.1.2 利用者の鍵ペア生成

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

適格証明書については、利用者鍵が生成され、認められた適格署名作成装置(QSCD)内に格納される。
QSCD 認定のステータスを監視し、ステータスが変更された場合には適切な措置を講じる。

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 GlobalSign は、鍵生成の工程から利用者への証明書発行過程において、十分なセキュリティが保たれている時にのみ、それを担うことができる。SSL/TLS 証明書に関しては、秘密鍵及び証明書を含む、最短 16 文字のパスワードで暗号化された PCKS#12 (.pfx)ファイルを使用することで、上記の条件を満たす。証明書の申請時に最低 8 文字の文字列がシステムにより生成され、利用者に提供された上で利用者が最低 8 文字の文字列を指定する。SMIME 証明書に関しては、秘密鍵及び証明書を含む、利用者が選択した最低 12 文字のパスワードで暗号化された PCKS#12(.pfx)ファイルを使用することで上記の条件を満たす。

GlobalSign は公的に信頼された SSL 証明書用の秘密鍵は生成しない。

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

6.1.3. 証明書発行元へ公開鍵の配布

GlobalSign は、RA から伝送される経路が保護されており、その根源についての真正性と完全性が適切に検証された公開鍵のみを受け入れる。
RA は本 CPS の 3.2.1 項に準拠している場合のみ、利用者からの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

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

6.1.5. 鍵のサイズ

GlobalSign は、国立標準技術研究所（NIST）の特刊 800-133(2012 年)-暗号鍵生成勧告-ルート認証局、発行 CA、及び利用者用の鍵ペアの選択において推奨されるタイムライン及びベストプラクティスについて-に準拠している。また GlobalSign の直接管理下にない、信頼されたルートプログラムに属する下位認証局も同様のベストプラクティスを実行することが契約上義務付けられているものとする。GlobalSign は、以下の鍵のサイズ/ハッシュ値からルート証明書、発行 CA の証明書、エンドエンティティ証明書、並びに CRL/OSCP 証明書のステータスレスポンダを選択する。これらの選択肢は SSL の Baseline Requirements 及び EV ガイドラインに準拠している。

証明書はアルゴリズムの種類、鍵のサイズに関して下記の要件を満たさなければならない。

ルート CA 証明書

	有効期間は 2010 年 12 月 31 日より、又はそれ以前より開始する	有効期間は 2010 年 12 月 31 日以降に開始する

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 [5]	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

	有効期間は 2010 年 12 月 31 日より、又はそれ以前より開始し、2013 年 12 月 31 日に、又はそれ以前に終了する。	有効期間は 2010 年 12 月 31 日以降に開始し、2013 年 12 月 31 日以降に終了する。
ダイジェスト アルゴリズム	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1 [6], 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 [7], 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 [8]	

6.1.6. 公開鍵パラメーター生成及び品質検査

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

6.1.7. 鍵の使用目的(X.509 v3 鍵使用フィールドにおいて)

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

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

1. ルート CA 自身を表すための、自己署名証明書
2. 下位認証局及び相互認証の証明書
3. インフラストラクチャの目的(管理職の証明書、Internal CA を運営する機器の証明書)を想定した証明書
4. OCSP からのレスポンスを検証する証明書

[5] 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。
[6] SHA-1 は、イントラネット SSL 利用者及び下位認証局の証明書に使用されているが、公的に信頼されるルートには関連付けられていない。
[7] SHA-1 は、7.1.3 項で定義された基準に従って、PersonalSign 証明書及び Code Signing 証明書用の RSA 鍵と併用可能。
[8] 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。

6.2. 秘密鍵保護及び暗号化モジュール技術管理

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

6.2.1. 暗号化モジュール規定及び管理

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

6.2.2. 秘密鍵(m 中の n) 複数の人員による管理

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

6.2.3. 秘密鍵の第三者委託

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

6.2.4. 秘密鍵のバックアップ

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

6.2.5. 秘密鍵のアーカイブ化

GlobalSign のデジタルサイニングサービス(DSS)を除き、GlobalSign は利用者の秘密鍵のアーカイブを行なわず、秘密鍵の生成過程で鍵が存在していた可能性のある一時的な記憶場所からも削除されることを保証する。

6.2.6. 暗号モジュール間の秘密鍵移行

GlobalSign 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(保存もしくは移行のため)にある場合は、暗号化されていることが必須となる。秘密鍵は、暗号モジュール外の環境にて、一般テキスト状態で存在しては絶対にならない。
万が一、下位 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 GlobalSign が認識した場合、GlobalSign は付与された秘密鍵に対応する公開鍵を含む全ての証明書を失効させる。

6.2.7. 暗号モジュールにおける秘密鍵の保存

GlobalSign は少なくとも FIPS140－2 レベル 3 もしくはそれ以上のデバイスにおいて保存するものとする。

6.2.8. 秘密鍵のアクティブ化方法

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

6.2.9. 秘密鍵の非アクティブ化方法

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

6.2.10. 秘密鍵の破棄方法

GlobalSign の秘密鍵は、不必要となった時点も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 GlobalSign は秘密鍵の如何なる部分も推定されないよう、HSM 内の関連する認証局の秘密アクティブ化データ全てを破棄する必要がある。
GlobalSign が生成した秘密鍵は、鍵ペアが利用者に取得されるまでの間 PKCS 12 形式で GCC に保管される。利用者の鍵ペアは、利用者が鍵ペアを受け取った時点、又は鍵生成から 30 日経過した時点で自動的に消去される。利用者の秘密鍵はその他の GlobalSign のシステムでは保管しないものとする。

6.2.11. 暗号モジュール　評価

6.2.1 項を参照

6.3. その他鍵ペア管理の要素

6.3.1. 公開鍵のアーカイブ化

GlobalSign は証明書の公開鍵をアーカイブ化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

GlobalSign が認証及び更新する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	秘密鍵　用途	最長証明期間
ルート証明書	25 年	30 年
TPM ルート証明書	30 年	40 年
パブリックな下位 CA/発行 CA	11 年	17 年
Trusted Root	規定無し	10 年
PersonalSign の証明書	規定無し	39 ヶ月
Nobel Energy 証明書	規定無し	5 年
Code Signing 証明書	規定無し	39 ヶ月
EV Code Signing 証明書	規定無し	39 ヶ月
AATL エンドエンティティ証明書	規定無し	39 ヶ月
適格 e シール、適格電子署名	規定無し	36 ヶ月
DV SSL 証明書	規定無し	825 日
AlphaSSL 証明書	規定無し	825 日
OV SSL & ICPEdu 証明書	規定無し	825 日
イントラネット SSL	規定無し	5 年
EV SSL 証明書	規定無し	27 ヶ月
Timestamping 証明書	11 年	11 年
Adobe CDS 用の PDF 署名	規定無し	39 ヶ月
NAESB 証明書	2 年	2 年
適格証明書	規定無し	27 ヶ月

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、その鍵ペアの運用期間終了までに失効しなければならない。

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

6.4. アクティブ化データ

6.4.1. アクティブ化データ生成及びインストール

GlobalSign の秘密鍵をアクティブ化する為に使用される、GlobalSign のアクティブ化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。アクティブ化データは適切な HSM(ハードウェアセキュリティモジュール)により自動的に生成、又は同じニーズを満たすような方法で生成される。その後、信頼された役割を担う鍵の持分所有者に配布されるものとする。配布方法においては、アクティブ化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. アクティブ化データの保護

発行 CA のアクティブ化データは、暗号化及び物理的なアクセス管理の仕組みを介して漏洩から保護されなければならない。GlobalSign のアクティブ化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. その他のアクティブ化データの要素

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

6.5. コンピュータ　セキュリティ　コントロール

6.5.1. 特定のコンピュータ　セキュリティ技術条件

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

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

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

6.5.2. コンピュータ　セキュリティの評価

GlobalSign の中核となるソフトウェアのバージョンはコモンクライテリア EAL4+に認定されている。

6.6. ライフサイクル　技術管理

6.6.1. システム開発管理

GlobalSign におけるシステム開発管理は以下の通り。

- 正式かつ書面化された開発方法にて設計並びに開発されたソフトウェアを使用しなければならない
- 全てのハードウェアは、供給の適合性、及び改ざんの証拠がないことを保証するために試運転の過程で検査されるものとする。入手したハードウェア及びソフトウェアは、どの特定の部品においても改ざんされうる可能性を低減する方法で購入されたものであること。(例：購入時に機器が無作為に選択されたものであることを確認するなど)
- 開発されたハードウェア及びソフトウェアが管理された環境において開発され、開発プロセスが定義された上で文書化されていること。この条件は商業的に流通するハードウェア及びソフトウェアには適用されない
- これらのハードウェア及びソフトウェアで行なう業務は認証局の業務に限定される。認証局の運営に関係のないアプリケーション、ハードウェアデバイス、ネットワーク接続又はインストールされたソフトウェアは存在しない。

- 正しい管理方法により不正なソフトウェアの機器への搭載を防いでいる。認証局の業務を行なうのに必要なアプリケーションのみが機器にインストールされ、ローカルポリシーにより認可されたソースから入手される。GlobalSign のハードウェア及びソフトウェアは、最初の使用時及びその後定期的に不正コードの検知の為にスキャンされる。
- ハードウェア及びソフトウェアの更新版は、元の機器と同様の条件で購入又は開発され、また信頼され教育を受けた人員によって、定められる条件に基づきインストールされる。

6.6.2. セキュリティ マネージメント コントロール

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

6.6.3. ライフサイクル セキュリティ コントロール

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

6.7. ネットワーク セキュリティ コントロール

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

6.8. タイムスタンプ

GlobalSign の全コンポーネント定期的に信頼できるタイムサービスとの同期を行う。GlobalSign は 1 つの GPS ソース、1 つの DCF77 ソース及び 3 つの非認証の NTP ソースのクロックを、正確な時刻を確立するために使用する。

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

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

6.8.1. PDF 署名タイムスタンピングサービス

CDS 利用者のデジタル ID によって作成される全てのデジタル署名には、RFC3161 に準拠し、Adobe ルート証明書にチェーンされたタイムスタンプ局(TSA)によって発行されたタイムスタンプを含むことができる。当該 TSA の証明書は FIPS140-2 レベル 2 かそれ以上の HSM に格納されなければならない。タイムスタンピングサービスは GlobalSign 又は GlobalSign が業務委託した代行業者によって提供される。タイムスタンピングサービスが代行業者によって管理されている場合、GlobalSign は当該 CPS に従ってタイムスタンピング証明書を発行する。

6.8.2. CodeSigning 及び EV CodeSigning タイムスタンピングサービス

CodeSigning 又はに EV CodeSigning よって作成される全てのデジタル署名には、RFC3161 に準拠し、GlobalSign ルート CA にチェーンされたタイムスタンプ局(TSA)によって発行されたタイムスタンプを含むことができる。当該 TSA の証明書は FIPS140-2 レベル 2 かそれ以上の HSM に格納されなければならない。タイムスタンピングサービスは GlobalSign 又は GlobalSign が業務委託した代行業者によって提供される。タイムスタンピングサービスが代行業者によって管理されている場合、GlobalSign は CPS に従ってタイムスタンピング証明書を発行する。

7. 証明書、証明書失効リスト、及びオンライン証明書ステータスプロトコルのプロファイル

7.1 証明書プロファイル

7.1.1. バージョン番号

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

7.1.2. 証明書拡張子

GlobalSign は、RFC5280 及び現在の CA/B Forum Baseline Requirements の 7.2.1.1 から 7.2.1.5 項を含む適用可能なベストプラクティスに従い、証明書を発行するものとする。名前の制限(NameConstraints)が設定された場合、依拠当事者を不要なリスクから守るために、重要度(クリティカリティ)についてはベストプラクティスに従って設定される。

7.1.3. アルゴリズム対象識別

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

SHA1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}
SHA256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
SHA384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
ECDSAWithSHA1	{iso(1) member-body(2) us(840) ansi - X9 - 62 (10045) signatures(4) 1 }
ECDSAWithSHA224	{iso(1) member - body(2) us(840) ansi - X9 - 62 (10045) signatures(4) ecdsa - with - SHA2(3) 1 }
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)}

7.1.4. 名称形式

GlobalSign は、RFC5280 に従う名称形式にて証明書を発行するものとする。また、公的に信頼されたルートにチェーンされている SSL 証明書及び EV CodeSigning 証明書に関しては、CA/B Forum Baseline Requirements の 7.1.4 項に準拠して発行する。

RFC 5280 の 4.1.2.4 項に記載の Name フィールドのチェーンに対応するため、証明書内の項目、発行者の識別名は発行 CA のサブジェクト識別名と一致していなければならない。

7.1.5. 名前の制限

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

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

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

- GlobalSign は Baseline Requirements バージョン 1.3 以降の 7.1.5 項に従い、id-kp-emailProtection extended key usage の証明書にも dNSName、iPAddress、及び DirectoryName に名前の制限(NameConstraints)をかけることも可能である。

7.1.6. 証明書ポリシー識別子

(規定なし)

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成と意味

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

7.1.9. クリティカルな証明書ポリシー拡張についての解釈方法

(規定なし)

7.1.10. シリアル番号

各発行 CA は、CSPRNG からの最低 64 ビットのアウトプットを含む、0 以上の連番でない独自の（発行者サブジェクト識別名及び CA 証明書シリアル番号内のコンテクスト）証明書シリアル番号を含む証明書を発行しなければならない。

7.1.11. 適格証明書の特約

7.1.11.1. 適格署名

適格署名証明書には次の適格命令文が含まれる。

- esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcCompliance } id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
- esi4-qcStatement-4 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcSSCD }
- id-etsi-qcs-QcSSCD OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }
- esi4-qcStatement-6 QC-STATEMENT ::= { SYNTAX QcType IDENTIFIED BY id-etsi-qcs-QcType } Id-etsi-qcs-QcType OBJECT IDENTIFIER ::= { id-etsi-qcs 6 } QcType::= SEQUENCE OF OBJECT IDENTIFIER (id-etsi-qct-esign)

7.1.11.2. 適格シール証明書

適格シール証明書には次の適格命令文が含まれる。

- esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcCompliance } id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
- esi4-qcStatement-4 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcSSCD }
- id-etsi-qcs-QcSSCD OBJECT IDENTIFIER ::= { id-etsi-qcs 4 }
- esi4-qcStatement-6 QC-STATEMENT ::= { SYNTAX QcType IDENTIFIED BY id-etsi-qcs-QcType } Id-etsi-qcs-QcType OBJECT IDENTIFIER ::= { id-etsi-qcs 6 } QcType::= SEQUENCE OF OBJECT IDENTIFIER (id-etsi-qct-eseal)

7.1.11.3. 適格証明書

適格証明書には次の適格命令文が含まれる場合もある。

- esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcCompliance } id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }

- id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 }
- esi4-qcStatement-6 QC-STATEMENT ::= { SYNTAX QcType IDENTIFIED BY id-etsi-qcs-QcType } Id-etsi-qcs-QcType OBJECT IDENTIFIER ::= { id-etsi-qcs 6 } QcType::= SEQUENCE { qcType OBJECT IDENTIFIER {{id-etsi-qct-web}}}CRL Profile

7.1.12. バージョン番号

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

- 発行者 GlobalSign XXX 等(製品による)
- 有効開始日 日付及び時間
- 次回更新日 日付及び時間
- 署名アルゴリズム sha1RSA, sha256RSA 等(製品による)
- 署名ハッシュアルゴリズム sha1, sha256 等(製品による)
- シリアル番号 失効された証明書のシリアル番号
- 失効日 失効日

7.1.13. 証明書失効リスト及び証明書失効リストエントリー拡張子

CRL は、以下の拡張子(エクステンション)を含む。

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

7.2 オンライン証明書ステータスプロトコル プロファイル

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

7.2.1. バージョン番号

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

- レスポンダ ID レスポンダの公開鍵の SHA-1 ハッシュ
- 生成時間 OCSP レスポンスが署名された時間
- 証明書ステータス 問い合わせを受けた証明書のステータス(有効/失効済み/不明)
- ThisUpdate/NextUpdate レスポンスの推奨有効期間
- 署名アルゴリズム SHA-1 RSA、SHA256 RSA 等(商材により異なる)
- 署名 レスポンダにより生成された署名
- 証明書 OCSP レスポンダの証明書

OCSP リクエストは下記のデータを含む必要がある：

- プロトコルのバージョン
- サービスリクエスト
- ターゲット証明書の識別子

7.2.2. オンライン証明書ステータスプロトコル 拡張子

OCSP リクエストにナンスフィールドが含まれている場合、対応するレスポンスも同じナンスを返送する。

8. 準拠性監査及びその他の評価

本 CPS に記載される手続きは、GlobalSign 運用が関与する複数の垂直的 PKI 業界に対する PKI 標準のうち、現状で適用可能な部分について網羅している。

dNSNameConstraints による制約を受けない Trusted Root CA は、下記の規定について準拠性監査を受ける。

- AICPA/CICA Trust Service Principles and Criteria for Certification Authorities
- AICPA/CICA WebTrust for Certification Authorities – Extended Validation Audit Criteria
- AICPA/CICA WebTrust Principles and Criteria for Certification Authorities – Code Signing
- AICPA/CICA WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing
- AICPA/CICA WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

8.1. 評価の頻度及び状況

GlobalSign は、資格を有する監査人を介して、AICPA は 1 年に 1 度、eIDAS は 1 年に 2 度、上述の AICPA/eIDAS の標準準拠性について継続的に評価するものとする。

8.2. 評価者の身元及び能力

GlobalSign の監査は、下記の要件と能力を有する公認監査人である Ernst & Young によって行われる。

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

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

8.3. 評価者と被評価者の関係

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

8.4. 評価対象項目

監査は、8.0 項に記載される、評価のための監査スキームの要件を満たさなければならない。これらの要件は、監査スキームの変更に伴って更新される可能性がある。更新された監査スキームは、それが採用された次年度から GlobalSign に対して適用可能となる。

8.5. 結果が不備である場合の対応

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

8.6. 結果についての連絡

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

8.7. 自己監査

GlobalSign は、発行された証明書のうち、少なくとも 3%(EV SSL 証明書及び EV Code Signing 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、少なくとも四半期ごとに自己監査を実施することにより、CP、CPS、及び「確認事項」の項に明記されたその他外部要件の準拠性を監視し、サービス品質を厳格に管理する。

9. その他ビジネス及び法的事項

9.1. 費用

9.1.1. 証明書発行及び更新費用

GlobalSign は証明書の発行及び更新に対して費用を請求できるものとする。また GlobalSign は、再発行(当該証明書の有効期間内における Re-key)に対しては費用を請求しない。費用及びそれに関連する約款は、申し込みの過程の WEB インターフェース及び GlobalSign の複数の言語の WEB サイト上にある営業・マーケティング資料を通じて、申請者に対して明確に提示されるものとする。

9.1.2. 証明書アクセス費用

GlobalSign は発行済み証明書を格納するデータベースへのアクセスに対して、費用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費用

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

9.1.4. その他サービスの費用

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

9.1.5. 返金ポリシー

GlobalSign は利用者に対し、GlobalSign の Web サイト https://www.globalsign.com/repository に掲載されている返金ポリシーに沿って、返金をする。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

GlobalSign nv/sa は、少なくとも 200 万米ドル($2,000,000)上限ポリシーの一般賠償責任保険を、また業務過誤や専門職業人賠償責任**保険**については、少なくとも 500 万米ドル($5,000,000)上限ポリシーの保険を保有するものとする。発行 CA の保有する保険のカバー範囲は、(1)EV 証明書の発行及び維持における行動、過失、不備、意図的ではない契約違反や不履行に対する損害請求、(2)如何なる第三者の所有権の侵害（コピーライト、特許、及び商標の侵害を除く）、プライバシーの侵害、及び広告侵害により生じた損害に対する請求、である。

保険会社は、現行版の最良の保険ガイド（又は格付け対象企業を会員とする企業団体）において評価が A- よりも上の評価を受けた会社であり、ここを通じて保険が提供されるものとする。

9.2.2. その他資産

(規定なし)

9.2.3. エンドエンティティに対する保険もしくは保証

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

9.3. 業務情報の機密性

9.3.1. 機密情報の範囲

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

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

9.3.2. 機密情報の範囲外に属する情報

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

9.3.3. 機密情報保護の責任

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

9.4. 個人情報保護

9.4.1. 保護計画

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

9.4.2. 個人情報として取り扱われる情報

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

9.4.3. 個人情報とみなされない情報

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

9.4.4. 個人情報保護の責任

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

9.4.5. 個人情報使用についての通知及び合意

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

9.4.6. 法的又は管理処理に従う開示

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

9.4.7. その他情報開示の場合

(規定なし)

9.5. 知的財産権

GlobalSign は第三者の知的財産権を、故意に損わないものとする。公開鍵及び秘密鍵はこれを正当に保持する利用者の財産である。GlobalSign は証明書の所有権を保持するものではあるが、その証明書が完全な形で複製・配布されるという条件にて、この証明書の複製・配布を利用者に非独占的かつ無償で許諾するものである。

GlobalSign®　及び GlobalSign のロゴは、GMO グローバルサイン株式会社(GMO GlobalSign K.K.)の登録商標である。

9.6. 表明保証

9.6.1. 認証局の表明保証

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

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

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

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

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

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

- **法的存在:** GlobalSign は、証明書が発行された日現在、当該証明書に記名されているサブジェクトが設立又は登録管轄区域内で有効な団体又は事業体として法的に存在することを、そのサブジェクトの設立又は登録管轄区域内の設立又は登録機関と確認する。
- **識別**: GlobalSign は、証明書が発行された日現在、証明書に記名されているサブジェクトの正式名称が、サブジェクトの設立又は登記管轄区域における設立又は登記機関の公式記録に記されている名称と一致していること、及び仮名が含まれている場合、その仮名がその事業所の管轄区域において、サブジェクトにより適切に登録されていることを確認する。

- **ドメイン名を使用する権利:** EV 証明書についてのみ、GlobalSign は、証明書が発行された日現在、証明書に記名されているサブジェクトが、証明書に記載された全てのドメイン名を使用する権利を有することを確認するために、合理的に必要な全ての措置を講じる。
- **EV 証明書の発行許可確認:** GlobalSign は、証明書に記名されているサブジェクトが証明書の発行を許可したことを確認するために、合理的に必要な全ての措置を講じる。
- **情報の正確性:** GlobalSign は、証明書が発行された日現在、証明書内の全ての情報が正確であることを検証するために合理的に必要な全ての措置を講じる。
- **利用契約:** 証明書に記名されているサブジェクトは、法的に有効かつ強制力のある利用契約を、該当ガイドラインの要件を満たす CA と締結する、又は、関連会社の場合、申請者の代表者は、利用条件を確認、同意する。
- **ステータス:** GlobalSign は、EV 及び EV Code Signing ガイドライン(該当する場合)の要件に従い、年中オンラインアクセス可能なレポジトリにおいては、証明書の有効又は失効のステータスに関する最新の情報を維持する。
- **失効:** GlobalSign は、EV 及び EV Code Signing ガイドラインの要件に従い、EV 及び EV Code Signing ガイドラインに明記された失効理由のいずれかに基づき、証明書を失効する。

9.6.2. 登録局(RA)の表明保証

RA は以下を保証する。

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

9.6.3. 利用者の表明保証

利用者及び申請者は下記の項目を保証する。

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

確認及び受諾: 申請者が利用契約又は利用条件の諸条件に違反した場合、又はフィッシング攻撃、詐欺、マルウェアの配布などの犯罪行為に証明書が使用されていることを GlobalSign が発見した場合、GlobalSign は、証明書を執行する権利を有することを申請者は確認し、受諾する。

9.6.3.1. 北米エネルギー規定委員会(NAESB)利用者

WEQ-012 の申請に証明書を使用する Business Practice Standard WEQ-012 v 3.0 に加入するエンドエンティティは NAESB EIR に登録し、電気再販業務に従事することが許可されていることを提示しなければならない。また、NAESB WEQ PKI Standards に定められた認証方法を利用したアプリケーションにアクセスする必要があるが、卸電気業者の資格を持たないエンティティや組織(規制当局、大学、コンサルティング会社等)も NAESB EIR に登録する必要がある。

登録されたエンドエンティティ及びそのユーザコミュニティは、これらの NAESB WEQ PKI Standards に定められたエンドエンティティの義務を全て果たす必要がある。

各利用者組織は NAESB WEQ PKI Standards に定められている以下の義務について理解していることを、GlobalSign を通じて示さなければならない。

各利用者組織は以下の NAESB WEQ PKI Standards の項目を確認し、同意していることを認証局に対して証明しなければならない。

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

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

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

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

また、エンドエンティティは以下の要件にも準拠しなければならない。

- 自分の秘密鍵を他者からのアクセスから保護すること
- 該当する場合、NAESB EIR を通し、GlobalSign を認定認証局として選んだエンティティを識別すること
- GlobalSign がエンドエンティティに安全な電子通信を提供するのに使用される証明書を発行するために必要な当 CPS に規定されている通り、全ての同意書及び契約書に準拠すること
- 当 CPS に規定されている全てエンドエンティティの義務に準拠すること、例えば、証明書申請手続き、申請者識別証明/審査、及び証明書管理手続き等に関して。
- PKI 証明書管理プログラムがあり、プログラムに参加する全ての従業員がトレーニングを受けること、また、当該プログラムへ準拠していることを確認すること。PKI 証明書管理プログラムは以下を含むが、それに限定されない。
  - 証明書秘密鍵セキュリティ及び運用ポリシー
  - 証明書失効ポリシー
- 利用者の本人確認情報を識別し(個人、役職、デバイス、も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

発行 CA の証明書を参照（依拠）する依拠当事者は下記の項目を保証する。

- 証明書を使用する技術的能力を有している
- 発行 CA 及び依拠当事者に関連する諸条件についての通知を受領する
- 正しい証明書パス検証手続きに従って発行局から発行された、証明書ステータス情報（例：CRL 又は OCSP）を使用して発行 CA の証明書を検証する
- 正確かつ最新版の検証方法により、証明書の全情報が検証される場合にのみ、発行 CA の証明書を信頼する
- 妥当であると判断される状況においてのみ、発行 CA の証明書に依拠する
- 依拠当事者が、秘密鍵が危殆化した可能性を察知した場合、適切な RA に直ちに通知する

依拠当事者が当該証明書に依拠することに妥当性があると判断した場合、その義務事項として下記が発生する。

- 依拠当事者に提示される現状の失効ステータス情報を使用して、認証局の証明書の有効又は失効を検証する

- 証明書もしくは本 CPS にて依拠当事者に示された、証明書の使用に関する全ての制限事項について注意を払う
- アプリケーションコンテキストによって提示されるその他のポリシー或いは規約と同様、発行 CA の証明書中の規定に関しても十分な注意を払う

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

9.6.4.1. 北米エネルギー規定委員会（NAESB）の依拠当事者

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

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

9.6.5. その他関係者の表明保証

（規定なし）

9.7. 保証の免責事項

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

9.8. 有限責任

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

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

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

9.9. 補償

9.9.1. GlobalSign による補償

GlobalSign は、アプリケーションソフトサプライヤー（ブラウザベンダー等）に対し、当 CA 発行の Extended-SSL 証明書、或いは Code Signing に関連して被ったところのいかなるクレーム、損害、或いは損失に対し、その訴因、法的根拠に拘わらず、これを防御し、補償し、免責しなければならない。

但し、これらサプライヤーが(1)有効かつ信頼性のあるＥＶ証明書を、(誤って)無効或いは信頼性欠如と表示してあった場合、また逆に(2)(ⅰ)期限終了の証明書、(ⅱ)失効された証明書、などについて失効情報がオンラインで確認可能な状況でありながら(誤って) これを信頼性ありと表示したような場合は除く。

9.9.2. 利用者による補償

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

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

9.9.3. 依拠当事者(1.3.4 参照)による補償

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

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

9.10. 期間及び終了

9.10.1. 期間

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

9.10.2. 終了

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

9.10.3. 終了の効果と存続

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

9.12. 改正条項

9.12.1. 改正手続き

本 CPS に対する変更があった場合は、適宜そのバージョン番号にて明確化する。

9.12.2. 通知方法及び期間

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

9.12.3. OID(オブジェクト識別子)を変更しなければならない場合

(規定なし)

9.13. 紛争解決に関する規定

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

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

万一、 CP に従い最初の通知がなされた後、紛争が 20 営業日以内に解決しない場合、ベルギー国裁判所法典の 1676 から 1723 項に従い、関係当事者は紛争を仲裁へと進める。

仲裁人は、各当事者が夫々1 名の委員を提案、また双方が 1 名を第三者から選出することで、全 3 名の仲裁人から構成される。仲裁の場所は、ベルギー国 Leuven となり、必要となる費用は調停委員が決定するものとする。

9.14. 準拠法

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

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

9.15. 適用法の遵守

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

9.16. 一般事項

9.16.1. 包括的合意

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

9.16.2. 譲渡

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

9.16.3. 分離条項

本 CPS は、その責任の制限の項目を含む何れかの規定が無効であるか、或いは法的強制力が失効となった場合にも、本 CPS の他の条項は当事者の本来の意図に沿った方法で解釈されるものとする。

有限責任を規定する本 CPS の各条項は、分離可能であり、いかなるその他の規定からも独立したものであることを意図しており、それ自体強制されるものである。

9.16.4. 執行 (弁護士費用及び権利放棄)

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

9.16.5. 不可抗力

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

9.17. その他の規定

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

この管理には以下を含むが、これだけに限定されるものではない。

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

9.17.1. CA チェーニング契約書

CA チェーニング契約書は、下記の契約上強制力を有する規定及び条件を含む。

- 利用者法人及びその子会社（50%以上の株式支配権所有）からの TrustedRoot に限定して使用すること
- 非商業的利用に限定：発行された証明書は自身の利用、従業員及び既存のビジネス用途及び処理において利用者と提携する第三者の利用に限定すること
- エンドエンティティ証明書種類（S/MIME, SSL クライアント証明書及び SSL サーバ証明書）への制限を行うこと
- GlobalSign により審査及び受諾された CPS を提出すること
- 本 CP に準拠すること
- 業界規定に遵守する、物理的、人員、ネットワーク、倫理的及び運用管理についての PKI 評価書類を提出すること
- CA 及びサブ CA の秘密鍵管理において、米国連邦標準規格 140-3 又は同等の暗号化モジュールを使用すること
- 相互認証署名を禁止すること
- 米国輸出規定に基づき、発行済み証明書への輸出管理を実施すること
- GlobalSign 及び・又はその監査人による年一度の監査を受諾すること
- CA 環境への変更により、PKI 評価及び CPS の報告内容と異なる場合は継続的に GlobalSign へ通知すること
- GlobalSign が GlobalSign レポジトリにおいて、（チェーニング系列 CA として）当利用者 CA のことを公開する場合があることを了解すること

GlobalSign 及び・又はその監査人により、これらのいずれの項目に対する違反が発見された場合は、CA 取消しの事態となり得る。

9.17.2. PKI 審査

TrustedRoot 利用契約の施行は、GlobalSign 及び・又はその監査人による、利用者側 PKI に対する審査の受入れ、及びその審査に基づくものである。この審査は、利用者の CA 階層及びセキュリティ対応策を記録するものである。

この審査には下記の項目を含むが、それだけに限定するものではない。

- 論理的セキュリティ対応が導入されている－人事事項かつ職務分掌及び二重制御も網羅されていること

- 物理的セキュリティ対応策が導入されていること
- ネットワークセキュリティ対応策が導入されていること
- CA 階層が導入されていること
- HSM（ハードウェア　セキュリティ　モジュール）の種類及びシリアル番号

9.17.3. 利用者 CA の導入

GlobalSign は、利用者 CA のテスト署名を GlobalSign のテスト CA と連動して行なうことを必須事項としてこれを実施する。GlobalSign のテスト CA は GlobalSign のルート証明書を複製するが、これはテスト目的であると識別され（テスト　CA　対　CA）、また第三者アプリケーションに装填されるものではない。テスト署名が成功した場合のみ、利用者 CA は GlobalSign ルート CA から署名される。

9.17.4. 継続条件及び監査

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

（以下空白）