GlobalSign CA Certificate Policy

(GlobalSign CA 証明書ポリシー)

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

Version: v.2.1

目次

書類履歴

配布リスト

Version Company Name + Title Action

V2.0 30.06.05 Andreas Mitrakas Second version

V 2.1 26.1.07 Johan Sys Distributed to Policy Board

Document Change Control

Version Release Date Author Status + Description

V 2.1 26.1.07 Johan Sys Added GlobalSign Root CA R2

V2.0 30.06.05 Andreas
Mitrakas
Second version

05.09.05 Jean-Paul
Declerck
Final version

謝辞

この GlobalSignCA の CP は、以下の各業界標準を、部分的または全体を支持する。

- CWA14167-1（2003 年 3 月）: Security requirements for trustworthy sysytems mananging certificates for electronic signatures - Part1: System Security Requirements
- CWA14167-2（2002 年 3 月）: Security requirements for trustworthy sysytems mananging certificates for electronic signatures - Part2: cryptographic module for CPS signing operations - Protection Profile (MCSO-PP)
- RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)
- RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
- RFC 2560: X.509 Inernet Public Key Infrastructure - Online Certificate Status Protocol - OCSP
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRl Profile
- ETSI TS 101 456: Policy requrements for certification authorities issuing qualified certificates.
- ETSI TS 101 862: Qualified certificate profile
- The ISO 1-7799 standard on security and infrastructure

上記に引用した CWA 14167-1 と CWA 14167-2 は、2003 年 7 月 14 日の委員会の決定の中に、公告されており、ヨーロッパ協議会の 1999/93/EC の指令に準拠した電子署名製品の、一般的に認知される標準の参照ナンバーとして、公表されている。

本 CP は、上記標準の要件を順守していることを査定するために提示したものであり、本 CP は以下のスキームの要件に従って評価されている。

- AICPA/CICA、WebTrust Program for Certification Authorities

本 CP は、上記スキームの要件に適合するように意図しており、適合日付は、GlobalSign のウエブサイトに公表する予定である。

1　概説

この GlobalSign 認証局(以降"GlobalSignCA"と称す)の証明書ポリシー(CP)は、GlobaLSign が管理するトップルート配下で発行されるデジタル証明書の管理と証明書発行に関連した、GlobaLSign CA のサービスに適用される。トップルート証明書は、エンド・エンティティ証明書と同様に、認証局証明書の階層構造を管理するのに使われる。本 CP は GlobalSign CA のリポジトリ
https://www.globalsign.net/repositoryにあり、適宜更新される。

証明書ポリシーとは、特定のコミュニティや一般的なセキュリティ要件をもつアプリケーションの分野に対する、適用性を示す規則集に名前をつけたものである。
本 CP は、広い意味での証明書ポリシーであり、目次、レイアウト、書式については 2003 年 11 月の Internet Engineering Task Force (IETF) RFC 3647 の正式な要件にも合致している。IETF により出される RFC は、証明書管理と電子署名の分野における標準化の実践という面で、権威あるガイドである。本ポリシーのいくつかの項のタイトルは RFC 3647 の構成に準じている一方、そのトピックは、必ずしも GlobalSign CA の証明書管理サービスの実装に適用していない。これらの項については削除している。必要な追加情報は、標準構成に小区分として提示している。RFC 3647 の要求フォーマットに合わせていくことは、GlobalSign CA の、第三者 CA に対するマッピングと相互運用性を、拡張・促進させることになる。また RelyingParty(証明書に信頼を置いて利用する組織・機関。以降"依拠当事者"と訳する)対して、GlobalSign CA の実務と手続の事前通知を提供する。本 CP での標準の採用に関する表明は、謝辞の章に記載している。

本 CP は、GlobalSign CA よって発行されたオフライン証明書ソリューションの全ライフサイクル期間中、CA 局のサービスにおける、技術的、手続上の要員ポリシーと実務について扱う。

認定スキームに関する GlobalSign CA の準拠性の情報についての要求は、本 CP に関する他の問合せと同様、以下で取り扱う。

GlobalSign CAは、GlobalSign NV/SAの活動範囲で運用している。本CPは「トップレベル証明書」を発

GlobalSign NV
Attn. Legal Practices
Ubicenter,
Philipssite 5
B-3001 Leuven
Belgium,
Tel:+32 (0) 16 287123
Fax:+32 (0) 16 287404
Wmail : legl@globalsign.net
URL: www.globalsign.net

行するCAの要件を取り扱う。「トップレベル証明書」は、「ルート証明書」又は「アンカー証明書」とも呼ばれる。GS CAは、その階層のレベルを変えることで、他の証明書タイプも発行する。より詳細な情報は、http://www.globalsign.net/repository から入手できる。

本 CP は、GlobalSign が提供する CA chaining サービスに関連するオフラインソリューションの全ての事例に適用される。本CPは、例えば、エンド・エンティティ証明書のような、GlobalSignの階層の最も下位レ

ベルで発行される証明書の、証明書パス検証の場合にも適用される。

本CPは、最終のものでGlobalSign NV/SAを拘束する。(所在地Ubicenter オフィス、Philipssite 5, B-3001 Leuven, VAT 登録番号 BE459. 134.256 の会社法人 で、商業登記番号 BE 0.459.134.256 RPR Leuven)。(以降"GlobalSign"と称す)
そして、
利用者と依拠当事者は、GlobalSign CAによって利用可能となる証明書サービスに、信頼を置くか、又は置こうとするものである。

利用者にとっては、利用者契約書を受け入れた時点で、本CPが有効となり拘束される。CA chainningサービスを望む利用者にとっては、本 CP は GlobalSign との CA chainning 契約書を締結した時点で、GlobalSign が所有または管理するルートに対して有効となる。依拠当事者に対しては、本 CP は、GlobalSign 証明書への証明書に関する要求をGlobalSignディレクトリに向けるだけで、拘束力を持つようになる。利用者契約書により、依拠当事者は同意に関係なく、本CPでの条件を受け入れることになる。

1.1. 概要

本 CP は、GlobalSign 自身の手続のもと発行されるトップレベル又はルートの証明書の管理を扱うGlobalSign CAの特定範囲に適用される。本CPの目的は、証明書を管理するGlobalSignの実務と手続を示し、GlobalSign 自身の手続に則りルート証明書の発行に関する要件に準拠していること(そのことは、要件準拠を追求していると正式な認定フレームワークで監査承認されているように)を説明するためである。本 CP は、上述の範囲にのみ適用し、その他への適用は除外する。本 CP は、エンド・エンティティ用クライアント証明書を発行する分離したCAによる、証明書交付サービスでのGlobalSign CAの促進を目的としている。この証明書タイプは、GlobalSign RootSignとして知られている。
本CPは、GlobalSignのルート証明書の使用、信頼、管理のライフサイクルに関与する、全ての機関の役割と責任と実務を、確認することを目的に定めたものである。

本CPは、GlobalSignのGlobalSignルート証明書を、発行・管理・使用するためのポリシー要件を記述している。
トップルートCA局としてGlobalSignは、www.globalsign.net/repository に公表した実務に従い、証明書の階層構造を管理している。

CP は「順守しなければならないこと」を述べており、従って、GlobalSign の製品とサービスに関する広い範囲の運用ルールの枠組みを定めている。そのレベルは、一般的には電子証明書のライフサイクル管理による、信頼のレベルを確かにしたい機関によって、定義される。GlobalSign CP は、単にエンド・エンティティ領域だけではなく、ルート証明書に焦点をあてた GlobalSign 証明書のすべてのアプリケーション範囲の要件を取り扱う。

GlobalSign 認証業務運用規定(以降"CPS"と訳す)は、本 CP を補足し、"この認証局が、如何にしてこの証明書ポリシーを守っていくか"を述べている。本 CPS は、エンドユーザに、プロセスの概要と、この認証局が電子証明書を生成・維持する上で使用する手続と一般的な条件を提示する。GlobalSign は、一般のエンティティ証明書に対しても、CPS を保有維持する。

CP と CPS に加え、GlobalSign は以下の同類のポリシー書類(但し、これだけに限定せず)を保持する。

- 保険の問題を取り扱う GlobalSign の保証ポリシー
- 個人データの保護に関する GlobalSign のデータ保護ポリシー
- 消費者保護に関する GlobalSign の消費者保護ポリシー
- 事業継続
- セキュリティポリシー
- 要員ポリシー
- 鍵管理ポリシー
- 登録手続
- その他

GlobalSign CA の利用者又は依拠当事者は、GlobalSign ルート CA の一般的な運用に関する通知と同様、GlobalSign ルート CA により発行される証明書の信頼確立のため、GlobalSign の CP を参照しなくてはならない。GlobalSign 証明書階層の証明書チェーン全体の信頼性を確立することは、必須の事柄である。それには、本 CP の表明が元となり信頼が確立される、ルート CA 局と運用上のルート(CA)を含む。

適用可能なすべての GlobalSign ポリシーは、継続的な権威ある第三者機関のセキュリティと監査が前提である。要求があれば、追加情報も提供可能である。

本 CP を適用する GlobalSign CA の正確な名称は以下の通り。

- GlobalSign Root CA
- GlobalSign Root CA R2

これらは、総称して GlobalSign Root CA と呼ばれる。RootSign は GlobalSign のサービスで、第三者 CA に、GlobalSign CA のひとつに(署名)チェーンを許すものである。

電子証明書は、電子的な取引に参加する機関に、他の参加者らに対し、彼らの認証を証すことを可能にし、データへの電子的署名を可能にする。電子証明書を用いて、GlobalSign は指名された機関(利用者)とその公開鍵との関係の確証を提供する。本 CP の目的から、エンド・エンティティは、GlobalSign 階層への参加を望む第三者認証局利用者である。GlobalSign 階層に入る効果は、ブラウザーその他の第三者アプリケーションでの偉大な機能と同様に、階層の信頼を広げることになる。GlobalSign は、第三者アプリケーションの中に、このトップルートを包含する事に関し、リーダーシップ地位を狙っている。この努力は、GlobalSign の改定する能力を損なうことはなく、将来に対する代替戦略を模索する。GlobalSign サービスの価値をあらゆるタイミングで評価し動すること、それは第三者 CA であるエンド・エンティティの分別であり義務である。

電子証明書を取得する手続は、電子証明書の、期限切れ、失効、発行などの証明書管理側面と同様に、クライアントの同一性識別、識別名、認証と登録である。
このような手続で電子証明書を発行することで、GlobalSign は、証明書ユーザに対して、その同一性識別に関し、適切で積極的確認を提供し、そのようなユーザが使っているという肯定的な関連をその公開鍵に与える。この例証には、ある環境下で要求される他の認証局の用途も含まれる。GlobalSign は、否認防止と認証に使用可能な、汎用の電子証明書も提供可能である。このような証明書の利用は、利用されるアプリケーションによる他の制約や保証ポリシーに従い、特定のビジネスや契約の関係、商取引に限定される。

本 CP は、GlobalSign 公開鍵基盤上で証明書を発行している GlobalSign CA によって、維持される。公開鍵基盤に基づく証明書管理において、発行局は、全てのエンドユーザ証明書が継承する信頼の階層を管理する機関である。

本 CP は、GlobalSign CA Roots の申請期間中、GlobalSign RootSign の発行を統治する。申請期間とは、ある CA が GlobalSign CA 証明書を発行できる期間を言う。この申請期間は、GlobalSign 階層の上位階層 CA によって GlobalSign Rootsign に発行された証明書に示されている。

本 CP は、発行 CA のリポジトリ(https://www. GlobalSign.net/repository)にてオンラインで参照可能である。
GlobalSign CA は、本 CP に関するコメントを、この書類のはじめに記載した宛先で受け付けている。

1.1.1. GlobalSign RootSign

本 CP は、GlobalSign の証明書階層に加入を望む認証局が、認定され、GlobalSign Rootsign を使用するための要件を取り扱っている。GlobalSign 階層への加入は、GlobalSign が関係機関に用意している CA chaining プログラムを通して実施される。
Rootsign 証明書は;

- 運用の実務と技術の実装に関する GlobalSign Rootsign サービスの契約とポリシーの要件への適合に同意する第三者 CA に対して、GlobalSign が発行するもの。
- CA に対してのみ、発行するもの

1.1.2. 電子証明書の用途

ある適用環境において、依拠当事者(Relying party)の CA の識別確立を促進する、第三者 CA の認証を可能にする GlobalSign Rootsign と Rootsign 証明書について、その使用にある一定の制限事項が適用される。

GlobalSign Rootsign と Rootsign 証明書の他のいかなる使用も禁止されている。

1.2. ドキュメント体系(名称等)

証明書にオブジェクト識別子を含むことにより、GlobalSign は、ETSI TS 102 042 に公示・識別される証明書ポリシー要件への適合性を保証している。
本 CP で特定している証明書ポリシーの識別子は、後ほど決定する。

1.3. PKI コミュニティの関係者

1.3.1. GlobalSign 認証局

認証局とは、パブリックドメイン、ビジネス、又は商取引の中で使用される電子証明書を発行する機関である。GlobalSign は認証局である。時により、認証局は発行局ともいう。
GlobalSign はまた、あるクラスやタイプの証明書を発行する場合のポリシーの原案を作成する責任がある。この認証業務運用規定が GlobalSign Rootsign 証明書の発行におけるポリシーであるので、

GlobalSign はポリシー機関でもある。

依拠当事者に情報と知識を提供するために、失効証明書や一時停止証明書に関する機能が、証明書失効リストへの適切な公開を要求する。GlobalSign はこのような(失効)リストを運用する。

GlobalSign CA chaining サービスのサブジェクトは、ルートサービスに関し GlobalSign と契約締結した第三者 CA となる。下位階層 CA により発行された電子証明書の信頼前のパス検証と同様、ルート証明書は、階層におけるトラストアンカーの認証を目的に発行される。その他の目的でのルート証明書の使用は禁止されている。

ルート証明書は、パブリックな目的には、どのような利用もできる。“パブリック”であるので、本 CP は、参加者間の私法での自由な同意のもと、CA 間での制限のない如何なる利用も考慮する。クローズユーザグループの利用も、GlobalSign 階層の活用のため許可される。

GlobalSign CA は、あるタイプやクラスの電子証明書発行に使われるポリシーを草案し、実装する。GlobalSign CA は、GlobalSign CA 証明書を発行するという観点から、ポリシー機関である。GlobalSign CA は、 GlobalSign CA Root とこの階層に属する後続ルートの管理とライフサイクルに関して、最終的な統制権を持つ。

GlobalSign CA は、GlobalSign CA Root の証明書管理下の全てのサービスが使える状態であることを確実にする。それには、証明書の発行、失効、ステータス検証と GlobalSign Rootsign を含み、特定の適用業務で使用され要求される。
GlobalSign CA はまた、GlobalSign CA Root 及び Rootsign のもとで発行される全ての証明書タイプの登録システムも管理する。

失効又は一時停止した証明書に関する作用の通知と知識を、依拠当事者が確実に取得するため、適切な(失効リストの)公開が必要である。公開は、オンラインディレクトリに出力される証明書失効リストに、失効又は一時停止の証明書含めることで明らかになる。発行された証明書もディレクトリに出力される。GlobalSign CA はこのようなディレクトリを運用する。

GlobalSign CA の責任領域は、証明書ライフサイクルの全体的な管理から成り、以下の活動を含む。

- 発行
- 一時停止
- 停止解除
- 失効
- 更新
- ステータス検証
- ディレクトリサービス

証明書ライフサイクルに付属するいくつかの仕事は、以下の 1.3.2 で説明するとおり、GlobalSign とのサービス契約のもと運用している GlobalSign RA に委譲される。

1.3.1.1. GlobalSign 外注代理業者

GlobalSign は、GlobalSign CA 証明書の、発行、一時停止、失効、更新、ステータス検証を含む CA サービ

スの提供と、セキュアな設備運用を、外注代理業者に頼っている。GlobalSign の外注代理業者は、サービス契約にもとづいて、GlobalSign をサービスを運用している。

1.3.1.2. GlobalSign の役割

GlobalSign は、2つの役割を担っている。第一は、信頼のサービス提供者として、トラストサービスをユーザ地域社会に、直接または代理人を介して提供する。ここでいう代理人には GlobalSign が定めた契約のもと運用する登録局(RAs)と呼ばれる第三者機関である。
第二は、GlobalSign は、私的又は公的機関に対し、高い信頼と品質の電子証明書を発行するために GlobalSign の手続と適切なブランド名を使い、信頼の第三者による国際ネットワークを運営する。そのような機関には、GlobalSign との契約のもと運営される、GlobalSign 認定の認証局と RA が含まれる。この役割は通常、GlobalSign トップルートとブランドに定着した信頼の継承を求める他の認証局への証明書発行に限られる。
GlobalSign の主な活動は、

- RA 群の国際ネットワークを管理し、PKI テクノロジーを利用する信頼の第三者機関として、GlobalSign のブランド名を確立すること。
- エンドユーザ機関に対し発行された証明書のライフサイクルを管理すること、同様に、GlobalSign 範囲における管理者と他の認証局に対する証明書発行のライフサイクルを管理すること。

GlobalSign のパブリック証明書サービスは、オンラインビジネスサービスとセキュアな電子商取引を、支援することを目的とし、電子署名利用における個人及び商用の要件を取り扱う。

1.3.1.3. GlobalSign ルートと階層

GlobalSign は、利用可能なリソースの唯一性と、エンドユーザ証明書の完全性を保証するため、独占的なルート階層を利用者が使えるようにする。アプリケーションに埋め込まれている GlobalSign ルートの優位性を享受する参加 CA と同様、GlobalSign が定めるレベルでのエンドユーザ証明書の発行のように、特定の目的を満たすようにセットアップされてきたルート群を含んだ GlobalSign 信頼ネットワークのより広い領域に、GlobalSign CA ルートは属す。
この GlobalSign 証明書ポリシーは、GlobalSign 階層のルートレベルを扱い、GlobalSign サービスの一般的な条件に関するガイドラインを示す。
GlobalSign CA ルートは、それに続く第三者 CA の個々の秘密鍵を認証するために使われてきた。そのような CA の証明書を検証することにより、GlobalSign に定着した信頼が、認定した第三者 CA ルートに拡張される。

1.3.2. GlobalSign 登録局

GlobalSign CA は、指定した登録局を通して利用者につながる RA は、本 CP のもと、証明書の発行、一時停止、失効、を要求する。
RA は証明書の生成と失効に必要なデータを CA に送信する。

GlobalSign RA は、エンドユーザにパブリック証明書管理サービスを届けるために、利用者とやり取りをする。
GlobalSign RA は、

- 証明書申請者の登録の受領、評価、承認、否認をする。
- GlobalSign CA 証明書サービスに利用者を登録する。
- 発行した証明書のタイプにより、GlobalSign CA の任命をうけ利用者の本人確認の全てのステージに参画する。
- 利用者申請書を検証するために、公式の公正証書、さもなくば認定された文書を使用する。
- 申請書の承認に続いて、証明書を発行のため GlobalSign CA に通知する。
- 証明書の一時停止、停止解除、失効の手続を開始し、GlobalSign CA からの証明書失効を要求する。

GlobalSign RA は、GlobalSign CA による承認と認可に基づいて現地で行動する。GlobalSign RA は、GlobalSign RA の手続文書と本 CP を含む GlobalSign CA の運用手順書に従い行動する。

特定の証明書タイプを許諾するため、GlobalSign RA は、第三者認証局により発行された証明書か、第三者のデータベースと情報ソースに信頼を置く場合がある。GlobalSign Root のもと発行される特定の証明書を管理するうえで、証明書依拠当事者は、適切な証明書ポリシーを参照し、特定の情報を探すよう促される。

検証成功のあと、証明書が申請者の機関に発行される。

いくつかの RA 機能が、ローカル登録局(LRA)で実施される場合がある。この場合、LRA は GlobalSign RA の管理監督のもと行動する。

1.3.3. 利用者

GlobalSign Root の利用者は、GlobalSign が管理する階層の証明書発行を求める第三者 CA である。GlobalSign サービスの利用者は、CA 証明書を申請する自然人か法人である。利用者は、GlobalSign 範囲内で、電子署名サービスを使う。
利用者は、以下の機関である。

- 証明書に記載されているサブジェクトの便益のため、GlobalSign CA を使った証明書サービス提供の枠組みを設定する。
- 証明書のサブジェクトにリストされている公開鍵と対をなす秘密鍵の最終権限を持つ。

法人は、委任代理人(委任取締役)により、正式に代表する人でなくてはならない。
法人は、証明書のサブジェクトには記載できない。

自然人である加入法人は、CA chaining サービスの利用者として条件付で受け入れられる。Chaining される CA とこれらの人々との関係を、正式に説明し、その正当性を GlobalSign に提示しなければならない。もし、第三者機関の表示が望まれるなら、GlobalSign は、事例毎の申し合わせになるが、代替の信用証(属性証明書又は役職証明書)を推奨する。

典型的には、利用者は ID カード、パスポート等、有効な同一性確認の書類を保持し、電子証明書発行の信用証明とし使用する。申請機関の追加の同一性確認書類が必要な場合もある。

1.3.4. サブジェクト(利用者識別情報)

GlobalSign Rootsign のサブジェクトは、GlobalSign により管理される階層内で、証明書発行を望む第三者 CA となる。

GlobalSign CA 証明書サービスのサブジェクトは、本人が利用者又は、利用者に関係する自然人である。サブジェクトは、利用者が指定する範囲の許可の下、電子署名サービスを利用する。
サブジェクトは以下の関係者である、

- 証明書を申請する者
- 証明書で識別される者
- 利用者証明書にリストされる公開鍵と対をなす秘密鍵をもつ者

サブジェクトは GlobalSign RA に加入するか、指定されたサービスで証明書利用を要求するサービスプロバイダーに加入する。サブジェクトは、証明書を申請するために、証明書申請者(＝利用者)を指名する。証明書申請者は、サブジェクトの代わりに活動する自然人なら誰でもなれる。

GlobalSign CA ルート証明書のサブジェクトは、申請組織と同様、GlobalSign CA chaining を望む第三者 CA である。

1.3.5. 証明書申請者

証明書申請者は証明書利用者になりたい者である。証明書申請者は、サブジェクトの代わりに以下のことをする、サブジェクトに指定された者である。

- 証明書を申請する
- CA 利用者契約を受け入れることに同意する

申請者は、

- サブジェクト自身と同じ、この場合個々に指名される
- サブジェクトにより雇用された個人
- コントラクターまたはサブコントラクターに雇用された個人で、明示的な承認もと活動する者

1.3.6. 依拠当事者

依拠当事者は、利用者の証明書にリストされた公開鍵を参照することで検証が可能なデジタル署名又は証明書を信頼する、自然人または法人である。例えば、GlobalSign CA のサブジェクトからの署名されたリクエストを受け取る GlobalSign のオペレータが GlobalSign 証明書の依拠当事者である。

電子証明書の有効性を検証するために、依拠当事者はいつも CA 失効情報(現在のところは証明書失効リスト"CRL")を参照しなければならない。検証は、証明書情報を信頼する前に行われる。代替として、依拠当事者は、利用可能なら OCSP プロトコルを使った自動応答を参照できる。依拠当事者は、本 CP に記載されているように、特定の責任をもつ。

1.4. 電子証明書の用途

GlobalSign CA 証明書の使用に関し、制限事項がある。

1.4.1. 電子証明書用途の範囲

GlobalSign CA により発行されるルート証明書は、以下のことを必要とする取引のあるパブリックドメインに対する証明書発行に使用できる。

- 認証
- リモート装置の識別の保証

エンド・エンティティで使えるようになった後は、追加の使用は個別に指定される。GlobalSign CA に許可されてい形で使用すると、GlobalSign CA によって利用者と依拠当事者に与えられている保証が取り消しとなる。

1.4.2. 禁止される電子証明書の用途

エンド・エンティティ証明書の使用は、証明書の拡張であるKeyUsageとextendedKeyUsageを使って制限される。これらの拡張と矛盾した証明書の利用は禁止されている。

1.4.3. 証明書拡張

GlobalSign ルート証明書の拡張は、マイクロソフトやネットスケープで使われているフォーマット等と同様、X.509 V.3 標準で定義されている。

GlobalSignは、国際標準化機構(ISO)の定義のとおり、パブリックPKIサービスに、制約と拡張を使用する。このような制約と拡張は、利用者証明書や CA の役割と位置づけを限定し、変化する役割のなかで利用者が識別できるようにしている。

Key usage 拡張が、証明書にリストされる公開鍵の技術目的を制限するので、
GlobalSign 自身の証明書も、鍵の機能を、証明書、失効リスト証明書、その他のデータへの署名に、制限する key usage 拡張を含んでいる。

証明書ポリシー拡張は、証明書の使用を、商用または法的前後関係の要求に制限する。GlobalSign は、産業の拡散のなかで、他の公的証明書が適切であるように、証明書ポリシー、又はその統治を支援し、参画する。

1.4.4. クリティカル拡張

GlobalSign は発行する証明書のなかで、以下のようにクリティカル拡張使っている。

- keyusage での基本の制約として、証明書が CA 用なのか否かを示す、
- 鍵の意図する使用法を示す、
- CA 証明書階層の中での、何番目かを示す。

1.5. 認証ポリシー

GlobalSign CA は、ドメイン内の証明書を管理するトップルート(トラストアンカーとも呼ばれる)である。GlobalSign CA は他の第三者認証局と、相互に交信したり、認証を模索する。

GlobalSign CA の Policy Managing Authority は本 CP を管理する。GlobalSign CA は、本 CP を登録し、整備を監視し、解釈説明する。GlobalSign CA は、GlobalSign CA ルートのもと発行される証明書のライフサイクル管理での運用条件を広く参照可能にする。各ルートでの運用条件は、本 CP の中で公表する。

1.5.1. 対象事項

公表した GlobalSign CP の信頼性を発動し、法的要件と認定によりよく対応する努力として、GlobalSign は、環境による要求に合うように、そのポリシーを改修・更新する。このような更新は、CP の更新バージョンが発表されてから 30 日後に、これまで発行された証明書とこれから発行する証明書に拘束力を持つ。

1.5.2. GlobalSign Policy Managing Authority

GlobalSign ポリシーの更新交付や新しいバージョン は、Policy Managing Authority によって承認される。現組織構造における Policy Managing Authority は、以下に示すメンバーで構成されている。

- 最低1名の GlobalSign の管理者
- 最低 2 名の GlobalSign ポリシーと実践に関する草案と開発に直接関与した認定代理人

上記管理者が職務上の Policy Managing Authority の議長となる。
全ての Policy Managing Authority メンバーは、各 1 票持ち。その他のものに留保される投票権はない。投票が同数となった場合は、、Policy Managing Authority 議長の投票を2票と数える。

1.5.3. CP の最新版の受領

CP 更新が Policy Managing Authority によって承認された時点で、その CP は、GlobalSign オンラインリポジトリ(https://www.globalsign.net/repository)に公布される。

GlobalSign は、そのような更新についての通知を、公開ウェブサイト(https://www.globalsign.net)に公布する。その更新バージョンは、通知後 30 日以内に申出がない限り、現利用者及び将来の利用者に対して、拘束力がでる。この期間経過後、更新版 CP は、前バージョンの GlobalSign CP のもと発行された証明書の利用者と依拠当事者を含む全ての者に、拘束力を発効する。

変更によって影響をうけた利用者は、通知から 15 日以内にポリシー管理機構に意見を提出できる。利用者とその管理権限者のみが、ポリシー変更に反対意見を出せる。利用者でない依拠当事者は、反対意見を出す権限はなく、出してもなかったものとしてみなされる。

GlobalSign は、少なくとも最新の CP2 バージョンをウェブサイトに掲載する。

1.5.3.1. 通知を伴う変更

本 CP の更新バージョンは、必要に応じて、監査人に通知される。

1.5.3.2. 版管理と変更の表示

変更は、CP の新しいバージョン NO.で示される。新しいバージョンは、整数値と後ろに、小数点0が付くもので示される。マイナーな変更は、小数 1 桁で示される。マイナー変更は以下を含む、

- 編集上の訂正
- 連絡先の変更

1.6. 用語の定義

用語の定義は本 CP の終わりに記載する。

2. 公開とリポジトリ

GlobalSign は、発行する電子証明書に関する情報を、公にアクセス可能なリポジトリに公布する。
GlobalSign は、証明書のステータス情報を第三者のリポジトリに公布する権利を、留保する。
GlobalSign は、本 CP を含むポリシーの中身と、その実践手続を公開する文書のオンラインリポジトリを持つ。GlobalSign は、GlobalSign のリポジトリ内での適切な方法により、ポリシーに関する情報を公開し、利用可能にする権利を留保する。
GlobalSign 証明書の発行、使用、管理に関連する全ての者に、GlobalSign は、電子証明書のステータス情報の提供に関して、皆がアクセス可能なディレクトリに、その情報を公開することを、通知する。
GlobalSign は、内部的なセキュリティポリシー、手続、セキュリティ等の書類要素の公開は差し控える。しかしこれらは、GlobalSign が順守する正式な認定スキームに関連する監査では、開示する。

2.1. リポジトリの参照方法

GlobalSign が、公開リポジトリや、ポリシー(例えば CP,CPS)へのアクセスを無料でするように努力する一方、第三者のデータベースやプライベートディレクトリでのステータス公開は、課金するかもしれない。

3. 識別と認証

GlobalSign は、証明書の発行に先がけて、GlobalSign CA または GlobalSign RA へのエンドユーザ証明書の申請者の識別と属性を認証する手続文書を保持する。
GlobalSign は、GlobalSign CA や RA を希望する機関や、CA チェイニングサービスを望む機関など GlobalSign の基盤と運用または相互運用する機関からの申請を受理するためには、認定された手順と基準を使う。
GlobalSign は、このポリシーの下、証明書の失効を望む機関からの要求を認証する。
GlobalSign は、名称におけるトレードマーク権の認識等、命名を取り扱う適切な手順を保持する。

3.1. 識別名

X.500distinguish names RFC-822 names and X.400names など、サブジェクトに割り当てられた名前のタイプを含む、命名と識別の規則に、GlobalSign は、利用者を識別するため、従う。
Rootsign 証明書を適用する場合、申請者の名前は、関連する製品仕様書と GlobalSignCPS で明示的に許可されない限り、重要である。GlobalSign は、名前を証明可能な申請書を送付する申請者に対して、証明書を発行する。
GlobalSign は、証明書に、トレードマーク、ロゴ、さもなくば、著作権のある図形やテキストを含む証明書は、受け付けない。

3.2. 新規登録時の利用者本人確認

CA chaining サービスを含む GlobalSign サービスの申請者の識別は、GlobalSign RA によって作成された手続文書に従って行われる。
サブジェクトフィールドにある利用者識別子は、GlobalSign に登録された公開鍵と対応する秘密鍵の所有を証明しなければならない。このような関連性は、例えば、証明書要求メッセージの電子署名により、証明される。
GlobalSign は、自身のネットワークと自身の階層のもとでの運用を望む、他の CA も受け入れる。
初期の査定と GlobalSign との特定の契約締結に続き、申請者 CA は、GlobalSign に、承認レターを含む会社定款を提出しなければならない。GlobalSign は、これに関する組織識別のため、第三者データベースに問い合わせる権利を保持する。
GlobalSign と申請機関との契約が締結されるなら、CA chaining サービスは、顧客の物理的な面談は要求しない。

3.3. 利用者の登録プロセス

GlobalSign は、以下を確認する

- 利用者が適切に識別され認証されていること
- 利用者証明書の要求が、完全で、正確で、承認されていること

特に、

- GlobalSignは、リポジトリ(www.globalsign.net/repository)で公開される専用のポリシーフレームワークとウェブサイト(www.globalsign.net)を通して申請者に通知する。
- 利用者と契約関係に入る前に、GlobalSign は CA chaining 同意書を締結し、GlobalSign に要求を出す前に承認しなければならない。
- GlobalSign のポリシーフレームワークは、GlobalSign's Limited Warrnty framework 同様 GlobalSign CP の中で説明したように、データ保護と消費者保護の法律と保証の下、制限されている。
- GlobalSign は、全ての、証明書配布に利用する外注代行業者、又は第三者登録機関との、契約関係を維持する。

3.3.1. 利用者の登録に使用される書類

GlobalSign 又は認定 GlobalSign RA は、適切な手段と文書化された手順で、申請者の同一性確認と、必要なら証明書特定の属性を検証する。上記に加えて、組織を識別するために、通常 GlobalSign は、付随

定款のコピーと場合により追加の識別要素を VAT 登録等の証しとして要求する。

3.3.2. 利用者の登録に必要な情報

CA chaining サービスに、要求される証拠には、以下のものがある。

- 利用者のフルネーム(姓と名)
- 出生地、国家的に認識される識別番号、又は、同じ姓名でも区別が可能となる利用者の属性。
- 関連する法人、又は他の組織機関、の正式名称と法的地位
- 関連する法人、又は他の組織機関、の関連する現在有効な登録情報(例えば、会社登記)
- 利用者が、その組織機関に所属する証拠

3.3.3. 仮名

GlobalSign RootSign 証明書には、仮名は許可されない。

3.3.4. 利用者の登録の記録

GlobalSign は、検証に使った書類参照番号や有効性の限界など、利用者の識別を検証するために使用した情報を全て記録する。
GlobalSign は、CA chaining 契約締結の記録と、申請を支援する以下の文書や資料(但しこれらに限定しない)を保持する。

- 申請者によって承認、締結された CA chaining 契約書
- CA サービス終結に備え本 CP が要求している条件で、登録に使われた情報と、その後の証明書ステータスの変化と、第三者への情報の送付等の記録を GlobalSign が保持することの承諾。
- 証明書に入っている情報が正確で正しいという趣旨の声明
- 利用者のフルネーム
- 組織背景の証拠
- 関連する法人または組織機関の正式名称と法的地位
- 関連する法人または組織機関の関連登録情報(例:会社登記)
- 利用者がその組織機関に関連していることの証拠

ビジネス文書法による指令により、上記で識別された記録は、証明書の期限切れ後、最低 5 年間保持される。GlobalSign RA はこのような記録を保持する。

3.4. 失効請求時の利用者本人の確認

Rootsign 証明書の失効要求の同一性確認と認証手続のため、GlobalSign は、失効要求する利用者の、署名入り供述書を要求する。

4. 証明書のライフサイクル運用の要件

第三者 CA、RA、利用者、及び他の参加者等、GlobalSign 範囲内のすべての機関は、証明書に入ってい

る情報の変更をすべて、GlobalSign CA に報告する継続した義務を持ち、その期間は、期限切れ又は失効されるまでの証明書の運用期間である。
GlobalSign CA は、GlobalSign RA により認証し署名された要求に従い、証明書の発行、失効、一時停止をする。
GlobalSign はこれらの仕事を第三者の代理人を使って実施する。しかしながら GlobalSign は、依拠当事者と同様この範囲内の全ての機関に対し、GlobalSign CA 内の CA 運用に関連するサービス提供に利用する代理人の、行動と不作為の義務と説明責任は、GlobalSign にあると考える。

4.1. ルート証明書の証明書申請

ルート証明書の申請手続には、GlobalSign との CA chainning 契約の締結が必要である。続いて、申請者は、ルート証明書に含むべき公開鍵と要求されている登録データを、安全な方法で GlobalSign に送付する。GlobalSign CA によるルート証明書の発行を要求する前に提示された(身分)証明書をもとに、GlobalSign RA は、申請者の識別を検証する。

4.2. 電子証明書申請審査(登録業務)

すべての証明書タイプで、GlobalSign RA は証明書申請に対し、その申請者の識別を検証するよう行動する。続いて、RA は証明書申請を承認、又は却下する。これら、承認もしくは却下について、申請者やその他の者に、その根拠を説明する必要はない。
RA は、手続を文書化し実務に導入している。

4.3. 電子証明書発行業務

証明書申請の検証と承認のあと、GlobalSign RA は GlobalSign CA に証明書発行要求を送信する。
GlobalSign CA 仕様に従い、利用者データとフォーマット含み有効に出来ているという条件で、RA からの要求に承認が与えられる。
発行された証明書がサブジェクトに届けられる。

4.4. 電子証明書生成

証明書の発行と更新に関して、GlobalSign は、全ての者に対し、下記の条件に従い、安全には発行していると明言する。

- ルート証明書を含む証明書発行の手続は、関連する登録と、利用者の生成された公開鍵の提供を含む証明書更新と、安全に結びつけられる。
- GlobalSign は、利用者に割り当てられた識別名の、この範囲内での唯一性を保証する。
- 登録データの秘匿性と完全性は適切な手段によっていつも、保証されている。
- RA 登録者の認証は、適切な(身分)証明書によって保証されている
- 証明書の要求と生成は、堅牢で試験された手続で支えられている
- 外部の登録サービス提供者を使う場合は、認証された登録サービス提供者と、登録データを交換する。
- GlobalSign はサービス実施の第三者の監査を受け入れる

4.5. 電子証明書の受領確認

発行された GlobalSign CA 証明書は、CA が発行した証明書の受領を RA が確認したとき、受領されたと見なす。
発行した証明書の受領に異議がある場合は、5 営業日以内に、GlobalSign CA に明示的に通知しなければならない。
GlobalSign CA は発行した証明書を公開する。

4.6. 利用者および署名検証者における鍵ペアと電子証明書の用途

証明書と鍵の使用に関連する責任については、以下の取り扱いに含める。

4.6.1. 利用者

利用者の義務は以下に含める

4.6.1.1. 利用者の義務

利用者の義務には以下のものを含む

1 GlobalSign リポジトリで公開される GlobalSign CP の適用可能な条項と条件を受容すること
2 その証明書の信頼性に実質的に影響を与える可能性のある提出情報の変更は、GlobalSign CA 又は、GlobalSign RA に通知すること
3 無効になった場合は、GlobalSign CA の証明書の使用を止めること
4 GlobalSign CA 証明書を、適切な環境で使用すること
5 秘密鍵の危殆化、紛失、公開、改ざん、その他秘密鍵の承認されない使用を防ぐこと
6 既に GlobalSign に承認されている、鍵ペアを適切に保護する製品や機器を使用すること
7 パートナーと代理人の行動と不作為に対し、利用者が秘密鍵を破壊するか、又は鍵供託を生成、保持すること
8 法律や他者の権利を侵害するようなステートメントを含む素材を GlobalSign 又は GlobalSign ディレクトリに送付することを控えること
9 GlobalSign CA 証明書の完全性が実質的に冒されるような出来事が発生した場合は、CA 証明書の失効を要求すること
10 証明書を不正に変更することを控えること
11 CP と CA chaining 契約に従って、承認された目的と適法にのみ証明書を使うこと

利用者はいつも、上記に表明した全ての義務を CA に対して持つ。利用者が、異なる名前のサブジェクトの代理人として申請するとき、(利用者の)ある義務はサブジェクトに移り軽減されるが、代わりに証明書ライフサイクルを冒すような不測事態をサブジェクトに知らせなくてはいけい。そのような軽減が発生した場合、上記義務の 2,3,4,5,6,8,9,10,11 項は、利用者ではなくサブジェクトに適用される。

証明書の有効性を実質冒すような事実や、証明書の有効期間中に CA 証明書に登場する情報になんらかの変更があった場合、利用者は、直接 GlobalSign RA に知らせる継続的義務を負う。この義務は、直接利用者か、又は代理人により実施される。

4.6.1.2. 自己責任での信頼

GlobalSign CA のリポジトリに登場している情報にアクセスし、それを評価・信頼することは、その者の責任で行うのもとする。

4.6.2. 依拠当事者

依拠当事者の義務は以下の通り

4.6.2.1. 依拠当事者の義務

証明書の依拠当事者とは、

- 依拠当事者のための関連する条件と GlobalSign CA からの通知を受け取る
- GlobalSign による証明書ステータス情報(例えば、CRL や OCSP)を用いて、GlobalSign CA 証明書を検証する
- 証明書のすべての情報がそのような検証手続を通して検証されたときのみ、GlobalSign CA 証明書が正しく、最新であると信頼する。
- その環境下で妥当であるような場合のみ、GlobalSign CA 証明書に頼る
- 失効されてない場合に限り CA 証明書を信頼する
- 依拠当事者自身の署名ポリシーとその実践が、実質的に冒されていないかを最低限検証する

4.6.2.2. GlobalSign CA リポジトリとウェブサイトの条件

利用者や依拠当事者など、GlobalSign CA リポジトリとウェブサイトにアクセスするものは、本 CP の条件と、GlobalSign CA が指定するその他の使用条件に同意する。電子証明書のステイタスを問合せることによって、もしくは与えられたサービスか情報に頼るか使うことによって、それらの者は、証明書の使用条件を受入れを表明する。GlobalSign CA リポジトリの使用は、以下の結果を導く、

- CA 証明書を検索した結果としての情報取得
- 証明書に含まれる公開鍵に対応した秘密鍵によって作られたディジタル署名のステータス検証
- GlobalSign CA のウェブサイトに公開された情報の取得

4.7. 電子証明書の更新

GlobalSign CA 証明書の更新はサポートされない。

4.8. 電子証明書の失効と一時停止

失効を申請した利用者の識別は内部手続によって行われる。
GlobalSign との事前同意に従い、GlobalSign RA は、証明書失効を望む(証明書)所有者の識別と認証を行う。
失効と一時停止の要求は、GlobalSign RAに、“GlobalSign, Philipssite 5, 3001, Leuven, Belgium”宛か、“ra@globalsign.net”宛か、本CPの導入部に記載の電話番号宛に、直接提出できる。

RA からの要求で、GlobalSign CA は、以下のいずれかであれば、CA 証明書を失効する。

- 証明書サブジェクトの秘密鍵の紛失、盗難、改ざん、許可されない公開、その他の危殆化した場合
- 証明書のサブジェクト又はその指定された利用者が、CP または CA chaining 契約に実質的な義務違反があった場合
- 災害、コンピュータや通信の障害、その他ひとによる妥当な努力を越える事態により、本 CP の下になすべき義務の遂行が遅れる又は妨げられ、他のひとの情報が脅威に晒され危殆化する場合
- 証明書サブジェクトの証明書に含まれる情報の改変が起こってしまった場合

要求者の識別を検証し、CP に要求される手続に従って要求が発行されたことを確認した時点で、GlobalSign RA は、速やかに証明書の失効を要求する。利用者が GlobalSign RA に提出した識別データにある情報の要素を通して、識別の検証は実施される。GlobalSign RA による要求で、GlobalSign CA は、速やかに証明書の失効を行う。

4.9. 証明書有効性確認サービス

GlobalSign CA は、CRL、OCSP、及び適切なウェブインタフェースで、証明書ステータス確認サービスを提供する。

4.10.利用者からの利用終了申請について

CA 証明書が失効、期限切れ、又はサービスが終了した場合、利用者の加入は終わる。

5. 管理、運用、及び物理的制御

この章では、鍵生成、サブジェクトの認証、証明書発行、証明書失効、監査、アーカイブの機能を遂行するため GlobalSign CA によって使われる、技術的でないセキュリティを記述する。

5.1. 物理的なセキュリティ管理

GlobalSign CA は、リース又は借りている建物に物理的な制御を実装している。GlobalSign CA はサービスを提供するために、サービス提供者に物理的制御を要求する。
GlobalSign CA の基盤は、他の目的で使用される証明書管理基盤と、論理的に分離されている。
GlobalSign CA のセキュアな建物は、高度なセキュリティ運用に適したエリアに位置している。
ある施設のエリアから他のエリアへのアクセスや、アクセス管理リストとトークンを使っての区域から区域への移動を要求し、セキュリティアラームによって物理的に監視・サポートされているセキュアコンピュータ室に置かれる CA 業務など、高セキュリティ区域へのアクセスを、制御する仕組を実装することにより、物理的にアクセス制限される。
火災加熱に対する手段と同様、GlobalSign CA は、防止と保護を実装する。
メディアはセキュアに保管される。バックアップメディアは、火や水のダメージから防御され、物理的にセキュアな離れた場所に格納される。

GlobalSign CA は、部分的なオフサイトバックアップを構築する

GlobalSign CA の構造物用地は、GlobalSign CA サービスを提供する基盤を提供する。 GlobalSign CA のサイトは、不正侵入検知やアクセス管理を含む適切なセキュリティコントロールを実装する。この構造物

用地へのアクセスは、アクセス管理リストに載った承認された人々に制限される。

5.2. 手続的管理

GlobalSign CA は、電子署名関連技術の分野での義務の十分な遂行と、スタッフメンバーとについて、信頼性と適性の適切な確実さを供する要員と管理を実施してゆく。
GlobalSign CA は、個人情報の保護と秘匿に関しての対策をとる。
管理者、セキュリティオフィサー、システム監査人、その他、それら運用に実質上影響する、鍵管理の運用のスタッフは全員、信頼された地位での勤務と考えられる。
GlobalSign は信頼された地位におけるメンバーの審査の訓練を実施する
GlobalSign は、行為遂行のすべての実施者の説明責任を、追跡する。
GlobalSign CA は、重大な CA 職務に対する、双対制御を実装する。

5.3. 要員的なセキュリティ管理

5.3.1. 要員の資格・経歴・身分証明

GlobalSign CA は、特定の任務における適正と、遂行するに必要な経歴、資格、経験を確立するための確認を実施する。経歴の確認には以下を含む

- 候補者の虚偽の陳述
- その他、必要と見なされることすべて

5.3.2. 教育訓練要件と手続

GlobalSign CA は、RA、CA の職務を実施するための要員教育訓練を用意する

5.3.3. 再教育訓練周期と再教育訓練手続

要員と手続の知識の最新状態と継続性を確実とするために、定期的な更新が実施される。

5.3.4. 要員の罰則規定

GlobalSign CA は、その環境下で適切である参加メンバーに説明責任を課す目的で、権限のない、行動、権限のない権限の使用、権限のないシステムの使用に対しては、罰則を課す。

5.3.5. 委託契約の管理

委託契約業者とその要員は、GlobalSign CA の要員と同じ、プライバシー保護と守秘条件に従う。

5.3.6. 初期教育訓練と再教育訓練の資料

GlobalSign CA と RA は、初期訓練と再訓練他で、要員書類を用意する

5.4. 監査ログ

監査ログ手続には、セキュアな環境を維持する目的で実装されたイベントログと監査システムを含む。
GlobalSign CA は、以下のコントロールを実装している。
GlobalSign CA の監査イベント記録には、以下のもの(ただし限定せず)が含まれる

- 証明書の発行
- 証明書の失効
- CRL の公表

監査証跡記録に含まれるのもは

- 業務の識別
- 業務の日時
- 業務に関与した証明書の識別
- 業務を実施した人の識別
- 業務要求の参照

監査に要求される文書

- 基盤計画と記述
- 物理的な再と計画と記述
- ハードウェアとソフトウェアの構成情報
- 要員の連絡リスト

GlobalSign CA は、指定した要員が定期的な間隔でのイベントログを精査し、特異なイベントを検知・報告することを、確実に行う。

GlobalSign CA、RA の承認された人と指定監査人による検査を目的に、ログファイルと監査証跡はアーカイブに保管される。これらログファイルは、アクセス管理メカニズムにより、適正に保護される。ログファイルと監査証跡はバックアップされる。

監査イベントはログ通知には入らない

5.5. 記録の保存

GlobalSign CA は、以下の項目についての内部記録を保持する

- CA 証明書の期限切れ後、最大10年間
- CA 証明書の発行の監査証跡、証明書発行後5年間
- CA 証明書の失効の監査証跡、証明書失効後5年間
- CA 証明書の期限切れ又は失効後、最低5年間の CRL
- CA 証明書の発行のサポート書類、期限切れ後5年間

GlobalSign CA は取出し可能なフォーマットで保存する。

5.5.1. 保存する記録

GlobalSign CA は、信頼できる方法で、GlobalSign CA 証明書、監査データ、証明書申請情報、ログファイルと証明書申請サポート書類を保持する

5.5.2. 記録の保存期間

GlobalSign CA は、CA 証明書の記録を期限切れ又は失効後最大10年間、信頼できる方法で保持する。

5.5.3. 記録の保存方法

記録文書の保護の条件には、以下を含む：
記録管理者（記録保持を義務とする指名されたメンバー）だけが、記録文書を一覧出来る：

- 一回書込みメディアにデータを格納するなど、記録文書の改変から防御する
- 記録文書削除からの防御
- 記録文書が格納されているメディア劣化からの保護、例えば、新しいメディアに周期的にデータ移行するという要件

5.5.4. 保存記録の確認方法

記録文書を取出し検証するために、GlobalSign CA は明確な階層コントロールと明確な職務分掌のもと、記録を保持する。
GlobalSign CA は、紙または電子フォートで記録を保持する。GlobalSign CA は、RA,利用者、又はその代理人に、この要件を支持するため適切な書類提出を求めることがある。
ファイリング期間は、期限切れや失効の日か始まる。このような記録は、紙または電子フォーマット、又は GlobalSign CA が適合と考えるその他のフォーマットで保持される。
GlobalSign CA は、承認要件に順守するため、記録保持期間を変更する場合がある。

5.6. 危殆化や災害時の対応

別の独立した内部文書として、GlobalSign CA は、危殆化レポートと処理手続など、適用可能な事案を文書化する。GlobalSign CA は、コンピュータリソース、ソフトウェア、及びデータが壊れたり、壊れたと疑念される場合に使う、復旧手順を文書化する。
GlobalSign CA は、災害やサーバ、ソフトウェア、データが崩壊した場合のサービス復旧を保証する、必要な手段を確立する。

5.7. CA または RA の終了

CA 活動を終了する前に、GlobalSign CA は GlobalSign CA 自身の費用で、指定された組織機構に、以下の情報を順を追って移転する

- GlobalSign CA に属するすべての情報、データ、書類、リポジトリ、記録文書

6. 技術的なセキュリティ管理

この章は、暗号化鍵と活性化データ(例えば、PIN、パスワード、相互に保持する鍵シェア)を保護するため、GlobalSign CA が取っているセキュリティ手段を詳しく述べる。

6.1. 鍵ペアの生成及びインストール

GlobalSign CA は、本 CP に従って秘密鍵を保護する。特定の証明書タイプに対して、GlobalSign CA は、各々の鍵の指定された使用に従って、秘密署名鍵を使用して CRL と OCSP レスポンスにだけ署名する。GlobalSign CA は、GlobalSign CA の対象事項から外れた如何なることにも、GlobalSign CA 内でその秘密鍵を使うことはしない。

6.1.1. GlobalSign CA 秘密鍵生成プロセス

GlobalSign CA は、ルート秘密鍵の生成には、文書化された手続に従った信頼できる手順を使用する。GlobalSign CA は、秘密鍵の秘密シェアを配布する。

6.1.1.1. GlobalSign CA 秘密鍵の使用法

GlobalSign CA の秘密鍵は、GlobalSign CA の発行証明書、GlobalSign CA 証明書失効リスト及び OCSP レスポンスへの署名に使用される。その他の使用は禁止する。

6.1.1.2. GlobalSign CA 秘密鍵のタイプ

CA ルート鍵としての使用で、GlobalSign CA は、鍵長 2048 ビットの RSA アルゴリズムを使用可能とし、最長 14 年までの有効期間をもつ。
運転可能な CA 鍵の使用で、GlobalSign CA は、鍵長 2048 ビットの RSA アルゴリズムを使用可能とし、最長 14 年までの有効期間をもつ。

6.1.2. GlobalSign CA 鍵生成

GlobalSign CA は、信頼できるシステムを使い、危殆化や権限のない使用法を防止するための必要な予防措置を講じ、その秘密鍵をセキュアに生成、保護する。GlobalSign CA は、本 CP 内に、鍵生成手続を構築、文書化する。
鍵生成は、証明書発行の目的に適していると認識されているアルゴリズムを使用し、実施される。
GlobalSign CA は RSA SHA-1 を使用する
CA 署名鍵として選択した鍵長とアルゴリズムは、CA による証明書発行の目的に適していると認識されているものである。

6.2. 鍵ペアの再生成と再インストール

GlobalSign CA は、活動している耐タンパ(不正改ざん防止)装置、バックアップ、エスクローのコピーの秘密鍵も同様に、過去に使用した鍵をすべて閉鎖し破壊する。

6.2.1. GlobalSign CA 鍵生成装置

GlobalSign CA の秘密鍵生成は、セキュアな暗号装置内で起こる。

6.2.1.1. GlobalSign CA 鍵生成の管理

GlobalSign CA の秘密鍵生成には、信頼される地位で勤務する適切に権限付与されたメンバー2名以上の管理を必要とする。この行為は、双対制御を必要とする。

6.2.2. GlobalSign CA 鍵の保管

GlobalSign CA は、ISO の適切な要求に適合するよう、セキュア暗号装置をつかってその秘密鍵を格納する。
署名生成装置の外にある場合は、証明書の GlobalSign 秘密署名鍵は、いつも暗号化されている。

6.2.2.1. GlobalSign CA 秘密鍵保管の管理

GlobalSign CA の秘密鍵の保管は、信頼される地位で勤務する適切に権限付与されたメンバー複数名の管理を必要とする。この行為は、双対制御を必要とする。

6.2.2.2. GlobalSign CA 鍵のバックアップ

GlobalSign CA の秘密鍵のバックアップ、保管、復旧は、信頼される地位で勤務する適切に権限付与されたメンバー複数名の管理を必要とする。この行為は、双対制御を必要とする。

6.2.2.3. 秘密シェア

GlobalSign CA の秘密シェアは、秘密鍵の信頼性を防護・向上し、鍵復旧を可能にするため、複数の権限付与された(秘密シェア)保持者を使う。GlobalSign CA は、秘密鍵をいくつかの対タンパ装置に保管する。この行為は、双対制御を必要とする。

6.2.2.4. 秘密シェアの受領

秘密シェア保持者は、秘密シェアを受領する前に、個人的にその秘密シェアの生成、再生成と配布と、またはその後の保管の連鎖を観察する必要がある。

秘密シェア保持者は、GlobalSign CA が認定したハードウェア暗号モジュールなど、物理メディアの中に秘密シェアを入れて受領する。GlobalSign CA は、秘密シェアの配布記録を保持する。

6.2.3. GlobalSign CA 公開鍵の配布

GlobalSign CA 自身の公開鍵配布は、GlobalSign CA の運用規定と、及びベルギー法律で要求される追加条件により行われる。
GlobalSign CA は自身の秘密鍵配布(方法)を明文化する。また、トークン保有者がその役割に交代が必

要となる場合に備え、GlobalSign CA はトークンの配布を変更できるものとする。

6.2.4. GlobalSign CA 秘密鍵の破壊

GlobalSign CA の秘密鍵は、それらが二度と取出されない・使われないことを保証するために、そのライフタイムの最後に、少なくとも有効な信頼できる証書2つの提示で破壊される。
鍵破壊の処理は、文書化され関連する記録と保存される。

6.3. 秘密鍵の信頼性と暗号モジュール

GlobalSign CA は、CA 鍵の管理のため、適切な暗号装置を使用する。これら暗号装置は、ハードウェアセキュリティモジュール(HSM)としてよく知られている。
これらの装置は、装置への不正行為を検知し、秘密鍵が暗号されない形で装置外に出せないことを保証する公式の要件に適合する。
CA の秘密鍵を保護するハードとソフトのメカニズムは書類化されている。この書類には、この CA 鍵保護メカニズムが、彼らが保護している CA 鍵の強度と少なくとも同等であると詳しく説明している。
GlobalSign CA 保管者は、秘密鍵を活性化と不活性化を行う職務で指名されている。その鍵は従って、決められた期間活性化される。
GlobalSign CA 秘密鍵はライフタイムの最後に破壊される。

6.4. その他鍵ペアに関する管理

GlobalSign CA は、自身の公開鍵を保存する。GlobalSign CA は利用者証明書を、その証明書に示されている使用期間で、発行する。

6.4.1. コンピュータリソース・ソフトウェア・データ等の重大障害時の対応手順

GlobalSign CA は、災害やサーバやソフト、データの崩壊が発生した場合のサービス復旧を確実にするための必要な手段を確立する。
もし、リソース又はサービスが、GlobalSign CA のコントロール下で保持できなかった場合、CA は、リソースのオーナー又はサービス提供者との契約が、災害復旧の要件に準拠していることを確認する(必要がある)

6.4.2. CA 公開鍵失効

万一、GlobalSign CA の公開鍵が失効した場合は、GlobalSign CA は直ちに、
- 相互認証しているすべての CA に通知する

6.4.3. CA 秘密鍵の危殆化

万一、GlobalSign CA の秘密鍵が危殆化した場合は、対応する証明書は、直ちに失効される。エンドユーザ証明書のすべての失効を含む追加の手段がとられる。

6.5. 活性化データ

GlobalSign CA は、自身の秘密鍵と運用に関連する活性化データを、セキュアに保存する

6.6. 認証設備のセキュリティ管理

GlobalSign CA は、コンピュータセキュリティ管理を実装する

6.7. ライフサイクルセキュリティ管理

GlobalSign CA は定期的に、開発管理とセキュリティ制御管理を実施する。

6.8. ネットワークセキュリティ管理

GlobalSign CA は、ファイアウォールを含む、上位レベルのネットワークのセキュリティを維持する。ネットワークへの侵害は検知される。特に、

- GlobalSign CA は RA との接続を、管理専用の証明書で暗号化する
- GlobalSign CA のウェブサイトは、証明書ベースのセキュアソケットレイヤー(SSL)接続とウィルス防御を提供する。
- GlobalSign CA ネットワークは、侵入検知システムと管理されたファイアーウォールで保護されている。
- CA ネットワーク外からの GlobalSign CA データベースへのアクセスは禁止されている。
- 情報の要求と配布のインターネットセッションは、暗号化されている。

7. 電子証明書及び CRL のプロファイル

この章は、証明書フォーマットと、CRL と OCSP フォーマットの明細を述べる

7.1. 電子証明書のプロファイル

GlobalSign CA は、正式に正当な要求を受信した場合、エンドユーザ証明書の証明書プロファイルを開示する。

7.2. CRL プロファイル

GlobalSign CA は、使用する CRL プロファイルの記録を、独立した技術文書として保持する。GlobalSign CA は、この書類を、理由を説明し要求する者に対して、GlobalSign CA の判断で開示する。
IETF PKIX RFC 2459 に適合して、GlobalSign は CRL を以下に準拠してサポートする

- CRL によってサポートされているバージョン情報と
- CRL と CRL エントリー拡張の投入と重要性

GlobalSign 証明書失効リストのプロファイルを下記テーブルに示す。

(省略)バージョン、発行者名称、今回の更新日時、次回更新日時、

失効証明書(CRL エントリー、証明書シリアル#、失効日時. . .)

7.3. OCSP プロファイル

GlobalSign CA は、使用する OCSP プロファイルの記録を、独立した技術文書として保持する。
GlobalSign CA は、この書類を、理由を説明し要求する者に対して、GlobalSign CA の判断で開示する。

8. 準拠性監査とその他監査基準

GlobalSign CA は、公開していないが、監査運用規定に準拠して、監査を受ける。GlobalSign CA は、それら監査の結果に従い実装する前に、それらを評価、検討する。
適用範囲と内容に関して独自に承認後、GlobalSign CA は、要件と標準化と手続と、本 CP に従ったサービスレベルと、適合していると公言する認定スキームが、適合していることを保証するため、この順守監査を受入れる。

8.1. 準拠性監査とその他監査基準

認定スキームの要件に適合する GlobalSign の情報は、そのような認定スキームにより、直接探求される。
GlobalSign は無事監査を通り、WebTrust for CA として知られる認定スキームの要件に、現在も適合している。GlobalSign CA は、この認定スキームを維持しようと努める。

GlobalSign は、要件と標準化と手続と本 CP に従ったサービスレベルであることを、保証するために、順守監査を受け入れる。GlobalSign CA は、取引に関する守秘などの一定条件のもと、公開していないが独自の監査運用規定に準拠して、この監査を受ける。このような監査は、直接または、GlobalSign が義務を負う代理人を通して、実施される。

8.1.1. 監査プロセスの条件

監査の実施人当たって、GlobalSign と直接・間接を問わず提携関係になく、また利害の衝突もない独立した監査人が指名される。
監査が実施される領域は、以下のもの(但し、これに限定しない)がある。

- GlobalSign 運用規定と手続の方針、及び本 CP により定められているているサービスレベルへの適合性
- CA サービスを実装する基盤の管理
- サイトの物理的基盤の管理
- 本 CP の厳守
- 関連する法律の厳守
- 同意サービスレベルの主張
- 監査証跡、ログ、関連書類他の検査
- 上記条件の順守失敗の原因

監査への適合性に関して、GlobalSign は、証明書を運用するために使用した下請業者の遂行の責任を、

下記の章に示すものを含め、取る

8.1.1.1. 事業提携

分散する電子商取引サービスプロバイダーとユーザの幅広い証明書ニーズにより良く対応するために、GlobalSignは、証明書の登録を含むPKI関連のサービスを提供するために、適切に選定するビジネスパートナーと協力し合う。GlobalSign は、そのサービスの提供面で、一部、又は全部を外部委託する。証明書ライフサイクル又は運用のある部分を管理するためにパートナー、又は代理人にかかわらず、GlobalSignが全プロセスの最終責任を持つ。GlobalSignは、GlobalSign CPの条件に従って、その責任を制限する。

8.1.1.2. セキュアデバイスと秘密鍵の保護

GlobalSignは、証明書をセキュアに発行し、管理し、格納する、不正開封防止装置とセキュアな装置の使用をサポートする。GlobalSign は、秘密鍵の危殆化を防ぐために、認定された信頼できるハードウェアを使用する。

9. 他のビジネス及び法的要件

この章で記載されるとおり、本CPのもとGlobalSign CA証明書の発行に適用される、ある法的条件がある。

9.1. 料金

GlobalSign CA証明書の発行と管理は、要求時に見積もられる料金を前提としている。

9.1.1. 返金ポリシー

GlobalSign は、返金要求を書面で受け取る。返金要求は、正式なものとして GlobalSign の法務サービスに送付される必要がある。GlobalSign によって提示されている保証のフレームワーク内での要求でなければ、GlobalSignが、受諾、許諾、返金する権利を保留する。

9.2. 財務的責任

GlobalSignは本CPのもと、認識する責任に適合する、十分なリソースを維持する。GlobalSign CAは、“あるがままで”サービスを提供する。

9.3. ビジネス上の秘密情報の管理について

GlobalSign CPに記載の通り、GlobalSignは、個人データのプライバシー規則と機密規則を監視する。機密情報には以下のものを含む

- 証明書に含まれる以外の利用者が識別できる個人情報
- 証明書ステータス情報に公開される以外の、CA証明書の失効理由
- 監査証跡

- CA サービスに関する通信
- CA 秘密鍵

以下の情報は、機密情報ではない。
- 証明書とその中身
- 証明書のステータス

GlobalSign は、以下の何れかを、認証または正当と判断できない限り、いかなる機密情報も開示又は、開示の要求をされることはない。
- その情報を極秘に保持するように、GlobalSign が義務を負っている相手が、情報を要求しているもの
- 裁判所の命令

GlobalSign は、そのような開示の手続に対し、事務手数料を請求する。

機密情報を要求し受け取る者は、要求した目的で使用し、危殆化からセキュアに守り、その他の使用と第三者への開示は控える、と言う仮定のもと許可を与える。

9.3.1. 開示条件

機密でない情報は、利用者と依拠当事者に、以下の条件で開示される
- 利用者又は依拠当事者の問合せ毎に、1つの証明が提供される
- 1証明書のステータスが、利用者または依拠当事者の問合せ毎に提示される
- 利用者は、彼らの情報を持つ CA に問合せることが出来る

機密情報は、利用者にも依拠当事者にも開示されない。GlobalSign CA は、適正に CA の人に情報の開示を管理する。

GlobalSign CA は、情報開示を要求するものを、以下の情報で認証する
- 利用者又は依拠当事者の要求時に提示される、認証用証明書
- OCSP 要求と CRL への署名応答

GlobalSign CA は、以下の機密情報を含む通信では、暗号化をする
- CA と RA 間での通信リンク
- 証明書及び、証明書ステータス情報を配布するときのセッション

法人情報への参照では、URL 他を含むテキストベースまたはコンピュータベースのポインターを GlobalSign CA は使用する。

9.4. 個人情報保護

GlobalSign CAは、申請者がGlobalSign CA証明書をウェブサイトを通しての申請する場合の個人情報の保護に、特定のデータ保護ポリシーを適用する。GlobalSign CA は、www.globalsign.net/repositoryに参照可能な文書化されたGlobalSign NVのプライバシーポリシーを厳守している。

GlobalSign CA の運用規定は、1992 年 12 月 8 日のベルギーのプライバシー保護法の規定内に入り、これは、1995 年 10 月 24 日のヨーロッパ議会(オフィシャルジャーナル L 281,23/11/1995 p. 0031-0050)での「個人情報の処理とその自由な移動に関する個人の保護」を定めたヨーロッパ指令 95/46/EC を実装した 1998 年 12 月 11 日に法改正された「個人データの処理」に関連している。

ベルギーにおける個人データ保護の規制は、「個人情報の処理とその自由な移動に関する個人の保護」を定めたヨーロッパ指令 95/46/EC を実装する。

GlobalSign CA は、電子通信セクターにおける個人データの処理とプライバシーの保護に関する 2002 年 7 月 12 日のヨーロッパ議会の指令 2002/58/EC を認知している。GlobalSign CA は、本 CP で明言している個人データ保護の条件のもと運用している。

GlobalSign CA は、保持、収集、処理した個人データの記録保存に関し、ベルギーのデータ保護委員会以前に適切な表明をしてきた。、ベルギーのデータ保護委員会には、Ministry of Justice,Waterloolaan 115,B-1000 Brussels, Belgium(tel. +32 2 5427206)に、連絡できる。

9.5. 知的財産権

GlobalSign CA は、データベース、ウェブサイト、GlobalSign CA 電子証明書と本 CP を含め GlobalSign CA が発信した出版に関連するすべて知的所有権を所有し、その権利を留保する。

GlobalSign CA の全ての CA の識別名は、GlobalSign CA だけの財産であり、その権利を施行する。

証明書は GlobalSign CA 又は GlobalSign に証明書管理を許諾する権利ある所有者の財産である。GlobalSign CA は、証明書の複製と交付を、非独占的、著作料なしのベースで、ただ GlobalSign CA の書面による許可なく、公にアクセス可能なリポジトリ又はディレクトリに証明書を公開できないことを除き複製も公布もフルに出来るという条件で、許可する。この制限の範囲は、証明書にある個人データの許可されない再発行から利用者を保護することを意図している。

GlobalSign CA は、他の者に明示的に所有権を移転していない自社の製品とサービスのすべての知的所有権を、所持し、留保する。

9.6. 責任と義務

GlobalSign CA は、本 CP と利用者契約書を使用し、GlobalSign CA 証明書の使用に関する法的条件を利用者と依拠当事者に移転する。
GlobalSign CA、RA、利用者、依拠当事者、その他必要な参加者は、陳情し、保証を引き当てる。
GlobalSign CA、RA、利用者を含む GlobalSign 範囲のすべての者は、対応する秘密鍵の完全性を保証する。万一、秘密鍵が危殆化したと疑わしく思う場合は、直ちに適正な RA に通知する。

9.6.1. 利用者の義務

本 CP で宣言されない場合、利用者は以下に責任をもつ
・ (証明書の)知識を持ち、必要なら電子証明書使用のトレーニングを受ける

- 信頼できるシステムを使い、秘密鍵―公開鍵ペアを生成する
- GlobalSign CA との通信で、正確で正しい情報を提供する
- GlobalSign CA に送信した公開鍵と、秘密鍵の使用とが正しく対応していることを確認する
- GlobalSign CA リポジトリに公開されている GlobalSign CA の CP と関連するポリシーのすべての条件と条項を受け入れる
- GlobalSign CA 証明書の不正な改ざんを防ぐこと
- GlobalSign CA 証明書を、本 CP に従って、適法かつ許可された目的に使用すること
- 提出情報に変更が発生したばあい GlobalSign CA または GlobalSign RA への通知すること
- リストされている情報が無効になった場合は、GlobalSign CA 証明書の利用をやめること
- GlobalSign CA 証明書が無効になった場合、その使用をやめること
- インストールした装置やアプリケーションが無効になった場合、GlobalSign CA 証明書を取り除くこと
- 道理にかなった環境で、GlobalSign CA 証明書を使うこと
- 秘密鍵の、危殆化、紛失、開示、改竄、その他許可されない使い方を防ぐこと
- 秘密鍵を生成、保持、第三者預託、又は破壊するために利用者が使うパートナー又は代理人の行為や不作為
- GlobalSign CA 又は GlobalSign CA ディレクトリに、他者の権利や法律を冒す陳述書を含むものを投稿することは防ぐこと
- GlobalSign CA 証明書の完全性を実質的に冒す事象は発生した場合、証明書の失効要求を出すこと
- 利用者が秘密鍵の危殆化が疑念されたり、危殆化にが付いた場合、直ちに適切な RA に通知すること
- 登録に関して、本 CP の要件に沿って、正しく完全な情報を GlobalSign に提出すること
- 本 CP と締結した CA chaining 契約書に基づき利用者に通知されている制限事項に従い、鍵ペアを電子署名にだけ使用すること
- 秘密鍵の許可されない利用を回避するよう十分な注意をして訓練すること
- 電子署名目的に適していると認識されているアルゴリズムを使用して利用者鍵を生成すること
- 電子署名目的に適していると認識されている鍵長とアルゴリズムを使用すること
- 証明書に示されている有効期間の終わり前に、以下のことが起こった場合、遅れることなく GlobalSign CA に通知すること
    - ― 利用者秘密鍵が紛失、盗難、危殆化の可能性があるか
    - ― 利用者秘密鍵のコントロールが、活性化データ(例えば PIN)の危殆化で、失われた場合
    - ― 利用者に通知された証明書コンテンツに不正確や変更が発生した場合

証明書を申請したとき、利用者にその選択の全責任がある。申請者と GlobalSign は、組織関係と同様、信頼する装置の使用法を定めなければならない。

トップルート局としてまた、唯一で重要なサービスを可能にするネットワークの運用者として、GlobalSign は、CA chaining 利用者とのより強固な信頼関係を探求していく。利用者は、いつの時点でも、GlobalSign の CA cahining サービスを使用しているときに、他の認証局による CA chaining サービスを探すことは控えるものとする。この制限は、ルートだけに考えられたものではなく、利用者組織の全体に適用するものである。

9.6.2. 依拠当事者の義務

GlobalSign CA 証明書の依拠当事者は、下記を約束する

- 電子証明書を使う技術があること
- GlobalSign CA からの通知と依拠当事者に対する条件を受け取ること
- 適切な証明書パス検証手続で GlobalSign CA から公開されている証明書ステータス情報(例えば、CRL)を使い、GlobalSign CA 証明書を検証すること
- 証明書に記載の情報が検証手続を通して、正しくかつ最新であると検証出来たときに限り、その GlobalSign CA 証明書を信頼すること
- その環境において道理が通って場合に限り、GlobalSign CA 証明書を信頼すること
- 秘密鍵が危殆化したと気づいたとき、又はその疑いがあるとき、直ちに適切な RA に通知すること

依拠当事者の義務は、証明書にかなり依存している場合、

- 依拠当事者に示された失効ステータスを使い、CA 証明書の失効または有効性を検証する
- CP 又は証明書の中で依拠当事者に示された、証明書の使用に関する制限に注意を払うこと
- 証明書が使われるアプリケーションで適用される、その他のポリシーや条件・条項と同様に、GlobalSign CA 証明書で規定しているその他の安全対策をとること

証明書が使われる特定の業務の中の環境で、依拠当事者は、いつもその環境を考慮して証明書を信頼することの正当性を確立しておかなければならない。

9.6.2.1. 依拠当事者の義務の伝達

失効情報への自由な(禁止がない)アクセスを与え、結果として自身のサービスの信頼を引き出すため、GlobalSign CA は、依拠当事者と彼らの義務を結びつける目的での証明書の検証をコントロールする、依拠当事者との契約は、実装をさし控える。
しかしながら、GlobalSign のパブリックサービスの参加者に現れるように、依拠当事者が使用する GlobalSign のリソースは、GlobalSign CP に例示されている GlobalSign のポリシーフレームワークで提示された条件で、暗黙に統治されている。
依拠当事者は、証明書を検証し信頼を確立する目的で GlobalSign リソースに問い合わせる度に、本 CP の中で使われている条件に拘束されることを、ここに、通告する。

9.6.3. 利用者の依拠当事者に対する義務

本 CP に述べられている利用者の義務を制限することなく、利用者は、CA 証明書の中の不実表示に関し、その表示を妥当に信頼する第三者に対し法的責任を負う。

9.6.4. GlobalSign CA リポジトリとウェブサイトの条件

GlobalSign CA リポジトリとウェブサイトにアクセスする者(利用者及び依拠当事者を含む)は、本 CP の規定と GlobalSign が規定する使用法に関する条件に同意する。CP の使用法に関する条件の受容は、その者が、CA 証明書のステータスの問合せを送信する、又はそのような情報やサービスを使用する、又は頼ることで明示する。GlobalSign CA リポジトリは下記を含む

- CA 証明書の検索結果で提供される情報

- 証明書にリストされる公開鍵に対応した秘密鍵で造られたディジタル署名のステータスを検証するための情報
- データを証明書に含まれる公開鍵で暗号化する前に、電子証明書のステータスを検証するための情報
- GlobalSign CA ウェブサイトに公開される情報
- このウェブサイトで、GlobalSign CA が通告又は提供するその他のサービス

GlobalSign CA は、その申請期間及び、証明書の期限切れ又は失効後5年間、証明書のリポジトリを保持する。GlobalSign RA のいつ何時の問合せに対し、完全性を検証するために、完全なリポジトリを用意する。
加えて、GlobalSign CA リポジトリは、依拠当事者も利用可能である。

9.6.4.1. 自己責任での信頼

GlobalSign CA リポジトリとウェブサイトにある情報にアクセスし信頼することは、そこにアクセスする者自身の責任である。その者は、証明書で提示されている情報に信頼を置くべきかを決断するための適正な情報を受取ったと認識する。GlobalSign CA は、証明書のステータスに関する記録とディレクトリを更新するに必要な全てのステップをとり、それに関する警告を発する。GlobalSign CA リポジトリとウェブサイトの使用条件に応じなかった場合、GlobalSign CA とその者との関係を終結する結果になるかもしれない。

9.6.4.2. 情報の正確さ

GlobalSign CA は、リポジトリにアクセスする者が、正確で、正しく、最新の情報を受け取ることを保証するため、全ての努力を厭わない。しかしながら、GlobalSign CA は、本 CP と GlobalSign CA 保険ポリシーに定めた制限を越えての責任を負うことは出来ない。

9.6.5. GlobalSign CA の義務

本 CP の関連する章で定義される範囲で、GlobalSign CA は以下の約束する

- 本 CP と、https://www.globalsign.net/repository に公開されるその修正に従うこと
- パブリック証明書管理サービスのための GlobalSign CA リポジトリとウェブサイトの確立と運用を含む、証明書サービスとその基盤を提供すること
- 信頼のメカニズムを提供すること。それには、鍵生成、鍵の保護、自身の基盤に関する秘密シェアの手続を含む
- 自身の秘密鍵が危殆化した場合、即座の通知
- パブリックに展開する証明書の色々なタイプの申請手続の提供と検証
- 本 CP に従った電子証明書の発行と、ここで表明している義務の提供
- RA からの有効で承認された証明書の失効要求の受領に伴う、本 CP に従った証明書失効
- 本 CP に従った、受容した証明書の公開
- 本 CP で記載されている、利用者と依拠当事者へのサポートの提供
- 本 CP に従った、証明書の期限切れに対する証明書更新の提供
- 本 CP に従った、全ての一時停止又は失効の証明書の CRL 又は OCSP レスポンスの公開
- サービスレベルアグリーメントに従った、サービスレベルの提供
- GlobalSign CA リポジトリへの CRL の公開による、依拠当事者への証明書失効の通知

上記に述べた項が直接の原因となる、立証される被害の GlobalSign CA の法的負債は、各証明書1枚につき1ユーロを上限とする。この上限は GlobalSign により改正されるかの知れない。GlobalSign は、証明書に含まれる情報の正確性から出てくるリスクに対する、追加の保険を模索する。GlobalSignは、限定保証ポリシーを提示する。

法が許す範囲で、GlobalSign CA は以下のことに関して法的義務は負わない

- 本 CP で定めた以外の証明書の使用
- トランザクションデータの改ざん
- 不正に構成され又は使用された装置で、CA の責任のもとで運用されていないもの、証明書を含んだトランザクションに使用されたもの。
- 証明書に関連する秘密鍵の危殆化
- 証明書に関連する秘密鍵を守る PIN コードの紛失、露出、誤使用
- 識別データ、シリアル番号、公開鍵の値を含む RA からの、間違った、不完全なデータ提示
- 自然災害
- 証明書の使用
- 相互認証 CA(下位 CA ではない)及びその依拠当事者の、公開鍵または秘密鍵の使用
- 自身の組織内で他の認証局との CA chaining サービスを保持する利用者に提供されたサービス。この制限は、サービスを提供した顧客組織全体に適用し、特定のルートとか CA が chain されたルートだけではない。

GlobalSign CA は本 CP のもと、これ以上の義務はないと認知している。

9.6.6. 登録局の義務

GlobalSign ネットワークないで運用している GlobalSign RA は、以下を約束する

- 信頼できるシステムを使用し、直接又は代理人を使い、RA の管理者鍵ペアを安全に生成する
- GlobalSign CA との通信で、正確で正しい情報を提供する
- GlobalSign CA に提示した公開鍵は正しい物であることを保証する
- GlobalSign CA に、彼らが要求する証明書に使用される新しいセキュア鍵ペアの生成
- この GlobalSign CP に従って、GlobalSign CA 証明書の申請を受け取る
- GlobalSign CA の手続と本 CP によって、規定される検証と認証の行為を実施する
- GlobalSign CA に、申請者の要求を署名メッセージ(証明書要求)で送信する
- GlobalSign CA の手続と GlobalSign CA の CP に従い、GlobalSign CA 証明書の全ての失効要求を、受取り、検証し、GlobalSign CA に中継する。
- 本 CP に従い、証明書の更新時に、利用者から提供される情報の正確さと真正性を検証する

9.6.7. 参照により電子証明書に組み込まれる情報

GlobalSign は、発行するすべての電子証明書に、以下の情報を参照により組み込む。

- 対応する CP の条項と条件
- 発行された GlobalSign 証明書に表明される、他の証明書ポリシー
- X.509 標準の必須エレメント
- X.509 標準の必須ではないが、カスタマイズされたエレメント
- 証明書には全ては記載されていない、拡張名称と拡張の中身
- 証明書のフィールドで、そうあるべきと示されているその他情報

9.6.8. 参照による組込みポインタ

参照による組込み情報として、GlobalSign は、コンピュータベース、テキストベースのポインタを使用する。GlobalSign は、URL や OID 等を使用する。

9.7. 保証外事項

この章には、保証の免責条項を含む

9.7.1. 保証の制限

GlobalSign CA は、以下は保証しない

- GlobalSign CA 保証ポリシーと本 CP の下記の関連製品記述に述べられていること以外の、証明書に含まれる情報の検証できない部分、の正確性
- フリーのテスト又はデモ用証明書に含まれる情報の、正確さ、真正性、完全性または適合性

9.7.2. ダメージの除外要素

いかなる場合(詐欺行為、意図的違法行為を除く)も、GlobalSign CA は下記の責任を負わない

- 利益の損失
- データの損失
- 証明書又はディジタル署名の、使用、配布、許諾、及び実行、不実行に関連し、そこから発生する全ての間接的、必然的、懲罰的ダメージ
- 取引又は、提供サービス又は、本 CP フレームワーク内のもの
- 証明書(無料、デモ、テスト用を除く)の検証情報に信頼を置いて被ったダメージを除いたその他全てのダメージ
- 上記のような検証情報のエラーが、申請者の詐欺行為、意図的違法行による結果であった場合、法的責任

9.8. 責任の制限

GlobalSign の賠償責任の上限は、GlobalSign の限定保障ポリシーに従い制限される
保障の条件の詳細は、www.globalsign.net/repositoryに掲示する

9.9. 補償

この章は、適用可能な損失保障を含む

9.9.1. 補償

法の許す範囲で、利用者は、損害賠償、損失、ダメージ、訴訟、その他適正な弁護士費用を含む経費など GlobalSign が被るであろう下記の行為又は不作為の結果から GlobalSign CA をその害から守り、損失

保障することに同意する。

- 利用者秘密鍵の保護の失敗
- 要求による信頼できるシステムの使用
- 利用者の秘密鍵の危殆化、紛失、開示、改ざん、許可されない使用等、を避けるために必要な予防措置
- GlobalSign ルートの完全性への注意

9.10.本規程の効力

本 CP は、ウェブサイトとリポジトリ上に、GlobalSign CA により反対(効力がないとの)の通知が出るまで、有効に効力を持つ。
通知される変更は、適切にバージョンに表示される。その後、30日で変更が公示される。

9.11.コミュニティにおける通知と連絡

GlobalSign CA は、本 CP に関する通知を、書面によるフォームもしくはディジタル署名されたメッセージにより受け取る。GlobalSign CA からのディジタル署名された受領確認の受信で、通知の送信者は情報伝達ができたと見なす。送信者は、そのような受領確認を20営業日以内に受け取る、さもなくば、紙による通知を、配達を確認する配達業者のサービスを通し、又は配達記録郵便か受取証明郵便で、前払い且つ受取り領収を要求して、以下のアドレスに送付しなければならない。
GlobalSign CAへの個人からの情報伝達は、legal@globalsign.netか、GlobalSignへの郵便は、この書類の、はじめにの章に記載した、住所に送付しなければならない。

9.12.改訂

本 CP の変更は、適切な番号付与で表される。
GlobalSign CA の Policy Management Authority でバージョンの付与番号を決める。

9.13.紛争解決手続

裁決やその他のタイプの代替論争解決(簡略裁判、仲裁裁判、拘束力のある専門家の勧告や協定、監視専門家・一般専門家の勧告)等の手段を使う前に、GlobalSign に論争と論争解決手段の考え知らせることに、合意する。

論争の通知を受けると、GlobalSign CA 管理にどのように論争を処理するかを助言する論争委員会を、GlobalSign は招集する。論争委員会は、論争の通知を受け取った日から20営業日以内に召集する。論争委員会は、法廷弁護士、データ保護オフィサー、GlobalSign の運用管理と、セキュリティオフィサから構成される。弁護士かデータ保護オフィサーが議長を務める。論争委員会は、調停プロセス GlobalSign の重役に上申する。GlobalSign の重役は、提案された調停案を残ったもの(当事者)に伝える。

9.13.1. 仲裁

論争が通知を受けてから20営業日以内に解決しなかった場合は、CPS にそって、ベルギーの法務コード 1676-1723 に従い、論争を仲裁に送る。

裁定人は 3 人となり、各当事者から 1 人提案され、論争当事者が 3 人目を選ぶ。仲裁の場所は、Leuven, Belgium で裁定者が関連する費用を決める。
技術関連の論争と本 CP に関連する論争では、各当事者は以下の仲裁を受け入れる。
Belgian branch of Geschillenoplossing Automatisering (Foundation for the Settlement of Automation Dispute) with registered office in
J. Scheepmansstraat 5,
3050 Oud-Heverlee, Belgium.
Tel:+32-47-733 82 965, Fax:+32-16-32 54 38

9.14.準拠法

本 CP は、ベルギーの法律にもとづき、統治、解釈される。この法の選択は、住居や、GlobalSign 電子証明書、他の製品やサービスの使用場所に関係なく、本 CP の解釈の一意性を保証するものである。GlobalSign が提供者、供給者、受益者として振舞い GlobalSign 製品とサービスに関連する関係で、本 CP が明示的又は黙示的に適用される、全ての GlobalSign の商業的・契約的の関係に、ベルギーの法律は適用される。
GlobalSign のパートナー、利用者、依拠当事者を含め各当事者は、無条件に、Leuven,Belgium の地方裁判所に送られる。

9.15.適用法の遵守

GlobalSign CA は適用可能なベルギーの法律に準拠する。GlobalSign CA パブリック証明書管理製品とサービスに使用されているある種のソフトウェアの輸出は、適正な権限機関の承認を必要とする。各当事者(GlobalSign CA、利用者と依拠当事者を含む)は、適用可能なベルギーの輸出の法律と規制に適合することに同意する。

9.16.雑則

9.16.1. 存続

“Legal Conditions”の章に含まれる、責任と制限事項は、本 CP の終了後も存続する

9.16.2. 分離条項

(分離された場合)本 CP のいかなる条項も、賠償責任の制限の条項を含め、無効で効力がなくなる。本 CP の残りの部分は、当事者のもともとの意図を発行する形で解釈される。

10. 用語の定義リスト

ACCEPT (A CERTIFICATE)

To approve of a digital certificate by a certificate applicant within a transactional framework.

ACCREDITATION

A formal declaration by an approving authority that a certain function/entity meets specific formal requirements.

APPLICATION FOR A CERTIFICATE

A request sent by a certificate applicant to a CA to issue a digital certificate.

ARCHIVE

To store records for period of time for purposes such as security, backup, or audit.

ASSURANCES

A set of statements or conduct aiming at conveying a general intention.

AUDIT

Procedure used to validate compliance with formal criteria or controls.

AUTHENTICATED RECORD

A signed document containing assurances of authentication or a message with a digital signature verified by a valid Class 3 certificate by a relying party.

AUTHENTICATION

A process used to confirm the identity of a person or to prove the integrity of specific information by placing them within the right context and veryfying such relationship.

AUTHORISATION

Granting of rights.

AVAILABILITY

The rate of accessibility of information or resources.

HARDWARE MODULE

The complete system of the hardware module used to keep the certificates and securely generate a key pair.

BINDING

A statement by an RA of the relationship between a named entity and its public key.

CERTIFICATE

The public key of a subject and the associated information, digitally signed with the private key of the issuer of the certificate. Unless explicitly specified, the certificates described here are the subscriber's ones .

CERTIFICATE REVOCATION LIST OR CRL

A list maintained by the CA of certificates that are revoked before their expiration time.

CERTIFICATION AUTHORITY OR CA

An entity that is trusted to associate a public key to the information on the subject, contained in the certificate. Unless explicitly specified, the CA described herein is the GlobalSign CA.

CERTIFICATION PRACTICE STATEMENT OR CPS

A statement of the practices in the management of certificates during all life phases.

CERTIFICATE STATUS SERVICE OR CSS

A service, enabling relying parties and others to verify the status of certificates.

CONTRACT PERIOD

The duration of the GlobalSign CA contract between the Dutch National Register and the CA organization.

CERTIFICATE CHAIN

A hierarchical list certificates containing an end-user subscriber certificate and CA certificates.

CERTIFICATE EXPIRATION

The end of the validity period of a digital certificate.

CERTIFICATE EXTENSION

A field in the digital certificate used to convey additional information on issues that include: the public key, the certified subscriber, the certificate issuer, and/or the certification process.

CERTIFICATE HIERARCHY

A level based sequence of certificates of one (root) CA and subordinate entities that include, CAs and subscribers.

CERTIFICATE MANAGEMENT

Actions associated with certificate management include, storage, dissemination, publication, revocation, and suspension of certificates.

CERTIFICATE REVOCATION LIST (CRL)

A list issued and digitally signed by a CA that includes revoked and suspended certificates. Such list is to me consulted by relying parties at all times prior to relying on information featured in a certificate.

CERTIFICATE SERIAL NUMBER

A sequential number that uniquely identifies a certificate within the domain of a CA.

CERTIFICATE SIGNING REQUEST (CSR)

A machine-readable application form to request a digital certificate.

CERTIFICATION

The process to issue a digital certificate.

CERTIFICATION AUTHORITY (CA)

An authority, such as the GlobalSign CA that issues, suspends, or revokes a digital certificate.

CERTIFICATE POLICY (CP)

A statement of the practices of a CA and the conditions of issuance, suspension, revocation etc. of a certificate. A CP is also used as guidance to establish the trustworthiness of a certification services infrastructure.

CERTIFICATE ISSUANCE

Delivery of X.509 v3 digital certificates for authentication and digital signature based on personal data and public keys provided by the RA and compliant with RFC 3647 and RFC 3039

CERTIFICATE SUSPENSION

Online service used to temporarily disable a digital certificate and to automatically revoke it if no request for re-activating it is submitted within a certain time period

CERTIFICATE REVOCATION

Online service used to permanently disable a digital certificate before its expiration date

CERTIFICATE REVOCATION LISTS

Online publication of complete and incremental digital certificates revocation lists compliant with RFC 2459

COMMERCIAL REASONABLENESS

A legal term from Common Law. In electronic commerce it means the usage of technology that provide reasonable assurance of trustworthiness.

COMPROMISE

A violation of a security policy that results in loss of control over sensitive information.

CONFIDENTIALITY

The condition to disclose data to selected and authorised parties only.

CONFIRM A CERTIFICATE CHAIN

To validate a certificate chain in order to validate an end-user subscriber certificate.

DIGITAL CERTIFICATE

A formatted piece of data that relates an identified subjext with a public key the subject uses.

DIGITAL SIGNATURE

To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial message has been altered since the transformation was made.

DISTINGUISHED NAME

A set of data that identifies a real-world entity, such as a person in a computer-based context.

DIRECTORY SERVICE

Online publication of certificates allowing the retrieval of a certificate based on its certificate identifier.

END-USER SUBSCRIBER

A subscriber other than another CA.

ENHANCED NAMING

The usage of an extended organisation field (OU=) in an X.509 v.3.0 certificate.

EXTENSIONS

Extension fields in X.509 v.3.0 certificates.

GENERATE A KEY PAIR

A trustworthy process to create private keys during certificate application whose corresponding public key are submitted to the applicable CA during certificate application in a manner that demonstrates the applicant's capacity to use the private key.

HASH

An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:

- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

IDENTIFICATION

The process to confirm the identity of an entity. Identification is facilitated in public key cryptography by means of certificates.

INCORPORATE BY REFERENCE

To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

KEY GENERATION PROCESS

The trustworthy process of creating a private/public key pair. The public key is supplied to a CA during the certificate application process.

KEY PAIR

A private key and its corresponding public key in asymmetric encryption.

NOTICE

The result of notification to parties involved in receiving CA services in accordance with this CP.

NOTIFY

To communicate specific information to another person as required by this CP and applicable law.

NOTARISED TIME STAMPING

Online service used to timestamp and securely archive a document; the document is re-timestamped on a regular basis

with up-to-date technology.

OBJECT IDENTIFIER

A sequence of integer components that can be assigned to a registered object and that has the property of being unique among all object identifiers within a specific domain.

PKI HIERARCHY

A set of CAs whose functions are organised according to the principle of delegation of authority and related to each other as subordinate and superior CA.

PRIVATE KEY

A mathematical key to create digital signatures and sometimes (depending upon the algorithm) to decrypt messages in combination with the corresponding public key.

PUBLIC KEY

A mathematical key that can be made publicly available that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can also be used to encrypt messages or files which can then be decrypted with the corresponding private key.

PUBLIC KEY CRYPTOGRAPHY

Cryptography that uses a key pair of mathematically related cryptographic keys.

PUBLIC KEY INFRASTRUCTURE (PKI)

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.

REGISTRATION AUTHORITY OR RA:

An entity that has the responsibility to identify and authenticate subscribers. The RA does not issue certificates. It merely requests the issuance of a certificate on behalf of applicants whose identity it has verified.

RELATIVE DISTINGUISHED NAME (RDN)

A set of attributes that distinguishes the entity from others of the same type.

RELIANCE

To accept a digital signature and act in a way that shows trust in it.

RELYING PARTY

Any entity that relies on a certificate for carrying out any action.

REPOSITORY

A database and/or directory listing digital certificates and other relevant information accessible on-line.

REVOKE A CERTIFICATE

To permanently end the operational period of a certificate from a specified time forward.

SECRET SHARE

A portion of a cryptographic secret that has been divided among a number of physical tokens, such as smart cards etc.

SECRET SHARE HOLDER

An person that holds a secret share.

SHORT MESSAGE SERVICE (SMS)

A service for sending messages of up to 160 characters (224 characters if using a 5-bit mode) to mobile phones that use Global System for Mobile (GSM) communication.

SIGNATURE

A method that is used or adopted by a document originator to identify himself or herself, which is either accepted by the recipient or its use is customary under the circumstances.

SIGNER

A person who creates a digital signature for a message, or a signature for a document.

SMART CARD

A hardware token that contains a chip to implement among others cryptographic functions.

STATUS VERIFICATION

Online service based on the Online Certificate Status Protocol (RFC 2560) used to determine the current status of a digital certificate without requiring CRLs

SUBJECT OF A DIGITAL CERTIFICATE

The named party to which the public key in a certificate is attributable, as user of the private key corresponding to the public key.

SUBSCRIBER

The subject of a digital certificate, or a party designated by the subject to apply for the certificate.

SUBSCRIBER AGREEMENT

The agreement between a subscriber and a CA for the provision of public certification services.

SUSPENDED CERTIFICATE

Temporarily discarded certificate, which nevertheless is kept on hold for one week until revocation or reactivation notice is given to GlobalSign CA by the RA.

TRUSTED POSITION

A role within a CA that includes access to or control over cryptographic operations that may allow for privileged access to the issuance, use, suspension, or revocation of certificates, including operations that restrict access to a repository.

TRUSTWORTHY SYSTEM

Computer hardware, software, and procedures that provide an acceptable level against security risks, provide a reasonable level of availability, reliability, and correct operation and enforce a security policy.

GLOBALSIGN CA REGISTRATION AUTHORITY:

An entity that verifies and provides all subscriber data to the GlobalSign CA.

GLOBALSIGN CA PUBLIC CERTIFICATION SERVICES

A digital certification system made available by GlobalSign CA as well as the entities that belong to the GlobalSign CA domain as described in this CP.

GLOBALSIGN CA PROCEDURES

A document describing the GlobalSign CA's internal procedures with regard to registration of end users, security etc.

WEB – WORLD WIDE WEB (WWW)

A graphics based medium for the document publication and retrieval of information on the Internet.

WRITING

Information accessible and usable for reference.

X.509

The standard of the ITU-T (International Telecommunications Union-T) for digital certificates.

11. 頭字語リスト

CA: Certification Authority
CEN/ISSS: European Standardisation Committee / Information Society Standardisation System
CP: Certificate Policy
CPS: Certification Practice Statement
ETSI: European Telecommunications Standards Institute
GSCA: GlobalSign Certification Authority
IETF: Internet Engineering Task Force
ISO: International Standards Organisation

ITU: International Telecommunications Union
OCSP: Online Certificate Status Protocol
PKI: Public Key Infrastructure
RFC: Request for Comments
SSCD: Secure Signature Creation Device
VAT: Value Added Tax