発行番号	4BUS_DM_18005_02
発行年月日	2019年　2月　1日

連絡書

セイコーソリューションズ株式会社
DXソリューション統括部

お客様各位

〒261-8507千葉県千葉市美浜区中瀬1-8
TEL　043-273-3342
FAX　043-273-3332

件　名：　タイムスタンプで利用している証明書の4096bit化について（改訂版）

拝啓、貴社ますますご清栄の段お慶び申し上げます。
平素は格別のご高配を賜り、厚く御礼申し上げます。
標記の件につきまして、下記の通りご連絡申し上げます。
ご対応のほど、よろしくお願い申し上げます。

敬具

－ 記 －

この度GMOグローバルサイン株式会社様から発行され、弊社タイムスタンプサービスにて使用している電子証明書の一部に変更が発生します。具体的には有効期限が10年間のタイムスタンプ暗号化強度対応のため、証明書の鍵長がRSA2048bitからRSA4096bitに変更になります。

つきましては下記内容をご確認の上、2019年3月10日までにお客様のタイムスタンプツール利用環境におきましてルートCA証明書および中間CA証明書の追加設定をお願い申し上げます。また、必要に応じプログラム改修を実施くださいますようお願い申し上げます。

1、対象のアプリケーション
・eviDaemon for PAdES（V4.5 以前）を利用しているお客様
~~・Adobe Reader を利用しているお客様~~
・独自アプリケーションを作成しているお客様（セイコータイムスタンプ利用のみ）
※eviDaemon for XAdES、かんたん電子契約は対象外となりますので対応は不要です。

2、変更日：2019 年 3 月 11 日

3、変更対象：ルート CA 証明書、中間 CA 証明書、TSA 証明書

4、影響範囲
2019年3月11日に、弊社タイムスタンプサービスで提供する新タイムスタンプのルートCA証明書、中間CA証明書およびTSA証明書の更新を実施いたします。新タイムスタンプを検証する環境において、これらの新しいルートCA証明書および中間CA証明書が登録されていない場合、電子証明書のパス検証が実施できないため、タイムスタンプ検証時にエラーが発生する可能性があります。

また、タイムスタンプ局より送付されるタイムスタンプトークン(データ)のサイズは当該仕様変更により、4.5Kバイト前後から7Kバイト前後に増加します。このため、該当サイズのデータ受信ができない場合、タイムスタンプの取得に失敗します。

タイムスタンプトークン（データ）の受取り用のバッファサイズが7Kバイト未満のアプリケーションについては、バッファサイズの修正が必要となります。バッファサイズに関してはアプリケーションの仕様に依存します。

お客様がご利用のタイムスタンプアプリケーションへの影響および対応方法については、各アプリケーションの提供元・開発元にお問い合わせください。

5、更新内容詳細

以下の証明書に変更となります。

種別	Subject名（DN）	RSA鍵長/ 署名アルゴリズム	有効期限
ルートCA証明書	CN = GlobalSign, O = GlobalSign, OU = GlobalSign Root CA - R6	4,096ビット/ SHA384withRSA	2034/12/10
中間CA証明書① (AATL用)	CN = GlobalSign CA for AATL - SHA384 - G4, O = GlobalSign nv-sa, C = BE	4,096ビット/ SHA384withRSA	2034/12/10
~~中間CA証明書② (AATL用)~~	~~CN = GlobalSign Partners TSA CA for AATL, O = GlobalSign nv-sa, C = BE~~	~~2,048ビット/ SHA384withRSA~~	~~2034/12/10~~
中間CA証明書③ (Windows用)	CN = GlobalSign Partners Timestamping CA - SHA384 - G4, O = GlobalSign nv-sa, C = BE	4,096ビット/ SHA384withRSA	2034/12/10

証明書の取得方法

種別	Subject名（DN）	取得方法
ルートCA証明書	CN = GlobalSign, O = GlobalSign, OU = GlobalSign Root CA - R6	下記より取得ください。 https://secure.globalsign.net/cacert/root-r6.crt
中間CA証明書① (AATL用)	CN = GlobalSign CA for AATL - SHA384 - G4, O = GlobalSign nv-sa, C = BE	下記より取得ください。 http://secure.globalsign.com/cacert/gsaatlsha2g4.crt
~~中間CA証明書② (AATL用)~~	~~CN = GlobalSign Partners TSA CA for AATL, O = GlobalSign nv-sa, C = BE~~	~~別途、弊社より提供させて頂きます。~~
中間CA証明書③ (Windows用)	CN = GlobalSign Partners Timestamping CA - SHA384 - G4, O = GlobalSign nv-sa, C = BE	下記より取得ください。 http://secure.globalsign.com/cacert/gsptnstsacasha384g4.crt

※中間CA証明書②（AATL用）につきましては、「Adobe Readerにおいてタイムスタンプトークンのサイズがオーバーフローし、タイムスタンプの埋め込みに失敗する。」という事象が発生することが明らかとなったため、AATL用につきましては中間CA証明書②を廃止し、「ルートCA証明書～中間CA証明書①～TSA証明書」の3階層とすることで、タイムスタンプトークンのサイズを縮小する方針に変更となりました。

6、対応期限

2019 年 3 月 10 日

7、留意事項

従来のルートCA証明書および中間CA証明書は引き続き有効であるため、タイムスタンプツール利用環境から削除しないようお願いいたします。なお、本作業は2019年3月10日より前に実施頂いても、現在のアプリケーションの動作に影響を与えることはございません。

また今回廃止となった中間CA証明書②(AATL用)につきまして、既にインストール済みであってもアプリケーションの動作に影響を与えることはございません。

8、テストサイトについて

下記にテストサイトを公開しております。

ホスト名:chsm2-timestamp.seiko-cybertime.jp
ユーザID:test1
パスワード:pass1

上記テストサイトは模擬証明書で構成した評価用AATLタイムスタンプを提供しておりますので、データ通信協会認定のタイムスタンプではございません。上記でタイムスタンプを取得後、模擬証明書を適切に配置もしくはインストールし、検証が正常に行われることをご確認ください。模擬証明書で問題がないことが確認できましたら本番用証明書も適切に配置もしくはインストールを行ってください。なお、eviDaemon for PAdESではテストサイトをご利用できませんので、別途ご案内させて頂く「eviDaemon for PAdESの信頼済み証明書ストア更新のお願いについて」を参照頂き、ご対応頂くようお願い申し上げます。

9、問い合わせ先

上記の件についてご質問は、担当営業または下記アドレス宛てにご連絡をお願い致します。

E-Mail : contact@seiko-cybertime.jp

以上