

2019 年 2 月 15 日

お客様各位

連絡書

寺田倉庫株式会社
ドキュメントソリューショングループ

タイムスタンプ証明書の 4096bit 移行について

拝啓 時下ますますご清祥のこととお喜び申し上げます。平素は格別のご高配を賜り、厚く御礼申し上げます。

さて、この度 GMO グローバルサイン株式会社から発行され、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。つきましては、お客様にはお手数をおかけしますが、下記の通りご対応くださいますよう、よろしくお願い申し上げます。

敬具

記

1. 変更内容

タイムスタンプサーバー証明書を下記の通り変更いたします

従来の証明書の階層（R3 ルート証明書チェーン）

- ルート CA 証明書：GlobalSign Root CA - R3（有効期限：2029 年 3 月 18 日）
- 中間 CA 証明書：GlobalSign CA for AATL - SHA256 - G2
- タイムスタンプサーバー証明書

変更後の証明書の階層（R6 ルート証明書チェーン）

- ルート CA 証明書：GlobalSign Root CA - R6（有効期限：2034 年 12 月 10 日）
- 中間 CA 証明書（L1）：GlobalSign CA for AATL - SHA384 - G4
- タイムスタンプサーバー証明書

2. 変更理由

タイムスタンプサービスの証明書に要求される長期間（11 年以上）の証明書発行に対応するため

3. 変更日

2019 年 3 月 15 日に実施いたします

4. 影響範囲

- 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
- 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. ご利用のプログラムにおける対応

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、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。

6. 証明書情報詳細

以下の証明書に変更となります

ルート CA 証明書：GlobalSign Root CA - R6

Subject DN	CN = GlobalSign O = GlobalSign OU = GlobalSign Root CA - R6
公開鍵アルゴリズム	RSA4096
証明書署名アルゴリズム	sha384RSA
CRL 配布先 URI	http://crl.globalsign.com/root-r6.crl
OCSP 提供 URI	http://ocsp2.globalsign.com/rootr6
証明書ダウンロード URI	https://secure.globalsign.net/cacert/root-r6.crt

中間 CA 証明書：GlobalSign CA for AATL - SHA384 - G4

Subject DN	CN = GlobalSign CA for AATL - SHA384 - G4 O = GlobalSign nv-sa C = BE
公開鍵アルゴリズム	RSA4096
証明書署名アルゴリズム	sha384RSA
CRL 配布先 URI	http://crl.globalsign.com/ca/gsaatlsha2g4.crl
OCSP 提供 URI	http://ocsp.globalsign.com/ca/gsaatlsha2g4
証明書ダウンロード URI	http://secure.globalsign.com/cacert/gsaatlsha2g4.crt

7. 対応期限

2019 年 3 月 14 日

8. 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 14 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。

9. 本件に関するお問合せ先

寺田倉庫株式会社

ドキュメントソリューショングループ

テラダタイムスタンプサービス 保守窓口

Mail: support_tsa@terrada.co.jp TEL: 03-5439-6100

以上