発行番号	4TSA_DM_23200_01
発行年月日	2023年 9月 16日

お客様各位

連絡書

セイコーソリューションズ株式会社
サイバータイムセンター

〒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：R45ルートCAから発行される電子証明書を使用したサービスの開始について

セイコータイムスタンプサービスは、現在使用しているルートCAの有効期限が2034年12月10日であることから、最低10年の検証を可能とするため、異なるルートCAから発行される証明書を使用するサービスを開始し、現在提供しているサービスを停止します。

お客様の環境にて、新たなサービスへの対応をお願いします。

1．変更内容

セイコータイムスタンプサービスが、時刻認証業務でデジタル署名を施すため使用している専用の利用者署名符号に対応した電子証明書（以下、TSA証明書）を発行するGMOグローバルサインは、長期間（11年以上）有効の証明書発行に対応するため、ルートCAをこれまでのR6ルートCAからR45ルートCAに変更します。

R6ルートCA：有効期限 2034年12月10日

R45ルートCA：有効期限 2045年3月18日

セイコータイムスタンプサービスは、長期間（10年以上）のタイムスタンプトークン検証を可能とするため、R6ルートCAから発行される証明書を使用したサービス（以下、R6サービス）は、2024年12月以前に停止する必要があります。このため、R6サービスを提供しつつ、R45ルートCAから発行されるTSA証明書を使用したサービス（以下、R45サービス）を開始します。

2．R45サービス

・サービス開始日は、2023年12月ごろを予定しています。
・R45証明書を使用したサービスの開始日はリポジトリで告知します。
・R45証明書を使用したサービスの内容は、時刻認証サービス運用規程1.2 DRAFT版をご覧ください。
・ポリシーはAccredited TypeA3およびAccredited TypeA3Lを予定しています。

3．デフォルトポリシーの変更について

R45サービスの開始半年後頃に、reqPolicyの指定なしで要求された場合に発行されるタイムスタンプトークンのポリシー（デフォルトポリシー）を変更します。

変更日当日に、reqPolicyの指定なしで要求された場合、発行されるタイムスタンプトークンのポリシーは、現行と変更後が混在します。混在を避けるためには、reqPolicyを指定して要求してください。

デフォルトポリシーの変更日はリポジトリで告知します。

	時刻認証局タイムスタンプポリシー	OID
現行	Accredited Type G	1.3.6.1.4.1.955.1.10.1.**3**.3
変更後	Accredited Type A3	1.3.6.1.4.1.955.1.10.1.**5**.3

4．R6サービスの廃止について

・R6ルートCAの有効期間が10年以下となる、2024年12月以前にR6サービスを廃止します。

・R6証明書を使用したサービスの廃止日はリポジトリで告知します。

5．お客様環境での対応について

R45サービスは2023年12月ごろ開始を予定していますのでお客様にて以下の対応と確認をお願いします。

① タイムスタンプの発行要求においてポリシー指定をしている場合は、以下のように変更をお願いします。

現行（R6サービス）		新規（R45サービス）	
ポリシー	OID	ポリシー	OID
Accredited TypeG Accredited TypeA2	1.3.6.1.4.1.955.1.10.1.3.3 1.3.6.1.4.1.955.1.10.1.5.1	Accredited TypeA3	1.3.6.1.4.1.955.1.10.1.5.3
Accredited TypeGL Accredited TypeA2L	1.3.6.1.4.1.955.1.10.1.3.5 1.3.6.1.4.1.955.1.10.1.5.2	Accredited TypeA3L	1.3.6.1.4.1.955.1.10.1.5.4

② 検証環境において、中間証明書もしくはルート証明書を証明書ストアに格納願います。

証明書情報

(1) GlobalSign Timestamping Root R45（ルートCA）

Subject DN	CN = GlobalSign Timestamping Root R45 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/timestamprootr45.crl
OCSP提供URI	http://ocsp.globalsign.com/timestamprootr45
証明書ダウンロードURI	http://secure.globalsign.com/cacert/timestamprootr45.crt

(2) GlobalSign R45 AATL TimeStamping Root CA 2021（中間CA）

Subject DN	CN = GlobalSign R45 AATL TimeStamping Root CA 2021 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/gsr45aatltimestampingrootca2021.crl
OCSP提供URI	http://ocsp.globalsign.com/ca/gsr45aatltimestampingrootca2021
証明書ダウンロードURI	http://secure.globalsign.com/cacert/gsr45aatltimestampingrootca2021.crt

CAの階層

ルートCA：GlobalSIgn Timestamping Root R45

⇒ 中間CA：Globalsign R45 AATL TimeStamping Root CA 2021

⇒ TSA証明書

6．その他

本内容は、総務大臣の変更申請認定前のものです。状況によって内容に変更の可能性があります。

以上