2021年5月10日

パートナー各位

デジサート・ジャパン合同会社

コードサイニング証明書における公開鍵長等の仕様変更について

平素は弊社製品の販売支援をいただき、誠にありがとうございます。

弊社では、CA/ブラウザが定めるコードサイニング証明書の発行に関する要求事項等の変更に伴い、2021年5月28日より、コードサイニング証明書、およびEVコードサイニング証明書に使用する公開鍵長を変更いたしますので通知申し上げます。詳細は下記をご参照ください。
なお、すでに発行された証明書、または適用日以前に発行される証明書は、その有効期限を迎えるまで問題なくご利用いただけます。

弊社では引き続きサービス向上に努めてまいりますので、今後ともご愛顧賜りますようお願い申し上げます。

記

1. 対象製品
・コードサイニング証明書
・EVコードサイニング証明書

2. 適用日
2021年5月28日（金）午前5:00 以降に発行される証明書

※同作業に伴うサービスの停止はございませんが、証明書が発行される時間帯により、従来の公開鍵長では発行できない場合がございます。また、時間は前後する場合がありますので何卒ご了承ください。

3. 変更内容および注意点
適用日以降にご申請いただくCSRの公開鍵長、およびこれを利用して新規/更新/再発行申請・発行される証明書の公開鍵長は、RSA3072bit以上となります。なお、当公開鍵長の変更は、エンドエンティティ証明書、中間CA証明書、ルート証明書に適用されます。

[ご注意ください]
- すでに発行された証明書、または適用日前に発行された証明書はその有効期限までご利用いただけます。証明書を再取得し、入れ替えていただく必要はございません。

- 従来仕様での証明書の発行をご希望の場合は、適用日前までに発行　(EVコードサイニング証明書の場合は、トークンへのインストレーション)を完了いただきますようお願いいたします。

- 適用日以降にCSRを提出してご申請いただく場合は、鍵長3072bit以上のRSA鍵で生成したCSRをご提出ください。

- EVコードサイニング証明書の場合、3072bit以上のRSA鍵をサポートする新しいトークン、またはHSMが必要となります。　適用日以降に発行される証明書には、既存のトークンは使用せず、弊社より送付する新仕様のトークンをご利用ください。　お客様で準備したHSMに証明書を格納して利用する場合は、鍵長の対応状況をあらかじめご確認いただきますようお願いいたします。

- 上記適用日以降に発行された対象製品の証明書には、新しい中間CA証明書が含まれております、必ずエンドエンティティに合わせて新しい中間CA証明書をご利用ください。

ご参考）【重要】コードサイニング証明書おける公開鍵長等の仕様変更について
https://knowledge.digicert.com/ja/jp/alerts/ALERT2757.html

4. 背景
コードサイニング証明書は、コードやプログラムに署名するために使用されますが、これら署名されたコードは長期間にわたり利用され、署名も長期間にわたって有効である必要があります。 より安全な運用のため米国NIST（米国標準技術研究所）の推奨事項や、マイクロソフト社のコード署名における鍵長RSA4096bitへの移行推奨をうけ、CA/ブラウザフォーラムではコードサイニング証明書のガイドラインに、2021年6月1日以降に発行するパブリックのコードサイニング証明書の鍵長をRSA3072bit以上とすることと改定されました。

ご参考）
Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, CA/Browser Forum (CAブラウザフォーラム) , May 3, 2021
https://cabforum.org/wp-content/uploads/Baseline-Requirements-for-the-Issuance-and-Management-of-Code-Signing.v2.3.pdf

5. 本件に関するお問合せ

テクニカルサポート
Email：authcode_info_jp@digicert.com
電話：03-4578-1368（自動音声ガイダンス3）
受付時間：土日祝日および年末年始を除く平日 9:30 - 17:30

認証に関するお問い合わせ
Email：auth_support_japan@digicert.com
電話：03-4578-1368（自動音声ガイダンス2）
受付時間：土日祝日および年末年始を除く平日 9:30 - 17:30

以上