

暗号便の電子署名検証用公開鍵情報の公開について
—暗号便以外でも電子署名の検証を可能に—

株式会社カオスウェア(代表取締役社長 梅野健)は、暗号便が電子署名で利用する 2048 ビットの公開鍵情報をホームページでの公開を開始しましたのでお知らせします。

この公開情報を利用することで、ユーザは暗号便サービスの提供状況や運用状況に問わず、過去に暗号便が提供する電子署名機能を利用し、暗号便名義で付与された電子署名の検証を行うことができるようになります。

背景:

暗号便では、これまでファイル暗号化転送サービス暗号便(<http://www.angobin.jp/>)で、安全なファイルの転送と併せて提供させていただいております電子署名技術(署名 Web)を広くご利用いただいております。

暗号便で作成される電子署名は、電子署名の正当性を確認する作業を Web 上で行うことができるため、電子署名で利用される鍵情報について特に意識をする必要がありませんでしたが、電子認証(電子署名の検証)の仕組みは暗号便の Web サービスに依存するものでした。

本電子署名用公開鍵情報の公開により、全てのユーザが、暗号便のサービス及び、暗号便運営企業=カオスウェアとは独立に電子署名の検証が可能となります。

電子署名用公開鍵閲覧ページについて:

暗号便電子署名用公開鍵閲覧ページは、誰もが暗号便が電子署名を行う際に利用する公開鍵を閲覧することができるページとなります。閲覧ページでは、以下の情報を閲覧・取得することができます。

- 電子署名アルゴリズム
- 電子署名用公開鍵情報
- RSA Modulus
- 公開鍵ビット長
- 公開鍵利用開始日時
- 公開鍵有効期限

暗号便で付与された電子署名情報を検証したい場合、検証者は電子署名用公開鍵閲覧ページで公開されている公開鍵の情報を利用することで、暗号便サービスとは独立して電子署名情報の正当性を確認することができるようになります。

暗号便 電子署名用公開鍵閲覧ページ

<https://www.angobin.jp/publickey/>

今後の展開:

本公開鍵情報を Twitter や、その他公開媒体を通して幅広く公開していき、より暗号便の認証基盤を強固・完全にいたします。

今後、暗号便アップローダー、CIPHERON、VSC-P2P にも本電子署名の技術を採用していき、暗号化のみならず電子認証サービスの提供、認証クラウドの構築を進めていきます。

連絡先:

株式会社カオスウェア

梅野 健

〒184-8795

東京都小金井市貫井北町 4-2-1

TEL: 042-359-6299

FAX: 042-359-6339

E-Mail: info@chaosware.com

URL: <http://www.chaosware.com/>

付属資料:



暗号化ファイル転送・ファイルストレージサービス

[今すぐファイル送信](#) · [Twitter](#) · [ログイン](#) · [新規ユーザ登録](#)

電子署名検証用公開鍵情報の開示

以下は暗号便で利用される暗号便サービスの電子署名検証用公開鍵情報です。
暗号便名義で行われた電子署名は、以下の電子署名用公開鍵情報を利用して暗号便サイト以外でも検証を行うことができます。

暗号便の電子署名検証用公開鍵情報

電子署名アルゴリズム
RSA
電子署名検証用公開鍵情報
-----BEGIN PUBLIC KEY----- MIIBjANBgkqhkiG9w0BAQEFAAOCAQIAMIIBcGkCAQEAxH7YBj68Ck7Ik+FHpC 85zU3HfP6Zereag2nQDuqGbnCYxrgtjRNvRtc1MUKy6Moe46oVCSN7jIYuF yEjRSzKzFZUBAVkHwo5M7EQChdxwWYATeFuaNBH4mHzPghS7PMZUPmJPeW HqhvCuueqBIDUJH9QLHn7p5dLjxxUMS9pWaeEeqgV19NNyFes+VW0ok6F fgdwS5haXohUqLW6VYTLAY/Hb+V6h13mzRlHfI3gr6ZaRk/nZx1QAYh YsvZgNu8ZdeJY8Q3VBlqgMaMjSW+mv1sXBppqSNWQTz9ON5NErVYsCWaFApA FwIDAQAB -----END PUBLIC KEY-----
RSA Modulus (n)
c47e080658fa03293b9652be147a5c: f39c04d8f1cf0665eae07aa0a7403: b90a066c0098c6b82daa544dbd4fd: 7353142b2e8ca1e7b6ea85424de2: 950b86c84a914b164a159209040664: 1f0c7933b10e3a1771c2b6804de7cf: ba83411f8a971e768fa14bb3cc899: b889893a07961e07adbc2b9a7a0d57: 943607fc9f602e186f469e5d2e5c71: c5433a46959a104a0955d7d7cd360: 15e7d28966b4a24e957c57675b9e61: 757a21714a8e5b0c5504f5018fc7bfe: 58baa1d77befb73462221b458a3de0: 9bc65a44afebc59c75400ca162cbed: 92036e0990de258f10d4506a80c68c: ba34885be9ef06c5fc669a92b6f590: 4f3f4e379344ad1595b0259a140a40: 17
公開鍵ビット数
2048bit
利用開始日時
2009/07/13 11:00:41
有効期限
2011/12/31 23:59:59

暗号便アップローダーのダウンロード
暗号便アップローダーは無料で以下のリンクからダウンロードすることができます。
ドラッグ&ドロップ操作で簡単に暗号便経由でファイルの送信が行えるようになります。

[暗号便アップローダーのダウンロードページ](#)

電子署名機能
暗号便電子署名機能(署名Web)は、暗号便からファイルを転送する際に暗号便が関連情報に対して署名を行い、正当な暗号便のユーザーからのファイルの送信であることをファイルの受信者に保障するサービスです。

[詳しくはこちら](#)

図 1: 暗号便の電子署名用公開鍵閲覧ページの概観