pgpとkeyid

Matsuzaki ‘maz’ Yoshinobu

<maz@iij.ad.jp>

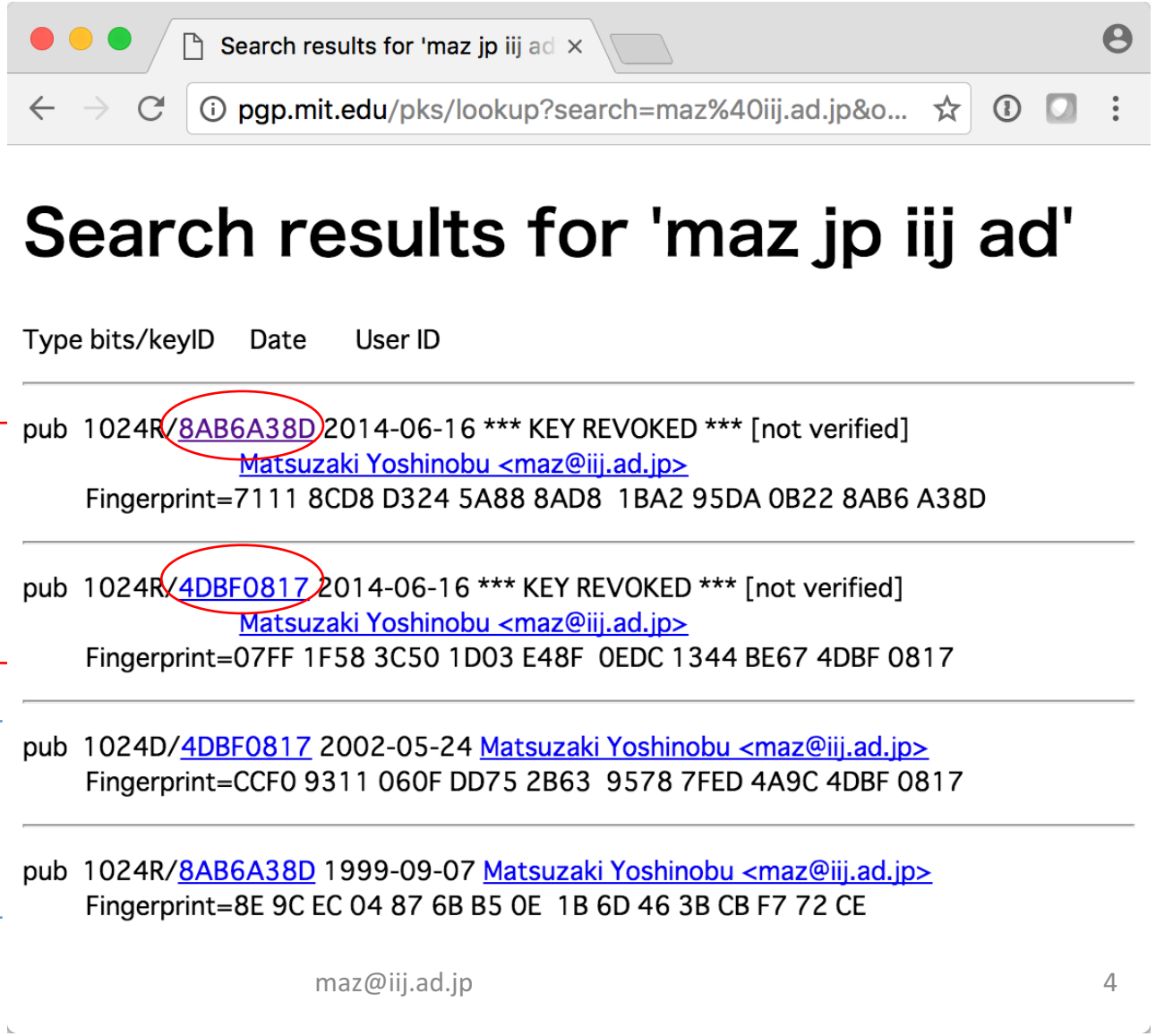
Pretty Good Privacy (pgp)

- 公開鍵暗号を利用したアプリケーション
  - データ暗号化、電子署名、認証などなど
  - TLSやDNSSEC等と異なり、鍵を検証するための基盤は提供されていない
    - 鍵と持ち主の対応関係は自分で確認する必要がある
- 自分の鍵ペアは自分で作る
  - 利便性のためにuidを複数設定できる
    - uid: 名前やメールアドレスの組み合わせ
  - 他の人に署名を付加してもらっても良い
    - 鍵の信頼性向上

keyserver

- pgp鍵を登録しておけるサーバ
  - 誰でも公開鍵を登録、取得できる
- 鍵の追加更新は可能だが、削除は不可能
  - 認証が全くないため
  - 秘密鍵の持ち主が鍵を失効(revoke)させることは可能
- keyseverから鍵を取り込む場合は、e-mailアドレスやkeyidを使って鍵を検索する
- pgp.mit.edu などが有名

同じkeyid/uidな僕の鍵が・・・



僕のじゃない

僕の

32bit keyid collision

- 昨今の計算資源を使えば、32bitのkeyidを狙って強衝突するpgp鍵を生成できる
  - 元の持ち主と同じuidを付ければ「偽鍵」の出来上がり
- 既に実証コードもあり、既存鍵に対する「偽鍵」のセットを生成した研究サイトがある
  - https://evil32.com/
- 誰かがこの「偽鍵」をkeyserverに登録しちゃった ☹
  - 研究サイトでは全ての「偽鍵」をrevoke
  - しかし、古い32bit keyidで鍵を扱うアプリケーションでは混乱する模様

IRRのauthってpgpだよね？

```
mntner:   MAINT-AS2497
descr:    People authorized to make changes for AS2497
          X-Keiro: noc@iij.ad.jp
admin-c:  Junichi Shimagami
tech-c:   Junichi Shimagami
upd-to:   noc@iij.ad.jp
mnt-nfy:  noc@iij.ad.jp
auth:     PGPKEY-8AB6A38D
auth:     PGPKEY-4A928EC5
auth:     PGPKEY-5D02FBCA
auth:     PGPKEY-6B8FF3B8
auth:     PGPKEY-5B5B746B
auth:     PGPKEY-08FDF462
auth:     PGPKEY-F0471B39
mnt-by:   MAINT-AS2497
changed:  noc@iij.ad.jp 20160531
source:   JPIRR
```

```
key-cert:  PGPKEY-8AB6A38D
method:    PGP
owner:     Matsuzaki Yoshinobu <maz@iij.ad.jp>
fingerpr:  8E 9C EC 04 87 6B B5 0E  1B 6D 46 3B CB F7 72 CE
certif:
 -----BEGIN PGP PUBLIC KEY BLOCK-----
 Version: PGP Key Server 0.9.5
+
 mQCNAzfU/toAAAEEAK22wkJ6+Nht4OkYw62AZPM3Kn0xGI8U0
:
 =ITRW
 -----END PGP PUBLIC KEY BLOCK-----
notify:    noc@iij.ad.jp
mnt-by:    MAINT-AS2497
changed:   noc@iij.ad.jp 20160531
source:    JPIRR
```

まとめ

- PGP鍵確認よろしく！
- 32bit keyidは捨て！
  - 今後は、せめてfingerprintの全桁チェック
  - keyserverを使って鍵を取得、更新する場合は要注意