

第14部

公開鍵証明書をを用いた利用者認証技術

木村 泰司

第1章 moCA WG 2023年の活動

moCA WGはCA (Certification Authority)の振る舞いや証明書の扱いに注目し、WIDEプロジェクトにおけるCAの運用実験を行っているWGである。moCA WGで運用されているCAのmoCAでは、WIDEメンバのためのWIDEメンバ証明書と、主にTLSのサーバのためのWIDEサーバ証明書が1年おきに一齐発行されている^{*1}。

moCA WGで運用されているWIDEルートCAは、2023年7月に有効期限の終了を迎えるため、新しい鍵と有効期限を持つ新たなWIDEルートCAの証明書を作成する"キーセレモニー"が、2023年5月のWIDE研究会に合わせて行われた。その後、新たなmoCAの鍵を使ったWIDEメンバ証明書の一齐発行も行われた。

第2章 2023年5月研究会で行われたキーセレモニー

WIDEルートCAのキーセレモニーは2023年5月20日、WIDE研究会moCA BoFの時間に、WIDE moCA WGメンバの立会いの下、下記の要領で行われた。

- オフライン状態で起動したUNIXサーバを用意する。(Raspberry Pi 3が使われた。)
- OpenSSLを利用してCA証明書を作成できる設定を行う。
- 公開鍵暗号として楕円曲線暗号(Elliptic Curve Cryptography)を用いて384ビットの鍵長で鍵生成を

行い、自己署名証明書を発行する。署名アルゴリズムには楕円曲線DSA (ECDSA)を用い、ハッシュアルゴリズムにはSHA-384を用いる。

- スクリーンに表示されたフィンガープリントの写真を撮るなどして記録を取り、これをWIDEルートCA証明書とする。
- WIDEルートCAの私有鍵は3つに分割して予め定めておいたオペレーター三名に分配し、生成に使われたUNIXサーバ環境からは安全に削除する。オペレーターはKorry Luke氏、尾上 淳氏、筆者(木村 泰司)の三名である。

続いて新たなWIDEルートCAを用いて、下記の要領でmoCAのCA証明書を再発行した。

- 公開鍵暗号として楕円曲線暗号(Elliptic Curve Cryptography)を用いて384ビットの鍵長で鍵生成を行い、証明書署名要求(CSR-Certificate Signing Request)を作成する。署名アルゴリズムには楕円曲線DSA (ECDSA)を用い、ハッシュアルゴリズムにはSHA-256を用いる。
- WIDEルートCAを用いてmoCAのCA証明書を発行する。
- 新たなmoCAのCA証明書は後日、WIDEメンバ証明書の発行などのためにサーバ環境に設定された。

各々のCA証明書の有効期限は下記の通りである。CA証明書の有効期限は、必ずしも利用を終了する日時を意味しておらず、これよりも前に更新する可能性はある。

*1 moCA WGで運用されているCAであるmoCAは、4種類のクライアント証明書を発行している。WIDEメンバに発行されるWIDEメンバ証明書、WIDEメンバの秘書さんに発行される秘書さん証明書、一時的にWIDE合宿等に参加するゲスト向けのテンポラリー証明書、WIDE合宿の事務局業務を行うためのWIDE事務局証明書である。サーバ証明書はWIDEサーバ証明書の1種類のみである。

- WIDE Root CA 04
有効期限: 2058年5月19日 10:00:52 JST
- members oriented CA 04
有効期限: 2033年7月1日 9:00:00 JST

第3章 moCAによる証明書発行の概況

2024年1月3日現在、WIDEメンバ総数は990名で、同数のWIDEメンバ証明書が発行されているほか、利用環境の変更等、メンバからの申告で再発行されたものが11あった。WIDEサーバ証明書は2のドメイン名に対して発行されている。2023年はWIDEサーバ証明書のオペレーターによる更新発行を行わなかった。2022年の同時期の集計によると、WIDEサーバ証明書が発行されているドメイン名は22であるが、2024年1月の段階でmoCAにサーバ証明書発行の要請は2件しかきていない。

第4章 WIDE Root CA 04フィンガープリント

WIDEプロジェクトにおける電子証明書のトラストアンカーを提供するために運用されている認証局の証明書「WIDE Root CA 04」のフィンガープリントを以下に示す。

SHA-256フィンガープリント

0E:DF:6A:78:2D:27:57:8B:0F:97:BC:EE:C9:19:5B:71:
CC:66:96:76:51:66:4A:29:FB:CF:5C:B1:7E:28:38:27

SHA-1フィンガープリント

99:0E:EE:06:0A:0B:B2:89:81:6E:6C:94:C1:6E:B9:10:
FA:11:8E:AC