SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

実用に向けた PKI-ID クロスドメイン認証鍵交換の評価
An Evaluation of PKI-ID Cross-domain Authenticated Key Exchange

飯島 悠介 * 向山 明夫 * 永井 彰 *
Yuhsuke Iijima Akio Mukaiyama Akra Nagai

キーワード ID ベース、PKI ベース、ペアリング暗号ライブラリ、認証、鍵交換

あらまし

認証技術として PKI をベースとした認証方法と ID をベースとした認証方法があり、近年、その両方の認証方法が利用される環境を想定して、PKI ベースと ID ベースとが混在した認証方法(PKI-ID クロスドメイン認証鍵交換)の研究が行われている[1] [2]。

PKI-ID クロスドメイン認証鍵交換を利用する例としては以下のものがある。IoT 機器とサーバの間で，秘密通信を行うことを想定する．サーバは，CA 局から発行された自身のクライアント証明書と対応する秘密鍵（署名鍵）を持っているとする．また，IoT 機器は，自身の ID と ID ベース暗号における秘密鍵を持っているとする．この時，サーバが自身のクライアント証明書を含むプロトコルメッセージを IoT 機器へ送り，IoT 機器は自身の ID とともに返信メッセージをサーバに送る．それぞれが受け取ったメッセージと自身の持つ秘密鍵を用いて，外部には秘密にしたままセッション鍵を生成して、秘密通信を行うことができる。

また、ID ベースの認証においては、IoT(Internet of Things)機器のような計算力が小さい、かつ、帯域幅が小さい機器で利用することを想定して、小計算力・狭帯域でも利用可能な方式が提案されており[3]、実際のサービスにも利用されている[4]。そのため、システムの計算力と帯域幅が小さい機器の認証には ID ベースで、計算力と帯域幅が大きい機器の認証には PKI ベースで行うように、認証を混在して利用することがあると考えられる。

しかし、現時点では、PKI-ID クロスドメイン認証鍵交換の研究はまだ数が少ないため、実用性については検討が進んでいない。

そこで、本稿では、PKI ベースと ID ベースとが混在する環境が増えることを想定し、実用に向けて、PKI-ID クロスドメイン認証鍵交換の処理に対して評価を行う。具体的には、評価の対象とする PKI－ID クロスドメイン認証鍵交換の方式について説明し、机上で PKI-ID クロスドメイン認証鍵交換の評価と考察を行う。

参考文献

[1] Ustao˘glu, B. Integrating identity-based and certificate-based authentited key exchange protocols. Int. J. Inf. Secur. 10, 201–212 (2011).
[2] Guo Y., Zhang Z. Authenticated Key Exchange with Entities from Different Settings and Varied Groups. In: Takagi T., Wang G., Qin Z., Jiang S., Yu Y. (eds) Provable Security. ProvSec 2012. (2012)
[3] Junichi Tomida, Atsushi Fujioka, Akira Nagai, and Koutarou Suzuki, Strongly Secure Identity-Based Key Exchange with Single Pairing Operation, ESORICS2019.
[4] 最先端の暗号技術と AI 技術を活用した高品質野菜の栽培実験を営農支援プラットフォーム「畑アシスト」にて開始. NTT 持株会社ニュースリリース. https://www.ntt.co.jp/news2020/2002/200212b.html#a2

* NTT 社会情報研究所, 東京都武蔵野市緑町 3-9-11, NTT Social Informatics Laboratories, 3-9-11 Midori-cho Musashino-shi Tokyo