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

# 分散台帳への秘密鍵の封入による協同運用可能な公開鍵証明書発行基盤の実装と評価

# Implementation and Evaluation of a Public Key Certificate Issuance Platform for Cooperative Operation by Enclosing Private Keys in a Distributed Ledger

熊谷 圭太 * 掛井 将平 * 白石 善明 † 齋藤 彰一 *
Keita Kumagai Shohei Kakei Yoshiaki Shiraishi Shoichi Saito

**キーワード** 公開鍵基盤，分散台帳技術，スマートコントラクト，Hyperledger Fabric，Intel SGX

## あらまし

認証局（Certificate Authority, CA）が信頼点となってユーザやデバイス，サービスなどの主体の真正性を保証し，認証された主体だけをシステムに接続させる仕組みとして公開鍵基盤が広く知られている．公的に信頼されたパブリック CA がインターネットにおいて利用される一方で，サービスのバックグラウンドのような限定的な範囲においては CA の機能を自由に拡張可能なプライベート CA の利用が適しているケースもある．Google は 2021 年 7 月にプライベート CA サービスである Google Cloud CA Service を開始し，ネットワークの規模が動的に変化する環境や IoT 環境などに適した証明書の発行をエンタープライズ向けに行っている [1]．また，Trusted Execution Environment（TEE）を用いてクラウド上で機密データを安全に利用するコンフィデンシャル・コンピューティング [2] が注目されており，秘密鍵の厳重な管理が必要な CA のようなオンプレミスでの運用が前提のシステムのクラウド利用が期待されている．

我々は先行研究 [3] において，コンソーシアムを構成する組織で公開鍵証明書発行基盤（以下，分散型公開鍵証明書発行基盤と呼ぶ）を協同運用するための要件整理とプロトコルの設計を行い，Intel SGX を利用した分散台帳技術である Hyperledger Fabric Private Chaincode（FPC）を用いて分散型公開鍵証明書発行基盤が構築可能であることを示した．本稿では，CA の基本的な機能である公開鍵証明書の発行・検証・失効の実現可能性を検討した先行研究をもとに，CA の秘密鍵の更新に対応できるように分散台帳のデータ構造を改良したうえで，提案基盤の実装と評価を示している．スマートコントラクトの実装には FPC で利用可能な C++を利用し，公開鍵証明書の作成・検証には OpenSSL のライブラリを用いた．そして，Hyperledger Fabric のテストネットワーク上に実装したスマートコントラクトをデプロイし，その性能評価を行っている．

## 参考文献

[1] Google. Announcing general availability of google cloud ca service. https://cloud.google.com/blog/products/identity-security/google-cloud-certificate-authority-service-is-now-ga.

[2] ITmedia. データ保護の欠けたピース「コンフィデンシャルコンピューティング」が普及する. https://atmarkit.itmedia.co.jp/ait/articles/2111/05/news121.html.

[3] 熊谷圭太, 掛井将平, 白石善明, 齋藤彰一. 分散型台帳への秘密鍵の封入による協同運用可能な公開鍵証明書発行基盤の検討. マルチメディア，分散協調とモバイルシンポジウム, pp. 165–172, 2021.

* 名古屋工業大学, 〒 466-8555 愛知県名古屋市昭和区御器所町, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Aichi, 466-8555, Japan
† 神戸大学, 〒 657-8501 兵庫県神戸市灘区六甲台町 1-1, Kobe University, Rokkodai-cho, Nada-ku, Kobe, Hyogo, 657-8501, Japan