＜参考情報（補足資料）＞

Recept とサイバートラスト、e シールを活用して Verifiable Credentials（デジタル証明書）の信頼性向上を実証

実証内容

本実証実験では、e シールの導入において、以下の三つの内容を中心に検証を行いました。

1. VC 発行者への e シール用証明書の発行

VC 発行者の秘密鍵に相対する e シール用証明書を発行し、両技術を連携して用いることが可能か、技術面を含め、検証を行いました。e シール用証明書は、今回実証では VC 発行者役となった Recept に対し、サイバートラストの iTrust 認証局から以下のプロセスで発行されました。

- VC 発行者である Recept において、VC 発行用の秘密鍵が HSM(Hardware Security Module)※1 で管理されていることを認証局として確認
- VC 発行者である Recept は、e シール用証明書発行を認証局に対して申請、iTrust 認証局は、Recept の登記簿を確認する等、申請者の実在性と真正性を自らの CP/CPS※2 に従って審査・確認
- 別途、Recept は、Recept の技術基盤上の HSM 内で、VC 発行用の秘密鍵を用いて証明書署名要求（CSR）を作成し、認証局に申請。iTrust 認証局において、CSR 内の VC 発行者情報等も確認の上、e シール用証明書を発行。Recept は、発行された証明書を Recept の技術基盤に取り込み

本実証実験では、具体的には、ECC_NIST_P256 で生成された秘密鍵に基づいて、サイバートラストが Recept に対し e シール用証明書を発行しています。上記により、VC と e シール用証明書に関わる技術を連携して用いることが可能であることが実際に確認されました。

2. VC 内に e シール用証明書を格納するためのベストプラクティスの調査・検証

VC 受取人が、受け取った VC の発行者の真正性を e シールの仕組みを用いて確認するには、VC 内に、e シールの検証で用いる e シール用証明書が含まれていること、または、受取人が同証明書にアクセス可能であることが必要となります。本実証実験では、VC 内に e シール用証明書を格納する方法について調査・検証を行いました。具体的には、Recept が現在採用している二つの VC フォーマットのそれぞれについて、以下のプロパティへの証明書情報格納を確認しました。

- JSON-LD：proof オブジェクトの x5c プロパティに e シール情報を格納
- SD-JWT： JWT ヘッダーの x5c プロパティに e シール情報を格納

上記において、いずれの格納方法でも適正に証明書情報を格納し、受取人に受け渡せることを確認しました。

3. e シールが付与された VC の発行

本実証実験として、最終的に Recept は、e シールが付与された 「proovy 公式パートナー証明書 VC」 の発行を行い、同 VC は、Recept が提供するユーザー用デジタルウォレットに格納されました。

また、VC の提示を受けた受取人は、従来同様に VC 自体の有効性や信頼性を確認するのみならず、その VC の発行者の真正性や実在性を e シールの仕組みによって検証できることが確認されました。e シールの検証では、e シール用証明書の失効確認を行うことで、VC 発

行者の秘密鍵の危殆化など、VC 発行者として有効ではない状態か等も検証可能であることも確認されました。

以上の本実証実験により、VC を活用するエコシステム全体のセキュリティと信頼性を向上させるスキームの検証ができたと考えます。

※1　HSM（Hardware Security Module）とは：Hardware Security Module という安全な機器で、秘密鍵を HSM に保管し不正に外部にコピーされない対策を行ったうえで、電子証明書を契約者本人以外が利用できないような厳格な認証を行い、クラウド上で電子署名することができる。

※2　CP/CPS とは：Certificate Policy（運用方針）/Certification Practices Statement（運用規程）。認証局の運用方式や信頼性・安全性を対外的に示す文書のこと。CP は認証局が電子証明書を発行する際の運用方針を定めた証明書ポリシーで、CPS は認証局の運用や鍵の生成・管理、責任など、実施手順を定めた認証局運用規程。

[関連情報] Recept とサイバートラスト、e シールを活用して Verifiable Credentials（デジタル証明書）の信頼性向上を実証（株式会社 Recept・サイバートラスト株式会社 2024 年 11 月 22 日発表プレスリリース）
https://www.cybertrust.co.jp/pressrelease/2024/1122-verifiable-credentials-eseal.html