セコムIS研究所
Intelligent Systems Laboratory

Internet Week 2023
「C8 PKIのこのごろ」
~~電子署名・PKI関連(仮)~~
電子署名の新たな出会い(仮)

2023年11月21日

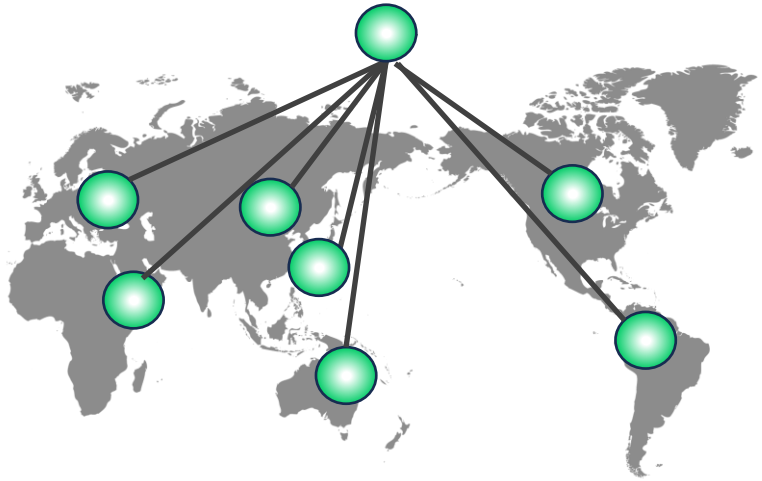
セコム株式会社　IS研究所
デジタルプラットフォームディビジョン
主幹研究員
佐藤　雅史

PKI(Public Key Infrastructure)

セコム IS 研究所
Intelligent Systems Laboratory

X.500 Directory Service

情報の共有・連携

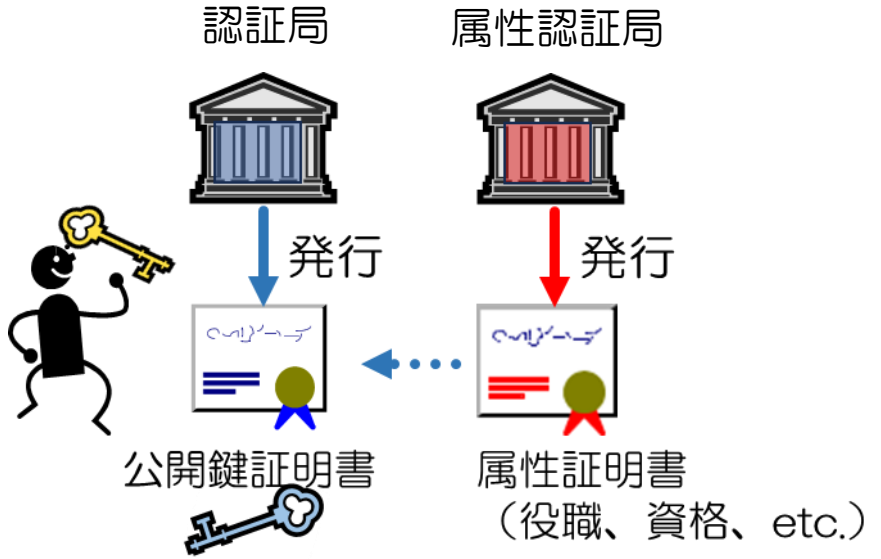


X.509 PKI・公開鍵証明書

エンティティの存在証明・識別子（識別名）・
検証鍵（公開鍵）

X.509 属性証明書

エンティティの属性の証明

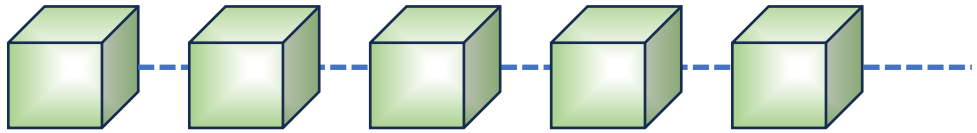


Digital Identity (Decentralized/Self-Sovereign)

セコム IS研究所
Intelligent Systems Laboratory

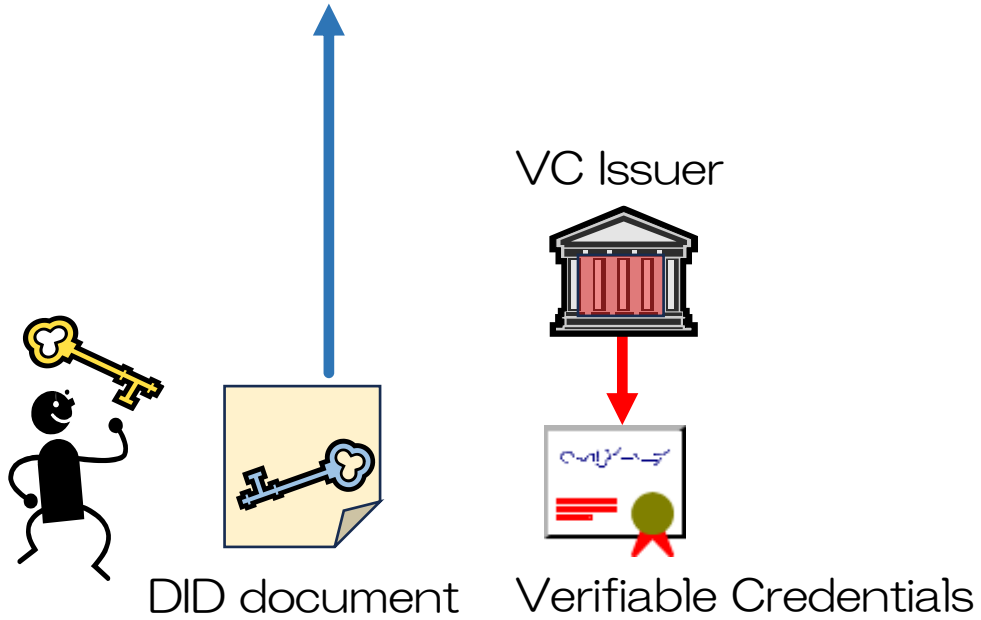
Distributed Ledger Technologies (DLT)

情報の共有・連携



Decentralized Identity (DID)

アイデンティティ・識別子・検証鍵（公開鍵）

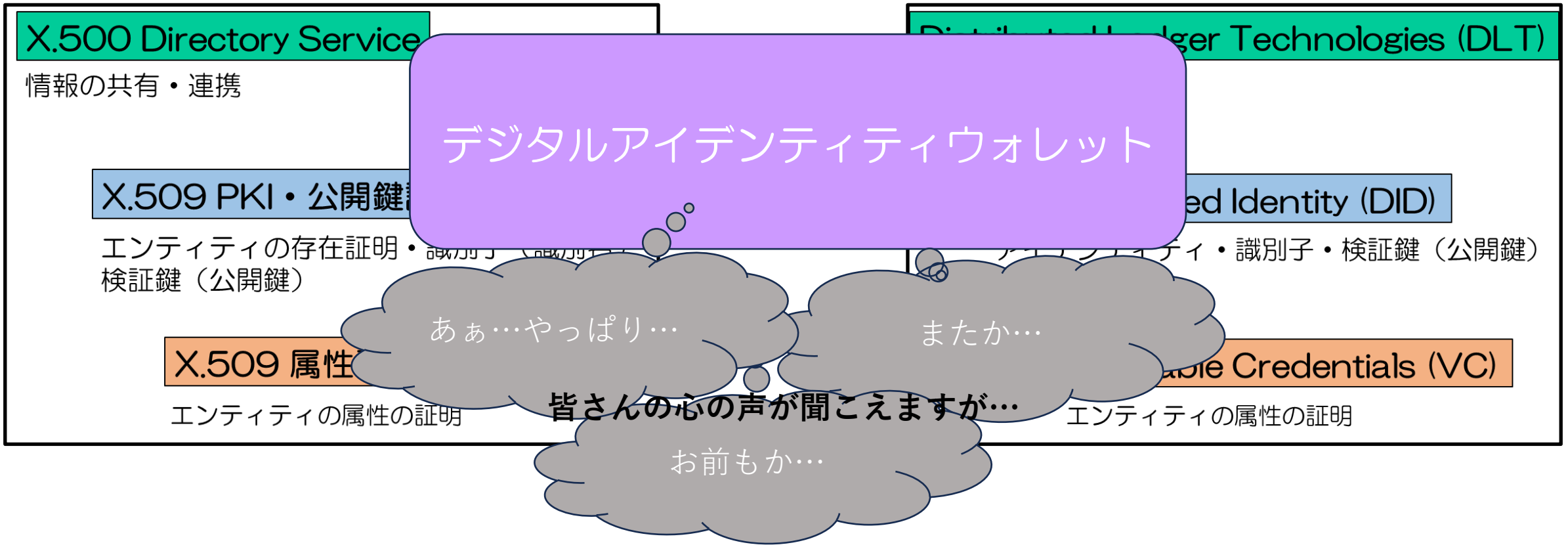


Verifiable Credentials (VC)

エンティティの属性の証明

両者の関係は？

トラストモデル、自己主権型・プライバシー保護強化などの考え方の違いはありますが…



電子署名（デジタル署名）生成方法の歩み

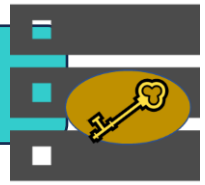
セコムIS研究所
Intelligent Systems Laboratory

ローカルアプリケーション
（ICカード等）

Webアプリ
（ICカード、ローミング鍵）

モバイル（SIM、NFC）

リモート署名サービス



電子署名の課題であった
・アプリケーションの普及
・UXの改善
につながるかも？

スマートデバイス（ウォレット）

Future?

リモートウォレット
（リモート署名サービス）

「*電子署名のために実行する*」から
「*何かをする先に電子署名もある*」へ

電子署名の新たな出会い(仮)