報道発表資料

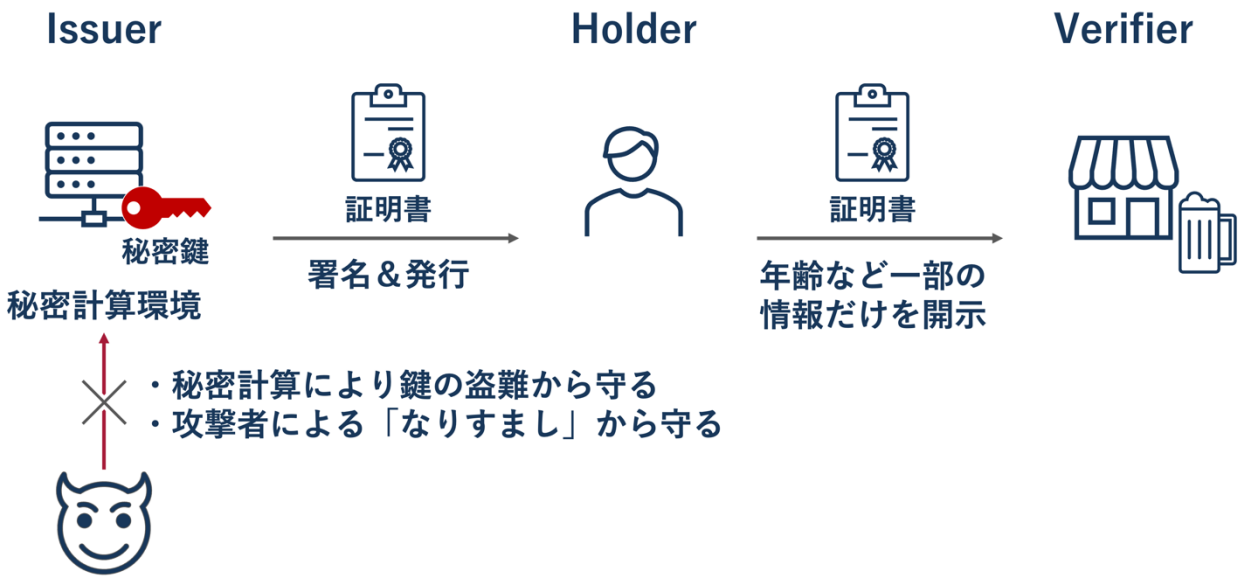
2024 年 5 月 22 日
TOPPAN デジタル株式会社
株式会社 Acompany

TOPPAN デジタルと Acompany、秘密計算を用いて プライバシー配慮と情報漏洩リスク極小化を両立する技術を開発

本人確認などの場面において、必要な情報だけを選択して開示できるプライバシー配慮と秘密鍵を分散管理して情報漏洩リスクの極小化を両立

TOPPAN ホールディングスのグループ会社である TOPPAN デジタル株式会社（本社：東京都文京区、代表取締役社長：坂井 和則、以下 TOPPAN デジタル）と、株式会社 Acompany（読み：アカンパニー、本社：愛知県名古屋市西区、代表取締役 CEO：高橋 亮祐、以下 Acompany）は、デジタル証明書（Verifiable Credential、VC）と秘密計算(※1)を用いて、自分の ID/個人情報を自分自身でコントロールできる分散型アイデンティティと、情報漏洩リスクの極小化を両立させる技術を開発しました。

本技術によりユーザーは、会員登録や本人確認などの場面において、必要な情報だけを選択的に開示することが可能になります。同時に、秘密計算を用いて真正性を保証する秘密鍵を分散管理するため、情報漏洩のリスクを極小化することが可能になります。



■ 背景

昨今、特定の企業に依存せず、サービス利用者が自身の意思で ID を管理できるようにする分散型アイデンティティの取り組みが加速しています。一般的には、メールアドレス/ユーザー名といった ID を企業が発行し、その ID に紐づく個人情報やパスワードなどを企業が管理しています。このような中央集権型の ID 管理では、個人情報の開示範囲は ID プロバイダーである企業に依存してしまうほか、一企業に依存するため情報漏洩のリスクがあります。このような中で、内閣官房デジタル市場競争本部において「特定のサービスに過度に依存せずに、Trust を向上する仕組み」として「Trusted Web」の構想が提唱されており、2030 年度にはインターネット全体で利用されることが予想されています。

他方で、分散型アイデンティティにおいて、情報の真正性を検証できるデジタル証明書は企業や自治体などの発行者が、秘密鍵でデジタル署名を行うことで真正性を保証しますが、秘密鍵が漏洩すると発行者の「なりすまし」などの事象が発生し真正性が保証できなくなってしまいます。この対策として、秘密鍵へのアクセスを厳格に制限するなどの対処方法がありますが、漏洩リスクを減らす一方で、使用時の不便さを増やしてしまいます。

このような中で TOPPAN デジタルと Acompany は、分散型アイデンティティを実現しつつ、秘密計算を用いることで、秘密鍵を複数に分割した状態でデジタル署名を生成し安全性を高める技術を開発しました。

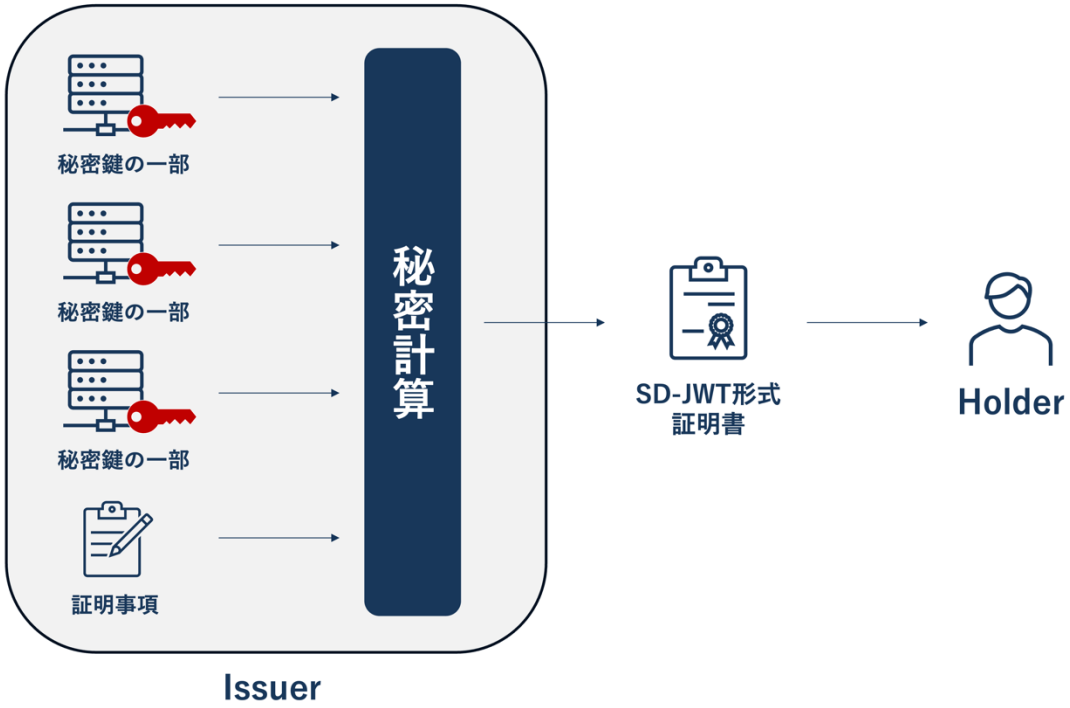
■ 開発した技術の概要

① ユーザーが自身のプライバシー情報をコントロール

ユーザーが、自分自身が保有するデジタル証明書に記載された情報をコントロールし、必要な情報のみを選択的に開示できるようにする手法として「SD-JWT(※2)」のフォーマット形式や、「BBS 署名(※3)」などが代表例として挙げられます。今回は「SD-JWT」と「BBS 署名」の 2 つの手法を実装。デジタル証明書を用いることで、必要な情報だけを選択的に開示しつつ、改ざんがされていないデジタル証明書として活用することが可能になります。

② デジタル証明書の発行者の秘密鍵を秘密計算を用いて安全に管理

プライバシー強化技術の1つである秘密計算を用いることで、秘密鍵を複数に分割したままデジタル署名を生成し安全性を高めます。秘密鍵が生成された後で複数に分割する場合は、生成された秘密鍵が盗難されるリスクが存在しますが、秘密分散法(※4)により分割した状態の秘密鍵が生成されるため一度も完全な秘密鍵が存在することなく安全な運用が可能になります。



■ 今後の目標

今回開発した技術を「Trusted Web」に取り組む企業を対象として 2025 年を目途に試験提供開始を目指します。今後は他の選択的情報開示手法の実装も視野にシステムの拡張を進め、個人がデータコントロール権を持ちつつ、企業側もプライバシーに配慮してデータ利活用が行える社会実現に向け、本技術の社会実装を進めます。

※1 秘密計算

秘密計算とは、計算対象のデータを秘匿化したまま計算を実行することができる技術の総称です。

※2 SD-JWT

SD-JWT は、JSON 形式の署名対象データに対して従来の署名形式 JWT(JSON Web Token)を応用して選択的開示可能な VC を生成する新たな仕様です。

※3 BBS 署名

BBS 署名は、JSON-LD 形式の署名対象データに対して選択的開示可能な JSON-LD 形式の VC を生成する楕円曲線を用いたデジタル署名技術とゼロ知識証明に基づいた新たな署名方式です。

※4 秘密分散法

秘密分散法とは、データをある特定の条件を満たさないと復元することができない秘匿化された複数のデータへ分割する手法の総称です。

＊ 本ニュースリリースに記載された商品・サービス名は各社の商標または登録商標です。

＊ 本ニュースリリースに記載された内容は発表日現在のものです。その後予告なしに変更されることがあります。

以　上