金融APIに関する認証・認可についての調査研究

A Survey of Authentication and Authorization about Financial API

木村 和紀・ネットワーク分科会・情報セキュリティ大学院大学

Recently, financial API is becoming to be noted because of the growth of FinTech enterprises. Technologies related to financial API include authentication and authorization. I focused on authentication especially FIDO that improve both convenience and security. And I explain the proposed method that improve of FIDO authentication.

金融APIとFinTech

FinTech企業は，金融機関の保有するデータに付加価値をつけて利用者にサービスを提供．一方，FinTech企業の金融機関に対するアクセス方法が未整備の状況

＜ウェブスクレイピングの問題＞

- 利用者のID･PWをFinTech企業に登録
- FinTech企業が利用者になり代わりインターネットバンキングにアクセス
- htmlの情報を読み取り，情報を加工

しかし･･･

- 金融機関とFinTech企業との契約関係なし
- 万一の際の利用者への補償等の基準が未策定

＜金融APIの整備＞

政府の「未来投資戦略2017」

2020年6月までに80行以上の銀行のAPI導入を目指す

そのほかにも以下のような組織で金融APIの整備を検討

母体	WG等
金融庁	①金融制度WG
全国銀行協会	②オープンAPIのあり方に関する検討会
FISC	③金融機関におけるFinTechに関する有識者検討会
	④API接続チェックリストWG

金融APIと「認可」技術

APIで用いられる認可プロトコル･･･OAuth 2.0(②で推奨)

･FinTech企業に金融機関のID,PWを登録せずアクセス権限を付与

･権限の範囲を明確にしたうえでアクセスの認可を与えられる

「認可」については指針が定まったが，「認証」について課題が残る

「認証」技術

インターネットバンキングでは二要素認証が広く用いられる

利便性の悪さから利用率が上がらず

例)「記憶認証」+「所持認証」

記憶認証(パスワード)	多数覚えるのが困難
所持認証(ハードウェアトークン等)	紛失･盗難のリスク，サービスの数だけ必要

＜FIDO認証＞　FIDO : Fast IDentity Online

利便性とセキュリティの両立を目指す，公開鍵暗号方式を活用した認証方式．

FIDOを推進する非営利団体には，250以上の企業･団体が参加

◎日本の主要参加企業

NTTドコモ，富士通，ヤフージャパン，LINE，三菱東京UFJ銀行等

＜U2Fプロトコル＞

記憶認証＋所持認証の二要素認証だが以下の点が異なる

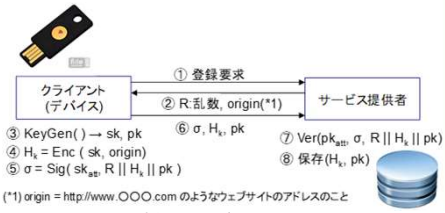
･パスワードが通信経路上を流れない

･FIDOに対応するサービスであればデバイスは1つでよい

＜Security Keys＞

U2Fプロトコルの実装

Googleの二要素認証で使用されている



※ 暗号化された秘密鍵を含むデータをキーハンドル(H_k)とよぶ

デバイス内部に3つの秘密鍵が格納されており，暗号化やデジタル署名に使用

利用するサービスが増加しても管理する鍵は増加しない

＜特徴＞

･サービス毎デバイスで鍵ペアを生成

･公開鍵とともに，秘密鍵を暗号化(*)してサービス提供者へ送信

サービス提供者が暗号化された秘密鍵と公開鍵を管理

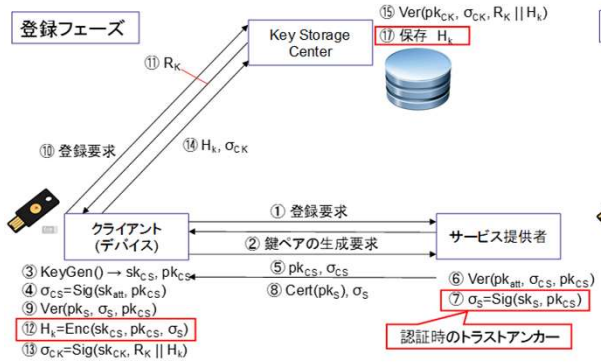
提案方式

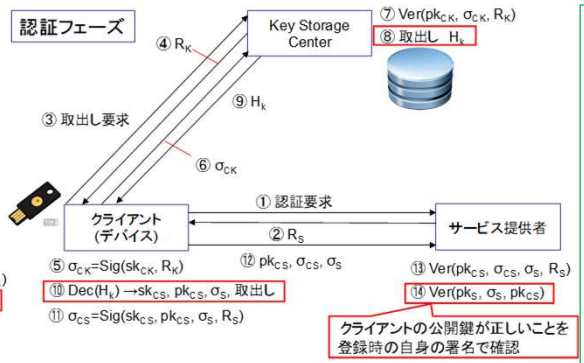
"Security Keys"の方式を改良

「クライアント」「サービス提供者」双方の鍵管理負担の軽減を目指す

･生成した鍵を保管する第三者機関"Key Storage Center"の設置

･サービス提供者の鍵管理負担を軽減した，デジタル署名を活用した認証方式(クライアントの負担は"Security Keys"と同等)





※ 登録フェーズの前段階で，クライアントとKSCとの間で鍵共有 (sk_{ck}, pk_{ck}) を行う必要あり

･登録時，クライアントの公開鍵にサービス提供者の持つ秘密鍵でデジタル署名

･秘密鍵，公開鍵，署名を暗号化してKSCで保管

･認証時，キーハンドルを復号し，秘密鍵，公開鍵，署名を取出し

･クライアントの署名を検証する公開鍵が正しいことを，登録時の自身の署名を使って証明