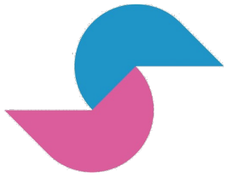
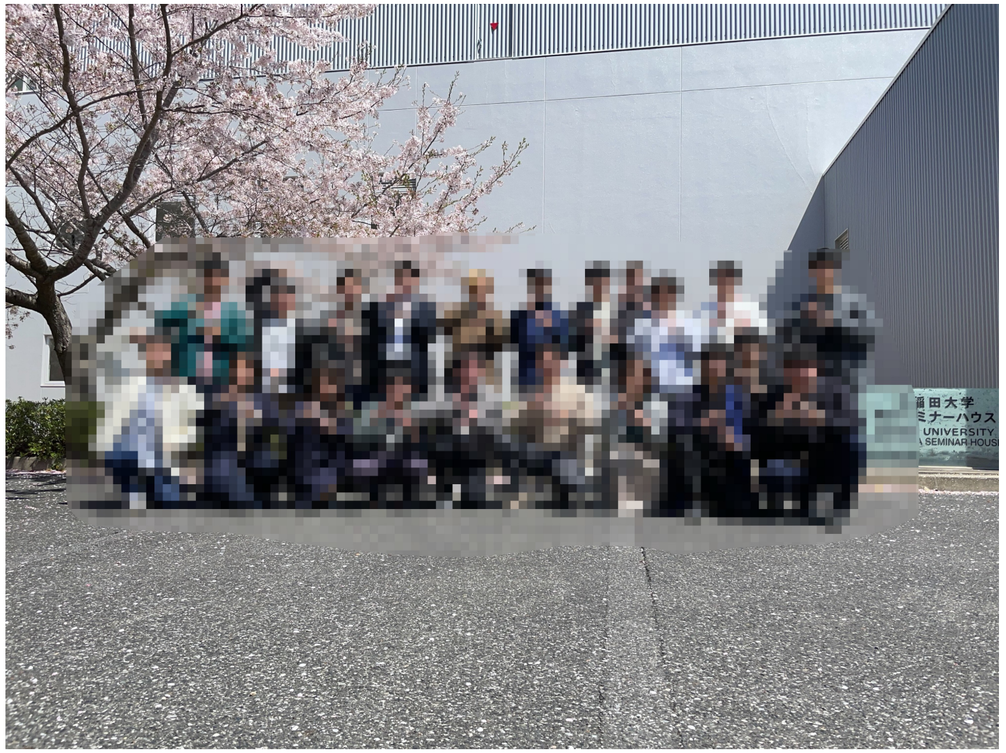


認証器に紐づいた検証可能なデジタル証明書

渡邉 健
川原 悠佑
水野 重弦
福田 岐弦

SKKN = SaKoKeN

早稲田大学の佐古研究室です！



プライバシーに配慮してモザイクを適用しております。

作ったプロダクト

認証器に紐づいたVerifiable Credentialsの発行と提示！

疑問

Verifiable Credentials(VC)って何だっけ…？

背景知識

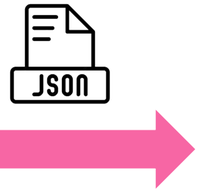
VCとは、あなたの氏名、所属、住所などの情報を証明する、デジタル証明書です(ニュアンス😌)

VC

Issuer

パスキー太郎氏の所属するZoozle社

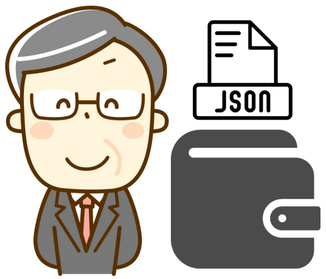
Zoozle



VC発行

Holder

VCを受け取ったパスキー太郎氏ウォレットに保管

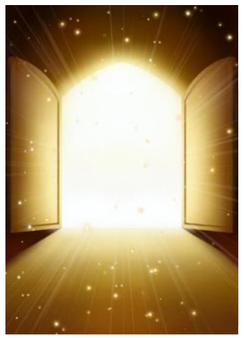


会社の発行した部長の社員証VCだ！

VP提示

Verifier

機密データの入った扉。部長以外開けられない。



背景知識

Issuer

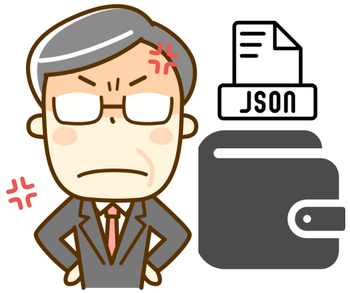
パスキー太郎氏の所属する
NVIDIA社

Zoozle

VC発行

Holder

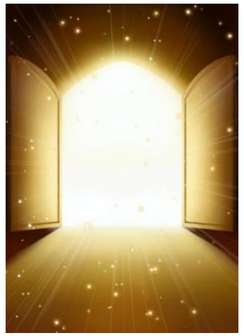
VCを受け取ったパスキー太郎氏
ウォレットに保管



VP提示

Verifier

機密データの入った扉。部長以外開けられない。



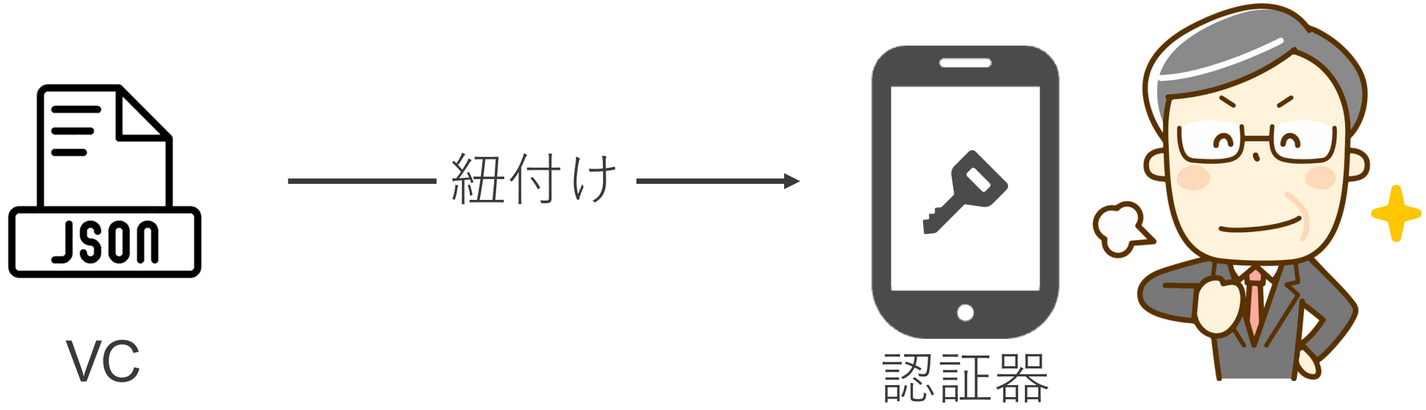
部長が脆弱なウォレットを
使ってるらしい！

ハッキングが得意な新入社員Aさん

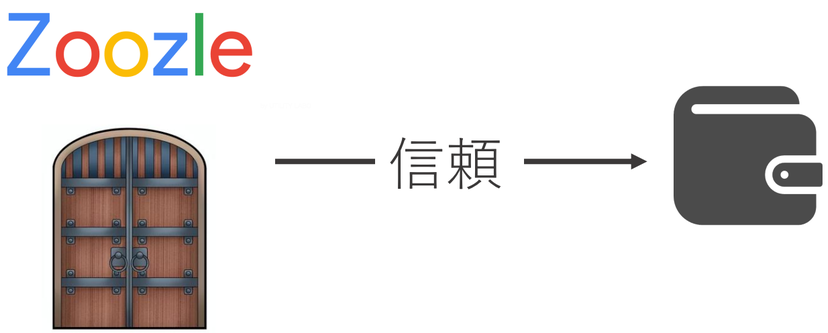
VP提示

やりたいこと

FIDO keyを持ってる人(部長)だけがVCを提示できるようにしたい！

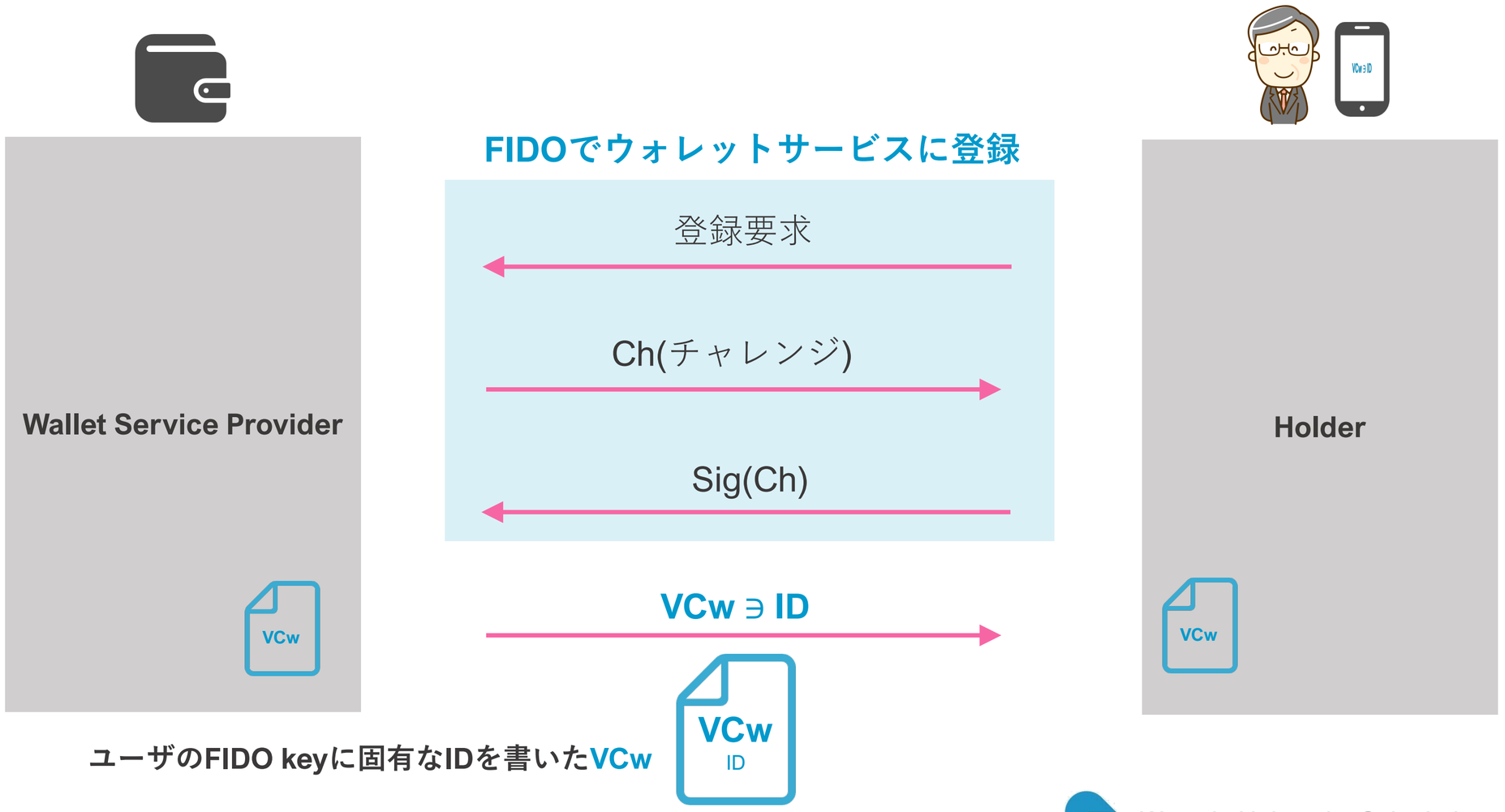


信頼できるウォレットサービスだけでVCを扱えるようにしたい！



プロトコル

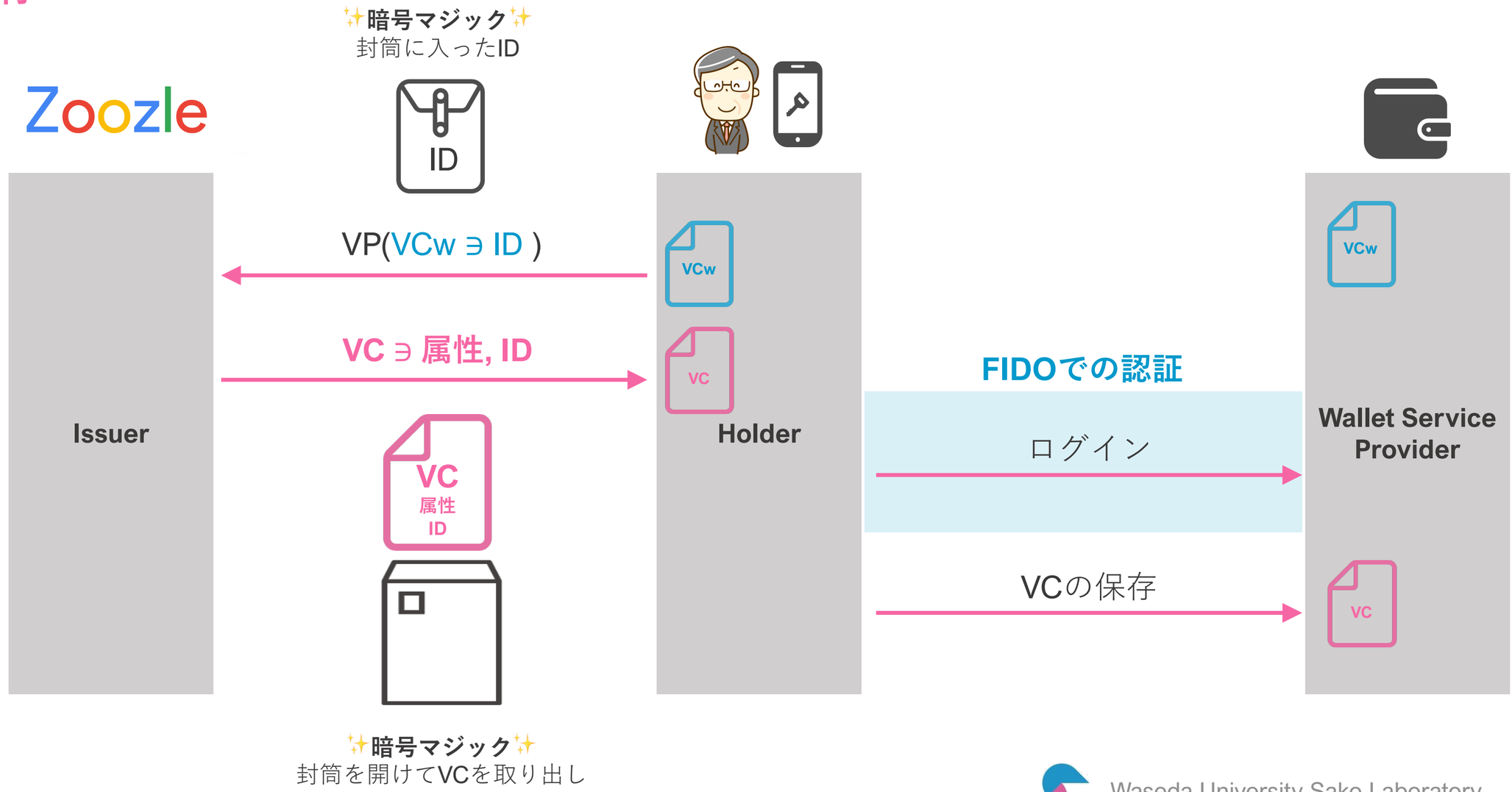
ウォレットサービスへの登録



ユーザのFIDO keyに固有なIDを書いたVCw

プロトコル

VCの発行


✨暗号マジック✨
封筒に入ったID
Zoozle
ID
VP(VCw ∋ ID)
VCw
VC ∋ 属性, ID
VC
FIDOでの認証
Issuer
Holder
Wallet Service Provider
ログイン
VCの保存
VCw
VC
VC
属性
ID
✨暗号マジック✨
封筒を開けてVCを取り出し

プロトコル

VCの提示

VCwを持っている
(=FIDOで認証された)
WalletからのVCだ！

VCの取り出し

VP(VCw ∋ ID)

VCwに書かれたID=VCに書かれたID
のゼロ知識証明

VP(VC ∋ 属性, ID)

VCwとVCの両方を知らないと
ドアを開けられない

VCwとVCの2段階認証

Verifier

Holder

VCw

VC

VCw

VC

Wallet Service Provider

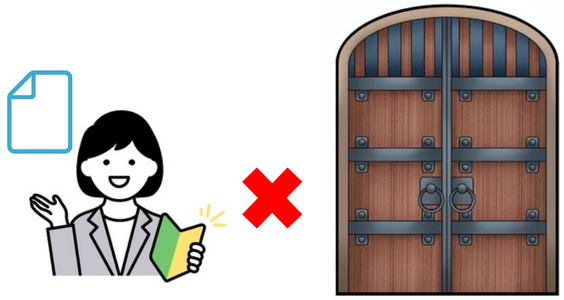
プロトコル

バックアップ(端末の移行)

嬉しいポイント

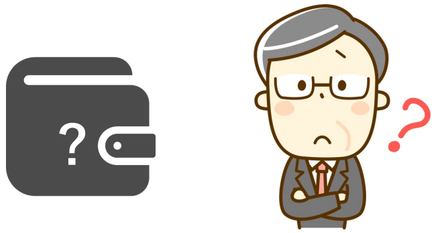
1. VCとFIDO keyを紐付けて発行、提示ができる

ハッキングの上手い新入社員がVCを知ってしまっても、
VCwを知らなければドアを開けられない！
=VCと認証器のバインディングができる



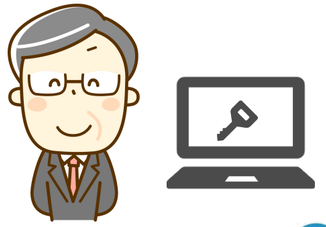
2. Issuer、 Verifierが信頼したウォレットサービスだけ利用可能

部長が怪しいウォレットサービスを使っている場合、
会社はVC発行、ドアやVP提示を拒否できる
=ウォレットサービスのトラスト形成



3. FIDOを使ってVC, ウォレットのアカウントのバックアップが可能

部長がスマホ(認証器)を壊されても、パスキーを同期した別のデバイスでリカバリーできる



それでは

デモへ