从 YutriKey 到 CanoKey

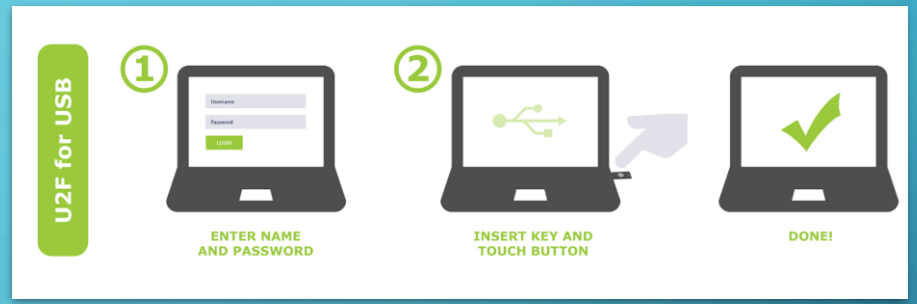
党凡

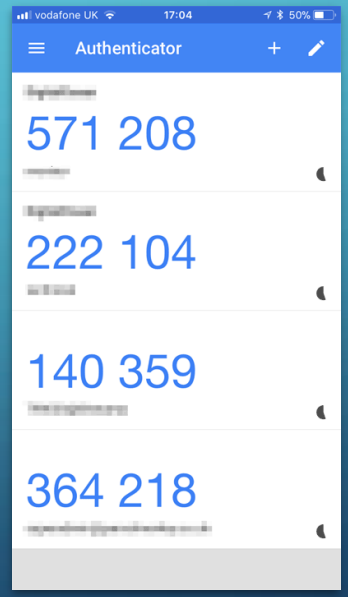
为什么要用KEY?

- 二步认证
  - 短信验证码
  - TOTP：基于时间的一次性密码
  - U2F / WebAuthn：通用二步认证协议
- 个人身份验证：PIV
  - 免密码登录系统
  - SSH访问服务器
- 通信内容加密和签名：OpenPGP
  - 发送带有签名、内容加密的电子邮件
  - SSH访问服务器

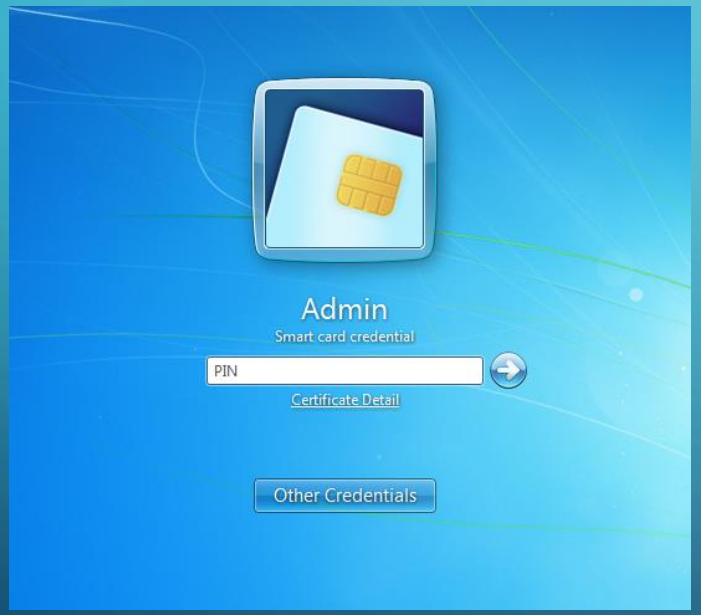
二步认证

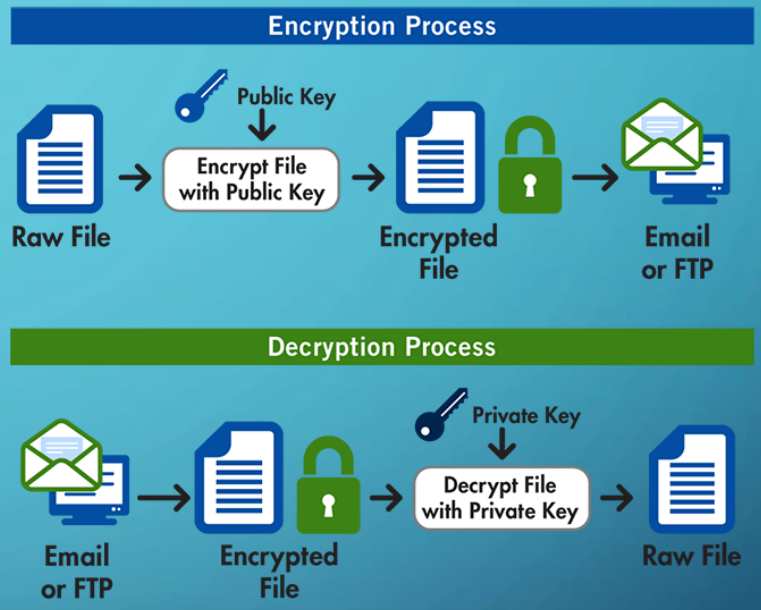

您的第二步验证方式
当您输入密码后，系统会要求您执行第二个验证步骤。了解详情
安全密钥 （默认）
yk4（添加时间：2017年7月30日）
上次使用时间：1月19日下午11:26
Chromebook（地点：香港）
添加安全密钥
“身份验证器”应用
已在 Android 设备上配置身份验证器
添加时间：1月4日下午6:58
更换手机
语音消息或短信
130 **** 8394 已验证
通过短信发送验证码。
添加手机号码

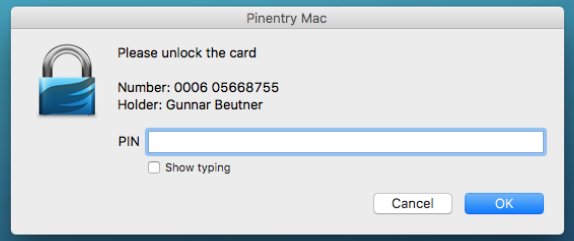

U2F for USB
1
ENTER NAME AND PASSWORD
2
INSERT KEY AND TOUCH BUTTON
DONE!


vodafone UK
17:04
50%
Authenticator
571 208
222 104
140 359
364 218

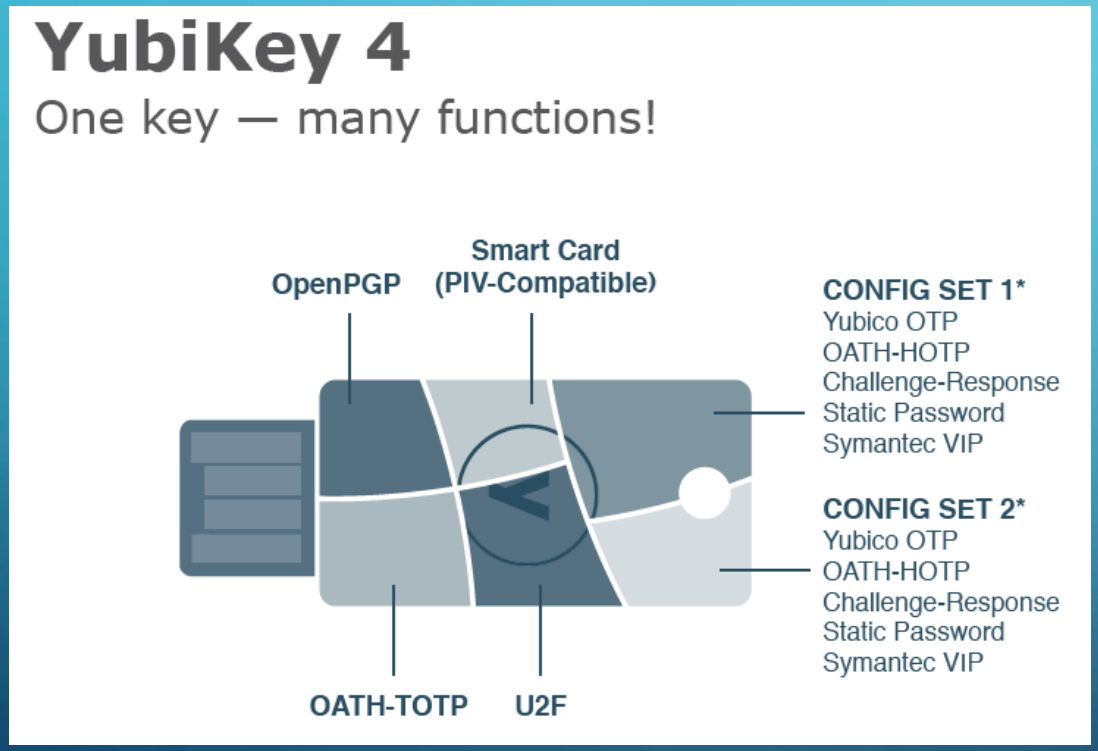
PIV & OPENPGP


Admin
Smart card credential
PIN
Certificate Detail
Other Credentials


Encryption Process
Public Key
Encrypt File with Public Key
Raw File
Encrypted File
Email or FTP
Decryption Process
Private Key
Decrypt File with Private Key
Email or FTP
Encrypted File
Raw File


Pinentry Mac
Please unlock the card
Number: 0006 05668755
Holder: Gunnar Beutner
PIN
Show typing
Cancel
OK

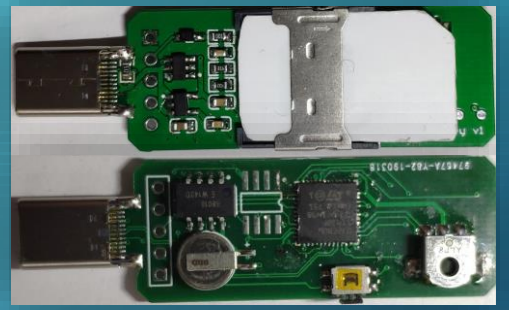
现有产品


YubiKey 4
One key — many functions!
OpenPGP
Smart Card
(PIV-Compatible)
OATH-TOTP
U2F
CONFIG SET 1*
Yubico OTP
OATH-HOTP
Challenge-Response
Static Password
Symantec VIP
CONFIG SET 2*
Yubico OTP
OATH-HOTP
Challenge-Response
Static Password
Symantec VIP


WIRED

YutriKey —— Powered by 宇翔

- 技术方案：STM32 MCU + Javacard
  - STM32 (~10 RMB)：USB接口和用户交互
  - JavaCard (<10 RMB)：密码学算法
- 硬件：已完成原型
- 软件
  - MCU：自己开发
  - TOTP：github.com/JavaCardOS/Oath-Applet
  - U2F：github.com/LedgerHQ/ledger-u2f-javacard
  - OpenPGP：github.com/JavaCardOS/OpenPGPApplet
  - PIV：github.com/arekinath/PivApplet

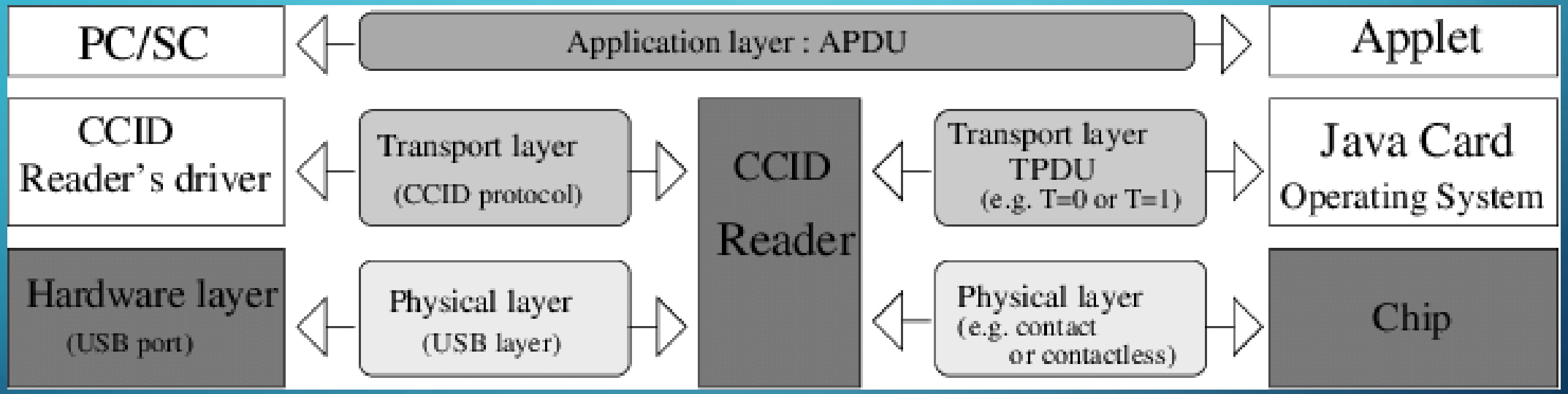


WHAT ABOUT NEXT?

CANOKEY

- FIDO2 / WebAuthn
  - 64 resident keys and unlimited normal keys
  - HMAC extension
- OpenPGP
  - OpenPGP Smart Card 3.4 Compatible
  - RSA 2048 / 4096
  - NIST P-256 / P-384
  - secp256k1
  - ED25519 / X25519
- PIV
  - NIST SP 800-73-4 Compatible
  - RSA 2048
  - NIST P-256 / P-384

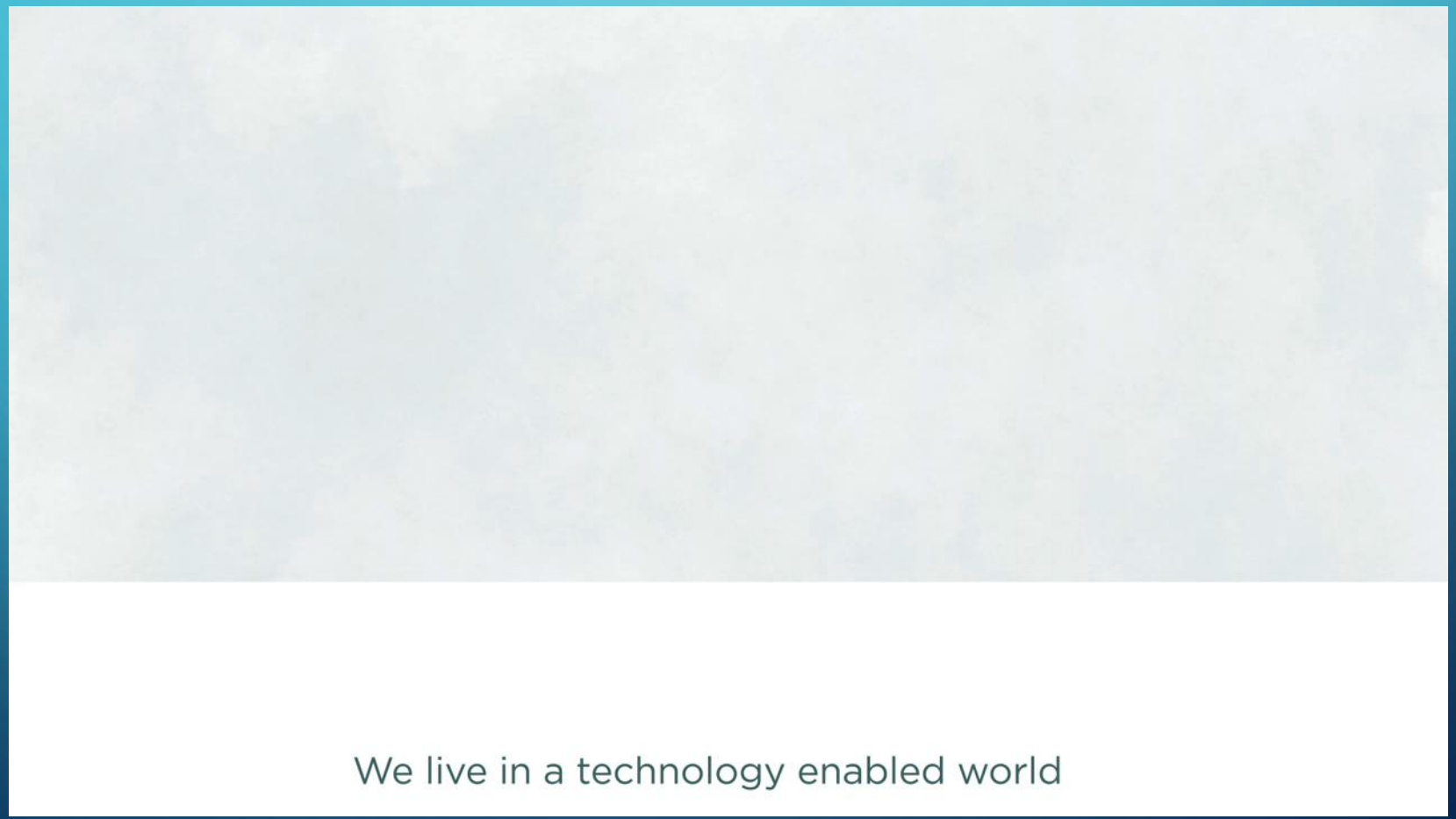
协议们


PC/SC
Application layer : APDU
Applet
CCID
Reader's driver
Transport layer
(CCID protocol)
CCID
Reader
Transport layer
TPDU
(e.g. T=0 or T=1)
Java Card
Operating System
Hardware layer
(USB port)
Physical layer
(USB layer)
Physical layer
(e.g. contact
or contactless)
Chip

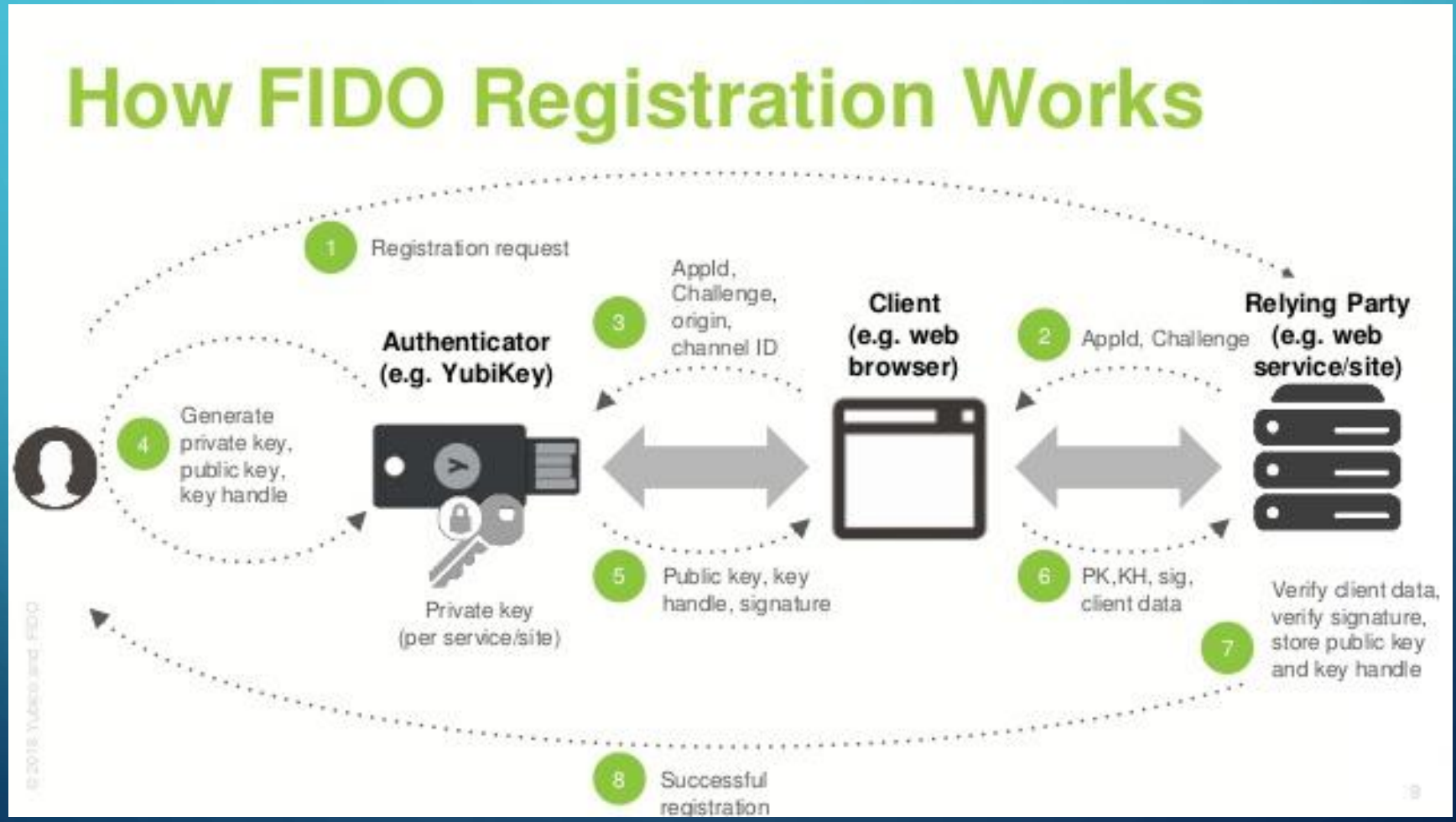
吐槽时间

- CCID 白名单
- CCID 占用问题
- HID 安全性

FIDO & WebAuthn

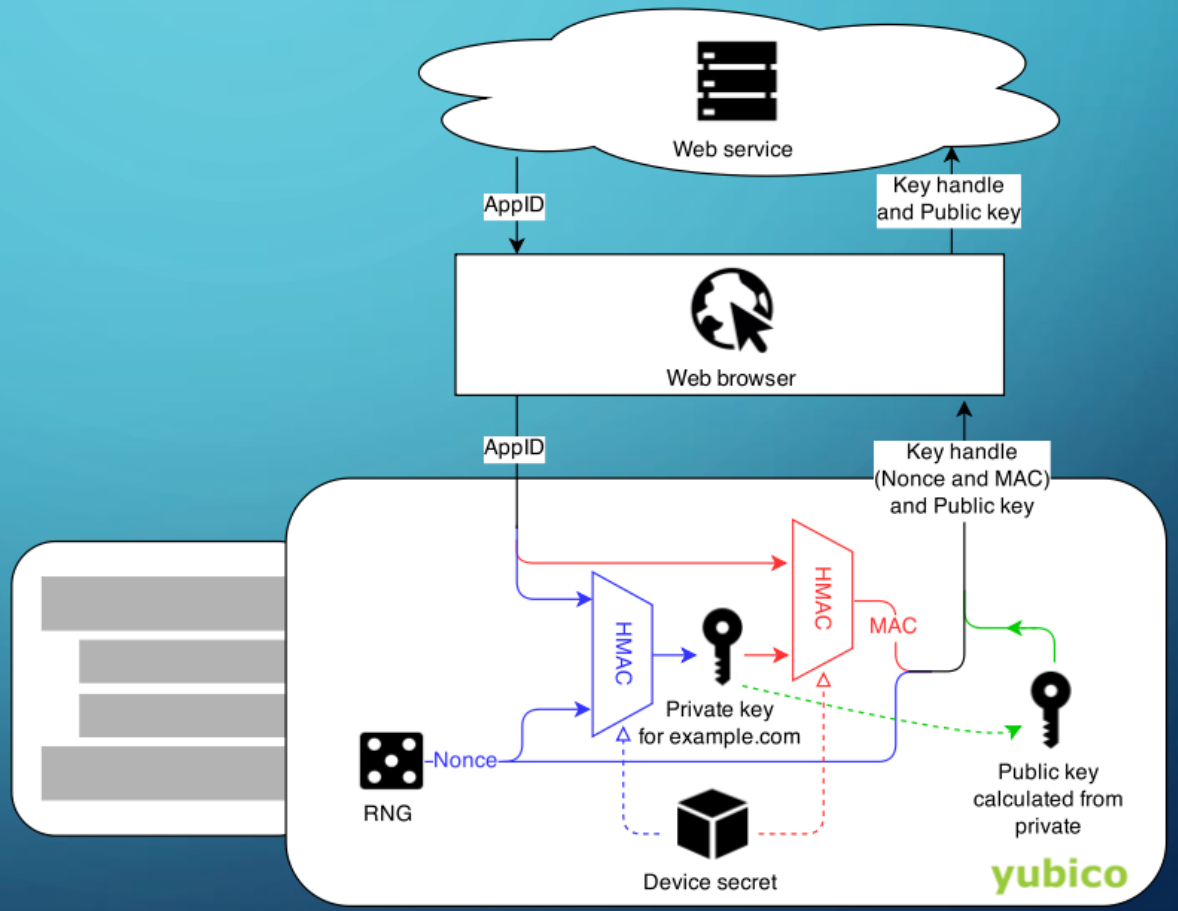


FIDO的工作原理


How FIDO Registration Works
1
Registration request
AppId, Challenge, origin, channel ID
3
Authenticator (e.g. YubiKey)
Client (e.g. web browser)
2
AppId, Challenge
Relying Party (e.g. web service/site)
4
Generate private key, public key, key handle
Private key (per service/site)
5
Public key, key handle, signature
6
PK,KH, sig, client data
Verify client data, verify signature, store public key and key handle
7
8
Successful registration

如何支持114514组密钥

- Key Wrapping



OPENPGP

- OpenPGP是PGP的一种实现
- Spec只良好定义了RSA、ECDSA，~~其他靠猜~~
- gpg：我有很多槽点
- 一点小插曲：独立的interface
- OpenKeychain & 25519

PIV

- 美国国家标准 SP 800-73-4
- 只支持RSA 2048和ECC P-256/P-384

开源版 VS 闭源版

- 共享核心代码（OpenPGP、PIV、FIDO等）
- 密码学运算加速
- 安全存储

谢谢
Q&A