YubiKey

YubiKey 是 Yubico, Inc. 发行的，具有 OTP、TOTP、FIDO 2FA、静态密码、Challenge-Response、PIV、OpenPGP Card 等功能的便携密码学硬件。本文主要描述其智能卡相关功能，即 PIV 与 OpenPGP Card。

YubiKey Neo, YubiKey 5 NFC 具有 NFC 功能，其余的 YubiKey 均通过 USB 与主机进行通信。

详细的访问方式如下表所示：

功能	接口	**AID**
OTP/静态密码 (NDEF)	USB-HID/NFC	D2 76 00 00 85 01 01
U2F	USB-HID/NFC	A0 00 00 06 47 2F 00 01
OpenPGP	USB-CCID/NFC	D2 76 00 01 24 01 02 00 00 00 00 00 00 01 00 00
PIV	USB-CCID/NFC	A0 00 00 03 08 00 00 10 00 01 00
TOTP(OATH)	USB-CCID/NFC	A0 00 00 05 27 21 01 01

Revision #5
Created 2018-04-10 22:25:11 CST by Harry Chen
Updated 2019-08-14 11:28:36 CST by ZZ