RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: IDY-R02

Securing Intel PC for FIDO support: Industry standard to remove passwords

Nitin Sarangdhar

Senior Principal Engineer
Platform Security Division, Intel
@SarangdharNitin

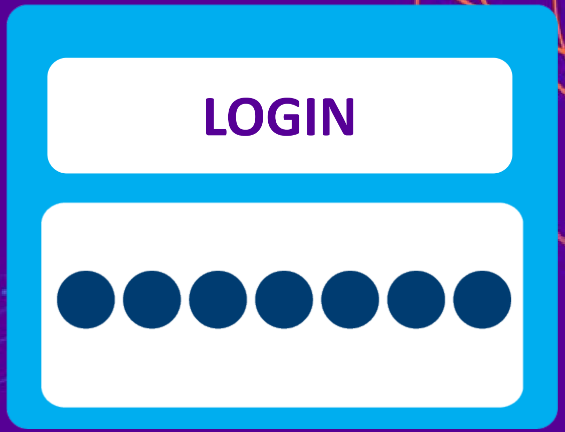
#RSAC

Session Topics

- Why password-based user authentication creates security challenges
- How FIDO* solves user authentication without passwords
- The security role of Intel hardware & firmware in a PC that supports FIDO

Hardware plays a strong role in security

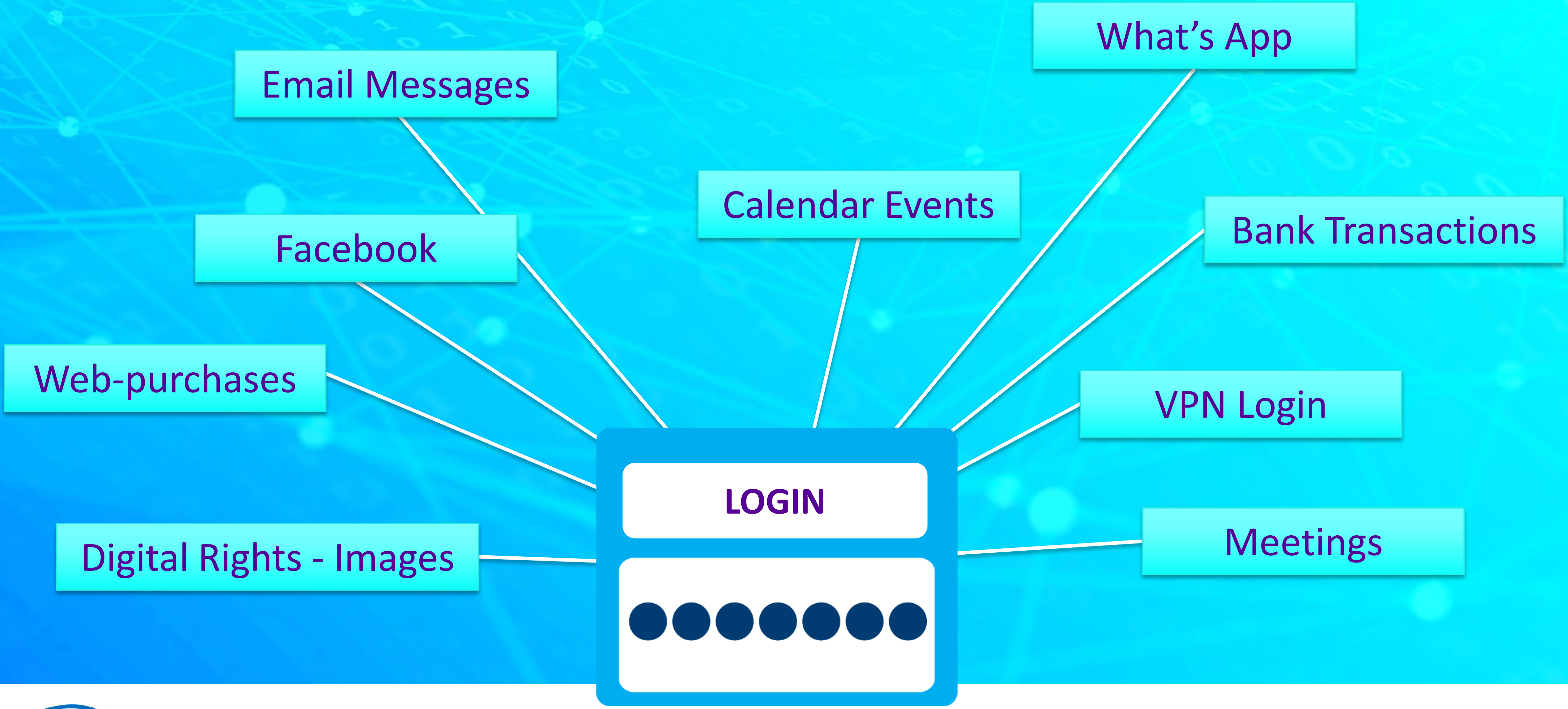
Why password-based user authentication creates security challenges



Why passwords create a security nightmare?

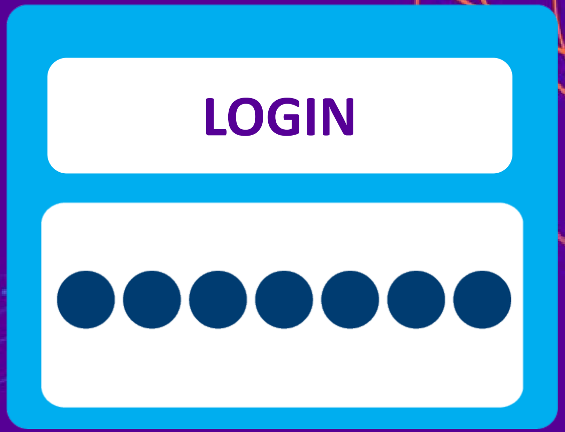
- Password re-use, no update, poor strength
- Social engineering & key-logger hacks
- Sophisticated password guessing tools
- Unsecure transmission over networks
- Direct server attacks on central user-store
- Lack of ability to recognize fraudulent activity from stolen credential

Day in the life of a password user



RSAConference2019

How FIDO solves user authentication without passwords



International Standards efforts to address authentication.

- NIST800-63-3 Digital Identity Guidelines
  - NIST 800-63-B Authentication and Lifecycle Management
- PKI
  - Public key infrastructure
  - ASIA PKI Consortium: Korea, Taiwan, Thailand, Macao, India
- ITU-T (SG17)
  - International Telecommunications Union, Security Study Group
- ISO/IEC JTC1 (SC27)
  - International Standards Organization IT Security Techniques

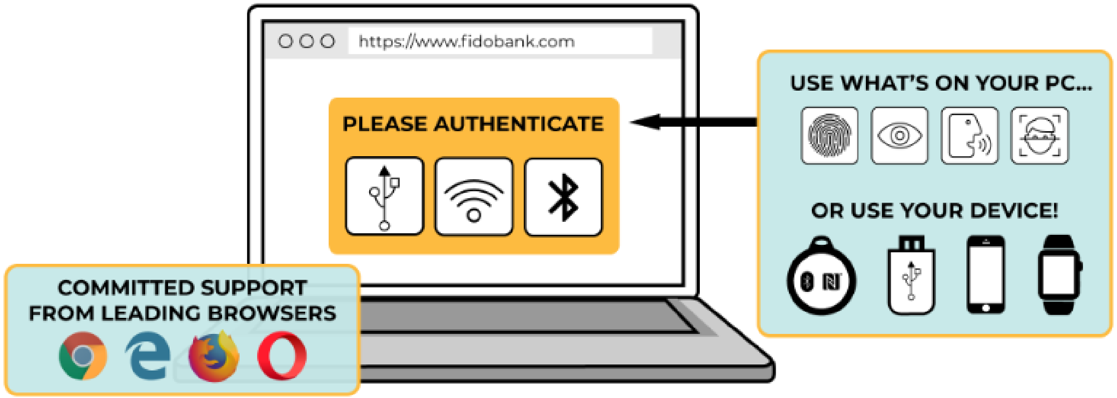
FIDO Introduction

- FIDO stands for Fast Identity Online
- FIDO protocol is adopted by W3C WebAuthn WG
- WIP Collaboration with
  - ITU-T (SG17) X.1277 & X.1278
  - ISO/IEC JTC1 SC37/SC27
- World's Largest Ecosystem for Standards-Based, Interoperable Authentication

fido™ ALLIANCE | simpler stronger authentication

3B+	Available to over 3 BILLION USER ACCOUNTS
300+	FIDO CERTIFIED SOLUTIONS

FIDO as a Solution



Targeted Solutions

- Social engineering email messages
- Bank transactions
- Web-purchases
- VPN login for enterprise

Investment in FIDO can be one component to combat "in the news" attacks

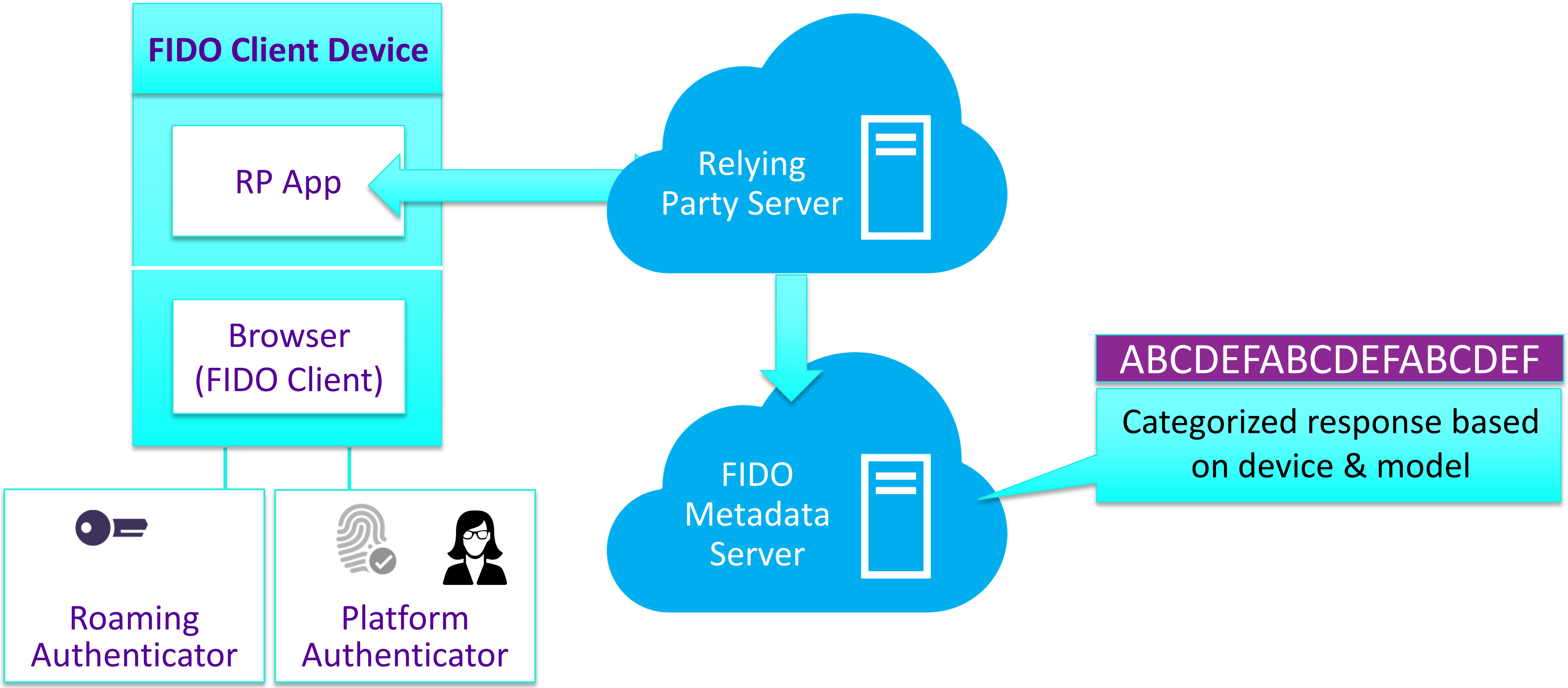
- Spreading fake news articles
- Creating cyber-attacks on infrastructure
- Voter fraud

Better user authentication will help address password related security challenges

FIDO Authenticator

	Platform authenticators		Roaming authenticators	
Multi factor authentication (possession + knowledge/inherence)	PC with TPM & biometric or pin capture	Smart phone with TPM & biometric or pin capture	Smart card with PIN or fingerprint sensor	Security key with PIN or fingerprint sensor
2nd factor (Login & Password + possession factor)	PC with TPM only		Smart card	Security key

FIDO System Architecture



FIDO Client Device

RP App

Browser (FIDO Client)

Roaming Authenticator

Platform Authenticator

Relying Party Server

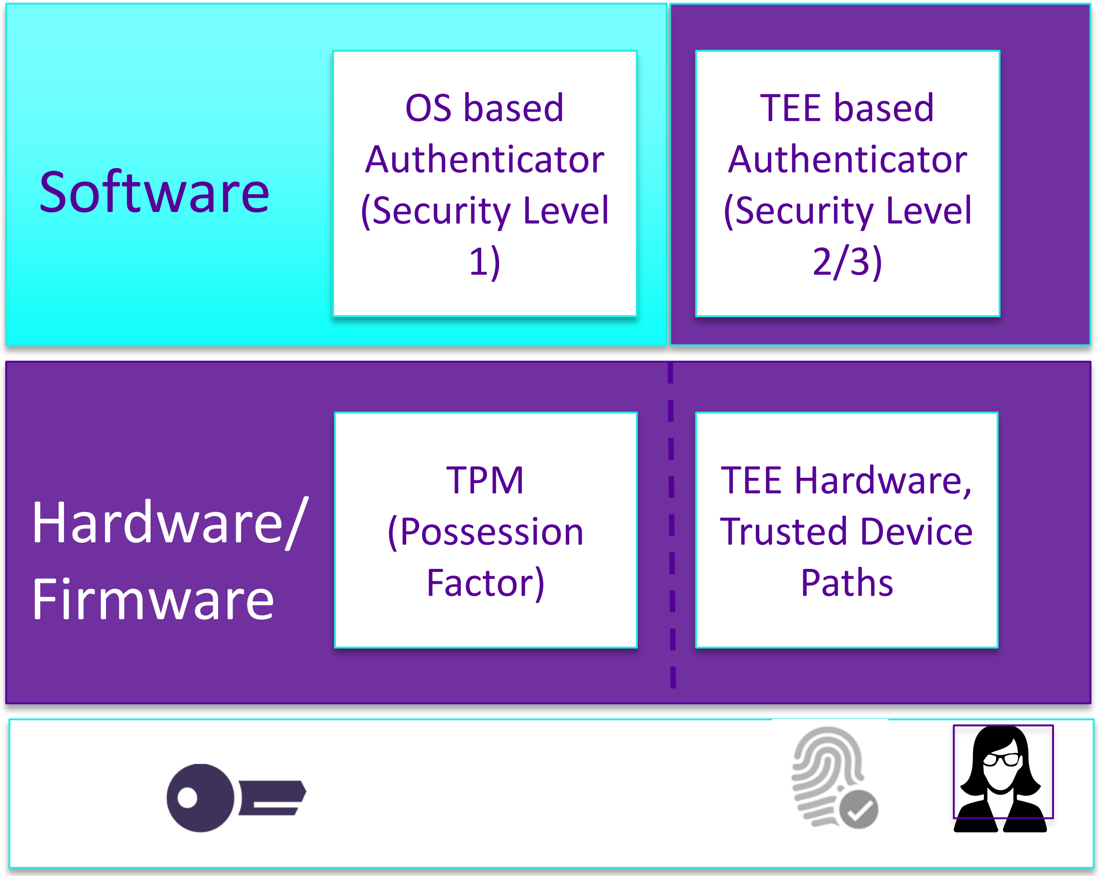
FIDO Metadata Server

ABCDEFABCDEFABCDEF

Categorized response based on device & model

FIDO* Authenticator Security Considerations

Block Diagram


Software
OS based Authenticator (Security Level 1)
TEE based Authenticator (Security Level 2/3)
Hardware/ Firmware
TPM (Possession Factor)
TEE Hardware, Trusted Device Paths

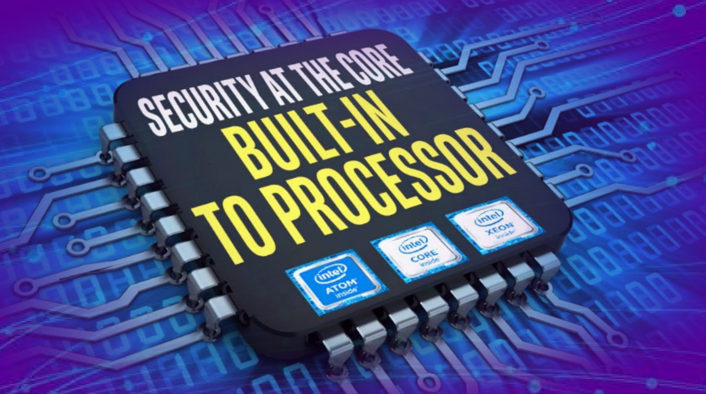
- **Extensions**
  - Distinguishing Knowledge Factors: pin, biometric (face, fingerprint)
  - Multiple Factors
- **FIDO Authenticator Metadata service**
  - Security Level 1: OS
  - Security Level 2: TEE + TPM + Trusted IO
  - Security Level 3: hardware attack protected TEE
- **Revocation/Lifecycle Management**
  - To manage security flaws discovered post field deployment by performing software/firmware updates

FIDO* Benefits

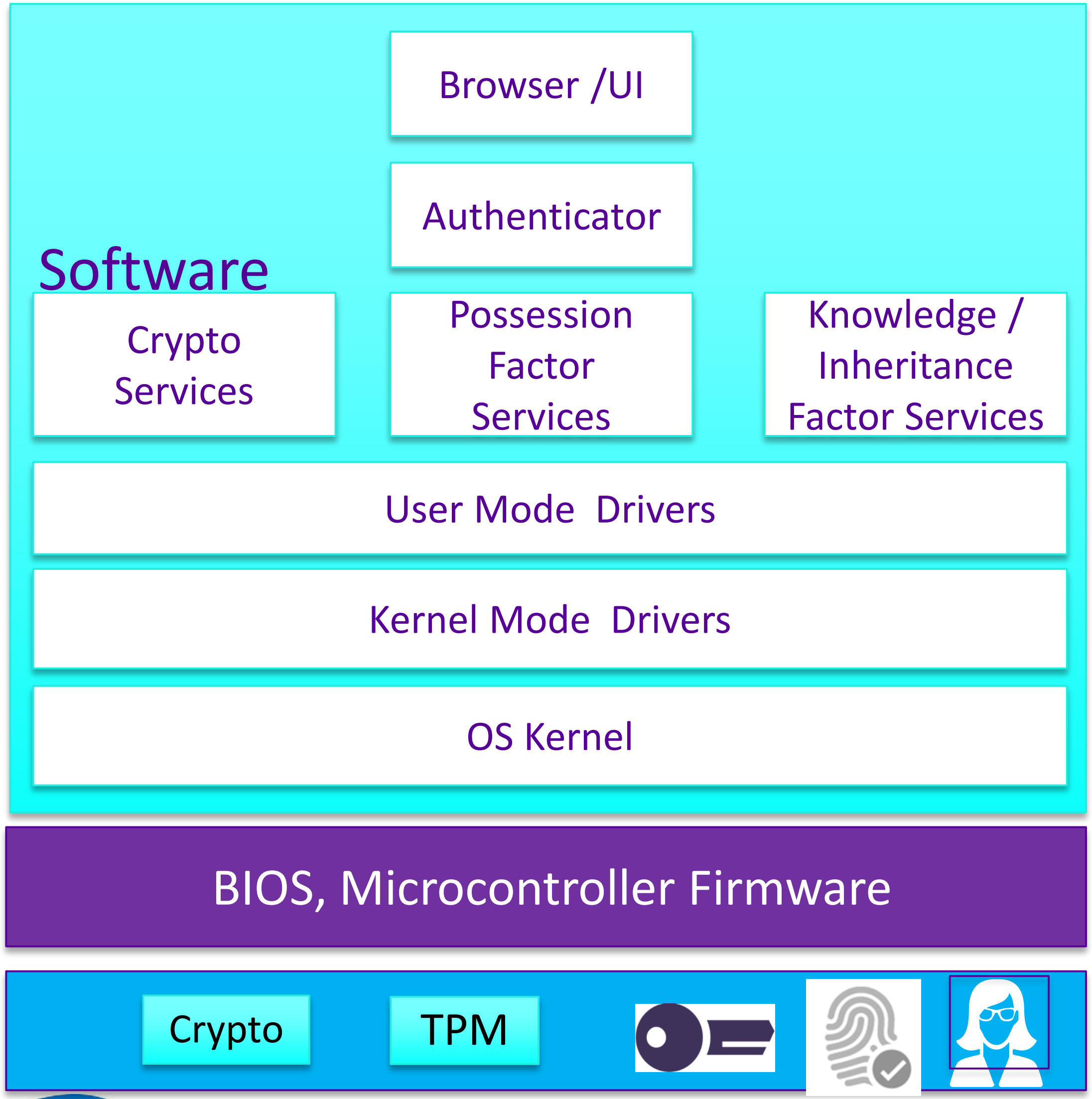
- **Better security for online services**
  - Service provider can perform proper risk assessment of FIDO user authentication security
- **Reduced cost for the enterprise**
  - Enterprise can deploy devices with properly maintained certified FIDO authenticator machines.
- **Simpler and safer for consumers**
  - Consumers do not have to worry about complex passwords as long as they use a properly maintained certified FIDO device.

RSA®Conference2019

The role of Intel hardware & firmware in FIDO* security



FIDO* Authenticator Trusted Computing Block Analysis

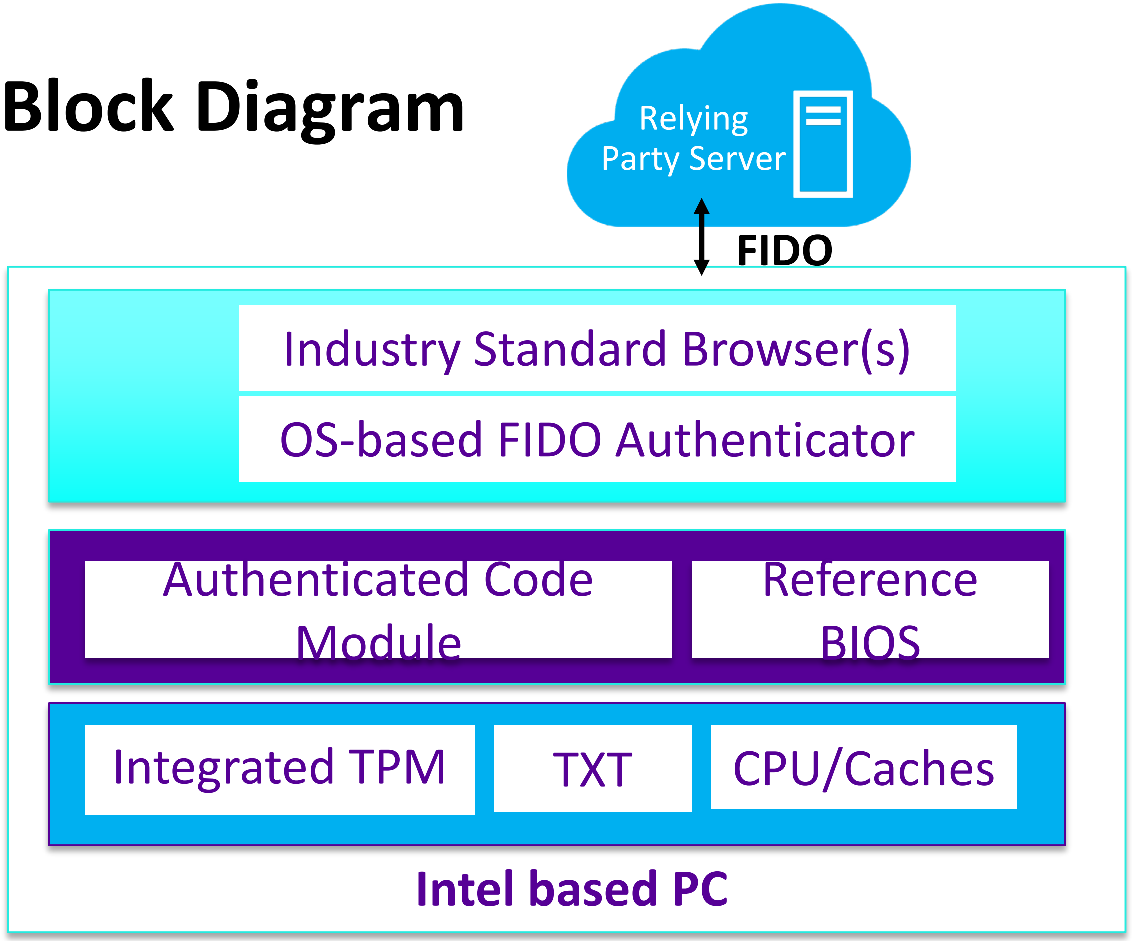


- **Potential Threats**
  - Disabling security features: Secure Boot, TPM
  - Unsigned software or firmware launch
  - Unsigned / Delayed firmware or software update containing vulnerability fixes
  - Interface Intrusion across various interfaces such as addition of filter drivers
  - Untrusted IO (Camera, Finger Print) drivers
  - Replay of previously captured data

Security Level 1 Authenticator

Software | Firmware | Hardware

Block Diagram


Relying
Party Server
FIDO
Industry Standard Browser(s)
OS-based FIDO Authenticator
Authenticated Code Module
Reference BIOS
Integrated TPM
TXT
CPU/Caches
Intel based PC

OS-based authenticator

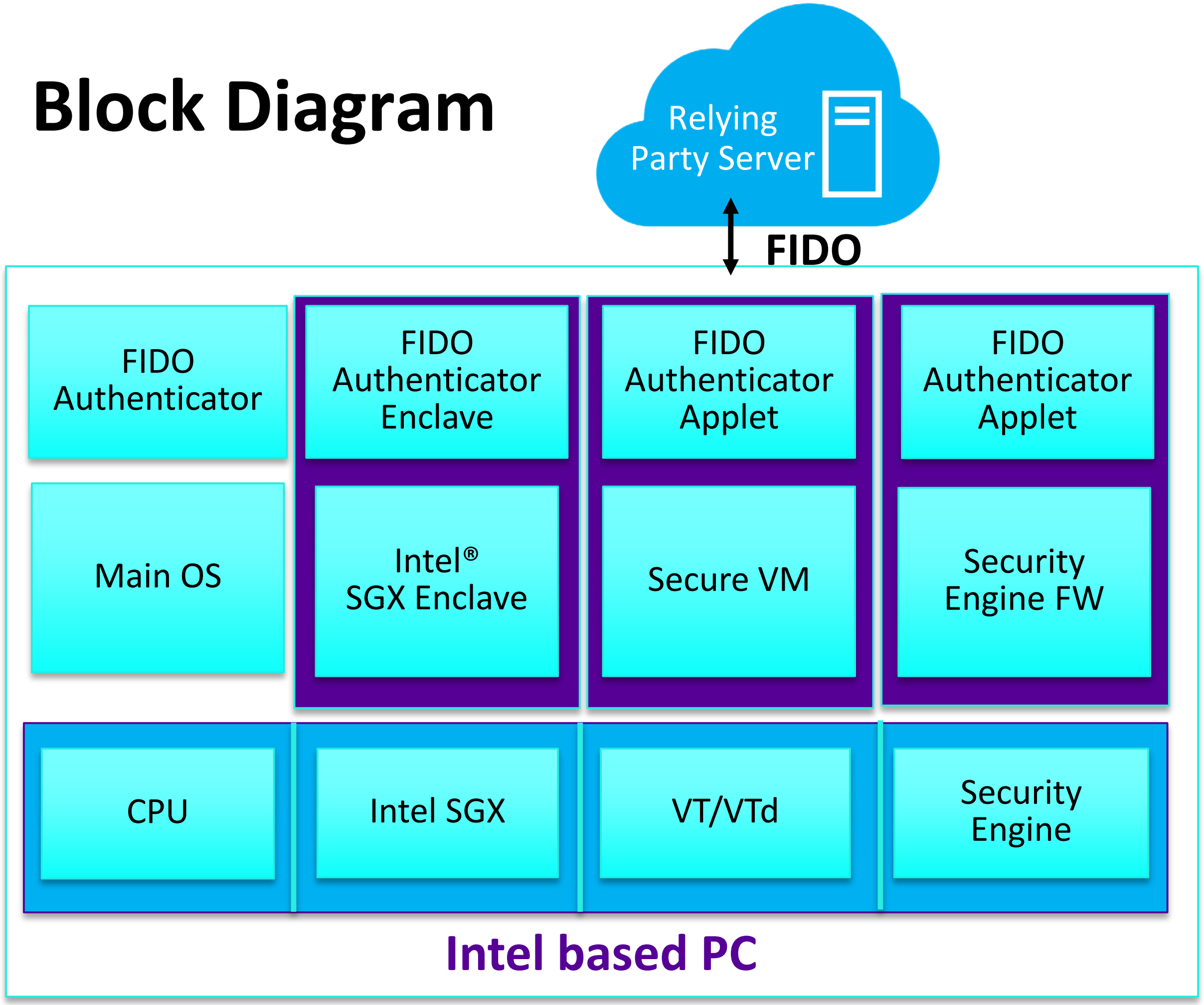
- Trusted Computing Block (TCB) relies upon OS, security
- Intel hardware & firmware:
  - Root of Trust for measurement: Trusted Execution Technology (TXT), Authenticated Code Module (Boot Guard)
  - Private key storage, Measured OS Boot, Integrated TPM (PTT)
  - Secure OS Boot: Intel reference BIOS
- Productized use cases
  - Apple MacBook*, Chromebook*, Windows* PCs

In mass deployment adoption model

Security Level 2, 3 Authenticator

Software | Firmware / TEE App | Hardware

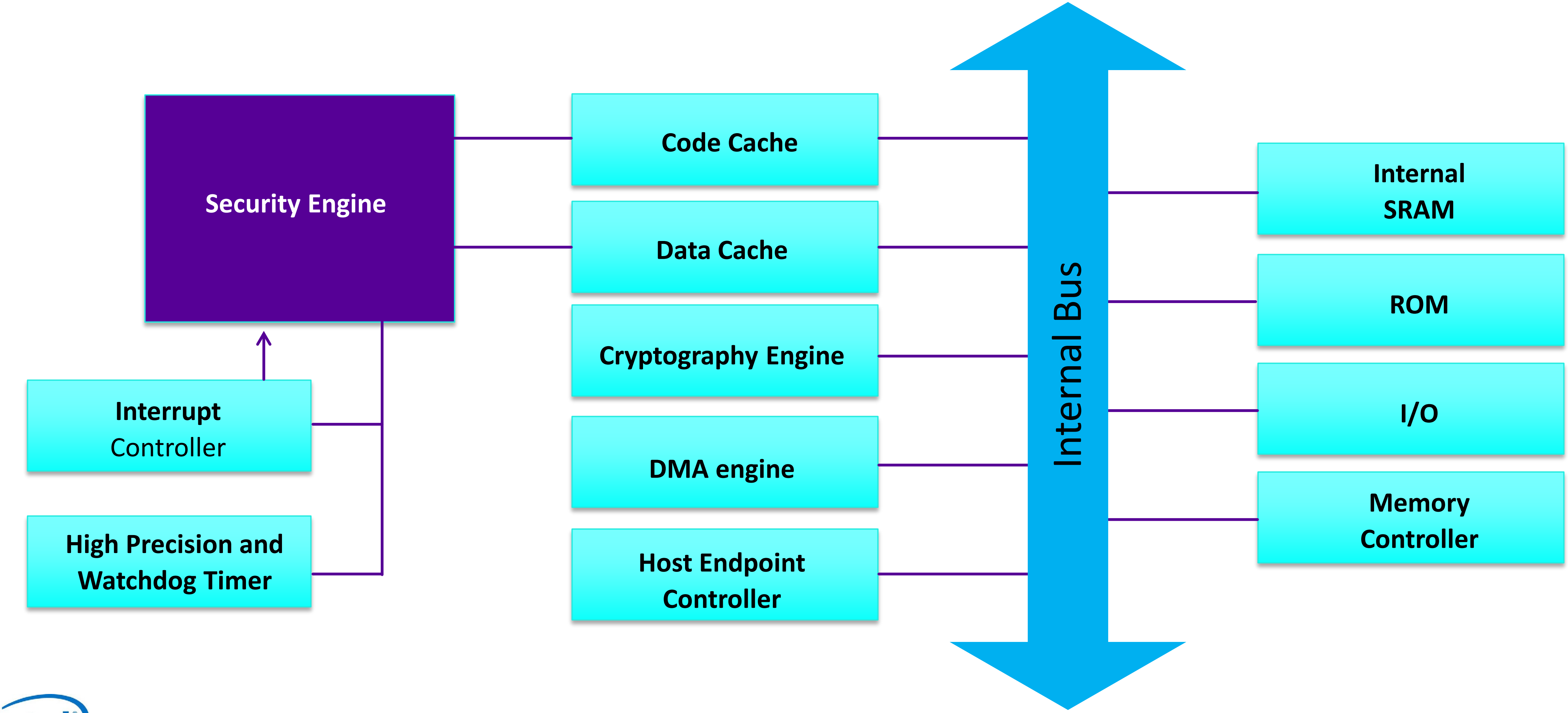
Block Diagram



TEE-based Authenticator

- Security Level 1 OS-based FIDO* authenticators can be compromised by sophisticated attackers on various interfaces between different OS modules due to large attack surface
  - E.g. Key-logger, TPM Key disable
- Security Level 2, 3 can be achieved by enabling Trusted Execution Environment (TEE) based Authenticators with smaller TCB + achieving additional requirements (e.g. software).
- Intel provides three hardware options for potential TEE
  - Security Engine
  - VT/VTd
  - Intel* Software Guard Extensions (Intel® SGX)

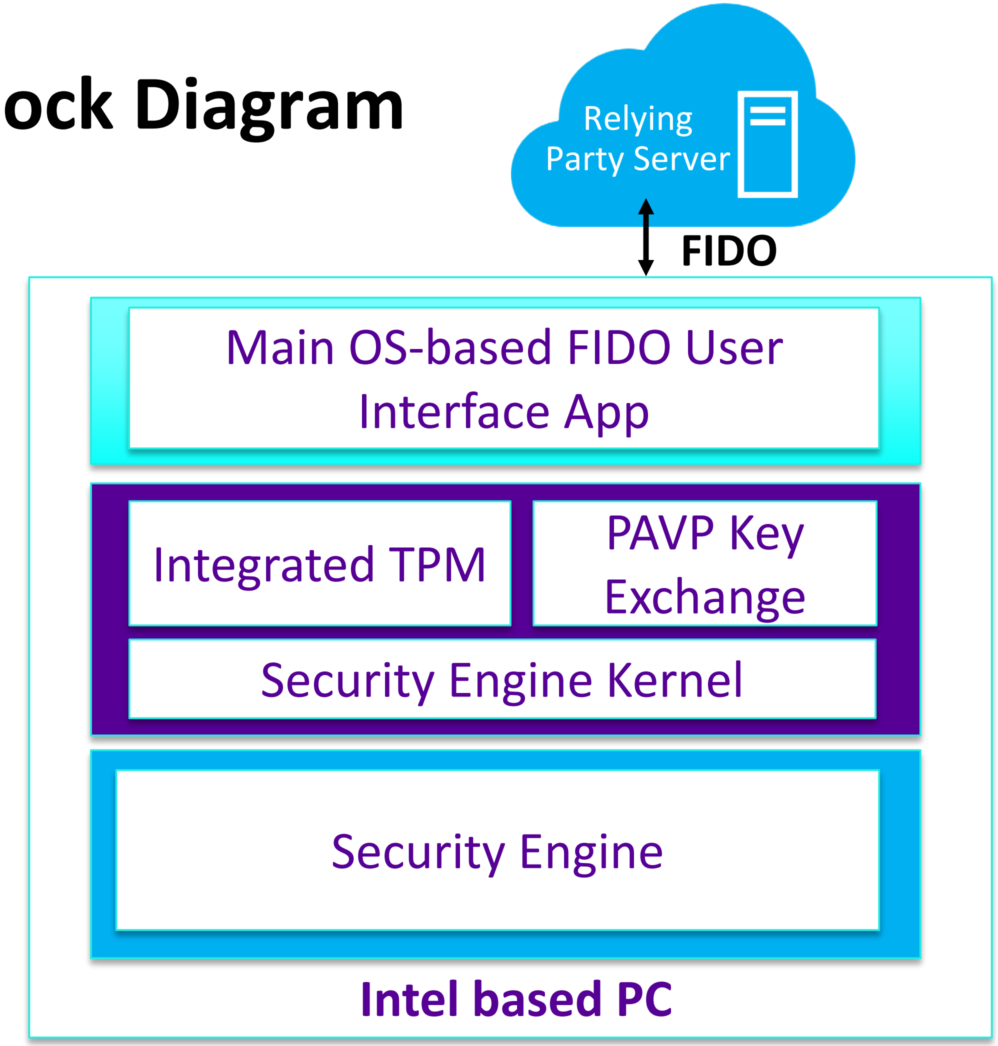
Security Engine Micro-architecture



Security Engine Architecture

Software | Firmware Apps | Hardware

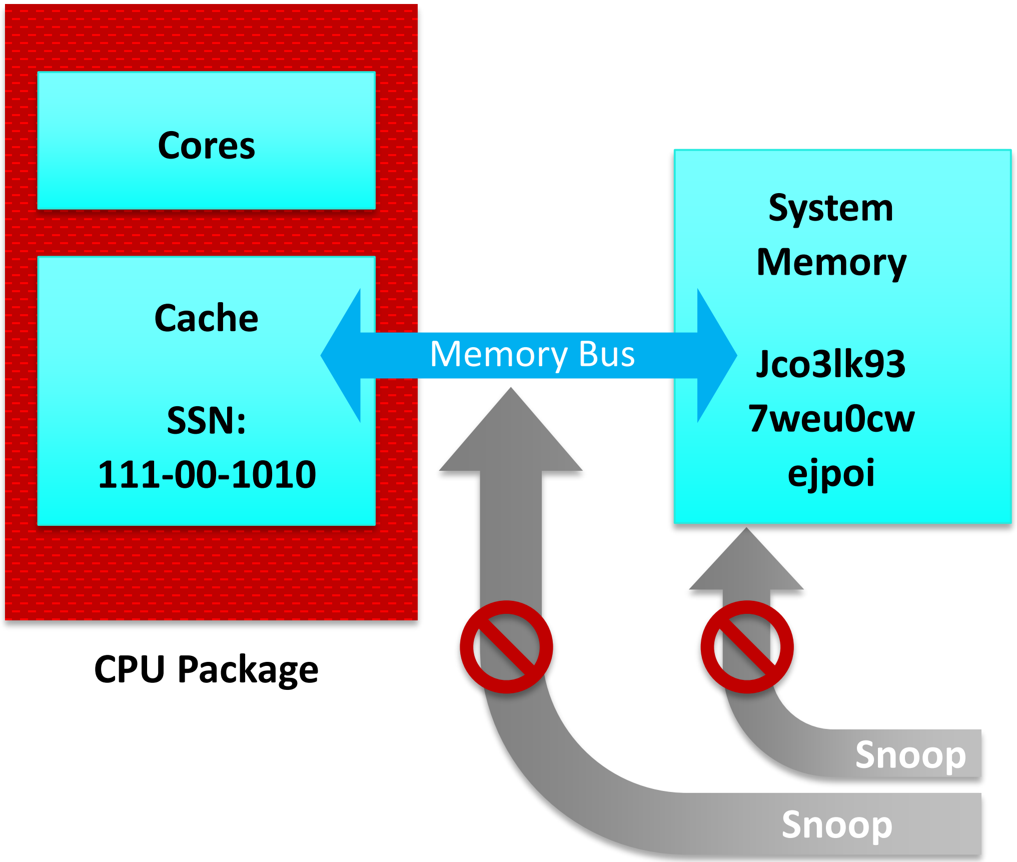
Block Diagram



Security Engine based Authenticator

- Key Benefits
  - Embedded Secure Element inside Intel SOC
  - FIDO Security Level 3 Potentially Capable
- Productized use cases
  - Integrated TPM: Possession Factor
  - Protected Audio Video Path Key Exchange

Intel Software Guard Extensions (Intel SGX) Micro-Architecture

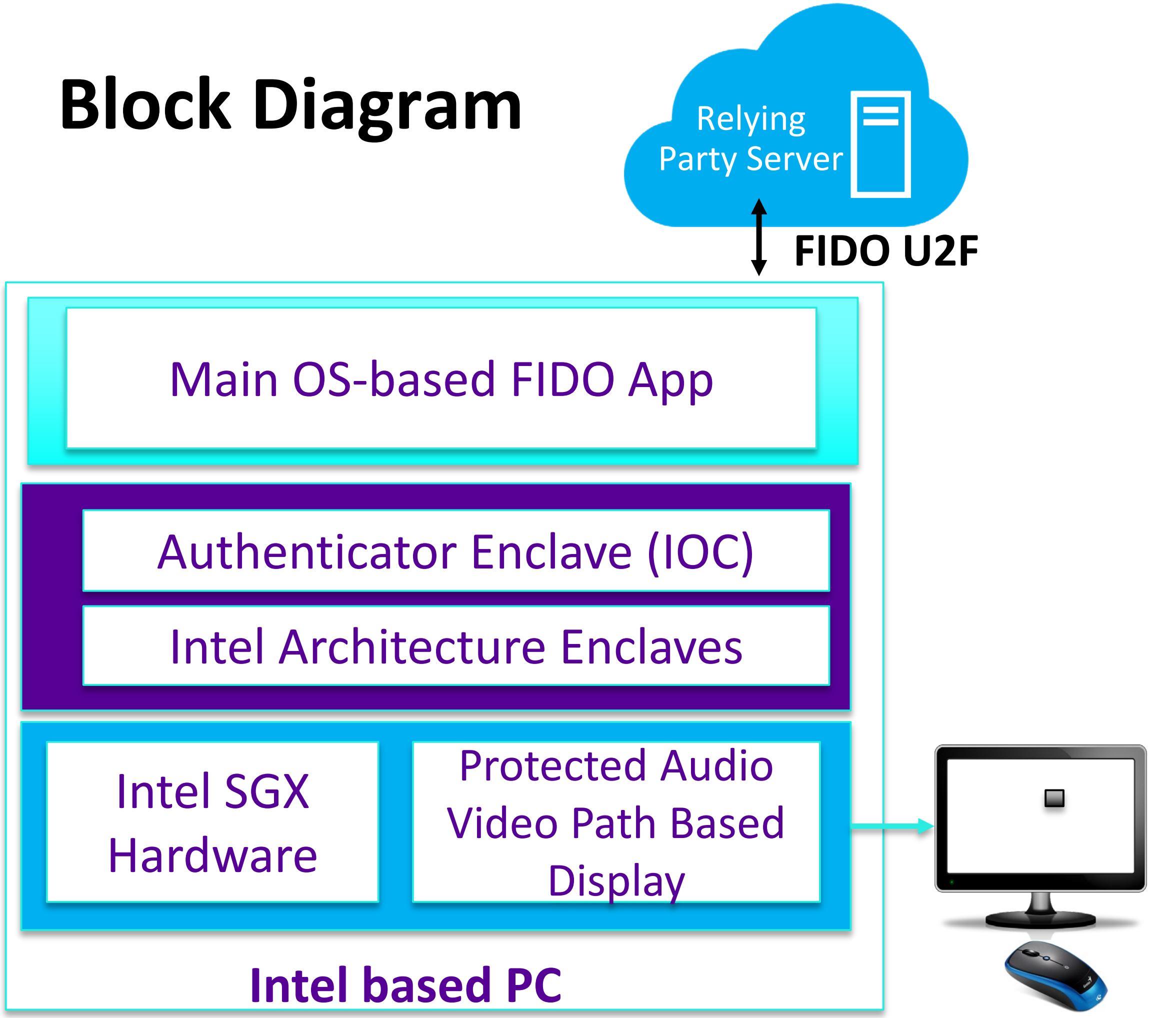


- CPU Hardware assisted Trusted Execution Environment
- Intel SGX supports 17 new instructions on CPU
- Applications (Enclaves) can set aside private regions of code and data.
- Better protection against direct attacks on executing code or data stored in memory.

Intel® Software Guard Extension FIDO Architecture

Software | Trustlet | Hardware

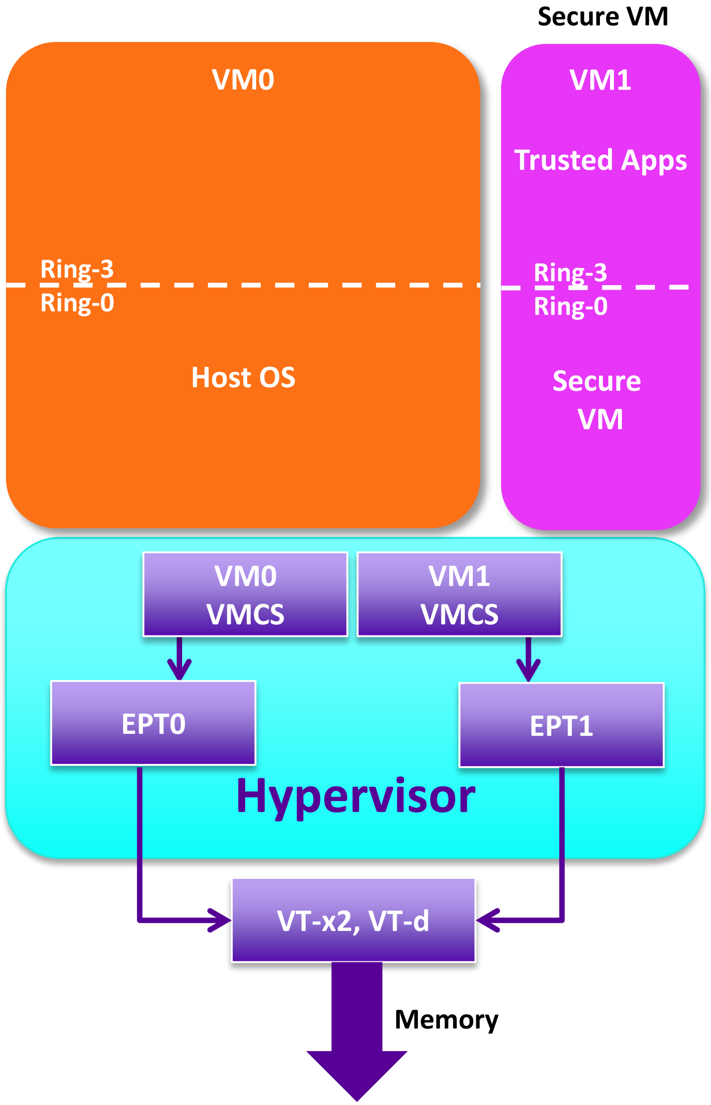
Block Diagram



Intel SGX based Authenticator

- Key Benefits
  - Small TCB that includes architectural enclaves and Intel HW/FW
  - Completely isolated from main OS, VMM and BIOS
- Productized use cases
  - FIDO U2F : Intel IOC
  - Displays OK button in a random location using Protected Audio Video Path, mitigates remote SW attacks

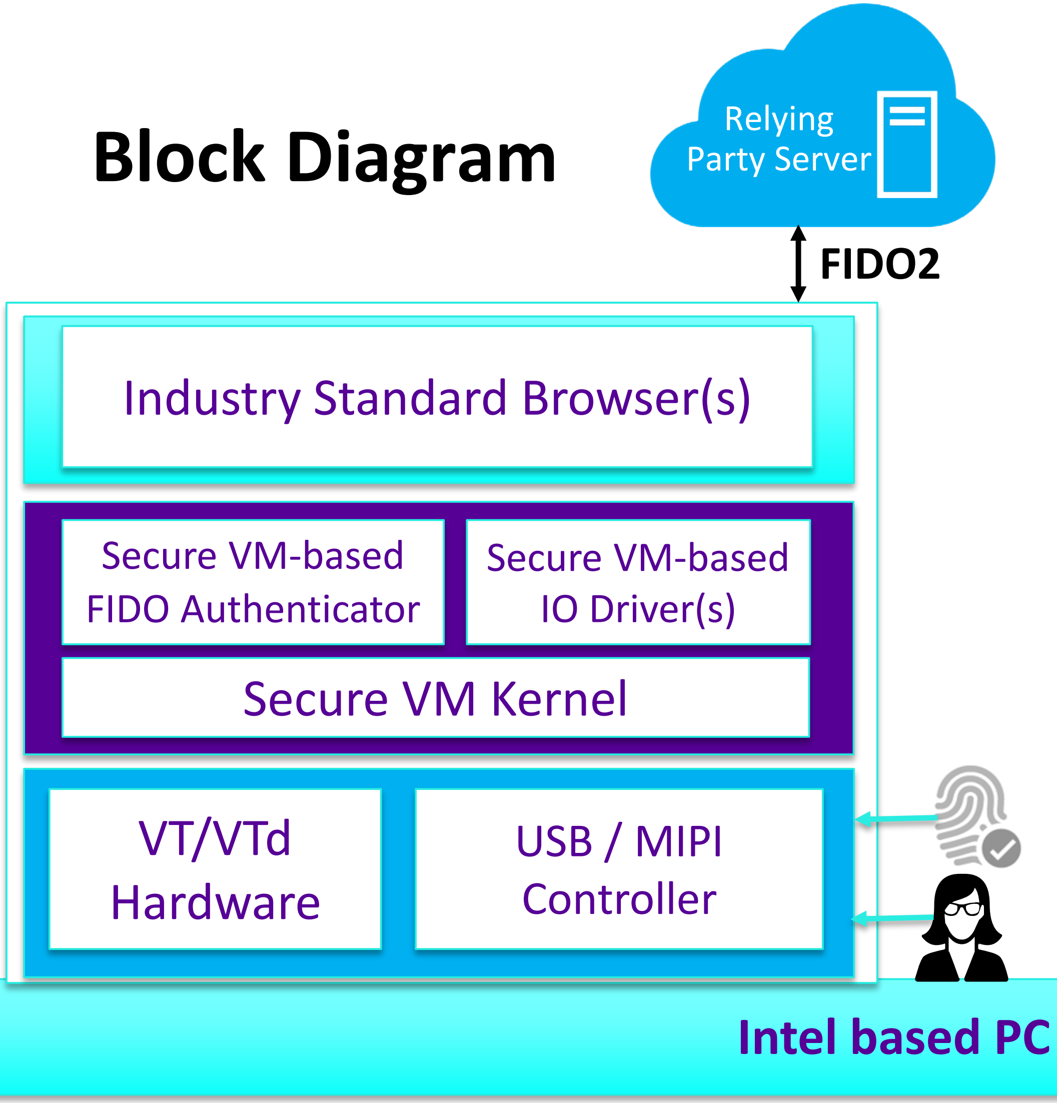
Virtualization Technology Architecture Overview



- VT HW provides memory space Read/Write/Execute access control as defined by Extended Memory Page Tables
- VTd HW support consists of ensuring DMA memory space access control as defined by the VTd Page Tables
- Enabled with Hypervisor and Trusted Applications running in a secure VM

Virtualization Technology FIDO Architecture

Block Diagram



VT/VTd Based Authenticator

- Key Benefits
  - Synergistic with OS & Browser initiatives (e.g. Windows VSM)
  - Enables trusted IO paths: Better protected from Host OS based replay attacks
- WIP use cases
  - Virtualization based protection WIP with customers / partners

To Summarize

- Intel hardware has a strong role in FIDO security
- Today we covered essentials of FIDO Security
  - Single factor: TPM only
  - Multiple factors: TPM + pin or TPM + biometrics
  - Level 1 (OS based), Level 2 and above (TEE based)
  - Revocation/Life-cycle management
- Intel hardware and firmware role in FIDO security.
  - CPU, TXT, TPM, VT/VTd, Intel SGX, Security Engine
  - Microcode, ACM, Security Engine Firmware, BIOS

Call to Action

- Stop by at Intel booth # to look for product demos
- Short Term
  - Encourage use of certified FIDO products on your client and server solutions
  - Ensure FIDO solutions are deployed with proper security configurations
  - As a relying party learn to discriminate between security levels
- Long Term
  - Deploy platforms with higher security levels of FIDO security
  - Solve major security challenges facing the industry together

Intel hardware has a strong role in FIDO security