## 中華電信零信任網路系統 xTrust











當責 交付成果、勇於負責 ACCOUNTABILITY







誠信 誠實遵法、信守承諾 INTEGRITY



## Agenda

- 1. 零信任概念
- 2. 各國零信任網路發展
- 3. 中華電信零信任網路系統 xTrust
- 4. Q&A



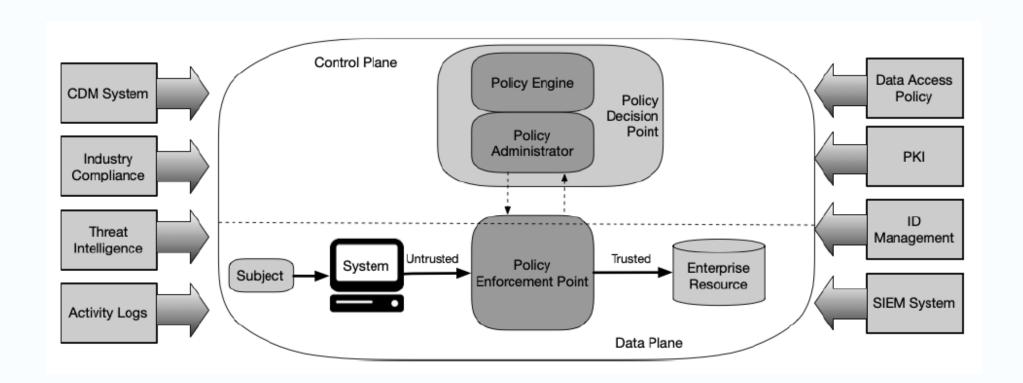


## 1. 零信任概念



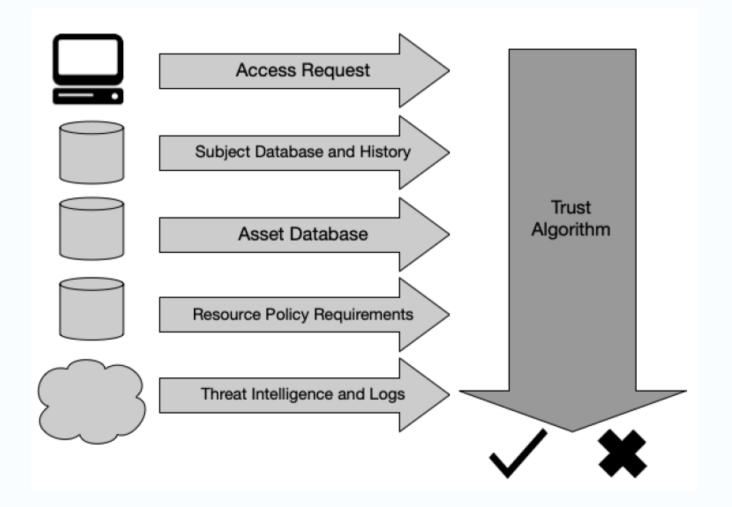


• NIST SP 800-207 : Logical Components of Zero Trust Architecture





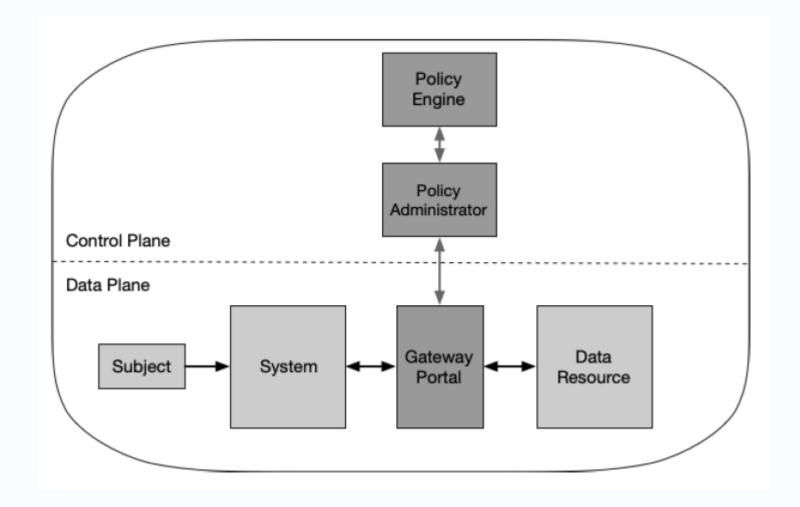
#### • NIST SP 800-27 : Trust Algorithm







#### • NIST SP 800-27 : Resource Portal Model







## 2. 各國零信任網路發展





## 中華電信 各國零信任網路說明

## 或 外 標

準 或 政

策

●零信任概念歷經10幾年發展,2020年美國國家標準技術研究院(NIST)正式頒 布標準文件SP 800-207:零信任架構(Zero Trust Architecture, ZTA), 成為各 界採用基礎

- SP 1800-35 Implementing a Zero Trust Architecture (2022)
- USA CISA Zero Trust Maturity Model (https://www.cisa.gov/zero-trustmaturity-model) (2022)
- USA DoD Zero Trust Reference Architecture (2022)

第六期「國家資通安全發展方案(110年至113年)」之「善用智慧前瞻科技、主 動抵禦潛在威脅」推動策略,將**發展零信任網路資安防護環境,推動政府機關** 導入零信任網路,完善政府網際服務網防禦深廣度

數位發展部優先推動A級公務機關導入零信任網路

為推動六大核心戰略產業,**厚植台灣資安產業自主研發能力**,貫徹「**資安即國安**」戰略, 政府將透過零信任網路之資安供需合作,**支持資安公司發展零信任網路資安產業鏈** 



2020年建立歐盟網 路安全戰略,提出 標準框架,協助成 員國轉型



2024年前聯邦網路 完成初步遷移,國 防部規劃2027年完 成零信任的部署



2021年發布網路 安全戰略,將零 信任網路安全策 略列為發展重點



2022年發布零信 任架構適用方針, 指引政府機關進行 零信任部署





## 重<sup>中華電信</sup> 政府零信任網路推動進程



政府機關 -111年起遴選機關逐年導入 零信任網路之**身分鑑別、設備鑑別及信任** 推斷3大核心機制 -後續於資通安全責任 等級A級公務機關推動導入

商用產品-配合111~113年之機關導入, 推動廠商開發符合政府零信任網路部署架 、部署原則及核心機制之商用產品 以因應後續A級公務機關之導入

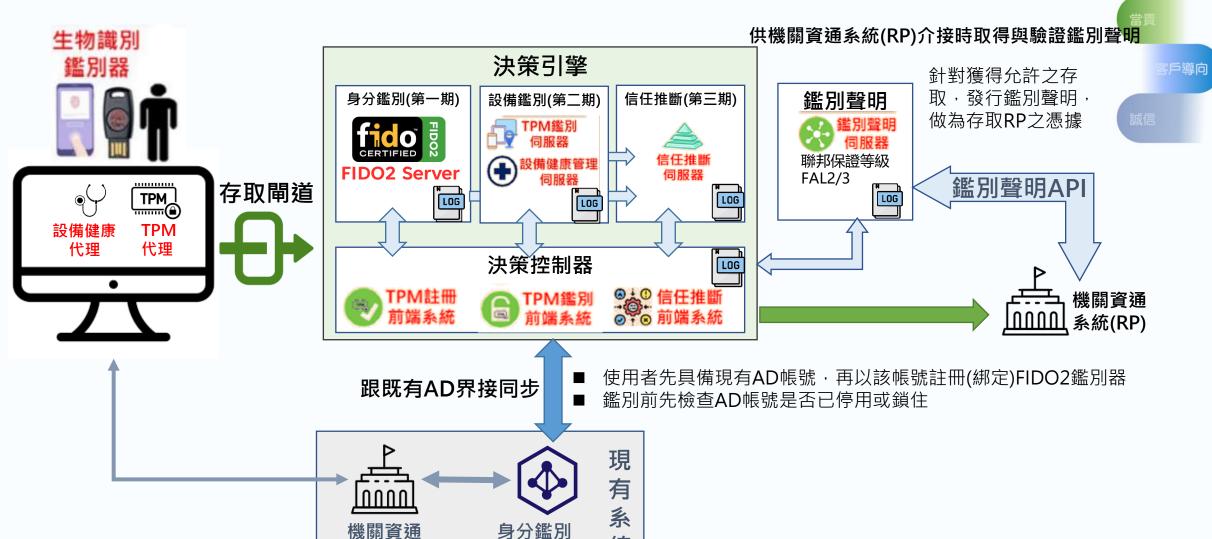
資通安全責任等級 112 111 113 A級公務機關 •身分鑑別 •設備鑑別 •信任推斷 基於信任平台模 以生物識別鑑別 依設備健康狀態、 組(TPM)之設備 器進行無密碼雙 資安威脅情資及使 因子身分鑑別 鑑別,並進行設 用者情境等資訊, 備健康管理 動態支援存取決策



## 中華電信 零信任網路架構圖

系統(RP)





伺服器(AD)



## 中華電信 身分鑑別

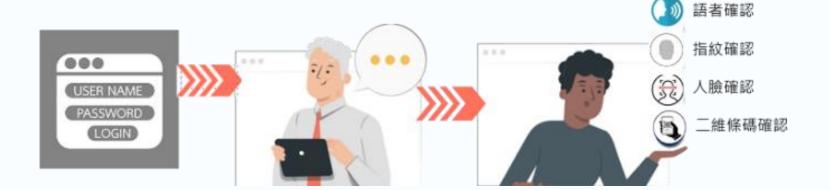
USB 認證器

#### ▶基於FIDO2之身分鑑別方法

- 國際FIDO聯盟制訂的共通安全規範,解決使用者需記憶複數組合帳號/密碼之沉重負擔。
- FIDO2使用PKI來實現身份驗證,避免了傳統密碼的弱點,如社會工程學攻擊、密碼盜竊和 重放攻擊。

帳密 多因子 FIDO2 ALLIANCE

身分鑑別 技術演進



https://fidoalliance.org/fido2/

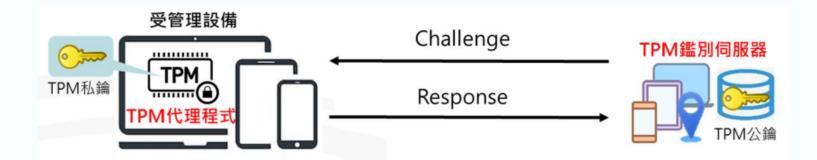


### 設備鑑別

# 當責客戶導

#### ▶基於信任平台模組(TPM)之設備鑑別方法

 TPM代表 Trusted Platform Module,是一種安全晶片,可以用於存儲和保護數位憑證、密 鑰和其他機密資料



#### ▶設備健康度管理

- 持續更新設備健康狀態
- 依設備健康狀態隨時換算設備健康信任等級

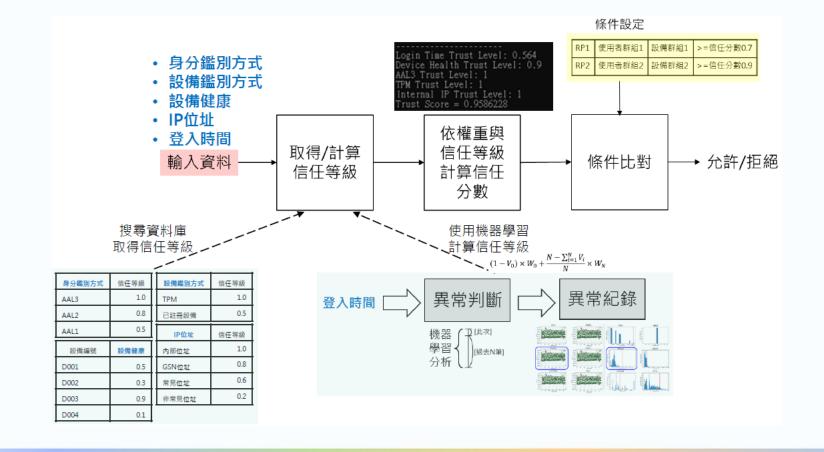
	note Pringely montaining to	TANADAM MERCAT		(Security Con	figuration Assessme
D Dates 000 a soline	P Incom BOOLD Made-415	Drage	作業余統更新 Car disp colors Il Marcal Physical Ethy 10 (1992)	23 10 Electrical School Const	71 60%
marry Calcold Certs	e ar			mi. Br. series	torse of Daniel
and property of the state of the	100 -10000			at St. Inches	50-00-0
		<b>O</b>	į.	-	-V
○ 	# 100 (100 (100 (100 (100 (100 (100 (100	0	entrational	, O	# 1967 to 2000, 100 # 1967 to 2000, 100 # 1967 to 2000, 100 # 1967 to 2000, 200 # 1967 to 2000, 200
<b>人</b>	● 107_(004_00) ● 107_(004_00) ■ 107_(004_00) ● 107_(004_00)	0	# 40 y (0 y, 40 y	. 0	- HET (2000) AND (2000
furbust from	更新	756	# 40 y (0 y, 40 y	. 0	# 100 company

設備編號	設備健康狀態	信任等級				
D001	AD	0.5				
D002	CD	0.3				
D003	ABC	0.9				
D004	D	0.1				
健康狀態/等級分配						
(A)作業系統更新:0.4						
(B)防毒更新 : 0.3						
(C)應用軟體更新: 0.2						
(D)組態合規 : 0.1						



## 中華電信 信任推斷

▶信任推斷依各類輸入資料(身分鑑別結果、設備鑑別結果、設備 健康信任等級及使用者情境Time, Location等),進行評估與計 算,輸出信任分數以提供存取決策。





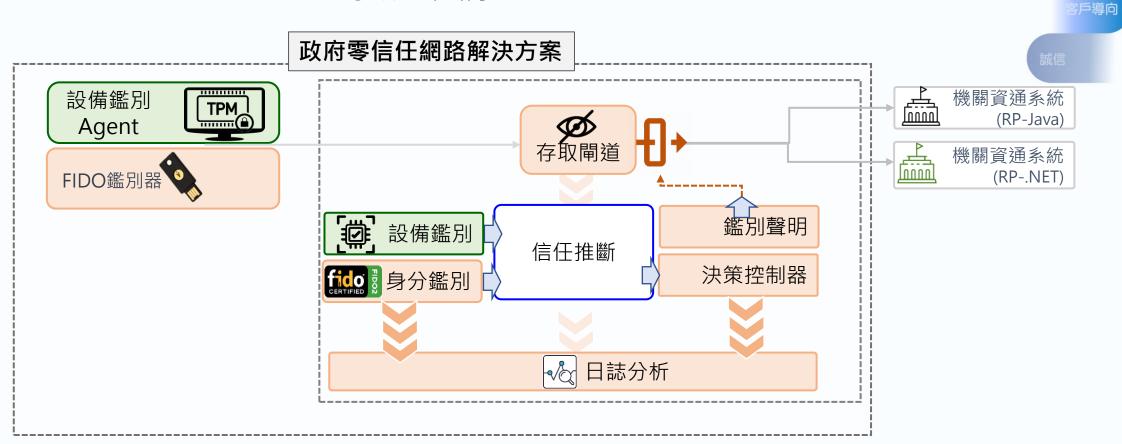
## 3. 中華電信零信任網路系統 xTrust





## 中華電信零信任網路系統 xTrust

#### 系統架構



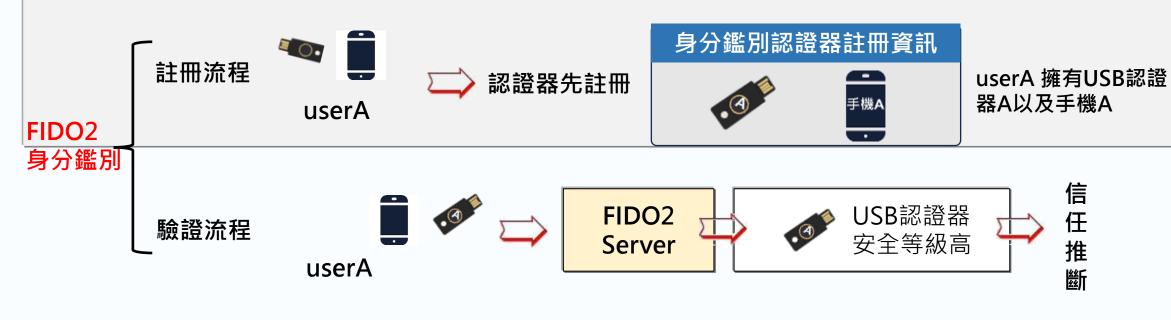


## ● 中華電信 XTrust決策引擎-身分鑑別



FIDO (Fast IDentity Online) 聯盟所訂定的一套網路識別標準,以解決使 用者需記憶複數組合帳號/密碼之沉重負擔,各大作業系統與瀏覽器均支援

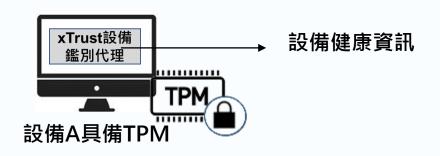


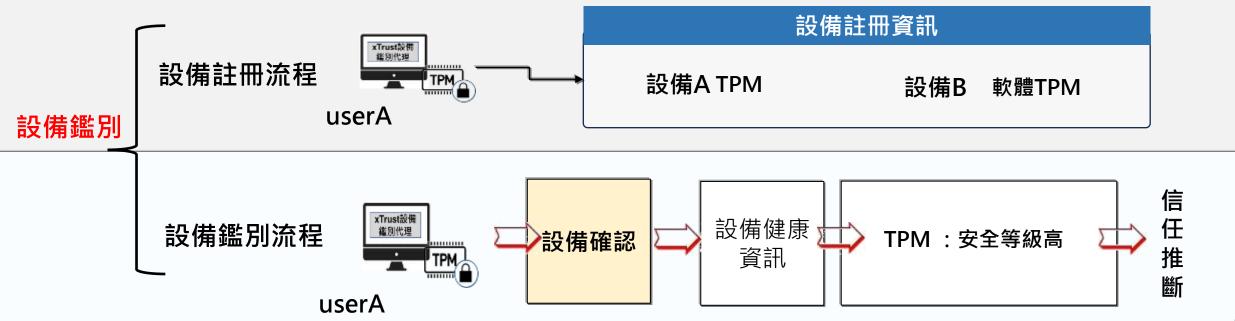




## ・ 中華電信 XTrust決策引擎-設備鑑別







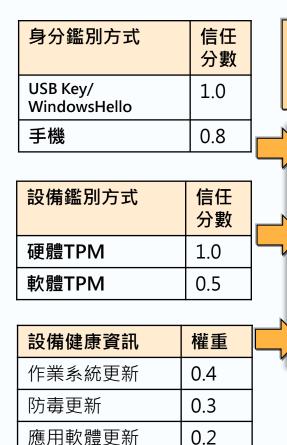


## 「中華電信 XTrust決策引擎-信任推斷



身分鑑別

設備鑑別



0.1

組態合規

IP位置 權 內部 1.0 外網專線 8.0 常見位置 0.6 非常見位置 0.2

信任分數計

算

情境異常

判斷

數進行 允入 或 拒絕

決策控制

依信任分

資訊系統分級表					
系統名	信任分數	信任等級			
資訊系統A	信任分數 > 0.3	低			
資訊系統N	信任分數 > 0.9	最高			

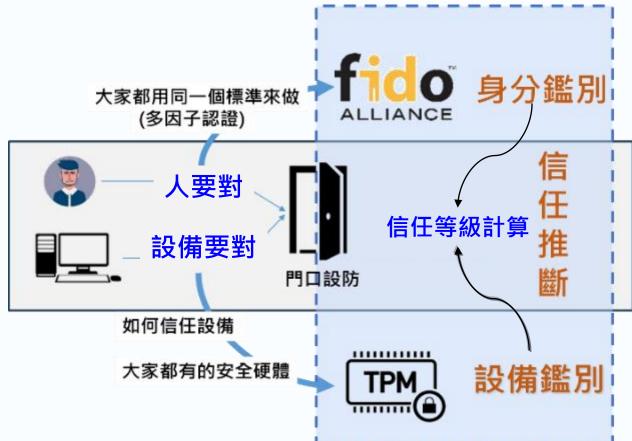


## 中華電信零信任網路系統xTrust特點



決策引擎(身分鑑別、設備鑑別及信任推斷)三大核心





#### 自主研發,通過國際/國家認證的身分鑑別





國家資通安全研究院 National Institute of Cyber Security

#### 自主研發信任推斷引擎

行為分析

#### 自主研發千錘百鍊的設備鑑別

IRMAS ☆ 硬體安全晶片



## 4. Q&A





## 謝節聽

THANK YOU







