

營業秘密



ALWAYS AHEAD

中華電信商用憑證服務簡介

為了你
—— 一直走在最前面

數據分公司
企業客戶處 連于婷
2016.05.11



Refresh your life

大綱



中華電信PKI業務概述

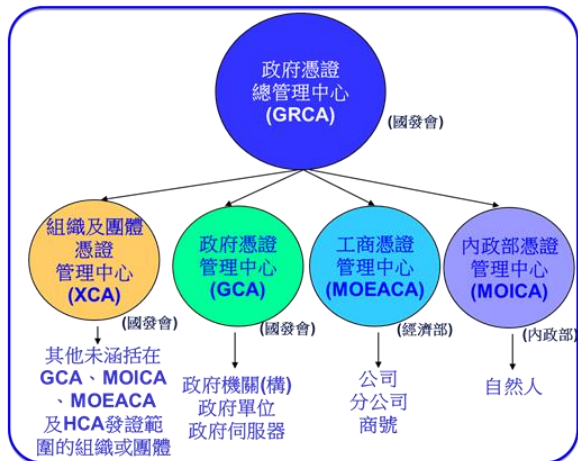
SSL憑證服務介紹

金融憑證服務介紹

中華電信PKI業務概述

中華電信PKI業務

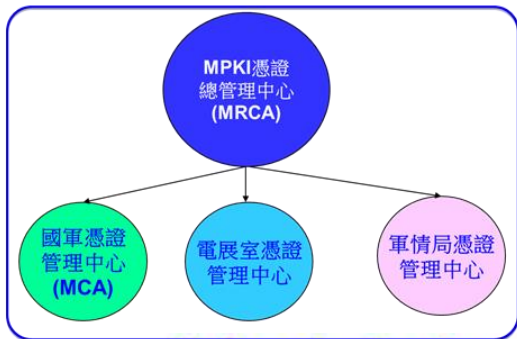
1. 政府PKI各CA系統建置維運
2. 提供政府PKI各類憑證IC卡



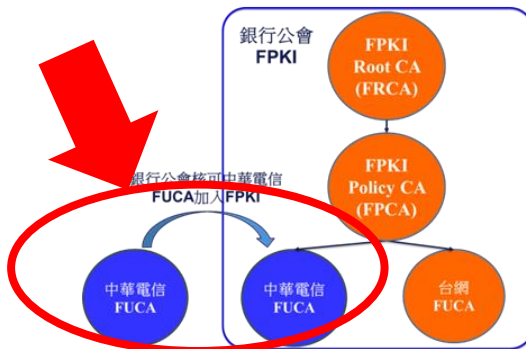
4. 商用PKI憑證服務 (中華電信ePKI)



3. 軍用PKI各CA系統建置及系統維護



- 銀行金融PKI憑證服務 (加入銀行公會FPKI)



6. PKI關聯產品



硬體密碼模組



藍芽讀卡機



NFC背夾 (iPhone 4/5)



HiPKI HiPKI安控套件

7. 海外CA系統建置

洽談中的國家包括：

- 瓜地馬拉
- 尼加拉瓜
- 聖文森

SSL憑證服務介紹

SSL憑證服務大綱

SSL憑證服務介紹

SSL憑證服務特色

SSL憑證服務優惠方案

SSL憑證服務申請方式

常見問題及Reference Site

SSL憑證服務介紹(1/2)

■ SSL (Secure Sockets Layer) 憑證

- ▶ 為一種安全傳輸協定
- ▶ 用於建立客戶端和伺服器之間的安全通道，防止資料在傳輸過程中被駭客截取或竄改，以保護網路使用者所傳輸的個人資料(如信用卡號、帳號、密碼等機敏資料)



用來保護登入時帳號密碼不會被駭客竊取



提供安全認證標章來凸顯網站的安全性

SSL憑證服務介紹(2/2)



■ 效益

- ▶ 網站認證：提供網站訪客確認是否登入正確的網站，防止消費者上到釣魚網站。
- ▶ 資料加密：避免私密資料外洩及盜用
- ▶ 專業標章：點選標章，可顯示網站的認證資料是否有效
- ▶ 理賠保證：提供最高理賠金額3百萬元，享有交易安全服務外及理賠的保障。

■ 適用對象

- ▶ 電子商務服務
- ▶ 網站內容涉及機敏資料傳輸
- ▶ 欲強化企業形象及欲增進Google搜尋排名者

使用中華電信SSL憑證之網站資訊

以IE為例：



以Chrome為例：



本網站提供即時災害示警資料，以國際Common Alerting Protocol (CAP)Version 1.2型式發布或申請主動推送的方式，獲取即時災防示警資訊。目前本站供應的即時訊息共有12項，包括

- ✓ 颱風警報、豪大雨特報(中央氣象局)
- ✓ 公路災害或預警
- ✓ 地震報告、海嘯資訊(中央氣象局)
- ✓ 停班停課訊息(9)

SSL憑證種類

種類	說明
單網域SSL憑證	憑證中只記載單一網域名稱 適用於大部分只架設單一網站的企業使用。 例如:www.cht.com.tw, www.epki.com.tw
多網域SSL憑證	每張多網域憑證預設可記載3個不同的網站名稱，客戶可視需要再增購，每張最多可增購至99個網站名稱。 方便企業需要同時架設多個SSL網站時選用，以節省建置經費。 例如：Unified Communication Server、Lync Server、Exchange Server
萬用網域SSL憑證	購買一張，應用範圍為多個次網域(Sub-domain)，即網域名稱的開頭可以包含萬用字元*號。 例如：伺服器上有5個網站 (例如：www.publicca.net、mail.publicca.net、data.publicca.net、test.publicca.net、backup.publicca.net)，你只需要申請一張名為*.publicca.net的萬用網域SSL憑證，5個網站使用。



SSL憑證服務特色-單網域一年期

產品 評比項目	HiNet SSL憑證	Symantec	TWCA	GlobalSign
產品來源	自行開發	併購VeriSign	代理Comodo或是外國CA產品	自行開發
銷售管道	中華電信	1. Symantec網站申請 2. 凱森興業銷售	自銷	匯智代理
國際驗證	通過國際WebTrust for CAs 及 SSL Baseline & Network Security稽核驗證	無資料 (2015年發生多起誤發憑證事件而遭google嚴厲警告)	WebTrust for CAs	WebTrust for CAs
通過國內審核	1. 通過經濟部審核設立 2. 提供中英文版之憑證實務作業基準	1. 未申請國內審核 2. 僅提供英文版之憑證實務作業基準 3. 發生事件需跨海求償	1. 通過經濟部審核設立 2. 提供中英文版之憑證實務作業基準	1. 未申請國內審核 2. 僅提供英文版之憑證實務作業基準 3. 發生事件需跨海求償
符合國際標準規範	使用CA/Browser Forum之組織鑑別型SSL憑證之物件識別碼	使用CA/Browser Forum之組織鑑別型SSL憑證之物件識別碼	未使用CA/Browser Forum之組織鑑別型SSL憑證之物件識別碼	使用CA/Browser Forum之組織鑑別型SSL憑證之物件識別碼
價格	一年期售價 12,000	一年期售價 16,000/年	未揭露	一年期售價 12,500元/年



SSL憑證服務-各產業應用範圍

產業別	應用範圍	產業別	應用範圍
網路科技業	<ul style="list-style-type: none"> ·會員登錄系統 ·線上付款機制 ·會員資料系統 ·電子市集系統 	金融產業	<ul style="list-style-type: none"> ·網路銀行 ·網路下單-證券、投信、投顧 ·網路投保 ·保單查詢系統
物流業	<ul style="list-style-type: none"> ·貨物追蹤系統 ·廠商登錄系統 	旅遊業	<ul style="list-style-type: none"> ·會員系統 ·線上訂購系統
電信電訊業	<ul style="list-style-type: none"> ·線上帳單暨付款系統 	運輸業	<ul style="list-style-type: none"> ·訂單查詢系統 ·線上購票系統
製造業	<ul style="list-style-type: none"> ·ERP、SCM、CRM 系統 ·B2B 電子訂單資料加密 ·經銷商管理系統 ·企業線上購買商店 (Corporate Store) ·詢價報價系統 	教育單位	<ul style="list-style-type: none"> ·線上捐款 ·線上選課 ·成績派送 ·eLearning
政府單位	<ul style="list-style-type: none"> ·資料查詢系統 ·公文流程控管系統 	醫療單位	<ul style="list-style-type: none"> ·網路掛號系統 ·病歷資料派送系統
線上遊戲業	<ul style="list-style-type: none"> ·遊戲主機資料傳送 ·會員註冊系統 ·點數採購付款系統 	不分類	<ul style="list-style-type: none"> ·職工福利委員會 ·採購系統電子郵件 WebMail ·FTP資料傳送系統

HiNet SSL憑證服務2016優惠方案



項目	憑證效期	牌價	當季優惠價(六四折)	校園優惠(二四折)
單網域SSL憑證	1年期	15,000	9,600	3,600
	2年期	28,000	15,680	7,200
	3年期	41,000	19,680	10,800
多網域SSL憑證	1年期	20,000	12,800	同當季優惠專案
		增加網域名2,000/個	增加網域名優惠價1,600/個	
	2年期	30,000	19,200	
		增加網域名3,000/個	增加網域名優惠價2,400/個	
	3年期	40,000	25,600	
		增加網域名4,000/個	增加網域名優惠價3,200/個	
萬用網域SSL憑證	1年期	75,000	38,400	19,000
	2年期	140,000	62,720	28,500
	3年期	200,000	76,800	38,000

優惠期間至
2016/12/31

原售價及老客戶續購優惠，請參考產品網址 <http://publicca.hinet.net/SSL-01.htm>

營業秘密

SSL憑證 + 網站偵防隊 Standard版 優惠價格

本優惠從即日起至2016年9月30日止

項 目	服務效期	優 惠 價	原 價
單網域SSL憑證 + 網站偵防隊	1年期 (12個月)	13,430元	19,188元 (單網域SSL憑證一年期每張15,000元 + 偵防隊每月599元x12個月)
	2年期 (24個月)	23,780元	33,976元 (單網域SSL憑證二年期每張19,600元 + 偵防隊每月599元x24個月)
	3年期 (36個月)	32,310元	46,164元 (單網域SSL憑證三年期每張24,600元 + 偵防隊每月599元x36個月)

申辦網址：

https://publicca.hinet.net/SSL-Promotion_IBA.htm

業務說帖與產品優勢

■ 優勢

▶ 本土化

▶ 提供第一線技術支援(本土化支援)

▶ 通過經濟部保證等級第三級審核及通過2項國際標章

▶ 目前國外憑證幾乎沒有經過主管機關審定、求償困難(外國法院訴訟)

▶ 價格優惠!!

▶ 通案優惠價64折、老客戶回饋56折、校園方案優惠價為售價24折。

▶ 搭配中華其他產品包裝另有優惠!(目前推出網綁網站偵防隊包裝)

▶ 透過SSL提升Google SEO搜尋排名

▶ Google在2014年的八月於官方Blog中發表了一篇採用HTTPS加密的網站在搜尋結果中的排名將會更高的文章。

■ 特色

▶ 提供30天鑑賞期

▶ 客戶申請Hinet SSL憑證服務後，由憑證簽發當日開始起算30天內，客戶可提出憑證廢止申請，則不會出帳給客戶。

▶ 採用線上填寫表單申請、提供多元化申請方式

▶ 提供完整憑證請求檔操作手冊

使用情境

https://www.abc.com.tw



網站訪客1



SSL 加密連線



網站伺服器



申請方式一(傳統申請書)：

申請

- 客戶上網填寫申請書並上傳憑證請求檔(請以2048 bits金鑰長度)
- 申請書列印後蓋公司大小章及檢附相關證件，寄至中華電信通用憑證管理中心窗口

受理

- 憑證註冊審驗窗口進行資料審核

竣工

- email通知客戶進行SSL憑證接受
- 客戶上網進行憑證接受並進行安裝

申辦網址

<http://publicca.hinet.net/SSL-03.htm>

申請方式二(使用工商憑證申購)：

申請

- 客戶上網填寫申請書並準備**由工商憑證IC卡**與讀卡機(目前先適用於IE)上傳憑證請求檔(請以2048 bits金鑰長度)

SSL憑證購買申請書(有 * 為必填項目)

以保證等級第3級憑證IC卡
數位簽章投單(只支援IE)

卡片密碼:

驗證憑證

(請插入IC卡片,目前支援MOEACA,XCA,GCA,MOICA與Public CA所發用戶憑證)

受理

- 憑證註冊審驗窗口進行資料審核

竣工

- email通知客戶進行SSL憑證接受
- 客戶上網進行憑證接受並進行安裝

申辦網址

<http://publicca.hinet.net/SSL-03.htm>



申請方式三-學校機構(電子公文交換)：

申請

- 客戶上網填寫申請書並上傳憑證請求檔(請以2048 bits金鑰長度)
- 申請書列印後加蓋關防並彩色掃描作公文附件，使用由XCA所發之憑證IC卡以公文電子交換發文給中華電信數分

受理

- 憑證註冊審驗窗口進行資料審核

竣工

- email通知客戶進行SSL憑證接受
- 客戶上網進行憑證接受並進行安裝

校園方案
申辦網址

<https://ra.publicca.hinet.net/SSLCertEnrolimen/SSLForm-01.jsp?ssltype=0&proCode=eduPCA1S01>

常見問題

Q1：SSL憑證服務是否有提供試用期？

Ans：HiNet SSL憑證服務無試用期，但提供鑑賞期30天，學校機關應最遲於憑證簽發後第29天寄送SSL憑證廢止申請書 (需用印)至中華數分資安處則不會產生費用。

Q2：SSL憑證到期是否會自動續約並寄出繳費通知？

Ans：HiNet SSL憑證到期後無法展期，故本案到期後無法進行續約，若有需要重新購買。

Q3：有關SSL憑證其他問題可以上哪查詢？

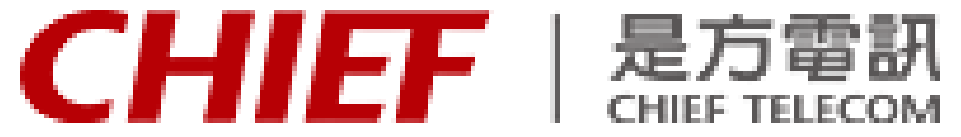
Ans：SSL憑證申請相關問與答可參考中華電信通用憑證管理中心網址：<http://publicca.hinet.net/SSL-01.htm>

各憑證請求檔產製，請上

http://publicca.hinet.net/SSL_ra.htm查詢

Reference Sites(1/3)

■ 單網域憑證:



Reference Site(2/3)



■ 多網域憑證:



南山人壽



Reference Site(3/3)



■ 萬用網域憑證:



金融憑證服務介紹

金融憑證服務介紹大綱

金融憑證服務概述

產品特色

優惠方案包裝

應用情境

成功案例

金融憑證服務概述-名詞解釋

憑證管理中心Certificate Authority(CA)

- 憑證的簽發機構，負責簽發、廢止與公告憑證資訊
- 經過財政部逐年審核通過的憑證簽發機構，才能透過金融機構單位發出數位憑證

憑證註冊中心Registration Authority(RA)

- 負責憑證使用者身份確認工作，將各項憑證操作提交予憑證發放機構(CA)，最後並將憑證管理系統(CA)產生之數位憑證提供給使用者下載。

Public CA個人憑證

- Public CA發放之軟體電子憑證，用於鑑別個人身分之用
- 用於證券、期貨及基金電子下單

FXML法人憑證

- FXML為銀行公會訂定之安控規格
- 用於各項轉帳及其他需確認身分之交易服務功能·如：網路銀行非約定及大額約定轉帳

金融憑證服務概述-流程說明

1. 金融電子憑證(Public CA、FXML)申請



中華電信
Chunghwa Telecom

憑證管理中心(CA)

Step 2
憑證操作需求

2. RA系統標準化服務

3. 憑證應用客製化服務

Step 3
憑證核發

Step 1
進行憑證申請

Step 4
憑證寫入



客戶
憑證使用者



安控文件



金融機構
註冊中心(RA)

金融憑證服務概述-服務內容說明



金融電子憑證 申請

提供PublicCA以及
FXML憑證申請

依照憑證申請張數
訂定級距價格

客戶根據申請憑證
張數計費

RA系統 標準化服務

憑證申請

憑證展期

憑證註銷

憑證暫禁 / 解禁

憑證證明單提供

憑證查詢

憑證下載

憑證應用 客製化服務

憑證操作流程修改

客製憑證操作畫面

其他相關需求
(例如：安控元件)

產品特色



可簽發多年效期的用戶憑證及註冊中心RA憑證

支援軟體憑證規格

支援硬體載具發卡

提供CRL/OCSP認證模式





金融憑證擴大推廣方案優惠包裝

PublicCA 個人憑證

單位：元/張

單位 (萬張)	牌價	優惠價
0~1	100	85
1~2	80	62
2~5	70	50
5~10	60	40
10~15	50	32
15~20	40	25
20以上	專案	專案

FXML 法人憑證

單位：元/張

單位 (千張)	牌價	優惠價
0~0.1	1000	900
0.1~0.3	950	850
0.3~1	900	800
1~2	850	800
2~3	800	750
3~5	750	700
5以上	專案	專案

憑證費用採預付制，
每次應付金額以實際簽發數量乘以單張金額計算，
最長於**五年內**需使用完畢。

RA系統標準化服務(不含硬體)

單位：元

服務費率

\$500,000

憑證應用客製化服務

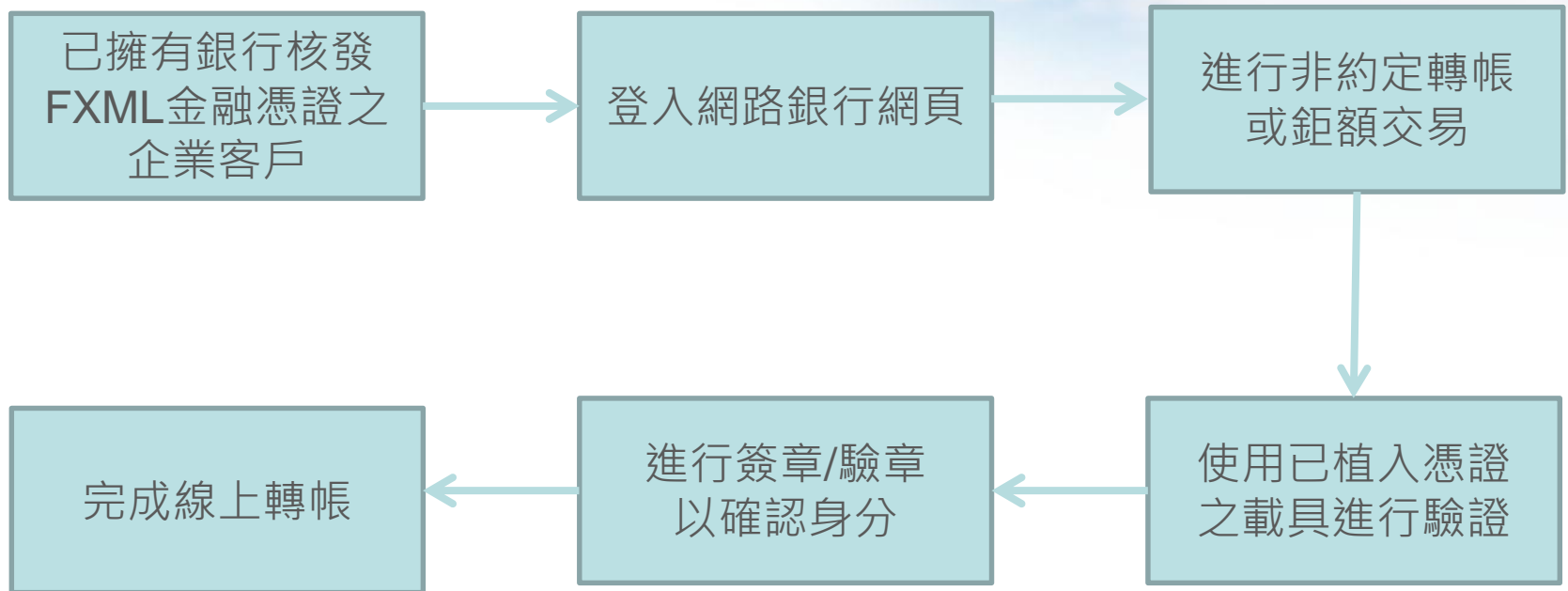
單位：元/人日

服務費率

專案報價 (每人日以10000元計)

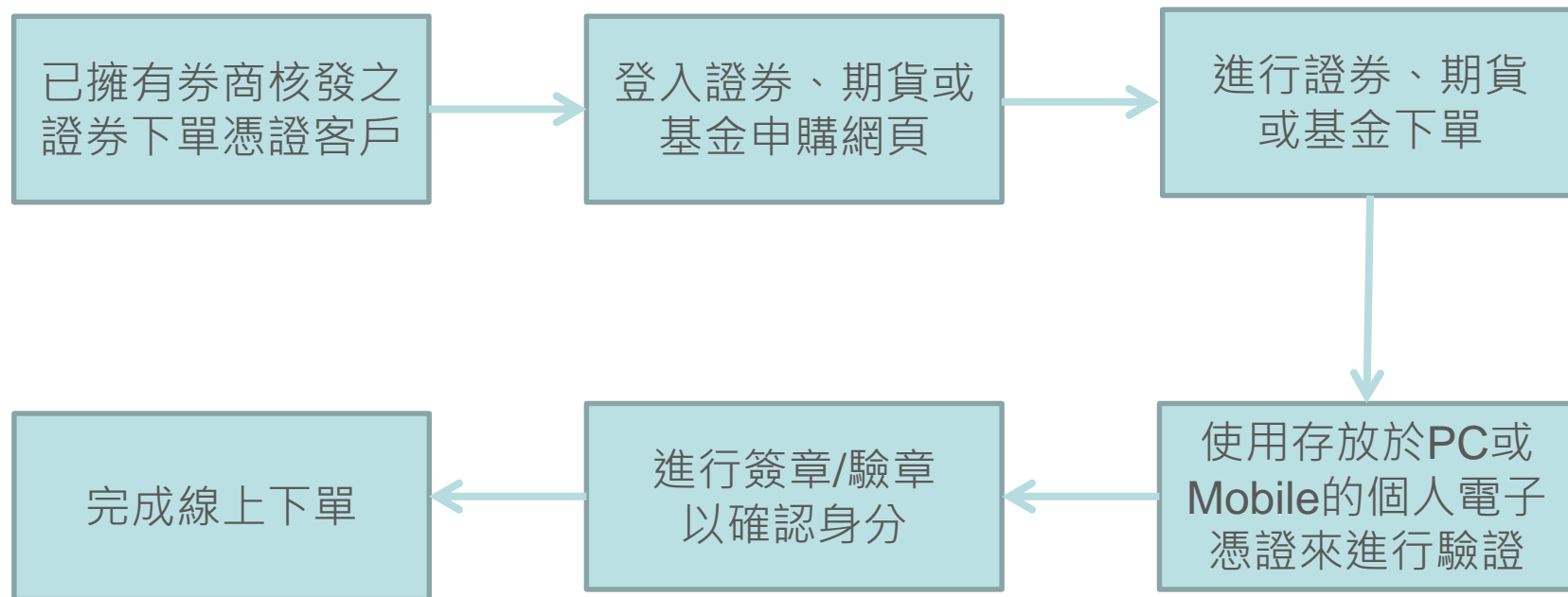
銀行FXML憑證應用情境

■ 以網路銀行轉帳交易為例



PublicCA個人憑證應用情境

■ 證券業：證券、期貨及基金電子下單



■ 保險業：線上電子保單

■ 其他：金融3.0 線上開戶應用、年度網路報稅。

成功案例

金融憑證客戶群

銀行FUCA

中國信託銀行
元大銀行
瑞穗商銀
星展銀行

企業PublicCA

大昌證券
大眾證券
中國信託綜合證券
元大證券
台新證券
兆豐證券
國泰證券
新光證券
群益金鼎證券
其他企業

成功案例 – 中O信託銀行



金融業
(中O信託銀行)



- ◎使用產品：金融憑證
 - ◎採購數量：20,00張
 - ◎營收金額：140萬/1年
- 衍生商機：105年委由本公司協助建立上海分行之金融憑證安控系統，系統建置金額約60萬，後續將再帶入憑證張數營收

5 業務應用

- ◎轉帳、跨行交易等線上銀行業務

4 成案關鍵因素

1. 與銀行公會建立良好關係，銀行公會引薦本公司給所屬會員
2. 了解客戶現況與需求，提供金融PKI相關產品及建議，技術能力獲得客戶認可與信賴
3. 掌握安控系統升級需求並提供透明的憑證採購級距價格

3 行銷話術

1. 本公司已取得合法之FUCA資格
2. 憑證價格依照購買憑證張數級距定價，價格透明
3. 具備政府/軍用/商用PKI、自然人憑證、工商憑證等多年政府經驗，產品及技術能力獲政府信任

2 客戶現況/痛點

原憑證服務廠商為TWCA

1. 原廠商逐年調漲憑證價格，造成客戶不滿
2. 服務態度不佳，無法符合客戶需求

1 選定行業別

◎金融業

成功案例 – 大昌證券



證券業
(大昌證券)



- ◎ 使用產品：PublicCA憑證
- ◎ 採購數量：20,000張
- ◎ 營收金額：50萬/1年

5 業務
應用

- ◎ 網路下單

4 成案
關鍵
因素

- ◎ 通路AM客戶關係與證券董事長(券商公會理事長)直接介紹
善加利用既有廠商(大州資訊)，提供優惠價格

3 行銷
話術

- ◎ 提出憑證費用歸戶計算並接受一次下單逐用付款收費模式

2 客戶
現況/
痛點

- ◎ 原憑證服務廠商為TWCA
 1. 原廠商逐年調漲憑證價格，造成客戶不滿
 2. 服務態度不佳，無法符合客戶需求

1 選定
行業別

◎ 證券業



*Value Creator for
Investors, Customers, Employees, and Society*

敬請指教！



網站偵防隊

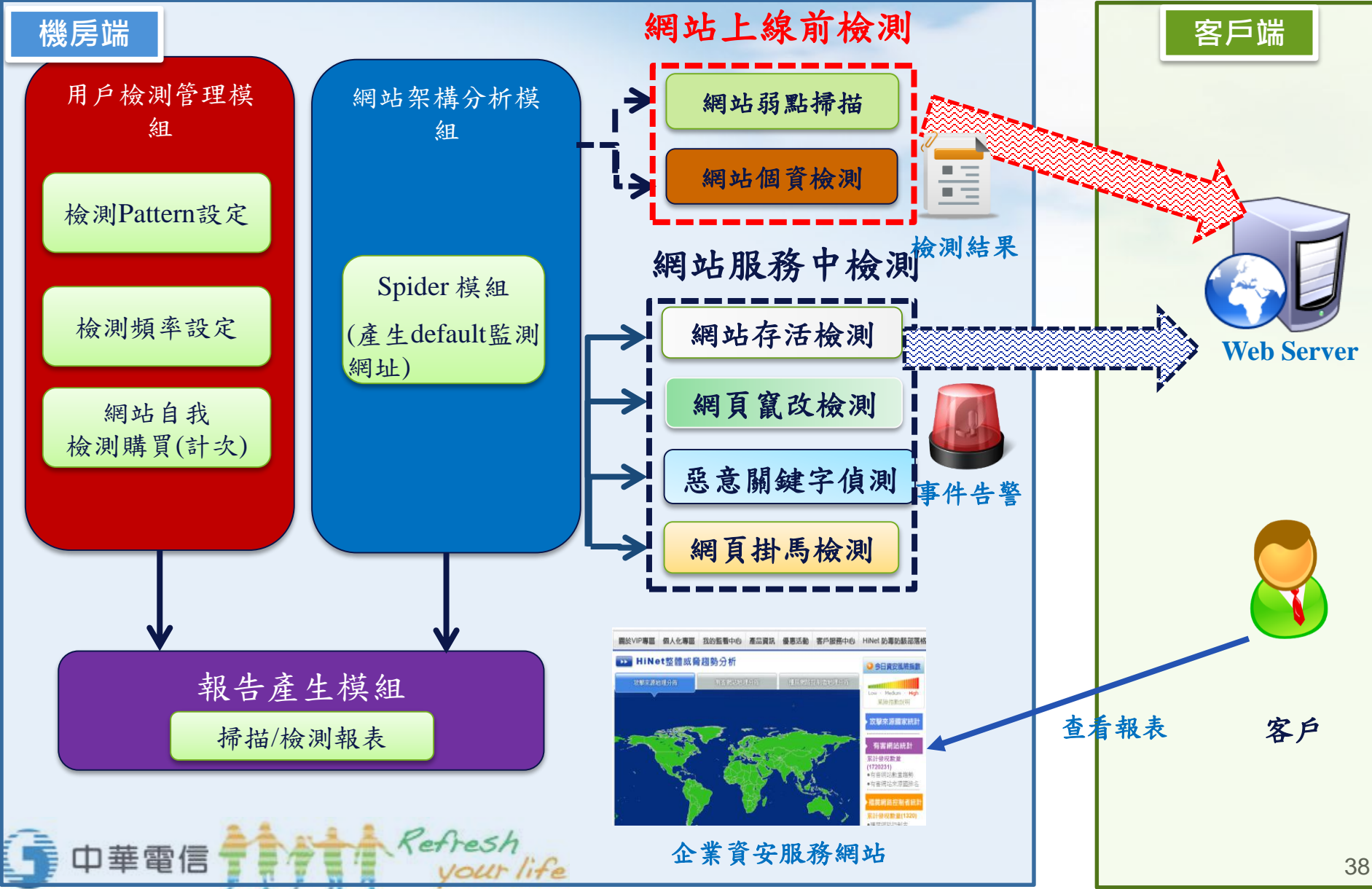
■ 概述

- ▶ 網站偵防隊以**雲端掃描**的方式，對客戶網站進行弱點掃描、個資檢測、掛馬檢測、網站存活檢測、網頁竄改檢測等
- ▶ 提供定期檢測及手動檢測，檢測完畢後主動寄送報表通知
- ▶ 不需要額外安裝軟體，只需要**提供URL**，即可使用服務
- ▶ 只要一般使用者可以連上的網站皆可服務

■ Standard版提供以下功能：

- ▶ 網站存活檢測（每20分鐘1次）
- ▶ 網頁弱點掃描（每月1次、手動2次）
- ▶ 網頁掛馬檢測（每天1次）

網站偵防隊服務架構



機房端

用戶檢測管理模組

檢測Pattern設定

檢測頻率設定

網站自我檢測購買(計次)

網站架構分析模組

Spider 模組
(產生default監測網址)

網站上線前檢測

網站弱點掃描

網站個資檢測

網站服務中檢測

網站存活檢測

網頁竄改檢測

惡意關鍵字偵測

網頁掛馬檢測

報告產生模組

掃描/檢測報表

客戶端



Web Server

檢測結果



事件告警

查看報表



客戶



企業資安服務網站

敬請指教