

SSL憑證與網路資安

Tim

認識 SSL憑證



加密保護



數位證書

為什麼 我們需要



最實惠的防護

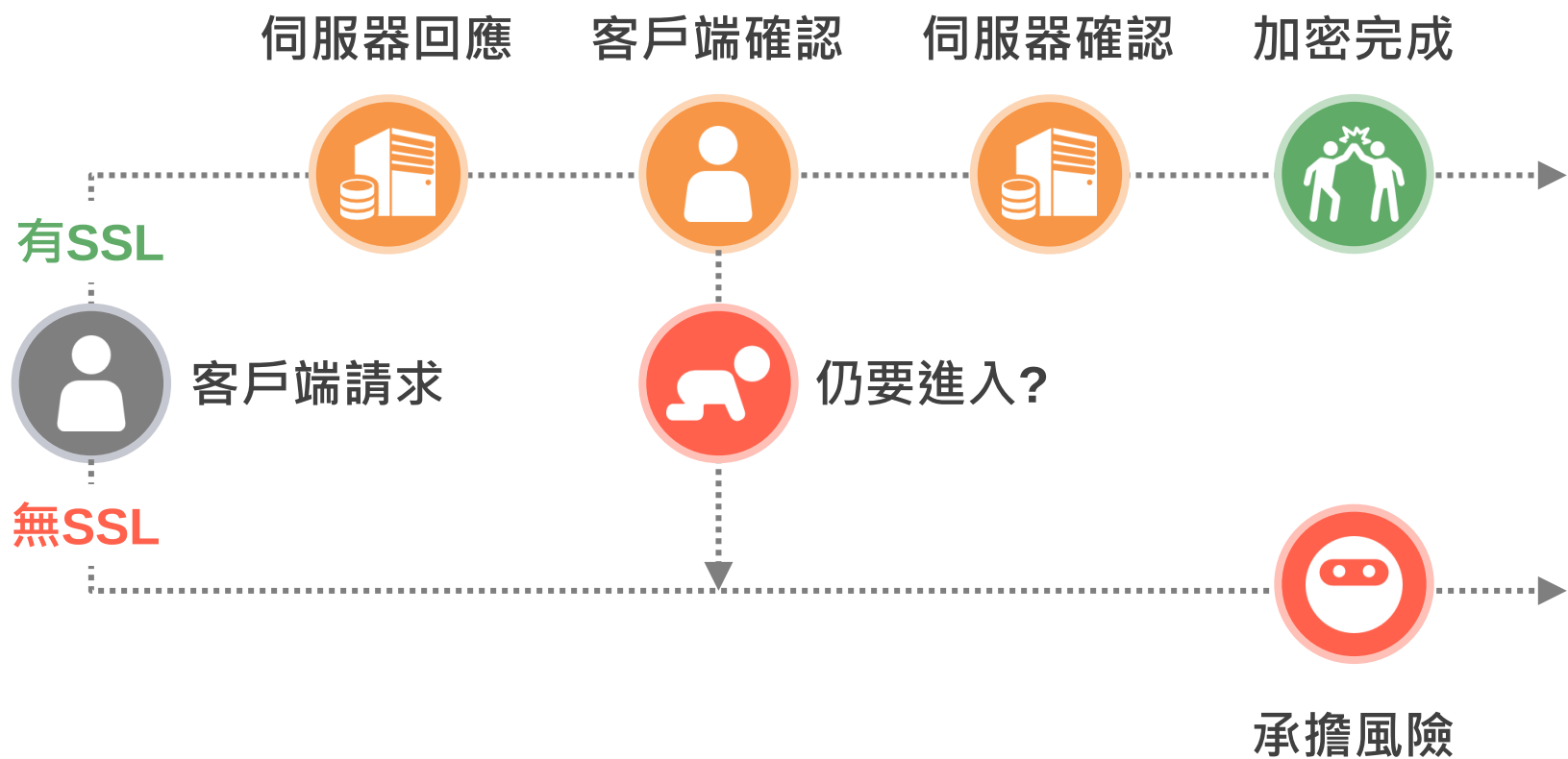


最高昂的代價



都是為了被看見

圖解 如何運作



安全協定 SSL & TLS

1994



Netscape
SSL 1.0

1996



SSL 3.0

1999



IETF
TLS 1.0

2018



TLS 1.3

近期大事記

2017.01



開始標示
不安全

2018.03



最高年限
縮減為2年

2018.07



不安全圖示
更明顯

2018.09



簡化
安全圖示

Current (Chrome 67)

 Secure | example.com

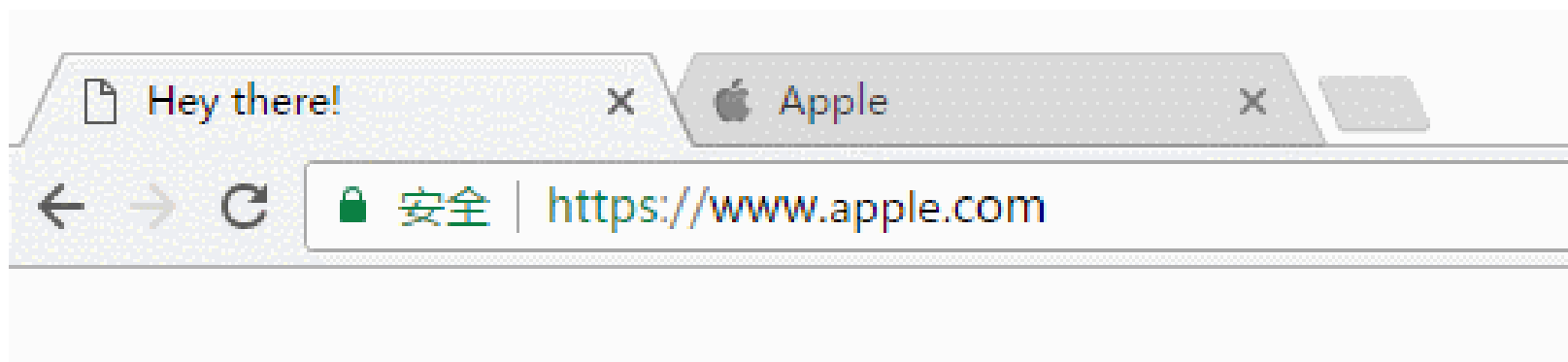
Sep. 2018 (Chrome 69)

 example.com

Eventually

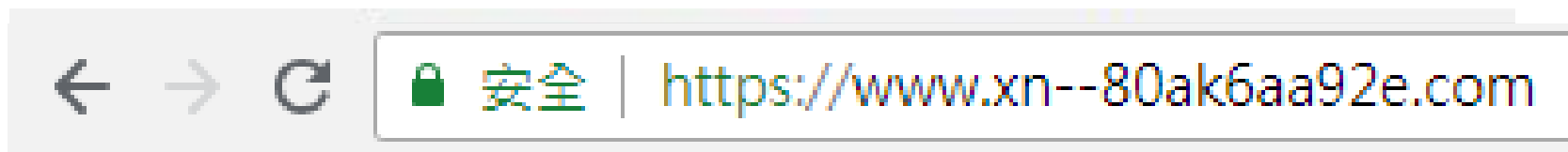
example.com

案例1 以假亂真



說明 眼見不一定為憑

IDN(Internationalized Domain Name)



說明 眼見不一定為憑

如果網站管理者本身就是**不法份子**，

那麼網站**加密**與否有差別嗎？

第十二屆域名研討會來啦！

我們一年一度的域名研討會將於10月舉行，涵蓋了**域名應**
GDPR隱私保護等相關議題，一次瞭解與您切身相關的重

台北場：2018/10/11, 集思交通部國際會議中心3樓

台中場：2018/10/16, CMoney中區教育訓練中心

高雄場：2018/10/18, 高雄高鐵站前訓練中心

立即報名

問題1 SSL與SEO的糾葛

安裝之後排名倒退了!?

效果多大?

網站變慢?

選擇 適合自己的憑證



保護對象



驗證方式

區分 保護對象

單域名 (Single)

www.net-chinese.com.tw
net-chinese.com.tw

通用型 (Wildcard)

net-chinese.com.tw
ssl.net-chinese.com.tw

⋮

多域名 (Multi , UCC/SAN)

net-chinese.com.tw
netc.asia

⋮

區分 驗證方式

EV(延伸驗證)



Net Chinese Co., Ltd. [TW]

OV(組織驗證)

DV(域名驗證)



種類 有哪些選擇？

	單域名 (Single)	通用型 (Wildcard)	多域名 (Multi)
DV(域名驗證)			
OV(組織驗證)			
EV(延伸驗證)			

案例2 我有好多個網站

1

一張多域名 (Multi) 憑證

2

多張單域名 (Single) 憑證

選項1 一張多域名憑證

優

管理方便

缺

成本較高，彈性較低

選項2 多張單域名憑證

優

成本較低，彈性較高

缺

管理不易

問題

沒有獨立IP怎麼辦

Server Name Indication (SNI)

管理員的好幫手

雙方版本支援、手動設定

問題2 付費 vs. 免費

優點

付費SSL

1. 可信度高
2. 理賠機制
3. 憑證標章
4. 售前、售後協助

缺點

1. 有成本
2. 手動續用

免費SSL

1. 幾乎沒有成本
2. 自動續用

1. 風險自負
2. 產品種類不齊

問題3 免費憑證的疑慮

1

過度濫用

2

認知不足

問題4 付費的一定好？

1

2015年處罰Symantec

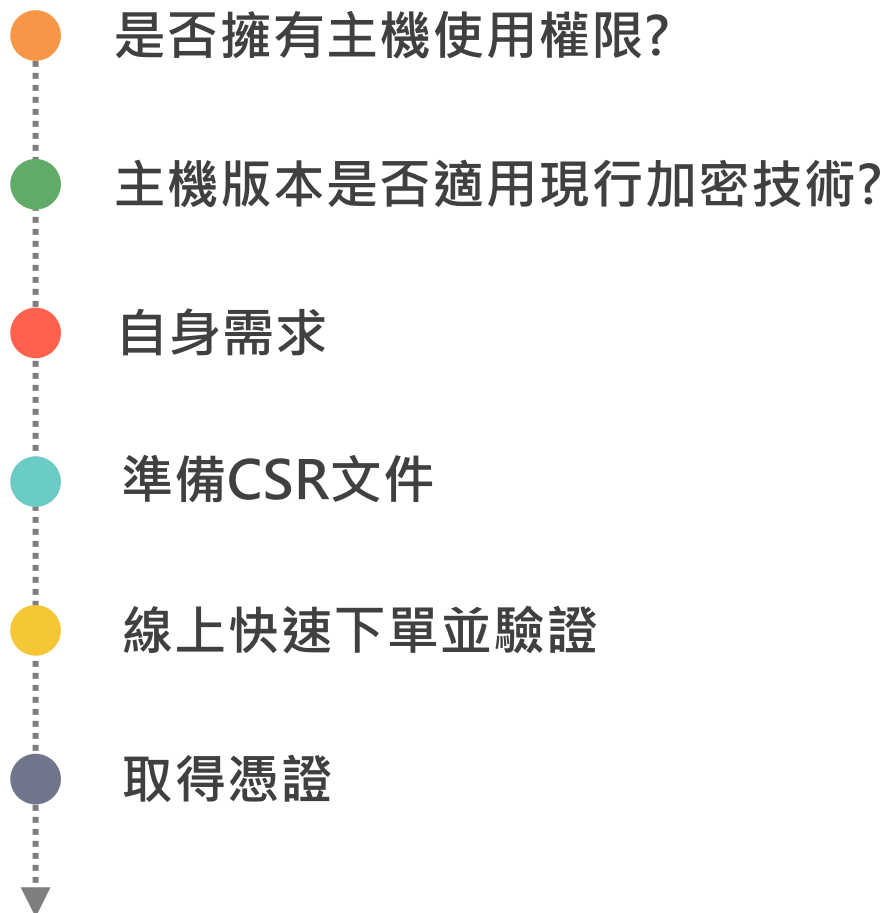


2

2017年封殺沃通(Wosign)



申請流程 找到理想的憑證



未來趨勢

1

使用持續普及

2

力道持續加強

3

觀念持續進步