

# Lotus knows.

Smarter software for a Smarter Planet.

## Notes/Domino 安全性考量及設定

沈偉 | IBM 高級軟體工程師



lotusknows.com

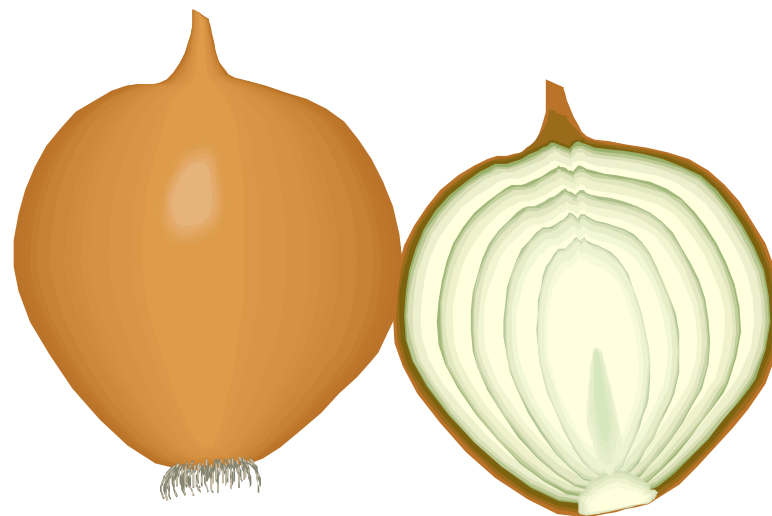
## 議程



- Notes/Domino 安全概述
  - ▶ 安全準則
  - ▶ Notes/Domino 安全
  - ▶ 驗證字和用戶 ID
  - ▶ Notes/Domino 的存取控制
- Notes/Domino 安全技術
- Notes/Domino 安全配置
- Notes/Domino 安全 --- 方法論

## Notes/Domino 安全概述 - 安全準則

- 物理安全
- 作業系統安全
- 網路安全
- Domino 域安全
- Domino 伺服器安全
- ID 安全
- 資料庫安全
- 表單 / 檔案安全
- 欄位安全

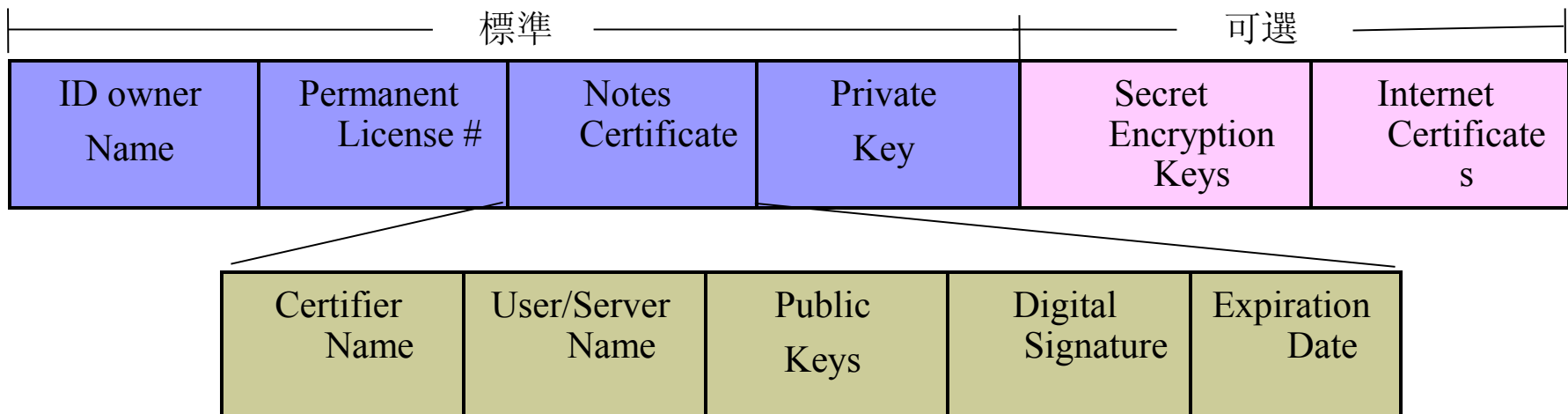


## Notes/Domino 安全概述 - Notes/Domino 安全

- 認證 - 驗證用戶的身份
  - ▶ 匿名
  - ▶ 用戶名稱 / 密碼
  - ▶ 驗證字
  - ▶ 數位憑證
  
- 許可權 - 確定用戶的存取權限
  - ▶ 7 層 ACL
  
- 加密 - 保障資料的安全傳輸
  - ▶ 消息、檔案、欄位、埠、本地資料
  - ▶ RSA 加密

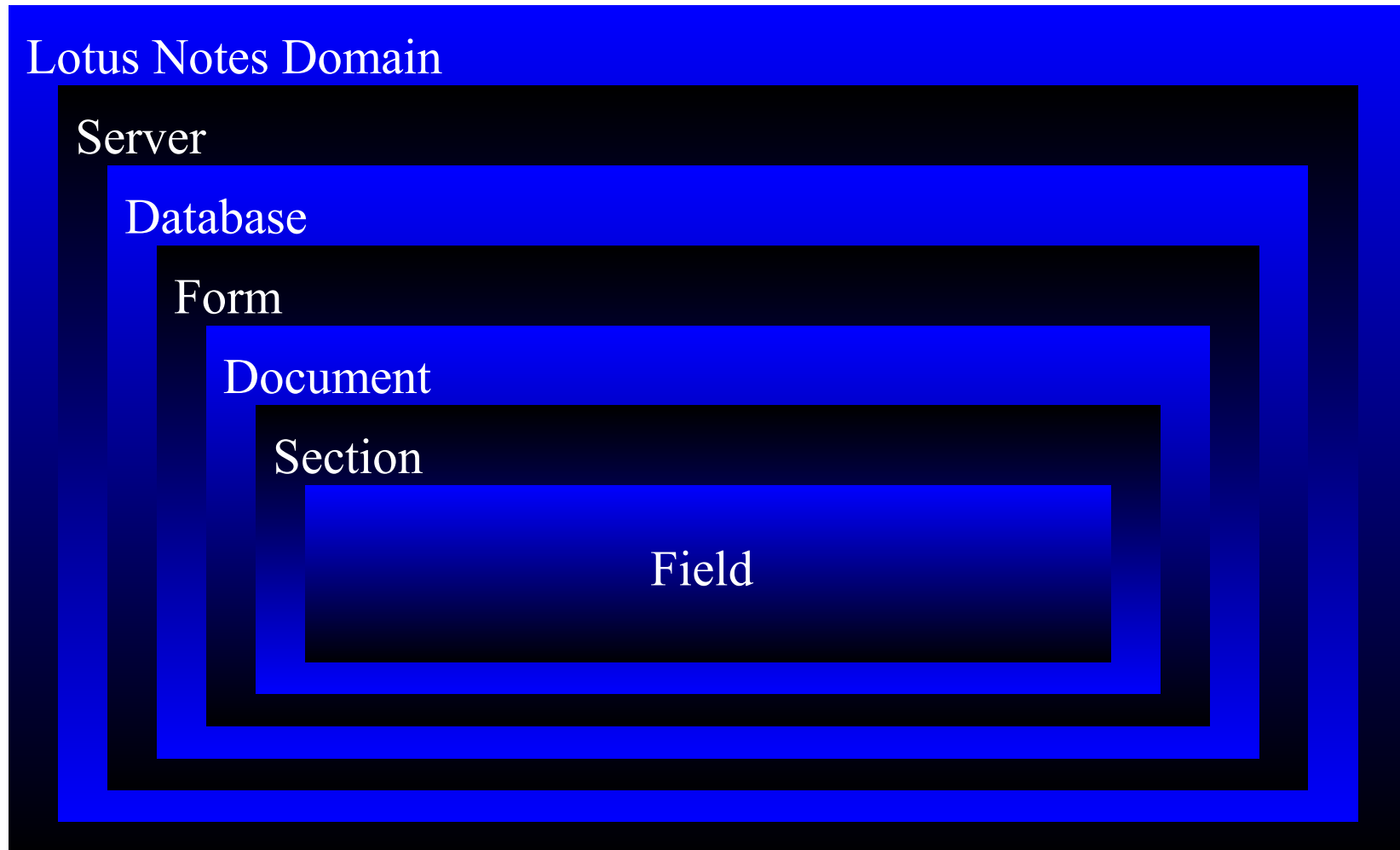
## Notes/Domino 安全概述 - 驗證字和用戶 ID

- Notes ID 包含使用者的簡要資訊，並包含必要的 RSA 金鑰對和 RC2/RC4 金鑰信息。這些 ID 是被密碼保護的。
- 使用者 ID 資訊：



- 1 RC2/RC4 金鑰資訊通過應用開發人員分發，允許對檔案中的欄位進行加密 / 解密

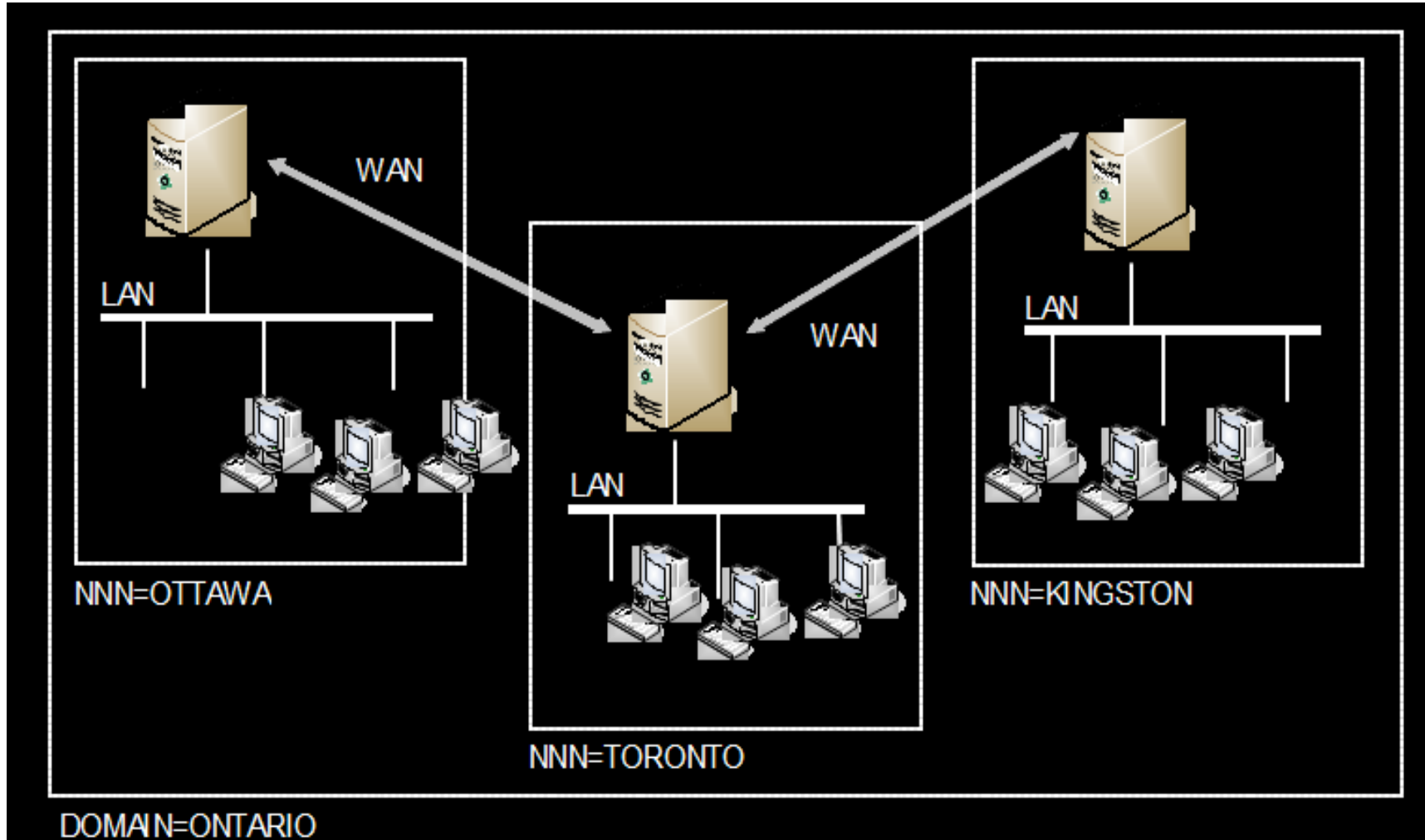
## Notes / Domino 的存取控制 - 概覽



## Notes/Domino 的存取控制 - Domino 域

- 在 Notes 安全中，域是一組伺服器 and 用戶端的集合，他們處在同一個管理架構下，因此共用主要的配置資訊，比如使用者和群組的定義
- Domino 域安全包括伺服器，工作站和證書的物理和邏輯訪問

## Notes/Domino 的存取控制 - 域





## Notes/Domino 的存取控制 - 伺服器

- 公共通訊錄中的伺服器檔案可以用於控制對 Notes 伺服器檔案的訪問。
- 伺服器存取控制：
  - ▶ 允許訪問伺服器的用戶列表
  - ▶ 訪問伺服器
  - ▶ 不能訪問伺服器
  - ▶ 創建新資料庫
  - ▶ 創建副本資料庫
  - ▶ 訪問伺服器 (中繼)
  - ▶ 傳遞途經 (中繼)
  - ▶ 電話呼叫原因 (中繼)
  - ▶ 允許的目標 (中繼)

| Server Access                 | Who can -  |
|-------------------------------|--|
| Access server:                | */IBM<br>*/Lotus<br>*/Tivoli Systems<br>*/ITV<br>MCO Capacity Monitors<br>D23Mail Divestiture Access Group |
| Not access server:            | Terminations<br>GWA_Production_Server_NoAccess<br>Webmail Basic Users                                      |
| Create databases & templates: | */N/IBM<br>*/H/IBM<br>D23 Admins<br>LocalDomainServers<br>D23 Admins_AU                                    |
| Create new replicas:          | */N/IBM<br>*/H/IBM<br>D23 Admins<br>LocalDomainServers<br>D23 Admins_AU                                    |
| Create master templates:      |  |
| Allowed to use monitors:      | *  |
| Not allowed to use monitors:  |  |

## Notes/Domino 的存取控制 - 資料庫

- 每個資料庫都有 **ACL** 控制使用者、伺服器 and 群組的存取權限
- 存取權限：
  - ▶ 管理者
  - ▶ 設計者
  - ▶ 編輯者
  - ▶ 作者
  - ▶ 讀者
  - ▶ 存放者
  - ▶ 不能存取者
- 可以使用 **Notes ID** 對資料庫進行加密

## Notes/Domino 的存取控制 - 表單

- 表單缺省的讀 / 創建檔案許可權
- 表單安全選項：
  - ▶ 誰可以讀取用該表單創建的檔案許可權
  - ▶ 誰可以用這個表單創建檔案
  - ▶ 加密金鑰
  - ▶ 禁止拷貝和列印
- 加密金鑰由管理員來創建並分發給相關的人員

Form

Default read access for documents created with this form

All readers and above

OtherDomainServers  
D23BKO11/23/A/IBM  
d23m0016/23/M/IBM

Who can create documents with this form

All authors and above

OtherDomainServers  
D23BKO11/23/A/IBM  
d23m0016/23/M/IBM

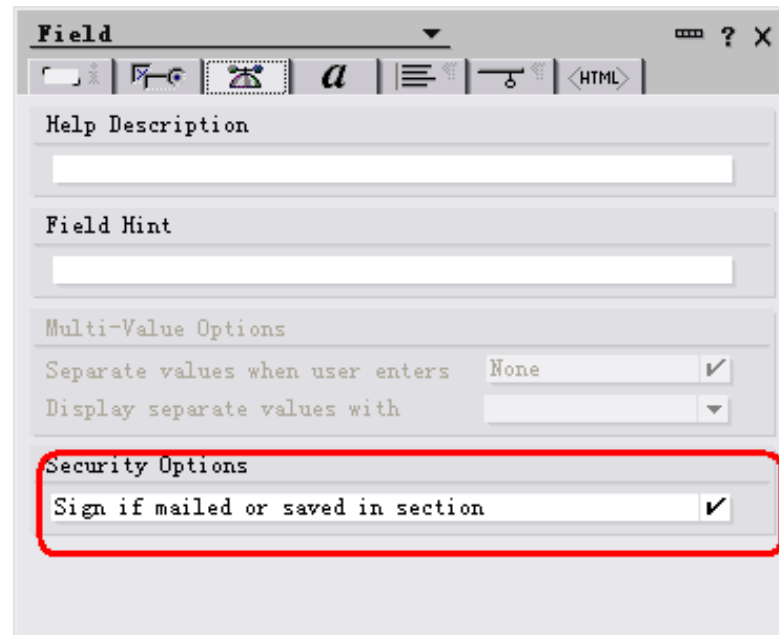
Default encryption keys

Disable printing/forwarding/copying to clipboard

Available to Public Access users

## Notes/Domino 的存取控制 - 檔案

- 檔案可以通過特定類型的欄位進行存取權限的控制
- 特定的欄位：
  - ▶ 讀者域：誰可以讀取文檔
  - ▶ 作者域：誰可以編輯文檔
  - ▶ 簽名域：用於附加數位簽章
- 如果表單中沒有一個簽名域，則檔案不能進行數位簽章

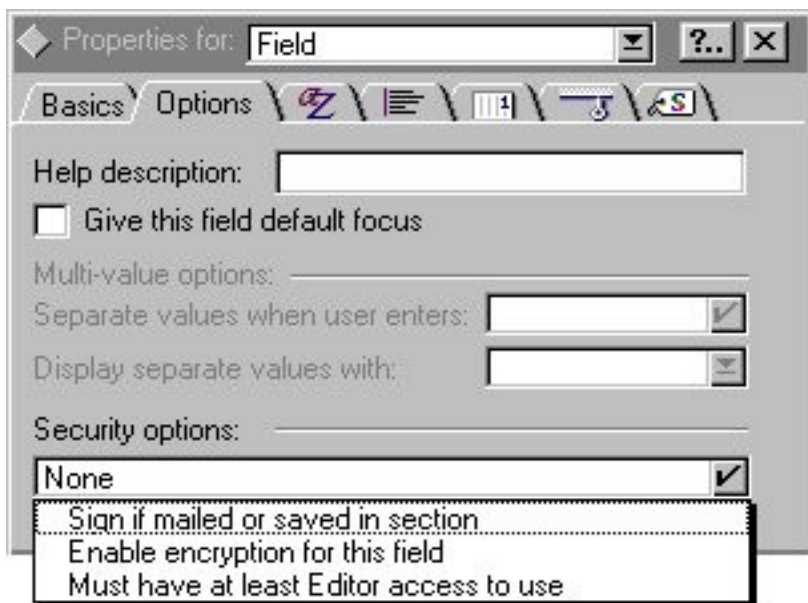


The screenshot shows the 'Field' properties dialog box in Lotus Notes. The 'Security Options' section is highlighted with a red box, indicating the 'Sign if mailed or saved in section' checkbox is checked. Other sections visible include 'Help Description', 'Field Hint', and 'Multi-Value Options'.

| Section             | Option                             | Value | Checked                             |
|---------------------|------------------------------------|-------|-------------------------------------|
| Multi-Value Options | Separate values when user enters   | None  | <input checked="" type="checkbox"/> |
|                     | Display separate values with       |       | <input type="checkbox"/>            |
| Security Options    | Sign if mailed or saved in section |       | <input checked="" type="checkbox"/> |

## Notes/Domino 的存取控制 - 區段和欄位

區段可以通過公式來進行存取權限的控制



欄位可以啟用加密

## 議程

- 1、 Notes/Domino 安全模型
- 2、 Notes/Domino 安全技術
  - ▶ 數位簽章
  - ▶ 公開金鑰架構 (PKI)
- 3、 Notes/Domino 安全配置
- 4、 Notes/Domino 安全方法論

## Notes/Domino 安全技術

- 數位簽章
- 公開金鑰架構 (PKI)
  - ▶ 安全通訊端層 (SSL) & 傳輸層安全 (TLS)
  - ▶ 安全多用途的網際郵件擴充協議 (S/MIME)
  - ▶ 證書註銷列表 (CRL)
  - ▶ 線上證書狀態協定 (OCSP)

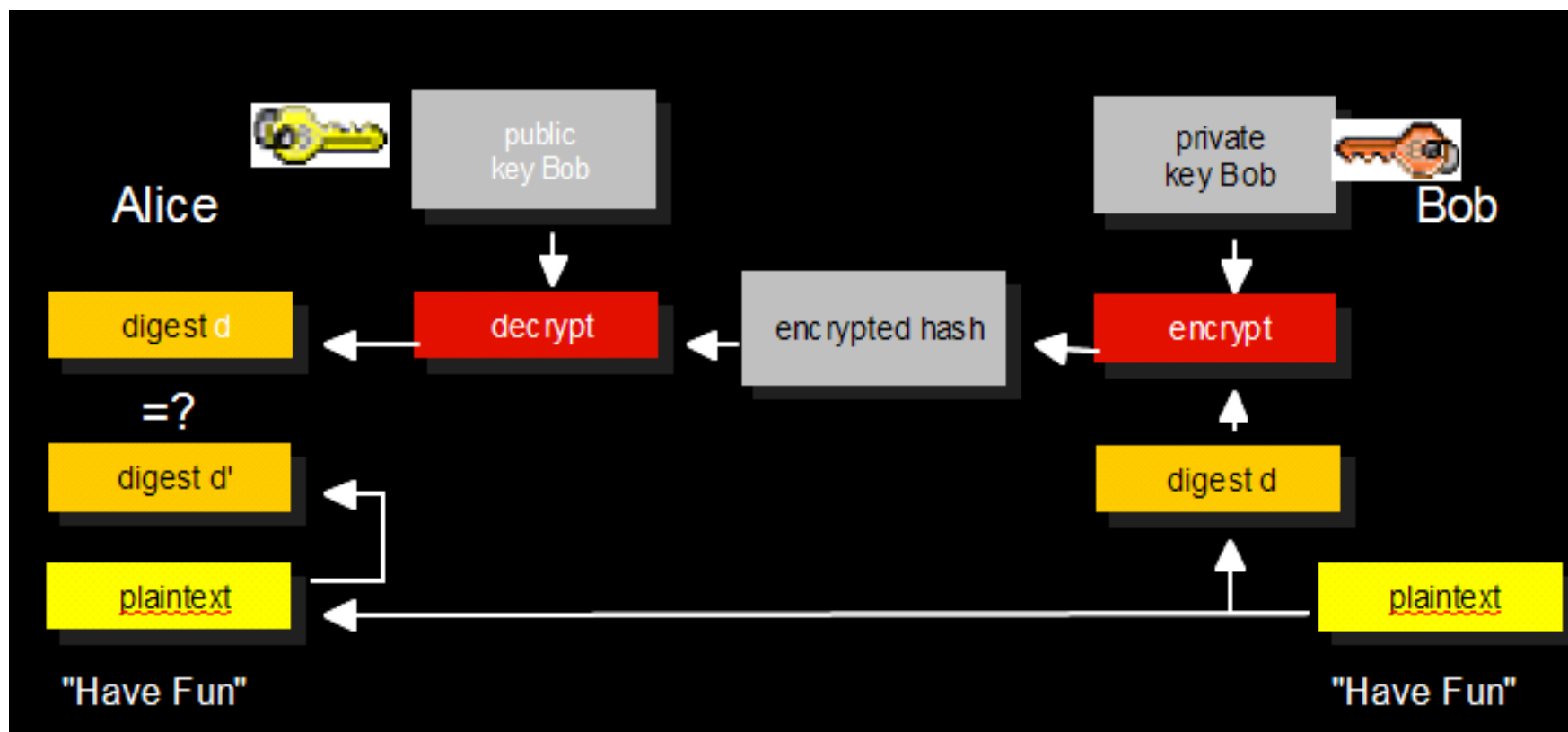
## Notes/Domino 安全技術 - 數位簽章是什麼？

- 數位簽章提供完整性，真實性和防止篡改
- 數位簽章使用 Hash 演算法（稱為單向函數）：
  - ▶ MD2 (RFC 1319) 和 MD5 (RFC1321): 128 bit
  - ▶ SHA-1 (NSA; FIPS 180-1): 160 bit
- 數位簽章可以對私密金鑰摘要資訊進行加密



## Notes/Domino 安全技術 - 數位簽章樣例

- Bob 發送一個簽名的郵件給 Alice...
- ... 使用 Bob 的私密金鑰進行數位簽章 ,Alice 使用 Bob 的公開金鑰進行數位簽章的驗證



## Notes/Domino 安全技術 - 什麼是 PKI?

- **PKI ( Public Key Infrastructure )** 即 " 公開金鑰基礎設施 "，是一種遵循既定標準的金鑰管理 平臺，它能夠為所有網路應用提供加密和數位簽章等密碼服務及所必需的金鑰和證書管理體系， 簡單來說， **PKI** 就是利用公開金鑰理論和技術建立的提供安全服務的基礎設施。 **PKI** 技術是資訊安全技術的核心，也是電子商務的關鍵和基礎技術。

## Notes/Domino 安全技術 - PKI 組件

### . Certification Authority

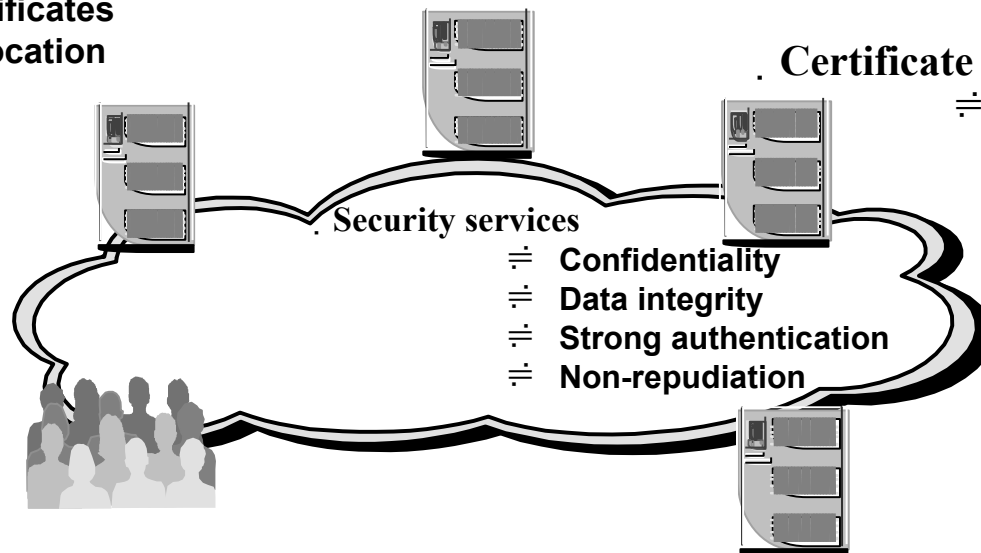
- ≡ Establishes policies, practices and controls
- ≡ Issues, revokes, suspends, renews certificate(s)

### . Directory

- ≡ Distributes certificates
- ≡ Distributes revocation status (opt)

### . Certificate Status Responder (opt)

- ≡ Distributes certificate status



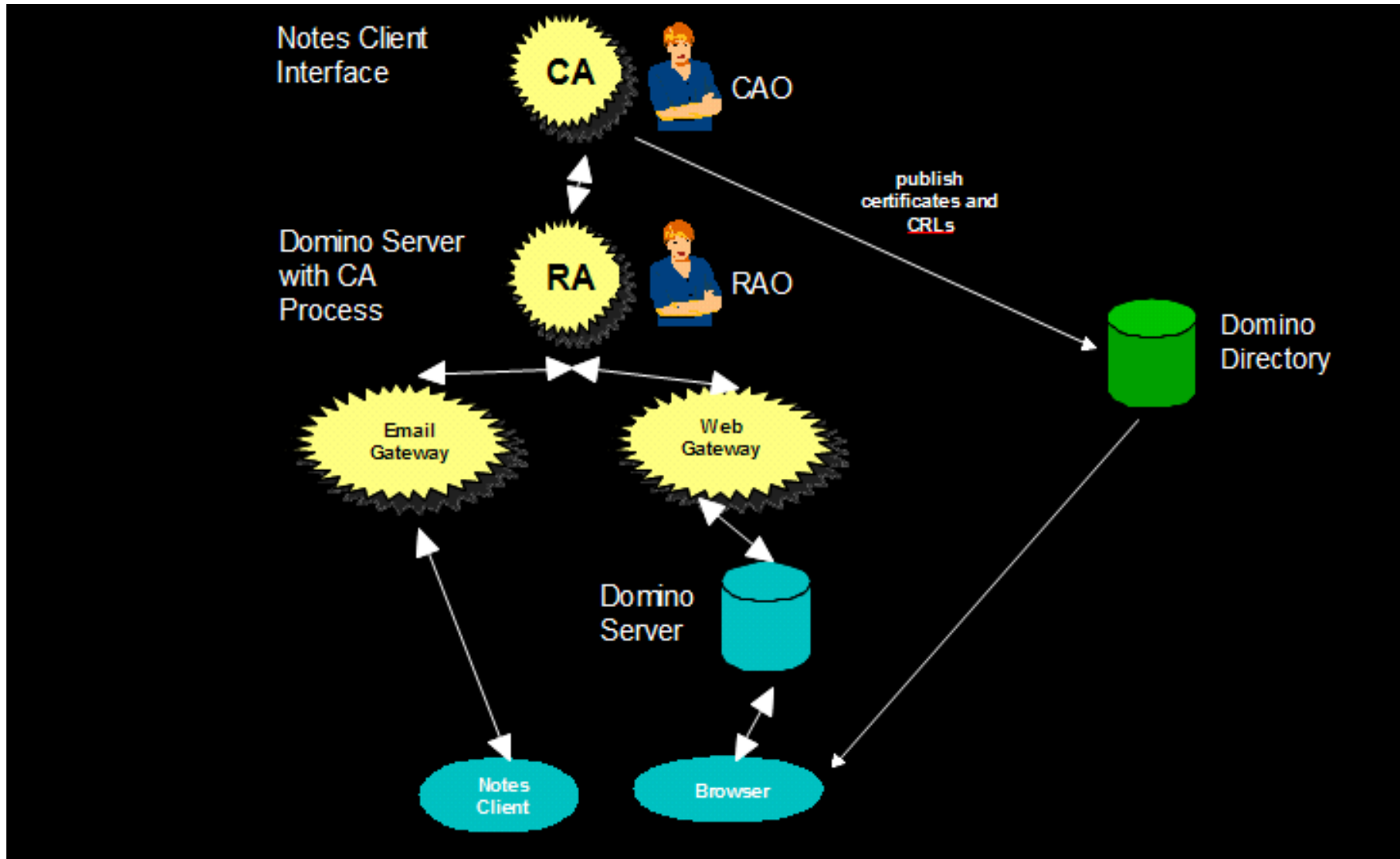
### . End-entities / Subscribing parties

- ≡ comply with policies
- ≡ use cryptographic services

### . Registration Authority

- ≡ Approves/rejects requests for certification of public keys
- ≡ Forwards user info to

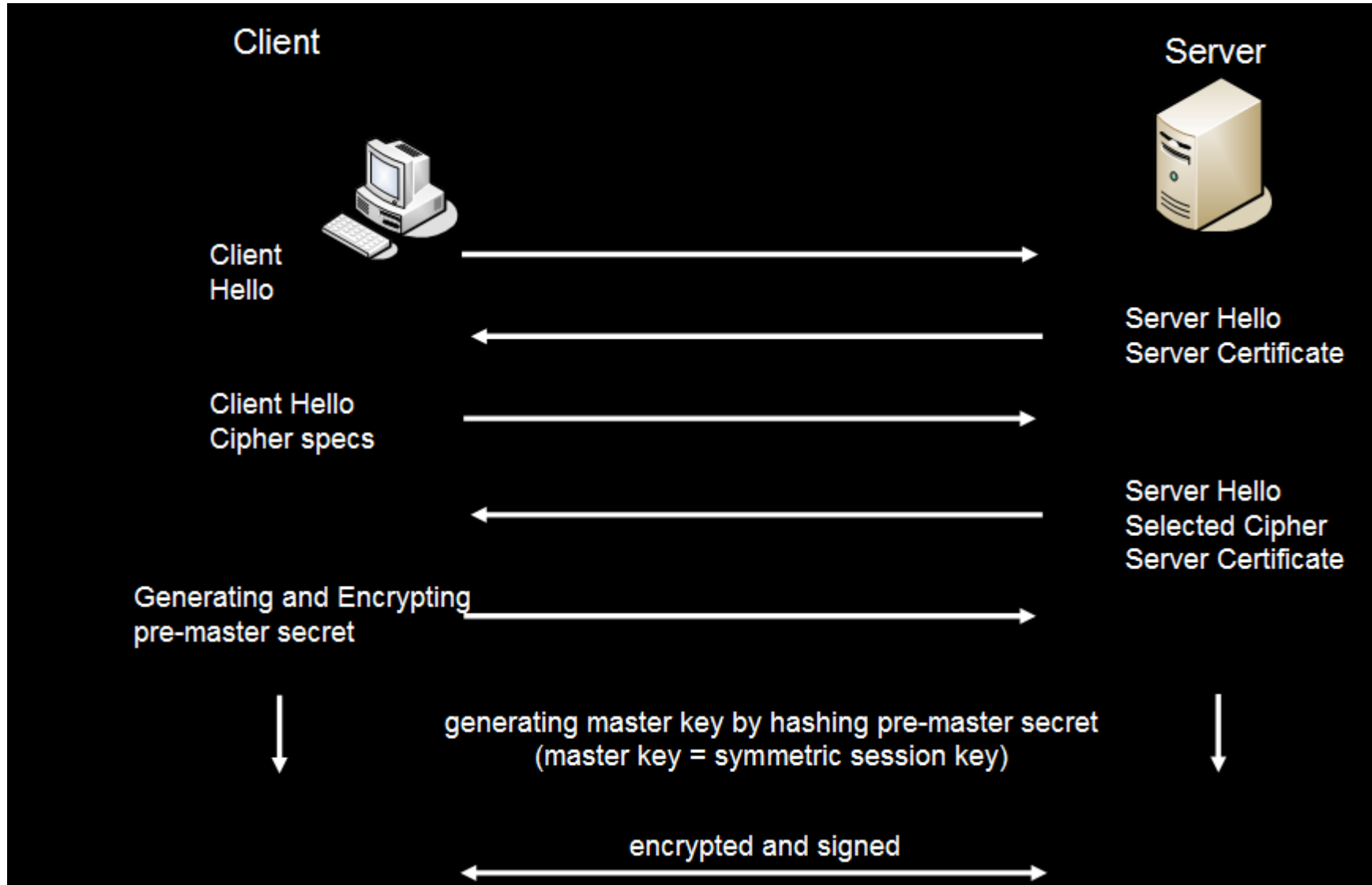
## Notes/Domino 安全技術 - PKI 組件 - Domino



## Notes/Domino 安全技術 - SSL & TLS

- Netscape 公司所研發的標準
- 支持 X.509v3 認證
- SSL 實現的安全目標：
  - ▶ 對網路上的資料進行加密
  - ▶ 通過簽名和校驗保障傳輸資料的完整性
  - ▶ 伺服器端的身分驗證 (SSLv2) 和用戶端的身分驗證 (SSLv3)
- 傳輸層安全 (TLS) 是在 SSLv3 增強的功能

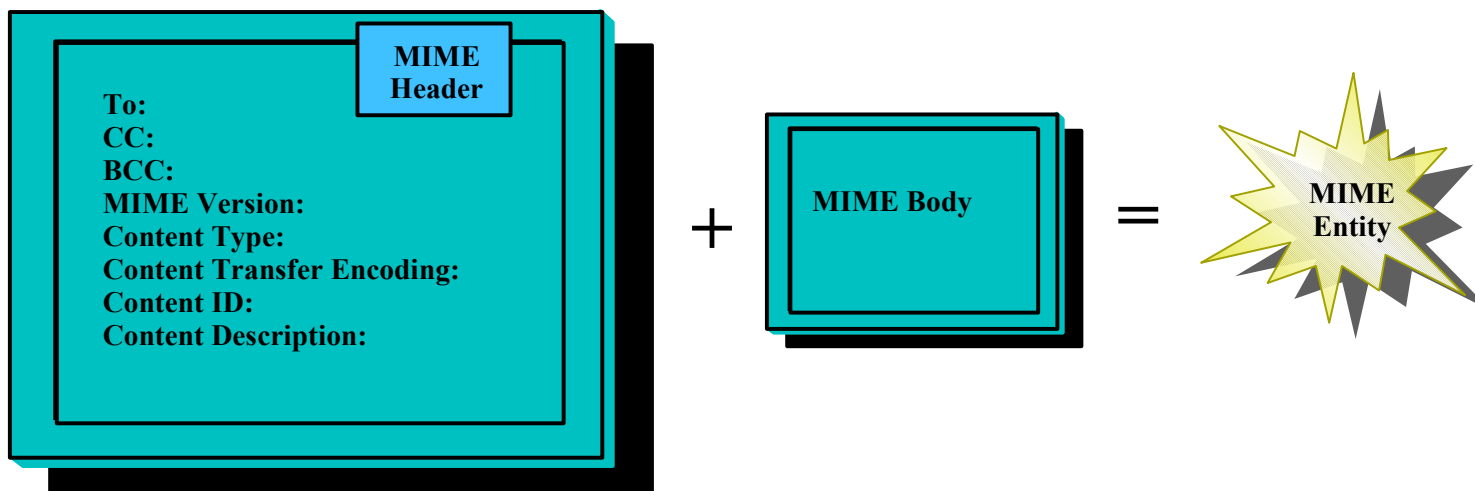
## Notes/Domino 安全技術 - SSL 握手過程



## Notes/Domino 安全技術 - S/MIME 是什麼？



- 安全多用途網際郵件擴充協議 (S/MIME)
- S/MIME 僅保護郵件的郵件主體，對頭部資訊則不進行加密，以便讓郵件成功地在發送者和接收者的開道之間傳遞。



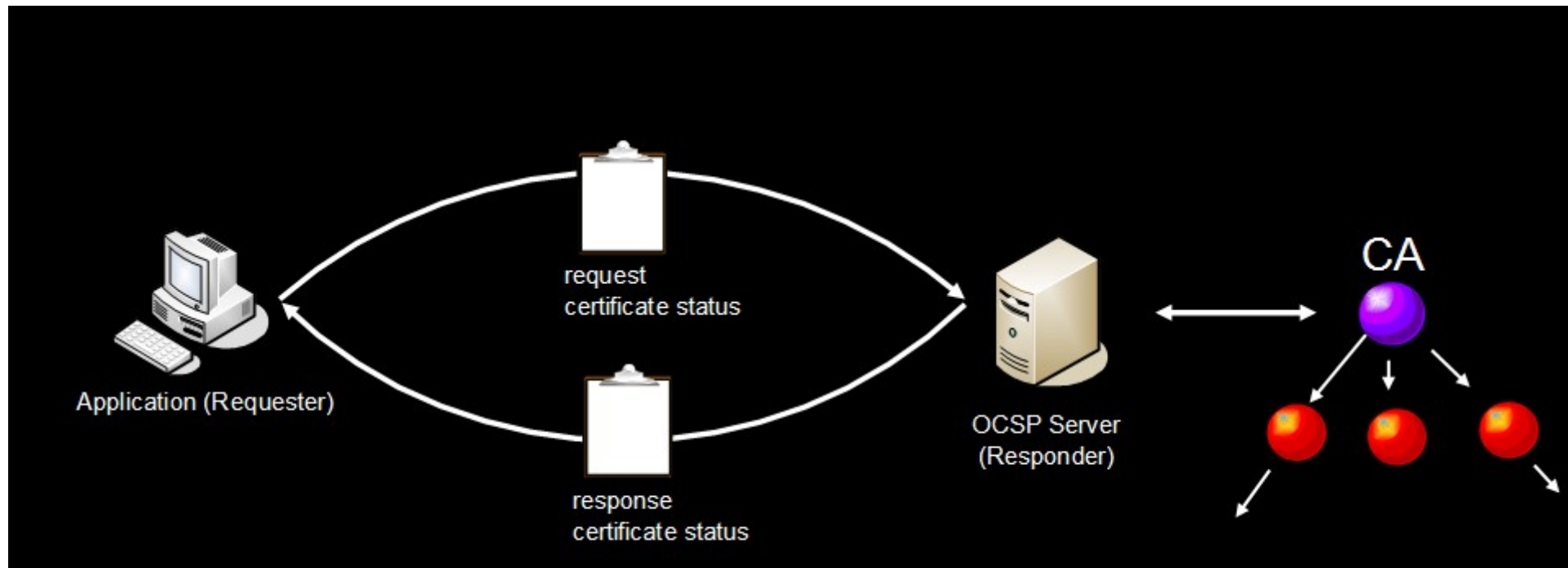
## Notes/Domino 安全技術 - 證書註銷列表 (CRL)

- CRL 是一個帶時間標記的清單，用以識別已吊銷的 Internet 證書，如屬於已離開的員工的證書。CA 進程發佈並維護每個 Internet 驗證者的 CRL。CRL 與驗證者關聯，由驗證者簽名，並駐留在驗證者的 ICL 資料庫中。
- CRL 有定期和非定期兩種類型。對於定期 CRL，應配置持續時間間隔（CRL 保持有效的時間段）以及發佈新 CRL 的時間間隔。每個驗證者都在指定的時間發佈 CRL，即使自從上一個 CRL 發佈以來尚未吊銷證書。也就是說，如果管理員吊銷了某個證書，該證書會出現在驗證者按計劃發佈的下一個 CRL 中。CRL 持續時間段應大於兩次 CRL 發佈之間的時間段。這樣可確保 CRL 保持有效。否則，CRL 可能在發佈新的 CRL 之前就到期。



## Notes/Domino 安全技術 - 線上證書狀態協定 (OCSP)

- OCSP:
  - ▶ 應用程式可以確定驗證的狀態
  - ▶ 定義回應端 (伺服器) 和請求端 (用戶端) 關於驗證狀態資料交換
- OCSP 回應:
  - ▶ 有效的證書, 撤銷證書, 未知證書



## 議程

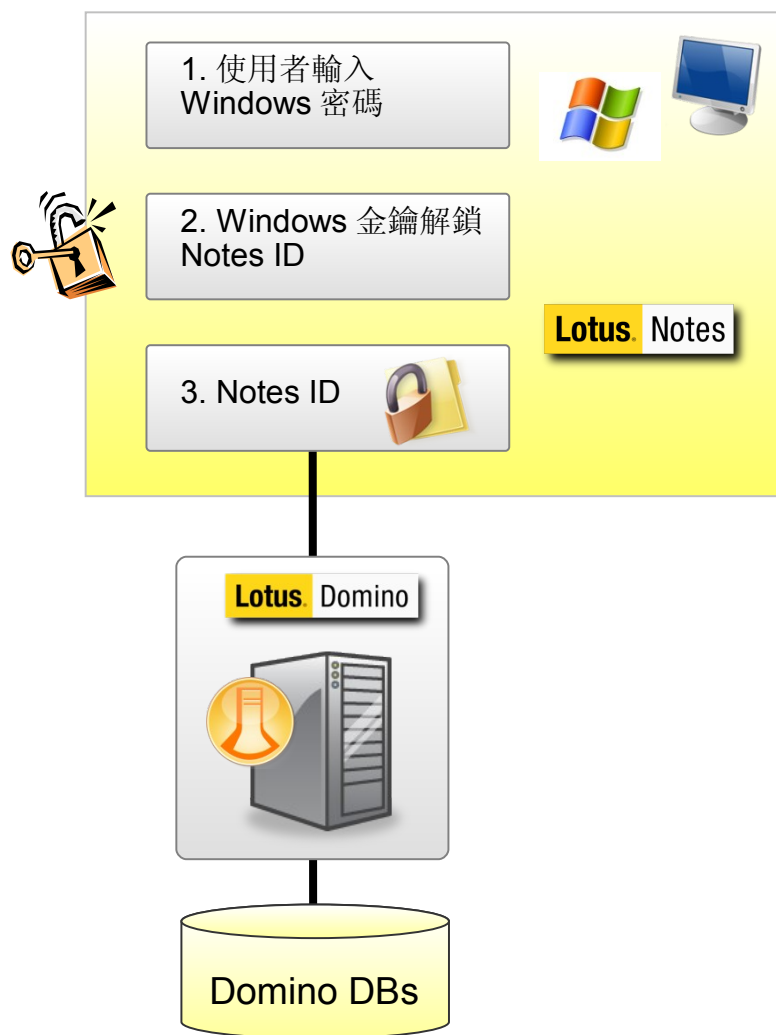


- 1、 Notes/Domino 安全模型
- 2、 Notes/Domino 安全技術
- 3、 Notes/Domino 安全配置
  - ▶ 單點登錄 / 共用登錄
  - ▶ 代理的安全性
  - ▶ Notes 用戶端 ECL 設置
  - ▶ 郵件加密和簽名設置
  - ▶ 本地資料庫加密
  - ▶ 驗證字回滾
  - ▶ OCSP 設置
  - ▶ Internet 密碼鎖定
  - ▶ Notes 識別字保險庫
  - ▶ xACL
  - ▶ 配置基於策略的管理
  - ▶ Domino 域監控 -- 安全探針
  - ▶ 防垃圾郵件設置
- 4、 Notes/Domino 安全 ---ISSL 方法論

## Notes/Domino 安全配置 - 單點登錄 / 共用登錄

- 共用登錄和單點登錄 = 用戶只需要登錄一次
  - ▶ 兩者的區別
    - 共用登錄 = Windows 和 Notes 安全認證的集成
    - 單點登錄 = 在 Domino Web 服務和其他 Web 伺服器之間的統一認證 (SSO 使用 LTPAToken2 可以增強系統的安全性)
  - ▶ 兩者相同的地方
    - 使用者只要記住一個密碼，並且只需要登錄一次。
  
- 共用登錄
  - ▶ AD/Windows 的使用者 credentials 資訊和 Notes ID 的密碼保持同步。
  - ▶ 通過協力廠商的工具進行同步集成

## Notes/Domino 安全配置 - 共用登錄



### 共用登錄 (Notes Shared Login)

- Windows 安全認證代替 Notes 的用戶名 / 密碼
- 無需 Notes 密碼即能啟動 Notes
- 沒有 Notes 密碼需要同步
- Notes ID 仍舊管理 Notes 的安全性
- 無需修改 Notes 密碼，只要需改 Windows 密碼

## Notes/Domino 安全配置 - 單點登錄 (SSO)

| Domain | Server       |
|--------|--------------|
| ▼ IBM  |              |
|        | atlpal07/ibm |
|        | atlpal08/ibm |
|        | atlpal09/ibm |

- Create Virtual Server
- Create URL Mapping/Redirection
- Create File Protection
- Create Realm
- View Current Configurations
- Create Web SSO Configuration**

### Web SSO Configuration for :

Basics<sup>2</sup> | Comments | Administration

#### Token Configuration

Configuration Name: 『LtpaToken』

Organization: 『』

DNS Domain: 『atl.ibm.com』

#### Participating Servers

Domino Server Names: 『atlpal07/ibm, atlpal08/ibm, atlpal09/ibm』

Save & Close | Keys... | Cancel

- Create Domino SSO Key
- Import WebSphere LTPA Keys**

Basics | Comments | Administration

#### Token Configuration

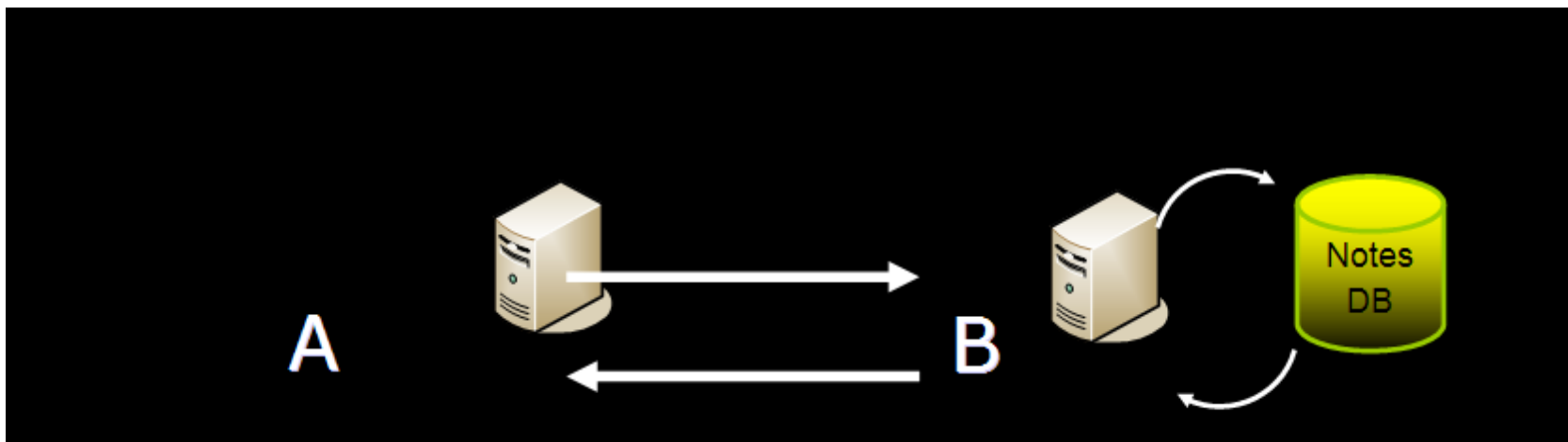
## Notes/Domino 安全配置 - 啟用 Notes 共用登錄

- 缺省情況下是禁用該功能。

The screenshot displays the 'Security Settings' console with the 'Notes Shared Login' section active. The 'Enable Notes shared login with operating system' setting is currently set to 'No'. Below this, the 'Allow User Changes?' option is set to 'No'. The 'Activation Notification' section shows 'How to notify users when enabled:' set to 'No notification'. A 'Select Keywords' dialog box is open, showing a list of keywords: 'System dialog', 'No notification', and 'Custom message dialog'. The 'No notification' keyword is selected. The 'Deactivation Notification' section shows 'How to notify users when disabled:' set to 'No notification'.

## Notes/Domino 安全配置 - 代理的安全性 - 可信任的伺服器

- 訪問遠端的伺服器
  - ▶ Server A 可以執行一段 Web Agent 訪問 Server B 上的資料庫。
  - ▶ Server A 必須列在 Server B 伺服器上的“可信任伺服器”
  - ▶ 兩個伺服器版本都必須在 R6 以上的版本。



## Notes/Domino 安全配置 - 代理的安全性 - On Behalf

Shared Mail | DB2 | Administration |

**Programmability Restrictions**    Who can -

Run unrestricted methods and operations:

Sign agents to run on behalf of someone else:

Sign agents to run on behalf of the invoker of the agent:

Run restricted LotusScript/Java agents:

Run Simple and Formula agents:

Sign script libraries to run on behalf of someone else:

Note: The following settings are obsolete in Notes 6. They are used for compatibility with prior versions.

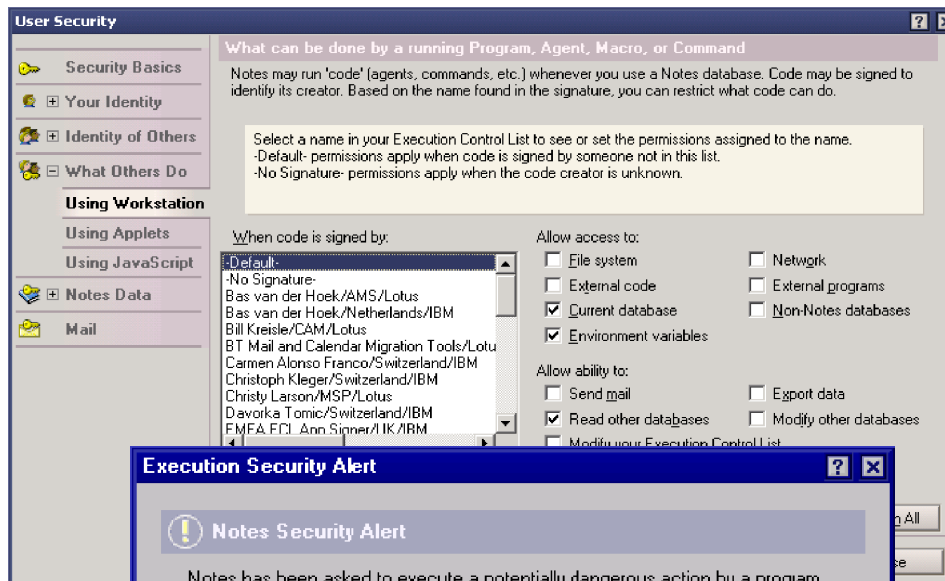
Run restricted Java/Javascript/COM:

Run unrestricted Java/Javascript/COM:



## Notes/Domino 安全配置 - Notes 用戶端 ECL 設置

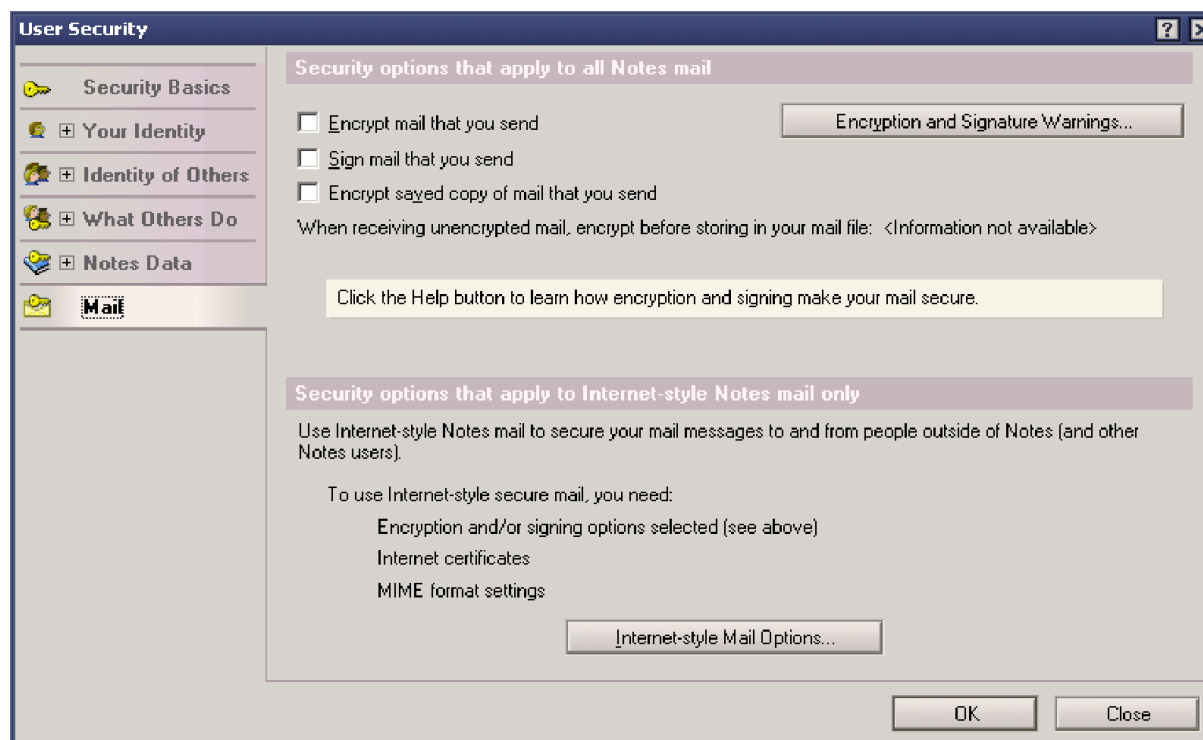
- 執行控制列表



- 執行安全警告

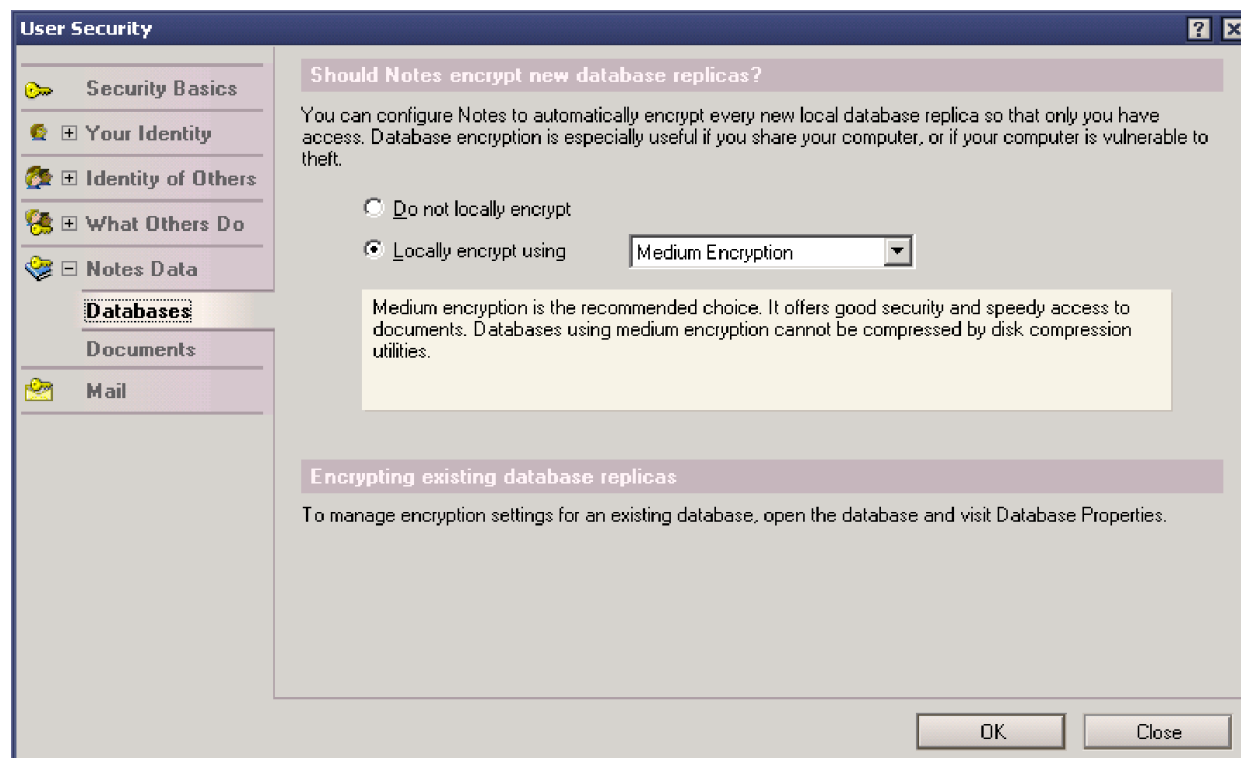
## Notes/Domino 安全配置 - 郵件加密和簽名設置

- 用戶可以統一設置外出郵件是否加密和簽名

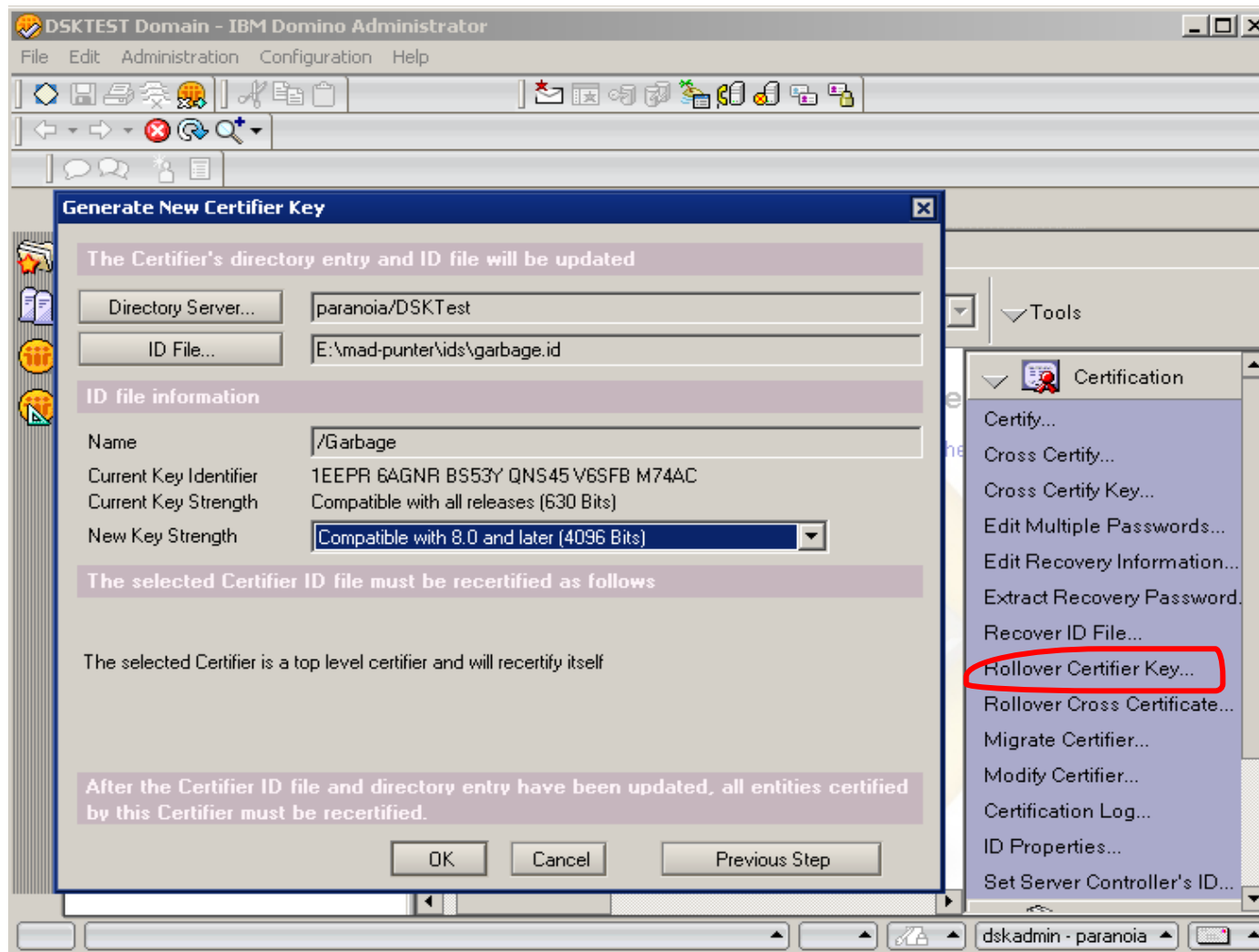


## Notes/Domino 安全配置 - 本地資料庫加密

- 設置本地的資料庫缺省情況下是否加密



## Notes/Domino 安全配置 - 驗證字回滾 (rollover)



## Notes/Domino 安全配置 - OCSP 設置

**Security Settings : OCSP enabled**

Basics | Password Management | Execution Control List | Keys and Certificates | Signed Plugins | Portal Server | Com

---

**Default Public Key Requirements**

Inherit Public Key Requirement Settings from Parent     Enforce Public Key Requirement Settings in Children

**User Public Key Requirements**

Minimum Allowable Key Strength: No Minimum

Maximum Allowable Key Strength: Compatible with Release 6 and later (1024 bits)

Preferred Key Strength: Compatible with Release 6 and later (1024 bits)

Maximum Allowable Age for Key: 36500 days

Earliest Allowable Key Creation Date: 08/01/1977

Spread new key generation for all users over this many days: 180 days

Maximum number of days the old key should remain valid after the new key has been created: 365 days

---

**Certificate Expiration Settings**

Warning Period: 21 days

Custom Warning Message:

---

**On-line Certificate Status Protocol (OCSP)**

Enable OCSP checking

Default OCSP Responder: <http://ocsp.openvalidation.org:80>

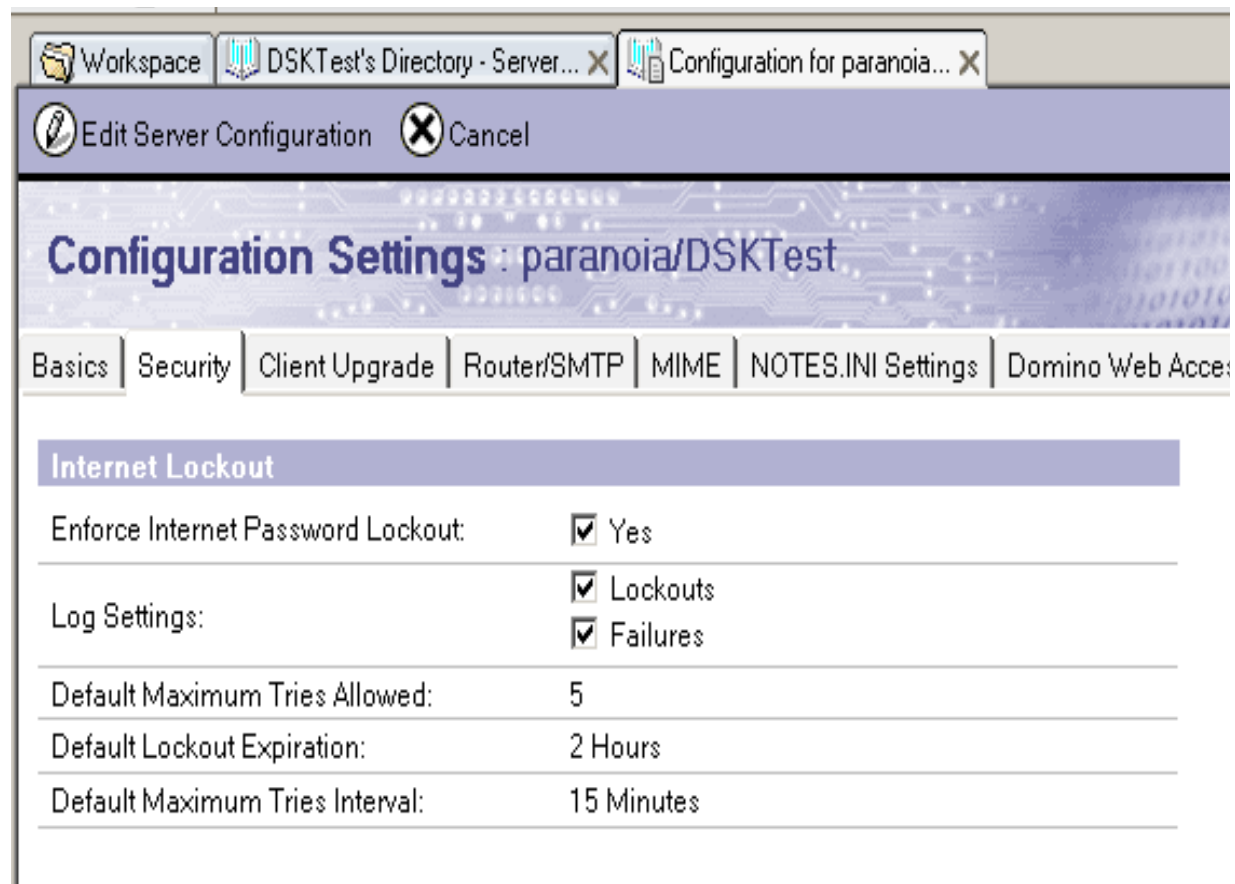
Always use Default OCSP Responder

Permitted Certificate Status: Allow use of all certificates

Level of Detail recorded in the Client Log: Log everything

## Notes/Domino 安全配置 - Internet 密碼鎖定

- 在嘗試 “X” 次登錄失敗後鎖定使用者的資訊
- 在配置文檔中啟用該特性並進行相應的配置



## Notes/Domino 安全配置 - Internet 密碼鎖定 - 策略

- 通過用戶的安全性原則設置可以覆蓋缺省的設置
  - ▶ 通常根據特定的需求使用者進行特定的設置
  - ▶ 只是在伺服器級別進行 Internet 密碼鎖定 (不能跨伺服器)

The screenshot shows the 'Security Settings: Hard lockout' configuration window. The 'Internet Password Lockout Settings' section is highlighted with a red circle. The settings are as follows:

| Section                            | Setting   | Value                                   | Inherit from parent policy:      | Enforce in child policies:       |
|------------------------------------|---|---|----------------------------------|----------------------------------|
| Password Management Options        | Use Custom Password Policy for Notes Clients                | No                                      | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
|                                    | Check password on Notes id file                             | No                                      | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
|                                    | Allow Users to Change Internet Password over HTTP           | Yes                                     | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
|                                    | Update Internet Password When Notes Client Password Changes | No                                      | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
|                                    | Enable Notes Single Logon with Workplace Rich Client        | No                                      | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
|                                    | <b>Internet Password Lockout Settings</b>                   |   |                                  |                                  |
| Internet Password Lockout Settings | Override Server's Internet Lockout settings?                | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
|                                    | Maximum Tries Allowed                                       | 5                                       | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
|                                    | Lockout Expiration  | 0Minutes                                | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
|                                    | Maximum Tries Interval                                      | 1Days                                   | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |

## Notes/Domino 安全配置 - Internet 密碼鎖定 - Inetlockout DB

- 當 Internet 密碼鎖定功能開啟後，伺服器會自動創建 Inetlockout 資料庫，大約需要 10 分鐘左右時間。
- 包含當前使用者的鎖定的狀態，但沒有歷史資訊，鎖定的歷史記錄存放在 DDM 資料庫
- 同一個 Domino 域每個資料庫用同樣的副本 ID，但是缺省情況下不進行複製
- 在不同的伺服器中的複製不會將同樣的使用者鎖定資訊進行累加，可以方便根據伺服器來進行分類查看
- 在 inetlockout.nsf 中刪除鎖定使用者資訊，將會解鎖

| Server Name   | User Name                   | Locked Out | Failed Attempts | First Failure Time |
|---------------|-----------------------------|------------|-----------------|--------------------|
| ▼ Sparta/Iris |                             |            |                 |                    |
|               | Phillipe Loher/Westford/IBM | No         | 3               | 11/29/2006 03:4    |
|               |                             |            |                 |                    |
|               |                             |            |                 |                    |
|               |                             |            |                 |                    |
|               |                             |            |                 |                    |
|               |                             |            |                 |                    |
|               |                             |            |                 |                    |
|               |                             |            |                 |                    |
|               |                             |            |                 |                    |



## Notes/Domino 安全配置 - Notes ID Vault

### ■ 主要功能

- ▶ 關鍵思想：把 ID 檔存儲在安全的伺服器資料庫中並在協定級與 Notes 客戶機整合
- ▶ 在每個域中可以有一個或多個保險庫
- ▶ 保險庫可以抄寫
- ▶ 使用者 / 保險庫映射使用基於策略的配置
- ▶ 對所有保險庫操作記錄審計日誌
- ▶ 採用了防止保險庫欺騙的方法

### ■ 優點

- ▶ 消除了成本高且容易出現錯誤的手動操作
- ▶ 自動地把 Lotus Notes ID 提供給 Notes 用戶端

### ■ 必要條件

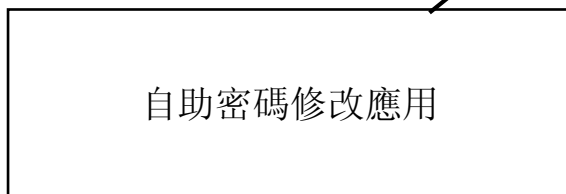
- ▶ Domino 8.5 伺服器
- ▶ Notes 8.5 用戶端

## Notes/Domino 安全配置 - Notes ID Vault

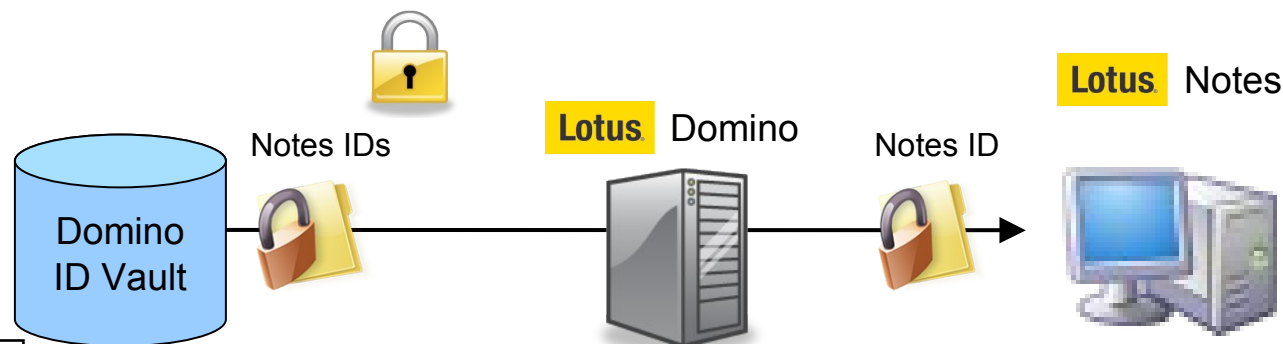
- 集中管理，存儲和同步使用者 ID 檔
- 新用戶註冊時 ID 檔進入 ID Vault
- 已存在用戶與伺服器認證時，ID Vault 自動捕捉 ID 檔
- Help Desk 或者使用者自助應用說明重設 Notes 密碼



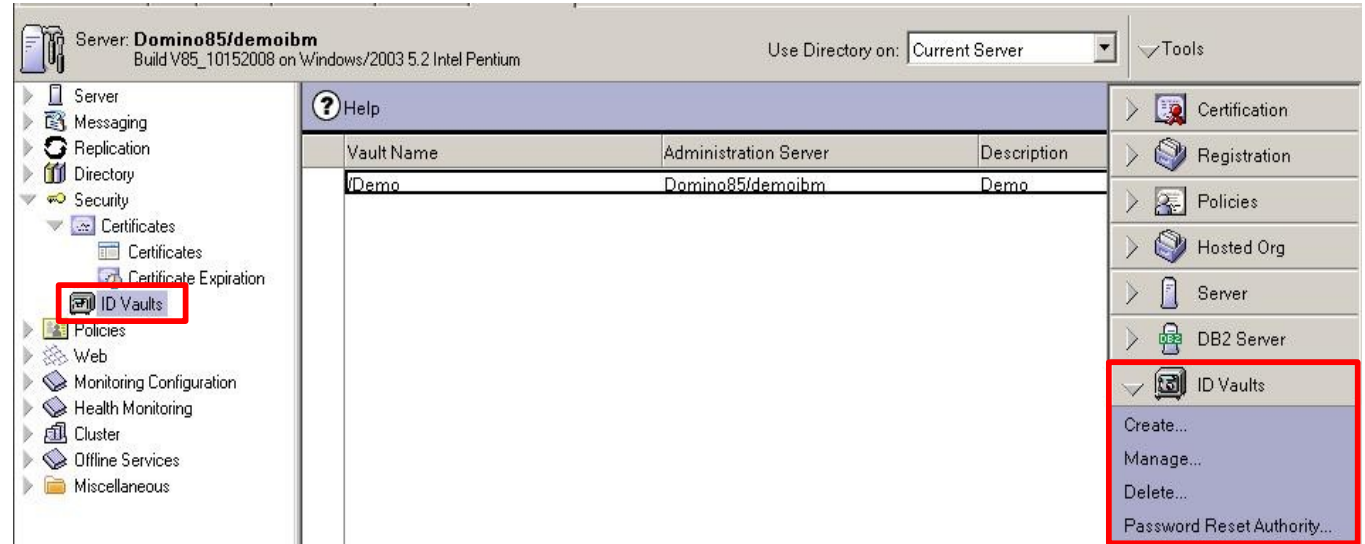
Helpdesk



自助密碼修改應用



## Notes/Domino 安全配置 - Notes ID Vault



## Notes/Domino 安全配置 - Xpage 安全

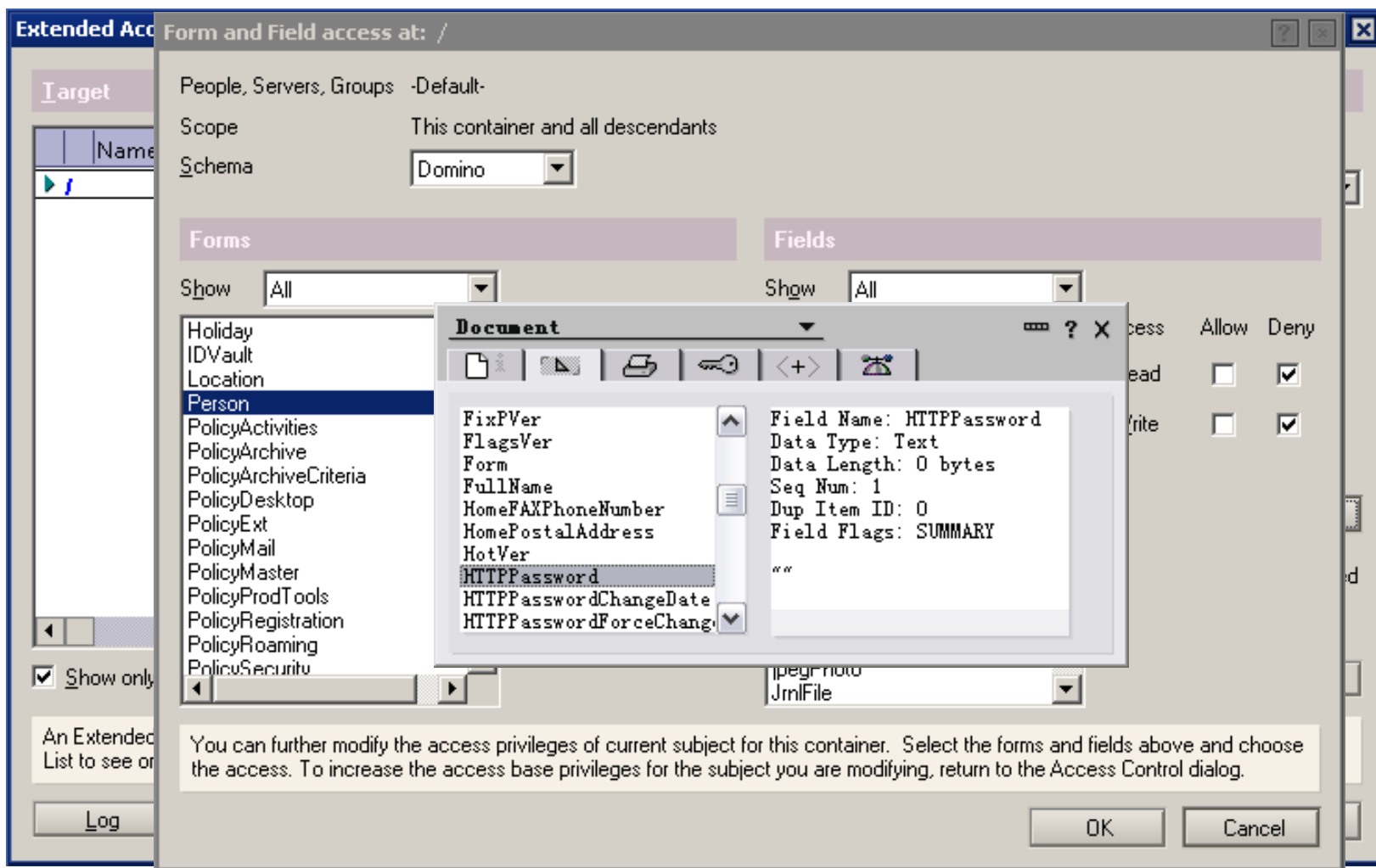
- 如何工作
  - ▶ 控制 XPage 執行許可權，與代理執行許可權的控制類似
- 優點
  - ▶ 確保在伺服器上執行的代碼是經過授權的
- 如何配置
  - ▶ 伺服器文檔 > 安全標籤 > 程式設計區段
    - Sign or run unrestricted methods and operations
    - Sign agents or Xpages to run on behalf of the invoker of the agent
- 必要條件
  - ▶ Domino 8.5 伺服器

| Programmability Restrictions                            | Who can -         |
|---|-------------------|
| <u>Sign or run unrestricted methods and operations:</u> | XPPage Builders ▾ |
| Sign agents to run on behalf of someone else:           | ▾                 |
| Sign agents or XPages to run on behalf of the invoker:  | XPPage Builders ▾ |
| Sign or run restricted LotusScript/Java agents:         | ▾                 |
| Run Simple and Formula agents:                          | ▾                 |
| Sign script libraries to run on behalf of someone else: | ▾                 |

## Notes/Domino 安全配置 - xACL - 介紹

- 擴展的資料庫 ACL 用於更進一步的細分用戶的存取權限—僅僅適用於 names.nsf 資料庫
  - ▶ 該功能類似於資料庫的 ACL，是架構在 NIF/NSF 層面
  - ▶ 不能覆蓋資料庫的 ACL 設置
- 能夠更好的去控制 names.nsf 的許可權—適用於
  - ▶ 容器或者個別 object
  - ▶ 對象 (form)
  - ▶ 欄位 (within forms)

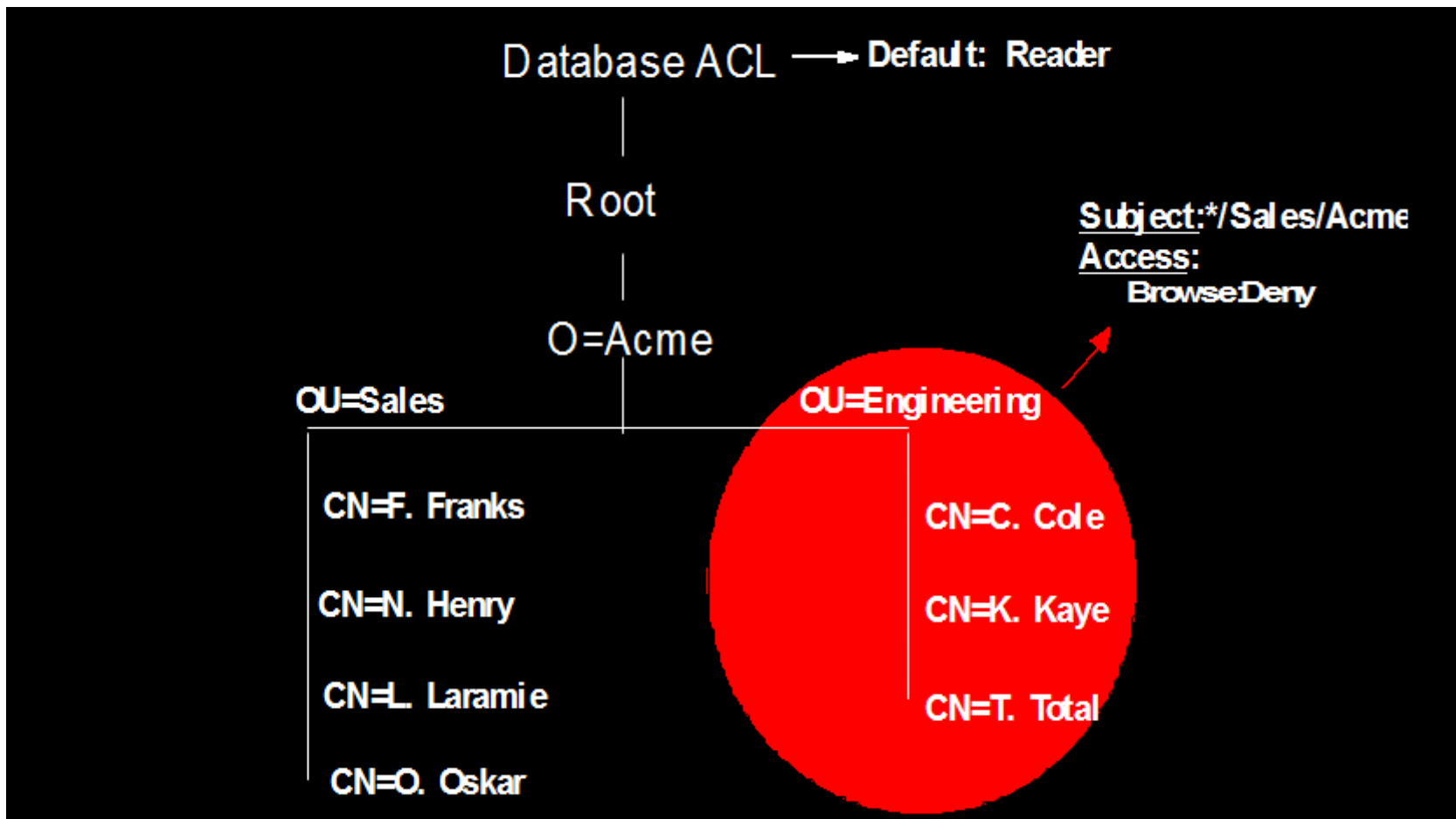
## Notes/Domino 安全配置 - xACL - 保證 Internet 密碼的安全



絕

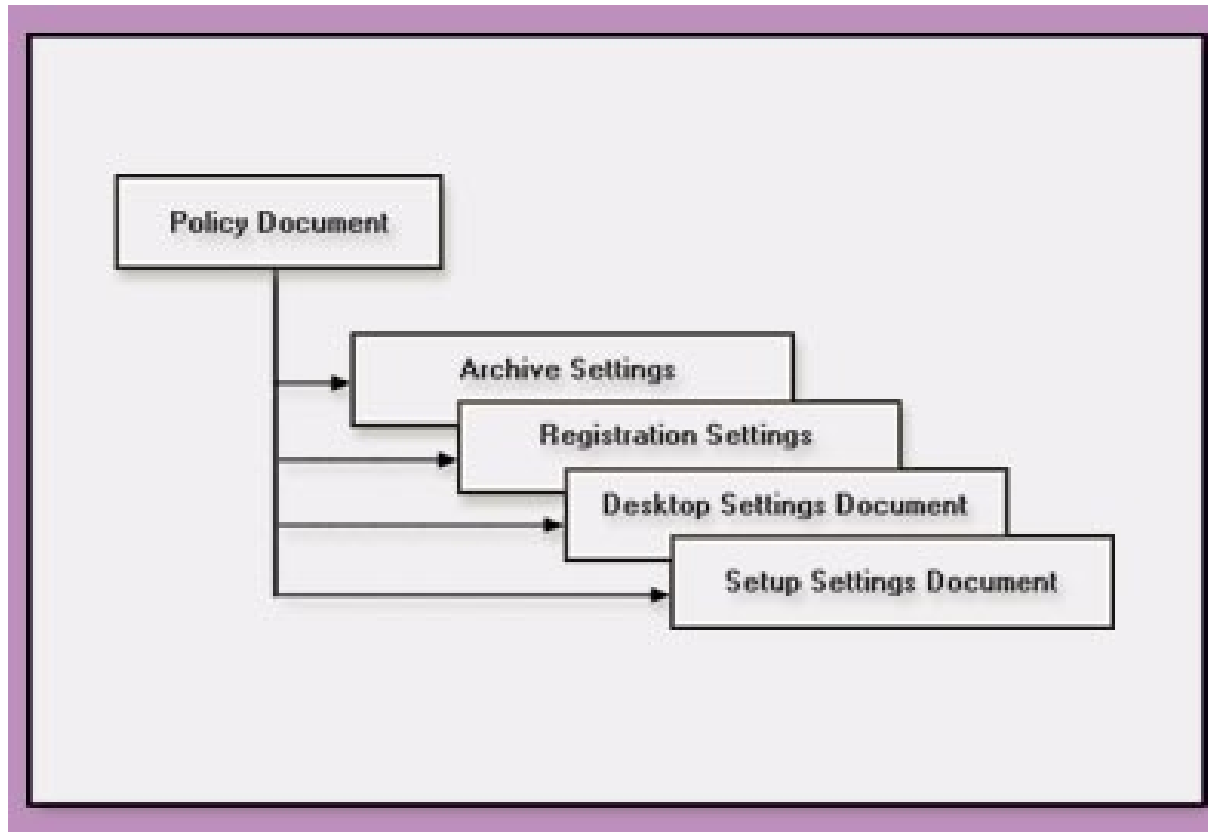
## Notes/Domino 安全配置 - xACL - 例子

- 禁止銷售人員去方位工程師的文檔





## Notes/Domino 安全配置 - 配置基於策略的管理

- 策略是對特定的用戶進行特定的設置





## Notes/Domino 安全配置 - 基於策略的管理

 Save & Close  Cancel

### Policy : /Samtleben.Net Global

Basics | Comments | Administration

---

#### Basics

Policy name:

Policy type:

Description:

#### Policy type help

Explicit policies can be explicitly assigned to users in their person document.

---

| Setting Type  | Setting Name  |                                       |
|---------------|---|---------------------------------------|
| Registration: | <input type="text" value="Global Registration"/> <input type="button" value="v"/> | <input type="button" value="New..."/> |
| Setup:        | <input type="text" value=""/> <input type="button" value="v"/>                    | <input type="button" value="New..."/> |
| Archiving:    | <input type="text" value=""/> <input type="button" value="v"/>                    | <input type="button" value="New..."/> |
| Desktop:      | <input type="text" value="Global Desktop"/> <input type="button" value="v"/>      | <input type="button" value="New..."/> |
| Security:     | <input type="text" value="Global Security"/> <input type="button" value="v"/>     | <input type="button" value="New..."/> |
| Mail:         | <input type="text" value=""/> <input type="button" value="v"/>                    | <input type="button" value="New..."/> |

## Notes/Domino 安全配置 - 註冊設置

### Registration Settings : Global Registration

[Basics](#) | [Mail](#) | [ID/Certifier](#) | [Miscellaneous](#) | [Comments](#) | [Administration](#)

| ID/Certifier User Registration Options  | Inherit from parent policy:      | Enforce in child policies:       |
|---|----------------------------------|----------------------------------|
| <input checked="" type="checkbox"/> Create a Notes ID   | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| <b>Certifier Information</b>  |                                  |                                  |
| Security Type:<br><input type="text" value="North American"/><br><input type="text" value="International"/>   | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Public Key Specification:<br><input type="text" value="Compatible with all releases (630 bits)"/><br><input type="text" value="Compatible with 6.0 and later (1024 bits)"/>   | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Password Key Width:<br><input type="text" value="Base strength on RSA key size"/><br><input type="text" value="Compatible with all releases (64 bits)"/><br><input type="text" value="Compatible with 6.0 and later (128 bits)"/> | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Certificate Expiration Date:<br><input checked="" type="radio"/> Static Date<br><input type="radio"/> Months from user creation<br>『26.10.2006 17:52』   | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| <b>Location for Storing User ID</b>   |                                  |                                  |
| <input checked="" type="checkbox"/> In Domino Directory   | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| <input type="checkbox"/> In File  | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |

## Notes/Domino 安全配置 - 安全設置 (密碼管理)

Inheritance
  Enforcement

### Security Settings : Global Security

Basics | Password Management | Execution Control List | Public Key Requirements | Comments | Administration

| Password Management Options                                 |  | Inherit from parent policy:      | Enforce in child policies:       |
|---|--|----------------------------------|----------------------------------|
| Allow Users to Change Internet Password over HTTP           | <input checked="" type="radio"/> Yes   | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Update Internet Password When Notes Client Password Changes | <input checked="" type="radio"/> No  | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Check Notes Password  | <input checked="" type="radio"/> Yes   | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Password Expiration Settings                                |  | Inherit from parent policy:      | Enforce in child policies:       |
| Enforce Password Expiration                                 | <input checked="" type="radio"/> Disabled  | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Required Change Interval                                    | <input type="text" value="0"/> days  | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Allowed Grace Period  | <input type="text" value="0"/> days  | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Password History (Notes only)                               | <input type="text" value="50"/> passwords  | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Password Quality Settings                                   |  | Inherit from parent policy:      | Enforce in child policies:       |
| Required Password Quality                                   | <input checked="" type="radio"/> Strong Password Possibly Crackable by Automated Dictionary Attack (8) | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Use Length Instead  | <input type="checkbox"/> Yes   | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |

## Notes/Domino 安全配置 - 安全管理 (使用者密碼策略)

Basics | Password Management | Execution Control List | Public Key Requirements | Comments | Administration

Password Management Basics | Custom Password Policy

| Custom Options                                  |            | Inherit from parent policy:      | Enforce in child policies:       |
|---|------------|----------------------------------|----------------------------------|
| Change Password on First Use                    | No ▾       | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Allow Common Name in Password                   | Yes ▾      | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Password Length Minimum                         | characters | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Password Length Maximum                         | characters | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Password Quality Miminum                        | characters | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Minimum Number of Alphabetic Characters Allowed |            | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Minimum Number of UpperCase Characters Allowed  |            | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Minimum Number of LowerCase Characters Allowed  |            | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Minimum Number of Numeric Characters Allowed    |            | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Minimum Number of Special Characters Allowed    |            | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Maximum Number of Repeated Characters Allowed   |            | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Minumum Number of Unique Characters Allowed     |            | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Password May Not Begin With                     | ▾          | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |
| Password May Not End With                       | ▾          | <input type="checkbox"/> Inherit | <input type="checkbox"/> Enforce |

## Notes/Domino 安全配置 - 安全管理 ( 公開金鑰 )

Save & Close Cancel Inheritance Enforcement

### Security Settings : Global Security

Basics | Password Management | Execution Control List | **Public Key Requirements** | Comments | Administration

#### User Public Key Requirements

|   |   |   |
|---|---|---|
| Minimum Allowable Key Strength:                                       | No Minimum                                      | ▼ |
| Maximum Allowable Key Strength:                                       | Compatible with Release 6 and later (1024 bits) | ▼ |
| Desired Default Key Strength:   | Compatible with Release 6 and later (1024 bits) | ▼ |
| Maximum Allowable Age for Key (in days):                              | 36500   |   |
| Earliest Allowable Key Creation Date:                                 | 01.08.77  |   |
| Spread new key generation for all users over this many days:          | 180 days  | ▼ |
| Priority relative to person document public key requirement settings: | Low   | ▼ |

## Notes/Domino 安全配置 - 動態策略

- 動態策略是什麼？
  - ▶ 通過在策略文檔中指定用戶或群組名稱來給特定的用戶和群組來分配策略
- 好處
  - ▶ 減少管理員的工作
  - ▶ 策略和組織中使用者的角色進行關聯（比如：群組用戶）
- 必要條件
  - ▶ Domino 8.5 伺服器
  - ▶ Notes 8.5 用戶端

## Notes/Domino 安全配置 - 動態策略 (續)

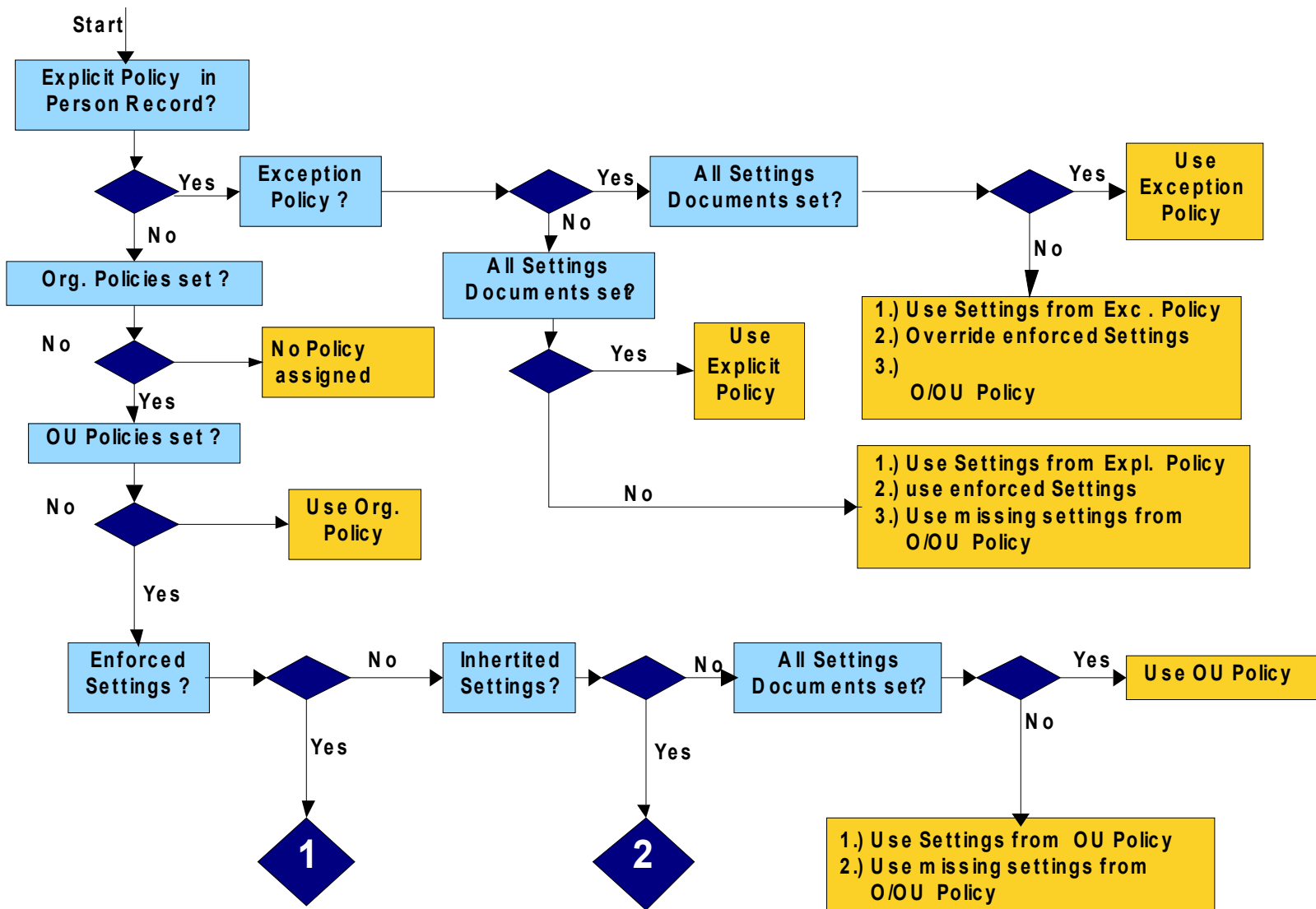
### 如何工作

- ▶ 在策略文檔中 “新建策略”
  - 增加需要遵守該策略的使用者
  - 增加需要遵守該策略的群組
- ▶ 策略的應用順序
  - 首先是組織策略
  - 然後是有動態策略的獨立策略
  - 最後才是沒有動態策略的獨立策略
  - Policy Synopsis
- ▶ 在視圖中調整動態策略的優先順序
  - 顯示動態策略的優先順序
  - 可以調整動態策略的優先順序



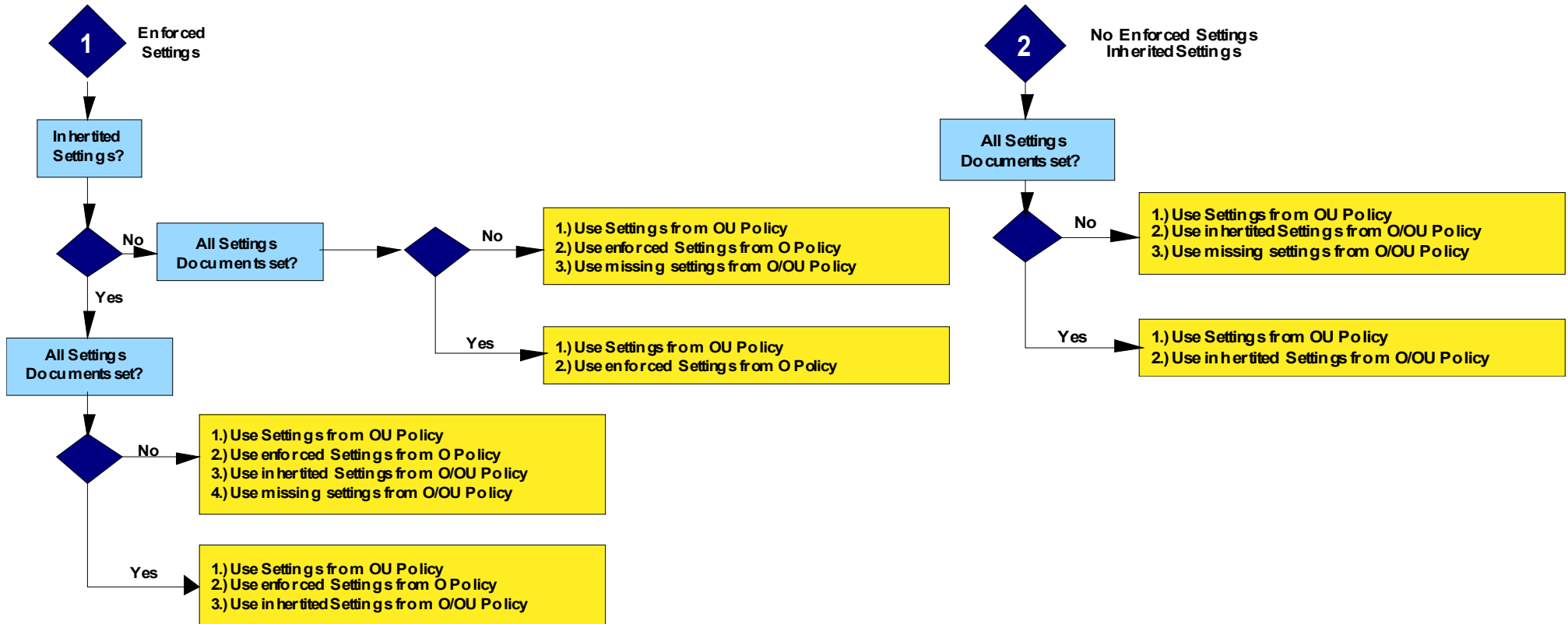
| Category          | Precedence | Dynamic Policy       | Author                   |
|-------------------|------------|----------------------|--------------------------|
| (Not Categorized) |            |                      |                          |
|                   | 0          | /RENVaultVaultPolicy |                          |
|                   | 1          | /Policy              | Domino Admin/renovations |

## Notes/Domino 安全配置 - 計算過程





## Notes/Domino 安全配置 - 計算過程 (續)



## Notes/Domino 安全配置 - Domino 域監控 (DDM)

- 自動確定問題，並在多個功能域中確定可能的原因。
- 利用 50 多個具有高度可配置的排程、內容和目標的新探測提供主動監控功能。
- 提供自頂向下、面向功能的網路域狀態視圖，能選擇性地查看狀態的詳細資訊。
- 提供視覺化的指示器，用於顯示哪些問題最重要，哪些問題已解決，哪些問題還未解決。
- 為探測配置提供缺省設置，使設置更輕鬆。
- 可在幾分鐘內發現並報告關鍵的伺服器 and 客戶機問題。
- 提供補救措施和指向資料庫的連結，以解決所報告的問題。

## Notes/Domino 安全配置 - DDM 安全探針

- 屬於 Domino Domain Monitoring 的一個部分
- 對於關鍵的配置資訊提供自動審查和比較
  - ▶ 和最佳實踐進行比較
  - ▶ 和特定伺服器配置進行比較
  - ▶ 資料庫 ACL
  - ▶ 資料庫安全審查

## Notes/Domino 安全配置 - DDM 安全探針

**Event Resource Center**

Open Domino Event Last computed 26.10.2004 18:39:17

Event has been reported from: Event summary for: Additional information:

Server: Blackslate/Samtleben.Net Server: Blackslate/Samtleben.Net User: All Users in the Domino Directory

Domain: Samtleben.Net Database: names.nsf : Person Document

Probe Doc: [Icon]

**Most recent event:**

26.10.2004 18:39:17: Security Best Practices Probe: Potential security risks have been found in 2 Person Document(s), and 2 have been reported to the details tab inside.

|            |                         |                   |                     |
|------------|-------------------------|-------------------|---------------------|
| Main Type: | Security, Configuration | First occurrence: | 26.10.2004 18:09:09 |
| Severity:  | Fatal                   | # Occurrences:    | 2                   |

Probable cause and possible solution: [Details](#)

**4 Person Document(s) from the domino directory were analyzed. The requested number of potential Security risks are reported below.**

| User Name                  | Link to Person Document |
|----------------------------|-------------------------|
| CA Protector/Samtleben.Net |                         |

| Field Name               | Field Value          | Recommendation  |
|--------------------------|----------------------|---|
| Check password           | Don't check password | It is recommended that this field be set to - Check Password. |
| Required change interval | 0                    | It is recommended to have a password change interval set.     |

Security risks have been found and reported to the details tab

deleted.

Early defined in probe

Documents have been analyzed.

Probe: Probe cannot run due to configuration information was

Configuration Documents have

## Notes/Domino 安全配置 - 防垃圾郵件設置

| DNS Blacklist Filters  |                                   | DNS Whitelist Filters  |  |
|--|-----------------------------------|--|--|
| DNS Blacklist filters:   | <input type="checkbox"/> Disabled | DNS Whitelist Filters:   | <input type="checkbox"/> Disabled                        |
| DNS Blacklist sites:   | <input type="checkbox"/>          | DNS Whitelist Sites:   | <input type="checkbox"/>                                 |
| Desired action when a connecting host is found in a DNS Blacklist:       | <input type="checkbox"/> Log only | Desired action when a connecting host is found in a DNS whitelist:       | <input type="checkbox"/> Silently skip blacklist filters |
| Custom SMTP error response for rejected messages:                        | <input type="checkbox"/>          |  |  |
| Private Blacklist Filter   |                                   | Private Whitelist Filter   |  |
| Private Blacklist Filter:  | <input type="checkbox"/> Disabled | Private Whitelist Filter:  | <input type="checkbox"/> Disabled                        |
| Blacklist the following hosts:   | <input type="checkbox"/>          | Whitelist the following hosts:   | <input type="checkbox"/>                                 |
| Desired action when a connecting host is found in the private blacklist: | <input type="checkbox"/> Log only | Desired action when a connecting host is found in the private whitelist: | <input type="checkbox"/> Silently skip blacklist filters |
| Custom SMTP error response for rejected messages:                        | <input type="checkbox"/>          |  |  |

- 1、 Notes/Domino 安全模型
- 2、 Notes/Domino 安全技術
- 3、 Notes/Domino 安全配置
- 4、 Notes/Domino 安全方法論



## Notes/Domino 安全 --- 方法論

- 1 安全是什麼？
- 1 IT 安全模型（評估 - 搭建 - 管理）
- 1 詳細的實施步驟
  - 1. 瞭解客戶的商業應用
  - 2. 威脅分析
  - 3. 風險分析
  - 4. 數據歸類
  - 5. 策略和過程
  - 6. 應對策略
  - 7. 實施和生成文檔
  - 8. 用戶培訓
  - 9. Compliance Testing 測試
  - 10. 結果回饋

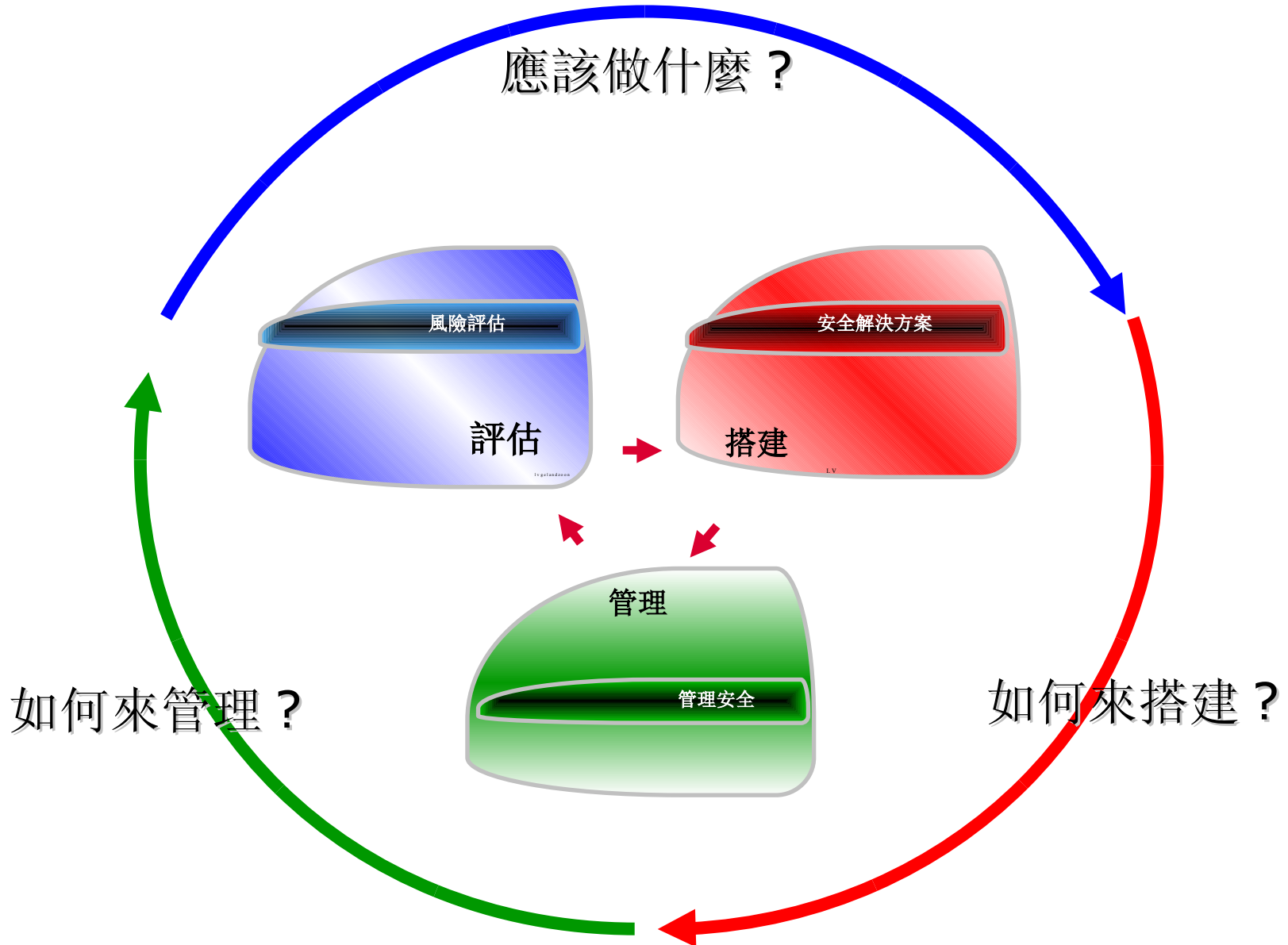
Notes/Domino 安全 --- 安全是什麼？

**"Security is a Process,  
*not* a Product"**

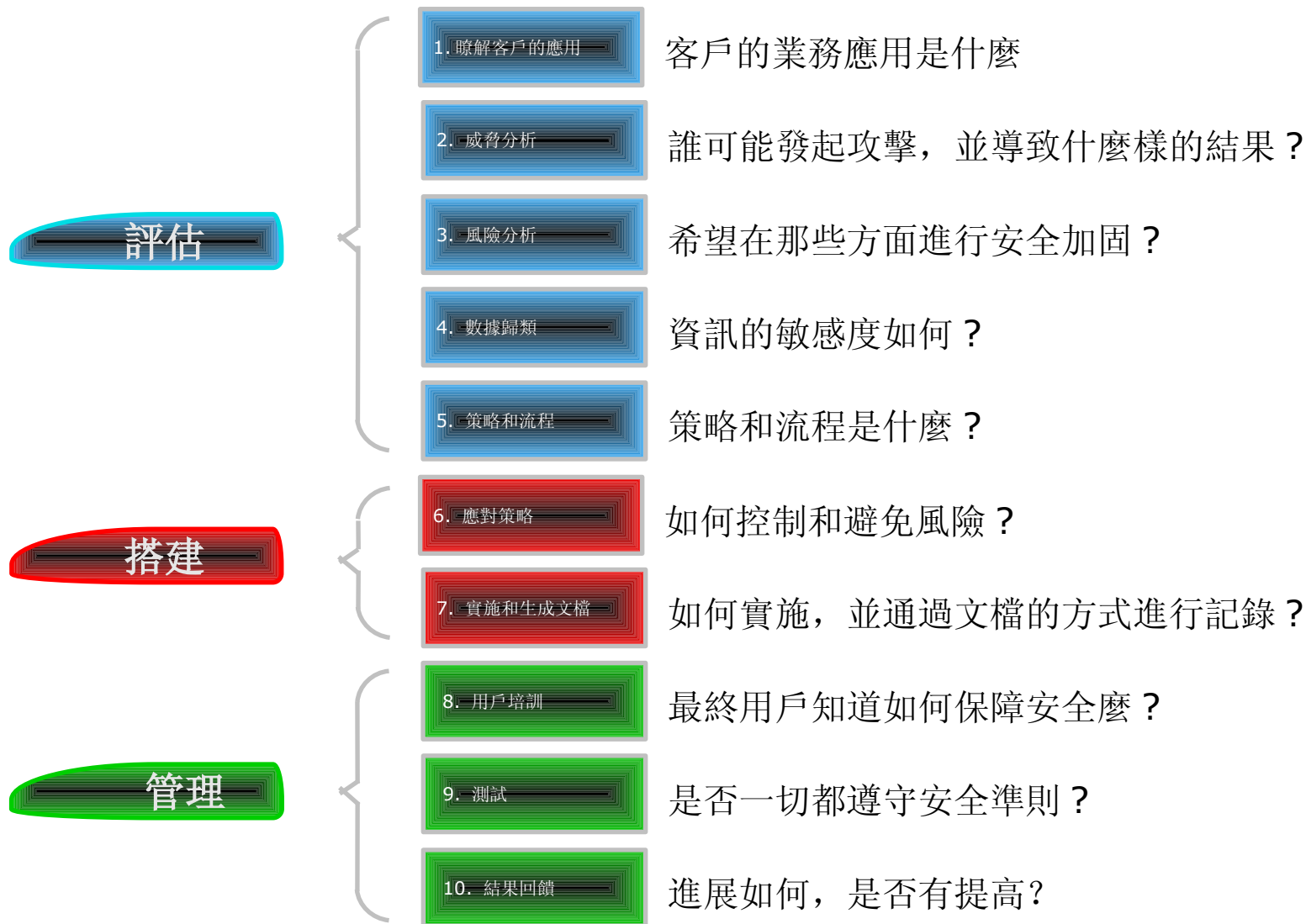
**Bruce Schneier,  
Father of Blowfish and Twofish  
Counterpane Security**



## Notes/Domino 安全 --- IT 安全模型



## Notes/Domino 安全 —— 詳細的實施步驟



## 客戶的業務應用是什麼？

- 目標：瞭解客戶的 IT 架構
- 1. 評審客戶目前的業務應用狀態
    - ▶ 瞭解客戶的核心業務
    - ▶ 統計業務使用人員分佈情況
    - ▶ 瞭解商業合作夥伴的情況
    - ▶ 分析競爭對手的情況
    - ▶ 行業的趨勢和標準分析
  2. 進行初步架構評估
    - ▶ 從硬體的角度對架構進行評估
    - ▶ 從軟體的角度對架構進行評估

## 誰可能發起攻擊，並導致什麼樣的結果？

- 威脅 = 可能的傷害或危險
- 1. 識別漏洞
    - ▶ 什麼是漏洞？
    - ▶ 漏洞可能在那些地方出現？
    - ▶ 這些漏洞有哪些可能被利用的可能性？
    - ▶ 對 IT 架構 / 業務的影響？
  2. 措施
    - ▶ 針對這些漏洞採取如何的措施？
    - ▶ 這些措施需要的開銷？
    - ▶ 這些開措施合適麼 ( 工作量和開銷 )？

## 希望在那些方面進行安全加固？

- 風險 = 影響 + 威脅 + 可能性
- 通過以下方式來評估：
  - ▶ 安全技術評估
  - ▶ 需要控制的目錄清單
  - ▶ 系統風險清單
- 風險分析的 5 個步驟
  1. 資產的認定
  2. 風險認定
  3. 出現的可能性評估
  4. 採取合適的措施，考評開銷大小
  5. 實施的對策

## 4. 數據歸類

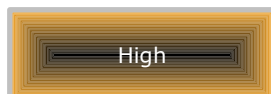
### 資訊的敏感度如何？

- 越敏感的資訊的丟失、曝光或損壞對組織造成的影響越大
- 敏感度級別

High



Top Secret Information



Secret Information

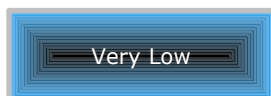


Confidential information



Internal Information

Low



Public or Unclassified Information

## 策略和流程是什麼？

- 安全性原則 = 組織策略和流程
- 1. 安全性原則
    - ▶ 系統覆蓋的範圍和誰會受到影響？
    - ▶ 如何實施和維護安全？
    - ▶ 加密那些內容，如何來做，是否需要使用什麼工具？
    - ▶ 需要培訓的物件，確保其安全的行為
  2. 安全責任人
    - ▶ 誰對組織的安全負責？
  
    - ▶ Executives -> Security Manager -> Process Owners -> Developers -> Users (troublemakers)

## 如何控制和避免風險？

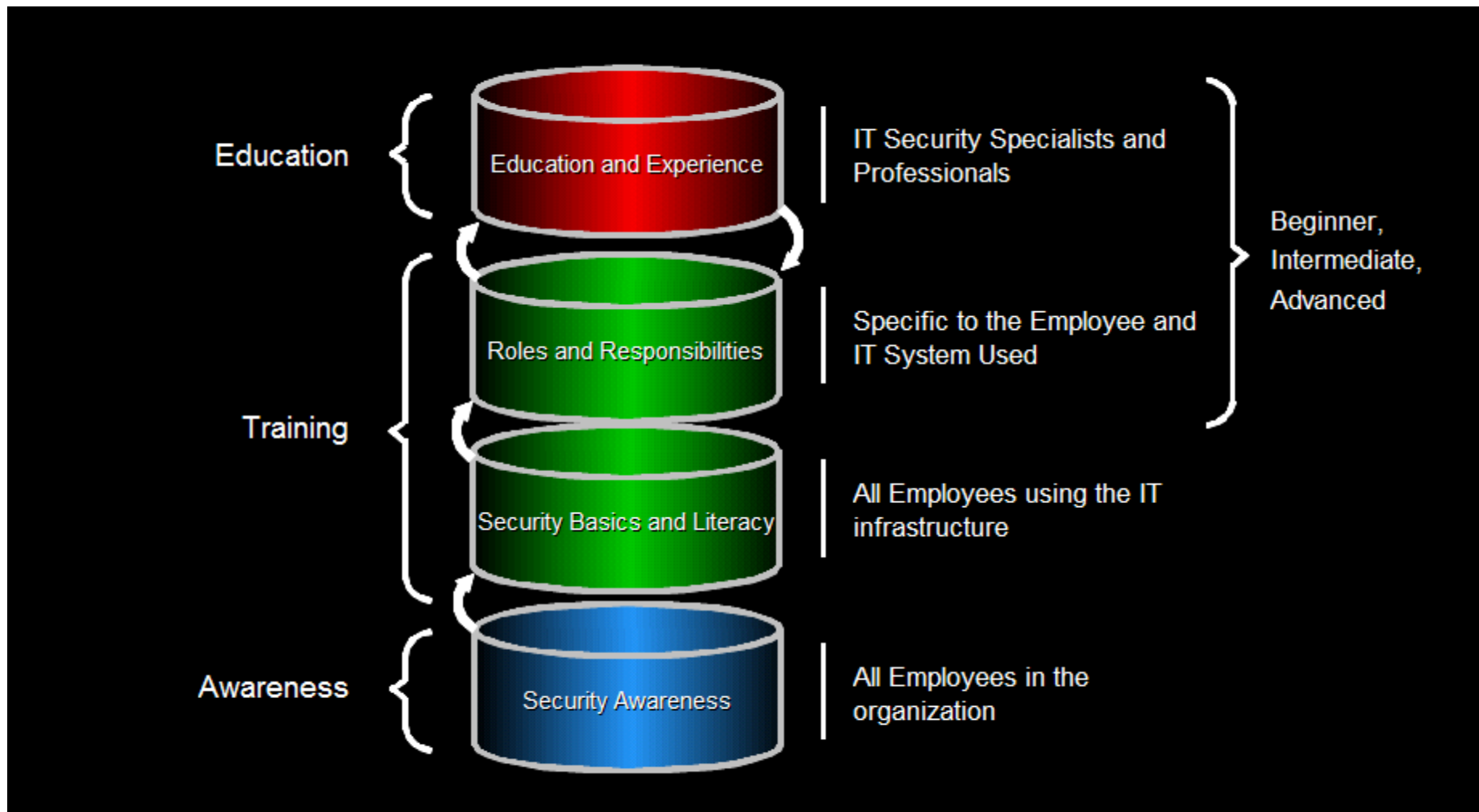
- 應對策略 = 工具，產品和服務
- 工具和產品
  - ▶ 公開金鑰加密 / 目錄管理工具
  - ▶ 病毒掃描和刪除
  - ▶ 安全資訊 / 安全闢道
- 服務
  - ▶ 安全審計人員
  - ▶ 道德駭客 ( 不破壞，只研究技術 )
  - ▶ 安全系統和工具部署人員
  - ▶ 安全管理服務



## 如何實施，並通過文檔的方式進行記錄？

- 安全專案 = 實施 & 生成文檔
- 1. 目標和結果的定義
    - ▶ 安全設計、實施和配置
  2. 安全的範圍
    - ▶ 系統的性能和監控
  3. 新架構上線計畫
    - ▶ 一次和多次測試路演
  4. 新架構上線
    - ▶ 最終用戶的支援和培訓

## 最終用戶知道如何保障安全麼？



## 是否一切都遵守安全準則？

- 遵守規則 = 願意遵守規則或規定
- 安全性原則應該：
  - ▶ 強制執行，像商務邏輯
  - ▶ 規劃需要使用的安全規則
  - ▶ 指定考核指標，以確保被遵守安全規則
- 在不遵守規則的情況下，安全性原則應該
  - ▶ 詳細的應對措施來處理不遵守規則的情況
  - ▶ 採取的懲罰措施的嚴重級別
  - ▶ 重新遵守規則的具體步驟
  - ▶ 提供回饋機制，以防止復發

## 是否一切都遵守安全準則？

- 回饋 = 提高 或者 廢除
- 安全是過程，不是產品：
  - ▶ 基於技術、流程和人員
  - ▶ 隨著業務的變化不斷的發展
  - ▶ 隨著技術的變化不斷的發展
  - ▶ 隨著風險和威脅的變化不斷的發展
- 回饋機制
  - ▶ 確保合理地實施了安全機制
  - ▶ 確保實施的安全性原則遵照了當初的設計
  - ▶ 確保安全是為了適應用戶的要求，而不是反過來
  - ▶ 確保安全滿足組織變化的需要

## 參考文獻

- Lotus Security Redbook
  - ▶ <http://www.redbooks.ibm.com/abstracts/sg247017.html?Open>
- Policy-based system administration
  - ▶ <http://www-10.lotus.com/ldd/today.nsf/Lookup/policy>
- Domino CA & CPS
  - ▶ <http://www-10.lotus.com/ldd/today.nsf/0/d3646dc17fba0b200256c410049d8d5?OpenDocument>
  - ▶ <http://www-106.ibm.com/developerworks/lotus/library/article/domino-cps/>
- Secure Messaging
  - ▶ <http://www-106.ibm.com/developerworks/lotus/library/article/securemessaging/>

## 問與答



# Lotus knows.

Smarter software for a Smarter Planet.

Thank  
YOU

## Legal Disclaimer

© IBM Corporation 2010. All Rights Reserved.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

IBM, the IBM logo, Lotus, Lotus Notes, Notes, Domino, and Lotusphere are trademarks of International Business Machines Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others.

All references to Renovations refer to a fictitious company and are used for illustration purposes only.