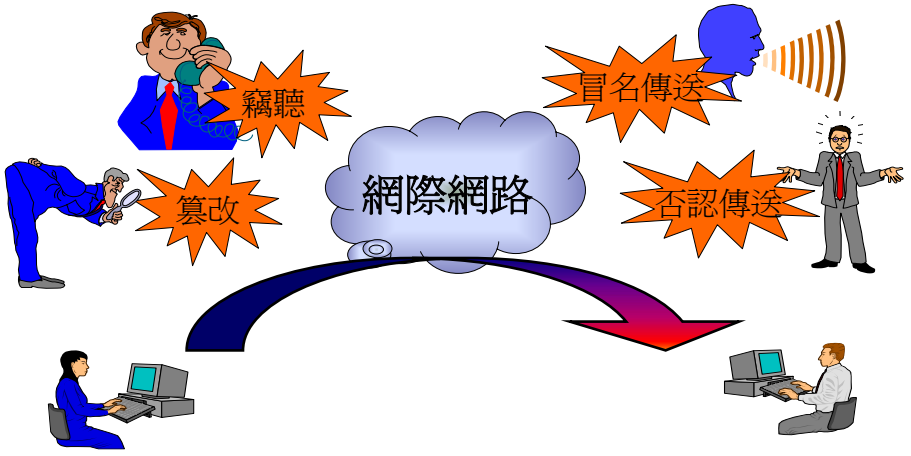
認證授權機制
以勞保網路申辦作業及共通作業平台為例

中華電信股份有限公司

日期：九十三年九月二十九日

網路的安全問題

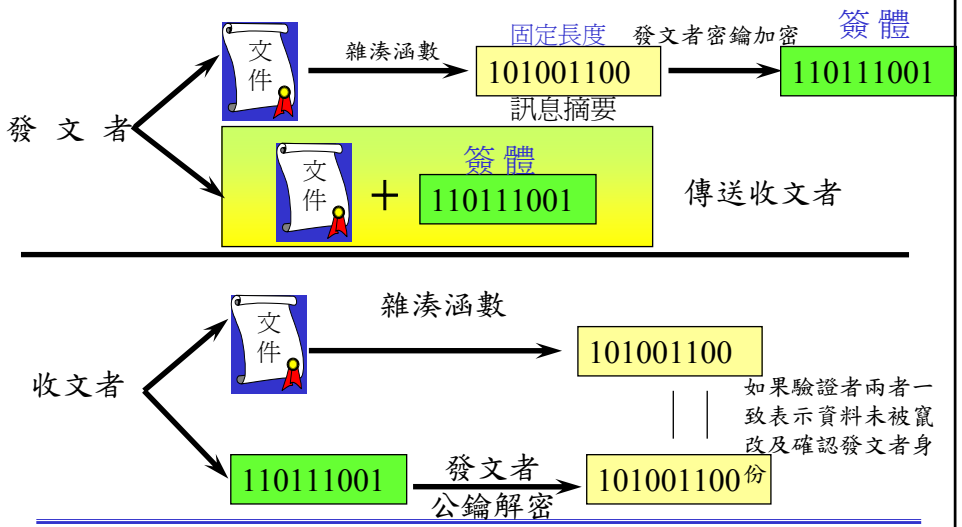


◆利用電子簽章可以達到下列目的：

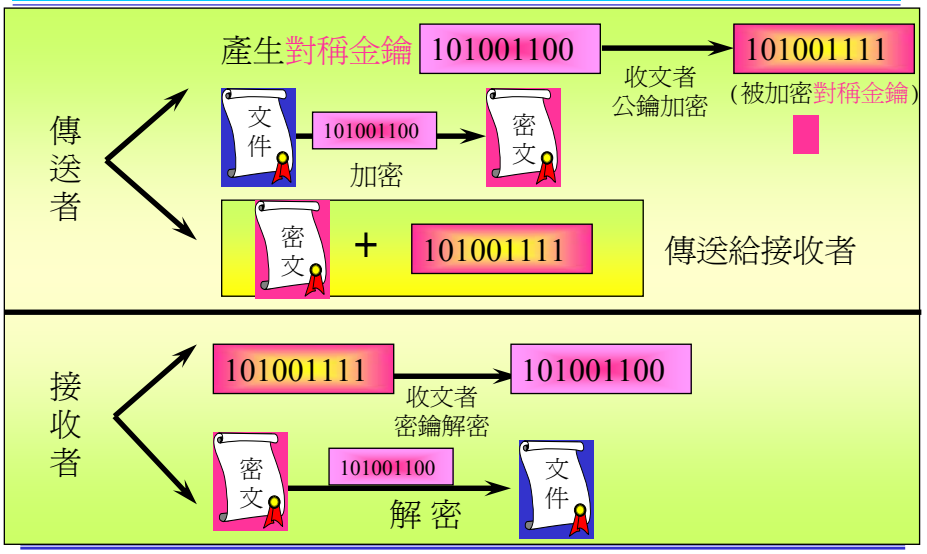
- □鑑別對方的身分
- □防止資料內容被竄改或偽造
- □防止事後否認

◆利用數位信封可以防止竊聽

數位簽章



數 位 信 封



認證與授權

安全管理可分成兩大部份：

認證：驗證使用者的身份

- 帳號+密碼
- 生物特徵-指紋、視網膜
- 憑證

授權：使用者可存取的系統資源

憑證

- 舊GCA
  - 自然人憑證 – 身分證號
  - 政府機關、單位憑證 – 機關代號、單位代號
  - 專屬憑證 – 保險證號(勞保局)
  - 伺服器應用軟體憑證 – IP Address 、網址

GPKI

- GRCA ：政府憑證總管理中心
- GCA：政府憑證管理中心
- MOICA ：內政部憑證管理中心
- MOEACA ：經濟部工商憑證管理中心
- XCA ：組織及團體憑證管理中心

各類憑證主體的唯一識別代碼

- 政府機關（構）：OID
- 政府單位：OID
- 公司：統一編號
- 分公司：統一編號
- 商號：統一編號
- 社團法人：OID
- 財團法人：OID
- 學校：OID
- 自然人：身分證字號後四碼、憑證主體名稱序號（注意：不是憑證序號）

新舊憑證差異

•舊GCA自然人憑證有身分證號
•MOICA自然人憑證只有身分證號後四碼

•舊GCA有勞保專屬憑證可以放入單位保險證號
•新的GPKI單位憑證無法放入單位保險證號

•舊GCA機關單位憑證放入機關代號單位代號
•新GCA機關單位憑證放入OID

➢因此需要註冊系統將新的GPKI單位憑證和單位保險證號建立連結

勞保網路申辦作業系統概述

- 勞保網路申辦作業系統提供投保單位透過網際網路申報投保資料及查詢投保資料。
- 系統設計涉及身分認證、授權管理、資料加密、資料完整性及不可否認性等需求。

系統功能

- 勞保網路申辦作業
- 農保網路申辦作業
- 敬老/老農津貼網路作業
- 個人網路查詢作業
- 網路申辦指派作業
- 系統維護作業

勞保網路申辦作業申請加入流程

1. 下載書表
2. 製作及申辦憑證
   單位憑證
   自然人憑證
3. 窗口審驗
4. 下載憑證
5. 指派作業
6. 申辦作業

身分認證

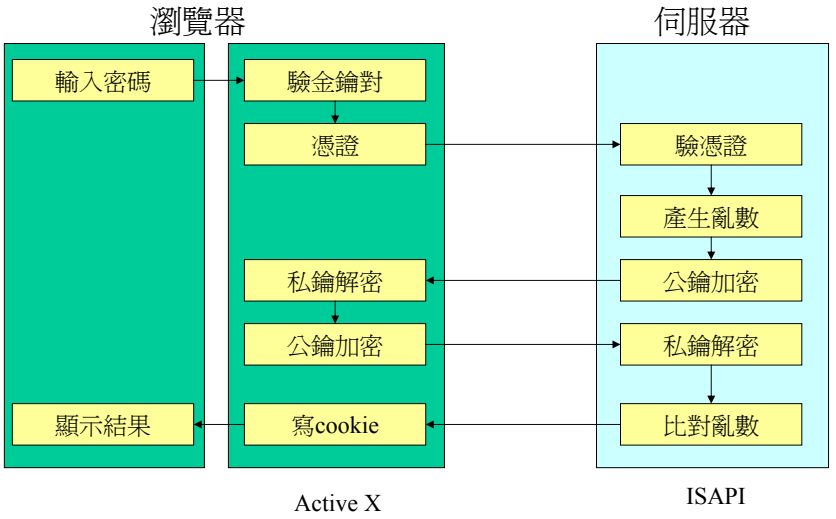
- 勞保局網路申辦系統身分認證採用GCA所簽發的電子憑證
- 目前勞保局網路申辦系統接受的憑證
  - 舊GCA
  - MOICA
- 未來可接受的憑證
  - GCA
  - MOEACA
  - XCA

授權

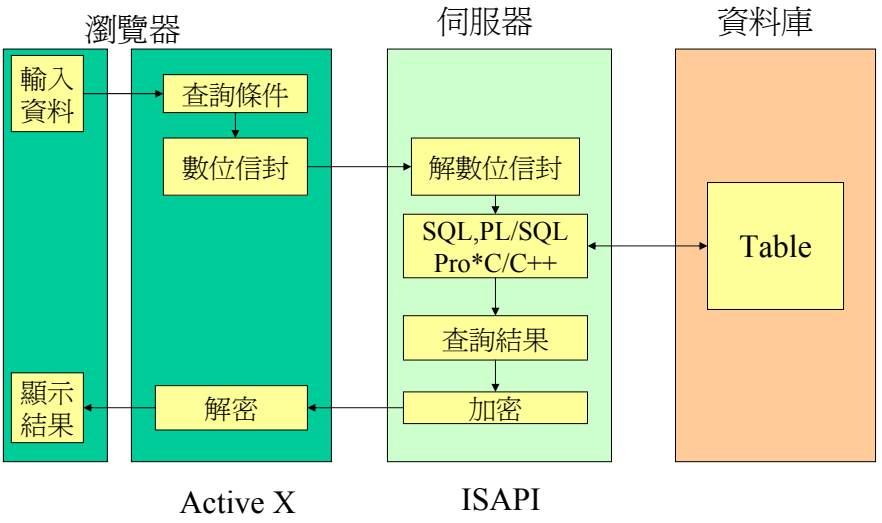
權限是由單位基本資料檔及權限控制檔設定

- ❑一般自然人可以查詢個人資料
- ❑單位承辦人可以執行被授權的功能
- ❑網路負責人可以授權單位承辦人
- ❑勞保局人員可以執行被授權的維運功能

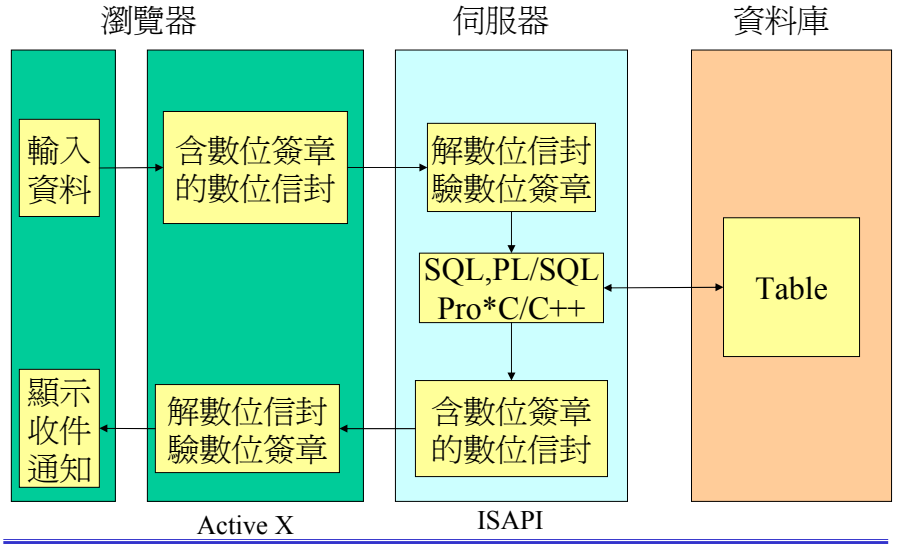
登錄作業



查詢作業

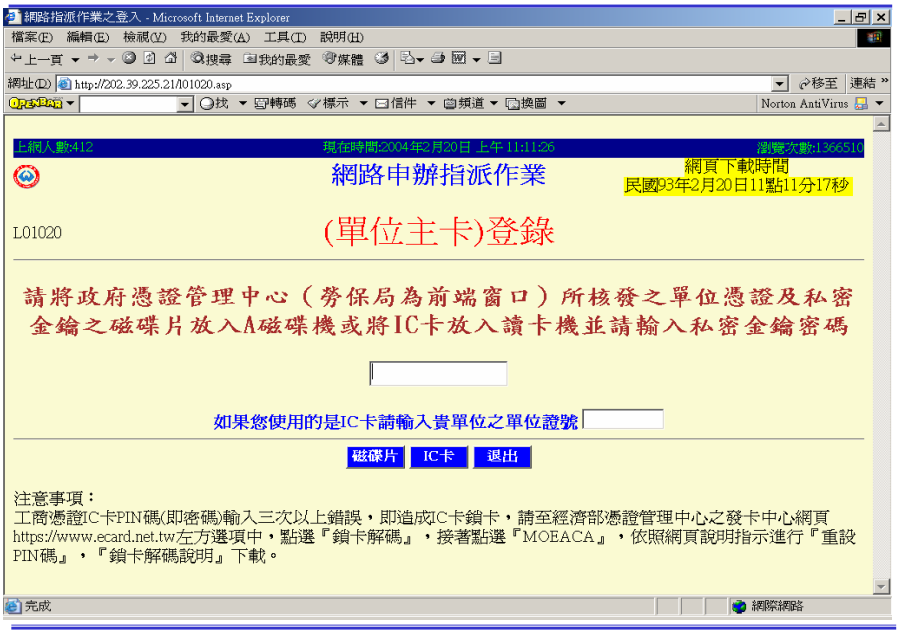

瀏覽器
伺服器
資料庫
輸入資料
查詢條件
數位信封
解數位信封
SQL,PL/SQL Pro*C/C++
Table
查詢結果
顯示結果
解密
加密
Active X
ISAPI

申報作業

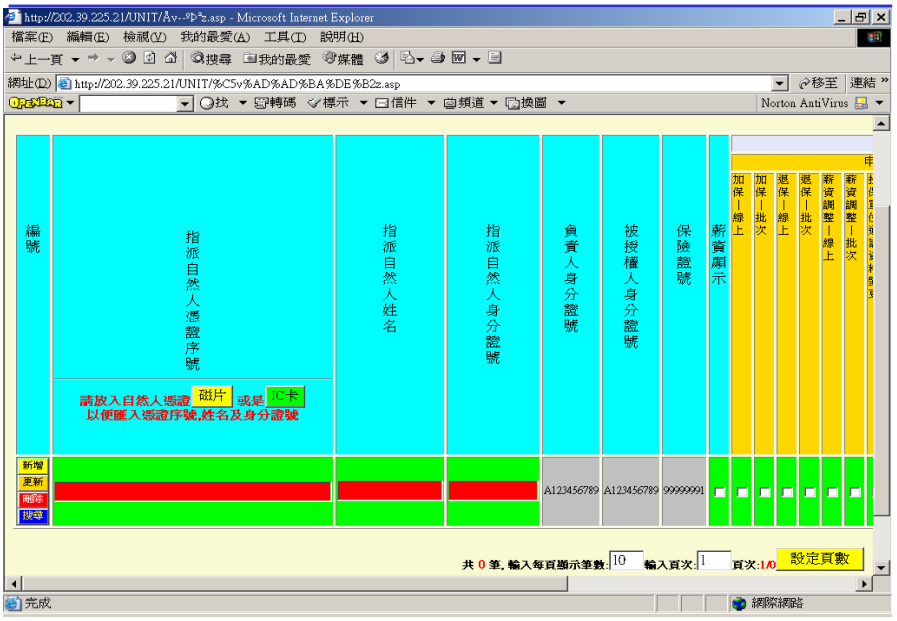

瀏覽器
伺服器
資料庫
輸入資料
含數位簽章的數位信封
解數位信封驗數位簽章
SQL,PL/SQL Pro*C/C++
Table
顯示收件通知
解數位信封驗數位簽章
含數位簽章的數位信封
Active X
ISAPI

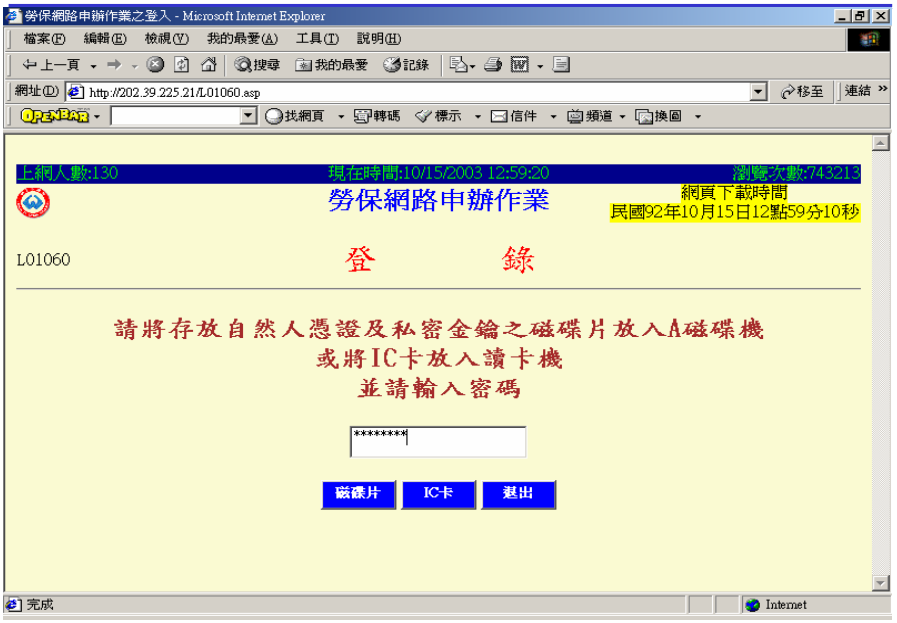
憑證查驗

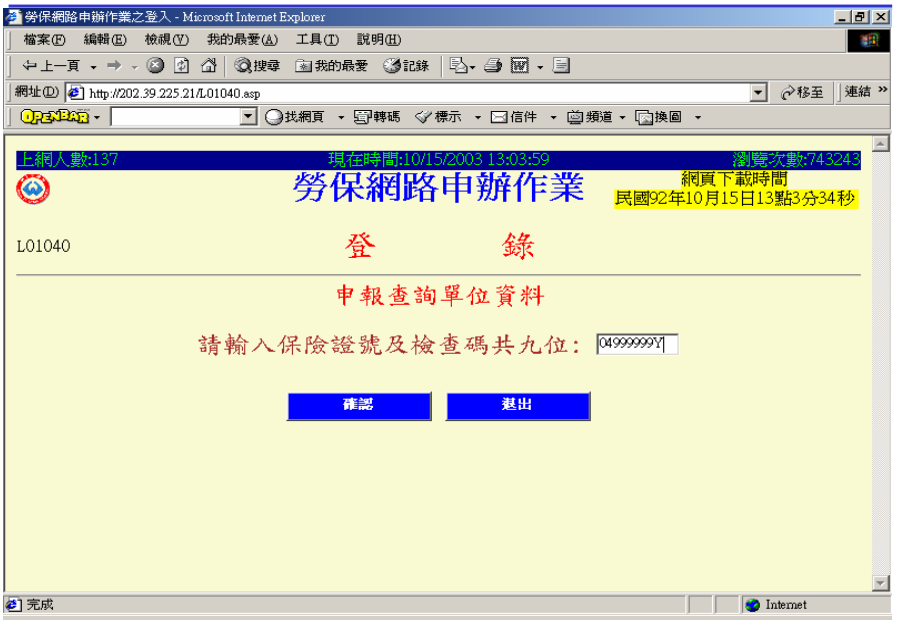
1.驗CA憑證
  是否爲GRCA所簽發的？
  是否過期？
  是否被廢止？(CRL檢查)
2.驗憑證
  是否爲CA所簽發的？
  是否過期？
  是否被廢止？(CRL檢查)

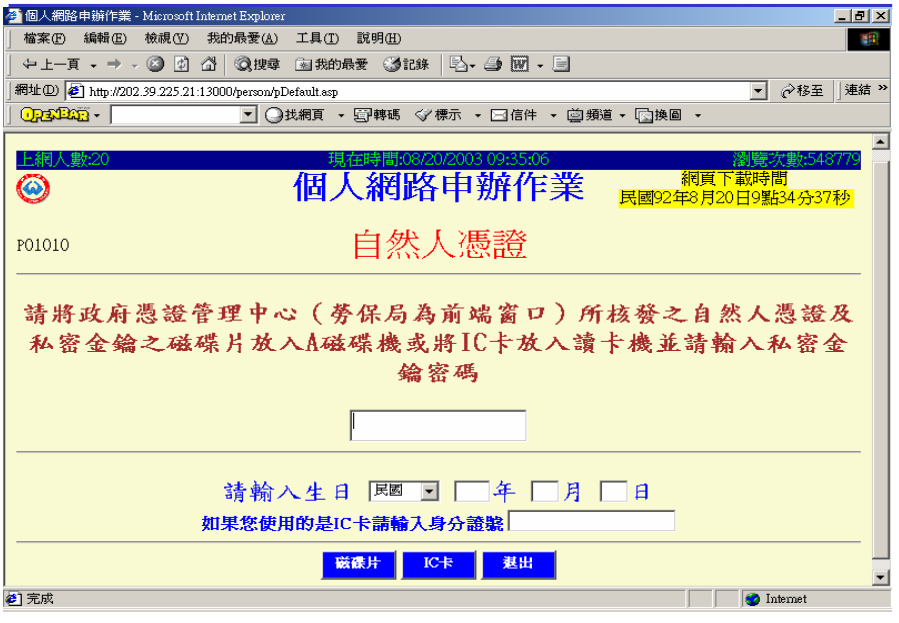

網路指派作業之登入 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
網址(D) http://202.39.225.21/l01020.asp
上網人數:412
現在時間:2004年2月20日 上午 11:11:26
瀏覽次數:1366510
網路申辦指派作業
網頁下載時間
民國93年2月20日11點11分17秒
L01020
(單位主卡)登錄
請將政府憑證管理中心（勞保局為前端窗口）所核發之單位憑證及私密金鑰之磁碟片放入A磁碟機或將IC卡放入讀卡機並請輸入私密金鑰密碼
如果您使用的是IC卡請輸入貴單位之單位證號
磁碟片
IC卡
退出
注意事項：
工商憑證IC卡PIN碼(即密碼)輸入三次以上錯誤，即造成IC卡鎖卡，請至經濟部憑證管理中心之發卡中心網頁https://www.ecard.net.tw左方選項中，點選『鎖卡解碼』，接著點選『MOEACA』，依照網頁說明指示進行『重設PIN碼』，『鎖卡解碼說明』下載。
完成
網際網路

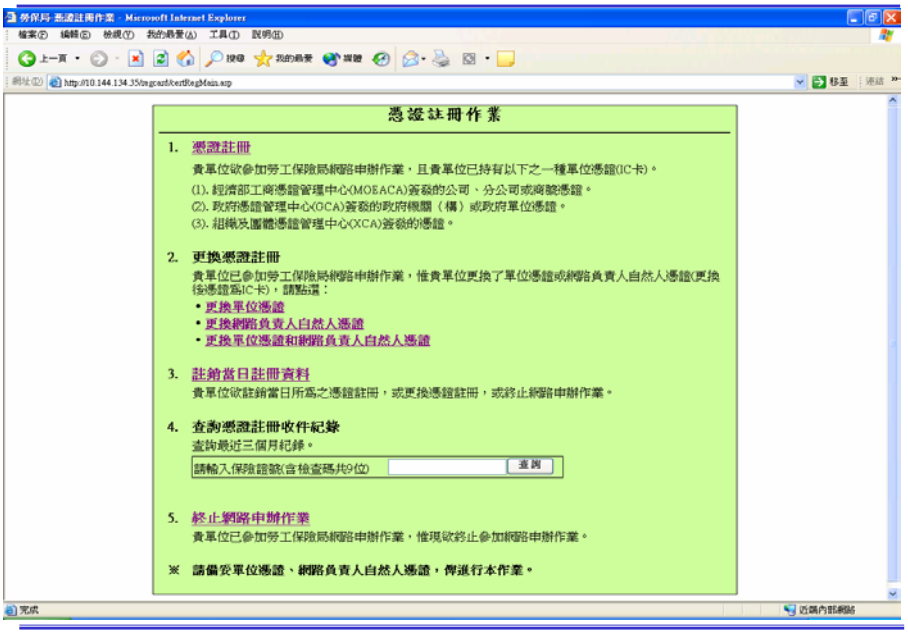

勞保網路申辦指派作業 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
網址(D) http://202.39.225.21/L01030.asp
上網人數:422
現在時間:2004年2月20日 上午 11:13:10
瀏覽次數:1366534
勞保網路申辦指派作業
網頁下載時間
民國93年2月20日11點12分47秒
L01030
勞工保險局(負責人或其授權之人)登錄
請將存放自然人憑證及私密金鑰之磁碟片放入A磁碟機或將IC卡放入讀卡機並請輸入密碼
如果您使用的是IC卡請輸入身分證號
磁碟片
IC卡
退出
完成
網際網路

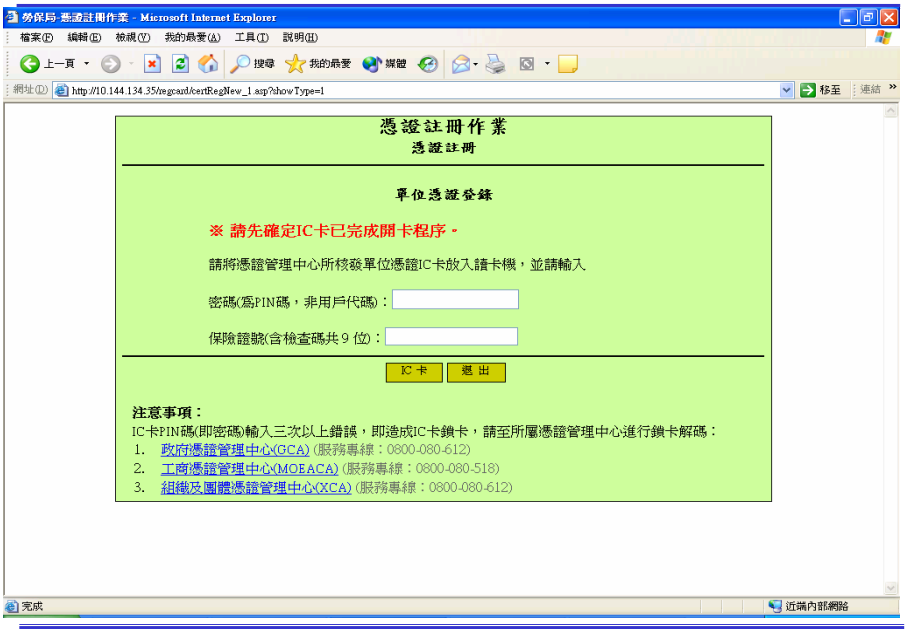

http://202.39.225.21/UNIT/Åv--ºÞ°¿.asp - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
網址(D) http://202.39.225.21/UNIT/%C5v%AD%AD%BA%DE%B2z.asp
編號
指派自然人憑證序號
請放入自然人憑證 磁片 或是 IC卡
以便匯入憑證序號,姓名及身分證號
指派自然人姓名
指派自然人身分證號
負責人身分證號
被授權人身分證號
保險證號
薪資顯示
加保-線上
加保-批次
退保-線上
退保-批次
薪資調整-線上
薪資調整-批次
新增
更新
刪除
搜尋
A123456789
A123456789
99999991
共 0 筆, 輸入每頁顯示筆數: 10 輸入頁次: 1 頁次:1/0 設定頁數
完成
網際網路

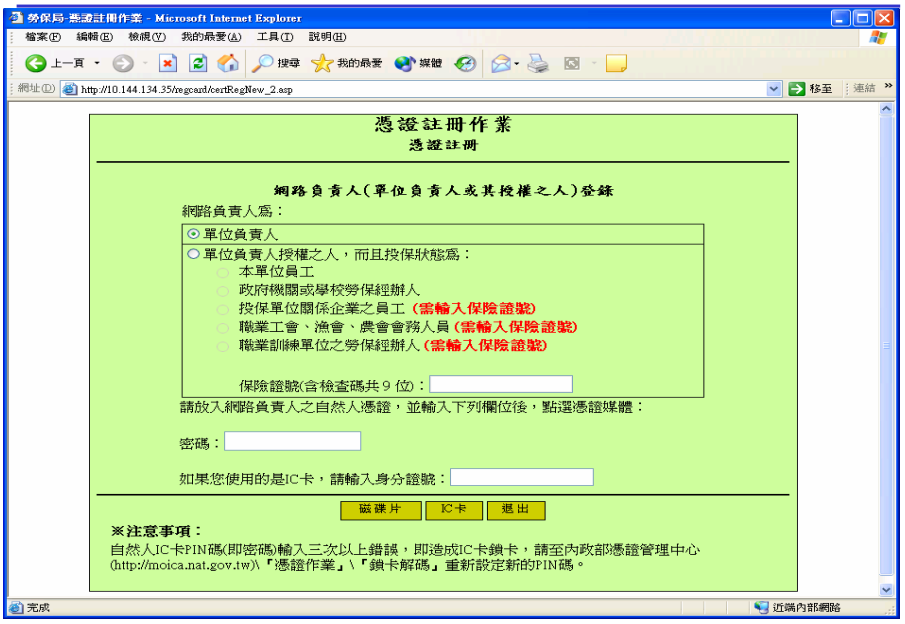

勞保網路申辦作業之登入 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
網址(D) http://202.39.225.21/L01060.asp
上網人數:130
現在時間:10/15/2003 12:59:20
瀏覽次數:743213
勞保網路申辦作業
網頁下載時間
民國92年10月15日12點59分10秒
L01060
登 錄
請將存放自然人憑證及私密金鑰之磁碟片放入A磁碟機
或將IC卡放入讀卡機
並請輸入密碼
磁碟片
IC卡
退出
完成
Internet

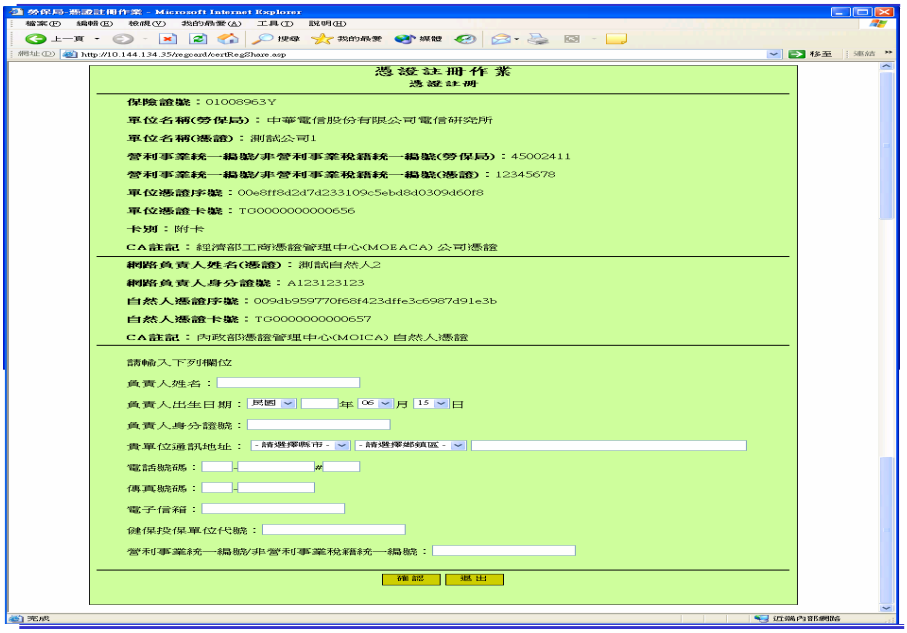

勞保網路申辦作業之登入 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛 記錄
網址(D) http://202.39.225.21/L01040.asp
移至 連結
找網頁 轉碼 標示 信件 頻道 換圖
上網人數:137
現在時間:10/15/2003 13:03:59
瀏覽次數:743243
勞保網路申辦作業
網頁下載時間
民國92年10月15日13點3分34秒
L01040
登 錄
申報查詢單位資料
請輸入保險證號及檢查碼共九位:
04999999Y
確認
退出
完成
Internet


個人網路申辦作業 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛 記錄
網址(D) http://202.39.225.21:13000/person/pDefault.asp
移至 連結
找網頁 轉碼 標示 信件 頻道 換圖
上網人數:20
現在時間:08/20/2003 09:35:06
瀏覽次數:548779
個人網路申辦作業
網頁下載時間
民國92年8月20日9點34分37秒
P01010
自然人憑證
請將政府憑證管理中心(勞保局為前端窗口)所核發之自然人憑證及私密金鑰之磁碟片放入A磁碟機或將IC卡放入讀卡機並請輸入私密金鑰密碼
請輸入生日 民國 年 月 日
如果您使用的是IC卡請輸入身分證號
磁碟片
IC卡
退出
完成
Internet


憑證註冊作業
1. 憑證註冊
貴單位欲參加勞工保險局網路申辦作業，且貴單位已持有以下之一種單位憑證(IC卡)。
(1). 經濟部工商憑證管理中心(MOEACA)簽發的公司、分公司或商號憑證。
(2). 政府憑證管理中心(GCA)簽發的政府機關（構）或政府單位憑證。
(3). 組織及團體憑證管理中心(XCA)簽發的憑證。
2. 更換憑證註冊
貴單位已參加勞工保險局網路申辦作業，惟貴單位更換了單位憑證或網路負責人自然人憑證(更換後憑證為IC卡)，請點選：
• 更換單位憑證
• 更換網路負責人自然人憑證
• 更換單位憑證和網路負責人自然人憑證
3. 註銷當日註冊資料
貴單位欲註銷當日所寫之憑證註冊，或更換憑證註冊，或終止網路申辦作業。
4. 查詢憑證註冊收件紀錄
查詢最近三個月紀錄。
請輸入保險證號(含檢查碼共9位)
查詢
5. 終止網路申辦作業
貴單位已參加勞工保險局網路申辦作業，惟現欲終止參加網路申辦作業。
※ 請備妥單位憑證、網路負責人自然人憑證，俾進行本作業。


憑證註冊作業
憑證註冊
單位憑證登錄
※ 請先確定IC卡已完成開卡程序。
請將憑證管理中心所核發單位憑證IC卡放入讀卡機，並請輸入
密碼(為PIN碼，非用戶代碼)：
保險證號(含檢查碼共9位)：
IC卡
退出
注意事項：
IC卡PIN碼(即密碼)輸入三次以上錯誤，即造成IC卡鎖卡，請至所屬憑證管理中心進行鎖卡解碼：
1. 政府憑證管理中心(GCA) (服務專線：0800-080-612)
2. 工商憑證管理中心(MOEACA) (服務專線：0800-080-518)
3. 組織及團體憑證管理中心(XCA) (服務專線：0800-080-612)


勞保局-憑證註冊作業 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛 媒體
網址(D) http://10.144.134.35/regcard/certRegNew_2.asp
移至 連結
憑證註冊作業
憑證註冊
網路負責人(單位負責人或其授權之人)登錄
網路負責人爲：
單位負責人
單位負責人授權之人，而且投保狀態爲：
本單位員工
政府機關或學校勞保經辦人
投保單位關係企業之員工 (需輸入保險證號)
職業工會、漁會、農會會務人員 (需輸入保險證號)
職業訓練單位之勞保經辦人 (需輸入保險證號)
保險證號(含檢查碼共 9 位)：
請放入網路負責人之自然人憑證，並輸入下列欄位後，點選憑證媒體：
密碼：
如果您使用的是IC卡，請輸入身分證號：
磁碟片
IC卡
退出
※注意事項：
自然人IC卡PIN碼(即密碼)輸入三次以上錯誤，即造成IC卡鎖卡，請至內政部憑證管理中心(http://moica.nat.gov.tw)\「憑證作業」\「鎖卡解碼」重新設定新的PIN碼。
完成
近端內部網路

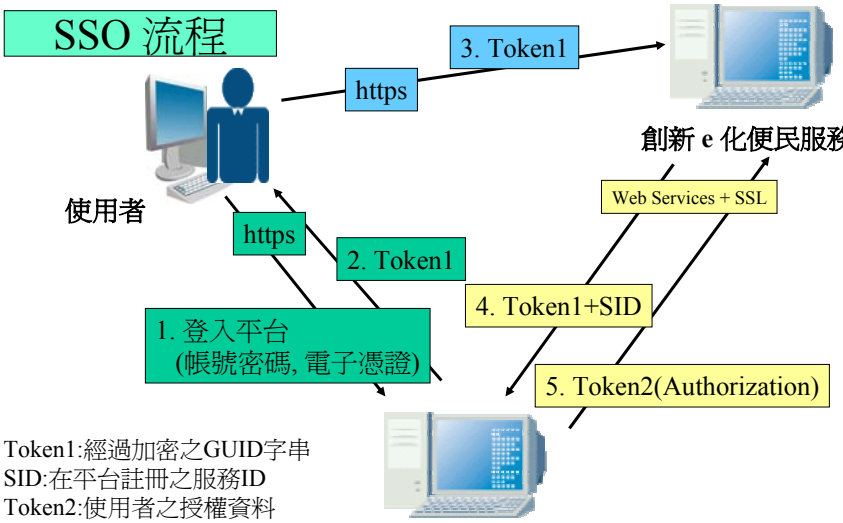

勞保局-憑證註冊作業 - Microsoft Internet Explorer
憑證註冊作業
憑證註冊
保險證號：01008963Y
單位名稱(勞保局)：中華電信股份有限公司電信研究所
單位名稱(憑證)：測試公司1
營利事業統一編號/非營利事業稅籍統一編號(勞保局)：45002411
營利事業統一編號/非營利事業稅籍統一編號(憑證)：12345678
單位憑證序號：00e8ff8d2d7d233109c5ebd8d0309d60f8
單位憑證卡號：TG0000000000656
卡別：附卡
CA註記：經濟部工商憑證管理中心(MOEACA) 公司憑證
網路負責人姓名(憑證)：測試自然人2
網路負責人身分證號：A123123123
自然人憑證序號：009db959770f68f423dffe3c6987d91e3b
自然人憑證卡號：TG0000000000657
CA註記：內政部憑證管理中心(MOICA) 自然人憑證
請輸入下列欄位
負責人姓名：
負責人出生日期：民國 年 06 月 15 日
負責人身分證號：
貴單位通訊地址：- 請選擇縣市 - - 請選擇郵遞區 -
電話號碼：
傳真號碼：
電子信箱：
健保投保單位代號：
營利事業統一編號/非營利事業稅籍統一編號：
確認
退出
完成
近端內部網路

共通作業平台

建構一個安全的電子化政府互通環境，
以整合政府資訊服務資源，
協同各級機關，
突破現有作業瓶頸，
推動跨機關創新e化服務。

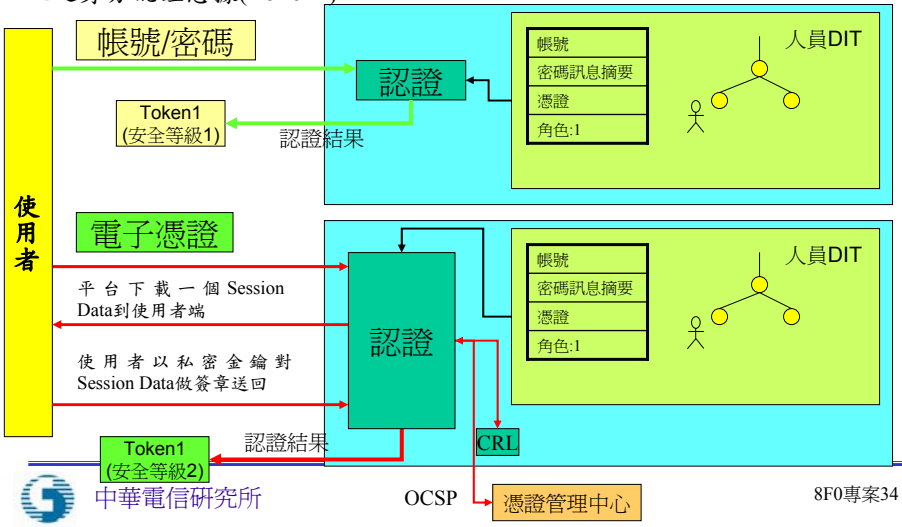
共通作業平台

共通作業平台-認證授權機制



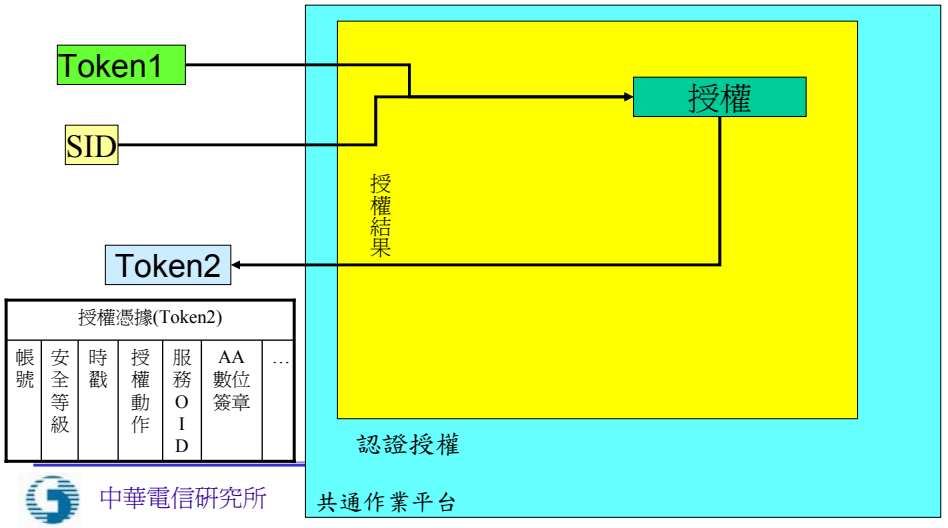
共通作業平台-認證授權機制

認證:根據帳號密碼/電子憑證透過目錄服務取得身分認證資料產生單一簽入之身分認證憑據(Token1)。



共通作業平台-認證授權機制

授權:以角色為主，根據身分認證憑據(Token1)與服務識別碼(SID)透過目錄服務取得授權角色及權限資料以產生授權憑據(Token2)。



共通作業平台-認證授權機制

單一簽入:使用者只要取得單一簽入結果Token1之後，使用任何跨網站服務皆不需再認證，即可直接以Token1要求被授權使用之服務。