管　理　與　系　統
第十七卷 第一期　民國九十九年一月
159-182 頁

Journal of Management & Systems
Vol. 17, No. 1, January 2010
pp. 159-182

適用於網路服務之高效率整合式存取控制系統設計與實作

Design and Implementation of Integrated Access Control Systems with High Efficiency for Web Services

曹偉駿　Woei-Jiunn Tsaur　　**黃美治**　Mei-Zhi Huang

大葉大學資訊管理學系

Department of Information Management, Da-Yeh University

(Received August 16, 2006; Final Version August 24, 2009)

摘要：網路服務技術是一個幫助企業降低營運成本並提高獲利極爲有效的資訊系統架構。但隨著交易環境的多元化，訊息內容的安全與如何有效執行存取控制，將成爲網路服務環境下一大課題。目前網路服務環境的安全需求中，多採用憑證爲基礎的公開金鑰密碼系統來解決相關的問題，這使得在身份驗證及管理上具有相當的複雜度。而在現行存取控制的方法上可分爲二大類。第一類是由使用者分別向不同的網路服務站台註冊以取得相關服務，但此方法的缺點爲，系統管理者必須持續爲短暫需求使用者建立使用權限；第二類則是使用者向單一站台註冊，而站台之間以鬆散偶合 (Loosely Coupled) 的方式連結，但此方法卻也有不同網域對於使用權限認定不一致的問題。因此，本論文基於低運算量之「植基於 ECC 的自我認證公開金鑰密碼系統」與角色爲基礎的存取控制方式，建構出具有高效率的整合式存取控制系統。是故，本系統能在不使用憑證的狀況下做到使用者身份識別，同時在不影響現行企業內部存取控制的前提下，解決跨網域存取權限不一的問題。此外，與現行存取控制進行比較後發現，本系統不論在安全性與效率上都有較優的表現。相信本系統應用在企業網路服務上，將可降低維護成本並且有效減輕系統管理者負擔，進而提升存取效率。

本文之通訊作者爲曹偉駿，e-mail: wjtsaur@mail.dyu.edu.tw。

本研究接受國科會研究計畫案 NSC 97-2631-H-212-001、NSC 97-2219-E-006 -003 經費補助，特此致謝。

關鍵詞：角色爲基礎的存取控制、橢圓曲線密碼系統、自我驗證公開金鑰密碼系統、資訊安全

Abstract: Web services technology is an extreme efficient structure of information system for promoting enterprises to lower operating cost and raise profits. Nevertheless, with the pluralism of trading platforms, the security of transmitting message and how to execute the access control for information systems will become an important issue for securing the web service environment. Using certificate-based public key cryptosystems to solve the problems related to the demand of security under the current environment of web services causes rather complicated identity verifying and management. The methods of access control in operation can be divided into two kinds. One is that each user must register at different web sites, and therefore the system administrator will be busy in establishing the authority connection for these users; the other is at one specific web site, but every single site is connected with the others through the way of “loosely coupled”, but user may face the problem of different level of authority from a variety of web domains. For this reason, in this paper the mechanism of integrated access control with high efficiency is constructed using the ECC-based self-certified public key cryptosystems and role-based access control scheme. The proposed mechanism can identify the user without employing certificates, and solve the limits of access authority across different web domains without any influence upon current system operations. Furthermore, after the comparisons with the current access control schemes for web services, we can find the proposed one will be superior to the others in terms of security and efficiency. We affirm that the proposed scheme will be able to lower the cost of maintenance and lighten the burden of system administrator, and thus promote the efficiency of access control to web services environments.

Keywords：Role-Based Access Control, Elliptic Curve Cryptosystems, Self-certified Public Key Cryptosystems, Information Security.

1. 緒論

企業爲了保有市場上的競爭優勢，大多數會採取 e 化的方式，藉由資訊科技的協助，以最有效率的運作模式降低成本、提高獲利來達成營運目標。而種種跡象顯示網路服務 (Web Services) 將是未來一個極爲重要的應用架構模式，然而在此前題下，一個關鍵性的問題就是「安全」。所謂安全，除了要保障各種網路資源穩定、可靠地運轉外，還必須控制資源被合法的使用，而存取控制就是讓企業在訊息資源共享的同時也要阻止非授權使用者對企業敏感訊息存取的策略。

但隨著交易環境的多元化也讓存取控制的應用趨於複雜，這使得存取控制成爲網路服務環境下極具挑戰的問題。

目前雖然有諸多文獻 (Coetzee and Eloff, 2005; Lim *et al.*, 2004; Park *et al.*, 2001) 提出以不同方式來解決存取控制的問題，但討論的範圍多在一個簡單架構環境下的運用，對於存取權限的認定也僅設定在一些簡單架構的組織上，並未深就組織架構層次較複雜甚至是跨網域在不同組織架構下的資料存取權限控制。就拿目前網路服務的存取控制來說，針對跨平台或資源保護的解決方法都不理想 (Coetzee and Eloff, 2004)；因爲在網路服務環境中，對於任何一個系統而言，若要維護另一個系統的身份驗證許可和存取控制清單是一種不實際的作法，此外網路服務沒有固定的使用模式、服務需求者也通常是不知名的使用者，這些種種因素，相對提高了網路服務環境下存取控制的困難度。因此本論文將探討如何有效率的解決在網路服務環境下跨不同組織架構的資料存取控制。

2. 文獻探討

本研究主要的目標是在網路服務環境下建構一個高效率的存取控制系統，因此以下將針對「存取控制」與「公開金鑰密碼系統」等觀念加以介紹與探討，並提出現行網路服務架構下存取控制的類型及缺點。

2.1 角色為基礎的存取控制

存取控制又稱授權控制 (Authorization Control)，是判斷使用者或處理人員是否具有存取特有系統的資源與所能允許的存取型態的一種機制。在一般的系統當中，存取控制包含了三個要素，即主體、受體及存取權限。主體包括了一般使用者、處理程序，而受體通常指的是檔案或是可使用的資源，存取權限則是指主體被允許來存取某個受體的權利，一般可分爲讀、寫、執行和擁有等權利。

以角色爲基礎的存取控制法 (Role-Based Access-Control, RBAC)，是由 Ferraiolo and Kuhn (1992) 等學者所提出的存取權限控管模組，由於傳統的權限控管系統 例如：(Access Control Lists, ACL) 大多是使用者直接對應到權利 (Users↔Permissions)，但是當管理者在維護兩者之間的關係時，卻是一件麻煩的事，例如：當一個人員改變職位時，管理者必須對所有的物件修改這個使用者的權限，而且當使用者和物件都越來越多時，要修改的東西也就越來越多，越來越複雜。然而 RBAC 是將傳統授予使用者權利的方式改成了使用者對應到角色、角色再對應到權利 (Users↔Roles↔Permissions) 的三層式架構，如圖 1 所示。也就是說一個使用者的權利是要根據他在組織中所擁有的角色來判定。如此一來，當使用者的職位有變動時，僅僅需要改變使用者和角色之間的對應，這樣就可以節省許多維護的成本，也可以提升管理的效率。

圖 1 RBAC 基本模型

2.2 公開金鑰密碼系統

談到資訊安全，就讓人聯想到五個重要的安全訴求：身份認證 (Authentication)、機密性 (Confidentiality)、不可否認性 (Non-repudiation)、完整性 (Integrity)、及存取控制 (Access Control)。尤其在網路服務環境下從事商業行爲時，這五項訴求更是相對重要的考量因素；而不斷改進的密碼學及演算法，就是爲了配合這五大訴求所應運而生的。

爲了保護資料在傳輸過程中的安全，使用者會將原始資料以無意義或亂數型態的暗碼方式加以呈現；其中透過數學演算法將明文轉變成密文的過程稱之爲加密，反之，若將密文轉變成明文的過程，即爲解密。在加解密的過程中需要透過一把金鑰來啓動演算法。以目前的密碼系統來說，大致可分兩大類：對稱式金鑰 (Symmetric Key) 及非對稱式金鑰 (Asymmetric Key) 密碼系統。所謂對稱式，就是加解密用同一把金鑰，優點是運作速度快，缺點是有金鑰分配上的問題存在；而非對稱式則是指加解密的過程使用兩種不同的金鑰，也就是每個人擁有唯一的公鑰與私鑰，此方式不但解決了金鑰管理上的問題，而且還能用私鑰來達到數位簽章的功能，使資料的遞送有不可否認性。

而橢圓曲線密碼系統 (Elliptic Curve Cryptosystem，ECC) 是由 Miller (1986) 和 Koblitz (1987) 兩位學者所提出，主要是基於在有限場 F_p 之下，給定橢圓曲線 E 上的兩個點 P 及 Q，當點的序 (order) 夠大時，要找出一個整數 x，使得 $Q = x \cdot P$ 是很困難的，利用這個解橢圓曲線離散對數問題的困難度來確保金鑰及資料的安全性。在其運算效率上，相較於使用大指數運算的 RSA 機制而言，其所運算的時間少了許多，且所需金鑰長度只需要 160 位元，比起 RSA 與 ElGamal 系統 1024 位元長度，因所需金鑰長度較短，故可提升加/解密、簽章/驗證簽章的效能及降低儲存的成本。

至於在身分認證方式上，一般採用以憑證爲基礎的公開金鑰密碼系統，主要架構爲每一位使用者擁有身分資訊、公鑰、私鑰與保證公鑰有效性的數位憑證。雖然憑證機構可以替數位憑證的持有人作合法身分的保證與提供公鑰的有效證明，但卻存在著(1)憑證機構需耗費儲存空間與計算成本去維護金鑰目錄與管理憑證，(2)憑證機構之間有階層式關係時，會造成驗證公鑰時傳輸成本與計算複雜度的增加等缺點。因此，Girault (1991) 提出自我驗證的公開金鑰密碼系統，強調驗證機制不需要任何的憑證，就能證明使用者的身分，同時利用解離散對數問題的困難度

來確保私鑰的安全性，而且能讓系統中心無從得知任何使用者的私鑰，以避免系統中心僞造使用者的事件發生。

綜合上述，本論文將基於曹偉駿 (民 92) 及 Tsaur (2005) 所提出「植基於 ECC 的自我驗證公開金鑰密碼系統」來設計在網路服務環境下存取控制系統，使其兼顧安全與效率。

2.3 現行網路服務的存取控制

現行網路服務的存取控制方式大致上可分爲四種：

(1) 分散式

其存取權限由各服務站台自行設定，當服務需求者提出服務請求時，只要在自己的網域做認證，再透過鬆散偶合 (Loosely Coupled) 連結即可取得服務提供者的相關服務，如圖2所示。

(2) 集中式

當服務請求者向服務提供者提出需求時，服務提供者必須在伺服器上爲每一個服務請求者建立新的身份及使用權限，做爲存取資源時的依據，如圖3所示。

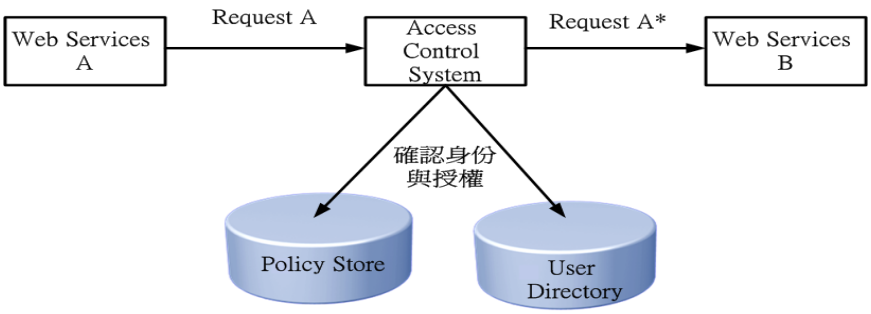

圖2 分散式存取控制模型

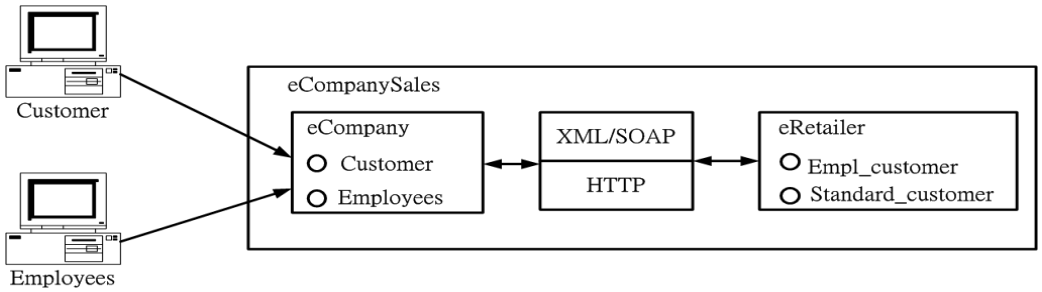

圖 3 集中式存取控制模型

(3) .NET Passport

.NET Passport 是由微軟公司提供的一種網路服務，這種服務讓使用者透過一組帳號和密碼執行登錄後，就可以獲得 Passport 合作商務網站的存取權限 (Rolf, 2004)。

圖 4 爲.NET Passport 的認證流程，其說明如下：

1) 消費者連結到相關的 Passport 合作商務網站要求服務。
2) 合作商務網站導引連結使用者到.NET Passport 網站進行登錄用戶資料。
3) 消費者依據合作商務網站的指引到.NET Passport 網站進行認證。
4) 然後消費者取得.NET Passport 網站的認證與授權。
5) 消費者持有授權證明向合作網站提出或使用相關 Web 服務。
6) 合作商務網站 Passport Manager 判讀授權內容後，檢驗通過就提供網站服務網頁給消費者進行服務與交易執行。

(4) XACML

XACML 是一種基於 XML 語言的存取控制，是由 OASIS 所提出一種網路服務環境下存取控制的標準，但若要做到跨網域的資料存取，前提是交易雙方都依靠 XACML 建立彼此的存取控制政策。

而整個XACML運作流程如圖5所示：

1) 使用者向政策執行單元 (Policy Enforcement Point, PEP) 提出資源存取請求。
2) PEP依照SAML格式，將存取請求傳送給對應授權決策的政策決定單元 (Policy Decision Point, PDP)。並且提供讓PDP可以提出授權決策所必須參考的所有屬性。
3) PDP檢查收到的存取請求，判斷是否已擁有提出授權決策的所有屬性。若是沒有，則PDP依照SAML格式對政策資訊單元 (Policy Information Point, PIP) 提出查詢所缺少屬性的要求。
4) PIP將所查詢到的屬性回傳給PDP後，PDP重新評估該存取請求並傳回給PDP。
5) PDP依照授權結果判斷是否執行存取請求。

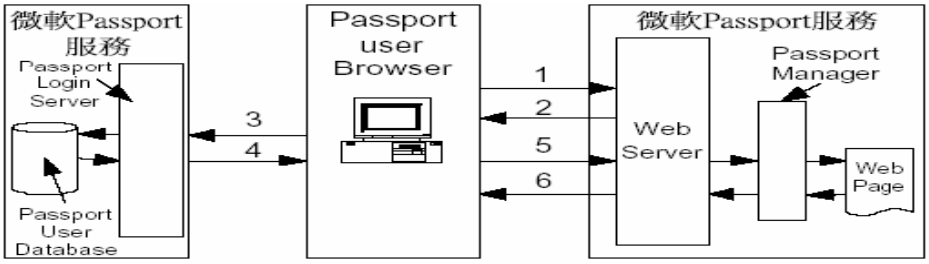

圖4 .NET Passport 認證流程

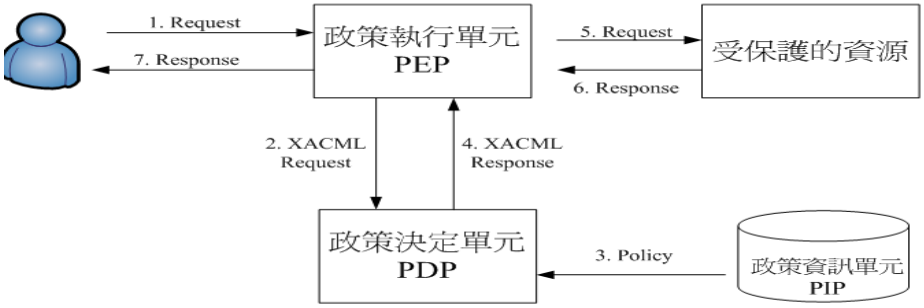

圖5 XACML存取控制模型

6) 將執行結果回傳PEP。

7) PEP 將最終結果回覆使用者。

綜合上述，可以發現目前網路服務環境下的跨平台存取控制政策不論是集中式、分散式、.NET Passport 或 XACML 都不盡理想。表 1 爲上述四種現行方式的優缺點比較。

以分散式來說，在網路服務環境下，服務需求者是透過跨網域或跨組織的方式向服務提供者提出存取需求，因此服務請求者所具備的角色身份，不見得能對應到服務提供者的存取權限；至於集中式看似較佳的方案，對服務提供者而言，這樣的存取需求可能只是短暫的行爲，但伺服器卻必須不斷忙碌的建立服務需求者的存取權限，而這樣的行爲對系統管理而言可謂是一大

表 1 現行網路服務存取控制之比較

存取控制方法	優點	缺點
分散式	使用者存取權限透過站台之間鬆散偶合即可取得。	造成使用者權限過大或過小甚至無法判別的情況。
集中式	使用者的存取權限可明確設定。	必須爲所有使用者建立存取權限，增加管理者負擔。
.NET Passport	使用者從登入到網站連結以及執行都很簡便。	採用帳號密碼的身份識別，對於系統的安全性具有較大的威脅；此外企業無法直接有效分析使用者資訊。
XACML	爲 OASIS 在網路服務環境所提出的標準。	當服務請求較爲複雜時，必須花費較多的處理時間而所造成的延遲會令人無法接受。

負擔。而.NET Passport 也是集中式存取控制的一種，在這種方案中，使用者的身份辨識僅依靠帳號、密碼而定，若使用者的帳號密碼被盜取時，對系統的安全將會出現較大的影響 (Rolf, 2004)，除了必須擔心顧客的資料遭到第三方的利用外，對於未來企業在顧客分析的效能上，也將會因資料的不夠充份而變得非常薄弱。最後，對於 XACML 而言，雖然是由 OASIS 所提供的一種網路服務環境下存取控制的標準，但若要做到跨網域的資料存取，前提是交易雙方都需依靠 XACML 建立彼此的存取控制政策。此外，在任何系統中，特別是企業級系統中，效能都是一個重要關鍵的因素。例如，當某個 Client 端透過 Http 請求呈現一個聚集了許多種資訊的網頁頁面時，若這種請求需要許多存取決策，由於 XACML 並不直接支援基於角色的存取控制 (Coetzee and Eloff, 2005)，如果利用 XACML 來處理這種狀況，勢必就會產生許多 Request，因爲每一個 Request 可能只包含單個授權存取的元素。這樣，收集所有存取決策所花費的處理時間和延遲是令人無法接受的。此外，由於一般企業或安全產品供應商都有提供存取規則設定，因此 XACML 必須能提供一種要與現有方式整合的簡單作法，才能取得企業的支持。因此本論文將在第三節提出一個在網路服務環境下，能夠有效率執行存取控制的方法。

3. 整合式存取控制系統

以角色爲基礎的存取控制比起傳統的存取控制，不僅在維護上提供較便利及彈性的管理外，還能對權限給予合理的分配，提高資訊系統的安全；然而文獻中多半都是針對企業內部的環境加以討論，並未探討跨網域或是跨組織下的存取控制。因此，在本論文中，除了配合網路服務的環境外，還考量到跨網域的存取控制多屬暫時性的存取需求，同時爲了兼顧系統的安全性，故本論文採用 Sandhu *et al.* (1996) 所提以角色爲基礎的存取控制模型的架構，並結合曹偉駿 (民 92)、Tsaur (2005) 所提出植基於 ECC 之自我認證公開金鑰密碼系統，建構出可在網路服務環境下使用的存取控制系統。

3.1 整合式網路服務存取控制運作流程

在本系統中，主要是結合角色爲基礎的存取控制與 ECC 爲基礎之自我認證公開金鑰密碼系統，並且適用於跨網域存取與內部存取的需求，其運作模式如圖 6 所示。

3.1.1 內部存取

內部存取的運作方式如圖 6 中 1.1 至 1.5 的步驟。以下將詳述其運作流程：

步驟 1.1 使用者 A 登入公司 A 的網路服務站台時，透過應用程式輸入身份資料及內部存取控制需求。

步驟 1.2 應用程式將使用者 A 身份交由認證伺服器確認使用者 A 是否爲一合法的內部使用者，並將驗證結果回傳給應用程式。

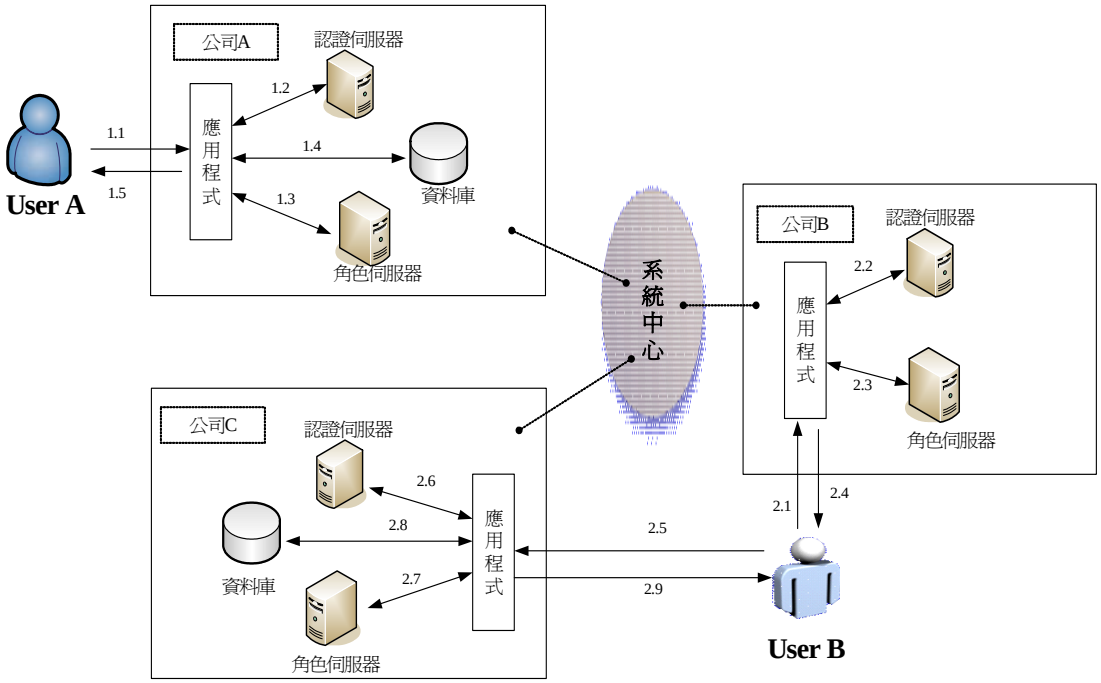

圖 6　整合式存取控制架構

步驟 1.3　應用程式確認使用者 A 爲合法使用者後，將其身份及服務請求傳給角色伺服，角色伺服器會依使用者身份計算角色存取權，並將結果回報應用程式。

步驟 1.4　應用程式依照角色存取權，判斷是否提供服務。

步驟 1.5　應用程式將執行結果回報給使用者 A。

3.1.2 跨網域存取

在圖 6 中 2.1 至 2.9 的步驟則爲跨網域存取的運作流程，其步驟詳述如下：

步驟 2.1　使用者 B 登入公司 B 的網路服務站台，透過應用程式輸入身份資料並且提出跨網域存取控制需求。

步驟 2.2　應用程式將使用者 B 身份交由認證伺服器。

步驟 2.3　驗證通過後，應用程式將使用者 B 身份傳給角色伺服計算角色值，並將結果回報應用程式。

步驟 2.4　應用程式將角色值回傳使用者 B。

步驟 2.5　使用者 B 透過公司 C 的應用程式輸入角色值與服務請求。

步驟 2.6　公司 C 的認證伺服器會先確認使用者 B 的身份，並將結果告知應用程式。

步驟 2.7　若使用者 B 身份驗證通過，即將角色值與服務請求傳給角色伺服器，計算角色存取

權限。

步驟 2.8 應用程式依角色存取權限判斷是否執行服務。

步驟 2.9 最後將服務結果告知使用者 B。

在了解了本系統的運作模式後，爲了具體實現高效率整合式存取控制系統，以下將針對本系統執行過程中的系統設定階段、註冊階段、登入及驗證階段、資料加解密以及存取控制設計等過程加以說明，並且進一步說明在本系統下如何有效執行內部存取以及網路服務環境下之跨網域存取的流程。

3.2 系統設定階段

在此階段中，系統中心會公佈相關資料，如系統中心的公開金鑰、橢圓曲線方程式以及系統中心的存取規則等。以下爲本系統所使用到的系統參數：

SA、WS_i、U_a：分別代表系統中心、網路服務站台 i 、使用者 a。

RS：角色伺服器。

E：橢圓曲線方程式 $y^2 = x^3 + ax + b$ ，其中 $4a^3 + 27b^2 \neq 0$ 。

p：大質數，長度 160 位元。

F_p：爲一有限場，且 F_p 爲 (x, y) 滿足方程式 E，$E(F_p)$表示 E∪{O}，其中 O 爲遠方的一個點。

B：序爲 n 的點，亦即橢圓曲線上的生成點，且 n 爲一大質數，長度爲 160 位元。

P_z：公鑰， $z \in \{SA, WS_i, U_a\}$ 其中 $P_{SA} = s_{SA} \cdot B \ (mod\ p)$。

s_z：私鑰， $z \in \{SA, WS_i, U_a\}$ 。

w_k ：公鑰證明， $k \in \{WS_i, U_a\}$ 。

I_k ：身份識別資訊， $k \in \{WS_i, U_a\}$ 。

rn_z：*隨機任選數值*， $z \in \{SA, WS_i, U_a\}$ ，$rn_z \in [2, n-2]$。

$h(\ )$：單項雜湊函數 (One-way hash function)，其輸出爲一固長度之整數 j， $j \in [2, n-2]$ 。

E 、 B 、p、 n 、 P_{SA} 、h：系統中心的公開參數。

此外，由於存取規則的制定與存取權限的建立每個企業都不盡相同，而這也使得在網路服務環境中的存取控制會產生主體或受體在不同網路服務站台 (Web Site) 中具有不同的定義。因此，在本論文中提出角色轉換 (Role Transform) 的做法，假設各 Web Site 從系統中心獲存取政策中含有 p 個存取角色 (本論文稱之 CA_Role) 所成的集合，且每個角色均給予一個不同角色值 (Role value)。而各 Web Site 即可依照內部存取定義與存取規則，建立一個角色轉換表 (Role Transform Table) 將 CA_Role 對應到 Web_Role，如表 2 所示，而跨網域使用者便可依照角色值在不同站台下取得相對應的服務。

表 2 CA_Role 與 Web_Role 對照

CA_Role	角色值	Web_Role
CA1	2	W3
CA2	3	W2
CA3	5	W1
CA4	7	W4

3.3 註冊階段

在本階段中，註冊的目的在透過 ECC 爲基礎之自我認證公開金鑰密碼系統以取得公鑰及私鑰。而在本系統中的註冊階段可分二個部份，第一部份註冊者爲網路服務站台 (Web Site) 向註冊單位 (系統中心) 註冊，其註冊程序如圖 7 中步驟 1-3 所示。而第二部份註冊者則爲使用者向註冊單位 Web Site 註冊，其程序如圖 7 中步驟 4-6 所示。

而以本機制中使用者註冊階段爲例，其 XML 語法如圖 8 所示。

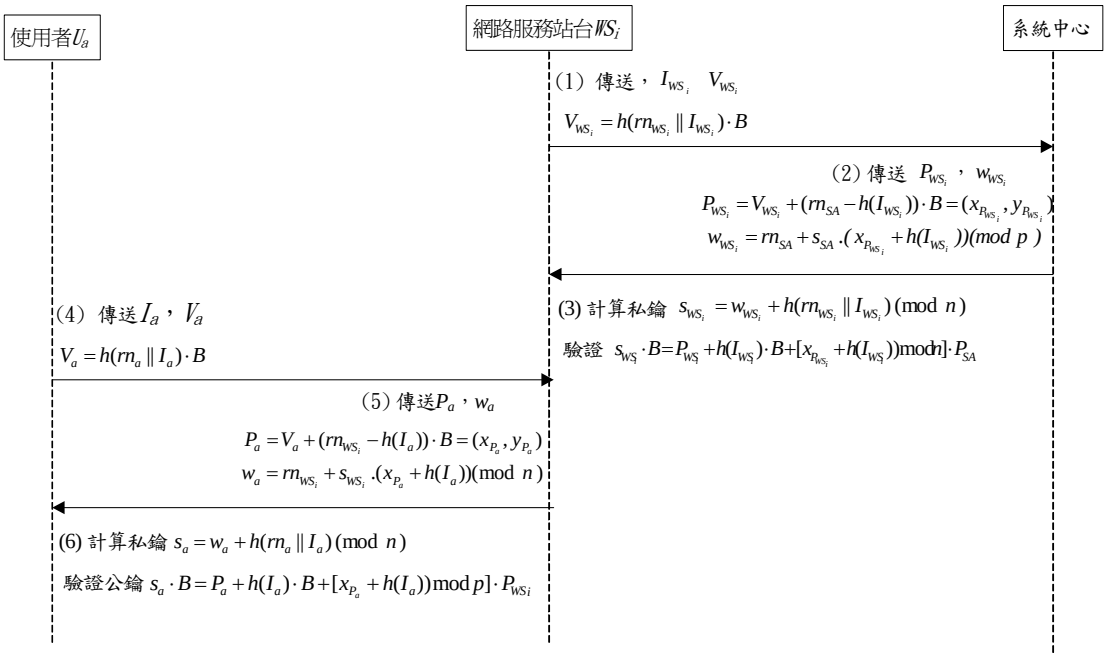

圖 7 本系統註冊階段程序

```
<?xml version="1.0" encoding="utf-8" ?>
- <xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/2002/XSL/Transform">
- <xsl:template match="/dataroot">
   <xsl:apply-templates select="使用者註冊" />
   </xsl:template>
- <table width="320" border="1">
   - <tr>
      - <td width="120">
      員工編號:
      <br />
      隨機亂數:
      <br />
      </td>
   - <td width="200">
      <xsl:value-of select="員工編號" />
      <br />
      <xsl:value-of select="隨機亂數" />
      <br />
      </td>
   </tr>
</table>
   </xsl:template>
   </xsl:stylesheet>
```

圖 8　使用者註冊之 XML 語法

3.4 登入與驗證階段

身份驗證階段主要目的是確認使用者爲一合法的使用者。當身份驗證通過後，註冊者才有權進入系統使用。本階段與註冊階段相同，具有二個部份。在第一部份中，當系統中心成功驗證站台 WS_i 的身份時，則可取得系統中心所設定的存取權限規則，如圖 9 中步驟 1 至 6 所示。而在第二部份若站台 WS_i 對使用者身份驗證成功，使用者即可登入站台，並取得相對應的角色，其程序如圖 9 中步驟 7 至 12 所示。

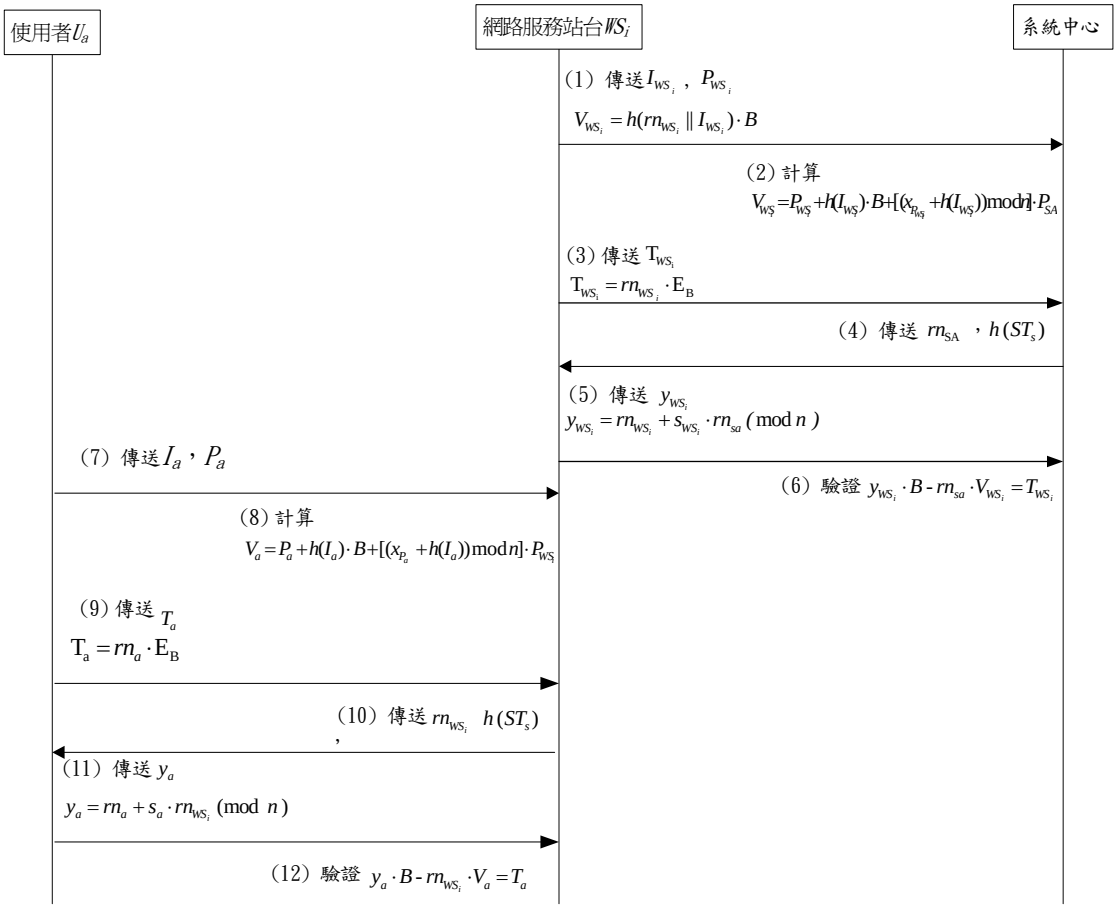

圖 9 認證階段程序

當服務站台通過系統中心的身份驗證後即可取得系統中心所設定的存取權限規則如圖 10 所示。

3.5 資料加/解密

本節將說明使用者與站台 i之間傳送與接收資料時，如何進行加密與解密，程序如圖 11 所示。

3.6 以角色為基礎的存取控制設計

當使用者登入經過身份驗證後，即可依照身份取得 Web Site 所提供相關的服務。而在角色權限的設計上，爲了能與身份驗證做一整合，加速處理上的效能，因此本論文利用 Hwang *et al.*

```
<AccessContorlPolicy>
    <Roles>
        <Role1>
            <CA_Role>CR1</CA_Role>
            <Rolename>Standard_Customer</Rolename>
            <RoleDescription>.....</RoleDescription>
            <RoleValue>2</RoleValue>
        </Role1>
        <Role2>
            <CA_Role>CR2</CA_Role>
            <Rolename>Gold_Customer</Rolename>
            <RoleDescription>.....</RoleDescription>
            <RoleValue>3</RoleValue>
        </Role2>
         :
         :
    </Roles>
</AccessContorlPolicy>
```

圖 10　系統中心存取權限政策

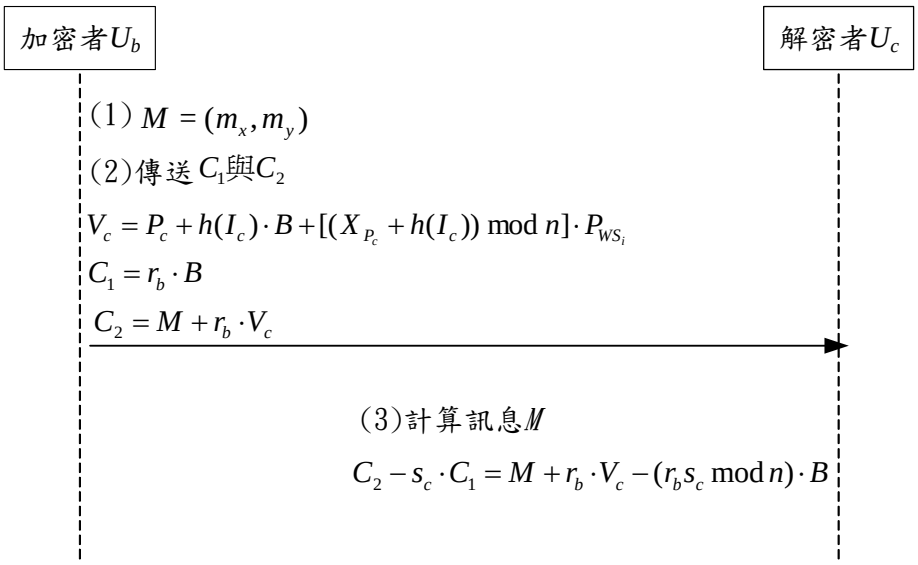

圖 11　訊息加/解密程序

(1992) 等學者所提出「將一整數分解成質因數的乘積是唯一」的特性，計算角色所含存取控制範圍。將每個存取權限與資源所產生的元素，對應一個質數值，且每個質數值都是唯一且彼此互質，如圖 12 所示。而每個角色與可用資源的授權關係如圖 13 所示

然而，以目前企業組織的架構來說，必定存在著一個職位階層的概念，因此假設 Web Site 的角色繼承關係如圖 14 所示。因此，便可以計算出每個角色的存取值（Role Control, RC）如表 3 所示。

而在存取控制的設計上，只要將每個角色所擁有的存取集合所對應的質數相乘，產生每個角色所具有的存取資訊。如此便可透過存取資訊與授權配對所對應乘積相除，而有效判斷使用者是否具有存取權限。

		存取權限		
		執行	讀取	寫入
可用資源	OR_1	3	5	7
	OR_2	11	13	17
	OR_3	19	23	29
	OR_4	31	37	41

圖 12　可用資源與存取權限對應關係

		可用資源授權集合
角色	W_1	{3 ，19 ，41}
	W_2	{13 ，23 ，31，1}
	W_3	{5，17，19}
	W_4	{7，23，1}

圖 13　角色與可用資源授權的對應關係

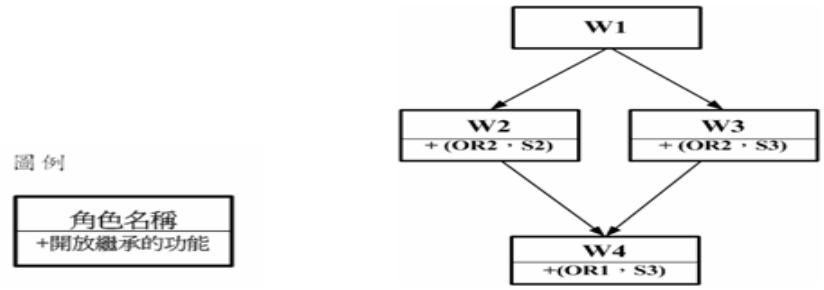

圖 14　角色階層架構

表 3　角色具有的存取資訊

角色	角色存取值	可用資源與權限
W_1	$3*19*41*13*17*7=3615339$	OR_1執行、OR_3執行、OR_4寫入、OR_2讀取、OR_2寫入、OR_1寫入
W_2	$13*23*31*7=64883$	OR_2讀取、OR_3讀取、OR_4執行、OR_1寫入
W_3	$5*17*19*7=11305$	OR_1讀取、OR_2寫入、OR_3執行、OR_1寫入

3.7 內部存取階段

當使用者登入時，站台可透過 ECC 自我認證公開金鑰密碼系統，判讀使用者是否爲內部使用者，若使用者爲內部使用者，角色伺服器即可依照使用者身份下達查詢指令，如圖 15 所示。並且依站台內自訂的存取控制政策確認是否提供相關的服務。其過程如圖 16 所示，並說明如下：

```
<bib>
  {
    for $b in document("bib.xml")//user
    where $b/department = "carcent" and $b/@id=3333
    return
        <user>
            { $b/@id }
            { $b/title }
            { $b/role_control}
        </user>
    sortby (title)
  }
</bib>
```

圖 15　查詢使用者身份

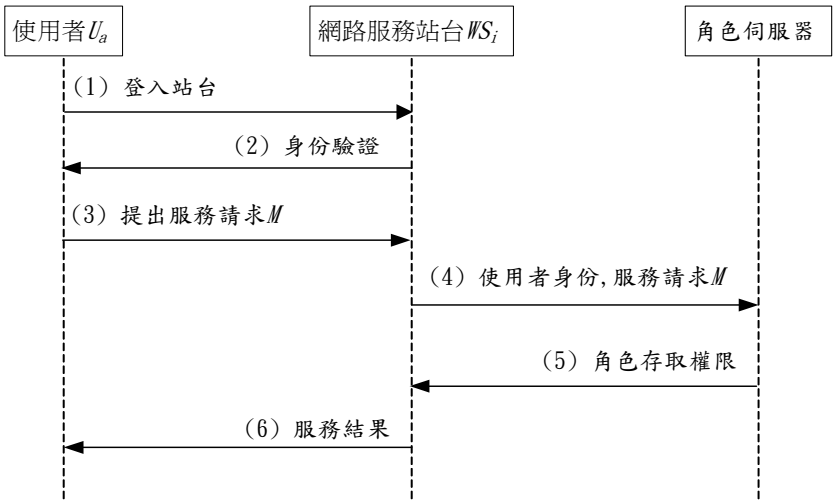

圖 16　內部存取階段程序

3.8 跨網域存取階段

在跨網域存取階段，主要是以網路服務環境下的跨網域存取控制爲主要應用，其程序如圖 17 所示。當使用者登入後，提出另一個站台的服務請求時，原註冊站台即能依照使用者所持有

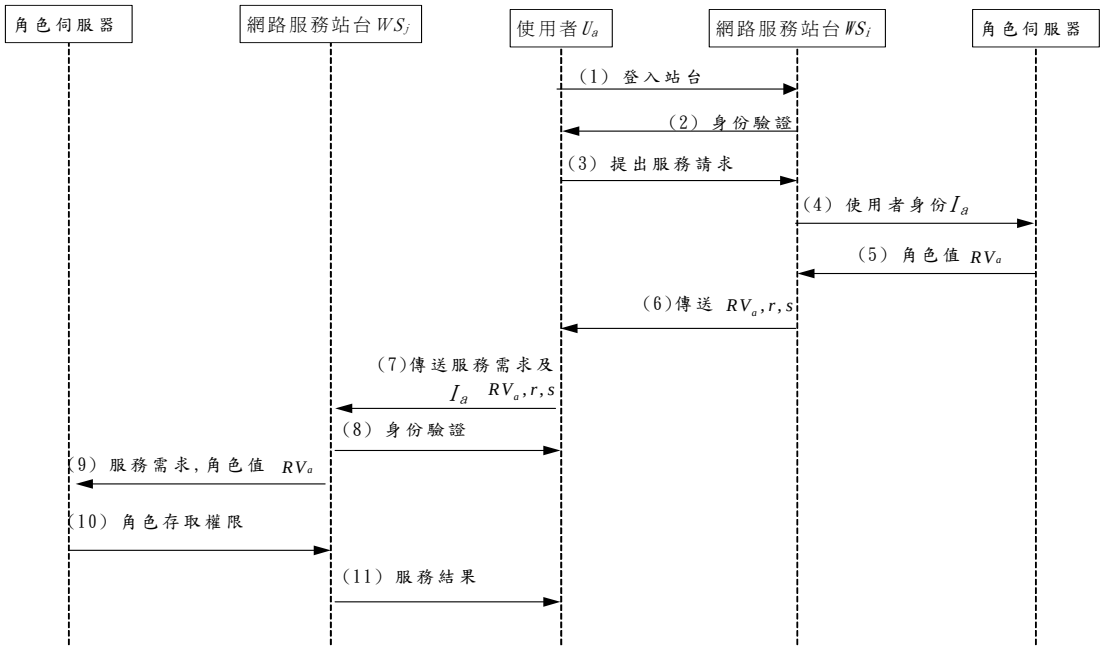

圖 17　跨網域存取階段程序

的身份，依照存取規則計算出系統中心所規範的角色值 (Role Value，RV)，並以數位簽章的方式將角色資訊傳送給使用者；而使用者就能持簽章後的角色值向跨網域站台提出服務需求。而跨網域站台亦能依照角色資訊，確認是否提供使用者相關的服務需求。

4. 安全性與效能分析

以下章節針對本論文所提系統的「安全性分析」、「效能分析」及「與現行機制比較」等相關內容進行探討與比較。

4.1 安全性分析

在本論文所提出的各項安全機制中，其安全性主要是基於解橢圓曲線離散對數問題與單向雜湊函數的困難度。以下分別列出本論文架構下滿足身份認證、機密性、完整性、不可否認性與存取控制的各項安全性分析：

■ 身份認證

根據自我驗證的方法，使用僞造的公鑰進行加/解密或簽章也不會成功，因此所有的僞冒行爲皆會被發現。此外，註冊單位無法推得註冊者的私鑰，除非能破解註冊者在註冊階段所生的 V_{WS_i} 或 V_a ，但不論 V_{WS_i} 或是 V_a 要破解其困難度是基於解單向雜湊函數問題的困難度，因此可避免假造身份的問題。

■ 機密性

在本論文所提系統下，攻擊者要從訊息傳送端傳遞的 C_1 與 C_2 解出明文，皆會遇到解橢圓曲線離散對數問題的困難度，另外，訊息傳送端每次使用不同的隨機整數 r_b ，因此攻擊者亦很難經由累積多個 C_1 與 C_2 而計算出明文。

■ 完整性

完整性是指在資料傳送過程中不會遭到惡意修改、刪除或寫入等攻擊。雖然攻擊者可以取得公鑰與身份識別資訊，但基於解橢圓曲線離散對數困難度，攻擊者無法從公鑰獲得使用者或站台的私鑰。也因此，攻擊者無法將攔截到的訊息加以解密與修改後，再傳至另一方。

■ 不可否認性

攻擊者如果要從網路服務站台所傳遞的數位簽章解出其私鑰，皆會遇到解橢圓離散對數問題的困難度。另外，使用者每次皆使用不同的隨機整數，因此攻擊者亦很難計算出 WS_i 的私鑰。而藉由私鑰的安全性，WS_j 將可確保使用者所持有的角色值爲 WS_i 所簽署核可。

■ 存取控制

存取控制除了必須設定合法使用者所具有的存取權限外，並且需要判斷使用者所提出的服務請求是否符合所授予的權限。因此，當使用者登入後，透過階層式角色爲基礎的存取控制，

可由角色伺服器取得使用者的相關存取角色值 RC，並利用「將一整數分解成質因數的乘積是唯一」的特性，判斷服務請求是否符合角色所含存取控制範圍，以達到存取控制的目的。

此外，表 4 是針對三種不同身分驗證與授權方式之分析比較。在表中“＋”代表該項具有優勢，“＋＋”代表更強的優勢；反之，“－”則代表該項不具有優勢。在各項評估標準中，安全性主要針對是否能阻擋惡意使用者通過身份驗證以存取資源爲主，由 Lopeza *et al.* (2004) 針對 .NET Passport 的探討中發現，以公開金鑰爲基礎的身份驗證與授權均優於 .NET Passport，故憑證爲基礎的方法與本方法的安全性皆優於 .NET Passport，但憑證爲基礎的方法其安全性須視憑證而定，而本方法由於不需使用憑證且能讓系統中心無從得知任何使用者的私鑰，故可具備更強的安全性。而在效率評估方面，則是針對驗證與授權時資料傳輸量與計算時間複雜度是否過多來做標準，由於 .NET Passport 之身分授權是依帳號與密碼進行辨識，故使用者從登入到網站連結都很簡便，但是其系統管理屬於集中式，系統必須爲所有使用者逐一建立存取權限，故管理者之運算負擔較重；憑證爲基礎的方法則於使用公鑰時，須耗費大量傳輸成本與計算複雜度來對其作驗證；而本方法的建構是基於低運算量之「植基於 ECC 之自我認證公開金鑰密碼系統」，故可大量減少花費在公鑰有效性驗證上的計算時間與傳輸成本。至於可測量性方面，其主要是評估是否能管理大量分散使用者的憑證，因 .NET Passport 屬於集中式管理，故無法管理大量分散使用者的憑證；憑證爲基礎的方法雖可用於分散式環境中，但若使用者因與多個服務站台作連結而擁有多個憑證時，則將大量增加管理上的負擔；而本方法於分散式環境中，除了使用者不需使用憑證進行身分驗證外，更因採用以角色爲基礎的存取控制機制，故節省了許多使用者存取權限管理上的成本。另外在互通性方面，則是評估是否能處理不同類型的身份憑證，因 .NET Passport 爲集中式管理，故無法處理分散式環境中不同類型的身份憑證；憑證爲基礎的方法對於不同憑證機構所核發的憑證，雖然可讓其彼此驗證所擁有憑證之有效性，但卻也增加許多的傳輸與計算成本；而本方法不需使用憑證即能驗證使用者的合法性，故無須考量是否能處理不同類型憑證的問題。最後在保密性的評估上，則是比較在資料傳輸過程中，是否能保護

表4　用以驗證和授權的方法之評估

評估標準	.NET Passport	憑證爲基礎的方法	本方法
安全性	－	＋	＋＋
效率	＋	－	＋＋
可測量性	－	＋	＋＋
互通性	－	＋	＋＋
保密性	－	＋	＋＋

不受惡意使用者的竊聽，由於 .NET Passport 僅依靠帳號與密碼進行使用者的身分驗證，故其保密性最差；憑證爲基礎的方法雖然使用高安全的公開金鑰密碼系統，但能否達成保密性端視系統中心的可靠與否；而本方法因採用了自我認證公開金鑰密碼系統，故可防範系統中心得知任一使用者的私鑰，進而阻絕系統中心僞冒使用者的可能性。

4.2 效能分析

在現行電子商務的應用上，多是以憑證爲基礎的方式來達成身份確認與存取控制的目的。雖然憑證爲基礎的存取控制方式已被認爲適用於分散式系統中，但在效能上，憑證必須針對每一個使用者訂定存取權限，因此，當使用者可能因同時需要與多個網路服務站台往來時，將造成使用者因獲得多個憑證而增加了管理及使用上的不便程度。表 5 爲本方法與憑證機制在身份認證與存取控制效能上的分析比較。

本論文所使用以角色爲基礎的存取控制中，是以角色爲導向來設定系統的安全存取策略，因此，當某角色對於系統資源的存取權限變動時，僅需修改角色與可用資源間的對應關係，並不需要更改使用者與角色的對應。而在身份認證上，本論文採用 Tsaur (2005) 所提出的『植基於 ECC 之自我認證公開金鑰密碼系統』，除了不必依靠系統中心就能達到身分確認，同時在加、解密或加、解簽署過程中，可在同一個邏輯步驟內一併完成公鑰有效性的驗證，如此將可減少花費在驗證上的時間。

表 5　本方法與憑證機制之效能比較

比較項目	憑證機制	本方法
身分認證機制之運算	大量模數指數與模數乘法運算	較快速的橢圓曲線密碼系統之點加法運算
公開金鑰目錄之內容	包含使用者身份、公鑰與憑證	僅有使用者身份與公鑰
公鑰有效性驗證的效率	須先驗證公鑰，才可執行其後續相關之密碼學應用的運算	驗證公鑰以及後續此公鑰的密碼學應用運算，可在一個邏輯步驟內同時完成
使用公鑰之至少長度	1024 位元	160 位元
加解密機制之運算	大量模數指數與模數乘法運算	較快速的橢圓曲線密碼系統之點加法運算
存取權限識別之方式	憑證資訊	角色值資訊

4.3 與現行網路服務存取控制相比較

相較於 2.3 節所描述之現行網路服務環境下的存取控制，本系統則採用 ECC 爲基礎之自我認證公開金鑰密碼系統，不僅可避免掉一般方法所使用的數位憑證外，同時可以在不增加管理者負擔的情況下依照使用者身份取得適當的存取權限。茲將相關比較列示於表 6 中。

表 6 中所提之任何一個機制都可以保有自己的存取控制政策，做爲內部運作的依據；對於跨組織或跨網域的服務需求，使用者可以將原網路服務站台所提供的使用權限，依照系統中心的角色轉換規則，成爲服務供給者存取控制機制中所能對應的角色及存取權限。然而，因本方法採用 ECC-based 自我認證公開金鑰密碼系統的身份認證方式，不僅可在網路服務環境下有較高的安全性，同時，ECC-based 自我認證公開金鑰密碼系統的低運算量，在系統執行效率上，比起憑證爲基礎的身份認證方式來得更有效率。

5. 系統實作與模擬

爲了驗證本系統所提架構之可行性與執行效能，我們使用以下環境進行存取控制之模擬比較。

- 測試環境
  - 硬體項目

    CPU：Intel Xeon 2.0GHz 雙 CPU

    RAM：2048Mbytes

    硬碟：160GBytes

表 6 本方法與現有機制比較分析

比較項目	分散式存取控制	集中式存取控制	.NET Passport	本方法
管理者負擔	僅網域內站台	多網域站台	多網域站台	僅網域內站台
跨網域存取能力	可	可	可	可
使用者於跨網域服務需求時，在不同站台所擁有的權限	均爲相同權限	可爲不同權限	可爲不同權限	可爲不同權限
綜合評比	未考慮到跨網域時的存取控制需求	可執行跨網域存取控制，但須增加管理者負擔	亦爲集中式管理，身份授權依帳號密碼辨識，安全性較差	兼顧管理者與使用者便利性與安全性之存取控制

- 軟體項目

  作業系統：Microsoft Windows 2003 Enterprise

  應用程式：以 Microsoft VS .NET 開發

  瀏覽器：Microsoft Internet Explorer 6.0 中文版，需支援 Java Applet，以提供密碼系統之相關運算

- 模擬情境

  本論文之模擬設計，主要由 50 位使用者，平均分成甲、乙兩組並且各自在不同的網路服務站台 A、B 進行註冊，然後針對身份驗證與跨網域存取兩大功能進行分析比較。

■ 模擬結果

- 身份驗證

  隨機抽樣 15 位使用者在所註冊的站台進行身份驗證時，站台成功驗證已註冊使用者身份的辨識率爲 100%。而在跨網域直接進行身份驗證時，當乙組使用者要求在站台 A 進行身份驗證時，由於站台 A 無法使用本身的公鑰去計算出使用者的私鑰，因此無法通過身份驗證；反之，甲組使用者亦無法通過站台 B 的身份驗證。其模擬結果如表 7 所示。

- 存取權限辨識

  隨機抽樣 15 位通過身份驗證的使用者，分別測試其在註冊站台的內部存取與跨網域站台的外部存取權限辨識。在內部存取上，系統會依照使用者身份，判斷所擁有的角色權限；而在外部存取權限辨識上，當外部使用者提出存取需求時，必須提供原站台所簽核的跨網域角色值、服務請求與身份資料供系統進行身份驗證與角色轉換的動作。在本項模擬實驗中，當使用者針對所註冊站台進行資料存取時，其存取權限辨識率爲 100%，而在跨網域存取權限辨識上，其辨識率也高達 100%，相關模擬結果如表 8 所示。

表 7　站台進行身份驗證之辨識率

使用者	站台 A	站台 B
甲組	100%	0%
乙組	0%	100%

表 8　存取權限辨識率

使用者	站台 A	站台 B
甲組	100%	100%
乙組	100%	100%

- 允許使用站台服務

  在通過存取權限辨識的 15 位使用者中，能使用其註冊站台所提供服務項目的百分比爲 100%，但在跨網域服務項目存取上，則平均 81.5%，其主要原因是因爲部份使用者要求存取大於本身權限的資料，因而遭到站台拒絕提供服務所致。其模擬結果如表 9 所示。

6. 結論

使用者認證 (Authentication) 與授權 (Authorization) 一直是電子商務與網路服務的重要課題，然而，隨著網路服務範圍的不斷擴大，上述兩者在管理上的複雜性，將成爲系統管理者的重大負擔。因此，本論文提出一個整合『植基於 ECC 自我認證公開金鑰密碼系統』及『以角色爲基礎的存取控制』的解決方案，做爲在網路服務環境下的存取控制機制。本論文貢獻可分成兩個部份來說明：(1)可轉換權限的存取控制；(2)角色與身份的有效識別。茲說明如下：

(1) 可轉換權限的存取控制

透過角色轉換的過程，可以在不增加管理者負擔的情況下，解決網路服務環境中交易雙方使用權限不一的情形，同時提供服務需求者取得適當的存取控制權限。

(2) 角色與身份的有效識別

本系統中將採用『植基於 ECC 自我認證公開金鑰密碼系統』執行身份識別，不僅其運算量較小，而且可以在不使用數位憑證的情況下達到與使用憑證相同的安全等級，同時本系統在執行效率上能較憑證爲基礎的識別方式來的更有效率。

本論文提出一個在網路服務環境下，可有效減輕內部管理的負擔同時又兼具安全考量的存取控制系統。使得在企業實際運作上，除了能夠考量其安全性與便利性外，更趨近於實際企業所需。

表 9　各站台服務之允許使用的比率

使用者	站台 A	站台 B
甲組	100%	88%
乙組	75%	100%

參考文獻

曹偉駿，「發展電子商務系統網路之安全基礎環境」，管理與系統，第十卷第二期，民國 92 年，343-364 頁。

Coetzee, M. and Eloff, J. H. P., "Towards Web Service Access Control," *Computers & Security*, Vol. 23, No. 7, 2004, pp. 559-570.

Coetzee, M. and Eloff, J. H. P., "An Access Control Framework for Web Services," *Information Management & Computer Security* , Vol. 13, No. 1, 2005, pp. 29-38.

Ferraiolo, D. and Kuhn, R., "Role-Based Access Control," In *Proceedings of the 15th NIST – NCSC National Computer Security Conference*, Elsevier Advanced Technology Publications, 1992, pp. 554-563.

Girault, M., "Self-Certified Public Keys," In D. W. Davies (Eds.), *Advances in Cryptology: EuroCrypt'91, Lecture Notes in Computer Science*, Berlin: *Springer-Verlag*, 1991, pp. 490-497.

Hwang, J. J., Shao, B. M., and Wang, P. C., "A New Access Control Method Using Prime Factorization," *Computer Journal*, Vol. 35, No. 1, 1992, pp. 16-20.

Koblitz, N., "Elliptic Curve Cryptosystems," *Mathematics of Computation*, Vol. 48, No. 17, 1987, pp. 203-209.

Lim, B. B. L., Sun, Y., and Vila, J., "Incorporating WS-Security into a Web Services-Based Portal," *Information Management & Computer Security*, Vol. 12, No. 3, 2004, pp. 206-217.

Lopeza, J., Oppligerb, R., and Pernul, G., "Authentication and Authorization Infrastructures (AAIs): A Comparative Survey," *Computers & Security*, Vol. 23, No. 7, 2004, pp. 578-590.

Miller, V. S., "Use of Elliptic Curves in Cryptography," In H. C. Williams (Editor), *Advances in Cryptology: Crypto'85, Lecture Notes in Computer Science*, Berlin: Springer-Verlag, 1986, pp. 417-426.

Park, J., Sandhu, R. S., and Ahn, G. J., "Role-Based Access Control on the Web," *ACM Transactions on Information and System Security*, Vol. 4, No. 1, 2001, pp. 37–71.

Rolf, O., "Microsoft .NET Passport and Identity Management," *Information Security Technical Report*, Vol. 9, No. 1, 2004, pp. 26-34.

Sandhu, R., Coyne, E. J., Feinstein, H. L., and Youman, C. E., "Role-Based Access Control Model," *IEEE Computer*, Vol. 29, No. 2, 1996, pp. 38-47.

Tsaur, W. J., "Several Security Schemes Constructed Using ECC-Based Self-Certified Public Key Cryptosystems," *Applied Mathematics and Computation*, Vol. 168, No.1, 2005, pp. 447-464.