利用雜湊樹於網格環境的委任鑑別機制

陳啟東
亞洲大學
資訊工程學系
chi9695@asia.edu.tw

林明村
亞洲大學
資訊工程學系
g96241006@ms1.asia.edu.tw

林詠章
中興大學
資訊管理學系
iclin@nchu.edu.tw

摘要

網格安全基礎設施 GSI(Grid Security Infrastructure)提供了網格計算的安全環境，它是以代理憑證(Proxy Certificates)做為委任工作的鑑別。目前，代理憑證撤消方面有二種方法，一是利用憑證廢止清單 CRL(Certificate Revocation List)撤消，但當撤除的憑證過多時，將會對系統造成負擔。另一種方法是將憑證的期限縮短，不過由於縮短憑證的時間，代理人需常常向使用者更新憑證。因此在本文中，我們提出以雜湊樹來做委任工作的鑑別。我們的方法只需做雜湊值的比對就可以達到撤消憑證的目的，而之前的方法必須等期限到期才能對憑證撤消。因此我們的方法比之前的方法更具彈性。

關鍵詞:網格計算、網格安全、委任、雜湊樹

1. 前言

網格[3]是一個系統，由各地不同的硬體和軟體所組成，它透過網路將不同地區的資源(資料庫、記憶體、PDA、CPU、伺服器等…)結合成一個虛擬組織如圖 1 所示，虛擬組織內的成員不必經由中央分配就可以動態的分享和使用資源。而網格計算就是利用網格來處理問題，Foster[4]定義網格計算是“在一個虛擬組織中，可以動態的協調多個資源分享和解決問題”。舉例來說:在網格中，有一個工作被提出來時，可透過網格分發到不同地區的資源，資源只需處理部分工作。如此一來，可節省相當多的時間。和分散式計算不同的地方在於，網格內的資源是異構(如:不同的軟硬體結構、作業平台)及大規模的資源共享。

在網格環境中，工作通常是由多個資源完成的，再加上我們必須防止工作內容被不法者所竊取，和保護每個資源的安全。所以，確保網格內的隱私與安全是很重要的[2]。因此我們列出網格的安全需求[1，7]:

（1） 鑑別(Authentication):確認使用者和每個資源是合法的，只有合法的使用者和資源才能提交工作及處理工作。

（2） 委任(Delegation):使用者將存取資源的權力交給代理人，由代理人代替使用者存取資源。如此一來，使用者不需常在線上，對使用者來說將變的更方便。

（3） 單點登入(Single Sign-on):因為在網格環境中，工作通常是由多個資源完成。如果使用者和每個資源相互鑑別，這將變得很煩瑣。因此在網格環境中，使用者只需和第一個資源做鑑別工作即可，不需再和其他資源鑑別。

（4） 資料私密與完整性(Data Confidentiality and Integrity):和其他的系統一樣，保護重要資料的私密性和完整性是很重要的。當資料被竊取或遭修改時，網格內的系統將被破壞殆盡。因此需防止未經授權的人進行資料修改。

（5） 憑證撤消和壽命(Certificate Revocation and Life-span):當使用者委任代理人時，使用者會給代理人一個憑證。代理人可根據憑證來證明他是合法的。憑證的壽命是有限的，當期限一到，憑證就會自動失效。此外，當工作完成後，憑證也需被撤消，才可防止資料遭到有心人士的修改。

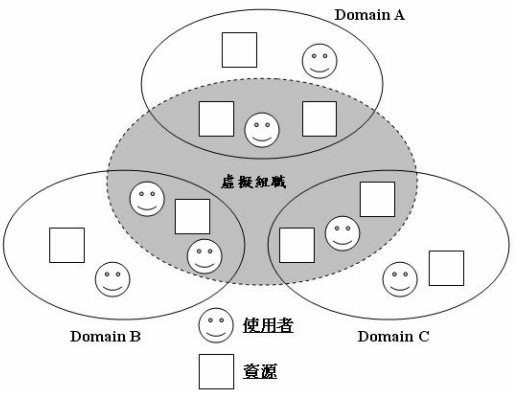

圖 1 網格的虛擬組織

網格環境中，是用代理憑證來進行鑑別、資料保密、委任和單點登入。在代理憑證要撤消時，有兩種方法。第一種方法是透過 CRL 做撤消。CRL 的撤消方式是由每個資源建立一

張清單，當憑證撤消時，資源會列在清單上，當有代理人以憑證拜訪資源時，資源會檢視該憑證是否在憑證撤消單上。但是當撤除的憑證數量過多時，存在資源內的清單容量相對的變多，以及在檢查憑證上，將變得更繁瑣[8，10]。此外，當 CRL 遭到阻絕服務攻擊時，CRL 將更難以運作[10]。

而另一種方法，是將憑證的期限縮短。Welch[9]提到在代理憑證撤消上，目前沒有比較有效的方法，因此只給代理憑證一個短的期限(大約為八個小時)。而 Geethakumari [5]也提過代理憑證的時間都很短。這樣的話，就不需要撤消憑證，因為代理憑證只有非常短的期限，代理人無法在短時間內做出非法的使用。如果當期限到期時，而工作尚未完成，使用者必須重新更新得到新的代理憑證。不過對於使用者來說，卻變得很麻煩，因為只要過幾個小時後，就要跟代理人重新鑑別並產生新的代理憑證，如果工作的時間很久的話，對於使用者來說也是項負擔。

上述兩種方法，CRL 需記錄撤消的憑證，過多的廢止憑證會對資源造成負擔。而縮短憑證的期限，則表示代理人需常常向使用者鑑別以更新憑證，對使用者來說也很麻煩。因此在本篇文章中，我們提出用雜湊樹的方法進行鑑別、委任和單點登錄。我們的方法只需做雜湊值的比對就可確認代理人是否已經撤消。我們的方法不需常常做更新，且不用記錄每張廢止的憑證。因此我們的方法可以在網格中，讓資源和代理人之間，變得更有彈性。

我們文章的架構如下:章節二將分別介紹雜湊樹的做法和憑證的產生。章節三我們提出將提出一個方法，將雜湊樹建立在網格環境之中。章節四分析與討論我們所提的方法。最後則是結論。

2. 相關文獻

在此章節中，我們將介紹代理憑證的產生和雜湊樹。

2.1 代理憑證

網格安全基礎設施 GSI(Grid Security Infrastructure)[1]以公開金鑰基礎設施(PKI)為基礎下所發展的[11]。GSI 透過 X. 509 代理憑證提供了網格內的鑑別、資料保密、委任及單點登入[1, 7]。下列，我們將介紹代理憑證的產生。

代理憑證是以公開金鑰憑證(Public Key Certificates)為基礎所發展出來的。代理憑證和公開金鑰憑證不同的地方在於，代理憑證可以由公開金鑰憑證或者上一個持有者發出。

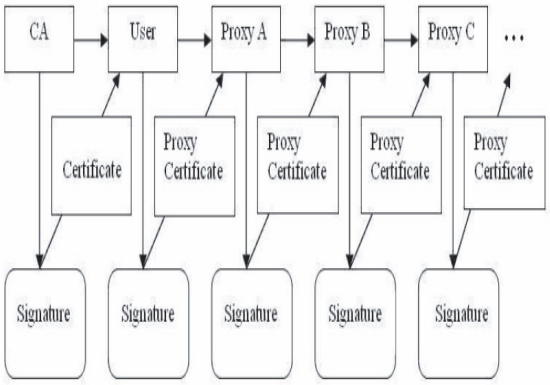

圖 2 代理憑證的信任鏈

如圖 2 所示，當 CA 發出一個憑證給使用者後，使用者也可以透過該憑證產生一個代理憑證給代理人 *A*，由代理人 *A* 幫助使用者完成工作。而代理人 *A* 利用代理憑證再產生一個新的代理憑證再發送給代理人 *B*。代理人 *B* 以代理憑證向資源證明他是代表使用者進行工作的存取，依此類推。因此，我們可以了解代理憑證是由公開金鑰憑證和上一位憑證持有者所發出，並不是 CA 發出。這一關系，我們可以稱為信任鏈(Trust Chain)[6]。

代理憑證的產生方法如圖 3 所示。下列我們將介紹代理憑證的產生過程[9]。

（1）如圖 3 所示，當使用者要委任權限給代理人時，雙方需先做相互鑑別，使用各自擁有的證書證明彼此是合法的。鑑別完後，一條安全的通道將被建立起來。此步驟可以透過安全通道層 SSL(Secure Socket Layer)來完成。

（2）在使用者說明委任的需求後，代理人產生一對金鑰(包含公鑰和私鑰)和憑證請求。

（3）代理人將憑證請求透過安全的通道傳送給使用者。

（4）使用者用自己的私鑰和代理憑證跟憑證請求做簽章，產生了一個新的代理憑證。使用者在適當的位置中，填上自己的要求，做為政策的方針。

（5）使用者將新的代理憑證透過安全的通道寄回給代理人。代理人將新的私鑰和新的代理憑證存放到安全的地方。最後，

代理人可以用新的代理憑證向資源證明，他是代替使用者工作的。

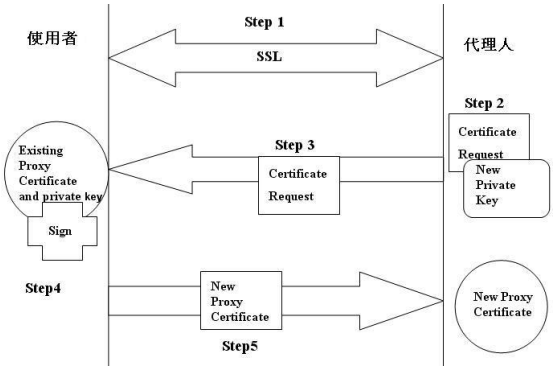

圖 3 代理憑證的產生

每個代理憑證都有一個合適的期限，當期限到時，如果工作還未完成，代理人需再向使用者相互鑑別以產生一個新的代理憑證。而工作完成且憑證壽命已到期，該憑證會自動失效。此外，當工作已完成而憑證的期限尚未失效，則需使用 CRL 來撤消憑證。CRL 的做法是把要撤消的憑證記錄在 CRL 裡，當有位代理人用憑證拜訪資源時，資源會確認該憑證資訊是否在 CRL 裡面。如果該憑證已撤消，則拒絕該代理人。如果不在 CRL 裡面，就同意該位代理人。但是，此種做法有個缺點，當憑證過多時，每個資源所以記錄的清單也將變得更多，因為憑證變多，清單內的容量將要更大，而且資源在檢查憑證是否在清單內時，將耗費更多時間。特別是在網格中，因為網格內的資源和使用者分佈各地。如此一來，將會對資源和使用者造成負擔。另外，如果有不法者對資源進行阻絕服務攻擊，資源將更難以招架[10]。

另外的方法就是給予憑證一個短的期限，這樣的話，就不需要撤消憑證，因為代理憑證只有非常短的期限，當期限一到，如果工作尚未完成，代理人必須和使用者做鑑別以更新代理憑證。相反地，假使工作已完成而憑證未到期，但由於憑證期限非常短。因此，代理人無法在非常短的期限內做出非法的使用。但是，此種方法卻有個缺點，因為代理憑證的期限非常短，代理人必須常常上線和使用者做鑑別以更新憑證。想像一下，使用者必須在幾個小時後和代理人持做鑑別以產生新的代理憑證，持續到工作完成。如此一來，這對使用者來說變的很繁瑣。

2.2 雜湊樹

我們的方法是以 Ren[8]提出雜湊樹的方法為概念設計出來的。因此，我們在下列先介紹 Ren 所表示的雜湊樹運算方法:

圖 4 為雜湊樹的例子，在圖 4 中，每個葉節點都有屬於自己的 n_1，$n_2 \ldots n_i$ 值，在此，我們假設 $i = 4$，n_1、n_2、n_3、n_4。接下來我們將葉節點底下的 n_i 做雜湊運算 $h(n_i)$，$h(\,)$為一次的雜湊運算。再用底下葉節點的 $h(n_i)$值相互做雜湊運算求出節點 A 和 B 的雜湊值。例如:節點 A 的雜湊值 $h_a = h\,(h(n_1) \mid h(n_2))$，節點 B 的雜湊值 $h_b = h\,(h(n_3) \mid h(n_4))$。當求出節點 A 和 B 的雜湊值後，再將節點 A 和 B 做雜湊運算，$h_r = h\,(h(n_a) \mid h(n_b))$，可以求出根節點的雜湊值 h_r，如此一來，每個節點的雜湊值都可計算出。h_r 的建立，主要是可以將葉節點的 $h(n_i)$值跟輔助鑑別資訊 AAI(Auxiliary Authentication Information)做運算，求出彼此間的 h_r 是否相同。如果相同，則該節點是有效的。AAI 的產生是根據葉節點的位置分配的。例如 n_4 的 AAI 為$<h_a, h(n_3)>$，n_1 的 AAI 為$<h_b, h(n_2)>$。

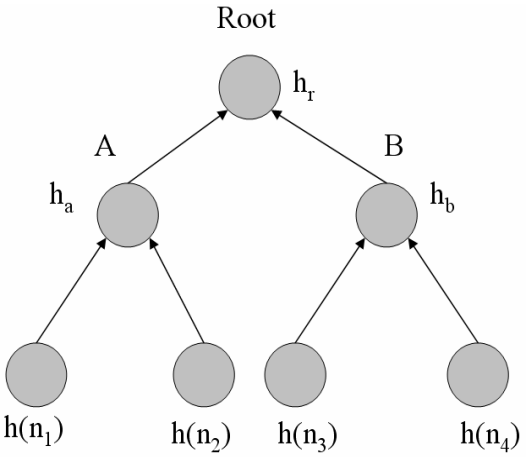

圖 4 雜湊樹

舉個實例來說明:假設有個使用者持有正確根節點的值 h_r，當 n_1 想和使用者做鑑別時，n_1 需發送 n_1 和 $AAI<h_b, h(n_2)>$給使用者。使用者依序將 n_1 和 $AAI<h_b, h(n_2)>$做雜湊運算，$h(n_1)$，$h_a = h(h(n_1) \mid h(n_2))$，$h_r = h(h(n_a) \mid h(n_b))$，求出 h_r 後，再跟自己所持有的 h_r 做比對，檢查是否相同。只有彼此間的 h_r 相同才能證明 n_1 是合法的。

由上述的方法可以了解雜湊樹只需做雜湊值的比對即可。不需記錄和檢查每個撤消的憑證，也不需做常常做更新。在網格內，可以比 CRL 和短期的代理憑證更具有彈性。在下一個章節中，我們將說明雜湊樹在網格中的應用。

3. 我們的方法

在此章節中，我們將提出以雜湊樹為概念，應用到在網格環境中，做委任鑑別的工作。

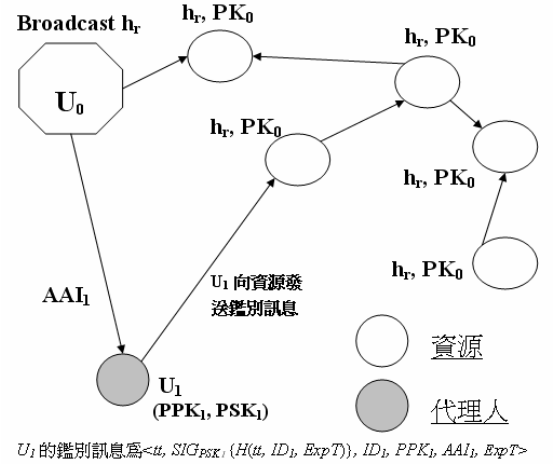

圖 5 當 U_1 想鑑別資源

3.1 參數說明

U_o:使用者
U_i:代理人
ID_i:代理人的身分號碼
$h(\ )$:雜湊運算
PK_0: U_o 的公開金鑰
SK_0: U_o 的私密金鑰
PPK_i:代簽公開金鑰
PSK_i:代簽私密金鑰
SIG:簽章
tt:時戳，防止重送攻擊
$ExpT$:期限，當期限一到，代簽金鑰則失去效用
AAI_i: 代理人的輔助鑑別資訊，依不同的代理人給予適當的 AAI_i

3.2 初始階段

當 U_o 想要委任權限給 U_i，由 U_i 代替 U_o 到資源做存取工作。首先，U_o 必須和 U_i 相互鑑別，產生一對代簽金鑰(包含了 PPK_i 和 PSK_i)，再將代簽金鑰群播給 U_i，此階段，可以透過 SSL 來完成。U_i 可以利用代簽金鑰代替 U_o 到資源內做存取工作。接下來，U_o 搜集底下 U_i 的代簽公開金鑰 PPK_i 和身分編號 ID_i 建構成雜湊樹，如圖 4 所示。並計算每個葉節點的 $h(n_i)$、h_a、h_b、h_r:

$h(n_i) = h(ID_i \| PPK_i \| ExpT)$
$h_a = h\,(h(n_1) \mid h(n_2))$
$h_b = h\,(h(n_3) \mid h(n_4))$
$h_r = h\,(h(n_a) \mid h(n_b))$

計算出來後，把 AAI_i 寄給 U_i。再由 U_o 群播 h_r 給網格內的每個資源。順帶一提，當 U_o 群播 h_r 給網格內的每個資源時，必須用 SK_0 將 h_r 加密，證明是由 U_o 所發出的。資源可以用 PK_0 解開。

3.3 鑑別階段

當 U_i 想代替 U_o 到網格內的某個資源進行存取工作時。需發送:
<tt, SIG_{PSKi}{$H(tt, ID_i, ExpT)$}, ID_i, PPK_i, AAI_i, $ExpT$>給資源。再由資源進行運算以判斷 U_i 是否為合法代理人。在此，我們假設 U_i 為 U_1，如圖 5 所示。因此，鑑別訊息為:
<tt, SIG_{PSK1}{$H(tt, ID_1, ExpT)$}, ID_1, PPK_1, AAI_1, $ExpT$>。而 AAI_1 的值為<h_b, $h(n_2)$>。

3.4 資源驗證階段

當資源收到 U_1 的鑑別訊息 <tt, SIG_{PSK1}{$H(tt, ID_i, ExpT)$}, ID_1, PPK_1, AAI_1, $ExpT$>時，計算:

(1)用 U_1 的 ID_1, PPK_1 和 $ExpT$ 計算 $h(n_1)$，$h(n_1) = h(ID_1 \| PPK_1 \| ExpT)$。接下來，用 AAI_1 <h_b, $h(n_2)$>分別求出 h_a 和 h_r 的值: $h_a = h(h(n_1) \mid h(n_2))$，$h_r = h(h_a \mid h_b)$。計算出 h_r 的值後，資源檢查計算的 h_r 是否和自己持有的 h_r 相同。如果相同，繼續下一步驟。

(2)使用 PPK_1 驗證 SIG_{PSK1}{$H(tt, ID_1, ExpT)$}，確認 $H(tt, ID_1, ExpT) = (SIG_{PSK1}${$H(tt, ID_1, ExpT)$}$)_{PPK1}$。如果相同，資源就同意 U_1 的存取要求。

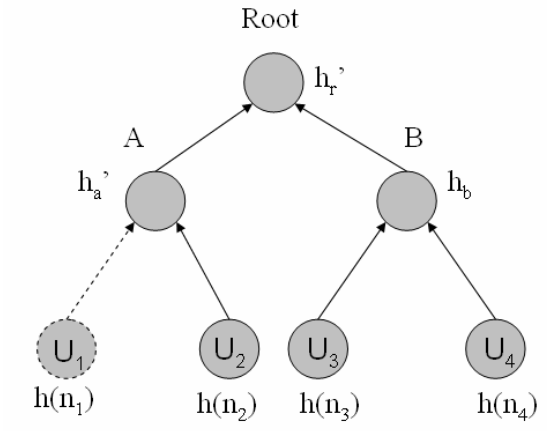

圖 6 當 U_1 被撤消

3.5 撤消階段

使用者可以依自己的需求設定合適的代理期限 $ExpT$，如果 $ExpT$ 到期，代理人所使用

的代簽金鑰將自動失去效用。另外，當 U_1 已完成工作要被撤消時，如圖 6 所示。U_0 重新產生新的 h_a'和 h_r'，$h_a' = h(n_2)$，$h_r' = h(h_a' \| h_b)$。然後將 h_r'和新的 AAI_i 分別群播給資源及 U_i。U_1 撤消後如圖 6 所示，如果 U_1 想用以前的舊資訊 AAI_1 到資源進行存取工作時，由於資源所儲存的驗證值已經更新為 h_r'，而 U_1 的資訊只能求出 h_r，而 $h_r' \neq h_r$，因為 h_r 不相同，所以資源將拒絕 U_1 的存取。

由上述所得知，我們的方法只需做雜湊運算和比對代理人和之間的 h_r 即可，不需儲存過多的憑證，也不需時常做更新的動作。因為我們的方法可以簡單撤消憑證，使用者可依自己的工作需求，自行決定合適的代理期限，就算期限大於工作時間，也可以簡單的撤消(做雜湊值的比對)，可以在使用者、資源和代理人三方面中變得更方便。因此，我們的方法在網格環境中可以比 CRL 和縮短憑證的期限更具有彈性。

4.分析與討論

在此章節中，我們分析我們所提出的方法看是否能達到之前上述的網格安全需求。

(1) 鑑別(Authentication):在我們所提出的方法中，當代理人要和資源鑑別時，會發出<tt, $SIG_{PSK1}\{H(tt, ID_1, ExpT)\}$, ID_1, PPK_1, AAI_1, $ExpT$>這段訊息。資源會先驗證 AAI_1 求出 h_r 以確定代理人還是有效的。

(2) 委任(Delegation): 當使用者想要委任權限給代理人，由代理人代替使用者跟資源做存取工作。首先，使用者必須和代理人相互鑑別，產生一對代簽金鑰(包含了 PPK_i 和 PSK_i)，如此一來，代理人可以用代簽金鑰代替使用者向其他資源做存取工作。

(3) 單點登入(Single Sign-on):在我們的方法中，使用者只需和代理人做鑑別，產生一對代簽金鑰(包含了 PPK_i 和 PSK_i)，代理人可以用代簽金鑰向其他資源鑑別，減輕使用者的負擔。

(4) 資料私密與完整性(Data Confidentiality and Integrity): 在 3.4 的第二步驟中，資源主要做的是 MAC 的動作，因為鑑別資料有用 PSK_1 加密，資源用 PPK_1 驗證 $SIG_{PSK1}\{H(tt, ID_1, ExpT)\}$，確認 $H(tt, ID_1, ExpT) = (SIG_{PSK1}\{H(tt, ID_1, ExpT)\})_{PPK1}$。如果二者相同，表示鑑別內容未遭受攻擊者修改，為合法代理人。

(5) 憑證撤消和壽命(Certificate Revocation and Life-span):根據我們前面所描述的二種方法:CRL 和短期的代理憑證。二者分別在憑證的廢止和壽命都有一些問題。CRL 是資源要記錄每個廢止的憑證，進而檢查新的憑證是否在廢止的清單內。對資源來說，需要相當多的容量和時間。而短期代理憑證，則需要代理人在幾個小時後向使用者申請新的憑證，假設使用者斷線時，工作將被暫停。這表示使用者需常常注意自己的狀態和頻繁的和代理人鑑別。而我們的方法，使用者可依自己的工作需求，自行決定合適的代理期限，就算期限大於工作時間，我們只需更新 h_r'，因為代理人所持有的是舊的 h_r。就算代理人想再進行工作，因為 $h_r' \neq h_r$，所以資源會拒絕代理人的申請。

表 1 做法及比較

	做法	撤消憑證
CRL	將失去效用的憑證存在廢止清單中，未做實際上的撤消。	否
縮短憑證的期限	將憑證的期限縮短(n 個小時)，時間一到，代理人需更新憑證。	否
我們的方法	要撤除代理人的權限時，使用者只需重新產生 h_r'即可。	可

由表1可得知，CRL和縮短憑證的期限都無法做到撤消的動作。CRL是由資源將撤消的憑證記錄在一張清單裡，再檢查欲拜訪資源的憑證是否已過期，這需要相當多的容量和時間。而縮短憑證的期限也沒有撤消的功能。它只給每張代理憑證幾個小時的期限，當期限到期時，代理人必須做更新的動作。使得代理人沒有足夠的時間做非法的存取工作。但這樣卻造成了使用者的負擔，因為代理人需常常向使用者更新憑證才能繼續工作。所以，這兩種方法都沒有撤消憑證的功能。因此，我們提出以雜湊樹在網格環境中做委任的工作。我們的方法只需進行雜湊值的比對就可以進行撤消的工作，比縮短憑證的期限和CRL更具有彈性。

5.結論

在本篇文章中，我們提出使用雜湊樹應用

到成員流動頻繁的網格環境中，我們的方法只需做雜湊運算和比較雙方的 h_r，我們的方法不需要記錄多個廢止的憑證，當有代理人要向資源進行存取工作時，資源也不需核查清單裡面的憑證，只需做雜湊值的比對即可。也不用常常更新代理憑證。因此，我們的方法可以在網格中，使資源、代理人和使用者之間，變得更有彈性。

參考文獻

[1] Chakrabarti, A., Damodaran, A. and Sengupta, S., "Grid computing security: A taxonomy," ***IEEE Security & Privacy***, Vol. 6, No. 1, pp. 44 - 51, 2008.

[2] Cody, E., Sharman, R., Rao, R. H. and Upadhyaya S., "Security in grid computing: A review and synthesis," ***Decision Support Systems***, Vol. 44, pp. 749-764, Mar. 2008.

[3] Foster, I. and Kesselman, C., ***The Grid: Blueprint for a New Computing Infrastructure***, USA: Morgan Kaufmann, 1999.

[4] Foster, I., Kesselman, C. and Tuecke, S., "The anatomy of the grid: Enabling scalable virtual organizations," ***International Journal of High Performance Computing***, Vol. 15, No. 3, pp. 200-222, 2001.

[5] Geethakumari, G., Negi, A. and Sastry, V. N., "Dynamic delegation approach for access control in grids," ***In Proceedings of First International Conference on e-Science and Grid Computing***, Melbourne, Australia, pp. 387 - 394, Dec. 2005.

[6] Li, M. C., Ma, J. and Yao, H., "Recovery mechanism of online certification chain in grid computing," ***In Proceedings of Availability, Reliability and Security (ARES)***, Vienna, Austria, pp. 558-562, Apr. 2006

[7] Lim, H. W., ***On the Application of Identity-Based Cryptography in Grid Security***, PhD thesis, London University, 2006.

[8] Ren, K., Lou, W., Zeng, K. and Moran, P. J., "On Broadcast Authentication in Wireless Sensor Networks," ***IEEE Transactions on Wireless Communications***, Vol. 6, No. 11, pp. 4136 – 4144, Nov. 2007.

[9] Welch, V., Foster, I., Kesselman, C., Mulmo, O., Pearlman, L., Tuecke, S., Gawor, J., Meder, S. and Siebenlist, F., "X.509 proxy certificates for dynamic delegation," **in *Proceedings of 3rd Annual PKI R&D Workshop, Gaithersburg***, MD, U.S.A., pp. 42-58, Apr, 2004

[10] Zhao, S., Aggarwal, A. and Kent, R. D., "A Framework for Revocation of Proxy Certificates in a Grid**," *In Proceedings of International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing,*** Qingdao, China, pp. 532 – 537, 2007.

[11] Zhao, S., Aggarwal, A. and Kent, R. D., "PKI-based authentication mechanisms in grid systems," ***In Processing of Networking, Architecture, and Storage (NAS)***, Guilin, Guangxi, China, pp. 83-90, July, 2007.