

PAWEŁ SZYCHOWSKI  
MIROŚLAW KOPEĆ  
Centrum Komputerowe Politechniki Łódzkiej  
MARCIN LAWENDA  
MARCIN WOLSKI  
NORBERT MEYER  
CEZARY MAZUREK  
MACIEJ STROIŃSKI  
Poznańskie Centrum Superkomputerowo Sieciowe

## MODEL BEZPIECZEŃSTWA DOSTĘPU DO ZASOBÓW W SYSTEMACH GRIDOWYCH

### Streszczenie

*W pracy przedstawiono sposób bezpiecznego dostępu do usług Naukowej Biblioteki Cyfrowej, która jest częścią systemu Laboratorium Wirtualnego. Została ona oparta na Systemie Zarządzania Danymi zrealizowanym w projekcie Progress (2883/C.T11 6/2001 – wspólnie finansowanym przez Ministerstwo Nauki i Informatyzacji i firmę SUN). Autorzy skupili się na kwestii zapewnienia bezpiecznego sposobu dostępu do danych oraz ich transferu do komputera użytkownika. W artykule zakłada się, że interfejs dostępowy został zrealizowany w postaci portalu. Prace są realizowane w ramach projektu 6 T11 0052 2002 C/05836 finansowanego przez Ministerstwo Nauki i Informatyzacji oraz firmę SGI.*

### 1. Wstęp

Obecnie laboratoria wirtualne zdobywają coraz większą popularność w środowiskach naukowych. Jest to związane z korzyściami, jakie niesie ze sobą koncepcja tego typu systemów. Do najważniejszych zalet możemy zaliczyć: łatwy dostęp do kosztownej aparatury naukowej, możliwość współpracy naukowców pochodzących z różnych, geograficznie odległych miejsc, łatwiejszy i szybszy proces kształcenia, dostęp do biblioteki pomiarów i publikacji. Idea ta jest szczególnie atrakcyjna dla nauk doświadczalnych i technicznych, w szczególności: fizyki, chemii, biologii strukturalnej, medycyny doświadczalnej, inżynierii w szerokim tego słowa znaczeniu [1], [20], [10], [11], [2], [4], [5].

Najważniejsze funkcje, jakie powinny być realizowane w ramach laboratoriów wirtualnych zostały przedstawione szerzej w pracy [6]. Jedną z nich jest zapewnienie możliwości przechowywania i zarządzania dużą ilością informacji, która jest wynikiem wykonywanych eksperymentów i obliczeń związanych z ich późniejszym przetworzeniem. Oprócz funkcji związanych z danymi wynikowymi system taki powinien udostępniać funkcjonalność związaną z operacjami dotyczącymi literatury, publikacjami oraz innymi materiałami przechowywanymi w postaci cyfrowej. W

systemie Laboratorium Wirtualnego (VLAB) funkcję taką pełni Naukowa Biblioteka Cyfrowa - NBC (ang. *Digital Science Library - DSL*).

Implementacja NBC została oparta o System Zarządzania Danymi (ang. *DMS – Data Management System*) [13] powstały w ramach projektu PROGRESS [8], rozwijany w projekcie SGI-Grid.

Systemy zarządzania danymi są istotnym składnikiem architektury wielu współczesnych systemów gridowych. Podstawowym zadaniem systemu zarządzania danymi jest przechowywanie, udostępnianie oraz katalogowanie danych. Nie jest to jednak powielanie funkcjonalności, jaką zapewniają bazy danych. Głównymi postulatami, stawianymi przed takimi systemami jest stworzenie środowiska umożliwiającego elastyczny i bezpieczny dostęp do danych, otwartość na najpopularniejsze protokoły transmisji i standardy definiowane przez organizacje gridowe (np. Global Grid Forum).

SZD jest wielowarstwowym środowiskiem oprogramowania, złożonym z elementów:

- system zarządzania usługami gridowymi wraz z ich środowiskiem komunikacyjnym,
- bezpieczeństwo zasobów sprzętowych oraz programowych,
- zarządzanie i przetwarzanie danych wraz z interfejsami do baz danych
- zarządzanie usługami i aplikacjami dostępnymi poprzez witrynę,
- wizualizacja obliczeń w ramach witryny.

W dokumencie autorzy swoją uwagę skupili na aspekcie bezpieczeństwa dostępu do danych przechowywanych w Systemie Zarządzania Danymi, rozwijanym w ramach projektu SGI-Grid [21]. Jest to bardzo ważna kwestia zwłaszcza dla naukowców, którzy przykładają dużą wagę do poufności wyników swoich badań. W opisie pominięto aspekt bezpieczeństwa w komunikacji pomiędzy modułami wewnątrz systemu. Będzie to tematem innego opracowania.

W rozdziale 2 zostały przedstawiona architektura Systemu Zarządzania Danymi. Rozdział 3 opisuje rozwiązanie warstwy bezpieczeństwa w projekcie SGI-Grid. Przedstawiono scenariusz autoryzacji użytkownika lub zleconego przez niego zadania algorytm bezpiecznego dostępu do zasobów. Rozdziały 4 i 5 stanowią podsumowanie rozważań z punktów wcześniejszych pod kątem wad i zalet proponowanego rozwiązania.

## 2. System Zarządzania Danymi

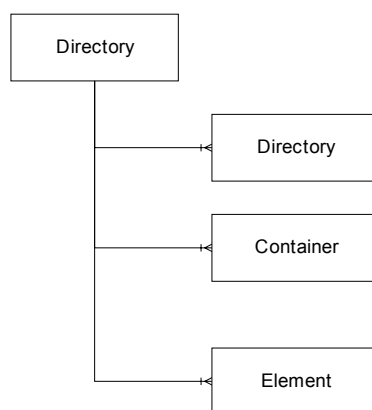
Obecnie głównym celem zespołu wdrażającego SZD jest poszerzenie jego funkcjonalności, a także dostosowanie systemu do specyficznych wymagań Laboratorium Wirtualnego [7].

System Zarządzania Danymi będzie służył do przechowywania danych generowanych i wykorzystywanych w ramach Laboratorium Wirtualnego. Dane te mogą być zarówno danymi wejściowymi aplikacji, niezbędnymi do obliczeń i wykorzystywanymi podczas eksperymentów naukowych, jak również mogą to być dane będące wynikiem przeprowadzonych eksperymentów. Istnieje ponadto potrzeba gromadzenia różnego rodzaju danych i publikacji powstałych w wyniku badań prowadzonych w innych systemach (laboratoriach), które mogą zostać wykorzystane w omawianym laboratorium. Środowiskiem, które umożliwi składowanie i dostęp do tych zasobów będzie SZD.

## 2.1. Architektura SZD

System Zarządzania Danymi jest systemem rozproszonym, opartym na modelu autonomicznych agentów, komunikujących się przy wykorzystaniu dostępnej infrastruktury sieciowej. Podstawowym zadaniem systemu SZD jest przechowywanie i udostępnianie danych w środowisku gridowym. Głównym założeniem funkcjonalnym było ukrycie przed użytkownikiem końcowym wewnętrznej złożoności programowej, systemu oraz stworzenie przejrzystej i intuicyjnej metody dostępu do danych. SZD posiada zunifikowany interfejs dostępowy zrealizowanych w technologii Web Services.

SZD stanowi, funkcjonalnie, rodzaj wirtualnego systemu plików przechowującego dane zorganizowane w strukturę drzewiastą. Podstawowe elementy tej struktury to metakatalogi, które pozwalają grupować inne obiekty oraz metapliki, które stanowią logiczną instancję danych. Dane przechowywane w SZD mogą zostać opisane dodatkowymi informacjami, tworzącymi warstwę metaopisów danych (Rysunek 1). Wypełnienie przyjętego postulatu swobodnego dostępu do danych wymaga wspierania powszechnych protokołów transmisji - obecnie SZD realizuje dostęp do danych poprzez protokoły HTTP, HTTPS, FTP, GridFTP oraz GASS.

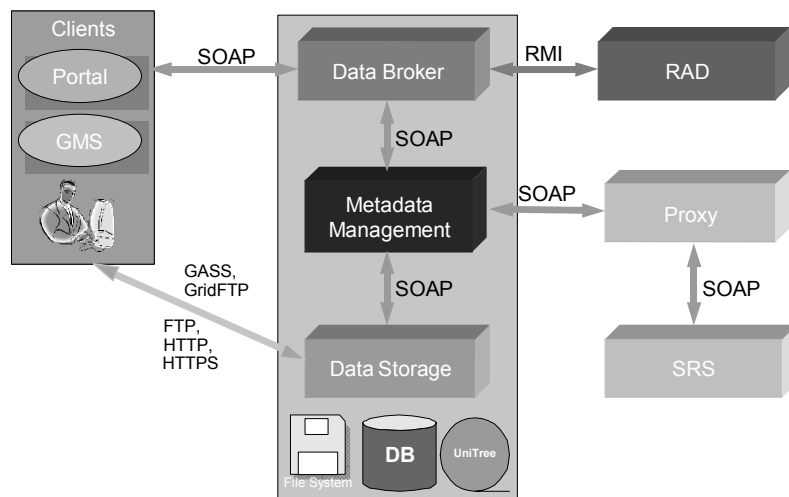


Rysunek 1 Struktura katalogowa SZD

SZD składa się z trzech podstawowych modułów: Brokera Danych, Repozytorium Metadanych oraz Kontenera Danych. Oprócz nich w systemie należy wyróżnić jeszcze moduł Proxy, który stanowi interfejs do zewnętrznych baz danych oraz Portal dostępowy pozwalający na wykonywanie operacji administracyjnych w systemie (Rysunek 2).

SZD udostępnia swoje usługi komponentom warstwy front-end w postaci uniwersalnego API wywoływanego w technologii Web Services. Należy przy tym zaznaczyć, iż SZD występuje w środowisku gridowym jako warstwa pośrednia (middleware), czyli udostępnia swoje usługi klientom końcowym poprzez interfejs dostępowy, jakim może być np. portal lub desktop.

System autoryzacji RAD (ang. *Resource Access Decision*) jest usługą opartą na standardzie CORBA, pozwalającą na kontrolę i zarządzanie dostępem do zasobów. RAD stanowi opcjonalny moduł autoryzacyjny, dostarczony jako dodatkowy pakiet do SZD.



Rysunek 2 Modułarna architektura SZD

### 3. Bezpieczeństwo w projekcie SGIGrid

Problem bezpieczeństwa w systemach gridowych jest złożony. W kontekście systemu SZD sprowadza się do trzech zagadnień:

- mechanizmu uwierzytelniania użytkownika.
- mechanizmu decyzyjnego (autoryzującego) dopuszczającego wykonywanie operacji na danym zasobie opierającego się o zdefiniowaną politykę bezpieczeństwa,
- mechanizmu transakcyjnego, gwarantującego integralność i spójność przebiegu złożonej operacji na zasobie.

Obecny stan w zakresie bezpieczeństwa systemów gridowych został przedstawiony w pracach [12], [14], [19].

#### 3.1. Uwierzytelnianie.

Uwierzytelnianie w SGIGRID jest zgodne z postulatem SSO (ang. *Single Sign-On*) [15], [16] czyli jednokrotnego podawania danych uwierzytelniających. Uwierzytelnianie w VLAB jest scentralizowane i opiera się o Web Service CAS (Central Authentication Service), przechowujący informacje o użytkownikach. Uwierzytelnianie jest dokonywane na podstawie certyfikatu X.509v3 lub pary atrybutów user/password.

#### 3.2. Kontrola dostępu.

Kontrola dostępu (autoryzacja) jest jednym z podstawowych mechanizmów bezpieczeństwa systemów informatycznych. Moduł kontroli dostępu, w projekcie SGIGRID, jest oparty o specyfikację RAD (ang. Resource Access Decision) grupy OMG [9]. Stanowi on integralną część warstwy bezpieczeństwa w środowisku gridowym. Zadaniem modułu jest dostarczenie usługi sieciowo-

wej polegającej na określeniu czy podmiot, żądający, w odniesieniu do danego zasobu, wykonania zadanej operacji, ma odpowiednie uprawnienia. Decyzja (TAK lub NIE) jest podejmowana na podstawie trójki czynników:

- tożsamości podmiotu (identyfikator – np. nazwa użytkownika, komputera itp.),
- wymaganego uprawnienia (rodzaju operacji – zapis odczyt, itp.),
- nazwy zasobu (identyfikator – nazwa katalogu, pliku, itd.).

Po przekazaniu tych argumentów do modułu kontroli dostępu, na podstawie nazwy zasobu, są wybierane obiekty odpowiedzialne za podjęcie decyzji – tzw. ewaluatory (ang. *evaluators*) komunikujące się z bazą kontroli dostępu w celu określenia częściowych decyzji autoryzacyjnych oraz kombinatory (ang. *combinator*) podejmujący końcową decyzję autoryzacyjną. Moduł kontroli dostępu korzysta z bazy kontroli dostępu przechowującej informacje o uprawnieniach użytkowników do zasobów. Baza kontroli dostępu może być heterogeniczna i rozproszona: np. część informacji może być przechowywana w relacyjnej bazie danych, część w LDAP. Poszczególne części bazy kontroli dostępu mogą być umieszczone na różnych maszynach.

### **3.3. Scenariusz operacji**

Istnieją dwie drogi komunikowania się użytkowników z SZD (Rysunek 3):

1. Eksploracja SZD (operacje na danych symbolicznych przechowywanych w Repozytorium Metadanych), w ramach której dostęp przebiega pośrednio poprzez Portal proxy (serwer aplikacji) stanowiący „front end” systemu SZD. System bezpieczeństwa SZD polega w tym przypadku na integralności sesji użytkownika otwartej w portalu.
2. Transfer plików (przesyłanie pliku fizycznego pomiędzy komputerem użytkownika i Kontenerem Danych), w ramach którego użytkownik zestawia bezpośrednie połączenie z Kontenerem Danych, na czas transferu. Przyjęcie połączenia przez Kontener jest uwarunkowane pozytywnym wynikiem wcześniejszej autoryzacji, zasygnalizowanym Kontenerowi przez Repozytorium Metadanych. System bezpieczeństwa w tym przypadku musi zapewnić spójność kontekstu (tzn. sprawdzić czy użytkownik, operacja i zasób są tymi samymi wartościami, które ustalono w czasie autoryzacji).

Wspólnym mianownikiem wskazanych dróg komunikowania się z SZD jest wymaganie zapewnienia poufności przesyłania wszystkich danych, czyli szyfrowania łącza. Zakładamy, że użytkownik już wcześniej został uwierzytelniony przez Portal.

W ramach aplikacji VLAB, dostęp do SZD będzie przebiegał wg wariantowego scenariusza:

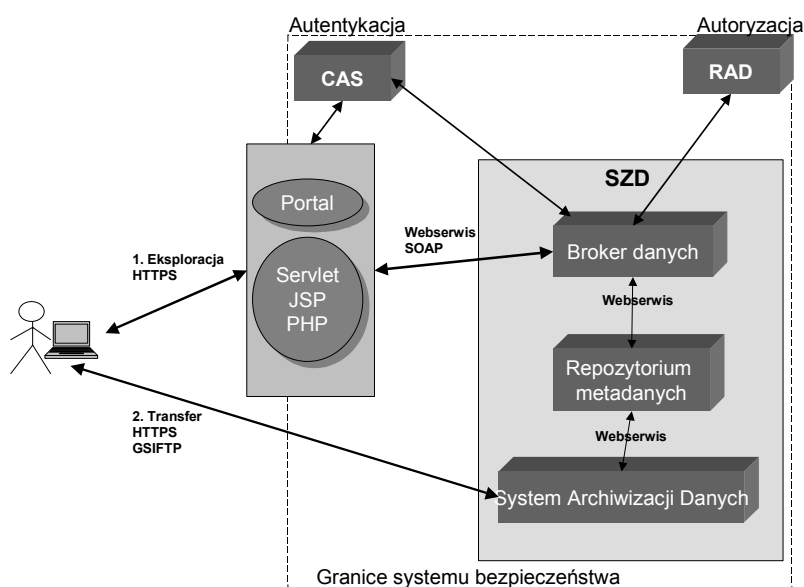
- W1. Użytkownik eksploruje Repozytorium Metadanych, za pomocą nawigatora udostępnianego przez Portal SZD. Jest to możliwe po uprzedniej autentykacji w oparciu o system uwierzytelniania CAS. Zlecenie wykonania operacji na pliku przez użytkownika (żądanie typu „r/w/x”) wywołuje podsystem autoryzacji RAD. Po pozytywnej autoryzacji następuje faza transferu danych (zapis/odczyt).
- W2. Użytkownik wykonuje obliczenia przy pomocy aplikacji obliczeniowej. Aplikacja w imieniu użytkownika, pobiera lub zapisuje dane w SZD. Przebieg uwierzytelniania, autoryzacji i transferu danych jest analogiczny jak w pkt. 1.

Powyższe scenariusze, różniące się stopniem interakcji użytkownika z aplikacją VLAB, z punktu widzenia bezpieczeństwa są identyczne i składają się z trzech faz:

- Faza I uwierzytelnienia użytkownika,
- Faza II autoryzacji, polegająca na porównaniu, przysłanego przez użytkownika, żądania

wykonania danej akcji na zasobie, z regułami bezpieczeństwa sformułowanymi w polityce bezpieczeństwa dla danego zasobu,

- Faza III transferu danych polegająca na bezpośrednim dostępie do Kontenera Danych oraz przesłaniu pliku przez sieć z zachowaniem poufności.



**Rysunek 3 Scenariusz wywołań**

Powyższe fazy stanowią spójną sekwencję zdarzeń wywołanych przez użytkownika. Jednak należy mieć świadomość, że fazy I-II oraz faza III korzystają z różnych komponentów SZD i kanałów transmisyjnych. Bez wprowadzenia specjalnych mechanizmów, zapewniających, że w trakcie wszystkich faz użytkownik, zasób i rodzaj operacji pozostaną niezmiennie, możliwy jest w fazie III negatywny scenariusz, polegający na zagarnięciu uprawnień przez innego użytkownika, lub odwołaniu do innego zasobu.

### 3.4. Założenia techniczne.

W punkcie zostały opisane założenia techniczne przyjęte do opracowania implementacji systemu bezpieczeństwa dostępu do zasobów SZD.

1. Parametry bezpieczeństwa w trakcie przebiegu trójfazowego scenariusza operacji na SZD:
  - a) Niezaprzeczalność w fazie III użytkownika, uwierzytelnionego w fazie I,
  - b) Niezaprzeczalność w fazie III operacji, autoryzowanej w fazie II,
  - c) Poufność transferu pliku w fazie III.
2. Środki realizacji modelu bezpieczeństwa:
  - a) Centralna autentykacja X.509, w oparciu o system CAS,

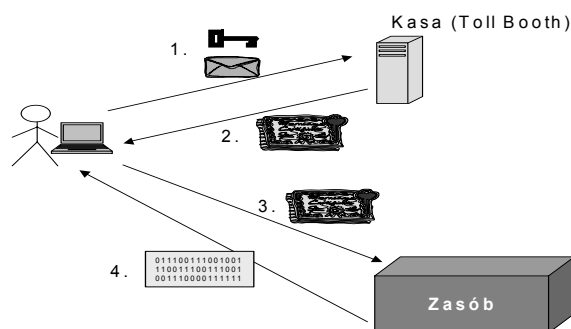
- b) Centralna autoryzacja operacji, w oparciu o system RAD,
  - c) Centralna delegacja uprawnień (certyfikatu proxy) dostępu do Kontenera Danych w oparciu o system CAS, oderwana od użytkownika (użytkownik nie ma prawa sam wygenerować certyfikatu proxy).
3. Technologie zgodne z GSI.(Globus Security Infrastructure) i RAD. Oznacza to:
- a) Uwierzytelnianie oparte o standardy PKI X.509,
  - b) Autoryzacja oparta na systemie RAD,
  - c) Dostęp do pojedynczego zasobu będzie za każdym razem reglamentowany na podstawie czasowych, krótkoterminowych certyfikatów X509v3 typu proxy, Transfer plików na bazie protokołów SSL/TSL.

### 3.5. Projekt

W świetle scenariusza i przewidywanych zagrożeń, należy wyposażyć SZD w mechanizm nadający operacjom na zasobach cechy transakcyjności.

Takim mechanizmem może być dobrze znany schemat biletowy (żetonowy) [17]. Wg tego schematu użytkownik zgłasza się do „kasy biletowej” (ang. *toll booth*) po bilet uprawniający do skorzystania z zasobu wg określonych warunków. Następnie, użytkownik zgłasza się do zasobu i po okazaniu biletu wykonuje określoną w warunkach nabycia biletu operację. Przykładem wykorzystania takiego schematu jest kino.

Ogólny schemat biletowy bezpiecznego dostępu do zasobu GRID, wygląda jak na Rysunek 4.

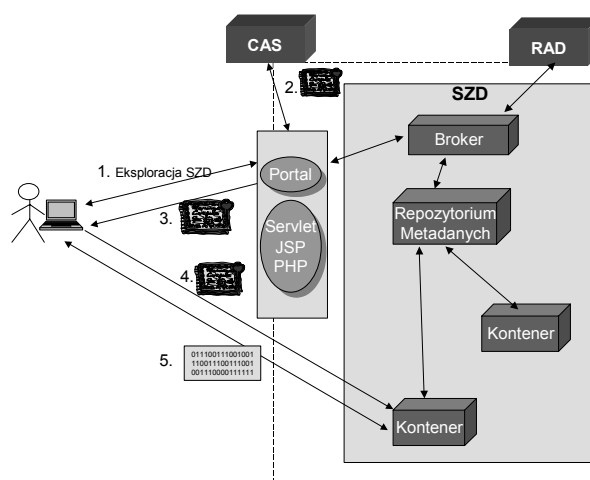


Rysunek 4 Ogólny schemat bezpiecznego dostępu do zasobów

Przebieg zdarzeń:

1. Użytkownik wysłał żądanie do „kasy” dysponującej dostępem do rzeczywistych danych. Żądanie jest podpisane cyfrowo kluczem prywatnym użytkownika.
2. „Kasa” generuje dla użytkownika bilet. Jest to formalnie certyfikat proxy X.509 [18]. „Kasa” podpisuje bilet swoim kluczem prywatnym, staje się więc wystawcą biletu. W polu DN certyfikatu zostaje umiesz- umieszczony identyfikator użytkownika. W

- tw. polityce biletu (opcjonalne pole „policy” w nagłówku X.509v3) „kasa” koduje identyfikator zasobu i dodatkowe warunki korzystania z zasobu.
4. Użytkownik zgłasza się z biletem bezpośrednio do zasobu. Certyfikat jest weryfikowany po kątem sygnatury podpisu (zasób sprawdza czy wystawcą biletu jest zaufana „kasa”) oraz właściciela określonego w polu DN nagłówka certyfikatu X.509.
  5. Jeżeli weryfikacja wypadnie pozytywnie, to zasób jest udostępniany przez protokół SSL.



Rysunek 5 Schemat bezpiecznego dostępu do fizycznych zasobów SZD

Architektura SZD (jedno repozytorium będące odpowiednikiem „toll booth” i wiele kontenerów danych - zasobów) predysponuje system do korzystania z ogólnego modelu biletowego: w zakresie udostępniania zasobów użytkownikom. Przebieg zdarzeń w przypadku zaadoptowania schematu biletowego do SZD (Rysunek 5) wygląda następująco:

1. Użytkownik, po uwierzytelnieniu w systemie CAS, eksploruje SZD za pośrednictwem Portalu, który komunikuje się z Brokerm Danych poprzez protokół SOAP. Żądanie wykonania operacji na pliku powoduje odwołanie się Repozytorium Metadanych, za pośrednictwem Brokera Danych, do systemu RAD w celu autoryzowania żądania. W wyniku pozytywnej autoryzacji Broker zwraca do Portalu właściwy metaopis pliku.
2. Portal formułuje bilet dla użytkownika. Polega to na przygotowaniu polityki oraz określenia czasu ważności biletu. Takie parametry wraz z identyfikatorem użytkownika, są przekazywane do CAS, który generuje czasowy bilet (certyfikat proxy).
3. Utworzony bilet jest przekazywany użytkownikowi. Upoważnia on do dostępu do Kontenera Danych (odwołanie do serwera GridFTP lub GASS).
4. Uwierzytelnienie użytkownika w Kontenerze Danych za pomocą certyfikatu proxy, weryfikacja polityki zawartej w certyfikacie.
5. Zestawienie kanału SSL i transfer pliku (GridFTP lub GASS).

#### **4. Wady i zalety**

Zaprezentowany w rozdz. 3.5 algorytm posiada niewątpliwą zaletę polegającą na zgodności z filozofią i standardami gridowych systemów bezpieczeństwa. Stosując algorytm mamy pewność, że złożone operacje na rozproszonych zasobach, cechują się atomowością i niezaprzeczalnością. Algorytm nie wymaga dodatkowej sygnalizacji między rozproszonymi zasobami. Wszelkie informacje opisujące sposób wykorzystania zasobu mogą być przenoszone w bilecie, bez skutków w postaci osłabienia systemu bezpieczeństwa.

Wadą rozwiązania jest konieczność korzystania po stronie zasobu z bardziej zaawansowanych serwerów, które oprócz weryfikacji certyfikatu pod kontem sygnatury podpisu, pozwalają również na dołączenie uchwytu („handlera”) badającego opcjonalne pola X.509v3. Większość typowych serwerów HTTPS, FTPS, SSH, a także GridFTP i GASS w wersji Globus Toolkit 2.4 i wcześniejszej nie spełniają tego warunku [3]. Aby korzystać z funkcjonalności opcjonalnych pól X.509 można zastosować Globus Toolkit 3.2 lub 4.0 lub własne modyfikacje serwerów HTTPS, FTPS itd.

#### **5. Podsumowanie**

Laboratoria wirtualne często postrzegane są jako pewne panaceum na problemy związane z zakupem drogich i unikatowych urządzeń, czy z ułatwionym i powszechnym dostępem do nich. Obecnie technologie z nimi związane są na etapie intensywnego rozwoju. Powstają nowe serwisy umożliwiające wykonanie prostych eksperymentów, w których można sterować niewielką liczbą parametrów. Obecny projekt VLAB jest pierwszym krokiem do budowy systemu, który jednocześnie spełnia założenia budowy laboratoriów wirtualnych jak i jest w pełni funkcjonalny i elastyczny. Każdy taki system oprócz dostępu do przyrządu powinien także umożliwiać przechowywanie danych jak i zarządzanie nimi.

Ponadto, ważne jest aby zaprojektowany system zapewniał bardzo wysoki poziom bezpieczeństwa. Jest on konieczny ze względu na duże znaczenie informacji jakie mają być przetwarzane i przechowywane z jego użyciem. Naukowcy, którzy są docelowymi użytkownikami systemu, przykładają ogromną wagę do własności intelektualnej i starają się chronić osiągnięte przez siebie wyniki. Oprócz aspektu własności intelektualnej istnieje także kwestia poufności wyników związana z tajnością prowadzonych badań (np. dla celów wojskowych). System Zarządzania Danymi powinien oprócz możliwości przechowywania danych zapewnić satysfakcjonujący poziom bezpieczeństwa, który ma być kompromisem między bezpieczeństwem danych i łatwością korzystania z nich.

W opracowaniu przedstawiono biletowy mechanizm bezpiecznego korzystania z zasobów SZD. Mechanizm ten wpisuje się w ogólny system bezpieczeństwa gridu, tzn. bazuje na tzw. silnej kryptografii i infrastrukturze zaufania PKI. Cechuje się niezaprzeczalnością autoryzacji operacji dostępu do zasobów oraz poufnością przesyłanych danych. Mechanizm biletowy posiada pewne wady, ale trudno wskazać dla niego co najmniej równoważną alternatywę.

#### **Literatura**

- [1] Diana Bosio, James Casey, Akos Frohner, Leanne Guy, Peter Kunszt, Erwin Laure, Sophie Lemaitre, Levi Lucio, Heinz Stockinger, Kurt Stockinger, “Next-Generation EU DataGrid Data Management Services”, Computing in High Energy and Nuclear Physics, 2003,

- <http://www.slac.stanford.edu/econf/C0303241/proc/papers/TUAT008.PDF>
- [2] Lawenda M., Meyer N., Rajtar T., „General framework for Virtual Laboratory”, Cracow Grid Workshop, 11-14 grudzień 2002, Kraków
  - [3] The Globus Toolkit WWW page: <http://www-unix.globus.org/toolkit/>
  - [4] Lawenda M., „Laboratorium Wirtualne i Teleimersja”, Raport wewnętrzny PCSS nr RW-34/01, Poznań 2001
  - [5] Lawenda M., „Projekt architektury warstw ogólnej oraz specyficznej dla koncepcji laboratorium wirtualnego”, Raport wewnętrzny PCSS nr RW-2/02, Poznań 2002
  - [6] R. W. Adamiak, Z. Gdaniec, M. Lawenda, N. Meyer, Ł. Popenda, M. Stroiński, K. Zieliński, Laboratorium wirtualne w środowisku gridowym, materiały z konferencji Pionier 2003, Poznań, kwiecień 2003, str. 155-166
  - [7] Portal Laboratorium Wirtualnego <http://vlab.man.poznan.pl/>
  - [8] PROGRESS - Polish Research on Grid Environment for SUN Servers, <http://progress.psnk.pl/English/index.html>
  - [9] Object Management Group <http://www.omg.org/>
  - [10] National Radio Astronomy Observatory <http://www.nrao.edu/>
  - [11] SHARP: An Architecture for Secure Resource Peering [berkeley.intel-research.net/bnc/papers/sharp-sosp03.pdf](http://berkeley.intel-research.net/bnc/papers/sharp-sosp03.pdf)
  - [12] P. Szychowski, M. Lawenda, M. Wolski, N. Meyer, M. Kopeć, C. Mazurek, M. Stroiński, „Bezpieczny dostęp do usług zarządzania danymi w systemie laboratorium wirtualnego”, Raport wewnętrzny PCSS nr RW-5/04, kwiecień 2004, Poznań
  - [13] Grzybowski P., Mazurek C., Spychała P., Wolski M.: Data Management System for grid and portal services. Submitted to Grid Computing: Infrastructure and Applications special issue of The International Journal of High Performance Computing Applications (IJHPCA), Cardiff University, UK, <http://progress.psnk.pl/English/DMS.pdf>
  - [14] Anne Zieger, Chief analyst, PeerToPeerSource.com, “Grid security: state of the art”, July 2003, <http://www-106.ibm.com/developerworks/grid/library/gr-security.html>
  - [15] Single Sign-On, Security WWW page <http://www3.ca.com/Solutions/Product.asp?ID=166>
  - [16] Chris Dune, Technical Director, Big Picture Software, “Build and implement a single sign-on solution”, 30 September 2003, <http://www-106.ibm.com/developerworks/library/wa-singlesign/>
  - [17] Manage credentials and access control in a grid application <http://www-106.ibm.com/developerworks/library/gr-cred/?Open&ca=daw-gc-dr>
  - [18] RFC 3820 Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile (<ftp://ftp.rfc-editor.org/in-notes/rfc3820.txt>).
  - [19] V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, S. Tuecke. „Security for Grid Services“, Twelfth International Symposium on High Performance Distributed Computing (HPDC-12), IEEE Press, to appear June 2003, <http://www.globus.org/Security/GSI3/GT3-Security-HPDC.pdf>
  - [20] Lawenda M., Meyer N., Okoń M., Rajtar T., Stroiński M., „Laboratorium Wirtualne – Wymagania Niefunkcjonalne”, Raport wewnętrzny PCSS nr RW-4/03, Poznań 2003
  - [21] Projekt architektury bezpieczeństwa dla struktury obliczeniowej realizowanej w ramach projektu SgiGrid. Pakiet roboczy WP7 PCSS, WCSS, Cyfronet.

*XI Konferencja „Sieci i Systemy Informatyczne”  
Łódź, październik 2004*

---

PAWEŁ SZYCHOWSKI

psz@p.lodz.pl

MIROŚLAW KOPEĆ

kopec@sir.p.lodz.pl

Centrum Komputerowe Politechniki Łódzkiej

90-924 Łódź, Wólczajska 175

tel.: (+48 42) 638-35-28 fax: (+48 42) 638-35-05

MARCIN LAWENDA

lawenda@man.poznan.pl

MARCIN WOLSKI

maw@man.poznan.pl

NORBERT MEYER

meyer@man.poznan.pl

CEZARY MAZUREK

mazurek@man.poznan.pl

MACIEJ STROIŃSKI

stroins@man.poznan.pl

Poznańskie Centrum Superkomputerowo Sieciowe

61-704 Poznań, Noskowskiego 10

tel. (0 61) 858-20-52 fax. (0 61) 852-59-54