Dagmara BUBEL
Lidia SZCZYGŁOWSKA
Politechnika Częstochowska
Biblioteka Główna

Łukasz KUCZYŃSKI
Politechnika Częstochowska
Instytut Informatyki Teoretycznej i Stosowanej

CZEGO JESZCZE NIE WIEMY O USŁUDZE POWSZECHNEJ ARCHIWIZACJI PLATON-U4

Długoterminowa archiwizacja, oprócz zapewnienia właściwej liczności udostępnianych zbiorów, standaryzacji oraz identyfikowalności treści, usług i osób, jest uznawana za najważniejszą cechę właściwie zorganizowanego środowiska informacji cyfrowej[1]. Największymi generatorami danych cyfrowych są biblioteki i archiwa, instytuty, uczelnie i jednostki naukowe oraz akademickie centra komputerowe. Skuteczne i wiarygodne zabezpieczenie lub archiwizacja tak dużych ilości danych jest ogromnym wyzwaniem i może przekraczać możliwości bibliotek. Usługa Powszechnej Archiwizacji oparta na oprogramowaniu Krajowego Magazynu Danych (KMD), które zostało wdrożone w redundantnej, wysoko wydajnej, skalowalnej i rozproszonej infrastrukturze serwerów i systemów przechowywania danych, wychodzi naprzeciw potrzebom zabezpieczania danych w instytucjach naukowych. System został tak zaprojektowany, aby spełnić wymagania użytkowników dotyczące: bezpieczeństwa danych, ich dużej trwałości, niezawodności i prostoty użytkowania. Kontynuacją projektu Krajowego Magazynu Danych – KMD2 – jest implementacja zaawansowanych mechanizmów zwiększających funkcjonalność rozproszonego systemu. W systemie KMD2 wysoki priorytet nadano bezpieczeństwu kopii zapasowych i archiwalnych. Usługa daje możliwość zaszyfrowania informacji jeszcze przed przesłaniem ich do systemu, a także automatycznej kontroli integralności pobieranych danych. Szyfrowanie pozostaje w gestii użytkownika. Znaczną część pracy włożono w realizację: bezpiecznego współdzielenia plików z innymi użytkownikami KMD2, importu-eksportu plików do systemu/poza system KMD2 oraz publikacji danych, co może być interesującym rozwiązaniem dla bibliotek cyfrowych.

Wstęp

Usługa Powszechnej Archiwizacji, która wychodzi naprzeciw potrzebom zabezpieczania danych w instytucjach naukowych, jest realizowana przez Poznańskie Centrum Superkomputerowo-Sieciowe w ramach projektu PLATON – Platformy Obsługi Nauki, na podstawie ogólnopolskiej akademickiej sieci naukowej PIONIER.

[1] M. Nahotko: Komunikacja naukowa w środowisku cyfrowym. Wydawnictwo SBP, Warszawa 2010, s. 189.

Usługa jest oparta na oprogramowaniu Krajowego Magazynu Danych (KMD), które zostało wdrożone w redundantnej, wysoko wydajnej, skalowalnej i rozproszonej infrastrukturze serwerów i systemów przechowywania danych. System został tak zaprojektowany, aby spełnić wymagania użytkowników dotyczące: bezpieczeństwa danych, ich dużej trwałości, niezawodności i prostoty użytkowania. W projekcie bierze udział 10 polskich centrów superkomputerowych i jednostek MAN, a jego koordynatorem jest Poznańskie Centrum Superkomputerowo-Sieciowe. To pierwsze rozwiązanie o tak dużym zasięgu w skali kraju[2].

Jedną z podstawowych technik zapewnienia wiarygodności przechowywania danych i ich trwałości oraz niezawodności usługi przechowywania jest replikacja danych w rozproszonym środowisku przechowywania oraz wykorzystanie redundantnych komponentów infrastruktury. Usługa dostarcza użytkownikom rozmaite interfejsy dostępu do danych składowanych w wirtualnym systemie plików oraz możliwość automatyzacji i optymalizacji procesu wykonywania kopii zapasowych i archiwalnych przez wykorzystanie aplikacji klienta opracowanego w projekcie KMD.

Infrastruktura Usługi Powszechnej Archiwizacji

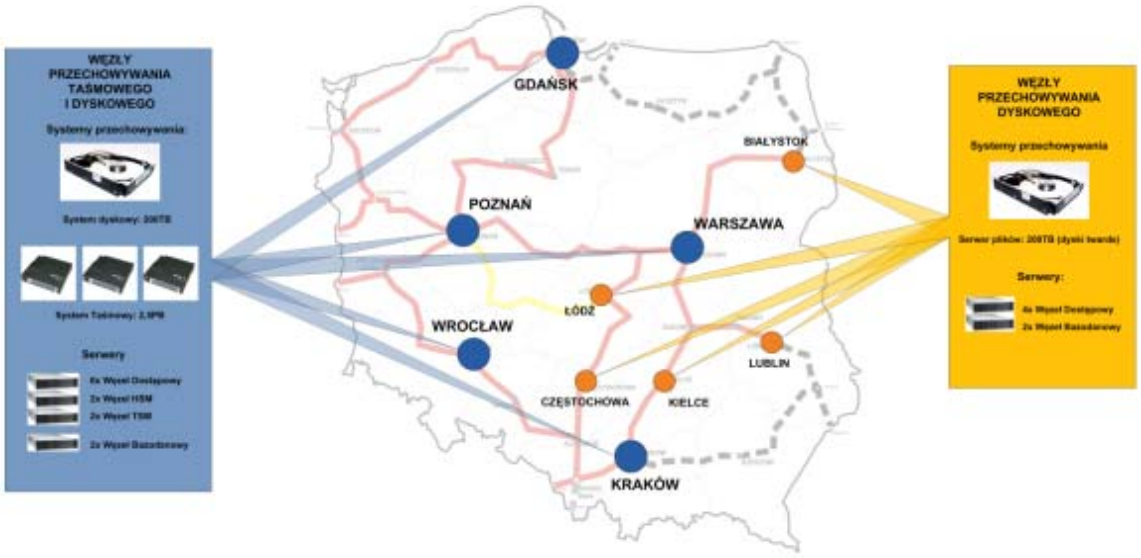
Infrastruktura Usługi Powszechnej Archiwizacji, w której została wdrożona architektura Krajowego Magazynu Danych, składa się z redundantnych, rozproszonych geograficznie elementów. Podstawowym składnikiem tej infrastruktury są systemy przechowywania, w tym macierze dyskowe i serwery plików o łącznej pojemności ok. 2 petabajtów, oraz systemy przechowywania taśmowego o pojemności 12,5 petabajta. Poza systemami przechowywania danych na infrastrukturę składają się serwery dostępowe, bazodanowe oraz serwery dla oprogramowania HSM – łącznie ponad 70 maszyn. Elementy instalacji są rozlokowane w 10 miastach Polski i połączone za pomocą wydajnych łączy sieciowych w PIONIER.

Infrastruktura Usługi Powszechnej Archiwizacji, w której wdrożona jest skalowalna architektura Krajowego Magazynu Danych, pozwala na oferowanie usług przechowywania danych, odpowiadających potrzebom użytkowników co do pojemności systemu, wydajności składowania, trwałości danych w systemie, wiarygodności usługi, a także bezpieczeństwa i poufności danych[3].

---

[2] M. Brzeźniak: PLATON: usługi powszechnej archiwizacji. „Pionier Magazine", nr 1 (6), 2011.

[3] M. Brzeźniak: Usługa Powszechnej Archiwizacji i jej zastosowanie w bibliotekach naukowych do zabezpieczenia i archiwizacji danych. „Biuletyn EBIB", nr 6 (115), 2010, [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://www.ebib.info/2010/115/a.php?brzezniak



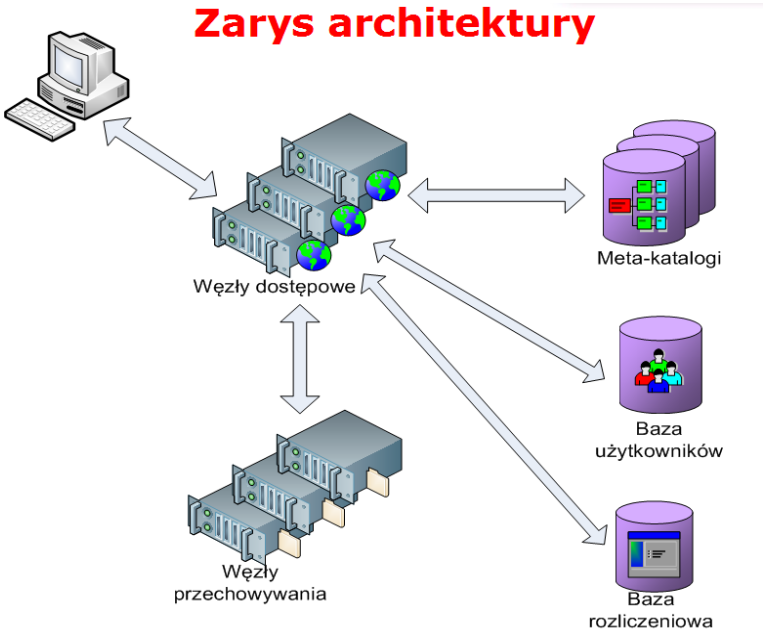
Rys. 1. Schemat infrastruktury Usługi Powszechnej Archiwizacji
Źródło: M. Brzeźniak: Usługa Powszechnej Archiwizacji i jej zastosowanie w bibliotekach naukowych do zabezpieczenia i archiwizacji danych. „Biuletyn EBIB", nr 6 (115), 2010, [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://www.ebib.info/2010/115/a.php?brzezniak

Charakterystyka architektury jest następująca:

- decentralizacja danych oraz usług,
- replikacja metadanych,
- liczne punkty dostępowe (węzły dostępowe),
- liczne lokalizacje przechowywania replik (węzły Składowania),
- centralna baza danych użytkowników (pojedyncze logowanie, ang. *single sign-on*),
- standardowe interfejsy pomiędzy warstwami: wirtualny system plików oraz standardowe metody dostępu do danych.

Poufność i bezpieczeństwo danych to:

- szyfrowanie połączeń klient-system i wewnątrz systemu (X.509),
- oddzielne przestrzenie nazw dla instytucji,
- audyty bezpieczeństwa systemu i oprogramowania,
- przechowywanie odpowiedniej liczby replik,
- wsparcie dla szyfrowania sprzętowego,
- komunikacja przez VPN.



Rys. 2. Zarys architektury
Źródło: S. Jankowski, M. Brzeźniak: Architektura i mechanizmy systemu. Warsztaty „Usługa powszechnej archiwizacji", [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://www.pionier.net.pl/ files/platon-u4_architektura_i_mechanizmy_final_mb.pdf

Dostęp do danych. Standardowe protokoły dostępu do danych i metadanych

Dane użytkowników są przechowywane w postaci wielu fizycznych replik danych rozmieszczonych w rozproszonych geograficznie lokalizacjach. Po stronie użytkownika jest typowe oprogramowanie klienckie:

- SSH/SCP/SFTP (WinSCP, SSHFS),
- HTTP/WebDAV (przeglądarka internetowa, klient WebDav, mapowanie dysków w Windows),
- GridFTP.

Po stronie systemu są emulowane systemy plików z danymi i metadanymi.

Jak zamówić usługę? Kroki rejestracyjne

Użytkownicy usługi muszą legitymować się certyfikatami cyfrowymi wystawionymi przez urząd certyfikacji uznawany w usłudze. Można wystąpić o wydanie certyfikatu (https://ra.wcss.pki.pionier.net.pl/ejbca/enrol/personal_orgs.jsp). Po zakończeniu procedury rejestracji otrzymujemy informację potwierdzającą proces zakończenia rejestracji i aktywację usługi.

Projekt KMD2

Kolejnym etapem budowy Krajowego Magazynu Danych – KMD2 – jest implementacja zaawansowanych mechanizmów zwiększających funkcjonalność rozproszonego systemu[4]. Projekt ten jest kontynuacją Krajowego Magazynu Danych i ma za zadanie dostarczyć poszerzonego wachlarza usług osadzonych na infrastrukturze bazowej, przygotowanej w ramach projektu KMD.

Szczególny nacisk jest położony na bezpieczeństwo opracowywanych rozwiązań:

- bezpieczne składowanie – przez wirtualne filesystemy i aplikacje klienckie,
- bezpieczne współdzielenie wewnątrz systemu,
- bezpieczny eksport-import danych,
- bezpieczna publikacja,
- wersjonowanie (dodatkowe wersje plików zwiększają możliwości odtwarzania).

Główne zadania KMD2 to: umożliwienie składowania kopii zapasowych i przechowywanie długoterminowe danych archiwalnych, bezpieczne udostępnianie, współdzielenie i wymiana dużych plików oraz przechowywanie i bezpieczne udostępnianie online zbiorów cyfrowych dużych rozmiarów[5].

Funkcjonalności, o jakie KMD2 wzbogaca system KMD, obejmują:

- współdzielenie danych wewnątrz systemu KMD2 przez użytkowników,
- bezpieczne udostępnianie danych użytkownikom zewnętrznym i bezpieczną publikację danych w tzw. ograniczonym środowisku udostępniania i wymiany plików (Sandbox),
- wersjonowanie danych, zarządzanie wersjami i prezentacja wersji plików,
- bezpieczne urządzenie kopiująco-szyfrujące – tzw. appliance – realizujące wydajną kryptografię (wspomaganą sprzętowo), a także funkcję współdzielenia danych wewnątrz organizacji.

W systemie KMD2 wysoki priorytet nadano bezpieczeństwu kopii zapasowych i archiwalnych. Usługa daje możliwość zaszyfrowania informacji jeszcze przed przesłaniem ich do systemu, a także automatycznej kontroli integralności pobieranych danych. Szyfrowanie pozostaje w gestii użytkownika. Fundamentem funkcjonalności bezpiecznego systemu składowania danych są mocne algorytmy szyfrujące. Rozwiązanie to zapewnia poufność oraz integralność składowanych danych, jak również umożliwia bezpieczne współdzielenie nawet w sytuacji, gdy użytkownik nie

[4] Krajowy Magazyn Danych (KMD2) – spotkanie robocze w CI TASK w dniach 12-14 czerwca 2013 r. w Gdańsku, [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://tv.task.gda.pl/?p=973

[5] Krajowy Magazyn Danych (KMD2), [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://www.wcss.wroc.pl/?c=static_projects&sid=150

ma zaufania do przestrzeni dyskowej dostawcy. W tym celu zaimplementowano algorytmy kryptograficzne ze wsparciem dla symetrycznego oraz asymetrycznego szyfrowania „w locie" (ang. *on the fly*) po stronie użytkownika[6]. Szyfrowane są zarówno nazwy plików, jak i ich zawartość. W ten sposób użytkownik może mieć pewność, że jego dane są bezpieczne niezależnie od miejsca, w którym są przechowywane. Ponadto KMD2 gwarantuje, że pliki przechowywane w systemie są dokładnie tymi, które przekopiował użytkownik. Po stronie użytkownika wyliczane są sumy kontrolne, które są sprawdzane podczas pobierania pliku. Kolejnym ważnym problemem, który powinien zostać rozwiązany w bezpiecznym systemie składowania danych, jest zapewnienie poprawności mechanizmowi zarządzania kluczami, przy jednoczesnym zachowaniu przyjaznego systemu dla użytkownika niebędącego ekspertem w dziedzinie kryptografii.

W KMD2 położono silny nacisk na wymogi bezpieczeństwa użytkowników, jak również na stworzenie intuicyjnego, przejrzystego oraz w pełni funkcjonalnego interfejsu dla użytkownika, ukrywającego niejako przed nim skomplikowaną architekturę systemu. Uproszczono interfejsy systemowe, tak aby użytkownicy mogli korzystać z KMD2, mając wrażenie pracy z lokalnym filesystemem, podczas gdy w rzeczywistości operują za pośrednictwem sieciowego systemu plików. Ponadto zaoferowano zaawansowane mechanizmy pozwalające na: wersjonowanie plików, zarządzanie wersjami, tagowanie danych, nadawanie adnotacji, wyszukiwanie po metadanych, bezpieczeństwo, współdzielenie pomiędzy organizacjami oraz intuicyjne zarządzanie uprawnieniami dostępu do plików za pośrednictwem zaawansowanych aplikacji[7].

System KMD2 przechowuje wersje archiwalne magazynowanych plików. Każda zmiana bądź każde nadpisanie pliku powoduje utworzenie nowej wersji. Stare wersje są usuwane po pewnym czasie, jednak istnieje możliwość ustawienia liczby przechowywanych wersji oraz zabezpieczenia konkretnej wersji przed automatycznym usunięciem.

Znaczną część pracy włożono w realizację bezpiecznego współdzielenia plików z innymi użytkownikami KMD2. Uprawnienia dostępu do nich zostały zrealizowane w formie systemowych uprawnień do odczytu, zapisu lub wykonania wybranej grupie bądź użytkownikowi. Dodatkowo w przestrzeni szyfrowanej kontrolę dostępu do danych zabezpieczają metody kryptograficzne.

---

[6] Krajowy Magazyn Danych (KMD2), [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://kmd.pcss.pl/
[7] Ibidem.

System KMD2 umożliwia także wymianę plików z użytkownikami zewnętrznymi. Mechanizm ten jest realizowany przez moduł Sandbox, który pozwala osobom niemającym konta w KMD2 uzyskać dostęp do wyeksportowanych plików. W przypadku eksportu plików należy zdefiniować, które pliki mają zostać wysłane, a także podać listę ich odbiorców (podać ich adresy e-mail). Jeśli użytkownik chciałby umożliwić komuś przesłanie plików do jego konta w KMD2, również jest to możliwe, po zdefiniowaniu zadania importu plików i określeniu w nim maksymalnego rozmiaru oraz liczby oczekiwanych plików (należy także podać e-maile osób, które mają prawo do przesyłania plików). W celu zwiększenia bezpieczeństwa importowane pliki nie są automatycznie zapisywane na koncie użytkownika, a ich przekopiowanie musi zostać potwierdzone przez właściciela docelowego konta. KMD2 wspiera także szyfrowanie eksportowanych oraz importowanych plików.

Wśród mechanizmów KMD2 istnieje także taki, który pełni funkcję publikacji przechowywanych treści. Aby upublicznić jakieś zasoby, wystarczy utworzyć przestrzeń publikacji, a następnie przypisać do tej przestrzeni wybrany folder lub wybrane pliki. Publikowane zasoby to tylko kopie plików znajdujących się w KMD2. W systemie istnieje powiązanie publikowanego zasobu z plikiem źródłowym. Użytkownik może „listować" zawartość publikowanych przestrzeni oraz zarządzać nimi. Zasoby są publikowane na stronie WWW.

Bezpieczne współdzielenie to:

- współdzielenie z użytkownikami KMD2 (możliwe szyfrowanie, dostęp dla wybranej grupy),
- współdzielenie publiczne,
- wysoki poziom bezpieczeństwa: sym. i asym.

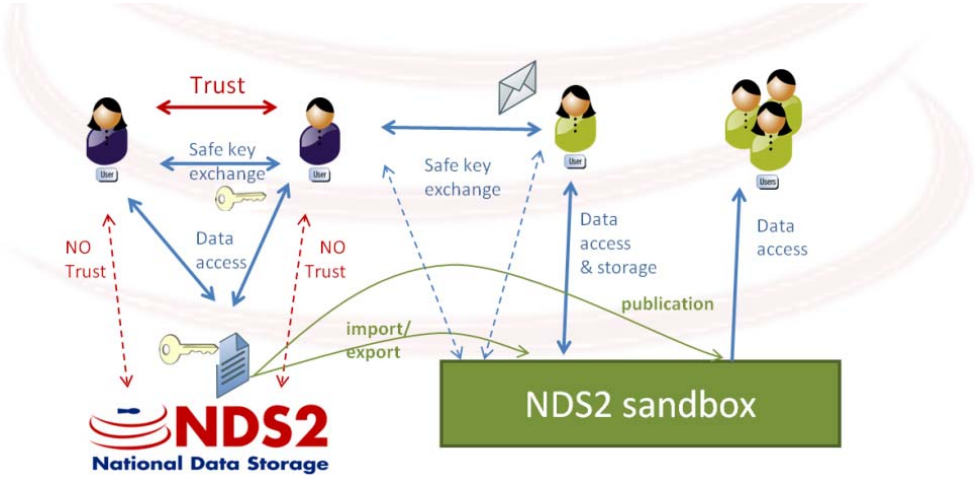
Bezpieczne publikowanie oraz import/eksport danych do systemu/poza system:

- jest podobne do *get file link'* w Dropbox,
- jest to praca w dwóch kierunkach.

Bezpieczniejsze niż z Dropbox…

Pasywny moduł Sandbox umożliwia import/eksport plików do systemu/poza system KMD2 oraz publikację danych. Nowe funkcjonalności systemu dają możliwość jego wykorzystania zarówno przez duże jednostki organizacyjne, jak i przez indywidualnych użytkowników[8].

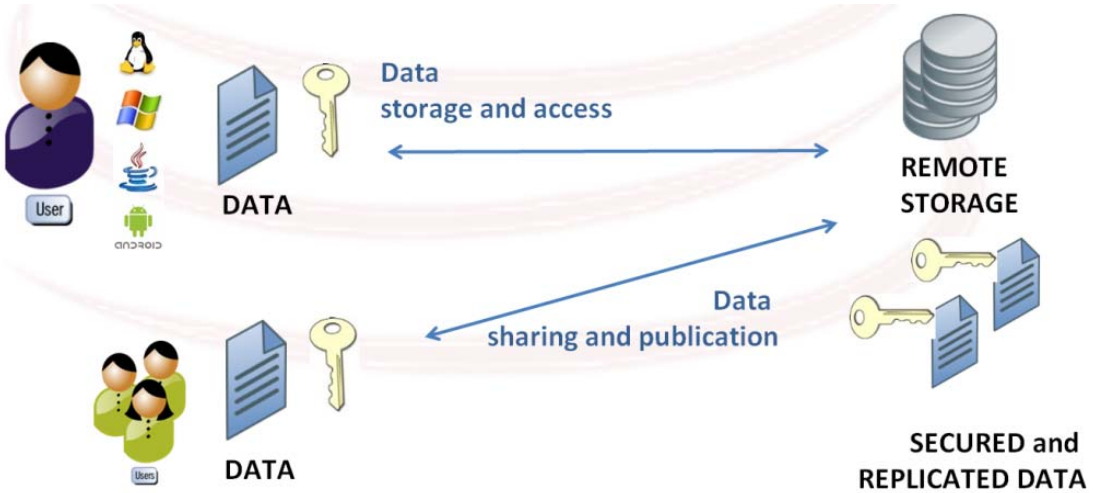
[8] Krajowy Magazyn Danych (KMD2), [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://www.wcss.wroc.pl/?c=static_projects&sid=150



Rys. 3. Schemat zaawansowanych mechanizmów KMD2
Źródło: S. Jankowski, M. Brzeźniak: National Data Store 2 Secure Storage Cloud with efficient and easy data access, [dostęp: 20.10.2013 r.]. Dostępny w Internecie: https://tnc2013.terena.org/getfile/733

Użytkownikowi indywidualnemu (naukowiec, badacz) zapewni:

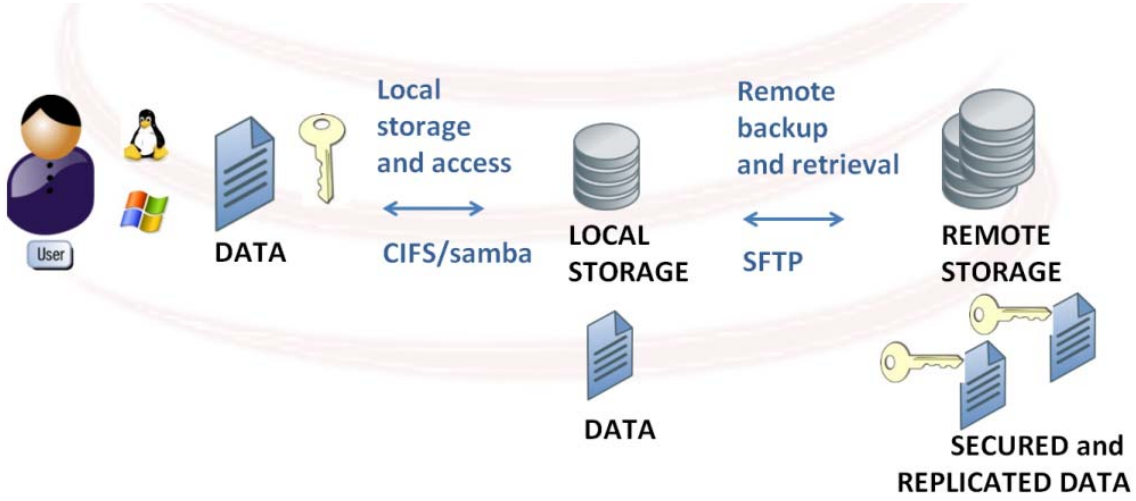
- bezpieczeństwo, dostępność i trwałość danych,
- łatwy, wydajny dostęp do danych z poziomu różnych systemów operacyjnych,
- transparentne, bezpieczne i poufne mechanizmy,
- możliwość dzielenia się danymi i możliwość ich publikowania.



Rys. 4. Przykład zastosowania usługi KMD2 przez indywidualnego użytkownika
Źródło: S. Jankowski, M. Brzeźniak: National Data Store 2 Secure Storage Cloud with efficient and easy data access, [dostęp: 20.10.2013 r.]. Dostępny w Internecie: https://tnc2013.terena.org/getfile/733

Instytucji, grupie użytkowników (biblioteka cyfrowa, repozytorium, projekt naukowy) zapewni on:

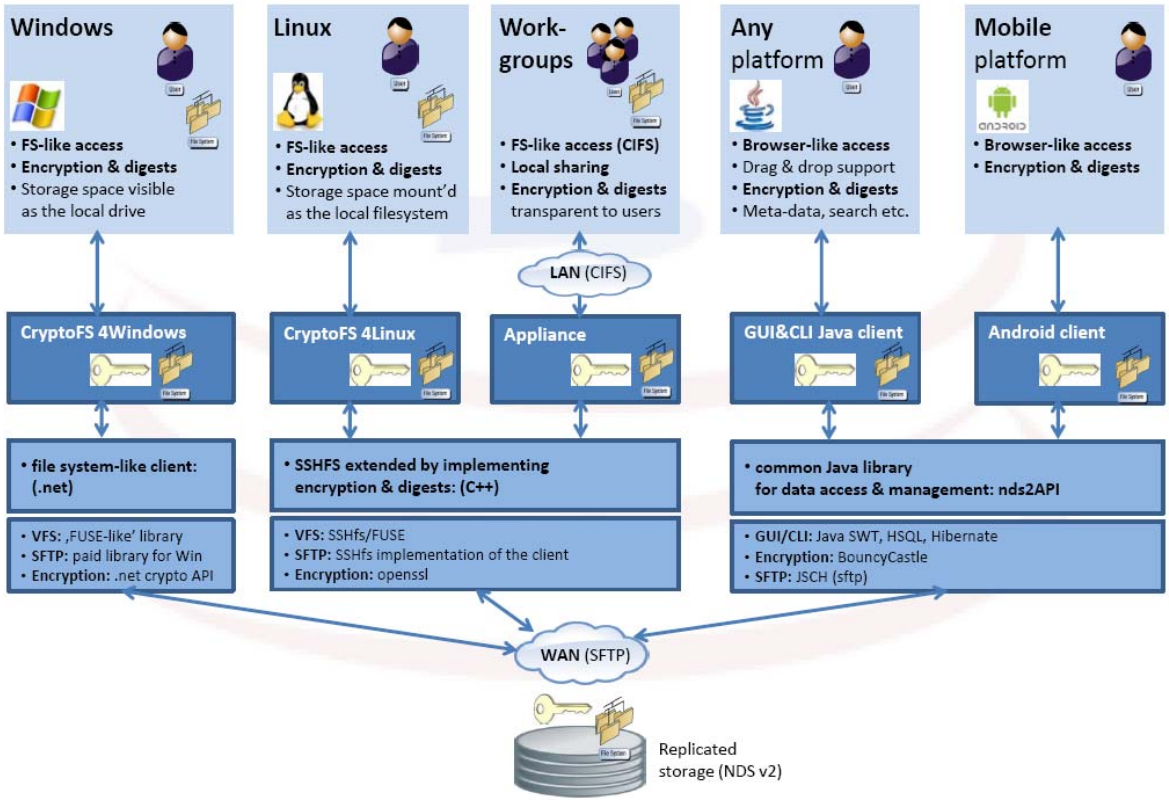
- bezpieczeństwo, dostępność, trwałość danych,
- lokalną przestrzeń pracy z prostym i skutecznym (wydajnym) dostępem poprzez typowe protokoły LAN (CIFS, NFS),
- lokalną przestrzeń poszerzoną o zdalną przestrzeń.



Rys. 5. Przykład zastosowania usługi KMD2 przez instytucje lub grupę użytkowników
Źródło: S. Jankowski, M. Brzeźniak: National Data Store 2 Secure Storage Cloud with efficient and easy data access, [dostęp: 20.10.2013 r.]. Dostępny w Internecie: https://tnc2013.terena.org/getfile/733

Aplikacje klienckie KMD2

Aby w pełni móc wykorzystywać większą funkcjonalność rozproszonego systemu plików KMD2, należy używać specjalnych aplikacji klienckich umożliwiających stosowanie mechanizmów przewidzianych w KMD2. Część funkcjonalności KMD2 jest wspierana klientów wirtualnych systemów plików (nds2cryptoFS4Lin/Win), dzięki którym można zamontować system i pracować na nim jak na lokalnym filesystemie. Przewidziano je dla dwóch systemów operacyjnych: Windows oraz Linux. Oprócz tego możliwe będzie korzystanie z wieloplatformowej aplikacji NDS2GUI, która pozwoli na pełne wykorzystanie wszystkich mechanizmów KMD2 oraz z klienta dla urządzeń mobilnych (NDS2DROID) wyposażonych w system operacyjny Android.



Rys. 6. Schemat koncepcji aplikacji dostępowych KMD2
Źródło: M. Brzeźniak, S. Jankowski: National Data Store 2 crypto-clients – demonstration, [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://www.terena.org/activities/tf-storage/ws14/slides/20130306-NDS2.pdf

Dla klientów korporacyjnych jest przewidziane jest inne rozwiązanie – dedykowane urządzenie Appliance wykonujące automatyczne backupy do konta KMD2. Analiza dostępnych na rynku interfejsów podobnych systemów wykazała, iż najbardziej przyjazny użytkownikowi byłby wirtualny system plików, zatem zaimplementowano ndsCryptoFs4Windows, wykorzystując do tego bibliotekę umożliwiającą dostęp do warstwy pomiędzy systemem operacyjnym a systemem plików, która współpracuje ze wszystkimi wersjami systemu Windows. Zaimplementowano szyfrowanie, obsługę kluczy, sprawdzanie sum kontrolnych, współdzielenie oraz zarządzanie dostępem do danych. Oprócz tego użyto innej biblioteki, obsługującej protokół SFTP na większości systemów z rodziny Windows. Dla systemu Linux stworzono podobną aplikację: ndsCryptoFs4Linux, która jest rozszerzeniem narzędzia SSHFS o funkcje kryptograficzne, sprawdzanie sum kontrolnych, a także wsparcie dla bezpiecznego współdzielenia danych.

Poza wirtualnymi systemami plików współpraca z systemem jest możliwa z wykorzystaniem przenośnej aplikacji Java, która pozwala użytkownikom w łatwy sposób przechowywać i przeglądać swoje dane. Implementacja aplikacji Java opera się na API, które dostarcza kompletnego interfejsu wykorzystującego wszystkie możliwe operacje na systemie KMD2, włączając szyfrowanie oraz kontrolę integralności danych. API Java daje aplikacjom interfejsu użytkownika możliwość wykonywania zaawansowanych operacji na systemie metadanych, tj. zarządzania wersjami plików, tagowania danych, wyszukiwania danych po metainformacjach, zarządzania współdzieleniem czy systemowym dostępem do danych. Na podstawie API Java zostało zaimplementowanych kilka aplikacji: GUI (opierające się na bibliotece SWT), aplikacja konsolowa CLI oraz aplikacja na urządzenia mobilne pracujące pod kontrolą systemu Android.

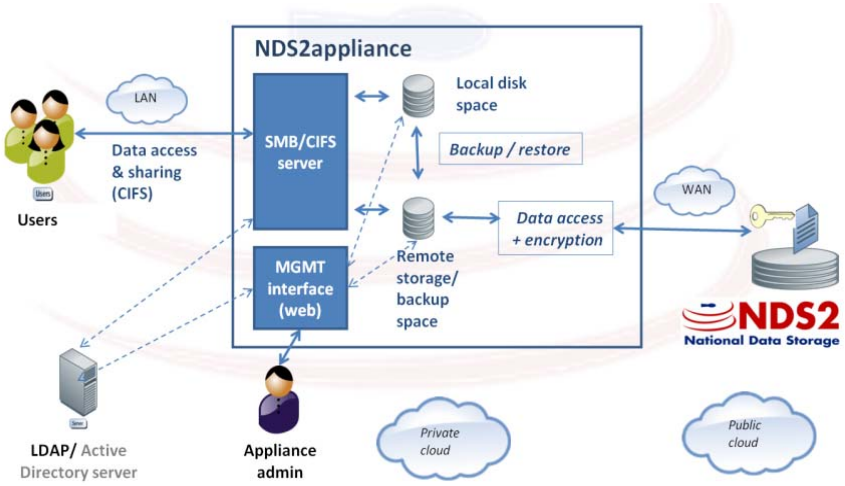
KMD2 – appliance – koncepcja dedykowanego urządzenia

Szyfrowane systemy plików KMD2 są zgodne ze standardami POSIX (poza małymi wyjątkami), które umożliwiają uruchamianie po stronie klienta aplikacji bezpośrednio z nich. Ta funkcjonalność została wykorzystana przez tzw. appliance – urządzenie przeznaczone dla instytucji lub małych grup. Użytkownicy tego urządzenia mogą przechowywać dane bezpośrednio na nim oraz konfigurować je tak, aby wykonywało kopie bezpieczeństwa do „chmury”, podczas gdy użytkownikom serwowana jest ta przestrzeń za pośrednictwem protokołu CIFS.

Zastosowanie urządzenia appliance zapewnia:

- współdzielenie danych przy użyciu lokalnego NAS (Network Attached Storage) appliance,
- ochronę danych przed zniszczeniem i atakiem: backup i szyfrowanie,
- komfort pracy przez wyposażenie w dyski lokalne (tworzące RAID), co daje dużą wydajność i małe opóźnienia oraz rozszerzenie przestrzeni dyskowej o przestrzeń zdalną KMD2 – lokalny dysk jest cache’em zdalnego.

Możliwe są dwie implementacje – w postaci fizycznego serwera lub maszyny wirtualnej.



Rys. 7. KMD2 – appliance – koncepcja dedykowanego urządzenia
Źródło: M. Brzeźniak, S. Jankowski: National Data Store 2 crypto-clients – demonstration, [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://www.terena.org/activities/tf-storage/ws14/slides/ 20130306-NDS2.pdf

a)

b)

Rys. 8. Platformy sprzętowe urządzenia szyfrującego: a) box dla małych grup/instytucji, b) rack server dla większych instytucji do montażu w szafie 19”
Źródło: M. Major, Ł. Kuczyński, M. Woźniak: Appliance szyfrujący dla MSP i instytucji. Prezentacja przygotowana na warsztaty: Krajowy Magazyn Danych, Politechnika Łódzka, 26.09.2013 r.

W obu przypadkach klucze są przechowywane na kartach SC (Smart Card) lub pendrive’ach. Istnieje także możliwość zastosowania maszyny wirtualnej na wirtualnej platformie klienta. Oprogramowanie KMD i Usługa Powszechnej Archiwizacji dają użytkownikom dostęp do skalowalnej i rozproszonej infrastruktury opartej na nowoczesnej technologii – nieosiągalnej dla większości instytucji. System został tak zaprojektowany, aby spełnić wymagania użytkowników dotyczące:

- bezpieczeństwa danych,
- dużej trwałości danych,
- niezawodności,

- prostoty użytkowania,
- innowacyjności względem istniejących rozwiązań.

Wewnątrz systemu poufność komunikacji zapewniają bezpieczne połączenia w ramach sieci PIONIER. Wirtualny system plików oferuje oddzielne przestrzenie nazw i oddzielne bazy metadanych dla różnych instytucji-klientów. Takie nowatorskie rozwiązanie powoduje wysoki poziom izolacji danych i metadanych (zwiększona poufność) i daje potencjał do rozbudowy systemu bez utraty wydajności. Dodatkowe zabezpieczenia to przechowywanie i weryfikacja sum kontrolnych, sprzętowe (de)szyfrowanie plików (na poziomie napędów taśmowych i napędów w macierzach dyskowych), a także audyty bezpieczeństwa oprogramowania i konfiguracji systemu prowadzone cyklicznie przez konsorcjum w infrastrukturze PLATONA.

Szyfrowanie pozostaje w gestii użytkownika, jednakże komunikacja z systemem odbywa się przy zastosowaniu wspomnianych bezpiecznych i standardowych protokołów, co ułatwia integrację usług systemu z narzędziami realizującymi dodatkowe techniki kryptograficzne. Rozbudowa systemu także uwzględnia zachowanie kompatybilności z już funkcjonującym systemem i umieszczonymi w nim danymi. Zmodernizowane zostają również już istniejące moduły, od tych zarządzających uwierzytelnianiem użytkowników, poprzez przechowujące/prezentujące metadane, zarządzające danymi, do metod weryfikujących obciążenie poszczególnych węzłów w celu wybrania optymalnego miejsca na replikę[9].

Poza rozszerzeniami funkcjonalnymi (z punktu widzenia użytkownika systemu) zostaną opracowane m.in. automatyczne szyfrowanie i kontrola integralności danych składowanych w systemie KMD2 po stronie użytkownika, realizowane przez odpowiedni interfejs systemu KMD2 lub urządzenie kopiująco-szyfrujące, oraz elementy monitorowania jakością usług i zarządzanie kontraktów SLA.

Bibliografia

1. Brzeźniak M.: PLATON: usługi powszechnej archiwizacji. „Pionier Magazine", nr 1 (6), 2011.
2. Major M., Kuczyński Ł., Woźniak M.: Appliance szyfrujący dla MSP i instytucji. Prezentacja przygotowana na warsztaty: Krajowy Magazyn Danych, Politechnika Łódzka, 26.09.2013 r.
3. Nahotko M.: Komunikacja naukowa w środowisku cyfrowym. Wydawnictwo SBP, Warszawa 2010.

[9] Krajowy Magazyn Danych (KMD2) – spotkanie robocze w CI TASK w dniach 12-14 czerwca 2013 r. w Gdańsku, [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://tv.task.gda.pl/?p=973

4. Brzeźniak M., Jankowski S.: National Data Store 2 crypto-clients – demonstration, [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://www.terena.org/activities/tf-storage/ws14/slides/20130306-NDS2.pdf
5. Brzeźniak M.: Usługa Powszechnej Archiwizacji i jej zastosowanie w bibliotekach naukowych do zabezpieczenia i archiwizacji danych. „Biuletyn EBIB", nr 6 (115), 2010, [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://www.ebib.info/2010/115/a.php?brzezniak
6. Jankowski S., Brzeźniak M.: Architektura i mechanizmy systemu. Warsztaty „Usługa powszechnej archiwizacji", [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://www.pionier.net.pl/files/platon-u4_architektura_i_ mechanizmy_final_mb.pdf
7. Jankowski S., Brzeźniak M.: National Data Store 2 Secure Storage Cloud with efficient and easy data access, [dostęp: 20.10.2013 r.]. Dostępny w Internecie: https://tnc2013.terena.org/getfile/733
8. Krajowy Magazyn Danych (KMD2) – spotkanie robocze w CI TASK w dniach 12-14 czerwca 2013 r. w Gdańsku, [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://tv.task.gda.pl/?p=973
9. Krajowy Magazyn Danych (KMD2), [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://www.wcss.wroc.pl/?c=static_projects&sid=150
10. Krajowy Magazyn Danych (KMD2), [dostęp: 20.10.2013 r.]. Dostępny w Internecie: http://kmd.pcss.pl/