Bezpieczeństwo udostępniania danych w systemie dLibra

Uwierzytelnianie

W systemie dLibra istnieją dwa rodzaje użytkowników – *użytkownicy normalni* oraz *użytkownicy IP*:

- *Użytkownicy normalni* mają zdefiniowany login oraz hasło. Wprowadzenie tych danych przez czytelnika w formularzu logowania powoduje uwierzytelnienie tego czytelnika jako konkretnego użytkownika w systemie. Opcjonalnie dla *użytkowników normalnych* można zdefiniować adresy IP (lub zakresy adresów, lub adresy domenowe lub maski adresów domenowych), z których podawanie hasła przy logowaniu nie jest wymagane. Przy dostępie z takiego adresu IP czytelnik wprowadza jedynie login, a zamiast hasła wykorzystywany jest adres IP, z którego nastąpiło połączenie.
- Ten mechanizm pozwala na uproszczone uwierzytelnianie w przypadku łączenia się z zaufanego adresu IP (np. z pracy czy z czytelni) oraz pełne uwierzytelnianie w przypadku łączenia się z adresu niezaufanego (np. z domu czy kawiarni internetowej).
- *Użytkownicy IP* posiadają jedynie login i adres IP (lub zakres adresów itd. jak wyżej). W przypadku, gdy czytelnik łączy się z adresu IP mieszczącego się w definicji konkretnego *użytkownika IP*, nie musi się wprost logować do systemu, lecz jest przez niego od razu postrzegany jako ten właśnie *użyt kownik IP*.

Ten mechanizm pozwala na uwierzytelnienie wyłącznie przy łączeniu się z zaufanego adresu IP, przy czym uwierzytelnianie jest realizowane w sposób praktycznie niewidoczny dla czytelnika. Przykładowa publikacja zabezpieczona w ten sposób dostępna jest pod adresem http://www.wbc.poznan.pl/dlibra/docmetadata?id=565.

Autoryzacja

System dLibra autoryzuje żądania dotyczące odczytu treści składowanych publikacji. Odczyt metadanych nie jest autoryzowany przez dLibrę, można to natomiast zrealizować zewnętrznie np. poprzez autoryzację na poziomie dostępu do serwera HTTP.

Redaktor pracujący w systemie dLibra ma możliwość przydzielenia prawa dostępu do publikacji użytkownikowi lub grupie użytkowników zdefiniowanych przez administratora. Grupa użytkowników to zbiór użytkowników normalnych i/lub użytkowników IP opisanych powyżej.

Czytelnik korzystający z systemu dLibra jest uwierzytelniany na podstawie loginu i hasła, loginu i adresu IP lub samego adresu IP (patrz punkt Uwierzytelnianie) i po pozytywnym uwierzytelnieniu jest widziany jako konkretny użytkownik systemowy. Przy próbie dostępu do treści publikacji system sprawdza, czy ten użytkownik systemowy posiada prawo odczytu treści publikacji. Jeżeli tak, to treść publikacji jest przesyłana do komputera czytelnika.

W systemie dLibra istnieje również możliwość uwierzytelniania przy pomocy tzw. grup dynamicznych, jednak mają one zastosowanie tylko w przypadku integracji dLibry z zewnętrznymi bazami danych użytkowników i nie zostały ujęte w tym opracowaniu.

Przesyłanie danych

Aplikacja czytelnika systemu dLibra dostępna jest przy pomocy protokołu HTTP. Stopień bezpieczeństwa przesyłania danych zależy bezpośrednio od konfiguracji serwera HTTP i może być oparte o połączenia SSL. W tej sytuacji czytelnik w przeglądarce WWW korzysta z połączenia HTTPS, wszystkie dane przesyłane między serwerem biblioteki cyfrowej, a komputerem czytelnika są szyfrowane. Siła szyfrowania zależy od konfiguracji mechanizmu SSL w serwerze WWW biblioteki cyfrowej.

Prezentacja danych na komputerze użytkownika

Po pozytywnym uwierzytelnieniu i autoryzacji czytelnika, czyli po faktycznym uzyskaniu dostępu do treści domyślnym zachowaniem systemu dLibra jest przesłanie treści publikacji na komputer czytelnika. W tym momencie kopia cyfrowej publikacji opuszcza bibliotekę cyfrową i to co się z nią dalej dzieje zależy przede wszystkim od czytelnika.

Pliki z treścią prezentowane są przez przeglądarkę WWW zainstalowaną na komputerze czytelnika, opcjonalnie przy pomocy dodatkowego oprogramowania (np. pliki PDF przy pomocy Acrobat Reader, o ile czytelnik zainstalował takie oprogramowanie). Domyślnie system dLibra nie blokuje w żaden sposób możliwości zapisywania wyświetlonej publikacji na dysk czy drukowania jej. Jeżeli sam format publikacji umożliwia zablokowanie pewnych czynności, np. zablokowanie drukowania z plików PDF, to dLibra nie ingeruje w żaden sposób w te mechanizmy.

Wyjątkiem jest tutaj wsparcie dla publikacji DJVu i prostych publikacji HTML, które mogą być prezentowane w systemie dLibra jako tzw. publikacje zabezpieczone. Odczyt takiej publikacji realizowany jest w przeglądarce WWW czytelnika przy pomocy specjalnego apletu Javy. Aplet ten pobiera z serwera WWW biblioteki cyfrowej zaszyfrowaną publikację (szyfrowanie niezależne od ustawień protokołu HTTP serwerze WWW) i wyświetla ją czytelnikowi nie dając możliwości zapisania treści na dysk czy wydrukowania jej. Czytelnik nadal oczywiście może wykonać zrzut ekranu, czy np. zrobić zdjęcie aparatem fotograficznym.