



Mechanizmy dostępu do bazy danych Palladion / Ulisses

I. Uwierzytelnianie i przyznawanie uprawnień dostępu do aplikacji Palladion

1. Założenia podstawowe

a) mechanizm uwierzytelniania oparty o użytkowników SQL

b) uprawnienia do obiektów bazy danych (procedur, funkcji, tabel):

W bazie danych zdefiniowany zostanie 1 użytkownik Palladion dla wszystkich aplikacji o minimalnych uprawnieniach zestawiania połączenia z bazą danych "DBConnect" (bez uprawnień dostępu do obiektów bazy danych). Uprawnienia do obiektów nadawane będą dynamicznie po zestawieniu połączenia z bazą danych przez aplikację i zalogowaniu się do określonej roli aplikacji. Ilość ról aplikacji będzie zależna będzie od wymagań posiadania różnych uprawnień dla aplikacji (pkt 1.c.).

Wszystkie aplikacje będą autoryzowały się wspólnym użytkownikiem Palladion i własną rolą aplikacji.

Przyznawane uprawnienia ról aplikacji będą na poziomie uprawnień (Select, Insert, Update, Delete, Exec)

c) klasyfikacja aplikacji Palladion ze względu na zróżnicowane wymagania uprawnień dostępu do bazy danych:

Aplikacje terminala:

-Terminal Alarmowy

-Raporty Crystal Reports terminala alarmowego

-Terminal UPS

-Raporty Crystal Reports terminala UPS

-usługa UTAPI - obsługa rozmów telefonicznych (brak dostępu do bazy danych)

Aplikacje serwera:



- usługa UOW – obsługa komunikacji z urządzeniami
- usługa UP – przetwarzanie odebranych danych z urzędzeń
- usługa UT – obsługa stanowisk terminalowych
- usługa UZ – obsługa historii zdarzeń
- usługa UK – kontrola pracy monitorowanych obiektów
- usługa UAK – wymiana kluczy szyfrujących IPS
- usługa UAO – aktualizacja oprogramowania IPS

Aplikacje narzędziowe:

- dystrybutor kluczy szyfrujących

Serwis WWW:

- serwer IIS

2. Uwagi do proponowanych rozwiązań

a) Zakres zmian aplikacji Palladion

- wdrożenie obsługi odszyfrowania haseł bazy danych z rejestru
- obsługa ról aplikacji jest zaimplementowana w bieżącej wersji aplikacji Palladion z wyjątkiem Crystal Reports (które wspiera tylko role bazy danych)

b) Dostęp do danych

-dwa etapy:

- uwierzytelnianie użytkownika o uprawnieniach "DBConnect" na podstawie loginu i hasła użytkownika zaszyfrowanego w rejestrze
- logowanie do roli aplikacji na podstawie loginu zaszytego w aplikacji i hasła w rejestrze.



II. Szyfrowanie konfiguracji połączenia baz danych

1. Założenia podstawowe

System Palladion umożliwia szyfrowanie danych konfiguracyjnych wykorzystywanych do podłączenia bazy danych systemu. Do przechowywania kluczy kryptograficznych oraz szyfrowania i odszyfrowywania danych zostały wykorzystane wbudowane mechanizmy systemu operacyjnego MS Windows - „Windows Data Protection (DPAPI)”.

Główną cechą wykorzystanego mechanizmu jest możliwość zapewnienia poufności zaszyfrowanych danych. W tym celu wykorzystano dwuetapowy mechanizm szyfrowania danych. Pierwszy etap polega na uwierzytelnieniu do danych zaszyfrowanych z wykorzystaniem wbudowanych wewnętrznych kluczy kryptograficznych i odczytaniu hasła konfiguracyjnego, które dopiero w drugim etapie zostaje wykorzystane do odszyfrowania właściwych danych. Mechanizm ten zapewnia brak dostępu do zaszyfrowanych danych osobom które mimo posiadania odpowiedniego oprogramowania administracyjnego nie znają prawidłowego hasła dostępu.

Ważną cechą „Windows Data Protection” jest brak możliwości przeniesienia zaszyfrowanych danych pomiędzy komputerami. Mechanizmy szyfrowania wprowadzają także pojęcie *kontekstu zaszyfrowanych danych*. Dane mogą zostać zaszyfrowane w kontekście systemu operacyjnego (będą możliwe do odszyfrowania przez wszystkich użytkowników poprawnie zalogowanych do systemu operacyjnego) lub dane mogą zostać zaszyfrowane w kontekście użytkownika (tylko wybrany użytkownik systemu Windows może odszyfrować dane konfiguracyjne). Wymaga się aby dane konfiguracyjne na serwerach systemu były szyfrowane w kontekście systemu operacyjnego, kontekst szyfrowania na terminalach alarmowych może być dowodowy wedle wymagań użytkownika.

Dodatkowe informacje:

<http://msdn2.microsoft.com/en-us/library/ms995355.aspx>



Elementy konfiguracyjne ujęte w procesie szyfrowania danych:

- hasło dostępu do konfiguracji zaszyfrowanych danych
- parametry logowania do serwera podstawowego bazy danych (DSN1)
- parametry logowania do serwera zapasowego bazy danych (DSN2)
- parametry logowania do serwera archiwalnego bazy danych (DSNARCH)
- hasła roli aplikacji wszystkich usług Palladion, terminali Palladion oraz systemu Palladion WWW (DataBaseConnectAppPswrd)
- parametry połączenia narzędzia raportującego (ReportViewer)
 - nazwa źródła danych ODBC
 - nazwa bazy danych
 - nazwa użytkownika bazy danych
 - hasło użytkownika bazy danych

2. Algorytmy pracy

Algorytmy działania oprogramowania szyfrującego dane konfiguracyjne

1. Aplikacje Palladion

- aplikacja Palladion odczytuje z rejestru systemu Windows zaszyfrowane hasło dostępu do konfiguracji parametrów połączenia i odszyfrowuje je korzystając z wewnętrznych kluczy kryptograficznych (*pole DataBaseProtectionKey*)
- w przypadku poprawnego odszyfrowania hasła dostępu zostają odczytane parametry logowania do bazy danych z rejestru systemu Windows, a następnie odszyfrowane przy pomocy poprzednio odszyfrowanego hasła
- Odszyfrowane parametry logowania zostają wykorzystane do podłączenia do bazy danych

2. Oprogramowanie Administracyjne

1. Odczyt parametrów konfiguracyjnych

- oprogramowanie „DBConfigurator” odczytuje z rejestru systemu Windows zaszyfrowane hasło dostępu do konfiguracji parametrów połączenia i



odszyfrowuje je korzystając z wewnętrznych kluczy kryptograficznych
(pole *DataBaseProtectionKey*)

- aplikacja porównuje odszyfrowane hasło z hasłem podanym przez użytkownika
- w przypadku wprowadzenia poprawnego hasła ostają odczytane parametry logowania do bazy danych z rejestru systemu Windows, a następnie odszyfrowane przy pomocy poprzednio wprowadzonego hasła

2. Zapis parametrów konfiguracyjnych

- oprogramowanie konfiguracyjne „DBConfigurator” szyfruje parametry logowania do bazy danych przy pomocy odprowadzonego hasła dostępu a następnie zapisuje zaszyfrowane wartości do rejestru systemu Windows
- w przypadku zmiany hasła dostępu do konfiguracji lub zmiany kontekstu szyfrowanych danych oprogramowanie szyfruje hasło korzystając z wewnętrznych kluczy kryptograficznych a następnie zapisuje zaszyfrowane wartości do rejestru systemu Windows
(pole *DataBaseProtectionKey*)