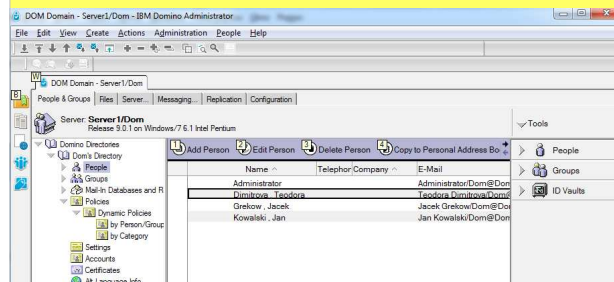


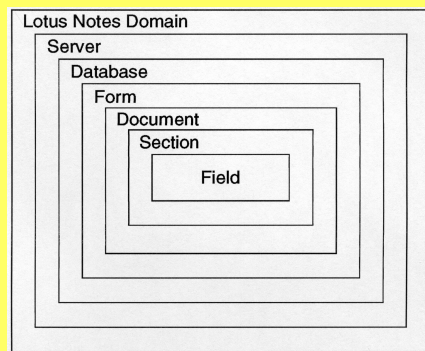
Elementy bezpieczeństwa w systemach pracy grupowej na przykładzie IBM Notes Domino

dr inż. Jacek Grekow
Politechnika Białostocka

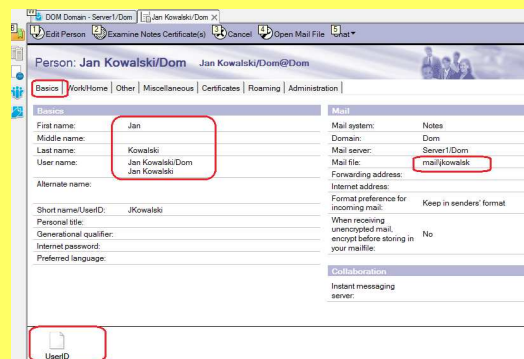
Użytkownicy



Poziomy



Dokument użytkownika w Publicznej Księżce Adresowej



Poziomy dostępu

- Dostęp do serwera
- Dostęp do bazy danych (Database Access Control)
- Form Access Control, View Access Control
- Document Access Control
- Ograniczenie dostępu do sekcji wewnątrz dokumentu
- Field Access Control

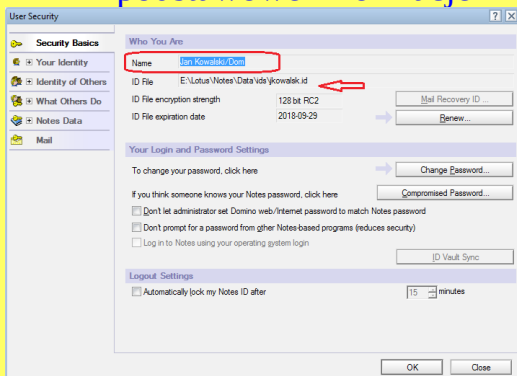
ID

- Bezpieczeństwo na poziomie systemu
- Plik: user.id
- Generowany przez administratora przy rejestracji użytkownika

ID zawiera

- Nazwę użytkownika
- Prywatny i publiczny klucz (wykorzystywany przy szyfrowaniu i podpisywaniu wiadomości)
- certyfikaty

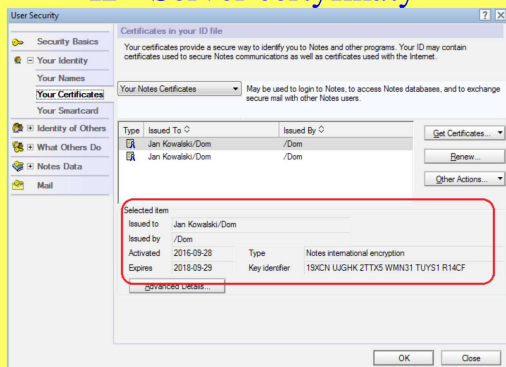
ID- podstawowe informacje



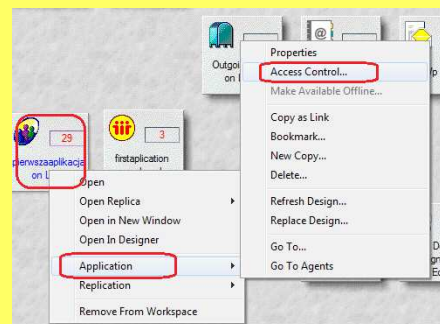
Dostęp do bazy danych ACL- Database Access Control

- Serce systemu bezpieczeństwa baz notesowych
- Określa kto i co może zrobić z danymi w bazach
- Kontroluje dostęp użytkowników, serwerów i grup do bazy danych

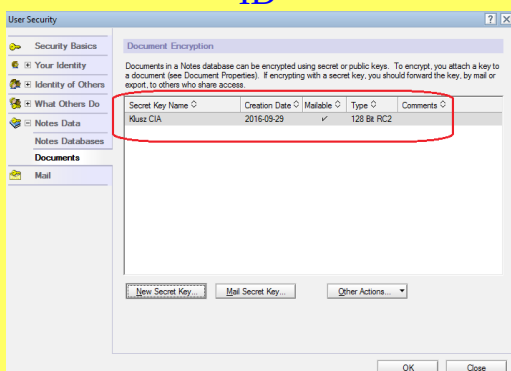
ID- Server certyfikaty



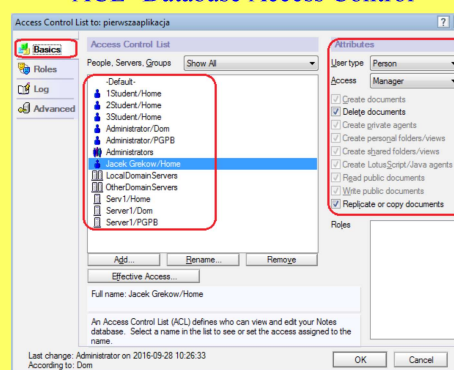
ACL- Database Access Control



ID



ACL- Database Access Control



ACL – poziomy dostępu

- Manager
- Designer
- Editor
- Author
- Reader
- Depositor
- No Access



ACL – poziomy dostępu Editor

- Może tworzyć i edytować wszystkie dokumenty
- Włącznie z dokumentami utworzonymi przez innych użytkowników

ACL – poziomy dostępu Manager

- Może modyfikować ACL
- Może kodować bazę lokalnie
- Może zmieniać ustawienia replikacji bazy
- Może skasować bazę
- Może wykonywać wszystkie zadania dozwolone na innych poziomach dostępu

Każda baza musi mieć co najmniej 1 Managera

ACL – poziomy dostępu Author

- Może tworzyć dokumenty i edytować te które stworzył
- Nie może edytować stworzonych przez innych użytkowników
- An **Authors field** works in conjunction with **Author access** in the database ACL. If you assign users Author access in the ACL, they can read documents in the database but **cannot edit their own documents**. If you **list** those users in an **Authors field**, they **can edit** documents in the database.

ACL – poziomy dostępu Designer

- Może modyfikować wszystkie elementy konstrukcyjne bazy (pola, formy, widoki, publiczni agenci)
- Może modyfikować formuły replikacji
- Może tworzyć indeks pełnotekstowy dla bazy (full-text index)
- Może wykonywać wszystkie zadania dozwolone na niższych poziomach dostępu

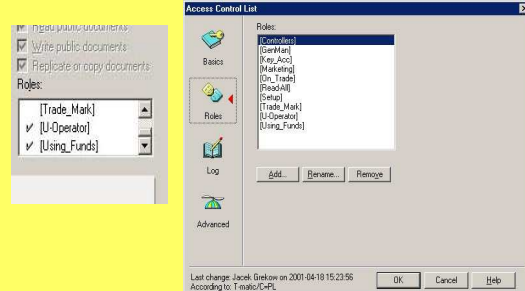
ACL – poziomy dostępu Reader

- Może czytać dokumenty
- nie może ich tworzyć lub edytować

ACL – poziomy dostępu Depositor

- Może tworzyć dokumenty
- Nie widzi dokumentów dokumentów

ACL- Role



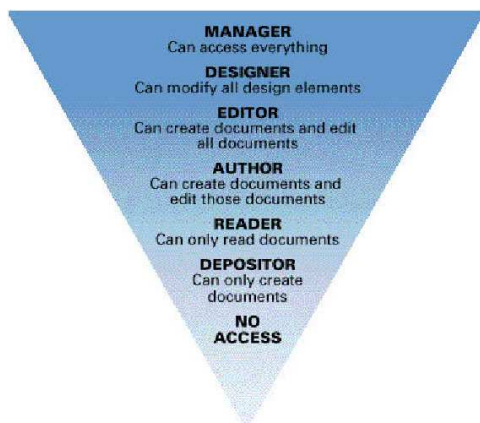
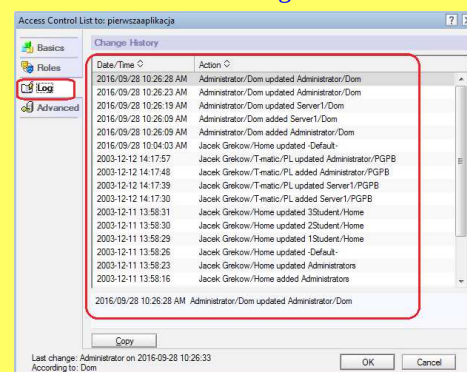
@UserRoles

@if (@IsMember (@UserRoles; "[Marketing]"); @True; @False)

ACL – poziomy dostępu No Access

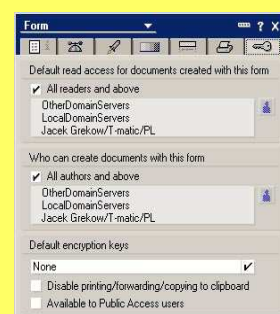
- Nie ma dostępu do bazy
- Używa się jako ustawienie domyślne dla innych użytkowników

ACL - log

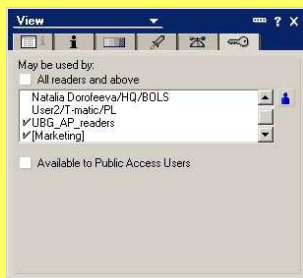


Form Access Control

- Określa kto może używać danej formy
- Zawęża użytkowników dopuszczonych przez ACL
- Może ograniczyć liczbę użytkowników którzy mogą czytać dokument za pomocą danej FORMY
- Może ograniczyć kto może utworzyć dany dokument za pomocą danej FORMY

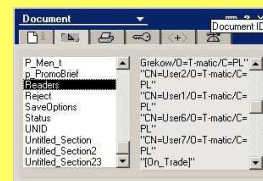


View Access Control



Document Access Control Reader fields

- Ustawiają restrakcje czytania danego dokumentu
- Zawierają listę nazw użytkowników którzy mogą czytać
- Mogą być edytowalne lub obliczane
- Dotyczy tylko osób, które mają prawo Reader w ACL bazy



Document Access Control

- Jeśli dokument już został stworzony właściciel dokumentu może określić prawa dostępu do danego dokumentu poprzez
- Stworzenie pól w formularzu typu **Reader** i **Author**
- Zawęza użytkowników dopuszczonych przez ACL

Document Access Control Author fields

- Osoby znajdujące się w tym polu mogą edytować dokumenty których nie stworzyli
- Dotyczy tylko osób, które mają prawo Author w ACL bazy
- Mogą być edytowalne lub obliczane

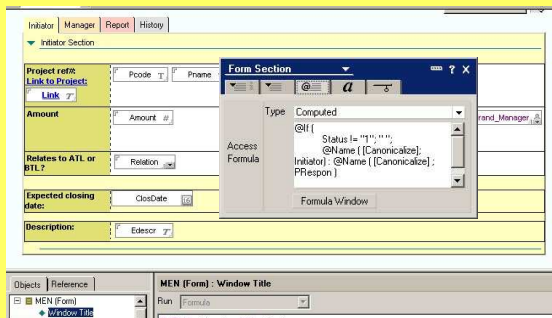
Document Access Control



Ograniczenie dostępu do **sekcji** wewnątrz dokumentu

1. **Standard Section**
 - Służy do zwiwania i rozwijania informacji
2. **Controlled Access Section**
 - Służy do zwiwania i rozwijania informacji
 - Kontroluje prawo edytowania obszaru sekcji

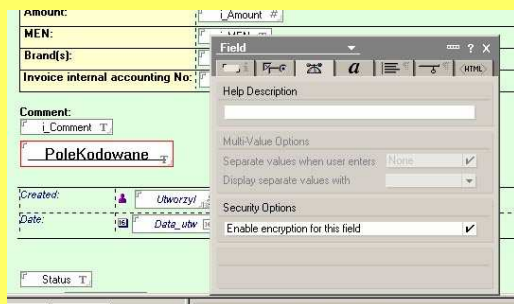
Ograniczenie dostępu do **sekcji** wewnątrz dokumentu



Pytania ?



Szyfrowanie zawartości pola



Poziomy bezpieczeństwa

