

Pizza & Beer: OpenEdge Authentication Gateway (Security Token Server)

**Spotkania techniczne dla partnerów aplikacyjnych
i klientów technologii Progress**

Agenda

Co to jest OpenEdge Authentication Gateway

Instalacja i konfiguracja OE Authentication Servera

Dodatkowe kroki

Proces logowania

Podsumowanie

Co to jest OpenEdge Authentication Gateway

OpenEdge Authentication Gateway - zestaw funkcji, które zapewniają zaufane zarządzanie tożsamością.

Właściwi użytkownicy uzyskują właściwy dostęp do właściwych informacji.

Co to jest OpenEdge Authentication Gateway

OpenEdge Authentication Server

Baza danych z włączoną funkcją wymuszonego korzystania z OpenEdge Authentication Server

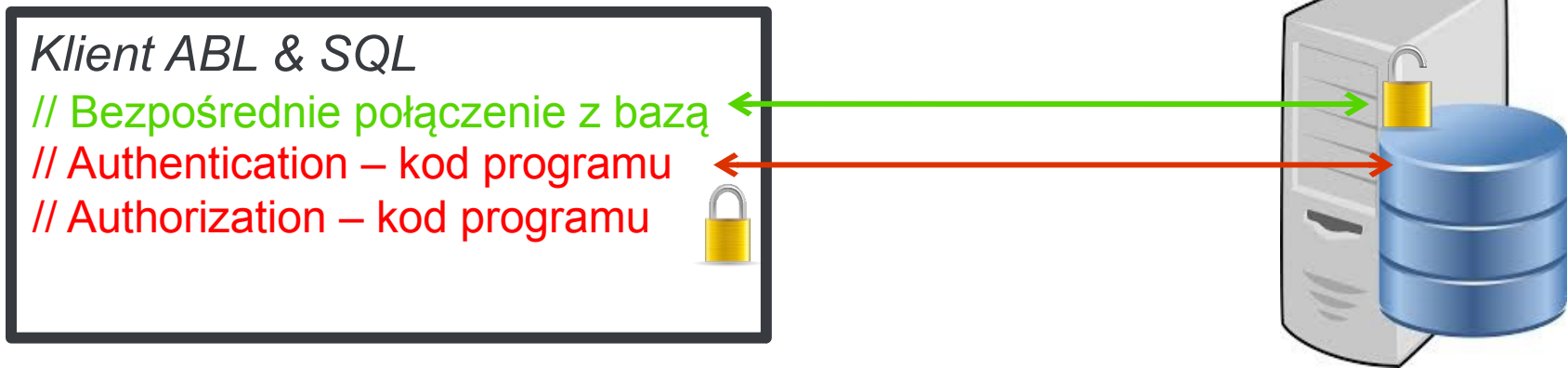
OpenEdge Client-Principal – tworzenie i weryfikacja

Client-Server – weryfikacja klucza

Narzędzia wspomagające konfigurację i debugowanie

Zabezpieczenie bazy przed OpenEdge Authentication Gateway

Zabezpieczenia w bazach obsługiwane przez klientów ABL i SQL



Instalacja i konfiguracja

ABL Clients



Application Server



OpenEdge Database



SQL Clients



OE Authentication Gateway Server



Instalacja i konfiguracja

Server OpenEdge Authentication Gateway jest aplikacją PASOE (oests.war)

- Można zarządzać nim i konfigurować jak każdą instancję PASOE
- Licencję OE Auth Gateway można uzyskać w przypadku zakupu licencji produkcyjnej PASOE

Instalacja

- Instalacja z bazą danych lub na oddzielnej maszynie

Start i weryfikacja czy OE Auth Gateway pracuje

- Test przy pomocy narzędzia **stsclientutil**

```
stsclientutil -url -nohostverify -cmd ping
```

```
stsclientutil -url -nohostverify -cmd authenticate -  
user test -password test
```

Połączenie się z serwisem uwierzytelniania innej firmy

ABL Clients



Application Server



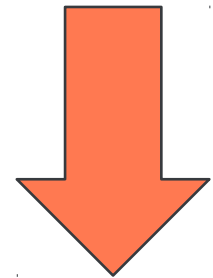
SQL Clients



OpenEdge Database



OE Authentication Gateway Server



Połączenie się z serwisem uwierzytelniania innej firmy

Konfiguracja

- LDAP
- Active Directory
- System operacyjny
- Plik użytkownika (domyślna konfiguracja do szybkiej walidacji)

W jaki sposób?

- Konfiguracja `sts.properties`
- Konfiguracja domeny w `domains.json`
- Utworzenie zaszyfrowanego magazynu kluczy (keystore) z kodem dostępu do domeny

Konfiguracja – domains.json

```
{
  "version": "1.0.0",
  "domains": [
    {
      "name": "local",
      "enabled": true,
      "description": "Domain supporting OS local logins",
      "actions": {
        "authenticate": {
          "enabled": true,
          "options": ""
        },
        "exchange": {
          "enabled": true,
          "options": "-processid"
        },
        "sso": {
          "enabled": false,
          "options": ""
        },
        "refresh": {
          "enabled": false,
          "options": ""
        }
      }
    },
    {
      "options": "",
      "authProvider": "_oslocal",
    }
  ]
}
```

Konfiguracja bazy dla serwera OpenEdge Authentication Gateway

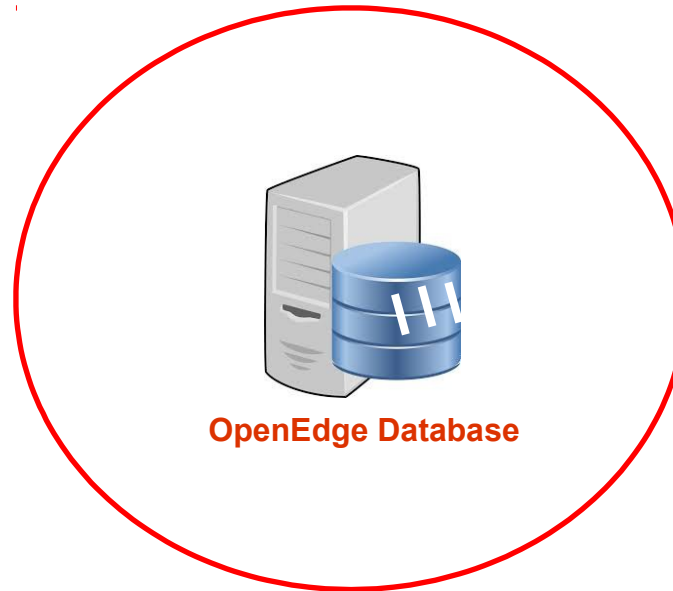
ABL Clients



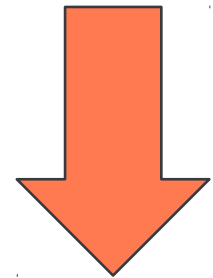
Application Server



SQL Clients



OE Authentication Gateway Server



Konfiguracja bazy danych OpenEdge

Test połączenia z maszyny z bazą danych do OpenEdge Authentication Servera

```
stsclientutil -url https://hostname:port -nohostverify -cmd ping
```

```
stsclientutil -url https://hostname:port -nohostverify -cmd  
authenticate -user user@domain -password password
```

Dodanie domeny bezpieczeństwa

- Dodać co najmniej 2 administratorów w domenie
- Jeden z nich odpowiada LDAP, Active Directory lub Sys. Op.

Dodanie domen, które odpowiadają domenom w domians.json OpenEdge Authentication Servera

Konfiguracja bazy danych OpenEdge c.d.

Dodanie do bazy URL OpenEdge Authentication Serwera

```
stsclientutil update -url https://hostname:port -ssl -nohostverify  
-db database -db-parameters
```

Włączenie w bazie funkcji korzystania z OpenEdge Authentication Serwera

```
proutil dbname -C enableauthgateway
```

Start serwera bazy

```
proserve dbname -nohostverify -S -H
```

Test czy można zalogować się do bazy

```
mpro dbname -U user@domain -P password
```

Dodatkowe kroki

Utworzenie klucza serwera oraz instalacja kluczy klientów

ABL Clients



Application Server



OpenEdge Database



SQL Clients



OE Authentication Gateway Server



HTTPS



Więcej funkcji zabezpieczeń

Utworzenie certyfikatu web serwera z poprawną nazwą hosta

- Teraz można przestać używać **-nohostverify**

Utworzenie zestawu kluczy klient-serwer dla OpenEdge Authentication Servera

Klucz serwera

```
stskeyutil create -url https://hostname:port
```

- - wprowadzić hasło
 - wprowadzić kod dostępu
- Modyfikacja **sts.properties**
 - aktywować klucz serwera
 - ustawić ścieżkę i nazwę pliku
 - wprowadzić kod dostępu
- Zrestartować OpenEdge Authentication Server

Więcej funkcji zabezpieczeń c.d.

Instalacja klucza klienta na maszynie z bazą danych

- Skopiować klucz serwera na maszynę z bazą danych
- Zainstalować klucz klienta z klucza serwera

```
stskeyutil install -url https://hostname:port -file serverkeyname
```

- wprowadzić hasło

Test OpenEdge Authentication Servera przy pomocy stscientutil

Skasować klucz serwera z maszyny klienta/bazy danych

Skopiować nowy certyfikat web na maszynę z bazą danych

Zrestartować bazę danych

Wykonać powyższe czynności, aby dodać klucz klienta do wszystkich instalacji klienta

Ograniczenie dostępu do bazy poprzez uprawnienia połączeń (*connection roles*)

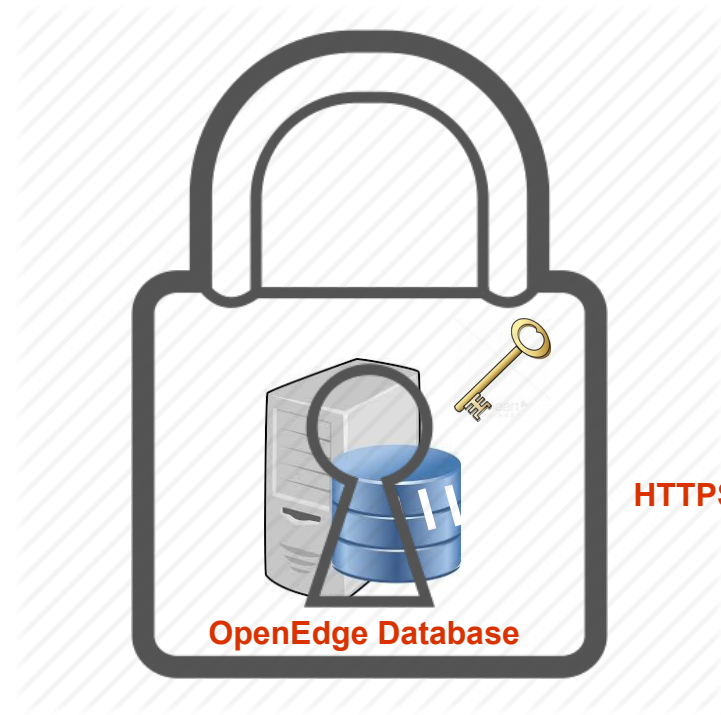
ABL Clients



Application Server



SQL Clients



OE Authentication Gateway Server



Ograniczenie dostępu do bazy poprzez uprawnienia połączeń (*connection roles*)

Dodanie autoryzacji dla połączeń do bazy

Włączenie autoryzacji

```
stsconnroleutil enable -db dbname -U user@domain -P password
```

- Teraz tylko user@domain może połączyć się z bazą danych

Dodanie następnego użytkownika

```
stsconnroleutil grantuser -grantee anotheruser@domain -db dbname -U user@domain -P password
```

Dodanie listy użytkowników

```
stsconnroleutil grantfile -file addusers.list -db dbname
```

Zasady i zdarzenia

Zasady (Domain policy)

- Konfiguracja w domains.json
- Jedna domena – jedna *domain policy*
- Klasa ABL

Zdarzenia (Event callback policy)

- Konfiguracja w domains.json
- Klasa ABL

Konfiguracja – *domain policy*

```
"version": "1.0.0",
"domains": [
  {
    "name" : "local",
    "enabled" : true,
    "description" : "O/S Authentication",
    "actions" : {
      "authenticate" : {
        "enabled" : true,
        "options" : ""
      }
    }
  },
  {
    "options" : "-processid",
    "authProvider" : "_oslocal",
    "policyProvider" : "login",
    "events" : {
      "provider" : "",
      "groups" : {}
    }
  }
],
...
"policyProviders" : {
  "login" : {
    "type" : "com.progress.sts.SampleLoginPolicy",
    "hash" : ""
  }
},
...
```

Konfiguracja – *domain policy c.d.*

```
// SampleLoginPolicy.cls
```

```
using Progress.Lang.*.  
using OpenEdge.Security.STS.IPolicyProvider.  
using OpenEdge.Security.Principal.  
using Progress.Json.ObjectModel.JsonObject.  
using OpenEdge.Security.PAMStatusEnum.block-level on error undo, throw.  
class com.progress.sts.SampleLoginPolicy implements IPolicyProvider:  
    method public PAMStatusEnum ApplyPolicy( input pcSender as character,  
        input pcPolicy as character,  
        input phClientPrincipal as Principal,  
        input pcDomainCtx as JsonObject,  
        output pcStatusDetail as character ):  
message "sender:" pcSender skip  
    "policy:" pcPolicy skip  
    "C-P Token" phClientPrincipal:Token skip  
    "context:" pcDomainCtx.  
pcStatusDetail = "OK".  
return PAMStatusEnum:Success.  
end method.  
end class.
```

Konfiguracja – *event callback*

```
"version": "1.0.0",
"domains": [
  {
    "name" : "local",
    "enabled" : true,
    "description" : "O/S Authentication",
    "actions" : {
      "authenticate" : {
        "enabled" : true,
        "options" : ""
      }
    }
  },
  "options" : "-processid",
  "authProvider" : "_oslocal",
  "policyProvider" : "",
  "events" : {
    "provider" : "login",
    "groups" : {
      "tokenAuthenticate" : true,
      "tokenExchange" : true
    }
  }
},
...
"eventProviders" : {
  "local" : {
    "type" : "com.progress.sts.SampleEventHandler",
    "hash" : ""
  }
}
```

Konfiguracja – *event callback*

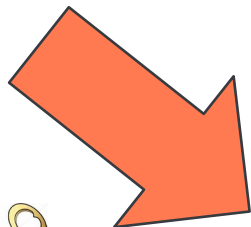
// SampleEventHandler.cls

```
using Progress.Lang.*.
using OpenEdge.Security.STS.IEventProvider.
using OpenEdge.Security.Principal.
using Progress.Json.ObjectModel.JsonObject.
block-level on error undo, throw.
class com.progress.sts.SampleEventHandler implements IEventProvider:
    method public void RecordEvent( input pcSender as character,
                                    input pcEvent as character,
                                    input poPrincipal as Principal,
                                    input poDomainCtx as JsonObject ):
        message "sender:" pcSender skip
        "event:" pcEvent skip
        "C-P Token" poPrincipal:Token skip
        "context:" poDomainCtx.
    end method.
end class.
```

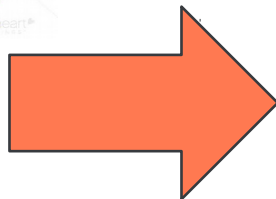

Proces logowania

Proces logowania

ABL Clients



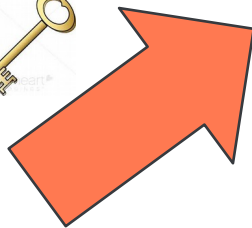
Application Server



OpenEdge Database

HTTPS

SQL Clients

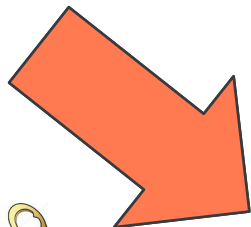


OE Authentication Gateway Server

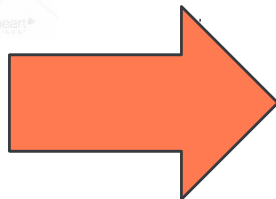


Proces logowania

ABL Clients



Application Server



OpenEdge Database

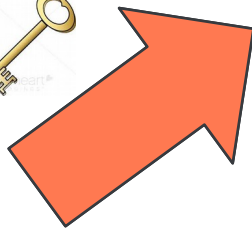


HTTPS

OE Authentication Gateway Server

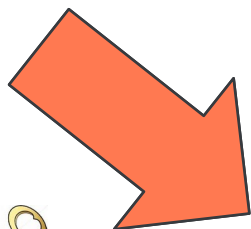


SQL Clients

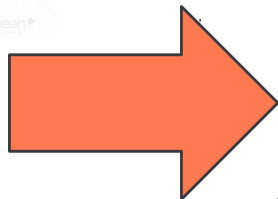


Proces logowania

ABL Clients



Application Server

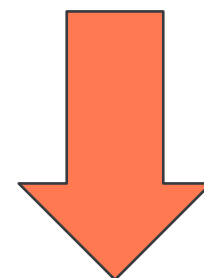


OpenEdge Database



HTTPS

OE Authentication Gateway Server

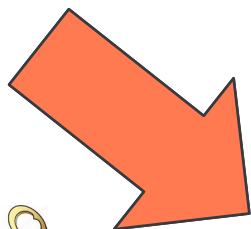


SQL Clients

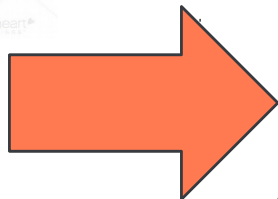


Proces logowania

ABL Clients



Application Server

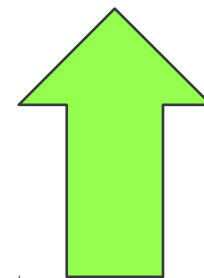


OpenEdge Database

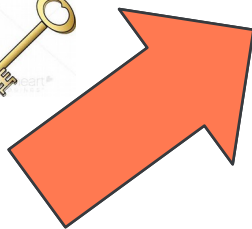


HTTPS

OE Authentication Gateway Server

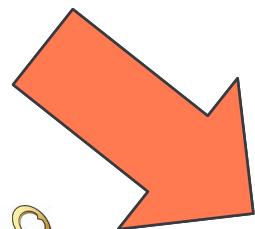


SQL Clients

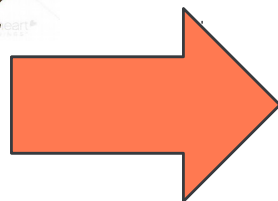


Proces logowania

ABL Clients



Application Server

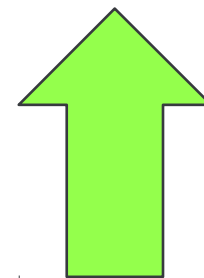


OpenEdge Database

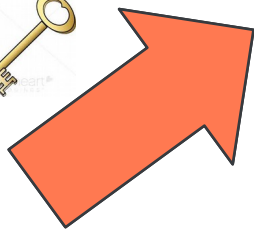


HTTPS

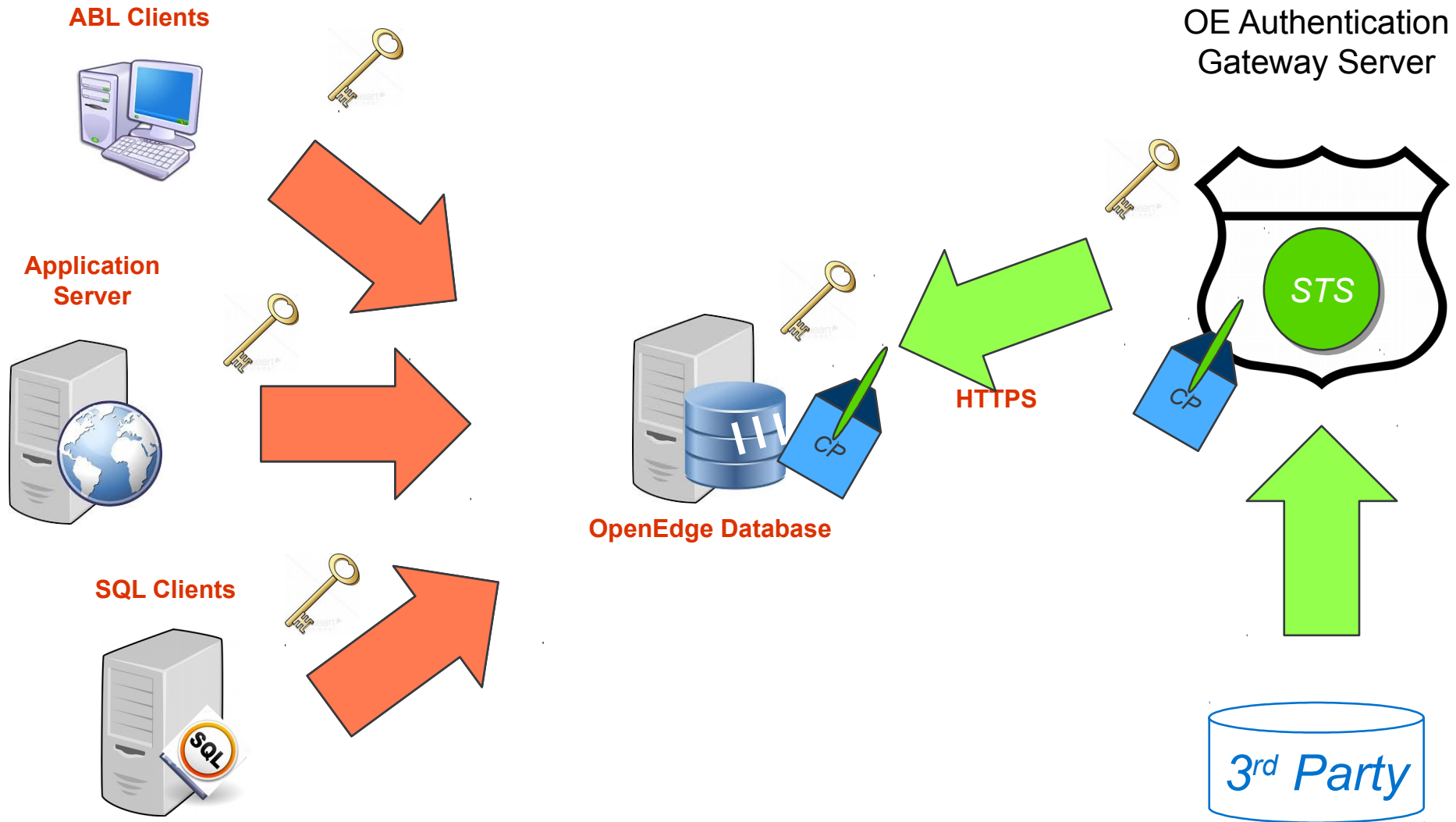
OE Authentication Gateway Server



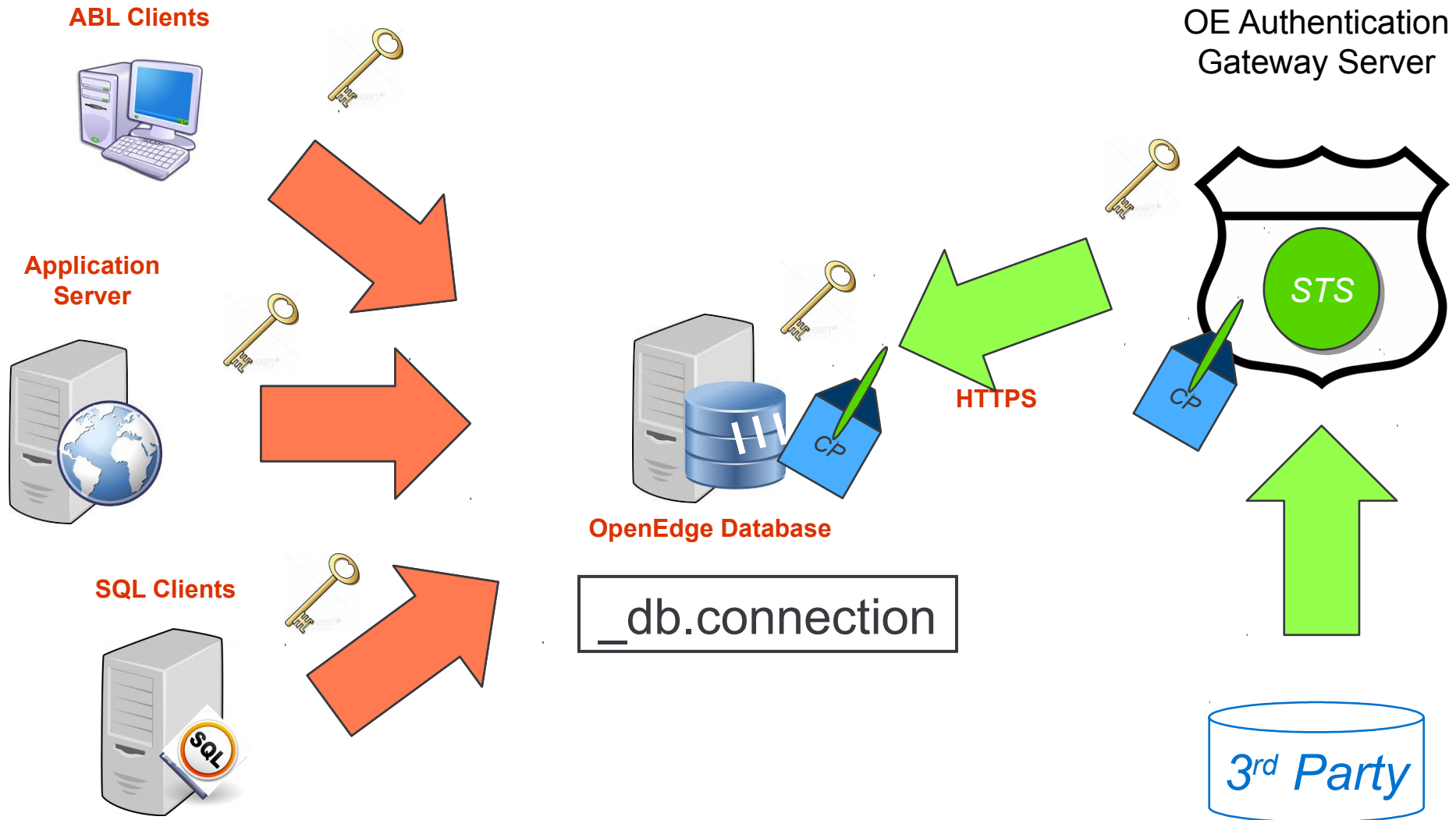
SQL Clients



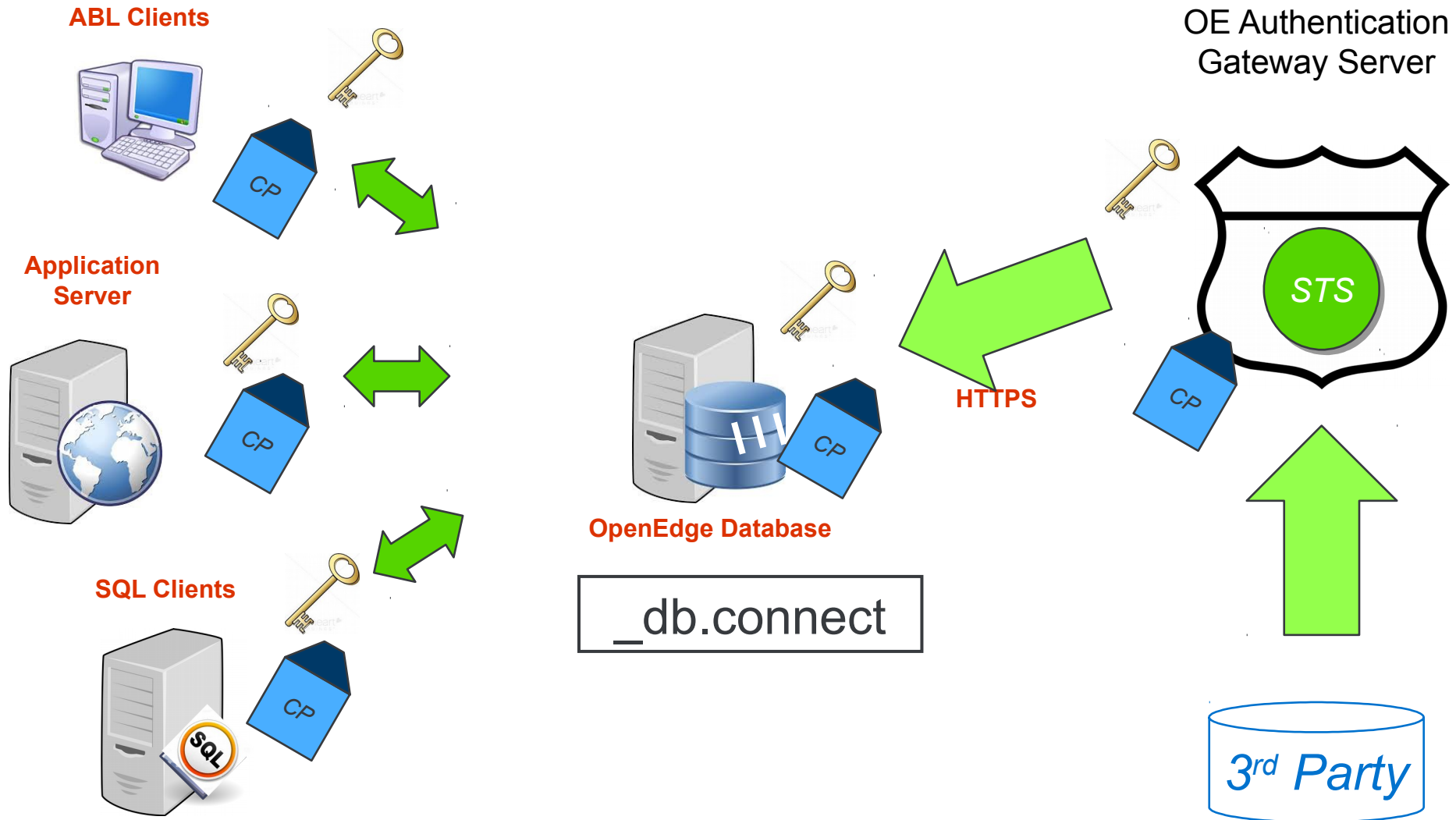
Proces logowania



Proces logowania



Proces logowania



Podsumowanie

Umożliwia korzystanie ze standardowych produktów uwierzytelniających

- Rozdzielenie obowiązków

 - Ktoś inny obsługuje użytkowników i hasła

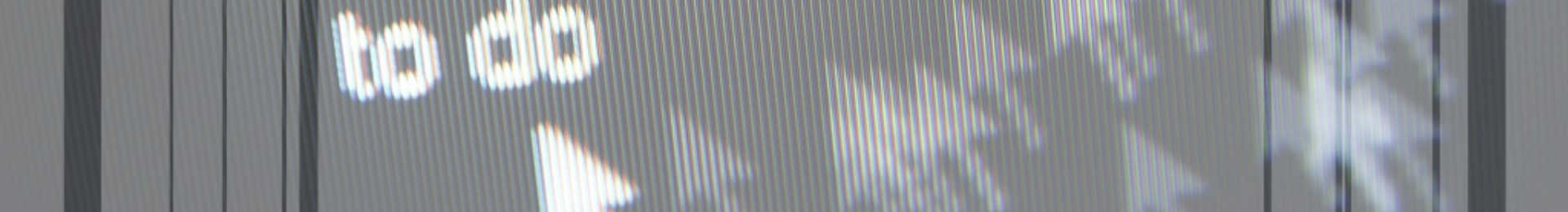

- Do nich należy zabezpieczanie użytkowników i haseł

Tworzenie i walidacja klientów (client principals) jest poza ABL

Administratorzy baz mogą zarządzać autoryzacją użytkowników

Szczegółowa autoryzacja

Nigdy więcej nie będziesz musiał napisać własnego kodu do uwierzytelniania!



to do

Dziękuję za uwagę

