KDPW

Dział Eksploatacji Systemów Informatycznych

Elektroniczny System Dystrybucji Komunikatów

Spis treści

1 Historia Zmian 3
2 Informacje ogólne 4
3 Architektura systemu 4
3.1 Serwer ESDK 5
3.2 Klient ESDK 6
4 Protokół komunikacyjny ESDK 7
4.1 Format komunikatu ESDK 7
4.2 Typy komunikatów ESDK 9
4.3 Sposób obsługi poszczególnych typów komunikatów przez system ESDK 11
5 Infrastruktura telekomunikacyjna systemu ESDK 13
5.1 Frame Relay 14
5.2 Internet 14
6 Bezpieczeństwo 15
6.1 Bezpieczeństwo transmisji danych 15
6.2 Podpis elektroniczny 15
7 Współpraca Klienta ESDK z Serwerem ESDK 17
7.1 Wariant I (klient – serwer) 17
7.2 Wariant II (serwer – serwer) 18
7.3 Mechanizmy uwierzytelniania użytkowników do systemu ESDK 19
7.4 Oprogramowanie klienta ESDK 20

1 Historia Zmian

Data	Opis zmiany
09.12.2008	Utworzenie dokumentu
01.10.2009	Zmiana z sposobie numeracji komunikatów (str. 9)
28.06.2018	Uaktualnienie opisu klienta ESDK, uaktualnienie nazewnictwa produktów IBM oraz obiektów IBM MQ

2 Informacje ogólne

Elektroniczny System Dystrybucji Komunikatów (ESDK) jest systemem komunikacji elektronicznej pomiędzy KDPW S.A. a Uczestnikami Krajowego Depozytu, dedykowanym do obsługi komunikacji zautomatyzowanej (system to system) w Nowym Systemie Depozytowo-Rozliczeniowym (NSDR). Został zaprojektowany do wymiany komunikatów pomiędzy KDPW S.A. a Uczestnikami w czasie rzeczywistym, z zastosowaniem środków technicznych umożliwiających zachowanie poufności i integralności przesyłanych informacji oraz zapewnienie niezaprzeczalności nadawcy. Mechanizmy bezpieczeństwa zastosowane w ESDK bazują na uznanych standardach kryptograficznego zabezpieczenia transmisji danych oraz wykorzystaniu podpisu elektronicznego.

Zadania realizowane za pośrednictwem systemu ESDK:

- wymiana dokumentów rozliczeniowych,
- wymiana dokumentów w ramach obsługi świadczeń z papierów wartościowych.

3 Architektura systemu

ESDK działa na zasadzie wymiany standaryzowanych komunikatów, w oparciu o mechanizmy kolejkowe dostarczane przez oprogramowanie IBM MQ Server. KDPW udostępnia zainteresowanym Uczestnikom zestaw dokumentacji, niezbędny do zrealizowania w pełni zautomatyzowanego procesu wymiany komunikatów.
Część komunikacyjna rozwiązania została zrealizowana w oparciu o oprogramowanie IBM MQ.

System realizuje następujące założenia:

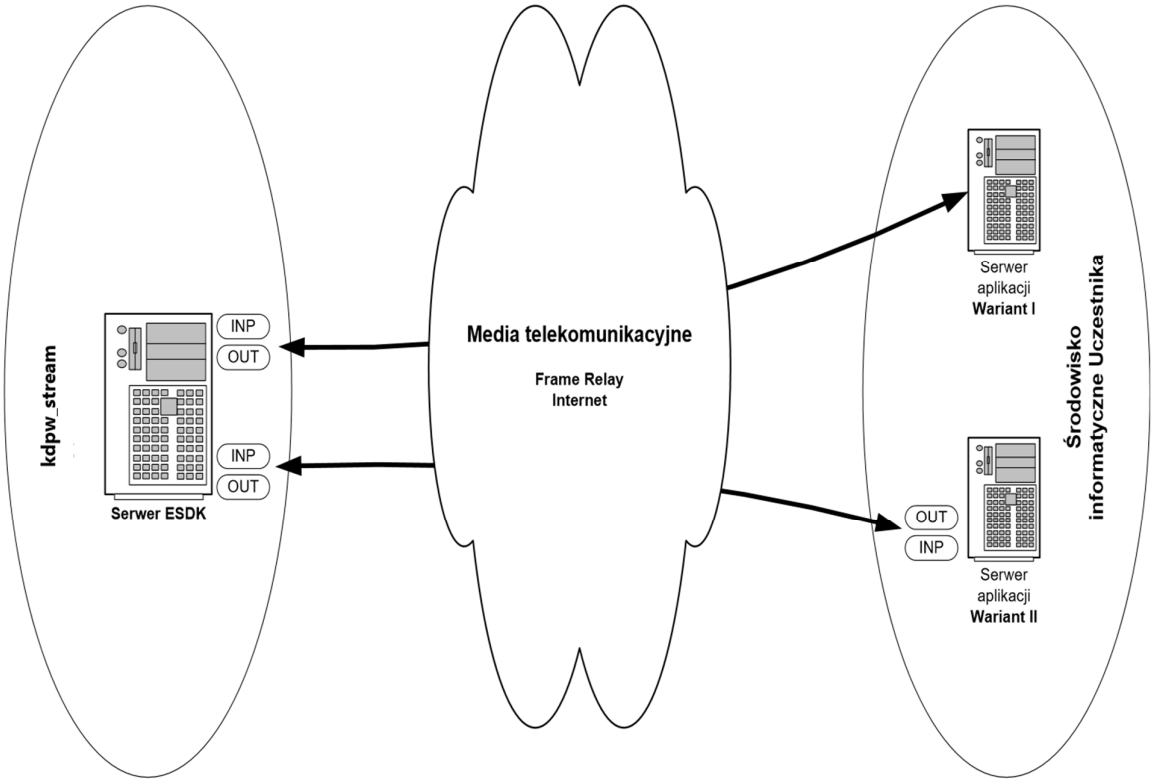
- komunikaty wymieniane za pomocą ESDK są podpisane elektronicznie - do dalszego przetwarzania w ramach systemu kdpw_stream przyjmowane są tylko komunikaty, których podpis został pozytywnie zweryfikowany,
- wymiana podpisanych komunikatów odbywa się poprzez szyfrowany kanał VPN,
- transmisja komunikatów jest dwukierunkowa,
- komunikaty są dystrybuowane do kolejek Uczestników natychmiast po ich

wygenerowaniu przez kdpw_stream,

- archiwizowane i przechowywane są kopie komunikatów wysłanych i odebranych, zgodnie z polityką przyjętą dla dokumentów rozliczeniowych.

W skład systemu ESDK wchodzą:

- Serwer ESDK,
- Klient ESDK.



Rysunek nr 1. Ogólny schemat ESDK.

3.1 **Serwer ESDK**

Serwer ESDK jest oprogramowaniem zbudowanym w oparciu o IBM MQ Server, realizującym następujące funkcje:

- odbiór komunikatów generowanych przez NSDR,
- podpisywanie komunikatów,
- umieszczenie komunikatu w kolejce wejściowej właściwego Uczestnika,

- odbiór komunikatów z kolejki wyjściowej Uczestnika,
- weryfikacja podpisu w odbieranych komunikatach,
- przekazywanie przesłanych przez Uczestników komunikatów do NSDR,
- składowanie kopii komunikatów wysłanych i odebranych na systemie plików
- utrzymywanie indeksu zeskładowanych komunikatów w bazie danych,
- autoryzację Uczestnika do właściwych kolejek MQ.

3.2 **Klient ESDK**

Klient ESDK jest to oprogramowanie funkcjonujące w ramach systemu informatycznego Uczestnika, umożliwiające wymianę komunikatów z Serwerem ESDK. Oprogramowanie to musi realizować następujące funkcje:

- komunikację z Serwerem ESDK, wykorzystującą oprogramowanie IBM MQ
- (w wersji Client lub Server),
- wysyłanie i odbieranie komunikatów zgodnie z Protokołem Komunikacyjnym ESDK,
- podpisywanie komunikatów wysyłanych,
- weryfikowanie podpisu elektronicznego komunikatów odbieranych.

KDPW nie dostarcza Uczestnikom oprogramowania Klienta ESDK. Uczestnicy są zobowiązani do zbudowania klienta ESDK we własnym zakresie.

KDPW w trybie budowania połączenia z Uczestnikiem przekazuje parametry techniczne niezbędne do skonfigurowania środowiska oprogramowania MQ:

- adresy IP i porty TCP wykorzystywane w procesie komunikacji,
- nazewnictwo i parametry kanałów MQ,
- nazewnictwo i parametry kolejek MQ.

4 Protokół komunikacyjny ESDK

Protokół komunikacyjny ESDK definiuje następujące parametry:

- format komunikatu ESDK,
- typy komunikatów ESDK,
- tryb obsługi poszczególnych typów komunikatów przez system ESDK.

4.1 Format komunikatu ESDK

Nazwa pola	Długość	Typ
Numer komunikatu	9	N
Data	10	A
Godzina	8	A
ID Adresata	10	A
ID Nadawcy	10	A
Typ komunikatu	24	A
Podtyp komunikatu	4	A
Obszar zarezerwowany	20	A
Długość danych	8	N
Dane	Długość danych	B
Długość podpisu elektronicznego	8	N
Podpis elektroniczny	Długość podpisu elektronicznego	B

Typy pól:

A – znakowe

B - binarne

N – numeryczne

Każdy komunikat jest jednoznacznie identyfikowany na podstawie pól:

- Numer komunikatu,
- Data,
- ID Nadawcy.

Numer Komunikatu: numer kolejny komunikatu nadawcy, identyfikowanego za pomocą ID Nadawcy. Numer kolejny jest unikalny (dla danego nadawcy) w ciągu dnia oraz ciągły począwszy od 1 do n,

Data: data wygenerowania przez NSDR komunikatu w formacie YYYY-MM-DD,

Godzina: godzina wygenerowania przez NSDR komunikatu w formacie HH:MM:SS,

ID Adresata: identyfikator adresata, w formacie SDK.TTTTNN,

gdzie:

TTTT kod uczestnika,

NN numer kolejny identyfikatora dla danego uczestnika.

ID Nadawcy: identyfikator nadawcy, w formacie SDK.TTTTNN,

gdzie:

TTTT kod uczestnika,

NN numer kolejny identyfikatora dla danego uczestnika.

Typ komunikatu: określa typ komunikatu (wyrównany spacjami do prawej strony),

Podtyp komunikatu: określa podtyp komunikatu. Domyślną wartością tego pola jest '0000'. W komunikatach merytorycznych pierwszy znak pola może otrzymywać wartości:

- '**T**' - dla komunikatów przekazywanych w formacie stałopolowym,
- '**X**' - dla komunikatów przekazywanych w formacie XML,
- '**0**' - jeżeli nie określono formatu komunikatu.

Obszar zarezerwowany: obszar, który w przyszłości może zostać wykorzystany do umieszczenia dodatkowych danych w nagłówku,

Długość danych: długość pola **Dane**.

Dane: dane, które są przesyłane za pomocą komunikatu,

Długość podpisu elektronicznego: długość pola **Podpis elektroniczny,**

Podpis elektroniczny: podpis elektroniczny bufora danych, składającego się z pól:

- **Numer Komunikatu,**
- **Data, Godzina,**
- **ID Adresata,**
- **ID Nadawcy,**
- **Typ komunikatu,**

- **Podtyp komunikatu,**
- **Obszar zarezerwowany,**
- **Długość danych,**
- **Dane**.

Podpis elektroniczny generowany jest w standardzie PKCS#7, przy wykorzystaniu certyfikatów elektronicznych wystawianych przez Urząd Certyfikacji KDPW.

4.2 Typy komunikatów ESDK

Pole **Typ komunikatu** może przyjmować poniższe wartości:

- **esdk.acc.001.01** potwierdzenie przyjęcia komunikatu,
- **esdk.rjc.001.01** informacja o odrzuceniu komunikatu,
- **esdk.tst.001.01** komunikat weryfikujący,
- nazwa typu komunikatu merytorycznego, generowanego przez NSDR i/lub Uczestnika.

Komunikaty, których pierwsze 4 znaki mają wartość „**esdk**", w dalszej części opracowania nazywane będą komunikatami technicznymi. Pole **Dane** w komunikatach technicznych (z wyjątkiem komunikatu **esdk.tst.001.01**) ma ściśle określony format.

Struktura pola **Dane** w komunikacie typu **esdk.acc.001.01:**

Nazwa pola	**Długość**	**Typ**
Numer komunikatu	9	N
Data	10	A
ID Nadawcy	10	A
Data akceptacji	10	A
Godzina akceptacji	8	A

Ww. struktura identyfikuje komunikat, który został przyjęty przez system ESDK oraz informuje o dacie i godzinie przyjęcia komunikatu przez system ESDK.

Struktura pola **Dane** w komunikacie typu **esdk.rjc.001.01**:

Nazwa pola	**Długość**	**Typ**
Numer komunikatu	9	N
Data	10	A
ID Nadawcy	10	A
Data odrzucenia	10	A
Godzina odrzucenia	8	A
Kod błędu	10	A
Opis błędu	256	A

Pola ***Numer komunikatu***, ***Data***, ***ID Nadawcy*** identyfikują komunikat, który został odrzucony przez system ESDK.

Pola ***Data odrzucenia*** **i** ***Godzina odrzucenia*** informują o dacie i godzinie odrzucenia komunikatu przez system ESDK.

Pola ***Kod błędu*** **i** ***Opis błędu*** opisują powód, z którego komunikat został odrzucony.

Pole **Dane** w komunikacie typu **esdk.tst.001.01** może zawierać dowolny ciąg znaków.

4.3 Sposób obsługi poszczególnych typów komunikatów przez system ESDK

Wszystkie komunikaty odbierane przez system ESDK są weryfikowane, w celu:

- sprawdzenia poprawności struktury komunikatu (zgodności z formatem określonym w pkt. 3.1),
- sprawdzenia unikalności identyfikatora komunikatu (patrz pkt 3.1),
- sprawdzenia integralności i autentyczności komunikatu (weryfikacja podpisu elektronicznego),
- sprawdzenia, czy nadawca ma prawo używać certyfikatu, którym podpisał komunikat,
- dokonania kontroli charakterystycznych dla danego typu komunikatu.

W wyniku zakończenia procedury weryfikacji komunikat zostaje przyjęty lub odrzucony. Informacje o wszystkich odebranych i wysłanych komunikatach zapisywane są w rejestrze komunikatów.
Dla klienta ESDK obsługa komunikatów technicznych nie jest obowiązkowa.

Moduł ESDK/400 obsługuje komunikaty techniczne wg. poniższych reguł:

Komunikaty esdk.acc.001.01:

- jeżeli komunikat **esdk.acc.001.01** zostanie przyjęty, nie jest wykonywana żadna dodatkowa akcja,
- jeżeli komunikat **esdk.acc.001.01** zostanie odrzucony, system ESDK wysyła informację o komunikacie i wyniku jego weryfikacji do administratora systemu ESDK.

Komunikaty esdk.rjc.001.01:

Po otrzymaniu komunikatu **esdk.rjc.001.01** system ESDK wysyła informację o komunikacie i wyniku jego weryfikacji do administratora systemu ESDK. W razie wystąpienia takiej sytuacji niezbędna jest interwencja administratora systemu ESDK.

Komunikaty esdk.tst.001.01:

- jeżeli komunikat **esdk.tst.001.01** zostanie przyjęty, system ESDK odsyła do nadawcy komunikat **esdk.acc.001.01,**

- jeżeli komunikat **esdk.tst.001.01** zostanie odrzucony, system ESDK odsyła do nadawcy komunikat **esdk.rjc.001.01** informujący o odrzuceniu i jego przyczynie.

Komunikaty merytoryczne:

- jeżeli komunikat merytoryczny zostanie przyjęty, system ESDK odsyła do nadawcy komunikat **esdk.acc.001.01**, a komunikat merytoryczny jest przekazany do systemu NSDR,
- jeżeli komunikat merytoryczny zostanie odrzucony, system ESDK odsyła do nadawcy komunikat **esdk.rjc.001.01** informujący o odrzuceniu i jego przyczynie.

5 Infrastruktura telekomunikacyjna systemu ESDK

System ESDK korzysta z następujących mediów teletransmisyjnych:

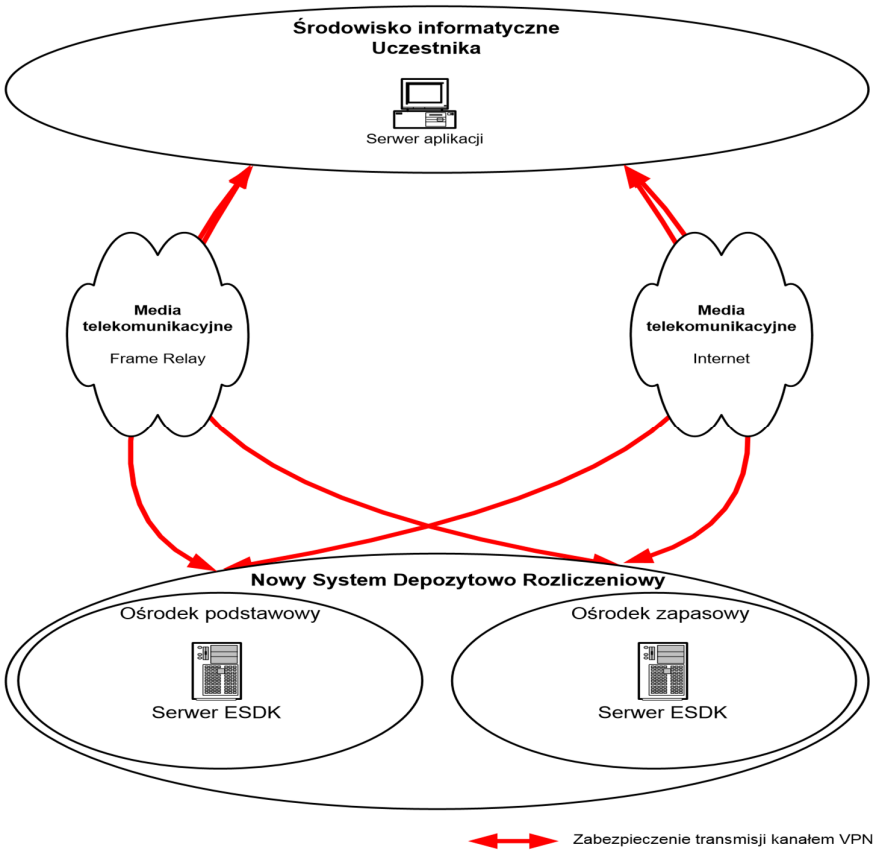
w lokalizacji podstawowej:

- Frame Relay/ATM w sieci Polpak T (TP S.A.),
- Frame Relay w sieci Exatel,
- sieć Internet;

w lokalizacji zapasowej:

- Frame Relay/ATM w sieci Polpak T (TP S.A.),
- sieć Internet.

Użytkownicy ESDK są zobowiązani do posiadania połączenia podstawowego (do lokalizacji podstawowej) oraz rezerwowego (do lokalizacji zapasowej).



Rysunek nr 2. Schemat telekomunikacji systemu ESDK.

5.1 Frame Relay

Dostęp Uczestnika do systemu ESDK jest możliwy między innymi przy użyciu protokołu telekomunikacyjnego Frame Relay. Dopuszcza się wykorzystanie jednego, wspólnego kanału PVC do wymiany danych z systemem ESDK oraz ESDI. Zalecana minimalna wartość parametru CIR dla jednego kanału PVC wynosi 32 kb/s.
KDPW umożliwia wymianę danych za pomocą technologii Frame Relay w ramach sieci:

- Polpak-T (ośrodek podstawowy i zapasowy),
- Exatel (tylko ośrodek podstawowy).

Ze względu na wysoką niezawodność oraz gwarancję pasma, Frame Relay jest preferowaną technologią przy wymianie danych z KDPW.

5.2 Internet

Dostęp KDPW do sieci Internet zrealizowany jest w oparciu o protokół BGP, przy wykorzystaniu łącz teletransmisyjnych podłączonych do dwóch niezależnych operatorów telekomunikacyjnych. Rozwiązanie takie zapewnia wysoki poziom odporności na awarie występujące w sieci.
Należy mieć na uwadze, że dostęp za pomocą sieci Internet nie zapewnia określonej przepustowości ani czasu odpowiedzi. Techniczne parametry połączenia takie jak: dostępne pasmo, chwilowa przepustowość, czy też bezawaryjność dostępu do sieci, zależne są od jakości usługi oferowanej przez danego operatora telekomunikacyjnego oraz chwilowego obciążenia sieci.

6 Bezpieczeństwo

6.1 Bezpieczeństwo transmisji danych

W celu zapewnienia bezpieczeństwa transmisji danych, komunikacja w ramach systemu ESDK pomiędzy uczestnikami a KDPW odbywa się za pośrednictwem bezpiecznych kanałów VPN zrealizowanych w oparciu o protokół IPSec. Wykorzystanie protokołu IPSec zapewnia możliwość uwierzytelnienia obydwu stron połączenia oraz gwarantuje zachowanie poufności i integralności danych na poziomie warstwy transportowej.
Po stronie KDPW kanały VPN terminowane są na koncentratorze VPN (Cisco VPN Concentrator 3030), pełniącym rolę węzła dostępowego, natomiast po stronie Uczestnika na dowolnym urządzeniu sieciowym wspierającym protokół IPSec (router, VPN box, firewall) lub bezpośrednio na komputerze PC wyposażonym w odpowiednie oprogramowanie klienckie (*Cisco VPN Client*), udostępniane Uczestnikom nieodpłatnie. Wymagane jest, aby w przypadku zestawiania kanałów pomiędzy dwoma serwerami MQ (wykorzystania po stronie klienta oprogramowania na bazie IBM MQ Server), komunikacja w tunelu VPN była dwukierunkowa, co warunkuje konieczność skonfigurowania kanału VPN po stronie Uczestnika w oparciu o urządzenia sieciowe.

Parametry protokołu IPSec:

- funkcja skrótu: **SHA-1**
- algorytm szyfrowania: **AES256**
- tryb pracy: **tunelowy**
- uwierzytelnienie: **na podstawie certyfikatu**

6.2 Podpis elektroniczny

Dla zapewnienia wiarygodności komunikatów przesyłanych za pośrednictwem systemu ESDK zastosowane zostały metody kryptograficzne oparte na rozwiązaniach PKI. Możliwość weryfikacji integralności oraz zapewnienie niezaprzeczalności przesyłanych komunikatów zapewnia umieszczenie w strukturze komunikatu podpisu elektronicznego. Podpis elektroniczny generowany jest dla bufora danych obejmującego komunikat merytoryczny oraz

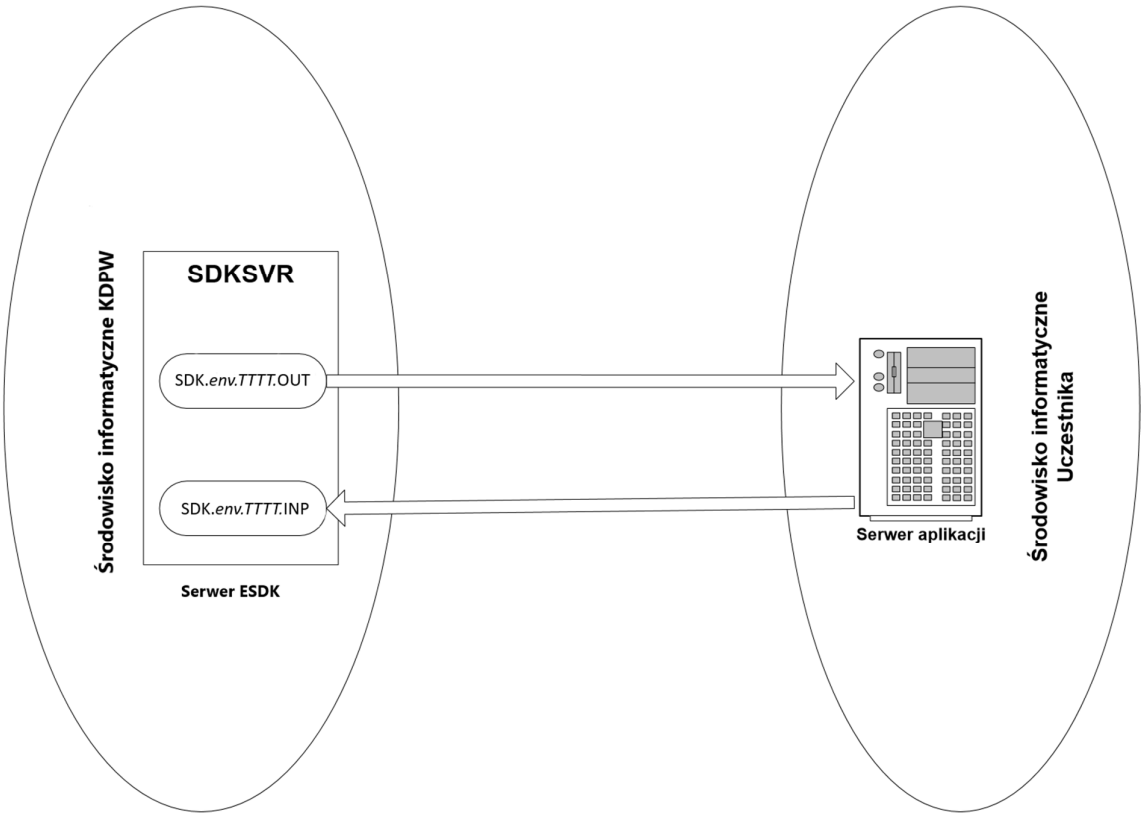
dane identyfikujące nadawcę, odbiorcę, numer i typ komunikatu oraz datę i czas utworzenia komunikatu. System ESDK akceptuje tylko komunikaty podpisane i poprawnie zweryfikowane. Do wydawania i zarządzania certyfikatami wykorzystano istniejącą w KDPW infrastrukturę PKI utworzoną na potrzeby systemu ESDI (Urząd Certyfikacji KDPW). Certyfikaty cyfrowe wystawiane przez Urząd Certyfikacji KDPW są zgodne ze standardem X.509 v.3. Analogicznie jak w systemie ESDI, podpis elektroniczny tworzony jest w formacie PKCS#7. Certyfikaty i klucze kryptograficzne składowane są na nośnikach wymiennych.

7 Współpraca Klienta ESDK z Serwerem ESDK

W związku z możliwością wyboru przez Uczestnika rodzaju klienckiego oprogramowania IBM MQ, możliwe są dwa warianty konfiguracji połączenia z *Queue Managerem* SDKSVR:

7.1 Wariant I (klient – serwer)

- Wariant ten zrealizowany jest w oparciu o oprogramowanie *IBM MQ Client*.



Rysunek nr 3. Wariant I

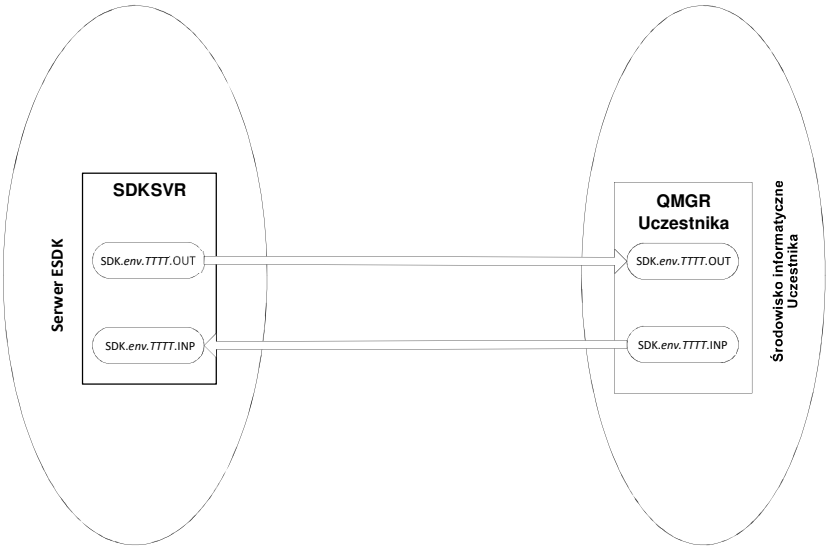
W celu umożliwienia połączenia oprogramowania *IBM MQ Client* z kolejkami *Queue Manager'a* SDKSVR, dla każdego z użytkowników zostaną skonfigurowane kanały MQ typu *SVRCN o nazwie **SDK.*env.TTTT*.C**, gdzie *env* to identyfikator środowiska (PROD, TSTA, TSTB), *TTTT* to identyfikator Uczestnika.

Aby nawiązać komunikację z *Queue Managerem* za pośrednictwem ww. kanału należy na stacji klienckiej skonfigurować kanał kliencki na podstawie dokumentacji klienta MQ.
Stacja kliencka musi mieć możliwość rozwiązania nazwy SDKSVR (za pomocą serwera DNS, lub tablicy hostów) na adres IP serwera SDKSVR.

Oprogramowanie *IBM MQ* jest udostępniane na zasadach komercyjnych przez firmę IBM. Oprogramowanie *IBM MQ Client* jest bezpłatne. KDPW nie pośredniczy w dystrybucji tego oprogramowania.

7.2 **Wariant II (serwer – serwer)**

- Wariant ten zrealizowany jest w oparciu o oprogramowanie *IBM MQ Server*.



Rysunek nr 4. Wariant II

W celu umożliwienia połączenia oprogramowania IBM MQ Server z *Queue Manager'em* SDKSVR, należy w porozumieniu z KDPW skonfigurować kanały komunikacyjne:

- **SDK.*env*.*TTTT*.KU** obsługujący wysyłanie komunikatów w środowisku *env* (PROD, TSTA, TSTB) z *Queue Managera* SDKSVR do *Queue Managera* Uczestnika o kodzie instytucji *TTTT*,

- **SDK.*env*.*TTTT*.UK** obsługujący wysyłanie komunikatów w środowisku *env* (PROD, TSTA, TSTB) z *Queue Managera* Uczestnika o kodzie instytucji *TTTT* do *Queue Managera* SDKSVR.

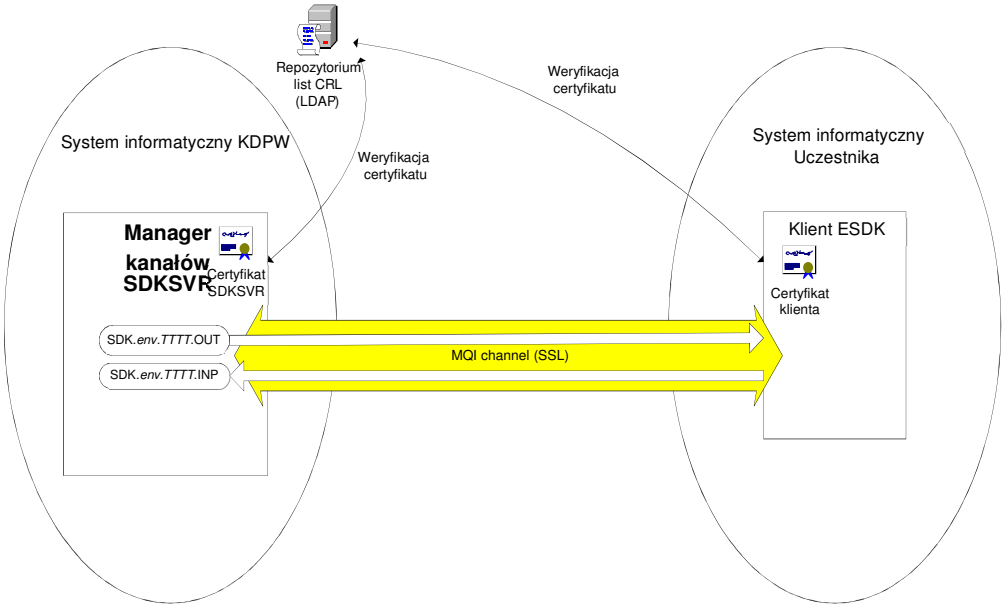
Oprogramowanie *IBM MQ Server* jest udostępniane na zasadach komercyjnych przez firmę IBM. KDPW nie pośredniczy w dystrybucji tego oprogramowania.

7.3 Mechanizmy uwierzytelniania użytkowników do systemu ESDK

Mechanizmy autoryzowania dostępu użytkowników do systemu ESDK oparte są na weryfikacji tożsamości użytkowników na podstawie certyfikatów elektronicznych z wykorzystaniem protokołu SSL.

W celu uzyskania dostępu do serwera SDKSVR strona kliencka musi zestawić bezpieczny kanał do managera kolejek MQ za pośrednictwem protokołu SSL. W procesie negocjacji połączenia następuje weryfikacja tożsamości obydwu stron połączenia (klienta i serwera) na podstawie ważnych certyfikatów elektronicznych zgodnych z normą X.509 v.3. Wykorzystanie SSL ma zastosowanie zarówno przy zestawianiu połączeń pomiędzy klientem a serwerem MQ, jak i tworzeniu kanałów pomiędzy dwoma serwerami (managerami kolejek). Autoryzacja klienta do wybranych kolejek wejściowych i wyjściowych następuje na podstawie konta użytkownika w systemie, określonego w konfiguracji kanału. Manager kolejek dokonuje mapowania kont użytkowników na certyfikaty strony klienckiej na podstawie unikalnych atrybutów certyfikatu (DN-Distinguish Name). Dostęp klienta do kolejek komunikatów następuje wyłącznie za pośrednictwem zestawionego wcześniej kanału SSL, co gwarantuje zachowanie poufności transmisji danych.

Do generowania, zarządzania i dystrybucji certyfikatów elektronicznych dla systemu ESDK, wykorzystany zostanie własny Urząd Certyfikacji KDPW. Certyfikaty pochodzące od innych wystawców nie będą obsługiwane. KDPW S.A. przekaże użytkownikom certyfikaty strony klienckiej oraz udostępni certyfikat Urzędu Certyfikacji.



Rysunek nr 5. Mechanizm uwierzytelniania klienta ESDK do managera kanałów SDKSVR

7.4 **Oprogramowanie klienta ESDK**

KDPW S.A. nie udostępnia Uczestnikom oprogramowania klienta ESDK przeznaczonego do zastosowania produkcyjnego. Uczestnicy są zobowiązani do zbudowania klienta ESDK we własnym zakresie.