



Politechnika Warszawska
Wydział Elektroniki i Technik Informacyjnych



Bezpieczny system telefonii VoIP opartej na protokole SIP

Leszek Tomaszewski



Cel

- Stworzenie bezpiecznej i przyjaznej dla użytkownika architektury sieci SIP zapewniającej:
 - Szyfrowane sygnalizacji
 - Szyfrowanie mediów



Przyczyny zagrożeń

- Otwarta infrastruktura sieciowa
 - Internet
- Niezależność dostawcy usługi i sieci
- Nieznana droga transmisji danych (wielu pośredników)



Ataki na sygnalizację

- Podsluchanie wiadomości
 - analiza przesyłu
 - odkrycie treści (URI użytkownika)
- Podszycie
 - Modyfikacja wiadomości
 - nagłówek *Connect* w metodzie REGISTER (Registration Hijacking)
 - nagłówek *From* w metodzie INVITE
 - Inne
 - Podrobienie
 - wysłanie spreparowanej wiadomości BYE (Tearing Down Session)



Ataki na media

- Podśluchanie wiadomości
 - analiza przesyłu
 - odkrycie treści



Ataki typu DoS

- Zalenie serwera wiadomościami sygnalizacyjnymi
- Zalenie serwera pakietami RTP

Przykład ataku podsłuchu

The image shows a Wireshark network traffic capture window. The filter is set to 'udp'. The packet list shows several SIP and RTP packets. The selected packet (Frame 3) is a SIP INVITE message. The details pane shows the following information:

- Request-Line: INVITE sip:0507004830@tutti.etel.pl SIP/2.0
- Method: INVITE
- [Resent Packet: False]
- Message Header
 - Call-ID: 4ece88e9ea82756405ac8b84bcc1844a@0.0.0
 - CSeq: 1 INVITE
 - From: "991234506" <sip:991234506@tutti.etel.pl>;tag=2a244766
 - To: <sip:0507004830@tutti.etel.pl>
 - Via: SIP/2.0/UDP 172.31.130.100:12752;branch=z9hG4bKf8e5db5d4c05071e27100d3ecf880695
 - Max-Forwards: 70
 - User-Agent: SIP Communicator 1.0 CVS-Sun_Mar_16_12-17-43_CET_2008
 - Contact: "991234506" <sip:991234506@172.31.130.100:12752;transport=udp>
 - Content-Type: application/sdp
 - Content-Length: 163
- Message Body
 - Session Description Protocol
 - Session Description Protocol Version (v): 0
 - Owner/Creator, session id (o): 991234506 0 0 IN IP4 172.31.130.100
 - Session Name (s): -
 - Connection Information (c): IN IP4 172.31.130.100
 - Time Description, active time (t): 0 0
 - Media Description, name and address (m): audio 5000 RTP/AVP 8 0 97 3 110 5 4
 - Media Description, name and address (m): video 5002 RTP/AVP 34 26 31
 - Media Attribute (a): recvnly

The packet bytes pane at the bottom shows the raw data of the captured frame.

Przykład ataku podsłuchu

The image displays a Wireshark network traffic analysis window. The main window shows a list of captured packets filtered by 'udp'. The selected packet is a SIP/SDP message. Overlaid on this is a 'VoIP Calls' window showing a detected call with the following details:

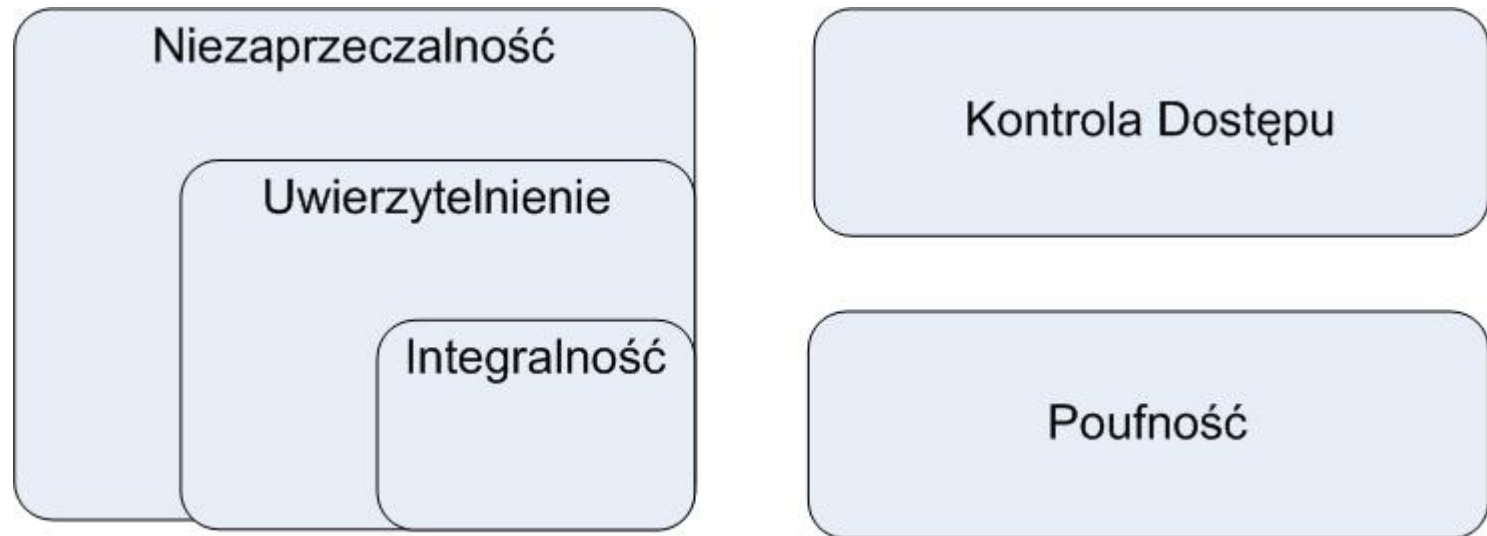
Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
0.000	20.968	172.31.130.100	sjp:991234506@tutti.etel.pl	sjp:0507004830@tutti.etel.pl	SIP	9	COMPLETED	

Below the call details is a 'VoIP - RTP Player' window showing two RTP streams. The top stream is from 172.119.66.222 to 172.31.130.100:5000, with a duration of 16.93 seconds and a drop rate of 0.4%. The bottom stream is from 172.31.130.100:5000 to 217.119.66.222:44274, with a duration of 16.90 seconds and a drop rate of 1.9%. Both streams show waveform visualizations of the audio data.

At the bottom of the RTP Player window, there is a 'Jitter buffer [ms]' set to 50, and buttons for 'Decode', 'Play', 'Pause', 'Stop', and 'Close'.

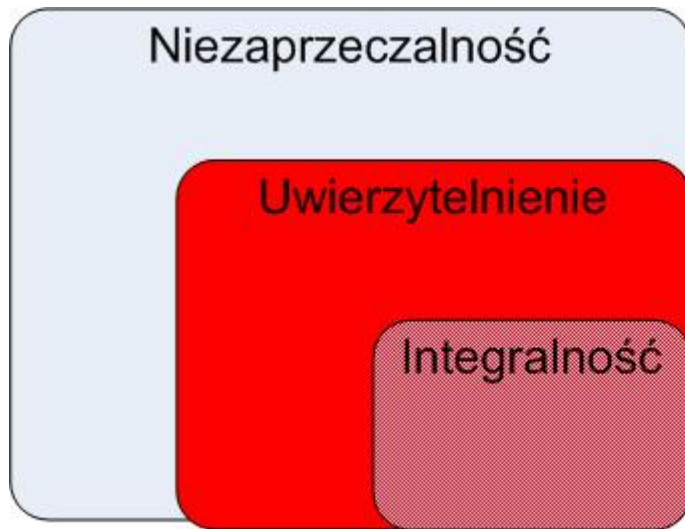


Usługi ochrony informacji





Usługi ochrony informacji





SIP – wymagania bezpieczeństwa (RFC 3261)

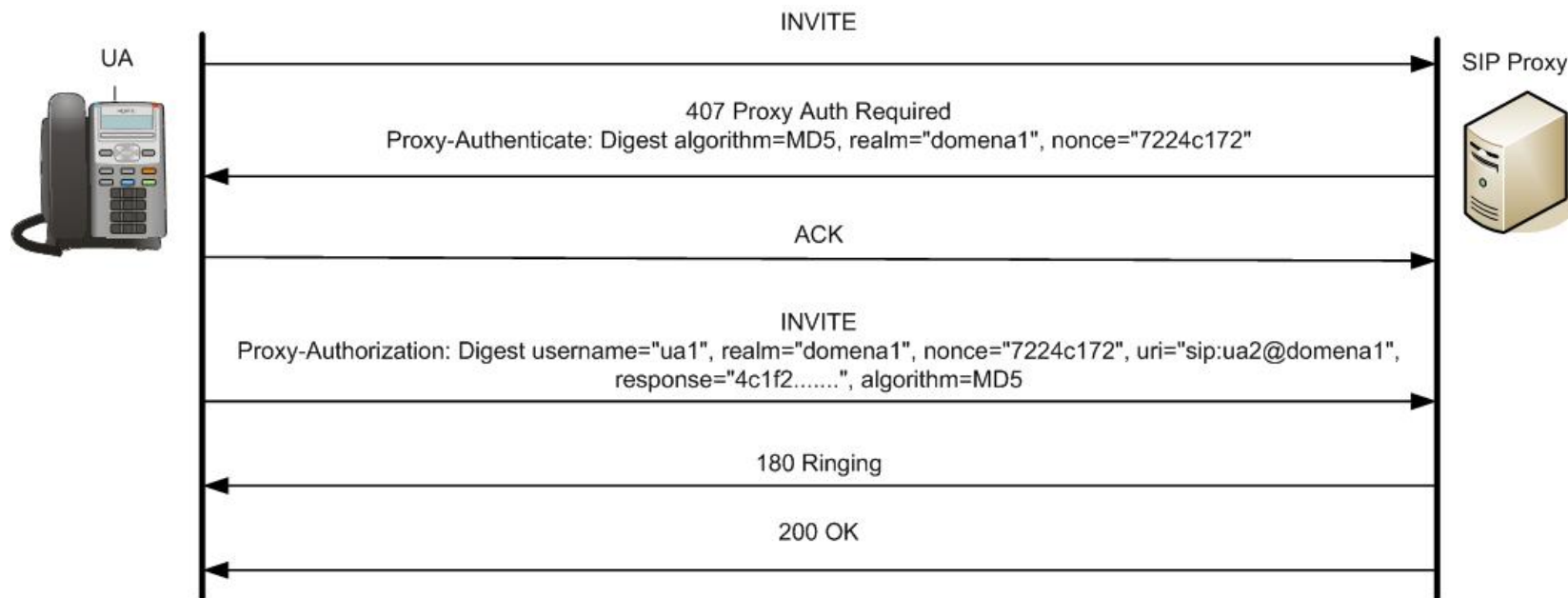
- Uwierzytelnienie
 - Tryb end-to-end
 - SIP DIGEST (obowiązkowy)
 - S/MIME
 - Tryb hop-by-hop
 - TLS
 - IPSec
 - SIPS URI



SIP – wymagania bezpieczeństwa(RFC 3261)

- Poufność
 - Tryb end-to-end
 - S/MIME
 - Tryb hop-by-hop
 - TLS
 - IPSec

SIP DIGEST

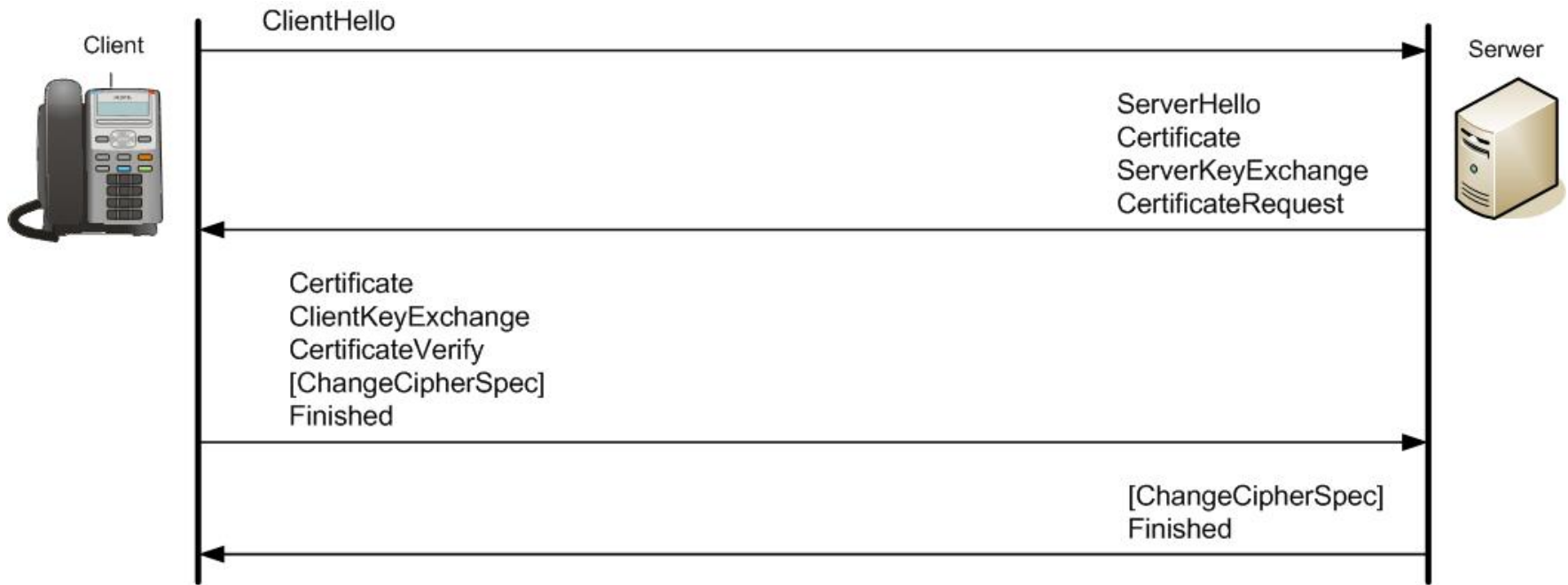




S/MIME

```
INVITE sip:bob@biloxi.com SIP/2.0
Contact: <sip:alice@10.1.3.3>
Content-Type: application/sdp
Content-Length: 147
v=0
o=UserA 2890844526 2890844526 IN IP4 here.com
s=Session SDP
c=IN IP4 100.101.102.103
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s
ghyHhHUujhJhjh77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jh77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjh776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756
--boundary42-
```

TLS





Bezpieczeństwo SIP - podsumowanie

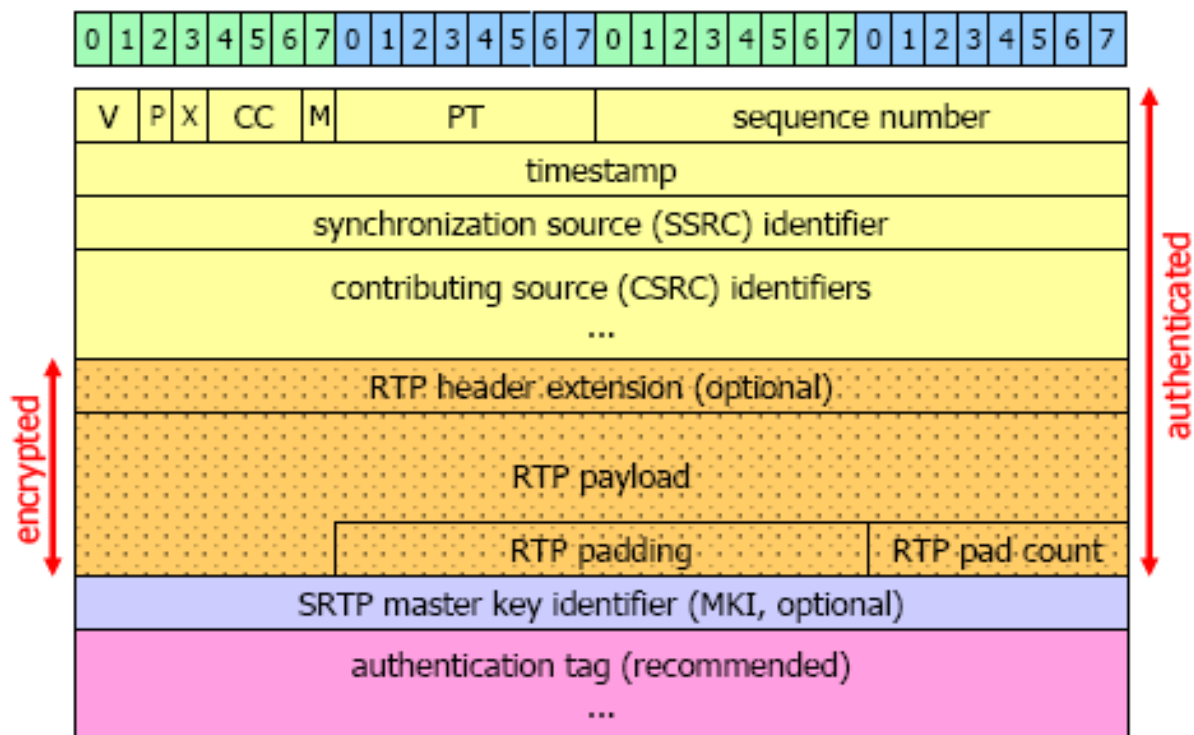
	Uwierzytelnienie	Poufność	Brak wymogów na dystrybucję kluczy lub certyfikatów	Obowiązkowość
Digest	+	-	+	+
S/MIME	+	+/-	-	-
TLS (DTLS)	+	+	+/-	-
IPSec	+	+	-	-



Bezpieczeństwo mediów

- **SRTP**
- IPSec
- TLS (DTLS)

SRTTP

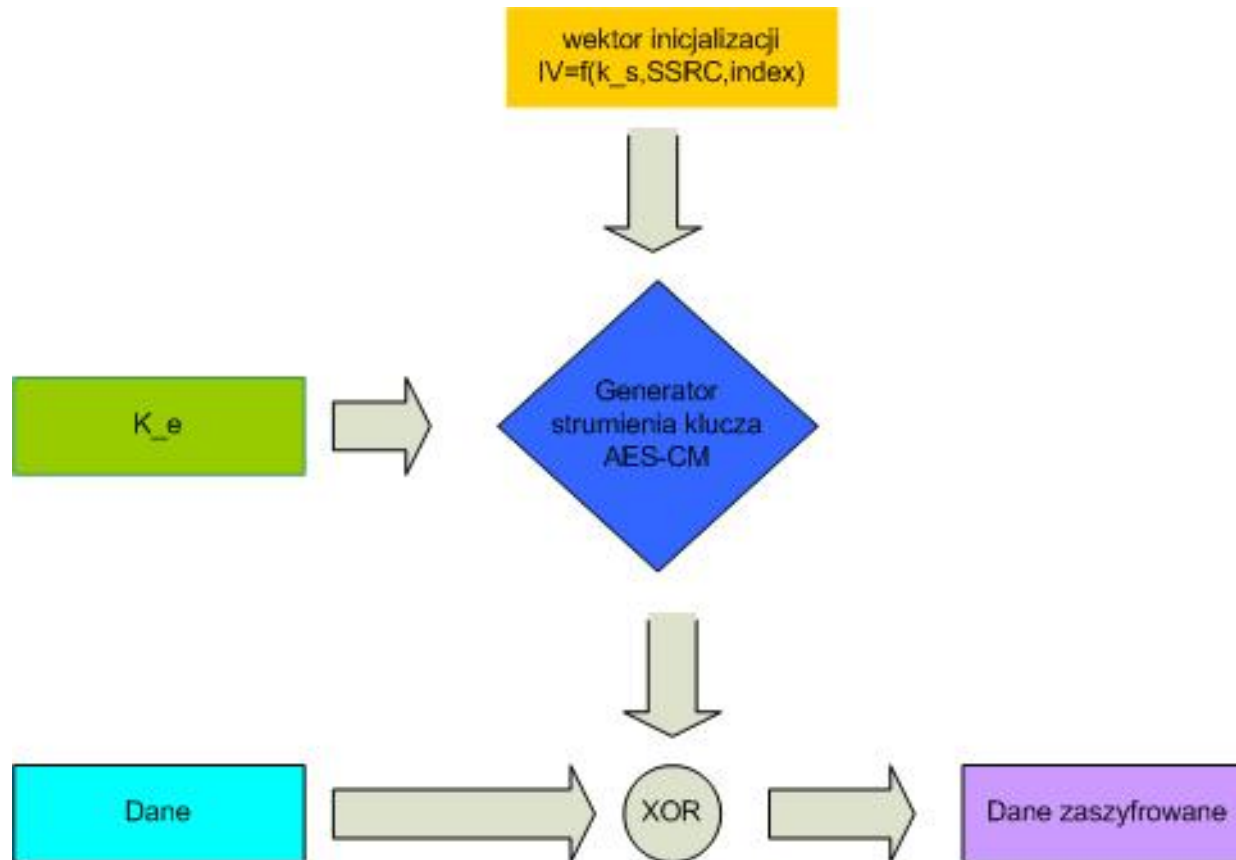




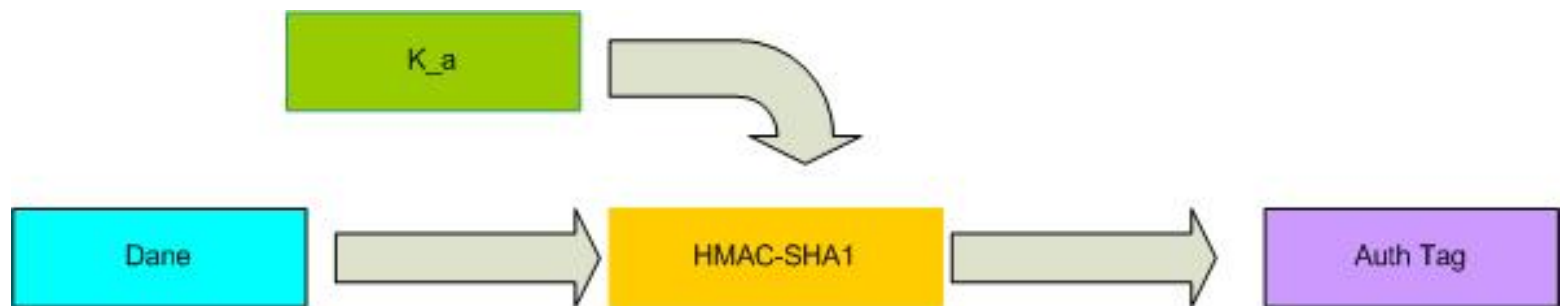
SRTP - algorytmy

- Szyfrowanie
 - AES-CM (domyślny, obowiązkowy)
 - AES-f8 (opcjonalny)
- Funkcja skrótu
 - HMAC-SHA1 (domyślna, obowiązkowa)

SRTP proces szyfrowania



SRTP podpis danych





S RTP – dystrybucja klucza głównego

- SDES (RFC 4568)

- Nie wymaga współdzielonego sekretu
- Nie wymaga Infrastruktury Klucza Publicznego (PKI)
- Wymaga bezpiecznego kanału transmisji

- MIKEY

- Nie wymaga bezpiecznego kanału transmisji
- Wymaga współdzielonego sekretu lub (PKI)



S RTP – dystrybucja klucza głównego

- Z RTP
 - Niezależny od sygnalizacji
 - Wymiana klucza algorytmem D-H
 - Uwierzytelnienie oraz integralność gwarantowana za pomocą parametru SAS (Short Authentication String)

SDES - dystrybucja klucza głównego

SIP-Communicator



SIP-Communicator



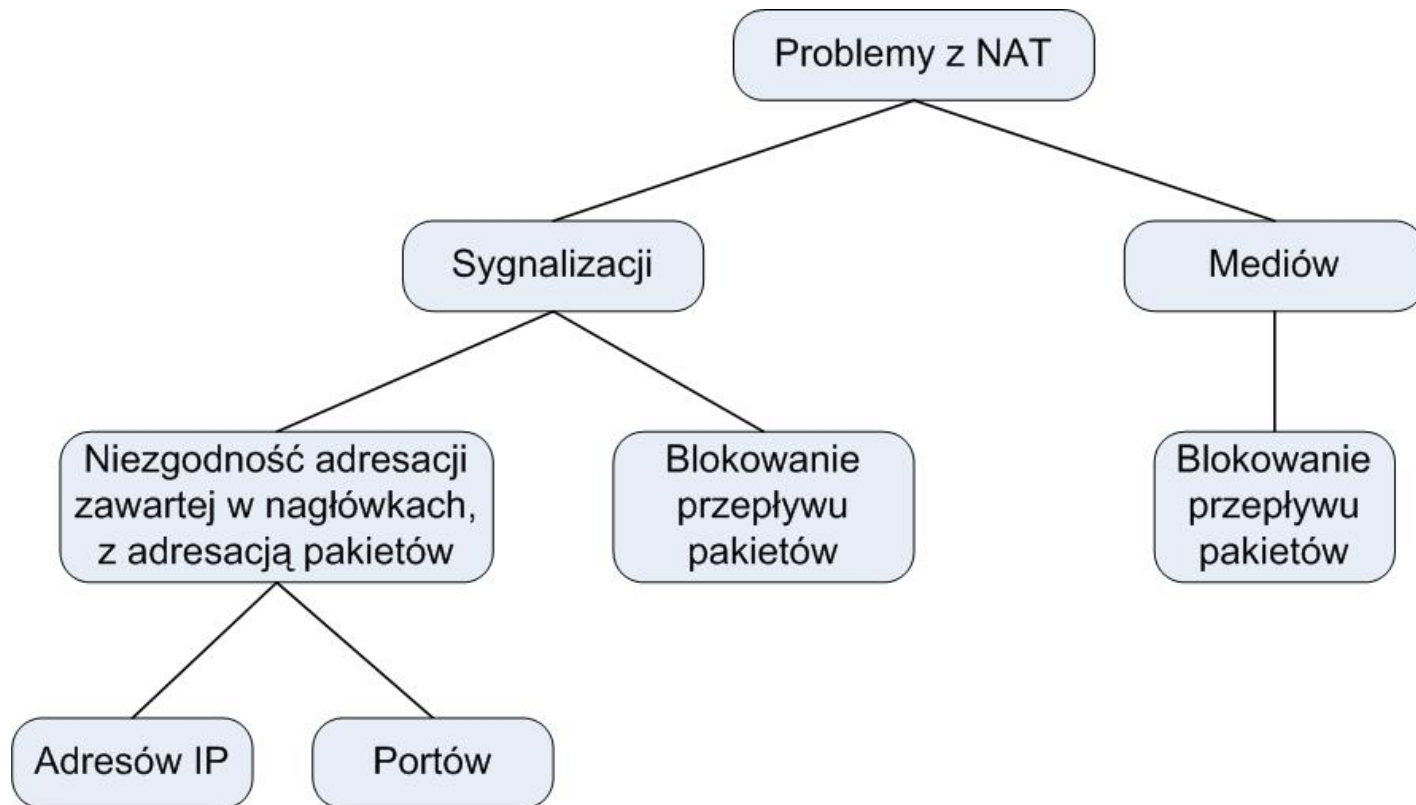
INVITE
m=audio 57676 RTP/AVP 0 8 9 2 3 18 4 101
a=crypto:1 AES_CM_128_HMAC_SHA1_32
inline:WbTBosdVUZqEb6Htqhn+m3z7wUh4RJVR8nE15GbN



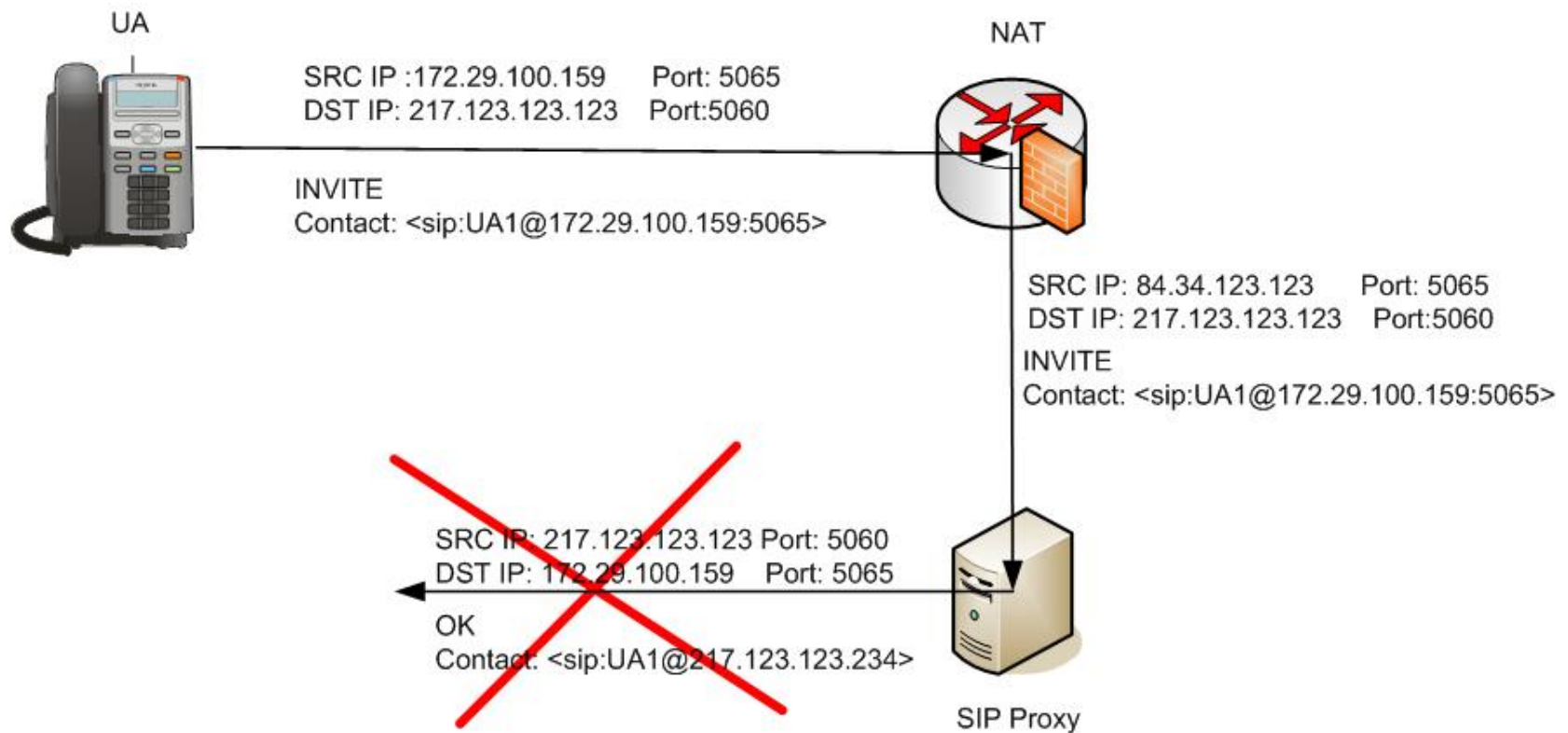
OK
m=audio 57076 RTP/AVP 0 101
a=crypto:1 AES_CM_128_HMAC_SHA1_32
inline:bmt4MzIzMmYxdnFyaWM3d282dGR5Z3g0c2k5M3Yx



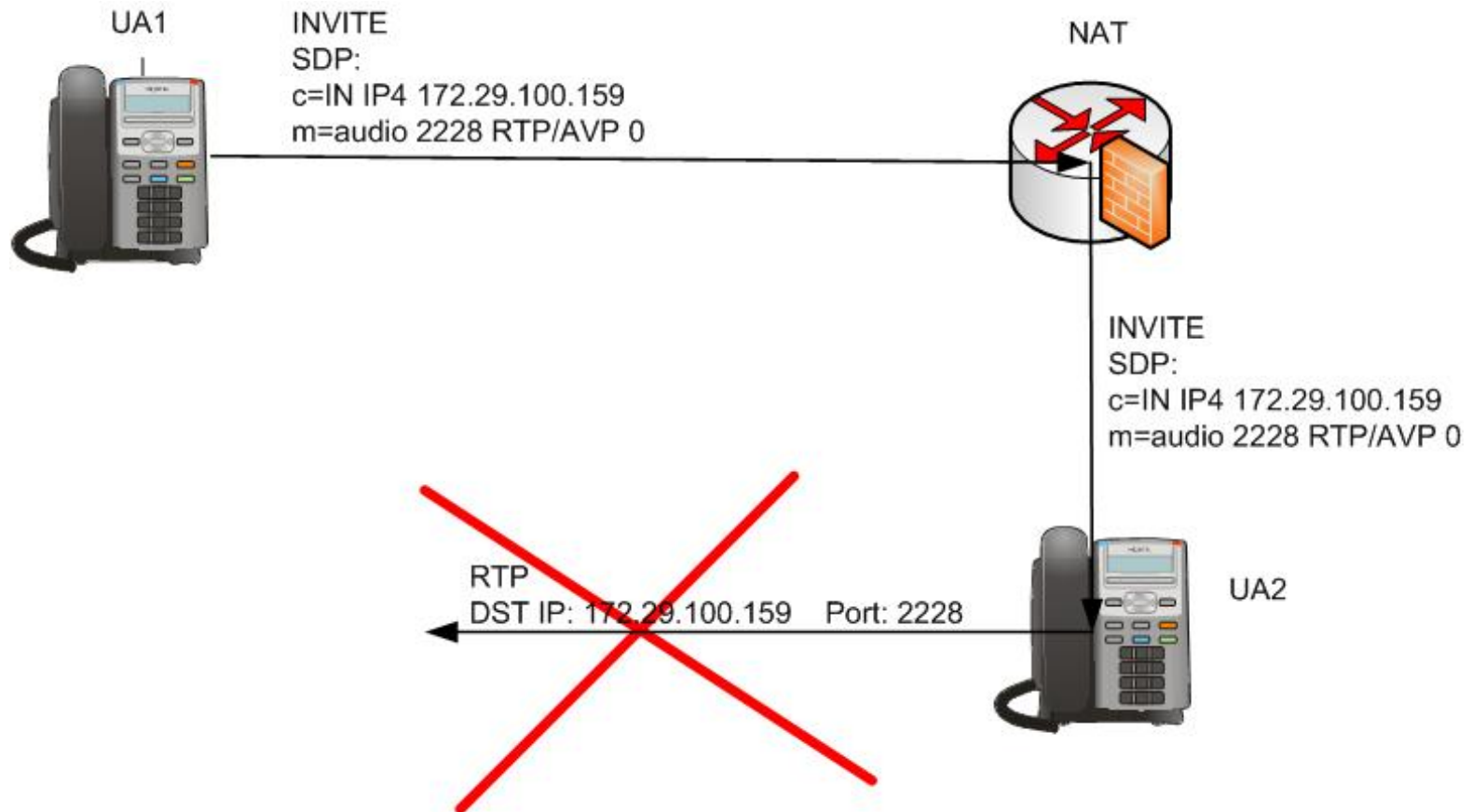
Problemy z NAT



Problemy z NAT – blokowanie sygnalizacji



Problemy z NAT – blokowanie mediów





Rozwiązania problemów z NAT

- **Routing symetryczny**
- **Keep-alive**
- STUN (Simple Traversal of UDP Through NAT)
- TURN (Traversal Using Relay NAT)
- **RTP-proxy**
- IGD (Internet Gateway Device)

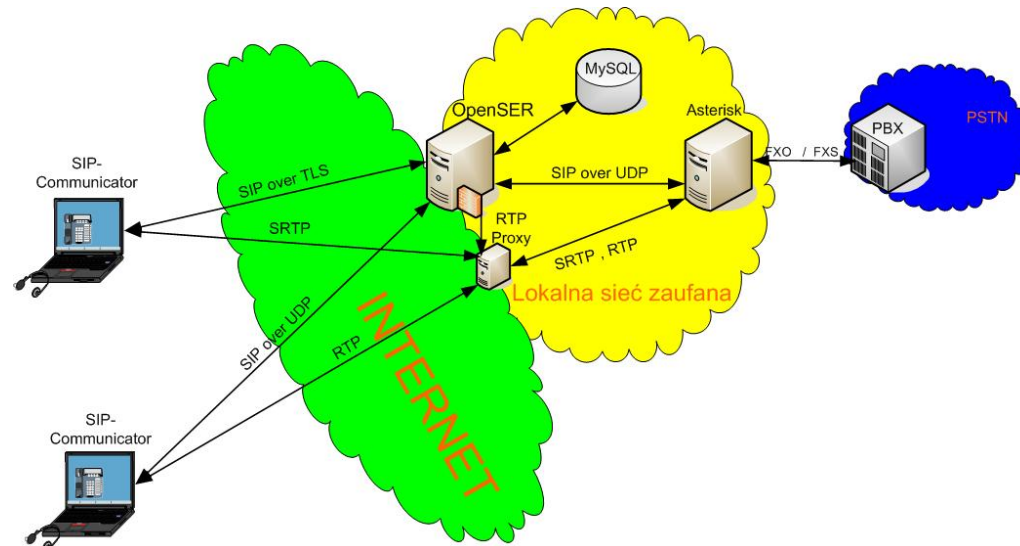
Komponenty + Architektura systemu

■ Serwer

- OpenSER
- RTP Proxy
- Asterisk
- MySQL

■ Klient

- SIP-Communicator





Astersk - cechy

- Otwarty software-owy PBX integrujący usługi VoIP i PSTN
- Obsługa protokołów **SIP**, H323, IAX2
- Możliwość wyposażenia w karty ISDN, FXO(modem)
- Bezpieczeństwo SIP – uwierzytelnienie Digest
- SRTP – moduł testowy oparty na libSRTP
- W pracy wykorzystany jako brama medialna pomiędzy siecią SIP a PSTN

The logo consists of a vertical black line on the left, a horizontal black line below the text, and a cluster of overlapping squares in yellow, red, and blue to the left of the text.

OpenSER

- Funkcje serwera Registrar i Proxy
- Skalowalność i elastyczność konfiguracji
- Współpraca z bazami danych (MySQL)
- Obsługa TLS
- Wsparcie dla NAT
 - RTP-proxy



SIP-Communicator

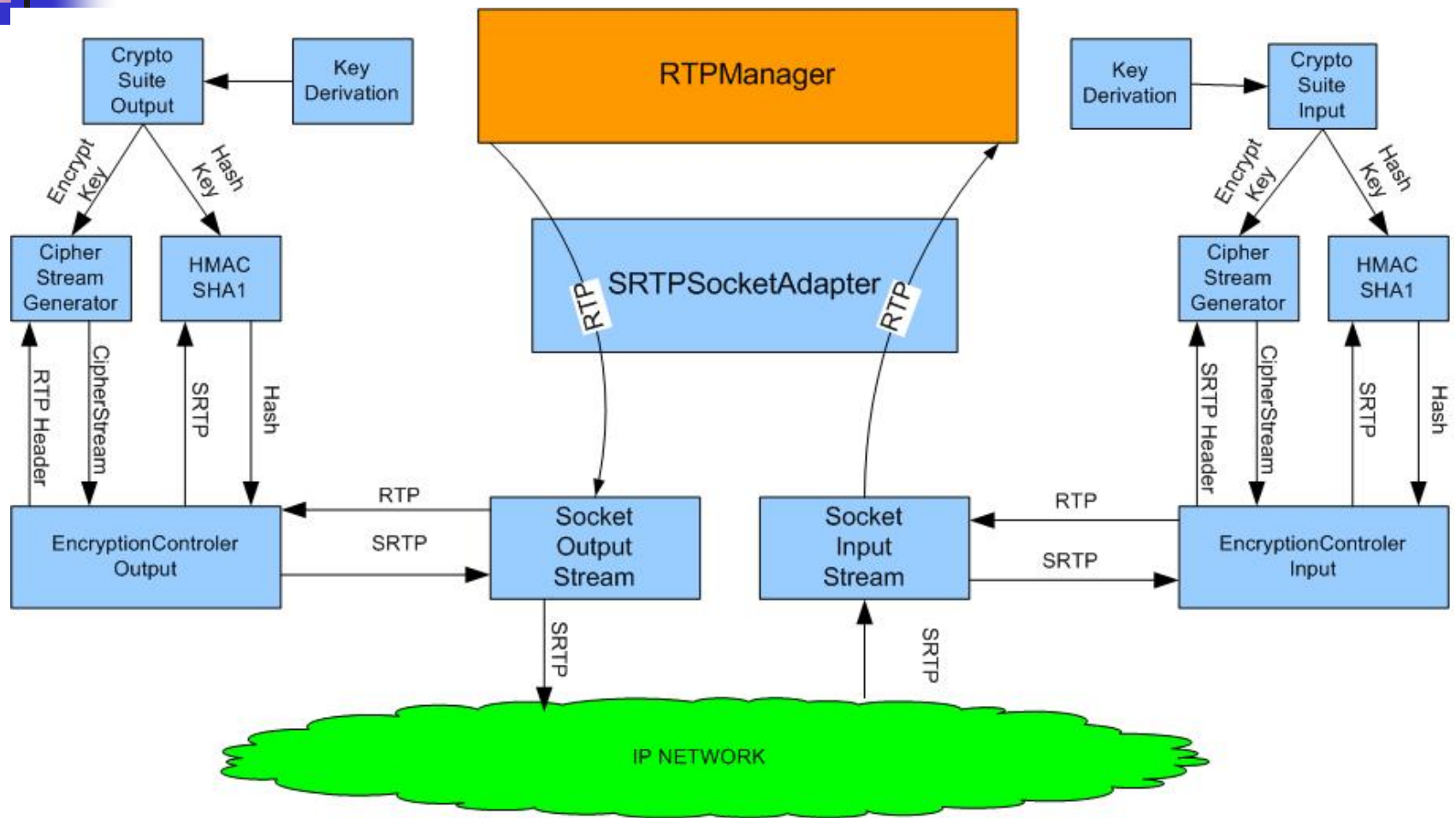
- Internetowy telefon oparty na interfejsie JAIN-SIP
- Obsługa protokołów UDP/TCP/TLS
- **Brak obsługi SRTP**
- **Brak obsługi SDES**



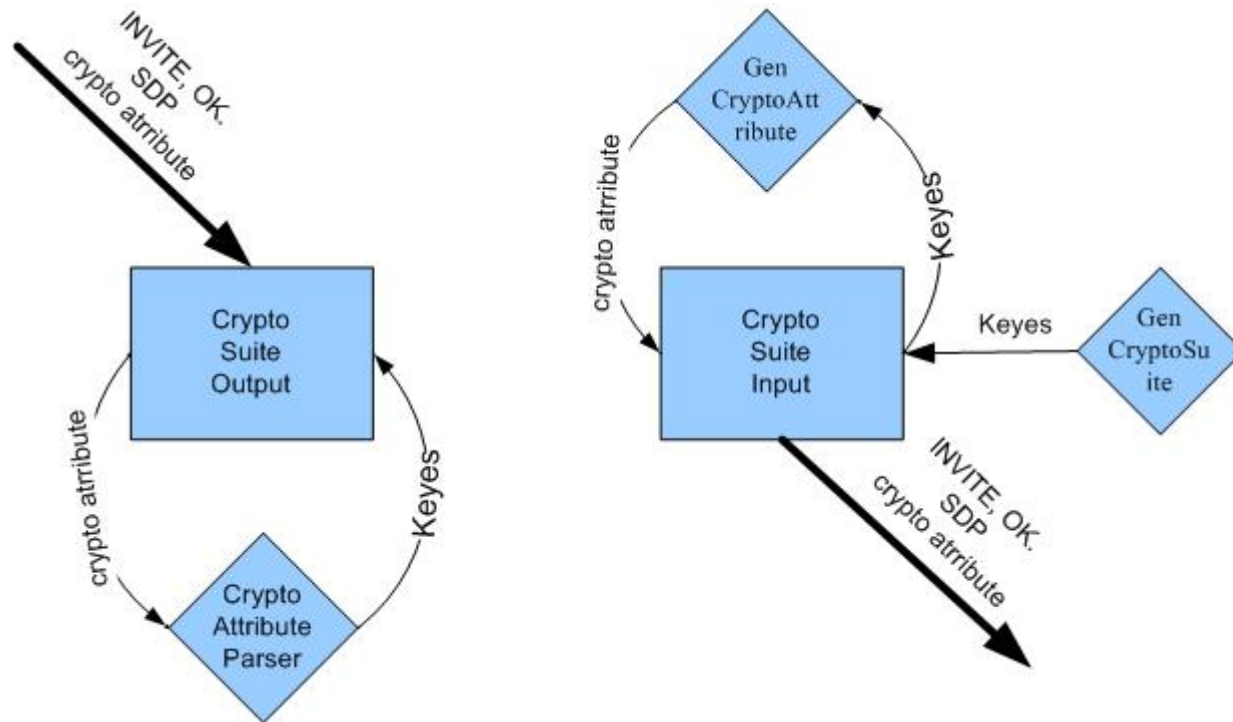
Zakres wykonanej pracy, napotkane problemy

- Implementacja obsługi protokołu SRTP w aplikacji SIP-Communicator (wykorzystanie biblioteki JCE oraz SunJCE)
- Implementacja obsługi wymiany klucza szyfrującego protokołem SDES
- Zarządzanie obsługą schematu URI typu SIPS po stronie klienta
- Kierowanie połączeń oraz obsługa schematu URI typu SIPS po stronie serwera (bloki routingowe)
- Mechanizmy powiadamiania użytkownika o niespełnionych wymaganiach bezpieczeństwa
 - 406 SIPS Not Acceptable
 - 416 SIPS Required
 - 480 SIPS Unavailable
- Powiadamiania użytkownika o zagrożeniach bezpieczeństwa
- Obsługa NAT (RTP Proxy)

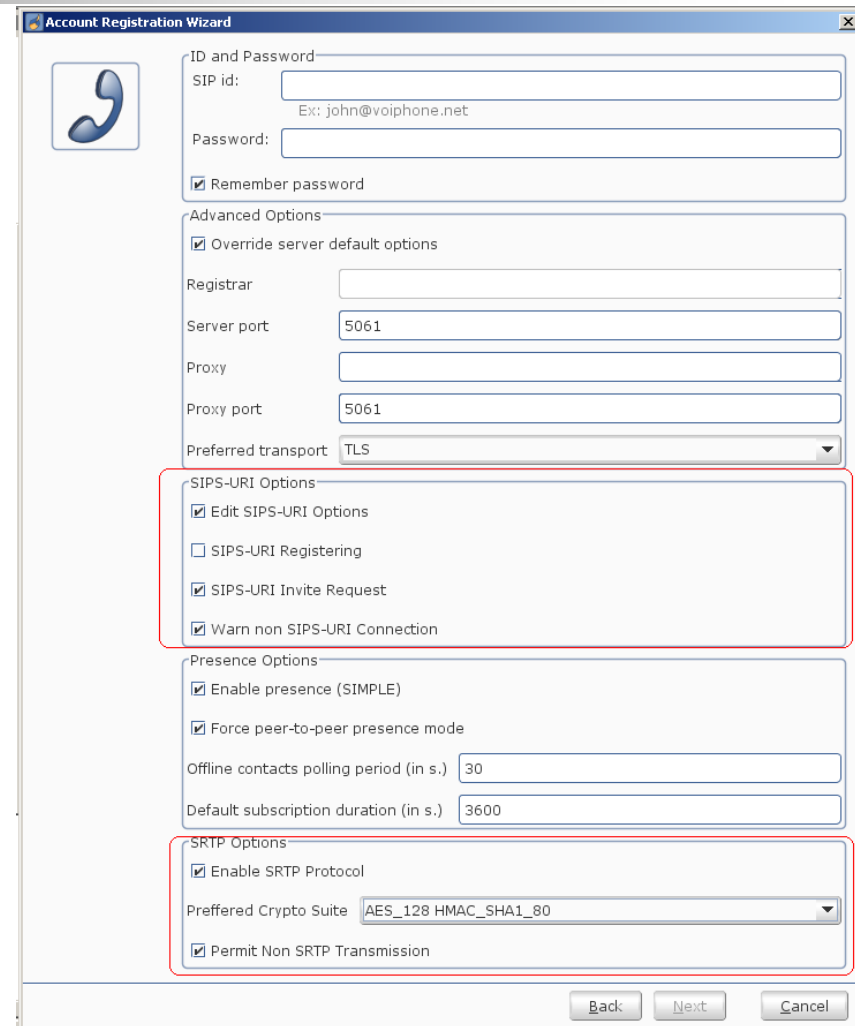
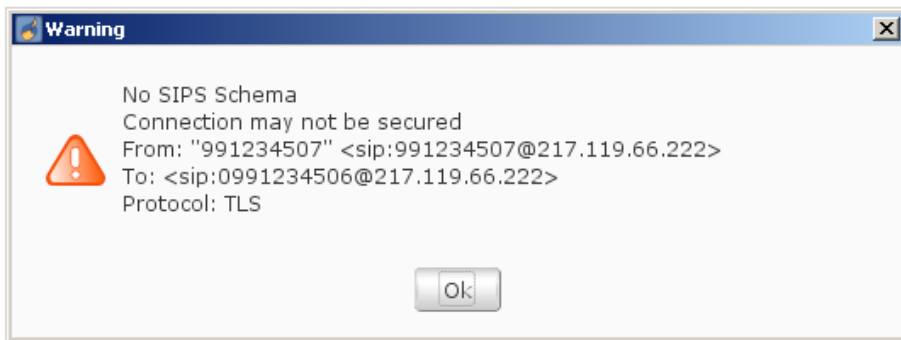
Implementacja SRTP



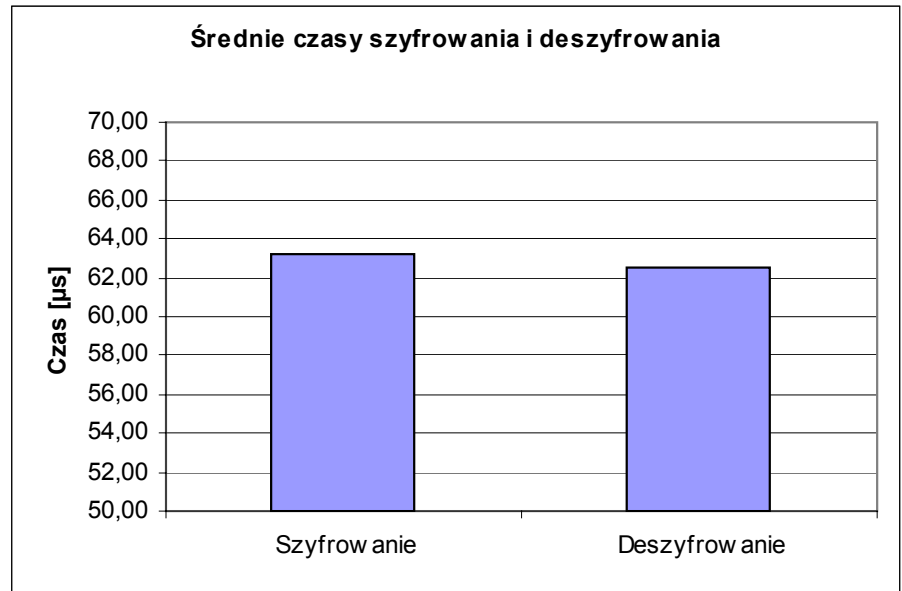
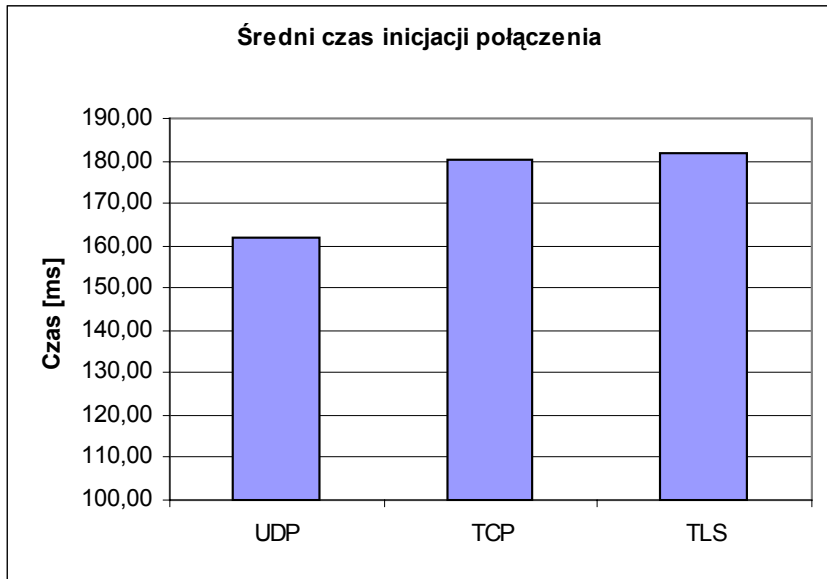
Implementacja SDES



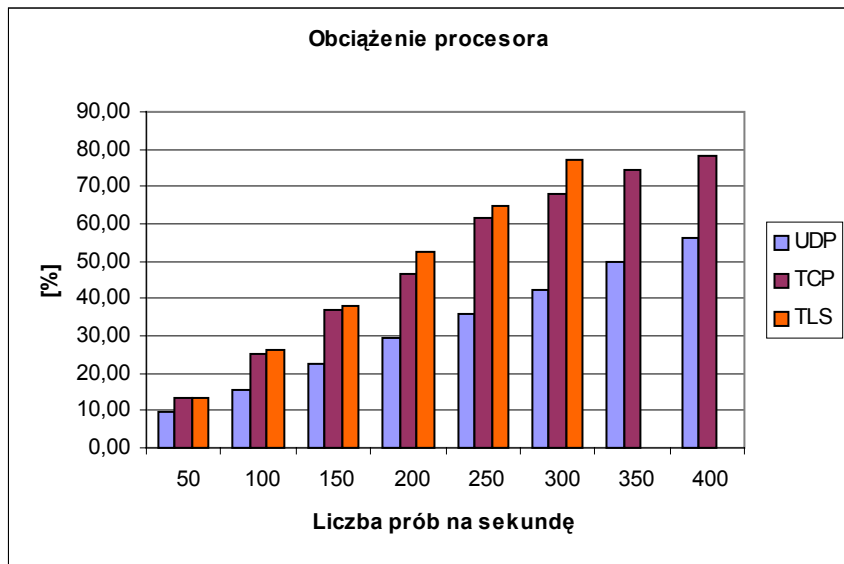
Okno dialogowe + panel konfiguracyjny



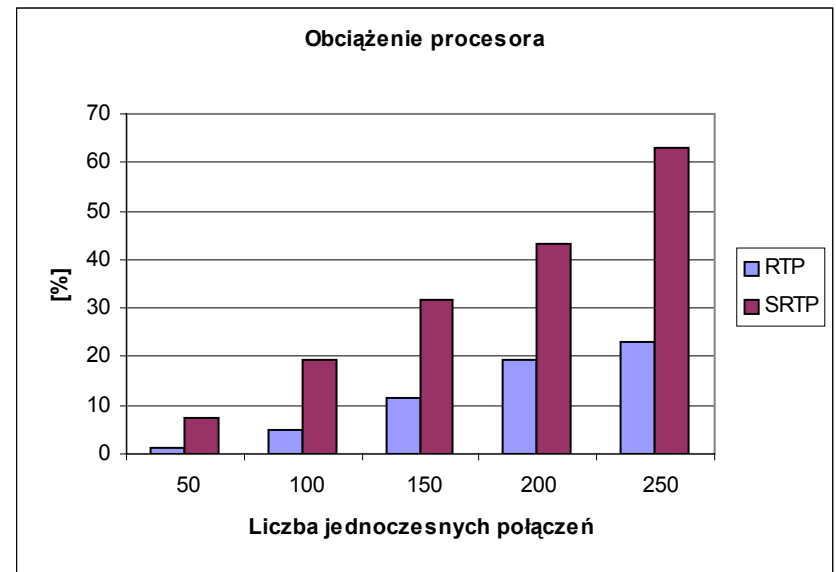
Test wydajności aplikacji



Testy wydajności serwera



Obciążenie procesora w zależności od liczby prób inicjacji sesji



Obciążenie procesora w zależności od liczby jednoczesnych połączeń



Dziękuję
