Canal seguro de comunicação VoIP na plataforma Android

André Luiz Lehmann

Roteiro

- Introdução
- Objetivos
- Fundamentação teórica
- Desenvolvimento
- Conclusão
- Extensões

Introdução

- VoIP
  - Redução de custos
- Plataforma Android
  - Mobilidade
- Segurança de dados
  - Criptografia de dados
  - Troca de chaves

Objetivos

- Realizar comunicação segura através de RTP
- Disponibilizar um *softphone* na plataforma Android utilizando RTP criptografado

VoIP

- Troca de dados de voz (ou vídeo)
- Sinalização
- SIP
  - Protocolo simples
  - Similar ao HTTP
- H.323, MGCP, Megaco/H.248 etc

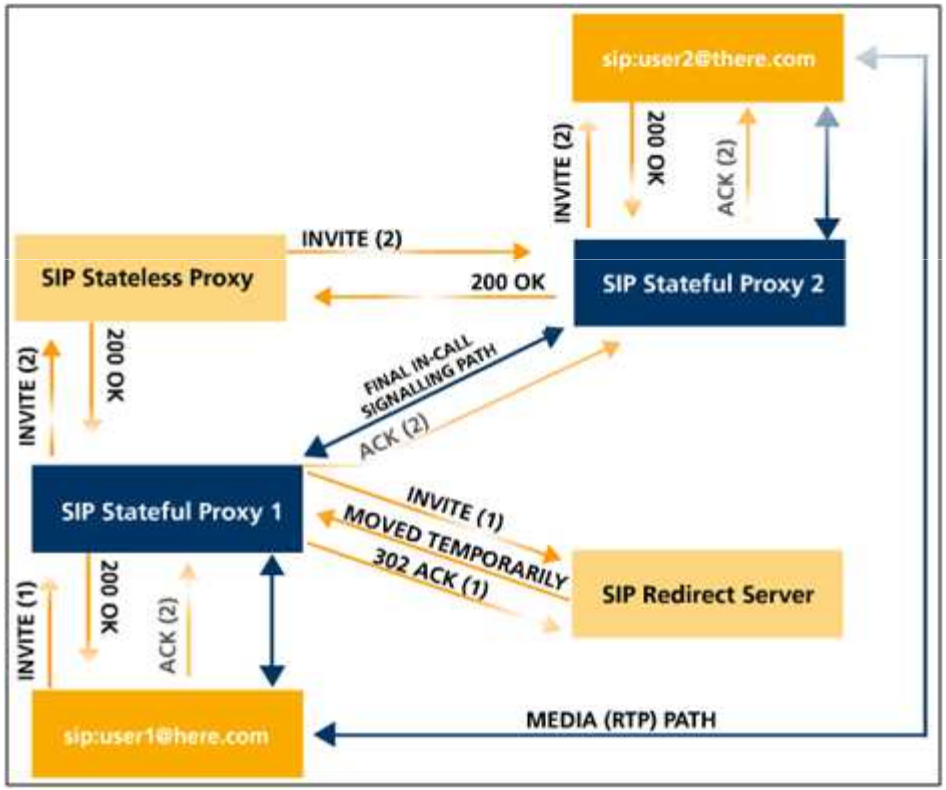
SIP

- Protocolo baseado em texto
- Definido pela RFC 3261
- Possui poucos comandos

Comando	Função
INVITE	Iniciar uma chamada
ACK	Confirmação de uma operação
BYE	Término e transferência de uma chamada
CANCEL	Cancela pesquisa e sinal de toque
OPTIONS	Requisição das características suportadas por outro participante
REGISTER	Registro de um cliente no servidor *Registrar*

SIP

- Exemplo


sip:user2@there.com
INVITE (2)
200 OK
ACK (2)
SIP Stateless Proxy
INVITE (2)
200 OK
SIP Stateful Proxy 2
FINAL IN-CALL SIGNALLING PATH
ACK (2)
INVITE (2)
200 OK
SIP Stateful Proxy 1
INVITE (1)
MOVED TEMPORARILY
302 ACK (1)
SIP Redirect Server
INVITE (1)
200 OK
ACK (2)
sip:user1@here.com
MEDIA (RTP) PATH

Plataforma Android

- Pilha de software, composta por
  - Sistema Operacional
  - *Middleware*
  - Aplicações básicas de operacionalidade
- Sistema aberto e livre

Segurança de dados

- Tornar ilegível
- Algoritmos simétricos e assimétricos
  - Força do algoritmo
  - Força da chave
- Troca de chaves

Segurança de dados

- Advanced Encription Standard (AES)
- Definido pelo NIST em 2001 como padrão para documentos secretos dos EUA
- Algoritmo simétrico
- Algoritmo iterativo, dependendo do tamanho da chave

Segurança de dados

- Diffie-Hellman (DH)
- Criado na década de 70 por Whitfield Diffie e Martin Hellman
- Algoritmo assimétrico
- Logaritmo discreto
- Usado para a troca de chaves para criptografia de algoritmos simétricos

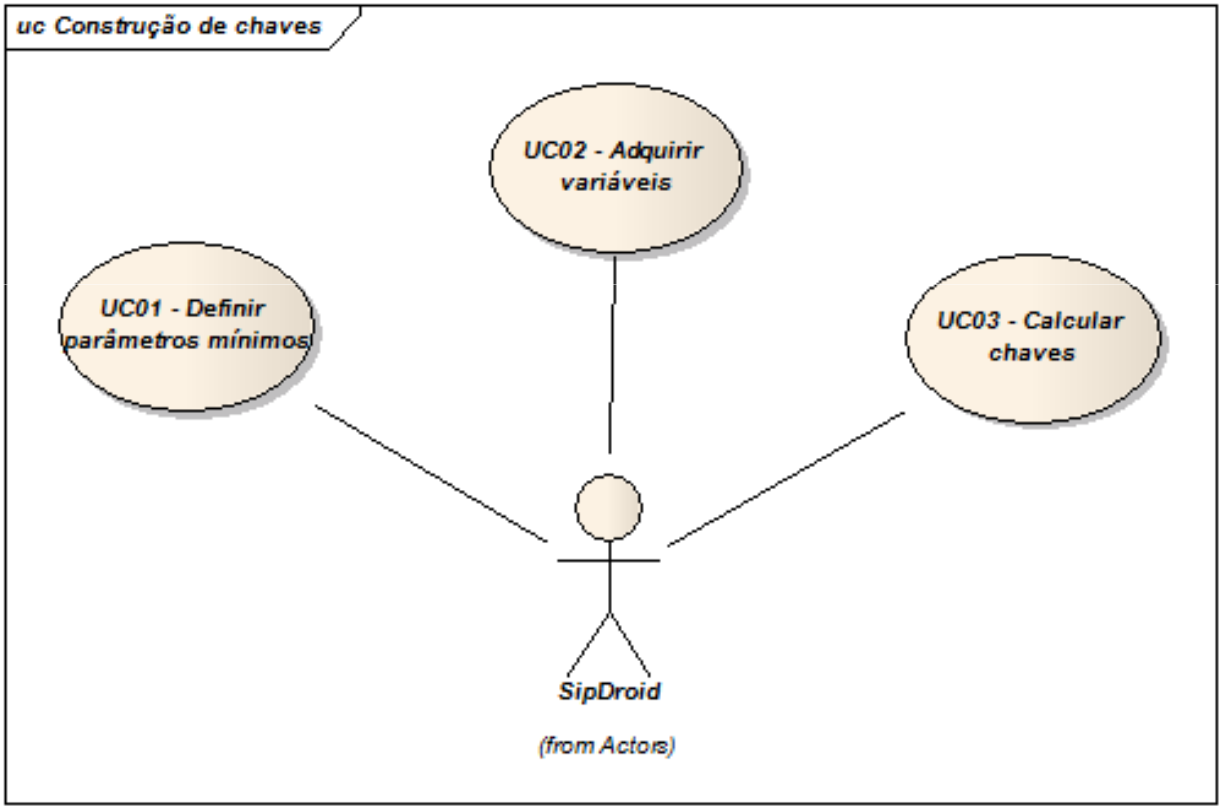
Segurança de dados

- Diffie-Hellman sobre curvas elípticas (ECDH)
- Variação do algoritmo de Diffie-Hellman, mas utilizando o problema de curvas elípticas
- Algoritmo assimétrico
- Possui um mesmo nível de segurança, mas com um tamanho de chave menor

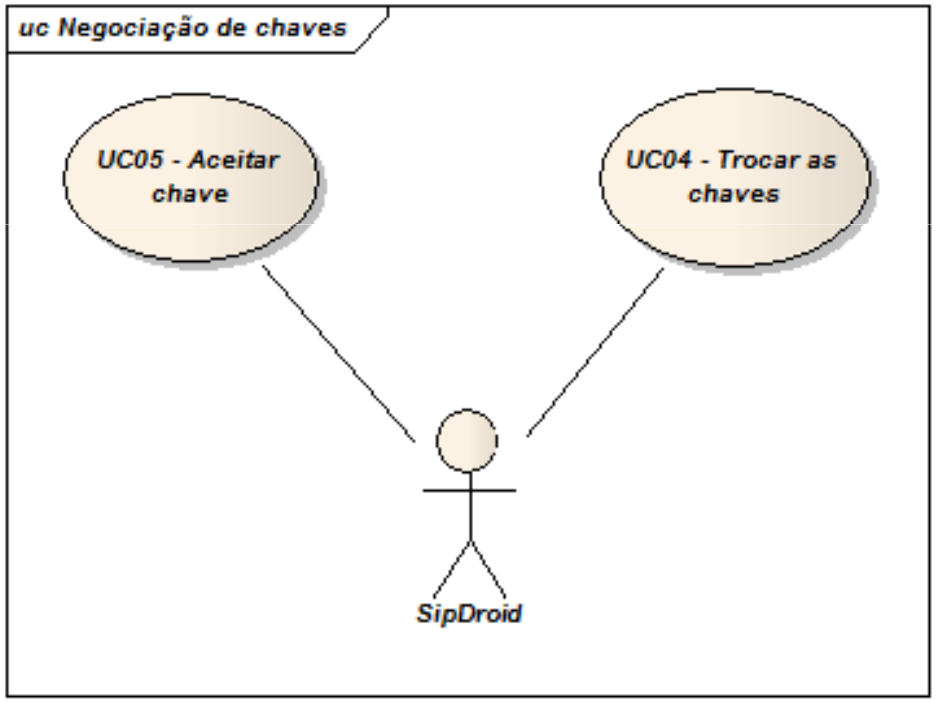
Requisitos

- Funcionais
  - Efetuar a troca de chaves criptográficas através do algoritmo de Diffie-Hellman
  - Gerar as chaves usando logaritmo discreto
  - Gerar as chaves usando curvas elípticas
  - Realizar comunicação VoIP criptografada com AES
  - Adicionar ao *Softphone* SIPDroid a capacidade de troca de pacotes criptografados

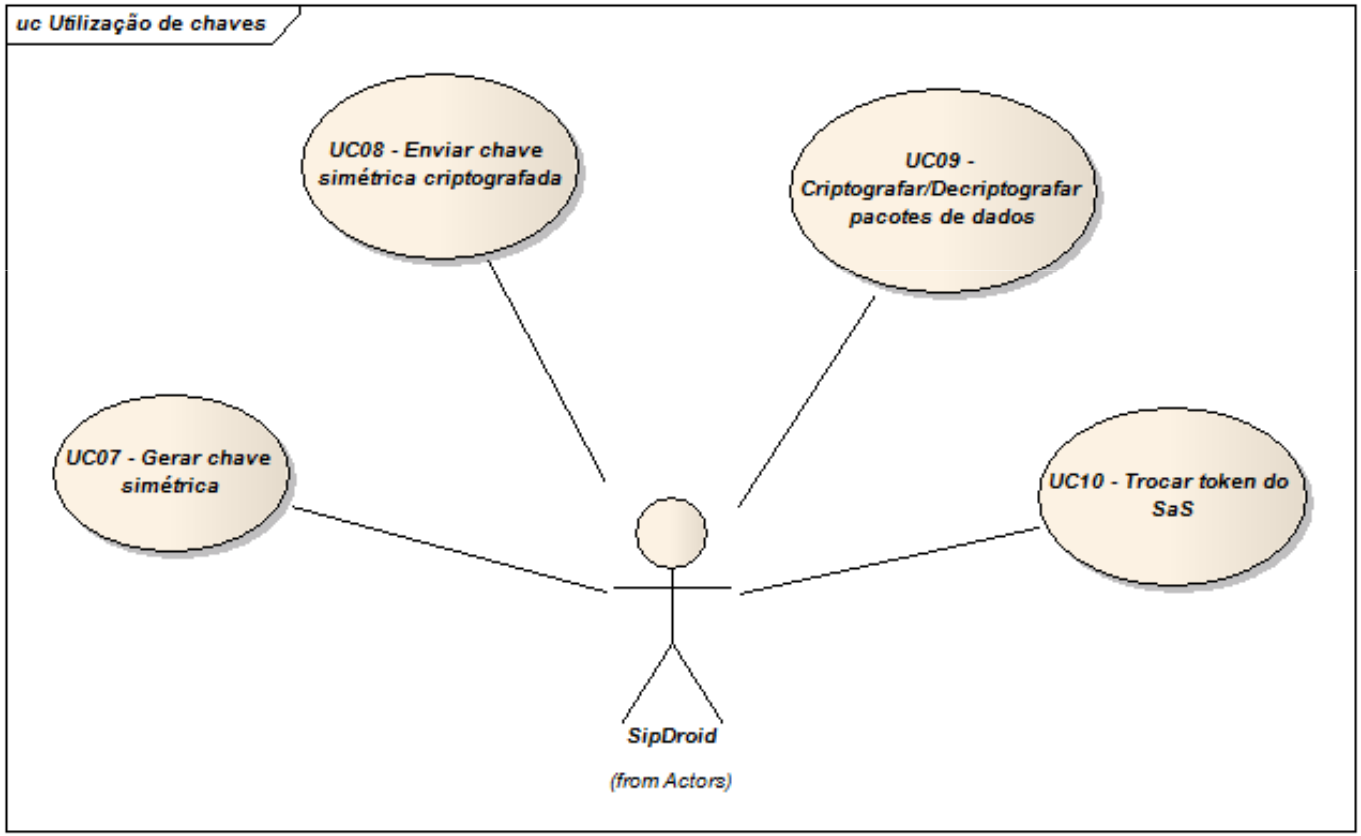
Casos de Uso


uc Construção de chaves
UC02 - Adquirir variáveis
UC01 - Definir parâmetros mínimos
UC03 - Calcular chaves
SipDroid
(from Actors)

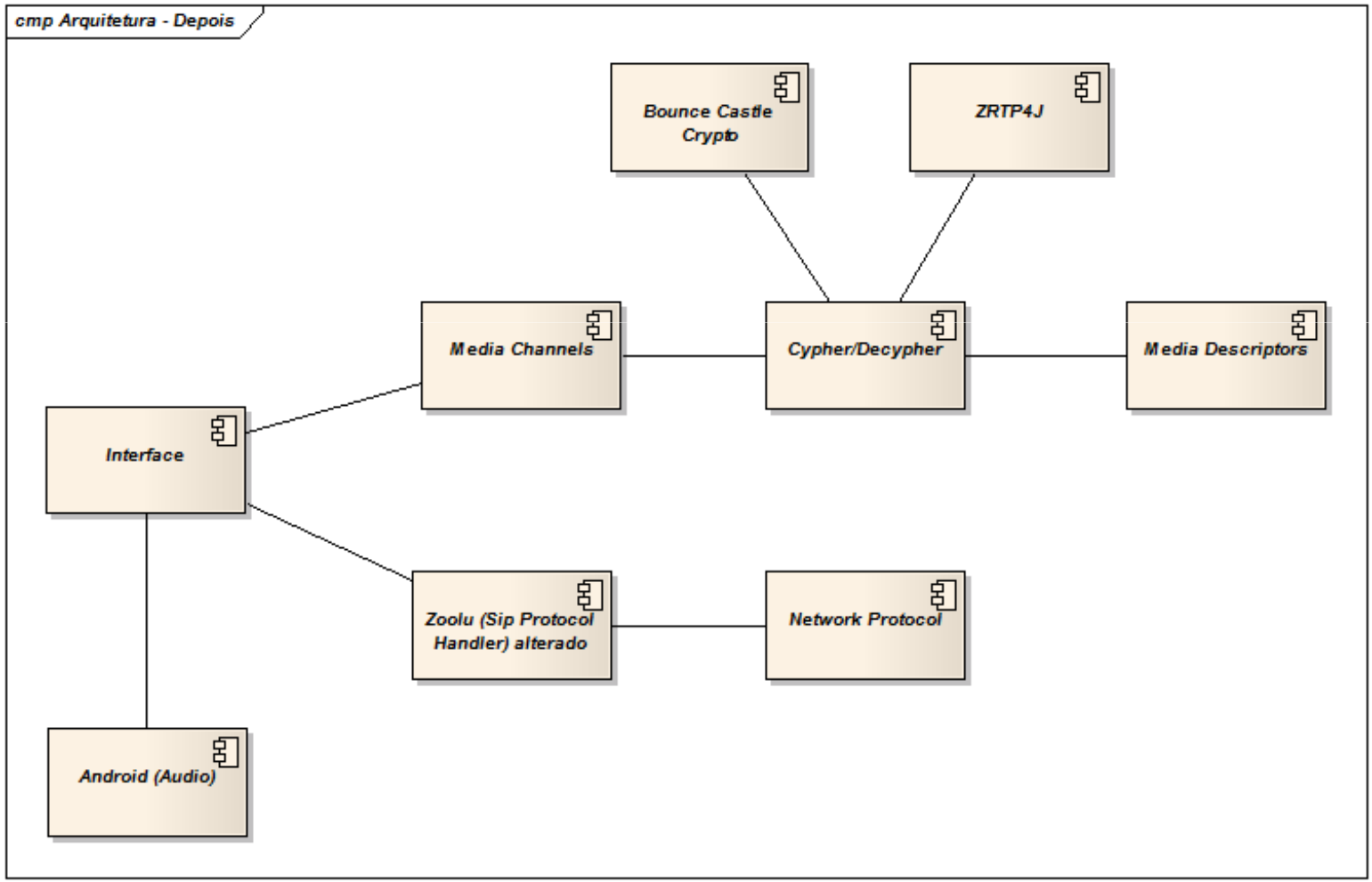
Casos de Uso


uc Negociação de chaves
UC05 - Aceitar chave
UC04 - Trocar as chaves
SipDroid

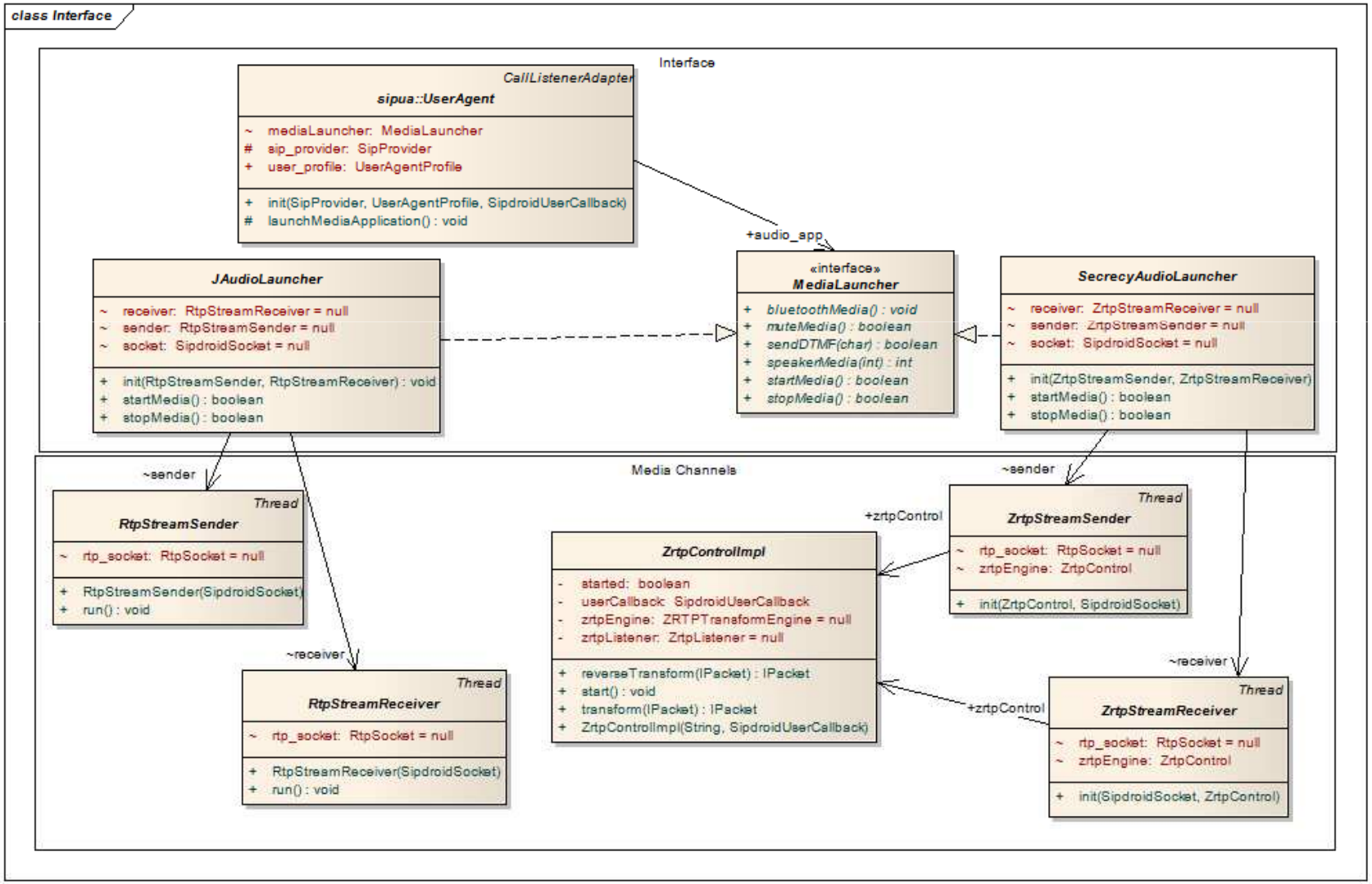
Casos de Uso


uc Utilização de chaves
UC08 - Enviar chave simétrica criptografada
UC09 - Criptografar/Decriptografar pacotes de dados
UC07 - Gerar chave simétrica
UC10 - Trocar token do SaS
SipDroid
(from Actors)

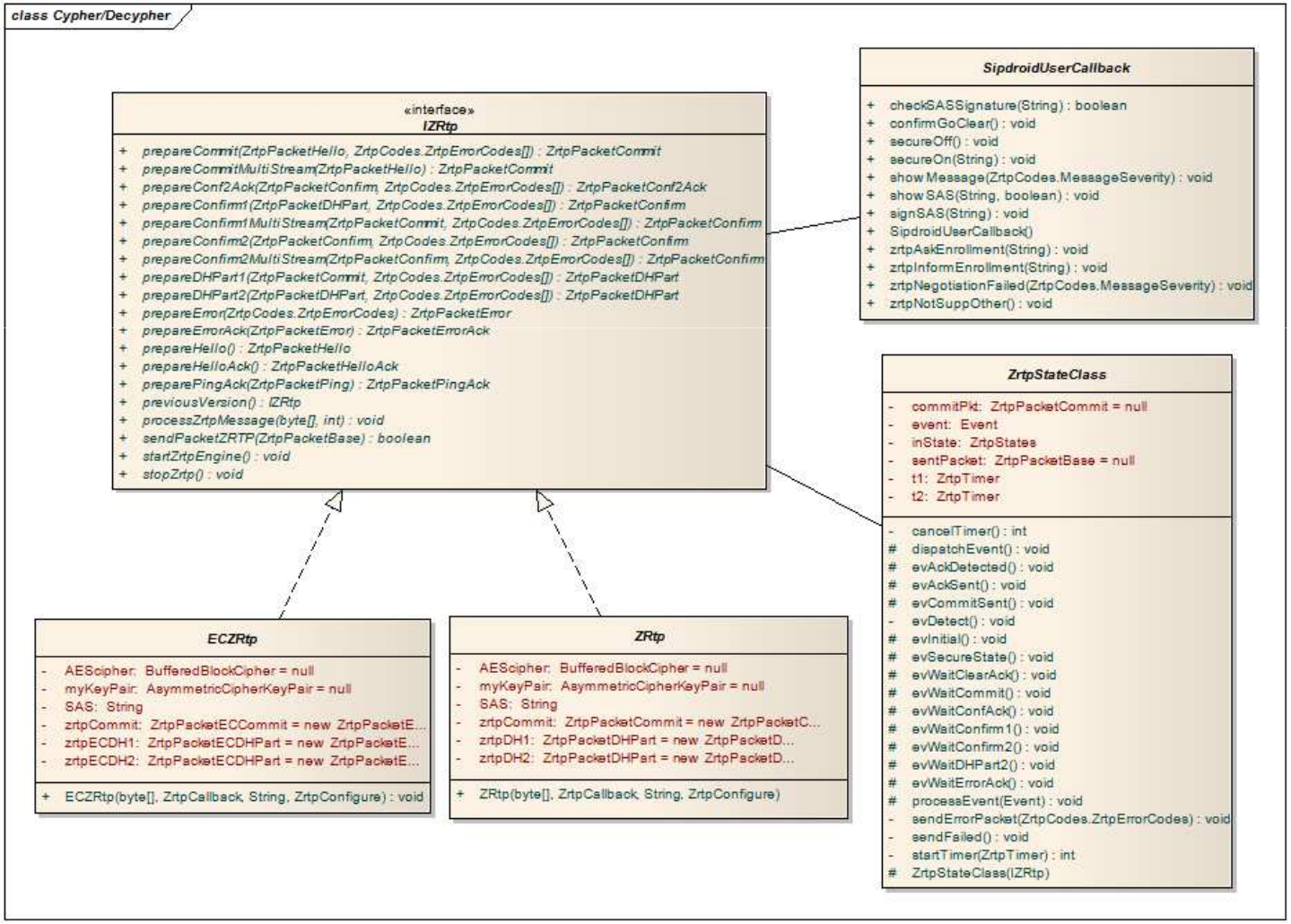
Arquitetura



Interface/Media Channels



Cypher/Decypher e ZRTP4J



Implementação

- Identificação de um protocolo para a troca das chaves criptográficas
  - As chaves deveriam ser efêmeras
- Protocolo ZRTP
  - *Draft* do IETF
- Realização do *port* da implementação Java da biblioteca ZRTP4J, versão 1.1, para a plataforma Android

Implementação

- Criação e adaptação das classes do projeto *SipDroid* para a biblioteca ZRTP4J
  - Adicionado atributo `zrtp-hash` ao corpo das mensagens SIP
  - *Utilização de chaves AES de 384 bits*
- Já é possível se comunicar com outros comunicadores VoIP que implementem ZRTP

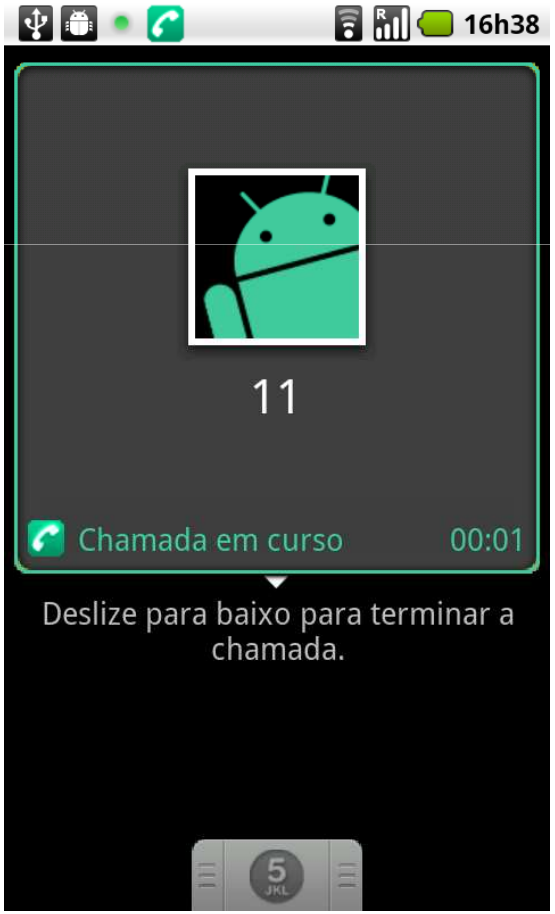
Implementação

- Alteração na biblioteca ZRTP4J
- Oferecer suporte a troca de chaves através de Diffie-Hellman sobre curvas elípticas
- Criação de uma versão 1.2 da biblioteca
- Alteração no conteúdo dos pacotes de dados transportados na negociação
  - Adicionar os dados relativos a curva elíptica

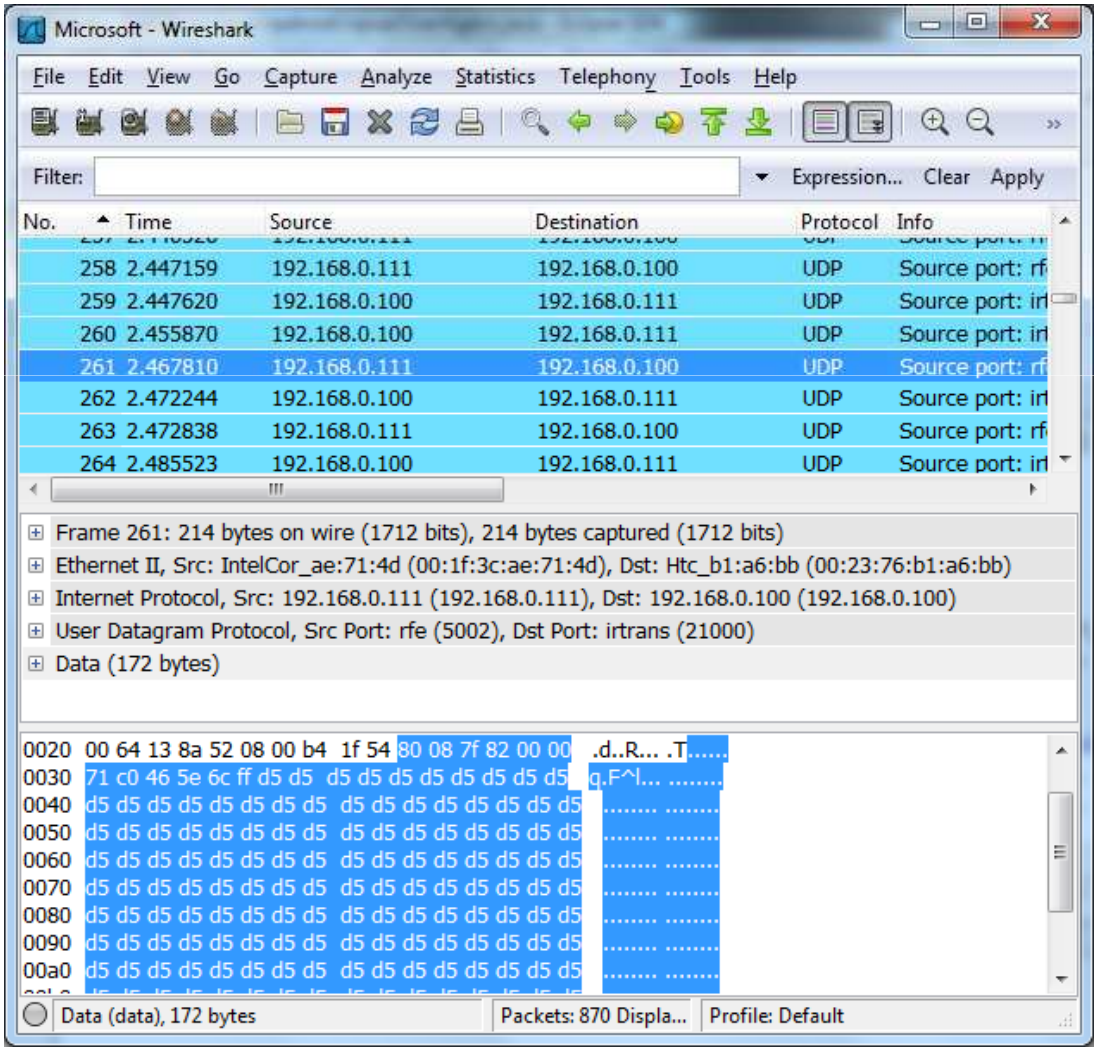
Implementação

- Provê suporte a retrocompatibilidade
  - Softphones que utilizem a versão 1.2 são compatíveis com a versão 1.1
- Definidas interfaces genéricas, que permitam futuras evoluções da biblioteca ZRTP4J

Dados sem criptografia

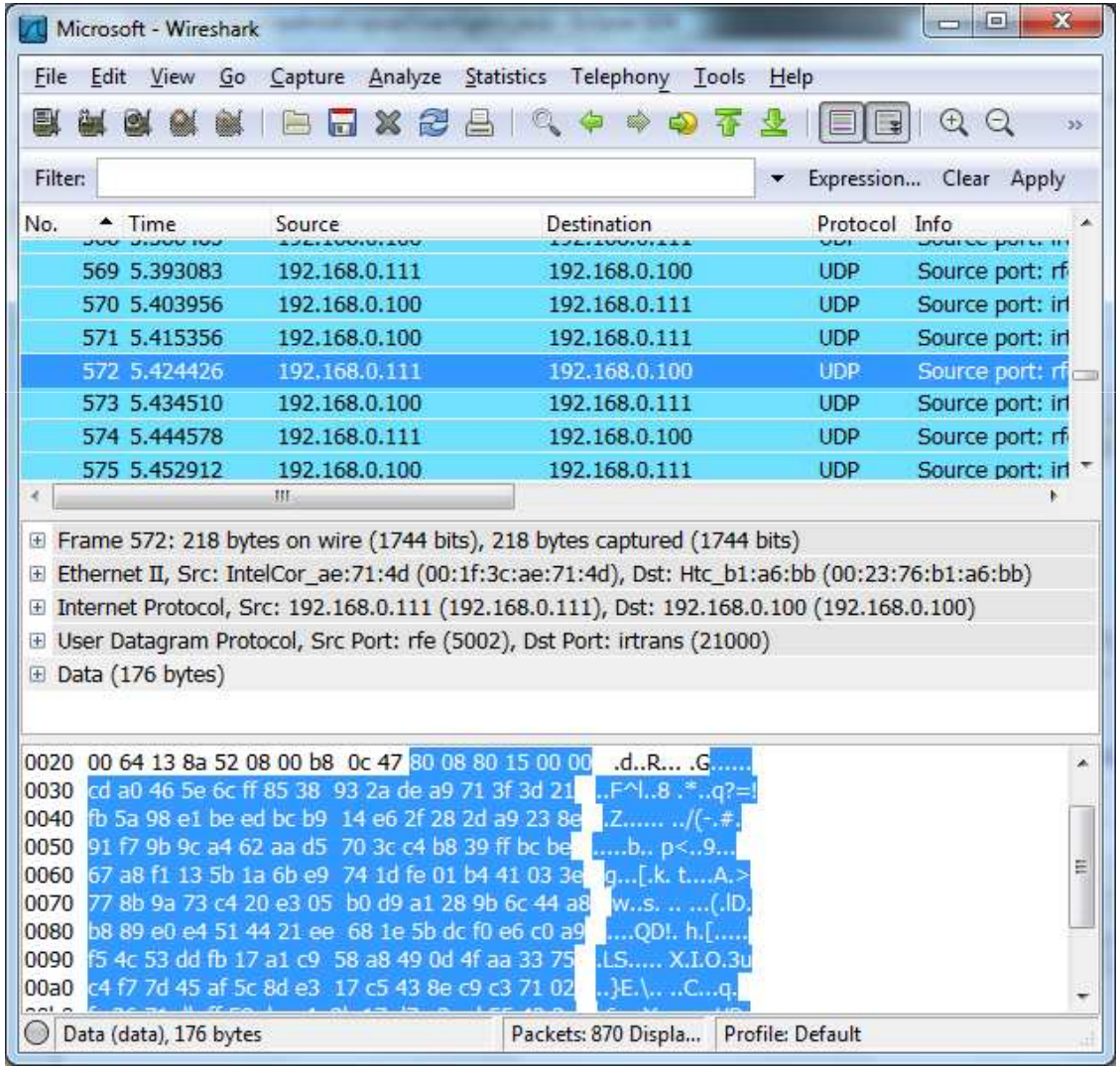


Dados sem criptografia



Dados criptografados

Dados criptografados



Resultados e discussão

- Troca de chaves ocorre da maneira esperada
- Foi permitido que haja interoperabilidade entre as versões
  - Ao detectar que a versão da outra parte é inferior, é utilizada a versão 1.1 da biblioteca ZRTP4J

Conclusão

- Resultados acima do esperado
  - Proporciona comunicação segura sem a presença de um terceiro confiável
  - Permite a utilização do algoritmo ECDH, que proporciona tamanhos de chaves significativamente menores
- Plataforma Android se mostrou estável, porém em cenários de *real-time* é impossível utilizar o seu emulador

Extensões

- Alterar a interface do SipDroid, para que haja o armazenamento das SAS
- Alterar a biblioteca ZRTP4J, simplificando o seu uso fora do framework JMF
- Alterar o comunicador SIP Communicator, para ele suporte a versão 1.2 da ZRTP4J
- Permitir a utilização de outros algoritmos para a geração de números pseudo-aleatórios

Obrigado!