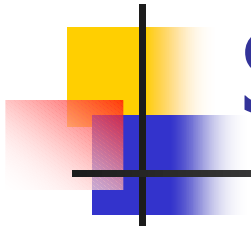
# PROTÓTIPO DE SOFTWARE PARA EMISSÃO DE CERTIFICADOS DIGITAIS PARA OBJETOS DISTIBUÍDOS

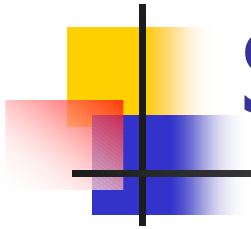
Acadêmico: Derlei Alvaro Mathias

Orientador: Paulo Fernando da Silva



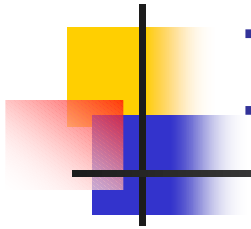
# Sumário

- Introdução
- Objetivos do Trabalho
- Conceitos Básicos
- Trabalhos Correlatos
- Requisitos Principais



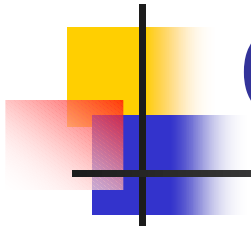
# Sumário

- Especificação
- Implementação
- Resultados e Discussão
- Conclusão
- Extensões



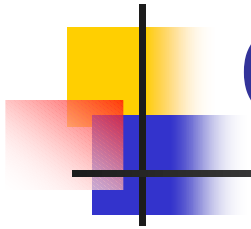
# Introdução

- *Middleware* com funcionalidades de uma AC
- Atender as requisições dos objetos distribuídos, gerenciar a emissão, a validade e a revogação dos certificados digitais



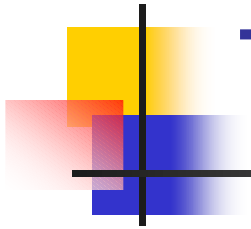
# Objetivos

- Gerar certificados digitais seguindo o padrão X.509
- Atender requisições dos objetos distribuídos
- Revogar certificados digitais
- Gerar lista de certificados revogados



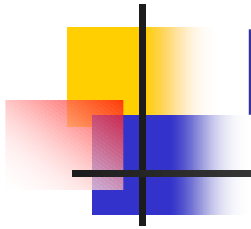
# Conceitos Básicos

- Criptografia de chaves públicas
- Certificado X.509
- Objeto distribuído
- Java RMI



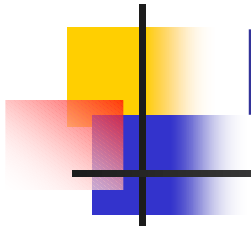
# Trabalhos Correlatos

- Um novo modelo de infra-estrutura de chaves públicas para uso no Brasil
- Metodologia para análise de segurança aplicada em uma infra-estrutura de chave pública
- Recuperação distribuída de imagens por similaridade



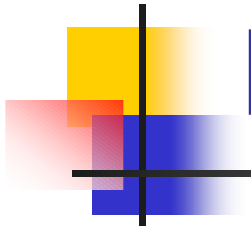
# Requisitos Principais

- Gerar par de chaves - RF
- Emitir certificados digitais auto-assinados - RF
- Emitir certificados para os objetos remotos - RF
- Permitir a comunicação entre objetos remotos - RF



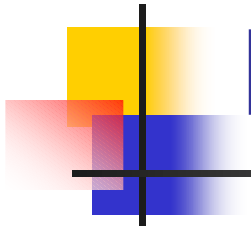
# Requisitos Principais

- Revogar certificado do objeto remoto - RF
- Manter lista dos certificados revogados - RF
- Implementado utilizando Java 5 - RNF
- Compatível com sistema operacional Windows 2000 e XP - RNF



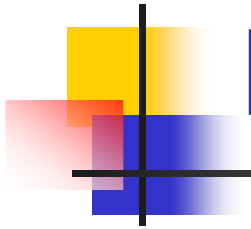
# Especificação

- Técnicas e Ferramentas Utilizadas
- UML
- Enterprise Architect 6.0



# Especificação

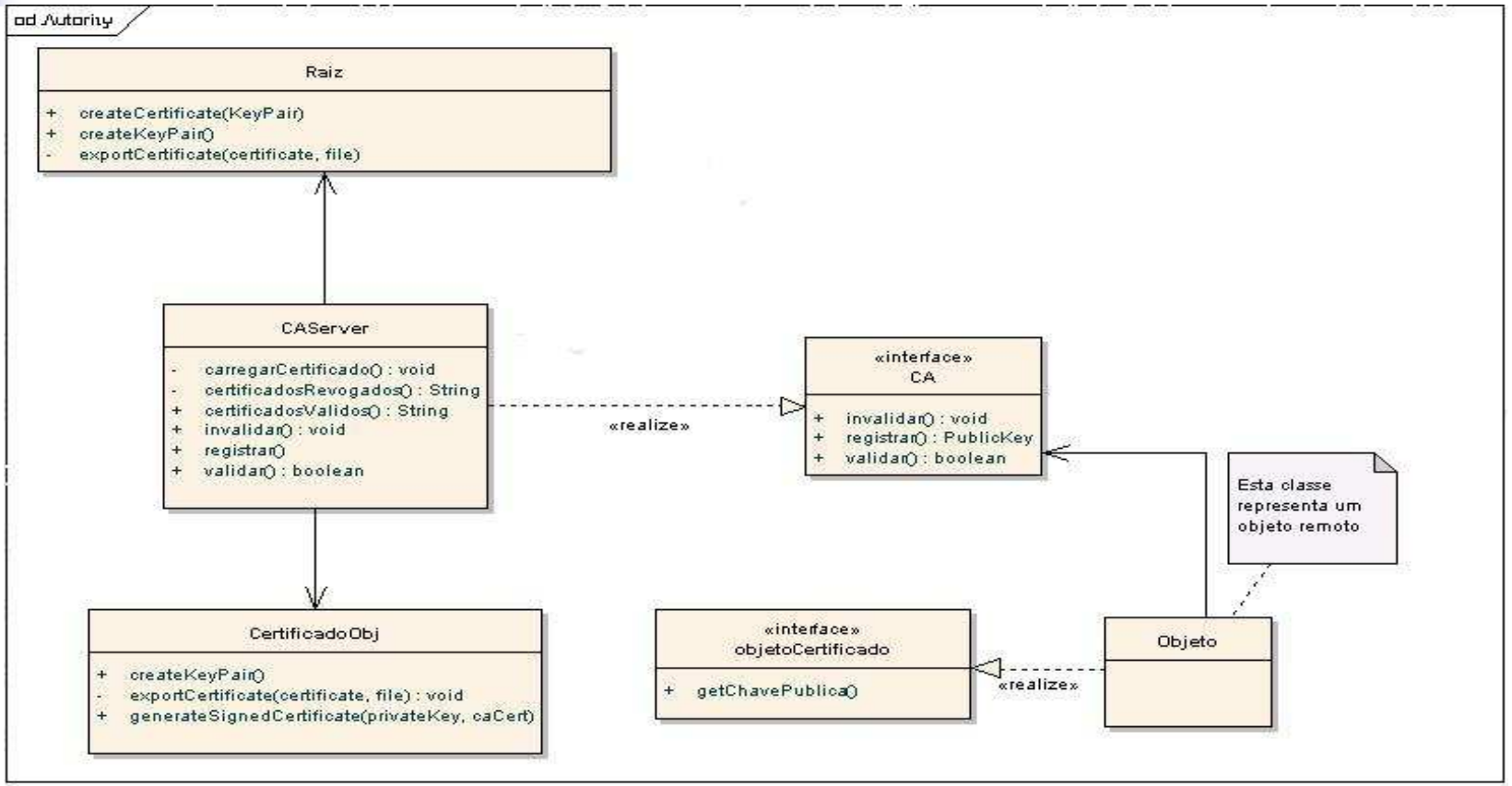
- A especificação será demonstrada através de diagrama de classes e diagramas de seqüência



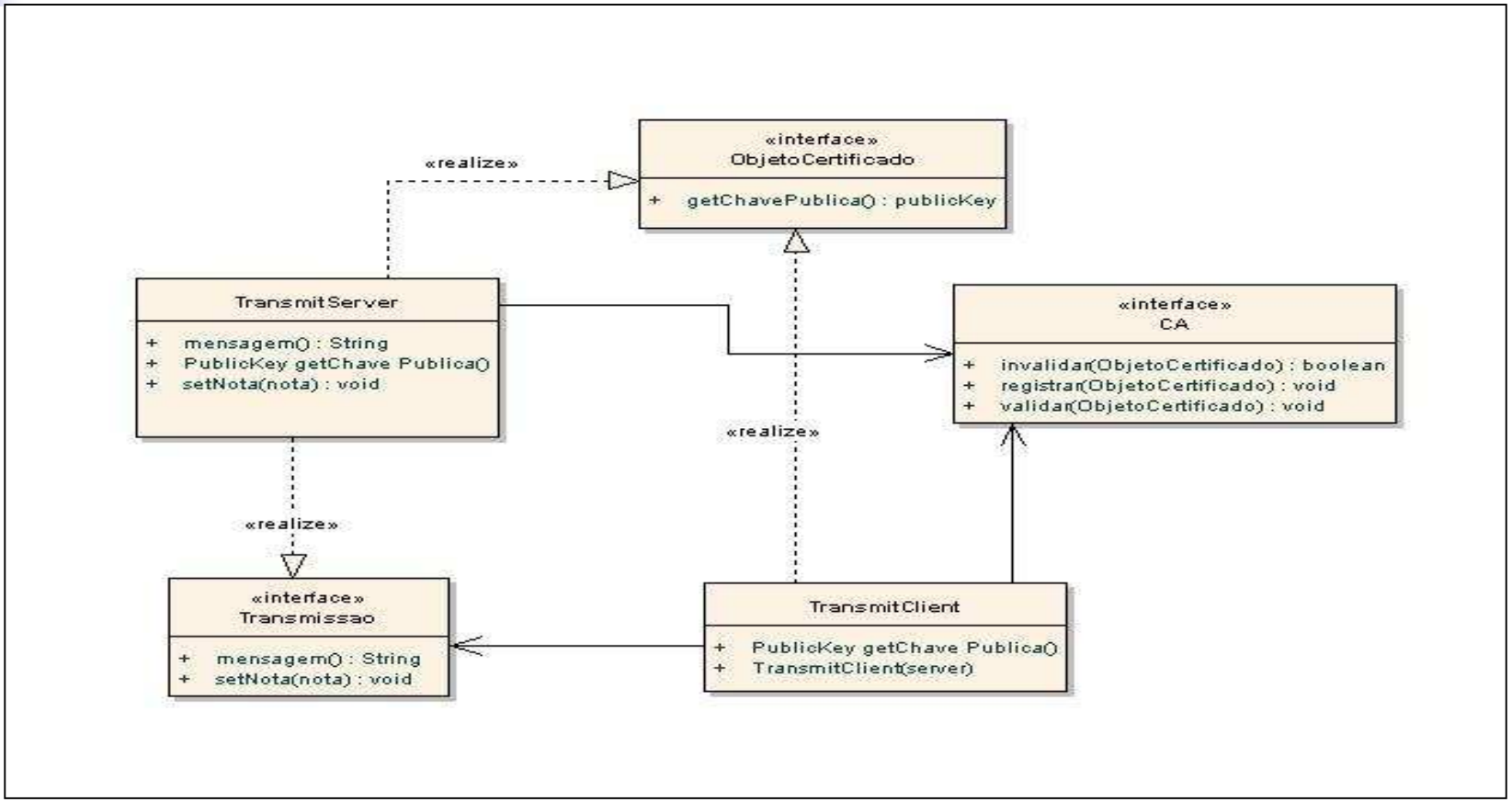
# Especificação

- Diagrama de classe middleware
- Diagrama de classe estudo de caso

# Diagrama de classe Middleware



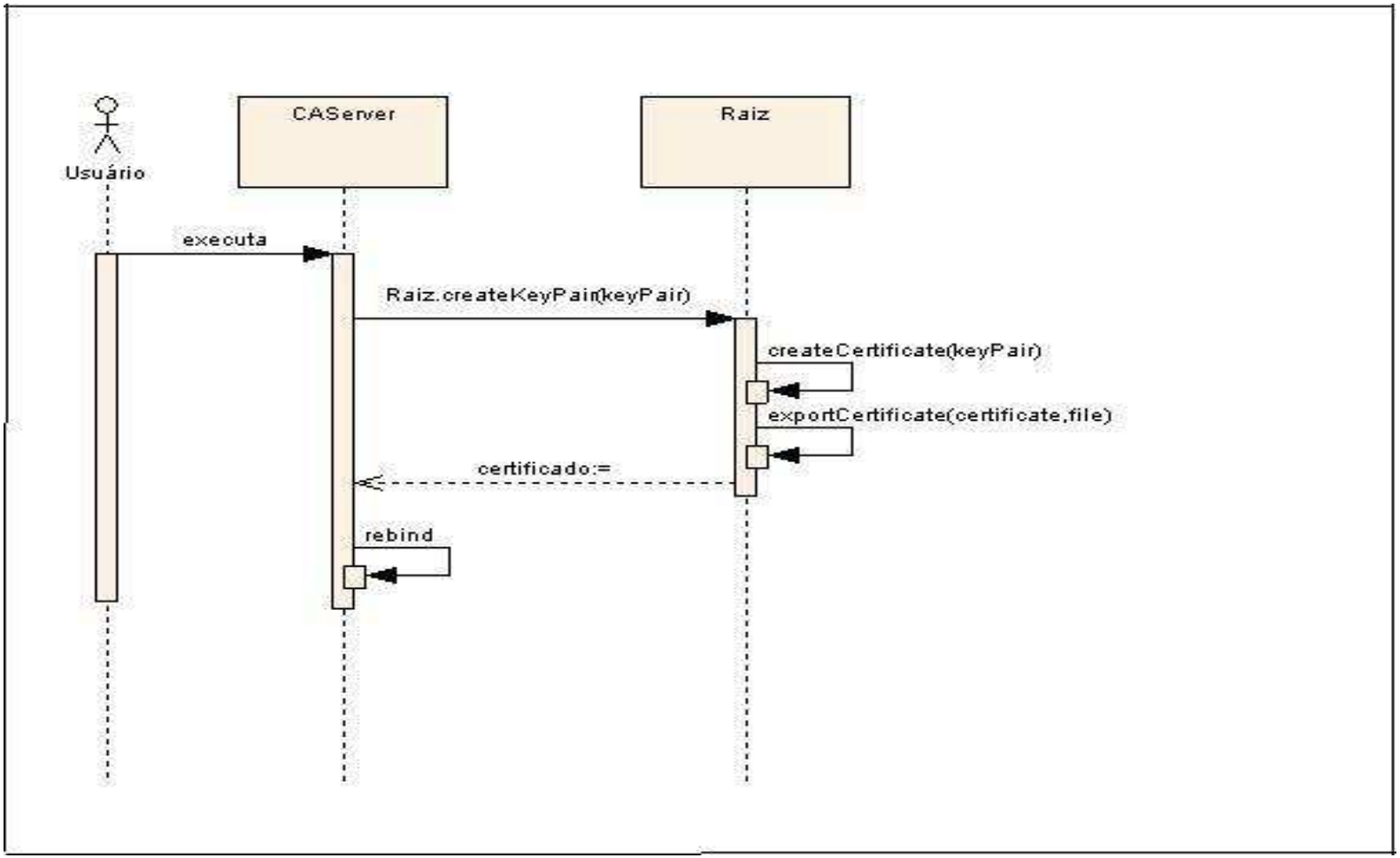
# Diagrama de Classe Estudo de Caso



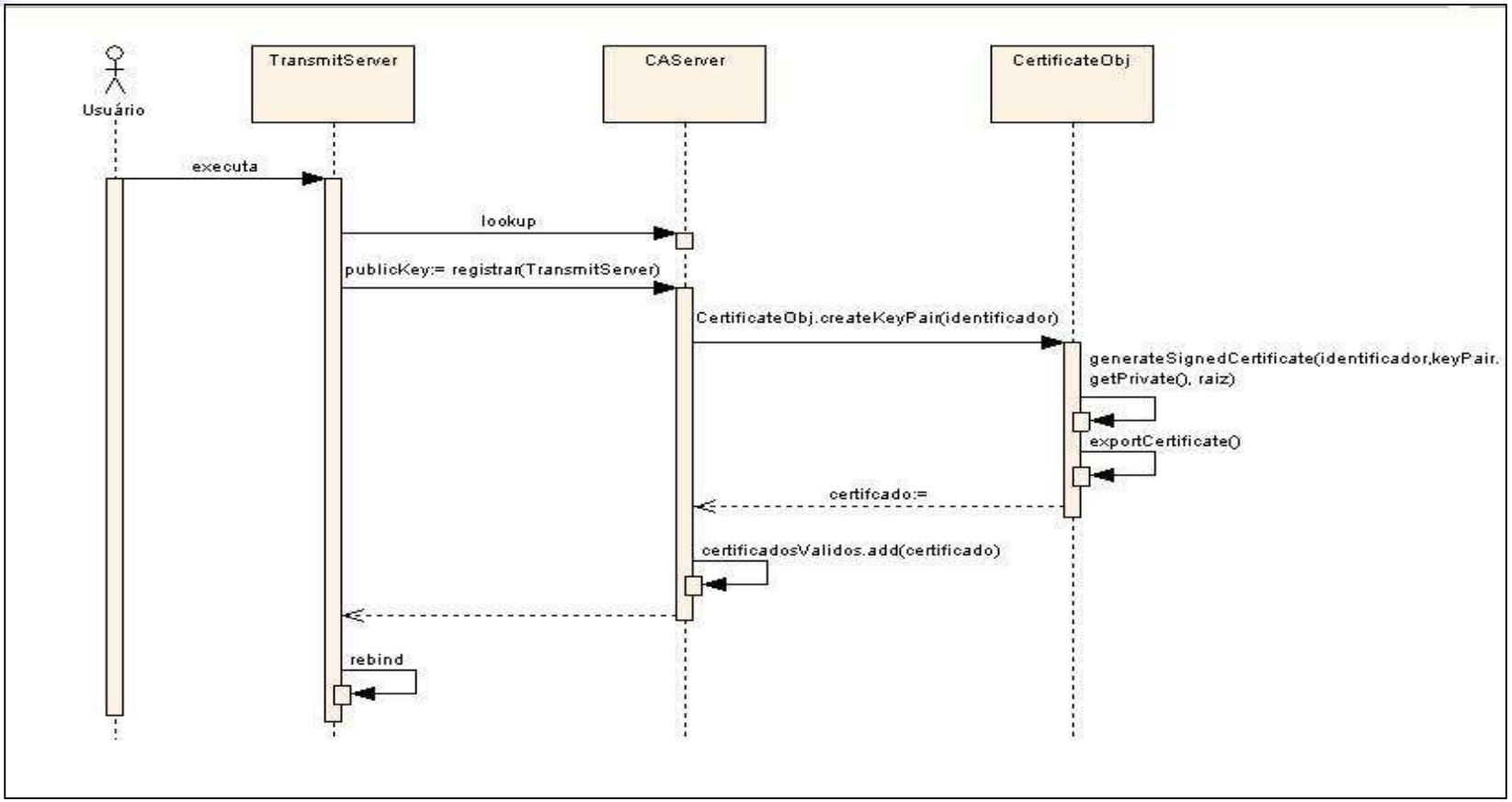
# Diagrama de Seqüência

- CAServer
- TransmitServer
- TransmitClient

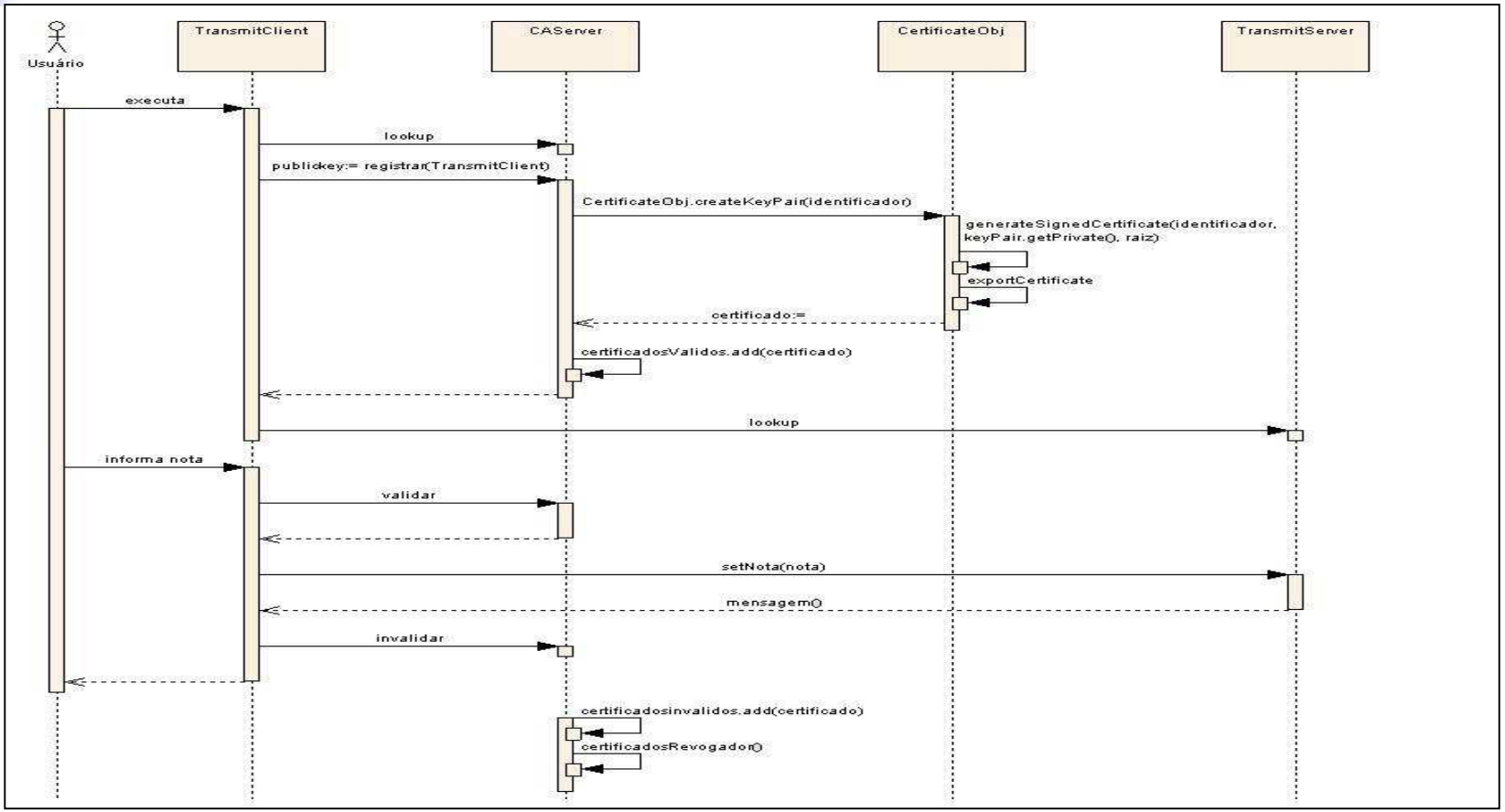
# Diagrama de Seqüência CAServer

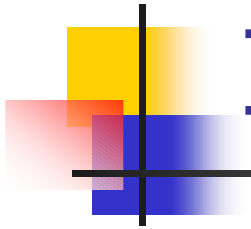


# Diagrama de Seqüência TransmitServer



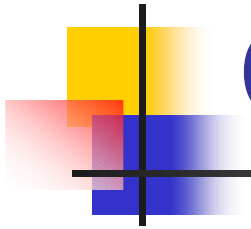
# Diagrama de Seqüência TransmitClient





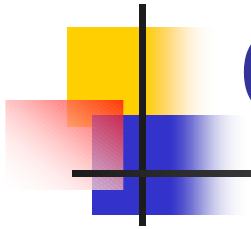
# Implementação

- Ferramentas Utilizadas
- Java 5
- API *Bouncy Castle*
- Eclipse 3.2



# Operacionalidade

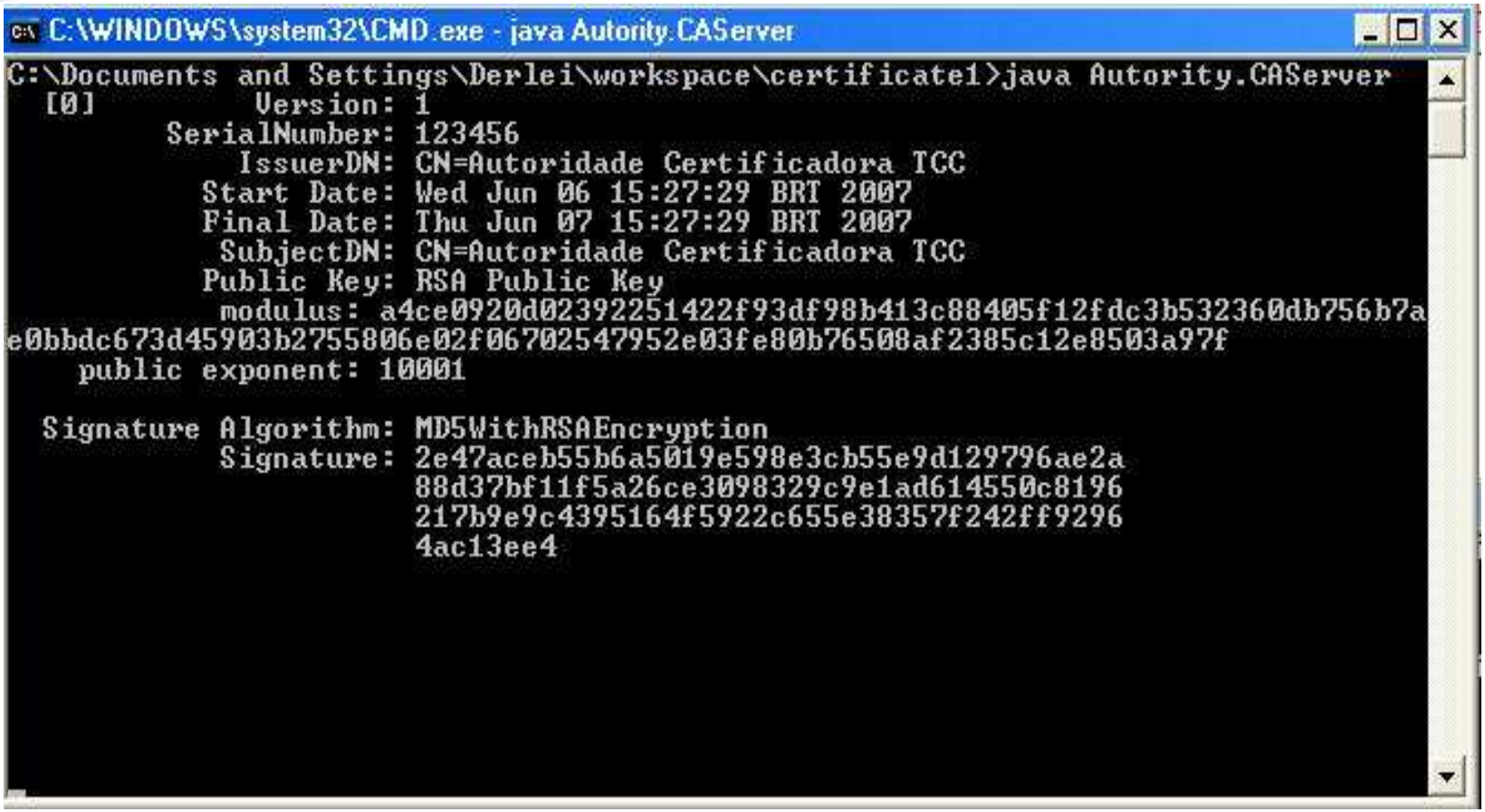
- No protótipo especificado simula o lançamento das notas de acadêmicos.

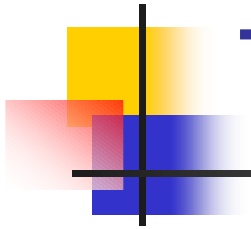


# CAServer

- Gera par de chaves
- Emite o certificado digital da raiz
- Registra servidor

# CAServer

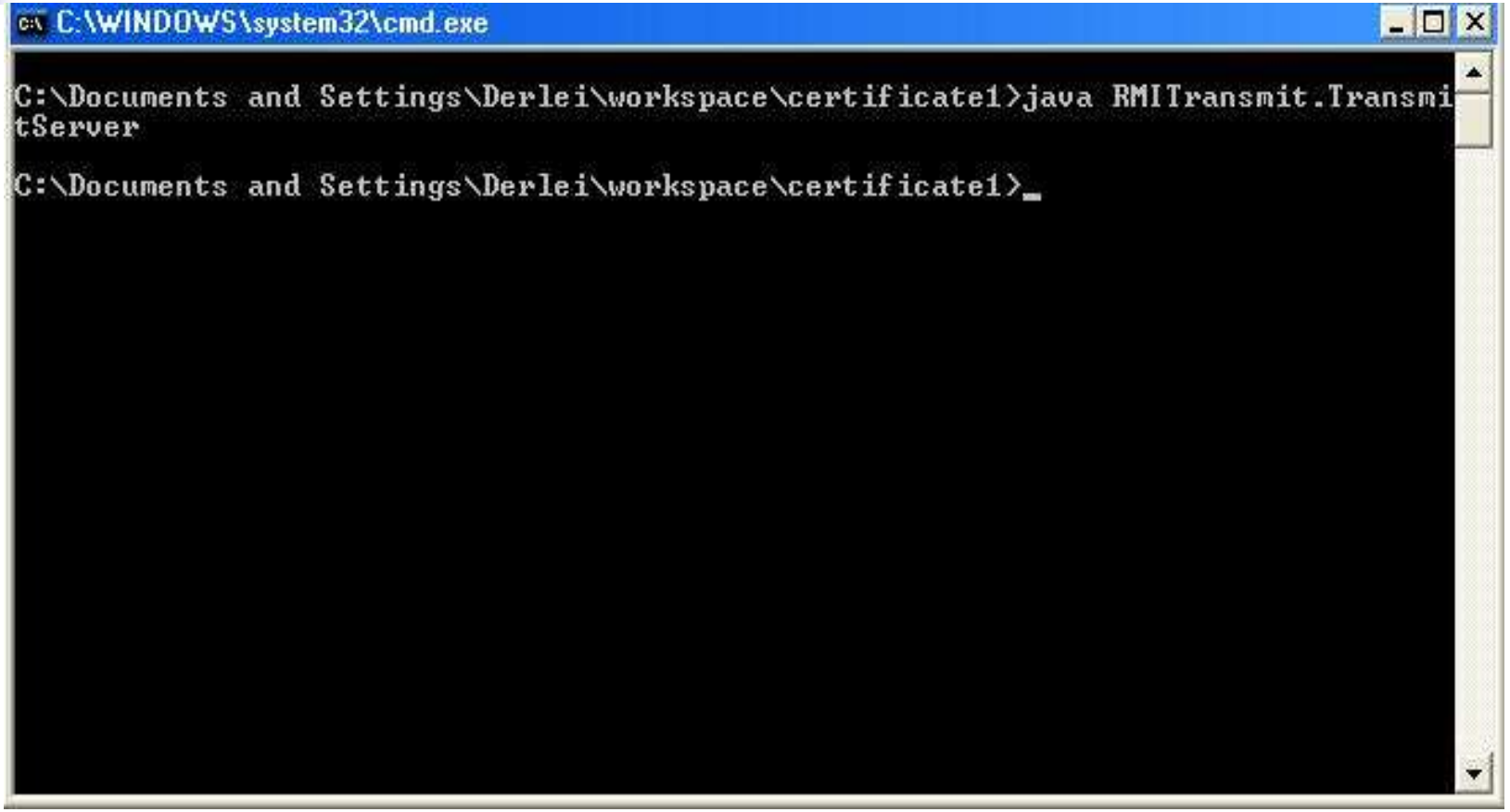

C:\WINDOWS\system32\CMD.exe - java Autority.CAServer
C:\Documents and Settings\Derlei\workspace\certificate1>java Autority.CAServer
[0] Version: 1
SerialNumber: 123456
IssuerDN: CN=Autoridade Certificadora TCC
Start Date: Wed Jun 06 15:27:29 BRT 2007
Final Date: Thu Jun 07 15:27:29 BRT 2007
SubjectDN: CN=Autoridade Certificadora TCC
Public Key: RSA Public Key
modulus: a4ce0920d02392251422f93df98b413c88405f12fdc3b532360db756b7a
e0bbdc673d45903b2755806e02f06702547952e03fe80b76508af2385c12e8503a97f
public exponent: 10001
Signature Algorithm: MD5WithRSAEncryption
Signature: 2e47aceb55b6a5019e598e3cb55e9d129796ae2a
88d37bf11f5a26ce3098329c9e1ad614550c8196
217b9e9c4395164f5922c655e38357f242ff9296
4ac13ee4

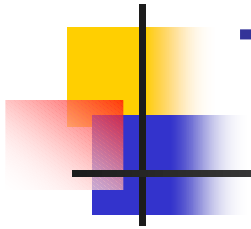


# TransmitServer

- Obtém referência do servidor CAServer
- Solicita certificado digital
- Registra servidor remoto

# TransmitServer

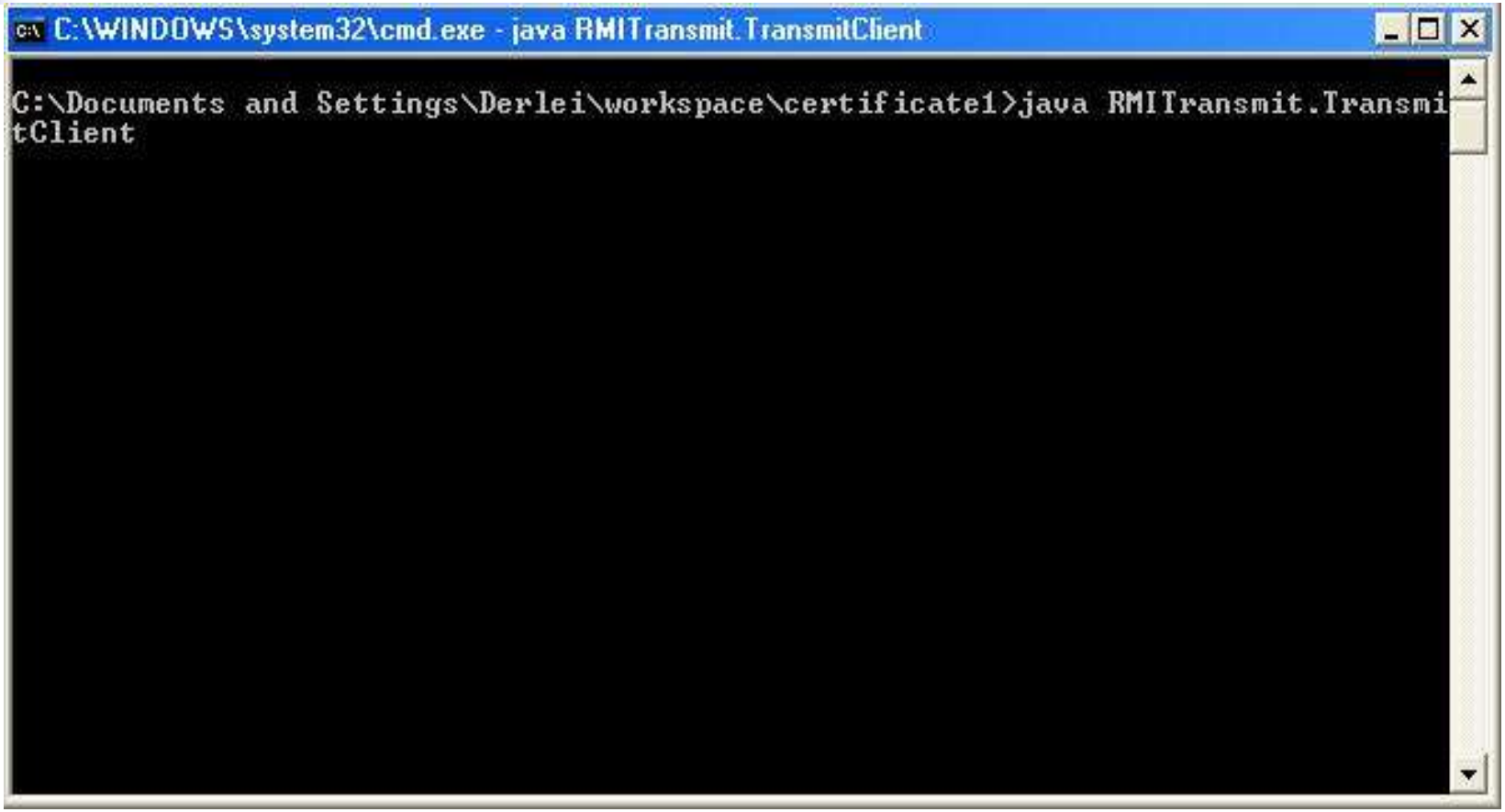


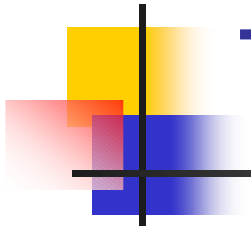


# TransmitClient

- Obtém referência do servidor CAServer
- Solicita e optem o certificado digital
- Obtém referência do servidor remoto

# TransmitClient

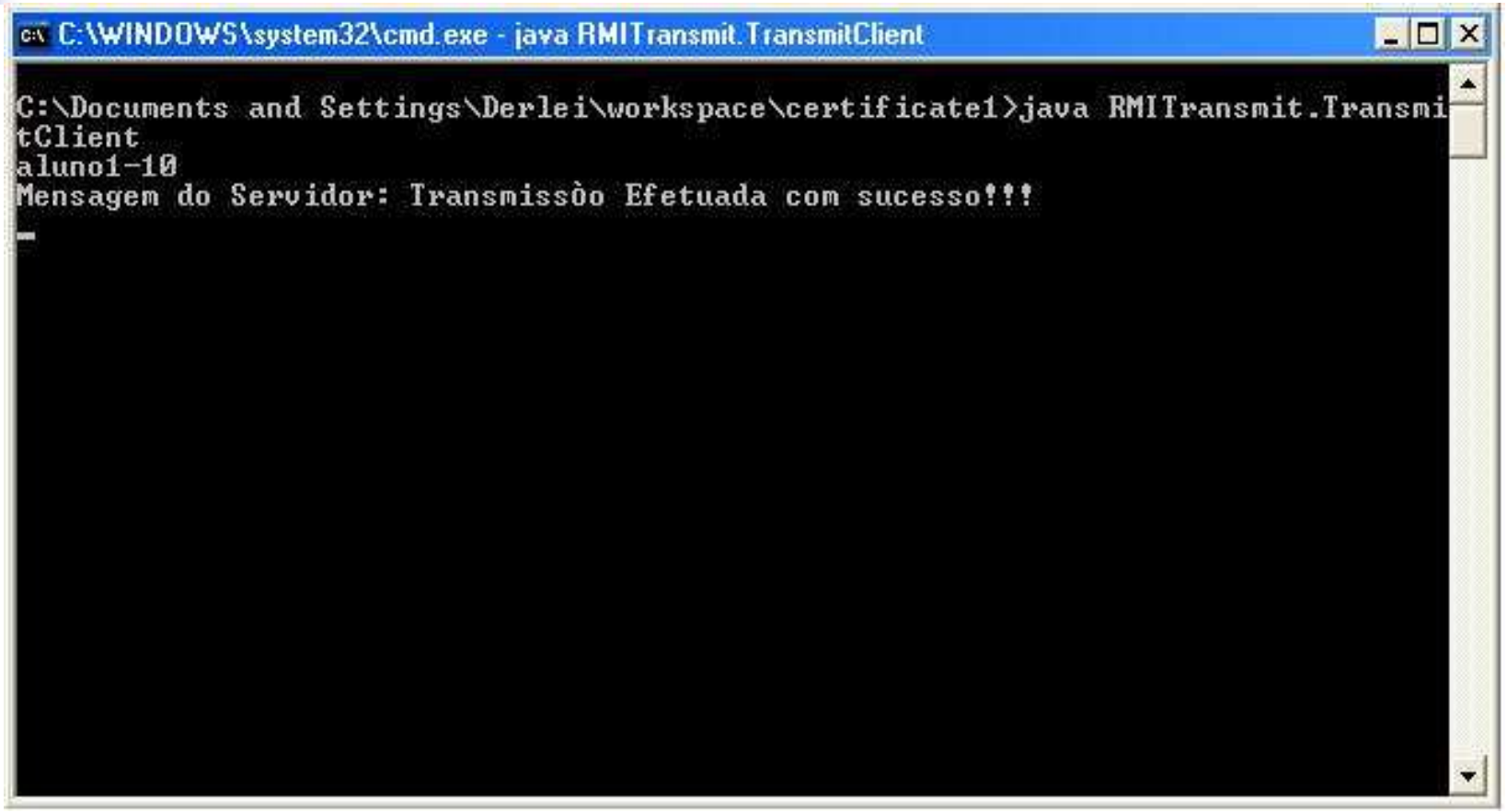




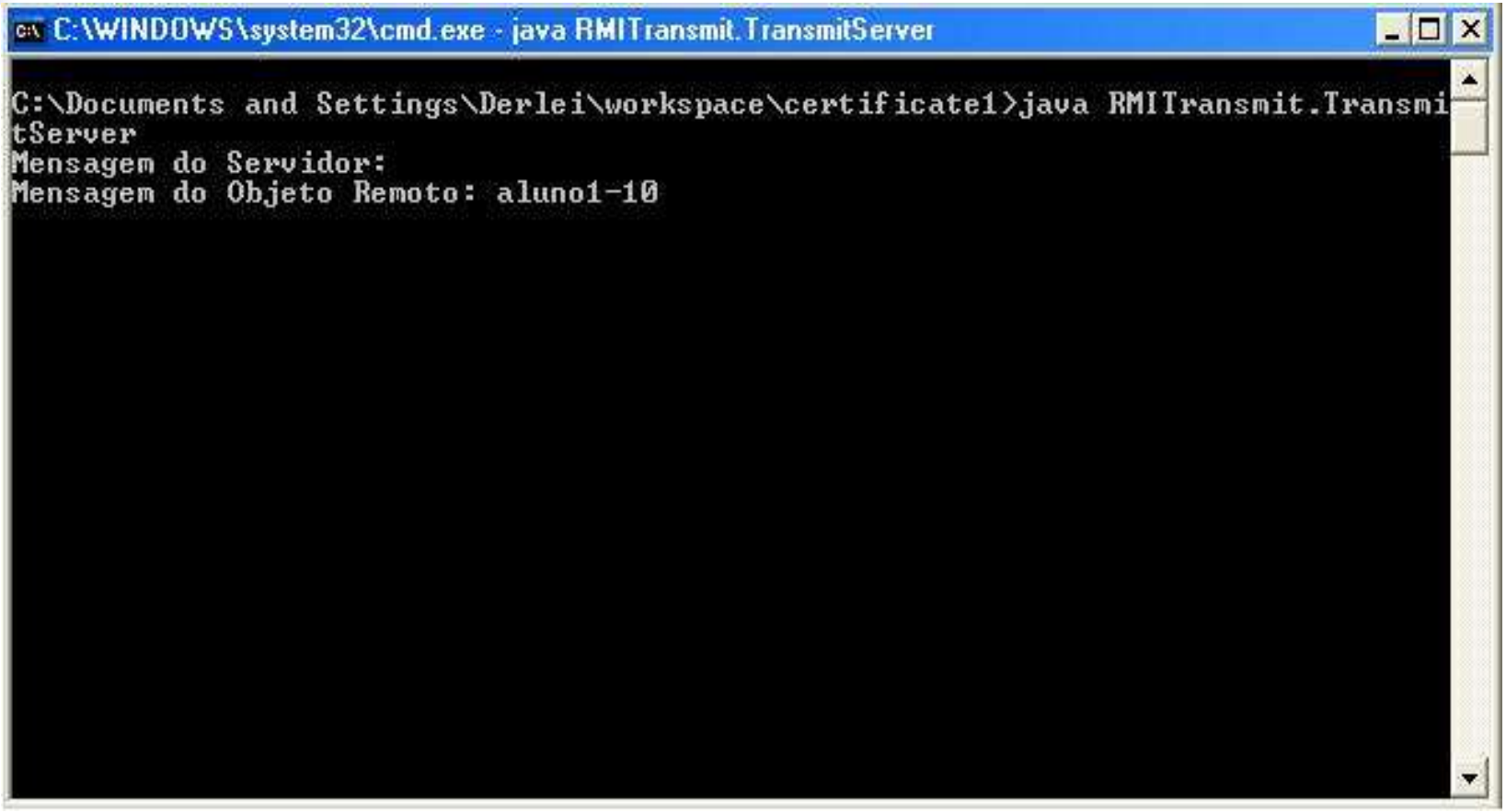
# Troca de Mensagens

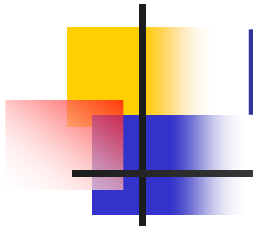
- Servidores rodando
- Certificados emitidos
- Troca de mensagens

# TransmitClient Mensagem



# TransmitServer Mensagem

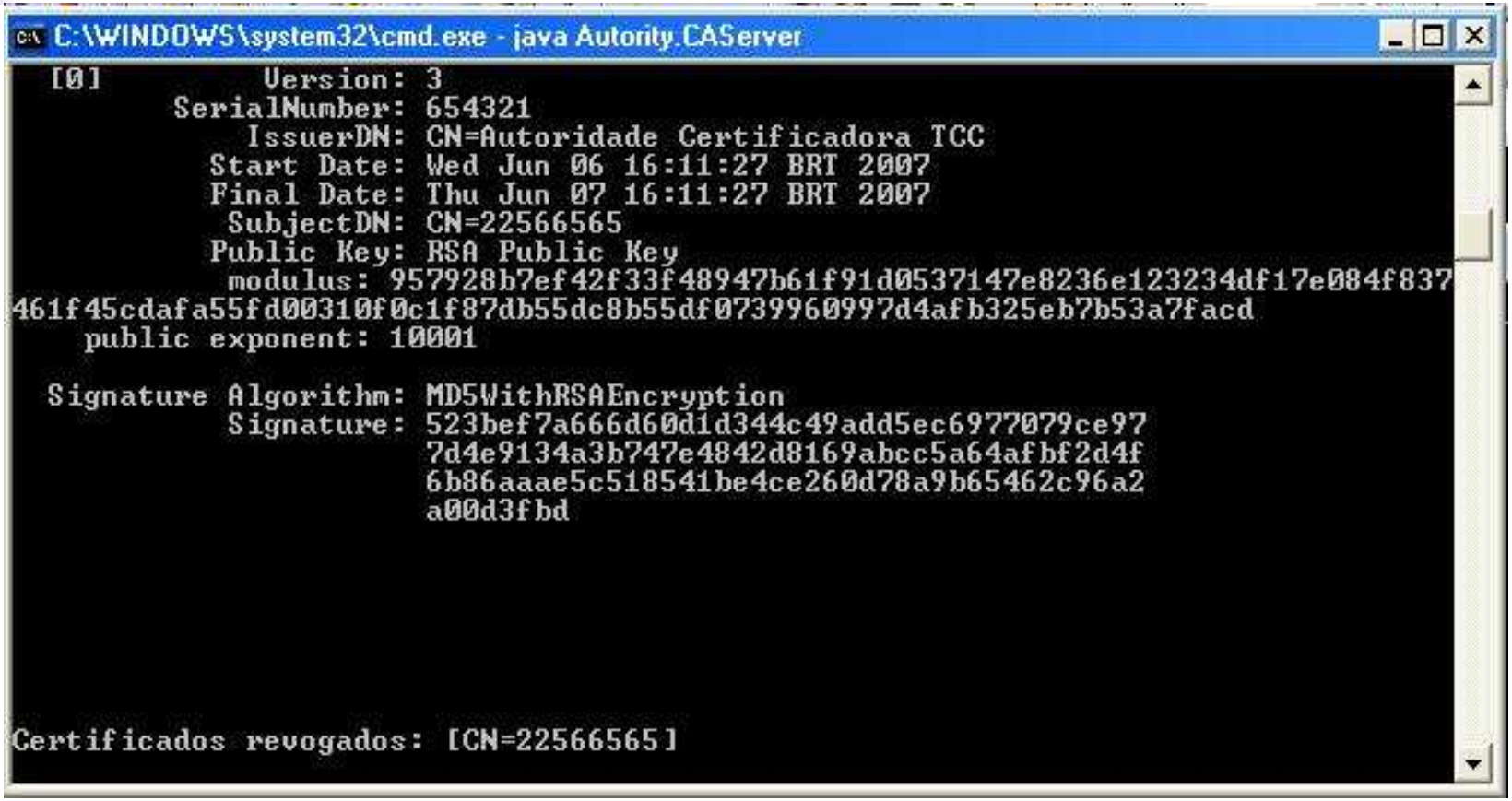




# Revogação

- Solicitação de revogação
- Lista de certificados revogados

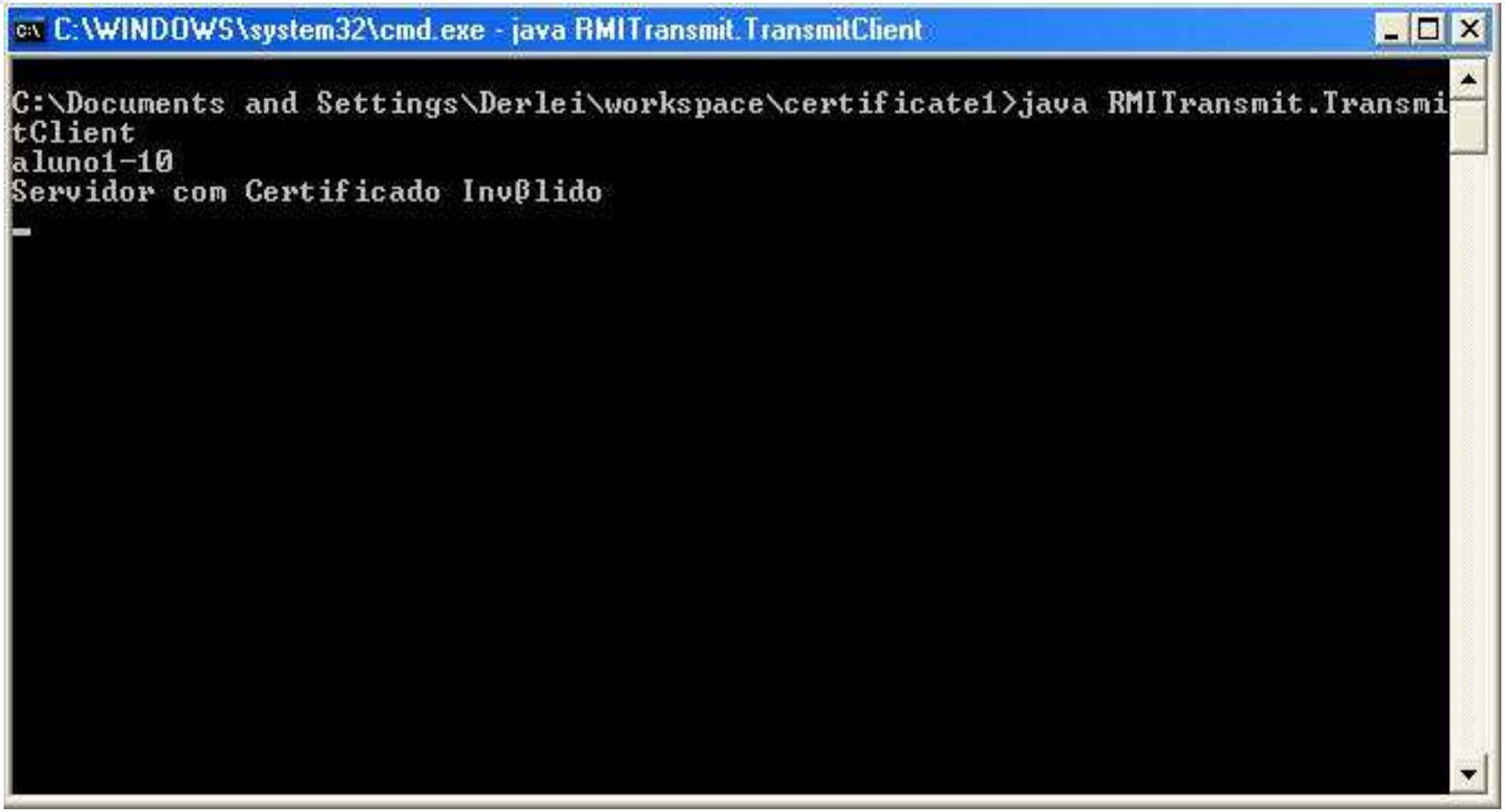
# Revogação

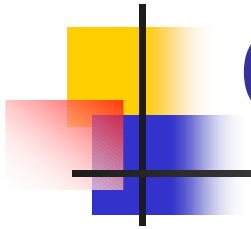

C:\WINDOWS\system32\cmd.exe - java Autority.CAServer
[0] Version: 3
SerialNumber: 654321
IssuerDN: CN=Autoridade Certificadora TCC
Start Date: Wed Jun 06 16:11:27 BRT 2007
Final Date: Thu Jun 07 16:11:27 BRT 2007
SubjectDN: CN=22566565
Public Key: RSA Public Key
modulus: 957928b7ef42f33f48947b61f91d0537147e8236e123234df17e084f837
461f45cdafa55fd00310f0c1f87db55dc8b55df0739960997d4afb325eb7b53a7facd
public exponent: 10001
Signature Algorithm: MD5WithRSAEncryption
Signature: 523bef7a666d60d1d344c49add5ec6977079ce97
7d4e9134a3b747e4842d8169abcc5a64afbf2d4f
6b86aaae5c518541be4ce260d78a9b65462c96a2
a00d3fbd
Certificados revogados: [CN=22566565]

# Resultados e Discussão

- Como neste protótipo não teve como objetivo de utilizar o certificado digital de forma a criar um canal seguro entre cliente e servidor, sendo a única persistência feita na transmissão remota é verificar se o certificado está válido

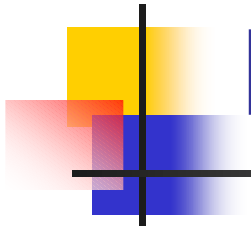
# Resultados e Discussão





# Conclusão

- Algoritmo RSA
- API *Bouncy Castle*
- Os objetivos foram atendidos



# Extensões

- Estabelecer canal seguro entre objetos distribuídos
- Criar AR
- Desenvolver certificação cruzada