Protótipo de software para envio de mensagens criptografadas para um dispositivo móvel utilizando a plataforma .NET

Acadêmico: Robson Ramos
Orientador: Prof. Francisco Adell Péricas

Roteiro de Apresentação

- Introdução
- Fundamentação Teórica
- Especificação
- Implementação
- Operacionalidade da implementação
- Resultado e Discussão
- Conclusões finais

Introdução

- Tomadas de decisões
- Oportunidades de Negócios
- Softwares para celulares

Objetivos do Trabalho

- Desenvolver um protótipo de um software para transmissão de mensagens criptografadas para dispositivos móveis (celular) de forma segura

Fundamentação Teórica

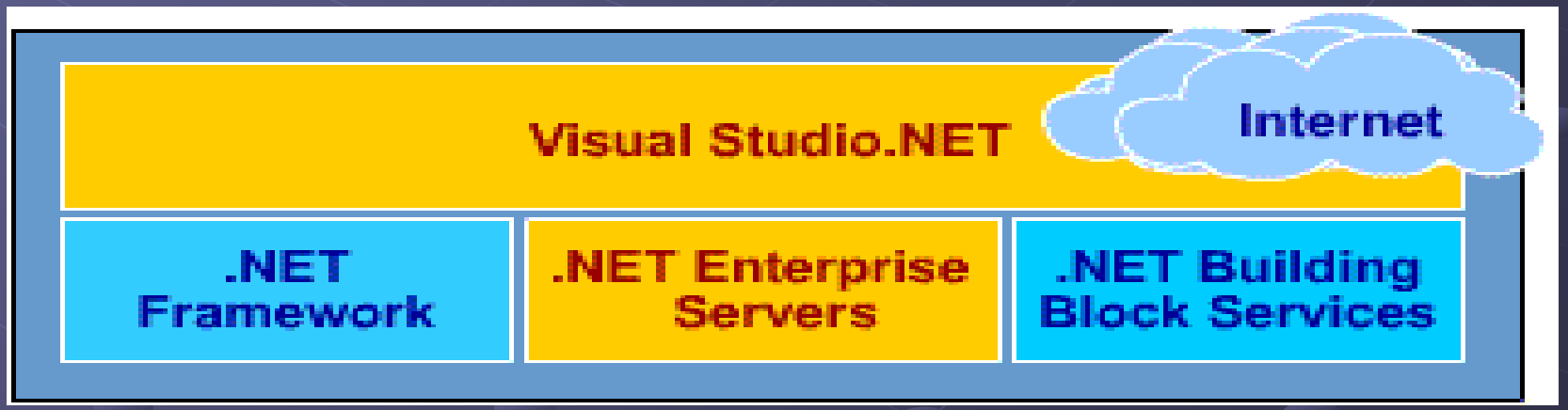
- Dispositivos Móveis
  - Smartphone
- .NET
  - Microsoft .NET
  - .NET Framework / .NET Compact Framework
  - Windows para SmartPhone
  - Criptografia

SmartPhone

- O que é SmartPhone?
- Perspectivas para o futuro

Microsoft .NET

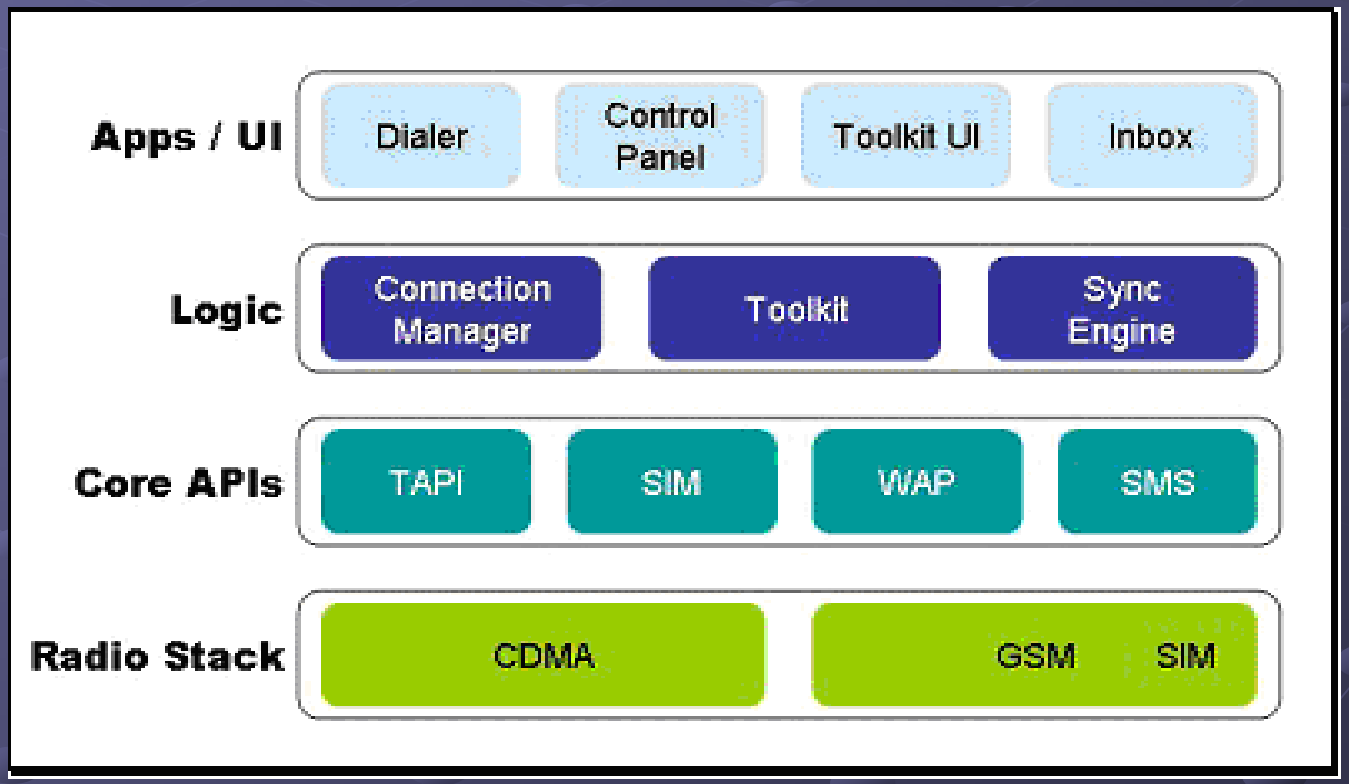
- Plataforma .Net
- Independência de linguagem e sistema operacional
- Estrutura da Plataforma .NET



.NET Framework / .NET Compact Framework

Windows para Smartphone

- Windows CE 3.0
- Arquitetura do Windows Smartphone



Criptografia

- Proteção dos dados
- Tipos de Criptografia:
  - Criptografia por chave secreta ou simétrica
  - Criptografia por chave pública ou assimétrica

Trabalhos Correlatos

Acadêmicos Itens	Este Trabalho	Santos (2003)	Depiné (2002)	Schaefer (2004)
Plataforma de desenvolvimento	.NET	.NET	JAVA	JAVA
Linguagem de programação	Visual Basic .NET	C#	JAVA (J2ME)	JAVA(J2ME)
Dispositivo Móvel	SmartPhone	PDA	Celular convencional	Celular convencional
Acesso a Web	Sim	Sim	Não	Sim
Criptografia	Sim	Não	Não	Não
Objetivo principal do trabalho	Segurança na transmissão de mensagens para dispositivos móveis através de criptografia	Visualizar notícias da *Web* através de um PDA	Realizar cálculos de tempo e deslocamento necessários em um Rally	Coletar Informações e envia-lás pra um *desktop* para futura análise dos dados

Requisitos do Smartphone

- Verificar se o colaborador está cadastrado na empresa através do *Web Service*
- Receber as mensagens enviadas pelo *Web Service*
- Decriptografar as mensagens
- Mostrar para o usuário as mensagens decriptografadas
- Permitir o cadastramento da chave secreta

Requisitos do Desktop

- Permitir o cadastramento do colaborador com a sua devida chave secreta
- Permitir o cadastramento do usuário do sistema
- Mostrar as mensagens cadastradas
- Permitir a inclusão das mensagens

Especificação

- Análise estruturada contendo:
  - Lista de eventos
  - Diagrama de contexto
  - Diagramas de fluxo de dados (DFDs)
  - Modelo Entidade-Relacionamento (MER) lógico

Lista de Eventos

Lista de Eventos do software do desktop

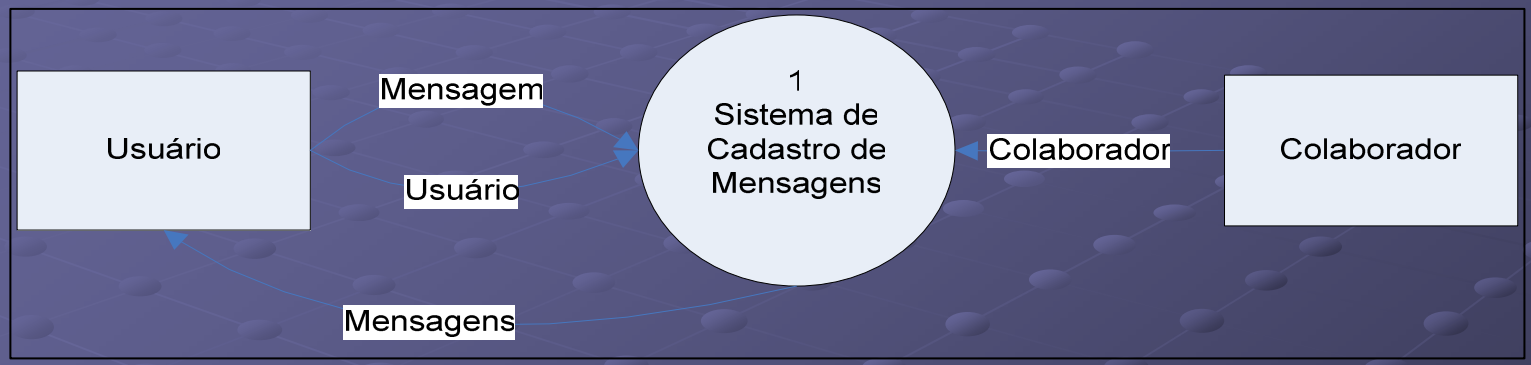
Nº	Nome do Evento
1	Usuário é cadastrado
2	Colaborador é cadastrado
3	Mensagem é cadastrada para o colaborador
4	Sistema mostra mensagens

Lista de Eventos do software do dispositivo móvel

Nº	Nome do Evento
1	Chave secreta é cadastrada
2	Colaborador é validado
3	Mensagem recebida do Web Service
4	É momento de decriptografar a mensagem
5	É momento de mostrar a mensagem ao colaborador

Diagrama de Contexto

- Diagrama de contexto do desktop



- Diagrama de contexto do dispositivo móvel

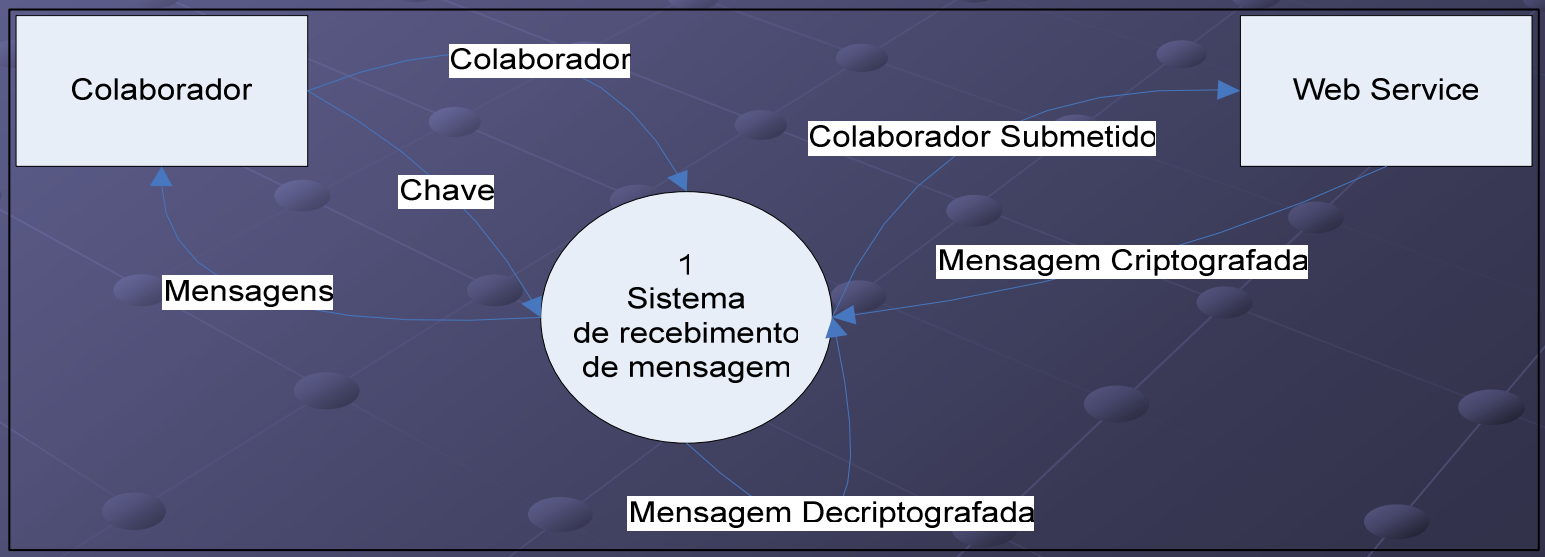
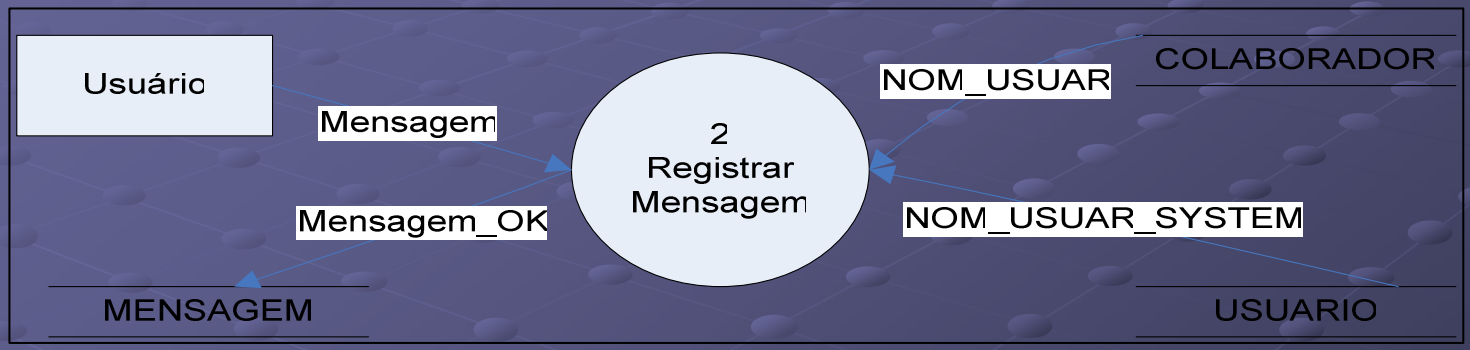
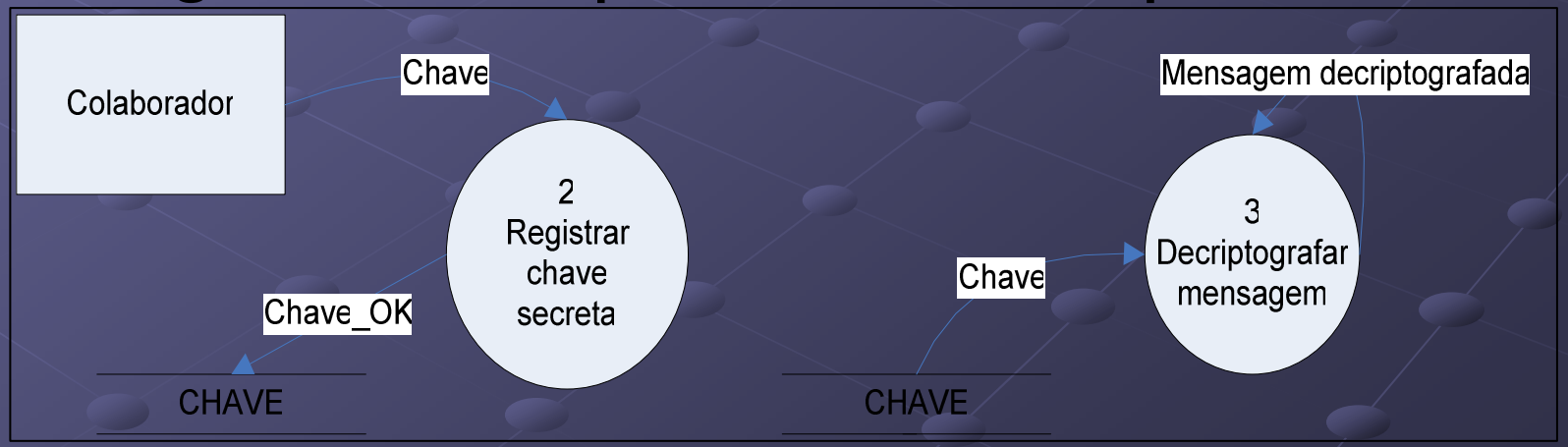


Diagrama de Fluxo de Dados (DFD)

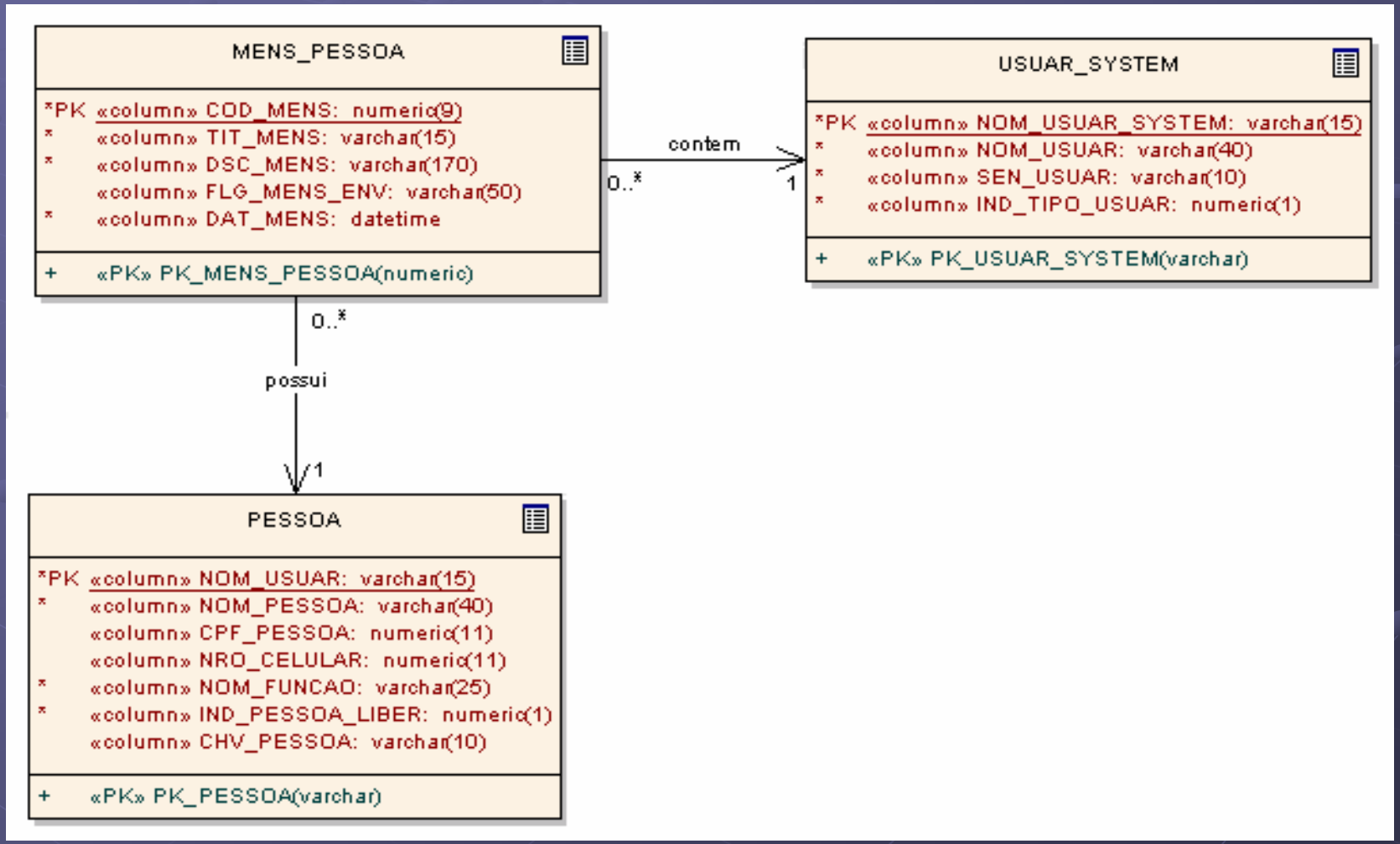
- Diagrama do aplicativo do desktop



- Diagrama do aplicativo do dispositivo móvel



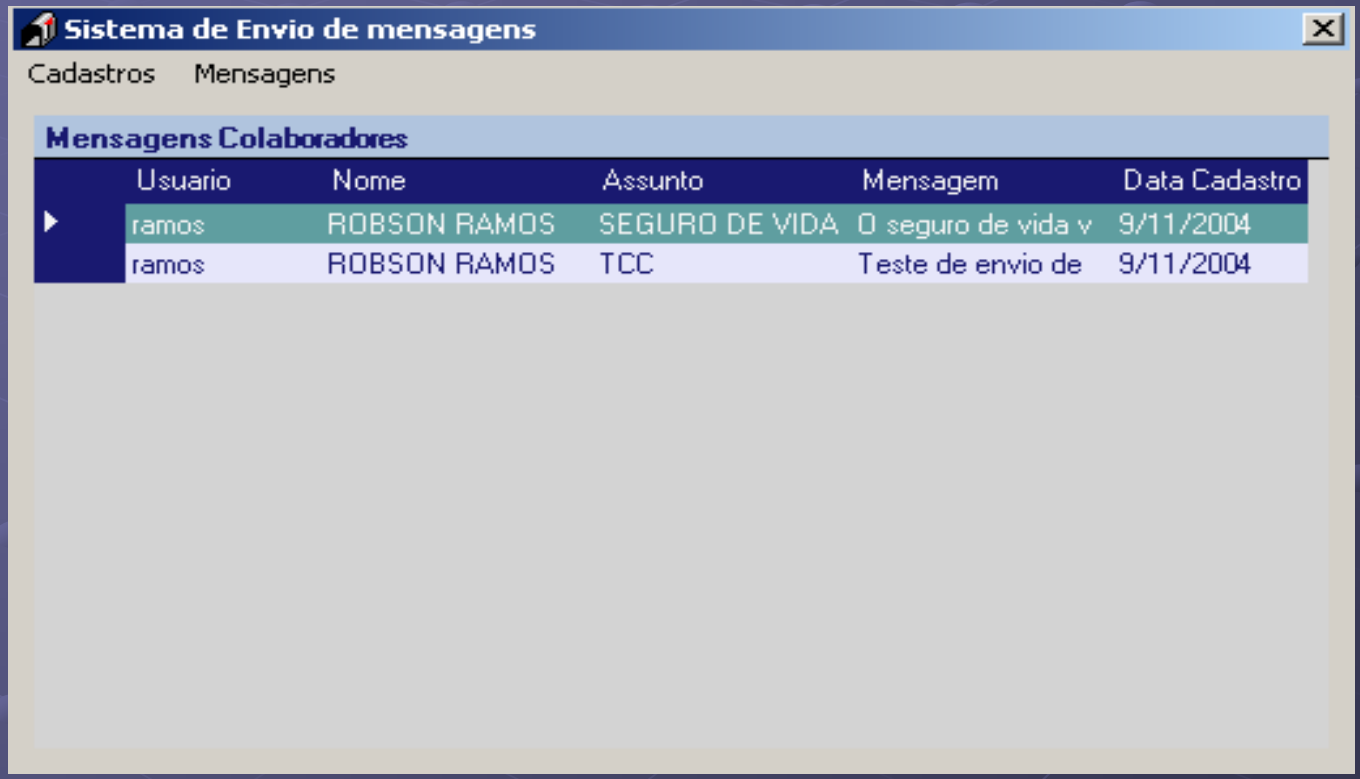
MODELO ENTIDADE RELACIONAMENTO



Implementação

- Ferramenta de desenvolvimento Visual Studio .NET 2003
- Linguagem de programação Visual Basic .NET
- Emulador Microsoft SmartPhone 2003
- Banco de dados Microsoft SQL Server
- Algoritmo de criptografia BlowFish

Operacionalidade da implementação



Operacionalidade da implementação

Resultados e Discussão

- Foi atingido o objetivo de transmitir mensagens do desktop para o dispositivo móvel de modo sigiloso
- O meio de envio da mensagem foi alterado de SMS para Web Service
- A resposta do Web Service a primeira solicitação é mais lenta em relação as requisições posteriores

Conclusões finais

- Tendência do mercado
- Plataforma .NET
- Inexistência de criptografia Nativa no .NET Compact Framework
- Integração das novas tecnologias

Extensões

- Maior iteração entre o usuário e a empresa
- Desenvolver o protótipo utilizando criptografia por chave pública através de um mecanismo de autenticação.