UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

FELIPE CORAL SASSO

UTILIZANDO CERTIFICAÇÃO DIGITAL NA PLATAFORMA ANDROID POR MEIO DO DESENVOLVIMENTO DE UMA APLICAÇÃO

CRICIÚMA

2012

FELIPE CORAL SASSO

UTILIZANDO CERTIFICAÇÃO DIGITAL NA PLATAFORMA ANDROID POR MEIO DO DESENVOLVIMENTO DE UMA APLICAÇÃO

Trabalho de Conclusão de Curso apresentado para obtenção do grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. MSc. Paulo João Martins

CRICIÚMA

2012

FELIPE CORAL SASSO

UTILIZANDO CERTIFICAÇÃO DIGITAL NA PLATAFORMA ANDROID POR MEIO DO DESENVOLVIMENTO DE UMA APLICAÇÃO

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Dispositivos Móveis.

Criciúma, 28 de novembro de 2012.

BANCA EXAMINADORA

Prof. Paulo João Martins - MSc. - (UNESC) - Orientador

Prof. Sérgio Coral - Esp. - (UNESC)

Prof. Fabrício Giordani - Esp. - (UNESC)

Dedico este trabalho á minha família, cuja educação e apoio me tornaram o que sou hoje. Dedico também aos meus amigos e namorada que sempre acreditaram, me ajudaram e torceram por mim.

AGRADECIMENTOS

A maior parte dos meus agradecimentos devem se voltar primeiramente a minha família, por sempre me darem forças em todos os momentos.

A minha namorada, que, mesmo nas minhas ausências, sempre depositou confiança, força e paciência em mim.

Aos amigos que fiz durante o curso, que sempre estavam lá pra responder algum email com alguma dúvida, e também me apoiando.

Ao meu orientador Paulo João Martins, pela paciência e ajuda no projeto.

E a todos aqueles que de alguma forma me auxiliaram na conclusão desse projeto.

RESUMO

No mundo em que vivemos atualmente, se faz cada vez mais necessário a utilização da informação a todo o momento. Certamente, o correio eletrônico é a ferramenta mais utilizada para transmissão de informações, desde o usuário comum à grandes corporações. Aliado ao crescente uso de dispositivos móveis, utilizando a transmissão de dados por redes de telefonia móvel, pode-se estar 100% conectado a grande rede de computadores, o que possibilita ao usuário o uso do correio eletrônico em qualquer lugar e a qualquer momento. Com o grande uso dessa ferramenta, é necessário garantir a segurança entre as informações transmitidas. Esta pesquisa apresenta um sistema para a plataforma móvel Google Android, cuja função é garantir a segurança de mensagens de correio eletrônico utilizando os conceitos de segurança com criptografia e certificação digital. Para isso foram realizados estudos sobre a plataforma Google Android, criptografia e certificados digitais.

Palavras-chave: Segurança. Google Android. Criptografia. Certificados Digitais.

ABSTRACT

In the world we live in today, it becomes increasingly necessary to use the information all the time. Certainly, the electronic mail is the most used tool for information transmission, since common users to large corporations. With the increasing use of mobile devices, using the data transmission by mobile phone networks, you can be 100% connected to a large computer network, which enables the user to use the e-mail anywhere and any time. With the high use of this tool, it is necessary to ensure the security of the information transmitted. This research presents a system for the Google Android mobile platform, whose function is to ensure the security of e-mail messages using the concepts of security with cryptography and digital certification. For this, studies were conducted on the Google Android platform, cryptography and digital certificates.

Key-words: Security, Google Android, cryptography, digital certificates

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AC	Autoridade Certificadora
API	Application Programming Interface
AR	Autoridade Registradora
ECC	Eliptic Curve Cryptography
IDE	Integrated Development Environment
ITU-T	Telecommunication Standardization Sector
MD2	Message-Digest Algorithm 2
MD4	Message-Digest Algorithm 4
MD5	Message-Digest Algorithm 5
OHA	Open Handset Alliance
PDA	Personal Digital Assistant
RSA	Rivest, Shamir, Adleman
SDK	Software Development Kit
SHA-1	Secure Hash Algorithm 1
SHA-256	Secure Hash Algorithm 256
SHA-512	Secure Hash Algorithm 512
SQL	Structured Query Language
XML	eXtensible Markup Language

SUMÁRIO

1 INTRODUÇÃO

A cada dia que passa, as pessoas estão cada vez mais conectadas entre si. Com o advento da Internet e dos computadores pessoais, uma informação que antigamente levaria de semanas à meses para chegar ao seu destinatário, hoje leva apenas alguns segundos.

Com o avanço da tecnologia, surgiram os aparelhos móveis, como smartphones, PDAs, celulares, entre outros. Com isto, tornou-se possível a realização de tarefas como acesso a Internet e transmissão de dados de forma móvel, por meio desses dispositivos, o que antes era possível apenas em computadores, que normalmente eram grandes demais para serem transportados.

Com o crescente uso de dispositivos móveis, utilizando a transmissão de dados por redes de telefonia móvel, pode-se estar 100% conectado a grande rede de computadores, o que possibilita ao usuário o uso do correio eletrônico em qualquer lugar e a qualquer momento. Com o uso dessa ferramenta, é necessário garantir a segurança entre as informações transmitidas.

Conforme Tanenbaum (2003), para que dados confidenciais não sejam descobertos, eles devem ser criptografados.

A criptografia consiste num conjunto de métodos e técnicas que tem como objetivo tornar uma informação totalmente ilegível para pessoas não autorizadas, é dividida em dois tipos, simétrica e assimétrica. Na simétrica, uma mesma chave é utilizada tanto para cifrar quanto decifrar uma informação, já na assimétrica, duas chaves são necessárias para realizar o processo, uma pública que é distribuída livremente, e uma privada, de posse exclusiva do seu respectivo dono. Neste tipo de criptografia, o que uma chave cifra, apenas seu respectivo par decifra.

De acordo com Housley e Polk (2001, tradução nossa), o grande problema da criptografia assimétrica está em determinar quem possui a chave privada correspondente à pública. Para isso surgiu o certificado digital, usado para garantir a ligação entre uma entidade e uma chave pública.

Aliado ao grande número de dispositivos móveis com a plataforma Google Android, essa pesquisa teve como objetivo o desenvolvimento de uma aplicação usando os conceitos de segurança com criptografia e certificados digitais para segurança de mensagens de correio eletrônicos.

1.1 OBJETIVO GERAL

Desenvolvimento de um aplicativo para correio eletrônico, que utilize de conceitos de segurança de dados por meio de criptografia e certificação digital.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos que esta pesquisa propôs foram:

a) descrever os aspectos do sistema Google Android;
b) entender e aplicar os conceitos sobre segurança em dispositivos móveis;
c) aplicar o uso da criptografia e certificados digitais em dispositivo móvel com sistema operacional Android;
d) desenvolver uma aplicação que utilize os conceitos de segurança descritos no projeto.

1.3 JUSTIFICATIVA

O sistema operacional Google Android tem sido uma das plataformas divulgadas pelos meios de comunicação que mais cresce atualmente. Conforme visto em Canalys (2010, tradução nossa), a participação da plataforma no mercado cresceu de 10% em 2009 para 35% em 2010, enquanto outras plataformas como Symbiam, da Nokia, reduziu de 45% para 26%. Ainda citando Canalys (2010, tradução nossa), no quarto trimestre de 2009, havia no mundo cerca de quatro milhões de dispositivos com o sistema Android, em 2010, esse número subiu para cerca de 33 milhões. E conforme apresentado em BusinessWire (2012, tradução nossa), até 2016, este sistema deverá ser o mais utilizado do mundo, ultrapassando o sistema operacional Windows.

Apesar desse grande número de dispositivos com a plataforma Android, o sistema é o menos seguro. Conforme demonstrado em CheckPoint (2012, tradução nossa), o sistema Android é apontado com uma das plataformas com mais riscos de segurança, e ainda citando CheckPoint (2012, tradução nossa), um dos maiores riscos para a segurança, é a transmissão de informações sigilosas através de redes sem fio inseguras.

Aliado a isso, tem-se o uso do correio eletrônico: conforme apresentado por Reuters (2012, tradução nossa), 85% das pessoas no planeta utilizam o *e-mail*, fazendo desta uma das ferramentas mais utilizada para comunicação na Internet.

No entanto, conforme apresentado por Cert (2012), somente no Brasil, no período compreendido entre Janeiro e Março de 2012, ocorreram mais de 10 mil fraudes virtuais, tais como roubo de identidade, falsificação de documentos ou assinaturas entre outros.

Conforme Burnett e Paine (2002), o uso de certificados digitais atualmente é uma das melhores soluções para esse problema, pois garante o sigilo e a integridade de uma informação, e ainda pode-se identificar a identidade de quem enviou.

Diante deste cenário, o desenvolvimento de uma aplicação para a plataforma Android, que utilize a certificação digital para garantir o sigilo e a integridade de mensagens de correio eletrônico se faz necessária.

1.4 ESTRUTURA DO TRABALHO

A presente pesquisa está dividida em 6 capítulos. No capitulo 1 é apresentada uma introdução ao projeto proposto, os objetivos gerais e específicos e a justificativa para a realização deste projeto.

No capitulo 2 é apresentada uma introdução ao sistema Android para dispositivos móveis, tal como sua história e sua arquitetura.

No capítulo 3 é apresentado um breve estudo sobre a segurança existente em dispositivos móveis, e um pouco sobre a história da criptografia, apresentando-se os conceitos existentes, os tipos de criptografia e sua utilização.

O conceito de certificado digital será mostrado no capítulo 4. Neste capítulo será explicado o que é um certificado, o que é uma infraestrutura de chaves públicas, seus componentes e o padrão X.509.

Diversos trabalhos correlatos são descritos no capítulo 5 a fim de proporcionar uma visão mais abrangente sobre criptografia, certificação digital e a plataforma Android.

Finalmente, no capítulo 6 será mostrado todo o desenvolvimento prático da pesquisa, onde serão demonstrados os conceitos do sistema, a modelagem

conceitual, as técnicas utilizadas para implementação e testes e os resultados obtidos com esse desenvolvimento.

2 ANDROID

Como citado em Silva e Pereira (2009), o Android é uma plataforma para tecnologia móvel completa, envolvendo um pacote com programas para celulares, já com um sistema operacional, middleware, aplicativos e interface do usuário. Foi idealizado por uma empresa chamada Android Inc., sendo adquirida pelo Google em 2005 (HASHIMI; KOMATINEMI; MACLEAN, 2010).

No fim de 2007, um grupo de empresas se reuniu em torno da plataforma para formar a Open Handset Alliance (OHA), que consiste em uma aliança de trinta e quatro empresas com o propósito de englobar todos os processos móveis, operadora móvel, fabricante, empresas de semicondutores e microchips, empresas de software, e empresas de comercialização (LECHETA, 2010; PEREIRA, 2009). Parte do objetivo da aliança é inovar rapidamente e responder melhor às necessidades dos consumidores.

A plataforma Android foi concebida para servir as necessidades das operadoras móveis, fabricantes de aparelhos e desenvolvedores de aplicativos (HASHIMI; KOMATINEMI; MACLEAN, 2010). O sistema foi lançado sobre o código aberto na Licença Apache versão 2.0.

Conforme Karch (2010), qualquer um pode usar e modificar o Android em seus aparelhos e desenvolver aplicações de forma gratuita. Como visto em Aquino (2007), os desenvolvedores que pretendem adotar esta plataforma podem utilizar o Android Software Development Kit (SDK) para o desenvolvimento de softwares, embasado na linguagem de programação Java.

2.1 CARACTERISTICAS

Conforme DiMarzio (2008), Android é um sistema operacional para dispositivos móveis baseado em Java que é executado sobre um kernel Linux 2.6 adaptado para este propósito. Citando, Steele e To (2010, tradução nossa), a plataforma possui algumas características que o torna diferente contra os demais, como as seguintes:

2.1.1 Multiprocesso e App Widget

Ainda citando Steele e To (2010, tradução nossa), o sistema operacional Android não restringe o processador a uma única aplicação por vez. Ele faz o gerenciamento de prioridades e threads de uma aplicação. Com isso tem-se o beneficio da multitarefa, onde é possível a execução de mais de uma aplicação por vez.

Steele e To (2010, tradução nossa) diz que isso pode abrir novas possibilidades, como por exemplo, enquanto o usuário joga, um processo de fundo pode verificar um estoque e disparar um alarme se necessário.

App Widgets são mini aplicativos que podem ser incorporados em outras aplicações. Elas podem processar eventos, como iniciar uma música, ou atualizar o nível da temperatura exterior, enquanto outro aplicativo está em execução. No entanto Steele e To (2010, tradução nossa) cita que cuidados devem ser tomados para evitar que aplicações drenem a bateria.

2.1.2 Toque, Gestos e Multitoque

As telas sensíveis ao toque (*touchscreen*), são uma interface intuitiva em um dispositivo de mão. Sua utilização é feita de forma quase que natural, sendo que se dá ao pressionar um dedo sobre a tela. Um exemplo é a forma prática de pressionar e arrastar para interagir com um gráfico. Muitas vezes é utilizado para fazer o zoom ou girar uma imagem.

Steele e To (2010, tradução nossa) cita que alguns eventos de toque estão disponíveis de forma transparente para o programador, onde não se tem a necessidade de implementar seus comportamentos detalhadamente. Gestos necessários podem ser definidos, se necessário.

Ainda citando Steele e To (2010, tradução nossa), é importante manter o uso consistente de eventos de toque em comparação com outros eventos.

2.1.3 Máquina Virtual Dalvik

Conforme Android (2012, tradução nossa), Dalvik é uma máquina virtual interpretadora que executa arquivos no formato *.dex*, um formato que é otimizado

para ocupar pouco espaço de armazenamento. A máquina virtual é baseada em registradores, e pode executar classes compiladas em Java que foram transformadas para o formato nativo usando a ferramenta dx, que conforme Anjos (2008), é uma ferramenta que faz conversão de arquivos de classes compiladas em Java para JVM em arquivos .dex para *Dalvik*.

O núcleo *Dalvik* se destina a fornecer uma base de desenvolvimento familiar para aqueles que programam em *Java Standard Edition*, mas é voltado especificamente para as necessidades de um dispositivo móvel.

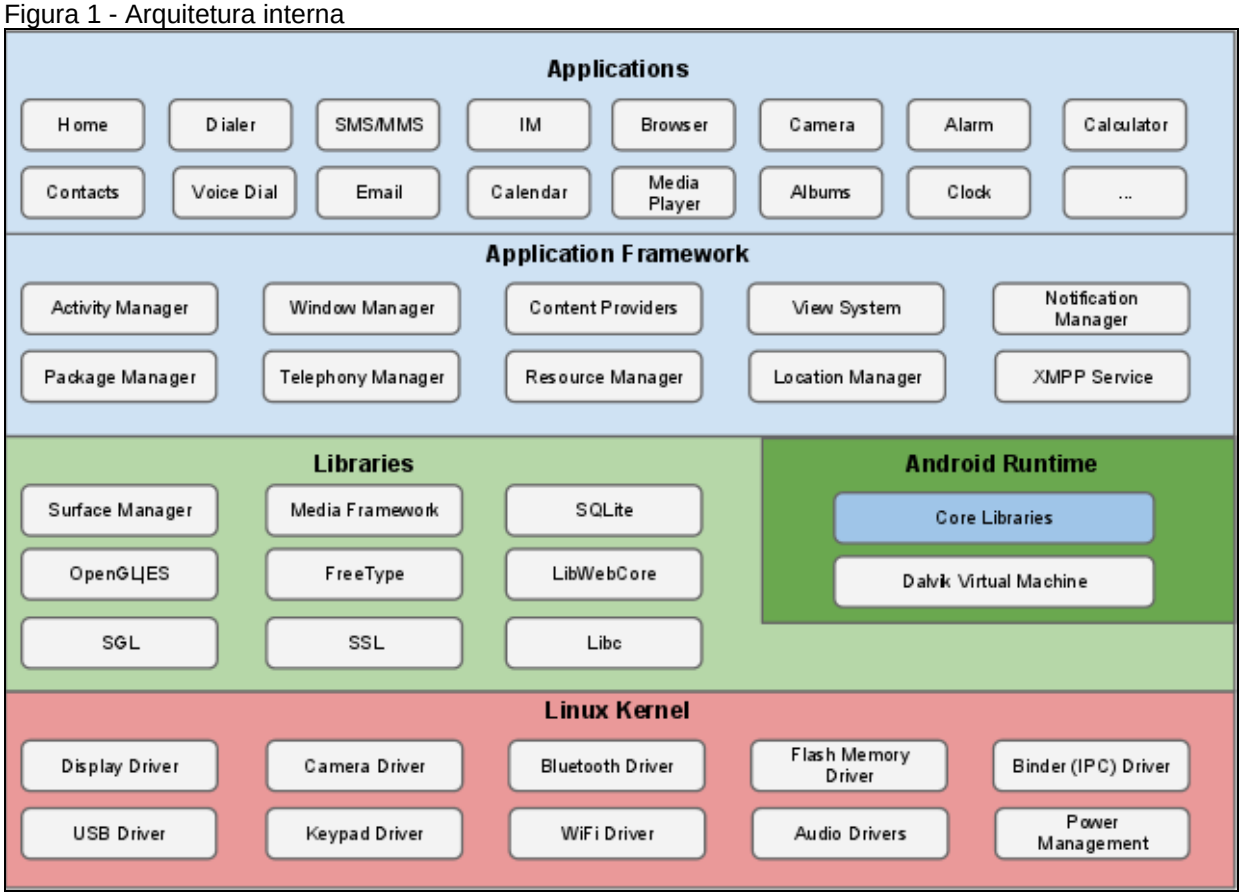
2.1.4 Armazenamento de Dados

O sistema Android oferece suporte completo para banco de dados SQLite. É um motor de banco de dados embutido. Diferentemente da maioria dos outros bancos, não tem um servidor em um processo separado. Lê e escreve diretamente para arquivos do disco (ANDROID, 2012, tradução nossa).

2.2 ARQUITETURA INTERNA

Conforme figura 1, a arquitetura interna do Android é separada em cinco camadas: Aplicações, Framework de Aplicações, Bibliotecas Nativas, Android Runtime e o Kernel Linux.

Figura 1 - Arquitetura interna



Fonte: ANDROID (2012)

2.2.1 Framework de Aplicações

Conforme apresentado por Aquino (2007), a arquitetura foi projetada para simplificar o desenvolvimento, baseando-se no reuso dos componentes, ou seja, qualquer componente da biblioteca padrão pode ser instanciado e utilizado pela aplicação.

E citando Silva (2009), o framework de aplicativo tem como objetivo fornecer componentes que auxiliam o desenvolvimento da aplicação como caixas de texto, botões, gráficos. O diferencial desta arquitetura é que os componentes padrões do sistema podem ser customizados pelo desenvolvedor para que se adequem à nova aplicação.

2.2.2 Bibliotecas Nativas

Conforme Silva (2009), para auxiliar no processo de desenvolvimento do software, a plataforma de suporte possui rotinas básicas pré-existentes, que se

repetem ou possuem um alto grau de complexidade. No Android existem uma série de bibliotecas em C/C++, como OpenGL, WebKit, FreeType, Secure Sockets Layers (SSL), LIBC, SQLite e Media.

O sistema de biblioteca em C é ajustado para dispositivos embarcados baseados em Linux. Tem suporte aos formatos mais comuns de áudio, vídeo e imagens. Também possui APIs que suportam Bluetooth, EDGE, 3G, Wifi e GPS (HASHIMI; KOMATINEMI; MACLEAN, 2010, tradução nossa).

2.2.3 Android Runtime

Em seguida, tem-se o Android Runtime, que é uma instância da máquina virtual Dalvik. Conforme Silva (2009), as aplicações desta plataforma são executadas de forma semelhante ao Java, que gera bytecodes, entretanto o Android gera códigos executáveis para a Máquina Virtual Dalvik. Após a compilação do projeto, todos os recursos da aplicação são compactados em um arquivo chamado Android Package File (.apk), pronto para ser instalado em qualquer dispositivo com o sistema operacional.

Segundo Aquino (2007), cada aplicação tem seu próprio processo e sua própria instância na máquina virtual, que ao mesmo tempo individualiza o gerenciamento da aplicação, porém otimizando a execução de máquinas virtuais concorrentemente.

2.2.4 Kernel Linux

Conforme apresentado por Silva (2009), os dispositivos móveis necessitam de um sistema operacional, para que o usuário possa utilizar os recursos do dispositivo, porém, para gerenciar tais recursos, é necessária a criação de softwares que não sejam apenas para um determinado modelo de equipamento, devido à variedade dos mesmos.

O núcleo da plataforma Android é baseado no kernel Linux versão 2.6.29 (HASHIMI; KOMATINEMI; MACLEAN, 2010, tradução nossa), que é responsável pelos drivers do dispositivo, acesso a recursos, gerenciamento de energia e outras tarefas do sistema. Ainda citando Silva (2009), por utilizar o Kernel do Linux, a

preocupação do desenvolvedor no acesso a dispositivos específicos não existe, promovendo uma camada de abstração entre o hardware e software.

2.3 FRAMEWORK DE DESENVOLVIMENTO

Conforme Silva (2009), o framework de desenvolvimento tem como objetivo prover uma estrutura que utiliza um conjunto de códigos, classes, funções e métodos suportado por uma determinada plataforma.

Para Silva (2009), o ambiente de desenvolvimento é composto basicamente por:

a) emulador: utilizado para testar e executar aplicações. Consegue simular hardware e software de um dispositivo móvel, inclusive simulando o recebimento e realização de chamadas. A figura 2 demonstra um emulador em execução:

Figura 2 - Emulador do Android

Fonte: ANDROID (2012).

b) *Debugger*: Utilizado em conjunto com o emulador, e é por meio de sua interface que se pode manipular os arquivos do sistema, como banco de dados criado por uma aplicação;

c) *Plugin*: fornece recursos como interface gráfica, adiciona suporte integrado com o projeto e ferramentas Android;

d) SDK: fornece bibliotecas e ferramentas de desenvolvimento necessárias para construir, testar e depurar aplicativos para o Android.

2.4 ANATOMIA DE APLICAÇÕES

Ainda citando Steele e To (2010, tradução nossa), uma aplicação consiste de várias funcionalidades, como editar uma nota, executar um arquivo de música, tocar um alarme, ou a abertura de um contato. Podem ser classificadas em *Activity, Service, BroadcastReceiver* e *ContentProvider.*

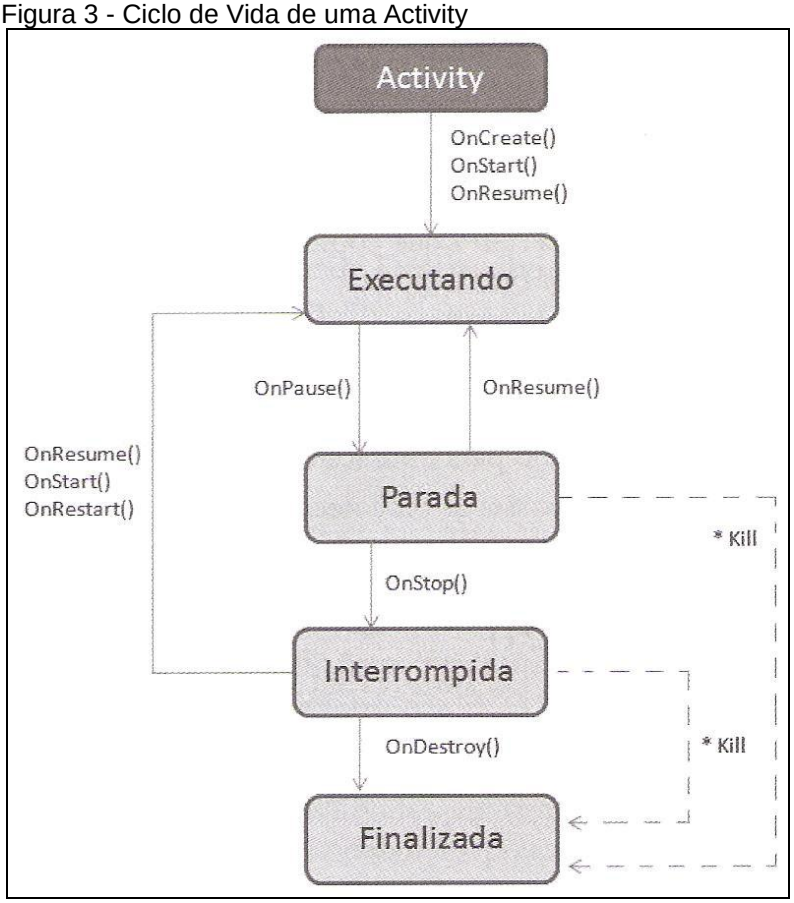
2.4.1 Activity

Conforme Android (2012, tradução nossa), uma *Activity* (Atividade), é a coisa mais simples que um usuário pode fazer. Quase todas as *Activities* interagem com o usuário, ela cuida da criação de uma janela onde pode-se colocar uma interface gráfica.

Embora são frequentemente apresentadas como janelas em tela cheia, eles também podem ser usadas de outras maneiras: como janelas flutuantes ou incorporado dentro de outra atividade. Como um usuário navega saindo e voltando dos aplicativos, cada instância da *Activity* transita entre diferentes estados em seu ciclo de vida. Por exemplo, quando uma é iniciada pela primeira vez, ela vem para o primeiro plano do sistema e recebe o foco do usuário. Durante este processo, o sistema Android chama uma série de métodos de ciclo de vida sobre a *Activity* em que foi configurado a interface de usuário e outros componentes.

Se o usuário executa uma ação que começa uma outra *Activity* ou muda para outro aplicativo, o sistema chama um outro conjunto de métodos de ciclo de vida*,* como se ela fosse movida para o plano de fundo, (onde não é mais visível, mas a instância e seu estado permanece intacta). A figura 3 demonstra o ciclo de vida de uma *Activity*:

Figura 3 - Ciclo de Vida de uma Activity



Fonte: Pereira e Silva (2009, p.12).

2.4.2 Service

Android (2012, tradução nossa) cita que um S*ervice* é um componente de aplicação que pode executar operações de fundo de longa duração e não fornece uma interface de usuário. Outro componente do aplicativo pode iniciar um *Service* e vai continuar a executar em segundo plano, mesmo se o usuário mudar para outro aplicativo.

Além disso, um componente pode se ligar a um *Service* para interagir com ele e até mesmo realizar a comunicação entre processos. Por exemplo, um serviço pode lidar com transações de rede, tocar música, ou interagir com um provedor de conteúdo, todos em segundo plano.

2.4.3 BroadcastReceiver

Conforme Ableson, Sen e King (2011, tradução nossa), o *BroadcastReceiver* é utilizado para responder a eventos globais, como uma

chamada de telefone ou uma mensagem de texto recebida. Como o *Service*, o *BroadcastReceiver* não tem uma interface do usuário.

2.4.4 ContentProvider

Ainda citando Android (2012, tradução nossa), *ContentProvider* (fornecedor de conteúdos) são um dos principais blocos de construção do Android, fornecendo conteúdo para aplicações. Eles encapsulam dados e os fornecem às aplicações através da interface *ContentResolver*.

Um *ContentProvider* só é necessário se é preciso compartilhar dados entre várias aplicações. Por exemplo, os dados de contatos é utilizada por várias aplicações e deve ser armazenado em um fornecedor de conteúdos.

2.4.5 AndroidManifest

Conforme visto em Android (2012, tradução nossa) cada aplicação deve ter um arquivo *AndroidManifest.xml* em seu diretório raiz. O manifesto apresenta informações essenciais sobre o aplicativo para o sistema, e este de deve ter as informações contidas no arquivo antes de executar qualquer código do aplicativo.

Também descreve os componentes da aplicação, tais como atividades, serviços, fornecedores de conteúdo, declara quais permissões o aplicativo deve ter para acessar partes protegidas da API e interagir com outras aplicações, entre outras coisas.

2.5 LICENÇA DE USO

Conforme citado em Ableson, Sen e King (2011, tradução nossa), o Android está lançado sobre duas licenças de código aberto diferente. O Kernel Linux foi lançado sobre a licença GNU General Public License (GPL), como é de exigido para qualquer um que está licenciando um Kernel de um sistema operacional de código aberto. A plataforma Android, desconsiderando o Kernel, é licenciado sobre a licença Apache Software License (ASL). Embora ambas as licenças são orientadas a códigos fonte abertos, a principal diferença é que a licença Apache é considerada

amigável para uso comercial. No próximo capítulo será descrito os aspectos de segurança.

3 SEGURANÇA

Conforme Medeiros (2001), a segurança da informação busca reduzir os riscos de vazamento, fraudes, erros, uso indevido, paralisações, roubo de informações ou qualquer outra ameaça que possa prejudicar o sistemas de informações.

Em sua forma mais simples, a segurança computacional se preocupa em garantir que pessoas mal-intencionadas não leiam ou modifiquem secretamente mensagens enviadas a outros destinatários (TANENBAUM, 2003).

Ou seja, a segurança da informação tem como principais objetivo garantir as seguintes propriedades (KOVACS; MONTEIRO, 2006):

a) confidencialidade: propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;
b) integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição);
c) disponibilidade: propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação;
d) não repúdio: propriedade que garante que o autor não negue ter criado ou assinado um documento.

3.1 SEGURANÇA NO CORREIO ELETRÔNICO

Conforme Moura (1995), o correio eletrônico, *eletronic mail* ou *e-mail*, é um sistema que possibilita a troca de mensagens entre usuários dos computadores interconectados por meio de uma rede de comunicação.

Ainda citando Moura (1995), além de possibilitar conversas amenas e informais entre usuários, o correio eletrônico faz com que pesquisadores e outros profissionais troquem informações em tempo extremamente curto.

Uma mensagem é constituída de três elementos:

a) o endereço eletrônico (*e-mail address*);

b) o assunto (*subject*);

c) o texto da mensagem.

Além desses três elementos, a toda mensagem enviada o programa gerenciador de correio eletrônico acrescenta um cabeçalho (MOURA, 1995).

Conforme citado por McFedries (1996), quando se envia uma mensagem, ela não trafega diretamente para o receptor. Ao invés disso, precisa, obrigatoriamente passar por uma série de outros sistemas. A Internet possui “pontos de verificação”, pelo quais as mensagens são obrigadas a passar durante suas jornadas. Ainda citando McFedries (1996), esses pontos de verificação são apenas computadores em alguma outra rede, e a cada parada há sempre a possibilidade de alguém interceptar a mensagem e lê-la.

3.1.1 S/MIME

Conforme Chernick (2002, tradução nossa), o Secure/Multipurpose Internet Mail Extensions (S/MIME) é um conjunto de especificações de correio eletrônico que descreve um protocolo para a adição de serviços de segurança criptográficos através do encapsulamento de objetos assinados digitalmente e criptografados.

É importante destacar que nem todos os navegadores dão suporte ao S/MIME. Se um usuário receber uma mensagem de correio eletrônico assinado ou criptografado utilizando essas especificações e acessar sua conta em um navegador sem suporte, apenas receberá um anexo com a mensagem cifrada ou assinada. Para mensagens assinadas o anexo será um arquivo com o nome “smime.p7s”, e para mensagens cifradas, o anexo terá o nome "smime.p7m"

3.2 SEGURANÇA EM DISPOSITIVOS MÓVEIS

De acordo com Isaca (2010, tradução nossa), muitos dos riscos associados a dispositivos móveis existem por causa da sua maior vantagem: a portabilidade. Dispositivos móveis transportam dados via redes sem fio, que normalmente são menos seguras que redes com fios, e podem deixar informações em risco de interceptação.

Conforme Reis, Goulart e Mendes (2010), estes são os tipos de ataques que podem ocorrer:

a) disfarce: o atacante personifica um usuário e com isso obtém algum dos recursos desautorizados da rede;
b) repetição: o atacante intercepta a transmissão e envia como se fosse o usuário legítimo;
c) modificação de Mensagem: o atacante altera uma mensagem legítima, apagando, adicionando, editando ou reordenando a própria mensagem;
d) negação de Serviço: o atacante dificulta o uso normal ou o gerenciamento dos dispositivos da rede, através de sobrecarga, impossibilitando que ele atenda a todas as requisições que lhe são feitas;

Ainda citando Isaca (2010, tradução nossa), em caso de ocorrer uma interceptação maliciosa em que a informação é adquirida, os dados podem ser interpretados e usados, resultando na exposição de informações que podem danificar a imagem de uma empresa.

Com isso, pode-se perceber que ainda existe uma falta de segurança entre informações que são transitadas de dispositivo para dispositivo (ou de dispositivos para computadores pessoais).

Esse problema atinge diretamente as propriedades fundamentais da segurança citados anteriormente. Se alguém quer enviar alguma informação secreta, ela pode até ser interceptada, o que causa a quebra da confidencialidade dos dados. Com uma interceptação, os dados podem ser alterados, causando a quebra da integridade.

Com uma interceptação e até alteração de informações confidenciais, os resultados podem não ser muito favoráveis para uma empresa ou pessoa.

Esses dados precisam, de alguma forma, serem escondidos de pessoas não autorizadas, e conforme Burnett e Paine (2002), uma das ferramentas mais importantes para proteção de dados é a criptografia.

3.1.1 Criptografia

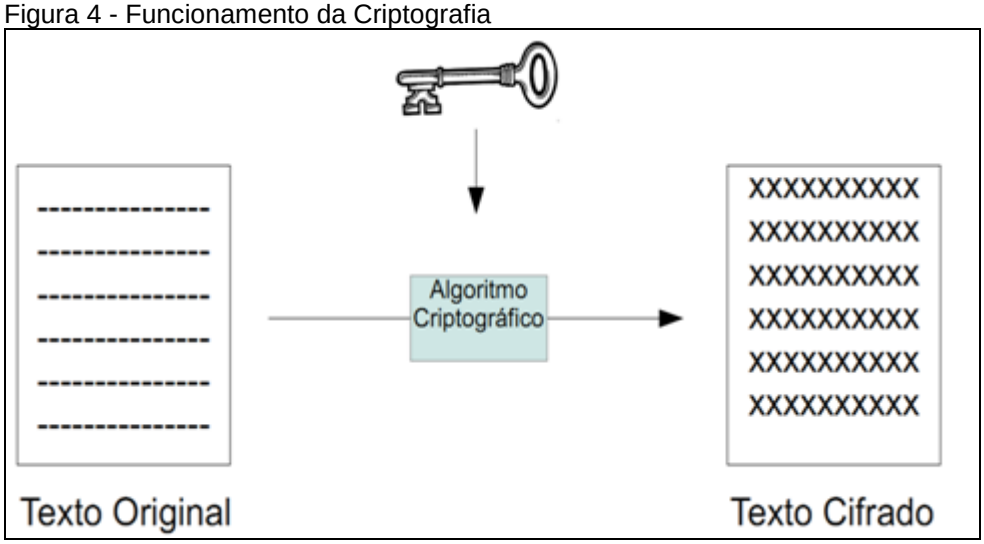
Conforme Carvalho (2001), a criptografia, do grego *kryptós* (escondido), e *gráphein* (escrita), consiste na ciência e na arte de se comunicar

secretamente. Ainda citando Carvalho (2001), o objetivo básico da criptografia é tornar uma mensagem ininteligível para um adversário, que possa vir a interceptar uma mensagem.

O processo pela qual a informação é transformada em algo sem sentido é chamada cifragem (ou transformação criptográfica). O processo inverso chama-se decifragem, onde o texto ilegível ou cifrado é tornado legível como na sua forma original.

Para a realização da cifragem, são necessários dois componentes: um algoritmo, que é um conjunto de instruções matemáticas que faz a transformação da mensagem clara em mensagem cifrada e vice-versa, e uma chave que é um conjunto de bits, aleatórios ou não, que agem em conjunto com o primeiro. Cada chave distinta faz com que o algoritmo trabalhe de uma forma ligeiramente diferente.

Figura 4 - Funcionamento da Criptografia



Fonte: Adaptada de Kohler e Bodemüller Junior (2007, p. 26).

Conforme figura 4, tem-se como entrada para o processo criptográfico o “Texto Original” e uma chave secreta. Essa última trabalha em conjunto com o algoritmo criptográfico e como saída tem-se o “Texto Cifrado”.

Uma chave criptográfica pode ter tamanhos variados. Por exemplo, uma chave de 8 bits permite uma combinação de 256 chaves. Quanto maior o tamanho das chaves, mais difícil será quebrá-la. Existem dois tipos de criptografia: simétrica e assimétrica. Ambos serão explicados em capítulos posteriores.

3.1.2 Criptografia simétrica

Na criptografia simétrica, é utilizado apenas uma chave (como visto anteriormente na Figura 4), tanto para a cifragem, quanto para a decifragem de uma informação. Nesse esquema, a chave precisa ser compartilhada entre os usuários autorizados antes que as mensagens possam ser trocadas. De acordo com Moreno, Pereira e Chiaramonte (2005), essa ação resulta num atraso de tempo e possibilita que a chave chegue a pessoas não autorizadas.

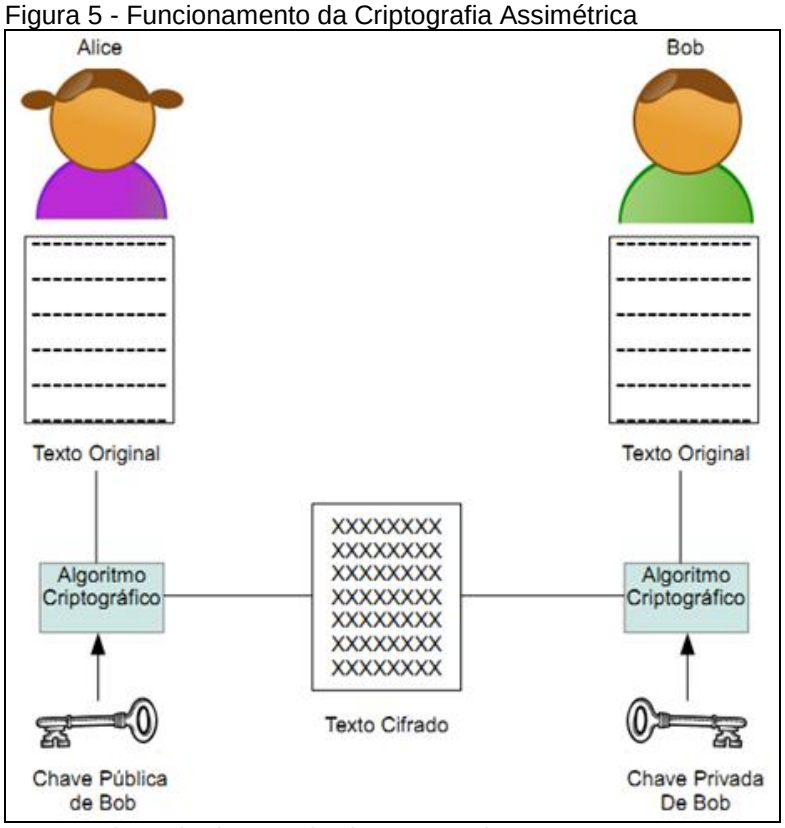
De acordo com Schneier (1996), a criptografia simétrica possui os seguintes problemas:

a) a chave precisa ser distribuída em segredo. Para sistemas de criptografia que estão espalhados pelo mundo, isso pode ser uma tarefa difícil;
b) se uma chave é comprometida (roubada, quebrada, adivinhada, entre outras), então pode-se decifrar todo o tráfego que cifrado com a chave secreta. Também pode produzir mensagens falsas;
c) supondo que uma chave é usada para cada usuário em uma rede, o número de chaves aumente conforme o número de usuários cresce. A rede necessita de n (n – 1) / 2 chaves. Por exemplo, 10 usuários exigem 46 chaves diferentes para que se tenha uma troca de informações segura entre eles. E 100 usuários exigem 4950 chaves. Este problema pode ser minimizado, mantendo um número de usuários de pequeno porte, o que nem sempre é possível.

3.1.3 Criptografia assimétrica

Na criptografia assimétrica, também chamada de criptografia de chave pública, é utilizado um par de chaves, uma pública e uma privada. A primeira será distribuída livremente, normalmente na Internet, já a segunda será conhecida apenas pelo seu dono. As duas chaves são utilizadas para cifragem e decifragem, no entanto, quando alguma informação é cifrada pela pública, apenas a respectiva chave privada poderá realizar a decifração. E quando algo é criptografado pela privada, apenas a respectiva chave pública poderá decifrar a informação.

Figura 5 - Funcionamento da Criptografia Assimétrica



Fonte: Adaptada de Moecke (2011, p. 10)

A figura 5 ilustra um exemplo de uso da criptografia assimétrica: se Alice quer enviar alguma informação sigilosa para Bob, ela irá utilizar a chave pública dele para cifrar a mensagem. Bob, por sua vez, irá utilizar sua chave privada que apenas ele tem acesso para decifrar a mensagem enviada por Alice.

Com esse esquema, é possível identificar e autenticar outras pessoas e dispositivos.

Conforme Carvalho (2001), o RSA é o algoritmo de criptografia de chave pública mais usado e testado, e ainda hoje é um dos mais utilizados para este tipo de criptografia. Esse nome se deve aos três professores do Instituto MIT que criaram o algoritmo: Ronald Rivest, Adi Shamir e Leonard Adleman. Outros algoritmos conhecidos são o ElGamal e o ECC.

Housley e Polk (2001, tradução nossa) citam que um dos problemas principais da criptografia assimétrica é determinar quem possui a chave privada correspondente. Para isso, foi criado o conceito de Certificação Digital, que será explicado em capítulo posterior.

3.1.4 Funções de resumo criptográfico (Hash)

Um resumo criptográfico é um arranjo de bits de tamanho fixo, que representa o resumo de uma mensagem.

Lima (2005, p. 137) diz que:

> Tem como única finalidade gerar uma curta sequência de bytes que representa unicamente qualquer montante de dados que seja submetido a função. Qualquer alteração nos dados de entrada da função, mesmo que seja apenas um bit seja invertido, deve gerar um resultado diferente.

Conforme Stallings (1998), uma função Hash deve ter as seguintes propriedades:

a) h deve poder ser aplicado em um bloco de bytes de qualquer tamanho;

b) h produz um bloco de bytes de tamanho fixo;

c) h(x) deve ser relativamente fácil de computar para qualquer x;

d) para qualquer h(x), deve ser impraticável encontrar x;

e) deve ser impraticável encontrar qualquer h(x) = h(y).

Os algoritmos comumente utilizados são: MD2, MD4, MD5, SHA-1, SHA-256 e SHA-512.

3.1.5 Assinatura digital

De acordo com Burnett e Paine (2002), a autenticação permite que alguém no mundo eletrônico confirme sua identidade, e o não repúdio impede que pessoas retifiquem sua palavra eletrônica. Uma maneira de implementar esses recursos é o uso de assinatura digital.

Como citado em Buchmann (2002), são utilizadas para assinar documentos eletrônicos.

As assinaturas digitais funcionam da seguinte maneira: Suponha que Alice queira assinar o documento m. Ela utilizará sua chave secreta e criptografará m. Bob, usando a pública correspondente, irá decifrar essa informação. Como é conhecido que apenas a pública pode decifrar algo cifrado pela chave privada, Bob poderá ter certeza que foi Alice que enviou a informação e de que essa não foi forjada.

Uma assinatura digital não provê segurança contra leitura da mensagem, mas assegura a autenticidade e o não-repúdio de uma informação.

No próximo capítulo será apresentada uma explanação sobre certificação digital, e o que ela tange. Além de ser também apresentado o que é um certificado digital, e também uma Infraestrutura de Chaves Públicas e seus componentes.

4 CERTIFICAÇÃO DIGITAL

Conforme Macedo (2008), a certificação digital é utilizada para autenticar programas, assinaturas de mensagens, documentos eletrônicos, controle de acessos e outros. Surgiu em função da necessidade de manter a integridade e segurança da informação e na interação junto à Internet (BERNARDINELLI, 2010). Marques, Castro e Veras (2011), citam que o uso da certificação digital em processos eletrônicos assegura alguns aspectos, como privacidade, integridade, autenticidade e não repúdio.

Bernardinelli (2010) cita que a certificação digital beneficia diversas áreas e setores da economia brasileira. Dentre essas vantagens pode-se destacar:

a) acompanhamento de processos jurídicos online;
b) contribuintes podem acessar informações junto aos órgãos públicos permitindo que renegocie suas dividas, realize cópias de documentos, consiga segunda via de impostos e tributos pagos entre outras;
c) entrega de obrigações principais e acessórias de maneira simplificada e segura;
d) evitar fraudes digitais ocasionadas por terceiros;
e) maior segurança na web;
f) maior produtividade, agilidade e competitividade através de um acesso simplificado das informações;
g) redução do volume de papéis oriundos da burocracia por documentos eletrônicos e digitais;
h) redução das filas intermináveis nas agências, secretarias, repartições públicas e outras organizações governamentais ou não;
i) transmissão de informação no meio eletrônico de maneira segura, garantindo a integridade do mesmo.

4.1 CERTIFICADO DIGITAL

Como visto em Bernardinelli (2010), um certificado digital pode ser entendido como um documento digital que visa identificar pessoas, empresas, computadores entre outras que buscam guardar informações com maior segurança.

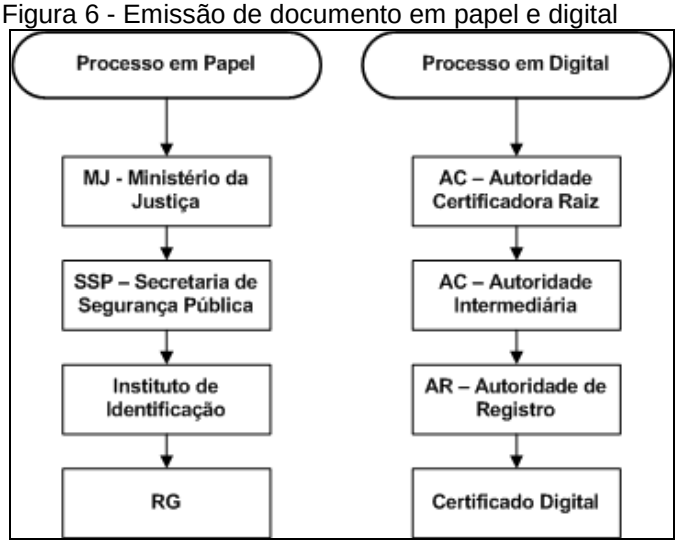
Cada certificado contém uma chave pública, e identifica o usuário que possui a chave privada correspondente. Também contém dois campos de data que especificam a emissão e a expiração do certificado. Também está incluído nele o nome de quem emitiu o certificado, chamado de emissor. Este inclui no certificado um número serial único, para identificar cada certificado. O certificado é protegido contra falsificações pela assinatura do emissor. O conteúdo do certificado é tratado como uma mensagem, e com isso é gerado a assinatura.

Housley e Polk (2001, tradução nossa) citam que o certificado digital ideal deve possuir as seguintes propriedades:

a) deve ser um objeto puramente digital, para ser distribuído através da Internet e processado automaticamente;
b) deve conter o nome do usuário que possui a chave privada correspondente, identificar o usuário, companhia ou organização, e incluir informações para contato;
c) deve ser fácil determinar se o certificado foi emitido recentemente.
d) deve ser criado por uma parte confiável, ao invés do usuário que possui a chave privada;
e) mesmo que a parta confiável crie vários certificados para um único usuário, deverá ser fácil distingui-los;
f) deve ser fácil determinar se o certificado é genuíno ou forjado;
g) deve ser a prova de violação, para que ninguém possa alterar seu conteúdo;
h) pode-se determinar se as informações contidas no certificado ainda são válidas;
i) pode-se determinar a partir do certificado quais tipos de aplicações que podem utiliza-lo.

De acordo com Monteiro e Mignoni (2007), o certificado digital possui o mesmo valor de um documento físico, como a carteira de identidade, por exemplo, e tem a emissão regulamentada por um órgão ligado à casa civil, fazendo deste também um prova de identificação. Na figura 6 é possível verificar o processo de emissão de um documento tradicional (papel) e um documento digital, neste caso o certificado.

Figura 6 - Emissão de documento em papel e digital



Fonte: Nunes (2007)

Para que os certificados sejam de uso comum entre todos os sistemas, foi estabelecido padrões para sua emissão. Segundo Sousa (2010), o padrão mais conhecido e utilizado atualmente é o X.509.

4.1.1 X.509

É um padrão da *Telecommunication Standardization Sector* (ITU-T), que define quais informações podem ser inseridas em um certificado, e descreve como anotá-los, sendo a versão 3 a mais recente. Conforme Burnett e Paine (2002), é o padrão mais amplamente aceito quanto à tecnologia de chave pública.

Conforme visto em Housley e Polk (2001, tradução nossa), o este certificado evoluiu em um poderoso e flexível mecanismo. Pode conter uma variedade de informações, muitas destas opcionais. A figura 7 demonstra a evolução deste tipo de certificado:

Figura 7 - Evolução do padrão X.509

Campos de um Certificado X.509, versão 1	Campos de um Certificado X.509, versão 2	Campos de um Certificado X.509, versão 3
Versão	Versão	Versão
Número de Série	Número de Série	Número de Série
Algoritmo de Assinatura da AC	Algoritmo de Assinatura da AC	Algoritmo de Assinatura da AC
Nome do Emissor	Nome do Emissor	Nome do Emissor
Período de Validade	Período de Validade	Período de Validade
Nome do Sujeito	Nome do Sujeito	Nome do Sujeito
Chave Pública do Sujeito	Chave Pública do Sujeito	Chave Pública do Sujeito
Valor da Assinatura	Valor da Assinatura	Valor da Assinatura
	ID Único de Emissor	ID Único de Emissor
	ID Único do Sujeito	ID Único do Sujeito
		Extensões

Fonte: Silva et al (2008)

4.1.2 Ciclo de vida de um certificado digital

De acordo com Tadano (2002), todo certificado passa por várias fases, desde seu requerimento até o fim de sua validade. Fica a autoridade certificadora, responsável pelo acompanhamento de todo o ciclo de vida dos certificados por ela emitidos.

Conforme Tadano (2002) e a figura 8, o ciclo de vida de um certificado digital é constituído das seguintes etapas:

a) requerimento: é o pedido do certificado, feito por uma entidade (física ou jurídica) à autoridade de registro;

b) validação do requerimento: é a função da AR em garantir que os dados da entidade sejam válidos

c) emissão do certificado: após a validação dos dados do requerente, a AR faz um solicitação para a autoridade certificadora, que emite o certificado;

d) aceitação do certificado pelo requerente: após a emissão, o requerente deve retira-lo da AR e confirmar a validade do certificado;

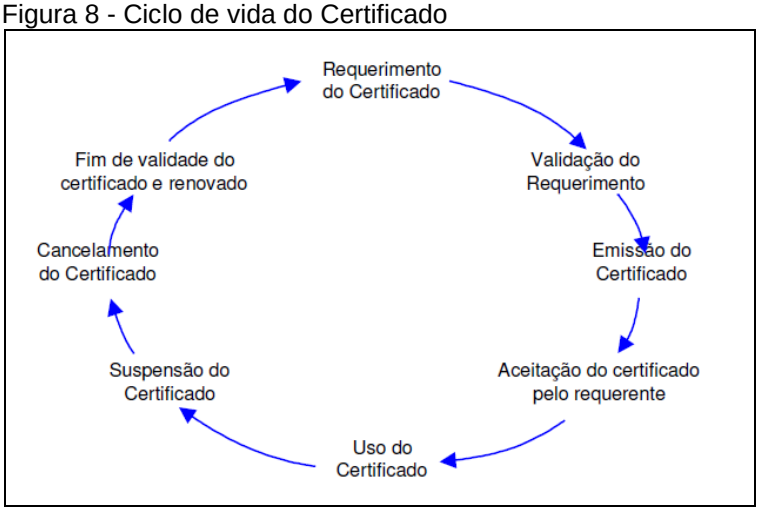
e) uso do certificado: é de total responsabilidade do requerente o uso correto do certificado;

f) suspensão do certificado: é o ato pelo qual o certificado torna-se temporariamente inválido para operações por algum motivo especificado pela AR, como o comprometimento da chave publica.

g) revogação do certificado: é o ato pela qual o certificado torna-se definitivamente inválido, seja pelo comprometimento da chave privada ou ocorrer algum fato que torne o certificado pouco seguro. Com isso, o certificado deve ser publicado em uma Lista de Certificados Revogados (LCR), que será descrito a seguir.

h) término da validade e renovação: assim como a revogação, o vencimento torna um certificado inutilizável.

Figura 8 - Ciclo de vida do Certificado



Fonte: Tadano (2002)

4.1.3 Lista de certificados revogados

Todo certificado emitido tem um prazo de validade, e é esperado que ele seja usado durante todo esse período. No entanto, várias circunstâncias podem causar a revogação de um certificado antes da expiração da validade. Tais circunstâncias incluem a troca de nome, mudança de associação entre o sujeito e a AC (por exemplo, um empregado deixa de trabalhar em uma organização), suspeita do comprometimento da chave privada correspondente. Sob tais circunstâncias, a autoridade responsável tem de revogar o certificado.

Como visto em Housley et al (1999), uma Lista de Certificados Revogados (LCR), é uma lista pública que é assinada por uma Autoridade Certificadora, e que contém certificados que de alguma forma não são mais válidos. Nessa lista, cada certificado é identificado pelo seu número de série.

É importante salientar que O certificado digital é o elemento mais básico de uma Infraestrutura de Chaves Públicas.

4.2 INFRAESTRUTURA DE CHAVES PÚBLICAS

Como visto em Cooper et al (2005), uma Infraestrutura de Chaves Públicas (ICP), é um conjunto de hardware, software, pessoal, política e procedimentos utilizados por uma Autoridade Certificadora para emitir e gerar certificados. Uma ICP também provê serviços de segurança para empresas que utilizam criptografia de chave pública. Esses serviços geralmente são implementados em ambientes de redes, trabalhando em conjunto com os softwares o lado cliente. A ICP Brasileira foi definida pela Medida Provisória Nº 2.200-2, de 24 de Agosto de 2001.

Conforme Housley e Polk (2001, tradução nossa), uma ICP é composta de vários componentes, cada um designado para realizar uma determinada tarefa. São eles: Autoridade Certificadora, Autoridade de Registro e os Repositórios.

4.2.1 Autoridade Certificadora

Uma Autoridade Certificadora (AC), é bloco básico em uma ICP. A AC é conhecida por dois atributos: nome e chave pública. Como apresentado por Housley e Polk (2001, tradução nossa), ela pode emitir certificados para usuários, outras ACs, ou para os dois. Quando ela emite um certificado, desta forma está atestando que o sujeito (a entidade presente no certificado), possui a chave privada correspondente à chave pública que está contida no certificado. Se a autoridade inclui informações adicionais no certificado, ela está assegurando que estas informações são verdadeiras.

Quando o sujeito é outra AC, o emissor garante que os certificados emitidos por essa autoridade são confiáveis. Ela também pode emitir uma Lista de Certificados Revogados (LCR). Essa autoridade somente pode emitir um certificado após a requisição de um certificado ser aprovado por uma Autoridade de Registro confiável.

4.2.2 Autoridade de Registro

Conforme apresentado por Housley e Polk (2001, tradução nossa), uma Autoridade de Registro (AR), tem como função verificar o conteúdo de um certificado. O conteúdo de um certificado deve refletir as informações apresentadas pela entidade que

solicitou o certificado. Cada AC possui uma lista de AR confiáveis e cada AR é identificada por um nome por uma chave pública. Essa autoridade somente faz verificações, ela não consegue emitir certificados.

Uma AR comumente fornece ainda essas funções (BURNETT; PAINE, 2002):

a) aceitar e verificar as informações de registro sobre novos registradores;
b) gerar chaves em favor de usuários finais;
c) aceitar e autorizar solicitações para um backup e uma recuperação de chave;
d) aceitar e autorizar solicitações para revogação de certificado;
e) distribuir ou recuperar dispositivos de hardware como tokens quando necessário.

4.2.3 Repositórios

Um repositório serve como ponto de distribuição de certificados e LCRs. Aceita certificados e LCRs de uma ou mais autoridade certificadoras, e os disponibiliza para terceiros que precisam deles para implementação de serviços de segurança. Housley e Polk (2001, tradução nossa) cita que um repositório é um sistema, acessível por endereços e protocolos e provê certificados e LCR para solicitação. A solicitação pode ser baseada no nome do usuário ou AC, ou outras informações.

5 TRABALHOS CORRELATOS

Neste capítulo são apresentados projetos com características semelhantes com o objetivo desta pesquisa, porém com seu foco alterado para outras funcionalidades.

5.1 APLICAÇÃO DE CRIPTOGRAFIA PARA SEGURANÇA DE MICROSD PARA ANDROID

Este trabalho de conclusão de curso foi proposto pelo Acadêmico Fábio Roberto da Silva no curso de Ciência da Computação, pela Universidade Anhembi Morumbi, no ano de 2010.

A proposta visa o estudo sobre segurança em dispositivos móveis e o desenvolvimento de um aplicativo que ofereça um mecanismo que aumente a segurança de dados no cartão de memória do smartphone que usa a plataforma Android.

5.2 DESENVOLVIMENTO DE APLICAÇÕES EMBARCADAS COM ANDROID

Proposto pelo Acadêmico Diogo Bonoto Salaberri do curso de Ciência da Computação pela Universidade Federal de Pelotas no ano de 2011, como requisito para obtenção do título de bacharel em Ciência da Computação.

Neste trabalho, o acadêmico realiza um estudo sobre o desenvolvimento de softwares embarcados para dispositivos móveis, sendo o sistema Android o principal objeto de estudo.

5.3 M-COMMERCE E A PLATAFORMA GOOGLE ANDROID

Trabalho de Conclusão de Curso apresentado pelo Acadêmico Diego Gomes Antonelli, pela Universidade do Extremo Sul Catarinense no ano de 2011.

A pesquisa apresenta um protótipo de sistema de comércio móvel utilizando a plataforma Google Android e serviços de intercâmbio de dados para permitir a compra de produtos utilizando por meio de celulares contendo a plataforma.

5.4 INTERFACEAMENTO ENTRE DISPOSITIVOS MÓVEIS E JOGOS ELETRÔNICOS DE COMPUTADORES UTILIZANDO O ACELERÔMETRO BASEADO NO SISTEMA OPERACIONAL ANDROID

Trabalho de Conclusão de Curso apresentado pelo Acadêmico William Bertan da Silva, pela Universidade do Extremo Sul Catarinense no ano de 2012.

A pesquisa apresenta um estudo sobre a plataforma Android, descrevendo sua arquitetura e funcionamento. E também o desenvolvimento de uma aplicação que utiliza o sensor de movimentos do dispositivo móvel com Android para controle de jogos eletrônicos em um servidor remoto.

5.5 AUTORIDADE CERTIFICADORA DE CORREIO ELETRÔNICO

Trabalho de Conclusão de Curso apresentado pelo acadêmico Martín Augusto Gagliotti Vigil, pela Universidade Federal de Santa Catarina, ano de 2007.

A pesquisa apresenta um estudo sobre criptografia e certificação digital. E por fim o desenvolvimento de uma autoridade certificadora de correio eletrônico.

6 APLICAÇÃO E-MAIL SEGURO

A pesquisa teve como objetivo o estudo da utilização de certificação digital em dispositivos móveis, a partir da plataforma Google Android.

Também se buscou o desenvolvimento de uma aplicação capaz de criptografar e assinar emails utilizando o conceito de certificação digital apresentados.

6.1 METODOLOGIA

A primeira etapa desta pesquisa compreende o levantamento bibliográfico a fim de obter referencial teórico. O principal estudo foi em relação à segurança em dispositivos móveis, criptografia e certificação digital. Em seguida, viu-se a necessidade de estudar e entender a plataforma Google Android, descrevendo suas características, e também seu kit de desenvolvimento. Também foi descrito os conceitos de segurança, com foco em criptografia e certificação digital.

Para o desenvolvimento da aplicação foram necessários alguns recursos, todos disponibilizados pelo próprio acadêmico. Recursos de *hardware* foram utilizados para se alcançar o objetivo, sendo eles um computador com sistema operacional Windows; dispositivo móvel com sistema operacional Android. Também se fez necessário alguns recursos de *software*, onde foi necessário um ambiente de desenvolvimento Eclipse com o SDK Android para o desenvolvimento da aplicação para o dispositivo móvel.

6.1.1 Ferramentas

A aplicação foi desenvolvida utilizando a *Integrated Development Environment* (IDE) Eclipse: Indigo Service Release 1 Build id: 20110916-0149, sendo que esta fora selecionada por possuir uma melhor integração com o Android SDK e suas ferramentas.

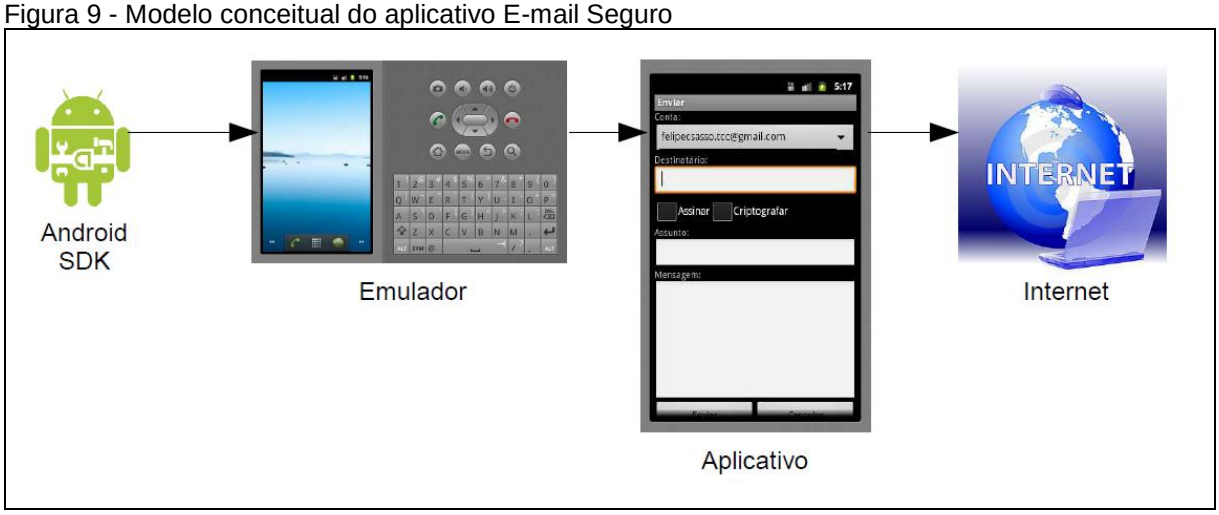
Foram utilizadas a ferramentas Android SDK 2.3.3, revisão 10, que é a API da plataforma utilizada no projeto; Android Development Toolkit (ADT) versão 12 que é um *plugin* para a IDE Eclipse ao qual proporciona um ambiente integrado, sendo assim, criar novos projetos de desenvolvimento para a plataforma, criar

aplicações de interface com usuários, entre outros recursos; Android SDK e AVD Manager, responsável pelo gerenciamento das API's e AVD's instaladas e disponíveis para uso, sua interface é intuitiva e simples como pode ser observado; Android Virtual Device (AVD), simula a plataforma Android em um dispositivo móvel, rodando a plataforma Android 2.3.3; e, LogCat ficando como responsável por auxiliar, ao desenvolver, depurar erros, sendo que ele mostra um log completo do sistema operacional e mensagens internas de aplicativos. Para a cifragem e assinatura de emails, foi utilizada a biblioteca *BouncyCastle*, que é uma coleção de APIs usadas para criptografia. Estão disponíveis em Java e C# e oferecem suporte para questões de segurança, tal como para certificados, assinaturas digitais, entre outros, além da biblioteca JavaMail-Android, para o envio de emails.

6.2.2 Modelagem Conceitual

O sistema desenvolvido possui uma estrutura envolvendo diferentes tecnologias. Na figura 9 é exposto o modelo conceitual do sistema.

Figura 9 - Modelo conceitual do aplicativo E-mail Seguro



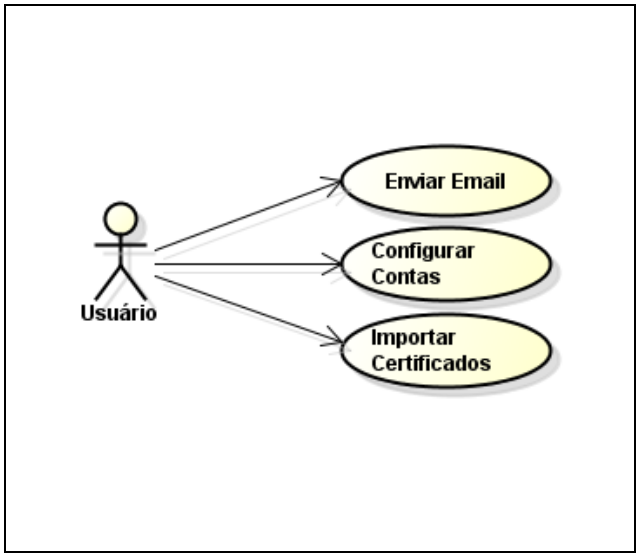
Fonte: Do Autor.

Como demonstrado na figura 9, o sistema é composto do SDK da plataforma, emulador ou celular com o Sistema Operacional Android, o aplicativo em si e conexão com a Internet, sendo que entre o aplicativo e a Internet, existe transferência de informações.

Na figura 10 demonstra-se o caso de uso da aplicação móvel, nela pode-se notar as principais funcionalidades da aplicação, ao qual seriam: Enviar Email, responsável pelo envio de emails, assinados ou cifrados; Configurar Contas, onde

pode-se adicionar novas contas de correio eletrônico que serão utilizadas para enviar emails; e Importar Certificados, responsável pela importação de certificados digitais que serão utilizados para criptografia.

Figura 10 - Diagrama de caso de uso da aplicação móvel



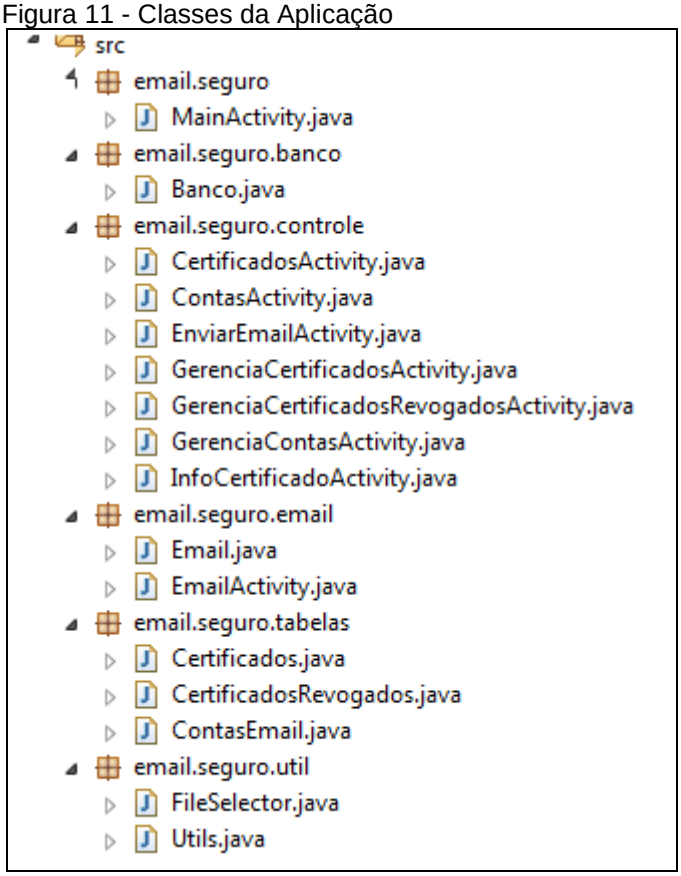
Fonte: Do autor.

6.2.3 Implementação

Com as tecnologias a serem usadas no projeto definidas, e com o estudo dessas, foi dado continuidade as etapas metodológicas, seguindo com a implementação da aplicação móvel.

A aplicação conta com os pacotes "email", "controle", “tabelas”, "banco" e “util”. A figura 11 demonstra todos os pacotes e suas respectivas classes e activities:

Figura 11 - Classes da Aplicação



Fonte: Do Autor.

No pacote "*email*" tem-se a *activity EmailActivity.java*, responsável pelo envio, através do método send(Email email), assinatura, utilizando método assinaEmail(), e a cifragem de emails, através da função cifrarEmail().

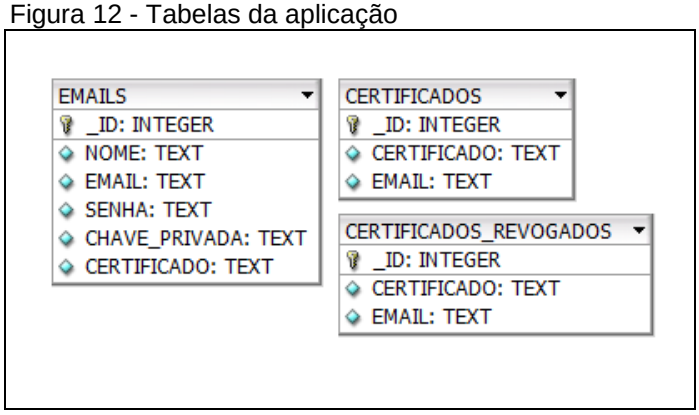
No pacote “controle” se tem as activities responsáveis pelo gerenciamento de contas de email e certificados. O gerenciamento das contas de email se faz através da Activity “*GerenciaContasActivity.java*”, onde é possível o cadastro, edição e exclusão de contas.

No pacote “controle”, tem-se a *activity* “GerenciaCertificadosActivity.java”, responsável pela importação e gerenciamento dos certificados, onde também é possível ver os detalhes dos certificados importados, como data de validade, emissor, chave pública, entre outros, por meio da activity “InfoCertificadoActivity.java”.

O pacote “tabelas” possui as definições de todas as tabelas utilizadas na aplicação. As tabelas nesse pacote foram modeladas a partir de classes que implementam a *interface BaseColumns*, que conforme visto em Android (2012), faz

com que a modelagem de banco de dados seja mais harmoniosa. A figura 12 demonstra as tabelas existentes no banco de dados da aplicação:

Figura 12 - Tabelas da aplicação



Fonte: Do Autor

No pacote “banco” está a classe responsável pela criação e gerenciamento do banco de dados da aplicação, onde se é possível definir o nome do banco da aplicação e também controlar sua versão. A criação das tabelas é feita no método público *onCreate(SQLiteDatabase db)*, onde se é utilizado as tabelas definidas na pacote “tabelas”.

6.2.4 Funcionamento

A aplicação utiliza os conceitos de certificação digital apresentados anteriormente, aplicada no envio de mensagens de correio eletrônico, onde estas podem ser assinadas ou criptografadas.

O funcionamento da aplicação é de forma simples. Na tela inicial existem três botões, sendo eles “Certificados”, “Adicionar conta do Gmail” e “Enviar E-Mail”.

Acessando o botão “Certificados”, tem-se mais outros dois botões, que são “Certificados” e “Certificados Revogados”. No botão “Certificados”, pode-se importar certificados de terceiros, que serão utilizados para a criptografia. Para importar, é necessário clicar no botão “Menu” do dispositivo móvel, e assim, realizar a importação do certificado. Ao importar um certificado, o aplicação irá verificar se o certificado está ou não com a data de validade expirada. Caso não esteja, a importação será concluída, caso contrário, o certificado será movido para a tabela de certificados revogados. Concluída a importação, o certificado aparecerá numa lista,

ainda em “Certificados”, sendo possível sua exclusão e também a visualização dos dados do certificado, como demonstrado na figura 13:

Figura 13 - Tela de informações do certificado

Fonte: Do Autor

Em “Certificados Revogados” estão os certificados que foram importados, mas que estão com data de validade expirada. Assim como em “Certificados”, aqui é possível ver as principais informações do certificado selecionado.

Em “Adicionar conta do Gmail”, é possível adicionar uma conta de correio eletrônico do Google Mail, sendo que foi escolhido esse servidor de correio eletrônico devido aos usuários do Android necessitarem de uma conta do Google e Gmail. Para isso é necessário clicar em “Menu” no dispositivo móvel, e selecionar “Adicionar”. A tela de cadastro possui 4 campos, sendo eles: E-Mail, onde o usuário informará a conta do correio eletrônico do Google Mail; Senha, onde será informado a senha da conta adicionada; Nome, onde o usuário informará o nome que aparecerá para outros usuários; e Certificado para Assinatura, que será o certificado que fará a assinatura das mensagens. Para este certificado será solicitado uma

senha para ao usuário, para que o certificado seja armazenado criptografado. Após o cadastro, também é possível a edição e exclusão de uma conta.

A figura 14 demonstra um conta de correio eletrônico sendo cadastrada.

Figura 14 - Cadastro de e-mails

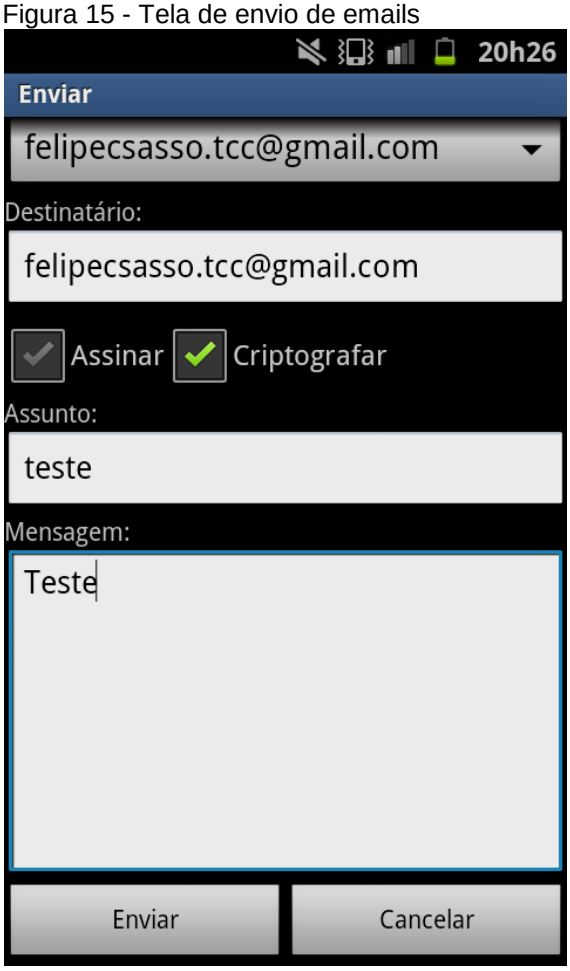
Fonte: Do Autor

Na tela principal, em “Enviar E-Mail”, o usuário poderá as enviar mensagens de correio eletrônico de três formas diferentes, sejam elas assinadas, cifradas ou sem o uso da criptografia. Em “Conta”, estarão disponíveis as de email cadastradas anteriormente, onde o usuário poderá selecionar qual será utilizada para o envio. Em “Destinatário”, serão informados os emails que serão o destino das mensagens enviadas, e por fim, os campos “Assunto” e “Mensagem”.

Ao enviar um email, o usuário terá as opções e cifrar ou assinar a mensagem. Caso selecione “Criptografar” e clique em “Enviar”, a aplicação irá buscar os certificados referentes aos emails informados em “Destinatário”, para realizar a criptografia. Caso algum email informado não possui um certificado equivalente, será emitida a mensagem “Para os destinatários sem certificados importados, o e-mail não foi enviado”. Para os destinatários com certificados válidos,

o email será enviado cifrado. Caso o usuário selecione a opção “Assinar” e clique em “Enviar”, a aplicação irá buscar o certificado importado no cadastro da conta selecionada, e irá utilizá-lo para assinar a mensagem. Caso não exista um certificado associado à conta de correio eletrônico informada, será emitida a mensagem “Não existe certificado associado à conta de e-mail”. A figura 15 demonstra a tela de envio de emails:

Figura 15 - Tela de envio de emails



Fonte: Do Autor

6.2.3 Testes de implementação

Os testes de implementação da aplicação ocorreram no emulador do kit de desenvolvimento, sob as configurações WQVGA400 (400x240) e 256Mb de memória RAM. Para fins de testes de criptografia e validação de assinatura, utilizou o Mozilla Thunderbird[1], versão 13.0, por ser uma ferramenta multiplataforma, gratuita e de código-fonte aberto, e também por suportar o padrão S/MIME. No aplicativo foram adicionadas contas de emails, e importados certificados digitais. Após, foram enviados alguns emails, assinados e cifrados para uma conta de correio eletrônico criada anteriormente, e que fora configurada no Thunderbird.

6.3 RESULTADOS OBTIDOS

Como resultado dessa pesquisa obteve-se uma aplicação móvel para o sistema operacional Google Android, onde é possível a criptografia e assinatura de mensagens de correio eletrônico, utilizando os conceitos apresentados. Esta pesquisa proporcionou a descrição de diversos conceitos envolvendo segurança na troca de informações, bem como a plataforma Google Android e seu kit de desenvolvimento.

Pôde-se concluir que todos os objetivos propostos no início da pesquisa foram atingidos, tendo como resultado uma aplicação de código livre e disponível a qualquer acadêmico que queira continuar e/ou utilizá-la como variantes de outros projetos.

[1] Cliente de e-mail.

7 CONCLUSÃO

Em um cenário onde o correio eletrônico é uma das ferramentas mais utilizada para a comunicação na Internet, na qual muitas informações confidenciais são transmitidas, garantir a segurança desses dados é essencial, e o uso da criptografia e assinatura digital é certamente a melhor maneira de garantir o sigilo e autenticidade dessas informações.

Durante a pesquisa foram efetuados estudos nos quais proporcionaram o entendimento sobre a plataforma Google Android, suas características de desenvolvimento e aspectos. Além do conhecimento adquirido para a plataforma móvel, obtiveram-se também conhecimentos no que tange a criptografia e certificação digital.

Através de toda essa gama de conhecimentos adquiridos, tornou-se viável alcançar o objetivo principal desta pesquisa que consistiu no desenvolvimento um aplicativo para correio eletrônico, que utilize de conceitos de segurança de dados por meio de criptografia e certificação digital.

O resultado da pesquisa demonstrou as possibilidades na junção de criptografia com certificação digital, e assim obtendo mais um mecanismo de segurança, para que dessa forma fosse possível demonstrar a viabilidade do estudo proposto, e atingir seus objetivos. A aplicação móvel gerada é exclusiva para a plataforma citada, não sendo possível sua execução em outras plataformas.

Durante o desenvolvimento prático do projeto, ocorreram algumas dificuldades, uma delas foi em relação ao uso das bibliotecas criptográficas. A princípio, se utilizaria a biblioteca BouncyCastle para a criptografia e assinatura, no entanto, verificou-se que a plataforma Android já possuí internamente uma versão mais antiga dessa biblioteca, o que impossibilita o uso de alguma versão atualizada, pois o sistema apenas reconhece a biblioteca interna. Com isso se fez necessária a utilização da biblioteca SpongyCastle, que basicamente tem as mesmas classes e funções do BouncyCastle, mas foi renomeada para ser utilizada pelo sistema Android sem entrar em conflito com a primeira.

A partir dos dados gerados por esta pesquisa, bem como as tecnologias abordadas, ficam como sugestões para trabalhos futuros:

a) desenvolvimento da decifragem de anexos cifrados pelo S/MIME e também a validação de anexos assinados;

b) habilitar na aplicação a possibilidade da criptografia e/ou assinatura de arquivos;

c) possibilitar a adição de contas de e-mail de outros servidores;

d) integração do aplicativo com clientes de e-mail existentes na plataforma;

Com isso, é necessário observar a importância da área de segurança da informação, visto que esta é mais uma pesquisa, e que há necessidade de sempre estar melhorando as pesquisas nesta área.

REFERÊNCIAS

ABLESON, W. Frank; SEN, Robi; KING, Chris. **Android in Action**. Second Edition [S. l.]: Manning Publications, 2011.

ANDROID. **Android Developers**. Disponível em: <http://developer.android.com> Acesso em: 11 jun. 2012.

ANJOS, Júlio. **Comparativo APIs Android x JavaME**, Porto Alegre: Universidade Federal do Rio Grande do Sul, BR-RS, 2008. 10 f. Disponível em: <https://saloon.inf.ufrgs.br/twiki-data/Disciplinas/CMP167/TF08JulioAnjos/artigo-comparativo.pdf>. Acesso em: 08 set. 2012.

ANTONELLI, Diego G. **M-Commerce e a Plataforma Google Android.** 2011. 90 p. Trabalho de Conclusão de Curso – Universidade do Extremo Sul Catarinense, Criciúma.

AQUINO, Juliana França Santos. **Plataforma de desenvolvimento para dispositivos móveis**. Pontifícia Universidade Católica do Rio de Janeiro. Rio de Janeiro: 2007. Disponível em: <http://www-di.inf.pucrio.br/~endler/courses/Mobile/Monografias/07/Android-Juliana-Mono.pdf>. Acesso em: 08 set. 2012.

BUCHMANN, Johannes A. **Introdução à Criptografia**. São Paulo: Berkeley, 2002.

BURNETT, Steve. PAINE, Stephen. **Criptografia e Segurança: O Guia Oficial RSA.** Rio de Janeiro: Campus, 2002.

BUSINESSWIRE. **Nearly 1 Billion Smart Connected Devices Shipped in 2011 with Shipments Expected to Double by 2016, According to IDC.** Disponível em: <http://www.businesswire.com/news/home/20120328005370/en/1-Billion-Smart-Connected-Devices-Shipped-2011> Acesso em: 06 jun. 2012.

CANALYS. **Google's Android becomes the world's leading smart phone platform.** Disponível em: <http://www.canalys.com/newsroom/google%E2%80%99s-android-becomes-world%E2%80%99s-leading-smart-phone-platform>. Acesso em: 06 jun. 2012.

CARVALHO, Daniel Balparda de. **Segurança de Dados com Criptografia: Métodos e Algoritmos**. Rio de Janeiro: Book Express, 2001.

CERT. **Incidentes Reportados ao CERT.br**. Disponível em: <http://www.cert.br/stats/incidentes/2012-jan-mar/tipos-ataque-acumulado.html>. Acesso em: 06 jun. 2012.

CHECKPOINT. **The Impact of Mobile Devices on Information Security.** Disponível em: <http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf>. Acesso em: 06 jun. 2012.

CHERNICK, C. Michael. **COMPUTER SECURITY**. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-49/sp800-49.pdf>. Acesso em: 09 jun. 2012.

COOPER, M. et al. Informational, **RFC 4158. Internet X.509 Public Key Infrastructure: Certification Path Building**. 2005. Disponível em: <http://tools.ietf.org/html/rfc4158>
Acesso em: 27 out. 2011.

DEITEL, Paul. DEITEL, Harvey. **Java: Como Programar.** São Paulo: Pearson, 2010.

DIMARZIO, J. F.; POLO, G. L. **Android, A Programmer's Guide**. [S. l.]: McGraw-Hill Osborne Media, 2008.

HASHIMI, S; KOMATINEMI, S; MACLEAN, D. **Pro Android 2**. Nova Iorque: Apress, 2010.

HOFF, A. V.; SHAIO, S; STARBUCK, O. **Ligado em Java: Criando Sites Web com Applets Java.** São Paulo: Makron Books, 1996.

HOUSLEY, R. et al. Standart Track, **RFC 2459. Internet X.509 Public Key Infrastructure Certificate and CRL Profile**. 1999. Disponível em: <http://www.ietf.org/rfc/rfc2459.txt> Acesso em: 26 out. 2011.

HOUSLEY, Russ. POLK, Tim. **Planning for PKI**: Best Practices Guide for Deploying Public Key Infrastructure. New York: Wiley, 2001.

ISACA**. Securing Mobile Devices**. Disponível em: <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx>. Acesso em: 15 nov. 2011.

KARSH, Marziah. **Android for Work:** Productiviy for Professionals.New York: Apress, 2010.

KOHLER, Jonathan Gehard; BODEMÜLLER JUNIOR, Rogério. **Contribuições ao sistema de gerenciamento do ciclo de vida de certificados digitais da intra-estrutura de chaves públicas para pesquisa e ensino (SGCI)**. Disponível em: <http://projetos.inf.ufsc.br/arquivos_projetos/projeto_691/SGCI2.pdf>. Acesso em: 22 nov. 2011.

KOVACS, Bruno Paulo Usiglio; MONTEIRO, Vanesa de Freitas. **Um estudo prático das ameaças de segurança em dispositivos portáteis com Windows Mobile.** 2006. 56 f. Monografia – Departamento de Informática, Pontifícia Universidade Católica, Rio de Janeiro, BR-RJ. Disponível em:< http://www-di.inf.puc-rio.br/~endler/projects/Anubis/Ameacas.pdf > Acesso em: 09 nov. 2011.

KUHN et al**. Introducion to Public Key Technology and the Feredeal PKI Infrastructure**: NIST, 2001. Disponível em:

<http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf> Acesso em: 13 nov. 2011.

LECHETA, Ricardo de. **Google Android:** Aprenda a criar aplicações para dispositivos móveis com o Android SDK**.** São Paulo: Novatec, 2010.

LIMA, Marcelo F. de. **Assinatura Digital: Solução Delphi e Capicom.** Florianópolis: Visual Books, 2005.

MCFEDRIES, Paul. **Guia incrível do correio eletrônico da Internet**. São Paulo: Makron Books, 1996

MEDEIROS, Carlos Diego Russo. **Segurança da Informação:** Implantação de Medidas e Ferramentas de Segurança da Informação. Disponível em: <http://www.linuxsecurity.com.br/info/general/TCE_Seguranca_da_Informacao.pdf> Acesso em: 16 nov. 2011.

MOECKE, Cristian Thiago. **Assinatura digital de documentos eletrônicos na ICP-Brasil**. Disponível em: <http://projetos.inf.ufsc.br/arquivos_projetos/projeto_790/monografia.pdf>. Acesso em: 22 nov. 2011.

MORENO, E. D.; PEREIRA, F. D; CHIARAMONTE, R. D. **Criptografia em Software e Hardware**. São Paulo: Novatec, 2005.

MORIMOTO, Carlos . **Dicionário técnico de informática**. Disponível em: <http://www.dominiopublico.gov.br/download/texto/hd000001.pdf>. Acesso em: 23 nov. 2011.

MOURA, Gevilácio Aguiar Coelho de. **RNP - Internet guia do usuário**. São Paulo: Ed. Atlas, 1995

NIELSENWIRE. **Android Leads in U.S. Smartphone Market Share and Data Usage**. Disponível em: <http://blog.nielsen.com/nielsenwire/consumer/android-leads-u-s-in-smartphone-market-share-and-data-usage/>. Acesso em: 10 nov. 2011.

OKAMURA, Fábio Rogério Hideki. **Curso Introdutório ao uso do PGP.** Disponível em: <http://www.rnp.br/_arquivo/documentos/ref0181.pdf>. Acesso em: 03 mai. 2012.

OLIVEIRA, Celso Henrique Poderoso de. **SQL : Curso Prático.** São Paulo: Novatec, 2002.

PEREIRA, Lúcio Camilo Oliva. SILVA, Michel Lourenço da. **Android para Desenvolvedores.** Rio de Janeiro: Brasport, 2009.

RESOLUÇÃO Nº 49 , de 03 de Junho de 2008. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/Resolucoes/Resolucao_49.pdf> Acesso em: 13 nov. 2011.

REIS, João Victor do Carmo; GOULART, Paula; MENDES, Luís Augusto Mattos. **Redes Wireless: Segurança uma questão gerencial**. Disponível em: <http://www.fsd.edu.br/revistaeletronica/artigos/artigo12.pdf>. Acesso em: 15 nov. 2011.

REUTERS. **Most of world interconnected through email and social media**. Disponível em: <http://www.reuters.com/article/2012/03/27/uk-socialmedia-online-poll-idUSLNE82Q02120120327> Acesso em: 12 jun. 2012

SALABERRI, Diogo B. **Desenvolvimento de Aplicações Embarcadas com Android.** 2010. Trabalho acadêmico (Graduação) - Bacharelado em Ciência da Computação. Universidade Federal de Pelotas, Pelotas.

SCHNEIER, Bruce. **Applied Cryptography: Protocols, Algorthms, and Source Code in C.** Wiley, 1996.

SILVA, Fábio Roberto da. **Aplicação de criptografia para segurança de MicroSD para Android.** 2010, 50 f. Trabalho de Conclusão de Curso – Universidade Anhembi Morumbi, São Paulo. Disponível em: <http://engenharia.anhembi.br/tcc-10/cco-10.pdf>. Acesso em: 13 nov. 2011.

SILVA, Luciano Édipo Pereira da. **Utilização da plataforma Android no desenvolvimento de um aplicativo para o cálculo do balanço hídrico climatológico**. Monografia. Universidade Estadual do Mato Grosso do Sul. Disponível em <http://bhcmovel.googlecode.com/files/TCC%20-%20Final.pdf>. Acesso em: 08 set. 2012

STALLINGS, Willian. **Cryptography and Network Security: Principles and Practice.** New Jersey: Prentice Hall, 2008.

STEELE, James; TO, Nelson. **The Android Developer's Cookbook: Building Applications with the Android SDK**. New York: Addison-Wesley Professional, 2010.

TANENBAUM, Andrew Stuart. **Computer Networks**. 4. ed. Amsterdam: Elsevier, 2003.

Utilizando Certificação Digital na Plataforma Android por meio do Desenvolvimento de uma Aplicação

Felipe Coral Sasso[1], Paulo João Martins[1]

[1]Curso de Ciência da Computação - Universidade do Extremo Sul Catarinense (UNESC)
Criciúma – SC – Brasil

felipecsasso@gmail.com, pjm@unesc.net

Abstract. *This paper describes the conclusion work submitted to obtain the achievement of bachelor degree in Computer Science at the UNESC, whose goal was the development of an application to sign and encrypt email messages using digital certification, using the Google Android platform. To achieve this goal, we performed a study of the mobile platform used and security in mobile devices. As a result, we obtained an application to the submitted platform that aims to increase the security of e-mail messages using the concepts presented.*

Resumo. *O presente artigo descreve o trabalho de conclusão de curso apresentado para obtenção do grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense, cujo objetivo foi o desenvolvimento de um aplicativo para assinatura e criptografia de mensagens de correio eletrônico utilizando certificação digital, voltado para a plataforma Google Android. Para a realização do mesmo, efetuou-se um estudo sobre a plataforma móvel utilizada e segurança em dispositivos móveis. Como resultado obteve-se uma aplicação para a plataforma apresentada que tem como função aumentar a segurança de mensagens de correio eletrônico utilizando os conceitos apresentados.*

1. Introdução

A cada dia que passa, as pessoas estão cada vez mais conectadas entre si. Com o advento da Internet e dos computadores pessoais, uma informação que antigamente levaria de semanas à meses para chegar ao seu destinatário, hoje leva apenas alguns segundos.

Com o avanço da tecnologia, surgiram os aparelhos móveis, como smartphones, PDAs, celulares, entre outros. Com isto, tornou-se possível a realização de tarefas como acesso a Internet e transmissão de dados de forma móvel, por meio desses dispositivos, o que antes era possível apenas em computadores, que normalmente eram grandes demais para serem transportados.

Com o crescente uso de dispositivos móveis, utilizando a transmissão de dados por redes de telefonia móvel, pode-se estar 100% conectado a grande rede de computadores, o que possibilita ao usuário o uso do correio eletrônico em qualquer lugar e a qualquer momento. Com o uso dessa ferramenta, é necessário garantir a segurança entre as informações transmitidas.

Conforme Tanenbaum (2003), para que dados confidenciais não sejam descobertos, eles devem ser criptografados.

A criptografia consiste num conjunto de métodos e técnicas que tem como objetivo tornar uma informação totalmente ilegível para pessoas não autorizadas, é dividida em dois tipos, simétrica e assimétrica. Na simétrica, uma mesma chave é utilizada tanto para cifrar

quanto decifrar uma informação, já na assimétrica, duas chaves são necessárias para realizar o processo, uma pública que é distribuída livremente, e uma privada, de posse exclusiva do seu respectivo dono. Neste tipo de criptografia, o que uma chave cifra, apenas seu respectivo par decifra.

De acordo com Housley e Polk (2001, tradução nossa), o grande problema da criptografia assimétrica está em determinar quem possui a chave privada correspondente à pública. Para isso surgiu o certificado digital, usado para garantir a ligação entre uma entidade e uma chave pública.

Aliado ao grande número de dispositivos móveis com a plataforma Google Android, essa pesquisa teve como objetivo o desenvolvimento de uma aplicação usando os conceitos de segurança com criptografia e certificados digitais para segurança de mensagens de correio eletrônicos.

2. Android

Como citado em Silva e Pereira (2009), o Android é uma plataforma para tecnologia móvel completa, envolvendo um pacote com programas para celulares, já com um sistema operacional, middleware, aplicativos e interface do usuário. Foi idealizado por uma empresa chamada Android Inc., sendo adquirida pelo Google em 2005 (HASHIMI; KOMATINEMI; MACLEAN, 2010).

No fim de 2007, um grupo de empresas se reuniu em torno da plataforma para formar a Open Handset Alliance (OHA), que consiste em uma aliança de trinta e quatro empresas com o propósito de englobar todos os processos móveis, operadora móvel, fabricante, empresas de semicondutores e microchips, empresas de software, e empresas de comercialização (LECHETA, 2010; PEREIRA, 2009). Parte do objetivo da aliança é inovar rapidamente e responder melhor às necessidades dos consumidores.

A plataforma Android foi concebida para servir as necessidades das operadoras móveis, fabricantes de aparelhos e desenvolvedores de aplicativos (HASHIMI; KOMATINEMI; MACLEAN, 2010). O sistema foi lançado sobre o código aberto na Licença Apache versão 2.0.

Conforme Karch (2010), qualquer um pode usar e modificar o Android em seus aparelhos e desenvolver aplicações de forma gratuita. Como visto em Aquino (2007), os desenvolvedores que pretendem adotar esta plataforma podem utilizar o Android Software Development Kit (SDK) para o desenvolvimento de softwares, embasado na linguagem de programação Java.

2.1 Características

A plataforma possui algumas características que o torna diferente contra os demais, como as seguintes:

2.1.1 Multiprocesso e App Widget

Ainda citando Steele e To (2010, tradução nossa), o sistema operacional Android não restringe o processador a uma única aplicação por vez. Ele faz o gerenciamento de prioridades e threads de uma aplicação. Com isso tem-se o beneficio da multitarefa.

2.1.2. Máquina Virtual Dalvik

Conforme Android (2012, tradução nossa), Dalvik é uma máquina virtual interpretadora que executa arquivos no formato .dex, um formato que é otimizado para ocupar pouco espaço de

armazenamento. A máquina virtual é baseada em registradores, e pode executar classes compiladas em Java que foram transformadas para o formato nativo usando a ferramenta dx.

2.1.3. Armazenamento de Dados

O sistema Android oferece suporte completo para banco de dados SQLite. Diferentemente da maioria dos outros bancos, não tem um servidor em um processo separado. Lê e escreve diretamente para arquivos do disco.

2.2. Arquitetura

Conforme figura 1, a arquitetura interna do Android é separada em cinco camadas: Aplicações, Framework de Aplicações, Bibliotecas Nativas, Android Runtime e o Kernel Linux.

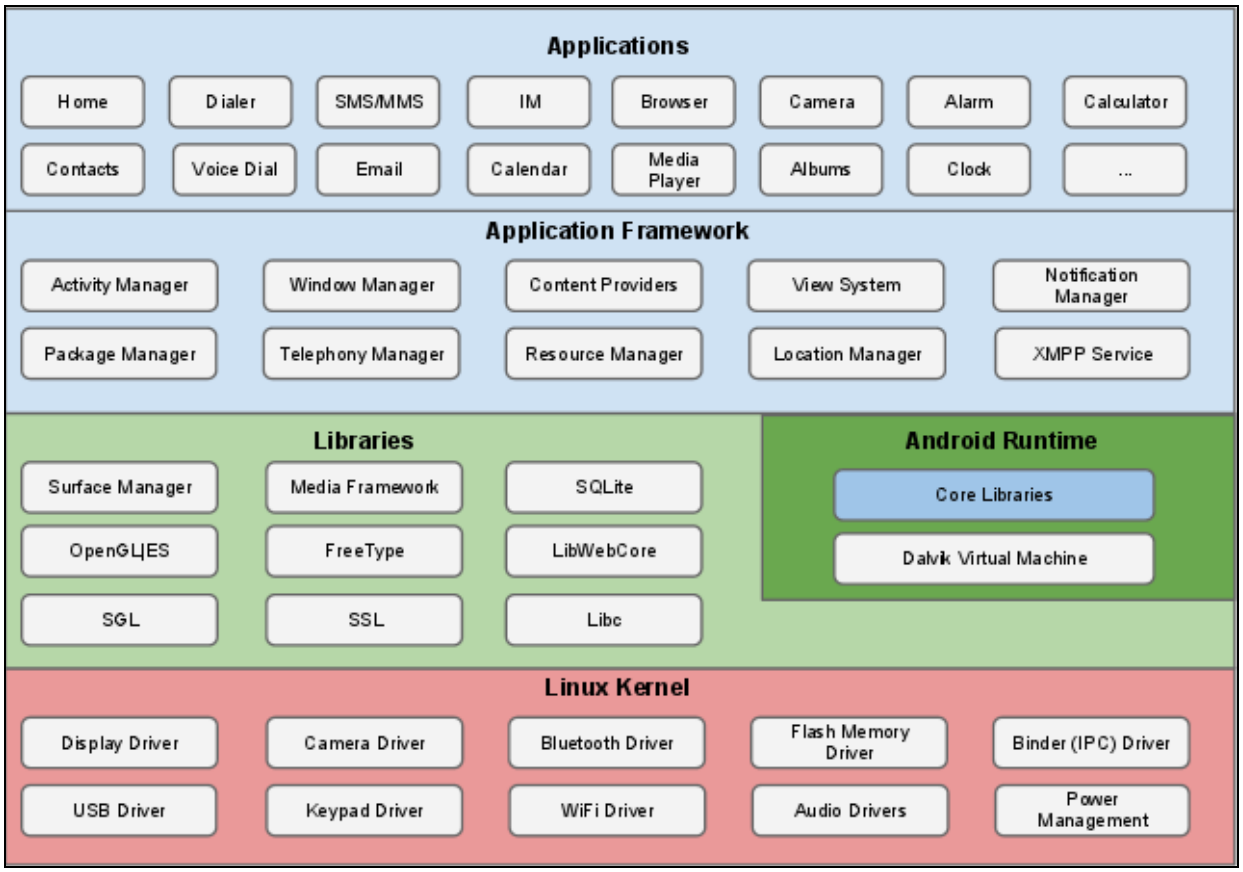


Figura 1. Arquitetura interna

3. Segurança

Conforme Medeiros (2001), a segurança da informação busca reduzir os riscos de vazamento, fraudes, erros, uso indevido, paralisações, roubo de informações ou qualquer outra ameaça que possa prejudicar o sistemas de informações.

Ou seja, a segurança da informação tem como principais objetivo garantir as seguintes propriedades (KOVACS; MONTEIRO, 2006):

a) confidencialidade: propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;

b) integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação

c) disponibilidade: propriedade que garante que a informação esteja sempre disponível para o uso legítimo

d) não repúdio: propriedade que garante que o autor não negue ter criado ou assinado um documento.

3.1. Criptografia

Conforme Carvalho (2001), o objetivo básico da criptografia é tornar uma mensagem ininteligível para um adversário, que possa vir a interceptar uma mensagem.

O processo pela qual a informação é transformada em algo sem sentido é chamada cifragem. O processo inverso chama-se decifragem, onde o texto ilegível ou cifrado é tornado legível como na sua forma original.

Para a realização da cifragem, são necessários dois componentes: um algoritmo, que é um conjunto de instruções matemáticas que faz a transformação da mensagem clara em mensagem cifrada e vice-versa, e uma chave que é um conjunto de bits, aleatórios ou não, que agem em conjunto com o primeiro. Cada chave distinta faz com que o algoritmo trabalhe de uma forma ligeiramente diferente.

3.2. Criptografia Simétrica

Na criptografia simétrica, é utilizado apenas uma chave tanto para a cifragem, quanto para a decifragem de uma informação. Nesse esquema, a chave precisa ser compartilhada entre os usuários autorizados antes que as mensagens possam ser trocadas.

3.3. Criptografia assimétrica

Na criptografia assimétrica, também chamada de criptografia de chave pública, é utilizado um par de chaves, uma pública e uma privada. A primeira será distribuída livremente, normalmente na Internet, já a segunda será conhecida apenas pelo seu dono. As duas chaves são utilizadas para cifragem e decifragem, no entanto, quando alguma informação é cifrada pela pública, apenas a respectiva chave privada poderá realizar a decifração. E quando algo é criptografado pela privada, apenas a respectiva chave pública poderá decifrar a informação.

3.4. Assinatura digital

De acordo com Burnett e Paine (2002), a autenticação permite que alguém no mundo eletrônico confirme sua identidade, e o não repúdio impede que pessoas retifiquem sua palavra eletrônica. Uma maneira de implementar esses recursos é o uso de assinatura digital.Como citado em Buchmann (2002), são utilizadas para assinar documentos eletrônicos.

As assinaturas digitais funcionam da seguinte maneira: Suponha que Alice queira assinar o documento m. Ela utilizará sua chave secreta e criptografará m. Bob, usando a pública correspondente, irá decifrar essa informação. Como é conhecido que apenas a pública pode decifrar algo cifrado pela chave privada, Bob poderá ter certeza que foi Alice que enviou a informação e de que essa não foi forjada.

4. Certificação Digital

Conforme Macedo (2008), a certificação digital é utilizada para autenticar programas, assinaturas de mensagens, documentos eletrônicos, controle de acessos e outros. Surgiu em função da necessidade de manter a integridade e segurança da informação e na interação junto à Internet (BERNARDINELLI, 2010). Marques, Castro e Veras (2011), citam que o uso da

certificação digital em processos eletrônicos assegura alguns aspectos, como privacidade, integridade, autenticidade e não repúdio.

4.1 Certificado Digital

Como visto em Bernardinelli (2010), um certificado digital pode ser entendido como um documento digital que visa identificar pessoas, empresas, computadores entre outras que buscam guardar informações com maior segurança.

Cada certificado contém uma chave pública, e identifica o usuário que possui a chave privada correspondente. Também contém dois campos de data que especificam a emissão e a expiração do certificado.

5. Metodologia

A primeira etapa desta pesquisa compreende o levantamento bibliográfico a fim de obter referencial teórico. O principal estudo foi em relação à segurança em dispositivos móveis, criptografia e certificação digital. Em seguida, viu-se a necessidade de estudar e entender a plataforma Google Android, descrevendo suas características, e também seu kit de desenvolvimento. Também foi descrito os conceitos de segurança, com foco em criptografia e certificação digital.

5.1. Modelagem Conceitual

O sistema desenvolvido possui uma estrutura envolvendo diferentes tecnologias. Na figura 2 é exposto o modelo conceitual do sistema.

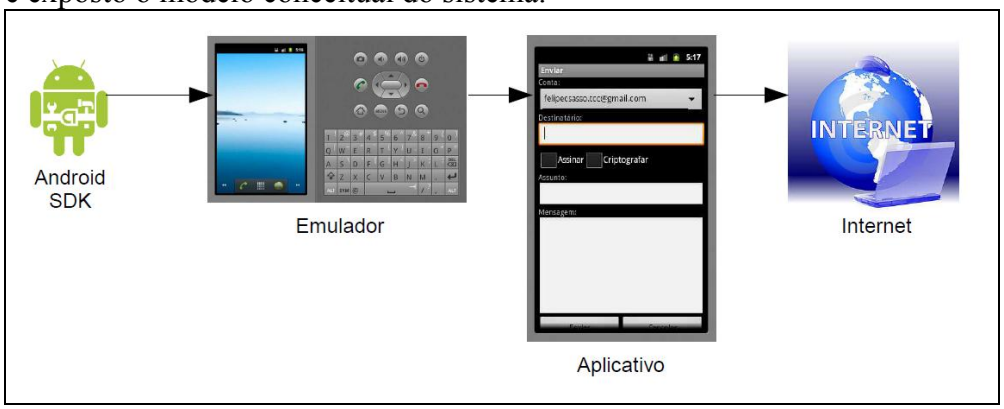


Figura 2. Modelo conceitual do aplicativo

Como demonstrado na figura 2, o sistema é composto do SDK da plataforma, emulador ou celular com o Sistema Operacional Android, o aplicativo em si e conexão com a Internet, sendo que entre o aplicativo e a Internet, existe transferência de informações.

Na figura 3 demonstra-se o caso de uso da aplicação móvel, nela pode-se notar as principais funcionalidades da aplicação, ao qual seriam: Enviar Email, responsável pelo envio de emails, assinados ou cifrados; Configurar Contas, onde pode-se adicionar novas contas de correio eletrônico que serão utilizadas para enviar emails; e Importar Certificados, responsável pela importação de certificados digitais que serão utilizados para criptografia.

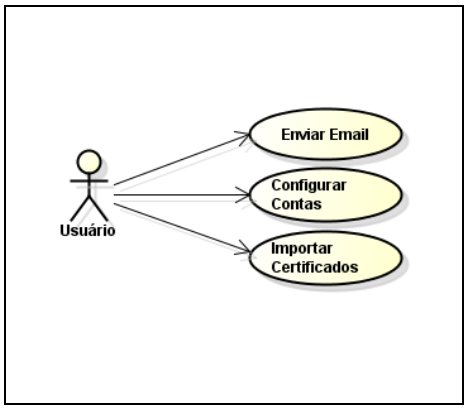


Figura 3. Diagrama de caso de uso da aplicação móvel

5.2 Implementação

Com as tecnologias a serem usadas no projeto definidas, e com o estudo dessas, foi dado continuidade as etapas metodológicas, seguindo com a implementação da aplicação móvel.

A aplicação conta com os pacotes "email", "controle", “tabelas”, "banco" e “util”. A figura 4 demonstra todos os pacotes e suas respectivas classes e activities:

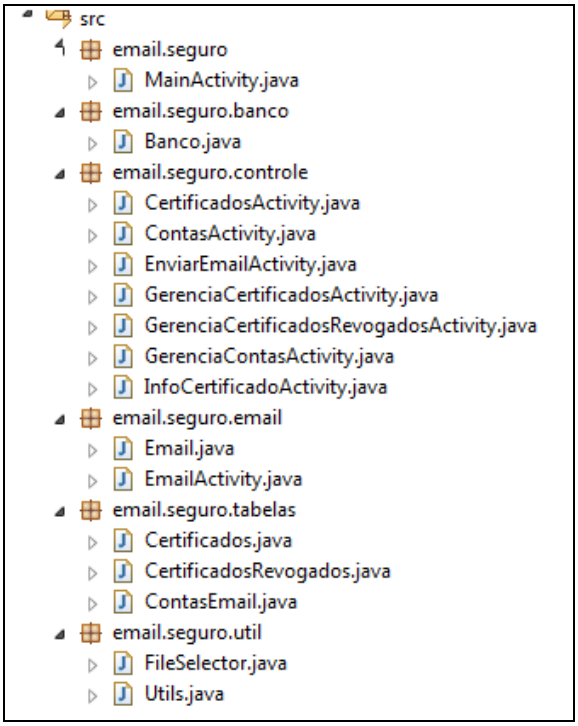


Figura 4. Classes da Aplicação

A figura 5 demonstra as tabelas existentes no banco de dados da aplicação:

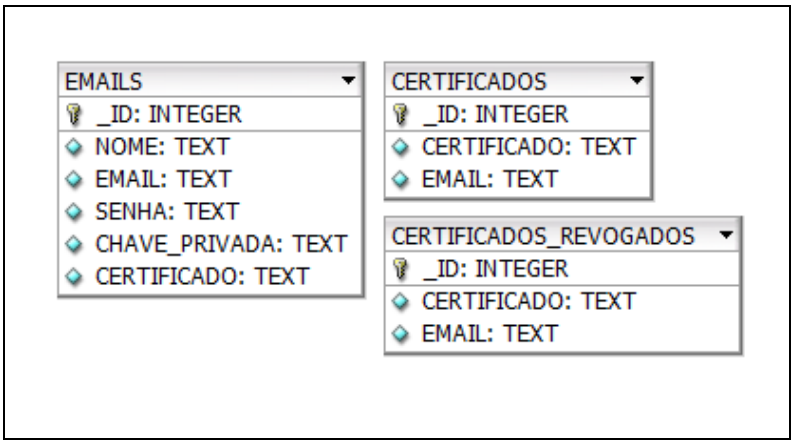


Figura 5. Tabelas da aplicação

5.3 Funcionamento

A aplicação utiliza os conceitos de certificação digital apresentados anteriormente, aplicada no envio de mensagens de correio eletrônico, onde estas podem ser assinadas ou criptografadas.

O funcionamento da aplicação é de forma simples. Na tela inicial existem três botões, sendo eles Certificados, Adicionar conta do Gmail e Enviar E-Mail.

Acessando o botão Certificados, pode-se realizar a importação de certificados que serão utilizados para a criptografia. Caso o certificado importado esteja com a data de validade expirada, será movido para a tabela de Certificados Revogados. É possível ainda o usuário ver os detalhes dos certificados

Em Adicionar conta do Gmail, é possível adicionar uma conta de correio eletrônico do Google Mail, sendo que foi escolhido esse servidor de correio eletrônico devido aos usuários do Android necessitarem de uma conta do Google e Gmail. Ao cadastrar uma nova conta, o usuário poderá importar a chave privada, que será utilizada para a assinatura.

Na tela principal, em Enviar E-Mail, o usuário poderá as enviar mensagens de correio eletrônico de três formas diferentes, sejam elas assinadas, cifradas ou sem o uso da criptografia. A figura 6 demonstra a tela de envio de emails:

Figura 6. Tela de envio de emails

65.4 Testes de implementação

Os testes de implementação da aplicação ocorreram no emulador do kit de desenvolvimento, sob as configurações WQVGA400 (400x240) e 256Mb de memória RAM. Para fins de testes de criptografia e validação de assinatura, utilizou o Mozilla Thunderbird[2], versão 13.0, por ser uma ferramenta multiplataforma, gratuita e de código-fonte aberto, e também por suportar o padrão S/MIME. No aplicativo foram adicionadas contas de emails, e importados certificados digitais. Após, foram enviados alguns emails, assinados e cifrados para uma conta de correio eletrônico criada anteriormente, e que fora configurada no Thunderbird.

5.4 Resultados Obtidos

Como resultado dessa pesquisa obteve-se uma aplicação móvel para o sistema operacional Google Android, onde é possível a criptografia e assinatura de mensagens de correio eletrônico, utilizando os conceitos apresentados. Esta pesquisa proporcionou a descrição de diversos conceitos envolvendo segurança na troca de informações, bem como a plataforma Google Android e seu kit de desenvolvimento.

[2] Cliente de e-mail.

6. Conclusão

Em um cenário onde o correio eletrônico é uma das ferramentas mais utilizada para a comunicação na Internet, na qual muitas informações confidenciais são transmitidas, garantir a segurança desses dados é essencial, e o uso da criptografia e assinatura digital é certamente a melhor maneira de garantir o sigilo e autenticidade dessas informações.

Durante a pesquisa foram efetuados estudos nos quais proporcionaram o entendimento sobre a plataforma Google Android, suas características de desenvolvimento e aspectos. Além do conhecimento adquirido para a plataforma móvel, obtiveram-se também conhecimentos no que tange a criptografia e certificação digital.

Através de toda essa gama de conhecimentos adquiridos, tornou-se viável alcançar o objetivo principal desta pesquisa que consistiu no desenvolvimento um aplicativo para correio eletrônico, que utilize de conceitos de segurança de dados por meio de criptografia e certificação digital. O resultado da pesquisa demonstrou as possibilidades na junção de criptografia com certificação digital, e assim obtendo mais um mecanismo de segurança.

Com isso, é necessário observar a importância da área de segurança da informação, visto que esta é mais uma pesquisa, e que há necessidade de sempre estar melhorando as pesquisas nesta área.

Referências

Android. Android Developers. Disponível em: <http://developer.android.com> Acesso em: 11 jun. 2012.

Anjos, Júlio. Comparativo APIs Android x JavaME, Porto Alegre: Universidade Federal do Rio Grande do Sul, BR-RS, 2008. 10 f. Disponível em: <https://saloon.inf.ufrgs.br/twiki-data/Disciplinas/CMP167/TF08JulioAnjos/artigo-comparativo.pdf>. Acesso em: 08 set. 2012.

Aquino, Juliana França Santos. Plataforma de desenvolvimento para dispositivos móveis. Pontifícia Universidade Católica do Rio de Janeiro. Rio de Janeiro: 2007. Disponível em: <http://www-di.inf.pucrio.br/~endler/courses/Mobile/Monografias/07/Android-Juliana-Mono.pdf>. Acesso em: 08 set. 2012.

Buchmann, Johannes A. Introdução à Criptografia. São Paulo: Berkeley, 2002.

Burnett, Steve. PAINE, Stephen. Criptografia e Segurança: O Guia Oficial RSA. Rio de Janeiro: Campus, 2002.

Carvalho, Daniel Balparda de. Segurança de Dados com Criptografia: Métodos e Algoritmos. Rio de Janeiro: Book Express, 2001.

Dimarzio, J. F.; Polo, G. L. Android, A Programmer's Guide. [S. l.]: McGraw-Hill Osborne Media, 2008.

Hashimi, S; Komatinemi, S; Maclean, D. Pro Android 2. Nova Iorque: Apress, 2010.

Housley, Russ. Polk, Tim. Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure. New York: Wiley, 2001.

Kovacs, Bruno Paulo Usiglio; Monteiro, Vanesa de Freitas. Um estudo prático das ameaças de segurança em dispositivos portáteis com Windows Mobile. 2006. 56 f. Monografia – Departamento de Informática, Pontifícia Universidade Católica, Rio de Janeiro, BR-RJ. Disponível em:< http://www-di.inf.puc-rio.br/~endler/projects/Anubis/Ameacas.pdf > Acesso em: 09 nov. 2011.

Lecheta, Ricardo de. Google Android: Aprenda a criar aplicações para dispositivos móveis com o Android SDK. São Paulo: Novatec, 2010.

Medeiros, Carlos Diego Russo. Segurança da Informação: Implantação de Medidas e Ferramentas de Segurança da Informação. Disponível em: <http://www.linuxsecurity.com.br/info/general/TCE_Seguranca_da_Informacao.pdf> Acesso em: 16 nov. 2011.

Pereira, Lúcio Camilo Oliva. SILVA, Michel Lourenço da. Android para Desenvolvedores. Rio de Janeiro: Brasport, 2009.

Steele, James; To, Nelson. The Android Developer's Cookbook: Building Applications with the Android SDK. New York: Addison-Wesley Professional, 2010.

Tanenbaum, Andrew Stuart. Computer Networks. 4. ed. Amsterdam: Elsevier, 2003.