ESTGA-UA

Proteção de Aplicações

Trabalho para Segurança Informática

Realizado por: Tiago Silva (Nº Mec. 87913)

Ano letivo 2019/2020 | 1º semestre

1 Índice

Proteção de Aplicações 0

1 Índice 1

2 Introdução 2

3 Arquitetura da Solução Pensada 3

3.1 Iniciação do Autor 3

3.2 Processamento do pedido de registo pelo Autor 4

3.3 Iniciação da Biblioteca 5

3.4 Efetuar um pedido de registo pela Biblioteca 6

3.5 Validação da licença por parte da Biblioteca 7

4 Funcionalidades Implementadas 8

5 Deficiências 10

6 Fontes Utilizadas 11

2 Introdução

O presente relatório foi elaborado como parte integrante do trabalho, associado à unidade curricular Segurança Informática, da Licenciatura em Tecnologias da Informação da Escola Superior de Tecnologia e Gestão de Águeda.

Neste trabalho foi proposto "desenvolver um sistema que permita distribuir aplicações de forma segura, garantindo que apenas são executadas pelos donos legítimos das mesmas."

O código da solução implementada encontra-se aqui: https://github.com/tiagomarquessilva/si

O presente relatório descreve a solução implementada.

3 Arquitetura da Solução Pensada

Para a solução trabalhar de forma correta o Autor deve estar a correr antes da Biblioteca.

Existem nesta solução 3 pares de chaves assimétricas:

- Par de chaves geradas para o Autor (Ak+ e Ak-);
- Par de chaves geradas para a Biblioteca (Lk+ e Lk-);
- Par de chaves do cartão de cidadão, sendo que o certificado do mesmo é considerado a componente pública (Uc e Uk-);

3.1 Iniciação do Autor

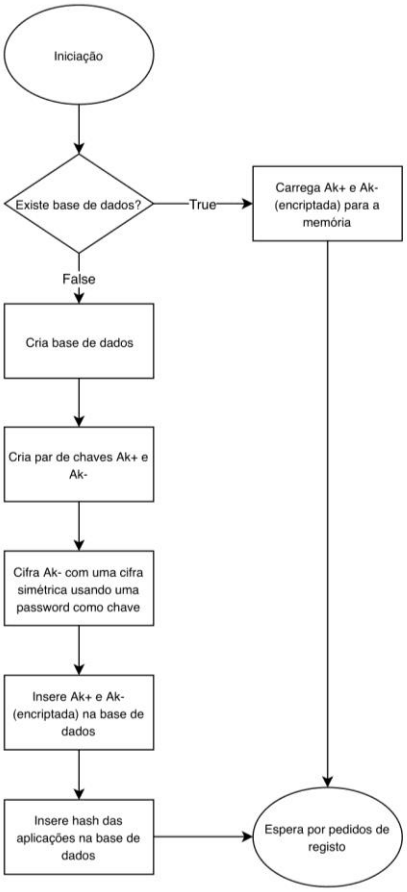

Figura 1 - Fluxograma da iniciação do autor

Neste fluxograma é descrita a iniciação do Autor. De destacar aqui a proteção com password da Ak-, pois as chaves privadas não devem ficar em claro.

3.2 Processamento do pedido de registo pelo Autor

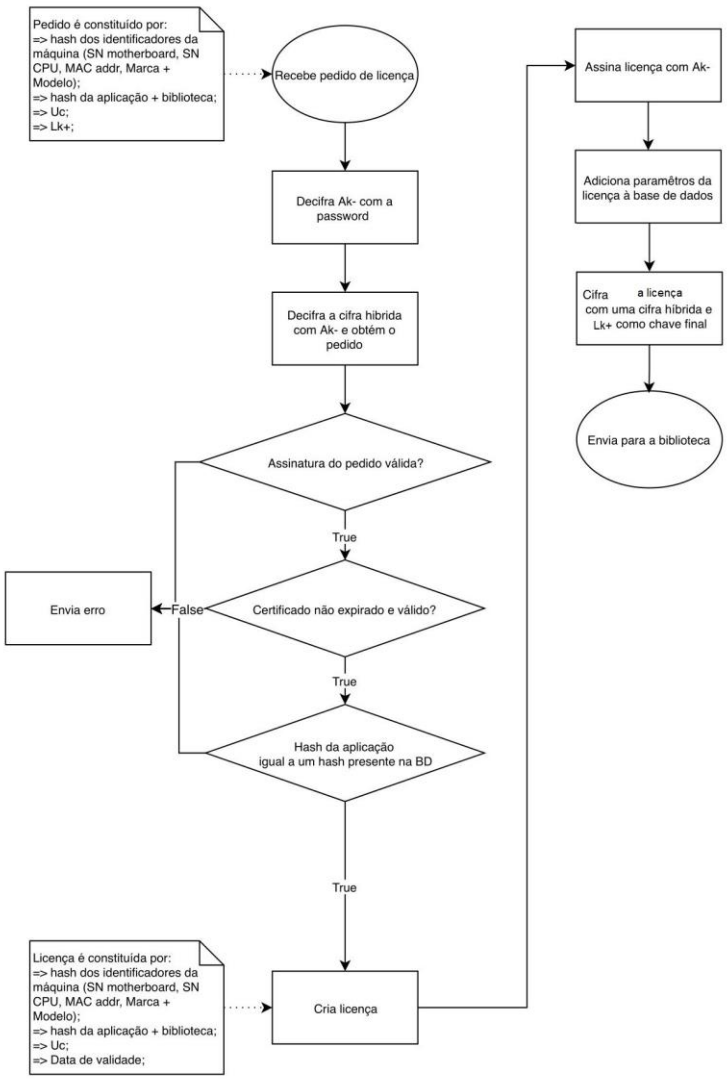

Figura 2 - Fluxograma de processamento de um pedido de registo pelo Autor

Neste fluxograma é descrito o processamento de um pedido de registo por parte do Autor. De destacar a:

- Validação do pedido de licença para garantir que é um utilizador real e para uma aplicação que esteja na base de dados:
- Assinatura da licença e sua cifra para garantir a integridade, autenticidade e confidencialidade;

3.3 Iniciação da Biblioteca

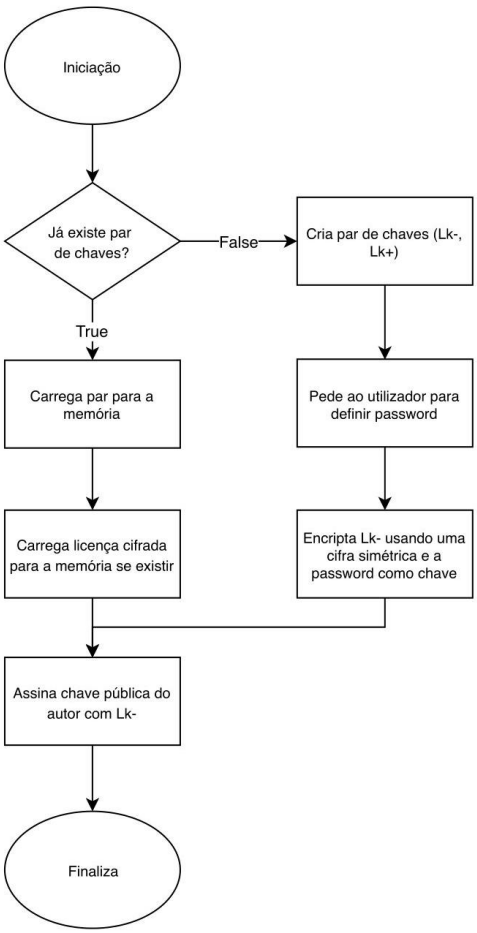

Figura 4 - Fluxograma de iniciação da biblioteca

Biblioteca

Neste fluxograma é descrita a iniciação da Biblioteca. De destacar aqui a proteção com password da Lk-, pois as chaves privadas não devem ficar em claro.

3.4 Efetuar um pedido de registo pela Biblioteca

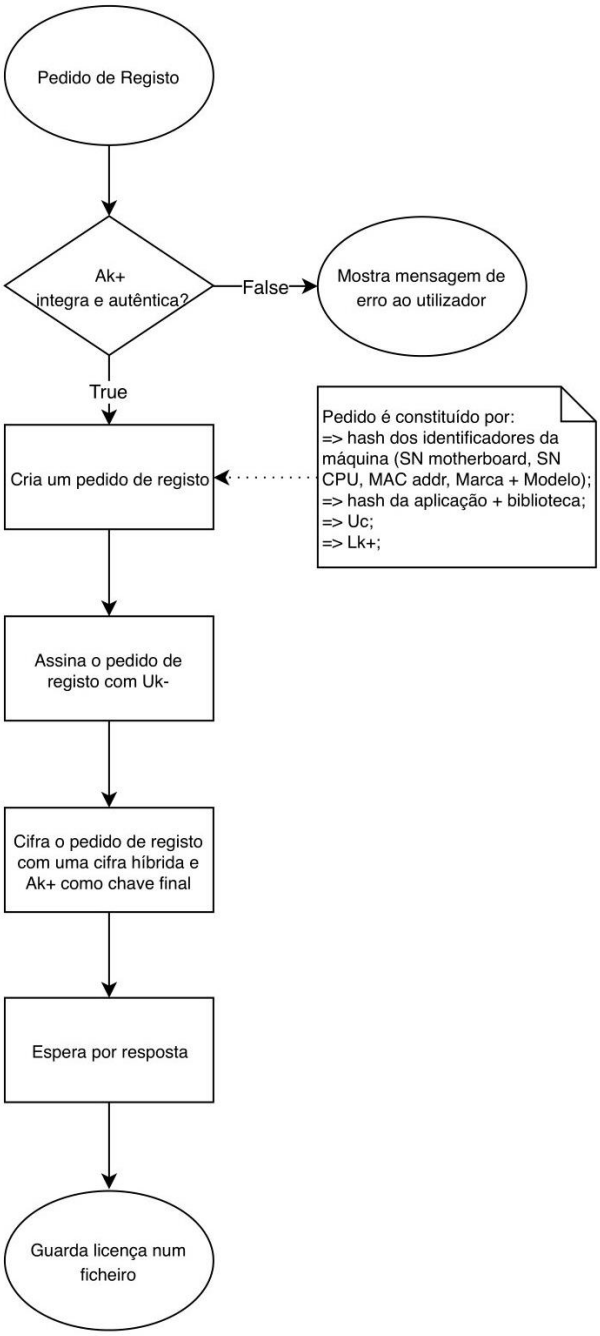

Figura 5 - Fluxograma de um pedido de registo da Biblioteca

Neste fluxograma é descrito o pedido de registo por parte da Biblioteca. De destacar a:

- Validação da chave pública garantindo que iremos cifrar com uma chave integra e autêntica;
- Assinatura do pedido de registo e posterior cifra garantido a sua autenticidade, integridade e confidencialidade;

3.5 Validação da licença por parte da Biblioteca

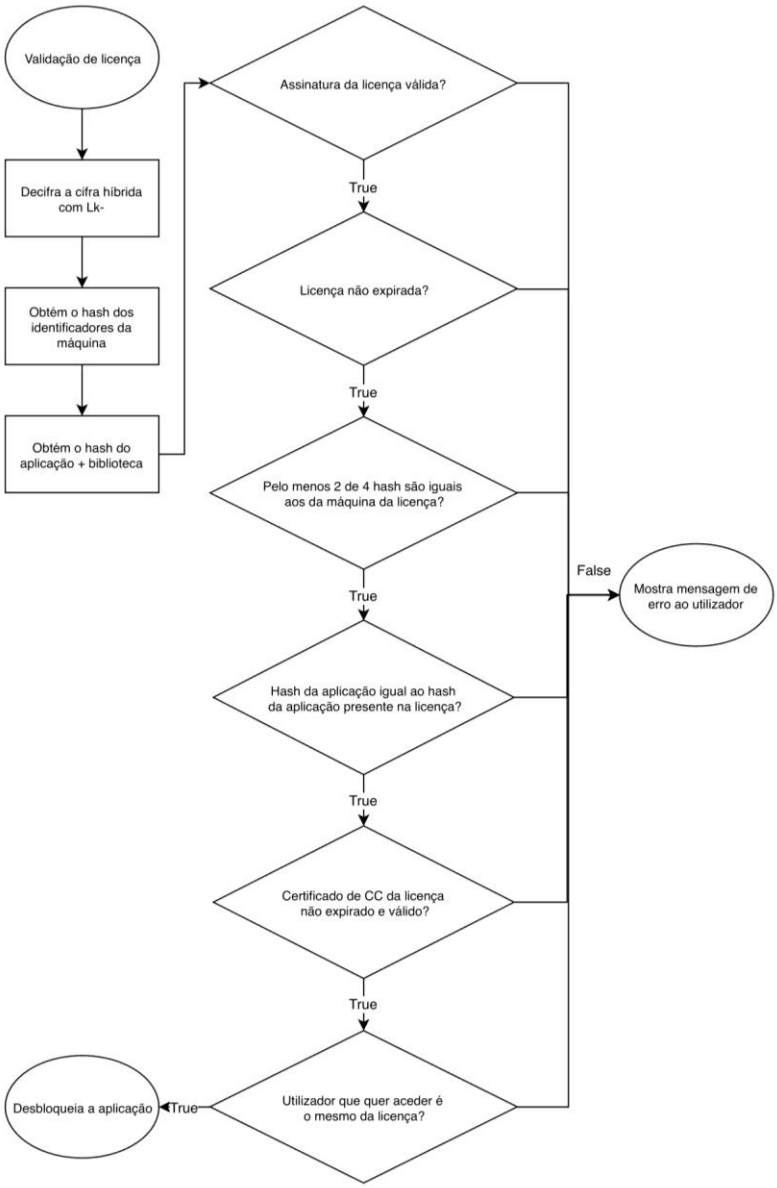

Figura 6 - Fluxograma de validação da licença pela Biblioteca

Neste fluxograma é descrita a validação da licença pela Biblioteca. De destacar a:

- Validação da licença;
- Garantia de que a aplicação apenas corre se for o utilizador, máquina e aplicação corretas;

4 Funcionalidades Implementadas

Em seguida segue a tabela com as funcionalidades implementadas e funcionais

Funcionalidade	**Implementada**	**Funcional**
Criação de um ficheiro com um pedido de licença que inclua a identificação do utilizador, dados sobre a plataforma para a execução da aplicação e dados sobre a aplicação	Sim	Sim
Proteção (integridade, confidencialidade, autenticação, não repudiação) do pedido de licença	Sim	Sim
Validação do pedido de licença	Sim	Sim
Emissão da licença, com todos os dados que garantam que apenas uma aplicação legitima pode ser executada no sistema autorizado e pelo utilizador autorizado	Sim	Sim
Proteção (integridade, confidencialidade, autenticação, não repudiação) da licença emitida	Sim	Sim
Validação do documento da licença	Sim	Sim

Proteção contra execução da aplicação noutro sistema	Sim	Sim
Proteção contra a execução da aplicação por outro utilizador	Sim	Não
Proteção contra a alteração da aplicação	Sim	Sim

5 Deficiências

A solução apresenta algumas deficiências tais como:

- Não se apresentam todas as mensagens de erro;
- Não se tratam todas as exceções;
- Supõe-se sempre que ao enviar um pedido de registo existirá sempre uma resposta;
- A *password* do Autor é guardada em memória;
- Não se valida a cadeia de certificados do certificado do cartão de cidadão;
- Não se emite um certificado para o Autor;
- Não se verifica se a aplicação corre numa máquina virtual;
- Não se consegue validar o utilizador atual, mesmo ele sendo o correto pois sempre que se tenta realizar a validação é lançada a exceção: *java.security.InvalidKeyException: Could not create RSA public key.*

6 Fontes Utilizadas

- https://docs.oracle.com/javase/tutorial/security/apisign/vstep4.html
- https://stackoverflow.com/questions/992019/java-256-bit-aes-password-based-encryption
- https://github.com/oshi/oshi/blob/master/oshi-demo/src/main/java/oshi/demo/ComputerID.java
- https://stackoverflow.com/questions/6358555/obtaining-public-key-from-certificate
- http://sweet.ua.pt/andre.zuquete/Aulas/Seguranca/14-15/docs/Ex6.pdf
- https://gist.github.com/itarato/abef95871756970a9dad