Criptografia Aplicada 2007/2008
Enunciado do Trabalho Prático

José Carlos Bacelar Almeida

Novembro 2007

1 Introdução

O objectivo deste trabalho consiste em desenvolver uma aplicação de conversação (*chat*) segura. As componentes aplicacionais do trabalho deverão ser desenvolvidas em Java, fazendo uso da *framework* JCA/JCE.

O desenvolvimento do projecto deverá ser realizado por grupos de até três elementos, elementos esses que serão responsáveis por defender o trabalho no final do semestre, numa sessão em data a combinar. Os grupos são incentivados a fazerem uso dos programas de exemplo que tem vindo a ser desenvolvidos nas aulas teórico-práticas da disciplina. A entrega do trabalho deverá ser acompanhada por um relatório que documente as opções tomadas ao longo do seu desenvolvimento.

2 Funcionalidade

Pretende-se desenvolver um ambiente de conversação para uma organização contendo um conjunto bem definido de utilizadores (e.g. departamento de uma empresa). Em termos da arquitectura do sistema, consideram-se as seguintes componentes:

Servidor: aplicação Java responsável por disponibilizar o serviço de *chat*;

Cliente: aplicação Java que possibilita o acesso dos utilizadores ao sistema;

CA: autoridade de certificação responsável por emitir os certificados requeridos para o funcionamento das aplicações.

Em termos de funcionalidade, pretende-se disponibilizar (pelo menos) os seguintes serviços:

- A identidade dos utilizadores deverá ser assegurada por intermédio da utilização de certificados X509. A emissão dos certificados necessários é parte integrante do projecto. No entanto, não se impõe que essa componente seja realizada por uma aplicação Java desenvolvida específicamente para esse fim — pode-se fazer uso de ferramentas de domínio público como o `openssl`.

- Um utilizador acede ao sistema através da aplicação cliente. Após apresentar as credenciais requeridas, terá acesso à "sala de conversação" onde poderá comunicar de forma segura com os utilizadores que se encontrem *on-line*.
- Um utilizador ligado ao sistema pode ainda solicitar uma conversação privada com um outro utilizador também disponível *on-line*. Nesse caso, e se o parceiro aceitar a comunicação, é estabelecida uma ligação segura entre eles.
- Deverá ser ainda possível a um utilizador enviar mensagens para serem lidas *off-line* por outros utilizadores. O servidor deverá assim gerir "caixas de correio" onde armazena as mensagens até que os destinatários se liguem ao sistema.

Em todas a comunicações estabelecidas deverão ser adoptados os requisitos de segurança sempre na perspectiva mais conservadora (e.g. um utilizador legítimo, se não estiver *on-line*, não deverá ser capaz de interceptar o conteúdo das mensagens trocadas na sala de conversação). A identificação clara dos requisitos de segurança, assim como escolhas fundamentada das técnicas criptográficas utilizadas, será dos aspectos mais valorizados na avaliação do trabalho.