

# REALabs – BOT (Remotely Accessible Laboratory)

## Federation: Infra-estrutura de Suporte para o REAL WebLab

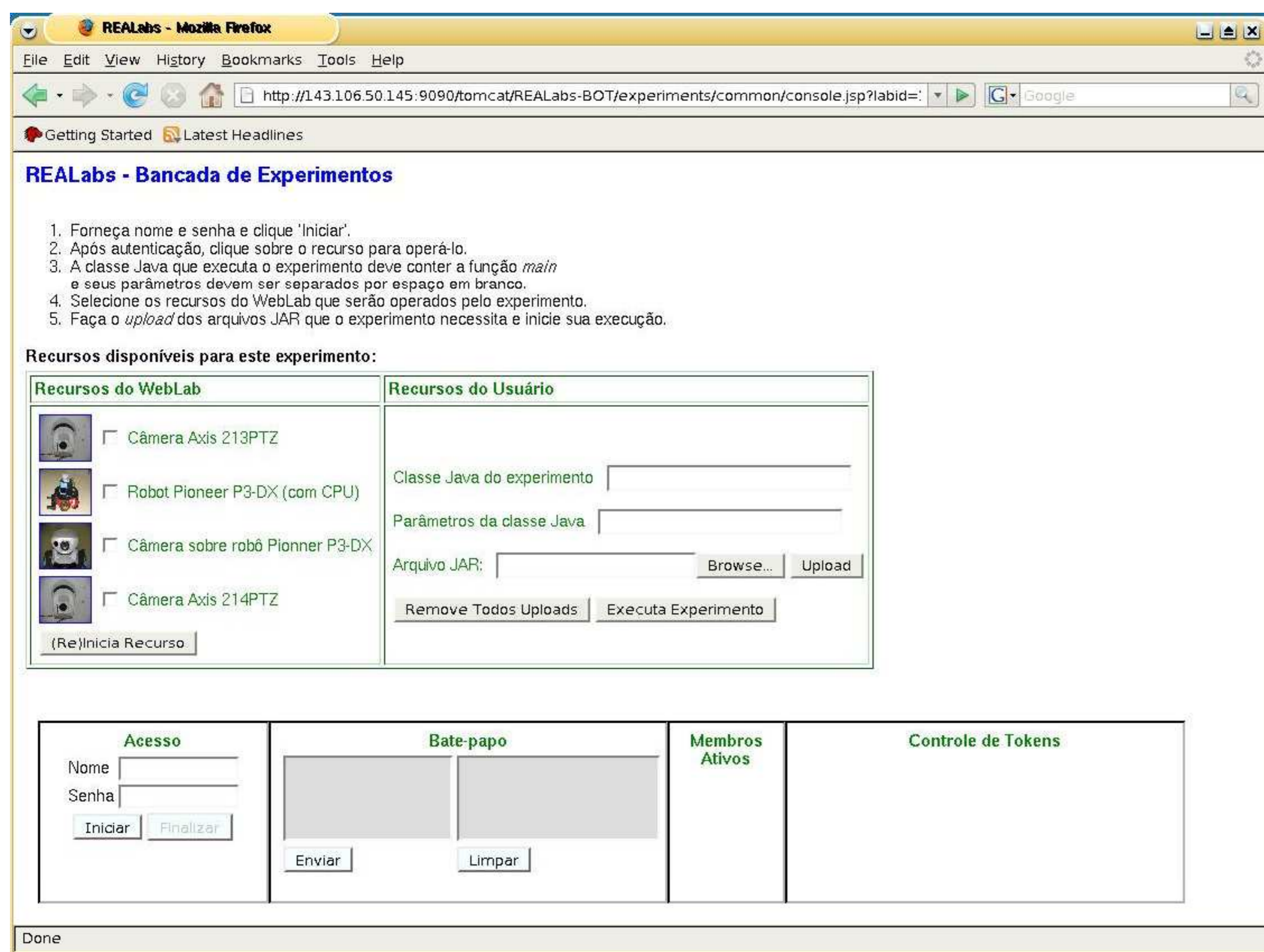


Autor: Henrique Nakashima - henrique.nakashima@gmail.com  
Orientadores: Dra. Eliane G. Guimarães (DRVC/CTI)  
Prof. Dr. Eleri Cardozo (FEEC/Unicamp)  
(eliane.guimaraes@cti.gov.br, eleri@dca.fee.unicamp.br)

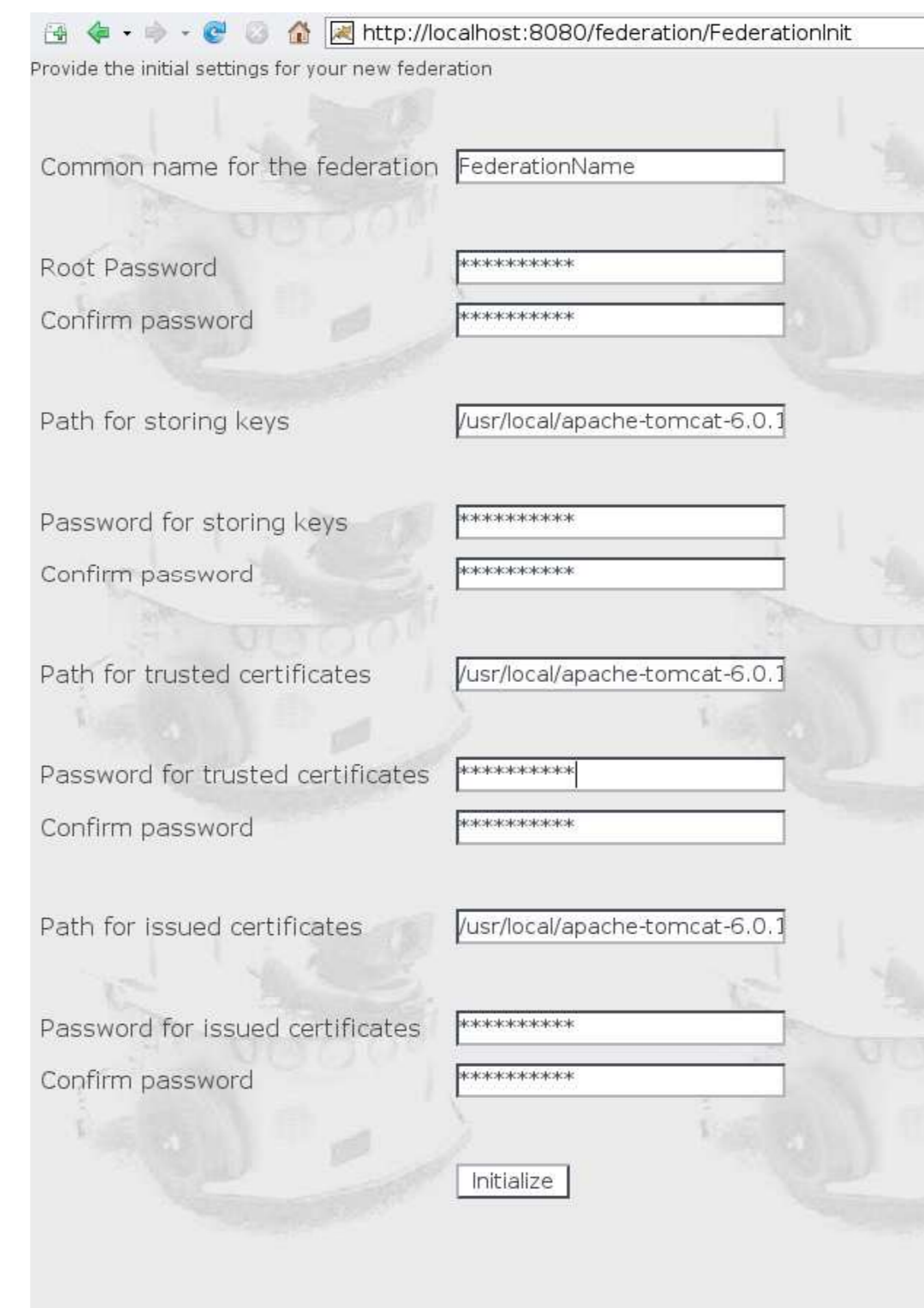
### Projeto REAL

O objetivo do projeto REAL/Gigabot WebLab é criar um Laboratório de Acesso Remoto (LAR) que permita que experimentos sejam realizados nele sem a presença física do experimentador, sendo toda a interação e comunicação entre o pesquisador e o laboratório realizadas por redes de alto desempenho ou pela internet.

Os experimentos são programas executados no computador do próprio experimentador, que se comunicam remotamente com os equipamentos do laboratório por Web Services que representam serviços do laboratório, como o serviço de visão (através da câmera) e o serviço de telemetria (através dos sensores do robô).



### Aplicação Federation



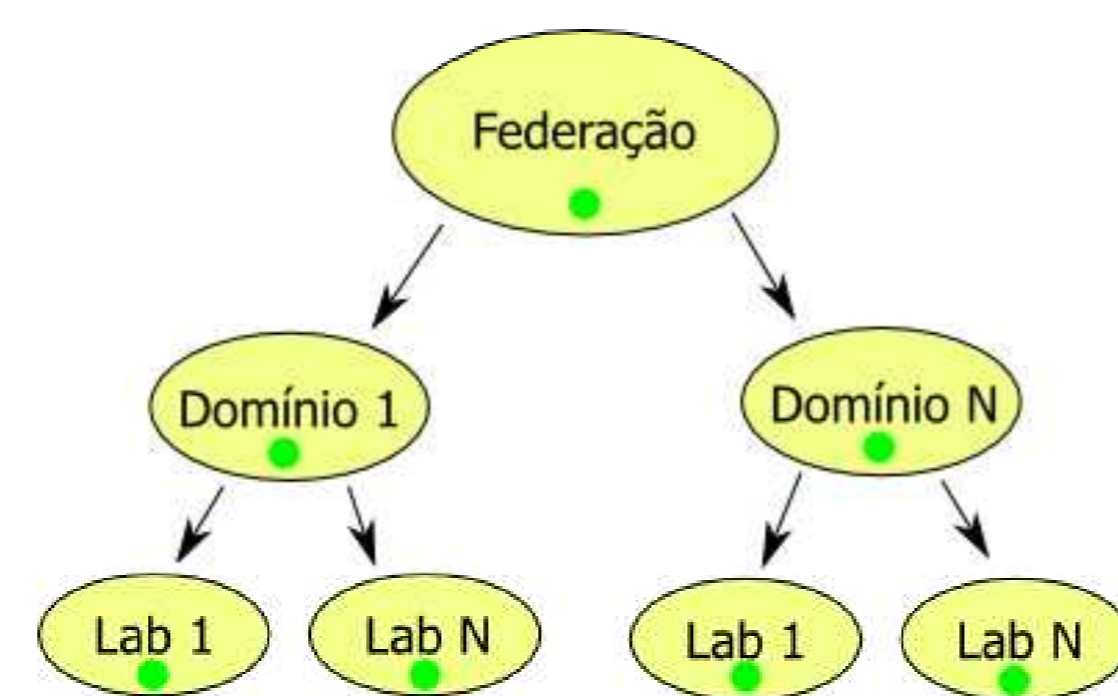
A Federation é uma aplicação web cuja função é gerenciar domínios segundo a hierarquia apresentada na seção "Federações de WebLabs". Ela utiliza um banco de dados MySQL para armazenar informações sobre os domínios e emite certificados digitais para eles, atestando que realmente pertencem àquela federação. Estes certificados são importantes para o sistema de single sign-on, pois para o seu funcionamento é necessário que sejam estabelecidas relações de confiança entre os domínios.

Os certificados digitais são arquivos que atestam a procedência de certa informação, utilizando criptografia de chave pública para permitir esta verificação. Estas técnicas envolvem uma chave pública e uma privada, sendo que a pública pode ser divulgada a qualquer um, e a privada deve ser mantida em segredo. Para assinar um documento, uma entidade usa sua chave privada, mas, para verificar a validade da assinatura, a pública é suficiente. Deste modo, poder verificar a assinatura não significa poder reproduzi-la.

A classe Federation encapsula todas as funcionalidades básicas necessárias para o gerenciamento da federação. Isto dissocia a camada de apresentação da camada lógica da aplicação, tornando fáceis as alterações ou substituições de páginas. A classe implementa as funcionalidades relacionadas à geração de certificados para os domínios, configuração inicial da federação e gerenciamento da lista de domínios federados, podendo ser reutilizada por qualquer outra aplicação de gerenciamento federação que utilize o mesmo esquema de certificados.

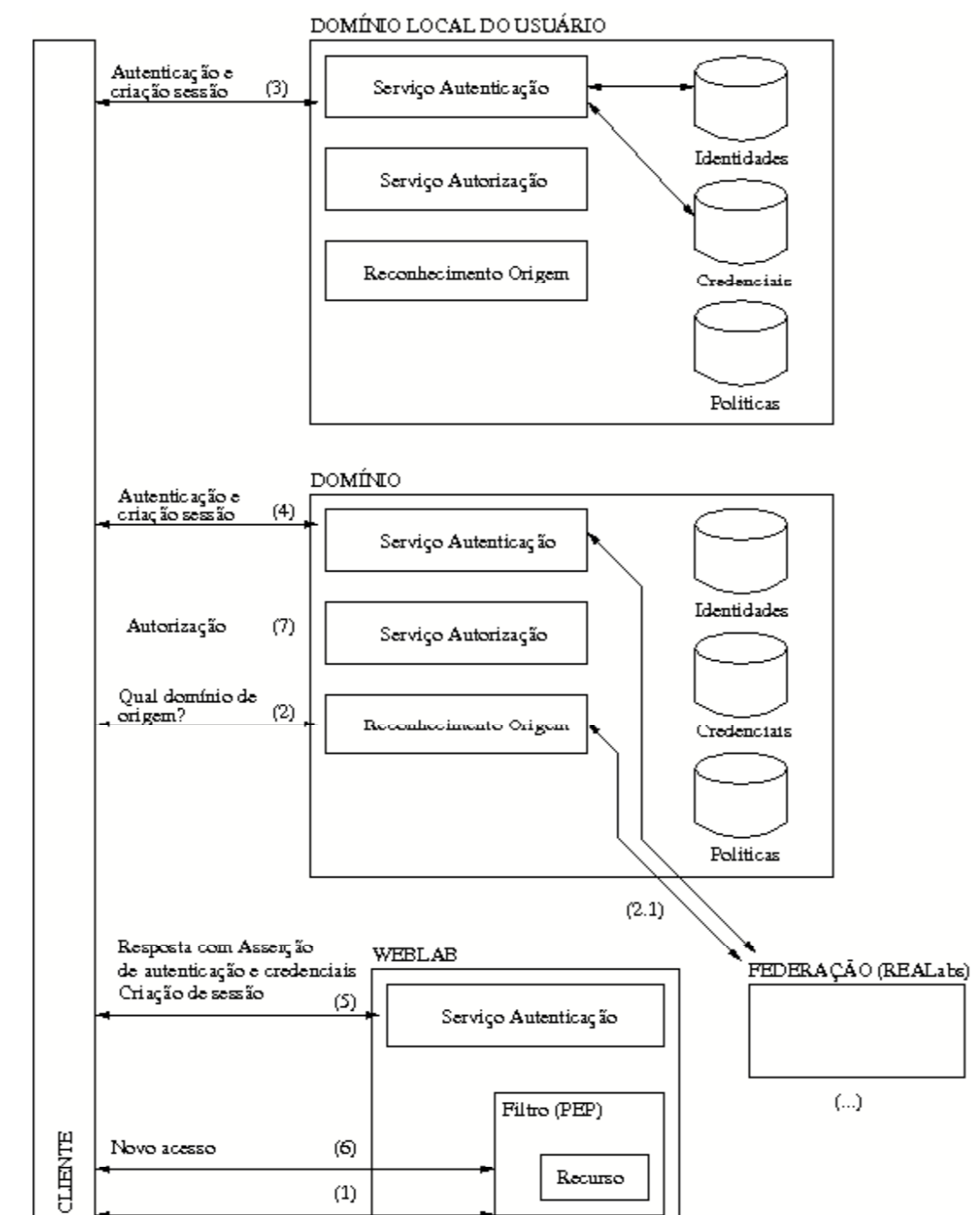
### Federações de WebLabs

Uma nova abordagem vem sendo criada para a extensão do modelo de Laboratórios de Acesso Remoto em uma Federação, na qual recursos laboratoriais possam ser compartilhados entre instituições. Neste novo modelo temos as figuras da Federação, Domínio e Laboratórios, como mostrado na figura ao lado.



Uma Federação engloba vários Domínios, que são unidades administradoras de Laboratórios de Acesso Remoto. Os pontos verdes em cada elemento demonstram a necessidade de uma camada de software capaz de prover mecanismos de Autenticação (utilizando Single Sign-On) e Controle de Acesso que tornem capaz o compartilhamento de recursos, de forma segura e seguindo os termos acordados pelos domínios pertencentes à Federação.

Uma das partes deste modelo de Federação é justamente uma aplicação para gerenciamento de certificados e chaves, além dos domínios que fazem parte de uma determinada Federação, como mostrado na seção seguinte.



Nas figuras, podemos ver duas telas da aplicação, a tela de inicialização da federação e a tela de adicionar domínio.

A tela de inicialização tem campos que recebem valores para as propriedades da federação que precisam ser configuradas, como as chaves para os certificados da federação e em que arquivo eles devem ser guardados.

A tela de adicionar domínio recebe, além de informações sobre o próprio domínio (nome, administrador, endereço web, endereço dos serviços de autenticação e autorização), um pedido de certificação emitido pelo domínio que quer se associar à federação, encriptado, e devido à dificuldade de manipulação de dados binários, codificado em base 64, um modo de representar a informação binária com caracteres normais. A partir desta requisição, ela gera um certificado que deve ser enviado (também em base 64) para o domínio, juntamente com o certificado da federação, criando uma "corrente de certificados" (certificate chain).

