3
Proposta

No capítulo 2 foram apresentadas tecnologias que são empregadas na autenticação e no controle de acesso envolvendo diferentes domínios. No entanto, elas apresentam limitações e características, como a falta de controle de acesso ou foco em cenários específicos, que as tornam inadequadas para uma solução mais geral.

É nesse contexto que propomos uma arquitetura para auxiliar a manutenção da segurança entre domínios, que disponibiliza pontos de adaptação para que as organizações possam ajustá-la às suas necessidades, o que facilita a integração com o parque tecnológico já existente. Essa arquitetura, mostrada na figura 3.1, é baseada em elementos das tecnologias apresentadas no capítulo 2, e tem como principais objetivos:

- Autenticar os usuários de instituições com as quais se mantém uma relação de confiança.
- Reduzir o esforço para a atribuição dos direitos de acesso sobre os recursos.
- Fornecer mecanismos de privacidade para os usuários envolvidos.

Assim como o Shibboleth e o Globus mantêm uma relação de confiança entre as instituições participantes, através, respectivamente, das *federações* e das Autoridades Certificadores, a arquitetura proposta também se baseia no estabelecimento desse tipo de relação entre as organizações envolvidas – adotaremos o mesmo termo do Shibboleth, *federação*.

Os usuários se autenticam nas instituições onde estão afiliados e recebem um passe para usar os recursos da federação. Esses recursos conseguem verificar que o passe foi gerado por uma das organizações da federação, mas não possuem meios para validar o usuário em si. Assim, eles devem confiar que, para fornecer esse passe, as instituições fazem as verificações necessárias, garantindo que usuários indevidos não recebam o passe. É com base nessa confiança que os serviços permitem o acesso.

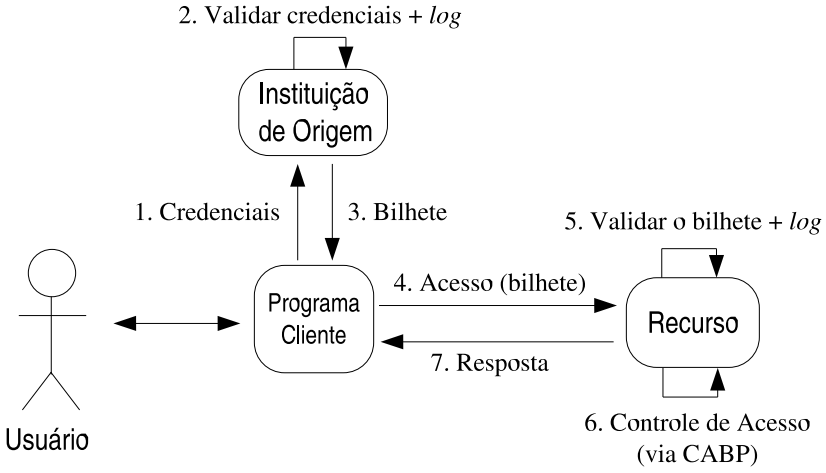

Figura 3.1: Arquitetura proposta.

As seções seguintes descrevem em mais detalhes esse processo de autenticação, bem como o controle de acesso e as implicações de privacidades decorrentes do envolvimento de várias organizações.

3.1 Autenticação

Existem duas estratégias que são muito adotadas, devido à sua simplicidade, para acessar serviços disponibilizados por outras organizações. A primeira consiste em replicar o cadastro do usuário em cada um dos domínios que ele deseja acessar. Essa replicação pode acabar levando a problemas de inconsistência, e também, demanda mais esforço, tanto do usuário, quanto dos administradores, para gerenciar os diversos cadastros e as permissões.

A segunda estratégia é cadastrar apenas uma identificação que será usada por um grupo de usuários. Apesar de diminuir o esforço da gerência, essa abordagem impede que se tenha conhecimento de quem realizou qual tipo de operação, impossibilitando responsabilizar alguém por danos causados ou gerar estatísticas precisas sobre os acessos.

A arquitetura proposta consiste de uma abordagem híbrida, evitando cadastros replicados de usuários, mas apresentando meios mais fáceis de controlar as permissões e a possibilidade de identificação individual. Todo o mecanismo de autenticação é baseado no uso de um bilhete que os usuários obtêm na instituição de origem, ou seja, na instituição onde eles estão afiliados, para autenticação perante os recursos. Esse bilhete é formado dos seguintes campos:

- **Identificador**: identifica unicamente o bilhete durante o seu período de validade.
- **Papel**: nome do papel que o usuário desempenha na sua instituição de origem.
- **Instituição de origem**: identificação da instituição onde o usuário está afiliado.
- **Data de criação**: marca quando o bilhete foi criado.
- **Tempo de validade**: indica por quanto tempo o bilhete é válido após a sua criação.
- **Assinatura**: assinatura digital da instituição de origem.

A assinatura digital em conjunto com a identificação da instituição garantem a autenticidade e integridade do bilhete, evitando que ele seja forjado ou alterado.

Os campos "data de criação" e "tempo de validade" funcionam como mecanismo de *leasing*, que força a retirada de um novo bilhete de tempos em tempos, garantindo a renovação do bilhete, e assim, da informação sobre o papel desempenhado. O *leasing* [31] também assegura uma janela de tempo máximo no caso do extravio de algum bilhete, isto é, se alguém obtiver indevidamente um bilhete, o dano que poderá ser causado se restringe ao seu período de validade.

Quando o usuário deseja acessar um serviço da federação, ele interage com o programa cliente, que entra em contato com a instituição de origem do usuários e solicita a criação de um bilhete (figura 3.1). Neste passo, a instituição requisita a apresentação de credenciais que garantam a identidade do usuário. Verificadas as credenciais, o bilhete é criado e devolvido.

O programa cliente apresenta o bilhete ao serviço, que verifica a assinatura digital usando a chave correspondente à identificação da instituição de origem. Além da assinatura, o prazo de validade também é verificado. Caso a validação seja bem sucedida, o usuário é considerado autenticado e pode realizar o acesso.

É nesse ponto que a relação de confiança das instituições que abrigam os serviços nas instituições geradoras de bilhetes é importante. Perceba que o serviço só possui meios de verificar qual instituição da federação criou o bilhete, e deve acreditar que ela realizou todas as verificações para assegurar a identidade do usuário. O contrário não é obrigatório, pois o processo de criação do bilhete é independente e emprega dados locais, não havendo necessidade de interação com outras organizações.

3.2 Direitos de Acesso

De uma forma geral, os mecanismos de permissões se baseiam em uma identificação individual derivada do processo de autenticação. Porém, em se tratando de um modelo interinstitucional, há questões de privacidade envolvidas (que serão discutidas mais detalhadamente na próxima seção), o que levou à escolha de não transportar no bilhete qualquer informação pessoal que pudesse identificar unicamente um usuário quando o mesmo requisitasse um serviço.

O modelo de controle de acesso baseado em papéis, descrito na seção 2.4, permite realizar o controle das permissões sem o emprego de qualquer identificação pessoal, casando com o propósito da arquitetura. Então, a identificação derivada da autenticação será o papel desempenhado pelo usuário em sua instituição de origem, que será usado junto com o modelo de controle de acesso via papéis. Isso também traz benefícios para a administração, pois o agrupamento dos usuários por classes (papéis) tende a diminuir o número de identidades externas que as instituições têm que lidar. E mais, se um usuário passar a desempenhar outro papel, isso não afetará o controle de acesso das organizações da federação, já que o controle não está atrelado a identidades pessoais. Entretanto, essa mudança só será refletida nos próximos bilhetes retirados pelo usuários, por isso, há a necessiadade de se definir um tempo adequado para a expiração do bilhete. Se o tempo for muito longo, o bilhete estará carregando informações incorretas sobre o usuário, mas por outro lado, se o tempo for muito curto, isso obriga a retirada constante de novos bilhetes, prejudicando o desempenho.

O papel que é extraído do bilhete poderia ser usado como entrada para uma implementação do modelo de CABP proposto pelo NIST, de onde seria obtido como saída as permissões efetivas de acesso. Entretanto, considerando um cenário amplo que englobe muitas instituições, haveria muitos papéis envolvidos e a idéia de reduzir o esforço da manutenção não se aplicaria. Uma solução é introduzir um mapeamento semelhante ao proposto pelo NIST, mas ao invés da sessão mapear usuários em papéis, ela iria mapear papéis externos em papéis locais. O novo modelo é ilustrado na figura 3.2. Note que a definição de quais papéis o usuário pode assumir é feita na instituição de origem e os demais na instituição provedora do serviço.

Cada organização define um conjunto de papéis locais, que detêm as permissões efetivas nos serviços. Através de algum mecanismo de mapea-

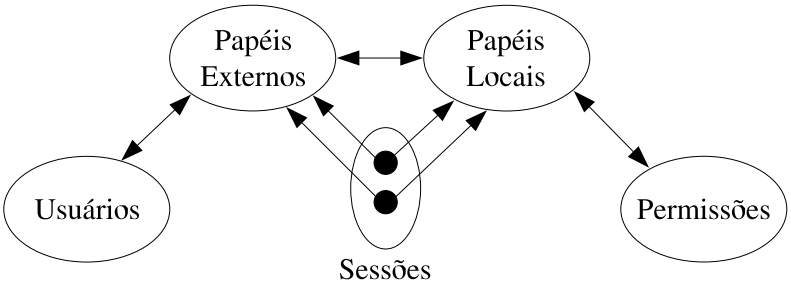

Figura 3.2: Mapeamento entre papéis externos e locais.

mento das sessões, é feita uma correlação entre o papel obtido na autenticação com um ou vários papéis do conjunto. Para exemplificar, suponha que a Rede Nacional de Pesquisa (RNP) define "pesquisador" como um de seus papéis locais, e atribui ao mesmo todos os direitos que lhe são pertinentes, e via mapeamento, ela o relaciona com o papel "professor", desempenhado por todos os professores de universidades. Desse modo, quando um usuário com o bilhete constando o papel "professor" se autenticar, todos os direitos serão verificados levando-se em conta o papel local "pesquisador".

No exemplo anterior, consideramos o mapeamento de um papel externo em apenas um papel interno. Há casos em que o papel externo estará relacionado a múltiplos papéis internos, e de acordo com o conceito de sessão, apenas os que forem necessários deverão ser ativados. Porém, é preciso saber quais papéis internos o cliente pode ativar. Enumeramos duas abordagens:

- Relacionamentos bem conhecidos: as instituições da federação definem e divulgam o mapeamento, tornando os usuários cientes das possibilidades.
- Descoberta dinâmica: o programa cliente recupera do serviço uma lista de possíveis papéis que podem ser ativados.

A descoberta dinâmica dos papéis é mais flexível e garante que as mudanças no mapeamento são propagadas com mais rapidez. Por outro lado, é necessário que o serviço ou o protocolo utilizado para a interação com o serviço proveja suporte à descoberta dos papéis.

3.3 Privacidade e Auditoria

Em se tratando de uma arquitetura voltada para um ambiente multi-institucional, com diversas políticas de privacidade envolvidas, é difícil prever quais dados dos usuários estarão disponíveis para que se possa realizar a autenticação e o controle de acesso. Empregar mecanismos de segurança que se baseiam em identificações pessoais pode ser arriscado.

A formulação do bilhete de autenticação levou em consideração o aspecto do anonimato do usuário, disponibilizando somente um conjunto de informações não pessoais, mas que mesmo assim pudessem ser usadas para garantir a autenticidade do acesso. Por outro lado, é do interesse dos administradores dos serviços possuir meios para auditoria dos acessos, o que permitiria determinar a responsabilidade por ações indevidas, ou para derivar estatísticas desses acessos. Levando em consideração somente os campos usados na autenticação (assinatura e prazo de validade), isso não seria possível.

A abordagem adotada para oferecer esse mecanismo de auditoria foi introduzir um identificador no bilhete, que não deve ter nenhuma ligação direta com os dados dos usuário. Como exemplo, podemos usar o *Universal Unique Identifier* (UUID), que é um número gerado através de informações da máquina, como endereço da placa de rede, com dados aleatórios. Na realidade, pode-se empregar geradores mais simples, desde que seja garantida a singularidade do conjunto identificador, data de criação e prazo de validade dentro de uma organização.

A instituição de origem, ao criar o bilhete, guarda em um arquivo de *log* o identificador, a data de criação e o prazo de validade do bilhete, bem como o usuário que fez a solicitação (figura 3.1). O serviço, no momento da autenticação, também faz o *log* das informações do bilhete. Se futuramente houver a necessidade de saber a identidade do usuário, o administrador do serviço entra em contato com a organização que gerou o bilhete usado no acesso, e através do cruzamento dos dados armazenados, é determinada a identidade do usuário.

3.4 Flexibilidade da Arquitetura

Cada instituição possui o seu conjunto de sistemas e plataformas, e apesar das semelhanças que possam haver, essas organizações nem sempre

são estruturadas da mesma forma.

A arquitetura apresenta pontos em aberto que foram deixados para serem adaptados de acordo com a realidade de cada organização. Os membros da federação são livres para adotar a opção que seja mais próxima do que há disponível, desde que respeitem os procedimentos e definições do resto da arquitetura. Os pontos de extensão são: a criação do bilhete, o protocolo de autenticação e a distribuição das chaves.

A estrutura do bilhete é especificada, mas quem o cria não. Ele poderia ser gerado através de um serviço que utiliza, por exemplo, RPC (*Remote Procedure Call*) ou objetos remotos CORBA. Esse serviço também seria responsável por verificar as credenciais dos usuários antes de fornecer o bilhete, além de consultar as informações internas da instituição para poder gerá-lo.

O protocolo de autenticação dependerá do tipo de serviço que está sendo acessado. A arquitetura especifica o bilhete como credencial de acesso, mas não força o conjunto de passos para que que ele seja obtido pelo serviço. No entanto, uma característica que o procotolo deverá ter é o suporte a privacidade, pois o bilhete não possui nenhum mecanismo de proteção contra extravio, ou seja, se o bilhete for transmitido pela rede sem nenhuma proteção, ele poderá ser capiturado por alguma pessoa mal intensionada e utilizado de forma indevida. O TLS [28] é um padrão para comunicação segura que é bem difundido, podendo ser adotado.

A estrutura de distribuição das chaves e certificados deve ser definida pelas organizações da federação. Os geradores de bilhetes necessitam de chaves para a assinatura digital, enquanto os serviços precisam delas para verificar essas assinaturas. Se muitos elementos estiverem envolvidos, uma abordagem automatizada de distribuição pode ser empregada. A freqüência com que a troca de chaves ocorre também deve ser levada em consideração na hora de elaborar a estratégia de atualização das chaves.