República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(21) **PI0711702-7 A2**

BRPI0711702A2

(22) Data de Depósito: 25/05/2007
(43) Data da Publicação: 29/11/2011
(RPI 2134)

(51) Int.Cl.:
G06F 15/00
H04L 9/32

(54) Título: DELEGAÇÃO DE CREDENCIAL DIRIGIDA POR POLÍTICA PARA ACESS DE ASSINATURA ÚNICA E SEGURO A RECURSOS DE REDE

(30) Prioridade Unionista: 26/05/2006 US 11/441588

(73) Titular(es): Microsoft Corporation

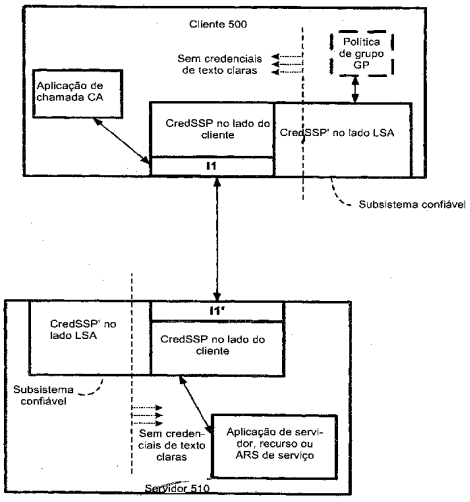
(72) Inventor(es): Costin Hagius, Cristian Ilac, Gennady Medvinsky, John E. Parsons, Mohamed Emad El Din Fathalla, Paul J. Leach, Tarek Buhaa El-Din Mahmoud Kamel

(74) Procurador(es): Nellie Anne Daniel Shores

(86) Pedido Internacional: PCT US2007012512 de 25/05/2007

(87) Publicação Internacional: WO 2007/139944de 06/12/2007

(57) Resumo: DELEGAÇÃO DE CREDENCIAL DIRIGIDA POR POLÍTICA PARA ACESSO DE ASSINATURA ÚNICA E SEGURO A RECURSOS DE REDE. Um provedor de suporte de segurança de credencial (Cred SSP) permite que qualquer aplicação delegue com segurança credenciais de usuários do cliente, por um software de Provedor de Suporte de Segurança (SSP) no lado do cliente, para um servidor alvo, pelo software SSP no lado do cliente. O Cred SSP proporciona uma solução segura que é baseada, em parte, em um conjunto de políticas. As políticas podem ser para qualquer tipo de credenciais de usuários, e políticas diferentes são elaboradas para atenuar uma ampla gama de ataques, de modo que a delegação adequada possa ocorrer para determinadas circunstâncias de delegação, condições de rede, níveis de confiança, etc. Adicionaimente, apenas um subsistema confiável, por exemplo, um subsistema confiável da Autoridade de Segurança Local (LSA), tem acesso às credenciais de texto de clientes, de modo que nem a aplicação de chamada das SSPI APIs, no lado do servidor, nem a aplicação de chamada das SSPI APIs, no lado do cliente, têm acesso às credenciais de texto claro.



"DELEGAÇÃO DE CREDENCIAL DIRIGIDA POR POLÍTICA PARA ACESSO DE ASSINATURA ÚNICA E SEGURO A RECURSOS DE REDE"

CAMPO TÉCNICO

A presente invenção ser refere a delegação de credencial dirigida por política para acesso de assinatura única e seguro a aplicações, recursos e/ou serviços em um ambiente de computação ligado em rede.

ANTECEDENTES

Algumas vezes, uma aplicação de servidor acessada por um cliente requer as credenciais de um usuário do cliente a ser delegado para o servidor, para suportar os cenários habilitados pela aplicação do servidor. Nessa situação de delegação, a senha do usuário do terminal remoto é necessária, no lado do servidor, para que as aplicações do servidor emulem a funcionalidade que é disponível quando um usuário é simplesmente registrado como um usuário local das aplicações do servidor.

No entanto, os sistemas atuais para a delegação de credenciais de um cliente a uma aplicação de servidor, para acesso às capacidades da aplicação do servidor, não são seguros o suficiente, isto é, existe uma proteção insuficiente quando das delegação / transmissão das credenciais do usuário do cliente para o servidor, deixando as credenciais do usuário vulneráveis a certas formas de ataque. Atualmente, por exemplo, a aplicação de chamada no lado do servidor ou do cliente tem, algumas vezes, acesso às credenciais de texto claras do usuário, e, desse modo, as credenciais do usuário são algumas vezes inseguras. Além disso, não há atualmente qualquer modo dirigido por política para controlar e restringir a delegação de credenciais de usuário do cliente para o servidor, que se aplique a qualquer tipo de credenciais de usuário, isto é, nome de usuário / senha, pino de cartão inteligente, códigos de passagem (OTP), etc.

Como descrito em mais detalhes abaixo com relação à invenção, seria desejável aperfeiçoar essas e outras deficiências do estado da técnica.

RESUMO

Em vista do que foi mencionado acima, a presente invenção proporciona um provedor de suporte de segurança de credencial (Cred SSP), que permite que qualquer aplicação delegue com segurança credenciais de usuário do cliente, pelo software Provedor de Suporte de Segurança (SSP) no lado do cliente, a um servidor alvo, pelo software SSP no lado do servidor em um meio de computação ligado em rede. Em uma modalidade, o Cred SSP é disponibilizado para o usuário pela Interface do Provedor de Suporte de Segurança (ISSP), que pode ser incluído como parte de um sistema operacional do cliente. O Cred SSP da invenção proporciona uma solução segura que é baseada, em parte, em um conjunto de políticas, incluindo uma política padrão que é segura contra uma ampla gama de ataques, que é usado para controlar e restringir a delegação de credenciais de usuário de um cliente

para um servidor. As políticas podem ser para qualquer tipo de credenciais de usuários, e políticas diferentes são elaboradas para atenuar uma ampla gama de ataques, de modo que a delegação adequada possa ocorrer para determinadas circunstâncias de delegação, condições de rede, níveis de confiança, etc. Adicionalmente, apenas um subsistema confiável, por exemplo, um subsistema confiável da Autoridade de Segurança Local (LSA), tem acesso às credenciais de texto de clientes, de modo que nem a aplicação de chamada das SSPI APIs, usando o Cred SSP no lado do servidor, nem a aplicação de chamada das SSPI APIs, usando o Cred SSP no lado do cliente, têm acesso às credenciais de texto claro.

Outros aspectos da presente invenção são descritos abaixo.

DESENHOS

A delegação de credencial dirigida por política para acesso de assinatura única e seguro a recursos, em um meio de computação em rede, é descrita adicionalmente com referência aos desenhos em anexo, em que:

a Figura 1 é uma visão geral de um diagrama de blocos da arquitetura do provedor de suporte de segurança de credencial da invenção, que permite a delegação segura de credenciais do cliente para o servidor;

as Figuras 2A e 2B ilustram uma implementação não limitante, exemplificativa da arquitetura do provedor de suporte de segurança de credencial, para delegação de credenciais a um servidor de terminal;

a Figura 3 é um fluxograma de um protocolo não limitante, exemplificativo utilizado pela arquitetura do provedor de suporte de segurança de credencial da invenção;

a Figura 4 é um fluxograma de um protocolo não limitante, exemplificativo utilizado pela arquitetura do provedor de suporte de segurança de credencial da invenção;

a Figura 5 é uma visão geral de um diagrama de blocos da arquitetura do provedor de suporte de segurança de credencial, que permite a delegação segura de credenciais do cliente para o servidor, com base em uma política de grupo de acordo com a invenção;

a Figura 6 é um diagrama de blocos de uma visão geral de três diferentes tipos de credenciais, que podem ser consideradas em um nível de política, de acordo com o risco de ataque de acordo com a invenção;

a Figura 7A é um diagrama de blocos representando um meio de rede exemplificativo, no qual a presente invenção pode ser implementada; e

a Figura 7B é um diagrama de blocos representando um meio de sistema de computação não limitante, exemplificativo, no qual a presente invenção pode ser implementada.

DESCRIÇÃO DETALHADA

Visão geral

Como mencionado nos antecedentes, há algumas aplicações de cliente / servidor que requerem que as credenciais dos usuários sejam delegadas ao servidor, para suportar

os cenários dos servidores. O Terminal do Servidor é um desses exemplos no qual algumas vezes a senha do usuário é usada no lado do servidor, para emular a sua funcionalidade no lado do cliente. No entanto, como mencionado, as técnicas de delegação da técnica anterior não proporcionam uma proteção suficiente para as credenciais dos usuários, quando enviadas para o servidor.

O Cred SSP da invenção é um novo "provedor de suporte de segurança", algumas vezes também referido como "provedor de serviço de segurança", que pode ser disponibilizado pela infra-estrutura de Interface de Provedor de Suporte de Segurança (SSPI) de um sistema operacional do cliente. O Cred SSP da invenção permite que uma aplicação delegue as credenciais do usuário do cliente, por exemplo, pelo software SSP no lado do cliente, para o servidor alvo, por exemplo, pelo software SSP no lado do servidor. Em uma modalidade não limitante, exemplificativa, o Cred SSP da invenção pode ser incluído no Servidor do Terminal. No entanto, o Cred SSP da invenção pode ser utilizado por outras aplicações, e pode ser disponibilizado a qualquer aplicação interna ou de terceira parte, usando a SSPI do sistema operacional aplicável.

A solução Cred SSP é uma solução mais segura que proporciona um conjunto de políticas, que pode ser usada para controlar e restringir a delegação de credenciais de usuários do cliente para o servidor. As políticas são elaboradas para abordar uma ampla gama de ataques, incluindo política de "segurança por padrão", que é a configuração particular por ajustes de política, que permite que uma máquina de cliente, por padrão, atenue uma ampla gama de ataques. O conjunto de políticas da invenção é aplicável para proteger qualquer tipo de credenciais de usuários, incluindo, mas não limitado a nome do usuário / senha, pino de cartão inteligente, códigos de passagem por tempo (OTP), etc. O Cred SSP da invenção protege as credenciais dos usuários de modo que a aplicação de chamada (da Cred SSP API), no lado do servidor ou cliente, não tenha acesso a credenciais de texto claro, porque apenas um subsistema confiável tem acesso às credenciais de texto claro.

O Servidor do Terminal (TS) da Microsoft é, por exemplo, um caso de um produto de servidor / cliente que requer, algumas vezes, que os usuários proporcionem credenciais de assinatura nos terminal / cliente, e deleguem aquelas credenciais assinadas ao servidor, para autorizar o serviço de aplicações, e a experiência de "computador de mesa" dos produtos dos sistemas operacionais Windows da Microsoft nos terminal / cliente. O TS pode ser imaginado como incluindo, de uma maneira geral, três partes principais: um servidor de núcleo multiusuário, o Protocolo de Computador de Mesa Remoto (RDP), que permite que a interface do computador de mesa do Windows seja enviada para os terminais pelo servidor, e o software do cliente que é executado em cada terminal. Em uma modalidade não limitante da invenção, os protocolos do provedor de suporte de segurança de credencial da invenção podem ser implementados em conjunto com o software do servidor do terminal.

Contexto suplementar

Algumas das várias modalidades são descritas no presente relatório descritivo com referência aos termos, que são geralmente entendidos por aqueles versados na técnica nos ramos de autenticação e delegação de credenciais. Ainda que essa seção não seja intencionada para substituir o conhecimento daqueles versados na técnica e não seja considerada como uma visão geral não exaustiva, não obstante, acredita-se que essa seção proporcione vantajosamente alguns contexto e antecedentes adicionais para certos termos, que são utilizados no contexto da operação de várias modalidades da invenção, como descrito em mais detalhes abaixo.

Contexto e antecedentes adicionais para os termos apresentados a seguir conhecidos, de uma maneira geral, por aqueles versados na técnica, são, desse modo, proporcionados no presente relatório descritivo: Kerberos, Gerenciador (NTML) de Rede de Área Local (LAN) do Windows NT, Mecanismo de Negociação (SPNEGO, abreviando) Interface de Programa de Aplicação de Serviço de Segurança Genérico Protegido (GSSAPI), Autoridade de Segurança Local (LSA), Interface de Provedor de Suporte de Segurança (SSPI) e protocolo de Camada de Soquetes de Segurança (SSL), e uma Infra-estrutura de Autenticação do Windows exemplificativa.

Kerberos

Kerberos é um método seguro para autenticação de um pedido em uma rede de computador. Emprestando seu nome do cão de três cabeças mitológico, que guarda a entrada para o Hades, o Kerberos deixa que um usuário peça um "tíquete" criptografado de um processo de autenticação, que pode ser depois usado para solicitar um serviço particular de um servidor, de modo que a senha do usuário não tenha que passar pela rede. O Kerberos inclui software nos lados de cliente e servidor, que propicia acesso a um servidor, incluindo um pedido de entrada no sistema (login) a um cliente por um usuário. O servidor, no entanto, requer um "tíquete" Kerberos, antes que honre o pedido para acesso às suas aplicações, recursos e/ou serviços. Para obter o tíquete Kerberos adequado, um pedido de autenticação é feito pelo cliente a um Servidor de Autenticação (AS). O AS cria uma "chave de sessão", que é também uma chave de criptografia, baseando a chave de sessão na senha do usuário obtida do nome do usuário, e um valor aleatório que representa o serviço solicitado. Nesse sentido, a chave de sessão é efetivamente um "tíquete - tíquete de concessão".

A seguir, o tíquete - tíquete de concessão obtido é transmitido a um serviço de concessão de tíquete (TGS). O TGS pode ser fisicamente o mesmo servidor que o AS, mas executa funcionalmente um serviço diferente. O TGS retorna o tíquete, que pode ser enviado para o servidor para o serviço pedido. O serviço ou rejeita o tíquete, se o tíquete for inválido, ou aceita o tíquete, como um tíquete válido, e executa o serviço. Em virtude do tíquete recebido do TGS ser estampado no tempo, o tíquete propicia pedidos adicionais, usando o

mesmo tíquete dentro de um certo período de tempo, sem que tenha que reautenticar o uso do usuário do serviço do servidor. Por outro lado, tornando o tíquete válido por um período de tempo limitado, fica menos provável que alguém diferente do usuário autorizado seja capaz de reutilizar o tíquete. Uma pessoa versada na técnica pode considerar que as particularidades do processo de autenticação Kerberos nos níveis de interface, protocolo, carga útil e acionador possam ser muito mais complicadas e que o procedimento do usuário pode variar um pouco de acordo com a implementação.

Gerenciador LAN do Windows NT (NTLM)

Uma alternativa ao Kerberos, o NTML é um protocolo de autenticação usado em várias implementações de protocolo de rede Microsoft e suportado pelo Provedor de Suporte de Segurança NTLM (NTLMSSP). Originalmente usado para autenticação e negociação de comunicações seguras de Meio de Computação Distribuído (DCE) / Chamada de Procedimento Remoto (RPC), o NTLM é também usado como um mecanismo de assinatura único integrado.

O NTLM emprega um mecanismo de resposta de desafio para autenticação, no qual os clientes são capazes de provar as suas identidades, sem enviar uma senha para o servidor. O mecanismo de resposta de desafio inclui três mensagens, referidas comumente como Tipo 1 (negociação), Tipo 2 (desafio) e Tipo 3 (autenticação). Em um nível alto, com o NTML, primeiro um cliente envia uma mensagem do Tipo 1 para o servidor, incluindo uma lista dos recursos suportados pelo cliente e solicitados do servidor. O servidor responde com uma mensagem do Tipo 2 para o cliente, incluindo uma lista de recursos suportados e aceitos pelo servidor e um desafio gerado pelo servidor. O cliente replica ao desafio com uma mensagem do Tipo 3, com vários pedaços de informações sobre o cliente, incluindo o domínio e o nome de usuário do cliente usuário e uma ou mais respostas para o desafio do Tipo 2. A ou as respostas na mensagem do Tipo 3 são um pedaço importante, pois provam ao servidor que o cliente usuário tem conhecimento da senha da conta.

Canal seguro (canal S)

O Canal Seguro, também conhecido como Canal S, é um provedor de suporte / serviço de segurança (SSP), contendo um conjunto de protocolos de segurança, que proporcionam autenticação de identidade e segurança de comunicação otimizada por criptografia. O canal S é basicamente usado para aplicações de Internet, que requerem uma segurança otimizada para comunicações de Protocolo de Transferência de Hipertexto (HTTP). A autenticação do servidor, quando o servidor proporciona prova da sua identidade para o cliente, é necessária pelos protocolos de segurança do canal S. Desse modo, os protocolos do canal S utilizam credenciais do canal S, que podem ser usadas para autenticar os servidores e, opcionalmente, os clientes. A autenticação do cliente pode ser pedida pelo servidor a qualquer tempo. As credenciais do canal S são os certificados X.509. As informações de

chaves públicas e privadas dos certificados são usadas para autenticar o servidor e, opcionalmente, o cliente. Essas chaves são também usadas para proporcionar integridade da mensagem, enquanto o cliente e o servidor trocam as informações necessárias para gerar e trocar chaves de sessão. O canal S implementa os protocolos SSL e TLS referidos em mais detalhes abaixo.

Mecanismo de Negociação GSSAPI Simples e Protegido (SPNEGO)

O SPNEGO é um pseudomecanismo de Interface de Programa de Aplicação de Serviço de Segurança Genérico (GSSAPI) padrão para que pares determinem que mecanismos GSSAPI são compartilhados, selecionar um e depois estabelecer um contexto de segurança com o mecanismo GSSAPI compartilhado. A especificação para o SPNEGO pode ser encontrada no Esboço da Força Tarefa de Engenharia da Internet RFC 2478 intitulado "GSS-API Negotiation Mechanism", datado de dezembro de 1998.

O uso do SPNEGO pode ser encontrado, por exemplo, na extensão "HTTP negotiate", que á uma extensão de autenticação que foi primeiro implementada no software de busca Internet Explorer e que proporcionou capacidades de assinatura única conhecidas como Autenticação Integrada do Windows. Os submecanismos Negociáveis do SPNEGO incluem NTLM e Kerberos, ambos podendo usar Diretório Ativo.

A GSSAPI proporciona uma interface genérica que pode ser estratificada acima dos diferentes mecanismos de segurança, de modo que se os paredes de comunicação adquirem credenciais GSSAPI para o mesmo mecanismo de segurança, então um contexto de segurança pode ser estabelecido entre eles. No entanto, a GSSAPI não prescreve o método pelo qual os pares GSSAPI podem estabelecer se têm um mecanismo de segurança comum.

O SPNEGO permite que os pares GSSAPI determinem em banda se suas credenciais compartilham um ou mais mecanismos de segurança GSSAPI, e sendo assim, invocar estabelecimento de contexto de segurança normal para um mecanismo de segurança comum, propiciando a negociação de diferentes mecanismos de segurança, diferentes opções dentro de um determinado mecanismo de segurança, ou diferentes opções para vários mecanismos de segurança. Isso é mais útil em aplicações que são baseadas em implementações GSSAPI, que suportam múltiplos mecanismos de segurança. Uma vez que o mecanismo de segurança comum é identificado, o mecanismo de segurança também pode negociar opções específicas de mecanismo, durante seu estabelecimento de contexto.

Com o SPNEGO, os dados de negociação são encapsulados em indicações a nível de contexto. Desse modo, os chamadores do GSSAPI não precisam estar cientes da existência das indicações de negociação, mas apenas do pseudomecanismo de segurança.

O modelo de negociação do SPNEGO funciona da seguinte maneira: o iniciador propõe um mecanismo de segurança ou uma lista ordenada de mecanismos de segurança,

e o alvo aceita o mecanismo de segurança proposto, ou seleciona um de um conjunto oferecido, ou rejeita o um ou mais valores propostos. O alvo então informa ao iniciador da sua seleção.

Na sua forma básica, esse protocolo requer um percurso extra-redondo. O ajuste da conexão de rede é uma característica de desempenho crítico de qualquer infra-estrutura de rede, e os percursos extra-redondos pelas ligações WAN, redes de rádio de pacotes, etc., podem, realmente, fazer uma diferença. Para evitar esse percurso extra-redondo, a indicação de segurança inicial do mecanismo preferido para o iniciador pode ser embutido na indicação inicial. Se o mecanismo preferido do alvo corresponder ao mecanismo preferido do iniciador, não são incorridos quaisquer percursos redondos adicionais por uso do protocolo de negociação.

O SPNEGO também proporciona uma técnica para proteger a negociação, quando o mecanismo subjacente, selecionado pelo alvo, é capaz de proteção de integridade. Quando todos os mecanismos propostos pelo iniciador suportam proteção de integridade ou quando o mecanismo selecionado suporta proteção de integridade, então o mecanismo de negociação fica protegido, uma vez que isso garante que o mecanismo adequado, suportado por ambos os pares, foi selecionado.

Autoridade de Segurança Local (LSA)

Embora em um conceito genérico a LSA seja um componente básico do processo de entrada no sistema (logon) para o sistema operacional Windows da Microsoft, as tecnologias são responsáveis pela validação dos usuários, para ambas as entradas no sistema local e remota. A LSA também mantém a política de segurança local.

Durante uma entrada no sistema interativa, local em uma máquina, uma pessoa introduz os seus nome e senha no diálogo de entrada no sistema. Essas informações são passadas para a LSA, que depois chama o pacote de autenticação adequado. A senha é enviada em um formato de chave secreta irreversível, suando uma função hash de uma só direção. A LSA então consulta a base de dados do Gerenciador de Conta de Segurança (SAM), para informações da conta do usuário. Se a chave proporciona comparações com um no SAM, o SAM retorna o Identificador de Segurança (SID) do usuário e os SIDs de quaisquer grupos aos quais pertence o usuário. A LSA então usa esses SIDs para gerar uma ou mais indicações de acesso de segurança. Essa descrição se aplica no caso de um usuário ter uma conta local, oposto a uma conta de domínio quando um tíquete de serviço Kerberos é obtido para autenticar o usuário na máquina.

Interface de Provedor de Suporte de Segurança (SSPI)

A SSPI define a mecânica de autenticação de um enxofre, isto é, verifica que o usuário é que o usuário reivindica ser, ou no mínimo, que o usuário conheça um segredo, por exemplo, a senha, associada com uma conta de usuário particular.

As credenciais usadas para essa conexão de autenticação podem ser: (1) as credenciais para uma ligação autenticada existente entre as máquinas do cliente e do servidor (por exemplo, um mapeamento de unidade existente); (2) as credenciais para a conta de usuário do cliente, se o servidor reconhecer a SID associada com essa conta; isso implica que tanto o cliente quanto o servidor estão sob o mesmo domínio, e que a conta do usuário é desse domínio; (3) as credenciais brutas (por exemplo, nome e senha) para uma conta local no servidor se for igual a ambos o nome e senha de usuário do cliente (nesse caso, a conta de usuário do cliente e a conta que ele usa no servidor são distintas); e (4) as credenciais (por exemplo, nome e senha) que são passadas explicitamente nela pelo usuário. A SSPI funciona por solicitação das aplicações de chamada (os processos do cliente e do servidor) para transmitir os blocos de dados para frente e para trás, até que o provedor de segurança subjacente esteja satisfeito.

Tendo carregado a biblioteca de ligação dinâmica de segurança (DLL) e tendo selecionado um pacote (outro termo para o provedor de segurança, tais como NTLM, Kerberos, etc.), o cliente inicializa a SSPI local ou do cliente e recupera o primeiro conjunto de dados para enviar ao servidor. Enquanto isso, o servidor inicializou a SSPI do servidor e, após receber o primeiro conjunto de dados, o servidor o alimenta à SSPI do servidor, que processa o primeiro conjunto de dados, resultando em um segundo conjunto de dados. No retorno, o servidor executa um cheque contra o segundo conjunto de dados resultante e, se os dados forem superiores a 0, o servidor envia o segundo conjunto de dados para o cliente, que por sua vez o alimenta à SSPI do cliente. A SSPI do cliente então ou pede que um terceiro conjunto de dados seja enviado ao servidor, ou diz à aplicação que a autenticação está completa. Isso continua até que ambas as SSPIs do cliente e do servidor estejam satisfeitas com os dados recebidos do outro.

Nesse ponto, o servidor retém uma alça de contexto, que (entre outras coisas) pode ser consultada para o nome de usuário do cliente. Dependendo das opções usadas pelo cliente, o servidor também pode ser deixado usar o contexto para personificar o cliente, assinar ou criptografar mensagens, e assim por diante. Há mais uma etapa adicional que pode ser executada. Para terminar o ciclo de envio - recebimento, alguns provedores de segurança podem pedir uma etapa de acabamento predefinida chamada CompleteAuthToken (CAT).

Protocolos de Camada de Soquetes Seguros (SSL) e de Segurança de Camada de Transporte (TLS)

O protocolo da Camada de Soquetes Seguros (SSL) e o protocolo de Segurança de Camada de Transporte (TLS), o seu sucessor, ambos implementados pelo canal S, são protocolos criptográficos que proporcionam comunicações seguras na Internet. Há ligeiras diferenças entre a SSL 3.O e a TLS 1.0, mas o protocolo se mantém substancialmente igual. O

termo "SSL" se refere algumas vezes a ambos os protocolos, a menos que esclarecido pelo contexto.

Os protocolos SSL/TSL proporcionam autenticação de ponto final e privacidade de comunicações pela Internet usando criptografia. Em uso típico, o servidor é autenticado (isto é, a sua identidade é garantida), enquanto que o cliente se mantém não identificado, ainda que autenticação mútua possa ser feita por disposição de infra-estrutura de chave pública (PKI) a clientes. Os protocolos permitem que as aplicações de clientes / servidores se comuniquem de um modo elaborado para impedir escuta às escondidas, violação e falsificação de mensagem.

Infra-estrutura de autenticação de Windows não limitante exemplificativa

Uma infra-estrutura de autenticação não limitante, exemplificativa é proporcionada pelas tecnologias dos sistemas operacionais Windows, que suportam diferentes métodos de autenticação pelo software de Provedor de Serviço / Suporte de Segurança (SSP).

Em uma implementação, o Windows suporta três SSPs primárias descritas acima: Kerberos, Desafio / Resposta NTLM e Protocolos de Segurança de Canal S. Ainda que o Kerberos seja o método de autenticação padrão no Windows 2000, outros métodos podem ser usados pela Interface do Provedor de Suporte de Segurança, ou SSPI. Além disso, por exemplo, o Windows pode usar as seguintes SSPs de rede, para proporcionar serviços de autenticação usando certificados digitais: Autenticação de Senha Distribuída (DPA) - um protocolo de autenticação na Internet, Protocolo de Autenticação Extensível (EAP) - uma extensão do protocolo Ponto-a-Ponto (PPP) e protocolos à base de chave pública, incluindo SSL, TLS e Tecnologia de Comunicação Privada.

<u>Delegação de credencial dirigida por política para assinatura única e acesso seguro a recursos da rede</u>

Como mencionado, a invenção proporciona software de provedor de suporte de segurança de credencial otimizado (Cred SSP), que permite que uma aplicação delegue as credenciais do usuário do cliente, por exemplo, pelo software SSP no lado do cliente, para o servidor alvo, por exemplo, pelo software SSP no lado do servidor. O Cred SSP da invenção pode ser utilizado por qualquer aplicação nativa de um sistema operacional ou qualquer aplicação de terceiros usando a SSPI aplicável, por exemplo, uma SSPI integrada com uma plataforma de aplicação de sistema operacional.

A Figura 1 é um diagrama de blocos de uma visão geral da arquitetura Cred SSP da invenção, que propicia a delegação segura de credenciais do cliente para o servidor, sem expor as credenciais de texto claro para a ou as aplicação de chamada. Em uma modalidade, o Cred SSP é implementado como um conjunto de dois pacotes: um pacote Cred SSP no lado do cliente (ou aplicação) Client-Side_CredSSP e um pacote Cred SSP no lado LSA LSA_CredSSP de um dispositivo D, para um dispositivo de computação de cliente ou um

dispositivo de computação de servidor.

O pacote Cred SSP no lado do cliente Client-Side_CredSSP é um software de provedor de suporte de segurança no lado do cliente, que é exposto a chamadores da Interface de Provedor de Suporte de Segurança, Interface Client-Side_CredSSP I1, proporciona negociação de canal S e expõe a funcionalidade de pacote de canal S, bem como comunicação com o pacote no lado LSA LSA_CredSSP pela Interface LSA-SideCred SSP I2. De acordo com a invenção, a manipulação da negociação e da funcionalidade do canal S, em um processo de usuário, facilita as operações encryptMessage e decryptMessage mais rápidas, comparadas com o desempenho pela LSA.

De acordo com a invenção, o pacote LSA LSA_CredSSP proporciona a negociação SPNEGO e codificação / decodificação de credencial e seguimento de credencial, bem como executa cheques de política contra as políticas definidas de acordo com o conjunto de políticas descrito acima das políticas da invenção.

Como mencionado, e como mostrado nas Figuras 2A e 2B em uma modalidade não limitante, a invenção é implementada em conjunto com um cliente de servidor de terminal 200 delegando credenciais para um servidor de terminal 250.

Como mostrado na Figura 2A, uma implementação de um cliente de servidor de terminal 200 interage com o processo de Servidor LSA 225 por uma biblioteca de autenticação segura 205, utilizando uma chamada de procedimento local (LPC) 215, que inclui a transmissão de dados pelo limite de processo 220. As funções 210 são executadas em uma biblioteca de autenticação segura 205 e podem incluir uma função de Contexto de Segurança de Inicialização de Cred SSP (Cred SSP.ISC), que inclui uma função de Camada de Soquetes Segura / Contexto de Segurança de Inicialização (SSL.ISC) e uma função de Camada de Soquetes Segura / Mensagem de Decodificação (SSL.EM). As funções 230 são executadas no processo Servidor LSA 225 e podem incluir uma função de Contexto de Segurança de Inicialização de Cred SSP (Cred SSP.ISC), que inclui uma função de SPNEGO / Contexto de Segurança de Inicialização (SPNEGO.ISC) e uma função de SPNEG / Mensagem de Decodificação (SPNEGO.EM).

Como mostrado na Figura 2B, uma implementação de um servidor de terminal 250 interage com o processo Servidor LSA 275 por uma biblioteca de autenticação segura 225, utilizando uma chamada de procedimento local (LPC) 265, que inclui um limite de processo de atravessamento 270. As funções 260 são executadas em um processo de autenticação seguro 205 e pode incluir uma função de Contexto de Segurança de Aceitação Cred SSP (Cred SSP.ASC), que inclui uma função de Camada de Soquetes Segura / Contexto de Segurança de Aceitação (SSL.ASC) e uma função de Camada de Soquetes Segura / Mensagem de Decodificação (SSL.DM). As funções 280 são executadas em um processo Servidor LSA 275 e podem incluir uma função de Contexto de Segurança de aceitação Cred SSP

(Cred SSP.ASC), que inclui uma função de SPNEGO / Contexto de Segurança de Aceitação (SPNEGO.ASC) e uma função de SPNEGO / Mensagem de Decodificação (SPNEGO.DM).

Um protocolo não limitante, exemplificativo utilizado pelo Cred SSP da invenção é mostrado em um modo exemplificativo no fluxograma da Figura 3. Em 300, um sinal de estabelecimento de comunicação SSL/TLS inicial ocorre entre um cliente e um servidor. Em 305, a negociação SPNEGO ocorre para selecionar um mecanismo de autenticação (por exemplo, Kerberos ou NTLM, ou outro mecanismo de negociação adequado entendido pelo cliente e pelo servidor). Em 310 e 315, por uso do mecanismo de autenticação negociado, o servidor é autenticado para o cliente, e o cliente é autenticado para o servidor.

Se, em 320, a autenticação adequada tiver sido feita entre o cliente e o servidor de acordo com as etapas 310 e/ou 315, então um segredo compartilhado (por exemplo, uma chave compartilhada) é estabelecido para todo o tráfego adicional em 330. No entanto, vantajosamente, se, em 320, a autenticação adequada não tiver sido estabelecida entre o cliente e o servidor, então nenhuma sessão é criada em 325, e muito gasto e tráfego computacionais são evitados. No passado, por exemplo, para as implementações anteriores de servidor de terminal, a autenticação era feita a um maior custo, por causa da tentativa de fazer a autenticação assim que a sessão era criada. Em comparação, de acordo com o protocolo do Cred SSP da invenção, a sessão entre o cliente e o servidor não é criada, a menos que a autenticação do cliente e do servidor, de acordo com o mecanismo de autenticação selecionado SPNEGO, seja feita.

Desse modo, considerando que em 320 a autenticação adequada tenha sido feita, por uso do mecanismo de autenticação selecionado, uma chave compartilhada é estabelecida para todo o tráfego adicional entre o cliente e o servidor em 330. No entanto, apenas por que a autenticação de limite tenha ocorrido, não significa ainda que o servidor é necessariamente confiável para o cliente. Desse modo, nesse ponto, ainda que uma sessão tenha sido criada entre o cliente e o servidor, o servidor pode ser considerado confiável ou não. Conseqüentemente, usando a política de grupo 335 da invenção, o LSA Cred SSP, na máquina do cliente, executa um cheque de política em 340, para determinar se delegar as credenciais do usuário. Se o servidor não for confiável, então em 345, as credenciais não são delegadas. Se a relação com o servidor é confiável de acordo com o cheque de política de 340, então em 350, a chave pública do servidor é autenticada para ajudar a evitar ataques de "interferência humana", nos quais um objeto de software de fim de arquivo imita o comportamento e a chave pública do servidor. Desse modo, se a chave pública do servidor não for autenticada em 350, então as credenciais não são delegadas de acordo com o risco de ataque de interferência humana em 335. Em 360, um formato de codificação é aplicado às credenciais que são entendidas apenas por um subsistema confiável da LSA. Em 465, as credenciais codificadas são delegadas do cliente para o servidor. Fazendo-se o formato de

codificação entendido apenas por um subsistema confiável da LSA, vantajosamente, as aplicações de chamada no cliente e no servidor para a LSA e o Cred SSP da invenção não têm qualquer acesso inadequado para as credenciais de texto claro.

A Figura 4 ilustra uma implementação mais detalhada do protocolo de delegação de credencial da invenção, como um fluxograma não limitante, exemplificativo. Em 400, um sinal de estabelecimento de comunicação SSL/TLS é completado entre o cliente e o servidor, e a chave de codificação SSL/TLS, $K_{SSL/TLS}$, é estabelecida entre o cliente e o servidor. K_{pub} é a chave pública no certificado do servidor. Então, em 410, pelo canal SSL/TLS codificado, a autenticação mútua do cliente e do servidor é completada usando o pacote SPNEGO. Dependendo da relação de confiança cliente / servidor, o pacote Kerberos ou NTLM é negociado e usado. Deve-se notar que no caso no qual NTLM é negociado, o servidor prova conhecimento da senha do cliente, mas outros servidores no mesmo domínio têm acesso à senha. K_{spnego} é uma chave de subsessão Kerberos ou de sessão STML compartilhada por ambos os lados por completamento da troca SPNEGO.

Em 420, o LSA Cred SSP na máquina do cliente executa um cheque de política com base no nome principal de serviço do servidor (SPN), informações de autenticação do servidor (PKI/KRP vs. NTLM) e os ajustes de política de grupo, para determinar se delegar as credenciais do usuário para o servidor. Depois, em 430, verifica-se que a $K_{SSL/TLS}$ pertence ao servidor alvo e não a uma interferência humana, por execução da seguinte troca de autenticação exemplificativa:

C -> S: $\{\{K_{pub}\}K_{spnego}\}$ $K_{SSL/TSL}$

S -> C: $\{\{K_{pub} + 1\}K_{spnego}\}$ $K_{SSL/TSL}$

Deve-se notar que a $K_{SSL/TSL}$ é usada para codificar toda comunicação cliente / servidor. Além do mais, essa etapa de autenticação de servidor pode ser baseada em Kerberos ou NTLM, se não for confiança baseada em PKI. A ligação segura do canal autenticado SSL/TLS para a autenticação com base em Kerberos, como descrita, pode ser conduzida na parte de topo de SSL/TLS. Expressa de outro modo, a invenção pode utilizar com segurança as credenciais com base em Kerberos, para autenticar uma chave mestre / de sessão negociada por SSL/TLS, que pode ser particularmente útil se não houver qualquer confiança PKI entre o cliente SSL/TLS e o servidor SSL/TLS.

Finalmente, em 440, as credenciais do usuário (por exemplo, senha) podem ser delegadas ao servidor em uma maneira que impede a revisão das credenciais de texto claro, exceto pelo subsistema LSA confiável da invenção, de acordo com a seguinte troca de dados simbólicos:

C -> S: $\{\{Senha\}K_{spnego}\}$ $K_{SSL/TSL}$

Como descrito acima, por exemplo, nas etapas 340 (e política de grupo 335) e 420 das Figuras 3 e 4, respectivamente, as políticas são utilizadas para controlar e limitar

a delegação das credenciais do cliente, de acordo com a invenção, para atenuar uma ampla gama de ataques de segurança. Como mencionado, o pacote LSA da invenção proporciona negociação SPNEGO, codificação / decodificação de credencial e encaminhamento de credencial. O pacote LSA da invenção também executa cheques de política contra as políticas definidas de acordo com a invenção. A finalidade dos ajustes de política de grupo da invenção é garantir que as credenciais do usuário não sejam delegadas a um servidor não autorizado, por exemplo, uma máquina sob o controle administrativo de um fim de arquivo ou sujeito a um agressor. Deve-se notar que, ainda que a confiança possa existir para facilitar a autenticação entre o cliente e o servidor, por exemplo, com base em autenticação PKI, Kerberos ou NTLM, essa confiança não significa que o servidor alvo seja confiável com as credenciais do usuário. Desse modo, a invenção inclui uma consulta de política, para garantir que o servidor alvo pode ser confiável com as credenciais delegadas.

A Figura 5 é um diagrama de blocos não limitante, exemplificativo da arquitetura Cred SSP da invenção, que permite a delegação segura das credenciais de cliente para servidor, sem expor as credenciais de texto claro para a ou as aplicações de chamada. Similar à Figura 1, o Cred SSP é implementado como um conjunto de dois pacotes em ambos o cliente C e o servidor S: um pacote no lado do cliente e um pacote no lado LSA. No cliente C, isso se traduz em um Cred SSP no lado do Cliente e um Cred SSP no lado LSA. No servidor S, isso se traduz em um Cred SSP' no lado do Cliente e um Cred SSP' no lado LSA. A Figura 5 ilustra que, de acordo com a invenção, s credenciais de texto claro do usuário não são nunca armazenadas ou acessíveis para a aplicação de chamada CA de um cliente 500 solicitando uma aplicação de servidor, recurso ou ARS de serviço de um servidor 510. A linha pontilhada segmentando uma parte de subsistema confiável das LSAs mostra que apenas a parte do subsistema confiável das LSAs tem acesso às credenciais de texto claro do usuário, isto é, a capacidade de decodificar / codificar. Além disso, a Figura 5 ilustra o Cred SSP no lado LSA nas consultas na máquina do cliente das políticas de grupo GP da invenção, como descrito em mais detalhes abaixo.

Nesse aspecto, os ajustes da política de grupo, apresentados abaixo na Tabela III, definem que os servidores são confiáveis com as credenciais do usuário, em que cada ajuste é uma lista de nomes principais de serviços (SPNs); em uma modalidade, cartões curinga são permitidos. Como uma pessoa versada na técnica de reconhecimento de cadeias vai considerar, os cartões curinga se referem a caracteres, tal como "*", que podem representar qualquer caractere ou cadeia permissível em um alfabeto de SPNs. Desse modo, de acordo com a invenção, o Cred SSP (lado do cliente) apenas delega as credenciais do usuário, se o servidor for autenticado para o cliente e a SPN do servidor passa um cheque de política, por exemplo, como definido pelos ajustes de política de grupo (GP),

mostrados abaixo na Tabela III.

Os ajustes de política para delegar as credenciais de usuário definidas abaixo na Tabela III são projetados para atenuar uma variedade de ataques, incluindo, mas não limitados a, os ataques listados na Tabela I:

1	Um software malicioso ou Cavalo de Tróia pode estar rodando na máquina do cliente, por exemplo, em um modo de Acesso de Usuário Limitado (LUA), não admin.
2	Ajustes de GP padrão vs. outros valores GP, que podem ser configurados por administrador (incluindo malversação de cartões curinga).
3	Envenenamento de Serviço de Nome de Domínio (DNS). Quando o cliente resolve o nome do hospedeiro, pode estar em comunicação com um servidor de fim de arquivo.
4	Negativa de ataques de serviço no centro de Distribuição de Chaves Kerbero (KDC).

Tabela I - Tipos de atenuação de ajustes de políticas de ataque

A decisão feita na qual as políticas definidas de acordo com a invenção (definidas de um modo não limitante, exemplificativo na Tabela III abaixo) se aplica a uma determinada situação, dependendo do protocolo de autenticação negociado entre o cliente e o servidor, como descrito acima em conjunto com as Figuras 3 a 5, e do tipo de credenciais. A Figura 6 mostra três tipos exemplificativos de credenciais com as quais as políticas podem ser baseadas de acordo com a invenção, incluindo Credenciais Frescas, Credenciais Padrão e Credenciais Salvas. As credenciais frescas são as credenciais que são introduzidas em tempo real por meio de uma interface de usuário de credencial, tal como CredUI 610. As credenciais salvas que tinham sido anteriormente introduzidas como credenciais frescas, e que são armazenadas para reutilização adicional por um gerenciador de credencial, tal como CredMan 600, por exemplo, por um período de tempo limitado. As credenciais salvas são consideradas mais fracas de um ponto de vista de segurança do que as credenciais frescas. Ainda menos seguras são as credenciais padrão, que, como o nome implica, são credenciais padrão que são elaboradas para uso pela LSA 620, na ausência de outras instruções para o uso de outras credenciais. Por exemplo, as credenciais padrão podem incluir as credenciais introduzidas quando do registro. As credenciais padrão podem ser totalmente corretas para certas circunstâncias, que não necessitam de uma segurança elevada, tais como

certas credenciais de sítios da rede. Também, ainda que menos seguras, as credenciais padrão têm a vantagem de serem imediatamente disponíveis para a LSA 620. Desse modo, há três tipos de credenciais, que podem ser utilizados em conjunto com um pedido por um cliente de servidor de terminal, TSC, como mostrado na Figura 6. A Tabela II apresenta os três tipos de credenciais considerados nessa modalidade não limitante, exemplificativa: Fresco, Salva e Padrão.

Credenciais Frescas	Credenciais de usuário coletadas por interface de usuário, tal como CredUI, e passadas diretamente para a SSPI (por exemplo, passadas para a chamada AcquireCredentialsHandle).
Credenciais Padrão	Credenciais que foram proporcionadas inicialmente pelo usuário, quando o usuário assinou primeiro no sistema (disponível para os SSPs).
Credenciais Salvas	Credenciais de um servidor alvo particular que o usuário elegeu para salvar no gerenciador de credenciais (por exemplo, CredMan).

Tabela II- Tipos of Credenciais

Como referido acima, a Tabela III abaixo inclui um conjunto não limitante exemplificativo de ajustes de política de grupo (GP), para controlar / restringir a delegação de credenciais de usuário por um cliente para um servidor, de acordo com a invenção. Como pode considerar uma pessoa versada na técnica de redes de computadores, Termsrv/* significa um conjunto de SPNs, em que o serviço é Termsrv e a máquina hospedeira chamada após o traço oblíquo dianteiro "/" podem ser qualquer servidor alvo em comparação com o cartão curinga *.

#	Ajuste de GP (Lista de SPNs)	Valor Padrão	comentários
1	AllowDefCredentials *Significado:* Senha pode ser passada para os alvos listados quando da autenticação com credenciais padrão.	NULL	Ajuste padrão: Por padrão, a delegação de credenciais padrão (aquelas introduzidas quando o usuário faz a primeira assinatura) não é permitida a qualquer máquina. Isso significa software malicioso na máquina de cliente (em modo LUA) não vai ser capaz de delegar credenciais padrão por chamada no Cred SSP (independentemente

			de todos os outros fatores, isto é, esquema de autenticação), uma vez que o cheque de política vai falhar.
2	AllowSavedCredentials *Significado:* Senha pode ser passada para os alvos listados, quando da autenticação com as credenciais salvas.	Termsrv/*	Ajuste padrão: O valor padrão permite a delegação de credenciais salvas do usuário para o serviço do terminal rodando em qualquer máquina. Deve-se notar que isso se aplica aos servidores que o usuário registrou previamente e selecionados para salvar essas credenciais em CredMan. (O nome do servidor alvo é armazenado juntamente com as credenciais do usuário em CredMan).
3	AllowFreshCredentials *Significado:* Senha pode ser passada para alvo, quando da autenticação com as credenciais frescas.	Termsrv/*	Por comparação com os ajustes apresentados acima, com AllowFreshCredentials, não há qualquer possibilidade de software malicioso ser executado em uma entrada no sistema silenciosa (sem que o usuário seja informado, considerando que os ajustes de política AllowSavedCredentials e AllowDefCredentials não são habilitados)
4	DenyDefCredentials *Significado:* Senha pode ser passada para alvo, quando da autenticação com as credenciais padrão.	NULL	Este ajuste é usado para restringir ainda mais a que servidores as credenciais padrão de usuário podem ser delegadas, e por elas mesmas não oferecem uma oportunidade para explorar. No entanto, o administrador deve ainda ter cautela, quando da construção de uma política para credenciais padrão por combinação de ajuste de *DenyDefCredentials & AllowDefCredentials.* Se a *AllowDefCredentials* cobre uma ampla gama de servidores, a lista de exceções expressa por *DenyDefCredentials* pode não compreender compreensivamente todos os servidores não confiáveis em um determina-

			do ambiente. Isso pode se tornar um aspecto particular com o tempo, na medida em que novos servidores entram em linha. Adicionalmente, software malicioso com privilégios administrativos pode remover servidores não confiáveis da lista de DenyDefCredentials. No entanto, software malicioso com privilégios administrativos é uma condição de "jogo terminado", uma vez que há vários modos de obter a senha do usuário nesse caso.
5	DenySavedCredentials *Significado:* Senha pode ser passada para alvo, quando da autenticação com as credenciais salvas.	NULL	Este ajuste é usado para restringir ainda mais a que servidores as credenciais padrão de usuário podem ser delegadas, e por elas mesmas não oferecem uma oportunidade para explorar.
6	DenyFreshCredentials *Significado:* Senha pode ser passada para alvo, quando da autenticação com as credenciais frescas.	NULL	Este ajuste é usado para restringir ainda mais a que servidores as credenciais padrão de usuário podem ser delegadas, e por elas mesmas não oferecem uma oportunidade para explorar.
7	AllowDefCredentialsWhenNTLMOnly *Significado:* Se o único pacote de autenticação for NTML, e o usuário autentica com credenciais padrão, permitir que a senha seja passada para os alvos listados.	NULL	Por padrão, esse ajuste fica fora, uma vez que a confiança baseada em Kerberos e PKI oferece uma metodologia de autenticação mais forte do que NTLM.
8	AllowSavedCredentialsWhenNTLMOnly *Significado:* Se o único pacote de autenticação for NTML, e o usuário autenti-	Termsrv/* (desunido) NULL (unido)	Para suportar a fraqueza inerente no protocolo NTLM, a delegação de credenciais de usuário é permitida com padrão, apenas com as máquinas não unidas com o domínio (nesse caso, a autenticação do

	ca com credenciais salvas, permitir que a senha seja passada para os alvos listados.		usuário é garantida para ser feita pelo único alvo suportado na máquina). Por padrão, para o caso de união com o domínio, NTLM, por ele mesmo, não for permitida (a autenticação do servidor é baseada em Kerberos ou PKI).
9	AllowFreshCredentials WhenNTLMOnly *Significado:* Se a única autenticação for NTLM, e o usuário autenticar com credenciais frescas, permitir que a senha seja passada para os alvos listados.	Termsrv/*	

Tabela III - Ajuste de política de grupo para controle / restrição de delegação de credenciais de usuário

Em suma, a solução Cred SSP da invenção proporciona uma solução mais segura do que no passado, proporcionando um conjunto de políticas que podem ser usadas para controlar e restringir a delegação de credenciais de usuários do cliente para o servidor. Como o conjunto de políticas não limitante, exemplificativo da tabela III ilustra, as políticas são elaboradas para abordar uma ampla gama de ataques, incluindo software malicioso rodando na máquina do cliente. Adicionalmente, o Cred SSP da invenção inclui uma política "segura por padrão", que é a configuração particular pelos ajustes de políticas, que permite que uma máquina de cliente, por padrão, atenue uma ampla gama de ataques. Além do mais, o conjunto de políticas da invenção é aplicável para proteção de qualquer tipo de credenciais de usuários, incluindo, mas não limitado a nome de usuário / senha, pino de cartão inteligente, códigos de passagem por tempo (OTP), etc. O Cred SSP da invenção protege as credenciais dos usuários de modo que a aplicação de chamada (da Cred SSP API), no lado do servidor ou cliente, não tenha acesso a credenciais de texto claro, porque apenas um subsistema confiável tem acesso às credenciais de texto claro.

Meios ligados em rede e distribuídos exemplificativos

Uma pessoa versada na técnica vai considerar que a invenção pode ser implementada em conjunto com qualquer computador ou outro dispositivo de cliente ou servidor, que possa ser disposto como parte de uma rede de computador, ou em um meio de computação distribuído. Nesse aspecto, a presente invenção diz respeito a qualquer meio ou sistema de

computador tendo qualquer número de unidades de memória ou armazenamento, e qualquer número de aplicações e processos ocorrendo por qualquer número de unidades ou volumes de armazenamento, que podem ser usados em conjunto com os processos para delegação de credenciais de um cliente para um servidor, de acordo com a presente invenção. A presente invenção pode se aplicar a um meio com computadores de servidor e computadores de cliente dispostos em um meio ligado em rede ou um meio de computação distribuído, tendo armazenamento remoto ou local. A presente invenção pode ser também aplicada a dispositivo de computação dedicado, tendo uma funcionalidade de linguagem de programação, capacidades de interpretação e execução para gerar, receber e transmitir informações em conjunto com serviços e processos remotos ou locais.

A computação distribuída proporciona o compartilhamento de recursos e serviços de computador por troca entre os dispositivos e sistemas de computação. Esses recursos e sistemas incluem a troca de informações, o armazenamento cache e armazenamento em disco para objetos, tais como arquivos. A computação distribuída tira vantagem da conectividade em rede, permitindo que os clientes tenham influência no seu poder coletivo, para beneficiar a empresa. Nesse aspecto, vários dispositivos podem ter aplicações, objetos ou recursos que podem implicar em sistemas e métodos para delegar credenciais de um cliente para um servidor da invenção.

A Figura 7A proporciona um diagrama esquemático de um meio de computação ligado em rede ou distribuído exemplificativo. O meio de computação distribuído compreende os objetos de computação 10a, 10b, etc e os objetos ou dispositivos de computação 110a, 110b, 110c, etc.. Esses objetos podem compreender programas, métodos, armazenamentos de dados, lógica programável, etc. Os objetos podem compreender partes dos mesmos ou de dispositivos diferentes, tais como PDAs, dispositivos de áudio / vídeo, tocadores de MP3, computadores pessoais, etc. Cada objeto pode se comunicar com o outro objeto por meio da rede de comunicações 14. Essa rede pode ela própria compreender outros objetos de computação e dispositivos de computação, que proporcionam serviços ao sistema da Figura 7A, e podem eles mesmos representar redes interligadas múltiplas. De acordo com um aspecto da invenção, cada objeto 10a, 10b, etc. ou 110a, 110b, 110c, etc. pode conter uma aplicação que pode fazer uso de uma API, ou outro objeto, software, programação em hardware e/ou hardware, adequado para uso com os sistemas e métodos para a delegação de credenciais de um cliente para um servidor, de acordo com a invenção.

Pode-se também considerar que um objeto, tal como 110c, pode ser alojado em outro dispositivo de computação 10a, 10b, etc. ou 110a, 110b, etc. Desse modo, embora o meio físico ilustrado possa mostrar os dispositivos conectados como computadores, essa ilustração é meramente exemplificativa e o meio físico pode ser alternativamente ilustrado ou descrito compreendendo vários dispositivos digitais, tais como PDAs, televisões, tocado-

res de MP3, etc., objetos de software tais como interfaces, objetos COM e assemelhados.

Há uma variedade de sistemas, componentes, e configurações em rede que suportam os meio de computação distribuídos. Por exemplo, os sistemas de computação podem ser conectados conjuntamente por sistemas com ou sem fio, por redes locais ou redes distribuídas amplamente. Atualmente, muitas das redes são acopladas à Internet, que proporciona uma infra-estrutura para computação amplamente distribuída e abrange muitas diferentes redes. Quaisquer das infra-estruturas podem ser usadas para as comunicações exemplificativas feitas inerentes a delegação de credenciais de um cliente para um servidor de acordo com a presente invenção.

Em meios ligados em rede domésticos, há pelo menos quatro meios de transporte em rede discrepantes, que podem todos suportar um único protocolo, tal como linha de força, dados (tanto com quanto sem fio), voz (por exemplo, telefone) e meios de entretenimento. A maior parte dos dispositivos de controle domésticos, tais como ligações e aparelhos leves, podem usar linhas de força para conectividade. Os serviços de dados podem introduzir a casa como uma banda larga (por exemplo, modem DSL ou a Cabo) e são acessíveis dentro da casa usando conectividade sem fio (por exemplo, HomeRF ou 802.11B) ou com fio (por exemplo, Home PNA, Cat 5, Ethernet, ainda linha de força). O tráfego por voz pode introduzir a cada como com fio (por exemplo, Cat 3) ou sem fio (por exemplo, telefones celulares), e pode ser distribuído dentro da casa usando fiação Cat 3. Os meios de entretenimento, ou outros dados gráficos, podem introduzir a casa por satélite ou cabo, e são tipicamente distribuídos na casa usando cabo coaxial. Os IEEE 1394 e DVI são também interligações digitais para grupos de dispositivos de mídia. Todos esses meios de rede e outros que possam emergir, ou que já tenham emergidos, como padrões de protocolo para formar uma rede, tal como uma Intranet, que pode ser conectada para o mundo externo por meio de uma rede de longa distância, tal como a Internet. Em suma, uma variedade de fontes diversas existe para o armazenamento e a transmissão de dados, e, conseqüentemente, os dispositivos de computação de movimentação para frente vão requerer modos de compartilhamento de dados, tais como os dados acessados ou utilizados inerentes aos objetos de programas, tal como durante a delegação de credenciais de um cliente para um servidor, de acordo com a presente invenção.

A Internet se refere comumente à coleção de redes e portas que utilizam o conjunto de protocolos Protocolo de Controle de Transmissão / Protocolo de Internet (TCP/IP), que são bem conhecidos na técnica de ligação em rede de computadores. A Internet pode ser descrita como um sistema de redes de computadores remotos distribuídos geograficamente, interligadas por computadores executando protocolos de ligação em rede, que permitem que usuário interajam e compartilhem informações por uma ou mais redes. Em virtude desse compartilhamento de informações bem disseminado, as redes remotas, tal como a Internet,

evoluíram, desse modo, para um sistema aberto, com o qual os desenvolvedores podem projetar aplicações de software, para executar operações ou serviços especializados, essencialmente sem restrição.

Desse modo, a infra-estrutura em rede permite que um hospedeiro de topologias de rede, tal como cliente / servidor, ponto-a-ponto, ou arquiteturas híbridas. O "cliente" é um membro de uma classe ou grupo, que usa os serviços de outra classe ou grupo ao qual não está relacionado. Desse modo, em computação, um cliente é um processo, isto é, aproximadamente um conjunto de instruções ou tarefas, que requer um serviço proporcionado por outro programa. O processo cliente utiliza o serviço solicitado, sem que tenha que "conhecer" quaisquer detalhes operacionais sobre o outro programa ou o próprio serviço. Em uma arquitetura cliente / servidor, particularmente, um sistema ligado em rede, um cliente é usualmente um computador que acessa recursos de rede compartilhados proporcionados por outro computador, por exemplo, um servidor. Na ilustração da Figura 7A, como um exemplo, os computadores 110a, 110b, etc. podem ser imaginados como clientes e os computadores 10a, 10b, etc. podem ser imaginados como servidores, em que os servidores 10a, 10b, etc. mantêm os dados que são depois replicados a computadores clientes 110a, 110b, etc., embora qualquer computador possa ser considerado um cliente, um servidor, ou ambos, dependendo das circunstâncias. Quaisquer desses dispositivos de computação podem ser serviços ou tarefas de solicitação ou dados de processamento, que podem implicar na delegação de credenciais de um cliente para um servidor, de acordo com a invenção.

Um servidor é, tipicamente, um sistema de computadores remotos acessível por uma rede remota ou local, tal como a Internet. O processo cliente pode ser ativo em um primeiro sistema de computadores, e o processo servidor pode ser ativo em um segundo sistema de computadores, comunicando-se com um outro por um meio de comunicações, proporcionando, desse modo, funcionalidade distribuída e permitindo que clientes múltiplos tirem vantagem das capacidades de reunião de informações do servidor. Quaisquer objetos de software, utilizados de acordo com as técnicas para delegação de credenciais de um cliente para um servidor da invenção, podem ser distribuídos pelos múltiplos dispositivos ou objetos de computação.

Um ou mais clientes e servidores se comunicam entre si, utilizando a funcionalidade proporcionada por uma ou mais camadas de protocolo. Por exemplo, o Protocolo de Transferência de HiperTexto (HTTP) é um protocolo comum, que é usado em conjunto com a Rede de Amplitude Mundial (WWW) ou "a Rede". Tipicamente, um endereço de rede de computadores, tal como um endereço de Protocolo de Internet (IP) ou outra referência, tal como o Localizador de Recurso Universal (URL), pode ser usado para identificar os computadores servidores ou clientes entre si. O endereço da rede pode ser referida como um endereço URL. A comunicação pode ser proporcionada por um meio de comunicações, por exemplo,

um ou mais clientes e servidores podem ser acoplados entre si por uma ou mais conexões TCP/IP para comunicação de alta capacidade.

Desse modo, a Figura 7A ilustra um meio ligado em rede ou distribuído exemplificativo, com o um ou mais servidores em comunicação com o um ou mais computadores por uma rede / barramento, no qual a presente invenção pode ser empregada. Em mais detalhes, vários servidores 10a, 10b, etc. são interligadas por uma rede / barramento de comunicações 14, que pode ser uma LAN, WAN, Intranet, a Internet, etc., com um número de dispositivos de computação clientes ou remotos 110a, 110b, 110c, 110d, 110e, etc., tal como um computador portátil, um computador carregável, cliente fino, aparelho ligado em rede, ou outro dispositivo, tais como VCR, TV, forno, luz, aquecedor e assemelhados, de acordo com a presente invenção. Considera-se, desse modo, que a presente invenção pode se aplicar a qualquer dispositivo de computação em conjunto com o que é desejável para delegar credenciais de usuários a um servidor.

Em um meio ligado em rede, no qual a rede / barramento de comunicações 14 é a Internet, por exemplo, os servidores 10a, 10b, etc. podem ser servidores da Rede, com os quais os clientes 110a, 110b, 110c, 110d, 110e, etc. se comunicam por vários de quaisquer protocolos conhecidos, tal como HTPP. Os servidores 10a, 10b, etc., podem também servir como os clientes 110a, 110b, 110c, 110d, 110e, etc., como pode ser característico de um meio de computação distribuído.

Como mencionado, as comunicações podem ser com ou sem fio, ou uma combinação, quando adequado. Os dispositivos clientes 110a, 110b, 110c, 110d, 110e, etc. podem se comunicar ou não pela rede / barramento de comunicações 14, e podem ter comunicações independentes associadas com ele. Por exemplo, no caso de uma TV ou um VCR, pode haver ou não um aspecto de ligação em rede para seu controle. Todos os computadores clientes 110a, 110b, 110c, 110d, 110e, etc. e os computadores servidores 10a, 10b, etc. podem ser equipados com vários módulos ou objetos 135a, 135b, 135c, etc. e com conexões ou acesso a vários tipos de elementos ou objetos de armazenamento, pelos quais arquivos ou fluxo de dados podem ser armazenados ou nos quais parte(s) ou arquivos ou fluxos de dados podem ser carregados, transmitidos ou migrados. Qualquer de um ou mais computadores 10a, 10b, 110a, 110b, etc. pode ser responsável para a manutenção e atualização de uma base de dados 20, ou outro elemento de armazenamento, tal como uma base de dados ou memória 20, para armazenar os dados processados ou salvos de acordo com a invenção. Desse modo, a presente invenção pode ser utilizada em uma meio de rede de computadores, tendo os computadores clientes 110a, 110b, que podem acessar e interagir com uma rede / barramento de computador 14 e computadores servidores 10a, 110a, etc., que podem interagir com os computadores clientes 110a, 110b, e outros dispositivos similares, e bases de dados 20.

Dispositivo de Computação Exemplificativo

Como mencionado, a invenção se aplica a qualquer dispositivo no qual pode ser desejável proteger uma aplicação primária da interferência de aplicações secundárias do dispositivo. Deve-se entender, portanto, que um dispositivo de computação portátil, carregável ou outros dispositivos de computação e objetos de computação de todos os tipos são considerados para uso em conjunto com a presente invenção, isto é, em qualquer local no qual um dispositivo pode delegar credenciais para um servidor (por exemplo, rede GSM por um dispositivo portátil, tal como um telefone móvel). Conseqüentemente, o computador remoto multipropósito descrito abaixo na Figura 7B é apenas um exemplo, e a presente invenção pode ser implementada com qualquer cliente tendo interoperacionalidade e interação de rede / barramento. Desse modo, a presente invenção pode ser implementada em um meio de serviços hospedados em rede, nos quais muito poucos ou mínimos recursos de rede são implicados, por exemplo, um meio ligado em rede, no qual o dispositivo cliente serve meramente como uma interface para a rede / barramento, tal como um objeto colocado em um aparelho.

Embora não necessário, a invenção pode ser parcialmente implementada por um sistema operacional, para uso por um desenvolvedor de serviços para um dispositivo ou objeto, e/ou incluída dentro do software de aplicação que opera em conjunto com um ou mais componentes da invenção. O software pode ser descrito no contexto geral de instruções executáveis por computador, tais como módulos de programas, sendo executados por um ou mais computadores, tais como estações de trabalho de clientes, servidores ou outros dispositivos. Aqueles versados na técnica vão considerar que a invenção pode ser praticada com outras configurações e protocolos de sistemas de computadores.

A Figura 7B ilustra, desse modo, um exemplo de um meio de sistema de computação adequado 100a, no qual a invenção pode ser implementada, embora como esclarecido acima, o meio de sistema de computação 100a é apenas um exemplo de um meio de computação adequado para um dispositivo de computação e não é intencionada para sugerir qualquer limitação para o âmbito de uso ou funcionalidade da invenção. Tampouco, o meio de computação 100a deve ser interpretado como tendo qualquer dependência ou requisito relativo a qualquer um ou a uma combinação de componentes ilustrados no meio operacional exemplificativo 100a.

Com referência à Figura 7B, um dispositivo remoto exemplificativo para implementar a invenção inclui um dispositivo de computação multipropósito, na forma de um computador 110a. Os componentes do computador 110a podem incluir, mas não são limitados a, uma unidade de processamento 120a, uma memória de sistema 130a, e um barramento de sistema 121a, que acopla os vários componentes do sistema, incluindo a memória de sistema, à unidade de processamento 120a. O barramento de sistema 121a pode quaisquer de

vários tipos de estruturas de barramentos, incluindo um barramento de memória ou controlador de memória, um barramento periférico, e um barramento local usando qualquer uma de uma variedade de arquiteturas de barramento.

O computador 110a inclui, tipicamente, vários meios legíveis por computador. Os meios legíveis por computador podem ser quaisquer meios disponíveis, que podem ser acessados pelo computador 110a. Por meio de exemplo, e não limitação, os meios legíveis por computador podem compreender meios de armazenamento em computador e meios de comunicação. Os meios de armazenamento em computador incluem ambos os meios removíveis e não removíveis, voláteis e não voláteis, implementados em qualquer método ou tecnologia para armazenamento de informações, tais como instruções legíveis por computador, estruturas de dados, módulos de programas ou outros dados. Os meios de armazenamento em computador incluem, mas não são limitados a, RAM, ROM, EEPROM, memória instantânea ou outra tecnologia de memória, CDROM, discos versáteis digitais (DVDs) ou outro armazenamento em disco óptico, cassetes magnéticos, fita magnética, armazenamento em disco magnético ou outros dispositivos de armazenamento magnético, ou quaisquer outros meios que podem ser usados para armazenar as informações desejadas e que podem ser acessadas pelo computador 110a. Os meios de comunicação abrangem, tipicamente, instruções legíveis por computadores, estruturas de dados, módulos de programas ou outros dados em um sinal de dados modulado, tal como uma onda portadora ou um outro mecanismo de transporte e inclui quaisquer meio de distribuição de informações.

A memória de sistema 130a pode incluir meios de armazenamento em computador, na forma de memória volátil e/ou não volátil, tal como memória exclusiva de leitura (ROM) e/ou memória de acesso aleatório (RAM). Um sistema básico de entrada / saída (BIOS), contendo as rotinas básicas que ajudam a transferir informações entre os elementos dentro do computador 110a, tal como durante partida, pode ser armazenado na memória 130a. A memória 130a também contém, tipicamente, dados e/ou módulos de programas que são imediatamente acessíveis à, e/ou sendo operados no momento pela, unidade de processamento 120a. Por meio de exemplo, e não limitação, a memória 130a pode também incluir um sistema operacional, programas de aplicação, outros módulos de programas e dados de programas.

O computador 110a também pode incluir outros meios de armazenamento em computador voláteis / não voláteis, removíveis / não removíveis. Por exemplo, o computador 110a pode incluir uma unidade de disco rígido, que lê de, ou escreve em, meios magnéticos não voláteis, não removíveis, uma unidade de disco magnético que lê de, ou escreve em, um disco magnético não volátil, removível, e/ou uma unidade de disco óptico que lê de, ou escreve em, um disco óptico não volátil, removível, tal como um CD-ROM ou outros meios ópticos. Outros meios de armazenamento em computador voláteis / não voláteis, removíveis

/ não removíveis, que podem ser usados no meio operacional exemplificativo incluem, mas não são limitados a, cassetes de fitas magnéticas, cartões de memória instantânea, discos versáteis digitais, fita de vídeo digital, RAM no estado sólido e assemelhados. Uma unidade de disco rígido é conectada, tipicamente, ao barramento do sistema 121a por uma interface de memória não removível, tal como uma interface, e uma unidade de disco magnético ou uma unidade de disco óptico é tipicamente conectada ao barramento do sistema 121a por uma interface de memória removível, tal como uma interface.

Um usuário pode introduzir comandos e informações no computador 110a por dispositivos de entrada, tal como um teclado e um dispositivo de apontamento, referido comumente como um mouse, trackball ou mesa de toque. Outros dispositivos de entrada podem incluir um microfone, um joystick, um acionador de jogo, uma antena parabólica, um escâner ou assemelhados. Esses e outros dispositivos de entrada são freqüentemente conectados à unidade de processamento 120a pela entrada de usuário 140a e a uma ou mais interfaces associadas, que são acopladas ao barramento do sistema 121a, mas podem ser conectadas por outras interface e estruturas de barramento, tal como uma porta paralela, uma porta de jogo ou um barramento serial universal (USB). Um subsistema gráfico também pode ser conectado ao barramento de sistema 121a. Um monitor ou outro tipo de dispositivo visor é também conectado ao barramento do sistema 121a por uma interface, tal como uma interface de saída 150a, que pode, por sua vez, se comunicar com a memória de vídeo. Além de um monitor, os computadores também podem incluir outros dispositivos de saída periféricos, tais como alto-falantes e uma impressora, que podem ser conectados por uma interface de saída 150a.

O computador 110a pode operar em um meio ligado em rede ou distribuído usando conexões lógicas a um ou mais computadores remotos, tal como o computador remoto 170a, que pode ter, por sua vez, capacidades, tais como capacidade de meios, diferentes do dispositivo 110a. O computador remoto 170a pode ser um computador pessoal, um servidor, um roteador, um PC em rede, um dispositivo par ou outro nó de rede comum, ou qualquer outro dispositivo de consumo ou transmissão de meios remoto, e pode incluir qualquer um ou todos os elementos descritos acima relativos ao computador 110a. As conexões lógicas ilustradas na Figura 7B incluem uma rede 171a, tal como a rede de área local (LAN) ou uma rede de longa distância (WAN), mas pode incluir também outras redes / barramentos. Esses meios de ligação em rede são usuais em lares, escritórios, redes de computador amplas de empresas, Intranets e a Internet.

Quando usado em um meio de ligação em rede LAN, o computador 110a é conectado à LAN 171a por uma interface ou adaptador de rede. Quando usado em um meio de ligação em rede WAN, o computador 110a inclui, tipicamente, um componente de rede (cartão de rede, modem, etc.) ou outro meio para estabelecer comunicações pela WAN, tal co-

mo a Internet. Um meio para conexão a uma rede, que pode ser interno ou externo, pode ser conectado ao barramento de sistema 121a pela interface de entrada de usuário da entrada 140a, ou outro mecanismo adequado. Em um meio ligado em rede, os módulos de programas relativos ao computador 110a, ou partes dele, podem ser armazenados em um dispositivo de armazenamento de memória remoto. Vai-se considerar que as conexões de rede mostradas e descritas são exemplificativas, e outros meios de estabelecer uma ligação de comunicações entre os computadores podem ser usados.

Estruturas ou arquiteturas de computação distribuídas exemplificativas

Várias de computação distribuídas foram e estão sendo desenvolvidas à luz da convergência pessoal e da Internet. Os usuários individuais e comerciais semelhantes são proporcionados com uma interface interoperacional total e uma interface habilitada por rede para aplicações e dispositivos de computação, tornando as atividades de computação crescentemente de navegação na rede ou orientadas na rede.

Por exemplo, a plataforma de código gerenciado pela MICROSOFT isto é, .NET, inclui servidores, serviços de blocos de estrutura, tal como armazenamento de dados com base na rede e software de dispositivo carregável. De uma maneira geral, a plataforma .NET proporciona: (1) capacidade para fazer com toda a gama de dispositivos de computação trabalhe em conjunto e tenha informações de usuários automaticamente atualizadas e sincronizadas em todos eles; (2) uma maior capacidade interativa para as páginas da Rede, habilitadas por maior uso de XML em vez de HTML; (3) os serviços em linha que caracterizam o acesso e a distribuição personalizados de produtos e serviços para o usuário de um ponto de partida central, para o gerenciamento de várias aplicações, tal como correio eletrônico, por exemplo, ou software, tal como Office .NET; (4) armazenamento de dados centralizado, que aumenta a eficiência e a facilidade de acesso a informações, bem como a sincronização de informações entre os usuários e dispositivos; (5) a capacidade para integrar vários meios de comunicação, tais como correio eletrônico, faxes e telefones; (6) para desenvolvedores, a capacidade de criar módulos reutilizáveis, aumentando, desse modo, a produtividade e reduzindo o número de erros de programação; e (7) muitos outros recursos de integração de linguagem e de plataforma cruzada também.

Ainda que algumas modalidades exemplificativas da presente invenção sejam descritas em conjunto com software, tal como uma aplicação de interface de programação (API), residindo em um dispositivo de computação, uma ou mais partes da invenção também podem ser implementadas por um sistema operacional, ou um objeto de "interferência humana", um objeto de controle, hardware, programação em hardware, instruções ou objetos de linguagem intermediária, etc., de modo que os métodos para delegar credenciais de um cliente para um servidor de acordo com a invenção possam ser incluídos em, suportados em ou acessados por todas as linguagens e serviços habilitados por código gerenciado, tal co-

mo código .NET, e também em outras estruturas de computação distribuídas.

Há modos múltiplos de implementação da presente invenção, por exemplo, uma API adequada, um kit de ferramentas, um código de acionador, um sistema operacional, objeto de software autônomo ou carregável, etc, que permita que as aplicações e serviços usem os sistemas e métodos para delegar credenciais de um cliente para um servidor da invenção. A invenção considera o uso da invenção do ponto de vista de uma API (ou outro objeto de software), bem como de um objeto de software ou hardware que receba um programa carregado de acordo com a invenção. Desse modo, várias implementações da invenção descritas no presente relatório descritivo podem ter aspectos que estão inteiramente em hardware, parcialmente em hardware e parcialmente em software, bem como em software.

Como mencionado acima, ainda que as modalidades exemplificativas da presente invenção tenham sido descritas em conjunto com os vários dispositivos de computação e arquiteturas de rede, os conceitos subjacentes podem ser aplicados a qualquer dispositivo ou sistema de computação, no qual é desejável delegar credenciais de um cliente para um servidor. Por exemplo, o um o mais algoritmos ou implementações de hardware da invenção podem ser aplicados ao sistema operacional de um dispositivo de computação, proporcionado como um objeto separado no dispositivo, como parte de outro objeto, como um controle reutilizável, como um objeto carregável de um servidor, como uma "interferência humana" entre um dispositivo ou objeto e a rede, como um objeto distribuído, como hardware, em memória, uma combinação de quaisquer dos precedentes, etc. Ainda que as linguagens de programação, nomes e exemplos ilustrativos sejam selecionados no presente relatório descritivo como representativos de várias seleções, essas linguagens, nomes e exemplos não são intencionados para serem limitantes. Uma pessoa versada na técnica vai considerar que há vários modos de proporcionar código e nomenclatura de objeto que atinge uma funcionalidade igual, similar ou equivalente obtida pelas várias modalidades da invenção.

Como mencionado, as várias técnicas descritas no presente relatório descritivo podem ser implementadas em conjunto com hardware ou software, ou, quando adequado, com uma combinação de ambos. Desse modo, os métodos e aparelho da presente invenção, ou de certos aspectos ou partes deles, podem assumir a forma de código (isto é, instruções) de programa incorporadas em meios tangíveis, tais como disquetes flexíveis, CD-ROMs, unidades de disco rígido, ou qualquer outro meio de armazenamento legível por máquina, em que, quando o código de programa é carregado em, e executado por, uma máquina, tal como um computador, a máquina se torna um aparelho para a prática da invenção. No caso de execução de código de programa em computadores programáveis, o dispositivo de computação inclui, geralmente, um processador, um meio de armazenamento legível pelo processador (incluindo elementos de memória volátil e não volátil e de armazenamento), pelo menos um dispositivo de entrada, e pelo menos um dispositivo de saída. Um ou mais pro-

gramas que podem implementar ou utilizar os métodos para delegação de credenciais de um cliente para um servidor da presente invenção, por exemplo, por uso de uma API de processamento de dados, controles reutilizáveis, ou assemelhados, são implementados preferivelmente em uma linguagem de programação orientada por objeto ou de processamento em alto nível, para se comunicar com um sistema computador. No entanto, o um ou mais programas podem ser implementados em linguagem de montagem ou de máquina, se desejado. Em qualquer caso, a linguagem pode ser linguagem compilada ou interpretada, e combinada com implementações de hardware.

Os métodos e o aparelho da presente invenção também podem ser postos em prática por meio das comunicações incorporadas na forma de código de programa, que é transmitido por algum meio de transmissão, tal como por uma ligação elétrica por fio ou cabo, por meio de fibras ópticas, ou por meio de qualquer outra forma de transmissão, em que, quando o código de programa é recebido e carregado em, e executado por, uma máquina, tal como por uma EPROM, um arranjo de circuitos, um dispositivo de lógica programável (PLD), um computador de cliente, etc., a máquina se transforma em um aparelho para a prática da invenção. Quando implementado em um processador multipropósito, o código de programa se combina com o processador para proporcionar um aparelho único que opera para invocar a funcionalidade da presente invenção. Adicionalmente, quaisquer técnicas de armazenamento usadas em conjunto com a presente invenção podem ser, invariavelmente, uma combinação de hardware e software.

Ainda que a presente invenção tenha sido descrita em conjunto com as modalidades preferidas das várias figuras, deve-se entender que outras modalidades similares podem ser usadas, ou modificações e adições podem ser feitas na modalidade descrita para executar a mesma função da presente invenção, sem desviar-se dela. Por exemplo, ainda que meios de rede exemplificativos da invenção sejam descritos no contexto de um meio ligado em rede, tal como um meio ligado em rede ponto-a-ponto, aqueles versados na técnica vão reconhecer que a presente invenção não é limitada a ele, e que os métodos, como descrito no presente pedido de patente, podem se aplicar a qualquer dispositivo ou meio de computação, tal como um console de jogo, um computador carregável, um computador portátil, etc., se ligado com fio ou não, e podem ser aplicados a qualquer número desses dispositivos de computação conectados por uma rede de comunicações, e interagindo pela rede. Além do mais, deve-se enfatizar que várias plataformas de computadores, incluindo sistemas operacionais de dispositivos portáteis e outros sistemas operacionais específicos de aplicações são considerados, especialmente, na medida em que o número de dispositivos ligados em rede sem fio continua a proliferar.

Ainda que as modalidades exemplificativas se refiram à utilização da presente invenção no contexto de constructos de linguagem de programação, a invenção não é assim

limitada, mas em vez disso pode ser implementada em qualquer linguagem, para proporcionar métodos para delegar credenciais de um cliente para um servidor. Ainda mais, a presente invenção pode ser implementada em, ou por, uma pluralidade de circuitos integrados ou dispositivos de processamento, e o armazenamento pode ser feito, de modo similar, por uma pluralidade de dispositivos. Portanto, a presente invenção não deve ser limitada a qualquer modalidade única, mas deve ser em vez disso considerada em amplitude e âmbito de acordo com as reivindicações em anexo.

REIVINDICAÇÕES

1. Método para delegar credenciais de usuários de um cliente para um servidor em uma meio de computação ligado em rede, **CARACTERIZADO** pelo fato de que compreende:

solicitação de um cliente para uma aplicação, serviço ou recurso no meio de computação ligado em rede, que implica na delegação de credenciais de usuários do cliente para o servidor;

iniciação de um sinal de estabelecimento de comunicação entre o cliente e o servidor;

negociação para selecionar um pacote de autenticação compartilhado entre o cliente e o servidor, para utilizar como um mecanismo de autenticação para autenticar as comunicações entre o cliente e o servidor;

autenticação mútua do servidor e do cliente utilizando o pacote de autenticação selecionado como o mecanismo de autenticação;

determinação se a autenticação mútua ocorreu de acordo com a dita etapa de autenticação mútua, e se a autenticação mútua ocorreu, o estabelecimento de uma sessão entre o cliente e o servidor, incluindo o estabelecimento de um segredo compartilhado para codificação de mensagens comunicadas entre o cliente e o servidor;

antes de transmitir as credenciais para o pedido, executar um cheque de política de acordo com a pelo menos uma política predefinida, estabelecida para que as credenciais dos usuários determinem se o servidor é confiável com as credenciais de usuários; e

se o servidor for confiável, transmissão das credenciais de usuários para o servidor para ganhar acesso à aplicação, serviço ou recurso solicitado do servidor oriundo do cliente.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a pelo menos uma política predefinida é uma pluralidade de políticas usadas para controlar e restringir a delegação de credenciais de usuários de um cliente para um servidor.

3. Método, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que a pluralidade de políticas aborda a mitigação de uma ampla gama de ataques, incluindo pelo menos um de cavalo de Tróia ou software malicioso rodando no cliente, ajustes de política de grupo padrão, e valores de política de grupo configuráveis por um administrador do cliente, envenenamento de serviço de nome de domínio (DNS) para evitar a resolução a um servidor de final de arquivo e negativa de ataques de serviço.

4. Método, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que a pluralidade de políticas inclui políticas em que pelo menos uma permite ou nega a delegação, com base em uma lista de nomes principais dos serviços (SPNs) do servidor.

5. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a execução inclui executar um cheque de política, de acordo com uma intensidade relativa do

mecanismo de autenticação.

6. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a execução inclui executar um cheque de política, de acordo com pelo menos uma política predefinida, estabelecida com base no tipo de credenciais de usuários.

7. Método, de acordo com a reivindicação 6, **CARACTERIZADO** pelo fato de que a execução inclui a execução de um cheque de política, de acordo com pelo menos uma política predefinida, estabelecida com base em se as credenciais de usuários são credenciais frescas, salvas ou padrão.

8. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a dita transmissão das credenciais de usuários inclui a transmissão de credenciais de usuários em um formato que apenas um subsistema confiável de um sistema de segurança local tem acesso às credenciais de usuários em um formato de texto claro.

9. Método, de acordo com a reivindicação 8, **CARACTERIZADO** pelo fato de que a execução do cheque de política é feita por uma autoridade de segurança local (LSA), e o subsistema confiável é um subsistema confiável da LSA.

10. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que compreende, após estabelecimento da sessão entre o cliente e o servidor, autenticação da chave pública do servidor.

11. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que as ditas etapas são conduzidas por um componente provedor de suporte de segurança de credencial, disponibilizado para o cliente que faz a solicitação por meio de uma interface de provedor de suporte (SSPI).

12. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o estabelecimento de comunicação inicial é um estabelecimento de comunicação de acordo com o protocolo da camada de soquetes segura (SSL) ou de segurança da camada de transporte (TLS).

13. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a negociação inclui negociar usando a negociação do Mecanismo de Negociação da Interface de Programa de Aplicação de Serviço de Segurança Genérico (GSSAPI) Simples e Protegido (SPNEGO).

14. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o pacote de autenticação selecionado é qualquer um de Kerberos ou Gerenciador de Rede de Área Local (LAN) NT (NTLM).

15. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o segredo compartilhado é a chave de sessão compartilhada.

16. Interface de programação de aplicação, **CARACTERIZADA** pelo fato de que compreende módulos de interface executáveis por computador, tendo instruções executá-

veis para execução do método de acordo com a reivindicação 1.

17. Dispositivo de computação cliente, **CARACTERIZADO** pelo fato de que compreende:

um componente provedor de suporte de segurança de credencial para manipular uma solicitação do dispositivo de computação cliente para uma aplicação, um serviço ou um recurso de um servidor no meio de computação ligado em rede, em que a solicitação implica na delegação de credenciais de usuários do dispositivo de computação cliente para o servidor; em que o componente provedor de suporte de segurança de credencial inicia um estabelecimento de comunicação entre o cliente e o servidor, negocia a seleção de um provedor de suporte de segurança, entre o cliente e o servidor, para utilizar como um pacote de autenticação, para autenticar as comunicações entre o cliente e o servidor, executa as etapas para autenticar mutuamente o servidor e o cliente utilizando o pacote de autenticação; em que, se autenticação manual tiver ocorrido, o componente provedor de suporte de segurança de credencial estabelece uma sessão entre o cliente e o servidor e um segredo compartilhado, para codificação de mensagens, comunicado entre o cliente e o servidor, de acordo com a sessão, executa um cheque de política de acordo com pelo menos uma política predefinida, usada para controlar e limitar a delegação de credenciais de usuários do dispositivo de computação cliente para o servidor, e transmite as credenciais dos usuários para o servidor, para ganhar acesso à aplicação, serviço ou recurso solicitado do servidor oriundo do cliente, apenas se o cheque de política tiver passado.

18. Dispositivo de computação cliente, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que o componente provedor de suporte de segurança transmite as credenciais de usuários em um formato no qual apenas um subsistema confiável de uma autoridade de segurança local (LSA) pode decodificar a um formato de texto claro.

19. Dispositivo de computação cliente, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que a pelo menos uma política predefinida aborda a mitigação de qualquer um ou mais de uma ampla gama de ataques, incluindo cavalo de Tróia ou software malicioso rodando no cliente, os ajustes de políticas de grupo padrão e os valores de política de grupo configuráveis por um administrador do cliente, envenenamento de serviço de nome de domínio (DNS) para evitar a resolução a um servidor de final de arquivo e negativa de ataques de serviço.

20. Dispositivo de computação cliente, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que a pelo menos uma política predefinida inclui uma política de delegação com base em uma intensidade relativa do mecanismo de autenticação.

21. Dispositivo de computação cliente, de acordo com a reivindicação 17, **CARACTERIZADO** pelo fato de que a pelo menos uma política predefinida inclui uma políti-

ca de delegação, baseada em se as credenciais dos usuários são credenciais frescas, salvas ou padrão.

22. Método para delegar credenciais de usuários, de um cliente para um servidor, em um meio de computação ligado em rede, como parte de um sinal único para os recursos do servidor, **CARACTERIZADO** pelo fato de que inclui:

receber as credenciais dos usuários por meio de um sinal único de um componente de interface de usuário de um cliente, para acessar um conjunto de recursos do servidor, e, em resposta, iniciar um estabelecimento de comunicação entre o cliente e o servidor, de acordo com o protocolo de segurança de camada de transporte (TLS);

negociar para selecionar um pacote de autenticação compartilhado entre o cliente e o servidor, para utilizar como um mecanismo de autenticação, para autenticar as comunicações entre o cliente e o servidor;

autenticar mutuamente o servidor e o cliente utilizando o pacote de autenticação selecionado como o mecanismo de autenticação;

se tiver ocorrido a autenticação mútua, estabelecer uma sessão entre o cliente e o servidor, incluindo o estabelecimento de um segredo compartilhado para codificação de mensagens comunicadas entre o cliente e o servidor; e

delegar com segurança as credenciais dos usuários para o servidor, para ganhar acesso ao conjunto de recursos.

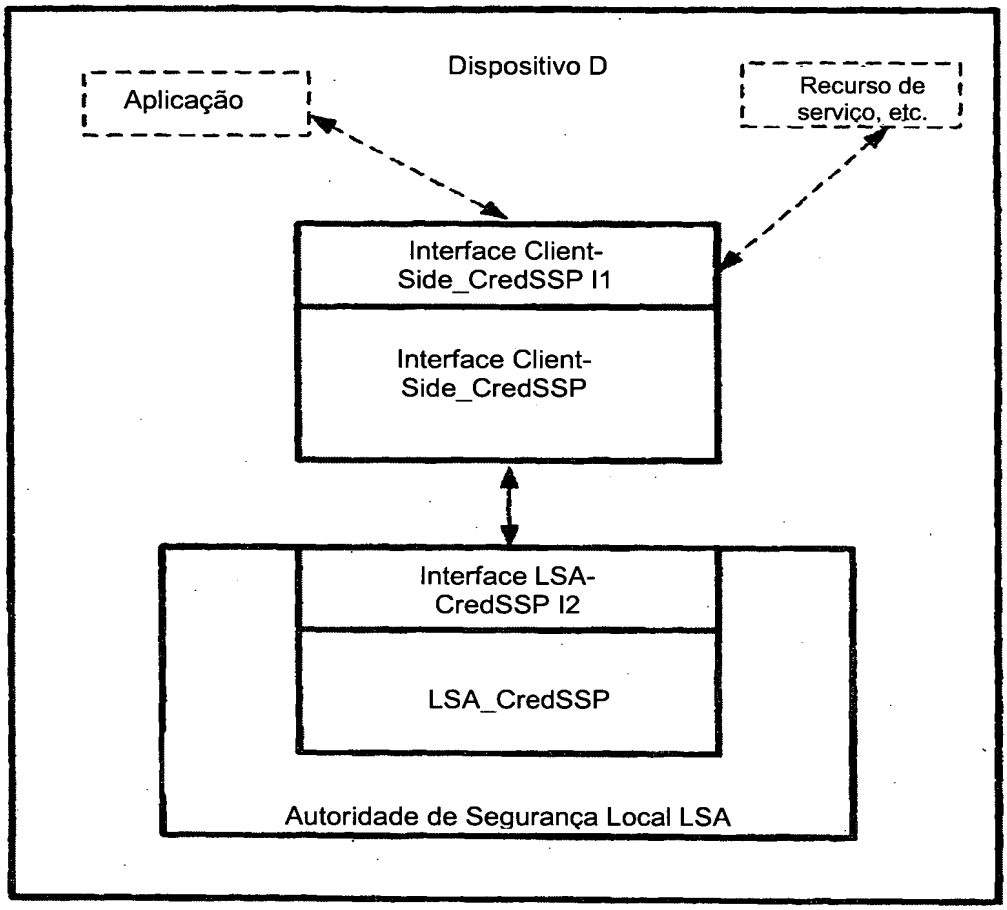

Dispositivo D
Aplicação
Recurso de serviço, etc.
Interface Client-Side_CredSSP I1
Interface Client-Side_CredSSP
Interface LSA-CredSSP I2
LSA_CredSSP
Autoridade de Segurança Local LSA

FIG. 1

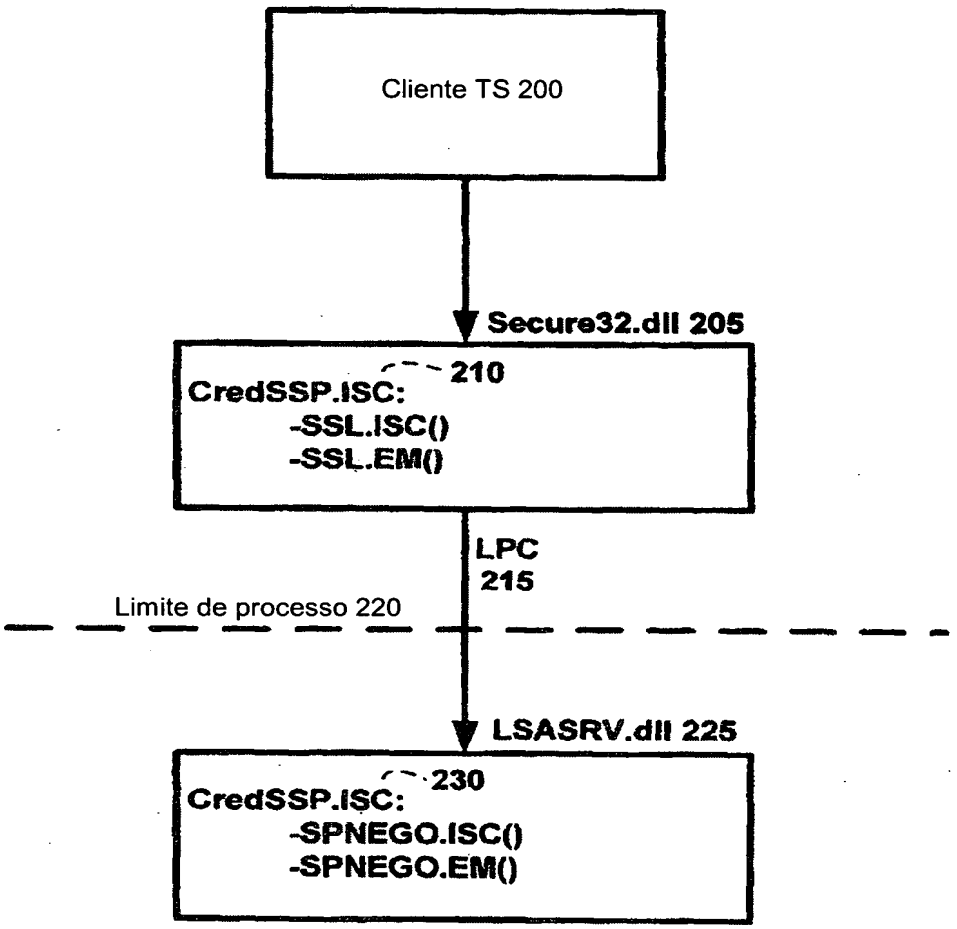

Cliente TS 200
Secure32.dll 205
210
CredSSP.ISC:
-SSL.ISC()
-SSL.EM()
LPC
215
Limite de processo 220
LSASRV.dll 225
230
CredSSP.ISC:
-SPNEGO.ISC()
-SPNEGO.EM()

FIG. 2A

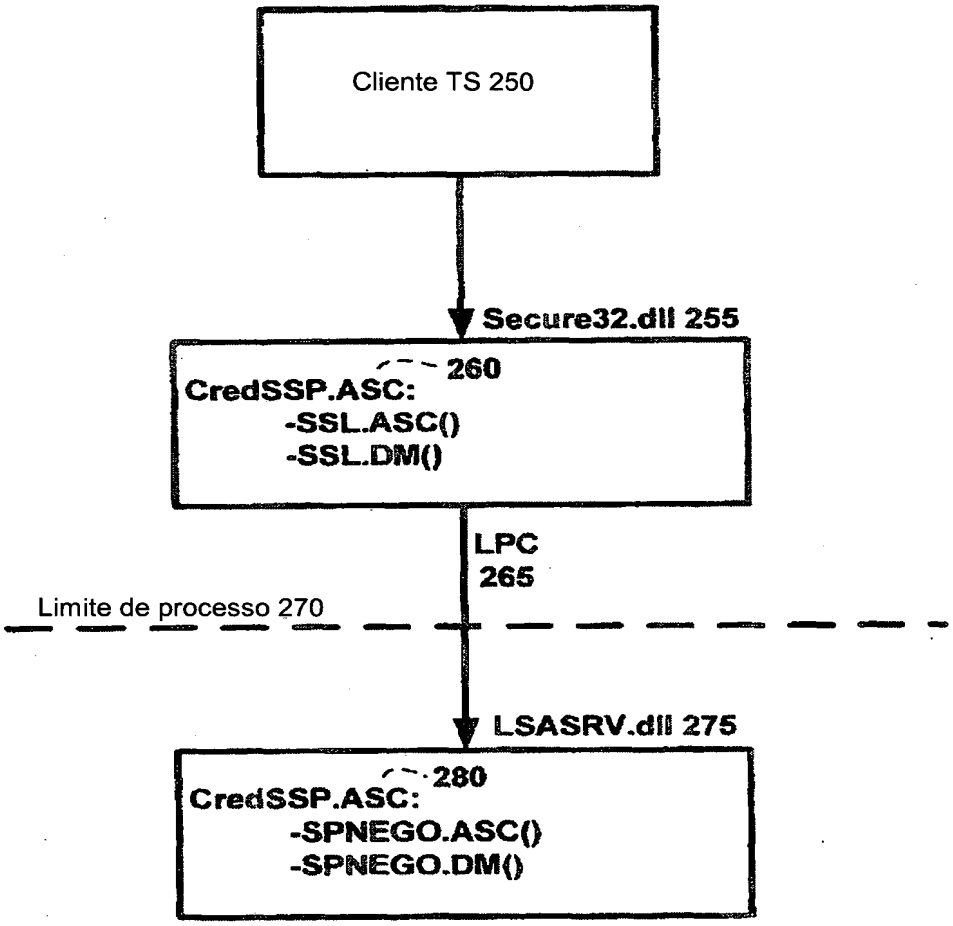

Cliente TS 250
Secure32.dll 255
260
CredSSP.ASC:
-SSL.ASC()
-SSL.DM()
LPC
265
Limite de processo 270
LSASRV.dll 275
280
CredSSP.ASC:
-SPNEGO.ASC()
-SPNEGO.DM()

FIG. 2B

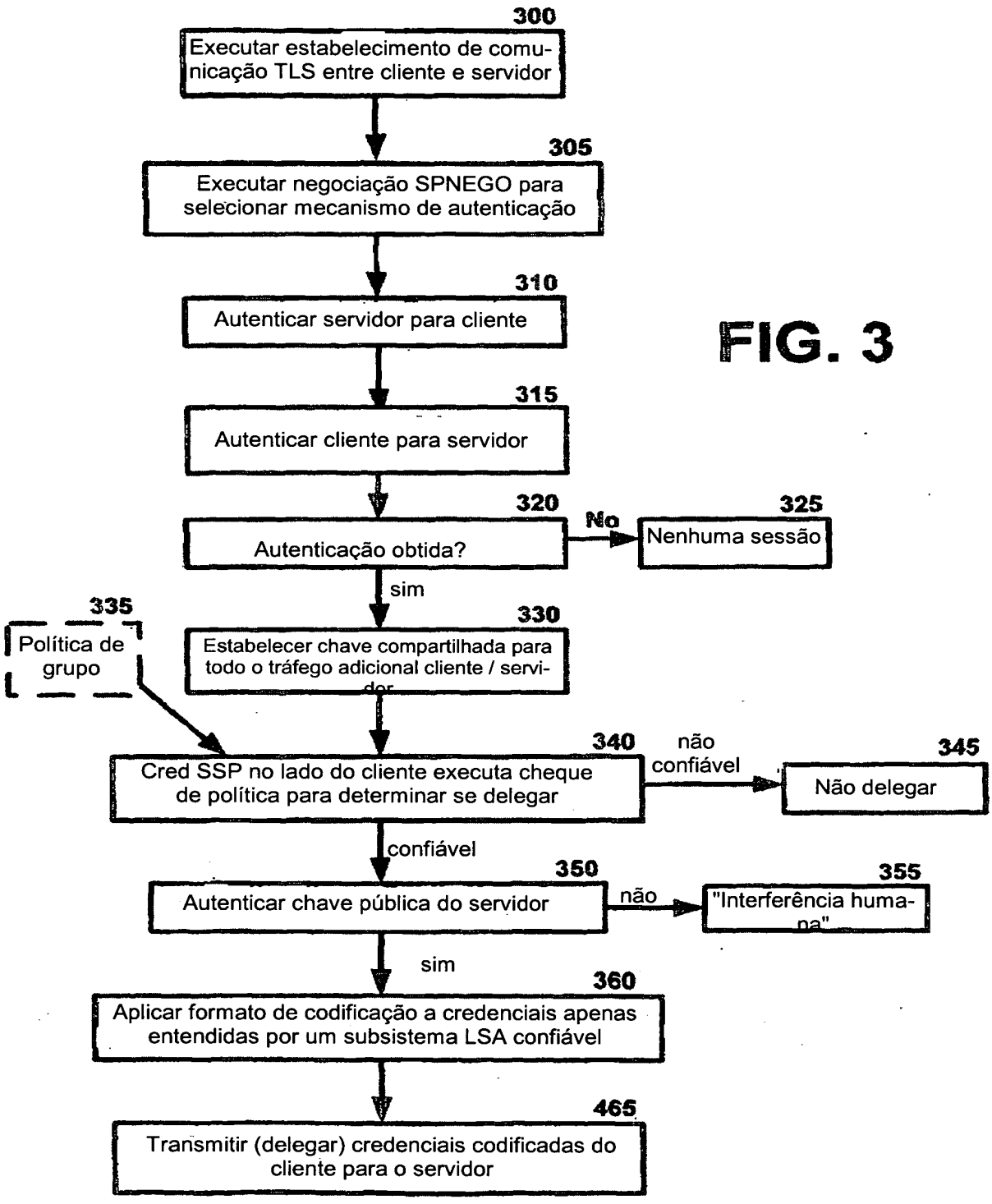

300
Executar estabelecimento de comunicação TLS entre cliente e servidor
305
Executar negociação SPNEGO para selecionar mecanismo de autenticação
310
Autenticar servidor para cliente
315
Autenticar cliente para servidor
320
Autenticação obtida?
No
325
Nenhuma sessão
sim
335
Política de grupo
330
Estabelecer chave compartilhada para todo o tráfego adicional cliente / servidor
340
Cred SSP no lado do cliente executa cheque de política para determinar se delegar
não confiável
345
Não delegar
confiável
350
Autenticar chave pública do servidor
não
355
"Interferência humana"
sim
360
Aplicar formato de codificação a credenciais apenas entendidas por um subsistema LSA confiável
465
Transmitir (delegar) credenciais codificadas do cliente para o servidor

FIG. 3

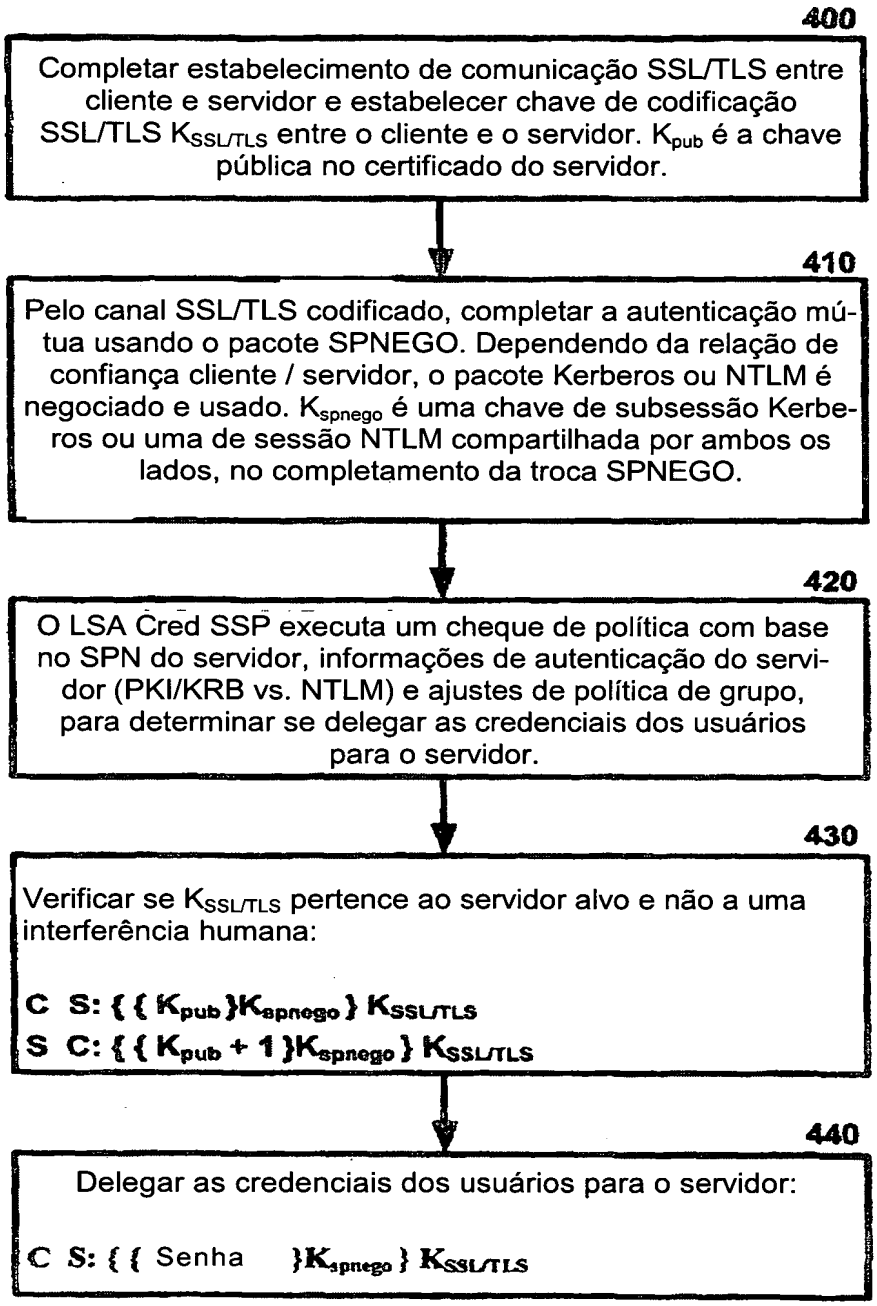

400
Completar estabelecimento de comunicação SSL/TLS entre cliente e servidor e estabelecer chave de codificação SSL/TLS $K_{SSL/TLS}$ entre o cliente e o servidor. K_{pub} é a chave pública no certificado do servidor.
410
Pelo canal SSL/TLS codificado, completar a autenticação mútua usando o pacote SPNEGO. Dependendo da relação de confiança cliente / servidor, o pacote Kerberos ou NTLM é negociado e usado. K_{spnego} é uma chave de subsessão Kerberos ou uma de sessão NTLM compartilhada por ambos os lados, no completamento da troca SPNEGO.
420
O LSA Cred SSP executa um cheque de política com base no SPN do servidor, informações de autenticação do servidor (PKI/KRB vs. NTLM) e ajustes de política de grupo, para determinar se delegar as credenciais dos usuários para o servidor.
430
Verificar se $K_{SSL/TLS}$ pertence ao servidor alvo e não a uma interferência humana:
C S: { { K_{pub} }K_{spnego} } $K_{SSL/TLS}$
S C: { { K_{pub} + 1 }K_{spnego} } $K_{SSL/TLS}$
440
Delegar as credenciais dos usuários para o servidor:
C S: { { Senha }K_{spnego} } $K_{SSL/TLS}$

FIG. 4

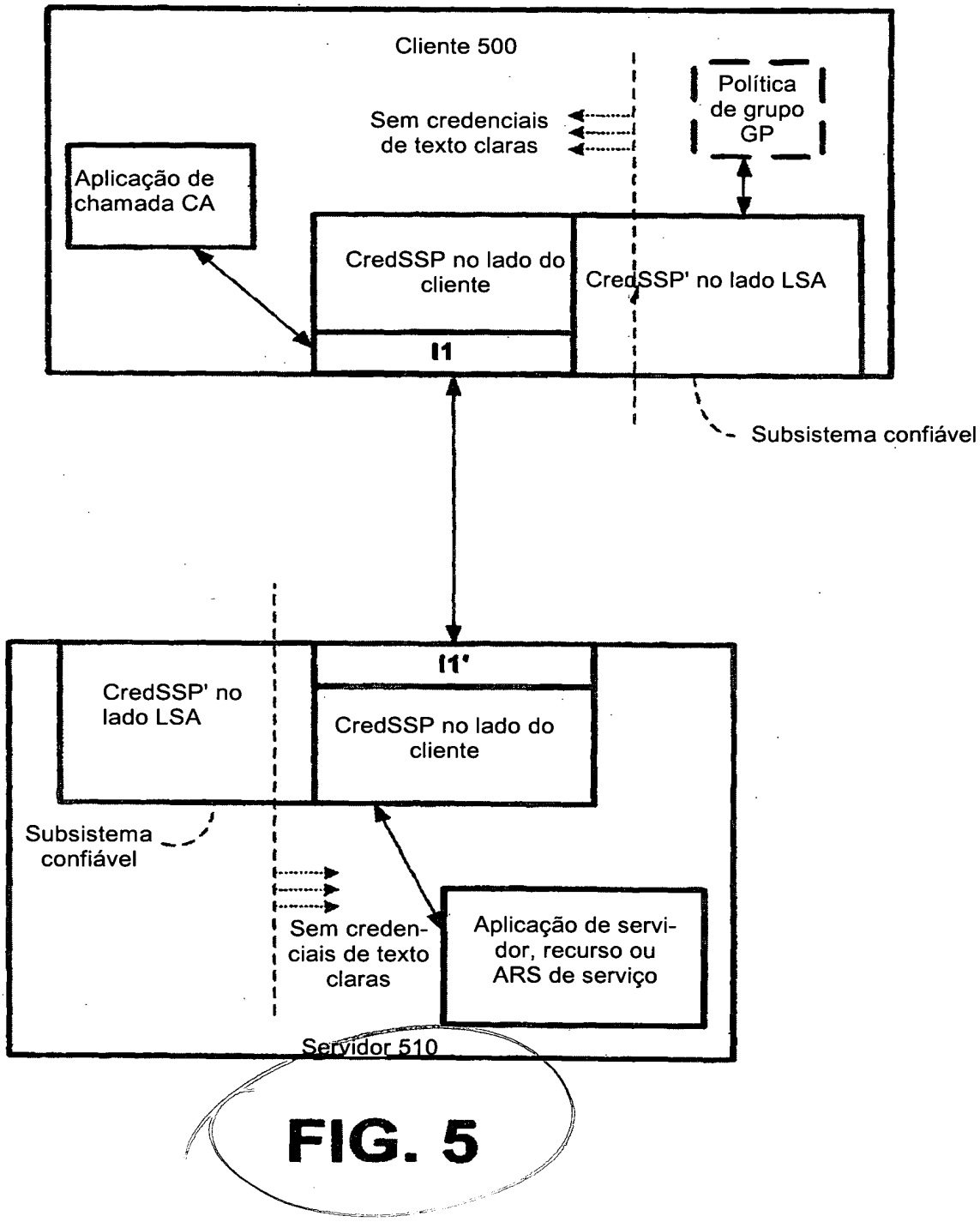

Cliente 500
Política de grupo GP
Sem credenciais de texto claras
Aplicação de chamada CA
CredSSP no lado do cliente
CredSSP' no lado LSA
I1
Subsistema confiável
I1'
CredSSP' no lado LSA
CredSSP no lado do cliente
Subsistema confiável
Sem credenciais de texto claras
Aplicação de servidor, recurso ou ARS de serviço
Servidor 510

FIG. 5

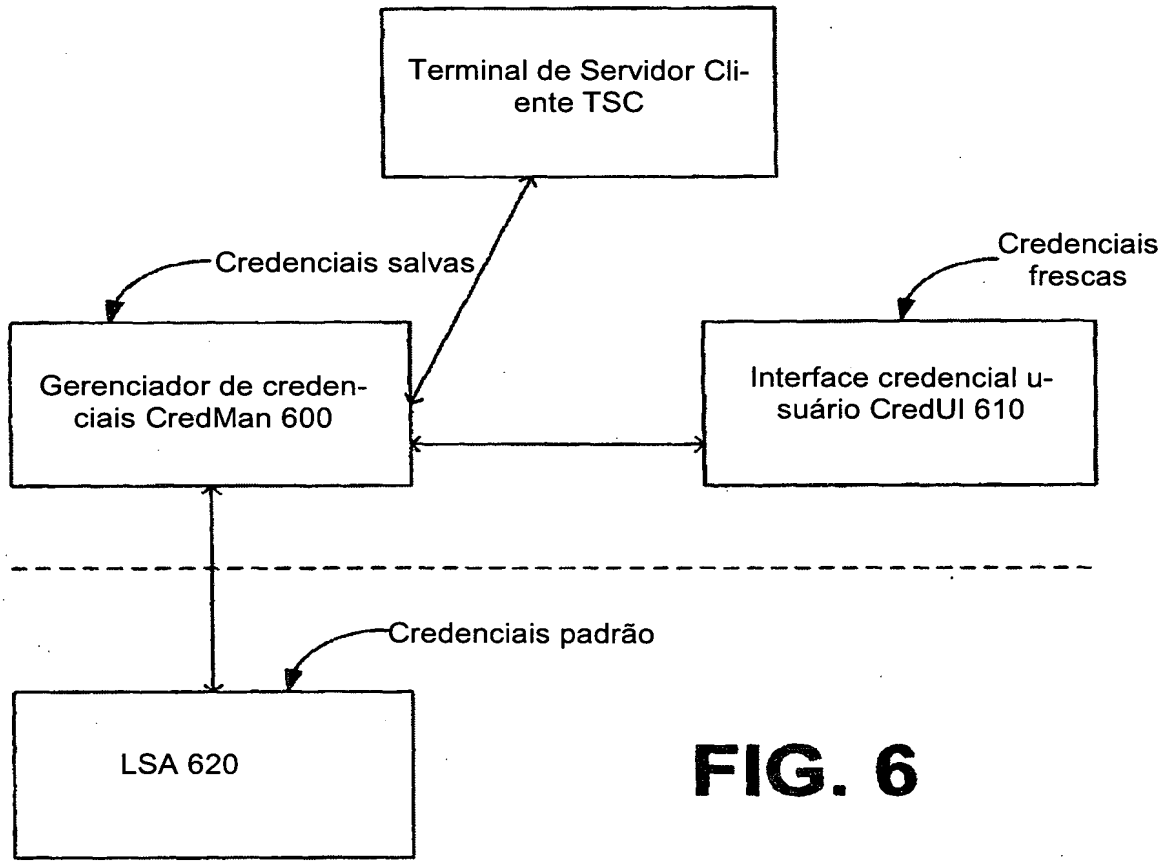

Terminal de Servidor Cliente TSC
Credenciais salvas
Credenciais frescas
Gerenciador de credenciais CredMan 600
Interface credencial usuário CredUI 610
Credenciais padrão
LSA 620

FIG. 6

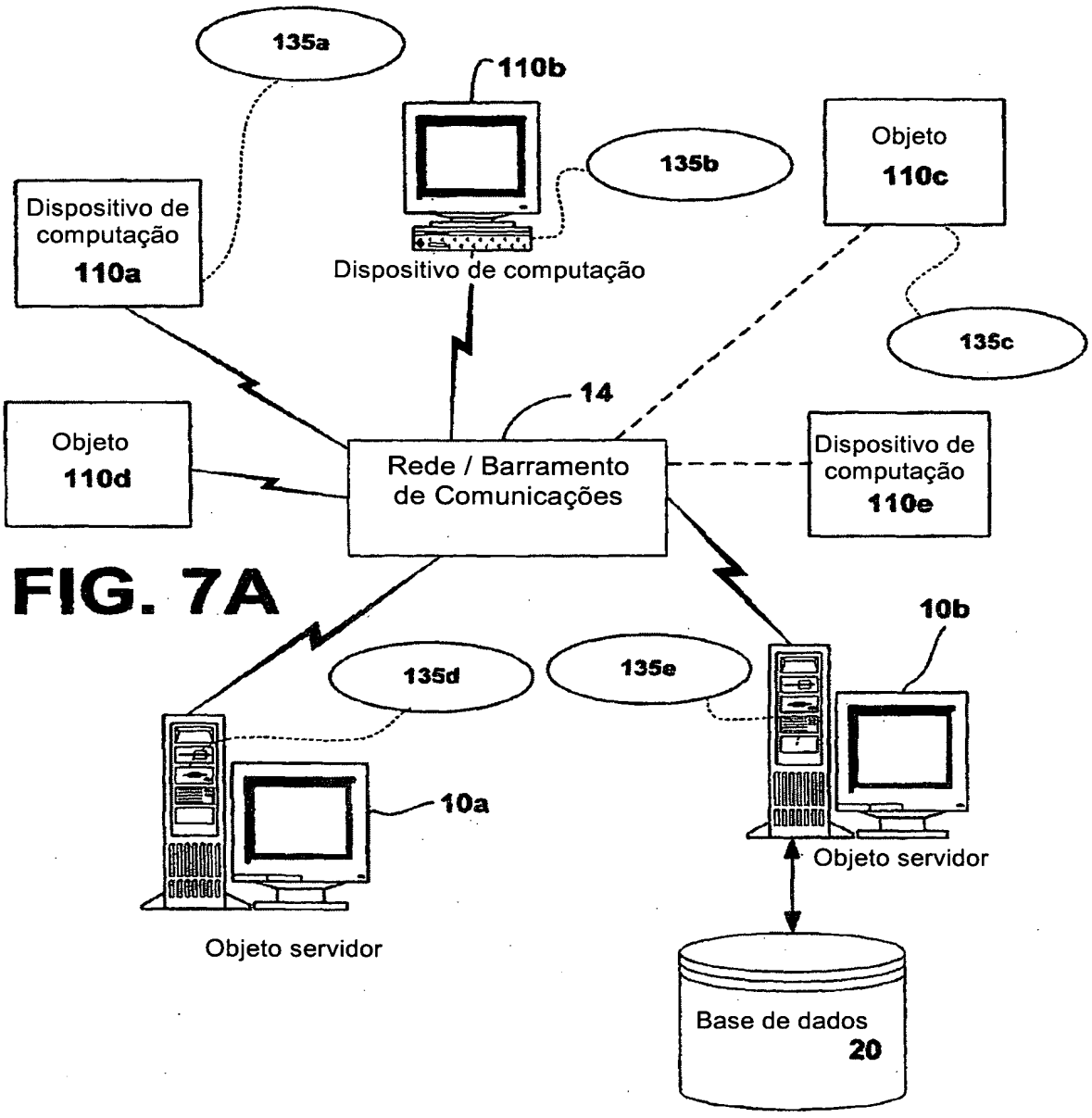

135a
110b
135b
Objeto
110c
Dispositivo de computação
110a
Dispositivo de computação
135c
14
Objeto
110d
Rede / Barramento de Comunicações
Dispositivo de computação
110e
10b
135d
135e
10a
Objeto servidor
Objeto servidor
Base de dados
20

FIG. 7A

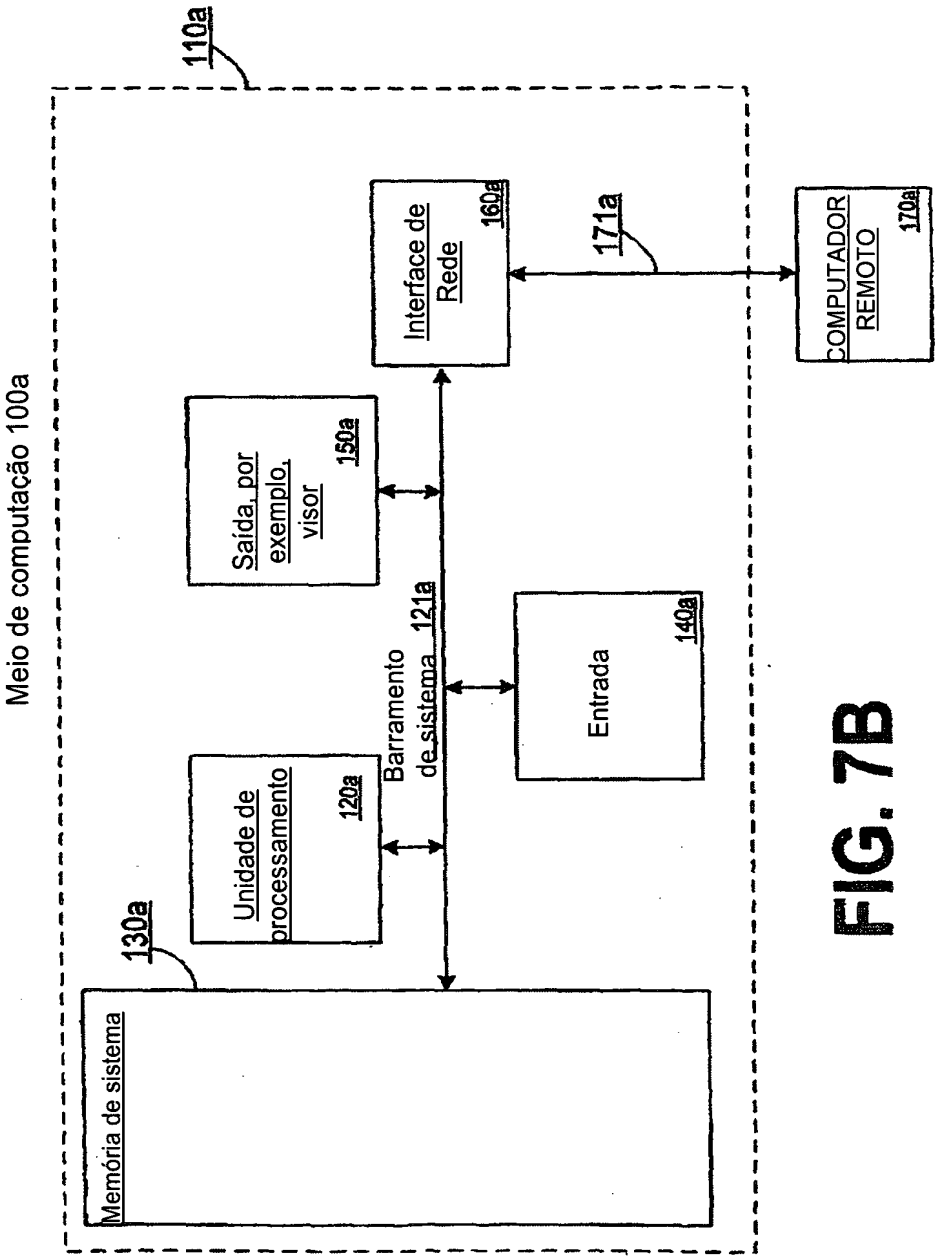

110a
Meio de computação 100a
Memória de sistema
130a
Unidade de processamento
120a
Barramento de sistema 121a
Saída, por exemplo, visor
150a
Entrada
140a
Interface de Rede
160a
171a
COMPUTADOR REMOTO
170a

FIG. 7B

PI-0711702-7

RESUMO

"DELEGAÇÃO DE CREDENCIAL DIRIGIDA POR POLÍTICA PARA ACESSO DE ASSINATURA ÚNICA E SEGURO A RECURSOS DE REDE"

Um provedor de suporte de segurança de credencial (Cred SSP) permite que qualquer aplicação delegue com segurança credenciais de usuários do cliente, por um software de Provedor de Suporte de Segurança (SSP) no lado do cliente, para um servidor alvo, pelo software SSP no lado do cliente. O Cred SSP proporciona uma solução segura que é baseada, em parte, em um conjunto de políticas. As políticas podem ser para qualquer tipo de credenciais de usuários, e políticas diferentes são elaboradas para atenuar uma ampla gama de ataques, de modo que a delegação adequada possa ocorrer para determinadas circunstâncias de delegação, condições de rede, níveis de confiança, etc. Adicionalmente, apenas um subsistema confiável, por exemplo, um subsistema confiável da Autoridade de Segurança Local (LSA), tem acesso às credenciais de texto de clientes, de modo que nem a aplicação de chamada das SSPI APIs, no lado do servidor, nem a aplicação de chamada das SSPI APIs, no lado do cliente, têm acesso às credenciais de texto claro.