(11) Número de Publicação: **PT 1751911 E**

(51) Classificação Internacional:
H04L 9/08 (2007.10)

(12) **FASCÍCULO DE PATENTE DE INVENÇÃO**

(22) Data de pedido: **2005.04.18**

(30) Prioridade(s): **2004.05.24 GB 0411560**

(43) Data de publicação do pedido: **2007.02.14**

(45) Data e BPI da concessão: **2009.06.24**
197/2009

(73) Titular(es):
GCYRPT LIMITED
ENTERPRISE HOUSE 21 BUCKLE STREET
LONDON E1 8NN **GB**

(72) Inventor(es):
MICHAEL ALCULUMBRE **GB**

(74) Mandatário:
MARIA MANUEL RAMOS LUCAS
LARGO DE S. DOMINGOS N° 1 2910-092 SETÚBAL **PT**

(54) Epígrafe: **MÉTODO DE CODIFICAÇÃO E TRANSFERÊNCIA DE DADOS ENTRE UM EMISSOR E UM RECEPTOR USANDO UMA REDE**

(57) Resumo:

Descrição

MÉTODO DE CODIFICAÇÃO E TRANSFERÊNCIA DE DADOS ENTRE UM EMISSOR E UM RECEPTOR USANDO UMA REDE

A presente invenção está relacionada com um método de codificação e transferência de dados entre um emissor e um receptor usando uma rede resultando assim numa transferência de dados de uma maneira segura.

Na actualidade, dados sensíveis são cada vez mais enviados de forma electrónica de um emissor para um receptor. Em tais circunstâncias, tem vindo a ser cada vez mais importante assegurar que os dados não possam ser interceptados ou lidos por pessoas não autorizadas, ou seja, os dados têm que ser transferidos de uma maneira segura de forma que só o emissor e o receptor possam ter acesso ao conteúdo da informação.

Num caso, pode ser estabelecida uma ligação segura entre um emissor A e um receptor B antes de acontecer a transferência de dados. No entanto, em situações onde digamos 10 pessoas individuais num escritório pretendem comunicar com e transferir dados sensíveis entre eles e para 10 pessoas num outro escritório remoto de uma maneira bidireccional, existe a desvantagem de que para organizar tantas ligações seguras é necessário hardware e software adicionais. Para além disto, estão envolvidos consideráveis recursos de hardware e de tempo para se manter tais ligações e os seus sistemas de palavra-chave associados.
Isto é especialmente verdade quando as pessoas em cada gabinete estão ligadas entre si por qualquer forma de Intranet ou Ethernet e que os gabinetes comuniquem através da Internet. É também necessário haver software complexo de

codificação e descodificação tanto no emissor como no receptor, o que requer sistemas adicionais de hardware e de software e os custos de manutenção especializada associados.

Num outro caso, um emissor individual pode querer transferir dados diferenciados para uma pluralidade de receptores individuais. No entanto, isto tem as mesmas desvantagens que aquelas acima mencionadas. Em especial, é necessário o emissor estabelecer provisões de segurança complexas para manter seguros os sistemas de palavra-chave. Para além disto, têm que ser configurados sistemas de hardware e de software adicionais para armazenar e manter tais sistemas.

Na realidade, numa época de dispositivos pequenos portáteis, tais como assistentes digitais pessoais, telemóveis com acesso à Internet e capacidade para correio electrónico, que têm capacidade limitada de memória e de processamento, não é muitas vezes tecnicamente praticável ter capacidade para ligações seguras bidireccionais onde estão envolvidos altos níveis de codificação e descodificação.

Ainda que possam ser usados certificados digitais para reduzir a chamada sobre recursos técnicos tanto para o servidor como para o receptor, estes envolvem um custo que pode muitas vezes não ser justificado para o receptor, mesmo quando este custo é pequeno.

Uma alternativa é a de um emissor codificar os dados a serem transferidos e depois enviar os dados codificados através de uma rede. No entanto, mais uma vez, o receptor tem que ter recursos de processamento de hardware

disponíveis conjuntamente com memória para que o software relevante seja capaz de descodificar os dados codificados. Para além disso, em situações onde o dispositivo do receptor tem recursos de hardware relativamente pobres, a ocupação de recursos valiosos para permitir a transferência segura de dados é muitas vezes impraticável.

O uso de técnicas de codificação e descodificação complexas requer a instalação de software especial no aparelho do emissor e no aparelho do receptor. Isto é tanto inconveniente como caro. Além disso, o procedimento de instalação pode ser complexo e demorado e pode causar conflitos com outro software nos seus respectivos aparelhos. Mais ainda, o software adicional pode exigir um nível energético de processamento que não esteja disponível no aparelho e que possa ocupar valioso espaço de memória; isto é especialmente verdade no caso dos dispositivos portáteis anteriormente referidos.

Fica claro pelo acima referido que métodos e sistemas conhecidos para a transferência de dados de maneira segura exigem bastantes recursos de regulação, assim como recursos importantes de processamento informático e de memória local. Isto claramente não é apropriado nas situações onde o emissor e/ou o receptor têm aparelhos com somente uma quantidade limitada dos recursos técnicos acima referidos.

Existe por isso a necessidade de um método e sistema para transferir dados de uma maneira segura que possa reduzir o nível de recursos técnicos exigidos pelos aparelhos do emissor e/ou do receptor. Também, no caso de ser usada codificação por chave pública/privada, o emissor tem que estar confiante que a chave pública que eles acreditam

pertencer ao receptor não foi substituída pela chave pública de um intrometido.

As características de um método conhecido de codificação e transferência de dados entre um emissor e um receptor usando uma rede estão definidas na parte de pré - caracterização da reivindicação1 e são conhecidas de US2003/0172262 que descreve um sistema de comunicação seguro para enviar dados de um dispositivo cliente para um recipiente através de um servidor de distribuição segura. O dispositivo cliente codifica os dados usando uma chave secreta e codifica a chave secreta usando uma chave pública associada com o servidor de distribuição segura. Os dados codificados e a chave secreta codificada juntamente com detalhes do recipiente são enviadas para o servidor de distribuição segura que descodifica a chave secreta. O servidor de distribuição segura codifica então a chave secreta descodificada com a chave pública do recipiente destinatário para produzir uma chave secreta segura específica do recipiente. Isto conjuntamente com os dados codificados é então enviado para o recipiente.

As características que caracterizam a presente invenção estão definidas na parte de caracterização da reivindicação 1.

De preferência, o método contém ainda o estabelecimento da ligação de comunicação entre o emissor e o servidor e o envio do dito identificador do receptor para o servidor.

Numa incorporação, o método compreende ainda o estabelecimento da ligação de comunicação entre o emissor e o servidor na forma de uma ligação segura.

Num caso, o método compreende ainda o estabelecimento da ligação de comunicação entre o emissor e o servidor sujeita a uma verificação pelo servidor de uma palavra-chave do emissor.

Numa outra incorporação, o método compreende ainda o estabelecimento da ligação de comunicação entre o receptor e o servidor e o envio do dito identificador do receptor para o servidor.

Num caso, o método compreende ainda o estabelecimento da ligação de comunicação entre o receptor e o servidor na forma de uma ligação segura.

Num caso particular, o método compreende ainda o estabelecimento da ligação de comunicação entre o receptor e o servidor sujeita a uma verificação pelo servidor de uma palavra-chave do receptor.

De preferência, o estabelecimento da transferência da chave de codificação específica tem lugar no emissor e a chave de codificação específica de transferência estabelecida é enviada ao servidor.

Num outro caso, a codificação dos dados usando a chave de codificação específica de transferência tem lugar no emissor.

Numa incorporação particular, o emissor recebe do servidor a chave de codificação específica de transferência e o emissor transfere os dados codificados e a chave de codificação específica de transferência para o receptor através da rede.

Numa outra incorporação, o receptor recebe do servidor a chave de codificação específica de transferência descodificada e a descodificação dos dados codificados usando a chave de codificação específica de transferência descodificada tem lugar no receptor.

E ainda numa outra incorporação, o estabelecimento da chave de codificação específica de transferência tem lugar no servidor.

Num caso particular, a codificação de dados usando a chave de codificação específica de transferência tem lugar no servidor.

Numa incorporação, o servidor transfere os dados codificados e a chave de codificação específica de transferência codificada para o receptor através da rede.

Numa outra incorporação, a descodificação dos dados codificados usando a chave de codificação específica de transferência descodificada tem lugar no servidor e o servidor transfere os dados descodificados para o receptor.

Por conveniência, o método compreende ainda:

o estabelecimento de um valor de código de autenticação de mensagem (MAC) para os dados antes da codificação;

a transferência do valor MAC conjuntamente com os dados codificados e a chave de codificação específica de transferência codificada; e

estabelecimento de um valor MAC para os dados depois de descodificação e a sua validação em comparação com o valor MAC transferido.

Numa incorporação, a codificação da chave de codificação específica de transferência usa um ou mais métodos de uma codificação de chave pública, um algoritmo 'blowfish', código secreto do servidor.

De acordo com outro aspecto da presente invenção é proporcionado um método de operar um servidor para codificação e transferência de informação entre um emissor e um receptor usando uma rede, compreendendo o método os passos de:

receber do emissor um identificador do receptor;

ter acesso a dados específicos do receptor de acordo com o identificador do receptor enviado pelo emissor e codificando, com os dados específicos do receptor, uma chave de codificação específica de transferência que é usada para codificar os dados;

caracterizada por

receber do receptor a chave de codificação específica de transferência e o identificador do receptor após os dados codificados e a chave de codificação específica de transferência terem sido transferidas através da rede para recebimento pelo receptor.

Numa incorporação, o método de operar um servidor compreende ainda estabelecer no servidor uma chave de codificação específica de transferência específica para a transferência

Numa outra incorporação, o método de operar um servidor compreende ainda receber do emissor uma chave de codificação específica de transferência específica para a transferência e transferir a chave de codificação específica de transferência codificada para o emissor.

De preferência, o método de operar um servidor compreende ainda a codificação dos dados no servidor usando a chave de codificação específica de transferência.

Numa outra incorporação preferida, o método de operar um servidor compreende ainda a transferência de dados codificados e da chave de codificação específica de transferência codificada através da rede para recebimento pelo receptor.

De preferência, o método de operar um servidor compreende ainda a transferência da chave de codificação específica de transferência descodificada para o receptor.

Numa outra incorporação, o método de operar um servidor compreende ainda a descodificação dos dados codificados no servidor usando a chave de codificação específica de transferência descodificada.

De acordo com um outro aspecto da presente invenção é proporcionado um meio computacional para um método de codificação e transferência de dados entre um emissor e um receptor usando uma rede, incluindo o meio:

código de computador para receber do emissor um identificador do receptor e estabelecer uma chave de codificação específica de transferência específica para a transferência;

código de computador para codificação dos dados usando a chave de codificação específica de transferência ;

código de computador para acesso a dados específicos do receptor de acordo com o identificador do receptor enviada pelo emissor e a codificação, com os dados específicos do receptor, da dita chave de codificação específica de transferência;

código de computador para transferência dos dados codificados e chave de codificação específica de transferência codificada através da rede para recebimento pelo receptor;

caracterizado por

código de computador para recebimento do receptor da chave de codificação específica de transferência codificada e do identificador do receptor e para acesso aos dados específicos do receptor segundo o identificador do receptor enviado pelo receptor para descodificação da chave de codificação específica de transferência específica; e código de computador para descodificação dos dados codificados usando a chave de codificação específica de transferência descodificada.

Um exemplo da presente invenção será agora descrito com referência aos desenhos juntos, em que:

A Figura 1 apresenta um diagrama esquemático de um sistema a operar um método da presente invenção codificar e transferir dados entre um emissor e um receptor usando uma rede;

A Figura 2 apresenta um diagrama de bloco esquemático dos módulos operacionais do servidor usado na figura 1;

A Figura 3 é um mapa de operação apresentando os processos envolvidos no emissor e para o servidor para a presente invenção enviar dados do emissor para o servidor;

A Figura 4 é um mapa de operação apresentado os processos envolvidos no receptor e no servidor em resposta a um correio electrónico recebido do servidor.

Com referência agora às figuras 1 e 2, estas mostram um sistema a operar uma incorporação de um método de codificação e transferência de dados entre um emissor e um receptor usando uma rede. Com referência aos desenhos, o sistema opera para codificar e transferir dados entre um aparelho emissor 100 e um aparelho receptor 200.

Neste exemplo, o aparelho emissor 100 é composto por um computador 101 ligado a um teclado 107, uma origem de dados 108 e um dispositivo mostrador externo 105. A origem de dados pode conter um leitor de disco de algum tipo ou uma ligação de interface com uma biblioteca de dados, a origem dos dados que armazena a informação a ser transferida para o receptor. O computador 101 tem um barramento de acesso geral 106 que liga a um microprocessador 102, uma memória 103, uma interface de mostrador 104, uma interface de dispositivo de entrada 109, e um browser da web 110 para ligação à Internet através de uma ligação 111.

A interface do mostrador 104 está ligada ao dispositivo mostrador externo 105 enquanto que a interface de dispositivo de entrada 109 está ligada ao teclado 107 e à origem de dados 108. A memória 103 tipicamente armazenará a Identidade do emissor e a palavra-chave do emissor ainda que estes possam entrar através do teclado 107 em resposta a solicitações no dispositivo mostrador 105.

Neste exemplo, o aparelho receptor 200 é composto por um telemóvel tendo capacidade para Internet através do browser da web 210 ligando à Internet através da ligação 211. Os detalhes de como tal ligação é estabelecida são bem conhecidos dos profissionais da especialidade e não serão aqui descritos. O browser é ligado a um barramento de acesso geral 206 que liga a um microprocessador 202, uma

memória 203, uma interface de mostrador 204 e uma interface de dispositivo de entrada 209. A interface de mostrador 204 está ligada a um dispositivo mostrador integral 205 enquanto que a interface de dispositivo de entrada 209 está ligada a um teclado integral 207. A memória 203 tipicamente armazenará a Identidade do receptor e a palavra-chave do receptor ainda que estes possam entrar através do teclado 207 em resposta a solicitações de écran no dispositivo mostrador 205. O aparelho 200 inclui ainda um cliente de correio electrónico 212 para enviar e receber correio electrónico através da ligação 213 à Internet.

Um servidor 300 está também ligado à Internet através de uma ligação 302. Na figura 2 está apresentado um diagrama de bloco detalhado da estrutura do servidor. Esta estrutura do servidor será explicada em combinação com uma descrição da operação do sistema da presente invenção.

Com referência às figuras 1 e 2, antes do uso do presente sistema, tanto o emissor como o receptor estão inicialmente registados com o servidor 300 e os seus detalhes estão armazenados num módulo de base de dados do servidor 306. Nesta incorporação, a informação armazenada inclui pelo menos uma Identidade e palavra-chave, para cada emissor e receptor.

O emissor deseja transferir dados contidos na origem de dados 108 para o receptor. Para que o emissor transfira os dados, o emissor necessita de conhecer a Identidade do receptor e o endereço web do servidor 300. Esta informação pode estar armazenada na memória 103 do emissor ou pode entrar manualmente através do teclado 107 em resposta a solicitações no dispositivo mostrador 105.

Como se mostra na figura 2, o servidor 300 inclui um servidor web 301 ligado à Internet através da ligação 302. O servidor web está ligado a um barramento de entrada 303 e é controlado por um microprocessador 304. Quando o emissor contacta o endereço web do servidor, é estabelecida uma ligação segura como por exemplo um SSL, cujos detalhes são bem conhecidos pelos profissionais desta especialidade. O microprocessador 304 não permite o acesso do emissor ao presente sistema até ser completada uma verificação de palavra-chave pelo módulo 305 em conjunto com acesso ao módulo da base de dados 306. Os detalhes de tais verificações de palavra-chave são bem conhecidos dos profissionais da especialidade e por isso não são aqui descritos.

Após a terminação da verificação de palavra-chave, é enviado ao emissor pelo servidor 300 um écran de apresentação. Ao completar esse écran, o emissor envia ao servidor a Identidade do receptor conjuntamente com os dados a serem transferidos, que são obtidos da origem de dados 108. Estas entradas são obedecidas pelos módulos em direcção ao limite superior da figura.

No recebimento da Identidade do receptor e dos dados a serem enviados, o microprocessador do servidor 304 reencaminha os dados para um módulo gerador de código de autenticação de mensagem (MAC) 307. Como é conhecido nesta especialidade, um tal gerador produz um item de código que é computorizada usando-se uma parte ou o todo dos dados em combinação com um algoritmo digest criptográfico. No caso presente, o conhecido algoritmo hash é usado para gerar um valor hash MD a partir dos dados. O valor hash MD é reencaminhado para um cliente de correio electrónico 312 ligado à Internet através de uma ligação 316 de forma a

estar pronto para processar formando uma parte de um correio electrónico.

Os dados recebidos são comprimidos no módulo 308 antes de serem codificados pelo módulo 309 usando uma chave de sessão obtida do módulo 310. Como é conhecido na especialidade, a chave de sessão é gerada de um número aleatório, proporcionado por um gerador de número aleatório 311. Esta chave de sessão é específica para estes dados e da transferência desses, por isso torna-se uma chave de codificação específica da transferência. Os dados codificados são consequentemente encaminhados para o cliente de correio electrónico 312 pronta para processamento formando parte de um correio electrónico.

A chave de sessão do módulo 310 é também codificada no módulo 313 usando-se a chave pública de uma técnica de codificação de chave pública/chave privada, por exemplo codificação RSA que é bem conhecida nesta especialidade. Por conseguinte, a saída do módulo 313 é ainda codificada no módulo 314 usando um algoritmo blowfish que incorpora a palavra-chave do receptor que é obtida da base de dados 306. Esta palavra-chave sai de acordo com a Identidade do receptor reencaminhado desde o microprocessador no barramento 315. A chave de sessão codificada é reenviada para o cliente de correio electrónico 312 pronta para processamento formando parte de um correio electrónico.

O cliente de correio electrónico 312 processa o valor hash MD, os dados codificados e a chave de sessão codificada na maneira conhecida para construir um correio electrónico que é depois enviado para o endereço apropriado do receptor fornecido pelo microprocessador no barramento 315 no seguimento do acesso à base de dados 306. Da maneira

conhecida, o cliente de correio electrónico atribui um rótulo único ao correio electrónico e regista o envio de este. Uma confirmação do envio do correio electrónico é também enviado para o emissor usando-se o servidor web 301 ou o cliente de correio electrónico 312.

O correio electrónico que é enviado pelo servidor 300 pode ser recebido da maneira típica pelo cliente de correio electrónico 212 do telemóvel 200. O conteúdo do correio electrónico é configurado ou para alertar o receptor para uma transferência de dados usando o sistema da presente invenção ou para automaticamente activar o web browser 210 para iniciar uma ligação de comunicação para o servidor 300. Em qualquer caso, sob controlo do microprocessador 202, o receptor contacta o endereço web do servidor e é estabelecida uma ligação segura tal como uma ligação SSL, cujos detalhes são bem conhecidos dos profissionais da especialidade. O microprocessador do servidor 304 não permite o acesso ao presente sistema até ter sido completada uma verificação de palavra-chave pelo módulo 305 em conjunção com acesso ao módulo de base de dados 306. Os detalhes de tais verificações de palavras-chave são bem conhecidos da especialidade e por isso não são aqui descritos.

Só depois da terminação da verificação bem sucedida de palavra-chave são enviados, os dados codificados, a chave de sessão codificada e o valor hash MD contidos no correio electrónico na ligação segura para o servidor 300 através do servidor web 301. Estes são obedecidos pelos módulos na direcção do limite mais baixo da figura.

Será evidente que se o método escolhido de envio e leitura de correio electrónico for por correio web então não é necessário o cliente de correio electrónico separado 213.

Na recepção deste, o microprocessador do servidor 304 reenvia a chave de sessão codificada para um módulo 320 que aplica um algoritmo blowfish invertido em combinação com a palavra-chave do receptor que é obtido da base de dados 306 no barramento 315 de acordo com a Identidade do receptor. A saída do módulo 320 é então novamente descodificada no módulo 321 usando-se a chave privada da codificação RSA usada para enviar os dados. Por virtude destes módulos, a chave de sessão original do módulo 310 é reproduzida.

Os dados codificados recebidos que estão em forma comprimida são descodificados no módulo 323 usando-se a chave de sessão descodificada antes de ser descomprimida no módulo 324.

Como com o módulo 307, um valor hash MD é gerado no módulo 325 dos dados descodificados e descomprimidos e sob controlo do microprocessador 304, o módulo 326 conduz uma verificação de comparação para validar o valor hash MD recentemente gerado em comparação com o valor hash MD recebido do receptor para assegurar que eles condizem.

Assumindo que o valor hash MD é correctamente validado no módulo 326, os dados descodificados do módulo 324 são enviados de volta ao receptor através da ligação segura.

A Figura 3 é um mapa de operação apresentando os processos envolvidos no emissor e no servidor para a presente invenção enviar dados do emissor para o servidor.

Inicialmente, o emissor deseja transferir dados específicos para um receptor específico que tem uma Identidade de receptor conhecida. No passo S1A, o emissor estabelece contacto com o servidor numa tentativa de estabelecer uma ligação de comunicação segura, por exemplo, uma ligação SSL. O estabelecimento desta ligação envolve a passagem por certos protocolos de ligação e a verificação de palavra-chave acima mencionada e pode ter a forma de uma apresentação de página web no dispositivo mostrador 105, a entrada de dados de início de sessão numa página web e assim por diante. Como anteriormente mencionado, o estabelecimento de uma tal ligação de comunicação e a verificação de palavra-chave são bem conhecidos dos profissionais da especialidade e não são aqui descritos em detalhe.

O servidor, em resposta ao contacto do emissor, tenta também no passo S1B estabelecer a ligação de comunicação passando por certos protocolos de ligação e a verificação de palavra-chave acima mencionada. O servidor verificará então no passo S2B se foi estabelecida uma ligação válida, ou seja, que foram cumpridos todos os protocolos de comunicação e que foram aceites todas as verificações de palavras-chave. Se a ligação não foi estabelecida, ou se falhou a verificação de palavra-chave, o servidor vai para o passo S3B de processamento de erro. Tal passo pode envolver mais tentativas para estabelecer uma ligação de comunicação. Assumindo que é estabelecida uma ligação de comunicação válida, o processo passa para o passo S4B para esperar pela recepção da Identidade do receptor e dos dados a serem transferidos. Se necessário, neste ponto pode ser incluído um passo de tempo de espera excedido.

No emissor, é feita uma verificação no passo S2A para também determinar se foi estabelecida uma ligação válida, ou seja que foram cumpridos todos os protocolos de comunicação e que foram aceites todas as verificações de palavras-chave. Se a ligação não foi estabelecida, ou se falhou a verificação de palavra-chave, o servidor vai para o passo S3A de processamento de erro. Tal passo pode envolver mais tentativas de estabelecer uma ligação de comunicação. Assumindo que é estabelecida uma ligação de comunicação válida, o processo passa para o passo S4A para enviar a Identidade do receptor e os dados a serem transferidos. Se necessário, neste ponto pode ser incluído um passo de tempo de espera excedido.

Num exemplo, é apresentada uma página web de transferência de dados no dispositivo mostrador 105 que requer a entrada da Identidade do receptor e um anexo dos dados, por exemplo um ficheiro localizado na origem de dados 108. A página de transferência de dados completada é então enviada para o servidor 300. Será notório que os dados a serem codificados podem entrar directamente na página de transferência de dados.

O conteúdo da página de transferência de dados é recebido pelo servidor 300 no passo S4B depois do qual o processo segue para o passo S5B. Neste passo, o servidor produz um valor hash MD único para os dados e reenvia o valor para o cliente de correio electrónico 312, depois do qual o processo segue para o passo S6B.

No passo S6B, os dados são comprimidos, por exemplo por zipagem. Então, no passo S7B é obtido do gerador de números aleatórios 311 um número aleatório para gerar a chave de sessão que é específica para essa transferência de dados.

Depois disso no passo S8B, os dados são codificados com esta chave de sessão e os dados codificados são reenviados para o cliente de correio electrónico 312.

O processo passa então para o passo S9B no qual é codificada a chave de sessão usando-se uma chave pública RSA. Depois disto, o processo passa para o passo S10B para obter a palavra-chave do receptor após o que, no passo S11B, o resultado do passo S9B é codificado com um algoritmo blowfish usando a palavra-chave obtida no passo S10B. A chave de sessão codificada resultante é então reenviada para o cliente de correio electrónico 312.

No passo seguinte S12B, é formulado um correio electrónico na maneira conhecida pelo cliente de correio electrónico 312 para um formato apropriado para transferência por HTML, por exemplo por codificação de base 64. Isto pode ter também um ficheiro anexo HTML, ou código HTML "in line" para os dados codificados e chave de sessão codificada. O correio electrónico é então enviado e o envio do correio electrónico é registado da maneira habitual e enviada confirmação ao emissor, após o que o processo termina.

Será evidente que o correio electrónico contém o valor hash MD, os dados codificados e a chave de sessão codificada, de preferência como ficheiros ocultos. O correio electrónico também inclui de preferência uma ligação HTML para permitir ao receptor contactar de volta o servidor. Esta ligação é configurada para automaticamente submeter os ficheiros ocultos na forma HTML novamente ao servidor. O cabeçalho de assunto do correio electrónico é o cabeçalho de assunto escolhido pelo emissor e o correio electrónico é endereçado para o endereço electrónico do receptor.

No passo S5A o emissor recebe confirmação do envio do correio electrónico e o processo termina.

A Figura 4 é um mapa de operação apresentando os processos envolvidos no receptor e no servidor em resposta a um correio electrónico recebido do servidor.

No passo S101A, o receptor 200 recebe o correio electrónico do servidor que contém, entre outras coisas, os dados codificados, a chave de sessão codificada, e o valor hash MD. O correio electrónico pode ser descarregado usando correio web ou usando o cliente de correio electrónico 212 através da ligação 213. No passo S102A, o receptor abra o correio electrónico e estabelece contacto com o servidor numa tentativa de estabelecer uma ligação de comunicação segura, por exemplo, uma ligação SSL. De maneira semelhante à acima descrita, o estabelecimento desta ligação envolve a passagem por certos protocolos de ligação e uma verificação de palavra-chave semelhante à acima ventilada em relação ao módulo 305 e pode ter a forma de uma apresentação de uma página web no dispositivo mostrador 105, a entrada de dados apropriados de início de sessão na página web e assim por diante. Como mencionando anteriormente, o estabelecimento de uma tal ligação de comunicação e a verificação de palavra-chave são bem conhecidos dos profissionais da especialidade e não serão aqui descritos em detalhe.

O servidor, em resposta ao contacto do receptor, tenta também no passo S101B estabelecer a ligação de comunicação passando por certos protocolos de ligação e pela verificação de palavra-chave acima mencionada. O servidor verifica então no passo S102B se foi estabelecida uma ligação válida, ou seja que todos os protocolos de comunicação foram cumpridos e que todas as verificações de

palavras-chave foram aceites. Se a ligação não foi estabelecida, ou se falhou a verificação de palavra -chave, o servidor vai para o passo S103B de processamento de erro. Tal passo pode envolver mais tentativas de estabelecer uma ligação de comunicação. Assumindo que está estabelecida uma ligação de comunicação válida, o processo segue para o passo S104B para esperar pela recepção da Identidade do receptor e outra informação incluindo os dados codificados, a chave de sessão codificada e o valor hash MD. Se for necessário, neste ponto pode ser incluído um passo de tempo de espera excedido.

No receptor, é feita uma verificação no passo S103A para também ver se foi estabelecida uma ligação válida, ou seja que todos os protocolos de comunicação foram cumpridos e que todas as verificações de palavra-chave foram aceites. Se não foi estabelecida a ligação, ou se falharam as verificações de palavra-chave, o emissor vai para o passo S104A de processamento de erro. Tal passo pode envolver mais tentativas de estabelecer uma ligação de comunicação. Se for necessário, neste ponto pode ser incluído um passo de tempo de espera excedido.

Assumindo que está estabelecida uma ligação de comunicação válida, o processo segue para o passo S105A para enviar a Identidade do receptor e a outra informação mencionada no parágrafo anterior. A segunda pode ser na forma de campos HTML ocultos no correio electrónico que são submetidos ao servidor 300. Será evidente que o protocolo para a temporização e arranjos para envio dos campos ocultos, Identidade, palavras-chave etc., podem ser alterados para servirem situações específicas.

O processo no servidor segue então para o passo S105B para obter do módulo 306 a palavra-chave do receptor depois do que, no passo S106B, a chave de sessão codificada é descodificada com o algoritmo blowfish usando-se a palavra-chave obtida no passo S105B. O processo segue então para um passo de descodificação RSA S107B no qual o resultado do passo S106B é descodificado usando-se a chave privada do servidor. Isto resulta em ser produzida a chave de sessão.

Depois disto, o processo segue para o passo S108B em que os dados que continuam comprimidos são descodificados usando-se a chave de sessão descodificada produzida do passo S107B. Depois disto, o processo segue para o passo S109B para descomprimir os dados.

No passo seguinte, S110B, o servidor produz um valor hash MD único para os dados do passo S109B. Depois, no passo S111B, o valor hash MD do passo S110B é verificado em comparação com o valor hash MD recebido no passo S104B. Assumindo que o valor hash é validado, o processo segue para o passo S113B e agora os dados não codificados do emissor são enviados para o receptor através de uma linha segura. O envio destes dados é registado e o processo termina. Se o valor hash MD não poder ser validado, o processo vai para S122B processamento de erro. Isto pode envolver o registo do erro e o envio de uma mensagem ao receptor para indicar que os dados podem ter sido corrompidos ou comprometidos.

No passo S106A o receptor recebe os dados não codificados e o processo termina.

Na incorporação da invenção acima descrita, o processo completo de codificação e descodificação é efectuado no

servidor 300. Assim, o emissor e o receptor não necessitam de qualquer software especial para serem capazes de enviar e receber dados com segurança. Em especial, não é necessário ter o software, ou usar a memória e recursos de processamento do hardware para permitir codificação RSA e codificação blowfish. Para além disto, o acesso a palavras-chave é mantido no servidor e não necessita de ser mantido no emissor. E mais ainda, uma vez que a codificação e descodificação têm lugar no servidor, não são necessários arranjos especiais para codificação e descodificação pelo emissor ou pelo receptor.

No entanto, a presente invenção também abrange a alternativa das funções dentro da caixa 317 da figura 2 serem proporcionadas no emissor. Isto quer dizer que, nesta modificação, a geração de uma chave de sessão de um gerador de números aleatórios e a compressão de dados e a codificação de dados comprimidos com essa chave de sessão são todos conduzidos no emissor. No entanto, é estabelecida uma ligação segura com o servidor como acima, mas neste caso só a chave de sessão gerada é enviada ao servidor. Depois da mesma verificação de palavra-chave como acima, os módulos S313 e S314 geram novamente uma chave de sessão codificada que neste caso é devolvida ao emissor. Os dados codificados, a chave de sessão codificada e o valor hash são então fornecidos a um cliente de correio electrónico emissor (não se mostra) que está também ligado à Internet. Este cliente de correio electrónico constrói um correio electrónico como acima indicado antes de o enviar ao receptor. Pode pois ser visto que os passos S5B a S8B na figura 3 têm agora lugar no emissor. Isto pode reduzir as chamadas de processamento colocadas no servidor.

O receptor recebe o correio electrónico no seu cliente de correio electrónico e pode processar o correio electrónico como na figura 4.

No entanto, a presente invenção também abrange a alternativa das funções dentro da caixa 322 da figura 2 serem proporcionadas no receptor uma vez recebido um correio electrónico do servidor. Isto quer dizer, nesta modificação, a descodificação de dados, a descompressão de dados, a geração de valor hash MD e a validação deste é tudo conduzido no receptor. No entanto é estabelecida uma ligação segura com o servidor como acima, mas neste caso só a chave de sessão codificada é enviada ao servidor. Após a mesma verificação de palavra-chave como acima, os módulos S320 e S321 outra vez descodificam a chave de sessão que neste caso é devolvido ao receptor. Os dados codificados são descodificados usando a chave de sessão descodificada, descomprimidos, um valor hash MD gerado e verificado para validade em comparação com o valor hash MD recebido no correio electrónico. Pode pois ser visto que os passos S108B a S113B na figura 4 têm agora lugar no receptor. Isto pode reduzir a chamada de processamento colocada no servidor.

Será apreciado que ambas as modificações acima mencionadas podem ser implementadas ao mesmo tempo. No entanto, com a presente invenção, a codificação da chave de sessão, em combinação com a palavra-chave do receptor, tem lugar no servidor.

Será apreciado que um grupo de utilizadores pode ser registado para receber correio electrónico quando necessário. Por exemplo, o departamento de Informática de uma firma pode registar todos os empregados. Neste caso,

pode ser consultada referência a outras palavras-chave nesse grupo, na eventualidade de falhar a verificação de palavra-chave no servidor.

Em incorporações da invenção que requeiram software especial instalado para o emissor ou para o receptor, como é sabido pelos profissionais da especialidade, este pode ser descarregado do servidor durante o processo de registo e depois instalado.

Será apreciado que uma vez que seja necessária uma palavra-chave correcta para descodificar os dados no algoritmo blowfish e a descodificação correcta é efectivamente verificada por validação do valor hash MD, a verificação de palavra-chave durante a ligação entre o receptor e o servidor no passo 102A pode se necessário ser dispensado.

Será também apreciado que se a descodificação não for bem sucedida, o servidor 300 pode ser arranjado para efectuar mais verificações para tentar obter a palavra-chave correcta, por exemplo, procurando palavras-chave antigas do receptor e tentar cada uma delas à vez para descodificar os dados. Se uma dessas palavras-chave produz o valor hash MD correcto então a descodificação foi bem sucedida. No entanto se nenhuma dessas palavras-chave funciona, então o receptor não é o receptor que se procura ou os dados foram corrompidos durante a transferência.

Se o receptor não tem uma palavra-chave e não está já registado no servidor 300, o servidor pode gerar uma palavra-chave de uso único que ele envia para o receptor por quaisquer meios seguros que sejam apropriados, por exemplo, por correio seguro ou por uma ligação segura ou por correio electrónico seguro, requerendo ao utilizador

que mude a sua palavra-chave para uma palavra-chave segura para ser usada dai em diante.

Com a presente invenção, as identidades tanto do emissor como do receptor podem ser verificadas de maneira que o emissor possa enviar dados para um receptor que não tenha software especial instalado de maneira que o receptor esteja confiante da origem dos dados. Para além disto, as tentativas de codificação e descodificação são registados, o que pode permitir a um emissor verificar se um receptor recebeu e descodificou os dados e pode permitir a um receptor verificar se os dados que esperava receber já foram despachados.

Os aparelhos do emissor e do receptor podem ter muitas formas, uma lista não exclusiva compreendendo por exemplo, um computador, um assistente digital pessoal ou outro dispositivo portátil, um computador portátil, um telemóvel. O servidor é de preferência um computador, ainda que possa ser também um tipo alternativo de dispositivo informático.

Será observado que com a presente invenção, nem o emissor nem o receptor são conhecedores da palavra-chave um do outro, sendo estes mantidos no servidor. Por consequência, o nível de segurança exigido pelo emissor e receptor não é tão elevado como em outras formas de transferência de dados de uma maneira segura.

Com a presente invenção, o servidor mantém a informação específica do receptor, tal como uma palavra-chave, que é usada pelo servidor num processo de codificação. O servidor obtém essa informação de um armazém de dados, que tem uma lista de Identidades de receptor e a informação específica de receptor que é mantida secreta. A informação específica

de receptor pode conter uma palavra-chave, uma frase senha, um número PIN, um valor hash ou qualquer outra informação a ser usada para verificação de identidade.

A rede usada com a presente invenção pode ser a Internet, uma Intranet local tal como uma rede Ethernet, uma rede telefónica, uma rede rádio, ou qualquer outro tipo de rede para transferência de dados. De preferência, quando é usada a Internet, é usada uma ligação SSL segura entre o servidor e o emissor e/ou entre o servidor e o receptor.

O emissor e o receptor podem ser identificados ao servidor pelos seus endereços de correio electrónico (ou outros endereços de rede). No entanto, eles podem também ter Identidades de utilizador que não estão relacionadas com os seus endereços de rede. O servidor pode ter uma lista de endereços de rede na sua base de dados, e/ou pode ter uma lista de Identidades de utilizador, onde o endereço de rede e/ou Identidades de utilizador estão cada uma associada com informação específica de receptor secreta.

Numa incorporação da presente invenção, o servidor 300 pode incluir um código secreto único para o servidor e só conhecido do servidor. Esse código secreto pode ser incluído nos módulos de codificação e descodificação blowfish. O código secreto pode ser usado codificação em adição ao uso de informação específica de receptor. Estas duas peças de informação podem simplesmente ser encadeadas para serem usadas no processo de codificação. O uso do código secreto proporciona ao sistema um nível de segurança mais elevado.

Será apreciado que o servidor não necessita de reter a chave de sessão ou qualquer dos dados a serem enviados para

o receptor. Estes podem ser armazenados numa memória volátil no servidor e substituídos quando são codificados novos dados e chaves. Isto tem a vantagem que o servidor não necessita de ter uma grande quantidade de memória disponível para armazenagem de dados e/ou chaves antigas possivelmente redundantes.

O meio de transporte pode compreender um meio transiente, por exemplo, um sinal eléctrico, óptico, micro-onda, rádio frequência electromagnético, acústico ou magnético (por exemplo um sinal TCP IP através de uma rede IP tal como a Internet), ou um meio de transporte tal como uma disquete, CD ROM, disco duro, ou dispositivo de memória programável.
[00102] Ainda que a invenção tenha sido descrita em termos do que são no presente as suas incorporações preferidas, será evidente para os que são especializados na matéria que podem ser feitas várias alterações às incorporações preferidas sem se sair do âmbito da invenção, que é definida pelas reivindicações. A presente invenção pode encontrar aplicação, por exemplo, com fornecedores de telemóveis que podem distribuir balanços de contas mensais numa base segura, o utilizador do telemóvel, ligando o utilizador para o servidor para obter um balanço de conta codificado. De maneira semelhante, os bancos podem distribuir detalhes de pagamentos a entrar para os seus clientes que podem simplesmente ligar para o servidor como acima descrito para obterem tais detalhes, com os detalhes a serem distribuídos de uma maneira segura.

Lisboa, 16 de Setembro de 2009

REIVINDICAÇÕES

1. Um método de codificar e transferir dados entre um emissor (100) e o receptor (200) usando uma rede, compreendendo o método os passos de;

um servidor (300) receber do emissor (100) um identificador do receptor;

estabelecer uma chave de codificação específica de transferência (310) específica para a transferência;

codificar os dados usando a chave de codificação específica de transferência (309);

o servidor (300) ter acesso a informação específica de receptor (306) de acordo com o identificador do receptor enviado pelo emissor e codificar (314), com a informação específica de receptor, dita chave de codificação específica de transferência;

transferindo os dados codificados e a chave de codificação específica de transferência através da rede para recepção pelo receptor (200);

caracterizada pelo

servidor receber do receptor a chave de codificação específica de transferência e o identificador de receptor; e o servidor ter acesso a informação específica do receptor (306) de acordo com o identificador do receptor enviado pelo receptor para descodificação da chave de codificação específica de transferência (320) e

descodificar os dados codificados usando a chave de codificação específica de transferência (323).

2. Um método de acordo com a reivindicação 1 compreendendo ainda estabelecer uma ligação de comunicação (111, 302) entre o emissor e o servidor e enviar o dito identificador do receptor ao servidor.

3. Um método de acordo com a reivindicação 2 compreendendo ainda o estabelecimento de uma ligação de comunicação entre o emissor e o servidor como uma ligação segura.

4. Um método de acordo com a reivindicação 2 ou 3 compreendendo ainda estabelecer uma ligação de comunicação entre o emissor e servidor sujeita a uma verificação pelo servidor de uma palavra-chave do emissor (305).

5. Um método de acordo com qualquer reivindicação anterior compreendendo ainda o estabelecimento de uma ligação de comunicação (211, 302) entre o receptor e o servidor e o envio do dito identificador do receptor ao servidor.

6. Um método de acordo com a reivindicação 5 compreendendo ainda o estabelecimento de uma ligação de comunicação entre o receptor e o servidor como uma ligação segura.

7. Um método de acordo com a reivindicação 5 ou 6 compreendendo ainda o estabelecimento de uma ligação de comunicação entre o receptor e servidor sujeita a uma verificação pelo servidor de uma palavra-chave do receptor (305).

8. Um método de acordo com qualquer reivindicação anterior onde tem lugar o estabelecimento de uma chave de codificação específica de transferência no emissor e a chave de codificação específica de transferência estabelecida é enviada ao servidor.

9. Um método de acordo com qualquer reivindicação anterior onde a codificação de dados tem lugar no emissor usando a chave de codificação específica de transferência.

10. Um método de acordo com a reivindicação 9 onde o emissor recebe do servidor a chave de codificação específica de transferência codificada e o emissor transfere os dados codificados e a chave de codificação específica de transferência codificada para o receptor através da rede.

11. Um método de acordo com qualquer uma das reivindicações 1 a 7 onde o receptor recebe do servidor a chave de codificação específica de transferência descodificada e a descodificação dos dados codificados tem lugar no receptor usando a chave de codificação específica de transferência descodificada.

12. Um método de acordo com qualquer uma das reivindicações 1 a 7 onde o estabelecimento da chave de codificação específica de transferência tem lugar no servidor.

13. Um método de acordo com a reivindicação 12 onde a codificação de dados usando a chave de codificação específica de transferência tem lugar no servidor.

14. Um método de acordo com a reivindicação 13 onde o servidor transfere os dados codificados e a chave de codificação específica de transferência codificada para o receptor através da rede.

15. Um método de acordo com qualquer uma das reivindicações 1 a 10 e 12 a 14 onde a descodificação dos

dados codificados usando a chave de codificação específica de transferência descodificada tem lugar no servidor e o servidor transfere os dados descodificados para o receptor.

16. Um método de acordo com qualquer uma das reivindicações anteriores compreendendo ainda:

o estabelecimento de um valor de código de autenticação de mensagem (MAC) (307) para dados antes da codificação;

a transferência do valor MAC juntamente com dados codificados e a chave de codificação específica de transferência codificada; e

o estabelecimento de um valor MAC (325) para os dados após descodificação e a sua validação (326) em comparação com o valor MAC transferido.

17. Um método de acordo com qualquer uma das reivindicações anteriores onde a codificação da chave de codificação específica de transferência usa um ou mais de um método de codificação de chave pública, um algoritmo blowfish e código secreto do servidor.

18. Um método de operar um servidor (300) para codificação e transferência de dados entre um servidor (100) e um receptor (200) usando uma rede, compreendendo o método os passos de:

receber do emissor (100) uma identificador do receptor;

ter acesso a informação específica do receptor (306) de acordo com o identificador do receptor enviado pelo emissor e codificar (314), com a informação específica do receptor, uma chave de codificação específica de transferência que é usada para codificar os dados;

caracterizada por

receber do receptor (200) a chave de codificação específica de transferência codificada e o identificador do receptor após os dados codificados e a chave de codificação específica de transferência terem sido transferidos através da rede para recepção pelo receptor;

ter acesso à informação específica do receptor (306) de acordo com o identificador do receptor enviada pelo receptor para descodificação da chave de codificação específica de transferência codificada.

19. Um método de operar um servidor de acordo com a reivindicação 18 compreendendo ainda o estabelecimento no servidor (310) de uma chave de codificação específica de transferência específica para a transferência.

20. Um método de operar um servidor de acordo com a reivindicação 18 compreendendo ainda receber do emissor uma chave de codificação específica de transferência específica para a transferência;
e transferir a chave de codificação específica de transferência codificada para o emissor.

21. Um método de operar um servidor de acordo com uma das reivindicações 18 a 20 compreendendo ainda codificação dos dados no servidor (309) usando a chave de codificação específica de transferência.

22. Um método de operar um servidor de acordo com qualquer uma das reivindicações 18 a 21 compreendendo ainda a transferência de dados codificados e a chave de codificação específica de transferência codificada através da rede para recepção pelo receptor.

23. Um método de operar um servidor de acordo com qualquer uma das reivindicações 18 a 22 compreendendo ainda transferência da chave de codificação específica de transferência descodificada para o receptor.

24. Um método de operar um servidor de acordo com qualquer uma das reivindicações 18 a 22 compreendendo ainda descodificação dos dados codificados no servidor (323) usando a chave de codificação específica de transferência descodificada.

25. Um meio computacional para um método de codificação e transferência de dados entre um emissor (100) e um receptor (200) usando uma rede, incluindo o meio:

código de computador para receber do emissor um identificador do receptor e estabelecer a chave de codificação específica de transferência (S7B) específica para a transferência;

código de computador para codificação dos dados usando a chave de codificação específica de transferência (S8B);

código de computador para ter acesso à informação específica do receptor (S10B) de acordo com o identificador do receptor enviado pelo emissor e codificar (S11B), com a informação específica do receptor, dita chave de codificação específica de transferência;

código de computador para transferência dos dados codificados e da chave de codificação específica de transferência codificada através da rede (S12B) para recepção pelo receptor;

caracterizada por

código de computador para receber do receptor (S101B) a chave de codificação específica de transferência

codificada e o identificador do receptor e para ter acessoà informação específica do receptor (S105B) de acordo com o identificador do receptor enviado pelo receptor para descodificação da chave de codificação específica de transferência codificada (S106B); e

código de computador para descodificação dos dados codificados (S108B) usando a chave de codificação específica de transferência descodificada.

Lisboa, 16 de Setembro de 2009

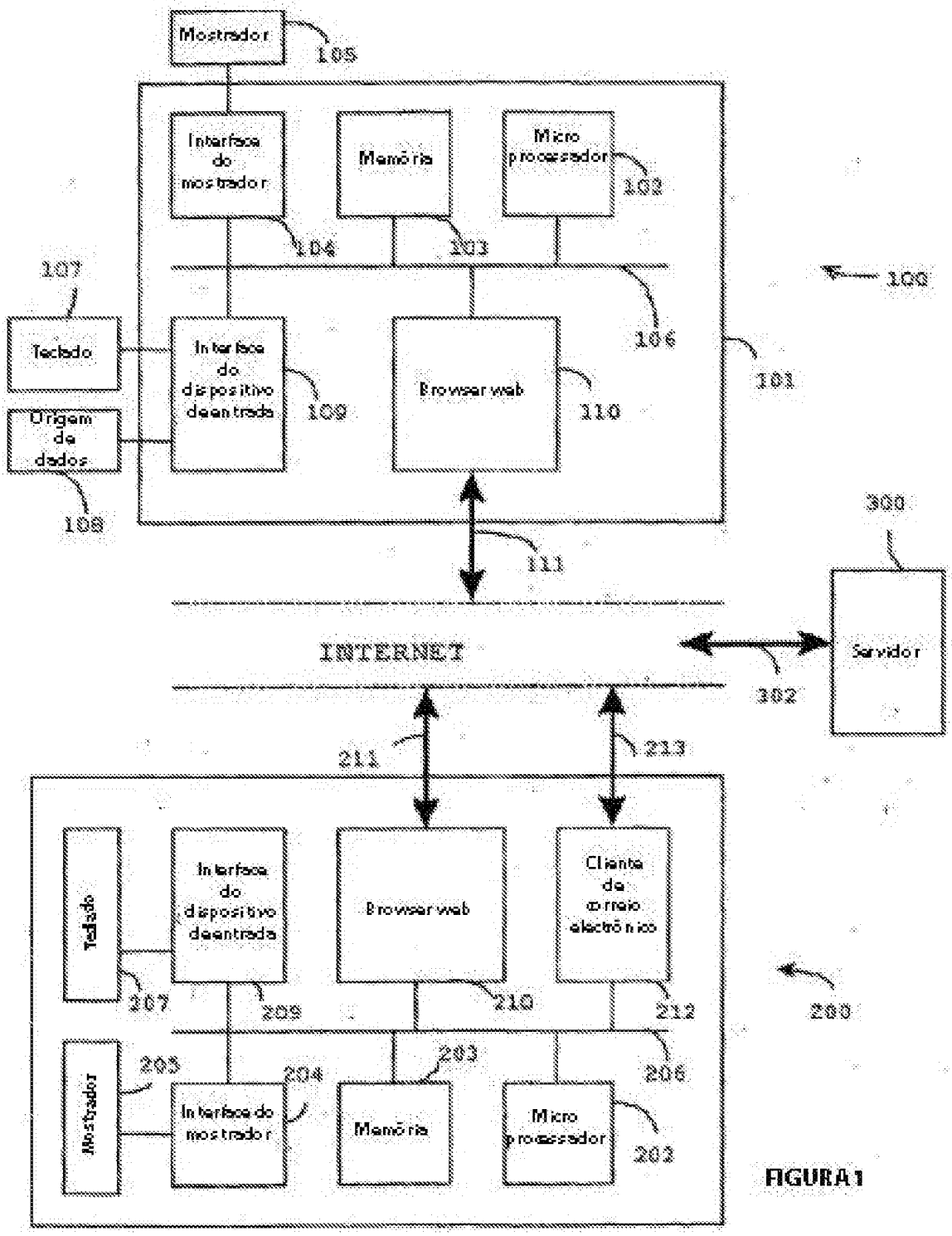
Mostrador
105
Interface do mostrador
Memória
Micro processador
102
104
103
107
100
Teclado
Interface do dispositivo de entrada
Browser web
106
101
Origem de dados
109
110
108
111
300
INTERNET
Servidor
302
211
213
Teclado
Interface do dispositivo de entrada
Browser web
Cliente de correio electrónico
207
209
210
212
200
Mostrador
203
204
206
Interface do mostrador
Memória
Micro processador
202

FIGURA 1

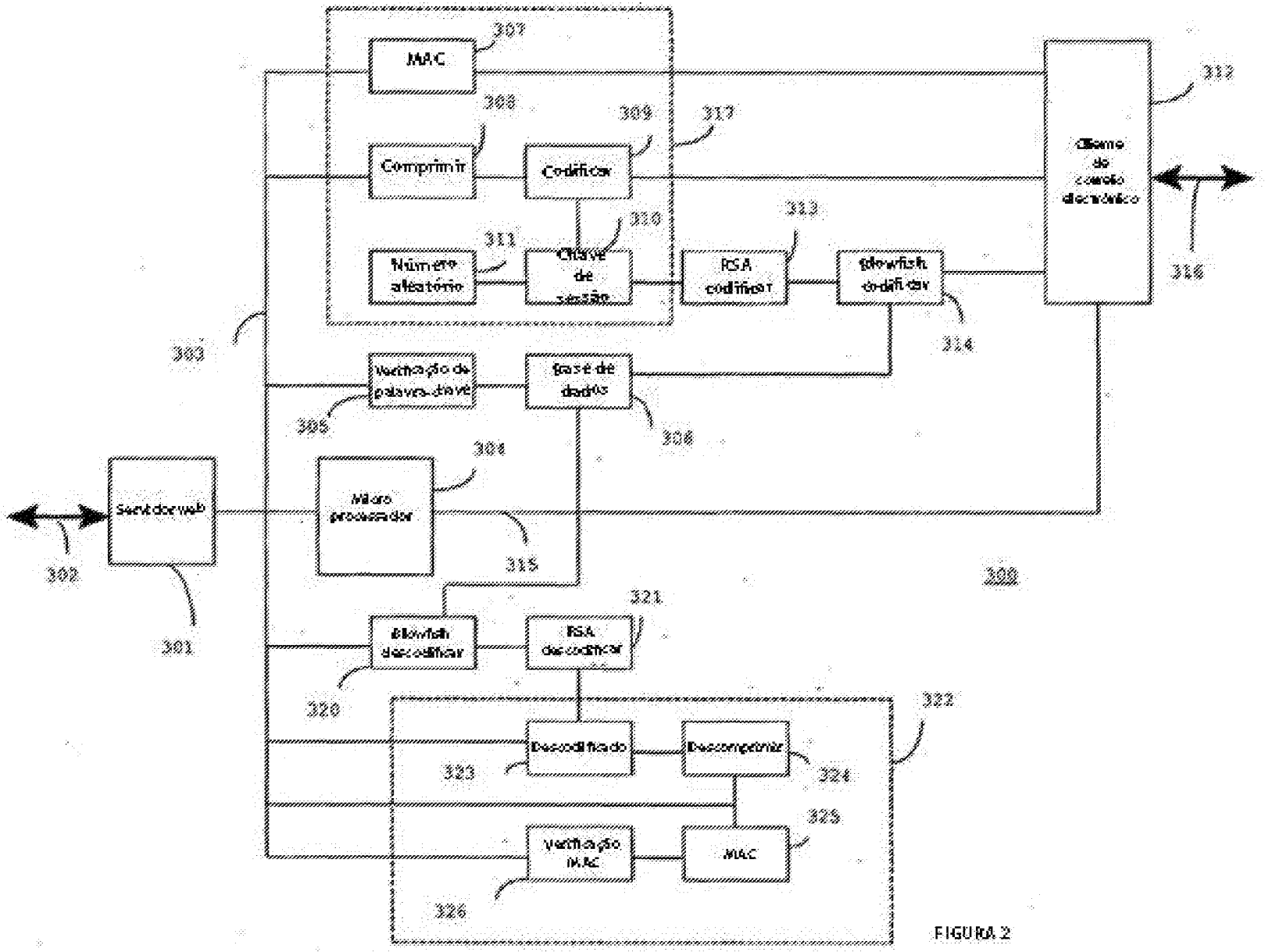
307
MAC
308
Comprimir
309
Codificar
317
310
311
Número aleatório
Chave de sessão
313
RSA codificar
Blowfish codificar
314
312
Cliente de correio electrónico
316
303
Verificação de palavra-chave
305
Base de dados
306
304
Motor processador
315
Servidor web
302
301
309
321
Blowfish descodificar
RSA descodificar
320
322
Descodificado
Descomprimir
323
324
325
Verificação MAC
MAC
326

FIGURA 2

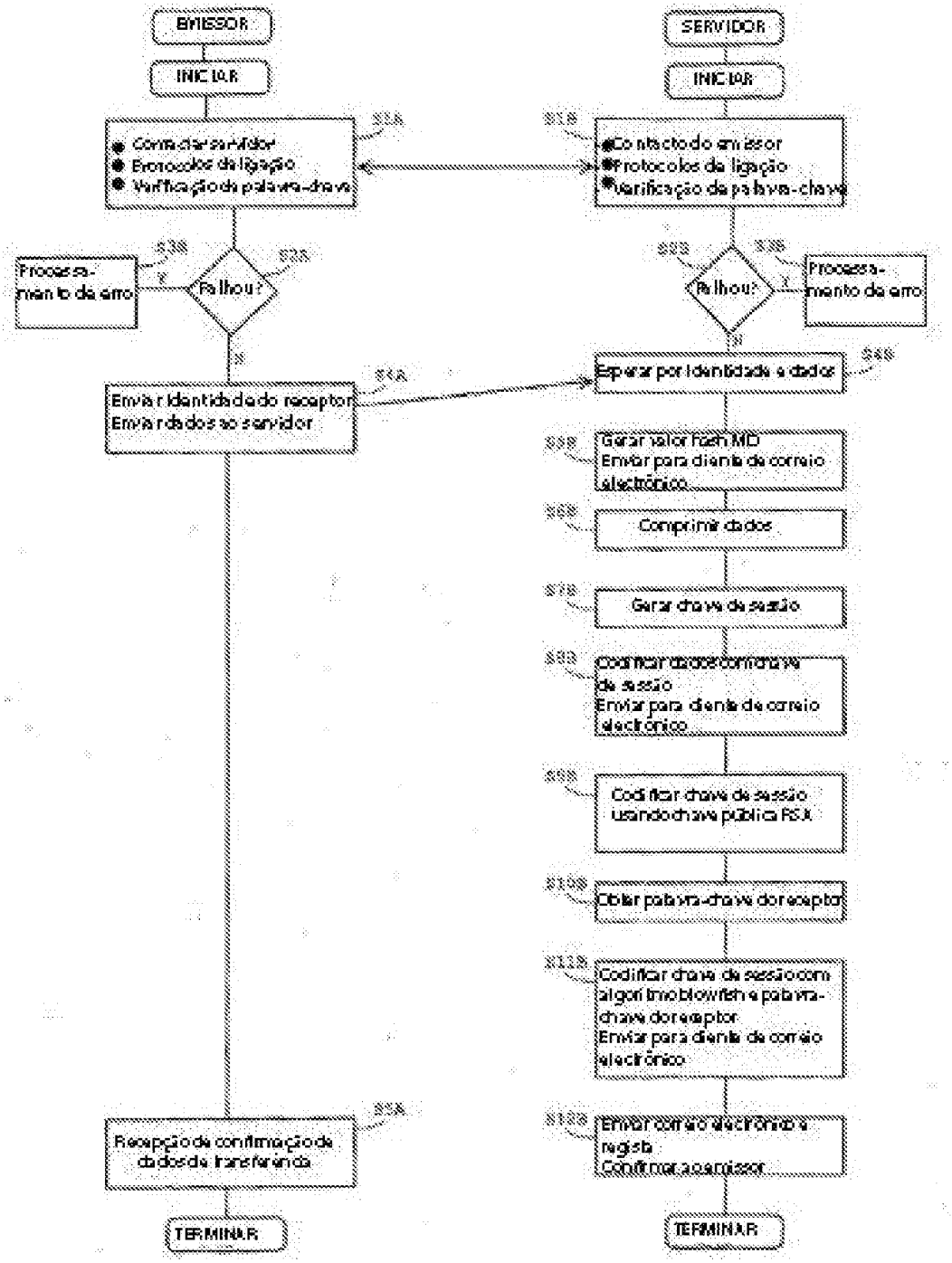
EMISSOR
INICIAR
S12A
Contactar servidor
Protocolos de ligação
Verificação da palavra-chave
S13B
Processamento do erro
Falhou?
S13A
N
S14A
Enviar identidade do receptor
Enviar dados ao servidor
S15A
Recepção da confirmação de dados de transferência
TERMINAR
SERVIDOR
INICIAR
S12B
Contacto do emissor
Protocolos de ligação
Verificação da palavra-chave
S13B
Falhou?
S13A
Processamento do erro
S14B
Esperar por identidade e dados
S15B
Gerar valor hash MD
Enviar para cliente de correio electrónico
S16B
Comprimir dados
S17B
Gerar chave de sessão
S18B
Codificar dados com chave de sessão
Enviar para cliente de correio electrónico
S19B
Codificar chave de sessão usando chave pública RSA
S110B
Obter palavra-chave do receptor
S111B
Codificar chave de sessão com algoritmo blowfish e palavra-chave do receptor
Enviar para cliente de correio electrónico
S112B
Enviar correio electrónico e regista
Confirmar ao emissor
TERMINAR

FIGURA 3

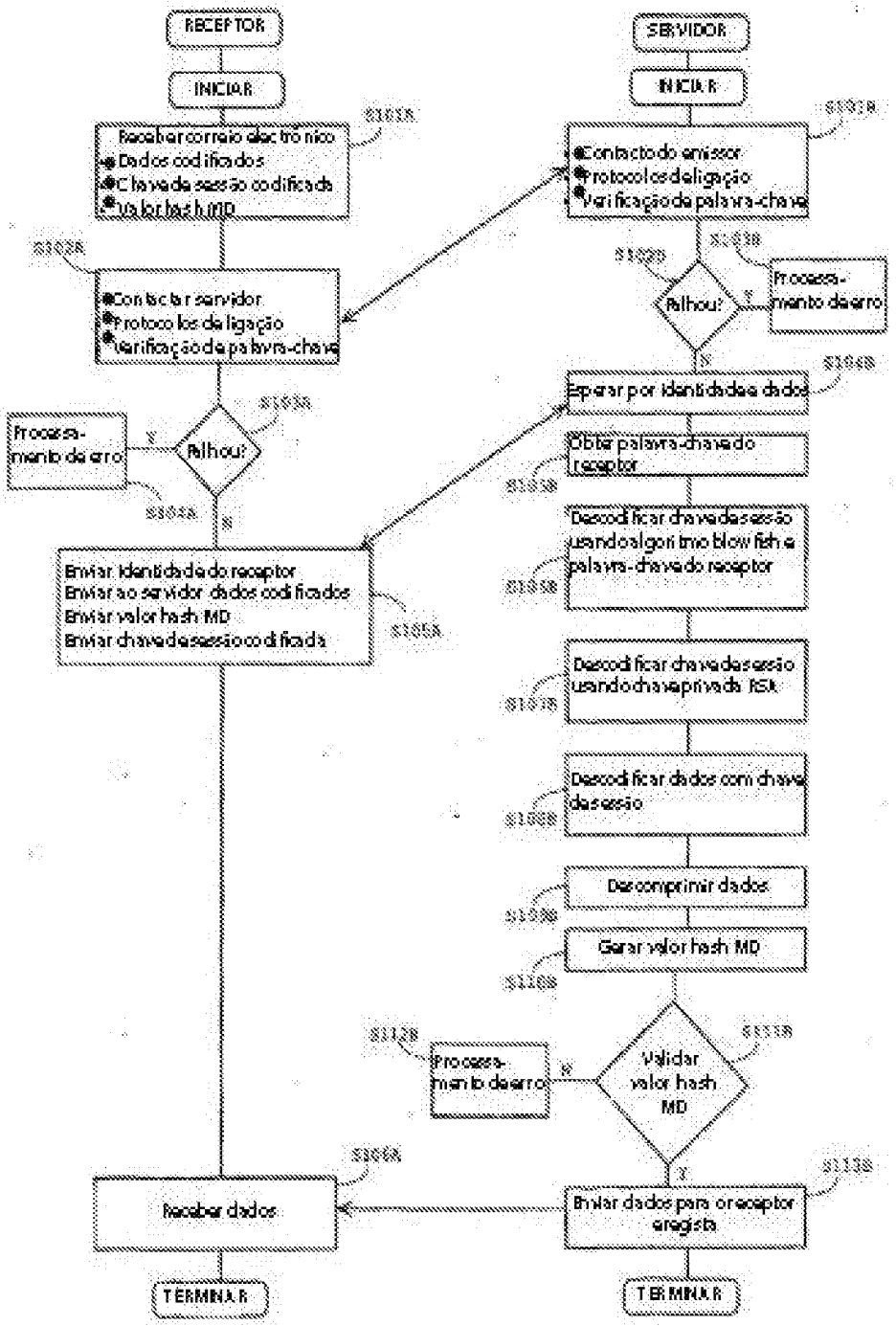
RECEPTOR
INICIAR
Recaber correio electrónico
Dados codificados
Chave de sessão codificada
Valor hash MD
S1028R
Contactar servidor
Protocolos de ligação
Verificação de palavra-chave
S1035R
Falhou?
S
Processamento de erro
S1045R
N
Enviar identidade do receptor
Enviar ao servidor dados codificados
Enviar valor hash MD
Enviar chave de sessão codificada
S1055R
S1060R
Receber dados
TERMINAR
SERVIDOR
INICIAR
S1018B
Contacto do emissor
Protocolos de ligação
Verificação de palavra-chave
S1025B
Falhou?
S
Processamento de erro
N
S1040B
Esperar por identidade dados
Obter palavra-chave do receptor
S1050B
Descodificar chave de sessão usando algoritmo blowfish e palavra-chave do receptor
S1055B
Descodificar chave de sessão usando chave privada RSA
S1070B
Descodificar dados com chave de sessão
S1080B
Descomprimir dados
S1090B
Gerar valor hash MD
S1100B
Validar valor hash MD
S1110B
S
Processamento de erro
N
S1120B
Enviar dados para o receptor registo
S1130B
TERMINAR

FIGURA 4