

(11) Número de Publicação: **PT 877507 E**

(51) Classificação Internacional:
H04L 9/08 (2006.01)

(12) FASCÍCULO DE PATENTE DE INVENÇÃO

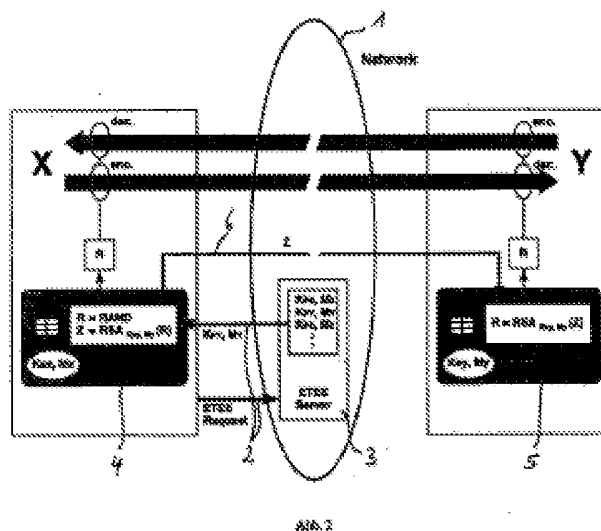
(22) Data de pedido: 1998.05.05	(73) Titular(es): T-MOBILE DEUTSCHLAND GMBH LANDGRABENWEG 151 53227 BONN DE
(30) Prioridade(s): 1997.05.05 DE 19718583	
(43) Data de publicação do pedido: 1998.11.11	(72) Inventor(es): STEFAN KALINER DE
(45) Data e BPI da concessão: 2007.09.26 002/2008	(74) Mandatário: LUÍS MANUEL DE ALMADA DA SILVA CARVALHO RUA VÍCTOR CORDON, 14 1249-103 LISBOA PT

(54) Epígrafe: **ENCRIPTAÇÃO EXTREMO A EXTREMO**

(57) Resumo:

RESUMO**"ENCRIPTAÇÃO EXTREMO A EXTREMO"**

O invento diz respeito a um processo para a geração e distribuição de chaves secretas para a encriptação extremo a extremo (*end-to-end encryption*) de informação veiculada numa ligação de comunicação entre dois assinantes (X, Y) de um sistema de comunicação digital. Caracteriza o invento o facto de a encriptação extremo a extremo recorrer a um processo de encriptação simétrico e a chave secreta (R) requerida para tal ser trocada entre os assinantes por um processo de encriptação assimétrica. Um dos dois assinantes gera a chave secreta, encripta a mesma com a parte pública de uma chave privada do outro assinante e a transmite o resultado ao segundo assinante por intermédio do sistema de comunicação. O segundo assinante decripta a grandeza encriptada recebida com a parte secreta da sua chave, obtendo deste modo a chave secreta para a encriptação extremo a extremo.



DESCRIÇÃO

"ENCRIPTAÇÃO EXTREMO A EXTREMO"

Objecto do invento é uma encriptação (cifragem) extremo a extremo, mais propriamente um processo para a geração e distribuição de chaves secretas para efeito da encriptação extremo a extremo de informação veiculada numa ligação estabelecida no âmbito de sistemas de comunicação digital.

Por "encriptação extremo a extremo" (*End-To-End Encryption*, cujo acrónimo é ETEE) entende-se a possibilidade de troca uni ou bidireccional de informação (em particular voz, mas também fax ou dados) sob uma forma

encriptada (cifrada) entre dois assinantes de um sistema de comunicação digital. Caracteriza-a o facto de a encriptação ser efectuada no local de emissão e a decrptação ser realizada apenas pelo receptor de uma mensagem, não exercendo o canal de comunicação intermediário qualquer influência sobre a encriptação. No âmbito da cadeia de transmissão digital não há nenhuma hipótese de reconversão da mensagem para o texto não cifrado original.

Os requisitos de processamento em tempo real impostos a processos de encriptação adequados obrigam necessariamente à utilização de algoritmos de encriptação simétricos com chaves secretas idênticas R quer no emissor, quer no receptor.

Um problema básico associado consiste na geração da chave secreta de ETEE, R, e na sua transmissão segura a ambos os parceiros da comunicação. A exigência básica imposta aos processos criptográficos no que respeita à segurança - que esta resida no secretismo das chaves e não no secretismo dos processos utilizados - conduz aos seguintes requisitos:

1. As chaves de ETEE têm de ter um valor individual imprevisível para cada sessão de comunicação.
2. O valor de partida para a geração da chave tem de ser individual no que respeita a cada assinante, ou seja, não são apropriados processos conhecidos em que

a chave individual é derivada de uma única chave mestra.

3. Em momento algum uma chave de ETEE pode surgir fora de um ambiente seguro do texto não encriptado ou sob uma qualquer outra forma que permita o cálculo do valor original. Apenas são considerados ambientes seguros os dispositivos de comunicação (terminais) pertencentes ao emissor e ao receptor.

EM US-A 5,481,613 é dado a conhecer um processo para a geração e distribuição de chaves secretas para a encriptação extremo a extremo de informação veiculada numa ligação de comunicação entre dois assinantes (X, Y) de um sistema de comunicação digital, em que a encriptação extremo a extremo é realizada com recurso a um processo de encriptação simétrico e a chave secreta (R) requerida para tal é permutada entre os assinantes por um processo de encriptação assimétrico, em que um dos dois assinantes gera a chave secreta (R), encripta a mesma com a parte pública de uma chave privada do outro assinante e a transmite através do sistema de comunicação ao segundo assinante, e o segundo assinante decripta a grandeza cifrada recebida com a parte secreta da sua chave, obtendo deste modo a chave secreta (R), em que os elementos públicos da chave (K_{PX} , M_X ou K_{PY} , M_Y) de cada um dos assinantes se encontram arquivados no componente central do sistema de comunicação, caracterizado por, na sequência de um pedido de encriptação por parte de um assinante (X) por intermédio de um canal de

dados ou sinalização independente da ligação de comunicação, serem disponibilizados a este assinante por parte do componente central do sistema de comunicação os elementos públicos da chave RSA (K_{PY} , M_Y) do outro assinante (Y), por ser gerada e armazenada uma chave secreta (R) sob a forma de número aleatório por parte do primeiro assinante (X), chave (R) essa que é encriptada pelo processo RSA que recorre aos elementos públicos da chave RSA (K_{PY} , K_Y) do segundo assinante (Y) de modo a que seja obtido um valor (Z) que é transmitido por intermédio do sistema de comunicação ao segundo assinante (Y), e por o valor (Z) recebido pelo segundo assinante (Y) ser decifrado e armazenado por parte deste com recurso aos elementos secretos da chave RSA (K_{SY} , K_Y) de modo a obter a chave secreta (R).

O documento mencionado dá a conhecer o processo que acabou de ser descrito na parte genérica da respectiva descrição, na qual são reconhecidas as técnicas anteriores relevantes para o mesmo.

No mesmo documento, o componente central do sistema de comunicação que é responsável pela gestão de determinados elementos é designado Sistema da Autoridade de Certificação ou CAS (do inglês "*Certification Authority System*").

O referido CAS é responsável pela gestão das chaves públicas de ambas as partes A e B, tendo a parte que

realiza a encriptação (por exemplo a parte A) de requerer ao CAS um certificado para, com base no mesmo e num número aleatório, proceder à encriptação, utilizando a chave pública da parte B.

Este sistema pressupõe que é segura a transferência de chaves entre o CAS e a parte responsável pela encriptação. Quando estão em causa grandes redes de computadores, situação que o documento de patente US-A-5481613 toma como ponto de partida, pode, de facto, ser este o caso. Neste documento de patente é pressuposta a presença de uma rede de computadores muito ramificada em que os utilizadores individuais (as partes) criam domínios de segurança e se parte do princípio de que uma parte sediada num dos domínios de segurança quer proceder a uma operação de encriptação em conjunto com uma parte sediada num outro domínio de segurança.

O que é problemático neste caso é o trajecto dos dados entre uma das partes e o CAS pressupor uma ligação de dados segura e impossível de comprometer.

Constitui uma desvantagem adicional o facto de, na rede de computadores muito ramificada mencionada, cada uma das partes poder iniciar um processo de encriptação com cada uma das partes restantes, correndo-se o perigo de determinadas partes não estarem autorizadas realizar tais processos de encriptação.

Acresce que o CAS mencionado no referido documento apenas se destina à distribuição de chaves públicas (certificados), não controlando a título de servidor o tráfego de dados, o que tem como desvantagem a obrigatoriedade de o trabalho de encriptação ter de decorrer em grande parte nos computadores dos próprios utilizadores que não dispõem de um meio seguro.

Ao invento subjazia por conseguinte a tarefa de aperfeiçoar um componente central de um sistema de comunicação do tipo anteriormente mencionado no sentido de possibilitar uma escolha (paga) entre um número diversificado de assinantes que fossem garantia de uma encriptação simples e segura.

Este objectivo foi alcançado pelo invento sob a forma dos ensinamentos técnicos constantes da reivindicação 1.

Constitui uma característica específica do invento a configuração do componente central do sistema de comunicação como elemento pago que, consequentemente, somente pode ser solicitado pelo utilizador na sequência de um pedido de autorização por parte do mesmo. Em conformidade, é obrigatoriamente dado despacho ao pedido de autorização efectuado pelo utilizador antes de o componente pago disponibilizar os serviços de um servidor de ETEE no qual decorre o essencial do trabalho de encriptação.

Deste modo, não só é simples a forma de gestão a realizar no servidor de ETEE, como os utilizadores propriamente ditos ficam dispensados de tais tarefas de gestão.

Os ensinamentos técnicos dados a conhecer pelo invento também providenciam uma encriptação segura, uma vez que prevêem que a mesma se processe num *chip card* contendo um circuito integrado. Deste modo, o utilizador tem a sua disposição um meio seguro, que pode retirar sem qualquer dificuldade do dispositivo de comunicação (terminal) e no qual encontra pronta a utilizar - como é do conhecimento geral - uma rotina de autenticação do utilizador. Deste modo, o *chip card* tem uma utilização dupla, uma vez que um pedido de autorização do utilizador desencadeia do modo usual a rotina de autenticação memorizada no *chip card*, ao mesmo tempo que neste se realiza a encriptação segura.

Consegue-se assim dispor de mecanismos de encriptação que decorre em meio seguro (*chip card*) e é particularmente simples e supervisionável.

No documento de patente europeia EP0529661A2 apenas é dada a conhecer uma forma particular de encriptação, não podendo dele ser depreendidas as características específicas essenciais do invento (elemento gestor pago alojado num servidor de ETEE, pedido de autorização e encriptação no *chip card*).

O objectivo do invento foi alcançado por via das características específicas indicadas na reivindicação 1.

Das reivindicações subsidiárias podem ser depreendidos aperfeiçoamentos e modificações vantajosos do invento.

O presente conceito satisfaz os requisitos de segurança e individualidade, sem que o sistema de comunicação tenha, ele próprio, conhecimento das chaves secretas (R). Simultaneamente, é contudo ao sistema que incumbe a iniciação da transmissão da chave e, portanto, o controlo da utilização da encriptação extremo a extremo. Caso o processo seja configurado como serviço suplementar pago, a autorização pode ser dada em função de determinadas características da relação entre assinantes. Simultaneamente, os assinantes ficam dispensados do armazenamento e gestão de elementos das chaves dos seus parceiros de comunicação.

O processo utiliza uma geração descentralizada da chave de ETEE, R, por parte do assinante requisitante da ETEE, X. A chave secreta R é transmitida ao assinante Y sob a forma encriptada pelo processo criptográfico conhecido como RSA (do sobrenome dos seus autores, Ronald L. Rivest, Adi Shamir e Leonard M. Adleman) em que são utilizados os elementos públicos da chave RSA do assinante Y, sendo decryptada por parte deste com recurso aos elementos secretos da sua chave, encontrando-se então ao dispor de

ambas as partes para efeito da encriptação da informação. Os elementos públicos da chave RSA do assinante Y foram previamente postos à disposição do assinante X por parte de um componente central do sistema de comunicação (servidor de ETEE). Todos os cálculos para a geração e transmissão da chave de ETEE, bem como o armazenamento dos elementos secretos da chave RSA decorrem num componente seguro (por exemplo num *chip card*) de que dispõe cada um dos assinantes.

O invento é em seguida descrito em mais pormenor com recurso aos desenhos que representam uma única forma de execução do mesmo. Dos desenhos e da respectiva descrição podem ser depreendidas características específicas adicionais do invento, bem como vantagens do mesmo. São mostrados:

Figura 1 esquemática e genericamente, o princípio básico de uma ligação encriptada entre dois assinantes X e Y;

Figura 2 esquematicamente, um processo de encriptação de acordo com o invento.

Na Figura 1 (assinalada com o termo alemão "Abbildung 1") encontra-se representado, de um modo esquemático e genérico, o princípio subjacente a uma ligação simetricamente encriptada entre dois assinantes X e Y. Cada um dos assinantes X e Y dispõe no seu terminal de uma chave secreta R que pode ser utilizada por qualquer uma

das partes quer para a encriptação (assinalada com o termo inglês "encryption"), quer para a decriptação ("decryption") dos dados transmitidos através de um sistema ou rede de comunicação.

O que pode revelar-se problemático é o facto de a chave secreta R ser do conhecimento exclusivo dos assinantes. Caso se trate de apenas dois assinantes, não há dificuldades de maior, uma vez que as partes podem, por exemplo, acordar previamente uma chave. O mesmo deixa de ser possível em caso de múltiplos assinantes, em particular quando, por questões de segurança, a chave secreta é substituída em permanência.

É nesta situação que o invento é aplicável. De acordo com a Figura 2 ("Abbildung 2"), o assinante X pretende tornar segura por meio de uma encriptação extremo a extremo (ETEE) uma ligação de comunicação existente ou a estabelecer com um assinante Y .

Cada um dos assinantes, X ou Y , dispõe de um terminal com um componente seguro 4 ou 5, respectivamente, por exemplo um *chip card* no qual se encontram armazenados não só os dados individuais do assinante, como também os elementos secretos individuais da chave (key) RSA, K_{SX} , M_X ou K_{SY} , M_Y . Os elementos públicos da chave RSA, K_{PX} , M_X ou K_{PY} , M_Y , etc. de cada assinante encontram-se armazenados num componente central 3 da rede ("network") de comunicação 1, tendo cada um dos assinantes autorizados na sequência do

respectivo pedido de autorização acesso aos mesmos.

Por via de um canal de dados ou sinalização independente 2 (por exemplo um serviço de mensagens curtas ou SMS [*Short Message Service*] nas redes GSM [*Global System for Mobile communications*]), o assinante X de um componente central 3 (por exemplo um servidor ["server"] de ETEE) do sistema de comunicação 1 envia o respectivo pedido de encriptação extremo a extremo ("ETEE request").

No componente central 3 do sistema de comunicação é examinado o direito à encriptação do assinante X, respondendo o sistema, em caso de afirmativo com a disponibilização dos elementos secretos da chave RSA, ou seja, a chave pública RSA K_{PY} e o módulo M_Y do assinante Y. O assinante X transfere os dados recebidos para um componente seguro 4.

O componente seguro 4 gera então enquanto valor aleatório (*random*, em inglês, assinalado como "RAND") uma chave de ETEE, R, e encripta a mesma com auxílio de K_{PY} e M_Y , obtendo o valor Z. A chave R é armazenada por parte do assinante X para efeito da sua utilização na seguinte combinação:

$$Z = \text{RSA}|K_{PY}, M_Y(R)$$

O valor Z é transmitido através de um canal de dados 6 do sistema ou rede de comunicação 1 ao assinante Y

e transferido por este para o respectivo componente seguro 5.

O componente seguro 5 decripta o valor Z com auxílio da respectiva chave secreta RSA , K_{SY} e do módulo M_Y , obtendo a chave secreta R . A chave R é armazenada por parte de Y .

$$R = RSA|K_{SY}, M_Y(Z)$$

Ambas as partes X e Y dispõem agora de chaves de ETEE, R , idênticas. Por conseguinte podem ser realizadas uma encriptação e uma decriptação simétricas da informação trocada entre as partes por intermédio da rede de comunicação 1.

Não é requerida uma securização especial das chaves R , uma vez que as mesmas apenas se encontram presentes nos dispositivos (terminais) emissor e receptor, além de perderem imediatamente a sua validade, uma vez terminada a comunicação submetida a ETEE. Cada nova comunicação sujeita a ETEE terá de ser realizada com novas chaves.

Igualmente não críticos são os elementos públicos da chave RSA no servidor de ETEE, bem como a sua transmissão ao assinante X . Pode assim prescindir-se de medidas preventivas de espionagem.

Legenda dos desenhos

R	chave secreta
X	assinante X
Y	assinante Y
Z	grandeza encriptada
1	sistema de comunicação
2	canal de dados
3	componente central
4	componente seguro
5	componente seguro
6	canal de dados

Lisboa, 20 de Dezembro de 2007

REIVINDICAÇÕES

1. Processo para a geração e distribuição de chaves secretas para a encriptação extremo a extremo de informação veiculada numa ligação de comunicação entre dois assinantes (X, Y) de um sistema de comunicação digital, em que a encriptação extremo a extremo, recorre a um processo de encriptação simétrico que utiliza um componente central do sistema de comunicações responsável pela gestão de determinados elementos da chave, e em que a chave secreta (R) requerida pelo processo é trocada entre os assinantes por um processo de encriptação assimétrico, em que um dos dois assinantes gera a chave (R), encripta a mesma com a parte pública de uma chave privada do outro assinante e a transmite através do sistema de comunicação ao segundo assinante, e o segundo assinante decripta a grandeza encriptada recebida com a parte secreta da sua chave, obtendo deste modo a chave secreta (R), em que os elementos públicos da chave (K_{PX} , M_X ou K_{PY} , M_Y) de cada um dos assinantes se encontram arquivados no componente central (3) do sistema de comunicação (1) a título de serviço suplementar pago (5.3, linha 2), em que é realizado no componente central do sistema de comunicação um controlo para verificar se o assinante está autorizado a requerer uma encriptação, na sequência de um pedido de encriptação por parte de um assinante (X) por intermédio de um canal de dados ou sinalização (2) independente da ligação de comunicação, #serem disponibilizados a este assinante por parte do componente central (3) do sistema de comunicação,

os elementos públicos RSA da chave (K_{PY} , M_Y) do outro assinante (Y), por ser gerada e armazenada por parte do primeiro assinante (X) uma chave secreta (R) sob a forma de número aleatório, a chave secreta (R) é encriptada pelo processo criptográfico RSA que recorre aos elementos públicos da chave RSA (K_{PY} , K_Y) do segundo assinante (Y) de modo a que seja obtido um valor (Z) que é transmitido por intermédio do sistema de comunicação ao segundo assinante (Y), e

por o valor (Z) recebido pelo segundo assinante (Y) ser decryptado e armazenado por parte deste com recurso aos elementos secretos RSA da chave (K_{SY} , K_Y) de modo a que seja obtida a chave secreta (R), e por os cálculos para a geração e transmissão da chave secreta (R), bem como o armazenamento dos elementos secretos da chave RSA serem realizados exclusivamente em *chip cards* pertencentes a cada um dos assinantes.

2. Processo de acordo com a reivindicação 1, **caracterizado por** a encriptação e decryptação do valor (R) serem realizadas pelo processo criptográfico RSA.

3. Processo de acordo com uma das reivindicações 1 ou 2, **caracterizado por** a chave secreta (R) gerada perder a validade uma vez terminada cada uma das ligações sujeitas a encriptação.

Lisboa, 20 de Dezembro de 2007

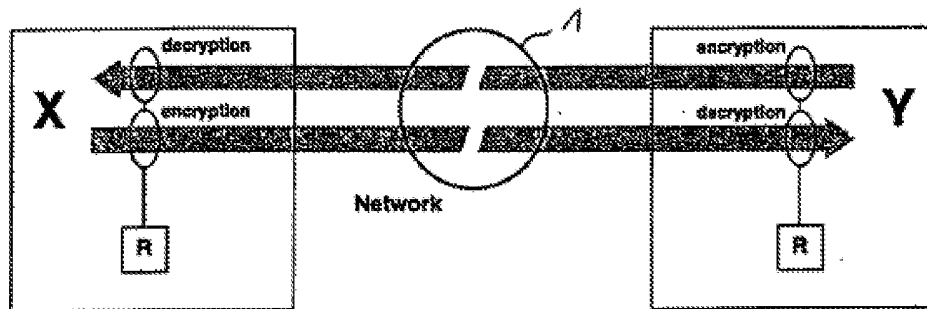


Abb. 1

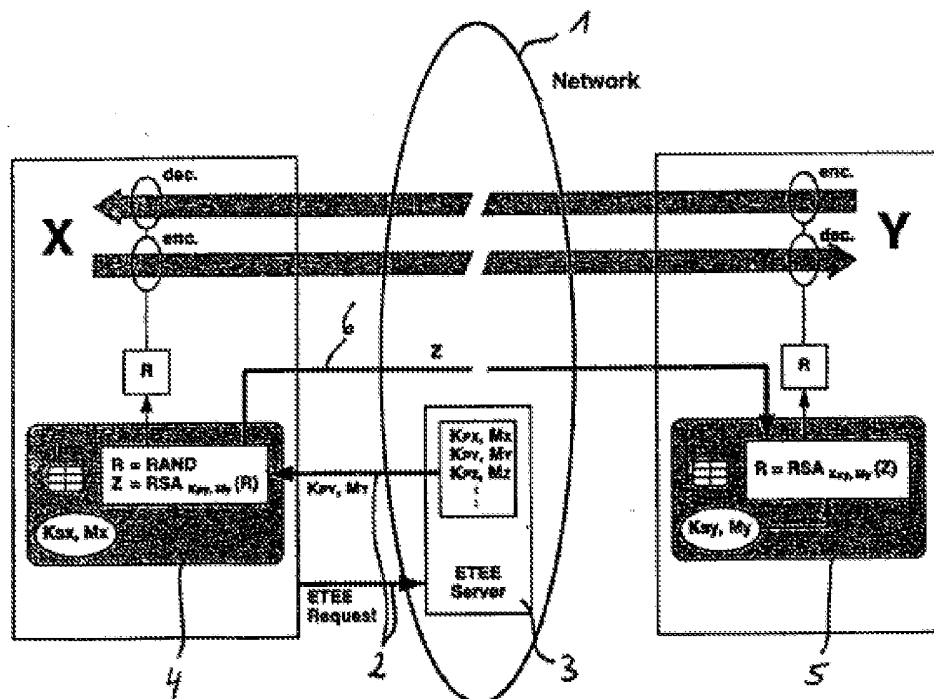


Abb. 2

REFERÊNCIAS CITADAS NA DESCRIÇÃO

Esta lista de referências citadas pelo requerente é apenas para conveniência do leitor. A mesma não faz parte do documento da patente Europeia. Ainda que tenha sido tomado o devido cuidado ao compilar as referências, podem não estar excluídos erros ou omissões e a EPO rejeita quaisquer responsabilidades a esse respeito.

Documentos de patentes citadas na descrição

- US 5481613 A

- EP 0529661 A2