

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

(21) **PI 1105431-0 A2**

(22) Data de Depósito: 25/10/2011  
(43) Data da Publicação: 26/02/2013  
(RPI 2199)



(51) *Int.Cl.:*  
H04L 9/32

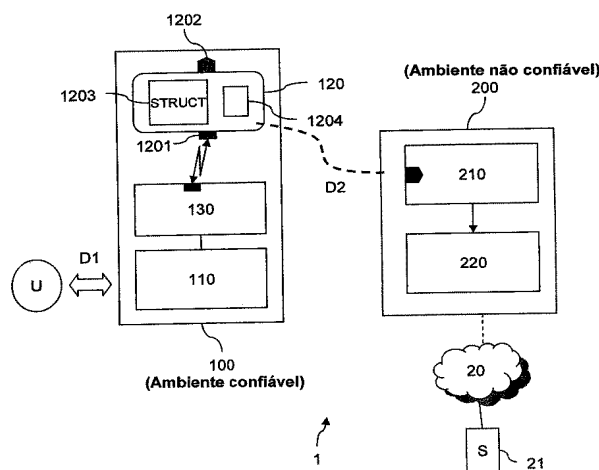
**(54) Título:** MÉTODO E SISTEMA PARA CONTROLAR A EXECUÇÃO DE UMA FUNÇÃO PROTEGIDA POR AUTENTICAÇÃO, MÓDULO DE MEMÓRIA, E, ENTIDADE ELETRÔNICA

**(30) Prioridade Unionista:** 26/10/2010 FR 1058771

**(73) Titular(es):** Oberthur Technologies

**(72) Inventor(es):** Alban Feraud

**(57) Resumo:** MÉTODO E SISTEMA PARA CONTROLAR A EXECUÇÃO DE UMA FUNÇÃO PROTEGIDA POR AUTENTICAÇÃO, MÓDULO DE MEMÓRIA, E, ENTIDADE ELETRÔNICA. A presente invenção envolve um método e sistema para controlar a execução de uma função protegida por autenticação de um usuário e que é fornecida por exemplo para o acesso a uns recursos. O método compreende introduzir, pelo usuário, dados pessoais usando um dispositivo de entrada, autenticar o usuário com os dados pessoais de entrada para autorizar ou não autorizar a execução da função; em um cartão seguro conectado para o dispositivo de entrada, armazenar dados de autenticação de validade limitada dependente dos dados de entrada, quando o cartão está conectado a um dispositivo de processamento através do qual o usuário gera uma mensagem cujo processamento implementa a mencionada função, usando os dados armazenados, levando em consideração a validade limitada, para autorizar ou não autorizar a execução daquela função.



‘MÉTODO E SISTEMA PARA CONTROLAR A EXECUÇÃO DE UMA  
FUNÇÃO PROTEGIDA POR AUTENTICAÇÃO, MÓDULO DE  
MEMÓRIA, E, ENTIDADE ELETRÔNICA’

Este pedido reivindica prioridade do pedido Francês de N°  
1058771 depositado em 26 de outubro de 2010, o qual pedido é incorporado  
aqui para referência.

CAMPO DA INVENÇÃO

A presente invenção diz respeito a um método e um sistema  
para controlar a execução de uma função protegida de autenticação.

CONTEXTO DA INVENÇÃO

Uma função é dita ser protegida por autenticação quando sua  
execução depende do resultado de uma autenticação, geralmente de um  
usuário.

Essas funções são em particular usadas para acessar recursos  
tal como sistemas, redes, aplicações, serviços em um cartão ou servidor  
remoto, e dados armazenados.

Tal uma função pode em particular corresponder à comandos  
implementados por uma entidade específica na recepção de uma mensagem  
solicitando o acesso a um recurso.

A autenticação do usuário envolvendo tal uma função para ter  
acesso a um daqueles recursos é convencionalmente realizada em um sistema  
de computador. Isto geralmente consiste de uma etapa de introduzir, pelo  
usuário, dados pessoais para identificação ou autenticação, usando um  
dispositivo de entrada, então de uma etapa de autenticar o usuário com base  
nos dados pessoais de entrada, por exemplo através de comparação com dados  
pessoais pré-gravados no sistema, para gerar uma autorização ou recusa para  
executar a função protegida possibilitando o acesso a um recurso.

Em caso de autorização, a função protegida é executada e o  
acesso ao recurso é obtido para o usuário.

Por meio de ilustração, os dados pessoais para identificação ou autenticação pode ser uma senha, um PIN (para “*Número de identificação Pessoal*”) ou dados biométricos.

Roubo de identidade é um problema recorrente que afeta a segurança dos sistemas para acesso a uns recursos por autenticação que processa aquelas funções protegidas por autenticação.

Em numerosas estratégias de ataque, roubo de identidade consiste em uma pessoa maliciosa roubando os dados pessoais particularmente confiáveis dos usuários para identificação ou autenticação, geralmente colocando software malicioso entre o dispositivo de entrada e o software de processamento que realiza uma autenticação com base nos dados pessoais de entrada.

O software malicioso recebe os dados confidenciais de entrada, faz uma cópia dos mesmos, então comunica aqueles dados para o software de processamento. Nesta maneira, nenhuma das duas partes envolvidas no acesso por autenticação (o usuário e o software de processamento) podem suspeitar da presença do software malicioso.

De posse dos dados pessoais confiáveis e conhecendo os recursos aos quais ele dão acesso (em particular porque o sistema de computador permite o acesso a um particular recurso, por exemplo uma caixa pagadora) possibilita Para pessoa maliciosa então a re-acessar os recursos, sob uma identidade falsa, aquela do usuário roubado.

Essas estratégias de ataque são conhecidas pelo termo “ataque de quem intercepta”. Elas são particularmente perigosas quando elas possibilitam ao ladrão de dados pessoais a identificação ou autenticação o acesso aos serviços por exemplo envolvendo transações financeiras. Elas são geralmente implementadas em relação a uns terminais de entrada não confiáveis, por exemplo terminais de pagamento nas lojas ou caixas pagadoras.

Há assim sendo uma necessidade de melhorar os mecanismos para verificar a execução de funções protegidas por autenticação, em particular quando elas possibilitam acesso aos recursos, em particular para combater tais estratégias de ataque.

5

### SUMÁRIO DA INVENÇÃO

Neste contexto, a invenção diz respeito em particular a um método de controle da execução de uma função protegida por autenticação, caracterizado pelo fato de compreender as seguintes etapas:

- armazenar, em uma estrutura de validade limitada, dados de autenticação pessoais dependentes dos dados pessoais de entrada, introduzindo os últimos por um usuário em um dispositivo de entrada;
- verificar a validade da estrutura de validade limitada antes de usar os dados de autenticação pessoais que ela contém para gerar uma autorização ou uma recusa para executar uma função implementada no processamento de uma mensagem gerada por um dispositivo de processamento que é distinto do dispositivo de entrada.

De acordo com a invenção, a entrada de dados pessoais e seu processamento para o acesso a uns recursos através da execução da função protegida pode ser dissociado no tempo ou no espaço. Isto é feito possível através do armazenamento em uma estrutura de validade limitada, de acordo com a invenção, dos dados de autenticação pessoais dependentes dos dados de entrada, assim sendo possibilitando ao elo de comunicação ser feito entre as duas operações de entrada e de processamento.

Ainda mais, essas duas operações são cada uma realizada em relação aos dispositivos distintos: o dispositivo de entrada para a primeira operação, e o dispositivo de processamento para a segunda. Assim sendo, o usuário não necessita efetuar uma introdução dos dados confidenciais no dispositivo de processamento, o que previne qualquer pessoa maliciosa tendo adulterado com aquele dispositivo de recuperar os dados confidenciais a partir

dos meios de entrada naquele dispositivo.

De acordo com a invenção, a dissociação das duas operações não possibilita a “quem intercepta” ambos, recuperar os dados confidenciais e conhecer os recursos aos quais eles possibilitam acesso (isto é para dizer a correspondente função protegida). Como será visto abaixo, o usuário pode usar um dispositivo de entrada no qual ele confia, por exemplo, um dispositivo que é específico para ele. Assim sendo, ele não é mais restringido aos dados pessoais de entrada em um dispositivo de terceiros de confiabilidade duvidosa.

No que se refere à validade limitada dos dados de autenticação pessoais, isto possibilita a eficiência da invenção a ser assegurada enquanto evitando dados confidenciais potencialmente roubados de serem usados indefinidamente, por exemplo, ao longo do tempo ou espaço, para possibilitar a pessoa maliciosa ter a função executada cuja execução é protegida por aqueles dados, e assim sendo ter acesso aos correspondentes recursos protegidos.

No caso de validade temporária, a duração da validade pode ser configurada nas bases dos riscos incorridos, e das funções e recursos envolvidos.

De forma similar, uma validade espacial definindo uma distância máxima para uso da estrutura a partir de um ponto inicial pode ser com base em uma medição de GPS.

Assim sendo, melhoramento é obtido no controle da execução das funções protegidas por autenticação e o possível acesso a uns recursos decorrentes.

De acordo com um aspecto da invenção, o método compreende as seguintes etapas:

- introduzir, pelo usuário, os dados pessoais usando o dispositivo de entrada;

- autenticar o usuário nas bases dos dados pessoais de entrada para gerar a autorização ou a recusa para executar a função protegida;

- executar uma função no caso de autorização;

em que:

5                   - as etapas de armazenar e verificar são implementadas em um módulo de memória respectivamente conectado ao dispositivo de entrada no momento da etapas de entrada e armazenamento, e ao dispositivo de processamento no momento das etapas de verificação e execução.;

10                  - a mencionada estrutura de validade limitada compreende dados de autenticação pessoais de validade limitada por associação de uma duração de validade com os dados de autenticação pessoais.

Embora seja possível a conexão ser física, é acima de tudo uma conexão lógica possibilitando a comunicação ser fornecida entre o dispositivo e módulo então envolvido.

15                  Somente um módulo de memória, que pode ser um cartão de microprocessador seguro convencional, manipula a estrutura de validade limitada de dados aqui, e assim sendo os dados de autenticação pessoais de validade limitada contidos por aquela estrutura. Em virtude das técnicas seguras que são amplamente conhecidas para este tipo de módulo ou cartão,

20                  esses dados podem ser gerenciados como chaves secretas internas, e são assim sendo manipuladas em maneira segura durante as duas fases de entrada e exploração para autorizar ou não autorizar a execução da função protegida.

25                  Em uma modalidade, a verificação da validade da estrutura para usar os dados de autenticação pessoais compreende verificar o tempo que passou desde a geração daquela estrutura de validade limitada comparada com a duração da validade que está associada com os dados de autenticação pessoais. Em outras palavras, esta disposição consiste em verificar que os dados de autenticação pessoais de validade limitada são ainda válidos quando eles são usado para o propósito de obter uma autorização para executar a

função. Re-suo em grande escala desses dados confidenciais de validade limitada por uma pessoa maliciosa é e por meio disso, evitado. De acordo com algumas modalidades, em particular determinada descrita abaixo, a geração da autorização ou da recusa pode, como uma variante, ser dependente do tempo passado desde o término o fornecimento da potência elétrica para uma memória armazenando a estrutura de validade limitada.

Em uma modalidade, gerar autorização ou a recusa é dependente de uma verificação dos dados pessoais introduzidos com dados de referência, o resultado da verificação sendo obtido usando os mencionados dados de autenticação pessoais armazenados na estrutura de validade limitada armazenada. Em maneira convencional, a autenticação do usuário aqui compreende a verificação dos dados pessoais de entrada para os propósito de autorizar ou não autorizar o acesso ao recurso. A presente disposição possibilita esses mecanismos serem mantidos em virtude do uso dos dados de autenticação pessoais de validade limitada que são armazenados no módulo de memória de acordo com a invenção.

De acordo com um particular recurso da invenção, o método compreende a etapa de comparar dados pessoais de entrada com dados pessoais pré-gravados no módulo de memória, e os dados de autenticação pessoais armazenados na estrutura de validade limitada compreende o resultado da comparação. Nesta configuração, as operações de autenticação são realizadas no dispositivo de entrada mas a autorização com base naquela autenticação não foi ainda dada. Para ser preciso, somente o resultado da autenticação (se a comparação dos dados de entrada é ou não positiva) é fornecido como um item de dados confidenciais de validade limitada de acordo com a invenção. Assim sendo comunicação dos dados pessoais como entrada (senha, código de PIN, etc.) para um dispositivo de processamento é evitada.

Como uma variante, os dados de autenticação pessoais

armazenados na estrutura de validade limitada compreende os dados pessoais de entrada, e seu uso compreende uma sub-etapa de comparação dos dados de autenticação pessoais armazenados na estrutura de validade limitada com dados pessoais pré-gravados no módulo de memória. Esta disposição torna possível simplificar as operações realizadas pelo dispositivo de entrada, em particular se ele tem recursos de processamento limitados ou se, para as necessidades da comparação, isto se mostra necessário, por exemplo, ter acesso a um banco de dados seguro.

Em uma modalidade da invenção, a duração de validade associada com os dados de autenticação pessoais é contabilizada através da descarga de uma capacitância elétrica fornecida no módulo de memória. A capacitância elétrica assim sendo serve como um contador de tempo. Esta configuração é em particular simples de implementar em qualquer tipo de entidade eletrônica capaz de armazenar os dados de validade limitada de acordo com a invenção.

Em particular, os dados de autenticação pessoais são armazenados em uma memória volátil do módulo de memória, a qual memória é temporariamente alimentada pela mencionada capacitância elétrica. O controle através de autenticação de acordo com a invenção é tornada ainda mais segura por esta disposição, já que os dados confidenciais de validade limitada são automaticamente eliminados na expiração da duração de validade, devido à natureza da memória volátil. Ainda mais, esta configuração é simples de implementar.

Em uma outra modalidade, os dados de autenticação pessoais são armazenados em uma memória volátil do módulo de memória, e a duração de validade associada com eles é definida pelas propriedades de evanescimento da memória volátil quando seu fornecimento de energia é cortado. Esta disposição tem a vantagem de não se basear em meios específicos para contabilizar a duração de validade. Mais particularmente,

devido à evanescência dos dados neste tipo de memória volátil, é assegurado que os dados confidenciais de validade limitada são automaticamente apagados ao expirar a duração da evanescência. Memória voláteis assim sendo serão escolhidas cujas correspondentes propriedades de evanescência são apropriadas para a duração de vida ou validade desejada para os dados de autenticação pessoais gerados.

Em ainda uma outra modalidade, os dados de autenticação pessoais são armazenados em uma memória volátil de um módulo de memória, que é continuamente energizado durante o controle da execução da função protegida ou em uma memória de re-escrita, por exemplo do tipo de EEPROM tipo (EEPROM para “*Memória de Somente Leitura Programável e Passível de Apagar Eletricamente*”), e uma duração de validade associada com eles é definida armazenando uma quantidade temporal, por exemplo uma duração de validade e tempo inicial da validade, ou um tempo de término da validade sozinho, em uma variável que está associada na memória com os dados de autenticação pessoais. Elementos suficientes são assim sendo fornecidos para o módulo de memória para ser capaz de verificar que os dados de autenticação pessoais usados para obter a autorização estão ainda válidos, através de comparação da duração da validade, ou tempo de término da validade (que é a data incluindo a hora, minuto, etc.) com o tempo que passou desde a geração daqueles dados.

De acordo com um recurso da invenção, o uso, por um módulo de memória, dos dados de autenticação pessoais de validade limitada compreende verificar a validade daqueles dados usando a para lê-lo pelo dispositivo de processamento. Esta disposição possibilita uma referência comum a ser usada para avaliar o limite temporal para validade. Ela pode em particular ser um relógio comum para os diferentes dispositivos (por exemplo um relógio de rede), ou um relógio específico para aqueles dispositivos.

Em uma modalidade, a função protegida é um comando

implementada, na recepção de uma mensagem a partir do dispositivo de processamento, através de um módulo de microprocessador armazenando a estrutura de validade limitada. De acordo com várias abordagens, o comando protegido pode ser diretamente indicado em uma mensagem fornecida ou ser  
5 um sub-comando que depende de tal um comando indicado na mensagem (por exemplo um sub-comando chamado na execução daquele comando).

De acordo com um outro recurso da invenção, um módulo de memória armazenando a estrutura de validade limitada e os dados de autenticação pessoais que ela contém são removíveis, e são colocados no  
10 dispositivo de entrada no momento da entrada e colocados no dispositivo de processamento no momento da verificação da validade da estrutura e no momento do uso dos dados de autenticação pessoais de validade limitada. Esta disposição é altamente conveniente para o usuário, que, para os propósitos de controle da execução de uma função protegida por autenticação  
15 de modo, por exemplo, a ter acesso a um recurso, pode transportar ou fornecer apenas o módulo de memória removível sobre o qual são gravados os dados confidenciais resultantes da entrada e que são necessários para a autenticação.

Como uma variante, um módulo de memória armazenando a estrutura de validade limitada e os dados de autenticação pessoais que ela  
20 contém é fisicamente ligada com o equipamento de entrada durante o controle e execução da função protegida (isto é para dizer, durante as duas etapas de entrada e de processamento), e o equipamento de processamento se comunica com um módulo de memória através de comunicação sem contato. Esta configuração se mostra simples de uso para o usuário, já que o usuário pode  
25 simplesmente introduzir seus dados pessoais confidencialmente em um dispositivo de entrada que é específico para ele (por exemplo seu telefone móvel) e apresenta o último para o dispositivo de processamento para efetuar as subseqüentes operações necessárias para controlar a execução da função por exemplo para acessar um correspondente recurso. Esta comunicação sem

contato também cobre o caso onde aquela comunicação passa via o dispositivo de entrada no qual um módulo de memória está embutida. Por exemplo, este é o caso quando um cartão SIM (SIM significa “*Módulo de Identidade do Assinante*”) em um telefone móvel usa um controlador de NFC (NFC significa “*Comunicação de Campo Próximo*”) do telefone móvel para se comunicar com um dispositivo de processamento externo.

De acordo com um particular recurso, o módulo de memória armazenando a estrutura de validade limitada e os dados de autenticação pessoais é um cartão de microprocessador seguro. Esta disposição é vantajosa no fato que, em uma maneira convencional, o cartão de microprocessador compreende meios para tornar os dados confidenciais seguros e também meios eficientes para comunicar com um ou outro dos dispositivos de entrada e de processamento.

Em particular, a comunicação entre o dispositivo de entrada ou o dispositivo de processamento e o mencionado cartão de microprocessador é sem contato. Nesta maneira, aqueles dispositivos e o cartão (módulo de memória) são conectados à cada uma das operações necessárias para controlar a execução da função. O canal de comunicação pode ser de acordo com o padrão de NFC, com o padrão de ISO 14443 ou com um padrão similar.

Como uma variante, em particular se o cartão de microprocessador é removível durante essas operações, comunicação por contato pode ser fornecido entre o dispositivo de entrada ou o dispositivo de processamento e o mencionado cartão de microprocessador.

Em uma modalidade, o processamento da mensagem a partir do dispositivo de processamento gera uma resposta caracterizada pelo fato de compreender pelo menos um valor de resposta que depende da autorização ou da recusa gerada. Esta configuração acha numerosas aplicações, que são geralmente definidas no sucesso ou falha de um acesso solicitado pelo usuário (por exemplo um pagamento feito ou não feito com sucesso, o acesso a uma

conta segura, etc.).

Em determinadas aplicações como uma variante, um valor de resposta pode contudo ser independente da autorização ou da recusa gerada (para todas ou algumas das funções protegidas). Como ilustrado abaixo, a  
5 execução de uma função protegida pode simplesmente efetuar a atualização de um estado do módulo de memória interno , tal como um atualizador de detecção de acesso fraudulento.

Em uma modalidade da invenção, o usuário introduz pelo menos um item de informação representando um item de dados financeiros, e  
10 o mencionado item de informação é armazenado na estrutura de validade limitada em comum com os dados de autenticação pessoais, para os propósitos de uma posterior operação financeira (por exemplo uma transação), a qual o acesso dependente da autorização ou da recusa gerada. Em virtude da invenção, é assim sendo possível tornar seguro todos os dados  
15 introduzidos pelo usuário para o propósito de uma operação posterior, se aqueles dados são ou não confiáveis. Esta disposição aumenta a confiança daqueles dados nesta maneira.

Em uma modalidade da invenção, o dispositivo de entrada é um equipamento confiável pelo usuário. Esta configuração se beneficia da  
20 total eficiência da invenção, já que a operação de entrada é fortemente protegida aqui. Assim sendo, como uma pessoa maliciosa é incapaz de acessar esse dispositivo confiável ele é incapaz de recuperar os dados pessoais diretamente introduzidos pelo usuário.

Em particular, o dispositivo de entrada é um telefone móvel do  
25 usuário.

Em uma maneira complementar, a invenção envolve um módulo de memória caracterizado pelo fato de compreender pelo menos uma memória e um processador para executar instruções, o módulo de memória sendo configurado por:

- armazenar, em uma estrutura de validade limitada, dados de autenticação pessoais que são dependentes dos dados pessoais introduzidos por um usuário e recebidos de um dispositivo de entrada ao qual um módulo de memória está ligado (isto é para dizer durante a entrada);

5                   - verificar a validade da estrutura de validade limitada antes de usar os dados de autenticação pessoais que ela contém para gerar uma autorização ou uma recusa para executar a função protegida por autenticação e implementada no processamento de uma mensagem recebida a partir de um dispositivo de processamento que é distinto do dispositivo de entrada.

10                  De forma similar, a invenção envolve um sistema para controlar a execução de uma função protegida por autenticação de um usuário, caracterizada pelo fato de compreender:

- um dispositivo de entrada para introduzir dados pessoais pelo usuário;

15                  - um dispositivo de processamento que é distinto do dispositivo de entrada e adaptado para gerar, sob a ação do usuário, uma mensagem para processar;

- um módulo de memória caracterizado pelo fato de compreender pelo menos uma memória e um processador, e que é  
20 configurado para autenticar o usuário nas bases dos dados pessoais de entrada a fim de gerar uma autorização ou uma recusa para executar uma função protegida implementada no processamento da mencionada mensagem;

em que o módulo de memória é configurado para:

- quando ele está conectado ao dispositivo de entrada, gerar e  
25 armazenar, em sua memória, dados de autenticação pessoais de validade limitada que são dependentes dos dados pessoais de entrada e associando-os com um parâmetro de validade; e

- quando ele está conectado ao dispositivo de processamento, usando os dados de autenticação pessoais armazenados para gerar a

autorização ou a recusa para executar a função dependendo do parâmetro de validade associado.

O módulo de memória e o sistema de autenticação têm vantagens similares àqueles do método estabelecido acima. Em particular, eles tornam possível dissociar as operações de introduzir os dados confidenciais e de processar aqueles dados para o propósito de obter uma autorização para executar a função protegida, procurando segurança autenticada contra os ataques por quem intercepta.

Opcionalmente, um módulo de memória ou o sistema pode compreender meios relacionados aos recursos do método estabelecido acima, e em particular uma capacitância elétrica usada para contagem regressiva da duração de validade, uma memória volátil que automaticamente ser apaga ao término da mencionada duração, uma memória fixa ou removível, um cartão de microprocessador para armazenar os dados de autenticação pessoais de validade limitada de acordo com a invenção entre os vários dispositivos, meios sem contato ou com contato para comunicação entre o cartão de microprocessador e os vários dispositivos.

Em particular, esses dispositivos podem compreender meios de entrada para introduzir, pelo usuário, os dados pessoais usando o dispositivo de entrada; meios de autenticação para autenticar o usuário nas bases dos dados pessoais de entrada a fim de gerar a autorização ou a recusa para executar a função protegida; meios de execução para executar uma função no caso de autorização. Ainda mais, um módulo de memória configurado para o armazenamento e para a verificação pode ser respectivamente conectado ao dispositivo de entrada no momento da entrada e do armazenamento, e ao dispositivo de processamento no momento da verificação e da execução. Neste caso, ele pode ser fornecido para a mencionada estrutura de validade limitada para compreender os dados de autenticação pessoais de validade limitada por associação de uma duração de

validade com os dados de autenticação pessoais.

Mais ainda, de acordo com uma outra modalidade, os dados de autenticação pessoais armazenados na estrutura de validade limitada pode compreender os dados pessoais de entrada. O módulo de memória ou o sistema pode então, de modo a usar aqueles dados, compreender uns meios para comparar os dados de autenticação pessoais armazenados na estrutura de validade limitada com os dados pessoais pré-gravados no módulo de memória.

De acordo com uma outra modalidade, a mencionada estrutura de validade limitada compreende dados de autenticação pessoais de validade limitada pela associação de uma duração de validade com os dados de autenticação pessoais. Neste caso, eles podem ser fornecidos para um módulo de memória para compreender uma capacitância elétrica tal que a duração de validade associada com os dados de autenticação pessoais é introduzida pela descarga da capacitância elétrica fornecido na módulo de memória.

Em particular mais ainda, um módulo de memória pode compreender uma memória volátil armazenando os dados de autenticação pessoais e temporariamente energizado pela mencionada capacitância elétrica.

De acordo com ainda uma outra modalidade, um módulo de memória pode compreender uma memória volátil que é continuamente energizada durante o controle da execução da função protegida ou uma memória de re-escrita, a qual memória armazena os dados de autenticação pessoais. Neste caso, um módulo de memória é configurado para associar uma duração de validade com aqueles dados de autenticação pessoais armazenando uma quantidade temporal em uma variável que é associada em memória com aqueles mesmos dados de autenticação pessoais.

A invenção também envolve uma entidade eletrônica caracterizada pelo fato de compreender:

- pelo menos uma interface de comunicação para receber

dados pessoais introduzidos por um usuário e uma mensagem para processar,

- uma memória que armazena, em uma estrutura de validade limitada de dados, dados de autenticação pessoais que são dependentes nos dados pessoais de entrada,

5 - uns meios para limitar, no tempo ou espaço, a validade da estrutura de dados armazenando os dados de autenticação pessoais, e

- uns meios para verificar a validade da estrutura de validade limitada antes de usar os dados de autenticação pessoais que ela contém para gerar uma autorização ou uma recusa para executar uma função protegida por autenticação e implementada no processamento da mensagem recebida.

10 Em particular, a entidade pode ser tio cartão de microprocessador.

A entidade eletrônica tem similares vantagens àquelas do método, do módulo de memória e do sistema estabelecidos acima.

15 Opcionalmente, a entidade eletrônica pode compreender meios relacionados aos recursos do método estabelecido acima, e em particular meios para implementar uma duração de validade, tal como uma capacitância elétrica ou uma variável em memória, e uma memória se volátil ou não.

### BREVE DESCRIÇÃO DOS DESENHOS

20 Outras particularidades e vantagens da invenção vão aparecer na seguinte descrição, ilustrada pelos desenhos anexos, nos quais:

- Figura 1 ilustra mecanismos convencionais para autenticação de um usuário U para acessar um recurso;

- Figura 2 é um diagrama de uma implementação da invenção;

25 e - Figuras 3 à 5 ilustra três exemplos de acesso a um serviço de assinatura digital protegido por uma autenticação de acordo com a invenção.

### DESCRIÇÃO DETALHADA DA INVENÇÃO

A Figura 1 ilustra mecanismos convencionais para acesso a

uns recursos por um usuário U, por exemplo, para acessar um serviço de pagamento em uma loja de varejo.

Essas operações requerem a interação entre um usuário U e um terminal de pagamento 10. Esta interação consiste em particular na entrada de dados pessoais para identificar ou autenticar que são confiáveis a possíveis ataques, usando um teclado ou qualquer outro tipo de meios de entrada 11. Por meio de ilustração, esses dados pessoais confiáveis podem ser uma senha, um número de PIN (PIN significa “*Número de Identificação Pessoal*”) ou dados biométricos possibilitando uma pessoa para autenticar a sinal próprio e para possibilitar uma transação financeira com o varejista a ser feita.

Outros dados não confiáveis também podem ser introduzidos naquele momento, por exemplo, um total indicado pelo usuário para a transação financeira com o varejista.

Uma mensagem solicitando uma transação financeira e caracterizada pelo fato de compreender aqueles dados de entrada, é então fornecida a uma aplicação de software 12.

Uma mensagem compreende em particular um comando para a transação financeira.

A execução daquele comando depende em particular na presença de direitos necessários específicos para aquele comando, neste caso uma autenticação válida produzido pela validação dos dados pessoais de entrada.

Usando mecanismos convencionais e geralmente através de comparação com dados pré-gravados, o software 12 verifica os dados pessoais introduzidos pelo usuário para gerar uma autorização ou recusa para executar a transação financeira. Por exemplo, a entrada de PIN por um usuário U pode ser comparado para um PIN armazenado em um cartão de pagamento inserido no terminal de pagamento 10.

Em caso de autenticação positivo, a execução do comando de

transação financeira é autorizada possibilitando o acesso para o serviço de pagamento S. Trocas com um servidor (simbolizado aqui pela rede 20 e o servidor 21) são então conduzidos.

No caso de autenticação negativa, a transação financeira não pode ser realizada.

Neste contexto, ataques por quem intercepta utiliza uma aplicação de software maliciosa 13 como representado diagramaticamente na figura. O software malicioso 13 intercepta os dados de entrada, se eles são ou não confiáveis, copiá-los e transferi-los para o software 12. A intervenção do software malicioso 13 é assim sendo transparente para o usuário e para o software 12.

A Figura 2 é um diagrama de um sistema 1 implementando a invenção de acordo com uma modalidade. O usuário U precisa fazer as mesmas entradas (de dados confidenciais e possivelmente de dados não confiáveis) como convencionalmente para o uso de comandos protegidos por direitos relativos a uma autenticação.

No sistema da Figura 2, o usuário U interage com um primeiro dispositivo de entrada 100. Este dispositivo é preferencialmente um dispositivo confiável, isto é para dizer um dispositivo do próprio usuário U, por exemplo. seu telefone móvel ou seu computador.

O dispositivo de entrada 100 compreende uma interface de entrada 110, um cartão de microprocessador seguro 120 e um leitor de cartão de microprocessador embutido 130. Outras funcionalidades convencionais de um telefone móvel pode ser fornecidas no dispositivo de entrada 100, sem elas sendo descritas aqui contudo. Em particular meios internos para alimentar de energia o dispositivo 100 (uma bateria, por exemplo) como fonte elétrica principal possibilita o cartão de microprocessador 120 a ser energizado.

A interface de entrada 110 pode tomar a forma de um teclado

de telefone convencional, por exemplo, para os propósitos de introduzir um código de PIN ou uma senha. Como uma variante ou em combinação, ele pode compreender um sensor biométrico adaptado para adquirir dados biométricos específicos para o usuário U, ou qualquer outra interface.

5                   O leitor embutido 130 pode igualmente ser sem contato ou com contato para ler de e/ou escrever para o cartão de microprocessador 120. Ele é ligado à interface de entrada 110 via uma arquitetura de sistema eletrônico convencional, por exemplo via um cabo de múltiplas vias de comunicação de dados e um microprocessador (não mostrado).

10                   O cartão de microprocessador ou “*cartão inteligente*” 120 é preferencialmente um cartão pessoal removível para o usuário U, por exemplo em formato de ID-1, que o usuário pode facilmente extrair do dispositivo de entrada 100 para apresentá-lo a um outro leitor de cartão de microprocessador 210 de um dispositivo de processamento 200, conforme descrito abaixo.

15                   Como uma variante, o cartão de microprocessador 120 pode ser fisicamente anexado ao dispositivo de entrada 100 durante a totalidade das operações para acesso aos recursos S, isto é para dizer durante a entrada, o controle do comando de acesso protegido por uma autenticação e a trocas durante o acesso.

20                   Em ambos esses casos, e em particular quando é fisicamente anexado o dispositivo de entrada 100, a cartão de microprocessador 120 pode ser substituído por um mais simples módulo de memória fornecido com uma memória e a micro-controlador ou processador, para a implementação das operações de acordo com a invenção. A memória pode ser volátil ou não

25                   como explicado abaixo.

                  O cartão de microprocessador 120 compreende uma interface sem contato 1201 para comunicação com o leitor sem contato 130 do dispositivo. O cartão de microprocessador 120 também compreende uma interface sem contato 1202 para comunicação com leitor sem contato 210 do

dispositivo de processamento 200. Em particular, essas duas interfaces são combinadas em uma interface única. Eles podem contudo ser distinto, por exemplo um sendo com contato e o outro sem contato.

Conforme será visto mais tarde, eles possibilitam o cartão de microprocessador a receber os dados introduzidos pelo usuário no dispositivo de entrada 100 e para receber uma mensagem pelo respectivo usuário, o processamento daquela mensagem em particular implementando o comando de acesso protegido por autenticação, ou porque ele o contém diretamente, ou porque chama tal comando que é interno para o cartão de microprocessador.

O cartão de microprocessador 120 também compreende uma memória 1203 possibilitando uma estrutura de dados STRUCT a ser armazenada conforme descrito abaixo, assim como meios 1204 tornando possível definir um parâmetro de validade para a mencionada estrutura, por exemplo uma duração de validade DV ou uma zona geográfica de validade. Para as seguintes explicações, referência principalmente será feita para uma duração de validade. Similares mecanismos àqueles descritos abaixo podem contudo ser implementados para uma validade geográfica.

O cartão de microprocessador 120 é configurado para gerar e armazenar, em sua memória 1203, quando ele está conectado ao dispositivo de entrada 100, dados de autenticação pessoais de validade limitada que são dependentes da entrada de dados pessoais pelo usuário e para associá-los com uma duração de validade, por exemplo via a mencionada estrutura.

Conforme descrito abaixo através de diferentes exemplos, os meios 1204 podem definir tal uma duração de validade DV explicitamente ou implicitamente dependendo das propriedades da arquitetura que é adotada.

A duração de validade DV é associada com a estrutura STRUCT para, por conseguinte, definir um limite temporal de validade.

Esta duração é dependente de um nível de desejado de segurança, que varia de uma aplicação para uma outra. À título de exemplo,

para um comando de transação financeira protegida tornado seguro através de código de PIN, a qual duração pode ser configurada em umas poucas dezenas de segundo, por exemplo 1 à 2 minutos. Para um comando para acesso seguro para um computador ou rede de comunicação, este pode ser mais longo, da ordem de uns poucos minutos, por exemplo 5, 10 ou 15 minutos.

Em uma modalidade, a memória 1203 é uma memória volátil.

A memória 1203 pode então ser continuamente energizada por uma fonte de energia principal (bateria do dispositivo 100), em particular quando o cartão 120 não é extraído a partir do dispositivo de entrada 100 para o todo das operações de acesso ao recurso. Neste caso, os meios 1204 podem consistir de uma variável na memória definindo a duração de validade DV da estrutura de dados STRUCT iniciando a partir de sua geração (que é para dizer, a partir de sua criação e/ou a partir de sua atualização), conforme descrito abaixo, ou definindo um tempo final de validade, ou um tempo de início de validade se a duração a partir daquele tempo é pré-fixado.

Se o cartão 120 é configurado para ser extraído do dispositivo de entrada 100 a ser apresentado para o dispositivo de processamento 200, uma memória volátil 1203 pode, quando a fonte de energia principal tiver sido desconectada, ser temporariamente energizado através de uma fonte interna com evanescimento de eletricidade, por exemplo uma capacitância elétrica carregada a partir da fonte de energia principal quando o cartão 120 está na posição no dispositivo de entrada 100.

A fonte interna com evanescimento coloca-se com meios 1204 já que ela é capaz de manter o fornecimento de energia da memória volátil (que esvazia quando toda a energia foi cortada) para a duração que depende de suas propriedades (em particular o valor de sua capacitância).

Em particular, no caso de uma capacitância elétrica, o valor da capacitância é escolhido nas bases da duração de validade DV desejada. No caso de total descarga da capacitância, a estrutura de dados STRUCT presente

na memória 1203 é então automaticamente apagada. Mecanismos para controlar carga e descarga da capacitância tornam possível fornecer uma contagem regressiva da duração de validade iniciando de um tempo preciso desejado, em particular quando o cartão 120 é extraído do dispositivo de entrada 100 ou quando a estrutura de dados STRUCT é gerada, e possivelmente continua a contagem regressiva quando o cartão 120 é de novo energizado pelo dispositivo de processamento 200.

Por exemplo, comandos para controlar a capacitância pode ser fornecida e usada pelo cartão 120 para controlar aquela duração de validade DV. Em particular, um comando de carga pode ser fornecido para carregar a capacitância e implicitamente o acionamento do início da contagem regressiva de DV no final da carga, um comando de descarga pode ser fornecido para descarregar a capacitância a fim de forçar um estado de invalidade para a estrutura de dados STRUCT, e um comando de nível de descarga de modo a conhecer o nível de carga da capacitância e assim sendo diretamente determinar se a duração DV expirou ou não.

Este caso geralmente pode se aplicar a qualquer memória adaptada para preservar dados somente por um tempo determinado (que implicitamente define uma duração de validade DV).

Em um outro exemplo, uma memória volátil 1203 escolhida pode ter propriedades de evanescimento (em particular uma duração de evanescimento) que são compatíveis com a duração de validade DV desejada. Neste caso, os meios 1204 são formados por aquelas propriedades de evanescimento, já que quando do corte da energia para a memória 1203 (em particular na extração do cartão 120 ou em um comando para terminar o fornecimento de energia para a memória), a estrutura de dados STRUCT permanece na memória 1203 até expirar a duração de evanescimento. Controles que possibilitam o fornecimento de energia e término do fornecimento de energia para aquela memória são fornecidos nesta conexão.

Em uma outra modalidade, a memória 1203 é uma memória de re-escrita, no qual caso os meios 1204 podem consistir de uma variável na memória definindo um item de informação temporal, por exemplo a duração de validade DV da estrutura de dados STRUCT a partir de sua criação ou  
 5 atualização, um data e hora do fim da validade, ou uma data e hora do início da validade se uma duração pré-fixada é acordada antecipadamente. Como uma variante, mesmo se uma memória é passível de ser re-escrita, os meios 1204 podem ser formados usando uma fonte interna com evanescimento (por exemplo, uma capacitância elétrica) que é dedicada para os mesmos,  
 10 carregados pela fonte de energia principal, e que se descarregam a partir do fim da carga na sequência de recepção de um comando de carga. Neste caso, enquanto a capacitância elétrica não está totalmente descarregada, a estrutura STRUCT é considerada como válida.

No particular caso de uma validade geográfica (que pode mais  
 15 ainda ser fornecida como um complemento de uma validade temporal conforme descrito acima), uma zona de validade pode ser definida em torno de um ponto inicial, por exemplo a localização do cartão 120 no momento em que a estrutura STRUCT foi criada. Esta permanece válida dentro daquela zona. Em particular meios adaptados podem ser fornecidos para  
 20 definitivamente apagar a estrutura (ou torná-la definitivamente inválida) assim que uma saída daquela zona ocorra. Como uma variante, qualquer retorno na zona após a saída pode de novo tornar a estrutura válida.

Os meios adaptados pode combinar um receptor do GPS capaz de computar distâncias relativas ao ponto inicial, uma distância limite  
 25 delimitando a zona (por exemplo um raio), e uma memória fornecida com meios para apagar assim que a distância correspondendo excede a distância limite.

Como indicado anteriormente, uma implementação da invenção consiste, para o usuário U, de introduzir dados pessoais para

identificação ou autenticação, isto é para dizer, dados pessoais confiáveis D1, por meio do dispositivo de entrada 100. Como um complemento, o usuário U pode também introduzir outros dados (possivelmente não confiáveis) que são necessários para o acesso e/ou para efetuar o serviço S que o usuário deseja ter acesso, por exemplo o total de uma transação financeira, o nome de um arquivo para recuperar, uma data, etc.

Esta ação de entrada conduz a atualização dos dados ou um estado que são internos para o cartão de microprocessador 120, em uma estrutura de dados STRUCT que pode ser criada naquele momento. A duração de validade é então associada com ele naquele momento, usando um dos meios referidos anteriormente.

A estrutura de dados STRUCT pode, sem ser limitado a ela, se um arquivo eletrônico simples, uma lista, uma árvore, um gráfico, um banco de dados, etc.

Como será visto nos seguintes exemplos, a estrutura de dados STRUCT pode diretamente armazenar, como dados de autenticação pessoais D2, os dados pessoais introduzidos pelo usuário U, sem qualquer processamento sendo realizado naqueles dados.

Como uma variante, o dispositivo de entrada 100 pode efetuar pré-processamento dos mesmos para produzir outros dados de autenticação pessoais D2 dependentes daqueles dados pessoais de entrada. À título de exemplo, a verificação de um código de PIN introduzido pelo usuário U é feita pelo terminal de entrada 100, aqui o telefone móvel do usuário U, e um item de informação representando o resultado de sua comparação com um código de referência de PIN (e não o próprio código de PIN introduzido) é armazenado em na estrutura de dados STRUCT (possivelmente com outros dados necessários para efetuar o serviço S desejado). Este resultado, por exemplo um único bit ou uma função Booleana, é um resultado de autenticação do usuário.

Dentro do cartão 120, a estrutura de dados STRUCT é segura. Mais particularmente, em uma maneira convencional o cartão 120 implementa numerosos mecanismos possibilitando a confidencia dos dados que ele armazena ser assegurada.

5                    Uma vez que a estrutura de dados STRUCT foi criada e atualizada, o usuário U desconecta o cartão de microprocessador 120 a partir do dispositivo 100, o efeito disso é acionar a contagem regressiva de uma duração de validade DV se isto já não ocorreu (no caso de acionamento por exemplo a partir do término da carga da capacitância na seqüência de um  
10 comando de carga ou quando uma duração DV é armazenada via um item de informação temporal na memória).

                    O usuário U então conecta o cartão 120 para o dispositivo de processamento 200, por exemplo, introduzindo o cartão em uma localização fornecida para aquele propósito, equipado com um leitor de cartão. O efeito  
15 desta conexão é claro que não para a contagem regressiva de uma duração de validade. Em particular, no caso do uso de uma capacitância, esta contagem regressiva não é parada a não ser que um específico comando de carga seja requerido para ser emitido para recarregá-lo.

                    O dispositivo de processamento 200 é convencionalmente um  
20 dispositivo de baixa confiabilidade e não seguro, tipicamente uma estação/um terminal de pagamento de terceiros, uma caixa pagadora, um Internet serviço de Internet, etc.

                    Como representado na figura, o dispositivo de processamento 200 compreende o leitor 210 para um cartão de microprocessador (ou uma  
25 memória de acordo com o caso) que é compatível com a interface de comunicação 1202 do cartão 120, e compreende um módulo de processamento 220. O dispositivo de processamento 200 também compreende uma interface de usuário (não representado) possibilitando ao usuário interagir com o equipamento em particular para ter acesso a um recurso

desejado.

O processamento módulo 220 assim sendo controla as trocas com o cartão 120 para efetuar aquele acesso para o recurso desejado, e em particular envia para ele uma mensagem para acesso ao recurso. A mensagem  
5 pode compreender um comando C protegido por autenticação ou chamar uma função, rotina ou comando C, também protegido por autenticação, implementado no cartão 120.

Então é o cartão de microprocessador 120 que controla a execução do comando protegido, por autenticação do usuário U usando os  
10 dados de autenticação pessoais D2 que ele armazena na estrutura de validade limitada. Este controle torna possível autorizar ou não autorizar a execução do comando, função ou rotina protegida, e assim sendo o acesso ou não ao serviço S desejado. Abaixo, referência principalmente será feita a um “comando protegido” para designar aqueles comandos, funções ou rotinas que  
15 são protegidos por autenticação.

Dependendo da associada duração de validade DV, o cartão de microprocessador 120 é assim sendo configurado para usar, quando conectado ao dispositivo de processamento 200, os dados de autenticação pessoais D2 armazenados para gerar a autorização ou a recusa para executar o comando  
20 protegido que ele recebeu.

Nesta maneira, a estrutura de dados STRUCT serve como uma interface entre a entrada de dados confidenciais no dispositivo 100 e seu uso no momento do acesso para o serviço S usando o dispositivo 200.

A invenção também se aplica ao acesso para serviços/recursos  
25 locais para o dispositivo de processamento 200 (por exemplo., uma funcionalidade daquele dispositivo ou dos dados que ele armazena), sem requerer acesso via uma rede de computador 20 com representado na figura.

No momento do controle da execução do comando protegido por autenticação do usuário, o cartão de microprocessador 120 leva em conta

a duração de validade DV associada com a estrutura STRUCT para usar ou não usar os dados de autenticação pessoais D2 que ela contém.

Assim sendo, quando o usuário gera, no dispositivo de processamento 200, o comando C/C para acesso protegido a um serviço requerendo envolvimento do cartão 120 para verificar os direitos demandados, a validade da estrutura STRUCT é primeiro de tudo verificada pelo cartão na recepção do comando.

Se a duração de validade é explícita (indicação do fim do tempo da validade, por exemplo), o cartão 120 verifica que a duração não expirou, em particular usando o relógio do dispositivo de processamento.

Se está implícito (por exemplo, uso de uma capacitância elétrica), o cartão 120 verifica se a capacitância está totalmente descarregada ou não. Isto pode ser realizado, por exemplo, usando um comando de nível de carga de capacitância, ou pode ser obtida tentando ter acesso à estrutura de dados STRUCT na memória volátil se a última é energizada pela capacitância ou se as propriedades de remanência são usadas. Mais particularmente, nesses casos, se a capacitância é totalmente descarregada ou a duração de remanência expirou, a estrutura de dados é apagada.

No caso de validade da estrutura de dados STRUCT, os dados de autenticação pessoais D2 são acessados, possibilitando ao cartão 120 verificar os direitos demandados, por exemplo, se ou não o código de PIN introduzido é ou não correto. A verificação dos direitos gera uma autorização ou recusa para executar o comando protegido em questão, e assim sendo de acessar o serviço desejado ou não.

O controle de acordo com a invenção assim sendo permite acesso seguro a ser obtido para um grande número de serviços fornecidos pelo dispositivo de processamento 200, via o cartão 120: transação financeira, assinatura digital, consulta de contas, acesso aos dados, etc., enquanto evitando exploração fraudulenta de dados confidenciais introduzidos por um

usuário.

Os dispositivos de entrada 100 e de processamento 200, assim como o cartão de microprocessador 120, compreendem meios de hardware e software configurados para implementar as diferentes etapas e operações aqui descritas.

Abaixo, exemplos serão referidos nos quais a execução de um comando C diretamente indicado na mensagem fornecida pelo dispositivo de processamento é dependente da autenticação bem sucedida do usuário usando os dados de autenticação pessoais contidos na estrutura de validade limitada STRUCT.

Contudo, conforme mencionado acima, um comando, função ou rotina protegida por autenticação pode ser implementada ao processar a mensagem, sem estar explicitamente indicado na mensagem.

Mais ainda pode ser notado que a invenção não é afetada se os dados de autenticação pessoais armazenados na estrutura STRUCT influenciam ou não o resultado fornecido pelo cartão 120 em resposta ao comando C. À título de exemplo, a resposta ao comando C pode ser o valor dos dados de autenticação pessoais armazenados (por exemplo o resultado da autenticação armazenado é produzido). Em um outro exemplo, o valor produzido pode depender do valor dos dados de autenticação pessoais (por exemplo, se um sub-comando C dentre vários não é executado, o resultado pode mudar). Por fim, em um outro exemplo, o resultado produzido é independente de se o comando protegido pela autenticação supra citada é ou não executado (por exemplo, a execução daquele comando permite um indicador interno do cartão 120 a ser atualizado).

Figura 3 ilustra um primeiro exemplo de acesso a um serviço de assinatura digital de acordo com a invenção.

Neste exemplo, o cartão 120 que armazena a estrutura STRUCT é removível. Ainda mais, os meios 1204 são implementados via

uma capacitância elétrica fornecida no cartão 120 para temporariamente alimentar de energia a memória volátil 1203. Ainda mais, os dados D1 introduzidos pelo usuário U são pré-processados no dispositivo de entrada 100 antes da armazenagem do resultado na estrutura STRUCT. Assim sendo, em uma primeira fase P1 começando na etapa E300, o cartão de microprocessador removível (ou módulo de memória) 120 é inserido no dispositivo de entrada 100, aqui o telefone móvel do usuário.

Esta inserção acarreta um sinal de alimentação de energia E302, acionamento da alimentação de energia do cartão de microprocessador 120 e sua iniciação E304 de acordo com mecanismos convencionais. Neste estágio, o microprocessador (não representado) e a memória 1203 do cartão 120 são alimentados de energia por uma fonte de fornecimento de energia principal (a bateria do telefone por exemplo).

Para o propósito da implementação de um serviço S desejado pelo usuário U, o usuário seleciona uma aplicação de pré-processamento via um menu e a interface 110, para o acesso ao serviço (E306).

Um comando para selecionar a aplicação é então gerado (E308) pelo dispositivo de entrada 100 destinado ao cartão 120. Este comando de seleção “Select” é de acordo com o padrão da ISO/IEC 7816-4 p para comunicação entre um cartão de microprocessador 120 e um leitor de cartão 130 (aqui equipando o dispositivo 100).

A aplicação selecionada é então executada (E310) no cartão 120, requerendo a entrada de um item de dados pessoais D1 para identificação ou autenticação do usuário U e possivelmente dados complementares necessários para o serviço desejado. No exemplo, o usuário U introduz, via a interface 110, seu código de PIN (E312).

Um comando de verificação do código de PIN “VERIFY PIN” de acordo com o padrão ISO/IEC 7816-4 supracitado é então fornecido (E314) para o cartão 120. Este comando compreende o código de PIN

introduzido pelo usuário U.

Em uma maneira convencional, o cartão 120 recupera o código de PIN introduzido, então o compara com um código de PIN de referência pré-gravado na memória segura do cartão 120 (E316) a fim de gerar uma resposta positiva OK no caso de PIN correto (E318) e uma resposta negativa NOK no caso de PIN errôneo (E320).

Em maneira paralela, o cartão 120 atualiza (cria se necessário) uma estrutura de dados STRUCT inserindo nele o resultado da comparação E316 (e possivelmente os dados complementares que foram recebidos), em uma etapa E322. Este resultado da comparação é, aqui, nomeado “dados de autenticação pessoais” D2 do usuário.

Na mesma ocasião, o cartão 120 fornece a duração de validade DV associada com a estrutura de dados e assim sendo com os dados de autenticação pessoais D2, enviando um comando para carregar a capacitância 1204. A duração DV é contada regressivamente por exemplo iniciando do fim da carga da capacitância elétrica 1204, até a progressiva descarga daquela capacitância.

Essas ações da etapa E322 podem, por exemplo, ser efetuadas por um programa de controle como a seguir:

```
if PIN OK{
  charge 1204;
  provide OK to STRUCT;
}
else{
  discharge 1204;
  provide NOK to STRUCT;
}
```

Em uma segunda fase P2, o usuário U termina o fornecimento de energia principal do cartão 120 pelo dispositivo de entrada 100, extraíndo o cartão 120 em particular, na etapa E324.

Em virtude da capacitância 1204 no decorrer da descarga, a memória volátil 1203 permanece temporariamente energizada e os dados (em particular STRUCT) que ela armazena são ainda válidos. Se o cartão 120 não

é re-usado antes da expiração de uma duração DV (assim sendo antes de completar a descarga da capacitância), a memória volátil e assim sendo a estrutura STRUCT são apagadas.

Na etapa E326, o cartão 120 é fisicamente movido em direção  
5 ao dispositivo de processamento 200 ao qual ele é então conectado.

A terceira fase P3 então começa pela etapa E328 de comandar a alimentação de energia do cartão (similar à E302), conduzindo a alimentação de energia e iniciação do cartão 120 (E330–similar à E304).

Um comando de destinação de seleção destinado ao cartão 120  
10 é então gerado (E332) em maneira similar para a etapa E308.

Na etapa E334, o usuário procura um serviço de código de PIN protegido (aqui a computação de uma assinatura digital) no dispositivo de processamento 200. Esta detecção aciona o envio de um comando C de “AUTENTICAÇÃO INTERNA” de acordo com o padrão da ISO/IEC 7816-4  
15 (etapa E336). Este comando é parametrizado com os dados para assinar e sua execução é, de acordo com o padrão, dependente da execução de comandos anteriores, por exemplo uma autenticação válida anterior como fornecida em um presente exemplo.

Em virtude da invenção, a condição de código de PIN validado  
20 (ou não validado como o caso pode ser) está presente na estrutura STRUCT do cartão 120 via dados de autenticação pessoais D2, sem o usuário U ter de introduzir seu código de PIN para o dispositivo de processamento 200.

Neste estágio, etapa E338 no cartão 120 consiste em verificar a validade da estrutura STRUCT, levando em consideração a duração de  
25 validade DV associada.

Esta verificação pode em particular consistir em verificar o nível de carga da capacitância 1204 (usando um comando apropriado) e/ou a presença da estrutura STRUCT na memória 1203. Para ser preciso, se a duração de validade expirou (a capacitância 1204 totalmente descarregou)

enquanto o cartão 120 não mai foi energizado, a memória volátil 1203 se tornou apagada e a condição de código de PIN validado não está mais disponível.

Se a duração DV expirou, a estrutura STRUCT pode ser marcada como inválida (por exemplo, via um bit) de modo a simplificar etapa E338 no momento das solicitações de acesso mais tarde.

Se a duração DV não expirou e assim sendo a estrutura STRUCT é de fato válida, na etapa E339, os dados de autenticação pessoais D2 são recuperados da estrutura STRUCT.

Na etapa E340, o comando C de “AUTENTICAÇÃO INTERNA” é executado levando em consideração os dados de autenticação pessoais D2 recuperados, como direitos requeridos. Assim sendo é executado exclusivamente se aqueles dados D2 revelam uma condição de código de PIN validado.

Por exemplo, uma particular função COPY D2 pode ser executada pelo cartão nesta etapa para copiar os dados D2 em um variável global convencionalmente usada para armazenar o resultado de um autenticação de PIN e que é acessada pela execução do comando de AUTENTICAÇÃO INTERNA. Assim sendo, ela não é modificada.

É claro que, como uma variante, uma função de VALIDATE PIN OK pode ser chamada para diretamente verificar se uma condição de código de PIN validado está de fato presente, e naquele caso diretamente autoriza a execução do comando de AUTENTICAÇÃO INTERNA.

No caso de uma condição de código de PIN validado, a assinatura dos dados a assinar, usando uma chave que é interna ao cartão 120, é realizada.

Devido a isto, a assinatura digital de dados (ou o acesso aos recursos/serviços) é protegida por uma verificação dos dados D2 positiva.

O cartão 120 então envia, para o dispositivo de processamento

200, uma resposta ao comando: os dados assinados (E342) ou uma mensagem de erro (E344) dependendo se foi possível executar o comando ou não.

A Figura 4 ilustra um segundo exemplo de acesso a um serviço de assinatura digital de acordo com a invenção e que é substancialmente similar àquele da Figura 3, além do fato que os dados pessoais D1 como introduzidos pelo usuário U são diretamente armazenados (sem modificação) na estrutura STRUCT.

Ainda mais, em vez de introduzir o código de PIN, este exemplo implementa a aquisição de uma medição biométrica do usuário U, por exemplo um impressão digital de dedo.

Na fase P1, as etapas E300 à E312 são similares àquelas descritas com referência à Figura 3, além do fato que o usuário U é solicitado a adquirir uma impressão digital de dedo mais propriamente do que um código de PIN.

Na etapa E312 consistindo em introduzir os dados confidenciais D1 pelo usuário U, os últimos presentes em um dedo para o sensor biométrico 110 a fim de adquirir os dados pessoais D1 para identificar quais representam a impressão digital de dedo.

Esses dados confidenciais D1 são fornecidos para o cartão 120 através de um comando de "PUT DATA" de acordo com o padrão da ISO/IEC 7816-4 (etapa E314').

No cartão 120, esses dados D1 são recuperados e então armazenados diretamente na estrutura de dados STRUCT (etapa E322').

É claro que dados complementares podem ser introduzidos/adquiridos pelo usuário U e armazenados em adição na estrutura STRUCT.

Neste estágio, a contagem regressiva de uma duração de validade DV pode ser acionada, pelo comando para carregara a capacitância 1204.

Adicionalmente a fase P1, fase P2 é similar aquela da Figura 3, i.e. compreendendo as etapas E324 e E326.

Fase P3 começa na mesma maneira que a mesma fase da Figura 3, com as etapas E328 à E332 em particular.

5 O dispositivo de processamento 200 pode ser configurado para enviar, na detecção do cartão 120, um comando para processar os dados D1 armazenados na estrutura STRUCT (etapa E336), no exemplo um comando para verificar a impressão digital de dedo com uma impressão digital de dedo de referência pré-gravada na memória do cartão 120.

10 É para ser notado que esta verificação pode ser realizada no cartão 120 em resposta ao comando C protegido conforme fornecido abaixo, sem ter de recorrer a este comando E336 anterior.

Na etapa E338, a validade da estrutura STRUCT é verificada com relação à duração DV associada.

15 Se a estrutura não é mais válida, é indicado como tal e uma resposta negativa NOK (E344) é enviada de volta para o dispositivo de processamento 200.

Se a estrutura é válida, os dados D1 são recuperados a partir da estrutura STRUCT na etapa E339.

20 As impressões digitais de dedo D1 adquiridas na fase P1 são então comparada (E340) com as impressões digitais de dedo de referência.

O resultado da comparação, correto OK (E342) ou incorreto NOK (E344), é retornado para o dispositivo de processamento 200.

25 Em paralelo, o resultado da comparação é armazenado em uma variável global (do cartão), convencionalmente usado para armazenar o resultado de uma autenticação por dados biométricos, e acessado pela execução mais tarde de um comando protegido tal como AUTENTICAÇÃO INTERNA.

Como uma variante, este resultado pode ser diretamente

armazenado em uma estrutura de dados STRUCT com condição de dados biométricos válida ou errônea.

Na etapa E346 o dispositivo de processamento 200 detecta que o usuário U está procurando um serviço (aqui a computação de uma assinatura digital) protegido por autenticação biométrica e assim sendo requerendo autenticação do usuário. Esta solicitação de serviço aciona o envio de um comando C de “AUTENTICAÇÃO INTERNA” de acordo com o padrão ISO/IEC 7816-4 (etapa E348), tendo como parâmetro os dados a assinar e sendo protegida por autenticação do usuário.

O cartão 120 então executa (E350) o comando C de “AUTENTICAÇÃO INTERNA”.

É para ser notado que se na etapa E340 o resultado da comparação é armazenado na variável global convencional, etapa E350 é ainda convencional, o comando AUTENTICAÇÃO INTERNA sendo condicional na presença de uma condição validada naquela variável global.

No caso da variante, uma função VALIDATE DATA OK pode ser executada para verificar na estrutura STRUCT a presença ou ausência da condição validada, e conseqüentemente autoriza ou não autoriza o comando AUTENTICAÇÃO INTERNA.

Onde apropriado os dados a assinar são assinados usando uma chave interna do cartão 120, de acordo com mecanismos convencionais.

O cartão então envia uma resposta para o comando de AUTENTICAÇÃO INTERNA, destinado ao dispositivo de processamento: os dados assinados (E352) ou uma mensagem de erro (E354).

Uma vez de novo, a assinatura digital dos dados (ou o acesso aos recursos/serviços) é protegida por uma verificação positiva dos dados biométricos.

Figura 5 ilustra um terceiro exemplo de assinatura digital de acordo com a invenção substancialmente similar àquele da Figura 3, no qual o

cartão 120 armazenando a estrutura STRUCT é permanentemente acomodado no dispositivo de entrada 100 (pelo menos durante a totalidade das operações descritas abaixo correspondendo ao todo do processo de autenticação do usuário U). Isto é, por exemplo, o caso para um cartão SIM em um telefone móvel.

Neste caso, as etapas E300 à E322 da fase P1 são idênticas as etapas da fase P1 da Figura 3.

Como para a fase P2, que está vazia já que não há dissociação física entre o cartão 120 e o equipamento 100. Esta fase P2 assim sendo começa assim que os dados pessoais de entrada para identificação D1 foram processados pelo cartão 120 sob o comando do dispositivo de entrada 100, isto é para dizer assim que as estruturas de dados STRUCT foram geradas com os dados D2 resultando do processamento. De forma similar, contagem regressiva da duração de validade começa a partir do final deste processamento, através da carga da capacitância 1204 por exemplo.

Durante a fase P3, o grupo {dispositivo de entrada 100—cartão 120} se comunica com o dispositivo de processamento 200, por exemplo, com a ajuda de um protocolo de comunicação sem contato (NFC ou equivalente).

É para ser notado que de acordo com uma modalidade, o dispositivo de processamento 200 pode diretamente se comunicar com o cartão 120. Isto é o caso no exemplo da Figura 2, onde a interface de comunicação 1202 possibilita comunicação direta com o equipamento 200. É para ser notado que se duas interfaces de comunicação 1201 e 1202 estão unidas, são fornecidas para desativar o leitor 130 do dispositivo de entrada 100 de modo a possibilitar comunicação do cartão 120 com dispositivo de processamento 200 sem interferência. Por outro lado, meios para diferenciar as comunicações com cada uma das interfaces 1201 e 1202 podem ser fornecidos.

Em uma variante, o dispositivo de processamento 200 pode se comunicar com o dispositivo de entrada 100 que então supre a informação e solicitações para o cartão 120. Neste caso o cartão 120 pode ser equipado com um único interface 1201 para comunicação com o leitor 130.

5                    Figura 5 ilustra fase P3 no caso no qual o dispositivo de processamento 200 se comunica diretamente com o cartão 120.

A iniciação da comunicação entre essas duas entidades é realizada durante trocas de mensagens convencionais, representada na figura pela etapa E330'.

10                    Seguindo as etapas E332 à E344 são similares as etapas comportando as mesmas referências da Figura 3.

É claro que, as diferentes modalidades referidas antes acima para os três exemplos da Figuras 3 à 5 podem ser aplicadas à cada um daqueles exemplos, por exemplo para modificar os meios 1204, a natureza da memória 1203, a interfaces de comunicação 1201 e 1202, para substituir o  
15                    cartão de microprocessador 120 por uma módulo de memória fornecido com um micro-controlador possibilitando comunicação com os leitores 30 e 210, etc.

Os exemplos precedentes são somente modalidades da  
20                    invenção que não é limitado a isto.

Em particular, embora a invenção tenha sido ilustrada acima para o acesso a um serviço de assinatura digital, ela pode igualmente ser aplicada ao acesso para dados armazenados ou para outros recursos.

Por exemplo, dados pessoais (biométricos, fotográficos ou de  
25                    identificação) são armazenados em uma passaporte eletrônico mas que é acessível de modo único, após autenticação. Usando um telefone móvel, o usuário pode pré-autorizar o acesso àqueles dados introduzindo um código de PIN gerando uma a estrutura de validade limitada STRUCT com a condição do código de PIN validado/errôneo, através do mecanismos de acordo com a

invenção.

O oficial da alfândega pode assim sendo acessar os dados pessoais em virtude desta pré-autorização durante uma duração de validade DV.

## REIVINDICAÇÕES

1. Método para controlar a execução de uma função protegida por autenticação, caracterizado pelo fato de compreender as seguintes etapas:

- armazenar, em uma estrutura de validade limitada, dados de autenticação pessoais dependentes dos dados pessoais de entrada, introduzindo os últimos por um usuário em um dispositivo de entrada;
- verificar a validade da estrutura de validade limitada antes de usar os dados de autenticação pessoais que ela contém para gerar uma autorização ou uma recusa para executar uma função implementada no processamento de uma mensagem gerada por um dispositivo de processamento que é distinto do dispositivo de entrada.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de compreender as seguintes etapas:

- introduzir, pelo usuário, os dados pessoais usando o dispositivo de entrada;
  - autenticar o usuário nas bases dos dados pessoais de entrada para gerar a autorização ou a recusa para executar a função protegida;
  - executar uma função no caso de autorização;
- em que:
- as etapas de armazenar e verificar são implementadas em um módulo de memória respectivamente conectado ao dispositivo de entrada no momento das etapas de entrada e armazenamento, e ao dispositivo de processamento no momento das etapas de verificação e execução;
  - a mencionada estrutura de validade limitada compreende dados de autenticação pessoais de validade limitada por associação de uma duração de validade com os dados de autenticação pessoais.

3. Método de acordo com a reivindicação 1, caracterizado pelo fato de que gerar a autorização ou a recusa é dependente de uma verificação dos dados pessoais introduzidos com dados de referência, o resultado da

verificação sendo obtido usando os mencionados dados de autenticação pessoais armazenados na estrutura de validade limitada armazenada.

4. Método de acordo com a reivindicação 2, caracterizado pelo fato de compreender uma etapa de comparar dados pessoais de entrada com dados pessoais pré-gravados no módulo de memória, e os dados de autenticação pessoais armazenados na estrutura de validade limitada compreende o resultado da comparação.

5. Método de acordo com reivindicação 1, caracterizado pelo fato de que os dados de autenticação pessoais armazenados na estrutura de validade limitada compreende os dados pessoais de entrada, e seu uso compreende uma sub-etapa de comparar os dados de autenticação pessoais armazenados na estrutura de validade limitada com dados pessoais pré-gravados.

6. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a mencionada estrutura de validade limitada compreende dados de autenticação pessoais de validade limitada através de associação de uma duração de validade com os dados de autenticação pessoais, e

- a duração de validade associada com os dados de autenticação pessoais é contabilizada através da descarga de uma capacitância elétrica.

7. Método de acordo com a reivindicação 6, caracterizado pelo fato de que os dados de autenticação pessoais são armazenados em uma memória volátil, temporariamente energizada pela mencionada capacitância elétrica.

8. Método de acordo com a reivindicação 1, caracterizado pelo fato de que os dados de autenticação pessoais são armazenados em uma memória volátil de um módulo de memória, que é continuamente energizado durante o controle da execução da função protegida ou em uma memória de re-escrita, e uma duração de validade associada com eles é definida

armazenando uma quantidade temporal em uma variável que é associada na memória com os dados de autenticação pessoais.

9. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a função protegida é um comando implementado, na recepção de uma mensagem proveniente do dispositivo de processamento, através de um módulo de microprocessador armazenando a estrutura de validade limitada.

10. Método de acordo com a reivindicação 1, caracterizado pelo fato de que um módulo de memória armazenando a estrutura de validade limitada e os dados de autenticação pessoais que ela contém são removidos, e são colocados no dispositivo de entrada no momento da entrada e colocados no dispositivo de processamento no momento da verificação da validade da estrutura e no momento do uso dos dados de autenticação pessoais de validade limitada.

11. Método de acordo com a reivindicação 1, caracterizado pelo fato de que um módulo de memória armazenando a estrutura de validade limitada e os dados de autenticação pessoais que ela contém é fisicamente ligada com ao equipamento de entrada durante o controle e execução da função protegida, e o equipamento de processamento se comunica com um módulo de memória através de comunicação sem contato.

12. Método de acordo com a reivindicação 10 ou 11, caracterizado pelo fato de que um módulo de memória armazenando a estrutura de validade limitada e os dados de autenticação pessoais é um cartão de microprocessador seguro.

13. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o processamento da mensagem a partir do dispositivo de processamento gera uma resposta caracterizada pelo fato de compreender pelo menos um valor de resposta que depende da autorização ou da recusa gerada.

14. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o dispositivo de entrada é um telefone móvel do usuário.

15. Módulo de memória, caracterizado pelo fato de compreender pelo menos uma memória e um processador para executar instruções, o módulo de memória sendo configurado para:

5 - armazenar, em uma estrutura de validade limitada, dados de autenticação pessoais que são dependente dos dados pessoais introduzidos por um usuário e recebidos de um dispositivo de entrada para o qual o módulo de memória está ligado;

10 - verificar a validade da estrutura de validade limitada antes de usar os dados de autenticação pessoais que ela contém gerar uma autorização ou uma recusa para executar uma função protegida por autenticação e implementada no processamento de uma mensagem recebida a partir de um dispositivo de processamento que é distinto do dispositivo de entrada.

15 16. Sistema para controlar a execução de uma função protegida por autenticação de um usuário, caracterizado pelo fato de compreender:

- um dispositivo de entrada para introduzir dados pessoais pelo usuário;

20 - um dispositivo de processamento que é distinto do dispositivo de entrada e adaptado para gerar, sob a ação do usuário, uma mensagem para processar;

25 - um módulo de memória compreendendo pelo menos uma memória e um processador, e que é configurado para autenticar o usuário nas bases dos dados pessoais de entrada a fim de gerar uma autorização ou uma recusa para executar uma função protegida implementada no processamento da mencionada mensagem;

em que o módulo de memória é configurado para:

- quando ele está conectado ao dispositivo de entrada, gerar e armazenar, em sua memória, dados de autenticação pessoais de validade limitada que são dependentes dos dados pessoais de entrada e associando-os

com um parâmetro de validade; e

- quando ele está conectado ao dispositivo de processamento, usando os dados de autenticação pessoais armazenados para gerar a autorização ou a recusa para executar a função dependendo do parâmetro de validade associado.

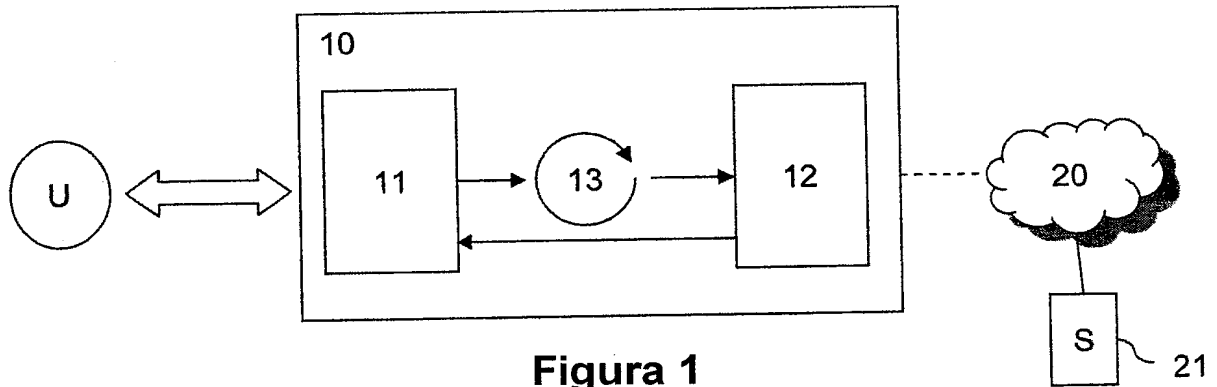
17. Entidade eletrônica, caracterizada pelo fato de compreender:

- pelo menos uma interface de comunicação para receber dados pessoais de entrada por um usuário e uma mensagem para processar,

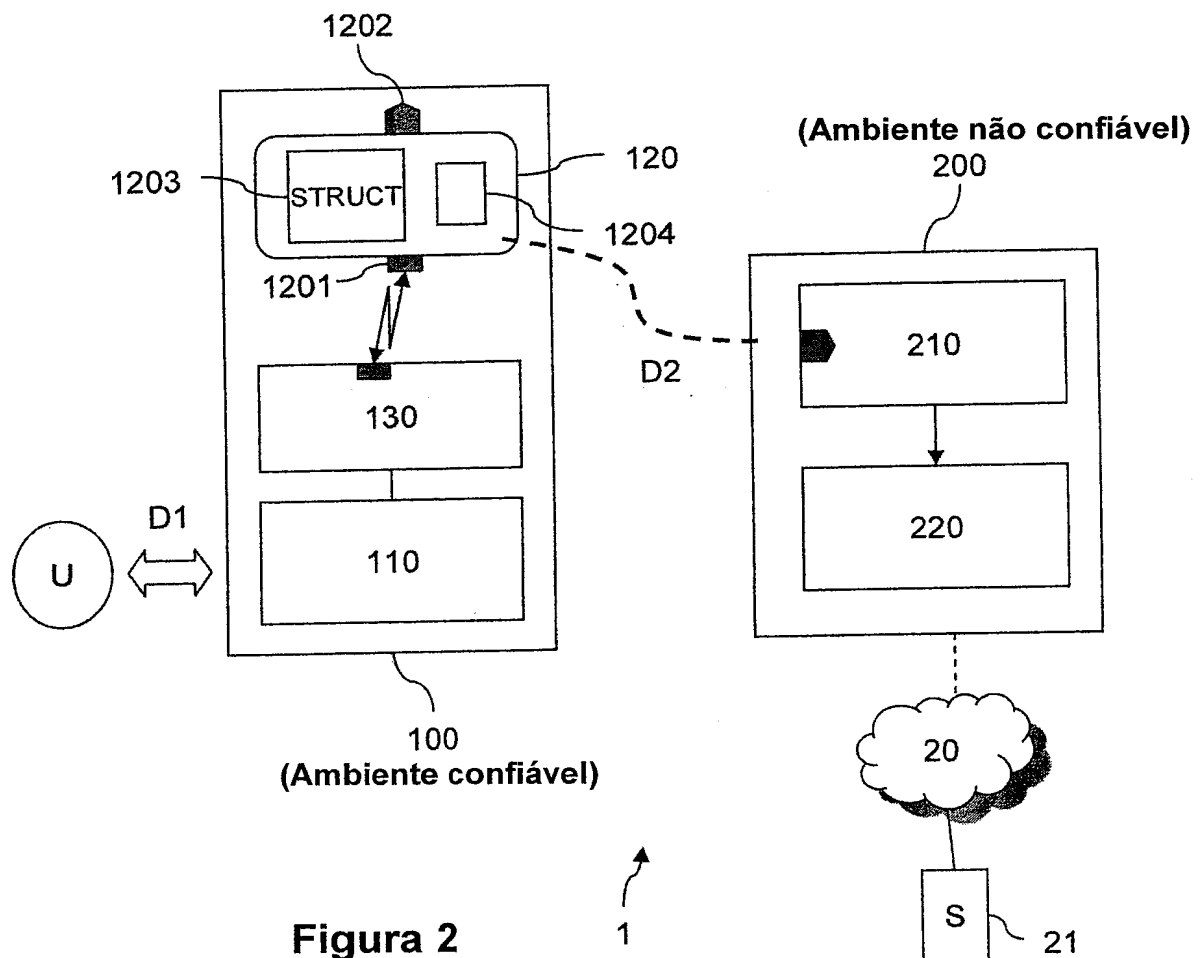
- uma memória que armazena, em uma estrutura de validade limitada de dados, dados de autenticação pessoais que são dependente dos dados pessoais de entrada,

- uns meios para limitar, no tempo ou no espaço, a validade da estrutura de dados armazenando os dados de autenticação pessoais, e

- uns meios para verificar a validade da estrutura de validade limitada antes usando os dados de autenticação pessoais que ela contém para gerar uma autorização ou uma recusa para executar uma função protegida por autenticação e implementada no processamento da mensagem recebida.



**Figura 1**  
Técnica Anterior



**Figura 2**

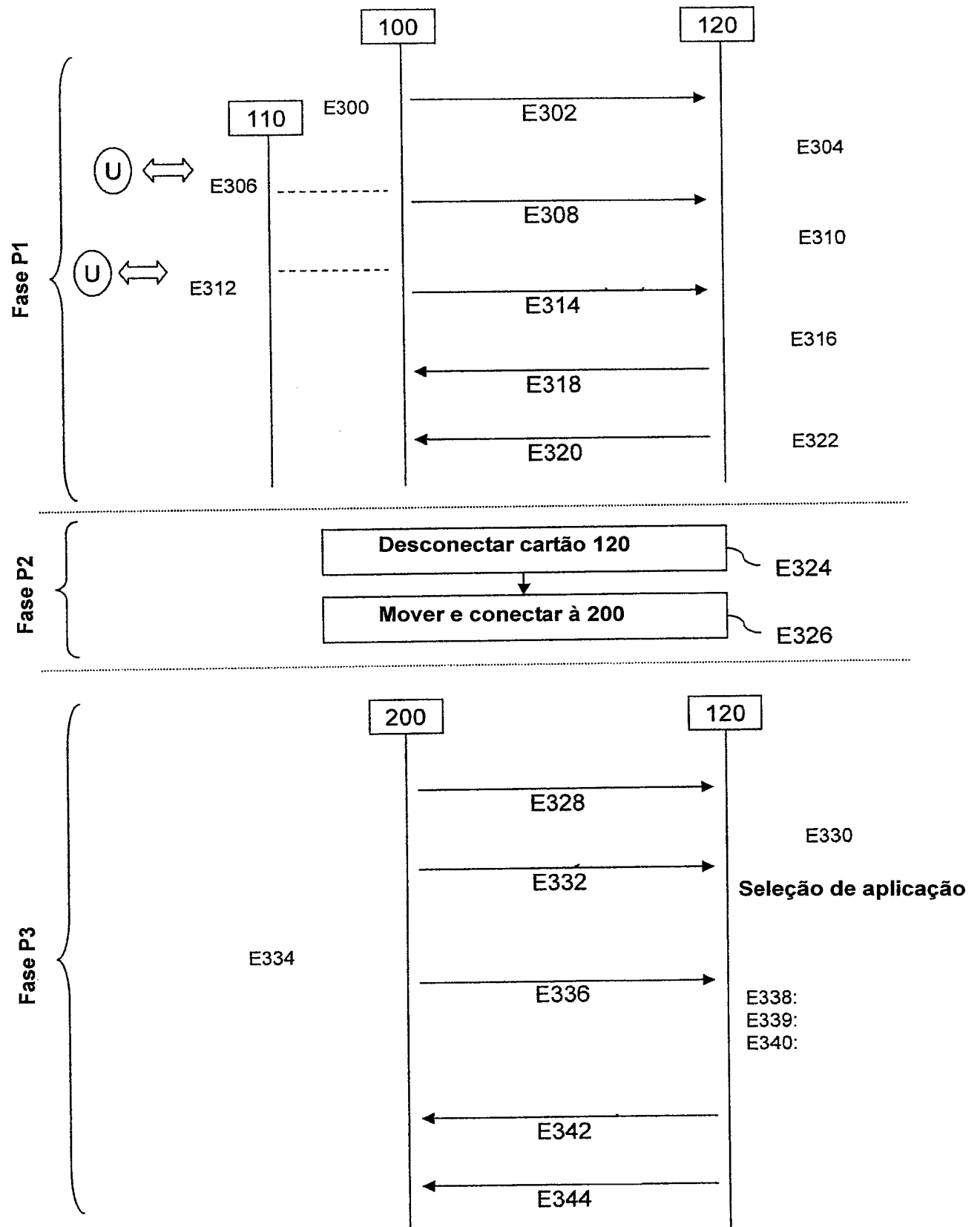


Figura 3

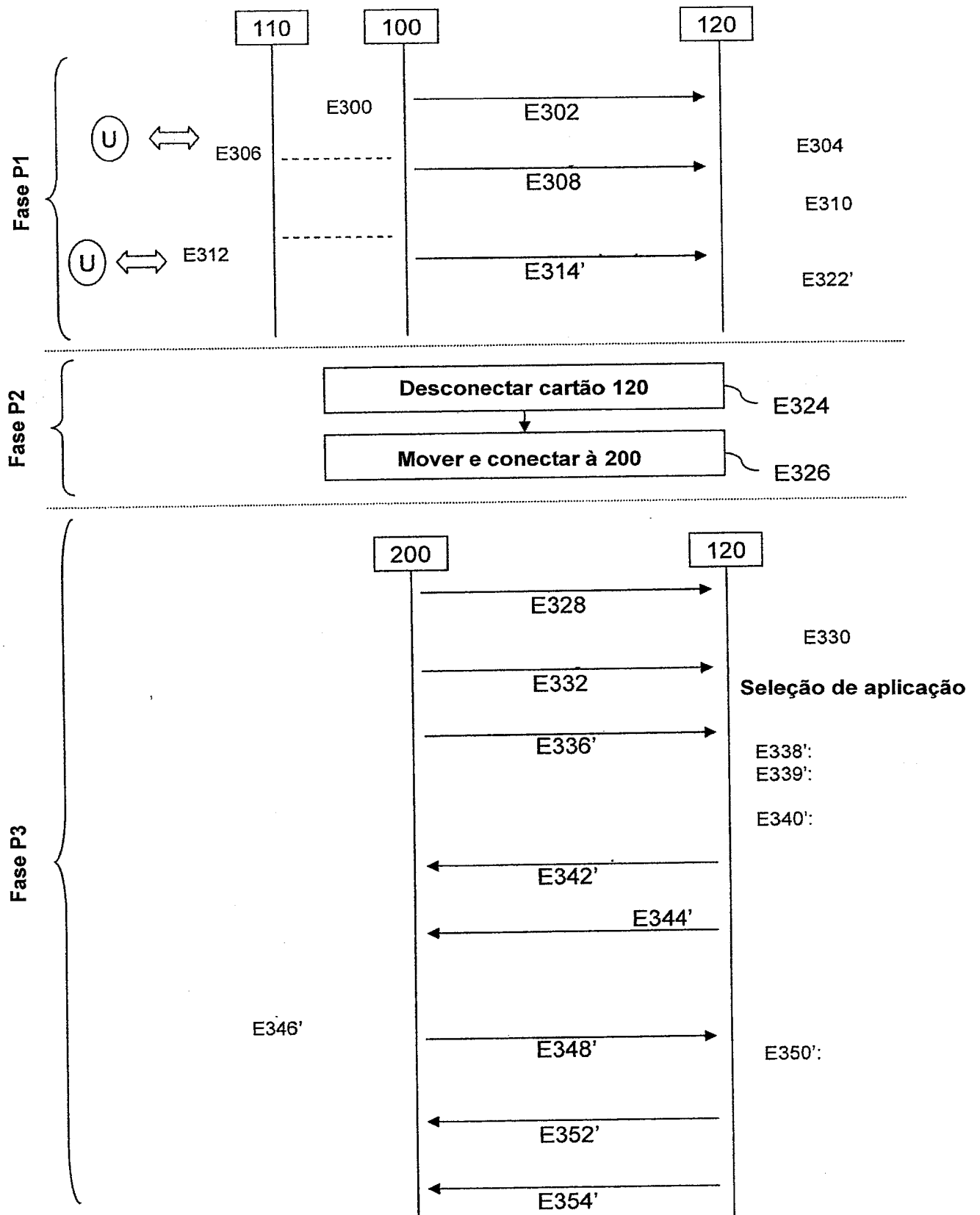


Figura 4

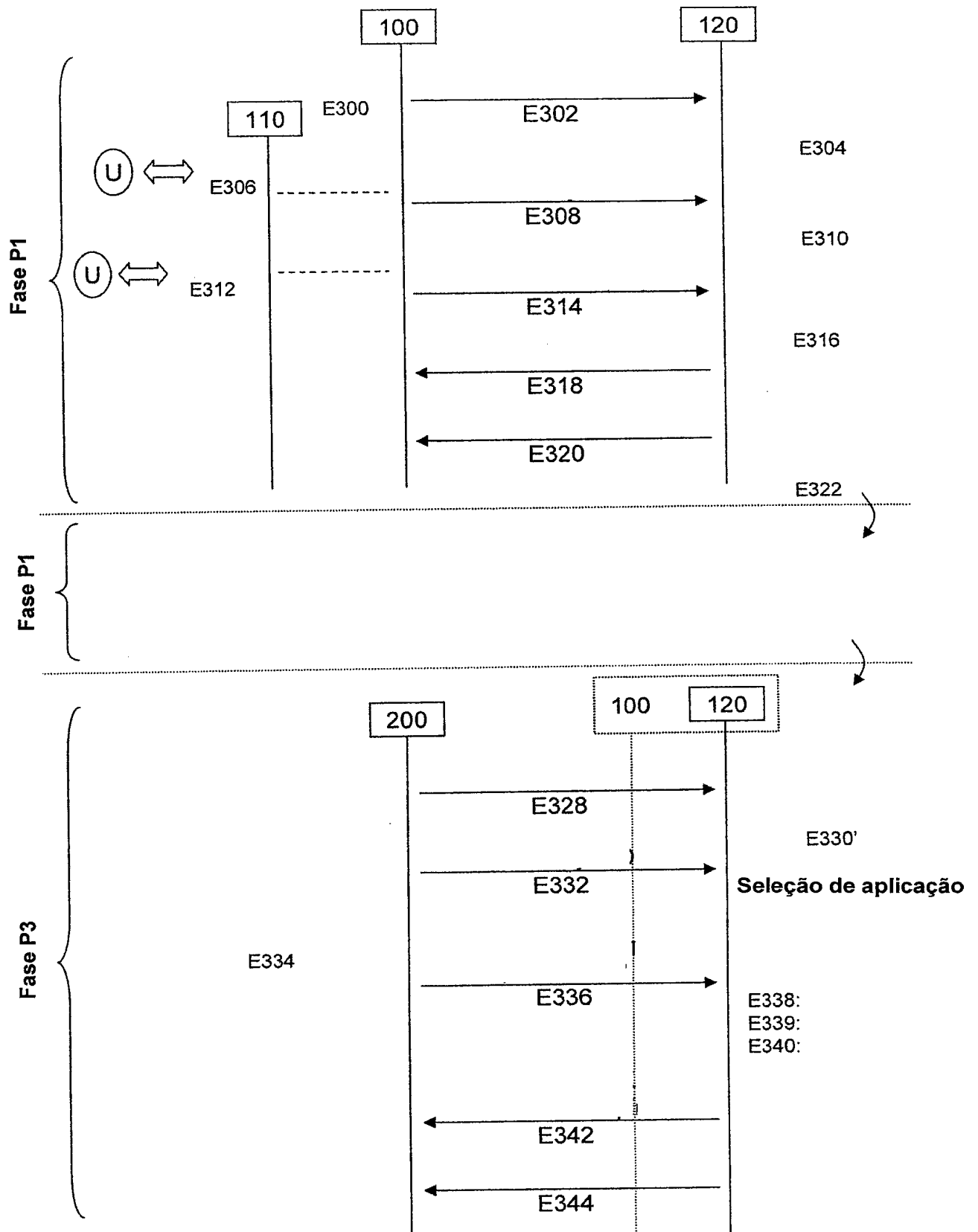


Figura 5

## RESUMO

‘MÉTODO E SISTEMA PARA CONTROLAR A EXECUÇÃO DE UMA FUNÇÃO PROTEGIDA POR AUTENTICAÇÃO, MÓDULO DE MEMÓRIA, E, ENTIDADE ELETRÔNICA’

5                   A presente invenção envolve um método e sistema para controlar a execução de uma função protegida por autenticação de um usuário e que é fornecida por exemplo para o acesso a uns recursos O método compreende introduzir, pelo usuário, dados pessoais usando um dispositivo de entrada, autenticar o usuário com os dados pessoais de entrada para autorizar  
10                   ou não autorizar a execução da função; em um cartão seguro conectado para o dispositivo de entrada, armazenar dados de autenticação de validade limitada dependente dos dados de entrada; quando o cartão está conectado a um dispositivo de processamento através do qual o usuário gera uma mensagem cujo processamento implementa a mencionada função, usando os dados  
15                   armazenados, levando em consideração a validade limitada, para autorizar ou não autorizar a execução daquela função.

‘MÉTODO E SISTEMA PARA CONTROLAR A EXECUÇÃO DE UMA  
FUNÇÃO PROTEGIDA POR AUTENTICAÇÃO, MÓDULO DE  
MEMÓRIA, E, ENTIDADE ELETRÔNICA’

Este pedido reivindica prioridade do pedido Francês de N°  
1058771 depositado em 26 de outubro de 2010, o qual pedido é incorporado  
aqui para referência.

CAMPO DA INVENÇÃO

A presente invenção diz respeito a um método e um sistema  
para controlar a execução de uma função protegida de autenticação.

CONTEXTO DA INVENÇÃO

Uma função é dita ser protegida por autenticação quando sua  
execução depende do resultado de uma autenticação, geralmente de um  
usuário.

Essas funções são em particular usadas para acessar recursos  
tal como sistemas, redes, aplicações, serviços em um cartão ou servidor  
remoto, e dados armazenados.

Tal uma função pode em particular corresponder à comandos  
implementados por uma entidade específica na recepção de uma mensagem  
solicitando o acesso a um recurso.

A autenticação do usuário envolvendo tal uma função para ter  
acesso a um daqueles recursos é convencionalmente realizada em um sistema  
de computador. Isto geralmente consiste de uma etapa de introduzir, pelo  
usuário, dados pessoais para identificação ou autenticação, usando um  
dispositivo de entrada, então de uma etapa de autenticar o usuário com base  
nos dados pessoais de entrada, por exemplo através de comparação com dados  
pessoais pré-gravados no sistema, para gerar uma autorização ou recusa para  
executar a função protegida possibilitando o acesso a um recurso.

Em caso de autorização, a função protegida é executada e o  
acesso ao recurso é obtido para o usuário.

Por meio de ilustração, os dados pessoais para identificação ou autenticação pode ser uma senha, um PIN (para “*Número de identificação Pessoal*”) ou dados biométricos.

Roubo de identidade é um problema recorrente que afeta a segurança dos sistemas para acesso a uns recursos por autenticação que processa aquelas funções protegidas por autenticação.

Em numerosas estratégias de ataque, roubo de identidade consiste em uma pessoa maliciosa roubando os dados pessoais particularmente confiáveis dos usuários para identificação ou autenticação, geralmente colocando software malicioso entre o dispositivo de entrada e o software de processamento que realiza uma autenticação com base nos dados pessoais de entrada.

O software malicioso recebe os dados confidenciais de entrada, faz uma cópia dos mesmos, então comunica aqueles dados para o software de processamento. Nesta maneira, nenhuma das duas partes envolvidas no acesso por autenticação (o usuário e o software de processamento) podem suspeitar da presença do software malicioso.

De posse dos dados pessoais confiáveis e conhecendo os recursos aos quais ele dão acesso (em particular porque o sistema de computador permite o acesso a um particular recurso, por exemplo uma caixa pagadora) possibilita Para pessoa maliciosa então a re-acessar os recursos, sob uma identidade falsa, aquela do usuário roubado.

Essas estratégias de ataque são conhecidas pelo termo “ataque de quem intercepta”. Elas são particularmente perigosas quando elas possibilitam ao ladrão de dados pessoais a identificação ou autenticação o acesso aos serviços por exemplo envolvendo transações financeiras. Elas são geralmente implementadas em relação a uns terminais de entrada não confiáveis, por exemplo terminais de pagamento nas lojas ou caixas pagadoras.

Há assim sendo uma necessidade de melhorar os mecanismos para verificar a execução de funções protegidas por autenticação, em particular quando elas possibilitam acesso aos recursos, em particular para combater tais estratégias de ataque.

5

### SUMÁRIO DA INVENÇÃO

Neste contexto, a invenção diz respeito em particular a um método de controle da execução de uma função protegida por autenticação, caracterizado pelo fato de compreender as seguintes etapas:

- armazenar, em uma estrutura de validade limitada, dados de autenticação pessoais dependentes dos dados pessoais de entrada, introduzindo os últimos por um usuário em um dispositivo de entrada;
- verificar a validade da estrutura de validade limitada antes de usar os dados de autenticação pessoais que ela contém para gerar uma autorização ou uma recusa para executar uma função implementada no processamento de uma mensagem gerada por um dispositivo de processamento que é distinto do dispositivo de entrada.

De acordo com a invenção, a entrada de dados pessoais e seu processamento para o acesso a uns recursos através da execução da função protegida pode ser dissociado no tempo ou no espaço. Isto é feito possível através do armazenamento em uma estrutura de validade limitada, de acordo com a invenção, dos dados de autenticação pessoais dependentes dos dados de entrada, assim sendo possibilitando ao elo de comunicação ser feito entre as duas operações de entrada e de processamento.

Ainda mais, essas duas operações são cada uma realizada em relação aos dispositivos distintos: o dispositivo de entrada para a primeira operação, e o dispositivo de processamento para a segunda. Assim sendo, o usuário não necessita efetuar uma introdução dos dados confidenciais no dispositivo de processamento, o que previne qualquer pessoa maliciosa tendo adulterado com aquele dispositivo de recuperar os dados confidenciais a partir

dos meios de entrada naquele dispositivo.

De acordo com a invenção, a dissociação das duas operações não possibilita a “quem intercepta” ambos, recuperar os dados confidenciais e conhecer os recursos aos quais eles possibilitam acesso (isto é para dizer a correspondente função protegida). Como será visto abaixo, o usuário pode usar um dispositivo de entrada no qual ele confia, por exemplo, um dispositivo que é específico para ele. Assim sendo, ele não é mais restringido aos dados pessoais de entrada em um dispositivo de terceiros de confiabilidade duvidosa.

No que se refere à validade limitada dos dados de autenticação pessoais, isto possibilita a eficiência da invenção a ser assegurada enquanto evitando dados confidenciais potencialmente roubados de serem usados indefinidamente, por exemplo, ao longo do tempo ou espaço, para possibilitar a pessoa maliciosa ter a função executada cuja execução é protegida por aqueles dados, e assim sendo ter acesso aos correspondentes recursos protegidos.

No caso de validade temporária, a duração da validade pode ser configurada nas bases dos riscos incorridos, e das funções e recursos envolvidos.

De forma similar, uma validade espacial definindo uma distância máxima para uso da estrutura a partir de um ponto inicial pode ser com base em uma medição de GPS.

Assim sendo, melhoramento é obtido no controle da execução das funções protegidas por autenticação e o possível acesso a uns recursos decorrentes.

De acordo com um aspecto da invenção, o método compreende as seguintes etapas:

- introduzir, pelo usuário, os dados pessoais usando o dispositivo de entrada;

- autenticar o usuário nas bases dos dados pessoais de entrada para gerar a autorização ou a recusa para executar a função protegida;

- executar uma função no caso de autorização;

em que:

5                   - as etapas de armazenar e verificar são implementadas em um módulo de memória respectivamente conectado ao dispositivo de entrada no momento da etapas de entrada e armazenamento, e ao dispositivo de processamento no momento das etapas de verificação e execução.;

10                  - a mencionada estrutura de validade limitada compreende dados de autenticação pessoais de validade limitada por associação de uma duração de validade com os dados de autenticação pessoais.

Embora seja possível a conexão ser física, é acima de tudo uma conexão lógica possibilitando a comunicação ser fornecida entre o dispositivo e módulo então envolvido.

15                  Somente um módulo de memória, que pode ser um cartão de microprocessador seguro convencional, manipula a estrutura de validade limitada de dados aqui, e assim sendo os dados de autenticação pessoais de validade limitada contidos por aquela estrutura. Em virtude das técnicas seguras que são amplamente conhecidas para este tipo de módulo ou cartão,  
20                  esses dados podem ser gerenciados como chaves secretas internas, e são assim sendo manipuladas em maneira segura durante as duas fases de entrada e exploração para autorizar ou não autorizar a execução da função protegida.

25                  Em uma modalidade, a verificação da validade da estrutura para usar os dados de autenticação pessoais compreende verificar o tempo que passou desde a geração daquela estrutura de validade limitada comparada com a duração da validade que está associada com os dados de autenticação pessoais. Em outras palavras, esta disposição consiste em verificar que os dados de autenticação pessoais de validade limitada são ainda válidos quando eles são usado para o propósito de obter uma autorização para executar a

função. Re-suo em grande escala desses dados confidenciais de validade limitada por uma pessoa maliciosa é e por meio disso, evitado. De acordo com algumas modalidades, em particular determinada descrita abaixo, a geração da autorização ou da recusa pode, como uma variante, ser dependente do tempo passado desde o término o fornecimento da potência elétrica para uma memória armazenando a estrutura de validade limitada.

Em uma modalidade, gerar autorização ou a recusa é dependente de uma verificação dos dados pessoais introduzidos com dados de referência, o resultado da verificação sendo obtido usando os mencionados dados de autenticação pessoais armazenados na estrutura de validade limitada armazenada. Em maneira convencional, a autenticação do usuário aqui compreende a verificação dos dados pessoais de entrada para os propósito de autorizar ou não autorizar o acesso ao recurso. A presente disposição possibilita esses mecanismos serem mantidos em virtude do uso dos dados de autenticação pessoais de validade limitada que são armazenados no módulo de memória de acordo com a invenção.

De acordo com um particular recurso da invenção, o método compreende a etapa de comparar dados pessoais de entrada com dados pessoais pré-gravados no módulo de memória, e os dados de autenticação pessoais armazenados na estrutura de validade limitada compreende o resultado da comparação. Nesta configuração, as operações de autenticação são realizadas no dispositivo de entrada mas a autorização com base naquela autenticação não foi ainda dada. Para ser preciso, somente o resultado da autenticação (se a comparação dos dados de entrada é ou não positiva) é fornecido como um item de dados confidenciais de validade limitada de acordo com a invenção. Assim sendo comunicação dos dados pessoais como entrada (senha, código de PIN, etc.) para um dispositivo de processamento é evitada.

Como uma variante, os dados de autenticação pessoais

armazenados na estrutura de validade limitada compreende os dados pessoais de entrada, e seu uso compreende uma sub-etapa de comparação dos dados de autenticação pessoais armazenados na estrutura de validade limitada com dados pessoais pré-gravados no módulo de memória. Esta disposição torna possível simplificar as operações realizadas pelo dispositivo de entrada, em particular se ele tem recursos de processamento limitados ou se, para as necessidades da comparação, isto se mostra necessário, por exemplo, ter acesso a um banco de dados seguro.

Em uma modalidade da invenção, a duração de validade associada com os dados de autenticação pessoais é contabilizada através da descarga de uma capacitância elétrica fornecida no módulo de memória. A capacitância elétrica assim sendo serve como um contador de tempo. Esta configuração é em particular simples de implementar em qualquer tipo de entidade eletrônica capaz de armazenar os dados de validade limitada de acordo com a invenção.

Em particular, os dados de autenticação pessoais são armazenados em uma memória volátil do módulo de memória, a qual memória é temporariamente alimentada pela mencionada capacitância elétrica. O controle através de autenticação de acordo com a invenção é tornada ainda mais segura por esta disposição, já que os dados confidenciais de validade limitada são automaticamente eliminados na expiração da duração de validade, devido à natureza da memória volátil. Ainda mais, esta configuração é simples de implementar.

Em uma outra modalidade, os dados de autenticação pessoais são armazenados em uma memória volátil do módulo de memória, e a duração de validade associada com eles é definida pelas propriedades de evanescimento da memória volátil quando seu fornecimento de energia é cortado. Esta disposição tem a vantagem de não se basear em meios específicos para contabilizar a duração de validade. Mais particularmente,

devido à evanescência dos dados neste tipo de memória volátil, é assegurado que os dados confidenciais de validade limitada são automaticamente apagados ao expirar a duração da evanescência. Memória voláteis assim sendo serão escolhidas cujas correspondentes propriedades de evanescência são apropriadas para a duração de vida ou validade desejada para os dados de autenticação pessoais gerados.

Em ainda uma outra modalidade, os dados de autenticação pessoais são armazenados em uma memória volátil de um módulo de memória, que é continuamente energizado durante o controle da execução da função protegida ou em uma memória de re-escrita, por exemplo do tipo de EEPROM tipo (EEPROM para “*Memória de Somente Leitura Programável e Passível de Apagar Eletricamente*”), e uma duração de validade associada com eles é definida armazenando uma quantidade temporal, por exemplo uma duração de validade e tempo inicial da validade, ou um tempo de término da validade sozinho, em uma variável que está associada na memória com os dados de autenticação pessoais. Elementos suficientes são assim sendo fornecidos para o módulo de memória para ser capaz de verificar que os dados de autenticação pessoais usados para obter a autorização estão ainda válidos, através de comparação da duração da validade, ou tempo de término da validade (que é a data incluindo a hora, minuto, etc.) com o tempo que passou desde a geração daqueles dados.

De acordo com um recurso da invenção, o uso, por um módulo de memória, dos dados de autenticação pessoais de validade limitada compreende verificar a validade daqueles dados usando a para lê-lo pelo dispositivo de processamento. Esta disposição possibilita uma referência comum a ser usada para avaliar o limite temporal para validade. Ela pode em particular ser um relógio comum para os diferentes dispositivos (por exemplo um relógio de rede), ou um relógio específico para aqueles dispositivos.

Em uma modalidade, a função protegida é um comando

implementada, na recepção de uma mensagem a partir do dispositivo de processamento, através de um módulo de microprocessador armazenando a estrutura de validade limitada. De acordo com várias abordagens, o comando protegido pode ser diretamente indicado em uma mensagem fornecida ou ser  
5 um sub-comando que depende de tal um comando indicado na mensagem (por exemplo um sub-comando chamado na execução daquele comando).

De acordo com um outro recurso da invenção, um módulo de memória armazenando a estrutura de validade limitada e os dados de autenticação pessoais que ela contém são removíveis, e são colocados no  
10 dispositivo de entrada no momento da entrada e colocados no dispositivo de processamento no momento da verificação da validade da estrutura e no momento do uso dos dados de autenticação pessoais de validade limitada. Esta disposição é altamente conveniente para o usuário, que, para os propósitos de controle da execução de uma função protegida por autenticação  
15 de modo, por exemplo, a ter acesso a um recurso, pode transportar ou fornecer apenas o módulo de memória removível sobre o qual são gravados os dados confidenciais resultantes da entrada e que são necessários para a autenticação.

Como uma variante, um módulo de memória armazenando a estrutura de validade limitada e os dados de autenticação pessoais que ela  
20 contém é fisicamente ligada com o equipamento de entrada durante o controle e execução da função protegida (isto é para dizer, durante as duas etapas de entrada e de processamento), e o equipamento de processamento se comunica com um módulo de memória através de comunicação sem contato. Esta configuração se mostra simples de uso para o usuário, já que o usuário pode  
25 simplesmente introduzir seus dados pessoais confidencialmente em um dispositivo de entrada que é específico para ele (por exemplo seu telefone móvel) e apresenta o último para o dispositivo de processamento para efetuar as subseqüentes operações necessárias para controlar a execução da função por exemplo para acessar um correspondente recurso. Esta comunicação sem

contato também cobre o caso onde aquela comunicação passa via o dispositivo de entrada no qual um módulo de memória está embutida. Por exemplo, este é o caso quando um cartão SIM (SIM significa “*Módulo de Identidade do Assinante*”) em um telefone móvel usa um controlador de NFC (NFC significa “*Comunicação de Campo Próximo*”) do telefone móvel para se comunicar com um dispositivo de processamento externo.

De acordo com um particular recurso, o módulo de memória armazenando a estrutura de validade limitada e os dados de autenticação pessoais é um cartão de microprocessador seguro. Esta disposição é vantajosa no fato que, em uma maneira convencional, o cartão de microprocessador compreende meios para tornar os dados confidenciais seguros e também meios eficientes para comunicar com um ou outro dos dispositivos de entrada e de processamento.

Em particular, a comunicação entre o dispositivo de entrada ou o dispositivo de processamento e o mencionado cartão de microprocessador é sem contato. Nesta maneira, aqueles dispositivos e o cartão (módulo de memória) são conectados à cada uma das operações necessárias para controlar a execução da função. O canal de comunicação pode ser de acordo com o padrão de NFC, com o padrão de ISO 14443 ou com um padrão similar.

Como uma variante, em particular se o cartão de microprocessador é removível durante essas operações, comunicação por contato pode ser fornecido entre o dispositivo de entrada ou o dispositivo de processamento e o mencionado cartão de microprocessador.

Em uma modalidade, o processamento da mensagem a partir do dispositivo de processamento gera uma resposta caracterizada pelo fato de compreender pelo menos um valor de resposta que depende da autorização ou da recusa gerada. Esta configuração acha numerosas aplicações, que são geralmente definidas no sucesso ou falha de um acesso solicitado pelo usuário (por exemplo um pagamento feito ou não feito com sucesso, o acesso a uma

conta segura, etc.).

Em determinadas aplicações como uma variante, um valor de resposta pode contudo ser independente da autorização ou da recusa gerada (para todas ou algumas das funções protegidas). Como ilustrado abaixo, a  
5 execução de uma função protegida pode simplesmente efetuar a atualização de um estado do módulo de memória interno , tal como um atualizador de detecção de acesso fraudulento.

Em uma modalidade da invenção, o usuário introduz pelo menos um item de informação representando um item de dados financeiros, e  
10 o mencionado item de informação é armazenado na estrutura de validade limitada em comum com os dados de autenticação pessoais, para os propósitos de uma posterior operação financeira (por exemplo uma transação), a qual o acesso dependente da autorização ou da recusa gerada. Em virtude da invenção, é assim sendo possível tornar seguro todos os dados  
15 introduzidos pelo usuário para o propósito de uma operação posterior, se aqueles dados são ou não confiáveis. Esta disposição aumenta a confiança daqueles dados nesta maneira.

Em uma modalidade da invenção, o dispositivo de entrada é um equipamento confiável pelo usuário. Esta configuração se beneficia da  
20 total eficiência da invenção, já que a operação de entrada é fortemente protegida aqui. Assim sendo, como uma pessoa maliciosa é incapaz de acessar esse dispositivo confiável ele é incapaz de recuperar os dados pessoais diretamente introduzidos pelo usuário.

Em particular, o dispositivo de entrada é um telefone móvel do  
25 usuário.

Em uma maneira complementar, a invenção envolve um módulo de memória caracterizado pelo fato de compreender pelo menos uma memória e um processador para executar instruções, o módulo de memória sendo configurado por:

- armazenar, em uma estrutura de validade limitada, dados de autenticação pessoais que são dependentes dos dados pessoais introduzidos por um usuário e recebidos de um dispositivo de entrada ao qual um módulo de memória está ligado (isto é para dizer durante a entrada);

5                   - verificar a validade da estrutura de validade limitada antes de usar os dados de autenticação pessoais que ela contém para gerar uma autorização ou uma recusa para executar a função protegida por autenticação e implementada no processamento de uma mensagem recebida a partir de um dispositivo de processamento que é distinto do dispositivo de entrada.

10                  De forma similar, a invenção envolve um sistema para controlar a execução de uma função protegida por autenticação de um usuário, caracterizada pelo fato de compreender:

- um dispositivo de entrada para introduzir dados pessoais pelo usuário;

15                  - um dispositivo de processamento que é distinto do dispositivo de entrada e adaptado para gerar, sob a ação do usuário, uma mensagem para processar;

- um módulo de memória caracterizado pelo fato de compreender pelo menos uma memória e um processador, e que é configurado para autenticar o usuário nas bases dos dados pessoais de entrada a fim de gerar uma autorização ou uma recusa para executar uma função protegida implementada no processamento da mencionada mensagem;

em que o módulo de memória é configurado para:

25                  - quando ele está conectado ao dispositivo de entrada, gerar e armazenar, em sua memória, dados de autenticação pessoais de validade limitada que são dependentes dos dados pessoais de entrada e associando-os com um parâmetro de validade; e

- quando ele está conectado ao dispositivo de processamento, usando os dados de autenticação pessoais armazenados para gerar a

autorização ou a recusa para executar a função dependendo do parâmetro de validade associado.

O módulo de memória e o sistema de autenticação têm vantagens similares àqueles do método estabelecido acima. Em particular, eles tornam possível dissociar as operações de introduzir os dados confidenciais e de processar aqueles dados para o propósito de obter uma autorização para executar a função protegida, procurando segurança autenticada contra os ataques por quem intercepta.

Opcionalmente, um módulo de memória ou o sistema pode compreender meios relacionados aos recursos do método estabelecido acima, e em particular uma capacitância elétrica usada para contagem regressiva da duração de validade, uma memória volátil que automaticamente ser apaga ao término da mencionada duração, uma memória fixa ou removível, um cartão de microprocessador para armazenar os dados de autenticação pessoais de validade limitada de acordo com a invenção entre os vários dispositivos, meios sem contato ou com contato para comunicação entre o cartão de microprocessador e os vários dispositivos.

Em particular, esses dispositivos podem compreender meios de entrada para introduzir, pelo usuário, os dados pessoais usando o dispositivo de entrada; meios de autenticação para autenticar o usuário nas bases dos dados pessoais de entrada a fim de gerar a autorização ou a recusa para executar a função protegida; meios de execução para executar uma função no caso de autorização. Ainda mais, um módulo de memória configurado para o armazenamento e para a verificação pode ser respectivamente conectado ao dispositivo de entrada no momento da entrada e do armazenamento, e ao dispositivo de processamento no momento da verificação e da execução. Neste caso, ele pode ser fornecido para a mencionada estrutura de validade limitada para compreender os dados de autenticação pessoais de validade limitada por associação de uma duração de

validade com os dados de autenticação pessoais.

Mais ainda, de acordo com uma outra modalidade, os dados de autenticação pessoais armazenados na estrutura de validade limitada pode compreender os dados pessoais de entrada. O módulo de memória ou o sistema pode então, de modo a usar aqueles dados, compreender uns meios para comparar os dados de autenticação pessoais armazenados na estrutura de validade limitada com os dados pessoais pré-gravados no módulo de memória.

De acordo com uma outra modalidade, a mencionada estrutura de validade limitada compreende dados de autenticação pessoais de validade limitada pela associação de uma duração de validade com os dados de autenticação pessoais. Neste caso, eles podem ser fornecidos para um módulo de memória para compreender uma capacitância elétrica tal que a duração de validade associada com os dados de autenticação pessoais é introduzida pela descarga da capacitância elétrica fornecido na módulo de memória.

Em particular mais ainda, um módulo de memória pode compreender uma memória volátil armazenando os dados de autenticação pessoais e temporariamente energizado pela mencionada capacitância elétrica.

De acordo com ainda uma outra modalidade, um módulo de memória pode compreender uma memória volátil que é continuamente energizada durante o controle da execução da função protegida ou uma memória de re-escrita, a qual memória armazena os dados de autenticação pessoais. Neste caso, um módulo de memória é configurado para associar uma duração de validade com aqueles dados de autenticação pessoais armazenando uma quantidade temporal em uma variável que é associada em memória com aqueles mesmos dados de autenticação pessoais.

A invenção também envolve uma entidade eletrônica caracterizada pelo fato de compreender:

- pelo menos uma interface de comunicação para receber

dados pessoais introduzidos por um usuário e uma mensagem para processar,

- uma memória que armazena, em uma estrutura de validade limitada de dados, dados de autenticação pessoais que são dependentes nos dados pessoais de entrada,

5 - uns meios para limitar, no tempo ou espaço, a validade da estrutura de dados armazenando os dados de autenticação pessoais, e

- uns meios para verificar a validade da estrutura de validade limitada antes de usar os dados de autenticação pessoais que ela contém para gerar uma autorização ou uma recusa para executar uma função protegida por autenticação e implementada no processamento da mensagem recebida.

10 Em particular, a entidade pode ser tio cartão de microprocessador.

A entidade eletrônica tem similares vantagens àquelas do método, do módulo de memória e do sistema estabelecidos acima.

15 Opcionalmente, a entidade eletrônica pode compreender meios relacionados aos recursos do método estabelecido acima, e em particular meios para implementar uma duração de validade, tal como uma capacitância elétrica ou uma variável em memória, e uma memória se volátil ou não.

### BREVE DESCRIÇÃO DOS DESENHOS

20 Outras particularidades e vantagens da invenção vão aparecer na seguinte descrição, ilustrada pelos desenhos anexos, nos quais:

- Figura 1 ilustra mecanismos convencionais para autenticação de um usuário U para acessar um recurso;

- Figura 2 é um diagrama de uma implementação da invenção;

25 e - Figuras 3 à 5 ilustra três exemplos de acesso a um serviço de assinatura digital protegido por uma autenticação de acordo com a invenção.

### DESCRIÇÃO DETALHADA DA INVENÇÃO

A Figura 1 ilustra mecanismos convencionais para acesso a

uns recursos por um usuário U, por exemplo, para acessar um serviço de pagamento em uma loja de varejo.

Essas operações requerem a interação entre um usuário U e um terminal de pagamento 10. Esta interação consiste em particular na entrada de dados pessoais para identificar ou autenticar que são confiáveis a possíveis ataques, usando um teclado ou qualquer outro tipo de meios de entrada 11. Por meio de ilustração, esses dados pessoais confiáveis podem ser uma senha, um número de PIN (PIN significa “*Número de Identificação Pessoal*”) ou dados biométricos possibilitando uma pessoa para autenticar a sinal próprio e para possibilitar uma transação financeira com o varejista a ser feita.

Outros dados não confiáveis também podem ser introduzidos naquele momento, por exemplo, um total indicado pelo usuário para a transação financeira com o varejista.

Uma mensagem solicitando uma transação financeira e caracterizada pelo fato de compreender aqueles dados de entrada, é então fornecida a uma aplicação de software 12.

Uma mensagem compreende em particular um comando para a transação financeira.

A execução daquele comando depende em particular na presença de direitos necessários específicos para aquele comando, neste caso uma autenticação válida produzido pela validação dos dados pessoais de entrada.

Usando mecanismos convencionais e geralmente através de comparação com dados pré-gravados, o software 12 verifica os dados pessoais introduzidos pelo usuário para gerar uma autorização ou recusa para executar a transação financeira. Por exemplo, a entrada de PIN por um usuário U pode ser comparado para um PIN armazenado em um cartão de pagamento inserido no terminal de pagamento 10.

Em caso de autenticação positivo, a execução do comando de

transação financeira é autorizada possibilitando o acesso para o serviço de pagamento S. Trocas com um servidor (simbolizado aqui pela rede 20 e o servidor 21) são então conduzidos.

No caso de autenticação negativa, a transação financeira não pode ser realizada.

Neste contexto, ataques por quem intercepta utiliza uma aplicação de software maliciosa 13 como representado diagramaticamente na figura. O software malicioso 13 intercepta os dados de entrada, se eles são ou não confiáveis, copiá-los e transferi-los para o software 12. A intervenção do software malicioso 13 é assim sendo transparente para o usuário e para o software 12.

A Figura 2 é um diagrama de um sistema 1 implementando a invenção de acordo com uma modalidade. O usuário U precisa fazer as mesmas entradas (de dados confidenciais e possivelmente de dados não confiáveis) como convencionalmente para o uso de comandos protegidos por direitos relativos a uma autenticação.

No sistema da Figura 2, o usuário U interage com um primeiro dispositivo de entrada 100. Este dispositivo é preferencialmente um dispositivo confiável, isto é para dizer um dispositivo do próprio usuário U, por exemplo. seu telefone móvel ou seu computador.

O dispositivo de entrada 100 compreende uma interface de entrada 110, um cartão de microprocessador seguro 120 e um leitor de cartão de microprocessador embutido 130. Outras funcionalidades convencionais de um telefone móvel pode ser fornecidas no dispositivo de entrada 100, sem elas sendo descritas aqui contudo. Em particular meios internos para alimentar de energia o dispositivo 100 (uma bateria, por exemplo) como fonte elétrica principal possibilita o cartão de microprocessador 120 a ser energizado.

A interface de entrada 110 pode tomar a forma de um teclado

de telefone convencional, por exemplo, para os propósitos de introduzir um código de PIN ou uma senha. Como uma variante ou em combinação, ele pode compreender um sensor biométrico adaptado para adquirir dados biométricos específicos para o usuário U, ou qualquer outra interface.

5                   O leitor embutido 130 pode igualmente ser sem contato ou com contato para ler de e/ou escrever para o cartão de microprocessador 120. Ele é ligado à interface de entrada 110 via uma arquitetura de sistema eletrônico convencional, por exemplo via um cabo de múltiplas vias de comunicação de dados e um microprocessador (não mostrado).

10                   O cartão de microprocessador ou “*cartão inteligente*” 120 é preferencialmente um cartão pessoal removível para o usuário U, por exemplo em formato de ID-1, que o usuário pode facilmente extrair do dispositivo de entrada 100 para apresentá-lo a um outro leitor de cartão de microprocessador 210 de um dispositivo de processamento 200, conforme descrito abaixo.

15                   Como uma variante, o cartão de microprocessador 120 pode ser fisicamente anexado ao dispositivo de entrada 100 durante a totalidade das operações para acesso aos recursos S, isto é para dizer durante a entrada, o controle do comando de acesso protegido por uma autenticação e a trocas durante o acesso.

20                   Em ambos esses casos, e em particular quando é fisicamente anexado o dispositivo de entrada 100, a cartão de microprocessador 120 pode ser substituído por um mais simples módulo de memória fornecido com uma memória e a micro-controlador ou processador, para a implementação das operações de acordo com a invenção. A memória pode ser volátil ou não

25                   como explicado abaixo.

                  O cartão de microprocessador 120 compreende uma interface sem contato 1201 para comunicação com o leitor sem contato 130 do dispositivo. O cartão de microprocessador 120 também compreende uma interface sem contato 1202 para comunicação com leitor sem contato 210 do

dispositivo de processamento 200. Em particular, essas duas interfaces são combinadas em uma interface única. Eles podem contudo ser distinto, por exemplo um sendo com contato e o outro sem contato.

Conforme será visto mais tarde, eles possibilitam o cartão de microprocessador a receber os dados introduzidos pelo usuário no dispositivo de entrada 100 e para receber uma mensagem pelo respectivo usuário, o processamento daquela mensagem em particular implementando o comando de acesso protegido por autenticação, ou porque ele o contém diretamente, ou porque chama tal comando que é interno para o cartão de microprocessador.

O cartão de microprocessador 120 também compreende uma memória 1203 possibilitando uma estrutura de dados STRUCT a ser armazenada conforme descrito abaixo, assim como meios 1204 tornando possível definir um parâmetro de validade para a mencionada estrutura, por exemplo uma duração de validade DV ou uma zona geográfica de validade. Para as seguintes explicações, referência principalmente será feita para uma duração de validade. Similares mecanismos àqueles descritos abaixo podem contudo ser implementados para uma validade geográfica.

O cartão de microprocessador 120 é configurado para gerar e armazenar, em sua memória 1203, quando ele está conectado ao dispositivo de entrada 100, dados de autenticação pessoais de validade limitada que são dependentes da entrada de dados pessoais pelo usuário e para associá-los com uma duração de validade, por exemplo via a mencionada estrutura.

Conforme descrito abaixo através de diferentes exemplos, os meios 1204 podem definir tal uma duração de validade DV explicitamente ou implicitamente dependendo das propriedades da arquitetura que é adotada.

A duração de validade DV é associada com a estrutura STRUCT para, por conseguinte, definir um limite temporal de validade.

Esta duração é dependente de um nível de desejado de segurança, que varia de uma aplicação para uma outra. À título de exemplo,

para um comando de transação financeira protegida tornado seguro através de código de PIN, a qual duração pode ser configurada em umas poucas dezenas de segundo, por exemplo 1 à 2 minutos. Para um comando para acesso seguro para um computador ou rede de comunicação, este pode ser mais longo, da ordem de uns poucos minutos, por exemplo 5, 10 ou 15 minutos.

Em uma modalidade, a memória 1203 é uma memória volátil.

A memória 1203 pode então ser continuamente energizada por uma fonte de energia principal (bateria do dispositivo 100), em particular quando o cartão 120 não é extraído a partir do dispositivo de entrada 100 para o todo das operações de acesso ao recurso. Neste caso, os meios 1204 podem consistir de uma variável na memória definindo a duração de validade DV da estrutura de dados STRUCT iniciando a partir de sua geração (que é para dizer, a partir de sua criação e/ou a partir de sua atualização), conforme descrito abaixo, ou definindo um tempo final de validade, ou um tempo de início de validade se a duração a partir daquele tempo é pré-fixado.

Se o cartão 120 é configurado para ser extraído do dispositivo de entrada 100 a ser apresentado para o dispositivo de processamento 200, uma memória volátil 1203 pode, quando a fonte de energia principal tiver sido desconectada, ser temporariamente energizado através de uma fonte interna com evanescimento de eletricidade, por exemplo uma capacitância elétrica carregada a partir da fonte de energia principal quando o cartão 120 está na posição no dispositivo de entrada 100.

A fonte interna com evanescimento coloca-se com meios 1204 já que ela é capaz de manter o fornecimento de energia da memória volátil (que esvazia quando toda a energia foi cortada) para a duração que depende de suas propriedades (em particular o valor de sua capacitância).

Em particular, no caso de uma capacitância elétrica, o valor da capacitância é escolhido nas bases da duração de validade DV desejada. No caso de total descarga da capacitância, a estrutura de dados STRUCT presente

na memória 1203 é então automaticamente apagada. Mecanismos para controlar carga e descarga da capacitância tornam possível fornecer uma contagem regressiva da duração de validade iniciando de um tempo preciso desejado, em particular quando o cartão 120 é extraído do dispositivo de entrada 100 ou quando a estrutura de dados STRUCT é gerada, e possivelmente continua a contagem regressiva quando o cartão 120 é de novo energizado pelo dispositivo de processamento 200.

Por exemplo, comandos para controlar a capacitância pode ser fornecida e usada pelo cartão 120 para controlar aquela duração de validade DV. Em particular, um comando de carga pode ser fornecido para carregar a capacitância e implicitamente o acionamento do início da contagem regressiva de DV no final da carga, um comando de descarga pode ser fornecido para descarregar a capacitância a fim de forçar um estado de invalidade para a estrutura de dados STRUCT, e um comando de nível de descarga de modo a conhecer o nível de carga da capacitância e assim sendo diretamente determinar se a duração DV expirou ou não.

Este caso geralmente pode se aplicar a qualquer memória adaptada para preservar dados somente por um tempo determinado (que implicitamente define uma duração de validade DV).

Em um outro exemplo, uma memória volátil 1203 escolhida pode ter propriedades de evanescimento (em particular uma duração de evanescimento) que são compatíveis com a duração de validade DV desejada. Neste caso, os meios 1204 são formados por aquelas propriedades de evanescimento, já que quando do corte da energia para a memória 1203 (em particular na extração do cartão 120 ou em um comando para terminar o fornecimento de energia para a memória), a estrutura de dados STRUCT permanece na memória 1203 até expirar a duração de evanescimento. Controles que possibilitam o fornecimento de energia e término do fornecimento de energia para aquela memória são fornecidos nesta conexão.

Em uma outra modalidade, a memória 1203 é uma memória de re-escrita, no qual caso os meios 1204 podem consistir de uma variável na memória definindo um item de informação temporal, por exemplo a duração de validade DV da estrutura de dados STRUCT a partir de sua criação ou  
5 atualização, um data e hora do fim da validade, ou uma data e hora do início da validade se uma duração pré-fixada é acordada antecipadamente. Como uma variante, mesmo se uma memória é passível de ser re-escrita, os meios 1204 podem ser formados usando uma fonte interna com evanescimento (por exemplo, uma capacitância elétrica) que é dedicada para os mesmos,  
10 carregados pela fonte de energia principal, e que se descarregam a partir do fim da carga na sequência de recepção de um comando de carga. Neste caso, enquanto a capacitância elétrica não está totalmente descarregada, a estrutura STRUCT é considerada como válida.

No particular caso de uma validade geográfica (que pode mais  
15 ainda ser fornecida como um complemento de uma validade temporal conforme descrito acima), uma zona de validade pode ser definida em torno de um ponto inicial, por exemplo a localização do cartão 120 no momento em que a estrutura STRUCT foi criada. Esta permanece válida dentro daquela zona. Em particular meios adaptados podem ser fornecidos para  
20 definitivamente apagar a estrutura (ou torná-la definitivamente inválida) assim que uma saída daquela zona ocorra. Como uma variante, qualquer retorno na zona após a saída pode de novo tornar a estrutura válida.

Os meios adaptados pode combinar um receptor do GPS capaz de computar distâncias relativas ao ponto inicial, uma distância limite  
25 delimitando a zona (por exemplo um raio), e uma memória fornecida com meios para apagar assim que a distância correspondendo excede a distância limite.

Como indicado anteriormente, uma implementação da invenção consiste, para o usuário U, de introduzir dados pessoais para

identificação ou autenticação, isto é para dizer, dados pessoais confiáveis D1, por meio do dispositivo de entrada 100. Como um complemento, o usuário U pode também introduzir outros dados (possivelmente não confiáveis) que são necessários para o acesso e/ou para efetuar o serviço S que o usuário deseja ter acesso, por exemplo o total de uma transação financeira, o nome de um arquivo para recuperar, uma data, etc.

Esta ação de entrada conduz a atualização dos dados ou um estado que são internos para o cartão de microprocessador 120, em uma estrutura de dados STRUCT que pode ser criada naquele momento. A duração de validade é então associada com ele naquele momento, usando um dos meios referidos anteriormente.

A estrutura de dados STRUCT pode, sem ser limitado a ela, se um arquivo eletrônico simples, uma lista, uma árvore, um gráfico, um banco de dados, etc.

Como será visto nos seguintes exemplos, a estrutura de dados STRUCT pode diretamente armazenar, como dados de autenticação pessoais D2, os dados pessoais introduzidos pelo usuário U, sem qualquer processamento sendo realizado naqueles dados.

Como uma variante, o dispositivo de entrada 100 pode efetuar pré-processamento dos mesmos para produzir outros dados de autenticação pessoais D2 dependentes daqueles dados pessoais de entrada. À título de exemplo, a verificação de um código de PIN introduzido pelo usuário U é feita pelo terminal de entrada 100, aqui o telefone móvel do usuário U, e um item de informação representando o resultado de sua comparação com um código de referência de PIN (e não o próprio código de PIN introduzido) é armazenado em na estrutura de dados STRUCT (possivelmente com outros dados necessários para efetuar o serviço S desejado). Este resultado, por exemplo um único bit ou uma função Booleana, é um resultado de autenticação do usuário.

Dentro do cartão 120, a estrutura de dados STRUCT é segura. Mais particularmente, em uma maneira convencional o cartão 120 implementa numerosos mecanismos possibilitando a confidencia dos dados que ele armazena ser assegurada.

5                   Uma vez que a estrutura de dados STRUCT foi criada e atualizada, o usuário U desconecta o cartão de microprocessador 120 a partir do dispositivo 100, o efeito disso é acionar a contagem regressiva de uma duração de validade DV se isto já não ocorreu (no caso de acionamento por exemplo a partir do término da carga da capacitância na seqüência de um  
10 comando de carga ou quando uma duração DV é armazenada via um item de informação temporal na memória).

                  O usuário U então conecta o cartão 120 para o dispositivo de processamento 200, por exemplo, introduzindo o cartão em uma localização fornecida para aquele propósito, equipado com um leitor de cartão. O efeito  
15 desta conexão é claro que não para a contagem regressiva de uma duração de validade. Em particular, no caso do uso de uma capacitância, esta contagem regressiva não é parada a não ser que um específico comando de carga seja requerido para ser emitido para recarregá-lo.

                  O dispositivo de processamento 200 é convencionalmente um  
20 dispositivo de baixa confiabilidade e não seguro, tipicamente uma estação/um terminal de pagamento de terceiros, uma caixa pagadora, um Internet serviço de Internet, etc.

                  Como representado na figura, o dispositivo de processamento 200 compreende o leitor 210 para um cartão de microprocessador (ou uma  
25 memória de acordo com o caso) que é compatível com a interface de comunicação 1202 do cartão 120, e compreende um módulo de processamento 220. O dispositivo de processamento 200 também compreende uma interface de usuário (não representado) possibilitando ao usuário interagir com o equipamento em particular para ter acesso a um recurso

desejado.

O processamento módulo 220 assim sendo controla as trocas com o cartão 120 para efetuar aquele acesso para o recurso desejado, e em particular envia para ele uma mensagem para acesso ao recurso. A mensagem  
 5 pode compreender um comando C protegido por autenticação ou chamar uma função, rotina ou comando C, também protegido por autenticação, implementado no cartão 120.

Então é o cartão de microprocessador 120 que controla a execução do comando protegido, por autenticação do usuário U usando os  
 10 dados de autenticação pessoais D2 que ele armazena na estrutura de validade limitada. Este controle torna possível autorizar ou não autorizar a execução do comando, função ou rotina protegida, e assim sendo o acesso ou não ao serviço S desejado. Abaixo, referência principalmente será feita a um “comando protegido” para designar aqueles comandos, funções ou rotinas que  
 15 são protegidos por autenticação.

Dependendo da associada duração de validade DV, o cartão de microprocessador 120 é assim sendo configurado para usar, quando conectado ao dispositivo de processamento 200, os dados de autenticação pessoais D2 armazenados para gerar a autorização ou a recusa para executar o comando  
 20 protegido que ele recebeu.

Nesta maneira, a estrutura de dados STRUCT serve como uma interface entre a entrada de dados confidenciais no dispositivo 100 e seu uso no momento do acesso para o serviço S usando o dispositivo 200.

A invenção também se aplica ao acesso para serviços/recursos  
 25 locais para o dispositivo de processamento 200 (por exemplo., uma funcionalidade daquele dispositivo ou dos dados que ele armazena), sem requerer acesso via uma rede de computador 20 com representado na figura.

No momento do controle da execução do comando protegido por autenticação do usuário, o cartão de microprocessador 120 leva em conta

a duração de validade DV associada com a estrutura STRUCT para usar ou não usar os dados de autenticação pessoais D2 que ela contém.

Assim sendo, quando o usuário gera, no dispositivo de processamento 200, o comando C/C para acesso protegido a um serviço requerendo envolvimento do cartão 120 para verificar os direitos demandados, a validade da estrutura STRUCT é primeiro de tudo verificada pelo cartão na recepção do comando.

Se a duração de validade é explícita (indicação do fim do tempo da validade, por exemplo), o cartão 120 verifica que a duração não expirou, em particular usando o relógio do dispositivo de processamento.

Se está implícito (por exemplo, uso de uma capacitância elétrica), o cartão 120 verifica se a capacitância está totalmente descarregada ou não. Isto pode ser realizado, por exemplo, usando um comando de nível de carga de capacitância, ou pode ser obtida tentando ter acesso à estrutura de dados STRUCT na memória volátil se a última é energizada pela capacitância ou se as propriedades de remanência são usadas. Mais particularmente, nesses casos, se a capacitância é totalmente descarregada ou a duração de remanência expirou, a estrutura de dados é apagada.

No caso de validade da estrutura de dados STRUCT, os dados de autenticação pessoais D2 são acessados, possibilitando ao cartão 120 verificar os direitos demandados, por exemplo, se ou não o código de PIN introduzido é ou não correto. A verificação dos direitos gera uma autorização ou recusa para executar o comando protegido em questão, e assim sendo de acessar o serviço desejado ou não.

O controle de acordo com a invenção assim sendo permite acesso seguro a ser obtido para um grande número de serviços fornecidos pelo dispositivo de processamento 200, via o cartão 120: transação financeira, assinatura digital, consulta de contas, acesso aos dados, etc., enquanto evitando exploração fraudulenta de dados confidenciais introduzidos por um

usuário.

Os dispositivos de entrada 100 e de processamento 200, assim como o cartão de microprocessador 120, compreendem meios de hardware e software configurados para implementar as diferentes etapas e operações aqui descritas.

Abaixo, exemplos serão referidos nos quais a execução de um comando C diretamente indicado na mensagem fornecida pelo dispositivo de processamento é dependente da autenticação bem sucedida do usuário usando os dados de autenticação pessoais contidos na estrutura de validade limitada STRUCT.

Contudo, conforme mencionado acima, um comando, função ou rotina protegida por autenticação pode ser implementada ao processar a mensagem, sem estar explicitamente indicado na mensagem.

Mais ainda pode ser notado que a invenção não é afetada se os dados de autenticação pessoais armazenados na estrutura STRUCT influenciam ou não o resultado fornecido pelo cartão 120 em resposta ao comando C. À título de exemplo, a resposta ao comando C pode ser o valor dos dados de autenticação pessoais armazenados (por exemplo o resultado da autenticação armazenado é produzido). Em um outro exemplo, o valor produzido pode depender do valor dos dados de autenticação pessoais (por exemplo, se um sub-comando C dentre vários não é executado, o resultado pode mudar). Por fim, em um outro exemplo, o resultado produzido é independente de se o comando protegido pela autenticação supra citada é ou não executado (por exemplo, a execução daquele comando permite um indicador interno do cartão 120 a ser atualizado).

Figura 3 ilustra um primeiro exemplo de acesso a um serviço de assinatura digital de acordo com a invenção.

Neste exemplo, o cartão 120 que armazena a estrutura STRUCT é removível. Ainda mais, os meios 1204 são implementados via

uma capacitância elétrica fornecida no cartão 120 para temporariamente alimentar de energia a memória volátil 1203. Ainda mais, os dados D1 introduzidos pelo usuário U são pré-processados no dispositivo de entrada 100 antes da armazenagem do resultado na estrutura STRUCT. Assim sendo,

5 em uma primeira fase P1 começando na etapa E300, o cartão de microprocessador removível (ou módulo de memória) 120 é inserido no dispositivo de entrada 100, aqui o telefone móvel do usuário.

Esta inserção acarreta um sinal de alimentação de energia E302, acionamento da alimentação de energia do cartão de microprocessador 120 e sua iniciação E304 de acordo com mecanismos convencionais. Neste

10 estágio, o microprocessador (não representado) e a memória 1203 do cartão 120 são alimentados de energia por uma fonte de fornecimento de energia principal (a bateria do telefone por exemplo).

Para o propósito da implementação de um serviço S desejado

15 pelo usuário U, o usuário seleciona uma aplicação de pré-processamento via um menu e a interface 110, para o acesso ao serviço (E306).

Um comando para selecionar a aplicação é então gerado (E308) pelo dispositivo de entrada 100 destinado ao cartão 120. Este comando de seleção “Select” é de acordo com o padrão da ISO/IEC 7816-4 p para

20 comunicação entre um cartão de microprocessador 120 e um leitor de cartão 130 (aqui equipando o dispositivo 100).

A aplicação selecionada é então executada (E310) no cartão 120, requerendo a entrada de um item de dados pessoais D1 para identificação ou autenticação do usuário U e possivelmente dados complementares

25 necessários para o serviço desejado. No exemplo, o usuário U introduz, via a interface 110, seu código de PIN (E312).

Um comando de verificação do código de PIN “VERIFY PIN” de acordo com o padrão ISO/IEC 7816-4 supracitado é então fornecido (E314) para o cartão 120. Este comando compreende o código de PIN

introduzido pelo usuário U.

Em uma maneira convencional, o cartão 120 recupera o código de PIN introduzido, então o compara com um código de PIN de referência pré-gravado na memória segura do cartão 120 (E316) a fim de gerar uma resposta positiva OK no caso de PIN correto (E318) e uma resposta negativa NOK no caso de PIN errôneo (E320).

Em maneira paralela, o cartão 120 atualiza (cria se necessário) uma estrutura de dados STRUCT inserindo nele o resultado da comparação E316 (e possivelmente os dados complementares que foram recebidos), em uma etapa E322. Este resultado da comparação é, aqui, nomeado “dados de autenticação pessoais” D2 do usuário.

Na mesma ocasião, o cartão 120 fornece a duração de validade DV associada com a estrutura de dados e assim sendo com os dados de autenticação pessoais D2, enviando um comando para carregar a capacitância 1204. A duração DV é contada regressivamente por exemplo iniciando do fim da carga da capacitância elétrica 1204, até a progressiva descarga daquela capacitância.

Essas ações da etapa E322 podem, por exemplo, ser efetuadas por um programa de controle como a seguir:

```
if PIN OK{
  charge 1204;
  provide OK to STRUCT;
}
else{
  discharge 1204;
  provide NOK to STRUCT;
}
```

Em uma segunda fase P2, o usuário U termina o fornecimento de energia principal do cartão 120 pelo dispositivo de entrada 100, extraíndo o cartão 120 em particular, na etapa E324.

Em virtude da capacitância 1204 no decorrer da descarga, a memória volátil 1203 permanece temporariamente energizada e os dados (em particular STRUCT) que ela armazena são ainda válidos. Se o cartão 120 não

é re-usado antes da expiração de uma duração DV (assim sendo antes de completar a descarga da capacitância), a memória volátil e assim sendo a estrutura STRUCT são apagadas.

Na etapa E326, o cartão 120 é fisicamente movido em direção  
5 ao dispositivo de processamento 200 ao qual ele é então conectado.

A terceira fase P3 então começa pela etapa E328 de comandar a alimentação de energia do cartão (similar à E302), conduzindo a alimentação de energia e iniciação do cartão 120 (E330–similar à E304).

Um comando de destinação de seleção destinado ao cartão 120  
10 é então gerado (E332) em maneira similar para a etapa E308.

Na etapa E334, o usuário procura um serviço de código de PIN protegido (aqui a computação de uma assinatura digital) no dispositivo de processamento 200. Esta detecção aciona o envio de um comando C de “AUTENTICAÇÃO INTERNA” de acordo com o padrão da ISO/IEC 7816-4  
15 (etapa E336). Este comando é parametrizado com os dados para assinar e sua execução é, de acordo com o padrão, dependente da execução de comandos anteriores, por exemplo uma autenticação válida anterior como fornecida em um presente exemplo.

Em virtude da invenção, a condição de código de PIN validado  
20 (ou não validado como o caso pode ser) está presente na estrutura STRUCT do cartão 120 via dados de autenticação pessoais D2, sem o usuário U ter de introduzir seu código de PIN para o dispositivo de processamento 200.

Neste estágio, etapa E338 no cartão 120 consiste em verificar a validade da estrutura STRUCT, levando em consideração a duração de  
25 validade DV associada.

Esta verificação pode em particular consistir em verificar o nível de carga da capacitância 1204 (usando um comando apropriado) e/ou a presença da estrutura STRUCT na memória 1203. Para ser preciso, se a duração de validade expirou (a capacitância 1204 totalmente descarregou)

enquanto o cartão 120 não mai foi energizado, a memória volátil 1203 se tornou apagada e a condição de código de PIN validado não está mais disponível.

Se a duração DV expirou, a estrutura STRUCT pode ser marcada como inválida (por exemplo, via um bit) de modo a simplificar etapa E338 no momento das solicitações de acesso mais tarde.

Se a duração DV não expirou e assim sendo a estrutura STRUCT é de fato válida, na etapa E339, os dados de autenticação pessoais D2 são recuperados da estrutura STRUCT.

Na etapa E340, o comando C de “AUTENTICAÇÃO INTERNA” é executado levando em consideração os dados de autenticação pessoais D2 recuperados, como direitos requeridos. Assim sendo é executado exclusivamente se aqueles dados D2 revelam uma condição de código de PIN validado.

Por exemplo, uma particular função COPY D2 pode ser executada pelo cartão nesta etapa para copiar os dados D2 em um variável global convencionalmente usada para armazenar o resultado de um autenticação de PIN e que é acessada pela execução do comando de AUTENTICAÇÃO INTERNA. Assim sendo, ela não é modificada.

É claro que, como uma variante, uma função de VALIDATE PIN OK pode ser chamada para diretamente verificar se uma condição de código de PIN validado está de fato presente, e naquele caso diretamente autoriza a execução do comando de AUTENTICAÇÃO INTERNA.

No caso de uma condição de código de PIN validado, a assinatura dos dados a assinar, usando uma chave que é interna ao cartão 120, é realizada.

Devido a isto, a assinatura digital de dados (ou o acesso aos recursos/serviços) é protegida por uma verificação dos dados D2 positiva.

O cartão 120 então envia, para o dispositivo de processamento

200, uma resposta ao comando: os dados assinados (E342) ou uma mensagem de erro (E344) dependendo se foi possível executar o comando ou não.

A Figura 4 ilustra um segundo exemplo de acesso a um serviço de assinatura digital de acordo com a invenção e que é substancialmente similar àquele da Figura 3, além do fato que os dados pessoais D1 como introduzidos pelo usuário U são diretamente armazenados (sem modificação) na estrutura STRUCT.

Ainda mais, em vez de introduzir o código de PIN, este exemplo implementa a aquisição de uma medição biométrica do usuário U, por exemplo um impressão digital de dedo.

Na fase P1, as etapas E300 à E312 são similares àquelas descritas com referência à Figura 3, além do fato que o usuário U é solicitado a adquirir uma impressão digital de dedo mais propriamente do que um código de PIN.

Na etapa E312 consistindo em introduzir os dados confidenciais D1 pelo usuário U, os últimos presentes em um dedo para o sensor biométrico 110 a fim de adquiri os dados pessoais D1 para identificar quais representam a impressão digital de dedo.

Esses dados confidenciais D1 são fornecidos para o cartão 120 através de um comando de "PUT DATA" de acordo com o padrão da ISO/IEC 7816-4 (etapa E314').

No cartão 120, esses dados D1 são recuperados e então armazenados diretamente na estrutura de dados STRUCT (etapa E322').

É claro que dados complementares podem ser introduzidos/adquiridos pelo usuário U e armazenados em adição na estrutura STRUCT.

Neste estágio, a contagem regressiva de uma duração de validade DV pode ser acionada, pelo comando para carregara a capacitância 1204.

Adicionalmente a fase P1, fase P2 é similar aquela da Figura 3, i.e. compreendendo as etapas E324 e E326.

Fase P3 começa na mesma maneira que a mesma fase da Figura 3, com as etapas E328 à E332 em particular.

5 O dispositivo de processamento 200 pode ser configurado para enviar, na detecção do cartão 120, um comando para processar os dados D1 armazenados na estrutura STRUCT (etapa E336), no exemplo um comando para verificar a impressão digital de dedo com uma impressão digital de dedo de referência pré-gravada na memória do cartão 120.

10 É para ser notado que esta verificação pode ser realizada no cartão 120 em resposta ao comando C protegido conforme fornecido abaixo, sem ter de recorrer a este comando E336 anterior.

Na etapa E338, a validade da estrutura STRUCT é verificada com relação à duração DV associada.

15 Se a estrutura não é mais válida, é indicado como tal e uma resposta negativa NOK (E344) é enviada de volta para o dispositivo de processamento 200.

Se a estrutura é válida, os dados D1 são recuperados a partir da estrutura STRUCT na etapa E339.

20 As impressões digitais de dedo D1 adquiridas na fase P1 são então comparada (E340) com as impressões digitais de dedo de referência.

O resultado da comparação, correto OK (E342) ou incorreto NOK (E344), é retornado para o dispositivo de processamento 200.

25 Em paralelo, o resultado da comparação é armazenado em uma variável global (do cartão), convencionalmente usado para armazenar o resultado de uma autenticação por dados biométricos, e acessado pela execução mais tarde de um comando protegido tal como AUTENTICAÇÃO INTERNA.

Como uma variante, este resultado pode ser diretamente

armazenado em uma estrutura de dados STRUCT com condição de dados biométricos válida ou errônea.

Na etapa E346 o dispositivo de processamento 200 detecta que o usuário U está procurando um serviço (aqui a computação de uma assinatura digital) protegido por autenticação biométrica e assim sendo requerendo autenticação do usuário. Esta solicitação de serviço aciona o envio de um comando C de “AUTENTICAÇÃO INTERNA” de acordo com o padrão ISO/IEC 7816-4 (etapa E348), tendo como parâmetro os dados a assinar e sendo protegida por autenticação do usuário.

O cartão 120 então executa (E350) o comando C de “AUTENTICAÇÃO INTERNA”.

É para ser notado que se na etapa E340 o resultado da comparação é armazenado na variável global convencional, etapa E350 é ainda convencional, o comando AUTENTICAÇÃO INTERNA sendo condicional na presença de uma condição validada naquela variável global.

No caso da variante, uma função VALIDATE DATA OK pode ser executada para verificar na estrutura STRUCT a presença ou ausência da condição validada, e conseqüentemente autoriza ou não autoriza o comando AUTENTICAÇÃO INTERNA.

Onde apropriado os dados a assinar são assinados usando uma chave interna do cartão 120, de acordo com mecanismos convencionais.

O cartão então envia uma resposta para o comando de AUTENTICAÇÃO INTERNA, destinado ao dispositivo de processamento: os dados assinados (E352) ou uma mensagem de erro (E354).

Uma vez de novo, a assinatura digital dos dados (ou o acesso aos recursos/serviços) é protegida por uma verificação positiva dos dados biométricos.

Figura 5 ilustra um terceiro exemplo de assinatura digital de acordo com a invenção substancialmente similar àquele da Figura 3, no qual o

cartão 120 armazenando a estrutura STRUCT é permanentemente acomodado no dispositivo de entrada 100 (pelo menos durante a totalidade das operações descritas abaixo correspondendo ao todo do processo de autenticação do usuário U). Isto é, por exemplo, o caso para um cartão SIM em um telefone móvel.

Neste caso, as etapas E300 à E322 da fase P1 são idênticas as etapas da fase P1 da Figura 3.

Como para a fase P2, que está vazia já que não há dissociação física entre o cartão 120 e o equipamento 100. Esta fase P2 assim sendo começa assim que os dados pessoais de entrada para identificação D1 foram processados pelo cartão 120 sob o comando do dispositivo de entrada 100, isto é para dizer assim que as estruturas de dados STRUCT foram geradas com os dados D2 resultando do processamento. De forma similar, contagem regressiva da duração de validade começa a partir do final deste processamento, através da carga da capacitância 1204 por exemplo.

Durante a fase P3, o grupo {dispositivo de entrada 100—cartão 120} se comunica com o dispositivo de processamento 200, por exemplo, com a ajuda de um protocolo de comunicação sem contato (NFC ou equivalente).

É para ser notado que de acordo com uma modalidade, o dispositivo de processamento 200 pode diretamente se comunicar com o cartão 120. Isto é o caso no exemplo da Figura 2, onde a interface de comunicação 1202 possibilita comunicação direta com o equipamento 200. É para ser notado que se duas interfaces de comunicação 1201 e 1202 estão unidas, são fornecidas para desativar o leitor 130 do dispositivo de entrada 100 de modo a possibilitar comunicação do cartão 120 com dispositivo de processamento 200 sem interferência. Por outro lado, meios para diferenciar as comunicações com cada uma das interfaces 1201 e 1202 podem ser fornecidos.

Em uma variante, o dispositivo de processamento 200 pode se comunicar com o dispositivo de entrada 100 que então supre a informação e solicitações para o cartão 120. Neste caso o cartão 120 pode ser equipado com um único interface 1201 para comunicação com o leitor 130.

5                Figura 5 ilustra fase P3 no caso no qual o dispositivo de processamento 200 se comunica diretamente com o cartão 120.

A iniciação da comunicação entre essas duas entidades é realizada durante trocas de mensagens convencionais, representada na figura pela etapa E330'.

10              Seguindo as etapas E332 à E344 são similares as etapas comportando as mesmas referências da Figura 3.

É claro que, as diferentes modalidades referidas antes acima para os três exemplos da Figuras 3 à 5 podem ser aplicadas à cada um daqueles exemplos, por exemplo para modificar os meios 1204, a natureza da memória 1203, a interfaces de comunicação 1201 e 1202, para substituir o  
15              cartão de microprocessador 120 por uma módulo de memória fornecido com um micro-controlador possibilitando comunicação com os leitores 30 e 210, etc.

Os exemplos precedentes são somente modalidades da  
20              invenção que não é limitado a isto.

Em particular, embora a invenção tenha sido ilustrada acima para o acesso a um serviço de assinatura digital, ela pode igualmente ser aplicada ao acesso para dados armazenados ou para outros recursos.

Por exemplo, dados pessoais (biométricos, fotográficos ou de  
25              identificação) são armazenados em uma passaporte eletrônico mas que é acessível de modo único, após autenticação. Usando um telefone móvel, o usuário pode pré-autorizar o acesso àqueles dados introduzindo um código de PIN gerando uma a estrutura de validade limitada STRUCT com a condição do código de PIN validado/errôneo, através do mecanismos de acordo com a

invenção.

O oficial da alfândega pode assim sendo acessar os dados pessoais em virtude desta pré-autorização durante uma duração de validade DV.

## REIVINDICAÇÕES

1. Método para controlar a execução de uma função protegida por autenticação, caracterizado pelo fato de compreender as seguintes etapas:

- armazenar, em uma estrutura de validade limitada, dados de autenticação pessoais dependentes dos dados pessoais de entrada, introduzindo os últimos por um usuário em um dispositivo de entrada;
- verificar a validade da estrutura de validade limitada antes de usar os dados de autenticação pessoais que ela contém para gerar uma autorização ou uma recusa para executar uma função implementada no processamento de uma mensagem gerada por um dispositivo de processamento que é distinto do dispositivo de entrada.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de compreender as seguintes etapas:

- introduzir, pelo usuário, os dados pessoais usando o dispositivo de entrada;
  - autenticar o usuário nas bases dos dados pessoais de entrada para gerar a autorização ou a recusa para executar a função protegida;
  - executar uma função no caso de autorização;
- em que:
- as etapas de armazenar e verificar são implementadas em um módulo de memória respectivamente conectado ao dispositivo de entrada no momento das etapas de entrada e armazenamento, e ao dispositivo de processamento no momento das etapas de verificação e execução;
  - a mencionada estrutura de validade limitada compreende dados de autenticação pessoais de validade limitada por associação de uma duração de validade com os dados de autenticação pessoais.

3. Método de acordo com a reivindicação 1, caracterizado pelo fato de que gerar a autorização ou a recusa é dependente de uma verificação dos dados pessoais introduzidos com dados de referência, o resultado da

verificação sendo obtido usando os mencionados dados de autenticação pessoais armazenados na estrutura de validade limitada armazenada.

4. Método de acordo com a reivindicação 2, caracterizado pelo fato de compreender uma etapa de comparar dados pessoais de entrada com dados pessoais pré-gravados no módulo de memória, e os dados de autenticação pessoais armazenados na estrutura de validade limitada compreende o resultado da comparação.

5. Método de acordo com reivindicação 1, caracterizado pelo fato de que os dados de autenticação pessoais armazenados na estrutura de validade limitada compreende os dados pessoais de entrada, e seu uso compreende uma sub-etapa de comparar os dados de autenticação pessoais armazenados na estrutura de validade limitada com dados pessoais pré-gravados.

6. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a mencionada estrutura de validade limitada compreende dados de autenticação pessoais de validade limitada através de associação de uma duração de validade com os dados de autenticação pessoais, e

- a duração de validade associada com os dados de autenticação pessoais é contabilizada através da descarga de uma capacitância elétrica.

7. Método de acordo com a reivindicação 6, caracterizado pelo fato de que os dados de autenticação pessoais são armazenados em uma memória volátil, temporariamente energizada pela mencionada capacitância elétrica.

8. Método de acordo com a reivindicação 1, caracterizado pelo fato de que os dados de autenticação pessoais são armazenados em uma memória volátil de um módulo de memória, que é continuamente energizado durante o controle da execução da função protegida ou em uma memória de re-escrita, e uma duração de validade associada com eles é definida

armazenando uma quantidade temporal em uma variável que é associada na memória com os dados de autenticação pessoais.

9. Método de acordo com a reivindicação 1, caracterizado pelo fato de que a função protegida é um comando implementado, na recepção de uma mensagem proveniente do dispositivo de processamento, através de um módulo de microprocessador armazenando a estrutura de validade limitada.

10. Método de acordo com a reivindicação 1, caracterizado pelo fato de que um módulo de memória armazenando a estrutura de validade limitada e os dados de autenticação pessoais que ela contém são removidos, e são colocados no dispositivo de entrada no momento da entrada e colocados no dispositivo de processamento no momento da verificação da validade da estrutura e no momento do uso dos dados de autenticação pessoais de validade limitada.

11. Método de acordo com a reivindicação 1, caracterizado pelo fato de que um módulo de memória armazenando a estrutura de validade limitada e os dados de autenticação pessoais que ela contém é fisicamente ligada com ao equipamento de entrada durante o controle e execução da função protegida, e o equipamento de processamento se comunica com um módulo de memória através de comunicação sem contato.

12. Método de acordo com a reivindicação 10 ou 11, caracterizado pelo fato de que um módulo de memória armazenando a estrutura de validade limitada e os dados de autenticação pessoais é um cartão de microprocessador seguro.

13. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o processamento da mensagem a partir do dispositivo de processamento gera uma resposta caracterizada pelo fato de compreender pelo menos um valor de resposta que depende da autorização ou da recusa gerada.

14. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o dispositivo de entrada é um telefone móvel do usuário.

15. Módulo de memória, caracterizado pelo fato de compreender pelo menos uma memória e um processador para executar instruções, o módulo de memória sendo configurado para:

5 - armazenar, em uma estrutura de validade limitada, dados de autenticação pessoais que são dependente dos dados pessoais introduzidos por um usuário e recebidos de um dispositivo de entrada para o qual o módulo de memória está ligado;

10 - verificar a validade da estrutura de validade limitada antes de usar os dados de autenticação pessoais que ela contém gerar uma autorização ou uma recusa para executar uma função protegida por autenticação e implementada no processamento de uma mensagem recebida a partir de um dispositivo de processamento que é distinto do dispositivo de entrada.

15 16. Sistema para controlar a execução de uma função protegida por autenticação de um usuário, caracterizado pelo fato de compreender:

- um dispositivo de entrada para introduzir dados pessoais pelo usuário;

20 - um dispositivo de processamento que é distinto do dispositivo de entrada e adaptado para gerar, sob a ação do usuário, uma mensagem para processar;

25 - um módulo de memória compreendendo pelo menos uma memória e um processador, e que é configurado para autenticar o usuário nas bases dos dados pessoais de entrada a fim de gerar uma autorização ou uma recusa para executar uma função protegida implementada no processamento da mencionada mensagem;

em que o módulo de memória é configurado para:

- quando ele está conectado ao dispositivo de entrada, gerar e armazenar, em sua memória, dados de autenticação pessoais de validade limitada que são dependentes dos dados pessoais de entrada e associando-os

com um parâmetro de validade; e

- quando ele está conectado ao dispositivo de processamento, usando os dados de autenticação pessoais armazenados para gerar a autorização ou a recusa para executar a função dependendo do parâmetro de validade associado.

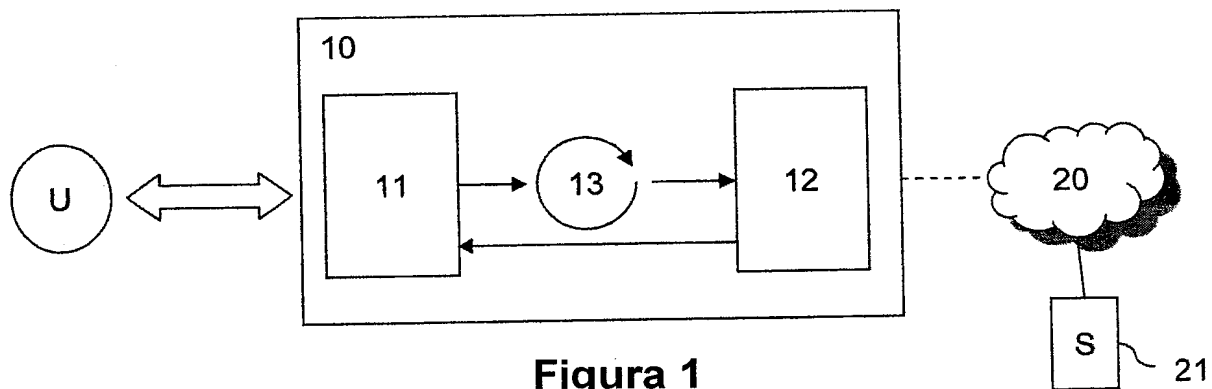
17. Entidade eletrônica, caracterizada pelo fato de compreender:

- pelo menos uma interface de comunicação para receber dados pessoais de entrada por um usuário e uma mensagem para processar,

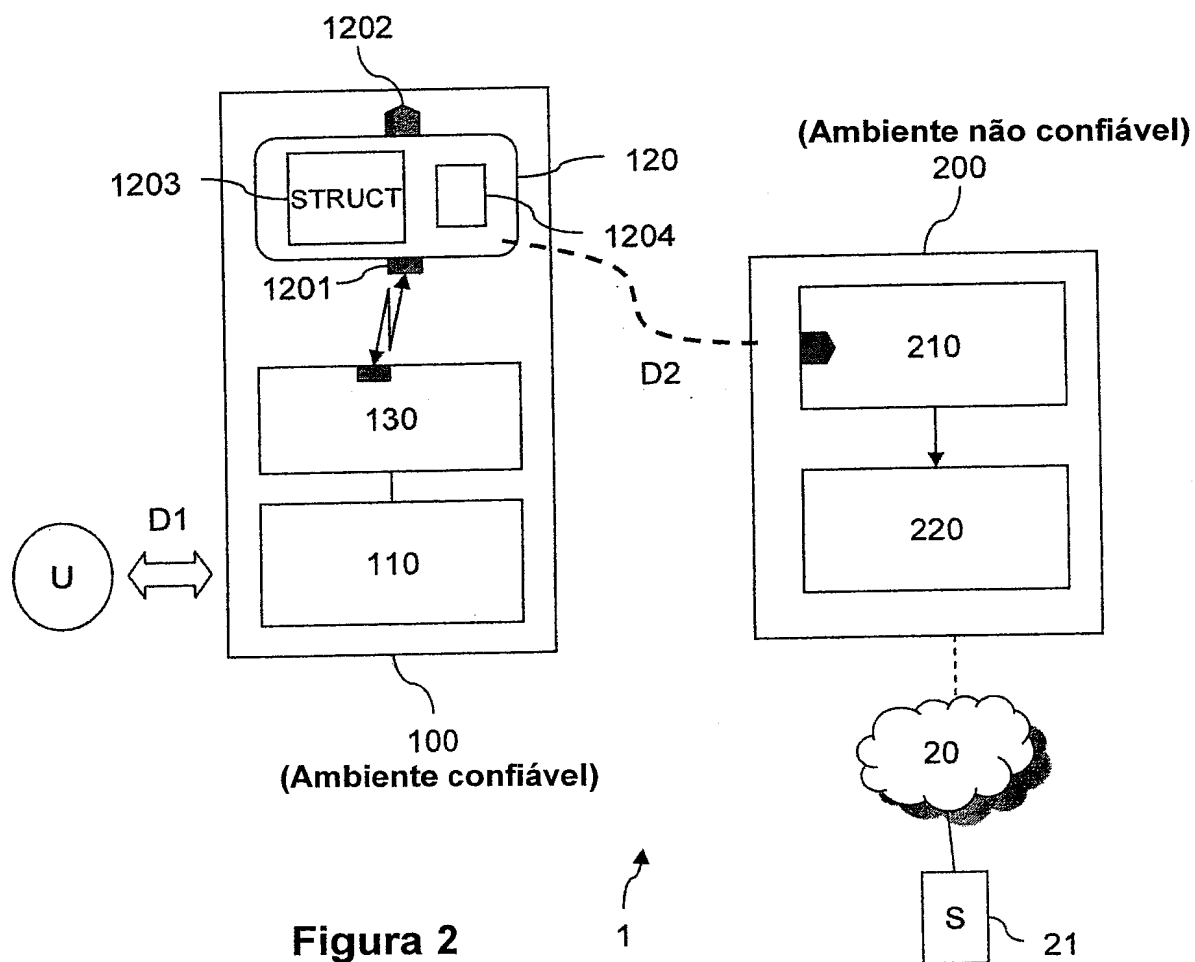
- uma memória que armazena, em uma estrutura de validade limitada de dados, dados de autenticação pessoais que são dependente dos dados pessoais de entrada,

- uns meios para limitar, no tempo ou no espaço, a validade da estrutura de dados armazenando os dados de autenticação pessoais, e

- uns meios para verificar a validade da estrutura de validade limitada antes usando os dados de autenticação pessoais que ela contém para gerar uma autorização ou uma recusa para executar uma função protegida por autenticação e implementada no processamento da mensagem recebida.



**Figura 1**  
Técnica Anterior



**Figura 2**

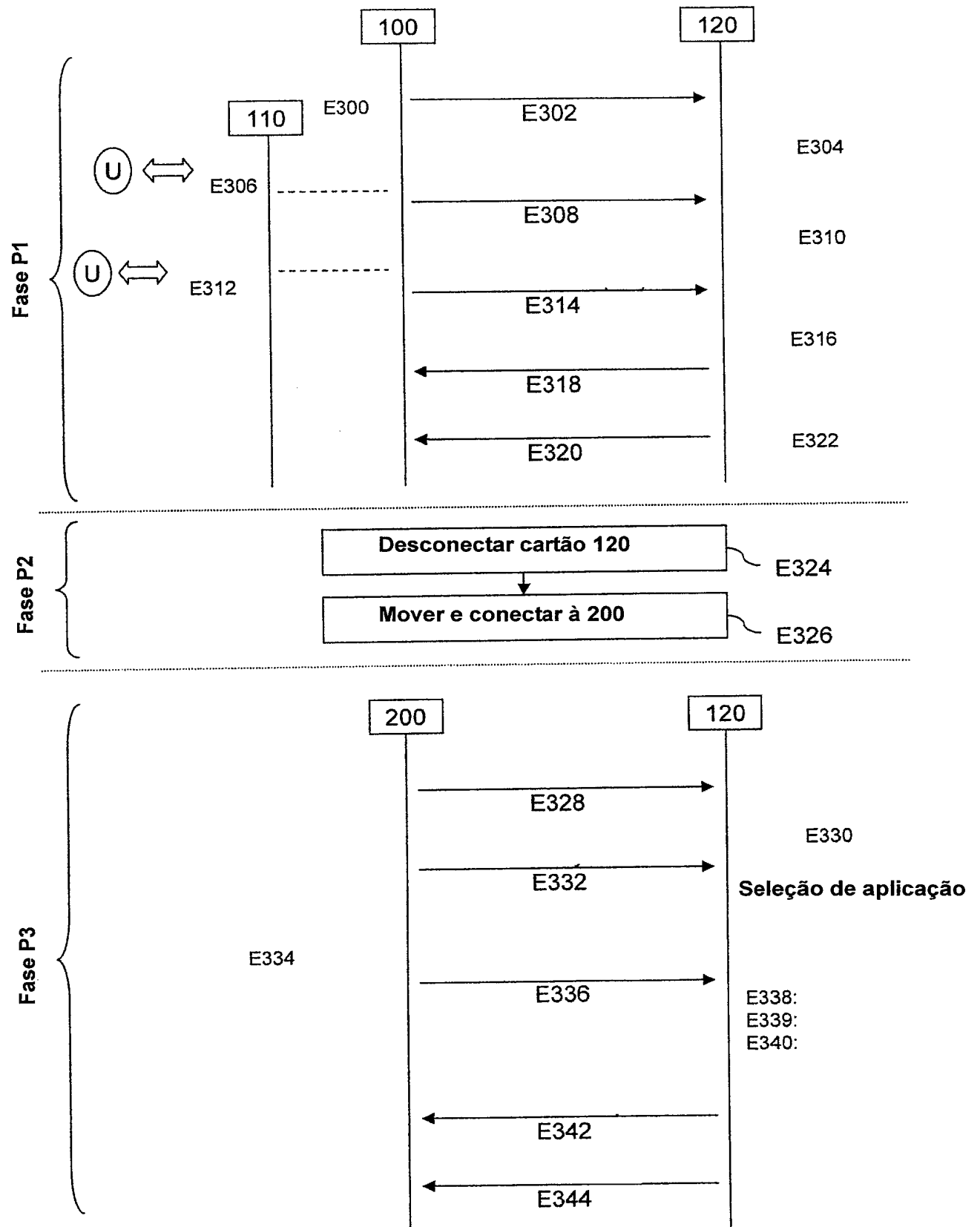


Figura 3

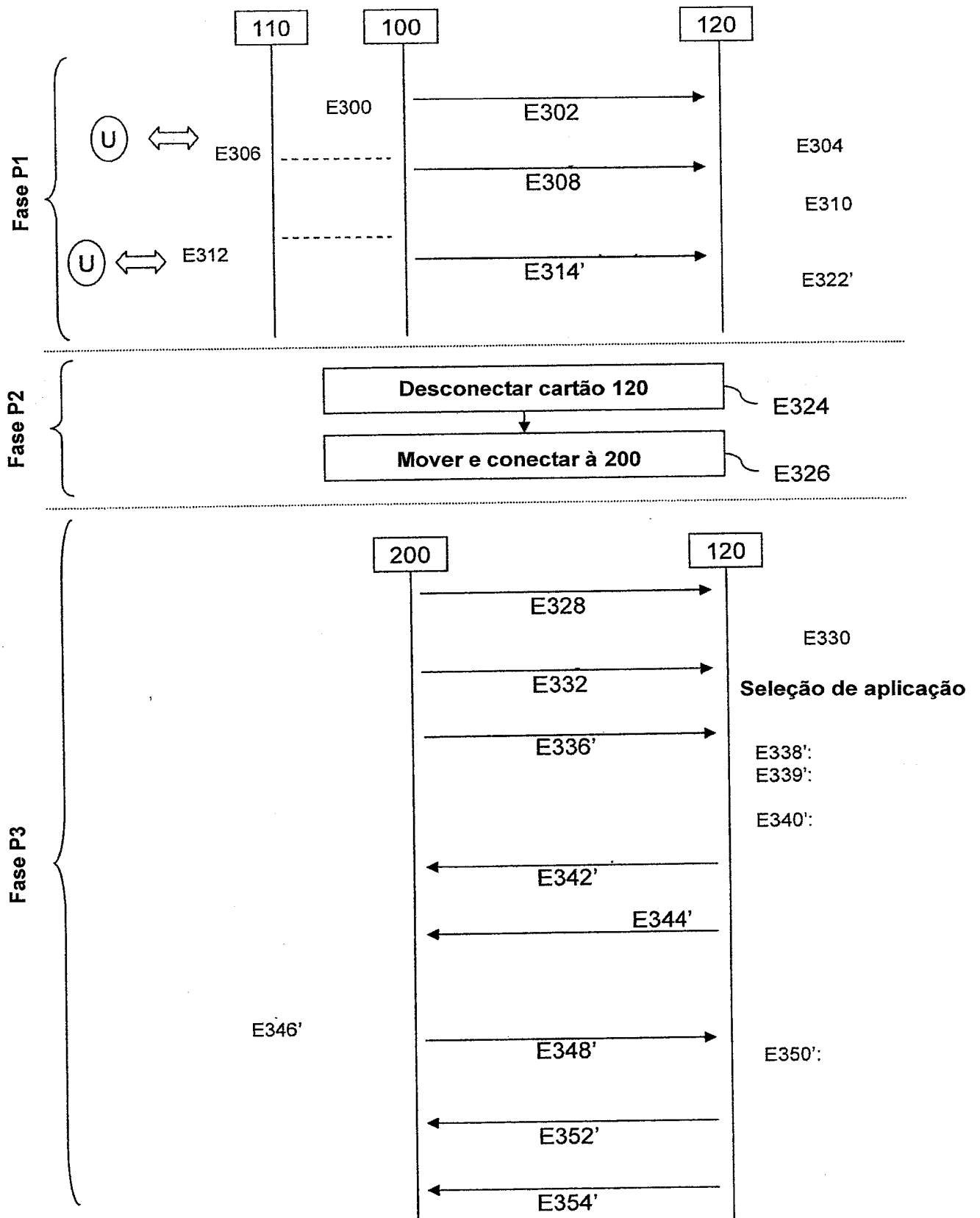


Figura 4

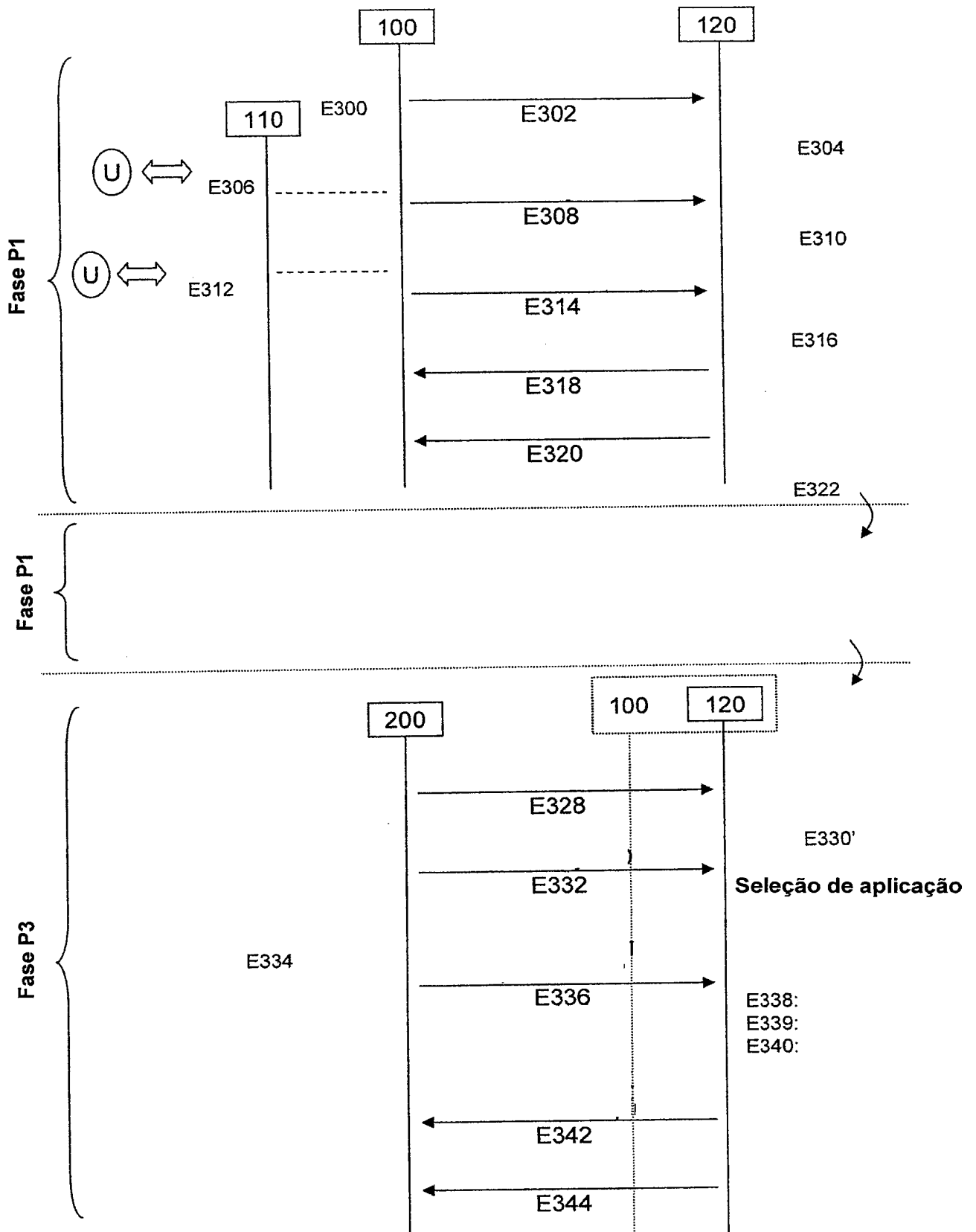


Figura 5

## RESUMO

‘MÉTODO E SISTEMA PARA CONTROLAR A EXECUÇÃO DE UMA FUNÇÃO PROTEGIDA POR AUTENTICAÇÃO, MÓDULO DE MEMÓRIA, E, ENTIDADE ELETRÔNICA’

5                   A presente invenção envolve um método e sistema para controlar a execução de uma função protegida por autenticação de um usuário e que é fornecida por exemplo para o acesso a uns recursos O método compreende introduzir, pelo usuário, dados pessoais usando um dispositivo de entrada, autenticar o usuário com os dados pessoais de entrada para autorizar  
10                   ou não autorizar a execução da função; em um cartão seguro conectado para o dispositivo de entrada, armazenar dados de autenticação de validade limitada dependente dos dados de entrada; quando o cartão está conectado a um dispositivo de processamento através do qual o usuário gera uma mensagem cujo processamento implementa a mencionada função, usando os dados  
15                   armazenados, levando em consideração a validade limitada, para autorizar ou não autorizar a execução daquela função.