

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

(21) **PI 0713470-3 A2**

(22) Data de Depósito: 19/06/2007
(43) Data da Publicação: 24/01/2012
(RPI 2142)



(51) *Int.Cl.:*
G06F 21/22

(54) Título: PROCESSO PARA DELEGAÇÃO DE PRIVILÉGIOS A UMA INSTÂNCIA DE PRIVILÉGIO INFERIOR POR UMA INSTÂNCIA DE PRIVILÉGIO SUPERIOR

(30) Prioridade Unionista: 27/06/2006 DE 10 2006 029 756.3

(73) Titular(es): Deutsche Telekom AG, T-Mobile International AG

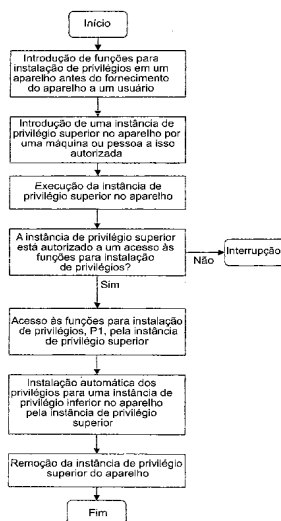
(72) Inventor(es): Katrin Jordan, Rainer Hillebrand, Stefan Schröder, Uwe Wilhelm

(74) Procurador(es): Dannemann ,Siemsen, Bigler & Ipanema Moreira

(86) Pedido Internacional: PCT EP2007005364 de 19/06/2007

(87) Publicação Internacional: WO 2008/000369de 03/01/2008

(57) Resumo: PROCESSO PARA DELEGAÇÃO DE PRIVILÉGIOS A UMA INSTÂNCIA DE PRIVILÉGIO INFERIOR POR UMA INSTÂNCIA DE PRIVILÉGIO SUPERIOR. A presente invenção refere-se a um processo para delegação de privilégios a uma instância de privilégio inferior por uma instância de privilégio superior, em que a instalação de privilégios, P1, para uma instância de privilégio inferior é executada automaticamente em um aparelho de processamento de dados, na medida em que o aparelho antes do fornecimento a um usuário ou por tele-transferência de dados é provido de funções para a instalação dos privilégios, para com auxílio de uma instância de privilégio superior, que é provida de privilégios especiais, P2, para concessão de privilégios, poder instalar privilégios, P1, para a instância de privilégio inferior.





PI0713470-3

Relatório Descritivo da Patente de Invenção para "PROCESSO PARA DELEGAÇÃO DE PRIVILÉGIOS A UMA INSTÂNCIA DE PRIVILÉGIO INFERIOR POR UMA INSTÂNCIA DE PRIVILÉGIO SUPERIOR".

A presente invenção refere-se a conferir controladamente privilégios a uma instância em um aparelho, como, por exemplo um terminal móvel, uma instância de privilégio superior, que possui o privilégio especial de conferir ela própria privilégios, instala os privilégios da instância de privilégio inferior no aparelho. Para tanto, usualmente é necessário que uma pessoa tenha um acesso físico a esse aparelho.

Um exemplo para um privilégio é o direito de acesso a uma função de um aparelho. Poder-se-ia verificar se uma instância possui o privilégio requerido, por exemplo por meio de uma assinatura criptográfica com a qual a instância é provida. Para tanto, por exemplo a uma função, como, por exemplo a leitura de uma lista de contatos, poderia ser associado ao aparelho assim chamado certificado "Root" para "Code Signing". Quando a assinatura pode ser verificada com sucesso com o certificado "Root", a instância recebe o privilégio de acessar a função se necessário.

Uma instância de privilégio superior poderia ser, por exemplo um software. Usualmente é empregado o seguinte processo:

Uma pessoa, por exemplo assim chamado administrador, coloca um aparelho em um estado, em que ele tem os privilégios necessários para a execução de um software, com o qual os privilégios para um software menos privilegiado podem ser instalados. Esse estado pode também ser designado como assim chamado estado de administração.

Aquele que usa o software menos privilegiado usualmente não pode colocar o aparelho nesse estado de administração.

O software para a instalação dos privilégios é executado pelo administrador e os privilégios são instalados.

O administrador tira novamente o aparelho do estado de administração.

A desvantagem do processo usualmente empregado reside em que um administrador precisa ter acesso físico ao aparelho. O administrador

caminha ou viaja para o local em que o aparelho se encontra ou o aparelho é trazido ao administrador. Em ambos os casos há custos: no primeiro caso, pelo tempo em que o administrador deixa de trabalhar no caminho para o aparelho, quer em meios de transporte como automóvel ou trem. No segundo caso, pelo tempo que o aparelho não é usado ou leva no transporte. Em
5 ambos os casos, além disso, resultam outros custos devido ao tempo de trabalho necessário para a instalação individual e administração. A isso acrescentam despesas com instrução, etc.

Essa problemática não deve ser confundida com a importação
10 de um certificado Root adicional em um Browser, entre outros, pelo usuário. Este último não está vinculado a uma concessão de privilégios (autorização) a instâncias habilitadas. Ele permite apenas a autenticação de instâncias habilitadas.

O objetivo da invenção reside, portanto, em indicar um processo
15 aperfeiçoado para a delegação de privilégios a uma instância de privilégio inferior por uma instância de privilégio superior.

Esse objetivo é alcançado, segundo a invenção, pelas características da reivindicação 1, a cujo teor se remete nesse ponto.

Configurações preferidas e características vantajosas da invenção se depreendem das reivindicações dependentes, a cujo teor se remete
20 nesse ponto.

Com a invenção deve ser conseguido, entre outros, reduzir o trabalho e assim os custos para a instalação de privilégios.

O processo segundo a invenção se baseia em que a instalação
25 de privilégios em aparelhos pode ser executada automaticamente e sem intervenção de um administrador. Para tanto, antes do fornecimento ao proprietário ou usuário o aparelho deve ter sido provido dos necessários privilégios, que são necessários para com uma instância mais privilegiada, que é provida de privilégios especiais para a concessão de privilégios, se poder
30 instalar privilégios para instâncias de privilégio inferior.

Para se instalar um privilégio em um aparelho, uma máquina ou pessoa a isso autorizada transmite uma instância de privilégio superior ao

usuário do aparelho ou diretamente ao aparelho. No primeiro caso, o usuário instala a instância no aparelho. No segundo caso, por exemplo já quando do fornecimento do aparelho ao usuário está presente no aparelho ou pode ser transmitida ao aparelho através de uma interface aérea. A instância é levada
5 à execução no aparelho com ou sem interação com o usuário. O aparelho pode, por exemplo verificar, com auxílio da assinatura criptográfica na instância, se a instância está autorizada a instalar privilégios menores para outras instâncias. Quando este é o caso, a instância tem acesso, por exemplo às funções especiais para instalação de privilégios. A instância, em seguida,
10 instala os privilégios, sem que o usuário deva levar o aparelho a um outro estado. Depois de os privilégios terem sido instalados com sucesso, a instância pode novamente ser removida do aparelho.

Em seguida, depois da instalação dos novos privilégios, instâncias a eles autorizadas podem então reivindicar esses privilégios inferiores.

15 A figura 1 mostra um decurso preferido do processo segundo a invenção.

REIVINDICAÇÕES

1. Processo para delegação de privilégios a uma instância de privilégio inferior por uma instância de privilégio superior, em que a instalação de privilégios, P1, para uma instância de privilégio inferior é executada automaticamente em um aparelho de processamento de dados, na medida em que o aparelho antes do fornecimento a um usuário ou por transferência de dados é provido de funções para a instalação dos privilégios, para com auxílio de uma instância de privilégio superior, que é provida de privilégios especiais, P2, para concessão de privilégios, poder instalar privilégios, P1, para a instância de privilégio inferior.

2. Processo, de acordo com a reivindicação 1, caracterizado pelo fato de que para a instalação dos privilégios, P1, para a instância de privilégio inferior são executadas as seguintes etapas:

- instalação da instância de privilégio superior no aparelho por uma máquina ou pessoa a isso autorizada,
- execução da instância de privilégio superior no aparelho,
- acesso às funções para instalação de privilégios, P1, pela instância de privilégio superior,
- instalação automatizada dos privilégios, P1, para a instância de privilégio inferior no aparelho pela instância de privilégio superior.

3. Processo, de acordo com uma das reivindicações 1 ou 2, caracterizado pelo fato de que a instância de privilégio superior é disponibilizada ao usuário e por ele instalada no aparelho.

4. Processo, de acordo com uma das reivindicações 1 ou 2, caracterizado pelo fato de que a instância de privilégio superior já está presente no aparelho quando do fornecimento do aparelho ao usuário ou é transmitida diretamente ao aparelho por uma interface aérea.

5. Processo, de acordo com uma das reivindicações 1 a 4, caracterizado pelo fato de que a instância de privilégio superior é executada automaticamente no aparelho.

6. Processo, de acordo com uma das reivindicações 1 a 4, caracterizado pelo fato de que a instância de privilégio superior é executada

por uma interação com o usuário no aparelho.

7. Processo, de acordo com uma das reivindicações 1 a 6, caracterizado pelo fato de que, com base em uma assinatura criptográfica na instância de privilégio superior, o aparelho verifica se a instância de privilégio superior está autorizada a ter acesso às funções para instalação de privilégios, P1, e a instalar privilégios, P1, para uma instância de privilégio inferior.

8. Processo, de acordo com uma das reivindicações 1 a 7, caracterizado pelo fato de que a instância de privilégio superior é removida do aparelho, depois de os privilégios, P1, para a instância de privilégio inferior terem sido instalados com sucesso.

9. Aplicativo de software com um código de programa, que executado em um aparelho de processamento de dados realiza um processo como definido nas reivindicações 1 a 8.

10. Produto de programa de processamento de dados, que abrange um aplicativo de software executável em um aparelho de processamento de dados para realização do processo como definido nas reivindicações 1 a 8.

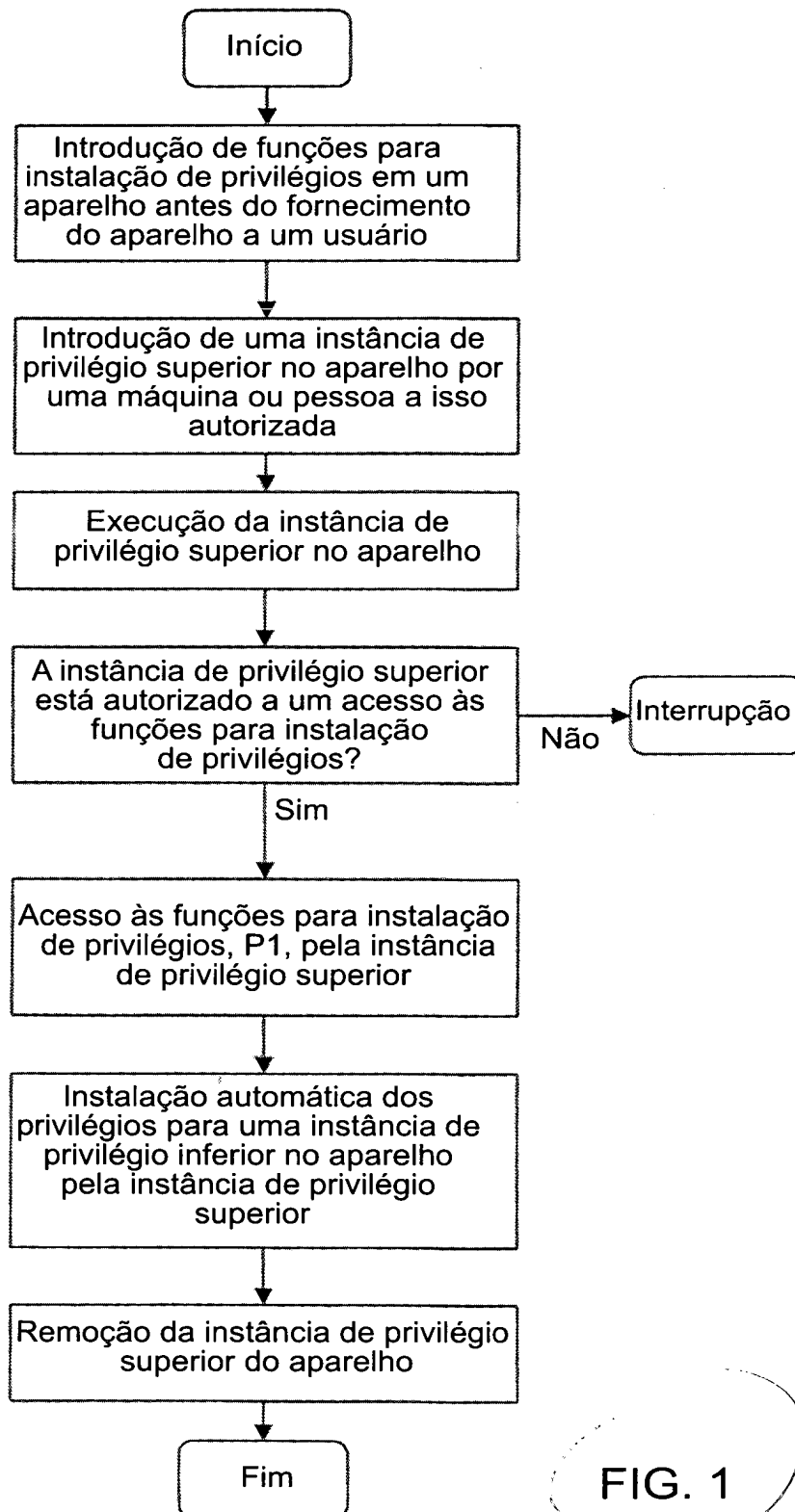


FIG. 1

RESUMO

Patente de Invenção: **"PROCESSO PARA DELEGAÇÃO DE PRIVILÉGIOS A UMA INSTÂNCIA DE PRIVILÉGIO INFERIOR POR UMA INSTÂNCIA DE PRIVILÉGIO SUPERIOR"**.

- 5 A presente invenção refere-se a um processo para delegação de privilégios a uma instância de privilégio inferior por uma instância de privilégio superior, em que a instalação de privilégios, P1, para uma instância de privilégio inferior é executada automaticamente em um aparelho de processamento de dados, na medida em que o aparelho antes do fornecimento a
- 10 um usuário ou por tele-transferência de dados é provido de funções para a instalação dos privilégios, para com auxílio de uma instância de privilégio superior, que é provida de privilégios especiais, P2, para concessão de privilégios, poder instalar privilégios, P1, para a instância de privilégio inferior.

Novo relatório descritivo, incorporando as alterações correspondentes às das páginas 2, 2a do pedido PCT, conforme relatório de exame preliminar.

Relatório Descritivo da Patente de Invenção para "**PROCESSO PARA DELEGAÇÃO DE PRIVILÉGIOS A UMA INSTÂNCIA DE PRIVILÉGIO INFERIOR POR UMA INSTÂNCIA DE PRIVILÉGIO SUPERIOR**".

A presente invenção refere-se a conferir controladamente privilégios a uma instância em um aparelho, como, por exemplo um terminal móvel, uma instância de privilégio superior, que possui o privilégio especial de conferir ela própria privilégios, instala os privilégios da instância de privilégio inferior no aparelho. Para tanto, usualmente é necessário que uma pessoa tenha um acesso físico a esse aparelho.

Um exemplo para um privilégio é o direito de acesso a uma função de um aparelho. Poder-se-ia verificar se uma instância possui o privilégio requerido, por exemplo por meio de uma assinatura criptográfica com a qual a instância é provida. Para tanto, por exemplo a uma função, como, por exemplo a leitura de uma lista de contatos, poderia ser associado ao aparelho assim chamado certificado "Root" para "Code Signing". Quando a assinatura pode ser verificada com sucesso com o certificado "Root", a instância recebe o privilégio de acessar a função se necessário.

Uma instância de privilégio superior poderia ser, por exemplo um software. Usualmente é empregado o seguinte processo:

Uma pessoa, por exemplo assim chamado administrador, coloca um aparelho em um estado, em que ele tem os privilégios necessários para a execução de um software, com o qual os privilégios para um software menos privilegiado podem ser instalados. Esse estado pode também ser designado como assim chamado estado de administração.

Aquele que usa o software menos privilegiado usualmente não pode colocar o aparelho nesse estado de administração.

O software para a instalação dos privilégios é executado pelo administrador e os privilégios são instalados.

O administrador tira novamente o aparelho do estado de administração.

A desvantagem do processo usualmente empregado reside em que um administrador precisa ter acesso físico ao aparelho. O administrador

caminha ou viaja para o local em que o aparelho se encontra ou o aparelho é trazido ao administrador. Em ambos os casos há custos: No primeiro caso, pelo tempo em que o administrador deixa de trabalhar no caminho para o aparelho, quer em meios de transporte como automóvel ou trem, No segundo caso, pelo tempo que o aparelho não é usado ou leva no transporte. Em
5 ambos os casos, além disso, resultam outros custos devido ao tempo de trabalho necessário para a instalação individual e administração. A isso acrescentam despesas com instrução, etc.

Essa problemática não deve ser confundida com a importação
10 de um certificado Root adicional em um Browser, entre outros, pelo usuário. Este último não está vinculado a uma concessão de privilégios (autorização) a instâncias habilitadas. Ele permite apenas a autenticação de instâncias habilitadas.

A EP 1 353 259 A1 descreve um processo para operação de um
15 sistema de computador, em que é instalado um módulo principal passível de execução de um programa no sistema do computador e armazenados dados de módulo para o módulo principal e/ou para um módulo adicional do programa no sistema de computador, sendo que os dados de módulo armazenados contêm uma parte de licença, que é necessária para a verificação da
20 presença da autorização ao uso do módulo principal e/ou adicional, e de preferência ainda uma parte de informação. Os módulos armazenados são avaliados para uma aquisição de uma outra autorização de uso para o módulo adicional ou para um outro módulo adicional e disponibilizadas informações para a aquisição do direito de uso em função do resultado da avaliação.

25 O objetivo da invenção reside, portanto, em indicar um processo aperfeiçoado para a delegação de privilégios a uma instância de privilégio inferior por uma instância de privilégio superior.

Esse objetivo é alcançado, segundo a invenção, pelas características da reivindicação 1, a cujo teor se remete nesse ponto.

30 Configurações preferidas e características vantajosas da invenção se depreendem das reivindicações dependentes, a cujo teor se remete nesse ponto.

Com a invenção deve ser conseguido, entre outros, reduzir o trabalho e assim os custos para a instalação de privilégios.

O processo segundo a invenção se baseia em que a instalação de privilégios em aparelhos pode ser executada automaticamente e sem intervenção de um administrador. Para tanto, antes do fornecimento ao proprietário ou usuário o aparelho deve ter sido provido dos necessários privilégios, que são necessários para com uma instância mais privilegiada, que é provida de privilégios especiais para a concessão de privilégios, se poder instalar privilégios para instâncias de privilégio inferior.

Para se instalar um privilégio em um aparelho, uma máquina ou pessoa a isso autorizada transmite uma instância de privilégio superior ao usuário do aparelho ou diretamente ao aparelho. No primeiro caso, o usuário instala a instância no aparelho. No segundo caso, por exemplo já quando do fornecimento do aparelho ao usuário está presente no aparelho ou pode ser transmitida ao aparelho através de uma interface aérea. A instância é levada à execução no aparelho com ou sem interação com o usuário. O aparelho pode, por exemplo verificar, com auxílio da assinatura criptográfica na instância, se a instância está autorizada a instalar privilégios menores para outras instâncias. Quando este é o caso, a instância tem acesso, por exemplo às funções especiais para instalação de privilégios. A instância, em seguida, instala os privilégios, sem que o usuário deva levar o aparelho a um outro estado. Depois de os privilégios terem sido instalados com sucesso, a instância pode novamente ser removida do aparelho.

Em seguida, depois da instalação dos novos privilégios, instâncias a eles autorizadas podem então reivindicar esses privilégios inferiores.

A figura 1 mostra um decurso preferido do processo segundo a invenção.

Novo quadro reivindicatório (total de 09 reivindicações), incorporando as emendas às reivindicações, conforme relatório de exame preliminar.

REIVINDICAÇÕES

1. Processo para delegação de privilégios a uma instância de privilégio inferior por uma instância de privilégio superior, em que a instalação de privilégios, P1, para uma instância de privilégio inferior é executada automaticamente em um aparelho de processamento de dados, na medida em que o aparelho antes do fornecimento a um usuário ou por transferência de dados é provido de funções para a instalação dos privilégios, para com auxílio de uma instância de privilégio superior, que é provida de privilégios especiais, P2, para concessão de privilégios, poder instalar privilégios, P1, para a instância de privilégio inferior.

2. Processo, de acordo com a reivindicação 1, caracterizado pelo fato de que para a instalação dos privilégios, P1, para a instância de privilégio inferior são executadas as seguintes etapas:

- instalação da instância de privilégio superior no aparelho por uma máquina ou pessoa a isso autorizada,
- execução da instância de privilégio superior no aparelho,
- acesso às funções para instalação de privilégios, P1, pela instância de privilégio superior,
- instalação automática dos privilégios, P1, para a instância de privilégio inferior no aparelho pela instância de privilégio superior.

3. Processo, de acordo com uma das reivindicações 1 ou 2, caracterizado pelo fato de que a instância de privilégio superior é disponibilizada ao usuário e por ele instalada no aparelho.

4. Processo, de acordo com uma das reivindicações 1 ou 2, caracterizado pelo fato de que a instância de privilégio superior já está presente no aparelho quando do fornecimento do aparelho ao usuário ou é transmitida diretamente ao aparelho por uma interface aérea.

5. Processo, de acordo com uma das reivindicações 1 a 4, caracterizado pelo fato de que a instância de privilégio superior é executada automaticamente no aparelho.

6. Processo, de acordo com uma das reivindicações 1 a 4, caracterizado pelo fato de que a instância de privilégio superior é executada

por uma interação com o usuário no aparelho.

7. Processo, de acordo com uma das reivindicações 1 a 6, caracterizado pelo fato de que a instância de privilégio superior é removida do aparelho, depois de os privilégios, P1, para a instância de privilégio inferior
- 5 terem sido instalados com sucesso.

8. Aplicativo de software com um código de programa, que executado em um aparelho de processamento de dados realiza um processo como definido nas reivindicações 1 a 7.

9. Produto de programa de processamento de dados, que a-
- 10 brange um aplicativo de software executável em um aparelho de processamento de dados para realização do processo como definido nas reivindicações 1 a 7.