(11) Número de Publicação: **PT 1698100 E**

(51) Classificação Internacional:
H04L 9/32 (2007.10) ***G06F 1/00*** (2007.10)

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

(22) Data de pedido: **2004.12.22**

(30) Prioridade(s): **2003.12.22 US 531865 P**
2004.12.07 US 5838

(43) Data de publicação do pedido: **2006.09.06**

(45) Data e BPI da concessão: **2007.11.21**
010/2008

(73) Titular(es):
GUARDTIME AS
VEERENNI 58A-22 11314 TALLINN **EE**

(72) Inventor(es):
MART SAAREPERA **EE**
AHTO BULDAS **EE**

(74) Mandatário:
MARIA DO ROSÁRIO MAY PEREIRA DA CRUZ ALVES GARCIA
RUA DO PATROCÍNIO 94 1399-019 LISBOA **PT**

(54) Epígrafe: **SISTEMA E MÉTODO PARA GERAR UM CERTIFICADO DIGITAL**

(57) Resumo:

DESCRIÇÃO

SISTEMA E MÉTODO PARA GERAR UM CERTIFICADO DIGITAL

REFERÊNCIA CRUZADA COM PEDIDOS RELACIONADOS

Este pedido reivindica prioridade do Pedido Provisório U.S. Nº 60/531, depositado em 22 de Dezembro de 2003.

CAMPO TÉCNICO

A presente invenção relaciona-se com a criação e a renovação de certificados digitais. Mais particularmente, a presente invenção relaciona-se com um sistema e método seguros para gerar um certificado digital.

ANTECEDENTES DA INVENÇÃO

Os registos electrónicos digitais são cada vez mais utilizados como prova de factos. Historicamente, selos, assinaturas, papéis especiais e outros instrumentos eram utilizados para provar a autenticidade de documentos e outros registos. Além disso, para além de provar a autenticidade de documentos e registos, estes e outros instrumentos têm sido utilizados para provar que um documento foi recebido ou produzido numa certa ordem. Estes métodos de provar a autenticidade e a ordem são úteis numa variedade de áreas, incluindo operações bancárias, negociações, apresentação de documentos legais e administração pública. Hoje em dia, estes serviços são oferecidos, tipicamente, por notários, auditores e outros.

Serviços semelhantes de autenticação e verificação de ordem são necessários no mercado de conteúdo electrónico digitalizado. Numa variedade de áreas deste mercado, os provedores de serviços electrónicos recebem registos digitais. Por exemplo, um sistema bancário electrónico recebe um registo digital da compra de um consumidor. Estes provedores de serviço registam a sequência em que os registos são recebidos e atribuem cada registo com um "valor de sequência". Depois do registo ter sido recebido e registado pelo provedor de serviço, tipicamente, é emitido um certificado digital para a parte interessada fornecedora do registo. Pode surgir, mais tarde, a necessidade do provedor do serviço ou outra parte interessada verificar a ordem em que registos específicos foram registados. Para satisfazer esta necessidade de verificação, os valores das sequências podem ser ligados a registos digitais de tal modo a provar, mais tarde, que os valores da sequência reflectem a ordem de registo de uma maneira correcta e autêntica.

Tipicamente, esta ligação dos números da sequência a registos digitais é conseguida por criptografia assimétrica ou, como método alternativo, por publicação. Uma ligação verificável é referida como um certificado de ordem. Sem ligações verificáveis, os provedores de serviço poderiam negar a validade de qualquer coisa que seja apresentada como um certificado.

Quando a criptografia assimétrica é utilizada para ligação verificável, o provedor de serviço, tipicamente, assina um registo digital (contendo um valor de sequência correspondente) com uma assinatura digital ou esquema de codificação, tal como RSA. A criptografia de chave pública é suficientemente rápida para permitir a geração quase instantânea de um certificado. No entanto, há uma fraqueza inerente em utilizar a criptografia assimétrica para criar assinaturas digitais: As chaves da assinatura criptográfica podem tornar-se comprometidas. Uma vez que uma chave

se tenha tornado comprometida, os certificados criados com aquela chave já não podem ser verificados. Uma vez que a possibilidade daquela chave tornar-se comprometida aumenta com o tempo, os certificados criados utilizando a criptografia com chave são úteis apenas durante um curto período de tempo.

Quando a publicação é utilizada para fazer a ligação verificável, o provedor de serviço, tipicamente, publica um registo digital juntamente com um valor de sequência de uma maneira amplamente testemunhada, por exemplo, num jornal. Se o provedor de serviço compromete-se com certas regras relativas à publicação, então pode-se confiar no teor publicado como sendo certificado pelo provedor de serviço. Uma vez que não são utilizadas chaves criptográficas no método de publicação, o problema do comprometido da chave não é uma preocupação. No entanto, o método de publicação é ineficientemente lento. A publicação é realística diariamente ou semanalmente, mas a criação de um certificado instantâneo, embora exigido pelo mercado electrónico moderno, é impossível.

Para verificar a autenticidade de um certificado por um longo período, e para fazê-lo de forma eficiente, ligações à base de publicações e/ou assinaturas de chaves múltiplas podem ser utilizadas em combinação. No entanto, uma vez que esta abordagem de combinação tem as desvantagens de ambos os sistemas, os certificados têm de ser actualizados regularmente, criando despesas adicionais para manter a validade das ligações.

Há um outro problema fundamental relacionado que se refere às propriedades dos próprios valores das sequências, tipicamente representados como números inteiros. Até um certo ponto, as ligações verificáveis entre os registos digitais e os números inteiros podem ser vistas por meio da verificação das partes como

prova de que os registos, de facto, receberam estes valores de sequência.

Muitas vezes, no entanto, os números de sequência atribuídos aos registos digitais não reflectem de forma precisa a ordem temporal real na qual os registos foram recebidos. Provedores de serviço mal intencionados podem atribuir números de sequência para registos em qualquer ordem que desejarem. Deste modo, surgiu uma necessidade de detectar o comportamento erróneo de um provedor de serviço. O conceito de numerar os registos pode ser excessivamente abstracto para reflectir o processo de registação. Por exemplo, uma declaração de que três registos foram registados antes de qualquer um registo específico não proporciona qualquer informação sobre como os registos foram registados. Uma maneira de superar este problema é definir o valor da sequência de um registo em particular como a regulação de todos os registos que precedem um registo específico no repositório. Tais "valores de sequência" representam a ordem da registação, mas uma vez que os mesmos também registam a história do repositório, os mesmos não podem ser negados pelo provedor de serviço.

No entanto, se cada valor de sequência reflectir toda a história do repositório, os valores podem tornar-se tão grandes de modo que fazem com que o seu cálculo e transmissão não sejam práticos.

Uma maneira de confirmar a história de um provedor de serviço é incluir um compilador criptográfico de todos os registos previamente registados no certificado digital emitido para a parte fornecedora de registo. Por exemplo, pode ser criada uma cadeia linear hash aplicando uma função hash criptográfica a uma concatenação de um registo recém-recebido e o registo recebido imediatamente antes deste. Tal método está descrito na Patente U.S.

Nº 5.136.646 de Haber *et al*. Os compiladores criptográficos que estão incluídos em certificados de ordem criam relações causais unidireccionais entre as confirmações e, deste modo, podem ser utilizados para verificar a sua ordem sem receio de comportamento erróneo pelo provedor de serviço, uma vez que a confirmação errónea é detectável por um verificador que examina a cadeia hash causal unidireccional. Os valores de sequência criados por tais processos são mais curtos por causa da utilização de funções cardinais criptográficas. No entanto, a verificação de tais valores ainda requer um cálculo de todos os registos no repositório e, deste modo, pode consumir recursos de processamento consideráveis. Este processo é adicionalmente desvantajoso pelo facto de não poder ser realizado sem interacção com o provedor de serviço.

"*Improving the avalilability of time standing services*" Arne Ansper, Ahto Buldas, Mart Saarepera, Jan Willemson. ACISP 2001, [On line] 11 de Julho de 2001, páginas 1-16, Sydney, Austrália, descreve um método digital de selagem de tempo utilizado para conservar o valor comprobatório de documentos electrónicos, protocolos de selagem de tempo e selagem de tempo com assinatura hash. Este documento descreve uma abordagem à base de ligação, em particular esquemas de ligação linear e ligação de árvore encadeada para proporcionar serviços de selagem de tempo digital.

Actualmente, ligações eficientes verificáveis são criadas com criptografia assimétrica. No entanto, em várias aplicações há uma necessidade para ligações eficientes verificáveis a longo prazo que são idealmente verificáveis sem a utilização de chaves criptográficas. Em concordância, surgiu uma necessidade para um sistema de registação de registos electrónicos digitais com procedimentos que permitem que os clientes substituam os certificados assinados digitalmente de curto prazo (por meio de métodos criptográficos assimétricos) por provas de certificado de

longo prazo que são baseados em compilações criptográficas e métodos de publicação.

A presente invenção é proporcionada para resolver estes e outros problemas.

SUMÁRIO DA INVENÇÃO

São descritos, um sistema e método para gerar um certificado digital em que os clientes submetem registos digitais a um provedor de serviço de registação. Os registos são registados e os clientes recebem um certificado assinado digitalmente que verifica a registação (e número de registo) do registo. Estes certificados assinados digitalmente podem, então, ser substituídos por uma prova certificada que é gerada aplicando uma função hash criptográfica ao repositório de todos os registos.

Numa forma de realização da presente invenção, são descritos, um sistema e método para gerar um certificado digital em que um cliente submete um registo digital a um provedor de serviço de registação. É gerado um valor digital composite que representa, pelo menos, um subconjunto de toda a história dos registos recebidos anteriormente, em que o valor digital composite é gerado pela aplicação de um algoritmo determinístico aos elementos armazenados num repositório. Um certificado de confirmação é, então, gerado e transmitido ao cliente, em que o certificado compreende, pelo menos, o registo digital, uma sequência numérica atribuída ao registo e o valor digital composite. O certificado é assinado digitalmente utilizando um esquema criptográfico assimétrico. Em seguida, o registo digital, ou uma representação do mesmo, é adicionada ao repositório.

Noutra forma de realização da presente invenção, são descritos, um sistema e método para publicar um compilador criptográfico de um repositório de registos digitais. É gerado um valor digital composite que representa, pelo menos, um subconjunto de toda a história de registos recebidos, em que o valor digital composite é gerado pela aplicação de um algoritmo determinístico aos elementos armazenados no repositório. É também gerado um número de sequência composite e regulado igual ao número de sequências actuais do repositório. Este valor digital composite e o número de sequência composite do repositório são, então, publicados ao público.

Noutra forma de realização da presente invenção, são descritos, um sistema e método para criar uma prova certificada para um registo digital, em que é gerado um valor digital de intervalo para o registo relativo a um valor digital composite publicado. É, então, gerada uma prova certificada, em que a prova certificada inclui, pelo menos, o valor digital de intervalo e o número de sequência do registo e pode incluir também um subconjunto do próprio registo digital, do valor digital composite e o número de sequência composite.

Outras características e vantagens da invenção tornar-se-ão evidentes a partir da seguinte memória descritiva, em conjunto com os desenhos a seguir.

BREVE DESCRIÇÃO DOS DESENHOS

A fim de entender a presente invenção, a mesma será agora descrita por meio de exemplo, com referência aos desenhos associados, em que:

a FIGURA 1 é o fluxograma genérico do sistema e método para gerar um certificado digital, ilustrando, em geral, os passos para registar um registo digital num repositório, publicar criptograficamente um compilador do repositório e gerar uma prova certificada para o registo digital.

A FIGURA 2 é um fluxograma de uma porção do sistema e método para gerar um certificado digital, ilustrando, em pormenor o procedimento para registar um registo digital num repositório e gerar um certificado digital verificando a registação do registo.

A FIGURA 3 é um fluxograma de uma porção do sistema e método para gerar um certificado digital, ilustrando em pormenor o procedimento para gerar uma prova certificada para um registo digital.

A FIGURA 4 é um fluxograma de uma aplicação do sistema e método para gerar um certificado digital, ilustrando o procedimento para utilizar uma prova certificada para verificar a recepção e o número de sequência de um registo digital.

A FIGURA 5 é um fluxograma de uma aplicação do sistema e método para gerar um certificado digital, ilustrando o procedimento para utilizar provas certificadas para verificar a recepção e os números de sequência de mais de um registo digital.

A FIGURA 6 é um diagrama de transição de estado da porção do sistema e método para gerar um certificado digital, ilustrando os estados e transições entre os mesmos para a geração de um primeiro certificado digital.

A FIGURA 7 é um diagrama de transição de estado da porção do sistema e método para gerar um certificado digital, ilustrando os estados e transições entre os mesmos para a geração de um segundo certificado digital e renovação de um primeiro certificado digital.

A FIGURA 8 é uma ilustração de uma estrutura de dados para utilização com o sistema e método para gerar um certificado digital, ilustrando uma floresta de árvores de busca binárias.

A FIGURA 9 é uma ilustração de uma estrutura de dados para utilização com o sistema e método para gerar um certificado digital, ilustrando uma floresta de árvores de busca binárias representadas como uma série indexada.

A FIGURA 10 é uma ilustração de uma estrutura de dados para utilização com o sistema e método para gerar um certificado digital, ilustrando uma floresta de árvores de busca binárias dispostas numa estrutura de dados em camada.

A FIGURA 11 é uma ilustração de uma tabela para utilização com o sistema e método para gerar um certificado digital, ilustrando o fluxo de trabalho de um algoritmo para registar um registo digital.

A FIGURA 12 é uma ilustração de uma tabela para utilização com o sistema e método para gerar um certificado digital, ilustrando o fluxo de trabalho de um algoritmo para gerar um valor de intervalo digital.

A FIGURA 13 é uma ilustração de uma tabela para utilização com o sistema e método para gerar um certificado digital, ilustrando, adicionalmente, o fluxo de trabalho de um algoritmo para gerar um valor de intervalo digital.

DESCRIÇÃO PORMENORIZADA

Embora esta invenção seja susceptível de realização em muitas formas diferentes, estão ilustradas nos desenhos e aqui descritas em pormenor as formas de realização preferidas com o entendimento de que a presente descrição deve ser considerada uma exemplificação dos princípios da invenção e não se destina a limitar o aspecto amplo da invenção em relação às formas de realização ilustradas.

Com referência, em pormenor, aos desenhos e inicialmente à FIGURA 1, é proporcionado um sistema e método para gerar um certificado digital. O sistema e método, em resumo, compreendem três funcionalidades primárias. A primeira funcionalidade primária é a registação de um novo registo digital. No passo 101, o novo registo digital é criado ou recebido. Um registo digital é uma representação de um item de dados e o item de dados pode representar qualquer tipo de informação digital. Por exemplo, o item de dados pode ser um documento electrónico, informação de ordem, informação de identificação ou qualquer outro tipo de informação representada digitalmente. Como uma representação do idem de dados, o registo digital pode compreender o item de dados na sua totalidade, pode compreender uma porção do item de dados ou pode compreender alguma outra representação do item de dados. Numa forma de realização preferida, o novo registo digital é recebido no passo 101. Noutra forma de realização preferida, o novo registo digital é criado no passo 101 com base num item de dados recebido e, depois, armazenado num repositório de registos digitais.

No passo 102, uma primeira função determinística é aplicada a, pelo menos, um subconjunto dos registos digitais armazenados no repositório, de modo a gerar um primeiro valor digital composite. Numa forma de realização preferida, a primeira função determinística é aplicada a todos os registos digitais armazenados

no repositório assegurando, deste modo, que o primeiro valor digital composite seja uma representação de toda a história do repositório e, deste modo, reduzindo a possibilidade de que o proprietário do repositório possa mais tarde interferir com o conteúdo do repositório.

Do mesmo modo, no passo 102, um número de sequência é atribuído ao novo registo digital. Numa forma de realização preferida, o número de sequência representa a ordem na qual o novo registo digital e recebido. Por exemplo, se houver dez registos digitais armazenados no repositório quando o novo registo digital é recebido, o número de sequência 11 será atribuído ao novo registo digital. No entanto, o número de sequência pode ser qualquer representação do tempo ou ordem na qual no novo registo digital é recebido.

No passo 103, é gerado um primeiro certificado, de tal modo que o certificado verifica a recepção do novo registo digital. O primeiro certificado compreende, pelo menos, o número de sequência atribuído ao novo registo digital e o primeiro valor digital composite. Numa forma de realização preferida, uma vez que o número de sequência indica o tempo ou a ordem na qual o novo registo digital foi recebido e o primeiro valor digital composite representa a história do repositório quando o novo registo digital foi recebido, o primeiro certificado pode, deste modo, ser utilizado para verificar o número de sequência.

No passo 104, pode-se acrescentar informação adicional ao primeiro certificado. Por exemplo, numa forma de realização preferida, o primeiro certificado compreende, adicionalmente, o novo registo digital ou uma porção do mesmo. Esta inclusão é útil na verificação de que o conteúdo do registo digital foi recebido correctamente pelo repositório. Noutra forma de realização

preferida, a informação adicional pode ser um *timestamp* indicando o momento preciso no qual o novo registo digital é recebido.

No passo 105, uma assinatura digital é aplicada ao primeiro certificado. A assinatura digital pode ser qualquer tipo de assinatura tal que a assinatura autentique a identidade do proprietário do repositório. Por exemplo, a assinatura digital pode ser baseada num esquema de chave cifrada privada/pública, tal como RSA. Numa forma de realização preferida, o primeiro certificado é assinado digitalmente utilizando uma chave privada do proprietário do repositório. De preferência, o primeiro certificado é transmitido ao criador ou provedor do registo digital.

No passo 106, o novo registo digital ou uma representação do mesmo é adicionada ao repositório. O passo 106 de adicionar o novo registo digital ao repositório pode ser realizado antes ou depois da geração do primeiro valor digital composite no passo 102. Numa forma de realização preferida, o novo registo digital é adicionado ao repositório depois da geração do primeiro certificado digital no passo 103, de modo a reduzir o tempo de espera necessário para o provedor do novo registo digital receber o primeiro certificado digital. Depois que o novo registo digital é adicionado ao repositório no passo 106, podem ser criados ou recebidos registos digitais adicionais; em outras palavras, o sistema pode retornar ao passo 101.

A segunda funcionalidade primária do sistema e método para gerar um certificado digital é a publicação da informação que diz respeito ao repositório. No passo 107, é gerado um segundo valor digital composite por meio da aplicação de uma segunda função determinística a, pelo menos, um subconjunto dos registo digitais armazenados no repositório. Como o primeiro valor digital composite, o segundo valor digital composite representa a história

do repositório num dado momento. Numa forma de realização preferida, a primeira e segunda funções determinísticas não são as mesmas funções. De preferência, a segunda função determinística é aplicada a todos os registos digitais armazenados no repositório e, deste modo, o segundo valor digital composite representa toda a história do repositório, reduzindo, deste modo, a ameaça de que o proprietário do repositório possa interferir com o repositório.

No passo 108, é gerado um número de sequência composite, em que o número de sequência corresponde à ordem em que o segundo valor digital composite é gerado. Deste modo, o número de sequência composite é uma indicação da qualidade temporal do segundo valor digital composite. No passo 108, o segundo valor digital composite e o número de sequência composite são publicados, isto é, transmitidos a um foro público. O foro público pode ser qualquer fonte de informação que esteja disponível ao público em geral. Por exemplo, o foro público pode ser um jornal, uma revista, um website da Internet, ou correio electrónico.

A terceira funcionalidade primária do sistema e método para gerar um certificado digital é a criação de um segundo certificado que prova a autenticidade do número de sequência do novo certificado digital. No passo 109, é gerado um valor de intervalo digital, em que o valor de intervalo digital é baseado no primeiro e segundo valores digitais composites. Numa forma de realização preferida, o valor de intervalo digital é o resultado da aplicação de uma terceira função determinística aplicada aos registos digitais armazenados no repositório entre a recepção do novo registo digital e a geração do segundo valor digital composite. Deste modo, o valor do intervalo digital pode reflectir a história do repositório entre a recepção do novo registo digital e a publicação do segundo valor digital composite. No entanto, o valor do intervalo digital também pode ser o resultado da aplicação de

uma função determinística aplicada a todos os registos digitais armazenados no repositório e, deste modo, reflectir toda a história do repositório.

No passo 110, é gerado um segundo certificado, em que o segundo certificado inclui, pelo menos, o valor do intervalo digital e o número de sequência do novo registo digital. Pelo facto do valor do intervalo digital reflectir a história do repositório desde que o novo sinal digital foi adicionado ao repositório, ou um tempo anterior, o valor do intervalo digital pode, deste modo, ser utilizado para verificar a precisão do número de sequência. O valor do intervalo digital também pode ser utilizado para renovar, isto é, estender a autenticidade do no registo digital. Uma vez que a geração do valor do intervalo digital não é baseado na utilização de chaves cifradas, a segurança do segundo certificado digital não está sujeita ao comprometimento da chave cifrada.

Com referência agora à FIGURA 2, são proporcionados, em pormenor, os passos do método para gerar um certificado digital. No passo 106, o novo registo digital 200 é adicionado ao repositório 210. No passo 205, uma primeira função determinística é aplicada a, pelo menos, um subconjunto dos registos digitais armazenados no repositório, de modo a produzir um primeiro valor digital composite 204. O passo de adicionar o novo registo digital 200 ao repositório 106 pode ser realizado tanto antes como depois do passo de aplicar a primeira função determinística 205 ao repositório 210. Um número de sequência 202 é atribuído ao novo registo digital 200, isto é, a ordem em que o novo registo digital 200 foi recebido.

No passo 103, é gerado o primeiro certificado 201. O primeiro certificado 201 inclui, pelo menos, o primeiro valor digital composite 204 e o número de sequência 202 do novo certificado digital 200. Além disso, o primeiro certificado 201 pode incluir o

novo registo digital 200 propriamente dito e outros dados adicionais 207. No passo 208, o primeiro certificado 201 é assinado com uma assinatura digital 209, em que a assinatura digital 209 é, de preferência, baseada num esquema cifrado de chave pública.

No passo 213, é aplicada uma segunda função determinística aos registos digitais armazenados no repositório 210 para gerar um segundo valor digital composite 212. É gerado um número de sequência composite 217 e, de preferência, é regulado igual ao actual número de sequência próximo disponível no repositório 210. No passo 109, é gerado um valor de intervalo digital 214, em que o valor de intervalo digital 214 reflecte a diferença temporal entre a recepção do novo registo digital 200 e a geração do segundo valor digital composite 212. Por último, no passo 110, é gerado um segundo certificado 215, em que o segundo certificado 215 compreende, pelo menos, o número de sequência 202 do novo registo digital 200 e o valor de intervalo digital 212. Além disso, conforme indicado no passo 110, o segundo certificado 215 pode compreender todo ou uma porção do primeiro certificado 201 e o número de sequência composite 217.

Com referência agora à FIGURA 3, é proporcionado em pormenor os passo de verificação do segundo certificado 215. Um primeiro certificado 210 é recebido do servidor 302 por um cliente 301, em que o primeiro certificado 201, de preferência, foi assinado com uma assinatura digital 209. Opcionalmente, mediante a recepção do primeiro certificado 201, um procedimento de verificação de assinatura 308 é realizado para inicialmente verificar a autenticidade do primeiro certificado 201. De preferência, o procedimento de verificação de assinatura 308 consiste em utilizar um esquema cifrado à base de chave.

O primeiro certificado 201 é recebido por um segundo cliente 303 e um procedimento de verificação de assinatura 308 é realizado para verificar a autenticidade do primeiro certificado 201. Numa forma de realização preferida, mediante a determinação no passo 308 de que a assinatura digital 209 do primeiro certificado 201 é inválida, o segundo cliente 303 será incapaz de confirmar ou validar o primeiro certificado 201. Mediante uma verificação de que a assinatura digital 209 do primeiro certificado 201 é válida, o primeiro certificado 201 é transmitido para um segundo servidor 304, no qual o primeiro certificado é renovado, estendido e validado por meio da aplicação do método aqui descrito para gerar o segundo certificado 215. O segundo certificado 215 é, então, transmitido para o segundo servidor 304. O segundo valor digital composite publicado 212 e o número de sequência composite 217 estão disponíveis publicamente para o segundo cliente 303. Deste modo, com base nestes valores, o segundo certificado 215 e o primeiro certificado 201, o segundo cliente pode verificar a validade do número de sequência 202 por meio do processo de verificação 307. Mediante uma determinação de que o primeiro certificado 201 e o segundo certificado 215 são coerentes, o segundo cliente 303 é capaz de confiar na autenticidade do número de sequência 202 e do registo digital 200 proporcionados pelo primeiro cliente 301.

Com referência agora à FIGURA 4, é proporcionada em pormenor outra forma de realização do sistema e método para verificar um registo digital 200. Um registo digital 200 é transmitido de um cliente 402 para um servidor de verificação 401. O segundo certificado 215 é recebido de um servidor de extensão 403, onde o processo de gerar o segundo certificado 215 foi realizado. O segundo valor digital composite 212 e o número de sequência composite 27, colectivamente referidos como os valores públicos 212, são publicados no servidor público 404 e são recebidos pelo servidor de verificação 401. O segundo certificado 215, o registo

digital 200 e os valores públicos 212 são utilizados no processo de verificação 405 aqui descrito. Deste modo, o servidor de verificação 401 pode confiar na validade do registo digital 200 submetido pelo cliente 402.

Com referência agora à FIGURA 5, é proporcionada em pormenor uma forma de realização do sistema e método para registar registos digitais, em que um servidor de verificação 501 pode verificar a ordem dos valores de sequência 202 de registos digitais em competição 200 proporcionados pelos primeiro e segundo clientes 502 e 504, respectivamente. Um primeiro cliente 502 transmite um primeiro registo digital 503 para o servidor de verificação 501, acompanhado pelo segundo certificado 509 correspondente ao primeiro registo digital 503. Um segundo cliente 504 transmite um segundo registo digital 510 para o servidor de verificação 501, acompanhado pelo segundo certificado 511 correspondente ao segundo registo digital 510. Deste modo, o servidor de verificação 501 pode utilizar o sistema e método aqui descritos para determinar qual dos registos digitais 200 em competição foi registado mais cedo.

Os valores públicos 512, publicados num servidor público 506, são recebidos pelo servidor de verificação 501. Ao utilizar o processo de verificação 507 aqui descrito, o servidor de verificação 501 pode confiar no primeiro e segundo registos digitais 200 e segundos certificados acompanhantes para determinar quais dos registos digitais 200 são autênticos. Além disso, uma vez que os números de sequência 202 dos registos digitais são reflectidos nos segundos certificados 215, o servidor de verificação 501 também pode determinar a ordem autêntica na qual os registos digitais 200 foram recebidos.

Com referência agora à FIGURA 6, é proporcionado um diagrama de transição de estado, ilustrando adicionalmente os estados e as transições entre os mesmos para registar um novo registo digital e gerar um primeiro certificado digital. No passo 603, o sistema de registação é iniciado. O valor de sequência é regulado em zero, o repositório é eliminado de registos digitais, e os valores digitais composites são eliminados. No passo 602, o sistema espera para receber um registo digital. Quando um registo digital é recebido, o primeiro valor digital composite é gerado no passo 604. No passo 605, um valor de sequência é atribuído ao novo registo digital e um primeiro certificado digital é gerado de acordo com os procedimentos aqui descritos. O primeiro certificado digital é assinado digitalmente. Por último, o novo registo digital é adicionado ao repositório. Depois da registação estar completa em 605, o sistema retorna a um estado de espera 602 para receber um outro novo registo digital.

Com referência agora à FIGURA 7, é proporcionado um diagrama de transição de estado, ilustrando adicionalmente os estados e as transições entre os mesmos para estender o primeiro certificado digital. O sistema tem início no passo 701 e no passo 703 o sistema é iniciado. O segundo valor digital composite é gerado aplicando a segunda função determinística ao repositório e o valor de sequência composite é gerado. O sistema, então, prossegue para um estado de espera 702 para a recepção de um certificado digital. Se não for recebido nenhum certificado, o sistema pode retornar, de forma intermitente, ao passo 703 para reiniciar e regenerar os valores composites. Quando um certificado digital é recebido, é gerado o valor de intervalo digital no passo 704, de acordo com o processo aqui descrito. Depois do valor de intervalo digital ser gerado, o sistema gera um segundo certificado digital no passo 705. Por último, o sistema retorna ao estado de espera 702 para receber outro certificado digital. Numa forma de realização preferida, uma

vez que a geração do segundo certificado digital depende do conteúdo do primeiro certificado digital, o sistema pode ser utilizado para renovar ou estender a autenticidade do primeiro certificado digital. O sistema também pode ser utilizado para verificar a autenticidade do primeiro certificado digital e também pode ser utilizado para verificar a autenticidade do registo digital correspondente ao primeiro certificado digital.

Com referência agora à FIGURA 8, é proporcionado um diagrama ilustrando uma estrutura de dados para utilização com o sistema e método para gerar um certificado digital. Numa forma de realização preferida, a estrutura de dados é uma floresta de árvores de busca binárias, em que cada vértice parente de uma árvore binária é um hash criptográfico dos vértices filhos. A construção da árvore de busca binária é realizada *on-the-fly*, com base na recepção de novos registos digitais. Os novos registos digitais são representados por valores hash de um tamanho predeterminado e são armazenados como folhas 802 das árvores de busca binárias. Devido à utilização de uma estrutura de dados de árvore binária, o número de registos digitais registados no repositório não necessita ser conhecido e os parâmetros topológicos do repositório, por exemplo, a altura e a largura, não necessitam ser determinados. Deste modo, a FIGURA 8 representa a estrutura de dados da floresta de árvores de busca binárias do repositório depois de ter recebido seis registos digitais.

Os vértices das folhas 802 da floresta são organizados naturalmente. O número de sequência n de uma folha determina a sua posição na floresta. Se um novo registo de dados x_n for recebido, o mesmo é primeiro armazenado como uma folha com o valor de sequência n e aquela árvore é, então, actualizada. O processo de actualização é organizado de modo a proporcionar que apenas os vértices da raiz 801 da floresta participarão nas futuras gerações de valores

digitais composites. A lista de vértices de raiz, deste modo, serve um hash de estado para utilização na geração de valores digitais composites. Durante o processo de gerar um valor digital composite, qualquer vértice da estrutura que possa ser computado é computado e armazenado imediatamente. Todas as folhas 802 são armazenadas na sua ordem computacional, de preferência correspondente ao transversal pós-ordem da árvore. Uma vez que os vértices de raiz 801 já representam os valores hash dos vértices das folhas 802, os vértices das folhas 802 não necessitam ser levados em consideração na geração de um valor digital composite. Deste modo, a estrutura de dados da floresta de busca binária possibilita um processamento muito rápido dos valores digitais composites.

Com referência agora à FIGURA 9, é proporcionado um diagrama ilustrando uma estrutura de dados para utilização com o sistema e método para gerar um certificado digital, em que a estrutura de dados da floresta de busca binária é adicionalmente ilustrada como uma série indexada. Os elementos de uma série que representam a floresta são armazenados na sua ordem computacional. Expresso de forma diferente, os elementos computados anteriormente têm índices menores do que os elementos computados mais tarde. O processo de construir a estrutura de dados de floresta, de preferência, depende da utilização de uma pilha contendo os valores hash de raiz $h1 \ldots h_s$ com h_s no topo da pilha. Se $(x_0 \ldots x_{n-1})$ são as folhas da floresta, o número de elementos na pilha é igual ao número de bits colocados na representação binária de n. Cada folha adicionada muda alguns valores no topo da pilha e o número de valores sendo mudado é igual ao número de 1-bits mais à direita na representação binária de n. Por exemplo, se $n = 23$ a *enésima* adição muda três elementos da pilha, porque $23 = 10111_2$.

Com referência agora à FIGURA 10, é proporcionado um diagrama ilustrando uma estrutura de dados para utilização com o sistema e método para gerar um certificado digital, em que a estrutura de

dados da floresta de busca binária é adicionalmente ilustrada como uma floresta de árvores de busca binárias em camadas. É preferível organizar as árvores binárias em camadas a fim de calcular eficientemente o valor do intervalo digital. A enésima camada 1001 é definida como um subconjunto mínimo de vértices que satisfazem duas hipóteses. Em primeiro lugar, a camada satisfaz a hipótese de que para todo n, a folha x_n pertence à enésima camada. Em segundo lugar, a camada satisfaz a hipótese de que se um dos vértices filho de um vértice v pertence à enésima camada e o outro filho pertence à camada $(n - k)^a$ (onde k ε {0…n}, então, também o vértice v pertence à enésima camada. A FIGURA 10 representa um exemplo de uma árvore de busca binária de seis nós organizados em camadas.

Com referência agora à FIGURA 11, é proporcionada uma tabela que ilustra o fluxo de trabalho de um algoritmo para utilização com o sistema e método para gerar um certificado digital. Numa forma de realização preferida, o algoritmo para registar um registo digital, onde n representa o número de sequência do repositório e x representa um novo registo digital, é proporcionado como:

```
Valor_composite = [], Repositório = []
n:=0
repetir
        Receber_Registar (x)
        Responder (n, Valor_composite, x)
        Anexar (Repositório, x)
        Actualizar (Repositório, Valor_composite, n, x)
        n:=n + 1
```

Encontra-se representado na FIGURA 11 um fluxo de trabalho que ilustra a aplicação deste algoritmo com entradas de registo digital [x_0, x_1, x_2, x_3, x_4]. A função Actualizar (Repositório, Valor_composite, n, x) pode ainda ser definida como:

```
a:=n
enquanto Odd (a) do
    x:= Hash (Pop (Valor_composite), x)
    Anexar (Repositório, x)
    a:= a >>1
    Empurrar Valor_composite, x)
```

Com referência agora à FIGURA 12, é proporcionada uma tabela que ilustra o fluxo de trabalho de um algoritmo para utilização com o sistema e método para gerar um certificado digital. Numa forma de realização preferida, o algoritmo para registar um valor de intervalo digital, onde n representa o número de sequência do repositório e N representa o valor de sequência composite, é proporcionado como:

```
cabeça:= [], cauda:= [], j:= ||n||1 + 1, b:= 1
enquanto f:= [(n ⊕ b) ou (b - 1)] ≤ N do
    se b & n = b
        Anexar (cabeça, Repositório [2f - j + 2])
        j:=j - 1
    ou
        Anexar (cauda, Repositório [2f - j])
    b:= b << 1
```

Encontra-se representado na FIGURA 12 um fluxo de trabalho que ilustra a aplicação deste algoritmo onde $n = 4$ e $N = 7$. Encontra-se representado na FIGURA 13 um fluxo de trabalho que ilustra a aplicação deste algoritmo onde $n = 3$ e $N = 7$.

Será entendido que a invenção pode ser realizada de outras formas específicas sem afastamento do espírito ou características centrais da mesma. Deste modo, as presentes formas de realização,

devem ser consideradas em todos os aspectos como ilustrativas e não restritivas e a invenção não está limitada aos pormenores aqui dados.

Lisboa, 3 de Janeiro de 2008.

REIVINDICAÇÕES

1. Método para gerar um certificado digital num sistema compreendendo um primeiro computador provedor de serviço que compreende um repositório e um segundo computador cliente (401 - 404, 501 - 506), **caracterizado por** compreender os passos de:

receber um novo registo digital no computador do provedor de serviço a partir do segundo computador;

atribuir um valor de sequência ao novo registo digital (202) no computador do provedor de serviço e armazenar os dados incluindo os registos digitais e valores hash no repositório (215);

gerar um primeiro valor digital composite aplicando uma primeira função (204) a uma primeira pluralidade dos dados armazenados no repositório, em que a primeira função computa um conjunto de valores de raiz para uma floresta de busca binária (801) não conectada;

gerar um primeiro certificado digital, em que o primeiro certificado digital compreende, pelo menos, o valor de sequência e o primeiro valor digital composite;

adicionar o novo registo digital no repositório;

gerar uma sequência de valores hash e armazenar a sequência de valores hash no repositório (215) aplicando uma segunda função (210) a uma segunda pluralidade dos dados armazenados no repositório, em que a segunda pluralidade dos dados inclui o novo

registo digital e, em que a segunda função computa a floresta de busca binária (801) não conectada,

gerar um valor de sequência composite (217);

gerar um segundo valor digital composite (212) aplicando uma terceira função a uma terceira pluralidade dos dados armazenados no repositório;

gerar um valor de intervalo digital (214) aplicando uma quarta função a uma quarta pluralidade dos dados armazenados no repositório, em que o valor de intervalo digital é baseado no valor de sequência e o valor de sequência composite;
e

gerar um segundo certificado digital, em que o segundo certificado digital compreende, pelo menos, o valor de sequência e o valor de intervalo digital.

2. Método de acordo com a Reivindicação 1, **caracterizado por** o valor de sequência ser representativo da ordem na qual o novo registo digital foi recebido.

3. Método de acordo com a Reivindicação 1, **caracterizado por** compreender ainda o passo de:

aplicar uma assinatura digital ao primeiro certificado digital.

4. Método de acordo com a Reivindicação 3, **caracterizado por** o primeiro certificado digital ser gerado utilizando um algoritmo criptográfico assimétrico.

5. Método de acordo com a Reivindicação 1, **caracterizado por** o passo de gerar o primeiro valor digital composite ser realizado aplicando a primeira função a todos os registos digitais armazenados no repositório.

6. Método de acordo com a Reivindicação 1, **caracterizado por** a primeira e a terceira funções não serem a mesma função.

7. Método de acordo com a Reivindicação 1, **caracterizado por** a primeira e a terceira funções serem a mesma função.

8. Método de acordo com a Reivindicação 1, **caracterizado por** o passo de gerar o segundo valor digital composite ser realizado aplicando a terceira função a todos os registos digitais armazenados no repositório.

9. Método de acordo com a Reivindicação 1, **caracterizado por** o primeiro certificado digital compreender ainda um novo registo digital.

10. Método de acordo com a Reivindicação 1, **caracterizado por** o segundo certificado digital compreender ainda, pelo menos, um de: no novo registo digital e o valor de sequência composite.

11. Método de acordo com a Reivindicação 1, **caracterizado por** o repositório do computador de registos digitais compreender uma estrutura de dados de floresta de busca binária não conectada.

12. Método de acordo com a Reivindicação 1, **caracterizado por** compreender ainda o passo de:

transmitir o segundo valor digital composite a um computador de foro público.

13. Método de acordo com a Reivindicação 1, **caracterizado por** compreender ainda o passo de:

transmitir o valor de sequência composite a um computador de foro público.

14. Método de acordo com a Reivindicação 1, **caracterizado por** o passo de gerar o primeiro valor digital composite ser realizado antes do passo de gerar o segundo valor digital composite.

15. Método para avaliar um certificado digital conforme gerado consoante o método de acordo com qualquer reivindicação 1 a 14, compreendendo, pelo menos um valor de sequência, um primeiro valor digital composite e um valor de intervalo digital, em que o primeiro valor digital composite é gerado aplicando uma primeira função a uma primeira pluralidade de dados registados no repositório de um provedor de serviço, em que a primeira função computa um conjunto de valores de raiz para uma floresta de busca binária não conectada e, em que o valor de intervalo digital é gerado aplicando uma segundo função a uma segunda pluralidade de dados armazenados no repositório de um provedor de serviço, o método **caracterizado por** compreenderos passos de:

gerar um segundo valor digital composite aplicando uma terceira função ao primeiro valor digital composite e o valor de intervalo digital e determinando se o segundo valor digital composite reflecte, de forma precisa, uma terceira pluralidade dos dados armazenados num computador de foro público.

16. Método de acordo com a Reivindicação 15, **caracterizado por** o valor de sequência ser representativo da ordem em que um registo digital foi recebido.

17. Método de acordo com a Reivindicação 15, **caracterizado por** o certificado digital compreender ainda um registo digital.

18. Método de acordo com a Reivindicação 15, **caracterizado por** o certificado digital compreender ainda um *timestamp* digital.

19. Método de acordo com a Reivindicação 1, adaptado para gerar uma pluralidade de certificados digitais, **caracterizado por:**

o valor de sequência aplicado ao novo registo digital no computador do provedor de serviço representar a ordem na qual o novo registo digital foi recebido;

o passo de gerar o primeiro certificado digital ser realizado aplicando a primeira função a todos os registos digitais armazenados no repositório e, em que a primeira função compreende uma primeira função determinística tendo um componente de função hash e o novo registo digital não é armazenado no repositório do computador do provedor de serviço quando a primeira função determinística é aplicada e, em que a primeira função determinística computa, pelo menos, um valor hash de raiz para uma floresta de busca binária não conectada;

o primeiro certificado digital compreender ainda o novo registo digital;

o método compreender ainda o passo de aplicar uma assinatura digital a um primeiro certificado digital, em que a assinatura digital é aplicada utilizando um algoritmo criptográfico assimétrico;

a seguir à adição do novo valor digital ao repositório, ser realizado o passo de gerar uma

sequência de valores hash aplicando a segunda função a todos os registos digitais armazenados no repositório e, em que a segunda função compreende uma segunda função determinística tendo um componente de função hash para todos os registos digitais armazenados no repositório;

o passo de gerar o segundo valor digital composite ser realizado aplicando uma terceira função a todos os registos digitais armazenados no repositório e, em que a terceira função compreende uma terceira função determinística tendo um componente de função hash;

o valor de sequência composite ser igual ao número de registos digitais armazenados no repositório do computador do provedor de serviço quando o segundo valor digital composite é gerado;

o passo de gerar o valor de intervalo digital ser realizado pela aplicação da quarta função a uma pluralidade de dados armazenados no repositório, em que a quarta função compreende uma quarta função determinística tendo um componente de função hash;

e

o segundo certificado digital compreender ainda, pelo menos, um dos novos registos digitais e o valor de sequência composite.

Lisboa, 3 de Janeiro de 2008.