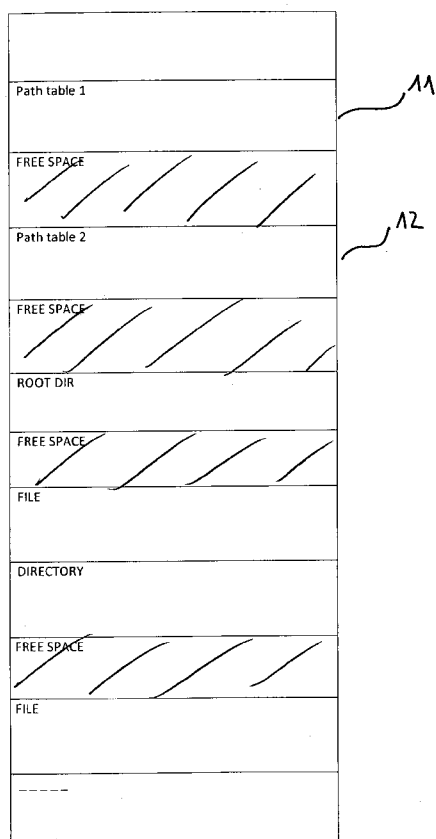




- (51) International Patent Classification:
G06F 17/30 (2006.01) *G06F 21/24* (2006.01)
- (21) International Application Number:
PCT/EP2011/072461
- (22) International Filing Date:
12 December 2011 (12.12.2011)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
10306530.6 28 December 2010 (28.12.2010) EP
- (71) Applicant (for all designated States except US):
GEMALTO SA [FR/FR]; Intellectual Property Dpt, 6 rue de la Verrerie, F-92190 Meudon (FR).
- (72) Inventors; and
(75) Inventors/Applicants (for US only): **DURAND, Stéphane** [FR/FR]; c/o Gemalto SA, Intellectual Property Dpt, 6 rue de la Verrerie, F-92190 Meudon (FR). **MARSEILLE, François-Xavier** [FR/FR]; c/o Gemalto SA, Intellectual Property Dpt, 6 rue de la Verrerie, F-92190 Meudon (FR).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continued on next page]

(54) Title: METHOD FOR UPDATING A FILE SYSTEM STORAGE FROM A REMOTE UPDATE SERVER



(57) Abstract: The invention relates to a token comprising a secure application and mass storage partitions, said mass storage partitions comprising a file system storage, said file system storage comprising areas of ordered metadata, and file content areas, characterized in that the file system storage has a structure adapted for remote partial updates.



(84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS,

SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

METHOD FOR UPDATING A FILE SYSTEM STORAGE FROM A REMOTE UPDATE SERVER

FIELD OF THE INVENTION

5

The present invention relates generally to the update of secure token and more specifically to the update of a file system storage.

BACKGROUND OF THE INVENTION

10

One of the prospected markets is to supply service providers with smart tokens that act as a secure mobile front-end to their online services. These tokens embed secured internal software as well as public software to be run on a computer. The public software is generally exposed over a mass storage device in the token, mostly featured inside a file storage system such as a CDROM image.

Due to the evolution of the proposed services, and of the distributed software, it is necessary to update the content of the CDROM image, as an application on the CDROM can evolve due a bug correction, enhancements, new features, branding, etc...

A CDROM image is as a non-editable object, with file system structures that are not designed to be modified. Therefore for updating a CDROM image, it is necessary to replace all the data. It is generally known to update a CDROM image Over The Internet or Over The Air, which requires a large network bandwidth as there are a lot of data to broadcast to many devices. Such requirement leads to expensive network infrastructure.

A possible solution is to use a stock file system. Nevertheless, with a stock file system, the modifications propagate, e.g. if a table grows, all the data behind the table shift accordingly, and the

references to this data accordingly are also updated in turn. This method requires more memory, and the process might be very difficult to carry out on a portable object.

There is then a need for lessen the amount of data to transport
5 over the network in the scope of such update and thus to reduce the cost of the updating.

It is then an object of the invention to provide a new architecture of a CDROM image and a method for updating such CDROM image.

10 Thereto, the present invention provides a token comprising a secure application and mass storage partitions, said mass storage partitions comprising a file system storage, said file system storage comprising areas of ordered metadata, and file content areas, characterized in that the file system storage has a structure adapted for remote partial
15 updates.

According to another aspect of the invention, the file system storage may comprise free spaces between metadata areas;

According to another aspect of the invention the file system
20 storage may be a CDROM image;

The invention also provides a method for updating data of a file system storage from a remote update server, said file system storage being stored in a token and areas of ordered metadata, and file content
25 areas, characterized in that it comprises updating only the most recent parts of data.

According to another aspect of the invention, the method may comprise leaving growth space between areas liable to grow during an
30 update.

According to another aspect of the invention, the method may comprise comparing the version of data in the remote server and the version of data in the file system storage.

According to another aspect of the invention, the method may
5 comprise relocating updated data within the file storage system if an area reaches its growth limit.

When the said CDRom image architecture and the update method are combined, it is advantageously possible to perform an update of the CDRom
10 image that will only consider the modifications of the existing image. All information contained in the CDRom image that is invariant with respect to the prospected update will not be carried in the update bundle whereas all changing informations will be concisely described. The final benefit is savings in both server data storage and network resources.

15

The various aspects, features and advantages of the invention will become more fully apparent to those having ordinary skill in the art upon careful consideration of the following Detailed Description, given by way of example thereof, with the accompanying drawing described below:

20 **FIG.1** schematically shows an architecture of a CDRom image according to the present invention.

DETAILED DESCRIPTION

25 The present invention may be understood according to the detailed description provided herein.

An USB token (not represented) features a microcontroller capable of running software and mass storage partitions. One of the mass storage partitions is a CDRom image 1 which holds public applications and data.
30 The CDRom image access may be controled by the microcontroller or not.

4

Some applications may embed secure mechanisms validated by the microcontroller or not.

Shown in Fig.1 is an architecture of the CDROM image 1.

The CDROM image 1 comprises several areas of ordered metadata, and
5 file content areas.

Ordered metadata follow a certain order according to the specification of their format. Metadata are stored in two groups: the metadata relating to the paths and the metadata concerning all other information about a file such as the size, the name, dates, etc... The
10 metadata relating to paths are ordered by name. As represented, there are two path tables 11,12.

According to the invention, the initial CDROM image 1 delivered with the token is structured to allow remote partial updates, for example by leaving growth space between all areas liable to grow during an
15 update. Then there are free spaces between metadata areas which allows these areas to grow or shrink, and thus to be modified in regard of the global structuring of the file system.

When the update consists in adding a new file, both content and associated file metadata are concerned. Entries are added in the file
20 system metadata area corresponding to the directory where the file is located and in the two path table 11,12.

When the update consists in deleting a file, associated metadata are concerned. Entries are removed in the directory where the file was located and in the two path tables 11,12.

25 When the update consists in modifying a file, new content, and, if the size is changed, the associated metadata (directory entry) are concerned. If the file grows and needs to be relocated, this is notified as the associated metadata are modified.

According to the method of the invention, only the parts that are
30 more recent in a CDROM image are updated, i.e. only parts which are new

such as new files, modified files, and the metadata accordingly modified including moved or deleted files, new directories, etc..., are transported over the network.

In an embodiment, a secure application in the USB token holds a version number associated with the CD-ROM content.

A public application allows connecting the server to the secure application, and the data exchange between the update server and the secure application.

The public application holds the address of a remote update server, which address is for example stored in the secure application. The update server holds the most recent version number and the high level description of updates from any version number to the most recent one.

Upon connection to the update server, the public application queries the version number of the CDROM from the secure application and sends it to the update server.

The update server compares the version number of the CDROM with the latest version number. If the received version number is older than the latest version number, the update server sends to the public application, high level description of the operations to perform in order to align both versions, as well as the new version number, such as delete/create directory, add/remove file, etc...

It will be well understood that the exchange between the update server and the public application may be or not encrypted and or signed.

The public application then sends the high level description to the secure application. It does not need to decrypt or verify the signature when present.

The secure application decrypts or verifies the signature of the high level description when applicable, and performs the associated operations. If no error is detected, it updates its version number to the one sent by the update server. The migration from the current version of

6

the token is done with a new "initial" CDROM image and an updated update server that computes necessary update instead of sending the whole raw CDROM image.

It will be well understood that if an area reaches its growth
5 limit, it can be relocated within the CDROM volume, its base address being modified in the referring structure(s).

In another embodiment, a prior step to transporting the updating data is to compute them. Based on the CDROM version in the token and the
10 new set of file (content and tree), areas to be modified, shrunk, expanded or moved are identified, and only these data are included in the update bundle as well as instructions to apply the modifications.

The versioning system depends on the implementation, and is not described here but is advantageously designed to easily build update
15 bundles without heavy server-side image storage overhead.

Thanks to the invention, the number of modifications on the file system during the update is limited and the modifications do not propagate.

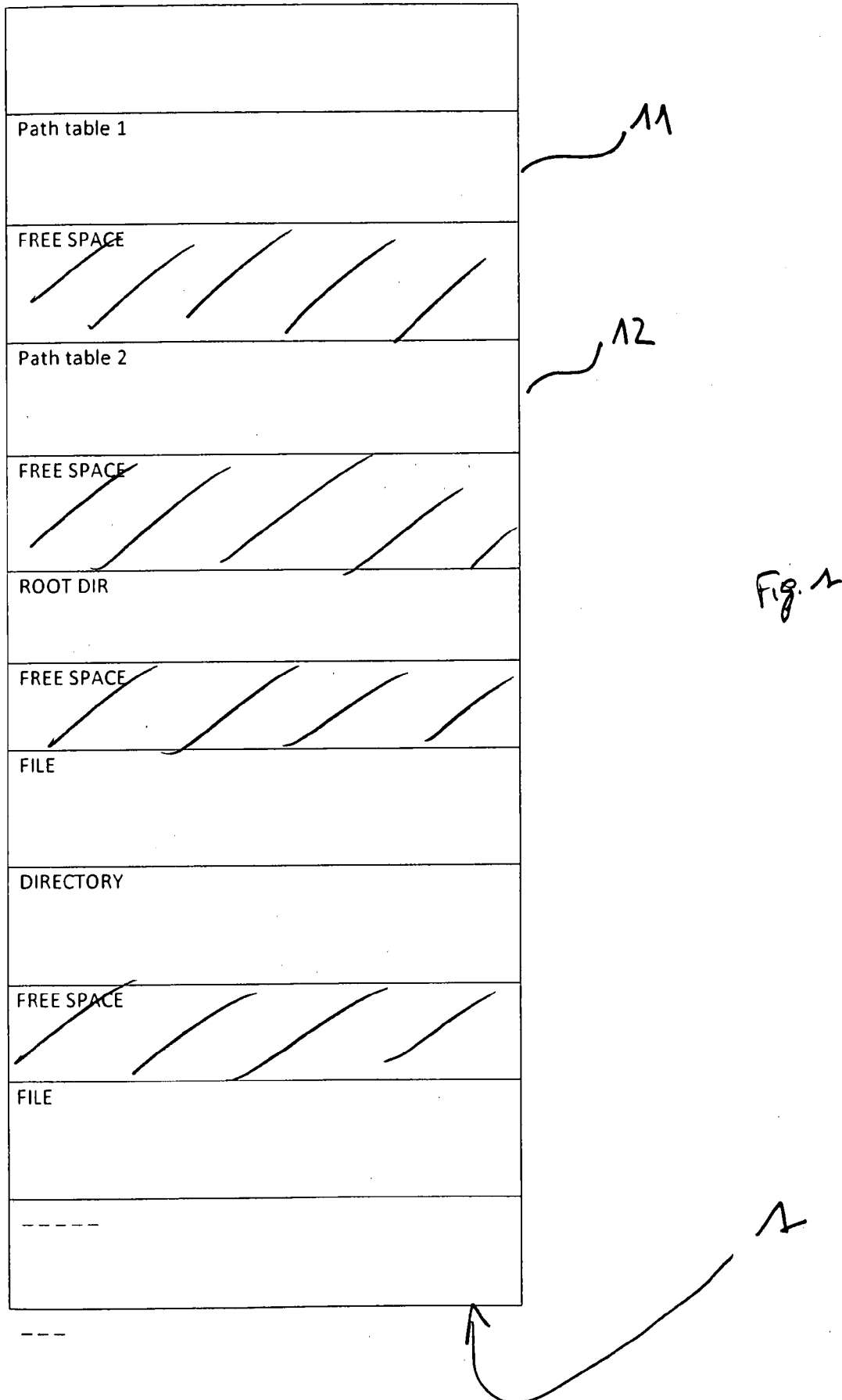
20 It will be well understood that other file system storage may be updated with this method.

25

30

CLAIMS

1. Token comprising a secure application and mass storage partitions,
5 said mass storage partitions comprising a file system storage, said
file system storage comprising areas of ordered metadata, and file
content areas, characterized in that the file system storage has a
structure adapted for remote partial updates.
- 10 2. Token according to claim 2, characterized in that the file system
storage comprises free spaces between metadata areas.
3. Token according to claim 1 to 2, characterized in that the file system
storage is a CDROM image.
- 15 4. Method for updating data of a file system storage from a remote update
server, said file system storage being stored in a token and areas of
ordered metadata, and file content areas, characterized in that it
comprises updating only the most recent parts of data.
- 20 5. Method according to claim 4, characterized in that it comprises
leaving growth space between areas liable to grow during an update.
6. Method according to claim 4 to 5, characterized in that it comprises
25 comparing the version of data in the remote server and the version of
data in the file system storage.
7. Method according to previous claims 4 to 6, characterized in that it
comprises relocating updated data within the file storage system if an
30 area reaches its growth limit.



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/072461

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F17/30 G06F21/24
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/114853 A1 (FISHER DIANA LOUISE [US] ET AL) 6 May 2010 (2010-05-06) abstract; figures 1,4,6,9,11,12 paragraph [0004] paragraph [0027] paragraph [0030] paragraph [0034] paragraph [0044] paragraph [0047] paragraph [0053] paragraph [0057] - paragraph [0059] paragraph [0081] ----- -/-	1-7



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

20 January 2012

Date of mailing of the international search report

10/02/2012

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Powell, David

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/072461

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/112113 A1 (GU JINSHENG [US] ET AL) 25 May 2006 (2006-05-25) abstract; figures 3-7 paragraph [0004] - paragraph [0005] paragraph [0018] paragraph [0023] - paragraph [0024] paragraph [0028] paragraph [0039] paragraph [0043] -----	1-7
A	US 2005/216746 A1 (SAIKA NOBUYUKI [JP]) 29 September 2005 (2005-09-29) the whole document -----	1-7
A	US 6 108 285 A (FREEMAN HARRISON L [US] ET AL) 22 August 2000 (2000-08-22) the whole document -----	1-7

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2011/072461

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010114853	A1	06-05-2010	CA 2742604 A1 14-05-2010
		EP 2350860 A2 03-08-2011	
		US 2010114853 A1 06-05-2010	
		WO 2010054120 A2 14-05-2010	

US 2006112113	A1	25-05-2006	NONE

US 2005216746	A1	29-09-2005	JP 4585213 B2 24-11-2010
		JP 2005275775 A 06-10-2005	
		US 2005216746 A1 29-09-2005	
		US 2008072319 A1 20-03-2008	

US 6108285	A	22-08-2000	EP 0389399 A2 26-09-1990
		JP 2054532 C 23-05-1996	
		JP 2280243 A 16-11-1990	
		JP 7086844 B 20-09-1995	
		US 6108285 A 22-08-2000	
