[Title]

System for scalable processing of files in the cloud

Field of the Invention

The present invention relates to a system and a method for secure transmission of files, which files are generated by a first user at a first client station, which first client station is connected by a first Local Area Network (LAN) to one or more local subordinate servers, which first server performs communication to a number of computer systems connected to the first LAN.

Background of the Invention

US 2011/0078532 A1 discloses a method and system for providing computer-generated output and in particular graphical output. The system includes a network configured to carry digital information. The system includes a server in communication with the network, the server configured to execute an application and a cloud engine module. The application provides a graphical output. The output capturing and encoding engine module is further configured to intercept the graphical output from the application on the server. The output capturing and encoding engine module is further configured to convert the graphical output into at least one of: graphical commands and video codec data. The output capturing and encoding engine module is further configured to transmit the converted output over the network. The system includes a client in communication with the server over the network, the client configured to execute a graphics and video decoding and rendering engine module. The graphics and video decoding and rendering engine module is configured to, responsive to receiving the transmitted converted output, rendering the graphical output. The graphics and video decoding and rendering engine modules are configured to intercept graphics and video decoding and rendering inputs at the client. The graphics and video decoding and rendering engine modules are configured to transmit the intercepted user inputs to the output capturing and encoding engine module.

The state of the Art comprises two main areas where print control systems and techniques are applied.

Duration: 21.11.2013 12:50:48 - 21.11.2013 13:30:23. This page 11 of 5013 12:57:23
Received at the EPO on Nov 21, 2013 13:30:23. Page 11 of 56
21/11/2013

One significant family of print control systems covers standard systems, which provide customer-centric deployment of said print control systems and control of user printing based on capturing the document during the spooling process.

The second family are the cloud based print control systems, where the system is user-centric, i.e. it does focus on providing a print control system features to users leveraging the cloud infrastructure and not imposing any maintenance costs to the organizations such as employers of the said users and often providing different ways of billing and profit generation than by selling software licenses to the customers. Examples of such systems are known under their marketing names Google Cloud Printing, HP ePrint and others.

Traditional Print Control Systems simply do not offer the benefits of the Cloud:
Zero Deployment of the application and services requiring usually no or substantially reduced costs of purchased software, hardware or other resources compared to traditional software and/or hardware products.

Different Billing and Payment Models such as pay-per-use, pay-per-click, pay-per-view are known by any skilled person. In the context of the Print Control Systems, this basically means that the purchasing costs of the system for the customer are minimal or non-existent and the whole price of the solution

Current cloud based print control systems bring many benefits typical for other cloud applications to printing, but suffer from additional drawbacks, which complicate or disqualify the deployment of cloud based print control systems in real customer environment. Cloud based print control system has essentially the same purpose as the traditional print control system: to route a user document in a digital form through a series of actions and transformations to the intended or appropriate printer, copier or multi-function printer device by means of so called spooling process. By extension to multi-function printer devices and scanners, the purpose of a print control system cloud-based or traditional is to route a document in hard copy form. The drawbacks of the cloud based print control systems are:

Print Job Exposure print jobs are routed to the cloud, i.e. print job data always leave the infrastructure and control of the end user organization. To preserve data integrity and confidentiality print job encryption and digital signature has to be employed, which is today not usual and might be problematic. By deploying an integrity protection mechanism, such as digital signatures, certain features simply cannot be implemented such as print job conversion, greyscale or duplex enforcement, etc. as such transformations need to modify print job data.

Wide Area Network Bandwidth Consumption when print job are transferred back and forth to the cloud. Print jobs can be very large files and their sizes usually vary from MBs to GBs. All these data have to be transferred. Wide Area Network connection usually provides less bandwidth and increased latency when compared to the LAN in most cases, so aside from incurred costs, user experience may also be hampered due to increased waiting times due to increased network latency.

Current cloud-based systems rely on the Internet connection and perform all operations online. When network connection to the cloud such as an Internet connection is not working or available, cloud based print control systems cannot provide any services to the users.

Object of the Invention

It is the object of the invention to achieve worldwide scalable files transferring processes without the need for transferring the files over the wide area net, but to retain the user's full access to any file. A further object of the invention is to prevent storage of large files at a plurality of servers in the corporate or public data centre during and after data transmission and processing.

Description of the Invention

The object can be fulfilled by a system or a method where a first server generates and transmits via the internet at least one meta data file related to the file stored in the data cache to a Master Server Unit (MSU), which MSU is part of a corporate or public data centre (CDC), to which CDC a number of second servers are communicating, where

Duration: 21.11.2013 12:50:48 - 21.11.2013 13:30:23. This page 13 of 56 013 12:58:38
Received at the EPO on Nov 21, 2013 13:30:23. Page 13 of 56
21/11/2013

any user can access the meta data file any client stationby any LAN connection to any of the second servers, which system, based on a user request an upon authorization performs transmission of the file from the first server, via the internet and the MSU towards the user.

Hereby it can be achieved that a user can store a file in the data cache at the server and maybe travel to somewhere else in the world where in the meantime the system has transmitted a meta file to one or more, or maybe a group, of master server units or one, or more, or maybe a group of servers, which MSUs or servers could be part of a number of different corporate or public data centres worldwide. Having arrived at a destination after a travel, via a client station to a local subordinate server the user can access the nearest master server unit(s) or the nearest server, depending on the system configuration, and in fact, in the meantime, a meta data file has been transmitted already so that access is provided to that meta data file in the appropriate MSUs or servers that are part of the family or the meta file transfer is initiated by the user interaction with said nearest MSU(s) or servers and the user will have to wait for the transfer to finish before proceeding. The system may automatically notify the user upon transfer completion. From the server the user has access to this meta file and as soon as the user has provided valid credentials, the user has access to his file(s) which he can then process or have processed (such as printed) in a traditional manner. In this way a follow-me system is achieved that operates in a highly efficient manner because no files are transmitted; only the meta data file is transmitted to master service units worldwide. It is also possible by this invention that a group of users have access to the same file, simply because they already have credentials which could be used when they have received the meta file to get access to the file. In this way, it is possible in large organisations to transmit, for example, documents to a lot of sub-offices where the documents are kept more or less all the time in the company, because the communication of maybe the secured document is performed directly through the computer communication systems without any storage somewhere in the world at servers waiting for further transmission. The transmission of data is in that way performed in a much cheaper way, because there will no payment for storing of large files at server somewhere in the world, such as by leveraging cloud-based file storage services. By traditional cloud transmission of, for example, documents, the user has to pay for a large database

somewhere in the cloud in order to have access to all the files. By the pending application, there is only a very small meta file that is being transmitted through the cloud between different data centres. The meta file comprises only a small data set compared to the files which have been transmitted. The use of storage in the cloud is probably reduced with more than 99 %. Together with the saving in storage, a higher degree of security and privacy is also achieved; because nobody can get secret information from the meta file itself because the secret information is simply not there.

In a preferred embodiment of the invention is the system a print system. Hereby any document, such as spooled documents, can be saved at the local sever and a meta data file can be transmitted into the cloud and further into a high number of corporate or public data centres (CDCs). To each CDC a high number of Master Server Units (MSUs) can be connected. At each client station connected through a server and a computer network via local serves to one of the MSUs, a user can by access to the meta file and by use of an authorization code start a transmission of the document to be printed directly through the computer network to the local client station. Hereby it is avoided that the document is stored on a number of severs for shorter or longer period of time.

In a first alternative embodiment of the invention, the files are digital documents based on a scanning process. Hereby any paper document can be transmitted in the same way as any file as previously disclosed.

In a furher preferred embodiment for the invention the files can be digital documents submitted to the system by a user from multi function printing device.

In a second alternative embodiment of the invention, the files are digital pictures. Hereby any digital picture can be stored locally. In addition, by the transmission of meta files the meta file can be accessed from any work station connected to a computer network where users can get access to the metafile and the user authorization code of large files on a high number of servers is avoided.

The server comprises a data cache, which data cache receives and performs a spooling process of the file generated at the client station, which data cache performs a temporary storage of the spooled file.

Because the meta data file has a limited size anyhow, there is no problem in storing the meta file in thousands of servers worldwide, however the meta file is only transferred to the servers or MSUs where it is really needed, such as the MSUs and the servers where the respective users are known to be operating frequently. The file is not transmitted until the users have logged in on at client stations to another server; however, the files are not stored in the servers on its way to the client station. Seen from a point of view of security it is very important that a file, which, so to speak, is sent out into the cloud, is not present there, but only the meta data file is available in the cloud. Therefore, a high degree of security is maintained because only the user has the necessary credentials required for accessing first the meta file, and subsequently to the files.

The servers can communicate by LAN or general computer network to and from an identity database. In order to transmit a meta data file it is important that the subordinate server can exchange data with an identity database or with the associated MSUs and in that way combine the user identifier, such as login name, with further data that has to be part of the meta file.

The data cache in the server can receive configuration data from the MSU. Hereby it is achieved that the data cache has received data and in that way it is ensured that the MSU receiving information is the correct MSU and that the data stream is transmitted in a language and a form that can be received by the MSU.

The communication to and from the server to and from the MSU may be encrypted and authenticated at both ends. Hereby it is achieved that that all the data transmitted has a high degree of security, integrity and confidentiality.

The communication to and from the server to and from the MSU is asynchronous. By asynchronous communication it is possible to transmit the data in periods where the data traffic is limited so there is sufficient space for the data transmission over the communication lines. The asynchronous communication further helps in keeping a high degree of security and scalability because asynchronous communication makes it possible to have data transmitted as packages in different roads in the data communication landscape.

Users can get access in a roaming mode to any second server, which server recognizes the users access, the server requests the MSU or the appropriate server for data transmission from the first server when the users is connected.

The present patent application further concerns a method for secure transmission of files, which method comprises the following steps:
A first user generates a file at a first client station,
transmit the file from the first client station by a first LAN to a first server,
perform a storing process at the first server connected to the first LAN,

which first server generates and transmits transmit meta data file related to the stored file via the internet to an MSU,
which MSU, upon request and authentication of the user(s) gives access to any second server sending related authentication information related to the meta data file,
which system transmits the stored file from the data cache in the first server, via the internet to the MSU and further to the actual second server,
i. transmit the stored file from the second server by a LAN to a second client station or computer system.

By the method as described above, it is possible to achieve a high degree of security and scalability in transmitting files or other data packages from a user at a client station to any computer system for processing placed somewhere else in the world where the data files or files are ready for being processed when one or more users triggers such processing if valid credentials are provided. Any user who has valid credentials will in that way have access to files stored locally at a server, maybe placed thousand

of kilometres away. Just by using the meta file and perform an authorisation, the file will be transmitted directly. Hereby can distribution of files be performed to a big group of users, or maybe one user can travel from one part of the world to another and have access to own document only. By transmitting large files, it is very important that the file transmission is performed directly and no storage is performed in data centres somewhere in the world. It is very expensive to perform storage of large data amounts somewhere in data centres. Therefore, by this invention only meta files are sent for the data centres for storage. Because the meta file only contains an authorisation code and a reference to the file, the meta file comprises only a relatively small data amount compared with the actual file that has to be transmitted. Probably a large file will also be transmitted significantly faster, because there will be a direct connection link between the server that transmits the file from the chase memory directly over the internet to the receiver.

In the pending patent application the wording "File" is used for any data set, such as any computer generated document, any digital images or any computer program.

In the pending patent application the wording "client station" is any computer system, such as a mobile phone, tablet computer, digital camera.

Description of the Drawing

Fig. 1 shows a possible embodiment for an internet communication system as the system described in the pending application.

Detailed Description of the Invention

Fig. 1 shows a first possible disclosure of a system 2, which system comprises a Local Area Network (LAN) 4 and behind is indicated further LANs 4A, 4B, 4C, but it is to be understood that the number of LANs could be extremely high and by extension, the number of (subordinate) servers can be extremely high. The first LAN 4 comprises a subordinate first server 6 which first server 6 comprises a data chase 8 and which server 6 is connected to a plurality of client's stations 10, 10a-n, which client stations

are operated by users 7 7a-n, and it is of course understood that a plurality of users each could use their own client station. The first server 6 is further connected to an identity database, for example, an active directory 12 and connected to an SMTP mail server 14. Further is the first server 6 connected to a network printer 16 which network printer comprises a terminal 18. The first server 6 is further connected by a communication line 20 to the cloud 22. The cloud 22 is a commonly accepted description for the world wide net. The cloud 22 is further connected to a corporate data centre 24 which is only one of a number, and therefore is indicated corporate data centres 24a-24n. The corporate data centre comprises at least a master server unit which takes care of the communication to the cloud 22. This master server unit MSU 26 comprises a SQL database 28. The MSU 26 is communicating with a central reporting server 30, and further is the server communicating with a SMTP mail server 32. The MSU 26 is further communicating with a number of second servers 34, 34a-n, 36, 36a-n, 38, 38a-n, 40, 40a-n. Each of these servers can be connected to a plurality of client stations as indicated by 42, 42a-n. All these client stations could be operated by users 7, 7a-n.

In operation a file generated by the user 7 at the client station 10 will by the system be stored in the data base 8 at the first server 6, and the server can by an identity management integration point that refers to the identity database 12 generate a meta file. This meta file is then transmitted from the first server 6 over the communication line 20 into the cloud 22. From this cloud can a high number of corporate data centres have access to that meta file and reach a copy of it which is stored on the servers. From here the meta file can be further communicated to a high number of second servers 34, 34a-n, 36, 36a-n, 38, 38a-n, 40, 40a-n where at each second server, a number of client stations 42,42a-n are connected.

In one possible embodiment the invention could be used for follow-me print roaming. In some environments where cloud printing systems are deployed for managing print, copy, scan and fax security and accounting over a wide network of locations, there is often a need to provide a local company-wide print follow-system for roaming users at any location within a company using stationary workstations or portable computers for printing to any configurable printers at any location. Another typical usage of the system would be optimized cloud printing where print jobs are (as files) processed local-

ly, but the system is managed by and from the cloud so that the system provides advantages in terms of privacy and incurred transmission and storage costs over current cloud printing systems known to the art.

Duration: 21.11.2013 12:50:48 - 21.11.2013 13:30:23. This page 20 of 56 2013 13:03:21
Received at the EPO on Nov 21, 2013 13:30:23. Page 20 of 56

CLAIMS

1. System for transmission and processing of files, such as files involved in a printing process, , which files are generated by a first user (7) at a first client station (10), which first client station (10) is connected by a first computer network such as a Local Area Network (LAN) (4) to one or more local servers (6), which first server (6) performs communication to a number of computer systems (10a-n) connected to the first LAN (4), **characterized in** that the first local server (6) generates and transmits via the internet (20) at least one meta data file related to at least one file stored in a data cache (8) to at least one Master Server Unit (MSU) (26), which MSU (26) is part of a corporate or public data centre (CDC) (24), to which CDC (24) a number of second servers (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) are communicating, which first user (7) or a number of users (7,7a-n) can access the meta data file related to the file by any client station (42,42a-n) by any LAN connection to any of the second servers (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n), which system (2) based on a user request and upon authorisation of the user or users performs transmission of the file from the first server (6) via the internet (20) and the MSU (26) towards the client station operated by the user (7,7a-n) .

2. System according to claim 1, **characterized in** the system is a system for spooling documents for printing.

3. System according to claim 1 or 2 **characterized in** that the files are digital documents produced by a scanning process.

4. System according to claim 1 or 2 **characterized in** that the files are digital documents submitted to the system by a user from multi function printer device.

5. System according to claim 1 or 2 **characterized** in that the files are digital pictures.

Duration: 21.11.2013 12:50:48 - 21.11.2013 13:30:23. This page 21 of 56 2013 13:04:00
Received at the EPO on Nov 21, 2013 13:30:23. Page 21 of 56
21/11/2013

6. System according to one of the claims 1-5, **characterized in** that the server (6) comprises a data cache (8) and performs a spool process, which data cache (8) receives spooled document file generated at the client station (10,10a-n).

7. System according to one of the claims 1-6, **characterized in** that the servers (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) communicates by a communication system such as a LAN to and from an identity database (12).

8. System according to one of the claims 1-7, **characterized in** that the data cache (8) in the first server (6) receives configuration data or control data from the MSU (26).

9. System according to one of the claims 1-8, **characterized in** that the communication to and from the first server (6) to and from the MSU (26) is encrypted and authenticated at both ends.

10. System according to one of the claims 1-9, **characterized in** that the communication to and from the server (6) to and from the MSU (26) is asynchronous.

11. System according to one of the claims 1-10, **characterized in** that the user(s) (7,7a-n) have access in a roaming mode to any second server (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n), which second server (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) recognizes the user(s) (7,7a-n) access, the second server(s) (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) request the MSU (26) for transmission of the file from the first server (6) when the user or users (7,7a-n) are connected.

12. System according to claim 11, **characterized in** that the user or users (7, 7a-n) has access to the meta data file at any server (6, 34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) related to the file, which user or users (7, 7a-n) by authorization downloads the file to the actual client station (42, 42a-n) or printer system (16, 18).

13. Method for secure transmission of files by a system as disclosed in one of the claims 1-12, which method comprises the following steps:

a. A first user (7) generates a file at a first client station (10),

b. which first client station (10) transmits the file by a first LAN (4) to a first server (6)

c. performs a storing process at the first server (6) connected to the first LAN (4),

d. which first server (6) generates and transmits at least one meta data file related to the stored file via the internet to an MSU (26),

e, which MSU (26), upon request and authenthication of the user, gives access to the meta data file to any second server (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) sending the authentication information related to the meta data file,

f. which system transmits the stored file from the data cache (8) in the first server (6) via the internet to the MSU (26) and further to the actual second server (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n),

h. transmit the file from the second server (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) by a communication system such as a LAN to a second client station (42, 42a-n) or computer system.

14. Method according to claim 13, **characterized in** perform storing of the spooled file in a data cache (8) storage in the first server (6).

[Title]

System for scalable processing of files in the cloud

Field of the Invention

The present invention relates to a system and a method for secure transmission of files, which files are generated by a first user at a first client station, which first client station is connected by a first Local Area Network (LAN) to one or more local subordinate servers, which first server performs communication to a number of computer systems connected to the first LAN.

Background of the Invention

US 2011/0078532 A1 discloses a method and system for providing computer-generated output and in particular graphical output. The system includes a network configured to carry digital information. The system includes a server in communication with the network, the server configured to execute an application and a cloud engine module. The application provides a graphical output. The output capturing and encoding engine module is further configured to intercept the graphical output from the application on the server. The output capturing and encoding engine module is further configured to convert the graphical output into at least one of: graphical commands and video codec data. The output capturing and encoding engine module is further configured to transmit the converted output over the network. The system includes a client in communication with the server over the network, the client configured to execute a graphics and video decoding and rendering engine module. The graphics and video decoding and rendering engine module is configured to, responsive to receiving the transmitted converted output, rendering the graphical output. The graphics and video decoding and rendering engine modules are configured to intercept graphics and video decoding and rendering inputs at the client. The graphics and video decoding and rendering engine modules are configured to transmit the intercepted user inputs to the output capturing and encoding engine module.

The state of the Art comprises two main areas where print control systems and techniques are applied.

One significant family of print control systems covers standard systems, which provide customer-centric deployment of said print control systems and control of user printing based on capturing the document during the spooling process.

The second family are the cloud based print control systems, where the system is user-centric, i.e. it does focus on providing a print control system features to users leveraging the cloud infrastructure and not imposing any maintenance costs to the organizations such as employers of the said users and often providing different ways of billing and profit generation than by selling software licenses to the customers. Examples of such systems are known under their marketing names Google Cloud Printing, HP ePrint and others.

Traditional Print Control Systems simply do not offer the benefits of the Cloud:
Zero Deployment of the application and services requiring usually no or substantially reduced costs of purchased software, hardware or other resources compared to traditional software and/or hardware products.

Different Billing and Payment Models such as pay-per-use, pay-per-click, pay-per-view are known by any skilled person. In the context of the Print Control Systems, this basically means that the purchasing costs of the system for the customer are minimal or non-existent and the whole price of the solution

Current cloud based print control systems bring many benefits typical for other cloud applications to printing, but suffer from additional drawbacks, which complicate or disqualify the deployment of cloud based print control systems in real customer environment. Cloud based print control system has essentially the same purpose as the traditional print control system: to route a user document in a digital form through a series of actions and transformations to the intended or appropriate printer, copier or multi-function printer device by means of so called spooling process. By extension to multi-function printer devices and scanners, the purpose of a print control system cloud-based or traditional is to route a document in hard copy form. The drawbacks of the cloud based print control systems are:

Print Job Exposure print jobs are routed to the cloud, i.e. print job data always leave the infrastructure and control of the end user organization. To preserve data integrity and confidentiality print job encryption and digital signature has to be employed, which is today not usual and might be problematic. By deploying an integrity protection mechanism, such as digital signatures, certain features simply cannot be implemented such as print job conversion, greyscale or duplex enforcement, etc. as such transformations need to modify print job data.

Wide Area Network Bandwidth Consumption when print job are transferred back and forth to the cloud. Print jobs can be very large files and their sizes usually vary from MBs to GBs. All these data have to be transferred. Wide Area Network connection usually provides less bandwidth and increased latency when compared to the LAN in most cases, so aside from incurred costs, user experience may also be hampered due to increased waiting times due to increased network latency.

Current cloud-based systems rely on the Internet connection and perform all operations online. When network connection to the cloud such as an Internet connection is not working or available, cloud based print control systems cannot provide any services to the users.

Object of the Invention

It is the object of the invention to achieve worldwide scalable files transferring processes without the need for transferring the files over the wide area net, but to retain the user's full access to any file. A further object of the invention is to prevent storage of large files at a plurality of servers in the corporate or public data centre during and after data transmission and processing.

Description of the Invention

The object can be fulfilled by a system or a method where a first server generates and transmits via the internet at least one meta data file related to the file stored in the data cache to a Master Server Unit (MSU), which MSU is part of a corporate or public data centre (CDC), to which CDC a number of second servers are communicating, where

any user can access the meta data file any client station by any LAN connection to any of the second servers, which system, based on a user request an upon authorization performs transmission of the file from the first server, via the internet and the MSU towards the user.

Hereby it can be achieved that a user can store a file in the data cache at the server and maybe travel to somewhere else in the world where in the meantime the system has transmitted a meta file to one or more, or maybe a group, of master server units or one, or more, or maybe a group of servers, which MSUs or servers could be part of a number of different corporate or public data centres worldwide. Having arrived at a destination after a travel, via a client station to a local subordinate server the user can access the nearest master server unit(s) or the nearest server, depending on the system configuration, and in fact, in the meantime, a meta data file has been transmitted already so that access is provided to that meta data file in the appropriate MSUs or servers that are part of the family or the meta file transfer is initiated by the user interaction with said nearest MSU(s) or servers and the user will have to wait for the transfer to finish before proceeding. The system may automatically notify the user upon transfer completion. From the server the user has access to this meta file and as soon as the user has provided valid credentials, the user has access to his file(s) which he can then process or have processed (such as printed) in a traditional manner. In this way a follow-me system is achieved that operates in a highly efficient manner because no files are transmitted; only the meta data file is transmitted to master service units worldwide. It is also possible by this invention that a group of users have access to the same file, simply because they already have credentials which could be used when they have received the meta file to get access to the file. In this way, it is possible in large organisations to transmit, for example, documents to a lot of sub-offices where the documents are kept more or less all the time in the company, because the communication of maybe the secured document is performed directly through the computer communication systems without any storage somewhere in the world at servers waiting for further transmission. The transmission of data is in that way performed in a much cheaper way, because there will no payment for storing of large files at server somewhere in the world, such as by leveraging cloud-based file storage services. By traditional cloud transmission of, for example, documents, the user has to pay for a large database

somewhere in the cloud in order to have access to all the files. By the pending application, there is only a very small meta file that is being transmitted through the cloud between different data centres. The meta file comprises only a small data set compared to the files which have been transmitted. The use of storage in the cloud is probably reduced with more than 99 %. Together with the saving in storage, a higher degree of security and privacy is also achieved; because nobody can get secret information from the meta file itself because the secret information is simply not there.

In a preferred embodiment of the invention is the system a print system. Hereby any document, such as spooled documents, can be saved at the local sever and a meta data file can be transmitted into the cloud and further into a high number of corporate or public data centres (CDCs). To each CDC a high number of Master Server Units (MSUs) can be connected. At each client station connected through a server and a computer network via local serves to one of the MSUs, a user can by access to the meta file and by use of an authorization code start a transmission of the document to be printed directly through the computer network to the local client station. Hereby it is avoided that the document is stored on a number of severs for shorter or longer period of time.

In a first alternative embodiment of the invention, the files are digital documents based on a scanning process. Hereby any paper document can be transmitted in the same way as any file as previously disclosed.

In a further preferred embodiment for the invention the files can be digital documents submitted to the system by a user from multi function printing device.

In a second alternative embodiment of the invention, the files are digital pictures. Hereby any digital picture can be stored locally. In addition, by the transmission of meta files the meta file can be accessed from any work station connected to a computer network, where users can get access to the metafile and the user authorization code to start transmission of one ore more digital pictures. Hereby storing of a high number of large files on a high number of servers is avoided.

The server comprises a data cache, which data cache receives and performs a spooling process of the file generated at the client station, which data cache performs a temporary storage of the spooled file.

Because the meta data file has a limited size anyhow, there is no problem in storing the meta file in thousands of servers worldwide, however the meta file is only transferred to the servers or MSUs where it is really needed, such as the MSUs and the servers where the respective users are known to be operating frequently. The file is not transmitted until the users have logged in on at client stations to another server; however, the files are not stored in the servers on its way to the client station. Seen from a point of view of security it is very important that a file, which, so to speak, is sent out into the cloud, is not present there, but only the meta data file is available in the cloud. Therefore, a high degree of security is maintained because only the user has the necessary credentials required for accessing first the meta file, and subsequently to the files.

The servers can communicate by LAN or general computer network to and from an identity database. In order to transmit a meta data file it is important that the subordinate server can exchange data with an identity database or with the associated MSUs and in that way combine the user identifier, such as login name, with further data that has to be part of the meta file.

The data cache in the server can receive configuration data from the MSU. Hereby it is achieved that the data cache has received data and in that way it is ensured that the MSU receiving information is the correct MSU and that the data stream is transmitted in a language and a form that can be received by the MSU.

The communication to and from the server to and from the MSU may be encrypted and authenticated at both ends. Hereby it is achieved that that all the data transmitted has a high degree of security, integrity and confidentiality.

The communication to and from the server to and from the MSU is asynchronous. By asynchronous communication it is possible to transmit the data in periods where the data traffic is limited so there is sufficient space for the data transmission over the communication lines. The asynchronous communication further helps in keeping a high degree of security and scalability because asynchronous communication makes it possible to have data transmitted as packages in different roads in the data communication landscape.

Users can get access in a roaming mode to any second server, which server recognizes the users access, the server requests the MSU or the appropriate server for data transmission from the first server when the users is connected.

The present patent application further concerns a method for secure transmission of files, which method comprises the following steps:
A first user generates a file at a first client station,
transmit the file from the first client station by a first LAN to a first server,
perform a storing process at the first server connected to the first LAN,
which first server generates and transmits transmit meta data file related to the stored file via the internet to an MSU,
which MSU, upon request and authentication of the user(s) gives access to any second server sending related authentication information related to the meta data file,
which system transmits the stored file from the data cache in the first server, via the internet to the MSU and further to the actual second server,
and transmit the stored file from the second server by a LAN to a second client station or computer system.

By the method as described above, it is possible to achieve a high degree of security and scalability in transmitting files or other data packages from a user at a client station to any computer system for processing placed somewhere else in the world where the data files or files are ready for being processed when one or more users triggers such processing if valid credentials are provided. Any user who has valid credentials will in that way have access to files stored locally at a server, maybe placed thousand of kilometres away. Just by using the meta file and perform an authorisation, the file

will be transmitted directly. Hereby can distribution of files be performed to a big group of users, or maybe one user can travel from one part of the world to another and have access to own document only. By transmitting large files, it is very important that the file transmission is performed directly and no storage is performed in data centres somewhere in the world. It is very expensive to perform storage of large data amounts somewhere in data centres. Therefore, by this invention only meta files are sent for the data centres for storage. Because the meta file only contains an authorisation code and a reference to the file, the meta file comprises only a relatively small data amount compared with the actual file that has to be transmitted. Probably a large file will also be transmitted significantly faster, because there will be a direct connection link between the server that transmits the file from the chase memory directly over the internet to the receiver.

In the pending patent application the wording "File" is used for any data set, such as any computer generated document, any digital images or any computer program.

In the pending patent application the wording "client station" is any computer system, such as a mobile phone, tablet computer, digital camera.

Description of the Drawing

Fig. 1 shows a possible embodiment for an internet communication system as the system described in the pending application.

Detailed Description of the Invention

Fig. 1 shows a first possible disclosure of a system 2, which system comprises a Local Area Network (LAN) 4 and behind is indicated further LANs 4A, 4B, 4C, but it is to be understood that the number of LANs could be extremely high and by extension, the number of (subordinate) servers can be extremely high. The first LAN 4 comprises a subordinate first server 6 which first server 6 comprises a data chase 8 and which server 6 is connected to a plurality of client's stations 10, 10a-n, which client stations are operated by users 7 7a-n, and it is of course understood that a plurality of users

each could use their own client station. The first server 6 is further connected to an identity database, for example, an active directory 12 and connected to an SMTP mail server 14. Further is the first server 6 connected to a network printer 16 which network printer comprises a terminal 18. The first server 6 is further connected by a communication line 20 to the cloud 22. The cloud 22 is a commonly accepted description for the world wide net. The cloud 22 is further connected to a corporate data centre 24 which is only one of a number, and therefore is indicated corporate data centres 24a-24n. The corporate data centre comprises at least a master server unit which takes care of the communication to the cloud 22. This master server unit MSU 26 comprises a SQL database 28. The MSU 26 is communicating with a central reporting server 30, and further is the server communicating with a SMTP mail server 32. The MSU 26 is further communicating with a number of second servers 34, 34a-n, 36, 36a-n, 38, 38a-n, 40, 40a-n. Each of these servers can be connected to a plurality of client stations as indicated by 42, 42a-n. All these client stations could be operated by users 7, 7a-n.

In operation a file generated by the user 7 at the client station 10 will by the system be stored in the data base 8 at the first server 6, and the server can by an identity management integration point that refers to the identity database 12 generate a meta file. This meta file is then transmitted from the first server 6 over the communication line 20 into the cloud 22. From this cloud can a high number of corporate data centres have access to that meta file and reach a copy of it which is stored on the servers. From here the meta file can be further communicated to a high number of second servers 34, 34a-n, 36, 36a-n, 38, 38a-n, 40, 40a-n where at each second server, a number of client stations 42,42a-n are connected.

In one possible embodiment the invention could be used for follow-me print roaming. In some environments where cloud printing systems are deployed for managing print, copy, scan and fax security and accounting over a wide network of locations, there is often a need to provide a local company-wide print follow-system for roaming users at any location within a company using stationary workstations or portable computers for printing to any configurable printers at any location. Another typical usage of the system would be optimized cloud printing where print jobs are (as files) processed locally, but the system is managed by and from the cloud so that the system provides ad-

vantages in terms of privacy and incurred transmission and storage costs over current cloud printing systems known to the art.

CLAIMS

1. System for transmission and processing of files, such as files involved in a printing process, which files are generated by a first user (7) at a first client station (10), which first client station (10) is connected by a first computer network such as a Local Area Network (LAN) (4) to one or more local servers (6), which first server (6) performs communication to a number of computer systems (10a-n) connected to the first LAN (4), **characterized in** that the first local server (6) generates and transmits via the internet (20) at least one meta data file related to at least one file stored in a data cache (8) to at least one Master Server Unit (MSU) (26), which MSU (26) is part of a corporate or public data centre (CDC) (24), to which CDC (24) a number of second servers (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) are communicating and receives the meta data file, which first user (7) or a number of users (7,7a-n) can access the meta data file related to the file by any client station (42,42a-n) by any LAN connection to any of the second servers (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n), which system (2) based on a user request and upon authorisation of the user or users performs transmission of the file from the first server (6) via the internet (20) and the MSU (26) towards the client station operated by the user (7,7a-n), and request transfer of the file or files for local processing and wherein the servers (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) communicates by a communication system, such as a LAN, to and from an identity database (12), and wherein the data cache (8) in the servers (6, 34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) receives configuration data or control data from the MSU (26).

2. System according to claim 1, **characterized in** the system is a system for spooling documents for printing.

3. System according to claim 1 or 2 **characterized in** that the files are digital documents produced by a scanning process.

4. System according to claim 1 or 2 **characterized in** that the files are digital documents submitted to the system by a user from multi function printer device.

5. System according to claim 1 or 2 **characterized in** that the files are digital pictures.

6. System according to one of the claims 1-5, **characterized in** that the server (6) comprises a data cache (8) and performs a spool process, which data cache (8) receives spooled document file generated at the client station (10,10a-n).

7. System according to one of the claims 1-6, **characterized in** that the communication to and from the first server (6) to and from the MSU (26) is encrypted and authenticated at both ends.

8. System according to one of the claims 1-7, **characterized in** that the communication to and from the server (6) to and from the MSU (26) is asynchronous.

9. System according to one of the claims 1-8, **characterized in** that the user(s) (7,7a-n) have access in a roaming mode to any second server (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n), which second server (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) recognizes the user(s) (7,7a-n) access, the second server(s) (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) request the MSU (26) for transmission of the file from the first server (6) when the user or users (7,7a-n) are connected.

10. System according to claim 9, **characterized in** that the user or users (7, 7a-n) has access to the meta data file at any server (6, 34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) related to the file, which user or users (7, 7a-n) by authorization downloads the file to the actual client station (42, 42a-n) or printer system (16, 18).

11. Method for secure transmission of files by a system as disclosed in one of the claims 1-12, which method comprises the following steps:

a. A first user (7) generates a file at a first client station (10),

b. which first client station (10) transmits the file by a first LAN (4) to a first server (6)

c. performs a storing process at the first server (6) connected to the first LAN (4),

d. which first server (6) generates and transmits at least one meta data file related to the stored file via the internet to one or more MSU (26), which MSU is part of a cor-

porate or pubic data centre (CDC) to which CDC a number of second servers (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) are communicating,e. which MSU (26), upon request and authentication of the user in the identity database (12) at the first server (6), gives access to the file to any second server (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) sending the authentication information related to the meta data file,

f. which system transmits the stored file from the data cache (8) in the first server (6) via the internet to the actual second server (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n),

h. transmit the file from the second server (34, 34a-n, 36,36a-n, 38,38a-n,40, 40a-n) by a communication system such as a LAN to a second client station (42, 42a-n) or computer system.

14. Method according to claim 13, **characterized in** perform storing of the spooled file in a data cache (8) storage in the first server (6).