Scalable Secure File Sharing System

Katsuhiko Yoshida[†]*, Masaki Tanikawa, Kazuyuki Takaya, Koji Morishita, and Hiroyuki Fujiwara*

Abstract

We have developed a scalable secure file sharing system that can safely, securely, and reliably transfer a file (up to 100 GB) that cannot be attached to an email because the file is confidential or too big. This system ensures high security by using the Camellia encryption algorithm and working with an authentication infrastructure. It is simple to use and its operation is similar to sending email. It is applicable to a wide spectrum of business activities.

1. Scalable file transfer

File transfer is now essential to a wide variety of industries and businesses, as shown in **Fig. 1**. NTT Laboratories has already developed and introduced a platform product that allows the provision of an application service provider (ASP) service for businesses that handle files that exceed the size limit for email attachments. This ASP service has become the de facto standard service for the printing and advertising industry and is used daily for the transfer of advertisement graphics for newspapers and magazines. In response to several major leakages of personal and confidential information recently, many industries and corporations are looking for a means to transfer files safely and securely to other parties, especially ones outside the organization. File transfer over the network is considered attractive not only because it is secure and convenient but also because it costs far less than physical distribution.

NTT Laboratories has been expanding the functionality of its platform product to strengthen its security by incorporating encryption and authentication and to increase the maximum size of files that can be transferred beyond the current limit of 2 GB. The Scalable Secure File Sharing System (hereafter referred to as the SSS) can transfer files safely, securely, and efficiently. The main functions of the system, which are illustrated in **Fig. 2**, are described below.

2. Systems functions

2.1 Encryption

File transfer over the Internet involves a risk that the file data might be seen by malicious third parties while the file is in transit or on a server. The SSS not only encrypts data transfer on the communication path using SSL (secure socket layer), but also encrypts the file itself by using Camellia [1] to protect the information from eavesdroppers.

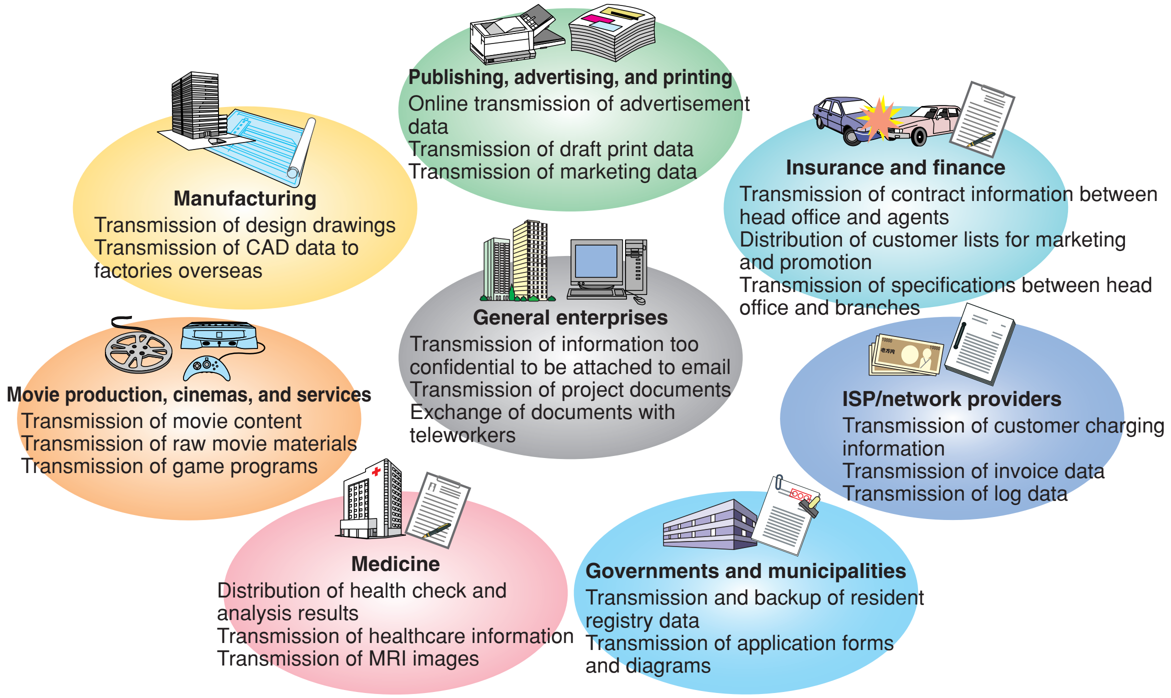
2.2 Authentication

To prevent information from being stolen by spoofing, both user authentication and server authentication are implemented. However, efforts to strengthen authentication can often reduce the ease of operation. To deal with this issue, we provided two different authentication methods: the user can choose to place priority on strong authentication or on ease of operation.

1) Electronic certificate

A certificate is sent to the user in the PKCS#12 format (PKCS: public key cryptography standards). Both server and user authentication are performed on the basis of this certificate.

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
Email: yoshida.katsuhiko@lab.ntt.co.jp


Publishing, advertising, and printing
Online transmission of advertisement data
Transmission of draft print data
Transmission of marketing data
Manufacturing
Transmission of design drawings
Transmission of CAD data to factories overseas
Insurance and finance
Transmission of contract information between head office and agents
Distribution of customer lists for marketing and promotion
Transmission of specifications between head office and branches
General enterprises
Transmission of information too confidential to be attached to email
Transmission of project documents
Exchange of documents with teleworkers
Movie production, cinemas, and services
Transmission of movie content
Transmission of raw movie materials
Transmission of game programs
ISP/network providers
Transmission of customer charging information
Transmission of invoice data
Transmission of log data
Medicine
Distribution of health check and analysis results
Transmission of healthcare information
Transmission of MRI images
Governments and municipalities
Transmission and backup of resident registry data
Transmission of application forms and diagrams

ISP: Internet service provider
CAD: computer aided design
MRI: magnetic resonance imaging

Fig. 1. Application areas of the SSS.

2) ID/password authentication

The server is authenticated using a certificate, but the user is authenticated using the user ID and password. This is easier to use and suitable for situations where the other party is known to be within a closed group such as within a virtual private network.

2.3 Certified delivery and tracking

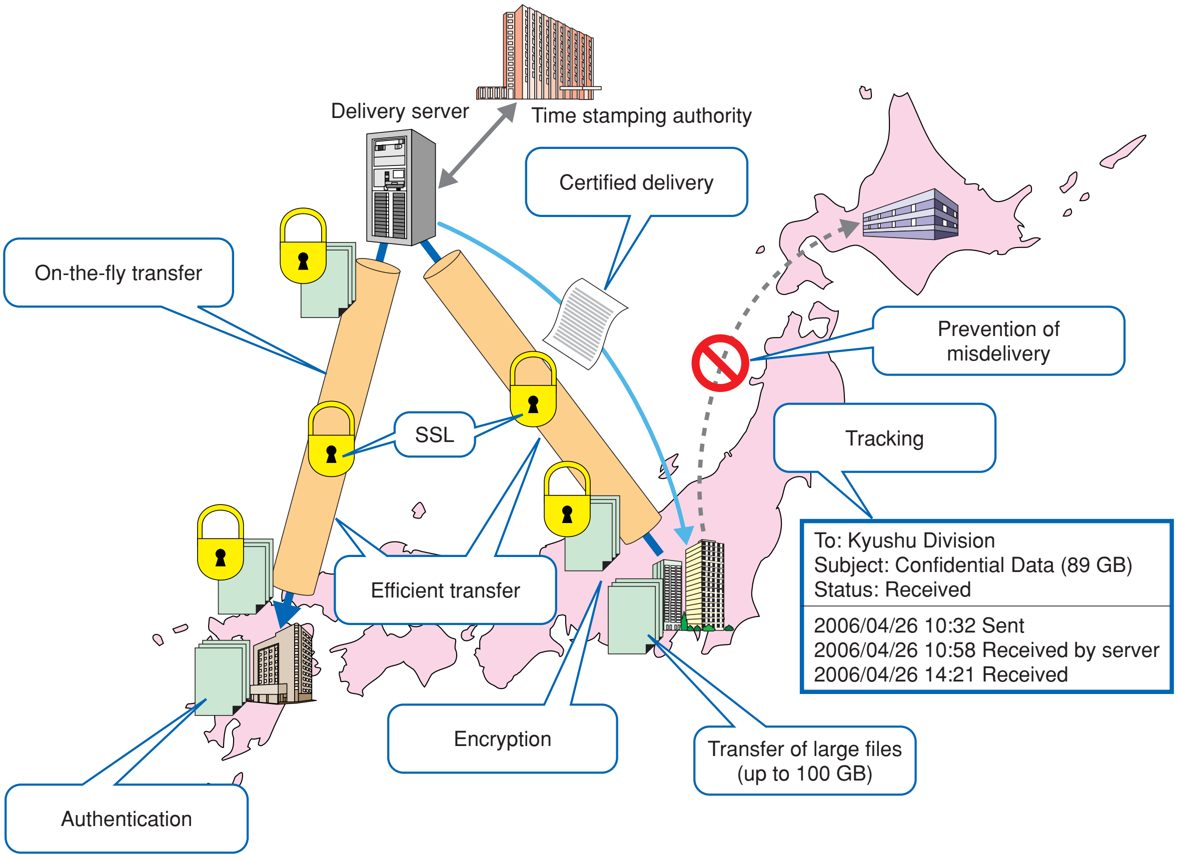
The SSS enables the sender of a file to keep track of its progress while it is waiting to be sent, is in transit, or has been received. Depending on the terms and conditions of a contract or of a scheduled workflow, it may be necessary to confirm or track the delivery state of content reliably. To certify a file exchange in such a case, the SSS works with a time stamping authority to issue an electronic data transfer certificate and a certificate certifying that a file has been transferred by a service provider. This enables the user to declare formally to third parties that a certain file was transmitted at such-and-such a time and received at such-and-such a time.

2.4 Prevention of misdelivery

The SSS allows the user to limit the range of possible destinations. For example, file transfer may be permitted only to a certain user or only to members of a predefined group. More detailed control of delivery is also possible, such as permitting a user only to send files or only to receive files. The state of permission to send or receive files is checked before a file is actually sent to the server so that even if an incorrect destination is specified, the file does not reach an unintended user.

2.5 Transfer of large files (up to 100 GB)

The printing and 3D CAD (three-dimensional computer aided design) industries usually need to transfer files in the 1- to 10-GB size range. The movie industry needs to transfer movie content with a size of 100 GB. Such large files often cannot be transferred reliably because of network instability or connection timeout. The SSS ensures reliable file transfer in the following way. A number of files to be transferred are bundled into a container. Each container is then divided into segments of a suitable size for reliable transfer. The receiver reassembles the container from the received segments. An application keeps track of the transfer of each segment, so that after an interruption, segment transfer can be resumed reliably. For exam-



To: Kyushu Division
Subject: Confidential Data (89 GB)
Status: Received

2006/04/26 10:32 Sent
2006/04/26 10:58 Received by server
2006/04/26 14:21 Received

Fig. 2. Overview of SSS functions.

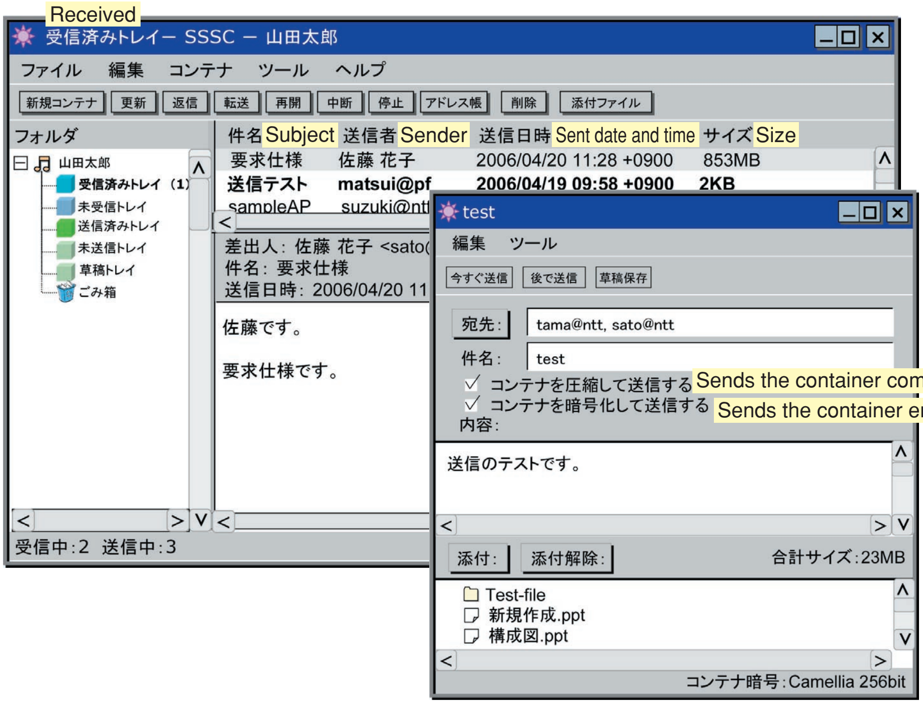
ple, even when a user terminal fails or a communication cable is disconnected accidentally during file transfer, the file transfer can be resumed from the point up to which reliable transfer had been confirmed. This avoids the waste of time that often occurs when an interrupted file transfer has to be restarted from the beginning.

2.6 Efficient transfer

The transfer of a file as large as 100 GB between two locations takes hours even when a high-speed link is used. Moreover, the time for transfer via a server usually consists of the sender's uploading time plus the receiver's downloading time, which doubles the end-to-end transfer time. For faster transfer, the SSS implements a "wait-free" transfer mode, which we call "on-the-fly", that enables the receiver to download file segments immediately after they have been received, while the sender is still uploading the remaining segments. This feature is similar to the "chase play" mode of hard disk recorders that allows a user to watch a TV program while it is being recorded instead of having to wait until the end of the recording in order to rewind the video cassette and replay it. This efficient transfer scheme means that the receiver can get a file almost as soon as the sender finishes sending it.

2.7 API and client applications

We provide a common application programming interface (API) in addition to application, browser, and command-line-based clients. The application client (**Fig. 3**) works just like ordinary email, so anyone who is used to using an email program can easily use all the available functions of the SSS. Although the browser client (**Fig. 4**) provides the selected functionality, it does not require any program to be installed: it works like Web mail. Therefore, this is suitable for light users. The command-line-based client enables shell scripts to be used to automate the transmission and reception of files. It can be customized to suit the particular workflow to be used. As shown in **Fig. 5**, these client applications run on top of the common API, which makes it possible to



受信済みトレイー SSSC ー 山田太郎

件名	送信者	送信日時	サイズ
要求仕様	佐藤 花子	2006/04/20 11:28 +0900	853MB
送信テスト	**matsui@pf**	**2006/04/19 09:58 +0900**	**2KB**
sampleAP	suzuki@ntt		

差出人：佐藤 花子 <sato(
件名：要求仕様
送信日時：2006/04/20 11

佐藤です。

要求仕様です。

受信中：2　送信中：3

test

宛先：tama@ntt, sato@ntt
件名：test
✓ コンテナを圧縮して送信する
✓ コンテナを暗号化して送信する
内容：

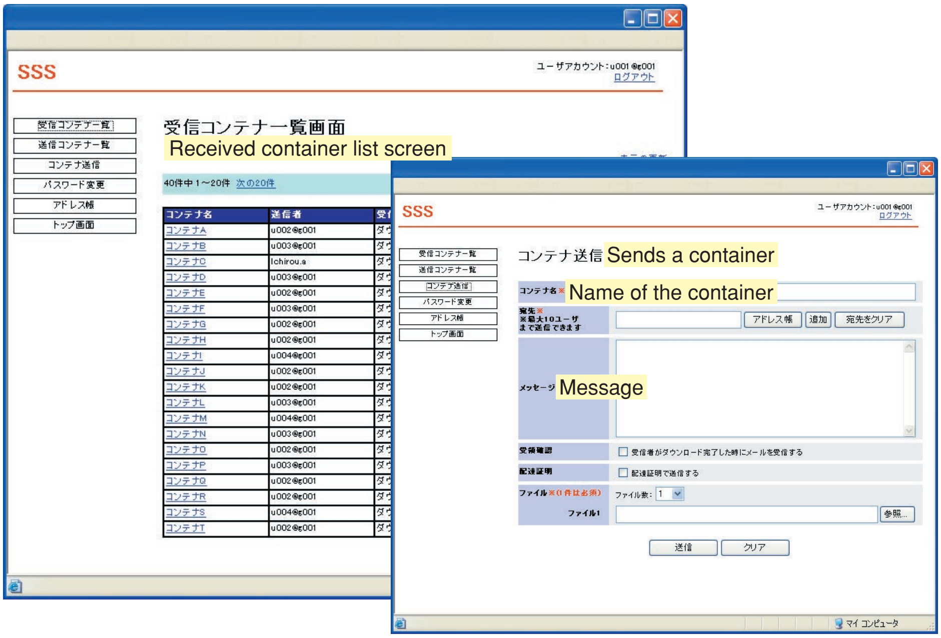
送信のテストです。

合計サイズ：23MB

Test-file
新規作成.ppt
構成図.ppt

コンテナ暗号：Camellia 256bit

Fig. 3. Example of windows of a dedicated application-type client (Japanese version).



ユーザアカウント：u001@g001

受信コンテナ一覧画面

40件中 1～20件 次の20件

コンテナ名	送信者	受
コンテナA	u002@g001	ダウ
コンテナB	u003@g001	ダウ
コンテナC	Ichirou.a	ダウ
コンテナD	u003@g001	ダウ
コンテナE	u002@g001	ダウ
コンテナF	u003@g001	ダウ
コンテナG	u002@g001	ダウ
コンテナH	u002@g001	ダウ
コンテナI	u004@g001	ダウ
コンテナJ	u002@g001	ダウ
コンテナK	u002@g001	ダウ
コンテナL	u003@g001	ダウ
コンテナM	u004@g001	ダウ
コンテナN	u003@g001	ダウ
コンテナO	u002@g001	ダウ
コンテナP	u003@g001	ダウ
コンテナQ	u002@g001	ダウ
コンテナR	u002@g001	ダウ
コンテナS	u004@g001	ダウ
コンテナT	u002@g001	ダウ

ユーザアカウント：u001@g001

コンテナ送信

コンテナ名※	
宛先※ ※最大10ユーザまで送信できます	
メッセージ	
受領確認	□ 受信者がダウンロード完了した時にメールを受信する
配達証明	□ 配達証明で送信する
ファイル※(1件は必須)	ファイル数：1
ファイル1	

Fig. 4. Example of windows of a browser-type client (Japanese version).

develop applications dedicated to a specific industry, a specific usage, or a specific business. By offering these capabilities, the SSS can support a wide range of services, from simple ASP services to the development of sophisticated applications dedicated to a specific workflow or usage.

3. Future work

Communication over the Internet may currently experience considerable delays due to the properties of TCP/IP (transmission control protocol, Internet protocol) or sheer physical distance, resulting in the

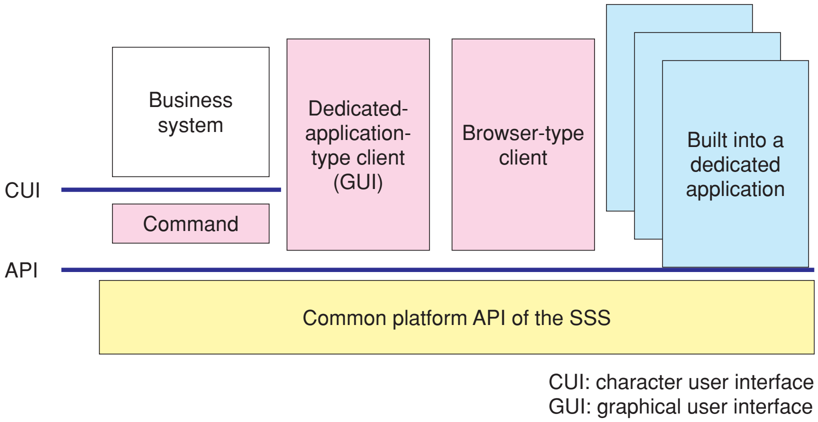

Business system
Dedicated-application-type client (GUI)
Browser-type client
Built into a dedicated application
CUI
Command
API
Common platform API of the SSS
CUI: character user interface
GUI: graphical user interface

Fig. 5. Application architecture.

effective communication speed possibly being much lower than the speed of the communication link used. When a user needs to deliver a large file, the effective communication speed might even be so low that it would be faster to burn the file to CDs and have them delivered by a motorcycle courier. We plan to develop an express delivery service that can reliably transmit a file faster than the normal Internet communication service. We will develop a mechanism for selecting the optimum transmission method on the basis of the actual network delay and throughput. This service will allow the rapid transmission of files larger than 1 GB, such as CAD data and artwork.

NTT Software Corporation currently sells an email encryption program called Cipher Craft/Mail (shortened to CC/Mail below). This add-on program gives the user's existing email program the functions of both Camellia-based email encryption and misdelivery prevention. We are studying a mechanism for switching between CC/Mail and the SSS, with the former being used when the file to be sent is small and the latter when it is large. This will enable the user to continue to use his/her existing email environment without having to decide which transfer method to use in each case because it will automatically and seamlessly select the ordinary email scheme for transmission of a non-confidential file, CC/Mail for a small confidential file, and the SSS for a large confidential file.

References

[1] https://info.isl.ntt.co.jp/crypt/eng/camellia/index_s.html
[2] K. Yamada and K. Ishikawa, "Secure, Reliable and Efficient Content Delivery System that Can Collaborate with Business Applications Easily," NTT Technical Journal, Vol. 13, No. 2, pp. 40-43, 2001 (in Japanese).
[3] T. Abe and M. Kawashima, "Highly Efficient File Transfer System Suitable for Scalable Data Transfer," IEICE Technical Report, IA2001-27, pp. 57-62, 2001 (in Japanese).
[4] "Platform for the Printing, Typesetting, Advertising and Publishing Industries (GTRAX)," Business Communication, Vol. 38, No. 6, pp. 26-27, 2001 (in Japanese).
[5] H. Arai and K. Ishikawa, "Highly Efficient BtoB Content Delivery System: MDS-Pack," NTT Technical Journal, Vol. 14, No. 4, pp. 39-43, 2002 (in Japanese).

Katsuhiko Yoshida

Senior Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.E. degree in telecommunication engineering from Tokyo Denki University, Tokyo, in 1989. He joined NTT in 1989. In 2003, he was transferred to NTT Information Sharing Platform Laboratories.

Masaki Tanikawa

Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees in systems science from Tokyo Institute of Technology, Tokyo, in 1993 and 1995, respectively. He joined NTT in 1995. He is engaged in R&D of a scalable file-sharing system. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Kazuyuki Takaya

Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees in electronics, information, and communication engineering from Waseda University, Tokyo, in 1998 and 2000, respectively. In 2000, he joined NTT Information Sharing Platform Laboratories, Tokyo, where he engaged in R&D of contents delivery network systems. He is a member of IEICE.

Koji Morishita

Research Engineer, Communication Platform SE Project, NTT Information Sharing Platform Laboratories.

He joined NTT in 1985. He has been engaged in research on IP networking structure and the measurement of service quality.

Hiroyuki Fujiwara

Senior Research Engineer, Communication Platform SE Project, Information Sharing Platform Laboratories.

He received the B.E., M.E., and Ph.D. degrees in electrical engineering from the University of Electro-Communications, Tokyo, in 1990, 1992, and 1995, respectively. He joined NTT in 1995. He is currently engaged in the development of a file sharing system.