Special Article on Advanced i-mode Mobile Phones

Security in i-mode —Secure Sockets Layer (SSL)—

Tatsuro Ooi, Yoshiaki Hiramatsu and Kyoko Inoue

In the 503i series, the security of i-mode communication is reinforced by SSL, which is a protocol that establishes secure communication against "impersonating", "bugging" and "tampering" associated with data communication.
This article reviews the SSL system and the implementations in i-mode.

1. Introduction

Recently, e-commerce websites and other sites involving transactions have been attracting a great deal of public attention. The prerequisite for services provided by these sites is a secure communication channel.

In i-mode, many sites have been providing transaction services from early years. Due to their extreme concern with reinforcing the security of i-mode, which is essential for enhancing these services, DoCoMo provided security protocols and algorithms for security-minded service providers of official sites in conventional i-mode services. The communication channel was secure but discontinuous, however, as the protocols and algorithms varied between content servers and i-mode servers, and between i-mode servers and mobile phones.

Thus, it has been DoCoMo's challenge to develop a continuous, secure, end-to-end communication channel, between content servers and mobile phones.

With this in mind, the 503i series adopts the Secure Sockets Layer (SSL), and thereby achieves a secure end-to-end communication platform.

This article explains the general SSL functions in brief, and reviews the SSL system and the implementations particularly with reference to specifications for i-mode.

2. Overview of SSL Functions

The SSL protocol has functions for preventing "impersonating", "bugging" and "tampering" [1], [2].

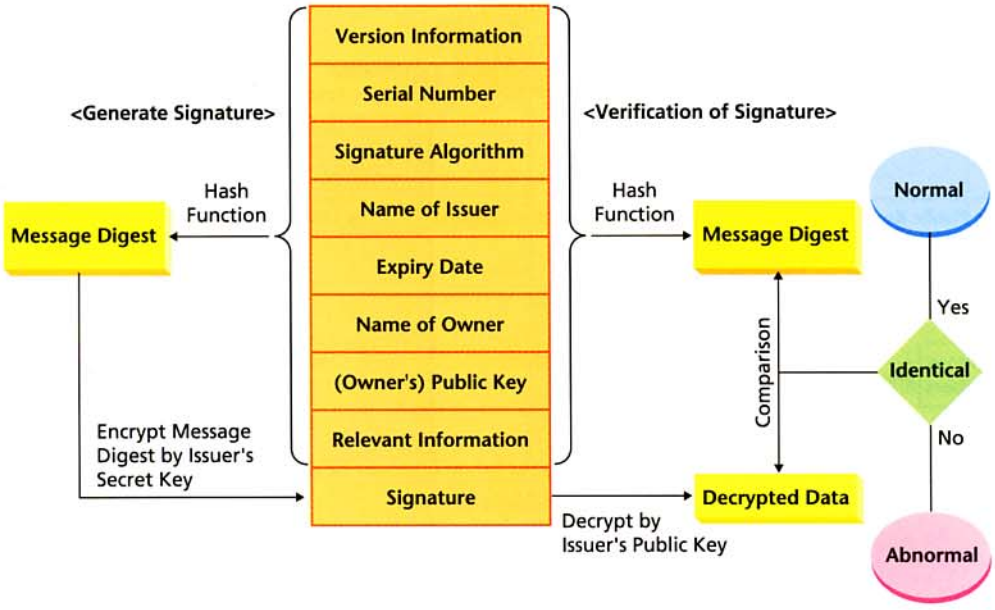

Figure 1 X.509 Certificate

2.1 Prevention of Impersonating

SSL prevents third parties from impersonating users by verifying their certificate prior to commencing encrypted communication, as a way of checking their identification. The data format of the certificate is specified by X.509[3] recommendation by the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), which is structured as shown in **Figure 1**. The public key cryptosystem is used for the verification of the certificate: the signature part encrypted by the secret key must be decrypted by the public key to determine the issuer of the certificate. SSL also verifies whether the certificate has been tampered with by calculating the message digest of the certificate data based on a one-way function called the hash function, and by comparing the results with the decrypted signature part.

2.2 Prevention of Bugging

Once the identification is confirmed, a common key will be generated for both sides, for encryption and decryption. As all data will be encrypted by the common key cryptosystem after this point, no malicious third party intervening in the communication channel will be able to eavesdrop the transmitted data without the common key. **Figure 2** illustrates how common keys are generated.

2.3 Prevention of Tampering

Third parties intervening in the communication channel might not be able to eavesdrop the encrypted data, but they can still tamper with the data itself. There are no ways to prevent data from being tampered with, but SSL is able to detect such tampering by attaching a Message Authentication Code (MAC) to the data that needs to be transmitted. MAC is a number computed from the Hash function, based on the contents of the data and a MAC secret key, which is secretly held by both the sender and the recipient.

No third party can reveal the MAC secret key or the contents of the transmitted data through MAC.

3. System Configuration

The system configuration required to make SSL connection possible in i-mode is described below.

3.1 Protocol Stack

As illustrated in **Figure 3**, SSL is on top of the Transport Layer (TL), and encrypts data in the Application Layer (AL) and higher layers. SSL is used upon request by the AL.

The AL can also directly use TL without SSL. The SSL protocol consists of two layers: the Record Layer protocol, which is placed right above the TL; and the Handshake/Alert/Change Cipher Spec protocol. The Handshake protocol deals with negotiation before starting encrypted communication, such as confirming the identification of the party at the other end and determining the encryption algorithm. The Record Layer protocol divides the received data into blocks of 214 bytes or smaller,

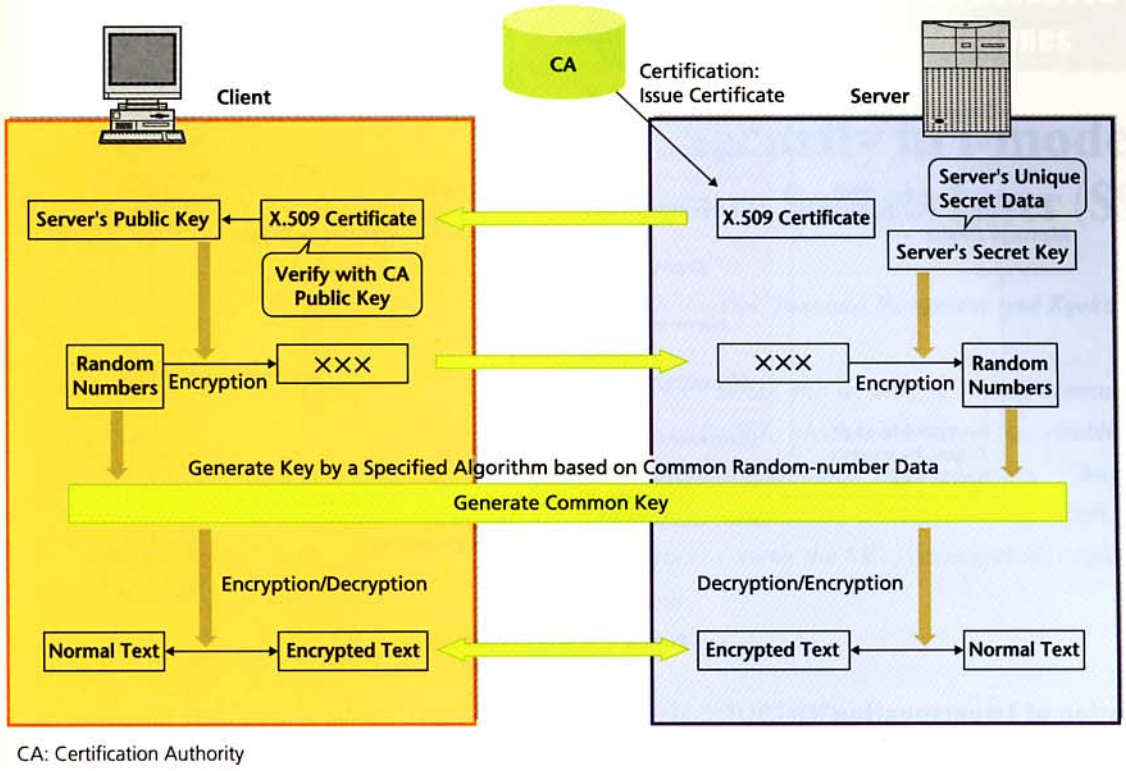

Figure 2 Procedures for Generating Common Key

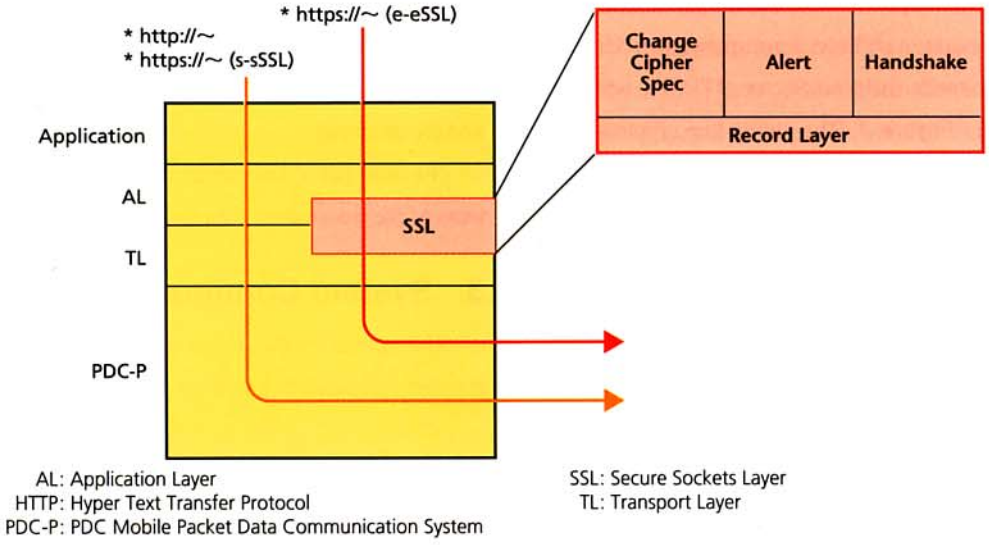

Figure 3 Protocol Stack

and puts them together into the required number of SSL data units. The data is divided upon transmission and assembled upon reception by the Record Layer protocol, transparently to the Handshake protocol.

3.2 Tunneling Protocol [4]

As described earlier, for conventional mobile phones, SSL communication has been available between the content server and the i-mode server (hereinafter referred to as "s-sSSL"). For the 503i series and later mobile phone models, however, DoCoMo must also enable SSL connection between the content server and the mobile phones (hereinafter referred to as "e-eSSL"), and thereby build a system that makes both s-sSSL and e-eSSL available.

The i-mode system relies on Internet connection via proxy servers. It therefore uses a tunneling protocol, as communica-

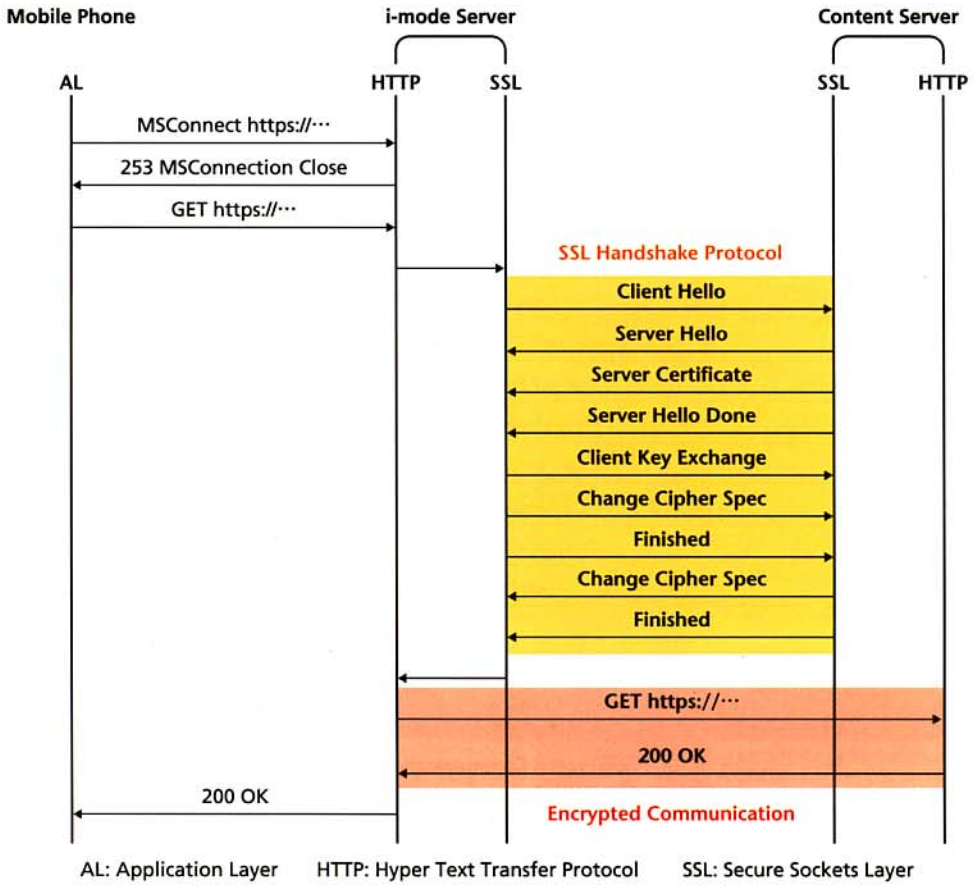

Figure 4 s-sSSL Sequence

tion must be transparent to the proxies for e-eSSL to work. When a 503i mobile phone is directed to a URL with "https" as the scheme, it will send a tunneling request to an i-mode server, with the URL information attached to it, before sending an HTTP request to the destination. The i-mode server will decide whether to allow tunneling based on the URL information, and return its decision to the mobile phone.

(1) s-sSSL

i-mode servers are equipped with a database that manages the URL of content providers who wish to have s-sSSL connection. The i-mode server is designed to reject a mobile phone's tunneling request for any destination URL that is registered with the database. When the tunneling request is rejected, the mobile phone acknowledges the communication protocol as s-sSSL, and sends an HTTP request to the i-mode server without SSL, as 502i mobile phones do.

Subsequently, the i-mode server receives the HTTP request, determines that the SSL protocol is required for communication by referring to the URL scheme (https), and establishes an SSL session. Then, it sends an HTTP request to the content server.

Figure 4 illustrates the sequence of s-sSSL connection with SSLv3 is in use.

(2) e-eSSL

On the other hand, the i-mode server accepts the mobile phone's tunneling request for a destination URL that is not registered with the database. When the tunneling request is accepted, the mobile phone acknowledges the communication protocol as e-eSSL, and establishes an SSL session. Then, it sends an HTTP request to the content server. As communication takes place transparently to the i-mode server once the tunneling request has been accepted, the end-to-end communication channel is both continuous and secure.

Figure 5 illustrates the sequence of e-eSSL connection with SSLv3 is in use.

4. Specification of SSL Implemented in Mobile Phones

This chapter describes the specifications of SSL implemented in the 503i series.

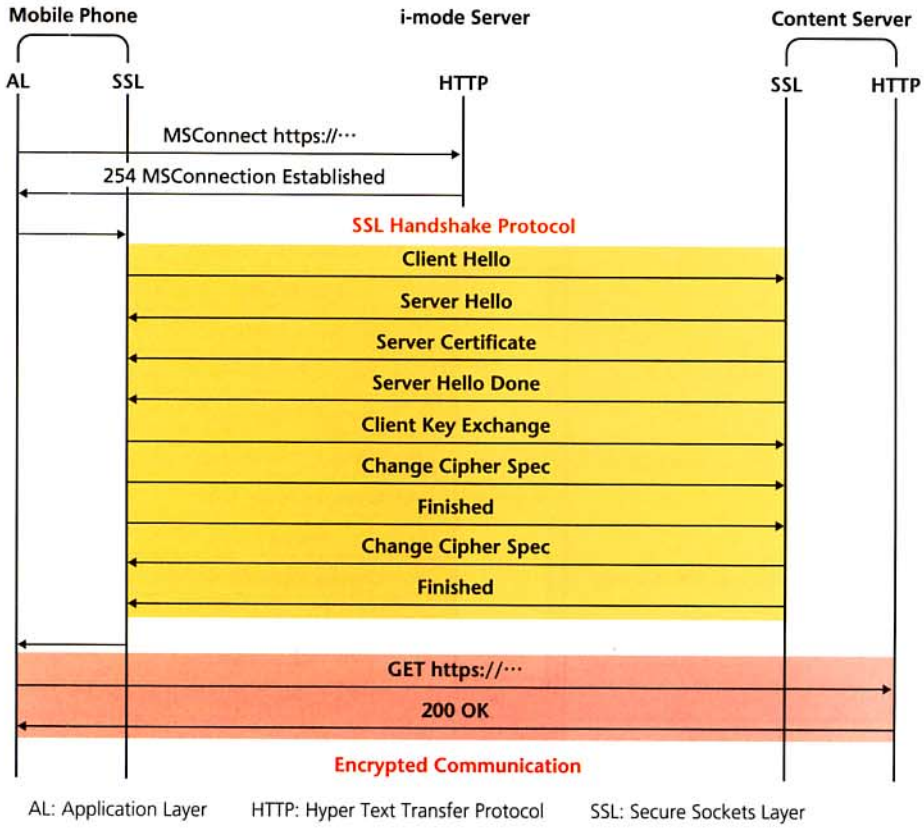

Figure 5 e-eSSL Sequence

4.1 Specifications

Table 1 shows the key specifications of SSL for the 503i mobile phones.

Table 1 Key Specifications of 503i Series

Version	SSLv2, SSLv3
Maximum Key Length Required (Common Key)	128 bit
Maximum Key Length Required (Public Key)	1024 bit
Certification Function	Server Certification
Implemented CA Certificates	VeriSign Class3 Primary CA
	VeriSign Class3 Primary CA G2
	RSA Secure Server CA
	GTE Cyber Trust Root
	GTE Global Root

CA: Certification Authority
SSL: Secure Sockets Layer

4.2 User Interface Functions

The SSL protocol is used when a relatively high level of security is required in communication. Hence, the user must be informed as to whether the connection relies on SSL. The 503i series has the following display functions to inform the user.

(1) Communicating/Browsing Message

During SSL communication, a notice is displayed on the screen to indicate that the communication is encrypted. When acquired contents are being displayed on the browser, the SSL pictogram flashes on the screen (**Figure 6**).

(2) Warning Message

When the user finishes browsing SSL-protected content, the user is warned that further connection or browsing will not be protected by SSL. The warning message informs the user that the SSL session is over.

(3) Error Message

If a critical error occurs and undermines the security of SSL communication, the connection will be terminated and the user will be informed of the reasons. Table 1 shows the certificates issued by Certification Authorities (CA) that are recognized by the 503i series. If the user accesses sites that are certified by other CAs, the message "This site might not be safe. Do you wish to connect?" will appear on the screen and prompt the user to decide whether to connect/disconnect.

(4) Certificate Reference Function

During browsing, the user can refer to the certificate of the server from which the content has been acquired. This enables the user to clearly identify the destination when sending passwords and other confidential information.

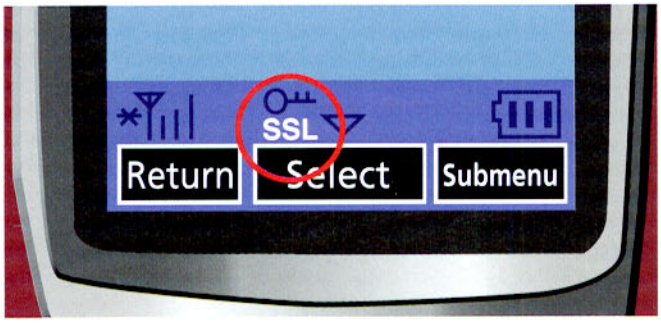

Figure 6 SSL Pictogram

5. Conclusion

This article reviewed the SSL system and its implementations in i-mode.

Out next challenge is to introduce more advanced certification technologies and to provide a communication platform with greater security.

GLOSSARY

AL: Application Layer
CA: Certification Authority
HTTP: Hyper Text Transfer Protocol
ITU-T: International Telecommunication Union-Telecommunication Standardization Sector
MAC: Message Authentication Code
MS: Mobile Station
PDC-P: PDC Mobile Packet Data Communication System
SSL: Secure Sockets Layer
TL: Transport Layer

REFERENCES

[1] A.O.Freier, P.Karlton, P.C.Kocher, "The SSL Protocol Version 3.0", draft-freier-ssl-version3-02.txt, Nov.1996.
[2] http://www.netscape.com/eng/security/ssl_2.html
[3] R.Housley, W.Ford, W.Polk, D.Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC2459, Jan.1999.
[4] A.Luotonen, "Tunneling SSL Through a WWW Proxy", draft-luotonen-ssl-tunneling-02.txt, Dec.1995.