Freescale Semiconductor
Application Note

Document Number: AN4363
Rev. 0, 10/2011

Connecting to an SMTP Server Using the Freescale NanoSSL Client

by: Paolo Alcantara
Microcontroller Solutions Group

Contents

1 Introduction.....1
2 Overview of the SMTP client application.....2
3 Conclusion.....10

1 Introduction

This document describes the necessary steps for connecting to a Simple Mail Transfer Protocol (SMTP) server from a Freescale NanoSSL™ client using the Secure Socket Layer (SSL) protocol. Freescale NanoSSL is an inexpensive royalty-free product intended for use with Freescale MQX™. At the end of the process described in this document, the application sends an email that can be used for logging, alerts, notifications, status, or as an input to another embedded application.

1.1 Scope

This document presents information about SMTP for an application that connects to a secure Gmail™ account using SSL. An example project can be obtained from the NanoSSL product after purchase. A web link is provided in the first reference at the end of this application note.

This document is intended to be used by all software development engineers, test engineers, and anyone else who is implementing an SMTP client using Freescale NanoSSL for an embedded device.

2 Overview of the SMTP client application

The SMTP client application connects to a remote SMTP server, in this case, Gmail (smtp.gmail.com). Communication is over SSL, a cryptographic protocol that provides security over the Internet. For SSL communication, the Freescale NanoSSL client software is used. The RTOS that works with this software is Freescale MQX. The API used in the application code is documented and can be obtained as soon as the software is acquired, making it easy to understand.

The SMTP server used can be changed to a customized SSL server by following the source code and this document.

2.1 SMTP client application details

The following sections address details that need to be considered for connection with an SMTP client application.

2.1.1 Basic SMTP over SSL

The complete application can be found in the mss_ssl_client.c application software. It performs the following actions:

1. Starts a basic socket and requests that the SSL protocol starts using the SMTP protocol
2. Starts an SSL socket and continues using the SMTP protocol over SSL
3. Requests that an email be sent, fills the email, and sends it to the SMTP server
4. Closes the connection.

Further information about SMTP can be found in application note AN3930, "Email Client Using MCF51CN Family and FreeRTOS."

2.1.2 Certificates used by the SSL client

Certificates are digital information that contains a digital signature from an authority that certifies the information. During the SSL protocol, the server certificate must be verified. As part of this verification, the SSL client compares its local SSL server certificate against the received SSL server certificate. If they match, communication continues; otherwise, it fails.

Parsing the received SSL server certificate means that there may be more than one certificate present during the communication. In this case, each one of the certificates is linked together as a certificate chain, shown in the diagram below. The last certificate in the chain is the root certificate. This last certificate is used by the NanoSSL client software to validate the SSL communication.

Freescale NanoSSL client software expects the application to provide a valid Certificate Authority (CA) certificate for checking during SSL communication. The following section shows how to determine the name of the certificate and how it can be obtained for the SMTP client application.

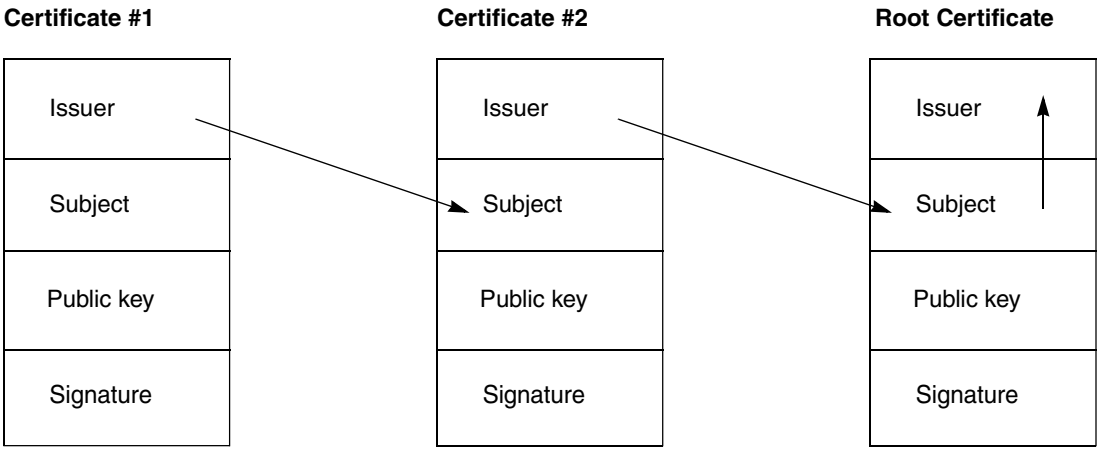

Figure 1. Certificate chain

Certificates used by the SMTP server have an expiration date, which means that at some point, the certificate used by the application must be updated with a new one. The following steps must be considered during this process.

2.1.2.1 How to get a certificate from an SMTP server

1. Configure an email desktop application with the settings of the remote SMTP server. In this example, Microsoft Outlook Express® is used as a Gmail server as shown in the figures below.

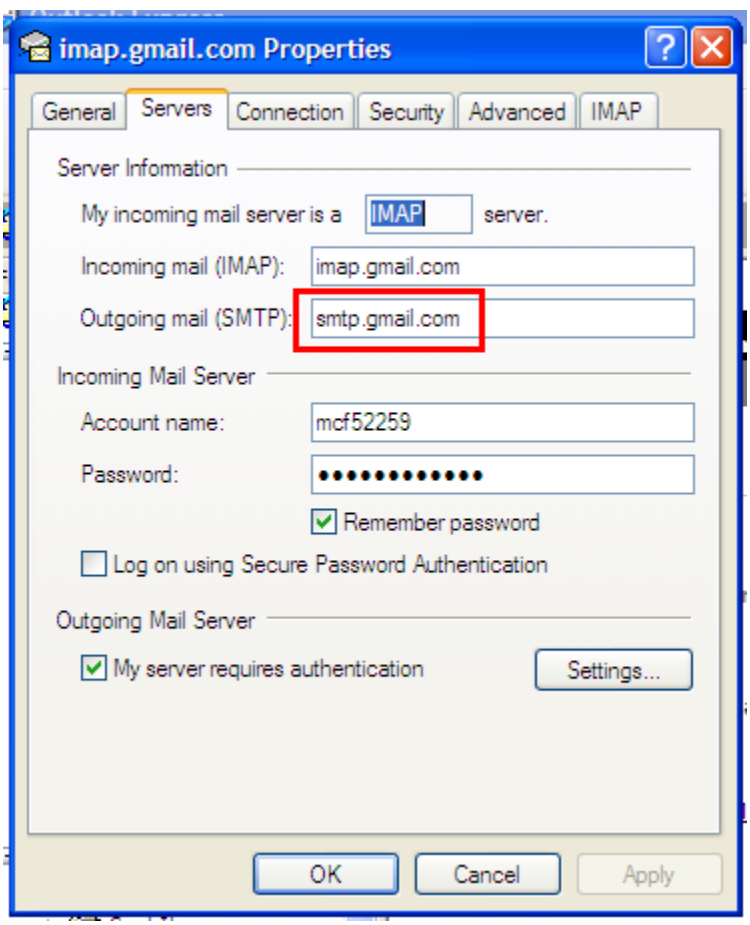

Figure 2. Outlook Express settings (1)

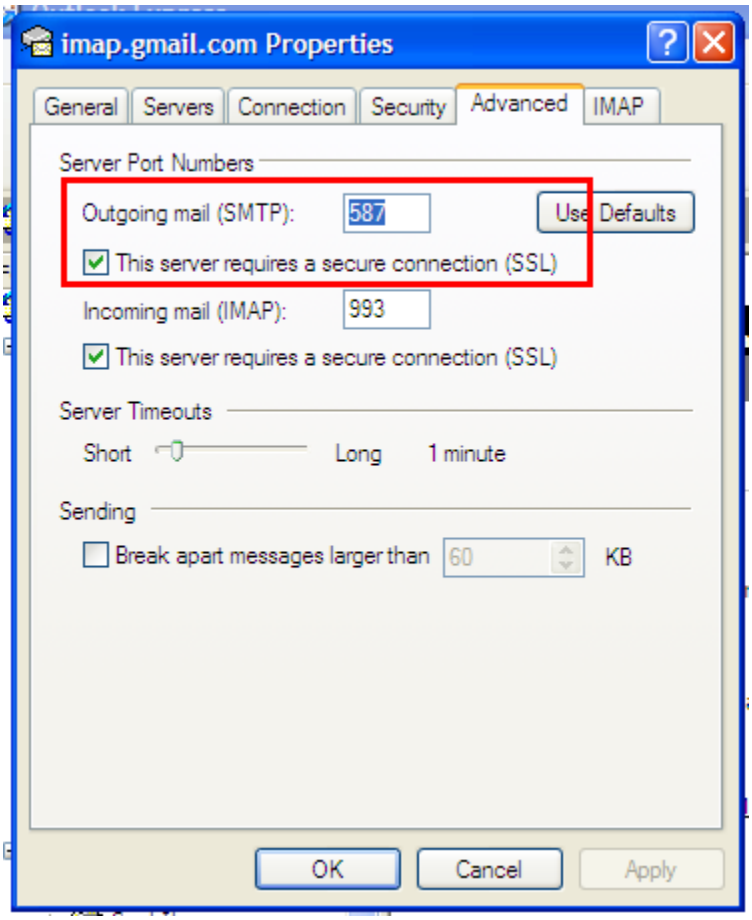

Figure 3. Outlook Express settings (2)

2. Send an email from the desktop email application. Check to see whether the email is received at the remote email account. If it doesn't work, the SMTP server might not be available through a desktop email application such as Outlook.
3. Repeat the previous step, taking a TCP/IP log file from the remote SMTP server. In this example, the Outlook Express application is logged using the Wireshark network protocol analyzer. The following figure shows an example:

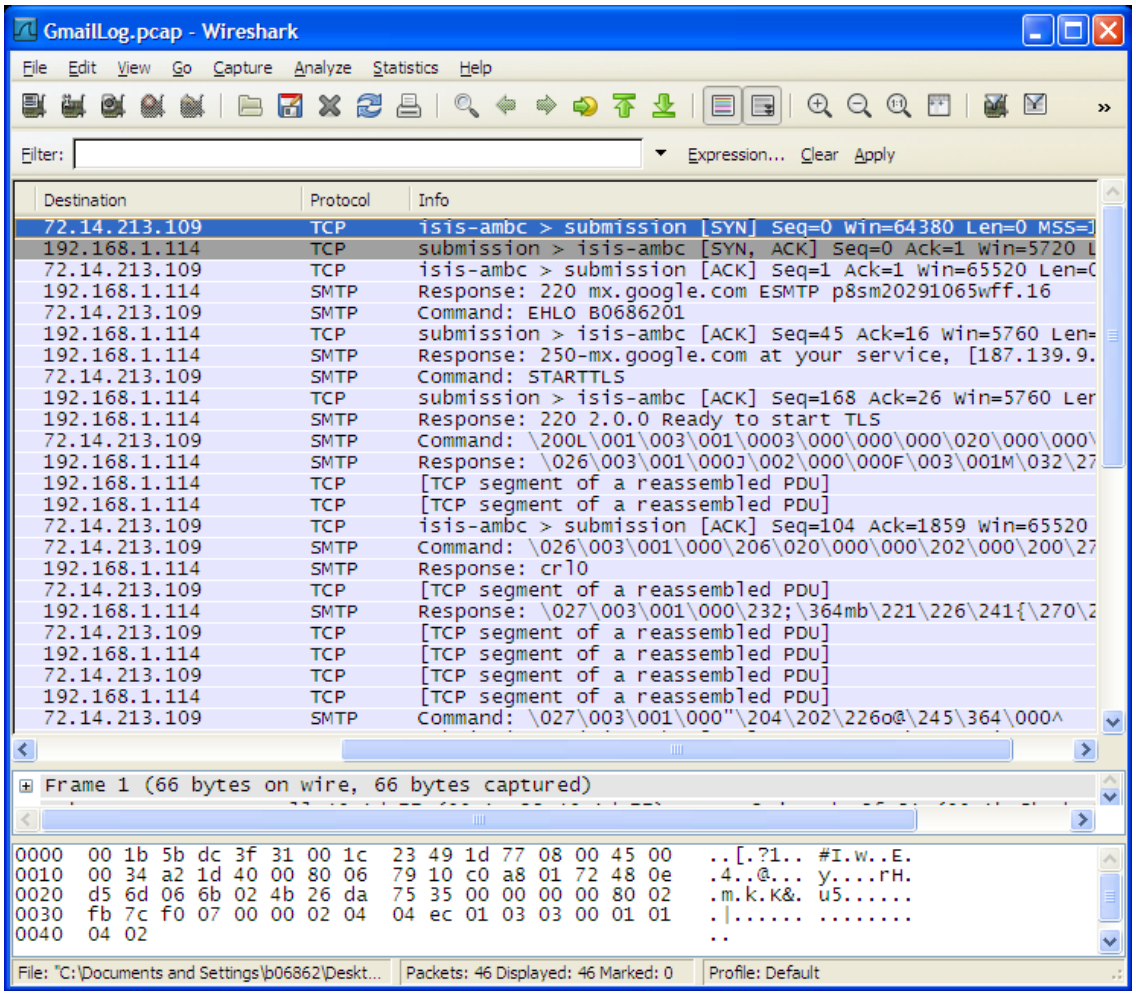

Figure 4. Wireshark filter

4. TCP communication between the email reader and remote SMTP server is only necessary for the next step. In this example, filter communication by using ip.addr == 72.14.213.109 as shown in the following figure.

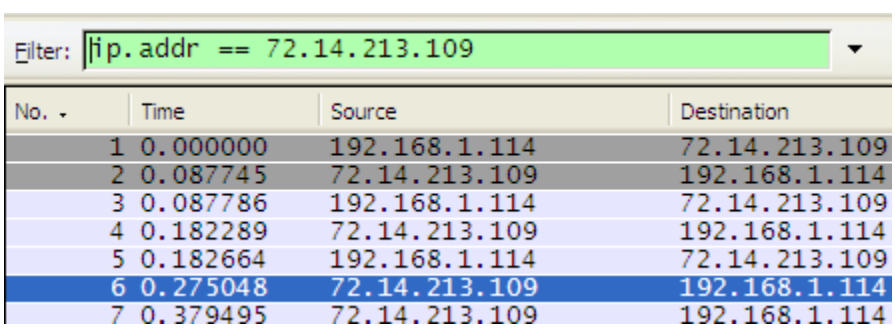

Figure 5. Wireshark filter

5. The log file should now show SSL communication. In the following example, SMTP is shown instead. To change, decode communication to SSL by right-clicking and selecting “Decode as” as shown in the following figures.

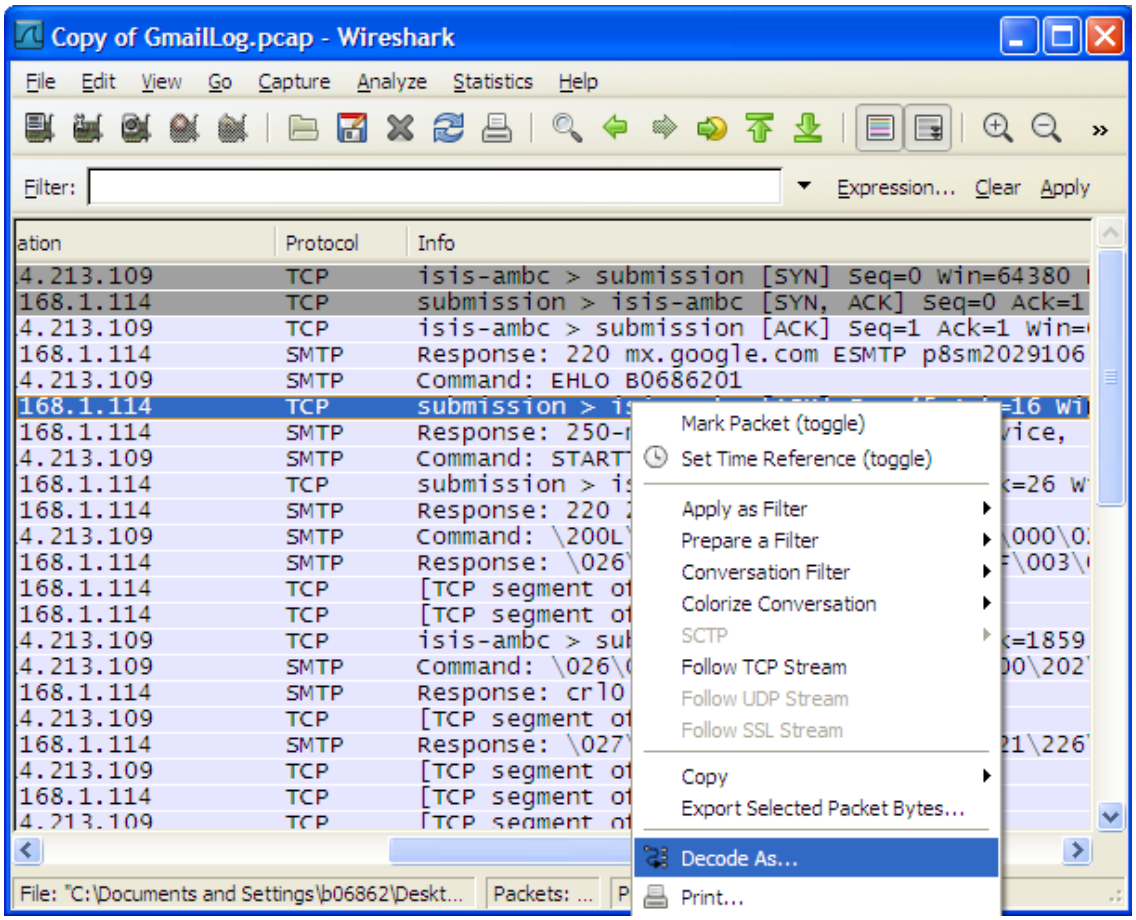

Figure 6. Decoding TCP communication as SSL in Wireshark

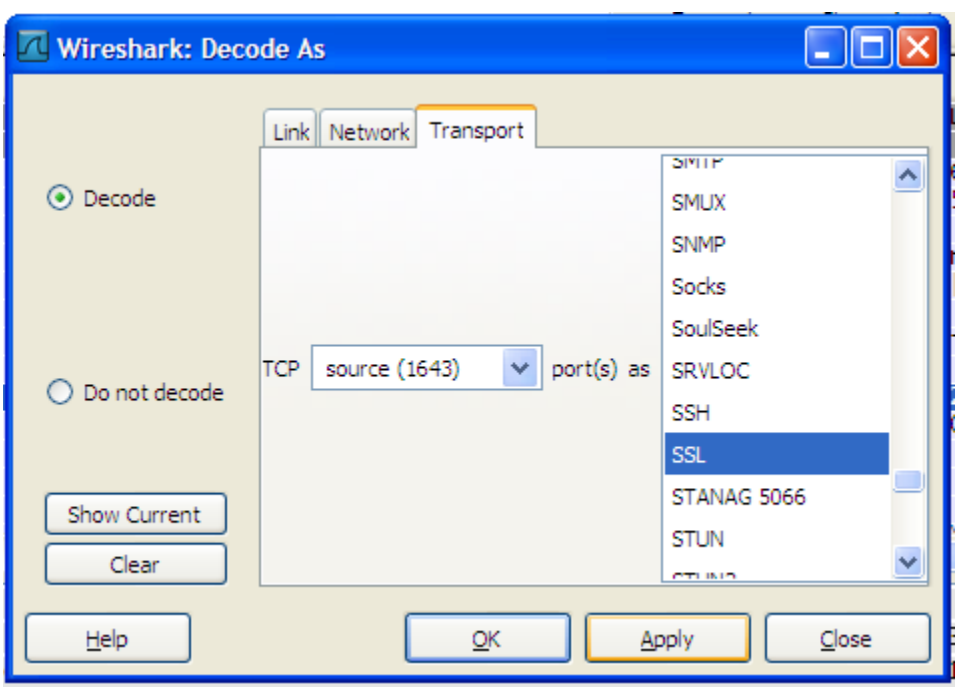

Figure 7. Selecting SSL as the decoding protocol

6. Now, browse the last certificate. In the following figure, the last certificate is outlined in red.

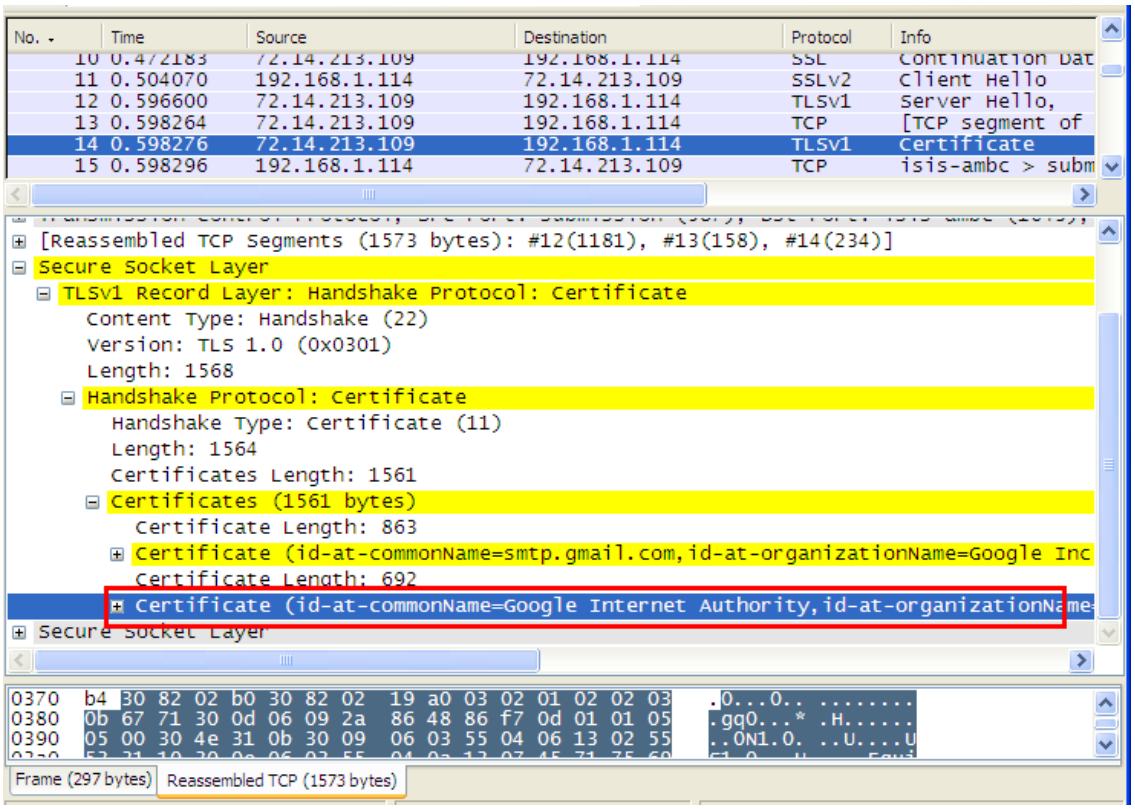

Figure 8. Using the last certificate from the chain

7. Extract the certificate string from the browsed certificate using this path: [Last Certificate] → Signed Certificate → Issuer → rdnSequence → [OrganizationalUnitName] → Item → DirectoryString → printableString →"Certificate Name." In this example, the string is "Equifax Secure Certificate Authority," as shown in the figure below.

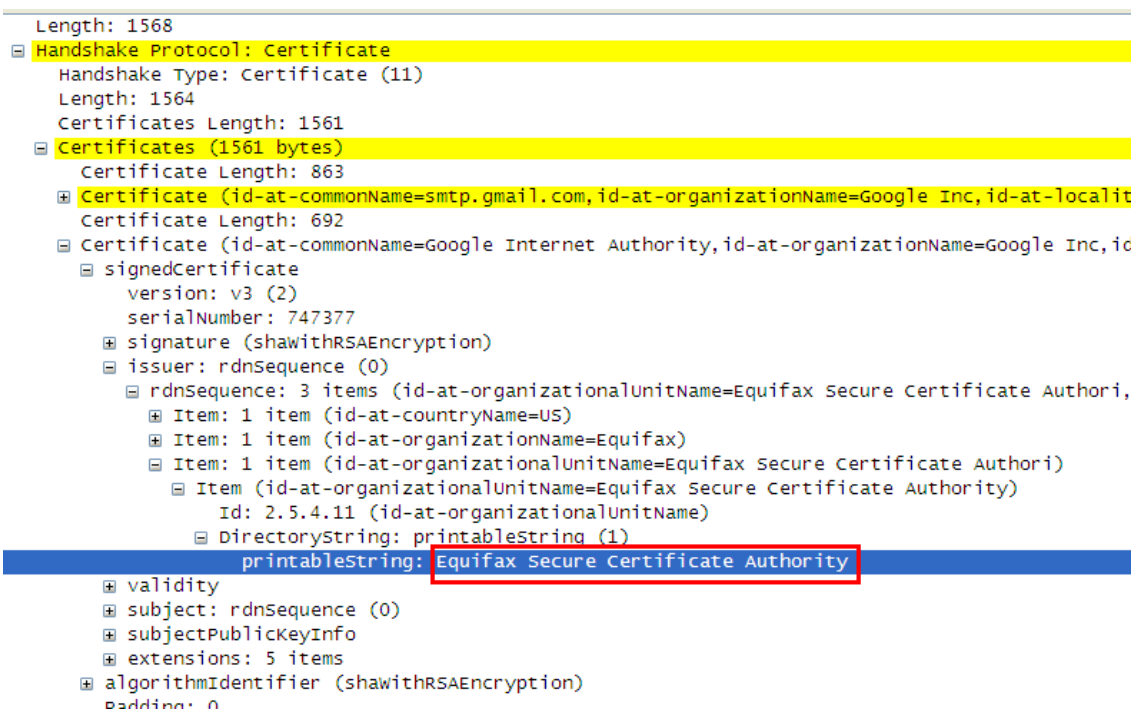

Figure 9. Extracting a string from the last certificate

8. Details about the certificate expiration date (validity) can also be extracted from last step.

9. Use the string to get the certificate from the web or a web browser application. In this example, the certificate is from Mozilla Firefox®, as shown in the following figure.

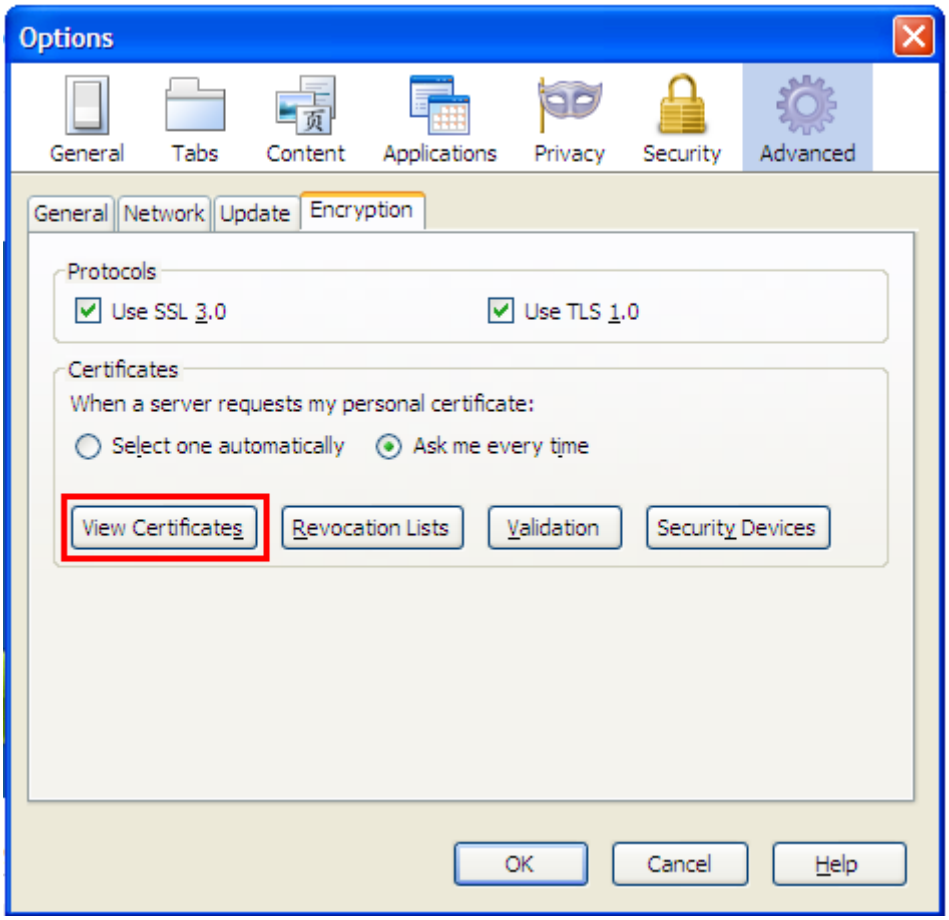

Figure 10. Extracting a certificate from Mozilla Firefox (1)

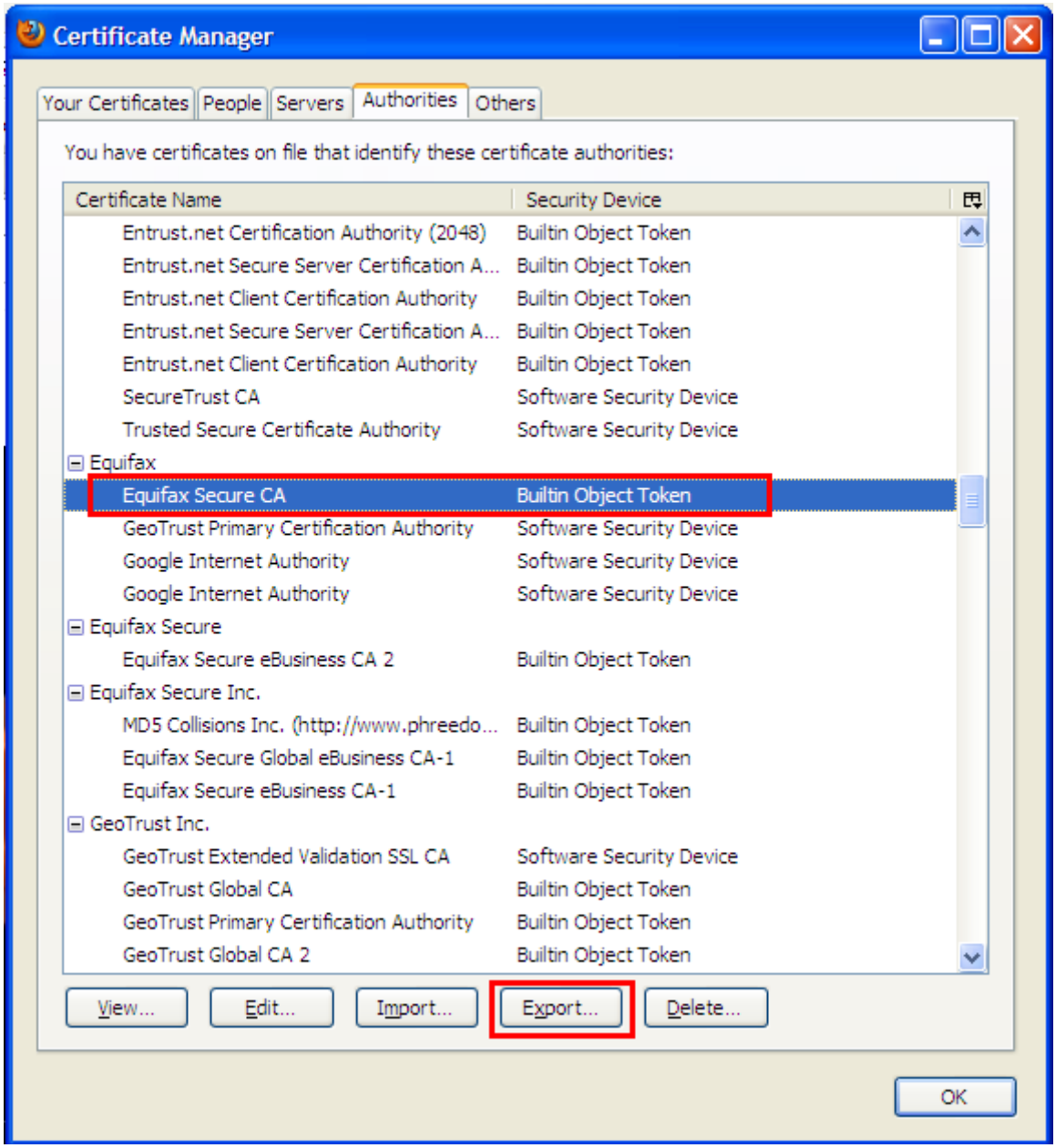

Figure 11. Extracting a certificate from Mozilla Firefox (2)

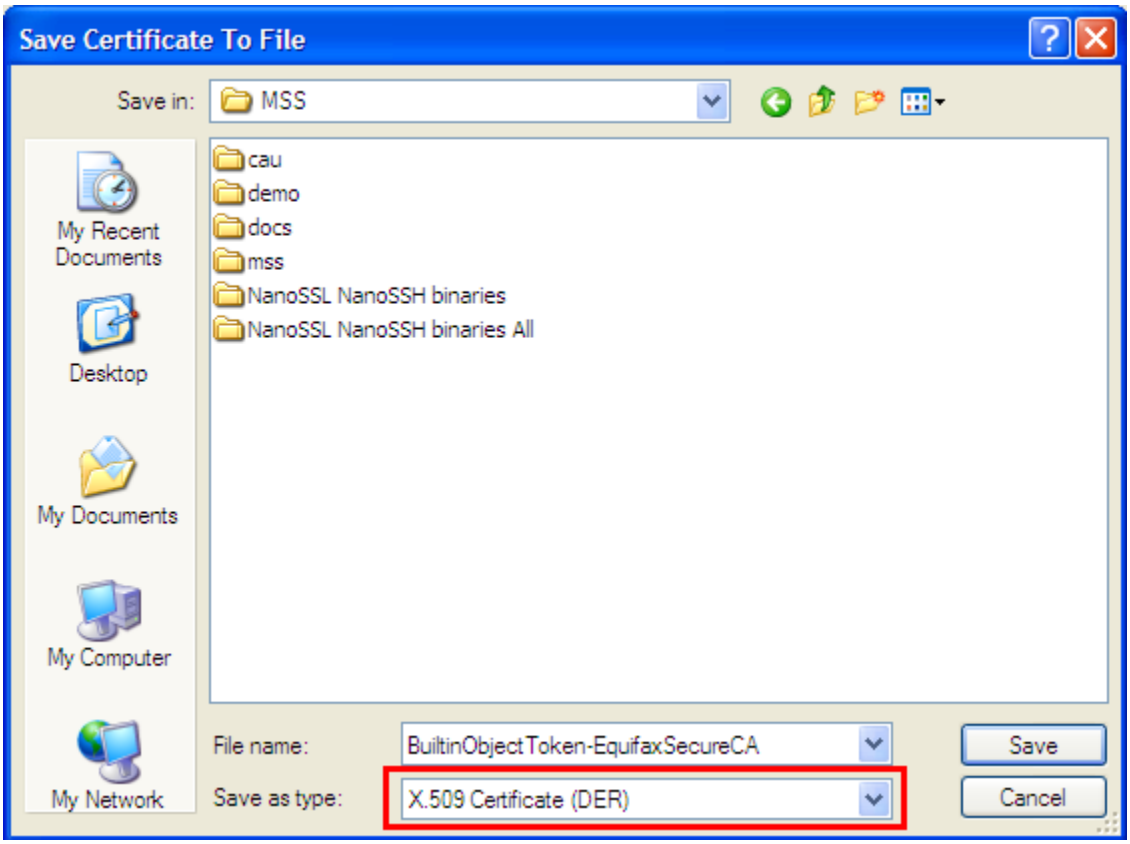

Figure 12. Extracting a certificate from Mozilla Firefox (3)

10. Open the extracted DER certificate and store the hexadecimal data as a C-language array in the source code. You can use a trial software package like Hex Editor Neo to get the hexadecimal information. An example is shown in the following figure.

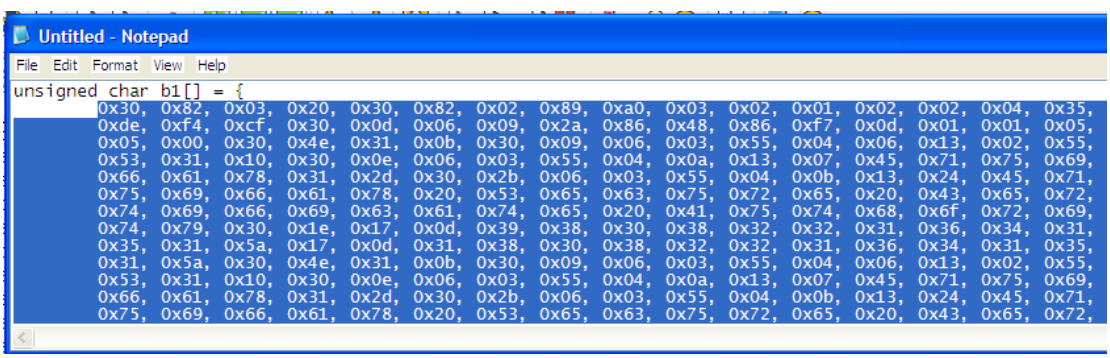

Figure 13. Certificate array to be used in the application software

11. The extracted C-language array must be inserted in the mss_ssl_client.c source as shown in the Gmail example code. This is used by the Freescale NanoSSL client example software.

3 Conclusion

This document describes how to send an email using an SMTP server through an SSL connection. Following the principles described above, you can explore several options for sending information from an embedded device, such as logging files, events, alerts, and so on. Further options, like WiFi, can be added to explore wireless options.

3.1 Reporting problems

Issues and suggestions about this document and the associated drivers should be provided through the Freescale support webpage at www.freescale.com/support. Please reference this application note.

3.2 Considerations and references

- Find the newest information about the Freescale NanoSSL client on the Freescale Semiconductor (www.freescale.com) and Freescale NanoSSL (www.freescale.com/nanossl) home pages.
- The software associated with this application note (AN4363SW) can be found on the Downloads area of the Freescale NanoSSL home page. It includes only the SMTP application; Freescale NanoSSL is not included.
- For further information about the SMTP protocol, see AN3930, "Email Client Using MCF51CN Family and FreeRTOS."

How to Reach Us:

Home Page:
www.freescale.com

Web Support:
http://www.freescale.com/support

USA/Europe or Locations Not Listed:
Freescale Semiconductor
Technical Information Center, EL516
2100 East Elliot Road
Tempe, Arizona 85284
+1-800-521-6274 or +1-480-768-2130
www.freescale.com/support

Europe, Middle East, and Africa:
Freescale Halbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
www.freescale.com/support

Japan:
Freescale Semiconductor Japan Ltd.
Headquarters
ARCO Tower 15F
1-8-1, Shimo-Meguro, Meguro-ku,
Tokyo 153-0064
Japan
0120 191014 or +81 3 5437 9125
support.japan@freescale.com

Asia/Pacific:
Freescale Semiconductor China Ltd.
Exchange Building 23F
No. 118 Jianguo Road
Chaoyang District
Beijing 100022
China
+86 10 5879 8000
support.asia@freescale.com

For Literature Requests Only:
Freescale Semiconductor Literature Distribution Center
1-800-441-2447 or +1-303-675-2140
Fax: +1-303-675-2150
LDCForFreescaleSemiconductor@hibbertgroup.com

Document Number: AN4363
Rev. 0, 10/2011