

**Application Note** 

# Connecting to an SMTP Server Using the Freescale NanoSSL Client

by: Paolo Alcantara Microcontroller Solutions Group

# **1** Introduction

This document describes the necessary steps for connecting to a Simple Mail Transfer Protocol (SMTP) server from a Freescale NanoSSL<sup>TM</sup> client using the Secure Socket Layer (SSL) protocol. Freescale NanoSSL is an inexpensive royaltyfree product intended for use with Freescale MQX<sup>TM</sup>. 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  $\text{Gmail}^{\text{TM}}$  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.

### Contents

1	Introduction	1
2	Overview of the SMTP client application	2
3	Conclusion1	0



# 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.



#### Overview of 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<sup>®</sup> is used as a Gmail server as shown in the figures below.

ĺ	a imap.gmail.com Properties									
	General Servers Connection Security Advanced IMAP									
Server Information										
My incoming mail server is a IMAP server.										
Incoming mail (IMAP): imap.gmail.com										
	Outgoing mail (SMTP): smtp.gmail.com									
1	Incoming Mail Server									
	Account name: mcf52259									
	Password:									
	Remember password									
	Log on using Secure Password Authentication									
	Outgoing Mail Server									
	✓ My server requires authentication Settings									
1	OK Cancel Apply									

Figure 2. Outlook Express settings (1)



overview of the SMTP client application

	🗟 imap.gmail.com Properties 🛛 🔹 🔀
	General Servers Connection Security Advanced IMAP
	Server Port Numbers
	Outgoing mail (SMTP): 587 Use Defaults
	This server requires a secure connection (SSL)
	Incoming mail (IMAP): 993
٩	This server requires a secure connection (SSL)
	Server Timeouts
	Short 🖓 Long 1 minute
	Sending
	Break apart messages larger than 60 KB
G	
	OK Cancel Apply



- 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:



🗖 GmailLog.pcap - Wireshark		
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u>	<u>A</u> nalyze <u>S</u> tati	istics <u>H</u> elp
	X 2 4	≞   °, ⇔ ⇔ 주 Ł   ≡ ≡   •, °, °, °'   ₩ M →
Eilter:		▼ Expression Clear Apply
Destination	Protocol	Info
72.14.213.109	ТСР	isis-ambc > submission [SYN] Seq=0 Win=64380 Len=0 MSS=1
192.168.1.114	TCP	submission > isis-ambc [SYN, ACK] Seq=0 Ack=1 Win=5720 L
72.14.213.109	TCP	isis-ambc > submission [ACK] Seq=1 Ack=1 Win=65520 Len=C
192.168.1.114	SMTP	Response: 220 mx.google.com ESMTP p8sm20291065WTT.16
/2.14.213.109	SMTP	Command: EHLO BU080201
192.108.1.114	EMTR	Submission > isis-ambc [ACK] Seq=45 ACK=10 Win=5700 Len=
72 14 213 109	SMTP	Command, STAPTTIS
192 168 1 114	TCP	submission > isis_ambc [ACK] Seg=168 Ack=26 Win=5760 Ler
192, 168, 1, 114	SMTP	Response: 220.2.0.0 Ready to start TLS
72.14.213.109	SMTP	Command: \200L\001\003\001\0003\000\000\020\000\000\
192.168.1.114	SMTP	Response: \026\003\001\000J\002\000\000F\003\001M\032\27
192.168.1.114	TCP	[TCP segment of a reassembled PDU]
192.168.1.114	TCP	[TCP segment of a reassembled PDU]
72.14.213.109	TCP	isis-ambc > submission [ACK] Seq=104 Ack=1859 Win=65520
72.14.213.109	SMTP	Command: \026\003\001\000\206\020\000\000\202\000\200\27
192.168.1.114	SMTP	Response: cr10
72.14.213.109	TCP	[TCP segment of a reassembled PDU]
192.168.1.114	SMTP	Response: \027\003\001\000\232;\364mb\221\226\241{\270\2
/2.14.213.109	TCP	[TCP segment of a reassembled PDU]
192.108.1.114	TCP	[ICP segment of a reassembled PDU]
102 168 1 114	TCP	[TCP segment of a reassembled PDU]
72 14,213,109	SMTP	Command: \027\003\001\000"\204\202\226o@\245\364\000
1211112131203	Jan 1	
<u>&lt;</u>		
⊞ Frame 1 (66 bytes on	wire, 66	bytes captured)
<		
0000 00 1b 5b dc 3f 31	00 1c 2	3 49 1d 77 08 00 45 00[.?1 #I.WE.
0010 00 34 a2 1d 40 00	80 06 7	9 10 c0 a8 01 72 48 0e .4@ yrH.
0020 d5 6d 06 6b 02 4b	26 da 7	5 35 00 00 00 00 80 02 .m.k.к&. u5
0030 fb /c f0 0/ 00 00	02 04 04	4 ec 01 03 03 00 01 01 .
0040 04 02		··· ·
File: "C:\Documents and Settings\b068	62\Deskt	Packets: 46 Displayed: 46 Marked: 0 Profile: Default .:

### 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.

Eilter:  ip.addr == 72.14.213.109												
No	Time	Source	Destination									
	1 0.000000	192.168.1.114	72.14.213.109									
	2 0.087745	72.14.213.109	192.168.1.114									
	3 0.087786	192.168.1.114	72.14.213.109									
	4 0.182289	72.14.213.109	192.168.1.114									
	5 0.182664	192.168.1.114	72.14.213.109									
	6 0.275048	72.14.213.109	192.168.1.114									
	7 0.379495	72.14.213.109	192.168.1.114									

### 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.

#### overview of the SMTP client application

Copy of GmailLog.pd	cap - Wiresl	hark				×
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> a	apture <u>A</u> naly	ze <u>S</u> tatistics <u>H</u> elp				
	🖻 🛃 🗙	1 🔁 占 I 🔍 🔶	\$	🥹 🛧 🕹   🗐 🖬	Ð. Q.	»
<u>F</u> ilter:				▼ Expression C	lear <u>A</u> pply	,
ation	Protocol	Info				
4.213.109	TCP	isis-ambc > sub	omiss	ion [SYN] Sea=0 Win:	=64380	1
168.1.114	TCP	submission > is	is-a	ambc [SYN, ACK] Seq=(	0 Ack=1	
4.213.109	TCP	isis-ambc > sub	miss	ion [ACK] Seq=1 Ack	=1 Win=	
168.1.114	SMTP	Response: 220 m	ix.go	ogle.com ESMTP p8sm	2029106	
4.213.109	SMTP	Command: EHLO B	0686	5201		
168.1.114	тср	<pre>submission &gt; is</pre>	- N	(ark Dacket (teeple)	=16 Wi	
168.1.114	SMTP	Response: 250-r	~	lark Packet (toggle)	/ice,	
4.213.109	SMTP	Command: START	Θs	et Time Reference (toggle)		
168.1.114	TCP	submission > 15			(=26 W	
168.1.114	SMTP	Response: 220 2	A	ppiy as Hiter		. —
4.213.109	SMTP	Command: \200L	P	repare a Filter		:
168 1 114	JMTP	TCD sogmont of	C	Conversation Filter	10031	
168 1 114	TCP	TCP segment of	C	Colorize Conversation		
4 213 109	TCP	isis_ambr > sub	S	CTP I	-1859	
4,213,109	SMTP	Command: \026\(	F	ollow TCP Stream	$10^{202}$	•
168.1.114	SMTP	Response: cr10				
4.213.109	TCP	TCP segment of	_	ollow ODF Stream		
168.1.114	SMTP	Response: \027		ollow SSL Stream	21\226	•
4.213.109	тср	[TCP segment of	C	Copy		
168.1.114	TCP	[TCP segment of	F	woort Selected Packet Bytes		
4.213.109	тср	<b>ETCP</b> segment of		Aport Deletted Forest Dytestin		~
<			SI D	ecode As	>	ļ
File: "C:\Documents and Sett	tings\b06862\D	eskt Packets: P	占 P	rint		

Figure 6. Decoding TCP communication as SSL in Wireshark

Wireshark: Deco	ode As	
	Link Network Transport	
<ul> <li>Decode</li> </ul>		SMUX
		SNMP
		Socks
		SoulSeek
🔘 Do not decode	ICP source (1643) port(s) as	SRVLOC
		551
		STANAG 5066
Show Current		STUN
Clear		
Help		pply <u>C</u> lose

### 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.



#### **Overview of the SMTP client application**

						-
No	Time	Source	Destination	Protocol	Info	^
	10 0.4/2183	/2.14.213.109	192.168.1.114	SSL	соптіпиатіон рат	
	11 0.504070	192.168.1.114	72.14.213.109	SSLV2	Client Hello	-
	12 0.596600	72.14.213.109	192.168.1.114	TLSV1	Server Hello,	
	13 0.598264	72.14.213.109	192.168.1.114	TCP	[TCP segment of	
	14 0.598276	72.14.213.109	192.168.1.114	TLSV1	Certificate	
	15 0.598296	192.168.1.114	72.14.213.109	TCP	isis-ambc > subm	~
<					>	
		cross stococos, or c	Torer Submission (Sory)			~
⊞ [R	eassembled TCP	Segments (1573 by	tes): #12(1181), #13(158)	), #14(234)]		-
🖃 Se	cure Socket La	yer				
	TLSV1 Record L	ayer: Handshake Pro	otocol: Certificate			
	Content Type	: Handshake (22)				
	Version: TLS	1.0 (0x0301)				
	Length: 1568					
	🗉 Handshake Pr	otocol: Certificato	e			
	Handshake	Type: Certificate	(11)			
	Length: 15	64	()			
	Contificat	og Longth, 1561				
	Certificat	es Length: 1561				
	Certificat	es (1561 bytes)				
	Certific	ate Length: 863				
	⊞ <mark>Certific</mark>	ate (id-at-commonNa	ame=smtp.gmail.com,id-at-	-organizatio	nName=Google Inc	
	Certific	ate Length: 692				
	🗉 Certific	ate (id-at-commonN	ame=Google Internet Autho	ority,id-at-	organizationName	
🗄 Se	cur <mark>e socket La</mark>	yer				~
<					>	
0270		-0 -0 -0 -0 -0 -0		0		
03/0	04 30 82 02 05 67 71 20	DU 30 82 02 19 a0	03 02 01 02 02 03 .0	.0	•	^
0390	05 00 30 4e	31 0h 30 09 06 03	55 04 06 13 02 55 0N	и о п	ii ii	
10550	5 71 10 70		12 07 45 71 75 60 61 0		4	⊻
Frame	(297 bytes) Reassem	bled TCP (1573 bytes)				

### 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.



### overview of the SMTP client application

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<sup>®</sup>, as shown in the following figure.

Options							×			
General	Tabs	页 Content		Brivacy	Security					
General Labs Content Applications Privacy Security Advance										
General Ne	etwork Up	date   Encry	ption							
Protoco	ls									
Use Use	: SSL <u>3</u> .0		<ul> <li>Image: A start of the start of</li></ul>	Use TLS <u>1</u> .	.0					
Certifica	ates									
When a	server req	uests my pe omatically	ersonal certificat	e: erv time						
U Sej	ett one aut	Officiality	Maxine eve	ery une						
View C	Certificate <u>s</u>	Revoca	tion Lists	alidation	Security	Devices				
							_			
				ж	Cancel	<u>H</u> elp				

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



Your Certificates       People       Servers       Authorities         Vou have certificates on file that identify these certificate authorities:       Ertificate Name       Security Device       Ertificate Name         Entrust.net Certification Authority       Builtin Object Token       Entrust.net Secure Server Certification A       Builtin Object Token         Entrust.net Clent Certification Authority       Builtin Object Token       Entrust.net Clent Certification A       Builtin Object Token         Entrust.net Clent Certificate Authority       Builtin Object Token       SecureTrust CA       Software Security Device         Trusted Secure Certificate Authority       Software Security Device       Trusted Secure Certificate Authority       Software Security Device         Beguifax       Secure Chificate Authority       Software Security Device       Google Internet Authority       Software Security Device         Google Internet Authority       Software Security Device       Google Internet Authority       Software Security Device         Builtin Secure       Equifax Secure Business CA 2       Builtin Object Token       Builtin Object Token         Builtin Secure Inc.       MDS Collisions Inc. (http://www.phreedo       Builtin Object Token       Builtin Object Token         Builtin Secure Global Business CA-1       Builtin Object Token       Builtin Object Token       Builtin Object Token	C	Certificate Manager		
You have certificates on file that identify these certificate authorities:         Vou have certificates on file that identify these certificate authorities:         Certificate Name       Security Device         Entrust.net Certification Authority       Builtin Object Token         Entrust.net Secure Server Certification A       Builtin Object Token         Entrust.net Client Certification Authority       Builtin Object Token         Entrust.net Client Certification Authority       Builtin Object Token         Entrust.net Client Certificate Authority       Software Security Device         SecureTrust CA       Software Security Device         Trusted Secure Certification Authority       Software Security Device         Google Internet Authority       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Ob		Your Contiferation (Reads) Converse Authorities Oth		
You have certificates on file that identify these certificate authorities:         Certificate Name       Security Device       R         Entrust.net Certification Authority (2048)       Builtin Object Token       R         Entrust.net Client Certification Authority       Builtin Object Token       R         Entrust.net Secure Server Certification A       Builtin Object Token       R         Entrust.net Client Certification Authority       Builtin Object Token       R         Entrust.net Client Certification Authority       Builtin Object Token       R         Entrust.net Client Certificate Authority       Software Security Device       R         Trusted Secure Cat       Builtin Object Token       R         GeoTrust Primary Certification Authority       Software Security Device       Google Internet Authority       Software Security Device         Google Internet Authority       Software Security Device       Google Internet Authority       Software Security Device         Equifax Secure       Builtin Object Token       Builtin Object Token       Builtin Object Token         Equifax Secure Business CA 1       Builtin Object Token       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token       Builtin Object Token <th></th> <td>Tour Certificates People Servers Additionales Oth</td> <td>ers</td> <td></td>		Tour Certificates People Servers Additionales Oth	ers	
Certificate Name       Security Device       C         Entrust.net Certification Authority (2048)       Builtin Object Token         Entrust.net Client Certification Authority       Builtin Object Token         SecureTrust CA       Software Security Device         Trusted Secure Certificate Authority       Software Security Device         GeoTrust Primary Certification Authority       Software Security Device         Google Internet Authority       Builtin Object Token         Equifax Secure eBusiness CA 2       Builtin Object Token         Equifax Secure Inc.       Builtin Object Token         Equifax Secure Blobal eBusiness CA-1 <t< td=""><th></th><td>You have certificates on file that identify these cer</td><td>tificate authorities:</td><td></td></t<>		You have certificates on file that identify these cer	tificate authorities:	
Entrust.net Certification Authority (2048)       Builtin Object Token         Entrust.net Secure Server Certification A       Builtin Object Token         Entrust.net Clent Certification Authority       Builtin Object Token         Entrust.net Cleint Certification Authority       Builtin Object Token         Entrust.net Cleint Certification Authority       Builtin Object Token         Entrust.net Cleint Certification Authority       Builtin Object Token         SecureTrust CA       Software Security Device         Trusted Secure Catificate Authority       Software Security Device         GeoTrust Primary Certification Authority       Software Security Device         Google Internet Authority       Software Security Device         Builtin Object Token       Equifax Secure         Equifax Secure Elsuiness CA 2       Builtin Object Token         Equifax Secure Inc.       MDS Collisions Inc. (http://www.phreedo       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token       Equifax Secure Business CA-1       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token       Equifax Secure Business CA-1<		Certificate Name	Security Device	Ę
Entrust.net Secure Server Certification A       Builtin Object Token         Entrust.net Client Certification A       Builtin Object Token         Entrust.net Client Certification A       Builtin Object Token         Entrust.net Client Certification Authority       Builtin Object Token         SecureTrust CA       Software Security Device         Trusted Secure Certificate Authority       Software Security Device         © Equifax       Eduitin Object Token         GeoTrust Primary Certification Authority       Software Security Device         Google Internet Authority       Software Security Device         GeoTrust Primary Certification Authority       Builtin Object Token         Equifax Secure Business CA 2       Builtin Object Token         Equifax Secure Inc.       Builtin Object Token         Equifax Secure Global eBusiness CA-1       Builtin Object Token         Equifax Secure Global CA       Builtin Object Token         GeoTrust Inc.       GeoTrust Extended Validation SSL CA		Entrust.net Certification Authority (2048)	Builtin Object Token	<u>~</u>
Entrust.net Client Certification Authority       Builtin Object Token         Entrust.net Client Certification AL       Builtin Object Token         Entrust.net Client Certification Authority       Builtin Object Token         SecureTrust CA       Software Security Device         Trusted Secure Certificate Authority       Software Security Device         Equifax       Equifax Secure CA         GeoTrust Primary Certification Authority       Software Security Device         Google Internet Authority       Software Security Device         Guifax Secure       Builtin Object Token         Equifax Secure Business CA 2       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token         GeoTrust Inc.       GeoTrust Extended Validation SSL CA       Software Security Device         GeoTrust Soloal CA       Builtin Object Token       Impor		Entrust.net Secure Server Certification A	Builtin Object Token	
Entrust.net Secure Server Certification A       Builtin Object Token         Entrust.net Clent Certification Authority       Builtin Object Token         SecureTrust CA       Software Security Device         Trusted Secure Certificate Authority       Software Security Device         Equifax       Equifax Secure CA       Builtin Object Token         GeoTrust Primary Certification Authority       Software Security Device       Google Internet Authority       Software Security Device         Google Internet Authority       Software Security Device       Google Internet Authority       Software Security Device         Google Internet Authority       Software Security Device       Google Internet Authority       Software Security Device         Bequifax Secure       Equifax Secure eBusiness CA 2       Builtin Object Token       Builtin Secure Inc.         MDS Collisions Inc. (http://www.phreedo       Builtin Object Token       Equifax Secure eBusiness CA-1       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token       Equifax Secure Eduiness CA-1       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token       Equifax Secure Eduiness CA-1       Builtin Object Token         Equifax Secure Cobal CA       Builtin Object Token       GeoTrust Inc.       GeoTrust Extended Validation SSL CA       Software Security Device      <		Entrust.net Client Certification Authority	Builtin Object Token	
Entrust.net Client Certification Authority       Builtin Object Token         SecureTrust CA       Software Security Device         Trusted Secure Certificate Authority       Software Security Device         Equifax       Equifax         Equifax       Software Security Device         GeoTrust Primary Certification Authority       Software Security Device         Google Internet Authority       Software Security Device         Equifax Secure       Builtin Object Token         Equifax Secure Inc.       MDS Collisions Inc. (http://www.phreedo         MDS Collisions Inc. (http://www.phreedo       Builtin Object Token         Equifax Secure Global eBusiness CA-1       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Object Token         Equifax Secure Inc.       GeoTrust Inc.         GeoTrust Inc.       GeoTrust Clobal CA         GeoTrust Schoal CA       Builtin Object Token         GeoTrust Global CA       Builtin Object Token         GeoTrust Global CA 2       Builtin Object Token <tr< td=""><th></th><td>Entrust.net Secure Server Certification A</td><td>Builtin Object Token</td><td></td></tr<>		Entrust.net Secure Server Certification A	Builtin Object Token	
SecureTrust CA       Software Security Device         Trusted Secure Certificate Authority       Software Security Device         Equifax       Equifax Secure CA       Builtin Object Token         GeoTrust Primary Certification Authority       Software Security Device       Google Internet Authority       Software Security Device         Google Internet Authority       Software Security Device       Google Internet Authority       Software Security Device         Google Internet Authority       Software Security Device       Equifax Secure       Equifax Secure         Equifax Secure Business CA 2       Builtin Object Token       Equifax Secure Inc.         MD5 Collisions Inc. (http://www.phreedo       Builtin Object Token       Equifax Secure Global eBusiness CA-1         Equifax Secure Business CA-1       Builtin Object Token       Equifax Secure Business CA-1       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token       Equifax Secure Global eBusiness CA-1       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token       GeoTrust Inc.       GeoTrust Extended Validation SSL CA       Software Security Device         GeoTrust Global CA       Builtin Object Token       GeoTrust Global CA 2       Builtin Object Token         Wiew       Edit       Import       Export       Delete <th></th> <td>Entrust.net Client Certification Authority</td> <td>Builtin Object Token</td> <td></td>		Entrust.net Client Certification Authority	Builtin Object Token	
Trusted Secure Certificate Authority       Software Security Device         Equifax         Equifax Secure CA       Builtin Object Token         GeoTrust Primary Certification Authority       Software Security Device         Google Internet Authority       Software Security Device         Google Internet Authority       Software Security Device         Google Internet Authority       Software Security Device         Equifax Secure       Equifax Secure eBusiness CA 2         Equifax Secure Inc.       MD5 Collisions Inc. (http://www.phreedo         MD5 Collisions Inc. (http://www.phreedo       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Object Token         GeoTrust Inc.       GeoTrust Inc.         GeoTrust Global CA       Builtin Object Token         GeoTrust Global CA 2       Builtin Object Token         Wiew       Edit       Import         Wew       Edit       Import		SecureTrust CA	Software Security Device	
Equifax         GeoTrust Primary Certification Authority       Software Security Device         Google Internet Authority       Software Security Device         Equifax Secure       Equifax Secure eBusiness CA 2         Builtin Object Token       Equifax Secure Inc.         MD5 Collisions Inc. (http://www.phreedo       Builtin Object Token         Equifax Secure Global eBusiness CA-1       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Object Token         GeoTrust Inc.       GeoTrust Inc.         GeoTrust Extended Validation SSL CA       Software Security Device         GeoTrust Global CA       Builtin Object Token         GeoTrust Global CA 2       Builtin Object Token         Wiew       Edit       Import         Export       Delete		Trusted Secure Certificate Authority	Software Security Device	
Equifax Secure CA       Builtin Object Token         GeoTrust Primary Certification Authority       Software Security Device         Google Internet Authority       Software Security Device         Google Internet Authority       Software Security Device         Google Internet Authority       Software Security Device         Equifax Secure       Equifax Secure eBusiness CA 2         Equifax Secure Inc.       Builtin Object Token         Equifax Secure Global eBusiness CA-1       Builtin Object Token         Equifax Secure Global eBusiness CA-1       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token         Equifax Secure Global eBusiness CA-1       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Object Token         GeoTrust Inc.       GeoTrust Extended Validation SSL CA       Software Security Device         GeoTrust Global CA       Builtin Object Token       Import         Wiew       Edit       Import       Export       Delete		🖃 Equifax		
GeoTrust Primary Certification Authority       Software Security Device         Google Internet Authority       Software Security Device         Google Internet Authority       Software Security Device         Equifax Secure       Equifax Secure eBusiness CA 2         Builtin Object Token       Equifax Secure Inc.         MD5 Collisions Inc. (http://www.phreedo       Builtin Object Token         Equifax Secure Global eBusiness CA-1       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Object Token         GeoTrust Inc.       GeoTrust Inc.         GeoTrust Extended Validation SSL CA       Software Security Device         GeoTrust Global CA       Builtin Object Token         GeoTrust Global CA 2       Builtin Object Token         View       Edit       Import       Export         View       Edit       Import       Export		Equifax Secure CA	Builtin Object Token	
Google Internet Authority       Software Security Device         Google Internet Authority       Software Security Device         Equifax Secure       Equifax Secure eBusiness CA 2       Builtin Object Token         Equifax Secure Inc.       MD5 Collisions Inc. (http://www.phreedo       Builtin Object Token         Equifax Secure Global eBusiness CA-1       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Object Token         GeoTrust Inc.       GeoTrust Extended Validation SSL CA       Software Security Device         GeoTrust Extended Validation SSL CA       Builtin Object Token       Import         GeoTrust Global CA       Builtin Object Token       Import         View       Edit       Import       Export         View       Edit       Import       Export       Delete		GeoTrust Primary Certification Authority	Software Security Device	
Google Internet Authority       Software Security Device         Equifax Secure       Equifax Secure eBusiness CA 2       Builtin Object Token         Equifax Secure Inc.       MD5 Collisions Inc. (http://www.phreedo       Builtin Object Token         Equifax Secure Global eBusiness CA-1       Builtin Object Token         Equifax Secure Business CA-1       Builtin Object Token         GeoTrust Inc.       GeoTrust Extended Validation SSL CA       Software Security Device         GeoTrust Global CA       Builtin Object Token       GeoTrust Global CA         GeoTrust Global CA 2       Builtin Object Token       V         View       Edit       Import       Export       Delete		Google Internet Authority	Software Security Device	
<ul> <li>Equifax Secure</li> <li>Equifax Secure eBusiness CA 2</li> <li>Builtin Object Token</li> <li>Equifax Secure Inc.</li> <li>MD5 Collisions Inc. (http://www.phreedo Builtin Object Token</li> <li>Equifax Secure Global eBusiness CA-1</li> <li>Builtin Object Token</li> <li>Equifax Secure eBusiness CA-1</li> <li>Builtin Object Token</li> <li>GeoTrust Inc.</li> <li>GeoTrust Extended Validation SSL CA</li> <li>Software Security Device</li> <li>GeoTrust Global CA</li> <li>Builtin Object Token</li> <li>GeoTrust Global CA 2</li> <li>Builtin Object Token</li> <li>Vjew</li> <li>Edit</li> <li>Import</li> <li>Export</li> <li>Delete</li> </ul>		Google Internet Authority	Software Security Device	
Equifax Secure eBusiness CA 2       Builtin Object Token         Equifax Secure Inc.       MD5 Collisions Inc. (http://www.phreedo       Builtin Object Token         Equifax Secure Global eBusiness CA-1       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Object Token         GeoTrust Inc.       GeoTrust Extended Validation SSL CA         GeoTrust Extended Validation SSL CA       Software Security Device         GeoTrust Global CA       Builtin Object Token         GeoTrust Global CA       Builtin Object Token         GeoTrust Global CA 2       Builtin Object Token         View       Edit       Import         View       Edit       Import       Export         OK       OK       OK		Equifax Secure		
Equifax Secure Inc. MD5 Collisions Inc. (http://www.phreedo Builtin Object Token Equifax Secure Global eBusiness CA-1 Builtin Object Token Equifax Secure eBusiness CA-1 Builtin Object Token © GeoTrust Inc. GeoTrust Extended Validation SSL CA Software Security Device GeoTrust Global CA Builtin Object Token GeoTrust Global CA Builtin Object Token GeoTrust Global CA Builtin Object Token Wiew Edit Import Export Delete		Equifax Secure eBusiness CA 2	Builtin Object Token	
MD5 Collisions Inc. (http://www.phreedo Builtin Object Token Equifax Secure Global eBusiness CA-1 Builtin Object Token Equifax Secure eBusiness CA-1 Builtin Object Token © GeoTrust Inc. GeoTrust Extended Validation SSL CA Software Security Device GeoTrust Global CA Builtin Object Token GeoTrust Primary Certification Authority Builtin Object Token GeoTrust Global CA 2 Builtin Object Token $\underbrace{View}$ Edit Import $\underbrace{Export}$ Delete		🖃 Equifax Secure Inc.		
Equifax Secure Global eBusiness CA-1       Builtin Object Token         Equifax Secure eBusiness CA-1       Builtin Object Token         Image: GeoTrust Inc.       GeoTrust Extended Validation SSL CA         GeoTrust Extended Validation SSL CA       Software Security Device         GeoTrust Global CA       Builtin Object Token         GeoTrust Primary Certification Authority       Builtin Object Token         GeoTrust Global CA 2       Builtin Object Token         Import       Export         View       Edit         Import       Export         OK		MD5 Collisions Inc. (http://www.phreedo	Builtin Object Token	
Equifax Secure eBusiness CA-1       Builtin Object Token         GeoTrust Inc.       GeoTrust Extended Validation SSL CA       Software Security Device         GeoTrust Global CA       Builtin Object Token         GeoTrust Primary Certification Authority       Builtin Object Token         GeoTrust Global CA 2       Builtin Object Token         View       Edit       Import         View       Edit       Import         OK       OK		Equifax Secure Global eBusiness CA-1	Builtin Object Token	
<ul> <li>GeoTrust Inc.</li> <li>GeoTrust Extended Validation SSL CA Software Security Device</li> <li>GeoTrust Global CA Builtin Object Token</li> <li>GeoTrust Primary Certification Authority Builtin Object Token</li> <li>GeoTrust Global CA 2 Builtin Object Token</li> <li>✓</li> <li>✓</li> <li>✓</li> </ul>		Equifax Secure eBusiness CA-1	Builtin Object Token	
GeoTrust Extended Validation SSL CA       Software Security Device         GeoTrust Global CA       Builtin Object Token         GeoTrust Primary Certification Authority       Builtin Object Token         GeoTrust Global CA 2       Builtin Object Token         View       Edit         Import       Export         View       Edit		🖃 GeoTrust Inc.		
GeoTrust Global CA       Builtin Object Token         GeoTrust Primary Certification Authority       Builtin Object Token         GeoTrust Global CA 2       Builtin Object Token         View       Edit         Import       Export         OK		GeoTrust Extended Validation SSL CA	Software Security Device	
GeoTrust Primary Certification Authority Builtin Object Token GeoTrust Global CA 2 Builtin Object Token View Edit Import Export Delete OK		GeoTrust Global CA	Builtin Object Token	
GeoTrust Global CA 2     Builtin Object Token       View     Edit       Import     Export       Delete		GeoTrust Primary Certification Authority	Builtin Object Token	
View Edit Import Export Delete OK		GeoTrust Global CA 2	Builtin Object Token	✓
OK		View Edit Import	Export	
ОК				
				ОК

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



Save Certificate To File ୍ 🕝 🤌 📂 🖽 -Save in: MSS cau )demo docs /w Recent Documents hmss NanoSSL NanoSSH binaries NanoSSL NanoSSH binaries All Desktor My Documents My Computer BuiltinObjectToken-EquifaxSecureCA File name: Save Save as type: X.509 Certificate (DER) Cancel My Network

### 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.

ł																	
	D Untitled - Notepad																
	File Edit Format View Help																
unsigned char b1[] = {																	
		0x30,	0x82,	0x03,	0x20,	0x30,	0x82,	0x02,	0x89,	0xa0,	0x03,	0x02,	0x01,	0x02,	0x02,	0x04,	0x35,
		0x0e,	0x14, 0x00.	0x30.	0x30, 0x4e.	0x00,	0x06,	0x09,	0x2a, 0x09.	0x80, 0x06.	0x48, 0x03.	0x80,	0x17, 0x04	0x0a,	0x01, 0x13.	0x01, 0x02, 0x02	0x05, 0x55.
		0x53,	0x31,	0x10,	0x30,	0x0e,	0x06,	0x03,	0x55,	0x04,	0x0a,	0x13,	0x07,	0x45,	0x71,	0x75,	0x69,
		0x66,	0x61,	0x78,	0x31,	0x2d,	0x30,	0x2b,	0x06,	0x03,	0x55,	0x04,	0x0b,	0x13,	0x24,	0x45,	0x71,
		0x75, 0x74.	0x69,	0x66,	0x61, 0x69.	0x78,	0x20,	0x53, 0x74.	0x05, 0x65.	0x03, 0x20.	0x/5, 0x41.	0x/2, 0x75.	0x05, 0x74.	0x20,	0x43, 0x6f.	0x03, 0x72, 0x72	0x/2, 0x69.
		0x74,	0x79,	0x30,	0x1e,	0x17,	0x0d,	0x39,	0x38,	0x30,	0x38,	0x32,	0x32,	0x31,	0x36,	0x34,	0x31,
		0x35,	0x31,	0x5a,	0x17,	0x0d,	0x31,	0x38,	0x30,	0x38,	0x32,	0x32,	0x31,	0x36,	0x34,	0x31,	0x35,
		0x31, 0x53.	0x5a, 0x31.	0x30, 0x10.	0x4e,	0x31,	0x06	0x30,	0x09,	0x06, 0x04	0x03, $0x0a$ .	0x55, 0x13.	0x04,	0x06,	0x13, 0x71.	0x02,	0x55, 0x69.
		0x66,	0x61,	0x78,	0x31,	0x2d,	0x30,	0x2b,	0x06,	0x03,	0x55,	0x04,	0x0b,	0x13,	0x24,	0x45,	0x71,
		0x75,	0x69,	0x66,	0x61,	0x78,	0x20,	0x53,	0x65,	0x63,	0x75,	0x72,	0x65,	0x20,	0x43,	0x65,	0x72,
	<																

## 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 Information in this document is provided solely to enable system and software implementers to use Freescale Semiconductors products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits or integrated circuits based on the information in this document.

Freescale Semiconductor reserves the right to make changes without further notice to any products herein. Freescale Semiconductor makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does Freescale Semiconductor assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any liability, including without limitation consequential or incidental damages. "Typical" parameters that may be provided in Freescale Semiconductor data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including "Typicals", must be validated for each customer application by customer's technical experts. Freescale Semiconductor does not convey any license under its patent rights nor the rights of others. Freescale Semiconductor products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which failure of the Freescale Semiconductor product could create a situation where personal injury or death may occur. Should Buyer purchase or use Freescale Semiconductor products for any such unintended or unauthorized application, Buyer shall indemnify Freescale Semiconductor and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claims alleges that Freescale Semiconductor was negligent regarding the design or manufacture of the part.

RoHS-compliant and/or Pb-free versions of Freescale products have the functionality and electrical characteristics as their non-RoHS-complaint and/or non-Pb-free counterparts. For further information, see http://www.freescale.com or contact your Freescale sales representative.

For information on Freescale's Environmental Products program, go to http://www.freescale.com/epp.

 $\label{eq:FreescaleTM} Freescale TM and the Freescale logo are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners.$ 

© 2011 Freescale Semiconductor, Inc.



Document Number: AN4363 Rev. 0, 10/2011