# STS Association

## STS600-9-2

**Edition 1.0**
**April 2023**

## Key management - Email Gateway services manual

CONTENTS

## Contents



Revision History:

| Revision | Clause | Date | Change details from previous Edition |
|---|---|---|---|
| 1.0 | | Apr 2023 | Initial Revision - based on PR-D2-1089 Rev1.0.1 2020 document published by Prism Payment Technologies |

# INTRODUCTION

The Standard Transfer Specification (STS) is a secure message protocol that allows information to be carried between point of sale (POS) equipment and payment meters and it caters for several message types such as credit, configuration control, display and test instructions. It further specifies devices and codes of practice that allows for the secure management (generation, storage, retrieval and transportation) of cryptographic keys used within the system.

In order to simplify the interface between users of the STS and the key management centre (KMC), additions to the key management system (KMS) were commissioned to allow certain services to be requested via an email gateway.

This companion specification is intended for use by users of the KMC in order to remotely obtain certain services normally requested via requests to KMC operators.

## 1 Scope

This document is for users and integrators of the mail-based services provided by the STS KMS E-mail Gateway. It explains what services are available, how to access them using a regular mail client, and how to integrate with them to automate key management in STS vending or manufacturing software.

## 2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62051, *Electricity metering – Glossary of terms*

IEC 62055-41, *ELECTRICITY METERING – PAYMENT SYSTEMS – Part 41: Standard transfer specification (STS) – Application layer protocol for one-way token carrier systems*

STS 600-4-2, STANDARD TRANSFER SPECIFICATION – Companion Specification – Key Management System, Ed 1.3, January 2016

## 3 Terms, definitions and abbreviations

For the purposes of this standard, the terms and definitions given in IEC 62051, IEC 62055-41, STS600-4-2, and the following terms apply.

Where there is a difference between the definitions in this standard and those contained in other referenced IEC standards, then those defined in this standard shall take precedence.

| | |
|---|---|
| DNSBL | Domain Name System Blacklist |
| POS | Point of sale |
| KLF | Key Load File |
| KMC | Key Management Centre |
| KMS | Key management system |
| SMTP | Simple Mail Transfer Protocol |
| STS | Standard Transfer Specification |
| STS6 | Protocol Compliant with STS600-4-2and STS600-8-6 specifications |

## 4 Basic Principles

The e-mail address of the KMC gateway can be found in clause 6.

The Gateway only understands messages in “Plain Text” format (see clause 7).

- The service you are requesting is indicated in the Subject line of your e-mail. Refer to clause 5 for the Subject to use.
- The Gateway’s e-mail address must be in the To: field of your e-mail. The gateway will ignore e-mails not addressed to it, including CC’s and BCC’s.
- If the service requires you to attach a file, the attachment must be a “text/plain” file. The easiest way to do this is to ensure that the filename ends in “.txt”.
- The Gateway has multiple protections against spam and mail loops:
    - If you send too many messages in a short space of time your messages may be deferred, or you may be blocked for a period of time. You will be sent a notification if this happens;
    - The Gateway will ignore any auto-generated e-mail response, any mail that has a Subject prefix indicating that it is a reply or forward or auto-response, and any e-mail that appears to originate from a mailing list;
    - The Gateway will ignore most large messages, in particular those with attachments (other than those expected by the service you are requesting).
- In general, the Gateway will not respond to any e-mail that is not a well-formed service request addressed to the Gateway. Use the correct Subject and body for the service you are requesting.
- Every service request accepted by the gateway may result in one or more reply e-mails.
    - In most cases there is only one reply, but in some cases, you may be sent notices (for example if processing is deferred).
- Under normal circumstances you can expect a reply in 5 – 10 minutes (but this can be heavily affected by mail propagation delays).

*Remember to:*

- *Use “Plain Text” format;*
- *Put the Gateway e-mail address in the To: field;*
- *Put the service code in the Subject: field;*
- *Add content or attachments as required by the service;*
- *Do not spam or flood the Gateway, it will block you.*

# 5 Services

## 5.1 Available services

### 5.1.1 General

The following services are available on the email gateway:

| Service | Email Subject Line | Function |
|---|---|---|
| Help service | {KMS:Help} | Requests instructions for using the mail-based services |
| Get public key service | {KMS:GetPublicKey}" | Retrieve the Public Key of the KMS, which is required by Security Modules to generate a Vending Key Load Request |
| Get Keyload File (STS Ed2) service | {KMS:GetKlfStsEd2} | Obtain a Key Load File for a STS Edition2 security module |
| Send an update file to the KMC | {KMS:SmUpdateStsEd2} | reserved for the STSA only. |

### 5.1.2 Help service

#### 5.1.2.1 General

Requests instructions for using the mail-based services

The Help service comprises the following elements.

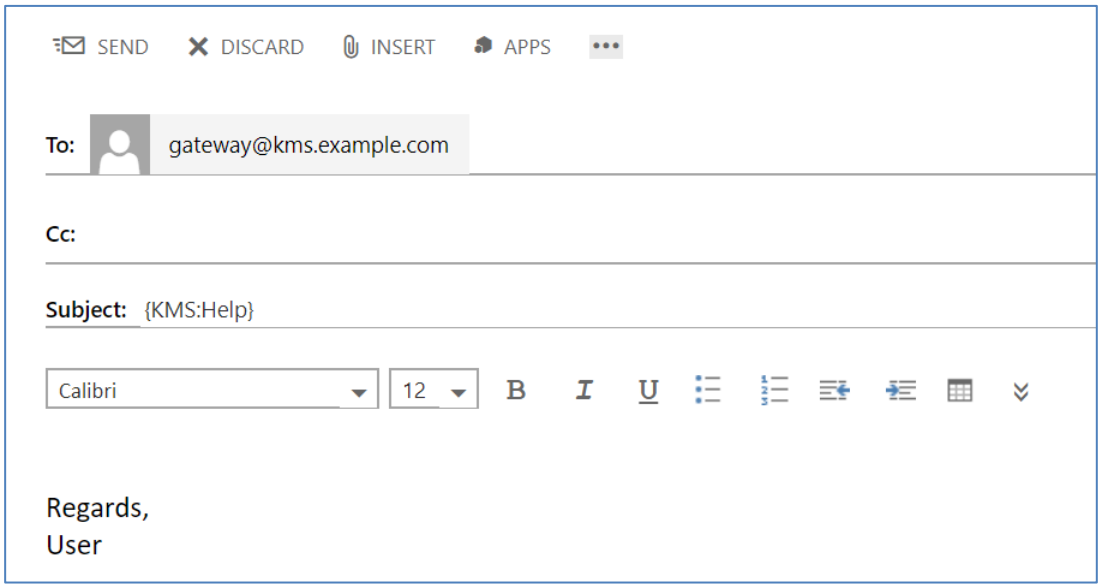
#### 5.1.2.2 Request

- Send a “text/plain” e-mail;
- The Subject must start with “{KMS:Help}”.

#### 5.1.2.3 Response

The response will contain human-readable instructions for basic use of the Gateway.

#### 5.1.2.4 Example request




### 5.1.3 Get Public Key service

#### 5.1.3.1 General

Retrieve the Public Key of the KMS, which is required by Security Modules to generate a Vending Key Load Request.

The Get Public Key service comprises the following elements.

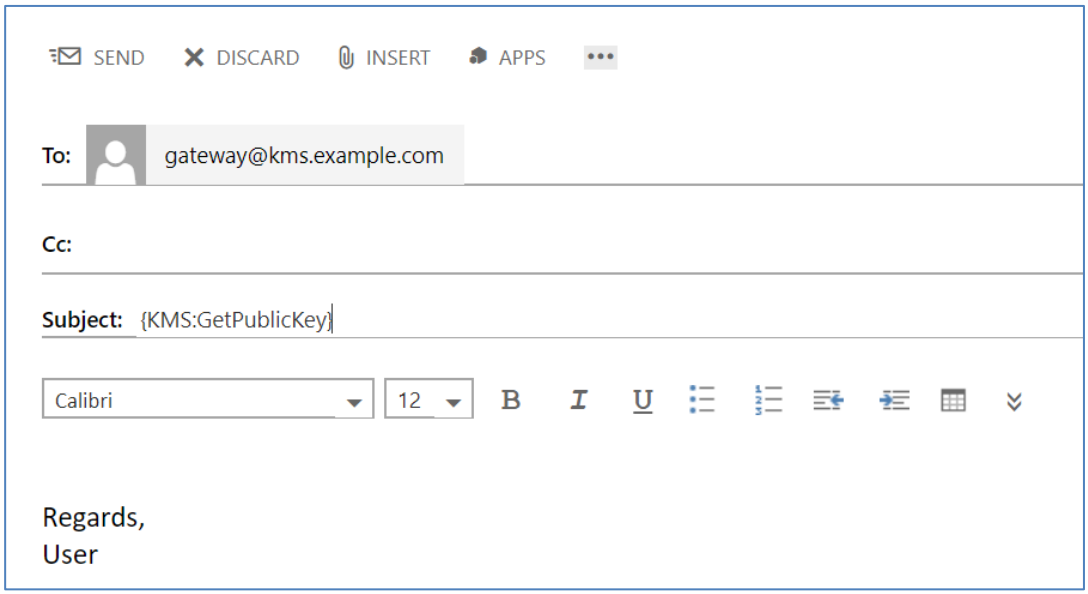
#### 5.1.3.2 Request

- Send a “text/plain” e-mail;
- The Subject must start with “{KMS:GetPublicKey}”.

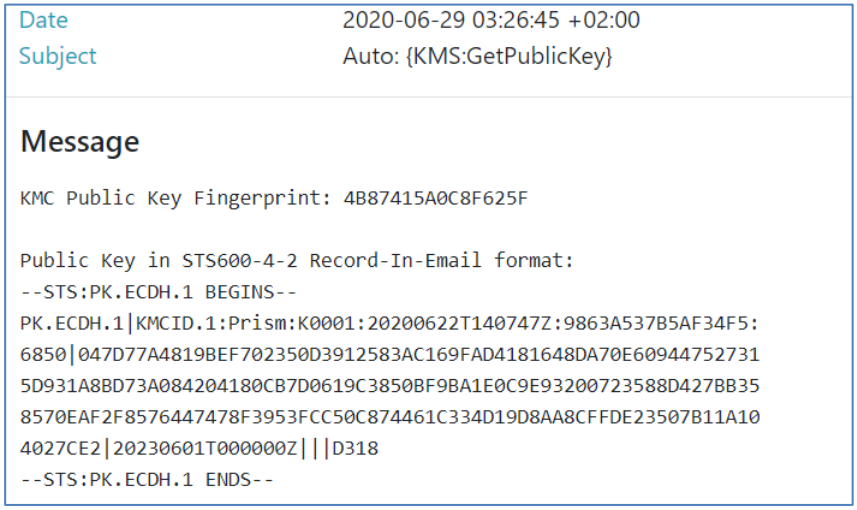
#### 5.1.3.3 Response

The response will contain the current EDCH Public Key of the KMS, in STS600-4-2 Record-in-Email format.

#### 5.1.3.4 Example request



#### 5.1.3.5 Example response




### 5.1.4 Get Key Load File (STS Edition2) service

#### 5.1.4.1 General

Obtain a Key Load File for an STS Edition 2 (STS6) Security Module (SM).

The Get Key Load File service comprises the following elements.

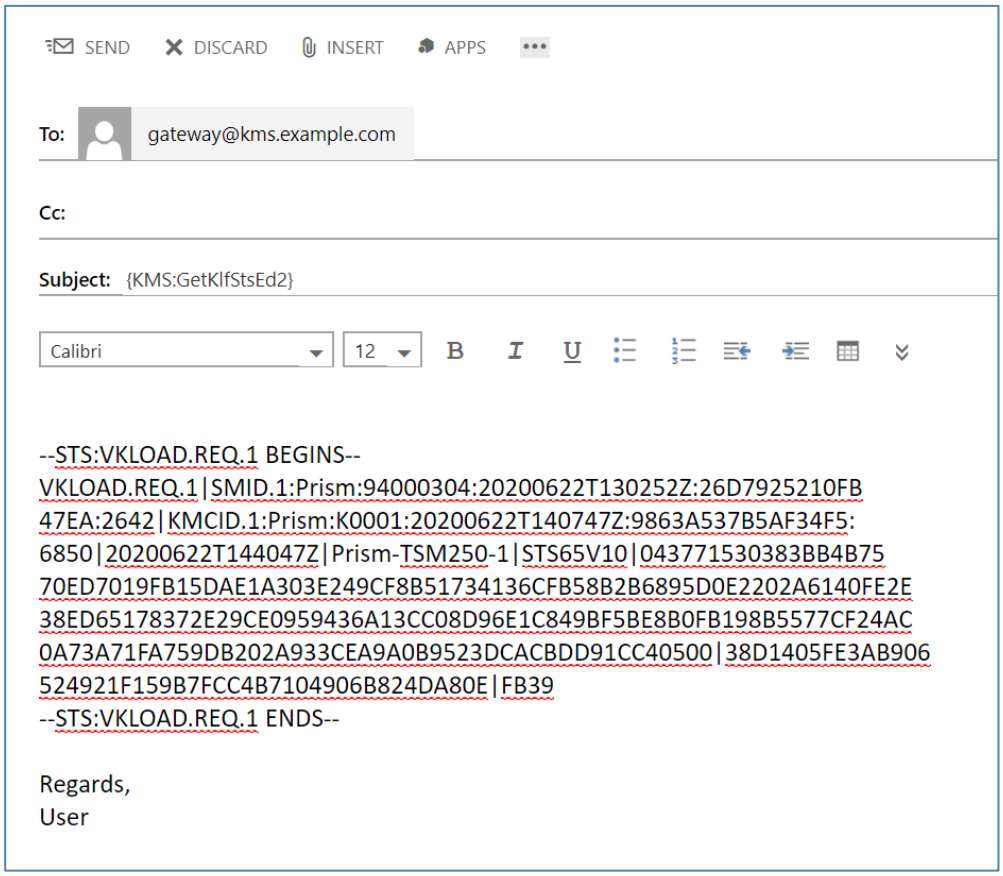
#### 5.1.4.2 Request

- Send a “text/plain” e-mail;
- The Subject must start with “{KMS:GetKlfStsEd2}”;
- The e-mail body must contain a fresh Vending Key Load Request (VKLOADREQ) in Record-in-email format.

#### 5.1.4.3 Response

If processing is successful the reply will have the Key Load File as a “text/plain” attachment; otherwise, the reply will explain what processing failed.

#### 5.1.4.4 Example request




## 6 Email addresses

The email address for the live KMS is shown below.

| |
|---|
| stsa_kmc_01@stskms.org.za |

## 7 Working with mail client software

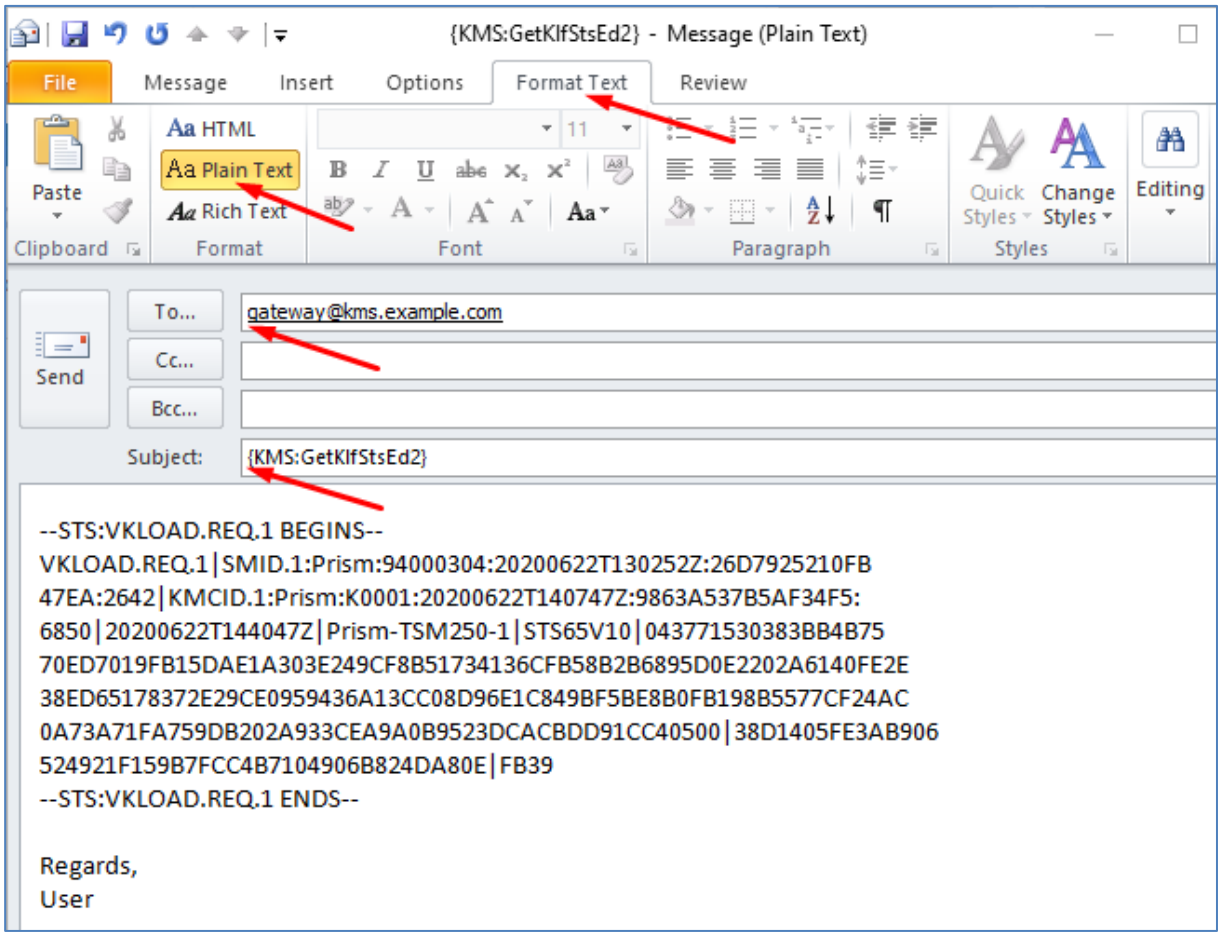
### 7.1 Example clients

#### 7.1.1 General

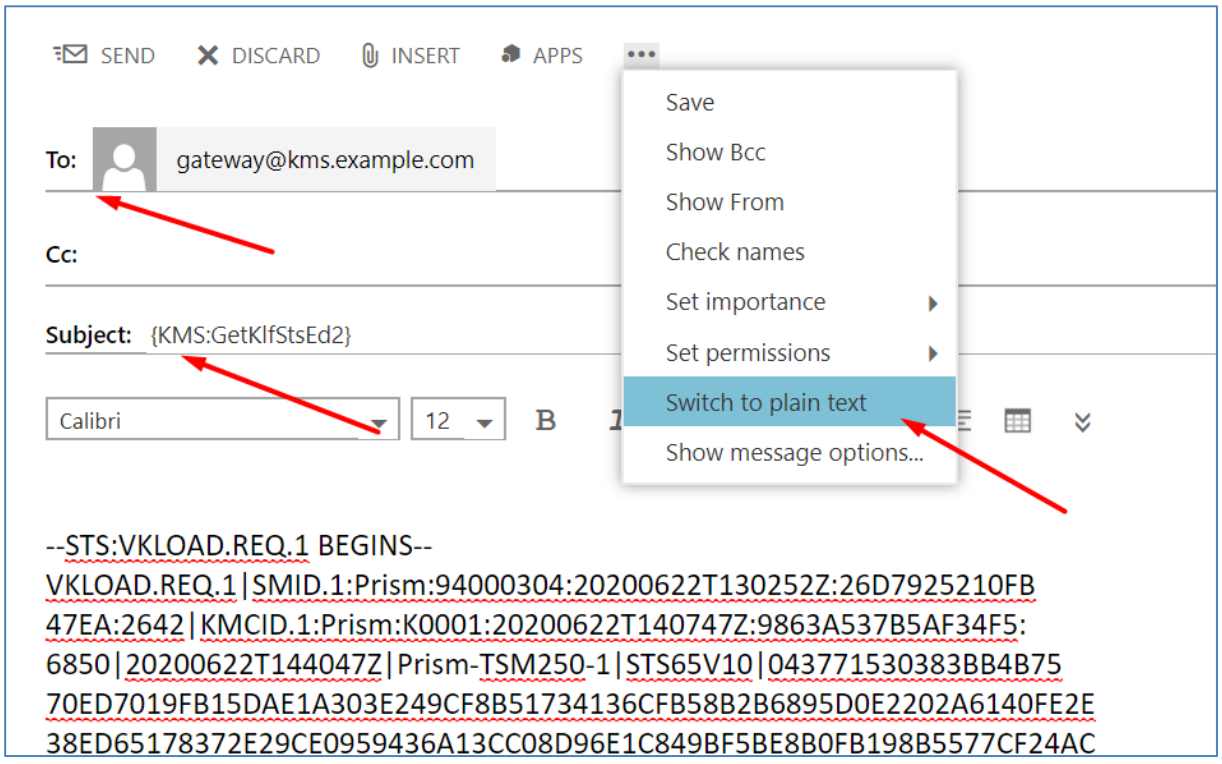
Several examples are shown below using standard email clients.

#### 7.1.2 Outlook

When converting the message to Plain text you may get the Compatibility Checker popup window appearing. Click continue to convert the message to Plain text.



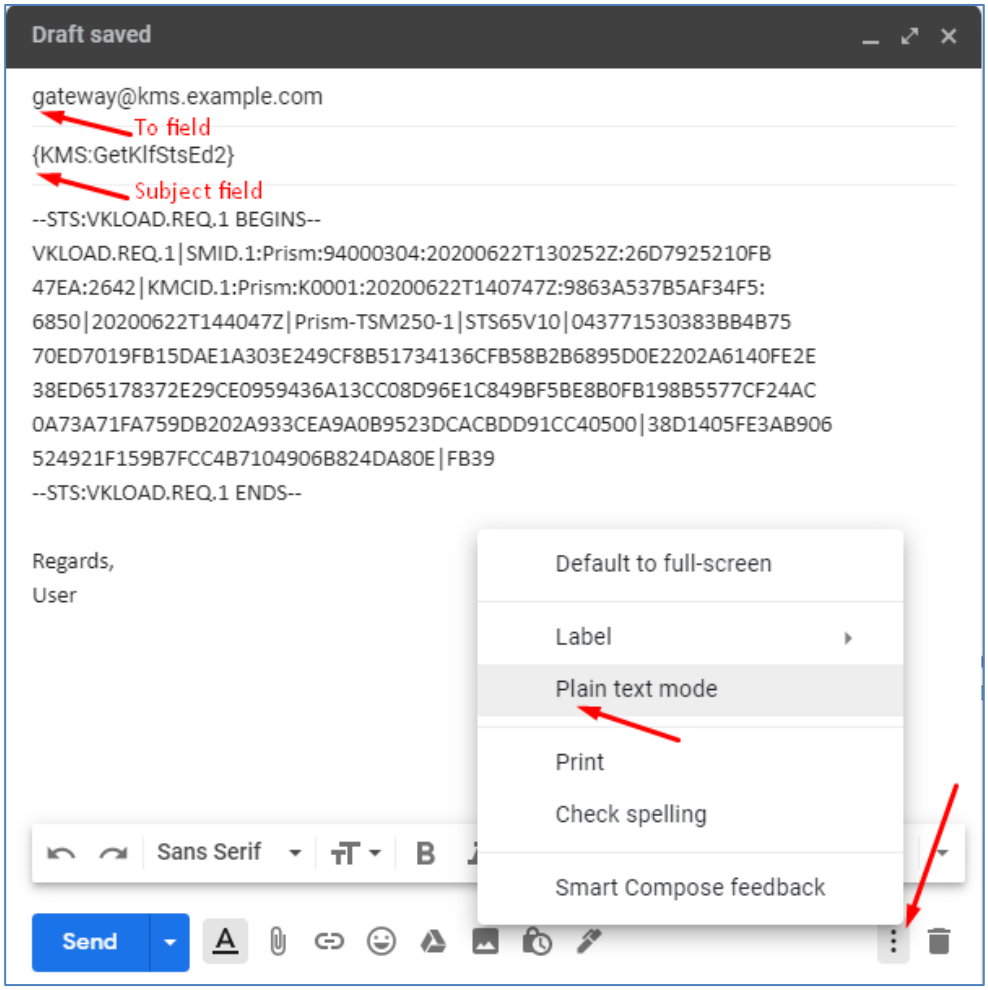

### 7.1.3 Outlook.com



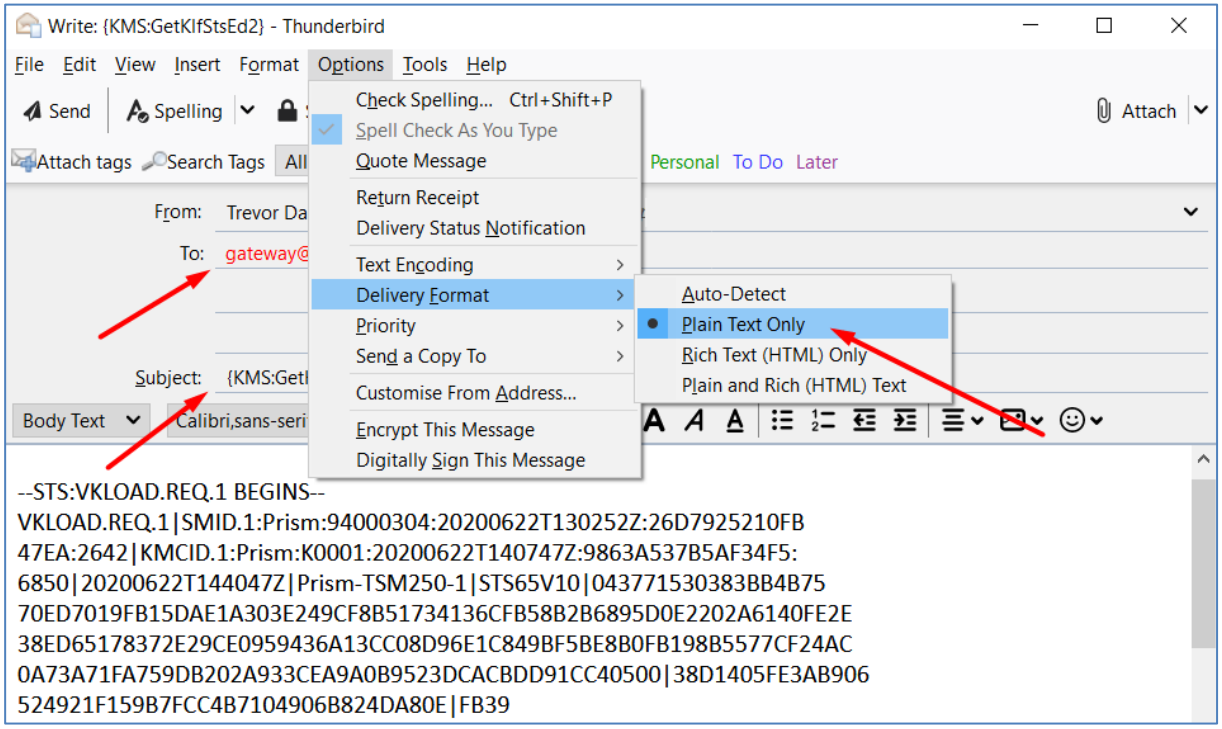
### 7.1.4 Gmail

Please note that with Gmail there is a feature called “turnoff/on Less secure App Access”, which is not turned on by default.

- This feature must be turned ON.
- Do not cc the email when sending requests to the KMS email gateway.



### 7.1.5 Thunderbird



# 8 Integrator's guide

## 8.1 General

This section is for software developers and system integrators who want to integrate with the STS-KMS E-mail Gateway.

Before reading this section, you should be familiar with the "Standard Transfer Specification – Companion Specification – Key Management System" standard [STS600-4-2], in particular:

- The "Vending Key Load Request and Response Process" in [STS600-4-2 Section 4];
- The various record types including PUBKEY, VKLOADREQ, and VKLOADREQ;
- The File-of-records format [STS600-4-2 Appendix D]; and
- The Record-in-email format [STS600-4-2 Appendix C].

## 8.2 Technical constraints on request messages

In addition to the basic principles, you should understand these technical constraints on the request messages sent to the Gateway:

- The Gateway generally follows the RFC3834 behaviour for a Service Responder, and uses the appropriate mail loop suppression mechanisms. If your message contains any headers that identify it as a mail responder, it will be ignored;
- Your message must contain a valid Return-Path. This is not under your control, but is set by your SMTP server. You should ensure that your mail service provider has a well-behaved SMTP server;
- The Gateway's mail service provided uses spam filters and DNSBL/RBL. You should ensure that your mail service provider has a properly configured and well-behaved SMTP server that is not on a block list;
- The Gateway requires that the Subject line starts with a service code, but has no constraints on what follows the service code;
- Attachments, if required, must have Content-Disposition: attachment, and Content-Type: text/plain;
- Follow exactly the request requirements described by the service.

## 8.3 Guarantees on replies

### 8.3.1 General

The integration shall provision the following guarantees:

- The Gateway will generally reply to all e-mails where the Subject line starts with "{KMS:*}", and will generally ignore all other e-mails;
- Replies are sent to the Reply-To list if present, otherwise the first From address if present, otherwise the Sender address;
- The reply will be a MIME message. It may have Content-Type "text/plain" or "multipart/mixed"; if the latter then one of the MIME parts will have Content-Type "text/plain". This is the "text body" of the reply;

- The Subject line of the reply will be the prefix “Auto: ” followed by the Subject line of the request. Since the trailing part of the Subject (after the service code) is ignored by the Gateway, this can be used to hold a sequence number of UID for request/response matching (if required by your software);

- The Gateway will set the InReplyTo header of the reply to match the MessageId of the request, but your SMTP server may not allow you to control the MessageId of your requests, so you should not rely on recognising the InReplyTo header;

- You cannot rely on other headers being propagated from request to reply, except for the Subject line as described above;

- The reply will include multiple mail loop suppression headers (including “Auto-submitted” and “Precedence”) some of which may cause aggressive spam filters to treat these replies as junk. You should organise to add the Gateway’s mail sending address to an allow list on any mail filters;

- The Gateway makes a best effort to include a “X-Gateway-Result” header in its replies. The format is described below. Recipients should not rely on the presence of this header, as it may not be present on notification e-mails (which are not results), or Deliver Report e-mails generated by the mail network.

### 8.3.2 X-Gateway-Result

The “X-Gateway-Result” header, if present, is a HTAB-separated list conforming to one of the following:

- The first element “Success”, followed by a human-readable summary. This result indicates that the request was successful, and the reply will have the structure/contents as described in this document. The summary or equivalent information will be contained in the message body. This is a final result; there will be no further e-mails relating to this request;

```
X-Gateway-Result: Success
      The operation completed successfully
```

- The first element “Error”, followed by an error code string, then a human-readable error description, then zero or more parameter fields (that are specific to the error code). The error description may include guidance on how to proceed. This is a final result; there will be no further e-mails relating to this request;

```
X-Gateway-Result: Error
      EVkloadExpired
      The VKLOADREQ is stale; generate a fresh VKLOADREQ and try
again
```

- The first element “Notice”, followed by a notice code string, then a human-readable notice message, then zero or more parameter fields (that are specific to the notice code). The notice message may include guidance on how to proceed. This is not a final result; further e-mails relating to this request should be expected;

```
X-Gateway-Result: Notice
      Deferred
      Operation failed but will be retried; you don’t need to do
anything
```

## 9 Bibliography

PR-D2-1089 Rev 1.0.1 2020: STS-KMS E-mail Gateway Mail-based Services Manual (Prism Payment Technologies)