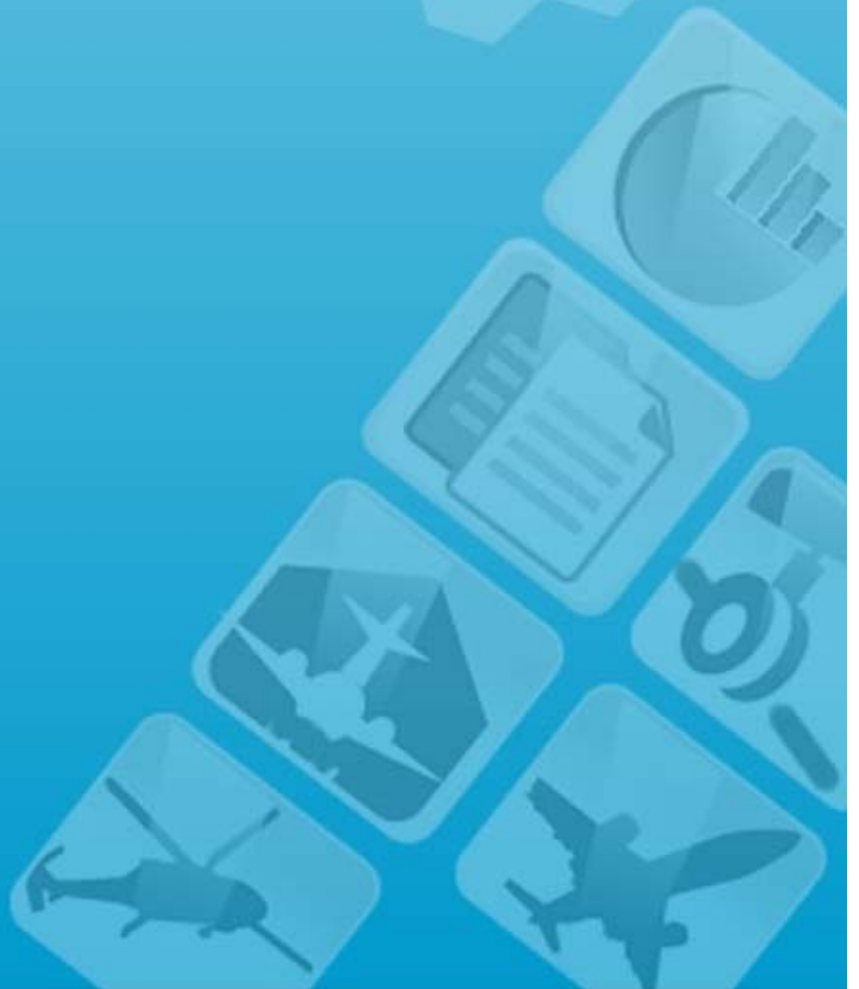




Utilities

User Guide

Version 5.3



DISCLAIMER

©2010 Ramco Systems Ltd. All rights reserved. All trademarks acknowledged.

This document is published by **Ramco Systems Ltd.** without any warranty. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose without the written permission of **Ramco Systems Limited.**

Improvements and changes to this text necessitated by typographical errors, inaccuracies of current information or improvements to software programs and/or equipment, may be made by Ramco Systems Limited, at any time and without notice. Such changes will, however, be incorporated into new editions of this document. Any hard copies of this document are to be regarded as temporary reference copies only.

The documentation has been provided for the entire Aviation solution, although only a part of the entire solution may be deployed at the customer site, in accordance with the license agreement between the customer and Ramco Systems Limited. Therefore, the documentation made available to the customer may refer to features that are not present in the solution purchased / deployed at the customer site.

About this manual

This manual briefly describes the basic processes and functions in Ramco Aviation Solution.

Who Should Read This Manual

This manual is intended for users who are managing the Aviation industry processes and are new to Ramco Aviation Solution.

This manual assumes that the user is familiar with the Aviation Industry nomenclatures and systems based software.

How To Use This Manual

Ramco Aviation Solution provides extensive Online Help that contains detailed instructions on how to use the application. Users are suggested to use this manual for specific references, along with the Online Help. This manual contains enough information to help the users perform the basic tasks and points toward the Online Help for more detailed information.

How This Manual is organized


The User Guide is divided into 2 chapters and an index. Given below is a brief run-through of what each chapter consists of.

Chapter 1 provides an overview of the entire **Utilities** business process chain. The processes are explained in the remaining chapters.

Chapter 2 focuses on the **Objects Attachments** process.

The **Index** offers a quick reference to selected words used in the manual.

Document Conventions

- ▶ The data entry has been explained taking into account the "Create" business activity. Specific references (if any) to any other business activity such as "Modify" and "View" are given as "Note" at the appropriate places.
- ▶ **Boldface** is used to denote commands and user interface labels.
Example: Enter **Company Code** and click the **Get Details** pushbutton.
- ▶ *Italics* used for references.
Example: *See Figure 1.1.*
- ▶ The  icon is used for Notes, to convey additional information.

Reference Documentation

This User Guide is part of the documentation set that comes with Ramco Aviation Solution.

The documentation is generally provided in two forms:

- ▶ The Documentation CD in Adobe® Systems' Portable Document Format (PDF).
- ▶ Context-sensitive Online Help information accessible from the application screens.

Whom To Contact For Queries

Please locate the nearest office for your geographical area from www.ramco.com for assistance.

Table of Contents

Chapter 1/ Introduction.....	1
-------------------------------------	----------

Chapter 2/ Object Attachments.....	3
---	----------

Setting parameters for uploading documents.....	4
---	---

Uploading documents	7
---------------------------	---

Chapter 3/ Electronic Signature.....	11
---	-----------

Configuration of Smart Card Interface	13
---	----

Enrollment of users	15
---------------------------	----

Issuing smart cards	16
---------------------------	----

Administration of the Smart Card Interface process	18
--	----

Affixing e-signature in e-documents/records/functions.....	20
--	----

User authentication.....	20
--------------------------	----

E-signature authentication failure	20
--	----

Changing user PIN	20
-------------------------	----

Returning smart card by user	22
------------------------------------	----

Recording return of smart card.....	22
-------------------------------------	----

Troubleshooting user authentication problems.....	23
---	----

Prerequisites for e-signature using Smart Card Interface	24
--	----

Annexure.....	25
---------------	----

Chapter 4/ Technical Document Interface	27
--	-----------

Set Tech Doc System Options	28
-----------------------------------	----

Setting options for Technical Document System	28
View Technical Documentation	31
Viewing maintenance document details	31

Index.....	I-1
-------------------	------------

Chapter 1/ Introduction

The business process chain, Utilities comprises of processes that extend the capabilities of Ramco Aviation Solutions by helping users to;

- ▶ Upload object/files/documents
- ▶ Create and incorporate E-signature
- ▶ Create and interact with technical documents
- ▶ Interact with third party software/objects
- ▶ Create customized reports
- ▶ Facilitate audit

Chapter 2 of the Utilities user guide elaborates on the **Object Attachments** process, which provides the interface to upload and store objects/documents attached to any business process into a central depository, for future reference.

Chapter 3 of the Utilities user guide explains the **Smart Card Interface** process that enables the use of electronic signature (e-sign) by users.

Chapter 4 Utilities user guide explains about the **Technical Document Interface (TDI)** makes the external technical document systems (CMS) easily accessible to Ramco Aviation solution users, thereby providing the maintenance personnel with a single point access to refer to the required maintenance documents without having to opt for multiple document access systems. The TDI allows you to perform the following:

▼ Create Maintenance Change Request

The OEMs communicate the change notifications to fleet operators in the form of SBs and ADs. These SBs and ADs are available in SGML format. The TDI allows you to upload the SGML document to automatically create a Maintenance Change Request (MCR) in Ramco Aviation solution

▼ View maintenance documents

Maintenance documents will be available through predefined Technical Document Systems. The TDI allows you to access the technical document systems for viewing the maintenance document details. In addition, links may be provided in the Ramco Aviation Solution screens to directly access the relevant chapters of the Technical Document Systems.

Chapter 2/ Object Attachments

This chapter explains the sub tasks involved in the **Object Attachments** process including setting parameters for uploading files and the procedure for the actual upload of files.

Typically, Aviation business like any other engineering business/industry generates documents such as task cards, agreements, contracts, work orders, engineering orders and diagrams, invoices, etc. during daily tasks/transactions. These documents become crucial means of reference at a later point of time as they hold vital information required for the continuity of the very transactions/business that created them in the past. Sizeable pieces of information held in these documents may be graphical/dynamic/movie/animation in nature. Such information is typically converted into digital format and stored along-with the entity as associated “attachments” for reference. Thus, the management of these crucial documents becomes a critical requirement impacting the effectiveness of the business. The document management process **Object Attachments** enables users to store, maintain, print, retrieve and archive documents associated with any business process in the entire Ramco Aviation application. The Object Attachments process supports documents in a range of formats including pdf, doc, xls, ppt, jpeg, wmv, etc.

These digital objects can be stored in a central repository (typically a file storage device) on upload.

Setting parameters for uploading documents

Prior to the actual upload of files, the following tasks must be

- ▶ Setting up FTP server
- ▶ Setting up parameters for document upload

Subsequent to the above, you may upload files/documents associated with various business processes/tasks/maintenance objects into the central repository.

You must define the path for the destination folder in the FTP to which files must be uploaded before the upload process. You can upload files, documents or reference information for various organization units and business components. The maximum file size and the file save option for an organization unit and business component combination must also be defined prior to upload.

1. Select the **Set Options** link under the **Object Attachments** business component. The **Set Options** page appears as shown in *Fig 2.1*.

The screenshot shows the 'Set Options' web application interface. At the top, there's a title bar with 'Set Options' and a trailbar. Below it, a 'Date Format' dropdown is set to 'mm/dd/yyyy'. The main content area is divided into two sections: 'File Upload Options' and 'Destination Path Details'.

File Upload Options:

- FTP Server Name:** rsiftp.ramco.com
- Default Destination Path:** /Aviationsupport/ObjectAttach/
- Default Max.Upload File Size (KB):** 50000.00
- Default action if file exists:** User Selectable (dropdown)
- Upload User Name:** aviationsupport
- Password:** *****
- Read User Name:** aviationsupport
- Password:** *****

Destination Path Details:

A table with 10 rows and 7 columns. The columns are: #, Org. Unit Name, Business Component Name, Destination Path, Org. Unit #, Max.Upload File Size (KB), and Action if file exists. The table contains data for various business components like Account Group, Account Rule Definition, Accounting Setup, Advance Shipping Note, Aircraft, Aircraft History, Aircraft Maintenance Forecast, Aircraft Maintenance Program, and Aircraft Reliability.

At the bottom of the 'Destination Path Details' section, there is a 'Set Options' button.

Record Statistics:

Last Modified by: DMUSER
Last Modified Date: 11/12/2009

Figure 2.1. Setting parameters for file upload

2. In the **File Upload Options** group box, specify the **FTP Server** into which you want to upload files.

3. Specify the **Default Destination Path** for uploaded files. The system uploads the document or reference information in this path, if the destination path for any organization unit and business component combination is not specified by users.
4. Specify the maximum file size limit for any file that you want to upload in the **Default Max. Upload File Size (KB)** field. The system limits the size of any file for upload for any organization unit and business component combination to the size you specify here.
5. Use the **Default Action If File Exists** drop-down list box to set the default action to be performed, if a file already exists in the destination path. The system displays the options “Append”, “Overwrite”, “Retain” and “User Selectable”. The system displays “Retain” by default. If you select,
 - ▶ Append – The system provides the Append option at the time of file upload.
 - ▶ Overwrite – The system provides this option at the time of file upload.
 - ▶ Retain – The system provides this option at the time of file upload.
 - ▶ User Selectable – The system provides all the above options at the time of file upload.

The system sets the default action for file upload for any organization unit and business component combination to the action that you specify here.

6. Specify **Upload User Name** and **Password** for access to the FTP server to upload files.
7. Specify **Read User Name** and **Password** for access to the FTP server to view files .

In the **Destination Path Details** multiline, specify the following for organization unit and business component combination.

8. The **Destination Path** where the documents/files/reference information must be stored.
9. The maximum upload size of a file in kilobytes in the **Max. Upload File Size (KB)** field.
10. Use the **Action If File Exists** drop-down list box to set the action to be performed, if a file already exists in the destination path. The system lists the options “Append”, “Overwrite” and “Retain”.
 - ▶ Append – The system provides this option at the time of file upload.
 - ▶ Overwrite – The system provides this option at the time of file upload.

Object Attachments

- ▶ Retain – The system provides this option at the time of file upload.

11. Check the box in the multiline for the records you want to save.

12. Click the **Set Options** pushbutton, to update the destination path details



*Note: If you do not specify **Destination Path**, **Max. Upload File Size** or **Action If File Exists** for any organization unit and business component combination, the system uploads files on the basis of the following fields: **Default Destination Path**, **Default Max. Upload File Size** and **Default Action If File Exists**.*

Uploading documents

You can upload documents/files attached to a maintenance object/task such as component work order, hangar work order, repair order, aircraft or component. The files/documents are uploaded into a pre-defined folder in the FTP server.

You may upload a single file or multiple files at a time. The files for upload may be sourced from a folder in the local disk or the Intranet.

1. Select the **Upload Documents** link under the **Object Attachments** business component. The **Upload Documents** page appears. See Figure 2.2.

Figure 2.2. Uploading documents

2. In the **Org. Unit Details** group box, specify the **Org. Unit Name** for which you want to upload files or reference documents.

Single file upload

3. In the **Upload File Details** group box, use the **Business Component Name** drop-down list box to select the business component for which you want to upload files/reference documents.

4. Use the **Ref. Doc #** drop-down list box to select the type of the reference document. The drop-down list box displays document types, such as Component Work order, Aircraft Maintenance Exe. Ref #, Eng. Doc, Goods Receipt, Maintenance Change Request, Repair Receipt, Purchase Order, Part Data Change, Repair Order, Supplier Order Based Invoice, Short Term Esc. Ref #, Engineering Service Request and Engineering Advice Note. Specify the identification number of the reference document in the field alongside.
5. Specify the maximum upload size of the file in kilobytes in the **Max. Upload File Size (KB)** field. The system displays **Max. Upload File Size (KB)** specified for the business component and organization unit combination or **Default Max. Upload File Size (KB)** defined in the **Set options** activity.
6. Use the **Action If File Exists** drop-down list box to select the action to be performed, if a file already exists in the destination path. The drop-down list displays options on the basis of the **Action if File Exists** defined for the business component and organization unit combination in the **Set Options** activity.
7. Select the source document in the local folder or intranet that you want to upload to the destination folder, in the **Select File** field. Data entry in this field is *Mandatory*, if the **Source Path** field is entered.
8. The **Keycode** for the document you want to upload. The system automatically generates the keycode for a document. However, you may specify your own keycode, which will overwrite the keycode allotted to the document by the system.
9. Select the **Browse** pushbutton to choose the required file from a local folder or Intranet.
10. Select the **Upload** pushbutton to save the selected file in the destination path.

Multiple file upload

In the **Bulk Upload File Details** group box, specify the **Source Path** from where the files must be retrieved for upload.

11. Click the **Browse** pushbutton to traverse to the required folder in the source path.
12. Click the **List All Files** pushbutton to retrieve all the files from the selected source path and list them in the multiline.
13. In the **Default Details** group box, specify the following: **Business Component Name**, **Ref. Doc #**, **Action if file exists** and **Keycode**. The details that you specify in the Default Details group box are defaulted and displayed for all the files retrieved in the multiline. You may also provide details individually for each file in the multiline.
14. In the multiline, specify the **Source Path** for the file you want to upload.

15. Specify the following details for files you want to upload: **Source Path**, **Source File Name**, **Ref. Doc Type**, **Ref. Doc #**, **Business Component Name**, **Action if file exists** and **Keycode**.
16. Check the box for the records in the multiline you want to upload.
17. Click the **Upload** pushbutton.

Object Attachments

Chapter 3 / Electronic Signature

Electronic signature (e-signature) is the online equivalent of a handwritten signature of an individual. E-signature is affixed to or logically associated with a record/document, to indicate approval or authentication. An e-signature authenticates the creation, verification, approval or audit of electronic documents (e-documents) by an individual with the requisite authority.

An e-signature must possess attributes that guarantee the legitimacy of a handwritten signature. However, any information that identifies an individual found in an electronic/computer system may not constitute a signature. For example, the entry of an individual's name in an electronic/computer system may not constitute an electronic signature.

Regulatory organizations have specified acceptable forms of e-signature. These include digital signature, digitized image of a paper signature, a typed notation, an electronic code or any other unique form of individual identification that can be used as a means of authenticating a record, record entry or a document.

The **Smart Card Interface** offered by Ramco enables an individual who intends to e-sign on e-documents to create his/her e signature. The Ramco e-signature solution is based on the smart card-based authentication technique.

When a user logs into Ramco Aviation Solution using a user name and password, the system verifies the user credentials and if found valid lists activities for which the user has been granted access rights. This constitutes the first-level of authentication.

After gaining access to Ramco Aviation Solutions, users typically navigate to activities of their choice and perform transactions such as creating, editing, authorizing, canceling, reversing and viewing records. Not all these transactions may require authentication of users. Typically, transactions such as authorizing, canceling or reversing of records mandatorily require an e-signature of the user. This constitutes the next level of authentication. The system validates the e-signature of the user and then routes the record to the next stage of the workflow/process. Let us take the instance of an employee who could apply for leave using the electronic/computer system. The leave application is routed to the designated supervisor of the employee, who can access and stamp approval on the leave application by inserting his/her e-signature.

The completion of any transaction/task that requires e-signature of an individual is linked to smart card-based authentication. The actual procedure of e-signature works in the following way.

- ▶ The designated individual is issued a smart card that stores the personal identity (User ID) and personal identification number (PIN).
- ▶ When the individual is required to sign a transaction/record electronically, he/she inserts the smart card into the smart card reader connected to the client computer and enters the user ID and PIN.
- ▶ Thereafter, the system validates the user ID and PIN specified by the individual with that stored in the card.

Electronic Signature

- ▶ If found valid, the system processes the transaction or routes it to the subsequent stage in the workflow. As users are in possession of their smart cards and the PIN is known exclusively known to them, the second level of authentication is deemed to be ultimate.

The e-signature process facilitated by **Smart Card Interface** business component involves the following tasks.

- ▶ Configuration of smart cards
- ▶ Enrollment of users
- ▶ Administration of smart cards
- ▶ Smart card issue

For information on client installation and smart card reader setup, refer to the Smart Card Interface – User Installation Guide.

Typically, the Smart Card Interface process in an organization requires two roles: Administrator and User.

- ▶ The Electronic Signature Administrator who enrolls users, issues cards, configures and manages smart card system.



Note: All the tasks in this process must be performed by administrators only.

- ▶ The Electronic Signature User who uses the e-signature on e-documents.



Note: Users are granted access rights to components/activities that are enabled for electronic signature. Refer to the Annexure for a list of business components / activities / functions enabled for electronic signature.

Configuration of Smart Card Interface

You can configure Smart Card Interface at the following levels:

- ▶ Installation: Enabling the smart card interface for all the applicable user interfaces across all the organization units and business components.
- ▶ Component: Enabling the smart card interface only for specific business components of each organization unit.
- ▶ Function: Enabling the smart card interface only for specific activities/functions in specific components.

1. Select the **Smart Card Configuration** link under the **Smart Card Interface** business component. The **Smart Card Configuration** page appears. See Figure 3.1.

Figure 3.1: Configuring Smart Card process

In the **PIN Settings** group box, specify the following:

2. The maximum number of incorrect PIN entries that a user can make when inserting his/her e-signature in an e-document/activity/function in the **Maximum Number of Invalid PIN Entry**.



Note: The number of wrong PIN entries must be greater than 0 and less than 8.

3. The minimum size of a PIN in the **Minimum Number of Characters in PIN**. The number must be greater than '0' and less than '9'.
4. In the **Configuration Settings** group box, use the **Configuration At** drop-down list box to select the level at which **Smart Card Interface** must be enabled.
5. Select the **Get Details** pushbutton. The system retrieves all the business components, organization units and functions that enable **Smart Card Interface** in the multiline.
6. In the multiline, use the **Enabled** drop-down list box to enable or disable the **Smart Card Interface** for the business component, OU (organization unit) or function.

7. Click the **Save Configuration** pushbutton.



Note: The system sets the Enabled field to "Partial", if 1) The Configuration At field is set to "Installation" and Smart Card Interface is not enabled for some of the business components. 2) The Configuration At field is set to "Component" and the Smart Card Interface is not enabled for some of the functions in the business component.

Enrollment of users

Smart Card Interface administrators can enroll users to enable them to use their e-signature.

You can also temporarily stop a user from using his/her e-signature for a specific function within a business component.

1. Select the **User Enrollment** link under the **Smart Card Interface** business component. The **Smart Card User Enrollment** page appears. See Figure 3.2.

The screenshot shows the 'Smart Card User Enrollment' web application. At the top, there is a title bar with the text 'Smart Card User Enrollment' and a 'Trailbar' menu. Below the title bar, there is a search section with 'Employee ID' and a 'Get Details' button. Below this, there are input fields for 'SmartCard User Name' and 'Enrollment Status'. The main section is titled 'Enrollment Details' and contains a table with columns: '#', 'Component', 'OU', 'Function', 'User Status', and 'Remarks'. The table currently shows one record with '# 1'. Below the table, there is a horizontal scrollbar and an 'Enroll User' button at the bottom.

Figure 3.2: Enrolling users of smart cards

2. Specify the **Employee ID** of the Smart Card user.
3. Select the **Get Details** pushbutton to retrieve details of the specified Smart Card Interface user, if available.

In the **Enrollment Details** multiline,

4. Set the **User Status** to "Enabled", to enable the employee to e-sign the function in the business component/OU.
5. Enter any **Remarks** on user enrollment.

To restrict the user temporarily from e-signing in the application

6. Set the **User Status** to "Hold".
7. Enter **Remarks** on the reasons for withholding the user.
8. Click the **Enroll User** pushbutton to save the new information.

Issuing smart cards

You can issue smart cards to employees who are enrolled for e-signature. You can issue new smart cards, or reissue existing smart cards that were earlier used by other users. You can also set the expiry date for the smart card and specify the application for which the smart card must be used.

Before you start issuing smart cards, ensure that the smart card reader is connected to the computer and a new smart card is inserted. For more details on smart card reader installation, refer to the “Smart Card Interface-User Installation Guide”.

1. Select the **Smart Card Issue** link under the **Smart Card Interface** business component. The **Smart Card Issue** page appears. See *Figure 3.3*.

Figure 3.3: Issuing smart cars to e-signatories

2. In the **Card Information** group box, specify the **Employee ID** of the user to whom you want to issue the smart card.
3. Click the **Lens** icon positioned next to the **Employee ID** field, to retrieve the smart card user ID. Refer to the topic “Searching for smart card user IDs”, to know more on retrieving smart card user ID.
4. Set the **Smart Card Application** field to “Electronic Signature”.
5. Select the **Smart Card Type**.
6. Specify the date on which the smart card is issued, in the **Date of Issue** field.
7. Specify the date on which the smart card expires, in the **Date of Expiry** field.
8. Click the **Issue Card** pushbutton to issue a new smart card to the employee.

The system issues the smart card and assigns a unique ID to the smart card.



Note the following rules applicable to smart cards: 1) You can modify the PIN using the “Smart Card – Change User PIN” option provided in the “Start - Programs” menu. Refer to the topic “Changing user PIN in Smart Card Interface” for more details. 2) An employee can have any number of smart cards for a given application. Before issuing an additional card for an employee, all the existing smart cards issued to the employee must be set to “Blocked” status. 3) At any point of time, only one smart card can be active for usage in the application.

Reissuing existing smart card

9. Click the **Reissue Card** pushbutton to reissue an existing smart card.

The system will reissue the card to the selected employee, and assign a new smart card ID.



Note: You cannot reissue the smart cards that are in “Blocked” or “Cancelled” status to other employees.

Administration of the Smart Card Interface process

Administration of smart cards involves the following tasks,

- ▶ Configuring the Smart Card Interface and enabling business components/functions for the smart card interface.
- ▶ Settings the maximum number of invalid PIN entries and the minimum number of characters in a PIN.
- ▶ Enrolling users for Smart Car Interface and enabling them for components/activities
- ▶ Issuing smart cards to enrolled users

Further, administration of smart cards also includes activating, blocking, locking, unlocking, canceling and modifying the expiry date of smart cards on a need basis. You can activate, block, lock, unlock, and cancel smart cards by using the User Status attribute of the smart card. Similarly, you can reset the Date of Expiry of the card to extend the validity of the smart card.

1. Select the **Smart Card Administration** link under the **Smart Card Interface** business component. The **Smart Card Administration** page appears. See *Figure 3.4*.

Figure 3.4 Administering smart card process

2. Specify the **Search Criteria**, and click the **Search** pushbutton to retrieve the smart card details based on the search criteria.

To lock/unlock smart cards

3. Set the **Card Status** field in the **Search Results** multilines to “Lock” to lock smart cards that are in “Active” status.
4. Set the **Card Status** field to “Unlock” to unlock smart cards that are in “Locked” status.

To block smart cards

5. Set the **Card Status** field in the **Search Results** multiline to "Blocked" to block smart cards, which are in "Active", "Locked" or "Unlock" status.



Note: You cannot block those smart cards that are in "Cancelled" status.

To activate blocked or cancelled smart cards

6. Set the **Card Status** field in the **Search Results** multiline to "Active", to activate smart cards, which are in "Blocked" or "Cancelled" status.

To mark returned smart cards

9. Set the **Card Status** field in the **Search Results** multiline to "Returned", to indicate that the smart card is returned by the user.



*Note: The returned smart card can be issued as a new card to another employee, in the **Smart Card Issue** activity.*

To cancel smart cards

10. Set the **Card Status** field in the **Search Results** multiline to "Cancelled", to cancel the smart cards that are in "Active", "Blocked", "Locked" or "Unlock" status.

To set/reset expiry date

11. Specify the **Date of Expiry** for the smart card.

To save details

12. Click the **Update** pushbutton, to save the modified details.

Affixing e-signature in e-documents/records/functions

The e-signature process for end users/signatories would be as follows:

The smart card issued to a user will have the default Personal Identification Number (PIN) in it.

The user may change the default PIN to another PIN of his/her choice prior to using the smart card for e-signatures. (The **Smart Card –Change User PIN** screen facilitates changing the user PIN.)

The e-signature process begins with the launch of the **User Authentication** page. Henceforth, the user must undertake the following procedure for the successful completion of any activity/function that requires e-signature.

- ▶ The **User Authentication** page appears when the user clicks the relevant pushbutton in an application page (activity/function) enabled for e-signature.
- ▶ The user inserts the smart card into the Smart Card reader attached to the client system and types the PIN in the **User Authentication** page. The system validates the PIN entry against the user ID and the PIN stored in the card. The transaction is processed / completed, if the validation is successful.

User authentication

In a Ramco Aviation Solutions page, when you click on a pushbutton (task), which is enabled for e signature, the **User Authentication** page appears.

1. Enter your **Personal Identification Number (PIN)** for user authentication.
2. Click the **OK** pushbutton.

The entered PIN is validated against the PIN stored in the smart card and the transaction is completed on successful validation. On successful authentication, the system displays the message “Sign-Off Recorded successfully”. If an invalid PIN is entered, the system displays the error message “Incorrect Secret Code Submission” and the Electronic Signature cannot be completed.

3. Click the **Close** pushbutton to exit the page.

E-signature authentication failure

The user authentication can fail because of the following reasons:

- ▶ Inserting a smart card not issued to the user.
- ▶ Inserting the right smart card, but entering a wrong PIN.
- ▶ Inserting a smart card that is blocked, locked, cancelled or expired.

Changing user PIN

The smart card issued to users has a default Personal Identification Number (PIN) that can be changed to a code of their choice, before using it for Electronic Signature. The “Smart Card –Change User PIN” screen facilitates changing the user PIN in the smart card interface.

1. Select the **Smart Card – Change User PIN** option in the Start – Programs menu. The **Smart Card – Change User PIN** page appears. See Figure 3.5

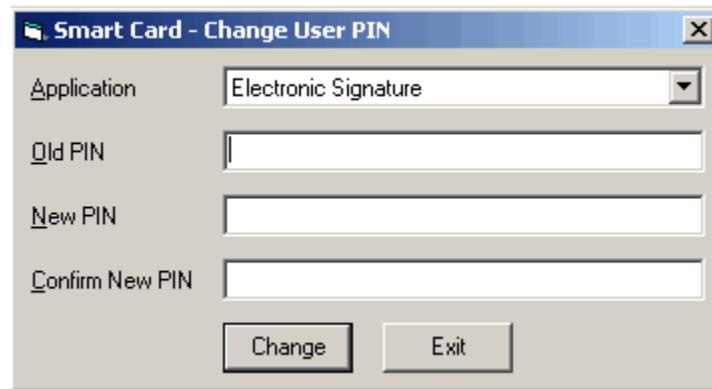


Figure 3.5 Changing user PIN in smart card interface

2. Insert the smart card into the smart card reader.
3. Select **Electronic Signature** in the **Application** field.
4. Enter the **OLD PIN** of the smart card.
5. Enter the **New PIN** for the smart card.
6. Repeat the new PIN value in the **Confirm New PIN** field.



Note: The system does not differentiate between uppercase and lowercase letters in the Personal Identification Number (PIN).

7. Click the **Change** pushbutton.

The system replaces the old PIN with the new PIN on confirmation.

8. Click the **Exit** pushbutton to exit the page.

Returning smart card by user

You can record the return of smart cards by users for various reasons such as change of department or role as a result of which they may no longer require the smart card or to acquire a new smart card. Cessation of association with the organization is another common reason for return of smart cards by employees.

Return of smart cards facilitates the reuse of these cards. Subsequent to the return of a smart card, the same card can be issued to another smart card user.

Recording return of smart card

1. Select the **Smart Card Return** link under the **Smart Card Interface** business component. The **Smart Card Return** page appears. See *Figure 3.6*.

The screenshot shows a web application titled "Smart Card Return". At the top, there is a "Trailbar" with icons for home, print, and other functions. Below the title bar, there are three main sections: "PIN Settings", "Configuration Settings", and "Details". The "Configuration Settings" section is expanded, showing a table with columns for "Employee ID", "SmartCard User Name", "Card Status", "Date of Issue", "Smart Card ID", and "Date of Expiry". The "Details" section at the bottom contains two buttons: "Return Card" and "Retrieve Card Info".

Figure 3.6 Recording return of smart card

2. Insert the smart card returned by the user into the Smart Card reader.
3. Click the **Retrieve Card Info** pushbutton to display details of the smart card from the Smart Card reader. The **Configuration Settings** group box displays smart card details.
4. Verify details of the smart card and ensure that the smart card is the one that is returned by the employee.
5. Click the **Return Card** pushbutton to indicate the return of the smart card.

Troubleshooting user authentication problems

Check for the following to avoid problems arising during user PIN authentication:

- ▶ The smart card client installation and the Internet Explorer (IE) settings.
- ▶ The smart card is inserted in the right direction in the smart card reader and the reader cable is inserted into the computer.



Note: For more details on smart card interface installation, refer to the “Smart Card Interface-User Installation Guide”.

- ▶ The e-signature is carried out using the smart card issued to the user.
- ▶ The Personal Identification Number (PIN) is entered correctly.



Note: If you enter a wrong PIN for more than the configured number of times, the smart card automatically gets into “Locked” status. Refer to the topic “Unlocking locked smart cards”, for more details on unlocking the locked smart cards.

- ▶ The Date of Expiry of the smart card. Contact the administrator to extend the expiry date for the smart card.
- ▶ The User Status of the smart card. The User Status must not be “Cancelled”, “Blocked”. Or “Help”. Contact the administrator to activate a smart card that is in “Cancelled” or “Blocked” status.

How to block and activate smart cards

A smart card is blocked under the following circumstances:

- ▶ When the card is lost or misplaced.
- ▶ When more than one smart card is issued to an employee for e-signature.

The administrator must be contacted, who will set the User Status of the smart card to “Blocked” using the Smart Card Administrator activity. The administrator sets the User Status of the smart card to “Active” in the same activity, to enable the card for e-signature once again.

How to cancel and activate smart cards

When a smart card is permanently lost or damaged, the User Status of the smart card is set to “Cancelled”. Contact the administrator to set the User Status of the cancelled smart card to “Active”, before using it for e-signature.

How to unlock locked smart cards

When a user tries to enter an invalid PIN for more than the configured number of times, the system locks the card automatically for security reason.

The administrator has to be informed, to unlock the card. The PIN of the unlocked card will be reset to the default PIN. Before the user can use the card again, the PIN must be changed using the **Change User PIN** screen.

How to extend the validity of smart cards

A smart card that has expired cannot be used any more for e-signatures. The administrator must be contacted, to extend the expiry date for the smart card.

How to return smart cards

When a user no longer needs the smart card, he/she must surrender the smart card to the administrator. The administrator sets the status of the smart card to "Returned". The returned smart card can be reused, and issued as a new card to another employee.

Prerequisites for e-signature using Smart Card Interface

- ▶ The smart card reader must be attached to the client system and configured to Ramco Aviation Solutions
- ▶ The smart card users must possess smart cards.
- ▶ The activities/functions that mandate e-sign must be enabled for smart card.
- ▶ The employees must have access rights to activities/functions that require them to e-sign, for completing the transaction.

Annexure

E-signature enabled activities and functions in business components

Ramco Aviation Solution – Hangar Work Reporting business component

Activity	Function/task/pushbutton
Record Inspector Sign-Off	Record Sign-Off
Record Inspector Sign-Off	Record Sign-Off & Completion
Record Employee Time Sheet	Sign-Off
Record Employee Time Sheet	Void Sub Task
Issue Certificate Of Maintenance	Create / Edit CoM
Issue Certificate Of Maintenance	Confirm CoM

Ramco Aviation Solution - Component Work Reporting business component

Activity	Function/task/pushbutton
Record Inspector Sign-Off	Sign-Off Tasks
Record Employee Timesheet	Sign-Off
Record Employee Timesheet	Void Sub Task
Issue Certificate Of Maintenance	Create / Edit CoM
Issue Certificate Of Maintenance	Confirm CoM

Chapter 4/ Technical Document Interface

Aircraft Original Equipment Manufacturers (OEMs) such as Boeing and Airbus provide guidelines for the maintenance and upkeep of aircraft. These guidelines are made available to the fleet operators and aircraft maintenance companies in electronic digitized form. The guidelines cover comprehensive documents like Aircraft Maintenance Manuals (AMMs), Illustrated Parts Catalogues (IPCs) and intermediate directives like Service Bulletins (SBs) and Airworthiness Directives (ADs). Usually aircraft maintenance personnel are provided access to the maintenance documents through the OEM's Technical Document Systems. For example, Airbus provides its maintenance documents through Airnav / ADOC Navigator while Boeing provides its maintenance documents through PMA and MyBoeingFleet.com. Similarly, independent third party document management systems such as "Jouve" and "Enigma", which host the OEM documents, can also be used.

The **Technical Document Interface** business process comprises the **Set Tech Doc System Options**, and **View Technical Documentation** activities.

The **Set Tech Doc System Options** activity allows you to set options for accessing the Technical Document Systems.

The **View Technical Documentation** activity invokes the Technical Document System for viewing maintenance documents.

Set Tech Doc System Options

The maintenance documents provided by the Original Equipment Manufacturers (OEMs) are made available through external Technical Document Systems. This activity allows you to set the options for connection information and authentication for accessing the technical document systems. You can select a particular technical document system and map the various manufacturers whose source documents must be viewed through the selected technical document system.



Setting options for Technical Document System

1. Select the **Set Tech Doc System Options** link under the **Technical Document Interface** business component. The **Set Tech Doc System Options** page appears. See Figure 4.1.

Set Tech Doc System Options

Tech Doc System Details

Tech Doc System: ePubs
 User ID: admin
 Home Page URL: http://ramcovm442/epubs31
 Integration Type: View AMM Reference
 Password:

Tech Doc System Ownership Attributes

Manufacturer #:
 Customer Name:
 Manufacturer Name:
 Reference Doc Type:
 Get Details

Tech Doc Interface Parameter Details

#	Parameter	Parameter Description	Permitted Value
1	Ouid	OUIINSTANCE	2
2	custid	Customer Id	2
3	AmmUniqueId	Amm Unique id Imported form Epubs	Imported ID from Epubs
4	AmmTaskNumber	Amm Task number to be viewed	Valid amm task number
5			

Default Tech Doc System Settings

Enable Default TDS: Yes
 Default Tech Doc System: ePubs
 Default Customer:
 Set Options

Record Statistics

Last Modified by: DMUSER
 Last Modified Date: 05/05/2010

Figure 4.1 Setting options for Technical Document System

2. In the **Tech Doc System Details** group box, select the **Tech Doc System** as “Jouve”, “Airnav” or “ePubs”, through which you wish to view the source document details.
3. Select the **Integration Type** of the Tech Doc System with the Maintenance & Engineering Application. The system lists the options “View AMM Reference” and “View Task Card” if the Tech Doc System is set as “Airnav” or “Jouve”. If the Tech Doc System is set as “ePubs”, the system lists the options “View AMM Reference”, “View Task Card” and “Print Task Card”.
4. Enter the **User ID** and **Password** for accessing the technical document system.
5. Enter the **Home Page URL** indicating the URL of the document which the user intends to view.

In the **Tech Doc System Ownership Attributes** group box,

6. Enter the **Manufacturer #** and **Manufacturer Name** whose source document details must be viewed through the selected technical document system.
7. Enter the login ID of the customer, using which the Tech Doc System can be viewed, in the **Customer Name** field.
8. Use the **Reference Doc Type** drop-down list box to specify the type of the reference document as “AMM”.
9. Click the **Get Details** pushbutton, to retrieve the details (if any) for the selected technical document system.

On clicking the Get Details pushbutton, the system automatically retrieves the following details for the selected “Tech Doc System”, in the **Tech Doc Interface Parameter Details** multiline:

- ▼ Parameter - The parameter specific to the Tech Doc System.
 - ▼ Parameter Description - The description of the parameter.
 - ▼ Permitted Value - The permitted value of the parameter. If the Tech Doc System is selected as “Airnav” and the Integration Type is selected as “View AMM Reference”, the system displays the string **Enter ‘1’ for ‘True’ and ‘0’ for ‘False’** for the parameters “Force” and “Open Administrator”.
10. Enter the **Value** defined for the parameter.
 11. Enter any additional **Remarks** pertaining to the technical document system.

In the Default Tech Doc System Settings group box,

12. Use the **Enable Default TDS** drop-down list box and select “Yes” to specify whether the technical document must be defaulted on launch of the page or not. Otherwise select the option “No”.
13. Select the **Default Tech Doc System** as “Jouve”, “Airnav” or “ePubs”.
14. Enter the name of the **Default Customer**.
15. Click the **Set Options** pushbutton to update the options for the technical document system.

View Technical Documentation

Maintenance documents provided by the Original Equipment Manufacturers (OEMs) will be available through the technical document systems. This activity allows you to view the source documents by invoking the technical document system set for the manufacturer in the **Set Tech Doc System Options** activity. You can select a manufacturer and launch the corresponding technical document system for viewing the source document details.



Viewing maintenance document details



Note: The manufacturer must have been mapped to a technical document system in the “Set Tech Doc System Options” activity.

1. Select the **View Technical Documentation** link under the **Technical Document Interface** business component. The **View Technical Documentation** page appears. See Figure 4.2.

Figure 4.2 Viewing maintenance documents

2. Select the **Tech Doc System** as “Jouve”, “Airnav” or “ePubs”, through which you wish to view the source document details.
3. Enter the number identifying the manufacturer whose source documents must be viewed, in the **Manufacturer #** field.

The system displays the **Manufacturer Name**.

4. Enter the login ID of the customer, using which the Tech Doc System can be viewed, in the **Customer Name** field.
5. Use the **Reference Doc Type** drop-down list box to specify the type of the reference document as “AMM”.

Based on the mapping done in the **Set Tech Doc System Options** activity, the system invokes the technical document system corresponding to the manufacturer, for viewing the source document details.

Index

A

Action If File Exists, 5, 8, 9
Administration of the Smart Card Interface process, 18
Affixing e-signature in
E-documents/records/functions, 20
Aircraft Maintenance Manuals, 27
Airworthiness Directives, 27
Annexure, 25

B

Bulk Upload File Details, 8
Business Component Name, 7, 8, 9

C

Card Information, 16
Changing user PIN, 20
Configuration At, 13
Configuration of Smart Card Interface, 13
Customer Name, 29, 31

D

Date of Expiry, 16
Date of Issue, 16
Default Action If File Exists, 5
Default Customer., 30
Default Destination Path, 5
Default Max. Upload File Size, 5
Default Tech Doc System, 30
Destination Path Details, 5

E

Electronic signature, 11
Enabled, 13
Enroll User, 15
Enrollment Details, 15
E-signature authentication failure, 20

F

File Upload Option, 4

G

Get Details, 29

H

Home Page URL, 29
How to block and activate smart cards, 23

How to extend the validity of smart cards, 23

How to return smart cards, 24

How to unlock locked smart cards, 23

I

Illustrated Parts Catalogues, 27
Integration Type, 29
Introduction, 1
Issuing smart cards, 16

K

Keycode, 8, 9

M

Maintenance document
Viewing details, 31
Manufacturer #, 29, 31
Manufacturer Name, 29, 31
Max. Upload File Size, 5, 8
Maximum Number of Invalid PIN Entry, 13
Minimum Number of Characters in PIN, 13
Multiple file Upload, 8

O

Object Attachments process, 1
Object Attachments, 3, 4
Org. Unit Details, 7
Org. Unit Name, 7

P

Parameter Description, 29
Parameter, 29
Password, 29
Permitted Value, 29
PIN Settings, 13
Prerequisites for e-signature using Smart Card Interface, 24

R

Ramco e-signature solution, 11
Read User Name and Password, 5
Ref. Doc #, 8, 9
Reference Doc Type, 29, 31
Reissuing existing smart card, 17
Returning smart card by user, 22

S

- Save Configuration, 14
- Select File, 8
- Service Bulletins, 27
- Set Options for Object Attachments, 4
- Set Tech Doc System Options, 27, 31
- Setting Options for technical document system, 28
- Single file upload, 7
- Smart Card – Change User PIN option, 21
- Smart Card Application, 16
- Smart Card Configuration, 13
- Smart Card Interface process, 1
- Smart Card Interface, 11
- Smart Card Return, 22
- Smart Card Type, 16
- Source Path, 8, 9

T

- Tech Doc System Details, 29
- Tech Doc System Ownership Attributes, 29
- Technical Document Systems, 27, 31
- To activate blocked or cancelled smart cards, 19

- To block smart cards, 19
- To cancel smart cards, 19
- To lock/unlock smart cards, 18
- To mark returned smart cards, 19
- To save details, 19
- To set/reset expiry date, 19
- Troubleshooting user authentication problems, 23

U

- Upload Documents, 7, 8, 9
- Upload File Details, 7
- Upload User Name and Password, 5
- User authentication, 20
- User ID, 29
- User Status, 15, 18, 23

V

- Value, 29
- View Technical Documentation, 27, 31
- Viewing
 - Maintenance document details, 31



Corporate Office and R&D Center

Ramco Systems Limited, 64, Sardar Patel Road, Taramani Chennai – 600 113, India

Tel: +91 (44) 2235 4510. Fax +91 (44) 2235 2884

www.ramco.com