

Introducing Galileo *Enhanced Privacy Protection*

Galileo is pleased to announce the launch of enhanced security functionality for all customers who access and utilise the Galileo and Apollo system. **If you airline does not have terminal type access to our system from one or more of your locations there is not a need to review this advisory.**

Airline's that have access do so from Airline Servicing Terminals, otherwise known as an AST. This access is more than likely through PC hardware that you have provisioned and could be via use of several possible applications. **If your access is through the new Galileo Desktop Interface Access (GDIA) this notice also does not apply to you.** If you are accessing through Focalpoint Net, an unmanaged VPN, Galileo provided hardware, or some other third party application please review this advisory for important information.

The aim of Galileo *Enhanced Privacy Protection* is to assist all Galileo customers in complying with many of the Payment Card Industry (PCI) Security Council standards and to help them protect themselves and their customers against credit/debit card fraud.

The purpose of this message is to advise you of the changes that are taking place, and to let you know that there may be a number of actions that must be completed before the 07 May¹ 2007 when Galileo *Enhanced Privacy Protection* is activated. Please understand that **failing to prepare means that you may lose the ability to access the Galileo system temporarily.**

Summary of Changes

The following system changes will apply from 07 May 2007 - the date of activation of Galileo *Enhanced Privacy Protection*.

- **Individual sign-on for each user.**

The primary focus of this initiative is to ensure that each person who accesses the Galileo system has their own sign-on and password. Currently some customers using Airline Servicing Terminals (AST's) operate in a multi-user or shared sign-on environment. Use of the 'multi-terminal' capability in Galileo to accommodate multiple users is no longer permitted. This will be monitored to ensure that this functionality is not used inappropriately. Please note that is your airline's responsibility to ensure that **each person accessing Galileo has an individual sign-on.**

- **Password controlled access for each user.**

Some AST customers are currently able to sign-on without using a password at all. This password bypass functionality will no longer be available, and everyone who accesses the Galileo system will be required to have their own private and secure password. The only exception to this will be for robotic applications where these are identified.

- **Minimum password length.**

All new passwords created beginning the 23rd of April 2007 (this element loads ahead of the other changes) will need to be between 7 and 10 alpha numeric characters long. Previously, the minimum was 6 characters.

- **Deletion of inactive user sign-ons.**

A new system clean-up utility will run regularly to delete any user sign-on that has not been utilised to log into Galileo for **more than 90 days**. This feature ensures that sign-ons allocated to members of staff who may have left or changed responsibility do not remain active unnecessarily – an identified security risk.

Please note that Galileo is implementing this functionality to allow Galileo customers to comply with **some** PCI requirements only. It is your company's responsibility to address all PCI security standards, not just those related to Galileo access only.

Full details of the PCI Security Standards can be found at:

- <http://www.pcicomplianceguide.org/> - a guide to achieving PCI compliance
- <https://www.pcisecuritystandards.org/tech/index.htm> - direct link to the PCI Data Security Standard

¹ Please note that activation will take place late on 07 May (U.S. Mountain time) therefore will take effect in most of the world on 08 May.

Please follow the steps below to ensure you are prepared for the implementation of Galileo Enhanced Privacy Protection initiative.

Preparing for Galileo Enhanced Privacy Protection:

Galileo has undertaken some preliminary investigation as to how each AST location utilises their sign-on's. Please use the table below for guidance as to any actions, if any, are necessary for your office:

If your AST Location:	Next step:
...meets all of the following criteria: <ul style="list-style-type: none"> • does not use Password Bypass at all • does not use Multi Terminal at all 	No action is required other than to understand the details contained within this advisory and ensure ongoing compliance.
... has Password Bypass activated for one or more of its Sign Ons.	Please advise those people accessing Galileo who do not currently utilise a password that passwords will be automatically enforced from the day after Enhanced Privacy Protection is activated (i.e. 08 May). This means that they will be prompted to set up a password the first time they sign on from this date onwards.
<ul style="list-style-type: none"> • ...has any sign-one's with Multi-Terminal set to 'Y' or yes 	Several actions need to be taken to review your location's sign on requirements in order to be ready for Galileo's Enhanced Privacy Protection initiative. Please review this document for the details. If any questions remain, please use the details shown under Contacting Galileo to contact us.

Determining your location's situation:

Step 1: Identify whether or not your location has a 'Secondary Level Authoriser'.

Secondary Level Authorisers

The key to a successful transition to Enhanced Privacy Protection is for each AST location to ensure they have one or more "Secondary Level Authorisers." These Secondary Level Authorisers will have the ability to manage other individual user sign-on's within that location. **In the past, we have seldom set up secondary authorisers for our airline customers, but now feel that it will help run your business more efficiently.**

The Secondary Level Authoriser within the AST location would be responsible for:

- Creating new user Sign-On's when new staff require access to Galileo.
- Deleting Sign-On's when staff leave the business or no longer require access.
- As necessary, allowing robotic application sign-ons to by-pass the password requirement.
- Resetting passwords for existing AST users when these have been forgotten (Please note that Second Level Authorisers will still need to contact Galileo using the online Airline Customer Centre <http://tdssupport.cendant.com/tdssupport/> to have their own passwords reset).

Effective use of the Secondary Level Authoriser function, will allow your business to take control of monitoring who accesses, and utilises Galileo, and to ensure your business maintains PCI compliance.

- Three consecutive characters are not allowed. (Example: AAA or 222.)
- The users' previous five passwords will be stored and may not be re-used.
- Password changes are limited to once per system day.
- At least three characters must change in the new password.
- Passwords are good for 90 days.

Managing forgotten passwords: Keywords

Keywords in Galileo are an additional security feature within the sign-on functionality that help identify a user when a password has been forgotten, and a request for password reset is made. Each user can update their sign-on to add their own keyword (see [Adding a Keyword](#) in the 'How to' Guide below) and this will remain hidden from **all** other users of the system. No-one but the user themselves can update or add a keyword to their sign-on.

For example: A user forgets their password and needs to request a reset from their secondary authoriser.

If the user requesting the reset is known to the Secondary Level Authoriser and is positively validated as the user making the request, then the authoriser can reset the password (see [Locked Sign-on/Resetting Forgotten Password](#) below) leaving **USE KYWD** set to **N**.

If the Secondary Level Authoriser cannot positively identify the user requesting the reset, they should set the **USE KYWD** flag in the sign-on to **Y**, so that the next time the user logs in they will be prompted to enter their keyword before they will be able to create their new password. This way you can protect against illegitimate reset requests from unauthorised users.

We strongly recommend that your business use this functionality and enforce the use of keywords to provide additional system security.

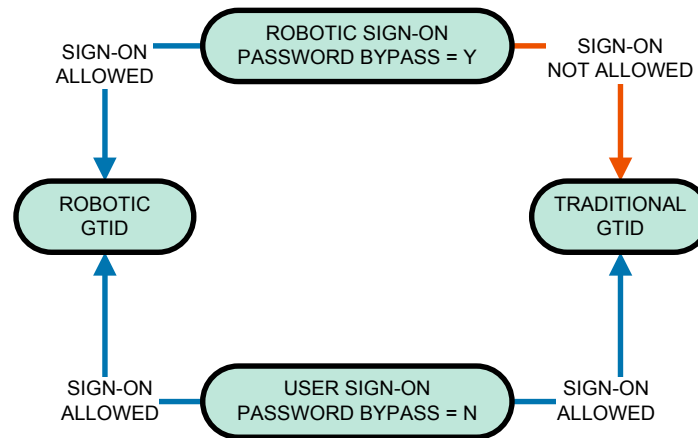
Suggested Preparation Timeline:

DATE	ACTION	OWNER	NOTES
IMMEDIATELY	Identify which of the three situations your AST location fits	AST owner at airline	See table above and take action as described.
IMMEDIATELY	Ensure all persons accessing Galileo have a unique, individual sign-on.	Second Level Authoriser	Create new sign-in's for each person as necessary. See below for instructions.
IMMEDIATELY	Ensure each person with a sign-in is using their own password.	Second Level Authoriser	Sign-ons can either be updated right away to ensure the PSWD BYPASS field is set to N . Or, if no action is taken this will be setting will be activated automatically once Enhanced Privacy Protection is implemented.
23 April	Minimum password length extended from 6 character to 7-10	Everyone who uses Galileo	Although this will be activated on 23 April, it will not come into effect until the next time each person sets a new password.
07 May	Galileo <i>Enhanced Privacy Protection</i> functionality is activated	Galileo	See On Activation below.
Post-Activation	Ensure that the Second Level Authorisers are responsible for user maintenance.	Second Level Authoriser	See How To Guide for more information.
Post-Activation	Ensure PCI compliance is monitored and enforced within the airline.	Airline AST owner	Full details of the PCI Security Standards can be found here: <ul style="list-style-type: none"> • http://www.pcicomplianceguide.org/ • https://www.pcisecuritystandards.org/tech/index.htm

Notes on Robotic Applications:

A robotic is an application that performs a predetermined set of automated tasks and does not usually have the ability to use a password or change a password every 90 days. Examples of robotic applications can include quality assurance and auto ticketing software and whilst these would generally apply more to Travel Agency locations, it is possible that they may also exist within some of our airline customer locations.

Unlike individual sign-ons, robotic sign-ons will not require a password. Therefore, the robotic sign-on can only be used in association with a “robotic” GTID terminal type. Typical individual user sign-ons can be used on a robotic GTID or a traditional GTID, but **robotic sign-ons can only be used on robotic GTIDs**. The following diagram shows the relationships:



GTIDs running robotics will have to be identified by the airline to Galileo. Airlines using robotics need to gather a list of all GTIDs and all sign-ons that will need to be designated as robotics. A re-initialisation of the GTID (sign off) will need to occur to make it a Robotic GTID. Therefore, Galileo will have to coordinate with the airline to update these.

Additionally, any Sign-On which needs to retain password bypass functionality for robotic use should be reported to your Second Level Authoriser so that the appropriate changes can be made (see [Configuring a Sign-on for Password Bypass](#)) to ensure continued operation once Galileo Enhanced Privacy Protection is activated.

In addition, all GTIDs associated with this sign-on must also be updated to a new terminal type of ‘robotic’. A list of all relevant GTIDs should be passed to Galileo using the Airline Customer Centre (<http://tdssupport.cendant.com/tdssupport/>) raising a new issue under Request Type General Issue and Request Category Airline Servicing Terminal. This will allow Galileo to clearly identify your request and take appropriate action.

IMPORTANT NOTES

For robotic GTIDs to be updated ahead of the 07 May load date, each Airline must **advise Galileo of impacted GTIDs**.

Please also note that whilst the ability to bypass passwords still exists in Galileo, this must only ever be used in legitimate cases where an application or robotic requires this functionality in order to access the host. This functionality is not to be used as a ‘workaround’ to allow access to the Galileo host without password control. Any location found to be using this functionality to bypass password-controlled access would not be PCI compliant.

Structured Data

There is no impact to structured data as a result of these changes. Structures already exist which can be used to sign in with a password and to change the password if the application wishes to use a password.

Troubleshooting On Activation Day:

Provided all the activities above are completed in advance of the 07 May Enhanced Privacy Protection activation date, users and applications should be unaffected. In the event that certain actions are not completed, the following are a list of possible issues and guidance for resolution:

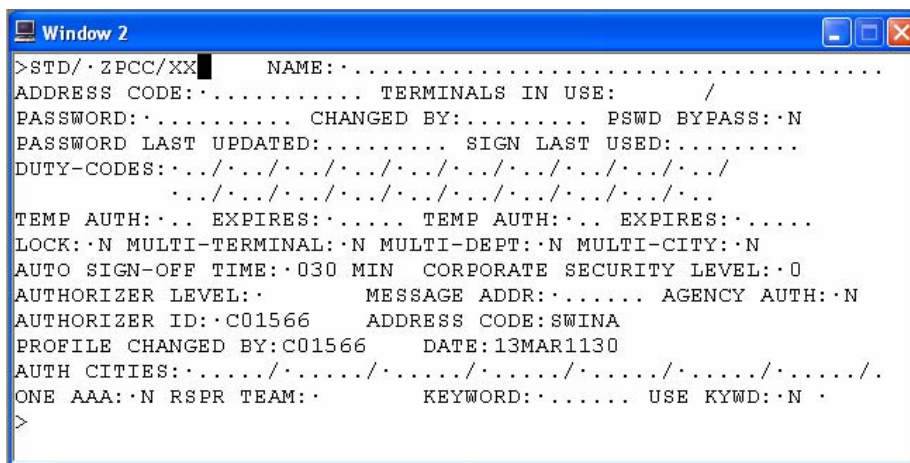
ISSUE	RESOLUTION
AST user does not have password set on day of activation.	The next time this person signs on to Galileo, they will be prompted to enter a keyword and password. These will need to be memorised and the password used each time the agent signs on.
AST user has password of only 6 characters on day of activation.	There is no change on day of activation. The next time the AST user's password expires they will be prompted to create a new password conforming to the new 7 character minimum.
AST users attempt to continue sharing sign-in's on day of activation.	If these shared sign-ons were previously used without password-controlled access, the first user to log into Galileo post-activation will be prompted to create a keyword and password preventing subsequent users from accessing the system. This would fail a PCI compliance audit. Galileo cannot restrict this activity. Galileo will monitor the use of 'multi-terminal' and 'M' type sign-ons but responsibility to ensure these are not used remains with the airline.
'Robotic' applications fail.	It is likely that the sign-in's for these applications have not been identified and reported to Galileo in advance before activation day. The user should report the issue to their Second Level Authoriser who should then update the impacted sign-on following the special instruction for configuring a sign-on for password bypass in the 'How to Guide' below. Additionally, the list of associated GTIDs should be reported to Galileo via the Airline Customer Center.

Important: There are likely a number of actions that **must** be completed by customers who access the Galileo system using an Airline Servicing Terminal (AST) before the **07 May** activation date of Enhanced Privacy Protection. **Failure to perform these tasks may mean lack of system access..**

Important: To ensure PCI compliance, it is the **Airline's responsibility** to control each individual user's access to confidential credit card information. Galileo does not have the visibility of the operational processes and staff within each location where the Galileo system is used, so cannot manage this on behalf of the airline or guarantee their compliance.

Format:	Explanation:
STD	Sign-on Table Display
/	Separator
Z	Mandatory identifier
PCC	Represents the Pseudo City Code for which sign-on profile is to be associated – please replace with your actual 3 or 4 character PCC
/	Separator
XX	Initials for the new user – please replace with the actual users initials

Screen response:



```

Window 2
>STD/·ZPCC/XX· NAME:.....
ADDRESS CODE:..... TERMINALS IN USE: /
PASSWORD:..... CHANGED BY:..... PSWD BYPASS:·N
PASSWORD LAST UPDATED:..... SIGN LAST USED:.....
DUTY-CODES:···/···/···/···/···/···/···/···/···/···/
····/···/···/···/···/···/···/···/···/···/
TEMP AUTH:··· EXPIRES:····· TEMP AUTH:··· EXPIRES:·····
LOCK:·N MULTI-TERMINAL:·N MULTI-DEPT:·N MULTI-CITY:·N
AUTO SIGN-OFF TIME:·030 MIN CORPORATE SECURITY LEVEL:·0
AUTHORIZER LEVEL:· MESSAGE ADDR:····· AGENCY AUTH:·N
AUTHORIZER ID:·C01566 ADDRESS CODE:SWINA
PROFILE CHANGED BY:C01566 DATE:13MAR1130
AUTH CITIES:·····/·····/·····/·····/·····/·····/·····/
ONE AAA:·N RSPR TEAM:· KEYWORD:····· USE KYWD:·N ·
>
  
```

Note: If a sign-on already exists with the initials that you have chosen, details of that sign-on will be displayed rather than the new, blank screen.

- Ensure that the INSERT key on your keyboard is switched OFF
- Tab to **NAME** field and enter the name of the user, family name first e.g. KERIN GERARD followed by 'AST'
- Tab to the **ADDRESS CODE FIELD** and:
 - If you are an **airline with a 2 alpha carrier code** e.g. BA:
 - Enter an X followed by your carrier code followed by your AST PCC followed by an / and then the carrier code again e.g. XBAPCC/BA for a British Airways site where PCC represents the PCC
 - If you are an **airline with a carrier code that contains a number** e.g. E8
 - Enter ABC followed by your AST PCC followed by an / and then the carrier code e.g. ABCPCC/E8 for an Alpi Eagles site where PCC represents the PCC
- Tab to the **PASSWORD** field and input a password, e.g. HOLIDAY1. The password should be a minimum of 7 characters and a maximum of 10. It must include at least one numeric character and cannot be the user name. When the user signs on for the first time the Galileo system will prompt them to change their password to one of their own choice
- Tab to the first space in the **DUTY CODES** field and enter **AG**
- Tab to the **LOCK** field. Change the **N** to **Y**, this means that the user sign-on will lock following 5 attempts to sign-on using an invalid sign-on password combination
- Tab to the **AUTO SIGN-OFF TIME** and change it to read **030**
- Tab through the screen until your cursor is flashing after the dot that is to the right of the **KYWD N** field
- Examples of fully completed screens are shown over the page
- Press the Enter key on your keyboard.

The screen response will be **AGENT PROFILE ADDED - GALILEO. (or Apollo)** This indicates that the new agent sign-on has been successfully created.

Screen response (using EA7 as an example PCC):

```

Window 1
THE FOLLOWING IS A LIST OF USER PROFILES INDEXED TO EA7
Z EA7/GK KERIN GERARD 02MAR1531 SEC
Z EA7/PS SHARP PAUL 01MAR0925 ---
Z EA7/TS SAIT TONY 02MAR0850 ---
Z EA7/000 ATB AUTOSON 01MAR1652 ---
END REPORT
>
  
```

Screen:	Explanation:
THE FOLLOWING IS A LIST.....	Header line including the PCC reference
Z	User sign-on indicator
EA7	Pseudo city the profiles are associated to
/	Separator
GK	User sign-on code
KERIN GERARD	Agent name
02MAR1531	Date and time sign-on was last used
SEC	Secondary level sign-on profile
---	Agent level sign-on profile

Configuring a Sign-on for Password Bypass

To allow the use of password bypass for Robotics, a new indicator will be added to the 3rd page of the User's Sign-on Profile. An example of a Sign On 3rd page is shown below:

```

>STD/ ZEA7/BB /** NAME: BASHAR
ADDRESS CODE: SWIEA7 TERMINALS IN USE: ...../.....
AUTHORITY LEVEL: SECOND REQUESTER ID: ..... TYPE: ....

STOCK ·N·N SALE ·N·N MCOST ·N·N CHKIN ·N·N COMM ·N·N
PAYMT ·N·N RFRSH ·N·N HLINE ·N·N DEBT ·N·N SELL ·N·N
CLEAR ·N·N PINV ·N·N APRT ·N·N ECCBP ·N·N CCBYP ·N·N
PDQA ·Y·Y PDQB ·N CFIL0 ·Y·Y CFILC ·Y·Y CFILM ·Y·Y
QSORT ·N·N CFILD ·Y·Y CFILR ·Y·Y CFILN ·Y·Y CFILT ·Y·Y
HORAC ·N·N RULB ·N·N RULD ·N·N RULX ·N·N ETOD ·N·N
CFILU ·N·N STRT ·N·N AATV ·N·N QFWD ·N·N QSUM ·N·N
TKMC ·N·N DOTA ·N·N HMLRG ·N·N CMSK ·N·Y RBTC ·N·N
  
```


be prompted to first enter their keyword (which is known only to them) before they will be able to enter their new password. In this way you can protect against illegitimate reset requests from unauthorised users.

5. Tab to the end of the profile to the tab stop after **USE KYWD: N** and enter.

The **L** will change to **N**. The user must sign on to the Galileo system using the new password, and they will be immediately be prompted to change it to a new one.

Note: A Galileo sign-on must have a minimum of 7 alpha/numeric characters.

If you have a second level sign-on and your profile is locked, please contact Galileo via the Airline Customer Centre (see [Contacting Galileo](#)).

To reset a password for an Agent Level Sign On, the same process is followed but the **Password** field is overwritten with the new password rather updating the **Lock** field.

Adding a Keyword

To add a keyword to your sign-on:

1. Enter **STD/ZGK** (where GK is an example of a sign-on)
2. Tab to the **KEYWORD** field add type your chosen keyword over the *******s**. The keyword must consist of numbers and/or letters (no symbols) and be 6 characters long. It is important that something memorable is used as a keyword. Since this does not need to be changed every 90 days, it is recommended that something easily memorable such as date of birth, mother's maiden name, favourite pet etc. is used.
3. Tab to the end of the profile to the tab stop after **USE KYWD: N** and enter.

Delete an Agent Level Sign On

A second level sign-on must delete an agent level sign-on profile.

Note: Only the Galileo Helpdesks are able to delete a second level sign-on profile.

A profile may only be deleted by the creator.

- 1) Display the profile: **STD/ZE7/MH**
- 2) Take Control of the Agent Level Sign On by over typing your sign-on into the authorizer ID field
- 3) Remove the profile **STR/ZE7/MH**

Delete an Secondary Level Sign On

Only the Galileo can delete a Secondary Level Sign-Ons therefore all requests must be made via the Airline Customer Center (see [Contacting Galileo](#))

Taking Control of Agent Level Sign On

If a Secondary Level user experiences difficulties when trying to update an Agent Level Sign On, they may need to 'take control' of that Sign On. To do this simply:

- Display the Agent Level Sign On (**STD/ZPCC/XX** where PCC represents your PCC and XX represents the Sign On)
- Tab to the **Authorizer ID** field and enter **ZPCC/XX** (where PCC represents your PCC and XX represents the Secondary Level Sign On)
- Tab to then end of the screen (i.e. to the right of Use Keyword:.N) and press **Enter**

The Secondary Level user will now have control of that Agent Level Sign On.

Contacting Galileo

An AST location will need to contact Galileo if they:

- They do not know if they have a Secondary Level Sign On or not
- Need any additional Secondary Level Sign Ons
- If the Secondary Level Sign On becomes locked (i.e. password is forgotten)
- If they require any GTIDs to be updated to Robotic status
- Have users using Multi Terminal and have not received a call from Galileo by 22 April

In each of these situations please log on to the Airline Customer Centre <http://tdssupport.cendant.com/tdssupport/> and raise a new issue under:

Request Type **General Issue**
Request Category **Airline Servicing Terminal**

This will allow Galileo to clearly identify your request and take necessary action.

If action is required on an existing Sign On please ensure the problem report includes full details of that Sign On and the PCC it resides within. If the action requires the creation of a new Secondary Level Sign On please ensure the problem report includes the full name of the new Secondary Level User. If the action requires GTIDs to be updated to Robotic status, please list the applicable GTIDS.

Copyright

Copyright © 2007 Travelport Corporation. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of the Travelport Corporation.

Trademarks

Travelport may have patents or pending patent applications, trademarks copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property rights except as expressly provided in any written license agreement from Travelport.

All other companies and product names are trademarks or registered trademarks of their respective holders.