

For: FFAS Federal and County Employees

LincPass Badge Tips

Approved by: Deputy Administrator, Management



1 Overview

A Background

Notice SEM-3 instructed FFAS employees to have and use their LincPass badges to access their work computers by December 1, 2011, **if** the technology exists on their computer.

As a result of Notice SEM-3 and employees' renewed effort in using their LincPass badge, EPD is receiving numerous questions about various functions of their LincPass badge for everyday computer operations. In an effort to reduce the number of calls received by EPD on the functionality of LincPass badge with FFAS's computing system, EPD is providing employees with tips found to cover the most requested topics by employees.

B Purpose

This notice provides helpful tips on using and managing employee LincPass badges.

Disposal Date	Distribution
May 1, 2012	All FAS, FSA, and RMA Federal and County employees; State Offices relay to County Offices

Notice SEM-9

2 Using and Managing LincPass Badges

A Sign On Using the LincPass Badge

When employees sign on to their computer using their LincPass badge, they should never have to enter another user ID and password for site access that requires their eAuthentication user ID and password.

Example: An employee has training to take in AgLearn and later that afternoon will need to enter their WebTA record. When the employee accesses these sites, they will **not** be prompted to enter their eAuthentication user ID and password. They will automatically have access to these sites because they signed on using their LincPass badge.

When employees step away from their computer, all they have to do is remove their LincPass badge from the card reader and the computer will automatically lock itself down. When employees return, they just re-insert the LincPass badge, enter their 6-8 digit personal identification number (PIN), and their computer will unlock.

B Encrypting E-Mails With the LincPass Badge

In the near future, employees will be able to use their LincPass badge to automatically encrypt e-mail and assign a digital signature to e-mails. When employees use their LincPass badge to assign a digital signature to their e-mail, if the e-mail is forwarded, the recipient who forwards the e-mail **cannot** change any of the text in the employee's original e-mail. This ensures that the employee's original e-mail is kept intact. To access the encrypting and signing e-mail function using the LincPass badge, do the following:

- on the Microsoft Outlook main screen, CLICK “**Tools**”
- on the drop-down menu, scroll down and CLICK “**Trust Center**”
- on the Trust Center window that will be displayed, CLICK “**E-mail Security**”
- on the Trust Center Encrypted e-mail Screen CHECK (✓) either of the following:
 - “Encrypt contents and attachments for outgoing messages”
 - “Add digital signature to outgoing messages”
- CLICK “**OK**”.

Note: Currently, to remove the encryption or digital signature option, UNCHECK (✓) the appropriate boxes from the Trust Center Encrypted e-mail Screen and CLICK “**OK**”.

Notice SEM-9

2 Using and Managing LincPass Badges (Continued)

C Checking the Certificate Expiration Date on LincPass Badges

Each LincPass badge has 2 expiration dates encoded in them. The obvious date is the LincPass badge expiration date that is displayed on the top right-corner of the LincPass badge. The second date is hidden and is for the gold certificate on the bottom center of the LincPass badge. The certificate date is maintained by GSA and GSA notifies the LincPass badge holder when this expiration is about to occur. A few months before the certificate expires, the USAccess system, "HSPD12ADMIN", will send the LincPass badge holder an e-mail with instructions on how to get their certificate rekeyed. These e-mails are sent to the LincPass badge holder at intervals of 90, 60, 30, 15, and 7 calendar days **before** the certificate actually expires. If the LincPass badge holder has successfully rekeyed their certificate, e-mails will no longer be sent.

Employees can manually check the expiration date of their LincPass badge certificate at a computer that has a card reader, as follows:

- from the Start Menu, CLICK:
 - "All Programs"
 - "ActivIdentity"
 - "ActivClient"
 - "User Console"
- in the "ActivClient" window, DOUBLE-CLICK "My Certificates" option
- double-click any of the certificates listed
- in the window displayed, the "valid from" second field will display the expiration date.

Note: The LincPass badge holder **must** know their PIN number **before** they can have their certificates rekeyed at a Light Activation site or a fixed enrollment site.

D Resetting the LincPass Badge PIN

Employees can reset their LincPass badge PIN by visiting either a Light Activation site or a fixed enrollment site. At the Light Activation or fixed enrollment site, activators will assist employees with resetting their PIN. Do **not** discard the LincPass badge because the PIN has been forgotten.