OFFICE OF THE CHIEF INFORMATION OFFICER
IDENTITY & ACCESS MANAGEMENT

# Digital Signature: Adobe Configuration Change to Registry Settings for Certificates

21 March 2011

USDA

United States Department of Agriculture

*Table 1. Document Revision & Version Information*

| Version No. | Date | Description | Author/Approval |
|---|---|---|---|
| 1.0 | 3/21/2011 | Version 1 Final | Todd Kaywood |

Digital Signatures_Adobe Configuration Change To Registry setting for Certificates_FINAL.doc

# Table of Contents



-- -- --

# 1. Summary

## 1.1 Overview of Digital Signatures

The Digital Signature project is focused on providing information and communication on how to use LincPass certificates to digitally sign documents. The benefit of digitally signing documents is the assurance the information hasn't been altered since the document was distributed, and verification of the signer's digital identity.

The USDA enterprise approach will ensure that all agencies can implement best practices, lessons learned, and common technologies using digital signatures and LincPass ID cards. By mid-September, our objective is to have completed a pilot with selected agencies and begin the full agency rollout. This will be followed by a proposed next-phase rollout plan with other related technologies.

We are creating an enterprise approach to digital signature technology that can be used across the USDA to achieve the strategic objectives of agencies and to continually build on and make better use of the LincPass (PIV card).

### 1.1.1 What Is the Digital Signature Project?

The purpose of the Digital Signature project is to enable the use of the LincPass card for digitally signing files and emails.

- Digital signatures are a variant of electronic signatures that include use of PKI for cryptographic assurance of the sender's identity, and an integrity check on the text received.
- It can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document that has been sent is unchanged.
- Digital signatures are much more difficult to forge or falsify.

The scope of the OCIO Digital Signature Rollout project will include:

- LincPass integrated.
- Integration with the following products and platforms:
    - XP Operating System:
        - Adobe Acrobat files and forms – Versions 8 & 9
        - Microsoft Office (Word, Excel, PowerPoint) – Versions 2003 & 2007
        - Microsoft Outlook – Versions 2003 & 2007

**At this time, email encryption *will not* be included in the scope of this effort.**

### 1.1.2 Why Are We Doing the Digital Signature Project?

USDA's Chief Information Officer (CIO), along with representatives from multiple USDA agencies, have requested a USDA Department-wide project rollout on the use of digital signatures using the USDA LincPass card.

Digital signature benefits:

- LincPass integrated.
- Assurance that the information has not been altered since it was sent.
- Verification of the signer's digital identity.

# 2. Digital Signature Required Technical Change

The OCIO-IAM team is recommending a modification to the existing configuration for Adobe Acrobat for users who are using or will be using the LincPass to digitally sign documents.

By default, Adobe Acrobat 9 and Acrobat Reader 9 are configured to use the Adobe Approved Trust List (AATL) for validating the certificate trust chain of certificates used to digitally sign PDF documents. The AATL is an Adobe hosted resource that contains a list of trusted Certificate Issuers. ***The issuing Certificate Authority for the HSPD-12 PIV certificates located on the USDA LincPass are not present in the AATL. The result is that LincPass digital signatures will not be trusted in Adobe by default.***

Adobe Acrobat 9 and Acrobat Reader 9 should be modified to use the Windows Certificate Store for the purpose of identifying trusted Certificate Authorities. Each agency has already implemented a change to trust the issuing Certificate Authority of the LincPass certificates in the Windows Certificate Store. When this configuration change is implemented, LincPass digital signatures will be recognized as trusted by these Adobe products.

## 2.1 Windows Certificate Store Configuration Change in Adobe

Signing and certificate security workflows require that users obtain and trust other people's certificates. They will use those certificates to trust someone else's signature and to encrypt documents for them. While Adobe Acrobat has its own trusted certificate store (the AATL), using the Windows Certificate Store is recommended for the USDA enterprise. Enabling Windows Integration in Adobe Acrobat 9 and Acrobat Reader 9 will allow Adobe to inherently trust the HSPD-12 PIV certificate issuing authority listed in the Windows Certificate Store.

Adobe is configurable for Windows integration through the application's Preference panel. Configuration options allow users to search the Windows store from the Trusted Identity Manager, set trust levels for any found certificate, and choose which certificates to use for encryption (once the certificate is located and added to the Trusted Identity Manager).

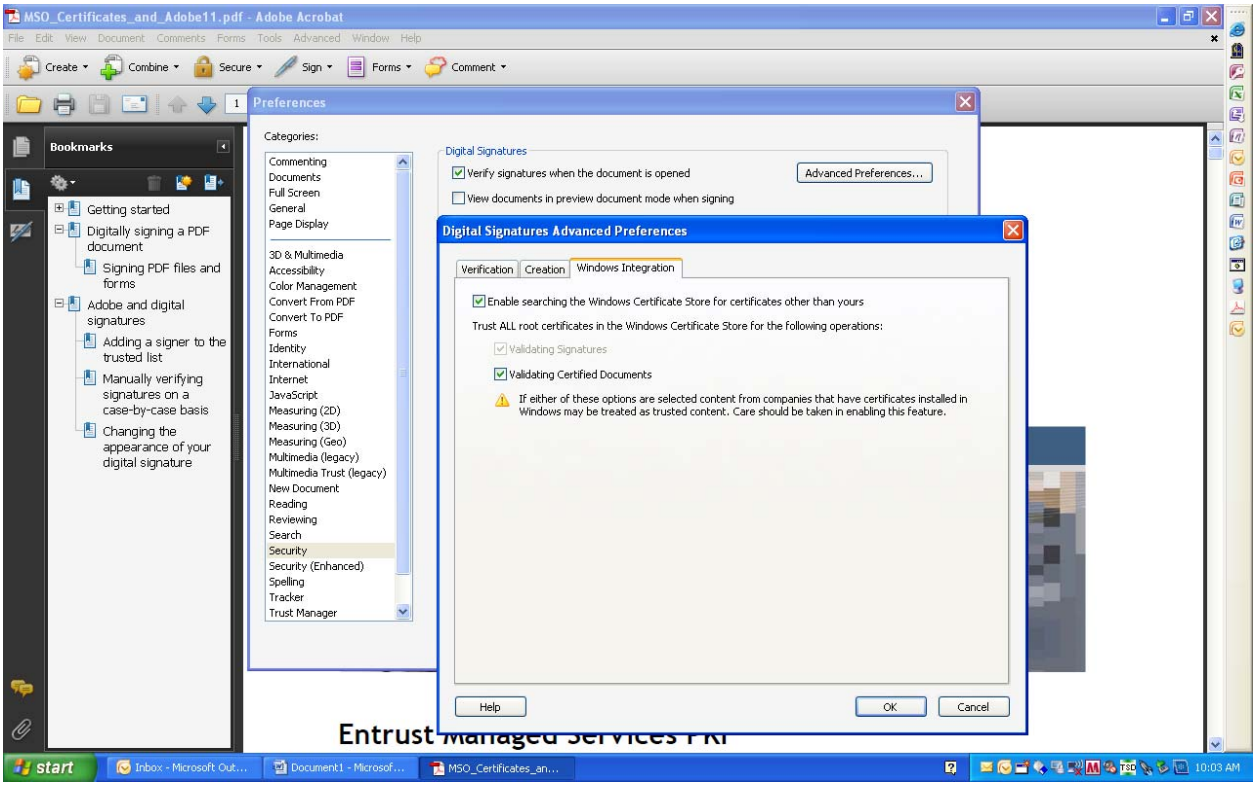
Currently, Adobe has a default setting to certificates from the Adobe Acrobat default certificates store. This current behavior will ask the end user to choose from a list of certificates that does not include the LincPass certificates (Windows Certificate Store), including administrators.

A registry setting can be adjusted to automatically set this required change. This change is outlined below in the Registry Configuration Changes section.

The setting change is applied in Adobe to the Preferences Function at: *"Security – Digital Signatures – Advance Preference – Windows integration"* setting.

Adobe interface setting in the Windows Integration preference areas that needs to be checked:

- Enable searching the Windows Certificate Store for certificates other than yours
- Validating Signatures
- Validating Certificates documents



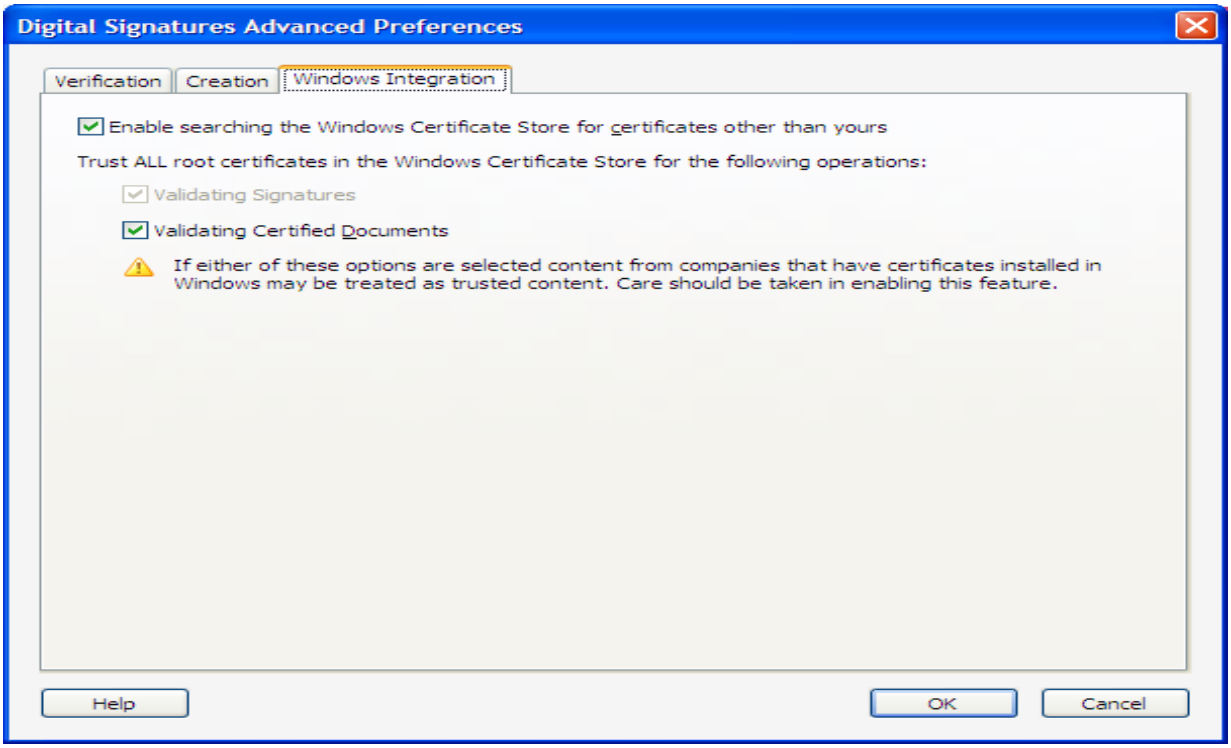



Figure 1 & 2: Screen shot of the preference settings screen for the manual change option.

## 2.2 Windows Certificate Store Registry Configuration Changes

To implement this configuration change via the Windows Registry, the following Adobe Acrobat registry keys must be modified on each client workstation:

Registry Entry Names:

- bCertStoreImportEnable
- iMSStoreTrusted

*This can be done through an SMS push / GPO or another policy setting change tool that your agency may utilize.*

Step # 1

Execute a search for these registry names.

Due to the multiple variations on Operating Systems, and Adobe versions, the most efficient way to locate these settings is to complete a search for them in the registry. The suggested paths below are from an XP operating system and Adobe version 9.0. If you have problems locating these, start at: Software / Adobe / Adobe Acrobat / (the version).

iMSStoreTrusted

*Path: HKEY_LOCAL_MACHINE\Software\Adobe\Adobe Acrobat\<security root>\cASPKI\cMSCAPI_DirectoryProvider*

bCertStoreImportEnable

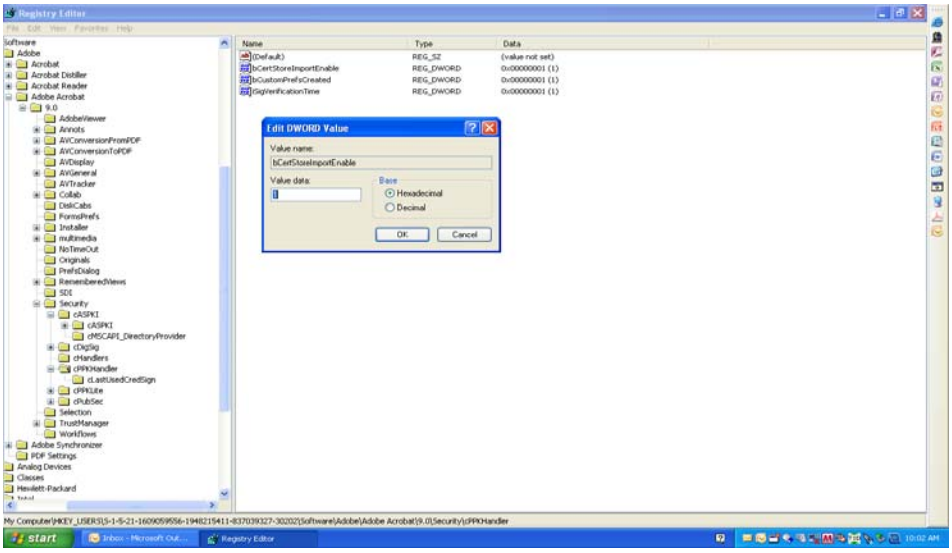
*Path: HKEY_LOCAL_MACHINE\Software\Adobe\Adobe Acrobat\ <security root>\PPKHandler*

Step # 2

Change the registry entries value data to the following:

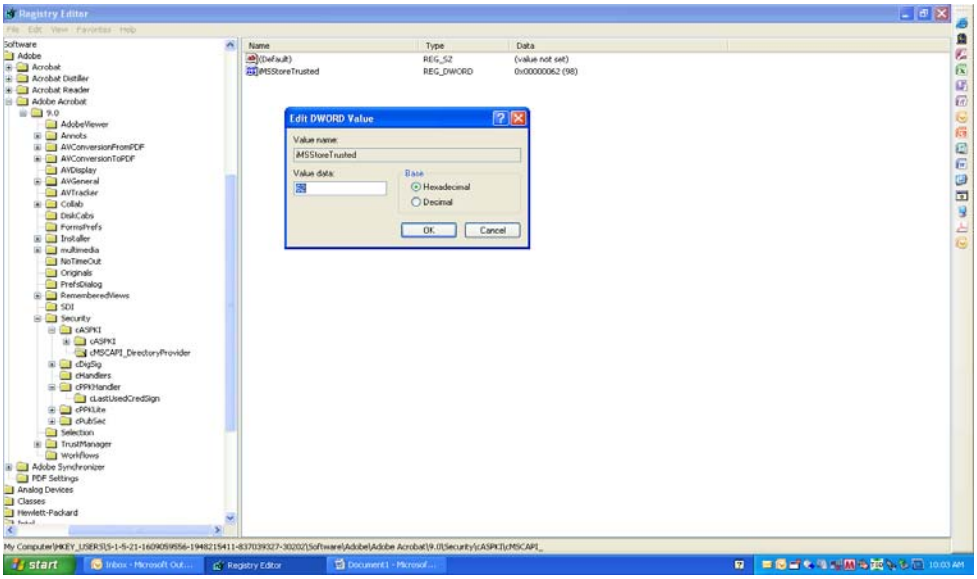
bCertStoreImportEnable "=1"

(The default setting for this item was "= 0")




iMSStoreTrusted '"=62"

(The default setting for this item was "= 0")



Step # 3

Execute a SMS or GPO (or other option your agency may utilize for technical policy changes) policy push to user's machines for both these registry changes.

The table below is supplied from Adobe on the details of the registry changes described above.

| Name | Type | Description |
|---|---|---|
| iMSStoreTrusted | int | (v. 7.0) Default: 0<br>**Path**: <security root>\cASPKI\cMSCAPI_DirectoryProvider<br>Maps to GUI item: **Validating Signatures** and **Validating Certified Documents**.<br>Controls whether or not certificates in the Windows Certificate Store are trusted for signing and certifying.<br>**60**: **Validating Signatures**<br>**62**: **Validating Signatures** and **Validating Certified Documents**.<br>Subject to lockdown as described in "Preventing End-User Modification" on page 84. |
| bCertStoreImportEnable | bool | (v 7.0) Default: 0<br>**Path**: <security root>\PPKHandler<br>Maps to GUI item: **Enable searching the Windows Certificate Store for certificates other than yours**<br>If true, then users can import from MSCAPI certificate stores into their Trusted Identity Manager. |

Figure 1: Excerpt of configuration from *Digital Signatures & Rights Management in the Acrobat Family of Products – Section: 5.2.4 Certificate Management.*

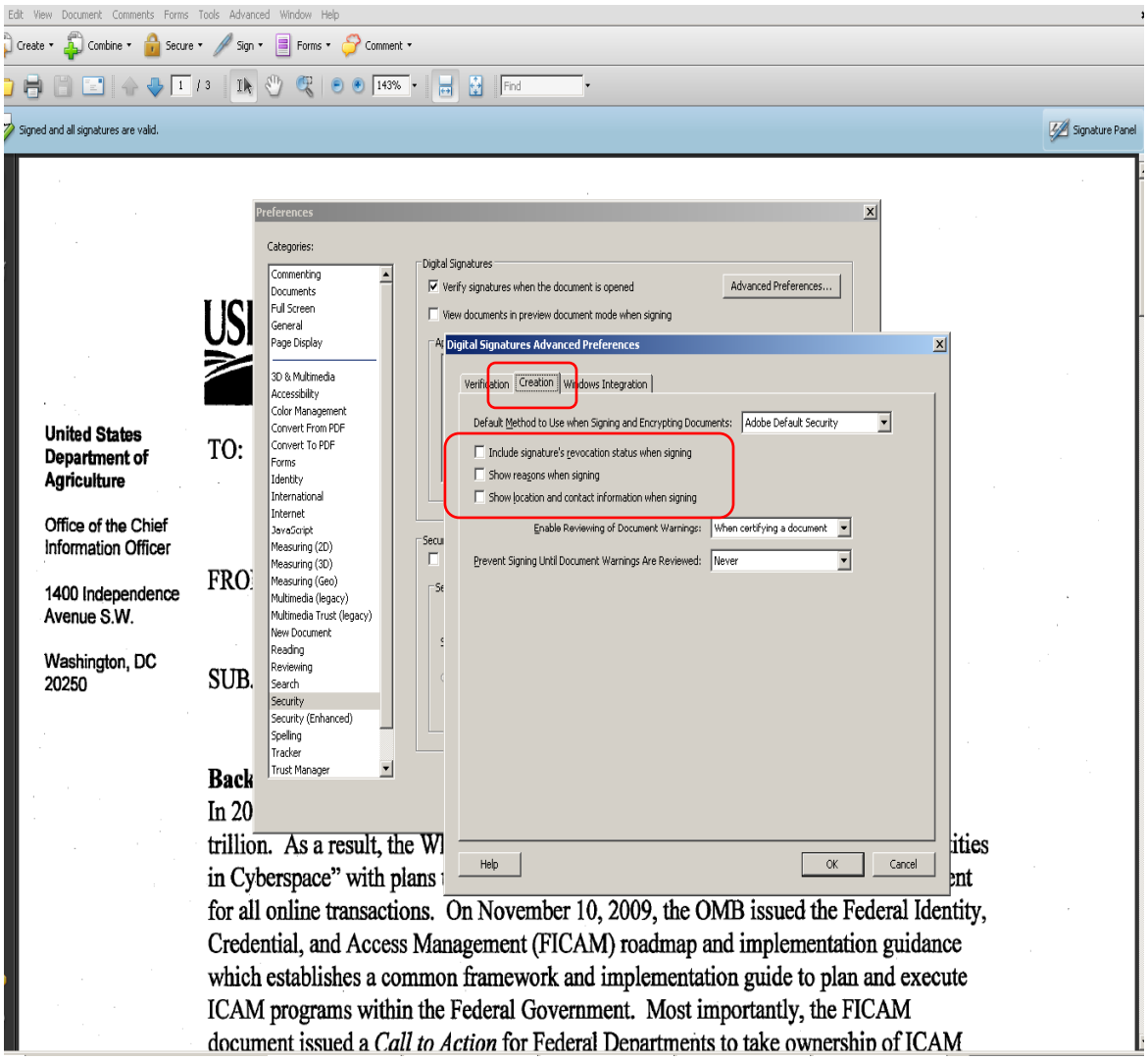
## 2.3 Adobe Signature "Creation" Configuration Change in Adobe

The Adobe default setting for Signature Creation is set to *Include signature's revocation status when signing* for all Adobe documents.

To make storing & sending signed Adobe documents manageable with document size it is recommended that this setting be changed.

The setting change is applied in Adobe to the Preferences Function at: *"Security – Digital Signatures – Advance Preference – Creation"* setting.
*Un-check the following:*

- Include signature's revocation status when signing
- Show reasons when signing
- Show location and contact information when signing



## 2.3 Adobe Acrobat Supporting Document

For more detailed Adobe technical content and direction on this change see the following document from Adobe:

Document Name:
**Digital Signatures & Rights Management in the Acrobat Family of Products**

**Acrobat® Family of Products 9.x**
**Modification date: 5/11/09**

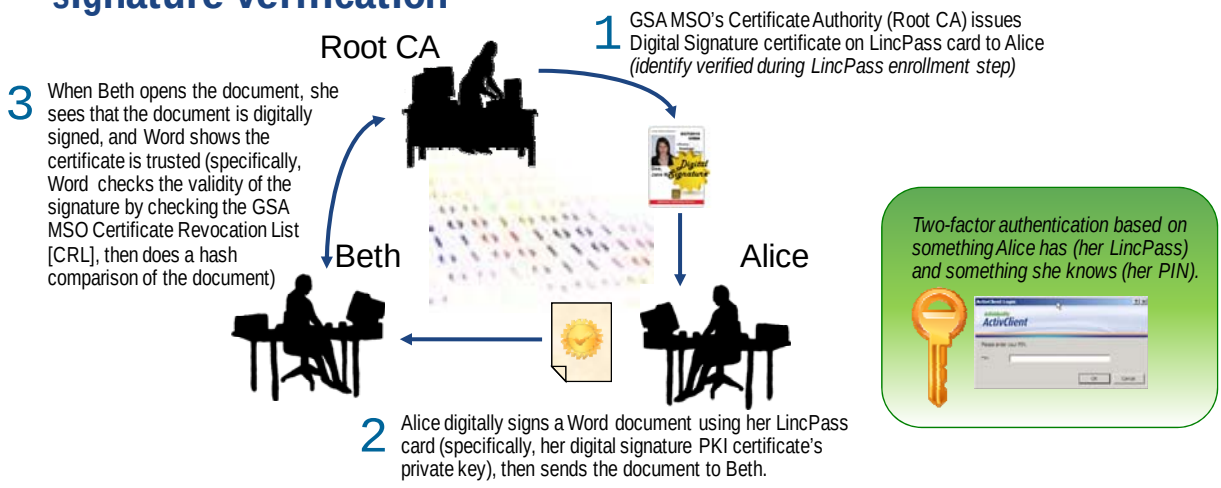
Document section on Certificate Management:
**5.2.4 Certificate Management**

Document URL at Adobe:
http://learn.adobe.com/wiki/download/attachments/52658564/acrobat_reader_security_9x.pdf?version=1

# 3. Digital Signature & PKI

The figure below depicts how USDA's PKI infrastructure supports digital signatures.

- **Public Key Infrastructure (PKI): the mechanism for digital signature verification**




- **The digital signature indicates the document is unchanged since Alice sent it (*any* change to the file destroys the digital signature, therefore, it is non-repudiable)**