Digital Signature Build Dictionary Specification

February 29, 2008

Adobe Solutions Network — http://developer.adobe.com

Digital Signature Build Dictionary Specification

March 2007

Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

Digital Signature Build Properties Dictionary

1 Introduction

This document describes the *build properties dictionary* referenced by the **BuildProp** key of the signature dictionary defined in the PDF 1.7 Reference (see Table 8.102 in Section 8.7 Digital Signatures on page 729) and ISO 32000-1 (see Table 252 in clause 12.8. Digital Signatures). The build properties dictionary shall only be present in signed signature fields, and its contents are implementation-specific by design. The dictionary should be used to store audit information that is specific to the software application that was used to create the signature.

Typical uses for the build properties dictionary can be:

- Auditing the signature by examining the software components and their versions that were used to create the signature.
- Detecting and identifying signatures created with development (pre-release) software.
- Allowing detection of signatures that may have been created with what is later found to be flawed software.

EXAMPLE 1 Use the build dictionary to identify signatures created with some flawed software which does not compute byte range digests correctly.

For PDF versions 1.3 and 1.4, the **R** key in the signature dictionary, referenced earlier, had been used to contain version information that shall now be saved in this build properties dictionary. That key has been deprecated and shall no longer be used. Developer specific information using developer's specific keys (prefixed by their registered prefix) can also be found in signature dictionaries created using those earlier specifications.

EXAMPLE 2 Adobe had been using an ADBE_Build key to store Acrobat specific information.

~~Build information has been defined for signature dictionaries since Acrobat 4.0. The information shall be provided by the value of the R key in the signature dictionary (an integer number representing the version of the signature handler) and ADBE_Build attributes key. The ADBE_Build attribute was insufficient because it is a string with a value that does not have a specified format and it therefore is not machine readable. Hence, the build properties dictionary was added in Acrobat 6.0 to provide more useful information, and use of the ADBE_Build and R attributes were deprecated.~~

NOTE 1 In PDF 1.6, signature build dictionaries could be used to specify that a later software component is required to validate a signature. This capability was removed in PDF 1.7.

~~(M.2) Note to Implementators~~

~~All information in the build properties dictionary is optional. Your PDF signing software implementation should only populate the build properties dictionary with correct information, else you should not add information to this dictionary. For example, if you are writing a signature handler, you should not have a Filter entry in the build properties dictionary with the Name entry set to Adobe.PPKLite. The Name value should be unique to your software implementation.~~

NOTE 2 All information in the build properties dictionary is optional. PDF signing software should only populate the build properties dictionary with information not provided in the digital signatures dictionary.

EXAMPLE 3 A signature handler should not put a **Filter** entry in the build properties dictionary with the **Name** entry set to *Adobe.PPKLite*. The **Name** value should be unique to the software application.

2 Build Properties Dictionary

The build properties dictionary and all of its contents shall be direct objects. A build properties dictionary is optional but should be used.

The build properties dictionary may contain a build data dictionary entry for each unique software module used to create the signature. The software modules involved in the signing process can vary depending on the viewing application. All signing implementations should include at least a **Filter** entry in the build properties dictionary.

Table 1 – Common entries in the build properties dictionary

Key	Type	Value
Filter	dictionary	(*Optional; PDF 1.5)* A build data dictionary (Table 2) for the signature handler that was used to create the ~~parent~~ signature. This entry is optional but be used for all signatures.
PubSec	dictionary	(Optional; PDF 1.5) A build data dictionary (Table 2) for the ~~PubSec~~ software module that was used to create the ~~parent~~ signature.
App	dictionary	(*Optional; PDF 1.5)* A build data dictionary (Table 2) for the viewing application software that was used to create the ~~parent~~ signature.
SigQ	dictionary	(*Optional; PDF 1.7)* A build data dictionary (Table 2) for the PDF/SigQ Conformance Checker that was used to create the ~~parent~~ signature. This entry is present only if the document conforms to the version of the PDF/SigQ definition indicated by the upper 16 bits of the **R** entry in this dictionary.

3 Build Data Dictionary

The build data dictionary shall contain information from the signature handler or software module that was used to create the signature. Not all entries are relevant for all entries in the build properties dictionary.

Table 2 – Common entries in build data dictionaries

Key	Type	Value
Name	name	(*Optional; PDF 1.5)* The name of the software module used to create the signature. When used as an entry in the data dictionary of the **Filter** attribute (Table 1), the value shall be the name of the signature handler. The value should be equal to the value of the **Filter** attribute in the signature dictionary.
Date	text string	(*Optional; PDF 1.5)* The software module build date. This string may be produced by the compiler that is used to compile the software, for example using the Date and Time preprocessor flags. As such, this is not likely to be in PDF Date format.
R	number	(*Optional; PDF 1.5)* The software module revision number. It is important that signature handlers and other software modules specify a unique value for **R** for every publicly available build of the software. If the module or handler is ever found to have been defective, for signatures where the value of **PreRelease** is **false**, the value of this attribute is likely to be the only way to detect that the signature was created with the defective release. A sample value might be 0x00020014, for software module version 2, sub-build 0x14. Various software modules may use this entry differently. ~~When present in the SigQ build data dictionary, the upper 16 bits of this value indicate the version of PDF/SigQ to which the viewing application's PDF/SigQ Conformance Checker was written, and the lower 16 bits indicate the implementation version for the Conformance Checker.~~

Table 2 – Common entries in build data dictionaries

Key	Type	Value
PreRelease	Boolean	(*Optional; PDF 1.5)* A flag that may be used by the signature handler or software module to indicate that this signature was created with unreleased software. If **true**, this signature was created with pre-release or otherwise unreleased software. The default value shall be **false**.
OS	array	(*Optional; PDF 1.5)* Array of text strings. Indicates the operating system, such as *Win98*. Currently there is no specific string format defined for the values of this attribute.
NonEFontNoWarn	Boolean	(*Optional; PDF 1.5)* If there is a **Legal** dictionary in the catalog of the PDF file, and the **NonEmbeddedFonts** attribute (which specifies the number of fonts not embedded) in that dictionary has a non-zero value, and the conforming reader has a preference set to suppress the display of the warning about fonts not being embedded, then the value of this attribute will be set to **true** (meaning that no warning need be displayed).
TrustedMode	Boolean	(*Optional; PDF 1.5)* If the value is **true**, the application was in trusted mode when signing took place. The default value shall be **false**. A viewing application is in trusted mode when only reviewed code is executing, where reviewed code is code that does not affect the rendering of PDF files in ways that are not specified by ISO 32000.
V	number	(*Optional; PDF 1.5; Deprecated for PDF 1.7)* Shall indicate the minimum version number of the software required to process the signature. (This attribute introduced behavior that was not consistent with the PDF 1.7 requirement of being independent of software implementation. Use of this attribute is now deprecated.

Table 3 – Additional entries in the build data dictionary when used as the App dictionary in a build properties dictionary (Table 1)

Key	Type	Value
REx	text string	(*Optional; PDF 1.6)* A text string indicating the version of the application implementation, as described by the **Name** attribute in this dictionary.

Table 4 – ~~Additional entries in the build data dictionary when used as the SigQ dictionary in a build properties dictionary (Table 1~~)

Key	Type	Value
Preview	Boolean	(*Optional; PDF 1.7)* Shall indicate whether the document was viewed using the signature preview mode when signed. If the viewing application does not support a signature preview mode that conforms to the PDF/SigQ definition, this attribute shall not be set or shall be set to **false**. The default value shall be **false**.

Table 5 – Common entries in the build properties dictionaries (Table 1)

Name	Properties Used
Filter	**Name** (extracted from handler; for example, **Adobe.PPKLite** or **Adobe.PPKMS**), **Date**, **R**, **PreRelease**.
PubSec	**Date**, **R**, **PreRelease**, **NonEFontNoWarn.**
App	**Name** ~~(one of Adobe.Reader or Adobe.Pro, or Adobe.Standard)~~, **R**, **OS**, **TrustedMode**, or **REx** ~~(added in Acrobat 7.0.5)~~.
SigQ	**R, Preview** (~~both added in Acrobat 8.0)~~.

Table 2 and Table 1 show a standard set of keys that collectively may be used in build data dictionaries. Table 2 shows which keys shall be appropriate for those specific dictionaries that are values of the keys in a build properties dictionary.

EXAMPLE

```
/Prop_Build
<<
    /Filter
        <<
            /Name /Adobe.PPKLite
            /Date (Sep 27 2006 00:11:15)
            /R 131101
            /PreRelease true
        >>
    /PubSec
        <<
            /Date (Sep 27 2006 00:05:54)
            /R 13102
            /NonEFontNoWarn true
            /PreRelease true
        >>
    /App
         <<
             /Name /Exchange-Pro
             /R 524288
            /REx (8.0.0)
             /TrustedMode true
             /OS [/Win]
            /Name /Adobe.Reader
            /TrustedMode false
            /R 63454
        >>
    /SigQ
        <<
            /R 65536
            /Preview true
        >>
>>
```