Using Digital Signatures in SAP® QM to Meet Regulatory Requirements

By Carl Dunlap, Cohesion, Inc.

This article was provided exclusively to SearchSAP.com by SAPtips, an online, subscription-based publication dedicated to SAP implementation and optimization. To preview additional SAPtips publications or to request a sample issue of SAPtips, go to http://www.SAPtips.com.

Editor's Note: For SAP customers, this is the age of "compliance." From Sarbanes-Oxley to GMP to the FDA's 21 CFR Part 11, it seems that every SAP user in every industry has some type of regulation that its SAP system must adhere to. Some of those regulations pertain to digital signatures, and the good news here is that if you implement SAP's digital signatures properly, you can achieve compliance with regulatory requirements, while also improving your company's workflow and document processing efficiency. To tackle this important subject, we are pleased to welcome Carl Dunlop, a QM functional expert who has dealt with digital-signature issues for a range of SAP users in health care and manufacturing. In this hands-on, illustrated guide, Carl walks us through the steps for installing SAP's digital signature functionality. He surrounds this content with an excellent overview of the latest FDA/digital signature requirements and how SAP has responded to its customers who are concerned about digital signatures and the need to be on the right side of "compliance."

Many SAP customers would like to "electronically sign" records within SAP. SAP includes standard functionality for the "Digital Signature" (also referred to as an "electronic signature") in Quality Management (QM) as well as other relevant areas (e.g. Document Management and Engineering Change Management). This functionality ensures that the users performing the transaction validate their unique identities when approving electronic records.

Of course, SAP users can't benefit from the use of digital signatures if they are not in accord with the latest regulatory guidelines. In recent years, regulatory bodies have instituted regulations and compliance guidelines for digital signatures. Perhaps the most significant of these guidelines was issued by the FDA. In March of 1997, the FDA issued part 11 of Title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures (otherwise known as 21 CFR Part 11). Part 11 provides criteria for acceptance by the FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. These regulations, which apply to all FDA program areas, were intended to permit the widest possible use of electronic technology, compatible with the FDA's responsibility to protect the public health.

Section 11.5 of the rule states:

Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

- The printed name of the signor

- The date and time stamp when the signature was executed, including the date and time local to the signor when multiple time zones are involved

- The meaning associated with the signature (such as review, approval, responsibility)

Using Digital Signatures in SAP® QM
to Meet Regulatory Requirements

This information is excerpted from:

Final Rule on Electronic Records and Electronic Signatures, 21 CFR Part 11, issued by the FDA, which can be found at:

http://www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf

Note: In August 2003 the FDA issued Draft Guidance on 21 CFR Part 11. This guidance document can be found at:

http://www.fda.gov/cder/guidance/5667fnl.pdf

On my consulting assignments, I've had the opportunity to implement digital signature functionality within SAP QM that abides by the latest FDA requirements. This white paper will show a "real-word" example of how the digital signature in Resulting Recording and Usage Decision can be used to satisfy the requirements of the Food and Drug Administration regulations regarding electronic records and electronic signatures—specifically 21 CFR Part 11.

Of course, digital signatures have many applications beyond compliance with 21 CFR Part 11. Many pharmaceutical producers, medical device makers, and food-related companies that use SAP can benefit from this standard functionality. The Digital Signature can also be used to meet GMP guidelines (Good Manufacturing Practices) for the approval of quality-related processes and documentation. This "hands-on" white paper will walk you through the specific configuration and master data that must be set up to enable the digital signature in QM Results Recording and Usage Decision.

Although many SAP customers turn to third-party products to deal with their digital signature authorizations, readers will be glad to know that starting with SAP version 4.6c, SAP's core R/3 product supports digital signature authentication (via R/3 User ID and Password) without the need for a third-party product. As this white paper demonstrates, the "out of the box" functionality that ships with R/3 is all you need to work digital signatures into your QM business processes.

For many SAP customers the "out of the box" functionality for digital signature should meet their requirements, particularly in closed systems. If another level of authentication is required, or the system is open to partners and customers, SAP supports the integration of external security products (i.e., smart card readers) and the use of public-key technology via the Secure Store & Forward (SSF) interface (starting with SAP version 4.0b). This is particularly relevant in SAP applications where digital information is exchanged electronically (i.e., electronic invoices) across enterprise boundaries.

In these cases, there are two keys involved. The document is signed using a private key, and the signature is verified using a public key. The private key can be stored on a computer (PC or server) or on a separate piece of hardware like a smart card. This white paper will focus on "single key" digital signature authentication. Depending on reader interest, we can potentially follow up this white paper with a look at the more complex "double key" authentication scenarios.

I. Background on Electronic or "Digital" Signatures

SAP defines a "Digital Signature" in the online documentation as follows:

Logistics - General (LO)

Equivalent to a handwritten signature for the processing of digital data.

The digital signature ensures that:

- *The signed transaction can only be carried out by users with a special authorization*

- *The signatory identification is unique and forgery-proof*

- *The signatory name is documented together with the signed transaction and the date and time, and cannot be falsified*

The Quality Management (QM) application component uses the simple signature. This means, that a document is signed or approved by the signature of a single authorized person. You can use the digital signature for the following functions:

- *During results recording*

- *At the usage decision*

- *When confirming the physical-sample drawing. This means, when releasing the first physical sample in a physical-sample drawing.*

This information is excerpted from:

http://help.sap.com/sapdocu/core/47x200/HELPDATA/EN/04/ec1003c3c811d182c90000e8323965/frameset.htm

II. Configuration (using the IMG)

General Settings:

In order to use the Digital Signature functionality, you must first define the "General Settings."

A) Time Zones (standard SAP setting should suffice here—see Figure 1)

```
Structure
 ▽ 🗎    SAP Customizing Implementation Guide
    🗎 🕓  Activation Switch for SAP R/3 Enterprise Extension Set
  ▽ 🗎     General Settings
     ▷ 🗎     Set countries
     ▷ 🗎     Setup Geocode
     ▷ 🗎     Currencies
        🗎 🕓  Check units of measurement
        🗎 🕓  Maintain calendar
        🗎 🕓  Maintain Calendar for Japan
     ▽ 🗎     Time Zones
           🗎 🕓  Maintain System Settings
           🗎 🕓  Maintain Time Zones
           🗎 🕓  Maintain Geographical Assignments
```
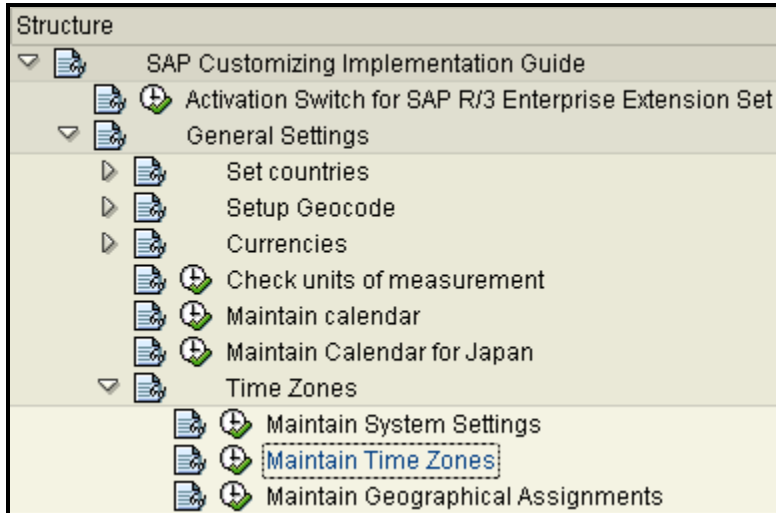
Figure 1: Maintain Time Zone

B) Assign Personal Time Zone (maintain User Defaults)

The "Personal Time Zone" for your User ID must be maintained. This assures that the signature date and time are correct for the individual user who "signs" the document.

This can be done using the following menu path *System → User profile → Own data (or transaction SU3.* Make sure to click on the "Defaults" tab (see Figure 2).
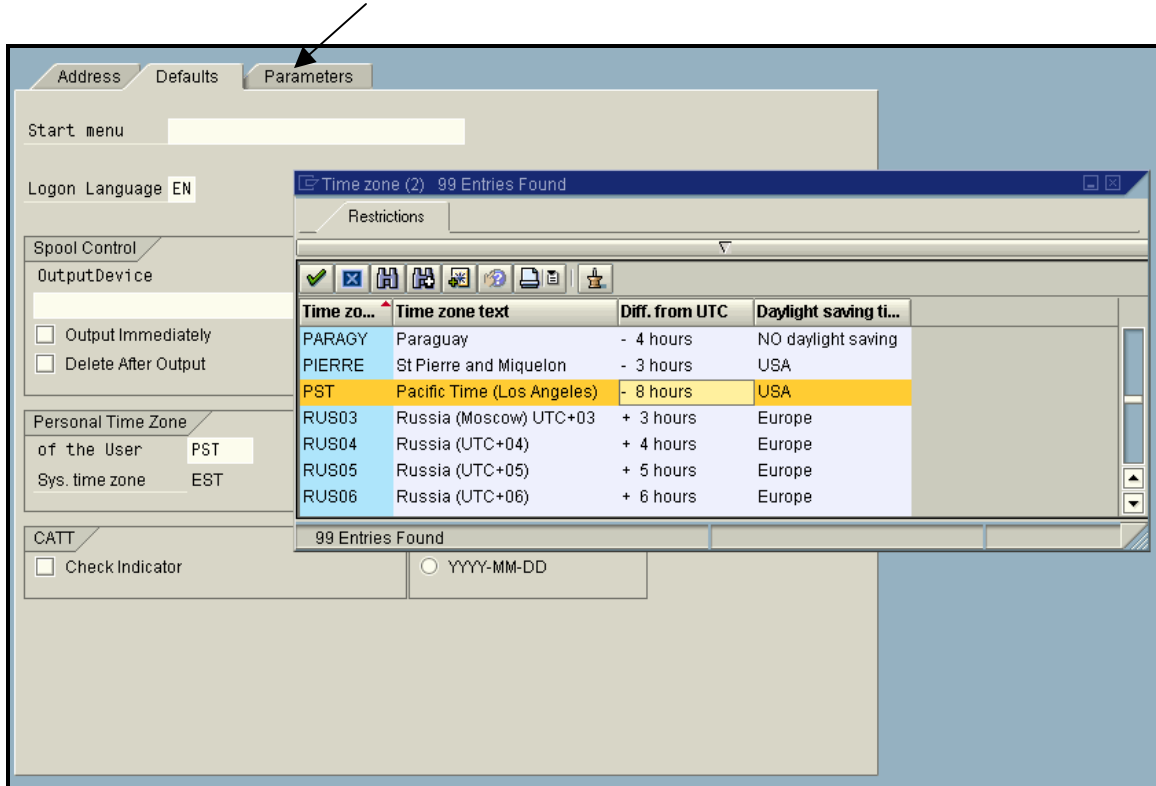
Figure 2: Assign Personal Time Zone to User ID

In this example, the system time zone is Eastern Standard Time (EST), but my user is located in California on Pacific Standard Time (PST).

C) Signature Method

There are two main options for the Signature Method (Listed below as 1. and 2.). For this white paper, we use Option 1 (System signature with authorization by SAP User ID and password). This option is only available from R/3 Version 4.6c forward.

1. System signature with authorization by SAP User ID and password

As noted by SAP: "Here, you do **not** need an external security product. Just like when logging on to the system, users identify themselves by entering their User IDs and passwords. The SAP system then executes the digital signature. The user name and ID are part of the signed document." -http://help.sap.com

This signature method is available "out of the box" and requires no additional hardware.

To configure the signature method, use the IMG to navigate to "Define Authorization Groups and Digital Signature" (see Figure 3).
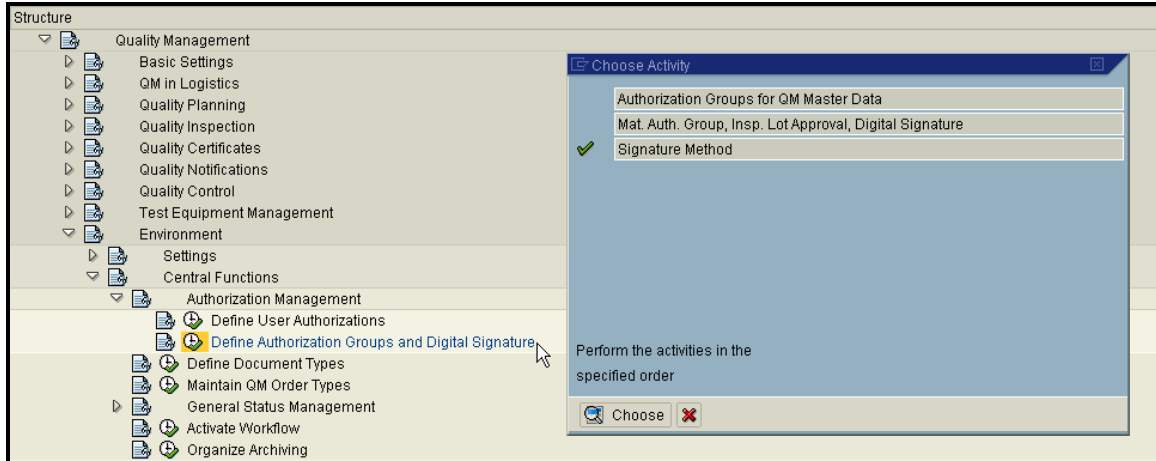
Figure 3: IMG Menu Path to Signature Method

Once in the "Specify Signature Method for Simple Signature" Table, click on the "New Entries" button.

In the Signature object type field, we select the entries for "Inspection Lot: Results Recording" and "Inspection Lot: Usage Decision" (see Figure 4).
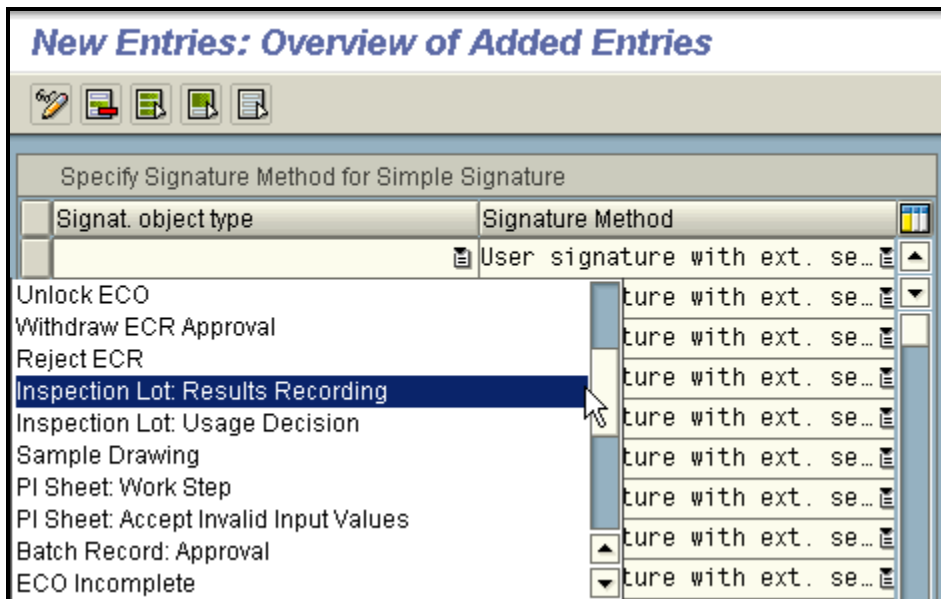
Figure 4: Assign Signature Object Type

In the Signature Method, field we select "System signature with authorization by R/3 user ID/password" (see Figure 5).
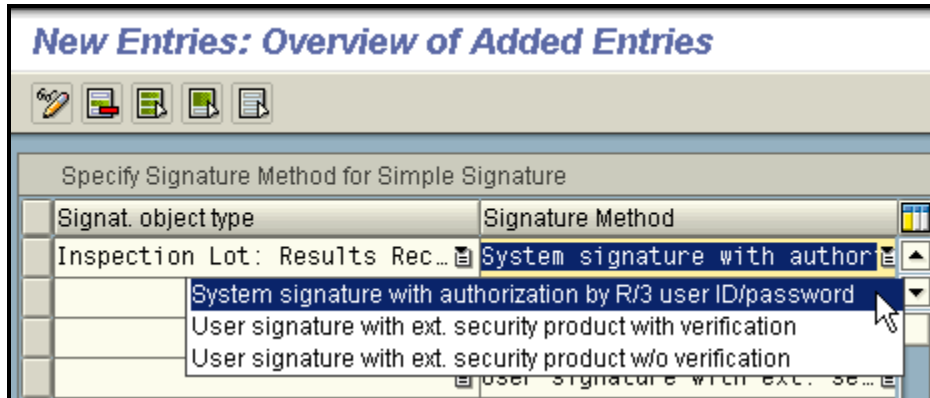
Figure 5: Assign System Signature as Method

When finished, the two rows you added should look like this:

Figure 6: Two Added Entries

2. User signature with and without verification

SAP notes: "Here, you need an external security product. Users execute digital signatures themselves using their private keys. The signature created by the security product is automatically checked for authenticity." This is done using the Secure Store and Forward (SSF) interface, which makes use of Public-Key Cryptographic Standards (PKCS).   http://help.sap.com

*NOTE - In this white paper, we do NOT use an external security product; therefore I will not detail the customizing settings for the (SSF) interface. For reference, they can be found in the IMG under: *SAP Web Application Server → System Administration → Digital Signatures (menu path for SAP 4.7)*

D) QM Material Authorization Group:

Quality Management (QM) in SAP is primarily a material-based system. The QM view of the Material Master is set up at an "organizational level" of "Plant." This means that the general Quality Control settings are activated based on a combination of Material and Plant. The case with digital signatures is also the same. In order to activate the digital signature in QM, you must

configure an authorization group in the QM View of the Material Master. This can be done in the following area of the IMG (same menu path as for Signature Method—see Figure 7):
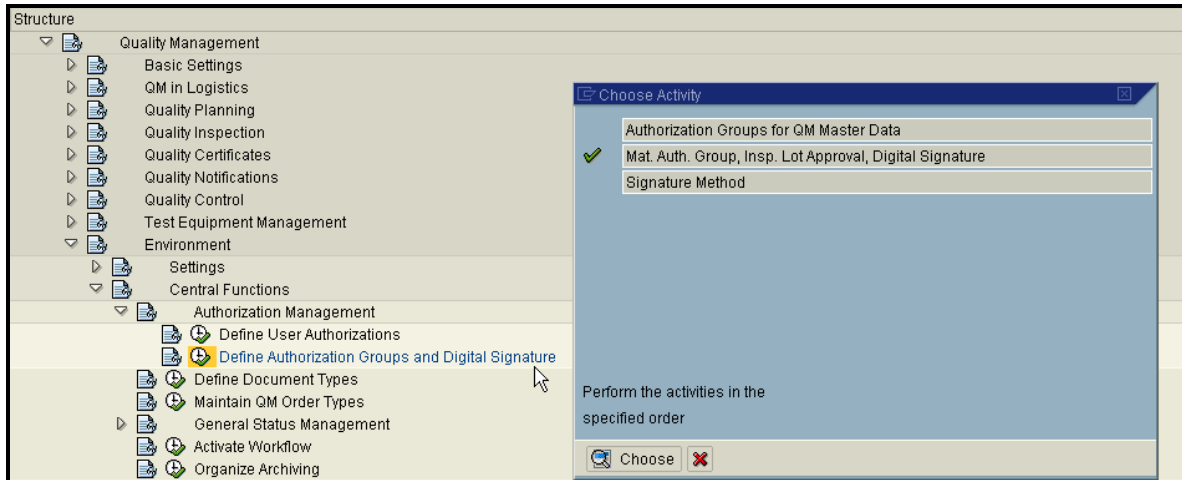
Figure 7: IMG Menu Path to Mat. Auth Group

In this table, you can change an existing entry or add a new entry to create a QM Material Authorization Group based on your requirements. For our example, we will add QM Material Authorization Group **000099** with the following settings:

- Approval for Inspection Lot – **approval not required**
- Digital Signature in Results Recording – **required for results recording**
- Digital Signature at Usage Decision – **required for making the usage decision**
- Digital Signature for Sample Drawing **– not required**

Figure 8: Entry Added for Digital Signature at RR & UD

Although not used in this white paper, notice that there is the ability to require a digital signature for the approval of the inspection lot and the physical sample drawing. The "Approval insp. lot" setting can require a digital signature for the approval of an inspection lot and depends on

whether a task list (i.e., inspection plan) or material specification is used. There is also the ability here to require a digital signature for the confirmation of a physical sample drawing.

Additionally, there is NOT a setting for Quality Notifications in this table. (Quality Notifications are not always based on a Material.) The digital signature for Quality Notifications is currently not available in Standard SAP (as of Release 4.7). This functionality could be added via a Business Add-In or "BAdI" as some SAP customers have done.

III. Master Data

A) Adding the QM Material Auth. Group to the QM View of the Material

Next we will add the QM Material Auth Group that we just created in Configuration to the QM View of the Material Master. As I stated earlier, the QM View is set up at an Organizational level of plant. I have an existing Material Master 10005723 that we will change via Transaction **MM02** (see Figure 9**)**.
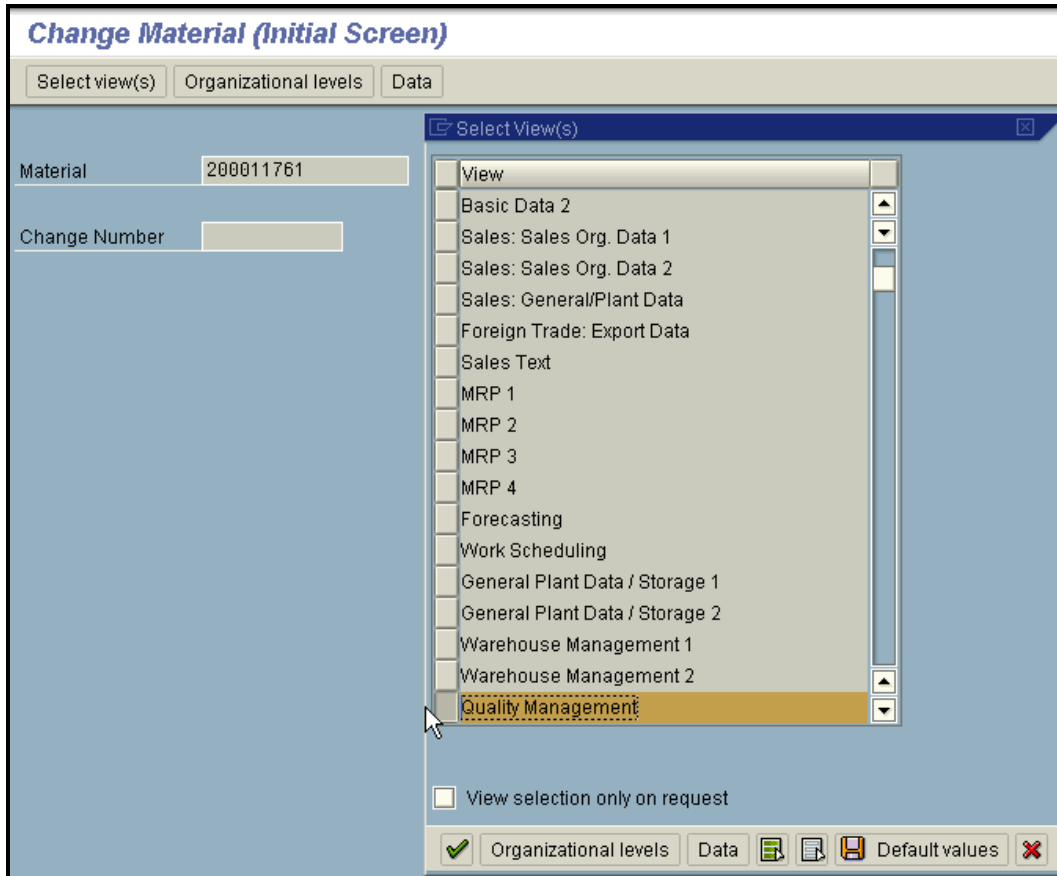

Figure 9: QM View of Material Master

Next, select the plant at which you want to change the QM Settings:
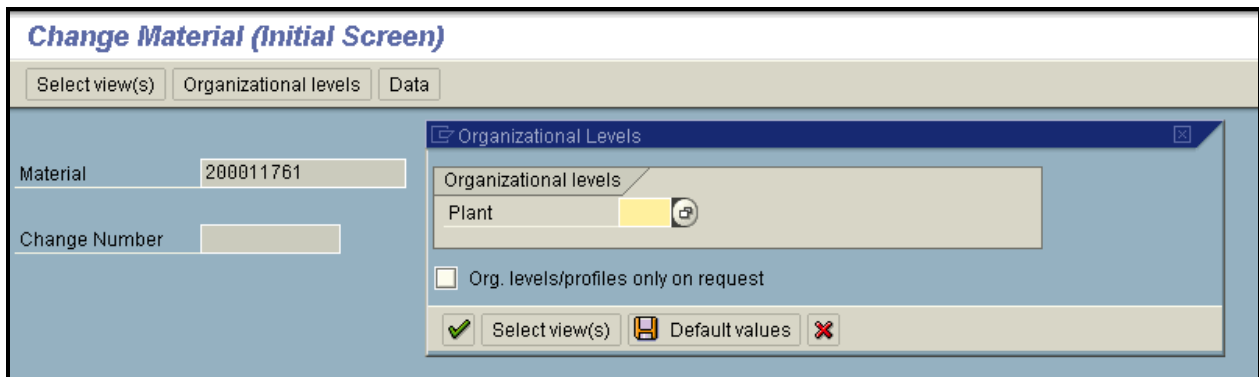
Figure 10: Organizational Level of Plant

Then, add QM Material Authorization Group 000099:
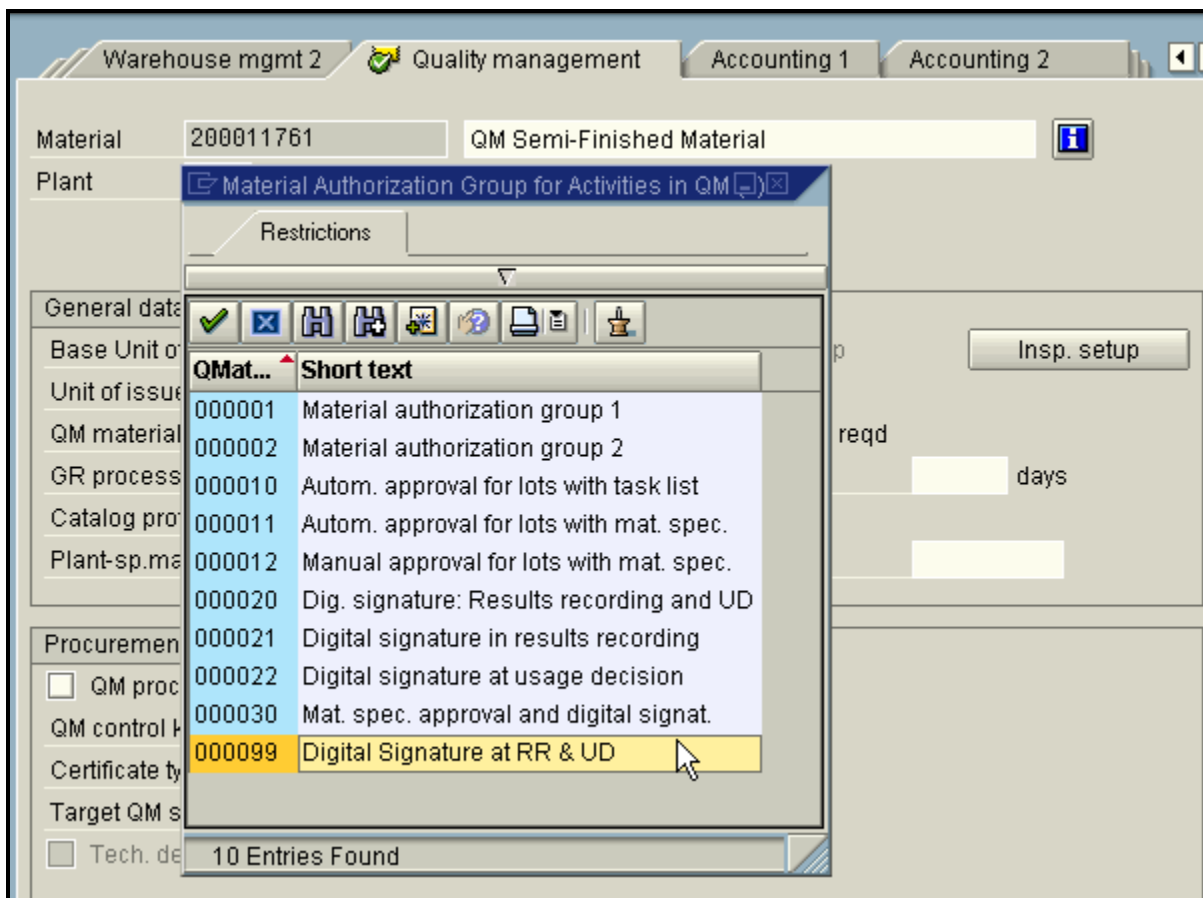
Figure 11: QM Auth Group in Material Master

QM Auth Group. **000099**, which we created earlier, will require a Digital Signature anytime we record results or make a usage decision for an inspection lot (for this material/plant combination—see Figure 12).

Figure 12: Entry Added

B) Reviewing the Inspection Data Setup:

In order to use the digital signature functionality, we must have the material set up to create an inspection lot. In this example, we have a Material Master that represents a semi-finished material that requires inspection at Goods Receipt from Production. In order to see the settings maintained for this material, click on the "**Insp. setup**" button:

Figure 13: QM Inspection Data Setup

You can see in the above screenshot that I have added Inspection Lot Origin 04 and activated it. The details for Inspection Lot Origin 04 are shown in the bottom half of the screen. In this example, we require that SAP create an inspection lot for the Goods Receipt from a production order and allow "early lot creation" at Production Order Release.

IV. Inspection Processing (Results Recording & Usage Decision)

In order to see the digital signature functionality in action, I have created an inspection lot.

A) Digital Signature at Results Recording

The digital signature for results recording happens at the time the user saves the results for the Operation (digital signature is at the Operation Level). In this example, a digital signature is required for results recording (for the material/plant combination). This means that when the results are saved, SAP will now ask the user to verify his unique identity. A digital signature will be required for every operation that results are recorded against (e.g., 3 Operations = 3 Signatures). SAP will automatically record the associated Inspection Lot and Operation number in the "remarks" section:

Figure 14: Digital Signature for Results Recording

The digital signature method we are using utilizes the SAP User ID and Password. This means that the person recording the results must enter their unique User ID (Signatory) and its associated Password in order to proceed. SAP will verify that the password is correct for that User ID, and then execute the digital signature—at which time the user name and ID become part of the signed document. If the password is incorrect, SAP will issue a message and allow the user to try again (up to the number of allowed attempts configured). In the case of too many failed attempts, SAP will lock the User ID.
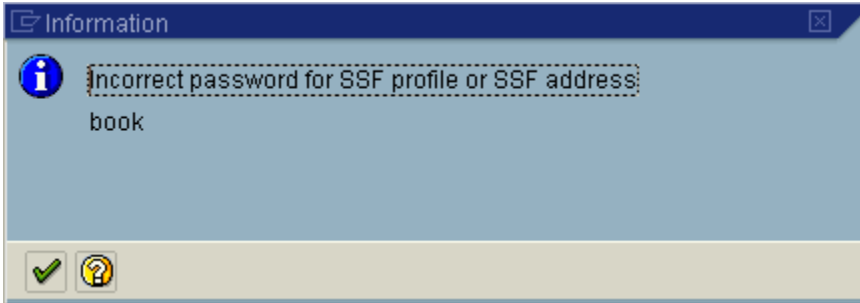
Figure 15: Error, Incorrect Password

It is possible to change the signatory to another User ID (the password must be correct for that User ID). This can be helpful in the case where a supervisor may need to sign off the results for one of her inspectors. The "Comment" section can be used for documentation.

B) Digital Signature at Usage Decision

The digital signature at Usage Decision happens at the time the user saves or changes a Usage Decision (transaction QA11 and QA12). This can happen for the stock posting or Usage Decision Code.

When the Usage Decision is saved, the Digital Signature box will appear:
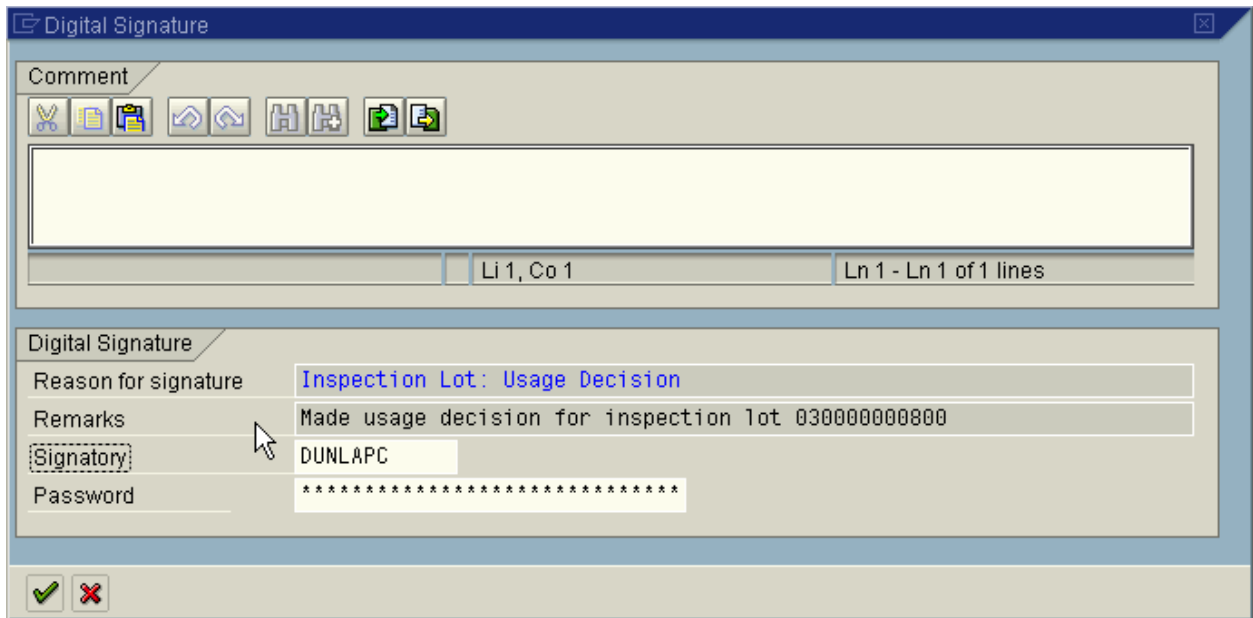
Figure 16: Digital Signature at Usage Decision

SAP automatically records the inspection lot number. The user can enter comments if needed and again must enter his unique User ID (Signatory) and its associated Password in order to proceed.

V. Audit Trail

A) Digital Signature Logs

Lastly, SAP provides a transaction to review the digital signature logs. This is accessed via Transaction **DSAL**. As this is a common transaction that is used for multiple applications, you must select the application "inspection lot" to narrow down the entries (see Figure 17).

Figure 17: Digital Signature Logs (Selection Screen)

Using this transaction, you can search for signatures of a particular Signatory (User ID), as well as look for signatures for a particular Date Range or Inspection Lot (see Figure 18). The transaction can also find unsuccessful attempts (e.g., user locked, wrong password, etc.).

Display logs

Date / Time / Signatory	Jumbe	Inspection Lot	Ind.UDtype	Version	Node	
▽ 📁 Logs on inspection lot						
🔴 01/02/2004 23:16:54 DUNLA(	1	030000000800			00000001	
🟢 01/02/2004 23:21:54 DUNLA(	1	030000000800			00000001	
🟢 01/02/2004 23:27:34 DUNLA(	1	030000000800	L		00000000	

Ty...	Message Text	Add.info to signature reason	Reason for signature
🟡	The digital signature was executed successfully by user DUNLA...	Made usage decision for inspection lot 030000000800	Inspection Lot: Usage Decision

Figure 18: Digital Signature Log (Output)

The following log shows the successful signature for the usage decision—notice that the Global date/time of the signature differ from Local signature date/time:

Last name, first name	Dunlap, Carl
Last name, first name	Dunlap, Carl
Global date of signatu	01/03/2004
Global time of signatu	07:27:34
Local signature date__	01/02/2004
Local signature time__	23:27:34
Date_____	
Time_____	
Add.info to signature	Made usage decision for inspection lot 030000000800

Figure 19: Digital Signature Log (Detail)

VI. Conclusion

In the past, SAP customers have found it challenging to prove that the Inspector who logged onto their SAP system was indeed the same Inspector (User) who recorded the results. This can often happen because many SAP users share a common desktop PC and leave it logged-on to SAP under one user's account. With the digital signature, a user is required to enter the signatory/password combination that is only known to that user. The value here is that the "digital signature" proves to the business and regulatory authorities that the inspectors entering results in QM are who they say they are (just as an inspector's stamp or written signature would).

As mentioned at the beginning of the white paper, the digital signature also helps SAP customers meet GMP guidelines as well as FDA 21 CFR Part 11 (for customers in the medical industry). Although the FDA is currently revising 21 CFR Part 11, they fully expect that companies using electronic records will take the needed steps to be in full compliance when the latest guidelines are released. As non-compliance can lead to fines and costs in millions of dollars, the cost of ignoring these issues can be steep. SAP, as well as their customers, has made compliance a priority.

As of release 4.7, SAP supports even more business processes with the digital signature functionality. SAP has also released a new generic digital signature tool (in R/3 version 4.7) that allows SAP customers to implement their own application-specific digital signatures. For example, this functionality could be used to add digital signatures to the approval process of a Quality Notification. With this new functionality, SAP has given its customers a great opportunity to use digital signatures to improve their business processes and be in compliance with the latest federal regulations.

Carl Dunlap, President of Cohesion, Inc (http://www.cohesion.biz). Carl has nine years of SAP QM experience from version 2.2c to 4.7 and has worked on over 25 SAP Projects Worldwide. In additional to Platinum Level QM consulting at Cohesion, Carl also manages software license sales of the Cohesion Reportlet Suite for SAP (a software product that allows SAP users to view and customize standard and Custom SAP ABAP reports within an Enterprise Portal, Intranet, or Website).

Prior to founding Cohesion, Carl worked as the Senior Business Development Manager for Enterprise Applications at Plumtree Software. Previous to Plumtree, Carl held the position of Practice Leader and Business Development Manager for BrightStar's SAP & Siebel practice. Carl came to BrightStar through the 1998 acquisition of Total Business Quality Associates, Inc. (TBQ, Inc.), an SAP Consulting firm he co-founded. Before founding TBQ, Inc., Carl was employed as a Senior Consultant for SAP America. While at SAP, Carl was vital to the creation of the SAP University Alliance Program. Carl's email address is: carl@cohesionportals.com

The information in our publications and on our Website is the copyrighted work of Klee Associates, Inc. and is owned by Klee Associates, Inc.

NO WARRANTY: This documentation is delivered as is, and Klee Associates, Inc. makes no warranty as to its accuracy or use. Any use of this documentation is at the risk of the user. Although we make every good faith effort to ensure accuracy, this document may include technical or other inaccuracies or typographical errors. Klee Associates, Inc. reserves the right to make changes without prior notice.

NO AFFILIATION: Klee Associates, Inc. and this publication are not affiliated with or endorsed by SAP AG. SAP AG software referenced on this site is furnished under license agreements between SAP AG and its customers and can be used only within the terms of such agreements. SAP AG and mySAP are registered trademarks of SAP AG.

All other company and product names used herein may be trademarks or registered trademarks of their respective owners.