

SUMMARY

OnBase Digital Signatures allows users to digitally sign OnBase documents to ensure their authenticity and integrity. Digital signatures use cryptographic procedures to determine whether a document has changed in any way since the signature was applied, making certain the document remains secure and unaltered. Through its tight integration with OnBase Workflow, Digital Signatures can be applied as an additional validation measure during any approval process.

KEY BENEFITS

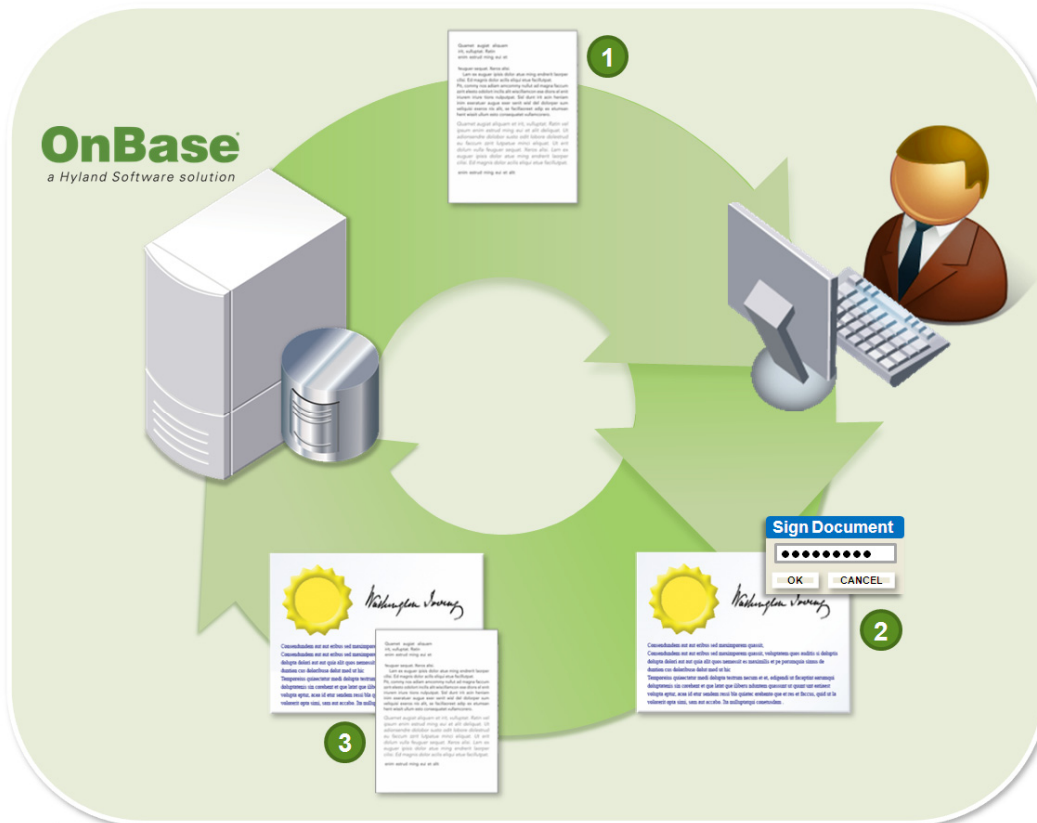
- **Securely sign documents** inside OnBase without the risk of paper being altered or placed in the wrong hands
- **Guarantee that a document has not been altered** since the signature was applied
- **Ensure proof** that a document has been signed by a designated signor or user
- **Increase efficiency** by allowing a user to electronically sign a document without printing, signing and disposing of paper
- **Automatically route documents** using Workflow processes
- **Accommodate** both internally generated and third party certificates

BUSINESS APPLICATION

- **Human Resources:** As part of the hiring process or in terminating an employee, Human Resource employees must acknowledge, approve and authorize a number of sensitive documents. To make sure the documents have not been compromised – that no forgeries or alterations have occurred – HR staff can employ Digital Signatures to ensure the integrity of employee reviews, benefit policies and other employee documentation.
- **Healthcare Registration** - Digital Signatures can be used in conjunction with Front Office Scanning to provide a front-end user interface that ensures registration documents are collected and protected by the registration office. After all of the necessary documents are captured, the admitting nurse can apply batch apply a Digital Signature to the entire package, verifying the accuracy and completion of all needed registration documents.

DESIGN

Digital Signatures

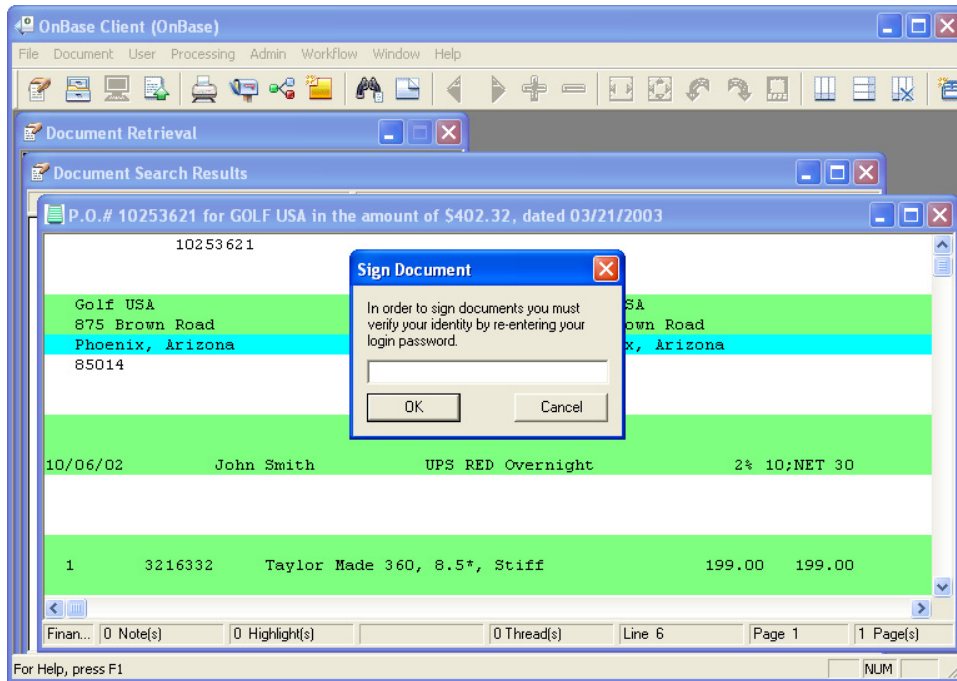


1. When a user initiates the signing process on a document, the document is retrieved from OnBase and the user is prompted for their password. 2. When the password is entered, a unique value is composed from a combination of the document and the Digital Certificate on the user's machine. 3. The unique value is then saved to the OnBase Database with a direct link to the document stored in the OnBase Disk Group.

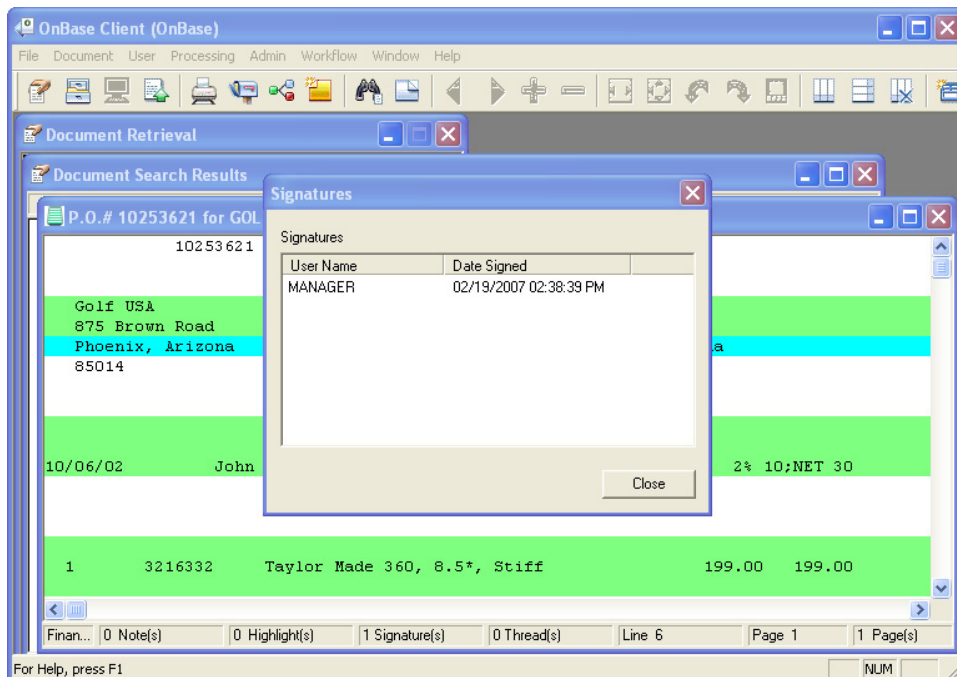
KEY FEATURES

- **Any document** configured in OnBase can be digitally signed
- **Simple verification of signed documents** through a right-click option guarantees signature is applied
- **Batch sign documents** for quick processing of multiple documents
- **Apply signatures** to document revisions and redacted documents
- **Use Workflow actions** to sign documents and verify valid signatures
- **Compatible** with most non-proprietary digital certificates, or those organizations acting as their own Certificate Authority
- **Supports industry standard technology**, such as X.509 Digital Certificates and PKCS7 message formats

INTERFACE



Users are required to enter a password at the time of signing.



Signatures can be viewed and verified from the signed document.

HYLAND
SOFTWARE