

# Document Security

[www.therefore.net](http://www.therefore.net)  
© 2009 ADOS Corporation

# Table of Contents

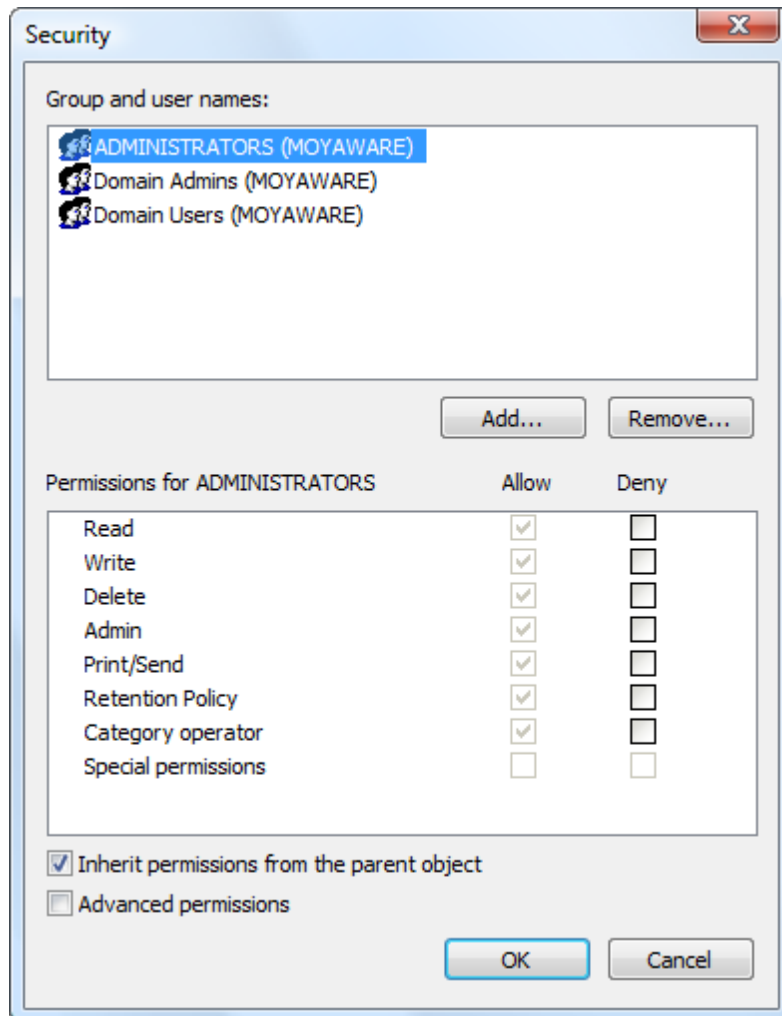
<b>1. Introduction</b>	3
<b>2. Managing Security of Therefore™ Documents</b>	4
<b>3. Storage of Therefore™ Documents</b>	5
3.1 Composite Files	5
3.2 Storage Locations	6
<b>4. Digital Signatures</b>	7
<b>5. Logging</b>	8

# 1. Introduction

Security of documents is a fundamental issue in any document management system; this white paper details how Therefore<sup>™</sup> handles this crucial topic. It starts by detailing how user and group rights are managed; continues with how documents are securely stored, then details how document integrity is ensured through means of document signatures, and finally looks at how Therefore<sup>™</sup> handles logging.

## 2. Managing Security of Therefore™ Documents

Therefore™ has an extensive rights access system which is managed via the Therefore™ Solution Designer. Objects are displayed using a tree-view, which enables rights to be given and inherited at various levels, including folders, sub folders, category, sub-category and then right down to single document level. Integration with Windows® integrated security (Active Directory, or Workgroups) simplifies selection of users and groups, and customizable permission sets, which group related rights, further simplifies the process of rights assignment.



For more details on assigning rights please refer to the Therefore™ Administration Manual. Furthermore, Therefore™ offers a rights server which makes it possible to implement an external rights server and enforce customer specific access rules.

### 3. Storage of Therefore™ Documents

#### 3.1 Composite Files

Therefore™ uses a non-proprietary composite file based on the Open Packaging Convention (open XML) and is part of the Office Open XML Standard (Microsoft®, ISO). This is the same format as used by Microsoft Office (.docx, xlsx, etc.). This allows a single document to consist of multiple single files (e.g. a Microsoft Word document and Microsoft Excel® sheet can make up one Therefore™ compound document). Index information and digital signatures form part of the compound file which carries the extension ".thex". In a worst case scenario, this makes it possible, to rebuild a system from the stored compound documents. The compound file can be opened using standard unzip software.

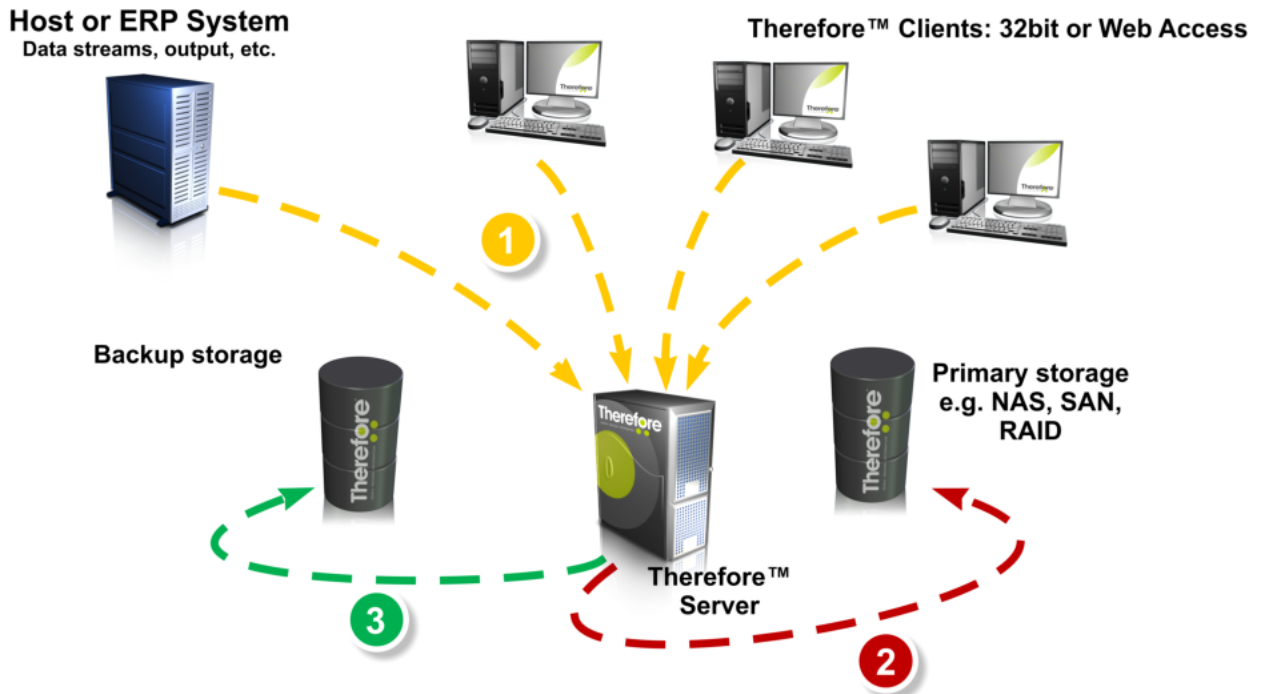


### 3.2 Storage Locations

When the Therefore™ server receives a document it is initially stored in the local buffer folder. A migration schedule then triggers a migration policy which moves documents from the buffer to a final storage location. The Solution Designer allows for the configuration of when migration should occur and to what media documents should be moved.

Therefore™ allows for, and recommends, the use of both primary and backup storage. Therefore™ verification tools enable administrators to ensure that all documents are accessible on primary and backup media. In the case of one storage location being corrupted or destroyed (e.g. disk crash), it can be repaired or replaced using the other.

Security of documents stored on external devices is ensured by requiring that only the Therefore™ Server service needs access to these locations. All normal users can be barred from accessing the documents directly from these storage locations.



## 4. Digital Signatures

The Therefore™ signs every document immediately after receiving it. When a user retrieves a document, the signature is verified by Therefore™ to guarantee that it is the original. Even the customer's system administrator cannot sign a changed document.

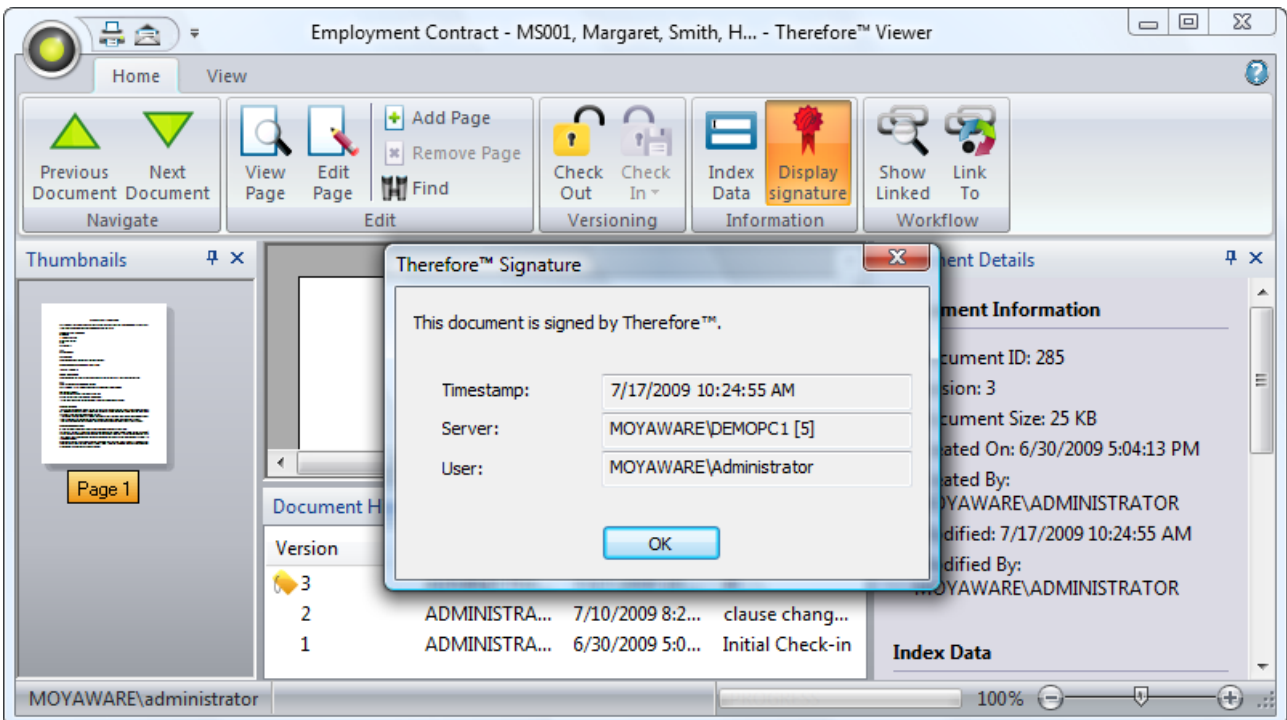
The signature comprises the following data, which is cannot be changed without invalidating the signature.

- All pages of the document (tiff, pdf, word, ...)
- Timestamp
- Name of the Therefore™ Server
- ID of the used key
- Username who triggered the archive operation
- Document number

The signature is stored within ".thex" document files and is created using a standard signing algorithm which computes the MD5 Hash and then encrypts this hash value with the RSA algorithm. Therefore™ generates an RSA key using the Microsoft Crypt API (length is configurable, default=800 bit). The private key is stored in the operating system only and is not exportable (i.e. no one can export the key and store it for later abuse). A key-pair is re-created every 30 days (time configurable) and the old private key is deleted, making it impossible to sign a document with the old key. The public key is stored in the Therefore™ database and is used during signature verification.

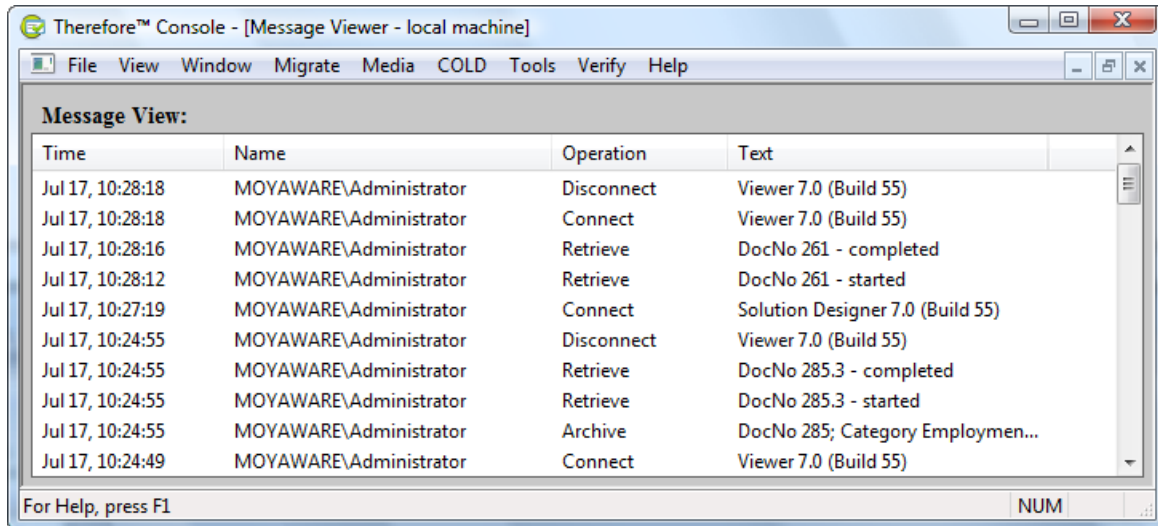
On retrieval of a document the server re-computes the MD5 Hash and then verifies the signature. Only documents with valid signatures are sent to the client; however, administrators can be given rights to bypass this check in order to analyse invalid documents.

Users with sufficient rights can check a document out edit it and check it back in as an edited version. This edited version is saved as new document version with new digital signature. Old document versions together with their digital signatures are retained and can be inspected using the Therefore™ Viewer.



## 5. Logging

The Message Viewer in the Therefore™ Console provides the ability to view logged events and track a number of user operations.



In addition Server logging writes detailed logs depending on the Server Logging settings in the Solution Designer. These logs are automatically stored in the Therefore™ Logfiles category which is in the Systems folder.

