



**White Paper**

# **Security**

**Version 1.0**

**Januar 2007**

DocuWare AG  
Therese-Giehse-Platz 2  
D-82110 Germering

**Legal notice:**

DocuWare AG

Therese-Giehse-Platz 2

D-82110 Germering

Telephone: +49.89.89 4433-0

Fax: +49.89.841 9966

Email: [infoline@docuware.com](mailto:infoline@docuware.com)

**Disclaimer:**

This document was compiled to the best of our knowledge and with great care. All references are to DocuWare products starting with DocuWare version 5. Essentially, this white paper sets out to describe the basic technical structure of the DocuWare products. There may be small or temporary differences with respect to individual functions in a particular version.

© Copyright 2007 DocuWare AG, all rights reserved.

## Contents

<b>1</b>	<b>Objectives of This White Paper</b>	<b>5</b>
<b>2</b>	<b>Introduction</b>	<b>6</b>
<b>3</b>	<b>Overview of System Architecture</b>	<b>7</b>
3.1	N-Tier Architecture	7
3.2	DocuWare System Architecture	7
3.3	Administration	9
<b>4</b>	<b>Authorization and Access Security</b>	<b>10</b>
4.1	Access Security	10
4.2	Login Methods	11
4.2.1	Login to LAN/VPN	11
4.2.2	Login via Internet	13
4.2.3	Passwords	13
4.3	Authorization Concept	13
4.3.1	Introduction and Terminology	13
4.3.2	Assigning Functional Rights	17
4.3.3	Settings at File Cabinet Level	17
4.3.4	Predefined Roles	18
4.3.5	Interaction of Rights and Authorizations	20
4.4	High Security Systems	21
<b>5</b>	<b>Secure File Cabinets</b>	<b>22</b>
5.1	Locking Documents in File Cabinets	22
5.2	Check-out	22
5.3	Encrypted File Cabinets	22
<b>6</b>	<b>Stamps and Electronic Signatures</b>	<b>23</b>
6.1	Stamps generally	23
6.2	Electronic Signatures	23
6.2.1	Tokens/ Certificates	24
6.2.2	Hash / Checksum	24
6.2.3	Time Stamps and Mass Signature	24
6.2.4	Verifying Signatures	25
6.2.5	Signatures of Third-Party Applications	25
6.2.6	Administrating Signatures	25
6.2.7	Signature Protocols and Standards	25
<b>7</b>	<b>Secure Communication and Transaction</b>	<b>26</b>
<b>8</b>	<b>Fail-Safety</b>	<b>27</b>

---

8.1	Failure of Authentication Server or Content Server	27
8.2	Authentication Server Database	28
8.3	Backup	28
8.4	Recovery	29
<b>9</b>	<b>Logging</b>	<b>30</b>
9.1	Log types	30
9.2	Logging Levels	30
9.3	Log Content	31
9.4	Storage Location and Scope	32
9.5	Authorizations	33
9.6	Predefined Logging	33
9.7	Viewing the Logs	35
<b>10</b>	<b>Glossary</b>	<b>36</b>
<b>11</b>	<b>Appendix</b>	<b>41</b>
11.1	Procedure for Developing Groups and Roles in an Organization	41
11.2	Definition of Rights in File Cabinets	42
11.3	Using Index Filters in File Cabinets	43
11.4	Procedural Examples	44
11.5	Functional Rights	45
11.6	File Cabinet Rights	49

## 1 Objectives of This White Paper

The purpose of this white paper is to present the security measures within the DocuWare software. The paper includes a discussion of the measures undertaken to achieve access security and to prevent downtimes – or at least to minimize their adverse effects on users. It includes all preventive measures against accidental or deliberate manipulation of managed content and against data loss caused by system failure. Security features also include measures to ensure data protection and the traceability of events within the system.

It mentions the underlying technologies and describes how they are used by the DocuWare system. This should provide readers with a technically sound understanding of the DocuWare system and the security it offers.

This document is intended for clients (users), consultancy companies, IT magazines and distribution partners. It assumes a certain level of technical knowledge about the structure of modern software applications, ideally of document management systems. Detailed knowledge of current or previous DocuWare systems is not required.

## 2 Introduction

The larger and more complex file cabinets become, the more extensive their security requirements. DocuWare provides comprehensive features relating to

- ❖ authorization and access security and
- ❖ protection against failure

An important element of the DocuWare system is Authentication Server, which not only ensures correct authentication, but also provides functions which protect against failure. To avoid the unauthorized use of DocuWare functions, the DocuWare servers contain the following security features:

- ❖ A state-of-the-art authentication system
- ❖ A comprehensive authorization concept
- ❖ Optional encryption
- ❖ Powerful electronic signature features
- ❖ Comprehensive logging options
- ❖ Secure communication protocols

For added system stability, many components can be configured redundantly and tasks can be distributed within the DocuWare system. In the case of large installations, this has the agreeable side-effect of allowing the workload to be distributed across multiple components, thereby improving response times.

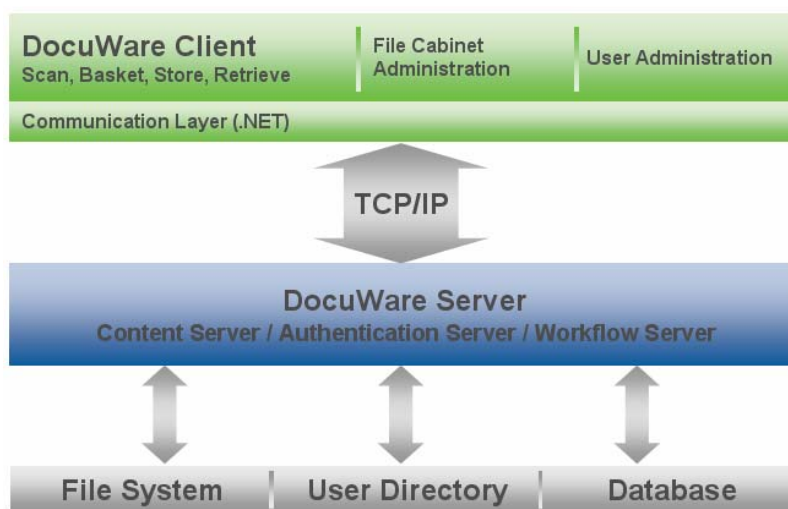
### 3 Overview of System Architecture

As an aid to understanding, this section presents a short overview of the system architecture. A separate white paper is available for the system architecture, which contains further information.

#### 3.1 N-Tier Architecture

The DocuWare system architecture conforms to the modern "N-Tier concept," which has evolved from the client-server principle. Its main characteristics are:

- ❖ Functions on the workstations are strongly dialog-oriented
- ❖ The application logic is located on one or more central DocuWare servers
- ❖ Several applications share common resources on one or more central background servers.



As in the classic client-server concept, the term *server* here refers to a software service, not to a piece of hardware. A DocuWare system therefore invariably consists of several (software) servers, all of which can – in extreme cases – run simultaneously on one hardware system.

Figure 1: Basic product architecture

#### 3.2 DocuWare System Architecture

A DocuWare system contains at least the following software components:

- ❖ **Rich Client**  
Dialog-intensive functions are integrated in the client component on each workstation. This provides optimum use of the benefits offered by the N-Tier architecture in terms of user comfort and performance.  
The rich client always comprises a scan client in order to provide this functionality at the workstation itself (provided a scanner is available).  
Providing a scan functionality at each client workstation is a response to the trend towards decentralized scanning. The aim is to make it as easy as possible for individual users to capture information.
- ❖ Of course, access can also be provided via a Web browser (see *INTERNET-SERVER* on the next page).
- ❖ **Authentication Server**  
Authentication Server manages all resources and users. It is the central "control station", which accepts logins, verifies authorizations, releases functions and resources and allocates (for example) servers to users.

❖ **Content Server**

Content Server manages the logical file cabinets (archives). It uses the database to manage index data and comments associated with the documents. The documents themselves are stored in the file system together with the header file. Comments are stored in the header file.

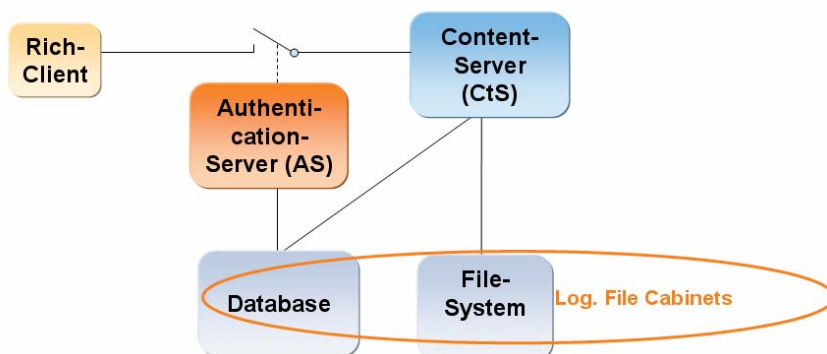


Figure 2: Minimal system architecture

With this basic system as the starting point, the DocuWare system is expandable and scalable in discrete steps. The next figure gives an example of how

- ❖ to expand functionality with Workflow Server,
- ❖ to integrate web clients,
- ❖ to use separate hardware systems for
- ❖ Authentication Server and Workflow Server
- ❖ Content Server
- ❖ a database, file system and INTERNET-SERVER

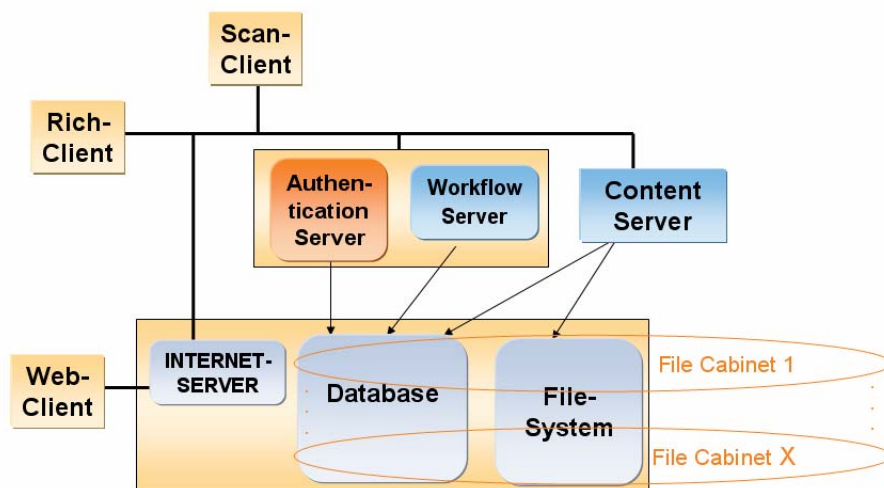


Figure 3: System expanded by functionality and hardware

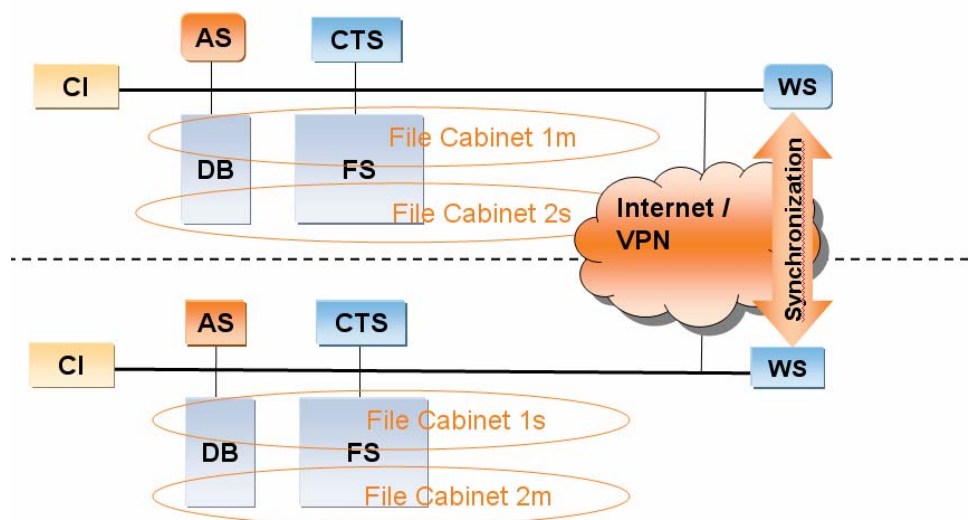
❖ **Workflow Server**

Workflow Server controls all automation and workflow processes. Automation processes include, for example, document import/export, file cabinet synchronization, migration and fulltext indexing. It also controls document workflows and the exchange of data with third-party applications.

❖ **INTERNET-SERVER**

INTERNET-SERVER can be used to connect web clients. These users require nothing more than a standard browser which allows them to store documents in DocuWare file cabinets as well as to retrieve and display them.

Communication between components takes place using standard protocols such as TCP/IP and HTTP. This allows systems to be implemented across different sites using Internet technology. If security is an important consideration, communication can also be realized via VPN (Virtual Private Network).



AS=Authentication Server, CI=Client, CTS=Content Server, DB=Data Base, FS=File System

Figure 4: File cabinets spanning several sites with Master (m) and Satellite (s).

This architecture not only allows reciprocal access to remote file cabinets but also the creation of redundant file cabinets in order to be able to work on the same file cabinets (archives) regardless of site and transmission capacity. Regardless of the file cabinet type ("master" or "satellite"), the full DocuWare functionality can be used at both sites, including copying any documents. Synchronization between "master" and "satellite" takes place via Workflow Server.

### 3.3 Administration

Ease of administration of even large and complex installations was an important design criterion in the development of the DocuWare software. All modules of a DocuWare system are therefore managed using *one* central administration software with *one* standard interface and standard user management. All settings for the various servers, clients, file cabinets, databases, etc. are configured using this tool.

This means that the entire installation, including all its organizations and taking into account security aspects, can be monitored and controlled from one central location. For example, it can be configured so that even rich clients - regardless of login requirements - have to register before they can access the DocuWare servers. Registered clients can also be disabled. In addition, centralized settings are possible, for example for caching on the client.

## 4 Authorization and Access Security

### 4.1 Access Security

Authentication Server manages all users and resources within the system. Before you can use the system, you must always log on to Authentication Server. It is therefore responsible for all access security, i.e. for

- ❖ user login,
- ❖ license management,
- ❖ administration of user-specific settings.

There can be one or more Authentication Servers for each DocuWare system, working across organizations. To avoid down times, Authentication Server may be installed redundantly. Authentication Server is therefore used by

- ❖ one or more organizations, each with
- ❖ at least one but up to hundreds of users.

Because DocuWare is multi-client capable, users are assigned to "organizations," which are managed via Authentication Server. An "organization" in this sense is a logical structure comprising:

- ❖ users and user groups
- ❖ logical file cabinets, including their associated disks
- ❖ processes
- ❖ templates for stamps, recognition schemes, select lists

DocuWare uses internal user IDs rather than the login user names. Only these user IDs are used as database keys. This means that users can be renamed at any time without having to change assigned settings.

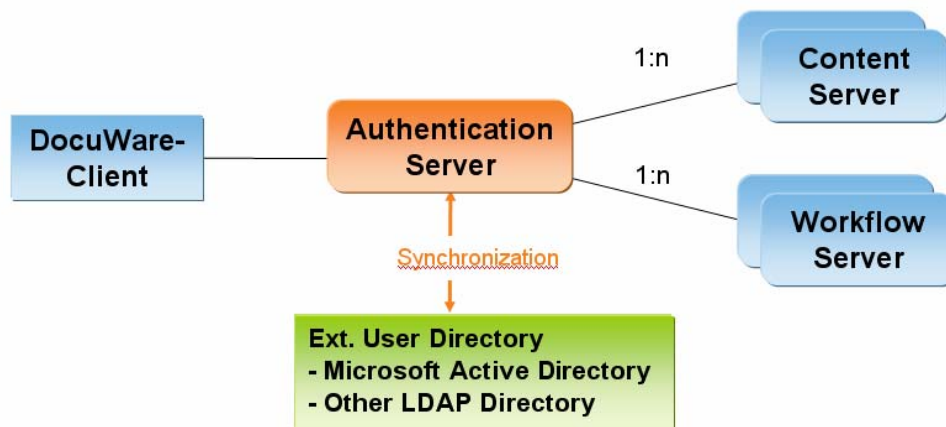


Figure 5: Authentication

When a user logs on, Authentication Server also checks the licenses for each organization and each user. Both "concurrent licenses" and "named licenses" are supported.

## 4.2 Login Methods

### 4.2.1 Login to LAN/VPN

The following user authentication methods are supported at login:

- ❖ **DocuWare Login**  
Users must prove their authorization by means of the name and password as stored in DocuWare. Users must only log in once, irrespective of the different DocuWare servers.
- ❖ **Trusted Login (Single-Sign-On)**  
The client identifies itself - without any other user input - using the login name of the Windows operating system. Authentication Server checks the login by means of the Windows user administration.  
This method also permits cooperation with other single sign-on systems. The directory services based on LDAP and Active Directory are supported.

The login to DocuWare must always go via Authentication Server. This login method also incorporates a verification of the licenses available to the user.

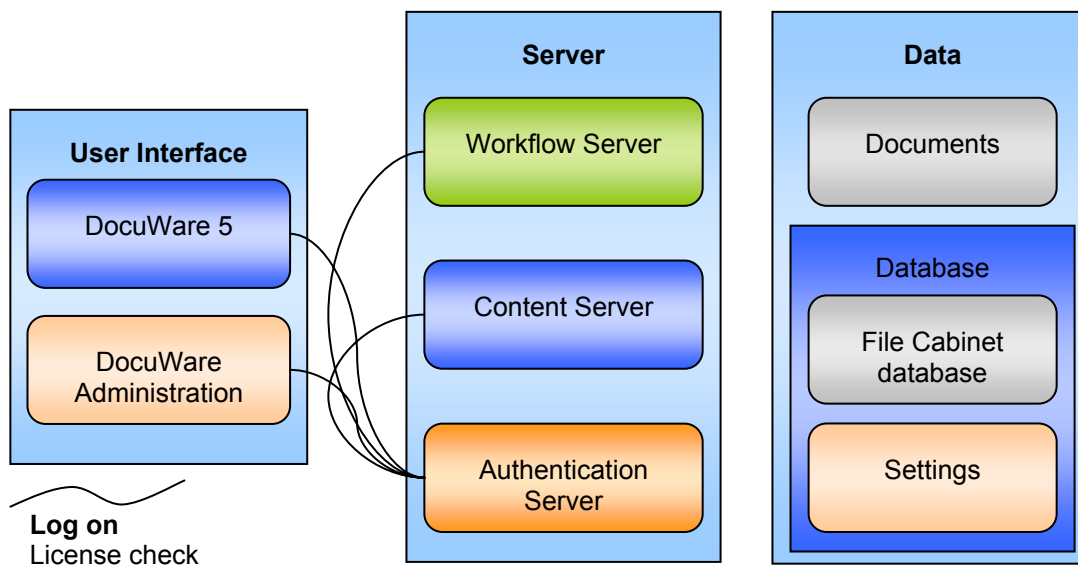


Figure 6: Login methods

DocuWare uses a "ticket-granting-ticket" (TGT) system, whereby a user or client identifies themselves to Authentication Server, requests a service, and is given a "ticket" which then allows them to use the service of another server, for example of a Content Server. To identify itself to Authentication Server, the client needs "credentials" which, as mentioned above, it receives either through user input (DocuWare login) or through the Windows user administration (trusted login). Authentication Server therefore exerts the central control function over the "sessions" within the system and can on the one hand impose the security features and on the other react proactively in the event of failure or overload of individual servers.

The [communication](#) between client and servers and between servers takes place securely.

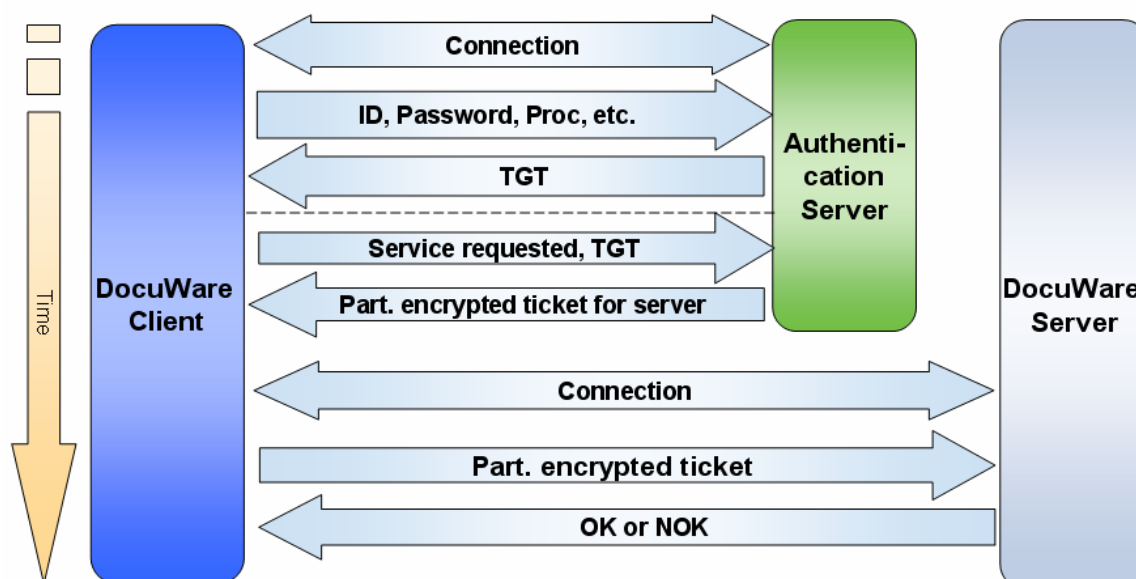


Figure 7: Ticket granting system

The actual authentication processes are described briefly below.

#### 4.2.1.1 Trusted Login – Single-Sign-On

1. The client typically authenticates itself to the Windows administration (domain or Active Directory) by means of a user name and a password. Microsoft offers other methods such as SmartCard, but these are currently rarely used.
2. Regardless of the login method used, the client receives a ticket from the Windows administration for this session of this user on this computer.

#### 4.2.1.2 Client Login to Authentication Server

General login procedure for Authentication Server:

1. Client establishes a secure, i.e. encrypted communication connection with Authentication Server.
2. DocuWare login only: the client asks the user for the user name and password.
3. Client identifies itself to Authentication Server using account name and password or through the ticket that it received from the Windows administration.
4. Authentication Server checks the information, creates a "Ticket-Granting-Ticket" (TGT) and sends it to the client. It also notes the license usage. That means, one license is blocked until logout (or timeout).

#### 4.2.1.3 Client Service Request to Authentication Server

Once it has logged on, the client can request the use of services from Authentication Server using the following procedure:

1. Client submits the following information to Authentication Server:
  - a. Required server type (Content Server, Workflow Server, SAP HTTP Server and future servers)
  - b. Additional required parameters, for example identification of the logical file cabinet
  - c. The TGT received above
2. Authentication Server determines the server to be used
3. Finally, Authentication Server sends the client a time-limited ticket for this server. The ticket includes a session key for communication between client and server.

#### 4.2.1.4 Client Login to Assigned Server

The client now uses this ticket to log on to the server assigned by Authentication Server. The procedure is as follows:

1. Client establishes a secure connection to the server to be used and submits the ticket received from Authentication Server.
2. Server evaluates the information contained in the ticket and checks the ticket's validity.
3. Server sends confirmation to the client and is now ready to receive requests.

If the ticket has expired, it is up to the client to request an extension of the ticket from Authentication Server. The procedure is similar to when requesting a new ticket. However, since the same session key is used, the session can be continued without loss.

#### 4.2.1.5 Client Logout from Authentication Server

At the end of a session, the client must log out of Authentication Server in an orderly fashion. The client establishes a secure connection to Authentication Server and submits its Ticket-Granting-Ticket. Authentication Server then releases the license again.

Licenses can only ever be used for a defined period. If the client fails, the license is freed by a timeout. After a failure and restart of Authentication Server, blocked licenses are also released.

### 4.2.2 Login via Internet

The login procedure for remote users over the web works is essentially the same as described for LAN/VPN users. However, here communication does not take place directly between client and DocuWare server, but via INTERNET-SERVER. Proxy servers and firewalls may also be interposed, although these have no influence on the sessions described here.

### 4.2.3 Passwords

User names and passwords are usually encrypted, or stored as hash values. The same applies to system settings such as the login for the database server.

It uses the "salted" hash procedure, whereby a random value ensures that even two identical passwords do not generate the same hash value. This means that passwords can neither be read nor reproduced.

When you enter a password, DocuWare generally only displays "\*\*\*\*". When you change a password, you must first enter the current password.

The login options are specified when a user is set up. If a user should forget their password, it can be reset by the organization administrator. However, this is not possible for users with "high security", see also section 4.4 High Security Systems.

## 4.3 Authorization Concept

### 4.3.1 Introduction and Terminology

Employees in large organizations deal with complex processes and are subject to a variety of rules and regulations. In order to carry out their tasks they need authorizations to use particular resources such as document and IT functions. These authorizations can take the form of electronic permissions. This goes hand in hand with certain restrictions to make sure that only authorized personnel have the right to do certain things, and to maintain transparency for everyone.

A document management system that supports existing processes must be capable of mapping existing authorizations. DocuWare uses a rights concept which allows you to define in great detail, for each DocuWare user, which activities he or she can perform within the DocuWare system. Thanks to DocuWare's transparent structure, these rights are easy to assign and administer.

## Functional Rights and File Cabinet Rights

An essential element of rights administration in DocuWare is the distinction between functional rights and file cabinet rights.

### Functional Rights

The assignment of functional rights defines which menu items and functions a user can execute within the DocuWare system.

These can include the right to import documents into the DocuWare system from the file system, to add annotations to documents and to set particular stamps.

A user can be assigned various functional rights.

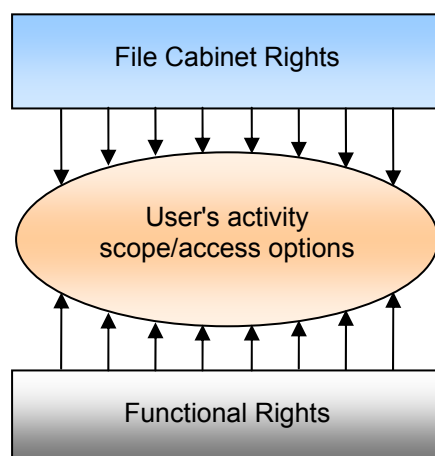
### File Cabinet Rights

File cabinet rights specify which access options a user has to file cabinets (stored documents and index data).

These rights include storing and retrieving documents, editing index entries or exporting stored documents to the file system.

A user can be assigned various file cabinet rights for each file cabinet.

The total of all a user's functional rights and file cabinet rights constitute this user's activity scope.



## Profiles and Roles

Profiles and roles enable you to assign sets of rights in "containers", instead of a lot of individual rights. The assignment of rights to profiles and roles has two major advantages:

1. Detailed, finely granulated sets of rights can be assigned at the touch of a button to as many users as required, without the administrator having to customize the complex rights structure manually for each user.
2. Sets of rights also exist without users, so when an employee leaves the company, their successor can be effortlessly assigned the same rights, regardless of how specific and detailed the rights assignment actually is.

**Functional Profiles**

Functional rights can be combined into functional profiles. Profiles are a convenient way of assigning even very complex combinations of rights. Profiles can be assigned to individual users and roles.

**File Cabinet Profiles**

File cabinet rights can be combined into file cabinet profiles. Profiles are a convenient way of assigning even very complex combinations of rights. Profiles can be assigned to individual users and roles.

**Roles**

Roles are sets of several profiles. A role can include both profiles with functional rights and profiles with file cabinet rights. Roles can be assigned to groups and to individual users.

**Users and User Groups**

Individual DocuWare users can be combined into different groups. A user can be a member of more than one group.

**User**

As a rule, one user is created for each member of staff who needs to work with DocuWare. Users receive a range of rights through the assignment of individual rights or sets of rights in the form of profiles and roles. Users can belong to groups.

**Groups**

Groups are sets of users. It is a good idea to combine into groups users who need to use the same program functionalities and be assigned the same file cabinet rights. Individual users receive these rights through their membership of the group, to which the appropriate role has been assigned.

**Inherited Rights and Explicit Rights**

When assigning rights to users, DocuWare distinguishes between inherited rights and explicit rights.

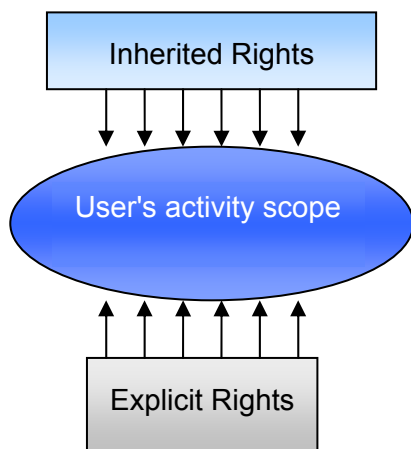
**Inherited Right**

Rights that a user has received through membership of a group or through a role or a profile, are called inherited rights.

**Explicit Right**

Rights which a user receives directly (and not via a role, profile, or group), are explicit rights. Only functional rights can be assigned as explicit rights.

Rights are always additive, in other words, the total of all a DocuWare user's inherited rights and explicit rights constitute this user's activity scope.



## Rights Assignment

There are three main methods of assigning rights to users:

1. Direct rights assignment:  
All employees are assigned the rights they need directly.  
This variant is only recommended if the organization contains only a few DocuWare users. Otherwise, this variant can become very time-consuming in the long run, and prone to error, so one of the following options is to be preferred.
2. Rights assignment via profiles:  
All rights are combined into profiles. These profiles are assigned to individual users.  
This variant is recommended if the organization contains only a few employees or if the employees have very specific tasks.  
Making changes with this variant is less time-consuming than with the first method, however in larger organizations we recommend assigning rights via roles and/or groups.
3. Using roles:  
Roles can be used to assign rights to individual users. The roles combine functional profiles and file cabinet profiles.
4. Using groups:  
DocuWare users with the same tasks can be combined into groups. The rights are then assigned to these groups via roles.  
This method is recommended for larger organizations, as it is the quickest method for making changes.

Naturally, you can also use a combination of all four variants.

DocuWare provides these variants so that administrators can choose the one with which they are familiar and which is best suited to their organization. Groups (as sets of users) and roles (as sets of rights) are different ways of looking at one and the same thing. The crucial point is the functions in the DocuWare system. From one perspective, the employees and corresponding users are the starting point. From the other, the starting point is the workflows and functions in the DocuWare system. Examples of both these variants can be found in appendix *11.1 Procedure for Developing Groups and Roles in an Organization*, page 41 .

### 4.3.2 Assigning Functional Rights

Functional rights are used to determine which menu items are available to a DocuWare user in the DocuWare main window, the DocuWare viewer and in the ACTIVE IMPORT add-on module. They also determine part of the user's activity scope in DocuWare Administration.

The assignment of individual menu functions as rights allows you to define precisely which functionalities are available to a user within the DocuWare system. The menu items of actions which they are not allowed to perform are removed. For example, if an employee is not allowed to staple and unstaple documents, the *Staple* and *Unstaple* menu items are not assigned. When the employee logs in to DocuWare, these menu items are not part of the menu.

The restriction of menu commands can also be used so that users only see those menu items that they need for their own work. This makes the user interface even clearer and excludes application errors.

### 4.3.3 Settings at File Cabinet Level

File cabinet rights are always combined into profiles. As with functional rights, file cabinet rights cannot be assigned directly to individual users. Only file cabinet profiles can be assigned to users or roles.

Just as with functional rights, file cabinet profiles are also additive. In other words, if several file cabinet profiles of a file cabinet are assigned to a user, this user receives all the rights that are shared by these profiles. This also means that rights cannot be restricted, only expanded. This procedure is explained in more detail in section 4.3.5 .

The following sections describe file cabinet rights, field rights, and rights to index filters.

#### File cabinet rights

File cabinet rights are divided into administrative and general rights. *Administrative file cabinet rights* include the right to: modify file cabinet rights for users, create search and store dialogs and result lists for this file cabinet, and migrate the file cabinet. *General file cabinet rights* include the right to store, retrieve, and delete documents.

File cabinet rights always relate to one file cabinet along with all the documents it contains. Different file cabinet rights can be assigned to different file cabinets.

#### Field rights

In addition to general file cabinet rights, rights can also be assigned at field level. These rights relate only to the specific field, not to all fields of a file cabinet. Field rights include the right to retrieve, to modify field contents, plus the right to use entries that are not available in a select list.

#### Index filters

Index filters are provided to enable rights within a file cabinet to be assigned selectively by index entry. Index filters can be used to select specific documents by their index entries. Limiting access to documents by means of index data is particularly useful when documents containing sensitive data are grouped together in a file cabinet.

**Example:**

Documents relating to employees are stored in an HR file cabinet. The employee name is one of the index entries available. HR department employees have access to all documents, while individual employees can only access those documents that have been stored with their own name in the index data.

Details on how to use index filters are given in the appendix 11.3 *Using Index Filters in File Cabinets*, page 43.

## Dialogs

Multiple search and store dialogs, result lists and information dialogs can be created for each file cabinet.

The visibility of index fields can be defined individually for all these dialogs. Search and store dialogs can be preset, so that unauthorized access or modifications are excluded in the very definition of the dialog.

You will find more information on dialog definitions in appendix *11.2 Definition of Rights in File Cabinets*, page 42.

### 4.3.4 Predefined Roles

After the initial installation, each DocuWare system contains predefined roles with predefined profiles; this means that administrative tasks are also subject to the authorization concept. These predefined roles can be assigned to different users or user groups.

## System Administrator

The system administrator manages the system from the point of view of the generally used basic components and the hardware. This includes managing the database connections, plus the administration of communication paths and document storage paths. The system administrator can be defined so that he or she cannot access individual organizational data, and specifically cannot intervene in the details of the user administration. However, only he/she can assign the "System Administrator" role to other users. This cannot be done within the organization's user administration.

The system administrator is also responsible for installing and updating the server software.

After DocuWare has been installed, he/she assumes the role of organization administrator for all organizations simultaneously. As each new organization is created, the system administrator initially automatically assumes the role of organization administrator, although this can then be assigned to another person.

### System Administrator Tasks

- Hardware, operating system, database
- Installing DocuWare server modules

Configuring system-wide settings for:

- Authentication Server
- Content Server
- Workflow Server
- SAP HTTP Server
- Connections
  - Databases
  - Data files
  - SAP remote connections
  - Time stamp services
- Storage systems
- User directories
- Logging

## Organization Administrator

The organization administrator manages an organization. A DocuWare system can include one or more organizations, each with its own organization administrator. The organization administrator manages in particular the rights, users and user groups of their organization. The role does not include access rights to file cabinets and their administration.

The assumption of this role does not require any detailed technical knowledge of the IT environment. The organization administrator can also assign or remove the role to and from other users. In particular, the role can even be removed from a system administrator.

### Organization Administrator Tasks (per organization)

- Installing clients for each organization
- Licenses
- DocuWare client

Configuration per organization:

- Client systems and baskets
- Stamps/signatures
- Viewer and external applications
- Select lists
- Validations
- Users and groups
- Logging
- Workflows

## File Cabinet Owner

The right of the file cabinet owner is automatically assigned by the DocuWare system to the person who creates the file cabinet. He or she can then assign this right along with other rights for carrying out administration tasks to other users.

The owner manages the file cabinet structure (e.g. index and disk structure) and assigns the access rights to the file cabinet in which he or she creates file cabinet profiles. With reference to the file cabinet, the owner also defines the settings for the organization administrator, so that the latter can assign the file cabinet profiles to users and/or roles.

### File Cabinet Owner Tasks (per file cabinet)

- Fulltext indexing
- Used database connection
- Document storage and disk concept
- Index fields
- Rights to file cabinet
- Dialogs for storage, retrieval and result list
- Logging

### 4.3.5 Interaction of Rights and Authorizations

#### Member of several groups, owner of several roles or profiles

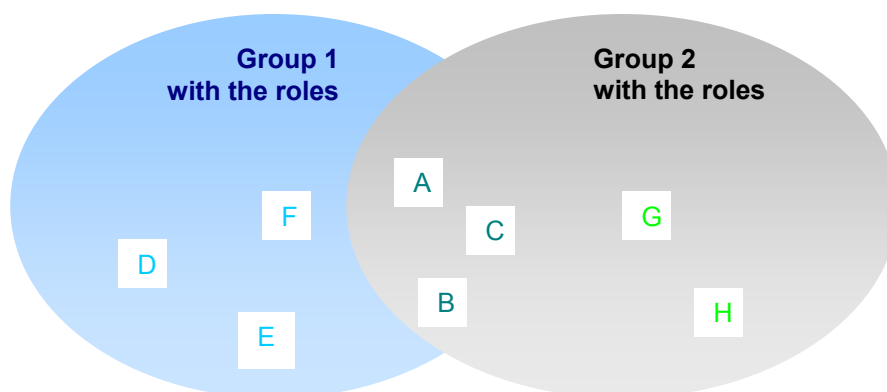
Rights are always additive, in other words, the total of all a DocuWare user's assigned rights constitute this user's activity scope.

If a user is a member of several groups, he or she has all the rights that are available through assignment to these groups and their roles.

If several roles or profiles are assigned to a user, this user has all the rights that have been assigned to these roles or profiles.

Examples:

- A user has received his set of rights via a role. If you now assign this user an additional role that has fewer rights, it does not change anything for that user, since rights are additive. In order to restrict his rights, you would have to remove the original role from him. (The same applies to groups.)
- A user is a member of two groups and has received his set of rights via the roles of these groups. If you now remove the membership of one group from him, he does not automatically lose all the rights that are assigned to him via the roles of this group, but only those that are not assigned via the other group.



If you remove the membership of group 2 from a user, he only loses roles G and H, as he still has roles A, B and C via group 1.

(The same applies also to roles and profiles assigned to a user.)

#### Functional Rights and File Cabinet Rights

File cabinet and functional rights are assigned independently of one another. However, for a logical rights canon, they should not necessarily always be viewed as independent of each other. Here is an example:

For a user to be able to search in a file cabinet, he needs the *Search* right and a search dialog assigned to him at file cabinet level. Under functional rights he also requires the *Search* menu right, otherwise he will not be able to open the search dialog. The same applies for storing documents in a file cabinet.

#### Dialog Settings and File Cabinet Rights

The options that a user has within a file cabinet result from the file cabinet rights, which also include the relevant "tools" - the dialogs. You can find examples of this in appendix 11.2 *Definition of Rights in File Cabinets*, page 42.

## Field Settings and File Cabinet Rights

The settings for the individual file cabinet fields and assigned file cabinet rights overlap in some areas. It is therefore possible to make special rights available to designated users, while "normal" user rights are controlled by means of field settings. You can find examples of this in appendix *11.2 Definition of Rights in File Cabinets*, page 42.

Summary: a user's file cabinet rights always override the field rights. Using a combination of both schemes should therefore be done with care.

## Using Index Filters

General file cabinet rights, such as storage, can be combined with file cabinet profiles based on index filter criteria. This allows rights to be finely balanced at file cabinet level, depending on special index entries.

You will find detailed descriptions of how to structure and use file cabinet profiles with index filters in appendix *11.3 Using Index Filters in File Cabinets*, page 43.

## 4.4 High Security Systems

A DocuWare system can be based on "high security."

At organization level, this means that the organization administrator is in a position to assign the "high security" property to certain users. For these users, the password can then no longer be reset by the organization administrator. Only the users themselves can change their password. If one of these users forgets their password, they must be recreated within the organization. These users can also not log on using a trusted login (see section *4.2 Login Methods*), since with trusted login security is not ensured by DocuWare.

If a system is set to "high security," you can also set selected file cabinets to "high security." It is then no longer possible to assign file cabinet profiles to roles for these file cabinets, since file cabinet profiles must be assigned directly to users. These users must have the "high security" property. This prevents access to especially sensitive areas being granted "by accident" through uncontrolled groups and role assignments.

## 5 Secure File Cabinets

In addition to the authentication system and the authorization concept, other measures exist for protecting file cabinets against misuse and inconsistencies. These include locking documents that are being revised, encrypting file cabinets and using stamps and electronic signatures.

### 5.1 Locking Documents in File Cabinets

When a user is displaying or editing a file cabinet document, the document is locked for all other users. Other users can still view the document in the viewer, but they cannot set annotations or stamps or open the document in an editor (read-only mode).

Technically, we call this "locking" documents. A locking table is created for each file cabinet. As soon as a document is opened by a user, an entry is made in this table to indicate that the document is locked. It also records when and by whom the document was locked.

If another user now tries to open the document, they receive a message that the document is currently locked for editing. They can only display the document in Read mode. All options for creating annotations or stamps for the document are disabled. These only become available again when the first user has finished editing the document and has returned it to the DocuWare file cabinet.

All locking data is recorded in the database. Special mechanisms ensure that locked and released documents are always restored to a consistent state, even after a failure of the client, the application, or even the server.

### 5.2 Check-out

Locking is controlled by the system and prevents the creation of inconsistent documents through accidental simultaneous editing by different users. In practice, however, documents can often remain in editing status for a long time, even if they are not continually opened by a user throughout this period. This is what the check-out function is for.

Check-out is controlled by users and is independent of system states. That means that a document can be checked out for days or even weeks, for example for extensive revision or offline use. Check-out is therefore independent of whether the file is open or the user is logged in.

Checked-out documents can still be accessed in Read mode. However, no changes can be made, nor can annotations or stamps be inserted. Storing a new version implicitly involves a "check-in".

### 5.3 Encrypted File Cabinets

Naturally enough, administrators must have extended rights when using the system. Since - especially in larger enterprises or in the case of multiple organizations - administrative tasks may be distributed between different people, DocuWare uses the different roles described earlier with different authorizations as appropriate. In cases in which even this level of security is not sufficient, encryption can also be used.

In these cases, the documents are encrypted and optionally also their associated header files. Fulltext files cannot be encrypted by DocuWare. In any case, the fulltext index can only be interpreted by someone with detailed knowledge of the procedure used. The index data in the database is also not encrypted. If the index data contains highly sensitive information, you should consult the options offered by the database provider.

Note that encrypted file cabinets can only be accessed by users that have the appropriate key. The keys for decrypting the documents are stored in the document header. The document keys are decrypted using an asymmetric procedure with a key stored in the database. Since the documents cannot be decrypted without the key in the database, if you are using encrypted storage you should make sure that regular backups are made of the DocuWare system tables, so that the key tables in particular can be restored if the database is lost. When backing up the database, use the database mechanisms provided by the developer.

## 6 Stamps and Electronic Signatures

### 6.1 Stamps generally

The DocuWare system has some special options for supporting work processes. Included amongst these are features for adding stamps and signatures, just like with paper documents, except that these are in electronic form. Electronic signatures are stamps with particular qualities.

The various stamp types are differentiated as follows:

- ❖ **Text**  
This stamp consists of any text into which you can integrate variables to be completed by the user at runtime and assigned to index fields. You can also use select lists in these form fields, just like in file cabinet fields. Borders, fonts, and colors can all be customized.
- ❖ **Freehand Drawing**  
A field is defined in which the user can enter any graphical data at runtime. The entry can be made with the mouse or other input device. Here not only the graphic is stored, but also the biometric characteristics<sup>1</sup> at creation.  
This allows you to represent classic signatures in existing processes while maintaining a high level of biometric security. The input devices most suited to this are Tablet PCs, since these allow you to enter signatures by writing on the screen and they can be used in much the same way as an ordinary notepad.
- ❖ **Bitmap**  
You can integrate any bitmap in one of the supported graphics formats. The easiest method is to copy the image of a previously used stamp or signature directly into the electronic world.

In practice this allows you to give your processes the same look and feel as before, for example with stamp layouts, colors, etc. A stamp can also contain a range of other attributes, which determine the functions available. For example, it can be defined as for use only with a particular file cabinet, or linked to a password, or the stamp can automatically be stored with the document after a specific period.

Stamps can be used to automatically enter or modify the values in a document's index fields. This allows revisions to be automatically documented with a person's name, date, and department, etc.

Stamps can be defined at organization level by administrators and assigned to users. In addition, users can create their own stamps, which are then only available to them.

Stamps are stored as special annotations in a document's XML header file. When the document is reproduced, it can be displayed with or without stamps.

### 6.2 Electronic Signatures

One of a stamp's definable attributes is the "signature." Here we mean signatures as defined by the EU directive. The options are:

- ❖ Simple signature (without certificate)
- ❖ Certificate-based signature (with certificate and private key)
- ❖ Time stamp (with certificate, but not linked to a specific person)

You can define which signatures can be used in the administration. For users there is no difference when applying the different signature types. The only differences lie in the use of certificates.

---

<sup>1</sup> The specific attributes depend on the installed hardware and the extent to which this supports the Microsoft interface. DocuWare envisages the following attributes: Number of points in X and Y direction, resolution x/y, Pressure in the Normal/tangent, Slope angle x/y, Azimuth orientation, Altitude orientation, Turning angle, Slope rotation, Roll rotation and Shearing angle.

### 6.2.1 Tokens/ Certificates

A certificate is an "electronic identity card", in which a "certification authority" (this can be an internal body, an official authority or another company) certifies the checking of an identity, assigns a key pair and confirms the information with its own electronic signature. This data can be stored on a specific hardware "token" (smart card, USB stick, etc.), or on a diskette or hard disk as a so-called "soft token." Windows provides specially protected areas on the hard disk (certificate stores) with import and export functions.

How strict the identity check was can be seen from the gradings contained along with the terms and conditions of business. The technical format of the different certificate classes does not vary. In other words, from a technical point of view the signature is created in the same way whatever the quality of the certificate.

For the DocuWare system it is therefore irrelevant whether certificates are qualified according to the national laws of European countries. If the certification provider (trust center, certification authority) supplies a qualified<sup>2</sup> certificate and the connected signature creation device (e.g. smart card reader) is identified as secure, DocuWare automatically generates "qualified signatures," which in Europe have equal status with a traditional signature. Other signatures are regarded as "advanced signatures" under European law.

Certificates for DocuWare can be supplied both by internal organizational units and by external certification authorities. The certificates are stored using the options provided by the Windows operating system. This means that both hardware-based solutions (smart card, USB stick) and purely software certificates are supported. It is thus a procedure with "public key infrastructure" (PKI), as defined in the internationally standardized PKIX model.

The DocuWare signature supports any certificate provided it exists in the X.509 standard and is stored in the Windows certificate store. DocuWare has no specific requirements as regards the origin of certificates. Other relevant standards are considered, and the signature is stored in the document header in line with XML-DSIG.

### 6.2.2 Hash / Checksum

A "signature" requires that a checksum is calculated for the stamped document (hashing) and that user data are associated with the document. Any subsequent modifications to the document are then immediately visible because of the variation in the checksum.

The certificate-based procedure then encrypts the checksum using the user's private key and stores this in the header file of the document.

The scope of the signature can be customized, i.e. you can define what information is to be included in the hashing. Since a DocuWare document can consist of a number of files ("DocuWare page"), hashing - and hence the signature - can extend to all of these files. However, you can also specify that only the currently displayed page (displayed file) is to be included in the signature. Comments associated with the document or the current page can also be signed.

### 6.2.3 Time Stamps and Mass Signature

DocuWare supports a variety of time stamp services. These are signatures that are not linked to a person, but are allocated by external time stamp service providers. This ensures that the stamp contains a valid time indication, which cannot be guaranteed when using system times. Time stamps may be combined with other certificate-based signatures.

In addition, so-called mass signatures are supported. This method provides a large number of similar documents with their own signatures, without users having to input their PIN every time in order to identify themselves as the legitimate owner of the token. This method is generally used for scanned images or for large-scale output management, such as sending out batches of invoices.

---

<sup>2</sup> In order to issue "qualified" certificates, the provider must fulfill a large number of organizational and technical requirements. Qualified certificates are particularly trustworthy.

## 6.2.4 Verifying Signatures

You can specify in the client configuration whether a signature is to be automatically verified in the viewer. But whatever the setting, the user can always initiate the verification of the signature of an incoming document manually.

This is true also of the supported time stamp services. Typically, the certificate is included with the signature to make verification of the signatures easier for the recipient.

Verification consists on the one hand of checking the hash value in order to identify any modifications, and on the other of checking the certificate, for example its validity period and the trustworthiness of the issuing organization. If revocation lists are available, the certificate is compared against these.

## 6.2.5 Signatures of Third-Party Applications

DocuWare can handle a large variety of different documents which might also include signatures. DocuWare makes sure that from the user perspective document handling is done in a consistent way, irrespective of whether documents are signed or not.

However, with signatures or specific signature formats that are embedded in third-party formats, DocuWare cannot perform a verification, as no standards have been established. This therefore remains the responsibility of each individual application.

## 6.2.6 Administrating Signatures

Under the Windows operating system, both the root certificates of the certification service providers and the user certificates must be set up on each client. This requires the user to have Windows administrator privileges.

The administration of user signatures and stamps is the responsibility of the organization administrator. He/she defines the available stamp and signature types. Signature types are filters for the attributes of the certificates. They ensure that only certificates issued by a particular certificate service provider are allowed to create signatures. They also provide the option of restricting individual users to certain certificates or certain stamps. This then also imposes certain conditions on the extent to which stamped/signed documents can be used.

The general rule is that a user can only use the stamps and signatures that have been allocated to him or to the profiles allocated to him and for which he has a certificate on his client.

## 6.2.7 Signature Protocols and Standards

DocuWare uses the standards of the PKIX model and the established Microsoft interfaces. The selection follows the recommendations of the ETSI ESI (European Telecommunications Standards Institute, Electronic Signature Initiative) - to the extent that this is possible and sensible.

The signature data is stored in an XML structure in the document header. The XML structure conforms to the XML DSIG standard. This structure contains the references to the document files in the form of URLs.

The scope of the signature is defined by a list of URLs, as per W3C XML-DSIG specification. This list of references is included in the signature in order to prevent manipulation of the scope of the signature - or to make it detectable.

The document header is saved along with the document.

The ETSI ESI Initiative results from the EESSI (European Electronic Signature Standardisation Initiative). Its objective is the greatest possible unification of the signature standards as used within the EU. Even though they are relatively new, the ETSI guidelines are finding increasing resonance with providers and users, particularly within government and public administration.

Microsoft's cryptography interface is used for creating and verifying signatures. The device creating the signature (usually SmartCard and Reader) must support this interface.

## 7 Secure Communication and Transaction

Communication between DocuWare components (servers, clients, third-party systems) generally occurs securely. The system administrator can turn the security mechanisms on or off for each incoming or outgoing connection. With the security mechanisms enabled, communication can happen via the available Windows mechanisms or via SSL. For cases where a security mechanism is not available on either side, alternatives can be provided.

The supported protocols are Microsoft NTLM and Kerberos. We recommend Kerberos because of its superior security. Only in cases where the partner system does not support this – for example, older Windows versions – is NTLM used for compatibility reasons.

Kerberos is a so-called "Ticket Granting Protocol" (see also [Access Security](#)). This was developed at the MIT in Boston; it is an IETF standard and widely supported.

The access to the DocuWare servers from clients via the Internet or an intranet occurs via encrypted communication channels after verification of the identity of the communication partners (see also [Login via Internet](#)). We recommend SSL encryption for communication outside of domains and via public access channels.

For SSL communication servers must have an appropriate certificate that is deposited in the Windows certificate store of the particular computer.

If the connection between servers is lost, this is automatically re-established. If a central components fails its functions can be taken over by a redundant components (see also [Fail Safety](#)).

To ensure that no instable system states occur with sensitive operations (for example server failure at the time of storing a document in the file cabinet), a transaction procedure has been implemented. If certain steps of such a transaction cannot be completed, the changes made are discarded automatically (rollback).

The operation of saving documents which causes a number of updates both in the database and the file store has been implemented as a transaction, thus ensuring the consistency of the system.

## 8 Fail-Safety

Any number of failures can occur in a complex system such as a DMS within a heterogeneous IT infrastructure. For this reason a number of measures are available to help prevent failures and/or to minimize the organizational and technical problems that might be caused. However, in the end it is always a matter of balancing the costs and the benefits, given that the cost of ensuring the last percentages of total fail-safety is disproportionately high.

In the case of a DMS, server platform failures are an important consideration. There are several solutions both from hardware and from operating system providers that address this problem, including "clustered" systems which not only offer improved fail-safety, but also provide load balancing between the components without DocuWare software having to worry about it. Both for Microsoft and for Linux systems suitable architecture and supplementary system software are available on the market.

[Authentication Server](#) stores all settings in the database, and it works in a "stateless" fashion, which means that no data are stored temporarily within an application. In this way, Authentication Server can make unrestricted use of the above platforms. It can also run on a system that is composed of several computers. Content Server on the other hand works in a "stateful" manner. Provided that several [Content Servers](#) run in parallel on the various systems, they can benefit from the additional performance and enhanced security of these platforms.

Very sophisticated procedures are also available for database servers. We recommend using these options, given the significance of the database for the DocuWare system. As far as storage technologies such as RAID drives are concerned DocuWare can make use of such technologies, but has no influence on these components.

An important element for increasing the availability of the DocuWare application is the installation of redundant DocuWare servers on high-availability platforms and networks. DocuWare makes its own contribution towards fail-safety by providing secure communication and transaction procedures. The highly sophisticated identity checks for users and systems among themselves (see [Access security](#)) also contribute to increased system availability, as these prevent downtimes caused by deliberate or grossly negligent behavior.

The following sections describe in more detail those aspects that DocuWare contributes to fail-safety; we do not here touch further on the options afforded by the platforms.

### 8.1 Failure of Authentication Server or Content Server

At login and after it has successfully authenticated the user and checked the license, Authentication Server allocates to the user the required and available servers, such as Content Server. If the Content Server is not available, the client goes back to the Authentication Server which then contacts the Content Server and detects if there has been a failure. If servers have been set up redundantly, a Content Server failure can be by-passed via a new login - thus allowing the user to continue working with DocuWare.

If an active client during live operation does not get a response to its requests from the Content Server within a certain time, it must then request a renewal of its ticket from the Authentication Server. This then sets in course the above mentioned mechanism.

Because the Content Server works in a transaction-oriented way, changes to the databases become effective only with the concluding "Submit" command. If this command is not issued due to a server failure, the original state prevails. This prevents an instability in the system.

Data is transmitted to the database via secure communication, and stored. Because the Authentication Server works in a stateless fashion, any failure can simply be overcome by using a second Authentication Server.

When an Authentication Server no longer responds, the client contacts the next Authentication Server. However, this does not occur automatically; instead, the user logs in again. For this purpose, a sequence of Authentication Servers can be configured on the client. When a new login occurs, all Authentication Servers are checked for their availability, one after the other. The same applies to DocuWare servers, which also need to login to Authentication Server in order to obtain a ticket for their operation.

## 8.2 Authentication Server Database

To achieve maximum security, Authentication Server uses the database in the following way:

- ❖ The Authentication Server works via its own database account.
- ❖ The database connection is secured. The exact procedure depends on the database used.
- ❖ Passwords are stored as "[salted Hash value](#)" which means they can neither be read nor guessed.

Not even the system administrator can manually change the Authentication Server tables in the database, thus preventing any intentional or erroneous action that might endanger the integrity of the data. All important transactions are tracked by the Authentication Server and logged in the database.

The rights allocated to the users are also stored in the database. These include individual rights established by roles, profiles and groups. The client stores local copies (local cache) of the rights on a temporary basis for the purpose of customizing the user interface.

Because rights are stored in the database, failed application components will not cause access problems due to missing rights, as long as redundant application components can take over the tasks.

The client does not require access to the Authentication Server database, only to the address of the appropriate Authentication Server (plus the Backup Authentication Server). This information resides in a local XML file.

## 8.3 Backup

Backup operations should be in place for the data and documents within the DocuWare system, just as for any environment. In the case of autonomous database servers, the backup of database data should be embedded in the company-internal procedures.

To do this, all system and organization relevant properties are stored in the DWSYSTEM database. We recommend for this database to be backed up at least once a month, but certainly after any extensive modifications (for example after synchronization of many users).

The data in the file cabinets are stored in the DWDATA database. During normal operation, this database ought to be backed up once a week.

In addition, the file cabinet contents themselves, i.e. the documents and associated XML files, must be backed up. This can be done using traditional procedures such as tape backups with "generation" procedures. However, it may be necessary to consider the very large data volumes in file cabinets which may not make it practical to use full backup. In such cases, incremental backups are usually preferable, as this method will keep the data volumes to a manageable level. Similar considerations apply to fulltext index files.

If (optical) removable storage media are used, creating manual copies of the production media might be the simplest solution. Depending on the storage sub-system<sup>3</sup> it may be possible to automatically create parallel backup media. Certain sub-systems implement redundant storage procedures or automatic mirroring, which to a large extent take the place of traditional backup procedures.

DocuWare functions too can be used for backup purposes. File cabinets including associated index data can be copied via the export options<sup>4</sup> and thus act as backups.

---

<sup>3</sup> Details see White Paper on "System Architecture"

<sup>4</sup> See also "Predefined Processes" in the White Paper on "System Architecture"

It is worth considering also that the creation of master/satellite file cabinets provides a very elegant option to resolve the backup problem without any manual intervention. Synchronization can then be used to automatically update the backup copy. What you need is sufficient storage and transmission capacity in the infrastructure.

Thus, you might set up a satellite file cabinet purely for backup purposes at another connected site, and then synchronize this automatically with the master file cabinet, for example every night.

## 8.4 Recovery

Access to stored documents is always via the index data in the database. Without this information, recovery is practically impossible. It is clear therefore that a loss of this information would be a major disaster and must be prevented.

We have already described the backup procedure for the database and the document store (documents and XML header files). These backup copies ought to enable you to restore the system and file cabinet to the state they were in at the time of the most recent backup.

The recovery as described here is for emergency cases only, i.e. for situations where the backup copies of the database are not available or are not usable because of technical issues. Note that with large-scale file cabinets recovery can take significant amounts of time.

In order to restore index data DocuWare uses the principle of "double data retention". This works by writing an additional copy of the index data for each document into the XML header file.

To restore a corrupt database, DocuWare needs the following information:

- ❖ the database fields, i.e. the structure of the database
- ❖ the file cabinet paths of the document files
- ❖ the index information for the stored documents

To provide the required information, the following questions must be considered:

- ❖ Is there an error-free (non-corrupt) backup copy of the database?
- ❖ Are all document files that are needed for the recovery actually available?
- ❖ Were all index entries also written to the header?

Since the index entries are contained in the header files, the required document stores must be available during the recovery operation.

A special challenge arises in cases where on account of revision-proof archiving requirements, documents and XML files were stored at a very early stage to non-modifiable storage media (e.g. WORM). In such a case it may not be possible to completely restore the index data, since changes that were made after the backup operation are no longer available because they could not be updated in the header (header was write-protected).

To conclude therefore we emphasize once again that conventional backups should only be used as an emergency solution, as they cannot ensure a complete recovery.

## 9 Logging

DocuWare provides a very flexible, powerful and easily customizable logging function for recording all relevant events. This serves as an optimal support mechanism for identifying the causes of any problems and for system monitoring purposes, and it can also act as the basis for invoicing services.

### 9.1 Log types

Each DocuWare server module is responsible for logging its activities. Depending on the rules that have been set up and the server module, administrators can selectively enable and disable logging functions.

Logging functions are subject to the DocuWare rights administration. In the same way as administrator roles, the following logs have been set up and must be configured by the administrators:

- ❖ System log
- ❖ Organization log
- ❖ File cabinet log

In addition, special logs are available for the predefined workflows in order to provide elegant monitoring for these automated processes.

The logging function can be customized to suit the requirements of a company. A wizard assists with the configuration. The usual procedure for defining a log includes these steps:

1. Definition of relevant events and target formats
2. Definition of the objects to be logged
3. Specification of the information to be logged
4. Definition of filters (e.g. if events are to be logged only if they were triggered by a particular user)

First, you decide what type of event (logging level) is to be recorded where. Then you specify the log content with the relevant objects and the information to be logged.

### 9.2 Logging Levels

For logging, you have a choice of different target formats (database, XML file, formatted file) and different events (information, warning, error, critical error). A lower level includes the events of a higher level. This means that enabling the "Information" level will produce a log of all events.

Errors of the "Error" and "Critical error" levels can automatically be added to the Windows log. These cases also permit automatic sending out of e-mails.

Events and their significance:

- ❖ **Critical error:**  
An unexpected error for which there is no standard handling routine.
- ❖ **Error:**  
Error for which handling routines exist, for example if a particular document cannot be accessed.
- ❖ **Warning:**  
An operation could not be performed, but the workflow is not adversely affected, for example: missing rights for writing index data.
- ❖ **Information:**  
Additional information on events that might be interesting for administrators.

Each event that causes a deviation from the planned sequence can generate an entry in the log. This means that logs capturing all events at runtime can become very large, thus adding to the system load. For this reason, you are advised not to log anything but errors during normal operation (see also [predefined logging](#)) and to enable additional information only during debugging.

For audit purposes you can use comprehensive logging at file cabinet level, for example if you wish to track changes of index data in the log.

### 9.3 Log Content

Events that are relevant for logging purposes are changes to the configuration by the administrators on the one hand and events that occur during runtime on the other.

Administrative events that are generally logged are the creation, modification and deletion of defined objects. The following table lists the objects that are logged during administration.

System level	Organization level	File cabinet level
<ul style="list-style-type: none"> <li>○ Authentication Server</li> <li>○ Content Server</li> <li>○ Workflow Server</li> <li>○ Connections</li> <li>○ Storage locations</li> <li>○ External user directory</li> <li>○ Time stamp service</li> <li>○</li> </ul>	<ul style="list-style-type: none"> <li>○ Licenses</li> <li>○ Clients</li> <li>○ Private and public stamps</li> <li>○ Viewers and editors</li> <li>○ External select lists</li> <li>○ Validations</li> <li>○ Baskets</li> <li>○ Miscellaneous settings</li> <li>○ User synchronization</li> <li>○ User administration</li> <li>○ Signature types</li> <li>○ Workflows:</li> <li>○ File cabinet synchronization</li> <li>○ Export</li> <li>○ Migration</li> <li>○ Converting DocuWare-4 file cabinet</li> <li>○ Restoring index</li> <li>○ Fulltext service</li> <li>○ AUTOINDEX</li> <li>○ DocuWare REQUEST</li> <li>○ Deletion</li> <li>○ SAP barcode transfer</li> </ul>	<ul style="list-style-type: none"> <li>○ General</li> <li>○ Database</li> <li>○ Documents</li> <li>○ Disks</li> <li>○ File cabinet profiles</li> <li>○ Search dialogs</li> <li>○ Store dialogs</li> <li>○ Result lists</li> <li>○ Link</li> </ul>

Table 1: Object types for logging within Administration

The log entry comprises:

- ❖ Name of setting
- ❖ Object type
- ❖ GUID
- ❖ User making the change, with name and organization

A filter can be used to further restrict the events to be logged. This allows one, at system level, to filter organizations, and at organization level, to filter file cabinets and users.

	System level	Organization level	File cabinet level
<b>Events</b>	Open and Close	Open and Close	Open, Modify and Close
<b>Objects</b>	<ul style="list-style-type: none"> <li>○ Authentication Server</li> <li>○ Content Server</li> <li>○ Database connection</li> <li>○ Storage location</li> <li>○ External user directory</li> <li>○ Time stamp service</li> </ul>	<ul style="list-style-type: none"> <li>○ Licenses</li> <li>○ User synchronization</li> <li>○ Additional organizations</li> <li>○ File cabinet synchronization</li> <li>○ Export</li> <li>○ Migration</li> <li>○ Converting DocuWare-4 file cabinet</li> <li>○ Restoring index</li> <li>○ Fulltext service</li> <li>○ AUTOINDEX</li> <li>○ DocuWare REQUEST</li> <li>○ Deletion</li> <li>○ SAP barcode transfer</li> </ul>	<ul style="list-style-type: none"> <li>○ Document</li> <li>○ Search dialogs</li> </ul>
<b>Object filters</b>	<ul style="list-style-type: none"> <li>○ Organization</li> <li>○ Server name</li> </ul>	<ul style="list-style-type: none"> <li>○ File cabinet</li> <li>○ User</li> </ul>	<ul style="list-style-type: none"> <li>○ User</li> </ul>
<b>Logged information</b>	<ul style="list-style-type: none"> <li>○ Name</li> <li>○ Object type</li> <li>○ GUID</li> <li>○ User, with name and organization</li> </ul>	<ul style="list-style-type: none"> <li>○ Name</li> <li>○ Object type</li> <li>○ GUID</li> <li>○ User, with name and organization</li> </ul>	<ul style="list-style-type: none"> <li>○ Name</li> <li>○ DocID</li> <li>○ Index information</li> <li>○ File cabinet name</li> <li>○ GUID</li> <li>○ User, with name and organization</li> </ul>

Table 2: Logging during runtime

At every level (system, organization, file cabinet) several logs can be created at the same time.

## 9.4 Storage Location and Scope

The system administrator can define settings for the data sinks to be used, i.e. for database connections or file directories. He/she can also define the maximum size of the log file. The following actions can be specified for when the maximum size is reached: Overwrite oldest files, or create a new log file.

The limits and the size of the areas to be overwritten can be selected freely. In the case of databases or XML files as storage locations, maximum size is indicated as number of records, otherwise as number of MB.

When creating new files on reaching the maximum, you can indicate a new maximum size.

## 9.5 Authorizations

The option for specifying the logging mechanism is, just like other functions, subject to the authorization concept. This provides a special right for creating and deleting logging specifications ("logging agents").

The administrator who defines a storage location for the logs can indicate whether this location may be used by other administrators, or not. If not, then only he/she can define log specifications using this storage location.

A log can only be viewed by users that have the necessary administration rights for that particular level. Thus, an organization administrator cannot necessarily view the log of a file cabinet, unless he/she has the administrator rights for it.

## 9.6 Predefined Logging

Even without any user-defined logs, certain events within the system should be recorded. To ensure this, a specification is automatically set up during installation for one log each for the system, the organization and the file cabinet levels.

When installing a new organization or a new file cabinet, these specifications are also installed by default. These are database tables with a total size of 10,000 entries maximum.

Predefined logging at system and organization level logs all errors (critical and non-critical). With file cabinets, logging includes runtime events at warning level and administrative events at error level.

Property	Default setting
General Information	
Name	DWArchiv<file_cabinet_name>
Status	started
Logging level	Error
Target	DWLOG <file_cabinet_name>
Additional output devices	none
Administrative view	
Objects	Events
All settings	Create, modify, delete
View at runtime	
Objects	Events
Exceptions	
Document	Create, delete
Potential information	
Document name	
DocID	
Index information and changes	
File cabinet name, GUID	
User name	
User organization	
Filter	none

Table 3: Example: Default logging for a file cabinet

Property	Default setting
General Information	
Name	DWOrganisation<organization_name>
Status	started
Logging level	Error
Target	DWLOG_<organization_name>
Additional output devices	none
Administrative view	
Objects	Events
All settings	Create, modify, delete
View at runtime	
Objects	
Exceptions	
Potential information	
Settings name	
Type	
GUID	
User name	
User organization	
Filter	none

Table 4: Example: Default logging for an organization

Property	Default setting
General Information	
Name	DWSystem
Status	started
Logging level	Error
Target	DWLOG_SYSTEM
Additional output devices	none
Administrative view	
Objects	Events
All settings	Create, modify, delete
View at runtime	
Objects	Events
Exceptions	
Authentication Server session	Open, Close
Content Server session	Open, Close

Property	Default setting
Database connection	Open
Workflow Server	Open, Close
Potential information	
Settings name	
Type	
GUID	
Short User Name	
User organization	
Filter	none

Table 5: Example: Default logging for the system

Wizards are provided for taking the user through the steps required for defining the logs.

There are default logs for all kinds of workflow, enabling detailed monitoring of such automatic processes.

## 9.7 Viewing the Logs

The logs are displayed in table form showing the log entries and any additional information.

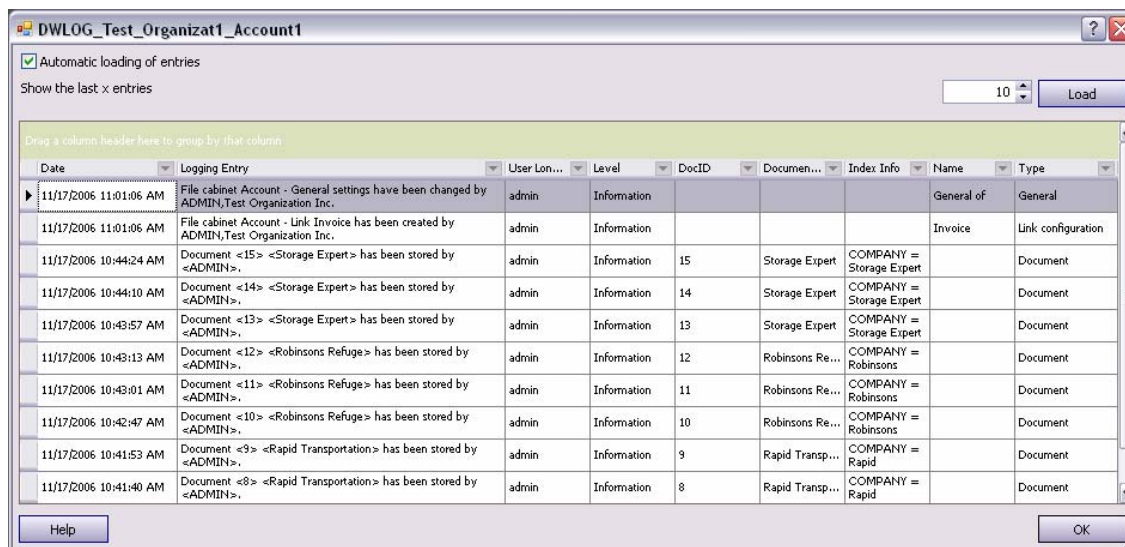


Figure 8 Log display

## 10 Glossary

Access rights	Access rights comprise access operations to file cabinets or menu functions within the DocuWare client.
Administrative rights	Administrative rights include the rights for modifying file cabinet definitions and definitions within an organization.
Authentication Server	The main functions of Authentication Server are license verification and the management of user and program rights. At start-up, each DocuWare client automatically establishes a connection to Authentication Server. This checks to see if a valid license exists for the program and for the user. Authentication Server can see which applications are running and which users are working in the DocuWare system at all times. It also handles the distribution of resources, for example by deciding which users can work with which Content Server (if there is more than one).
Certificate	For the purpose of identifying a signatory within the digital realm, a private key is needed for the signatory to produce the signature, and a public key to verify beyond doubt who is the originator of the signature. The private key must be stored securely and must be accessible to the legitimate user/signatory only. It can be held for example on a smart card. The public key - as its name suggests - must be publicly accessible. It is stored in a certificate. Qualified certificates identify the owner of a key pair unambiguously. They contain the name of the owner, his/her public key, possibly additional information on the certificate owner and information on the issuer of the certificate. Certificates and their contents are standardized to allow third parties working with another signature system to verify certificates. They are proofs of identity, issued by a trustworthy third party.
COLD	COLD is the only proprietary file format in DocuWare. It is an ANSI format and reads in the text spool data with the COLD/READ instruction.
Content Server	Content Server is responsible for the access of DocuWare clients to DocuWare file cabinets. The client cannot directly access the file cabinet documents that are stored in the directory. Instead, all file cabinet access operations must go via Content Server. If it needs information about licenses and user rights, Content Server fetches it from Authentication Server.
Document	A "document" is a term referring to all objects stored in the file cabinet which from the user's perspective form a logical unit – i.e. a document. A document may consist of any number of files. These may be scanned data in TIFF or multi-TIF format. However, files from output management systems, Office or graphics applications or even binary files are handled in the same way. A file can represent one or more page(s), but it may equally contain stamps, signatures, annotations or other, similar information associated with the document. Documents may also be files with content in different formats. They may be an Office file together with an email file and several TIFF files. Technically, every document in the file cabinet has its own directory listing the associated files, annotations, etc. A unique identification is provided by the DOCID. This technique allows sub-documents, e.g. pages, to have their own separate index information. It is also possible to generate several documents from one document and, conversely, to subsume several documents into one ("bracketing function").
DocuWare Client	The DocuWare client is the "rich client" which together with the DocuWare server constitutes a working installation on the user workstation. In principle, it can also be used via a web client. On the user side this requires nothing more than an HTML browser. In this case, an additional central component, the Internet server, takes over the client tasks and the necessary conversion for the browser.
DocuWare installation	See DocuWare system.

DocuWare Server	This is a collective term that refers to all server modules – Authentication server, Content server, and Workflow server. The DocuWare server therefore consists of several separate server modules.
DocuWare system	The DocuWare system comprises a functioning DocuWare installation with all necessary and any optional components. A DocuWare system is characterized by shared hardware and system settings for one or more "organizations". Occasionally the term "DocuWare" is used to refer to the DocuWare system.
Export	An export operation creates a copy of a file cabinet, or of individual documents. File cabinets are exported to create a backup copy or to export a file cabinet to a CD/DVD in order to use it offline. When a DocuWare file cabinet is exported, both the documents and the database are included. Export targets can be file cabinets within the DocuWare system or an external storage medium. Within the DocuWare system you can export to a new or to an existing file cabinet.
File cabinet (archive)	A file cabinet in DocuWare is a logical unit for receiving, storing, searching and retrieving documents. A file cabinet always comprises the actual storage location where the documents are physically held, with their associated database tables, index data and other descriptive or complementary elements belonging to a document. Optionally, a file cabinet may contain a full-text index which makes the documents accessible via full-text information. A range of storage media types are supported. "Logical disks" are allocated to the file cabinets which are mapped to the physical storage media according to certain rules. A file cabinet is a collection of indexed documents. For each file cabinet, granular access and administrative rights can be assigned.
File Cabinet Administrator	User who has administrator privileges for a file cabinet. This right is not transferable.
File Cabinet Owner	User who can create and manage a file cabinet. The file cabinet owner manages the file cabinet structure and allocates access rights to it. The administration right is transferable, i.e. the owner may delegate the tasks.
File cabinet profile	The file cabinet profile includes the access rights to a file cabinet. Among other things, this includes the access rights to index fields or documents that may also be dependent on certain index entries (field-dependent rights). A file cabinet profile can also include administrative rights within a file cabinet. A file cabinet profile is set up within a file cabinet.
Functional profile	A functional profile contains access rights to functions pertaining to the DocuWare client. These include the access rights to menu functions and stamps. Function profiles are defined at organization level. A functional profile can also include administrative rights at organization level.
Group	Independent of roles, users can be combined into groups to which roles can then also be assigned. A "group" is a set of users. The only way to assign rights to a group is via "roles". Groups facilitate the administration of large numbers of users.
Header	DocuWare uses XML for document storage, following the standard that is being developed by AIIM. DocuWare uses this format for storing the metadata and any additions (annotations, stamps, etc.). The actual content is stored separately (for performance reasons), except when exporting. This information is assembled in the "XML header file". Each document stored in DocuWare has a header file which is stored together with the document ("content") in the file cabinet.
Index data	See Header
Index filters	Index filters limit the access to DocuWare documents. You define the criteria each index field must contain to allow documents in a file cabinet to be retrieved or printed. Criteria for filtering documents can be text entries such as name and date, or numeric entries.

Inherited/Explicit rights	In terms of user rights, DocuWare distinguishes between inherited and explicit rights. Example: A user is assigned the "Advanced user" profile. This profile covers all functions within the DocuWare main window. The user inherits all these functional rights through being assigned the profile. Result: If this right is removed from the user, he/she also loses all his/her inherited rights. He/she can no longer use the functions within the main window. However, it is also possible to assign the functions of the DocuWare main window explicitly, rather than through a profile. This means, the user can continue to use those functions, even if the profile "Advanced user" is removed.
JPEG	Acronym for Joint Photographic Experts Group. Specification for compressing color images with a certain loss of quality. Loss of quality means that certain image information is irretrievably lost. JPEG is used to compress images with a large color space (great bit-depth). In such cases, the recommended option is PNG.
Logging Agent	A logging agent is a job that includes certain logging options and gathers relevant information. A logging agent can log events of different organizations and write them to different logging destinations. A logging destination is always either a file or a database entry.
Logging target (destination)	A file or database connection to which the logging entries are written.
Mass signature	DocuWare allows you to automatically affix signatures to documents (that have been scanned in, for example) in the "letter basket". The signing process is triggered between the documents entering DocuWare from the scanner and being stored in the file cabinet.
Master file cabinet	A master file cabinet is a file cabinet from which synchronization of DocuWare file cabinets is initiated. It functions as the base, or main, file cabinet. Any number of satellite file cabinets can be synchronized with the master file cabinet, i.e. brought up to the same status.
Menu function	A menu function is a function within a DocuWare client. This includes scanning and displaying or editing of documents.
Meta data	See Header
Migration	Migration is the transfer of documents within a file cabinet to another <a href="#">disk</a> with a different disk number. Usually, you start a migration workflow when you want to reduce the disk sizes within a file cabinet, or to combine (merge) disks. For example, you can save a file cabinet to disks with the capacity of a CD/DVD in order to prepare for transfer to an external storage medium.
Organization	An organization in the sense it is used here refers to the management of users. No hardware administration is performed within the organization. All system administration takes place at system level.
Organization administrator	As the name suggests, the organization administrator manages an organization. A DocuWare system may contain one or more organizations. The organization administrator manages in particular the rights and users belonging to an organization. He/she does not have access rights to file cabinets and their administration.
PNG	Acronym for "Portable Network Graphic" format, pronounced ping). The format that was developed and established as a standard by the World Wide Web Consortium (W3C) is license-free and is expected to replace GIF and image compression – without serious quality impairment.
Predefined roles	Predefined roles are supplied with the DocuWare system; they guarantee that the system works immediately after it has been installed. Pre-defined roles are: system administrator, organization administrator, and file cabinet owner.

Profile	Profiles are a collection of individual rights. They are divided into file cabinet profiles and function profiles. They can contain either administrative rights or access rights, e.g. to a file cabinet.
Qualified Electronic Signature	A so-called "token based" signature is an advanced or qualified electronic signature. It always requires a certificate. This certificate allows the signatory to be identified beyond doubt - even outside of the DocuWare system. The certificate administration function provides a number of different types of electronic signatures. A type acts as a filter that is applied to a certificate.
Rights	Rights allow the execution of particular functionalities within the DocuWare system. Individual rights can be allocated in file cabinets and at organization level.
Role	Within enterprise organizations, users are assigned different roles according to their place in the hierarchy (e.g. approval of vacation requests) and on their job description (e.g. purchaser). These roles can be mapped in DocuWare in order to simplify installation and administration. This is achieved by combining functions and access rights into profiles which in turn are allocated to roles. The DocuWare system also makes use of the role concept: certain roles with their associated profiles are predefined for handling administrative tasks. A role is a collection of profiles. Roles cannot contain individual rights. Predefined roles facilitate the allocation of administrative rights.
Satellite File Cabinet	A satellite file cabinet acts as the target file cabinet during synchronization of DocuWare file cabinets. The point of departure for a synchronization is always the master file cabinet. After synchronization, the satellite file cabinet contains the same documents and database entries as the master file cabinet.
Search dialog	DocuWare provides search dialogs for searching and retrieving documents stored in a file cabinet. A search dialog contains input fields that are labeled with the name of the index fields. You use these to enter your search terms. For example, you want to look for the company name <i>Müllermann</i> by searching all index fields with the <i>Company</i> label. DocuWare search dialogs can be defined for each file cabinet and assigned to users and to file cabinet profiles.
Select list	DocuWare provides users with select lists in store and search dialogs to help them to select entries for index fields and work faster. Select lists are defined at organization level and can be used by all file cabinets within the organization.
Simple electronic signature	A simple signature is for signing off, approving or releasing a DocuWare document. It is used within the DocuWare supported workflows. Once an electronic signature has been applied, actions such as adding comments or other stamps (except for other electronic stamps), merging, deskewing, and converting are no longer possible. When an electronic signature is set, DocuWare automatically generates a checksum. An electronic signature ensures the integrity of a document within the DocuWare system.
Store dialog	Before a document can be stored in a file cabinet it must be indexed so it can be retrieved easily in a search operation. The store dialog is used to store and index documents. DocuWare store masks can be defined for each file cabinet and assigned to users and profiles.
Synchronization	DocuWare permits the synchronization of two file cabinets at a time. The synchronization includes both the documents and the database. The starting point for a synchronization is always the source file cabinet, i.e. the master file cabinet. The destination is always a so-called "satellite" file cabinet. This may be a DocuWare file cabinet on a laptop that needs to be able to work with the latest documents in a master file cabinet without having access to the network. Synchronization can operate in both directions, i.e. from the master to the satellite and vice versa.
System	See DocuWare system.

---

System Administrator	The system administrator manages the system, particularly as far as hardware is concerned. This includes the administration of database connections, administration of communication paths, and document storage paths. The system administrator has no access rights to organizational information. In particular he/she cannot interfere with user administration.
Ticket	When a user logs into DocuWare and confirms his or her identity with the correct password, he/she obtains from the Authentication server a "certificate", or ticket as proof of his/her identity. This ticket gives you access to the DocuWare servers and their services. For security reasons tickets have a limited life span.
TIFF	Tagged Image File Format: The most important format in DocuWare is black and white (1 bit) TIFF, compressed according to CCITT Group 4. This format has become the established standard for electronic archiving of scanned documents. For the purposes of archiving, DocuWare generates a file for every page of a document.
Time stamp	Time stamp services are service providers that offer time stamps. Communication with an external provider is via the Internet. Alternatively, you can use internal services, provided you have the necessary hardware and software installed. In that case, access to the service is via the internal network.
User	Users have different roles within enterprise organizations. These roles can be mapped in DocuWare in order to simplify installation and administration. This is achieved by combining functions and access rights into profiles which in turn are allocated to roles. In the context of this White Paper, a user is always a DocuWare user. Users can be combined into groups. Users obtain rights by means of individual rights, profiles, or roles.
Workflow	A workflow is a predefined sequence of steps which DocuWare performs automatically when a predefined event occurs.
Workflow Server	The Workflow server is the module that executes the workflows at runtime.
XML	See Header

## 11 Appendix

### 11.1 Procedure for Developing Groups and Roles in an Organization

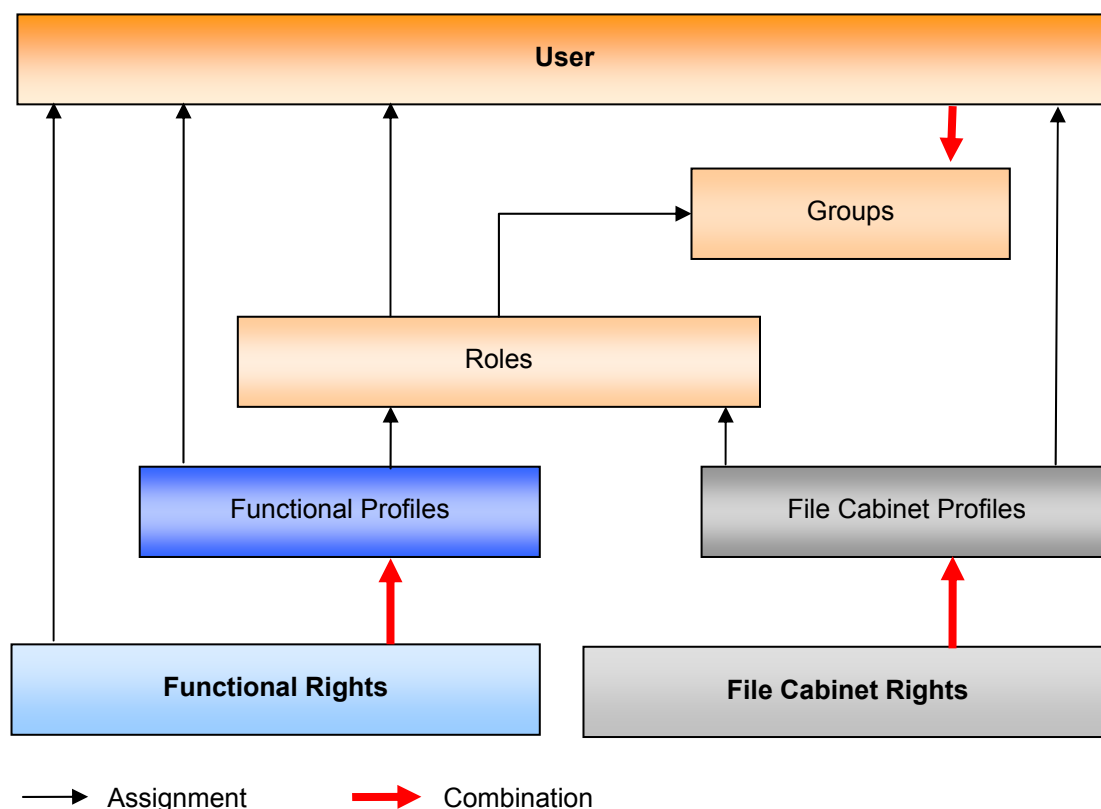
There are two ways for preparing the allocation of rights in DocuWare. You can start from the functions, analyze these and allocate them to the users within a rights canon. Alternatively, you can start by assigning individuals to groups and then make the functions available to these groups by defining roles.

#### 1. Functions perspective

The first step is to establish areas of responsibility and activities and to determine what rights and functions are needed in the DocuWare system to provide the necessary functionality. From this, you can then create different roles and assign these to the individual users. With larger organizations it is advisable to assign individuals to groups (for example the employees in a department) and to then assign the created role to these groups.

#### 2. Staff perspective

If you are used to working with groups in your user administration, you can do that in DocuWare too. In this case you first create groups to reflect the activities carried out by the members of staff in the company. You then provide these groups with the necessary rights by assigning roles to them. When new users arrive, you simply add them to the group that has the appropriate rights for their particular responsibility.



## 11.2 Definition of Rights in File Cabinets

For each file cabinet, search and store dialogs, result displays and information dialogs are defined.

In the search and store dialogs you can specify which index fields will be visible to the user. You can also predefine entries for the index fields. You can make these entries editable for the users, if you want to make it easier for them to enter information, or you can make them uneditable, if you do not want to give users a free choice. Fields that are not visible can also contain predefined entries.

### Example:

If you want external workers to have access to released documents only, you can provide them with a search dialog in which the *Document status* field has *Released* as its predefined index term (which you make uneditable). This field with its predefined entry can be applied to a search, without appearing on the search dialog. It is then not obvious to the external worker that he/she is performing a restricted search operation.

With result lists, you can decide which columns will be displayed: You specify the index fields who entries will be shown. In addition, you can define the functions that you want to be available via the result list. For example *Print document*, *Open document in Editor*, *Copy document to basket*.

For the Info dialog which is accessible from the result list and which allows you to edit the index terms, you can specify which fields you want to display, and which you want to make editable.

What options a particular user has within a file cabinet is determined by the rights and dialogs (i.e. the "tools" he/she has been assigned for working with the particular file cabinet.

### Example of the interaction between dialogs and file cabinet rights:

- If a user has the search right for a file cabinet but has not been allocated a search dialog they cannot perform a search, since that tool is not available to them.
- If a user is not allowed to search a particular index field but has been allocated a search dialog containing this field, they cannot enter anything into it - and hence not carry out the search. In this case the "forbidden" field is grayed out.
- Two users have a result list which provides the *Export to file system* option in its toolbar. One user has the *Export* file cabinet right and can therefore make use of this option. The other has not been given the *Export* right. His result list does not contain the *Export to file system* symbol.
- A user has the right to write to an index field, for example *Status*. If this user is then allocated an Info dialog which does not show the *Status* field, there is no way they can modify the entry.

### Example of the interaction between field settings and file cabinet rights:

- A file cabinet field has been defined with the *Not empty* option. This means this field must have an entry, otherwise the document cannot be stored.  
If, for this same file cabinet field, a user has the *Field may be empty* right, that user can store documents without having to make an entry in the field.
- A file cabinet field has been defined with the *From select list only* option and a user has the *Allow entries not in select list* right. This user is then authorized to use index terms that are not part of a select list.
- A file cabinet field has been specified as a *Fixed value* in the Store dialog, and a user has the right to modify index entries. This user is authorized to change the fixed field entry in the Store dialog and/or in the Info box of the result list.

The general rule therefore is that any rights assigned direct to the user have higher priority than generic file cabinet rights.

## Select Lists

Select lists can be set up for file cabinet fields. You can restrict access to these lists in the Search, Store and Info dialogs. You might want to assign select lists such as "zip North", "zip South", "zip East" and "zip West" to the "Zip code" field. You then restrict the dialog for staff working on the South to displaying the select list "zip South" only. This prevents erroneous and inconsistent data entries.

## 11.3 Using Index Filters in File Cabinets

Index filters are used to assign restricted rights to users within a file cabinet, depending on the index entries contained in the document. For the purpose of allocating index filters to file cabinet profiles, the contents of text fields, numeric fields and date fields may be used.

**Example:**

Members of the marketing team are allowed to read all documents in a file cabinet, modify the index terms of documents belonging to their own department, and edit documents that they themselves have stored.

This involves assigning the following rights:

Profile 1: **General file cabinet rights:** Search, read and access the dialogs

Profile 2: **Index filter 1:** If the *Department* index field contains the entry *Marketing*, this means that the right to modify index terms has been allocated.

Profile 3: **Index filter 2:** If the *Stored by* index field contains the name of the current user, the right to edit documents has been allocated.

If a user is assigned a file cabinet profile with index filters they must be given at least one other file cabinet profile without index filters. A profile containing index filters must always be combined with more generic profiles which provide the appropriate tools such as dialogs.

Administrative file cabinet rights, such as the right of the file cabinet owner, cannot be assigned with index filters, since no index information about a document is available to the administrative function.

The rights in the file cabinet profiles (of which there must be at least two) must be finely attuned to each other. Note that rights in DocuWare are always additive.

When assigning access rights via index filters, this means: The general profile gives the user the right to store documents. The search right, which he is assigned via a profile containing index filters applies to documents with a particular index entry, such as the name of the current user. In this way, a user can always store documents, but may display only those documents in the result list that have his or her name in a particular index field.

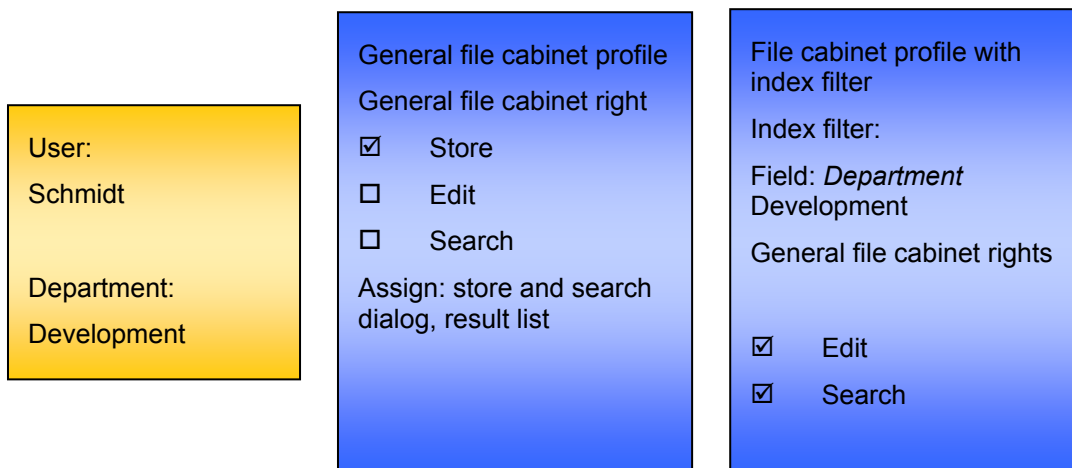
### Examples for combining file cabinet profiles

**Objective:** User Thomson may search and view all documents in the file cabinet, but only modify the index entries of documents that she stored herself.

**Solution:** The user is assigned a general file cabinet profile in which the general file cabinet rights *Search* and *Display* are enabled. At the same time, this profile gives the right to use the standard search dialog. The right to edit documents from the file cabinet is disabled. The user is assigned another file cabinet profile with index filter criteria. The index filter relates to the *Stored by* field and contains the user name of user Thomson. The general *Edit* file cabinet right is also enabled in this file cabinet profile. With these two file cabinet profiles, user Thomson can search the whole file cabinet but only modify the entries of documents that she stored herself.

**Objective:** User Smith can only store documents in the file cabinet and search for documents that belong to his department. He works in development. He is allowed to edit index entries of documents from his department.

**Solution:** User Smith is assigned a general file cabinet profile with the right enabled to store documents in the file cabinet. This profile assigns him the right to a store and search dialog. The general *Search* and *Edit* file cabinet rights are permanently disabled in this profile. In addition, user Smith is given a file cabinet profile with an active index filter. The *Department* index field contains the *Development* filter criterion. The general *Search and Edit* file cabinet rights are also enabled in this file cabinet profile. These two file cabinet profiles allow user Smith to store documents in the file cabinet, search for documents from his own department and modify the index entries.



## 11.4 Procedural Examples

The following tables are designed to help with setting up configurations. They can be customized to suit your own requirements. We recommend following the steps described below.

### Assigning Users to Groups

Defining groups and allocating users depend on the company's structure.

Users	Groups	[G1]	[G2]	[G3]	[G4]
[User1]					
[User2]					
[User3]					

### Assigning Roles to Groups

Defining roles is typically based on the tasks within processes (workflow organization).

Roles	Groups	[G1]	[G2]	[G3]	[G4]
[Role1]					
[Role 2]					
[Role 3]					

### Assigning Profiles to Roles

Defining profiles is typically based on the tasks within processes (workflow organization). However, compared to roles, profiles have a finer granularity. Once the profiles are defined, they are allocated to roles.

Role	[Role1]	[Role2]	[Role3]	[Role4]
<b>Profile</b>				
[F_Profile1]				
[F_Profile2]				
[F_Profile3]				
[A_Profile1]				
[A_Profile2]				
[A_Profile 3]				

## 11.5 Functional Rights

Functional rights come in two categories: rights for DocuWare Administration and rights for the DocuWare Main window, the DocuWare Viewer and the ACTIVE IMPORT module.

### Functional Rights for DocuWare Administration

These are the administrative functional rights:

- Create, modify and delete file cabinet
- Create, modify and delete stamps
- Create, modify and delete viewers and editors
- Create, modify and delete select lists
- Create, modify and delete logging agents
- Create, modify and delete users, groups, roles, and profiles
- Create and manage letter baskets centrally
- Manage workflows
- Create, modify and delete AUTOINDEX workflow
- Create, modify and delete barcode transfer workflow
- Create, modify and delete synchronization workflow
- Create, modify and delete export workflow
- Create, modify and delete migration workflow
- Create, modify and delete conversion workflow
- Create, modify and delete fulltext service workflow
- Create, modify and delete restore workflow
- Create, modify and delete user synchronization workflow
- Create, modify and delete the DELETE workflow
- Create, modify and delete the REQUEST workflow
- Create, modify and delete workflows for registering file cabinets

### Functional Rights for the DocuWare Main window

These rights reflect the functions of the main windows which are available via the menu. These are:

*File* menu

- Basket administration
- File cabinet administration
- Print
- Direct print
- Fax
- Import
- Export

*Edit menu*

- Scanning per document
- Scanning per sheet
- Move to trash
- Viewer
- Editor
- Delete
- Staple
- Unstaple
- Copy to basket
- Move to basket
- Update
- Language
- Rename
- To pending box
- Send
- Select all
- Automatic storage
- RECOGNITION
- Mass signature
- Synchronize
- Auto rotate
- Create data record
- Search across multiple file cabinets
- Record CD/DVD

*Store menu*

- Store dialog

*Search menu*

- Search dialog
- Hierarchical search

*Options menu*

- Toolbar
- Basket bar
- File cabinet bar
- Folder search bar
- Status bar
- MAPI profile
- Copy settings locally
- Scanner settings...
- New user
- ACTIVE IMPORT
- Office Add-In
- Window positions
- Import settings
- Export settings

*Window menu*

- Trash can
- Pending box
- Display window 1/2/3
- Index info
- SVGA
- XGA
- SXGA
- Call individual stored window positions

## Functional Rights for DocuWare Viewer

These rights reflect the functions of the DocuWare Viewer which are available via the menu. These are:

### *File* menu

- Open
- Display linked documents
- Convert
- Close
- Store annotations
- Print
- E-Mail

### *Edit* menu

- Text annotation
- Add voice
- Merge
- Split document
- Search
- Delete annotations
- Edit color
- Edit text
- Clone window

### *Document* menu

- Next page
- Previous page
- To page no.
- Multiple pages / One page
- Display improvement
- De-Skew
- Invert
- Line enhancement
- Checksum control
- Check signature
- Signature content

### *View* menu

- Zoom-In/Zoom-Out
- Display complete page
- Display full width
- Rotate left/right
- Next document
- Previous document
- Next foreign page
- Previous foreign page
- Toolbar
- Drawing toolbar
- Personal stamps
- Public stamps
- Status bar

### *Tools* menu

- Select drawing tool
- Write text on overlay
- Draw freehand line
- Highlight with a marker
- Draw arrow
- Draw line

- Draw rectangle
- Draw filled rectangle
- Draw ellipsis
- Draw filled ellipsis
- Draw transparent/non-transparent object
- Select color
- Select line width
- Enable/Disable level 1/2/3/4/5

#### *Indexing menu*

- OCR on whole page

#### *Settings menu*

- Show
- Scan
- Point'n'Shoot
- Store OCR settings
- Store barcode settings
- Automatically check electronic signature

#### *Help menu*

- Image file info
- Image file index info

#### *Context menu*

- Copy (original)
- Copy (current)
- Copy text
- OCR – Copy to clipboard
- OCR - Copy to store dialog
- Barcode - Copy to clipboard
- Barcode - Copy to Store dialog

## **Functional Rights for DocuWare ACTIVE IMPORT**

These rights reflect the functions of DocuWare ACTIVE IMPORT which are available via the menu. These are:

#### *File menu*

- Close window
- Exit

#### *Jobs menu*

- New job
- Copy job
- Edit job
- Edit job name
- Run once
- Star job
- Stop job
- Delete job
- Browser for external database

#### *Options menu*

- Toolbar
- Status bar
- Server mode

## 11.6 File Cabinet Rights

File cabinet rights are divided into administrative and general rights.

### Administrative File Cabinet Rights

*Administrative file cabinet rights:*

- Be the owner of a file cabinet, i.e. have all admin rights.
- Modify rights, i.e. be able to change the file cabinet rights of users
- Be the file cabinet administrator, i.e. have all file cabinet rights, except *File cabinet owner* and *Modify rights*
- Edit dialogs, i.e. the right to create and modify search and store dialogs as well as result lists
- Migration, i.e. the right to execute a migration workflow

### General File Cabinet Rights

*General file cabinet rights:*

- Store
- Append
- Search
- Edit
- Display documents
- Edit documents
- Delete documents
- Export (this is needed for printing also)
- Append to Read-Only, i.e. the right to append a document to another which is on a disk for which read access only exists
- Modify Read-Only, i.e. the right to modify index entries of a document on a disk for which read access only exists
- Update header

### Field Rights

The rights that can be assigned at field level:

- Field may be empty, i.e. there is no obligation to insert an entry
- Allow entries not in select list
- Allow new entries
- Read right
- Search right
- Write right
- Modify right

### Rights through functions of the result list

For each result list dialog you can define what functions will be available. The possible options are:

- Start new search
- Nested search
- Display linked documents
- Print result list
- Modify field entry
- To CONTENT-FOLDER
- Define settings in the result list
- Open document in viewer
- Open document in editor
- Open info box
- Display previous document
- Display next document
- Voice note

- Delete marked documents
- Copy to selected basket
- Checkout
- Show/hide checked-out documents
- Copy to pending box
- Send document
- Export document to file system
- Copy document to another file cabinet
- Append document from selected basket to stored document