Electronic Signatures and Encryption
Graphical User Interface (GUI)
OpenOffice.org 2.0 (OOo) and StarOffice (SO) 8

Note: Dialog Mockups Do Not Show Final Strings. Always Use Final Strings from Tables

Document - ID	Specification Owner	Last Change	Status
	Frank Loehmann	07. December 04~~28. Sept. 2004~~	Final

Conforms to	
Applies to	Writer, Calc, Impress, Draw, Scripting
Task ID(s)	i20883, 102146
Category	Feature

5 **The following spec defines only user interface/interaction (UI/GUI).**

Abstract [1]

Security for office document content can be divided into two features, digital signatures and encryption.

Digital signatures themselves are a relative new topic for office applications. However, the requirement to protect data from being modified is existing for a long time. In the past, it has been addressed by features that protect documents from being edited within the office application. With digital signatures, these features will be enhanced to offer secure protection of document content, inside OpenOffice.org(OOo)/StarOffice (SO), and outside of it.

Macro security is a very important topic, because when you download some macros or receive them via email you can't know if you can trust them or if they may harm your system.

You can not easily figure out if the macro could do any harm, so the decision whether to trust a macro or not to trust can be made based on the trustworthiness of the macro author. But how can you know that the macro really comes from the author it claims to come from, or that it was not modified by somebody else?

The best way to do this are digital certificates and signatures. The author can sign the macro with his private keys, everybody can verify the signature with the authors public keys. The digital signature will also assure that the content was not modified.

Encryption is a feature that is supported by office applications for a long time. Enhancement in this area mainly affected the encryption algorithm itself, that became more secure. However, since there was no standardized way how encryption algorithms are applied to documents, processing such document files outside an office application was elaborate. By supporting new XML encryption standards, and due to OO.o/SO's XML file format, this will become much easier.

i-Team Members

	Name	E-mail Address
Specification Owner	Frank Loehmann (FL)	frank.loehmann@sun.com
User Experience	Frank Loehmann (FL)	frank.loehmann@sun.com
Development	Michael Brauer (MIB)	michael.brauer@sun.com
	Matthias Huetsch	matthias.huetsch@sun.com
Quality Assurance	Frank Stecher (FST)	frank.stecher@sun.com
Documentation	Uwe Fischer (UFI)	Ufi@sun.com

Approved for Implementation

[1]Michael Brauer, May 2003 source: http://staroffice-doc.germany.sun.com:8080/Projects/StarOffice/SO_6.y/PCD/StarOffice-Q-PCD.sxw

http://specs.openoffice.org/appwide/security/Electronic_Signatures_and_Security.sxw

	Approved by	**Date**
User Experience	Frank Loehmann	01/29/2004
Development	Matthias Hütsch	01/29/2004
Quality Assurance	Frank Stecher	08/13/2004
Documentation	Uwe Fsicher	07/23/2004
String Review	Paul Compton/Elizabeth Matthis	07/05/04/ 7/6/04 / 2/3/05

Document Change History

Rev. Level	Change	Initials	Date
1.0	Working of 1. Draft	FL	10/23/2003
1.1	Add Q PRD Issues	FL	10/30/2003
1.2	Create "Final" Draft	FL	01/23/2004
1.3	Work on last changes	FL	01/26/2004
1.4	Work on last changes	FL	01/27/2004
1.5	Work on finalization and splitting specification into 3 parts	FL	01/29/2004
1.5	Change "Passwort" to "Kennwort" in German	FL	04/01/2004
1.6	Add macro signing behavior and make small changes to GUI	FL	05/27/2004
1.7	Add 4 new dialogs to Add... and view a signatures + add comments from MT	FL	05/28/2004
1.8	Work on comments from FS	FL	06/11/2004
1.9	Work on comments from FS	FL	06/22/2004
2.0	Work on string tables	FL	06/28/2004
2.1	Work on comments from MT/MIB/FST	FL	07/20/2004
2.2	Work on comments from UFI	FL	07/23/2004
2.3	Work on comments from MT	FL	07/28/2004
2.4	Move new password dialogs into feature section	FL	08/11/2004
2.5	Add Digital Signature... menu entry to Tools-Macros sub menu	FL	27. October 04
2.6	Add APOC "Protected" feature to security tab page	FL	12/07/2004

Contents

http://specs.openoffice.org/appwide/security/Electronic_Signatures_and_Security.sxw

1   Glossary

Term	Description
digital signature	Forgery is a growing concern among Netizens. After all, who's to say that a message with your name on it is really from you and not somebody pretending to be you? Digital signatures are a means of proving that a file or email message belongs to a specific person, much as a driver's license proves identity in real life. Digital signatures have the added benefit of verifying that your message has not been tampered with. When you sign a message, a hash function--a computation that leaves a specific code, or "digital fingerprint"--is applied to it. If the fingerprint on the recipient's message doesn't match the original fingerprint, the message has been altered. Digital signatures are often used in combination with strong-encryption software to create a secure channel of communication, in which both privacy and identity are protected.[2]
Encryption	Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (data encryption standard) are two of the most popular public-key encryption schemes. [3]
Digital Certificate	Citing concerns about security, many people are still wary of online transactions. In an attempt to assuage those fears, software vendors, security specialists, and online vendors have developed the concept of digital certificates. A digital certificate is a password-protected file that includes a variety of information: the name and email address of the certificate holder, an encryption key that can be used to verify the digital signature of the holder, the name of the company issuing the certificate, and the period during which the certificate is valid. Certificate authorities (CAs) gather information about a person or company and then issue certificates. These certificates can be used as online identification, much in the same way a driver's license can verify your identity in the physical world. If an email message or order form comes through with an attached digital certificate, the recipient can be more confident that the document is genuine. Several technologies (including SET, SSL, and Authenticode) are currently competing for market share, each hoping

---

2 Source: http://www.cnet.com/Resources/Info/Glossary/Terms/digitalsignature.html
3 Source: http://www.cnet.com/Resources/Info/Glossary/Terms/encryption.html

Term	Description
	to become the certificate of choice.[4]
One-Way Hash Functions	A one-way hash function is an important building block to help achieve data integrity.
	Informally, a one-way hash function is a function that is easy to compute but difficult to reverse.
	Also, it is difficult to find two input values for which the function would compute the same output value.
	You can use the hash function to calculate the hash value of a document, which can be a lot shorter than the document content. This value can be stored on a separate place or as part of the digital signature. Later you can use the same hash function to compute the hash value of the current document and verify these hash value to assure the content was not altered.
Symmetric Ciphers	A symmetric cipher is a transformation, operated under a secret key, that can translate its input, called plaintext, to its output, called ciphertext, in such a way that, excluding cryptanalysis, only those entities possessing the secret key can recover the plaintext from the ciphertext.
	Examples for symmetric ciphers are the quite old Data Encryption Standard (DES) and the more secure Advanced Encryption Standard (AES) .
	Symmetric ciphers are also called secret-key ciphers because the two communicating parties must share a secret key. This requirement creates some difficulties in key management and key distribution.
	Symmetric ciphers can also be stacked to improve the crypto strength of the whole system, such as in the case of triple-DES.
Asymmetric Ciphers	An asymmetric cipher is similar to a symmetric cipher, but instead it depends on a pair of keys rather than on only one key. The public key of the pair is used to encrypt plaintext. The private key of the pair is used to decrypt ciphertext. The keys are generated such that it is easy to deduce the public key, given the private key; the reverse, however, is very difficult. This property enables people to exchange their public keys over public channels and still conduct private communications.
	A distinct property of some asymmetric systems is that the encryption and decryption are reversible. This means that one can apply the decryption operation with the private key to the plaintext to get ciphertext, and one can recover the plaintext by applying the encryption operation with the public key to the ciphertext. In this case, because the public key is public, no confidentiality protection is provided. However, because only the holder of the private key can generate the ciphertext with these systems, the ciphertext can serve as a digital signature of the plaintext, and anyone with the public key can verify the authenticity of the

---

4   Source: http://www.cnet.com/Resources/Info/Glossary/Terms/digitalcertificate.html

Term	Description
	signature.
	RSA (named for its creators—Rivest, Shamir, and Adleman) is perhaps the most widely used asymmetric system that can also be used to produce digital signatures. Another system, Digital Signature Algorithm (DSA), can perform only digital signature functions; it cannot be used for encryption.
	To prove that it is the real owner of a public key, one party can present a certificate for verification by the other party. A public-key certificate is a digitally signed statement from one entity, saying that the public key and some other information of another entity have some specific value. A chain of certificates is possible, whereby each certificate contains a public key that is used to certify the public key in the succeeding certificate. The first certificate, often called the root certificate, does not have another public key to certify it. Thus, it normally is a self signed certificate in that its own public key is used to certify itself.
Digital Certificates	Users of public-key applications and systems must be confident that the public key of a subject—a user, organization, or other entity, such as a service—is genuine, that is, that the associated private key is owned by the subject. Public-key certificates are used to establish trust. A public-key certificate is a binding of a public key to a subject, whereby the certificate is digitally signed by the private key of another entity, often called a Certification Authority (CA).
	The standard digital certificate format is ITU-T X.509.
	An X.509 certificate binds a public key to a Distinguished Name.
	Frequently, such a certificate is called an identity certificate
Authentication	A basic security issue is authentication. Authentication is the process of confirming the identity of an entity (a user, a machine, or a machine operating on behalf of a user).
Authorization	Authentication serves as the basis for authorization. Specifically, once it knows the identity of a subject, an application may then specify what set of operations that subject may perform.
	The set of permissions granted can be configured within an external access control policy.

1   Motivation

Many governments in different countries are starting to move to paper-less communication with their citizens. Examples for this are the "BundOnline"[5] e-government initiative in Germany or eGov[6] in the US.

Since in many cases confidential and personal data needs to be exchanged it is mandatory to use appropriate *security mechanisms like digital signatures and encryption*. This is necessary in order to ensure that information does not get changed on the way between the citizen and the public authority.

Also it must be possible to *securely identify the author of a document*. This is especially true for documents that are used for requesting ID related documents like a driver license, passport or a badge.

People become more and more sensitive about security issues, and macro viruses can do a lot of harm. People must have the possibility to configure which macros are allowed to run and which not, so digital signatures and authentication are very important for them.

In addition, after tragic events like the airplane attack on September 11 people are more and more concerned about security issues in general. Companies fear "cyber attacks" and viruses like the ILOVEYOU and Melissa macro virus, that caused a lot of damage.

2   User Scenarios

This specification covers security and signature related issues. So the user scenarios are separated into two parts.

2.1   Security Related Scenarios

Scenario #1: User A is an attorney at law and uses OpenOffice to **edit/revise legal related documents**. She uses change tracking in her documents very often, but she is aware of the potential danger of those   working draft information when those might become public, because others can use such information against herself. Susan spends a lot of time controlling her final documents, that they do not contain track changes information anymore, but she always has a bad feeling using change tracking function at all.

Product Requirement 1.1: Add a new application **privacy option** to warn the user about **tracked changes, versioning and notice** information in current documents when the user saves, prints (not for versioning), PDFs (not for versioning) or sends a document.

Scenario #2: User B works for the Police Department as a secretary. She works in a department working on police internal inquiries. She writes down reports recorded on tapes. Since she has fears that her name could become known to the reported person, she always takes care that she removes her name from the properties of the document before saving the file. She always has a bad feeling, because she has to do it manually, but she could not remove her name from the User settings options of OOo, because in letters templates the fields will not be filled in were she needs her name in.

Problem 1: There is no automatism to do not store personal information within the file in OOo.

Product Requirement 2.2: Add an application **privacy option** to do not add personal information to the file properties when saving a file.

Scenario #3: User C works as a Controller in a company. He creates reports in Calc about the departments he is responsible for as a financial controller. He provides his report to the executive management of the company, but the report will be forwarded to the assistant of his manger. The information he is providing is very crucial and he has fears that the data could be changed before reaching his manager. Since the manager's assistant must have rights to print the document, because his

---

5 The plan for "BundOnline" http://www.bundonline2005.de/ is to implement an security infrastructure that uses digital signatures and encryption until the end of 2005. The systems integrator CSC Ploenzke created a plugin for Adobe Acrobat that fulfills the requirements for BundOnline (German: http://www.adobe.de/products/acrobat/pdfs/CSC_Ploenzke.pdf).

6 http://egov.gov/

manager insists of having a printed copy for his records, he has to give modify rights also to the assistant.

Problem 1: No real solution for this problem until a document rights management model is supported by OOo. All other solutions like **separate passwords for opening and modifying** of a document are only generating a false sense of security, because a document that could be opened could be saved as a new doc or could be copied to a new document via the clipboard and then saved as a new file. Thus allows to modify the document's copy...

Scenario #4: User D works in a bank. He often has to **encrypt documents**, because the content is related to customer's financial background. He is used to work with MS Office and hasn't used OOo before. When evaluating OOo he tries to encrypt a document. When calling the Save as dialog, he recognizes that there is a checkbox "Save with password". He is wondering, where he has to enter the password first to save it with the file. He checks the complete dialog for options to set the password, but did not find any.

Problem 1: Problem at this point is, that he did not know that the password dialog appears when saving the document because he had never used OOo before. Once he is used to this behavior, the function could be easily accessed.

Product Requirement 4.2: Change the check box into a button. If this is not possible, the password dialog has to appear directly after checking the box or the wording has to be changed.

Scenario #5: User E works at the University: She works on confidential data for her professor, so she decides to encrypt the document. Since she has worries not to remember the password, she decides to use her boyfriend's sure and last name as a password. She types in "Greg Smith" and recognizes the space between the names. She removes the Space, since she is not sure if it is allowed within a password. Then she works on the data and saves her changes frequently. In the evening she closes the document and shuts down the computer. On the next day she has an appointment with her professor and tries to open the document. She types in "Gregsmith" in one word at the password prompt, since she remembers that she has removed the space in the middle. Then she confirms the password dialog, but the document could not be loaded and OOo raises a dialog that the password is wrong. She calls the product support to decrypt the document, but the support could not help her. The document's data is lost.

Problem 1: She does not know that passwords are case sensitive and that spaces would have been allowed within the password. Furthermore she was not aware, that there is no way back when the password is lost and so she has not stored the password in a save place.

Product Requirement 5.2: Add a hint to the password dialog to explain that passwords are case sensitive and could contain spaces and other special characters. Furthermore we have to add a note that there is no way to decrypt the file without the password.

Scenario #6: User F is a Manager: He uses many different text document templates for his work. One of these templates is used for the monthly report of his division. Since these reports contain crucial data, he must ensure that this document is always saved with a password. He is missing a document option to force or recommend encrypted saving of the document.

Product Requirement 6.1: Add a new document option to prompt a dialog when saving documents that currently have no given password and recommended to save this document always with a password.

Scenario #7: User G is an English teacher: She works on courses written as text documents. These documents will be printed by her customers at home. Some customers saved changes to the document by mistake in the past, because the documents have read write access.

Product Requirement 7.1: Already possible in OOo 1.1. to publish those document as a PDF files via the integrated PDF export. Furthermore the setting "Printing modifies document" in Tools-Option of OOo has to be deactivated. Furthermore the document could already be opened Read-only by a checkbox in the File-Open Dialog. **But maybe this one is an issue when supporting signatures, because modifying the document (properties) will withdraw document's signature.**

Scenario #8: User H has to use a specific encryption method, because it fulfills the defined security requirements

Product Requirement 8.1: User can choose between different encryption types. The dialog to choose from available methods can be called by the Tools-Options-Security-Security option-Advanced... button.

2.2 Signatures Related Scenarios

Scenario #9: Department of Defense (DOD): The DOD is currently rolling out the DOD Common Access Card to all the employees. The card holds certificates and supports Java. Microsoft offers a solution for signing emails and potentially documents using the DOD Common Access Card.

Typically a user would use encryption for the email in order to prevent that unauthorized users can access the content. Attached documents would be signed for non-repudiation and integrity purposes but not encrypted. The email would not necessarily be signed, because the enclosed document would be the critical element. Besides, it often is not desired to encrypt documents because once the email has been received the document can be stored at a secure location. However, for both encrypting the email and signing the document the same technology (i.e. the DOD Common Access Card) should be used.

Product Requirement 9.1:

Scenario #10: Government: An example for a scenario in the government space would be a foreign citizen who needs to extend/renew his passport. First, he would either download a form from a public web site or via email from a consulate employee. Maybe this form would already have some personal and confidential data. Thus this form would have to be both signed and encrypted. Now the citizen would complete the form, sign and encrypt it and send it back. Finally the consulate employee would check the content of the form and send a signed (approved) and encrypted copy back to the citizen.

Product Requirement 10.1: Sign Complete OOo Documents

Product Requirement 10.2: Encrypt complete documents

Scenario #11: Education: Signing and encrypting documents in the education area is interesting, because it can replace the paper process of correcting dissertations, etc. Students would send their signed dissertations to professors, who would make annotation, sign these annotation and send the signed document back to the student.

Product Requirement 11.1: Sign Complete OOo Documents

Product Requirement 11.2: Encrypt complete documents

Product Requirement 11.3: Protect content via password and allow to add annotations (comments) or tracked changes only

Product Requirement 11.4: Sign tracked changes or annotations **(not for OO.org 2.0)**

Scenario #12: Enterprise: In enterprise environments signed documents can replace contracts and legal agreements. For this purpose documents often go through many reviews by different people that belong to different departments and companies. Therefore, it's required that it's always verifiable who made changes to a document at what time. In addition, there are often predefined approval processes that the office suite and related collaboration tools could support.

Product Requirement 12.1: Sign Complete OOo Document

Product Requirement 12.2: Allow multiple signatures

Product Requirement 12.3: Protect content via password and allow to add annotations (comments) or tracked changes only.

Scenario #13: User AA writes contracts in Writer. The contracts will be personalized directly in Writer. Since some parts must not be changed he want's to protect these section and to sign them.

Product Requirement 13.1: Sign Section in Writer **(not for OO.org 2.0)**

Product Requirement 13.2: Protection for signed sections **(not for OO.org 2.0)**

Scenario #14: User AB works on official company wide calculations. These calculations must not be changed and are tested. The data will be collected by Managers. Each Manager saves the document after he has filled in his data and saves it as a new version in the document. This saved version will be signed.

Product Requirement 14.1: Sign Single Table in Calc **(not for OO.org 2.0)**

Product Requirement 14.2: Sign versions of a document

Scenario #15: GUI related requirements

Product Requirement 15.1: Show Signatures

1. Application title "(Signed)"
2. Symbol in status bar
3. Symbol on objects, Calc tables, sections
4. Document properties

Product Requirement 15.2: Warning Dialogs

1. Signature is lost when
    1. saving document in non OOo XML format
    2. save as (a copy) in XML-Format
    3. Deleting a signature
    4. document is modified
        1. Undo after signing = modify = signature lost
    5. Content is not completely visible due to
        1. view settings
        2. track changes with not accepted/rejected parts
        3. notices
    6. formatting (i.e. hidden)
    7. linked sections, objects (i.e. graphics, OLE or DDE)
    8. fields

Scenario #16: Renew signature if signed area has been changed

1. Withdraw all assigned signatures and sign new

Scenario #17: User AF works in a small company. They want to use signatures to sign documents, but the company do not want to create official certificates because these cost money. They want to trust themselves.

Product Requirement 17.1: Create a self signed Certificate.

2.3 Macro Security Related Scenarios

Scenario #1: Macro security

Product Requirement 1.1: Security 18: Authorization, Fine Grained Macro Security.
OOo should allow to restrict the level of access to resources that components and scripts have. Configure policies which code from which author is allowed to read and write files, make system calls and other things.

Scenario #2: Macro security

Product Requirement 2.1: Security 21: Completely disable scripting.
Done in SO7: tools/options/security => Run macro never.

Scenario #3: Security Level

Product Requirement 3.1: Security 23: Default macro security settings must be set to "high".

Scenario #4: Security Level

Product Requirement 4.1: Security 26: Support very high, high, medium and low security settings. Very high allows only execution of macros from trusted locations regardless of the signed status. Maximum security allows only signed macros to run. Medium allows signed macros to run and asks for execution of unsigned macros. Low executes all macros without any confirmation.

215 **Scenario #5:** User AD develops macros in OO.org. The macros will be attached to documents and will be used within the company. He has problems that users suppress the execution of this macro, but the companies management does not allow to disable macro warning in OO.org.

Product Requirement 5.1: Sign OOo Script Projects. The user could trust a source, so that these macros will be executed automatically without displaying any further macro warnings.

3   Goals for Macro and Document Security

220

A must have for OpenOffice.org 2.0 are digital signatures for macros and authentication, so people can configure which macros are allowed to run and which not, based on the author of the macro.

Fine grained macro security, where you can configure in detail what macros from different authors are allowed to do would be nice, but this can not be done in the OpenOffice.org 2.0 time frame, because on top

225 of digital signatures and authentication you need configuration of policies, and each API implementation that directly accesses any resources must check if the permissions for that are granted.

Please see scenario section above for detailed goals of Macro and Document Security based on digital Signatures.

4   Requirements and Dependencies

4.1   Dependencies

230

The thumbnail feature has to be adjusted when this feature has been implemented:

http://specs.openoffice.org/appwide/desktop_integration/ooo_file_thumbnails.sxw

4.2   Requirements

Please see scenario section on page 4 (above) for requirements.

4.3   Technical Dependencies

235

Please see technical specification for details:
http://specs.openoffice.org/appwide/security/Technical_Specification_for_Electronic_Signatures_and_Security.sxw

5   Competitive Analyses

5.1   Overview

5.1.1 Products and Links

- **Microsoft Office**

  (http://www.microsoft.com/office/techinfo/administration/security.asp)

- **Adobe Acrobat Self-Sign + Approval**

  (http://adobedoc.kanisasolution.com/Acrobat5/Help.htm
  http://www.adobe.com/products/acrapproval/overview.html
  http://www.adobe.com/epaper/tips/acr5digsig/pdfs/acr5digsig.pdf)

- **i.Secure Office**

  (http://www.archisoft.com.hk/secureoffice.html)

- **Lexign ProSigner**

  (http://www.lexign.com/products/lexign_prosigner.htm
  http://www.lexign.com/demos/Digital_Signatures_ProSigner.ppt)

- **SafeGuard Sign&Crypt**

  (http://www.utimaco.de/eng/content_products/sg_office.html)

- **ApproveIt Desktop**

  (http://www.silanis.com/ns/products/adt/adt.asp?sc=com)

- **VisualSoft OfficeSecure**

  (http://www.visualsafe.com/securedesktop/officesecure.asp)

5.1.2 MS Office XP and Adobe Acrobat 5.0 Comparison

The comparison table below does not include OOo and tell where it's better or worse, because almost none of the features are available in OOo 1.1.

Adobe Acrobat seems to be superior over Microsoft Office in the security area. Therefore, Acrobat should be considered the standard to which OOo has to compete against.

The green marked features are most relevant for for OOo 2.0. The yellow ones have to be further evaluated.

Feature	MS Office XP	Adobe Acrobat 5.0
Signing documents		
Sign documents	yes – Word, Excel, PowerPoint	yes
Sign parts of documents	no	no
Multiple signatures on a single document	yes	yes
Add metadata to signatures (e.g., reason for signing, location)	no (???)	yes

Certificates		
Create simple certificates	yes, command line tool	yes, integrated in application
Smart card support	yes - access via operating system APIs	partly – via 3rd party Acrobat plug-ins
Trusted user certificate list	only for macros	yes

Feature	MS Office XP	Adobe Acrobat 5.0
View signature information		
Signed (yes/no)	yes - status bar, document title ("Signed"), options dialog	yes, signature window (tree view)
Name	yes	yes
Date	yes	yes
Time	yes	yes
Verification status	yes	yes

Appearance of signature		
Visual part of the signature can be placed anywhere in the document	no	yes
Handwritten name	no	yes
Logo	no	yes
Graphic	no	yes
Text explaining signing	no	yes

Collaboration		
Track changes between signings	no (no support for multiple signatures; but support for track changes for protected documents)	yes
Retrieve earlier signed version	???	yes
Compare two signed versions	yes	yes, side-by-side in tiled window

Signature Handler		
Plug able signature handler	???	yes, Acrobat plug-in
Default signature handler	Microsoft Authenticode	Acrobat Self-Sign
Included support for commercial certification authorities	???	Entrust Security
Other support for commercial certification authorities	Entrust, Verisign, ...	3rd party Acrobat plug-ins

Encryption		
Encrypt documents	yes, Word, Excel, PowerPoint	no
Encrypts parts of documents	no	no
Pluggable encryption handler	standard encryption (backward compatibility), CryptoAPI	no

Protect Document		
Tracked changes (users cannot turn off tracking)	yes	yes (for signed documents)
Comments allowed (content protected)	yes	yes
Forms (fields can change, doc. content protected)	yes	yes
Sections (only portions of document can change)	yes	no
Disable document printing	no	yes

Feature	MS Office XP	Adobe Acrobat 5.0
Disable document changes	yes	yes
Disable selecting	no	yes

Macro Security		
Sign macros	yes	??(i.e. no special security features for built-in JavaScript support)
Only run singed macros	yes	N??
Warning for untrusted macros	yes	??
Trusted sources list	yes	??

5.2   Security Related UI of Microsoft (MS) Word 2003

Competition offers a Tools menu in the Save As and the Open dialog of Office XP. This menu offers the file operations (i.e. delete, rename and file properties) and save document related options (i.e. Security Options).
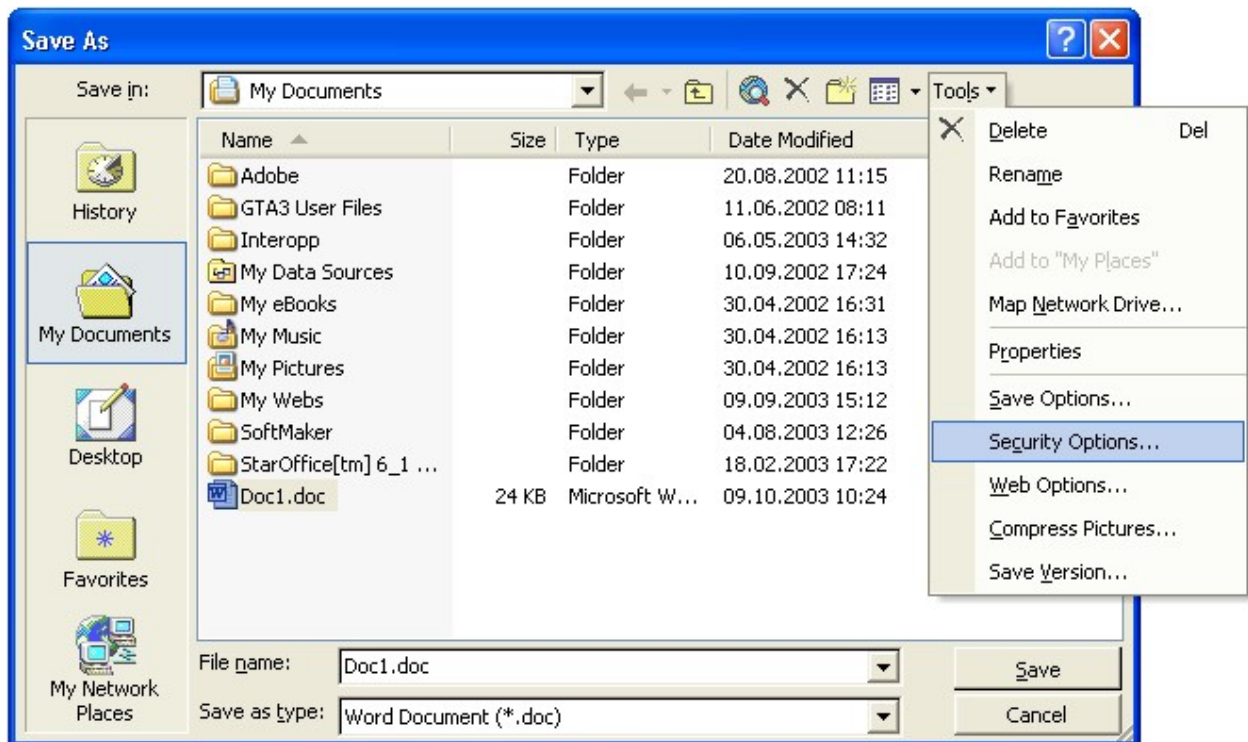
Illustration 1 File Save dialog in MS Office XP with open Tools menu

270   The file Open dialog shown below also has a tools menu. The available options are the same file related options minus the following save related options:

- Save Options
- Security Options
- Web Options

275   • Compress Pictures

- Save Version
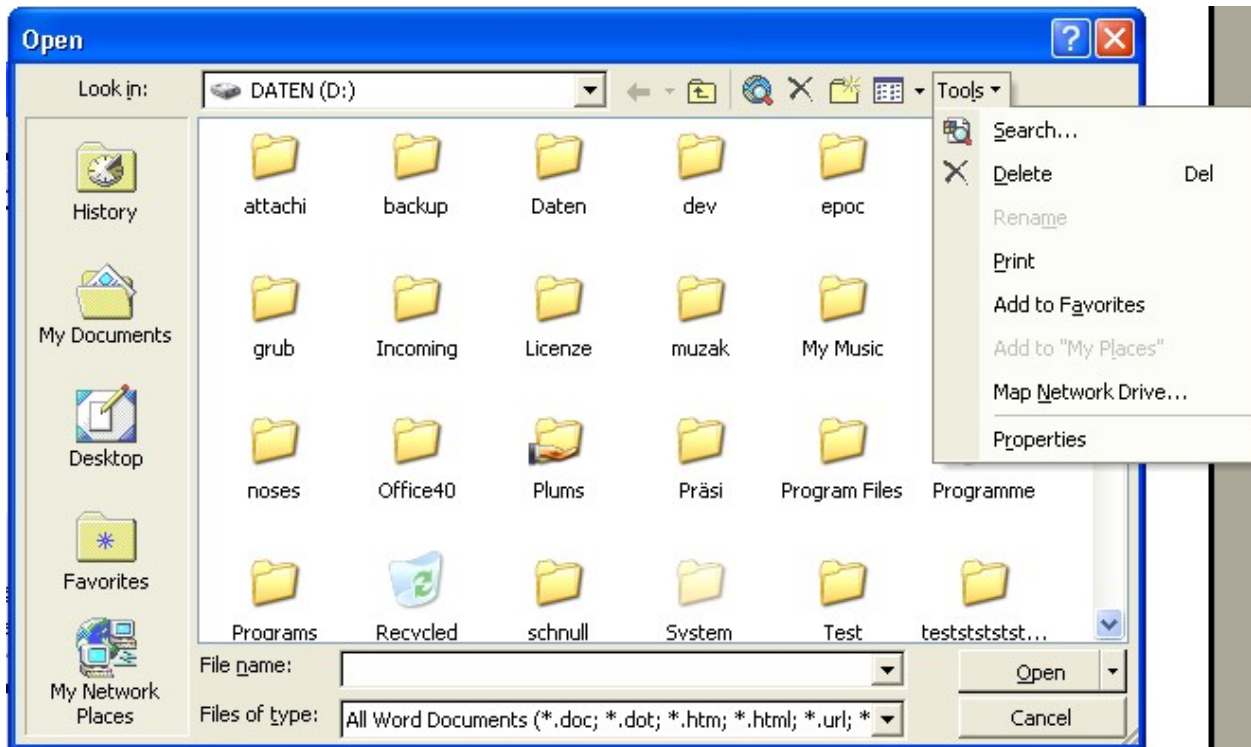
Illustration 2 File Open dialog in MS Office XP with open Tools menu

The Security dialog of MS Office XP offers settings for document **encryption** (separate passwords to open and modify documents), **digital signatures** and other protection features of MS Office. These protection features will be described below.

280   Privacy options section in the Security dialog allows to chose if a **unique identifier** (UID) is saved with the document and offers a **warning function on saving documents with redlining information**. Furthermore private information could be removed from current document, when it's being saved.
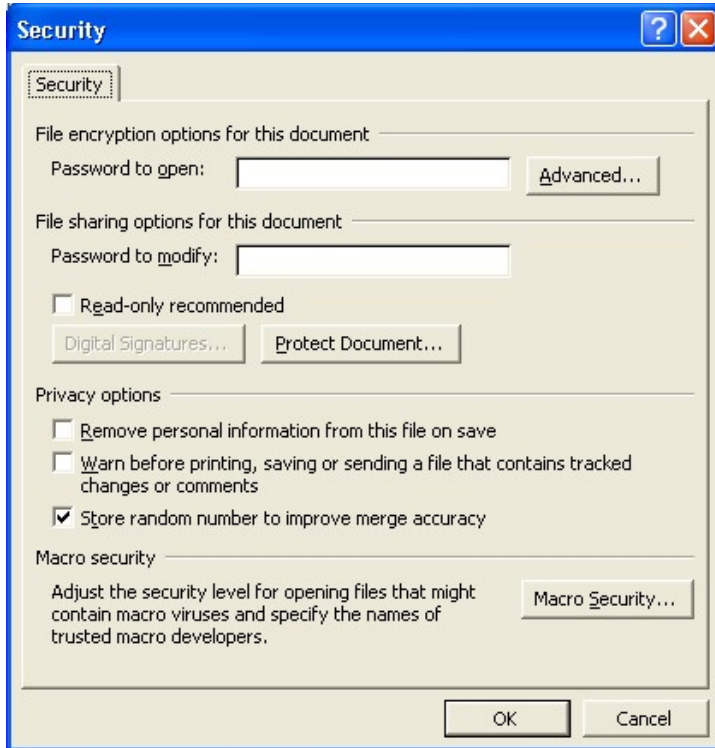
Illustration 3 Security dialog of MS Office XP

The following dialog appears if warning before saving, printing or sending document with tracked changes is active.
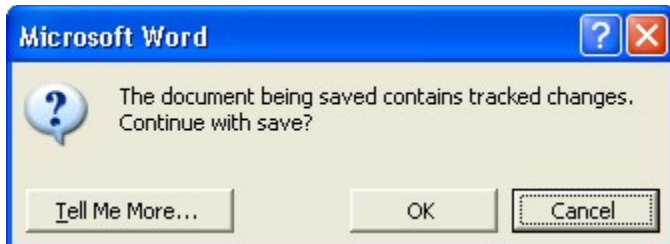
Illustration 4 Warning if track changes warning is active an
user saves, prints or send the document

285   Open a document in read-only mode could be recommended by the author by choosing "**Read-only rec-ommended**" option in the security dialog. When loading such a document, the following dialog appears on loading the document.
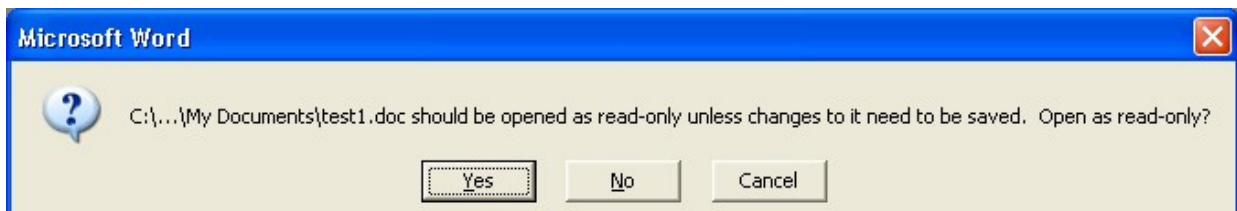
Illustration 5 Dialog comes up on loading a doc, if read-only was recommended by the author

The (Macro) Security dialog has two tab pages. The user can set a security level for the application?!
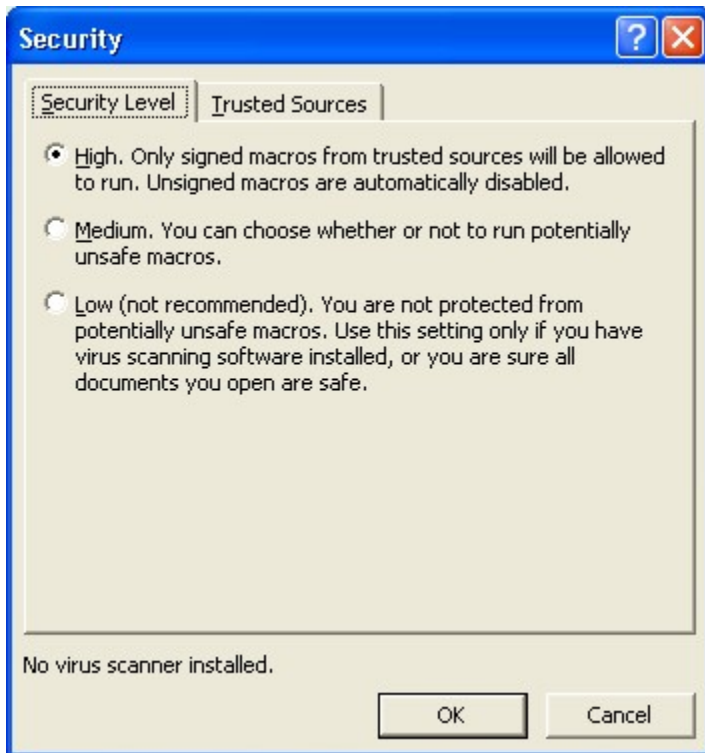
Illustration 6 Macro Security dialog – Security Level table

On the second tab the user can trust sources so that **macros signed** from those vendors could be executed without any problems.

290
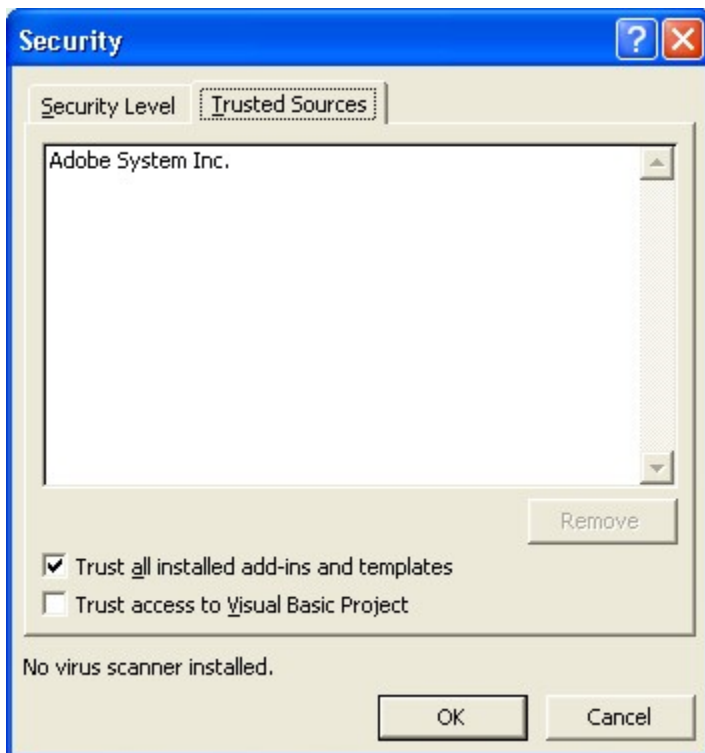
Illustration 7 Macro Security dialog – Trusted sources tab

The user can choose the **encryption type** used for the current document in the Encryption Dialog. This dialog can be reached by pressing the Advanced button. Furthermore the user can choose if the document properties will be encrypted or not.

Illustration 8 Encryption method can be chosen in Encryption Type dialog called by the Advanced button of the security dialog

The user can **protect** the document **against modification**. The user can except Sections from this protection or he can allow to add comments or redlining. The password protection for this setting is optional.

Illustration 9 Protect Document dialog
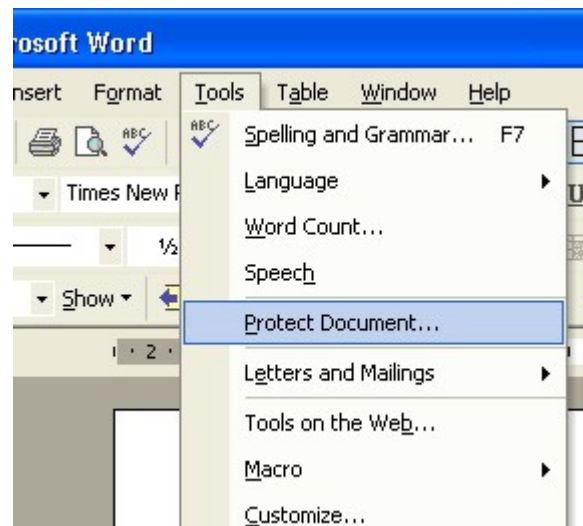
Illustration 10 Word XP Tools Menu calls dialog shown in Illustration 9

The Security dialog changes the Protect Document button to unprotect document, if protection was chosen for the document.
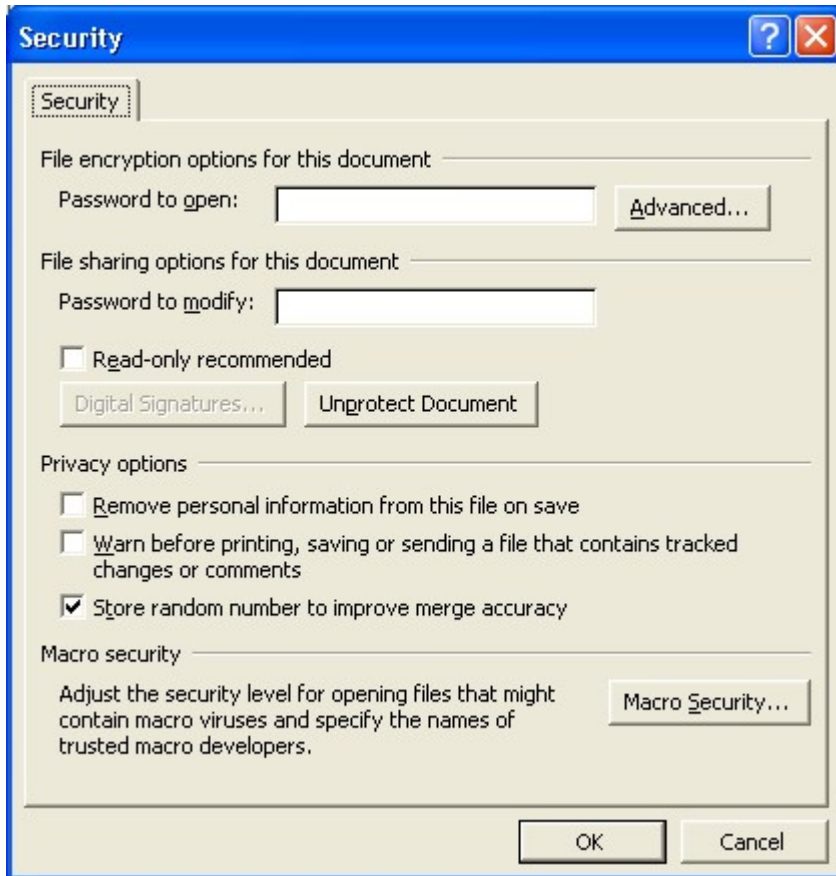
Illustration 11 Button changes to Unprotect Document in Security dialog after choosing Document Protection for current document

The following dialog is called to **confirm** a previously entered **password**. Furthermore a notice is provided to inform the user that there is no way of recovering this document, if the password is lost. And that passwords are case sensitive.

300

Illustration 12 Dialog to confirm a password to ensure that the user did not make a typo when entering the password

The Security dialog has a design problem, because two passwords could be entered at once in this dialog, but when the user confirms the dialog, the appearing password dialog does not contain any information which of these two passwords has to be confirmed.
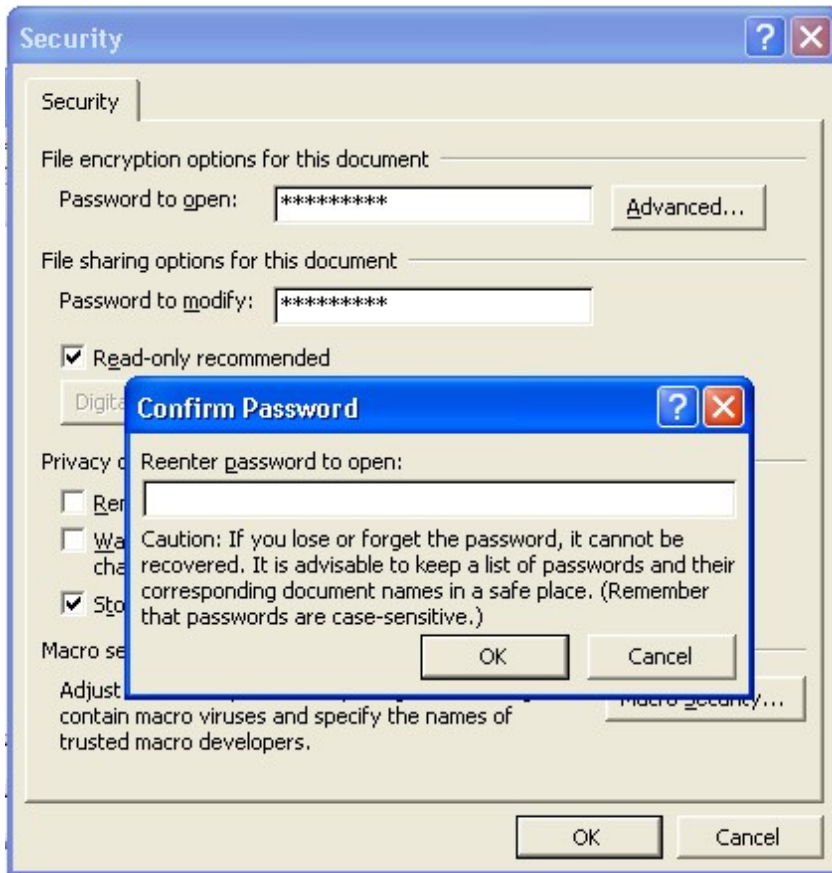
Illustration 13 Problem when confirming the dialog with two given passwords – the user does not know which password he has to confirm

The following dialog informs the user that the document's password gets lost when saving in none-native file formats.
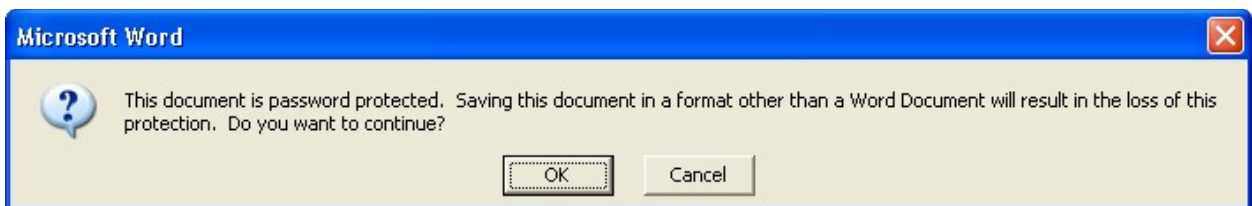
Illustration 14 Warning Dialog if the user changes the file format to not MS one

The Password dialog appears when loading a document which is protected by a password for opening the document. Dialog also shows a path information to the document being loaded.
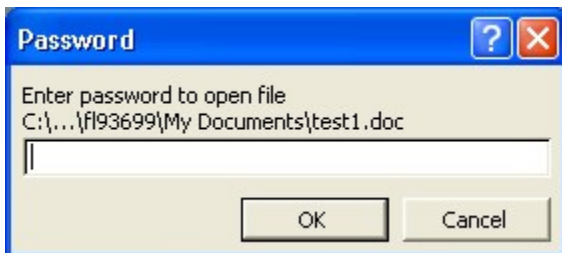
Illustration 15 Open a password protected file raises dialog

The following dialog appears if the entered password is invalid.
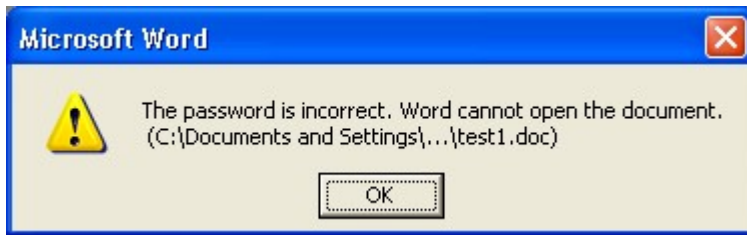
Illustration 16 Warning dialog if wrong password has been entered while opening the document

310

The Password dialog is shown if a password for modifying has been set for the currently loaded document. User can open the document in read-only if the user does not know the password by pressing the Read Only button.

Illustration 17 Second password dialog to enter write access password

If the user has entered a false password, the following dialog appears.

Illustration 18 Warning dialog if incorrect password has been entered

The Tools menu also contains a Save options dialog. The dialog contains application (Office) related settings only.
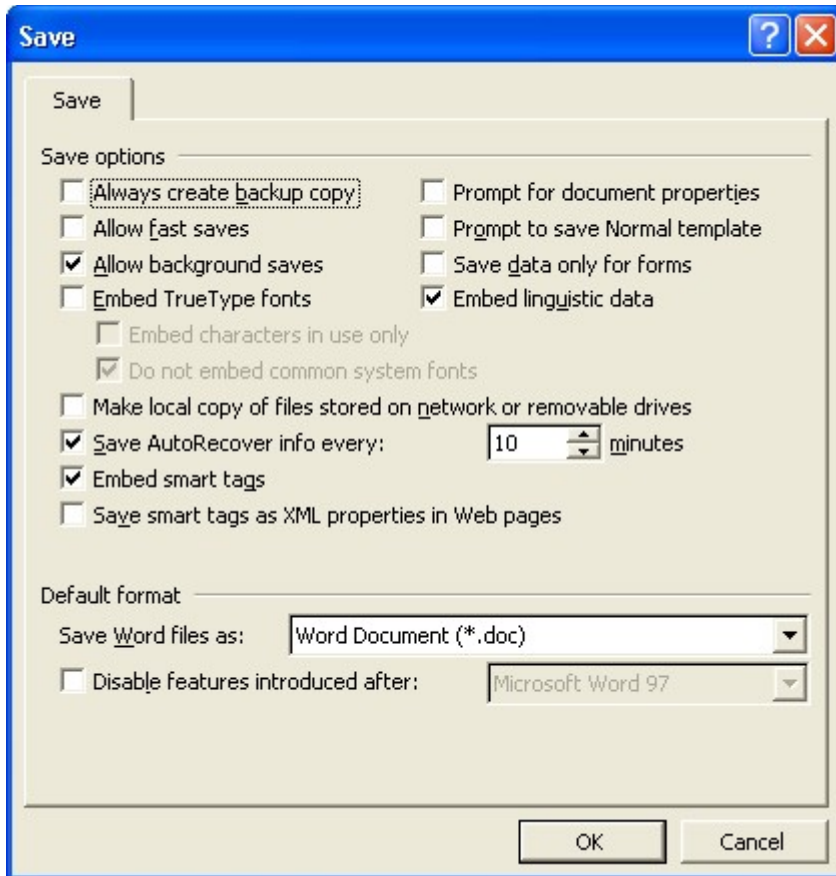
Illustration 19 Save options dialog - called from the Options menu in the file Save dialog

5.3 Signatures Related UI of Microsoft Word XP

315

5.3.1 Self Certifying Program Selfcert.exe

Microsoft Office offers a separate tool to create Selfcert.exe

Illustration 20 Self-signed digital certificate

5.3.2 Digital signature Dialog
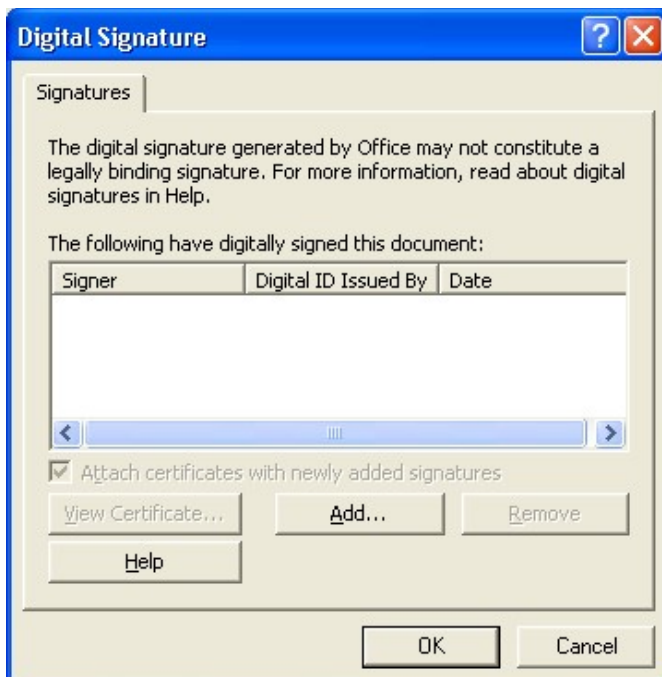
Illustration 21 Digital Signatures dialog of MS Office XP
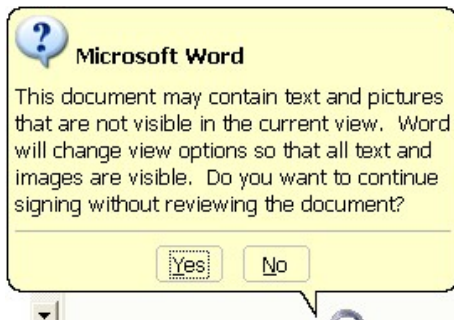
Illustration 22 Warning if a signature is added to a document and document does not show all it's content
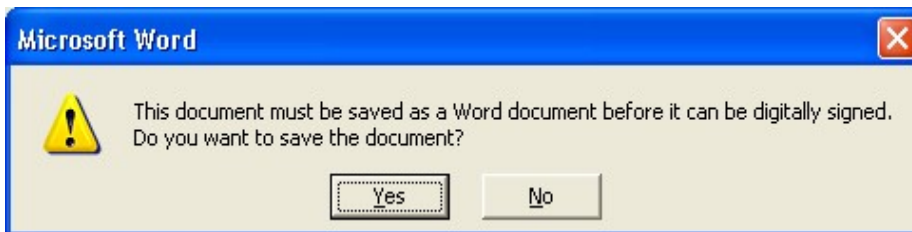
Illustration 23 Document has to be saved in Word Format
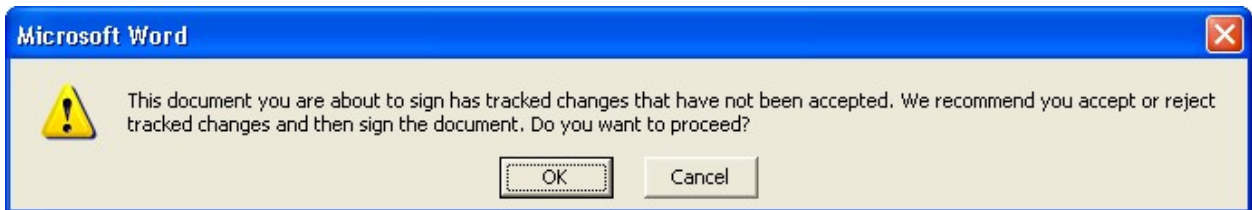
Illustration 24 Warning if track changes is active when signing a document

They do not warn if a certified and modified document is being closed.

320   A changed document could not be signed. It is required to add signature again to save document. Not very usable.
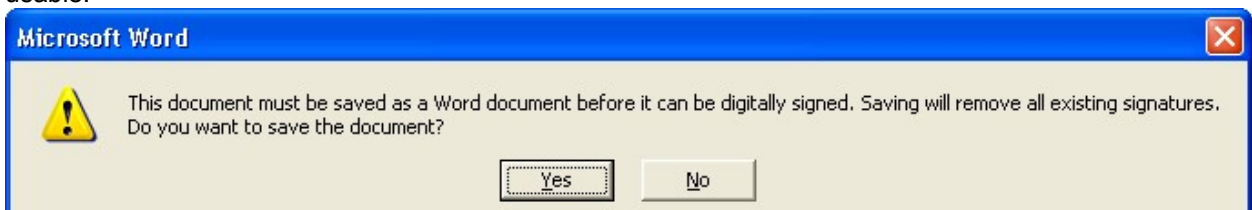
Illustration 25 Warning that unsaved documents have to be saved in Word format before signing
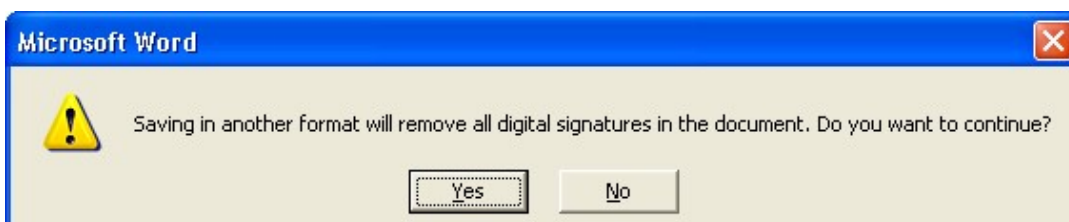
Illustration 26 Warning that saving in different format will remove signature

Illustration 27 Certificate Dialog – General tab
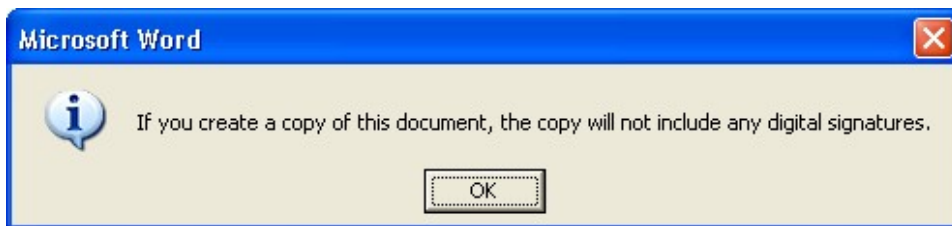
Illustration 28 Warning that save as will create a copy without signature
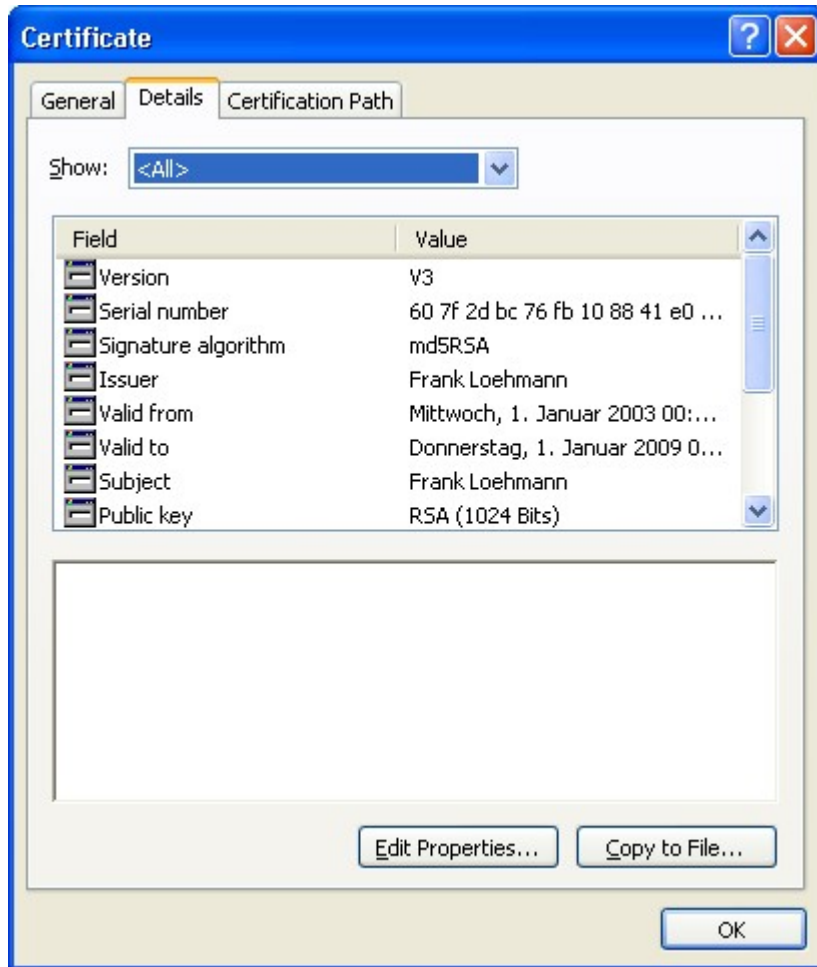
Illustration 29 Certificate - Details tab
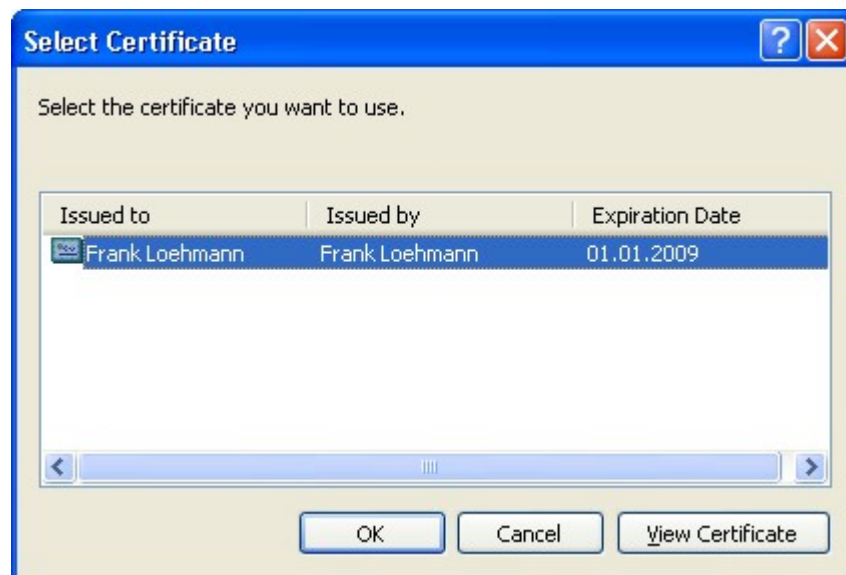
Illustration 30 Certificate Dialog

Illustration 31 Certificate Properties

Illustration 32 Certificate - Certification Path tab

Illustration 33 Certificate dialog with open Show list box
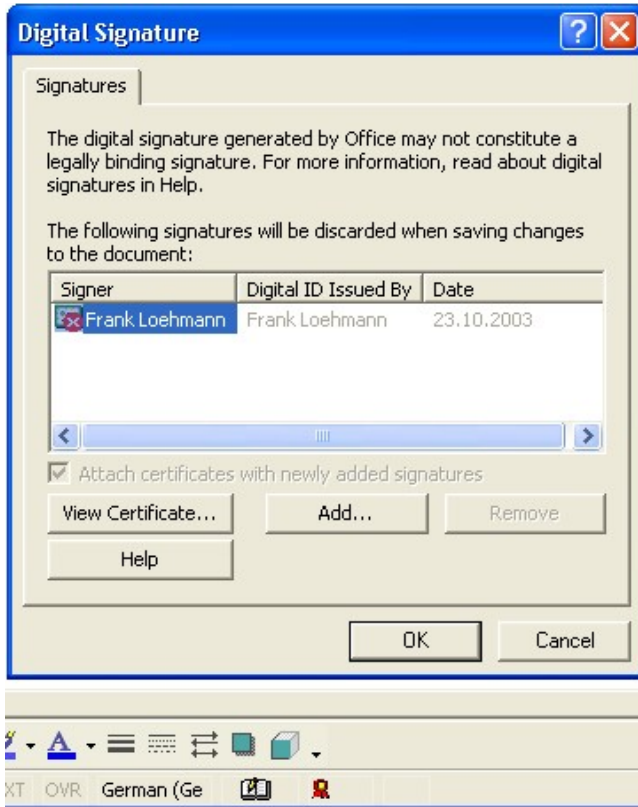
Illustration 34 Digital Signature
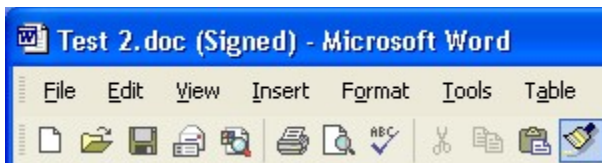
Illustration 35 (Signed) indicate that document has been signed

Illustration 36 Certificate Export Wizard

Illustration 37 Certificate Export Wizard
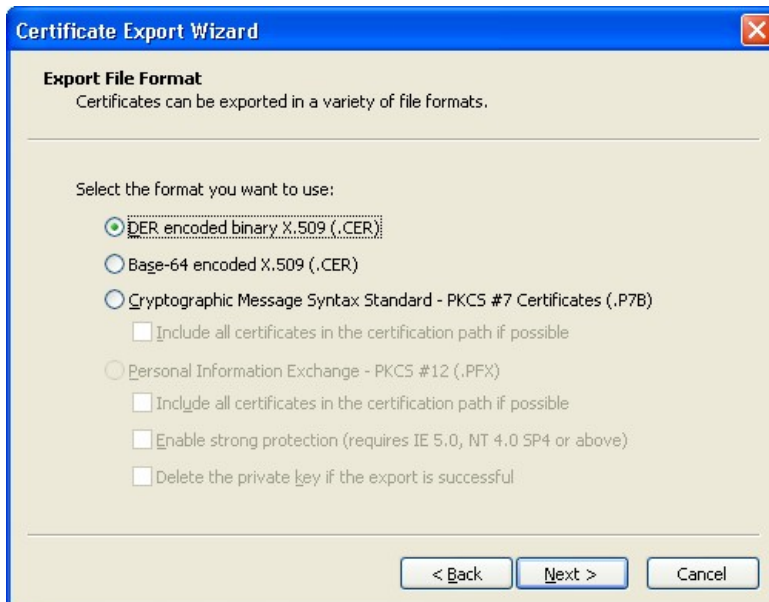
Illustration 38 Certificate Export Wizard

Illustration 39 Certificate Export Wizard

Illustration 40 Certificate Export Wizard

Illustration 41 Certificate Export Wizard

Illustration 42 Saving a digitally signed document calls warning dialog

5.4 Mozilla 1.4 Certificates and Security Related UI
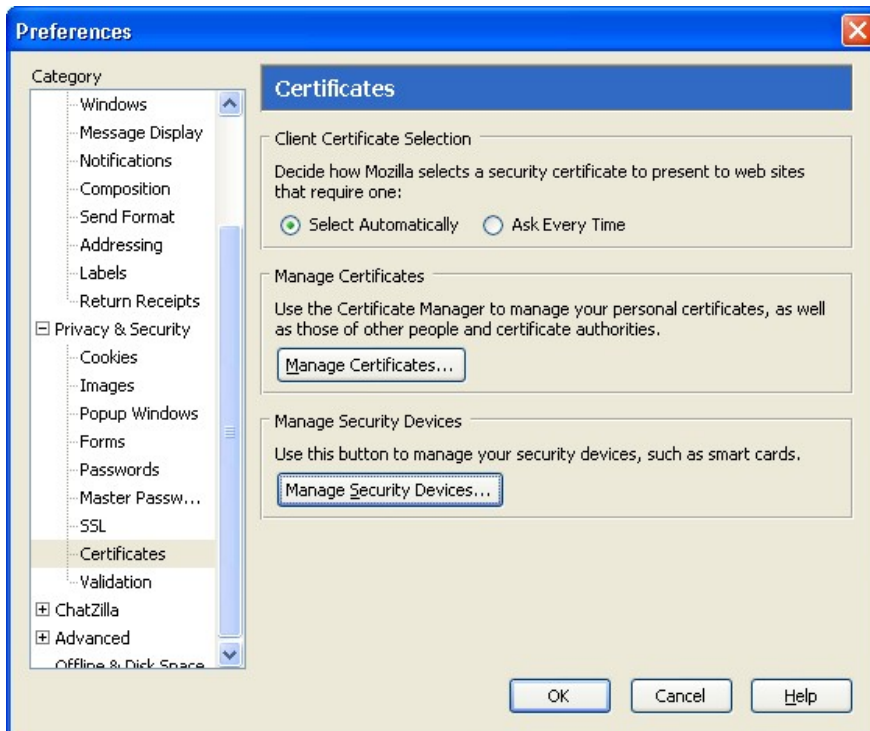
Illustration 43 Mozilla – Preferences

5.4.1 Mozilla 1.4 Security Related UI
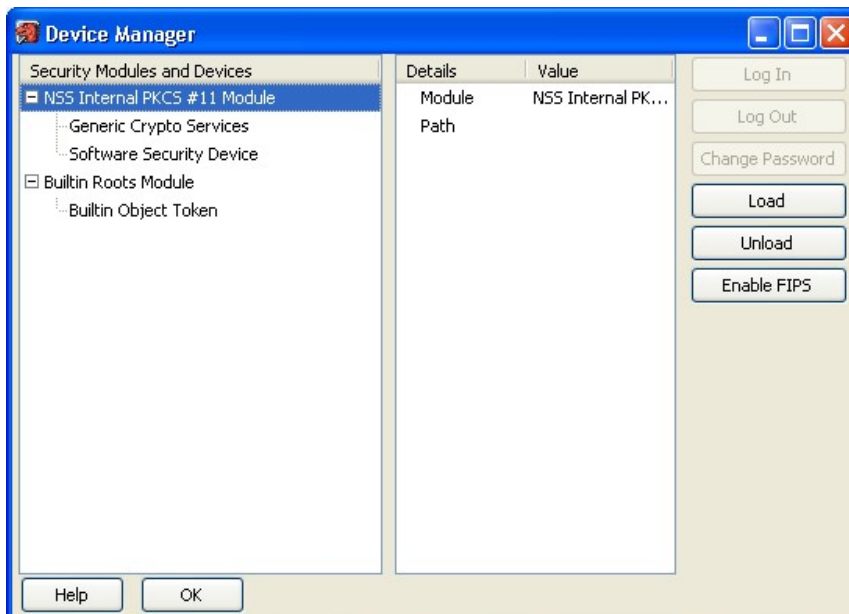
Illustration 44 Security Device Manger dialog

5.4.2 Mozilla 1.4 Certificates Related UI

325 Mozilla uses an own UI to manage certificates.
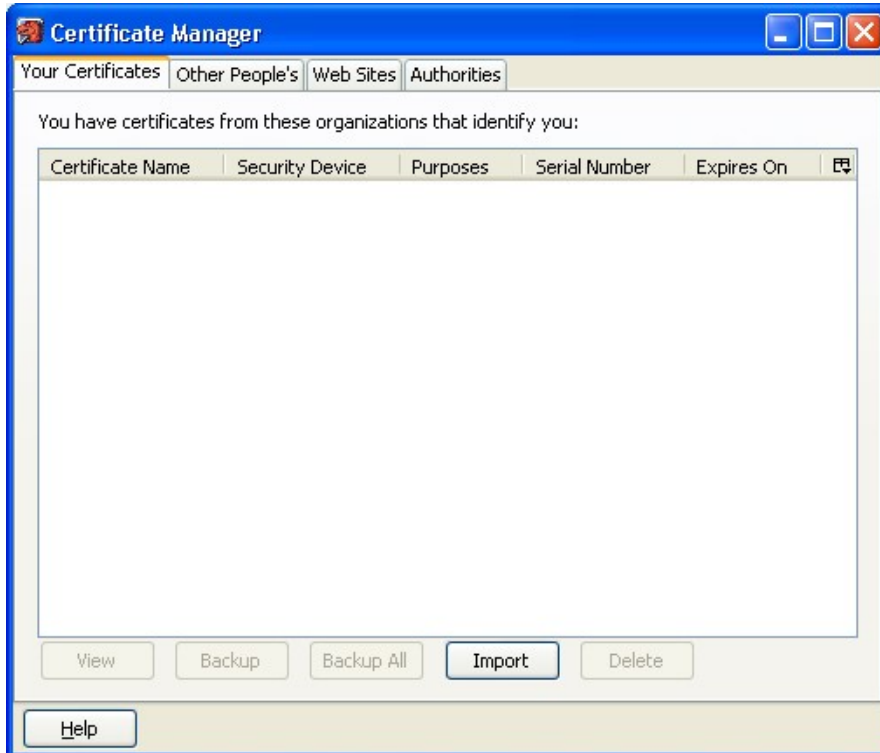
Illustration 45 Certificate Manager dialog
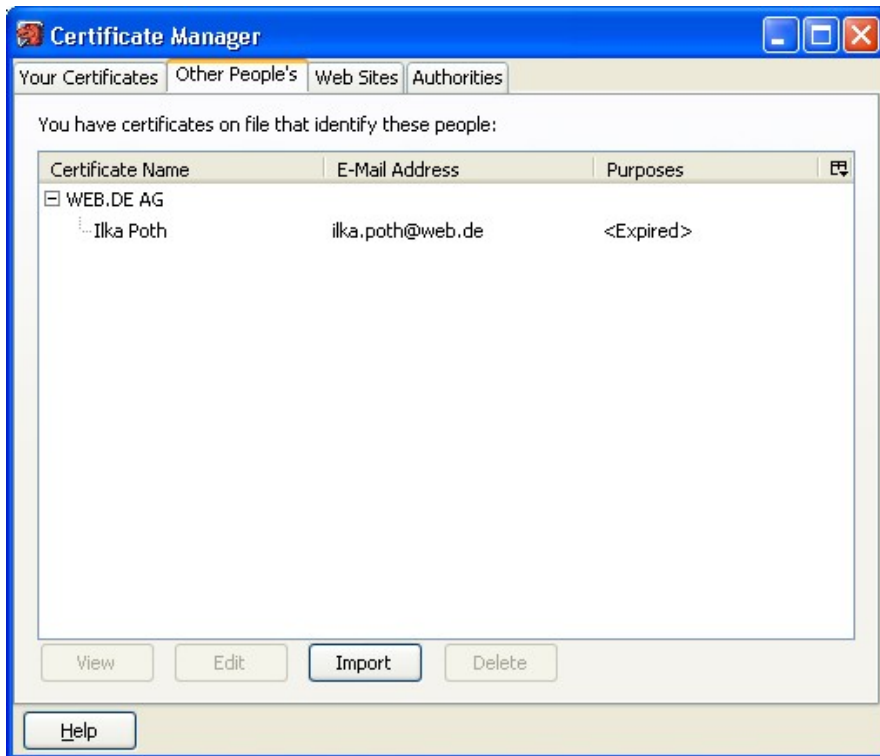
Illustration 46 Certificate Manager dialog
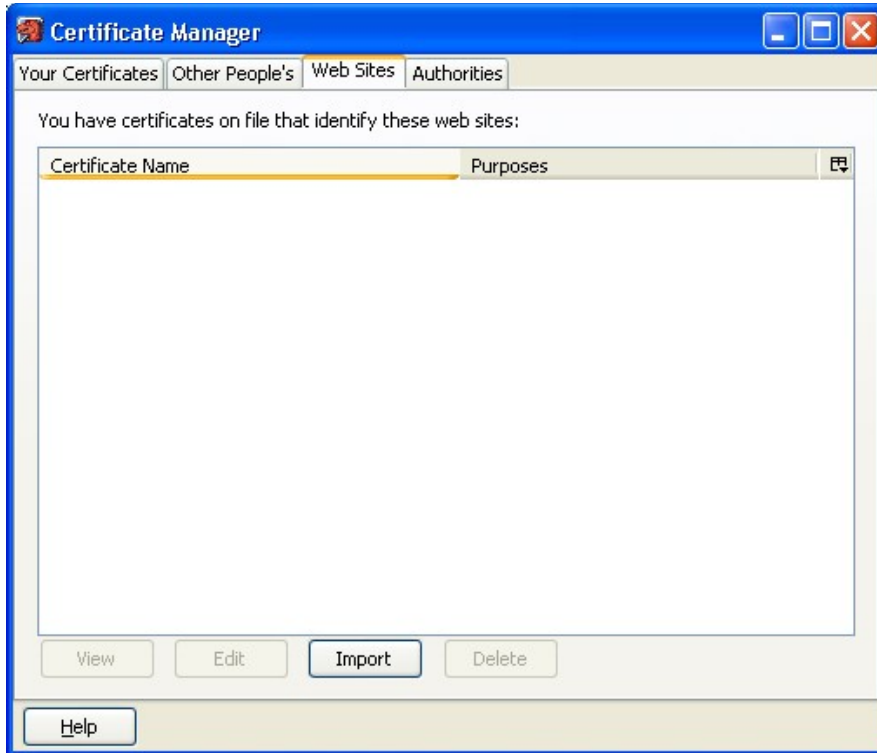
Illustration 47 Certificate Manager dialog
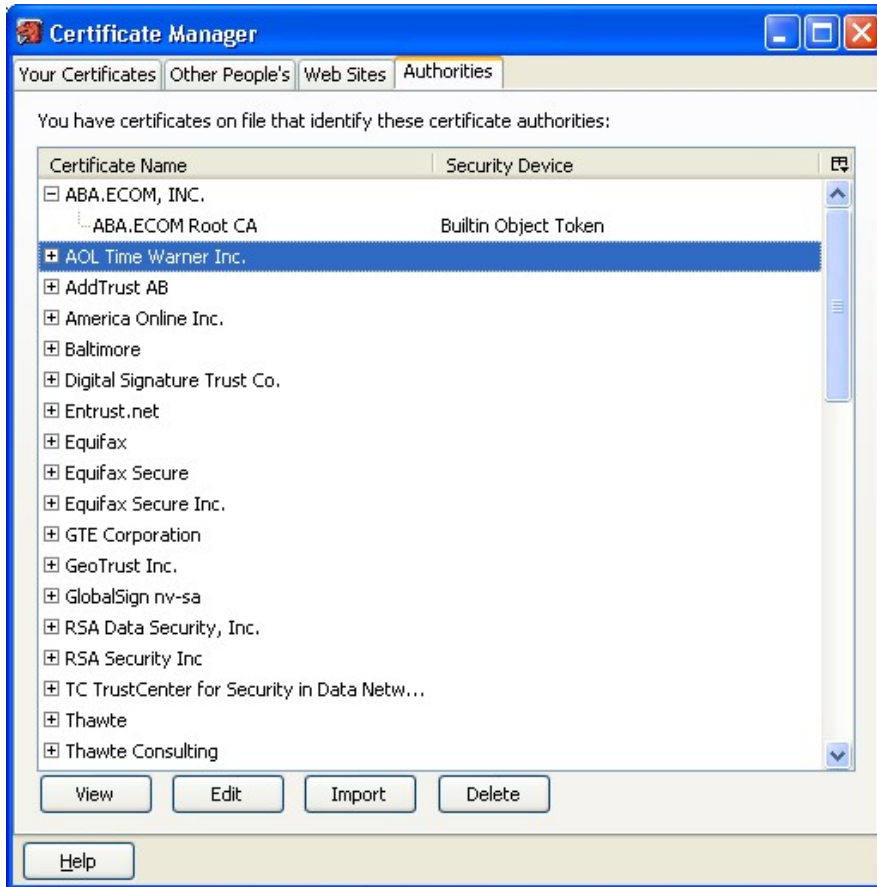
Illustration 48 Certificate Manager dialog

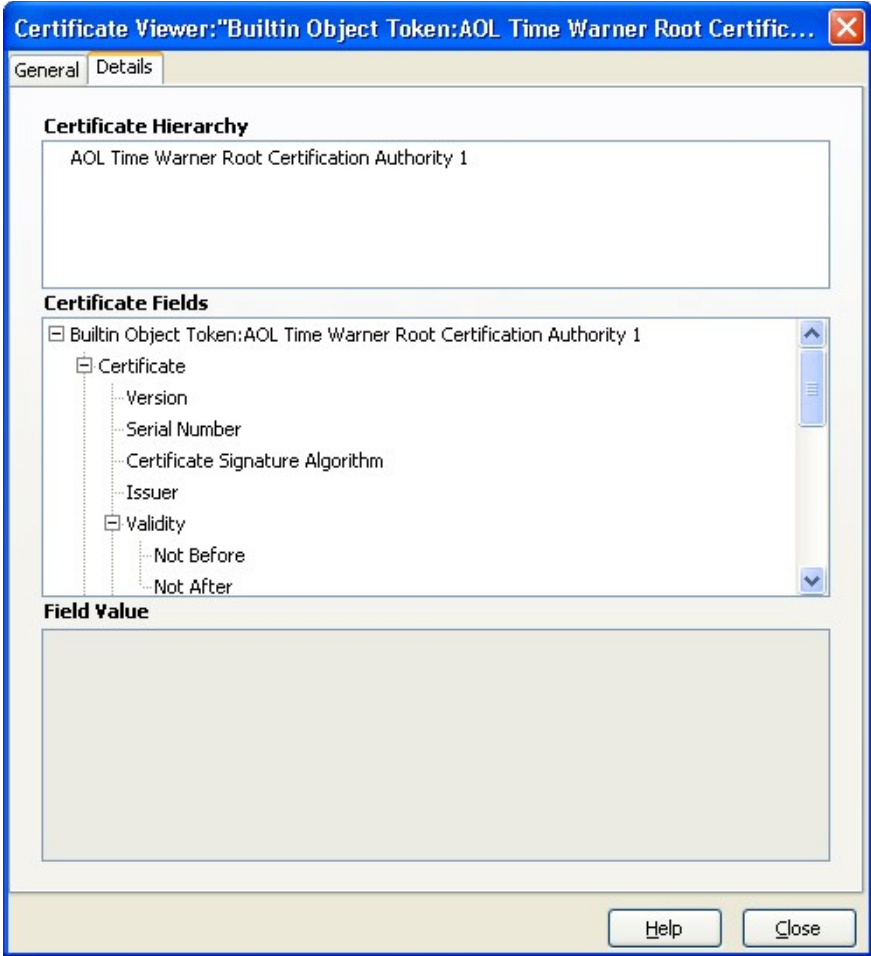*Illustration 49 Editing a certificate*
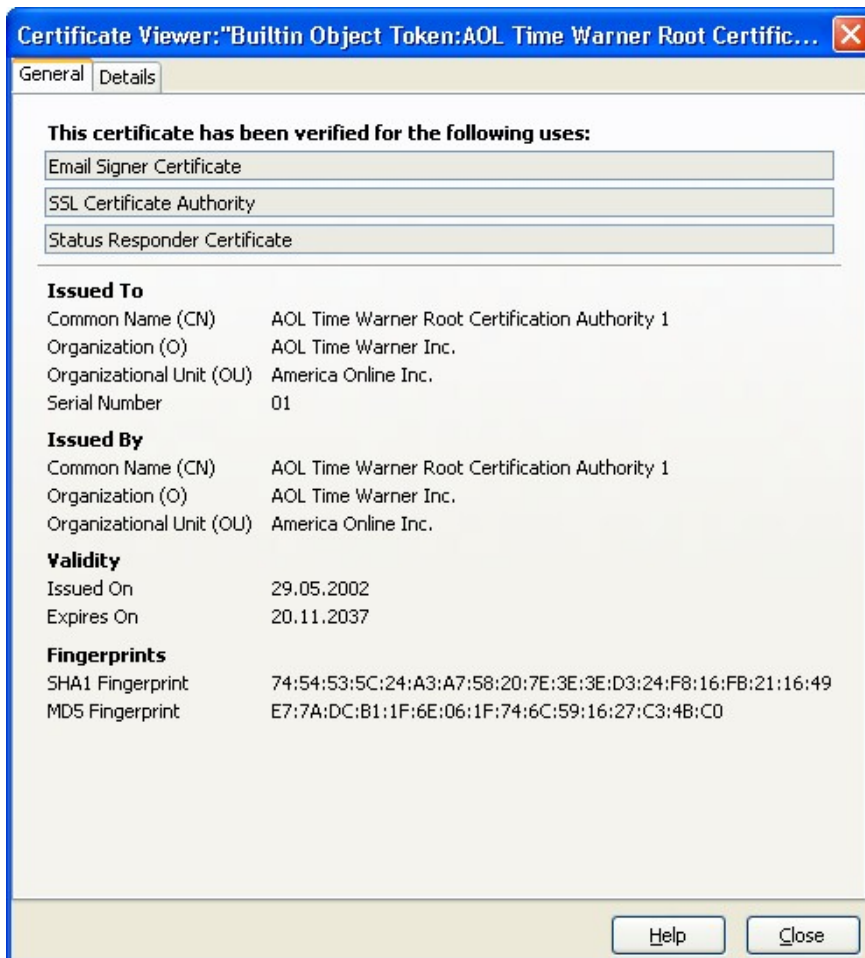
Illustration 50 View a certificate

Illustration 51 View a certificate

5.5 Adobe Acrobat Security / Signatures Related UI
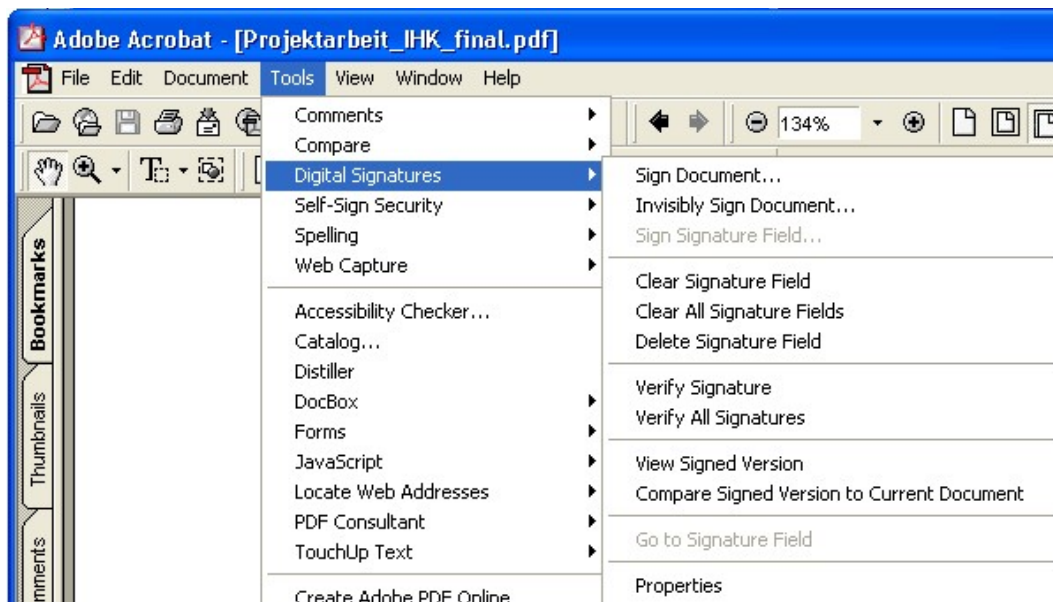

Illustration 52 Self Signing Security Dialog

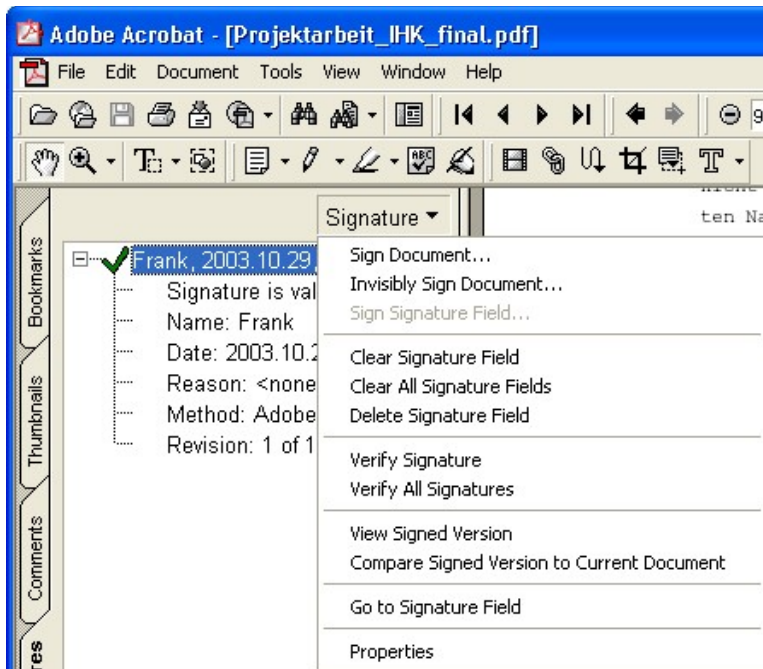*Illustration 53 Tools menu with two signature related functions*

Illustration 54 Digital signatures menu is also available in task pane

Illustration 55 Compare two versions of a signed document

Illustration 56 Sign document dialog

Illustration 57 Show options enlarges dialog and offers additional functionality
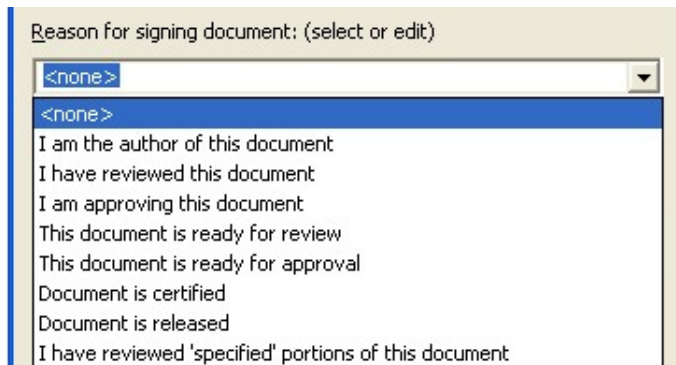

Illustration 58 Reasons list box offers special settings in Signing dialog

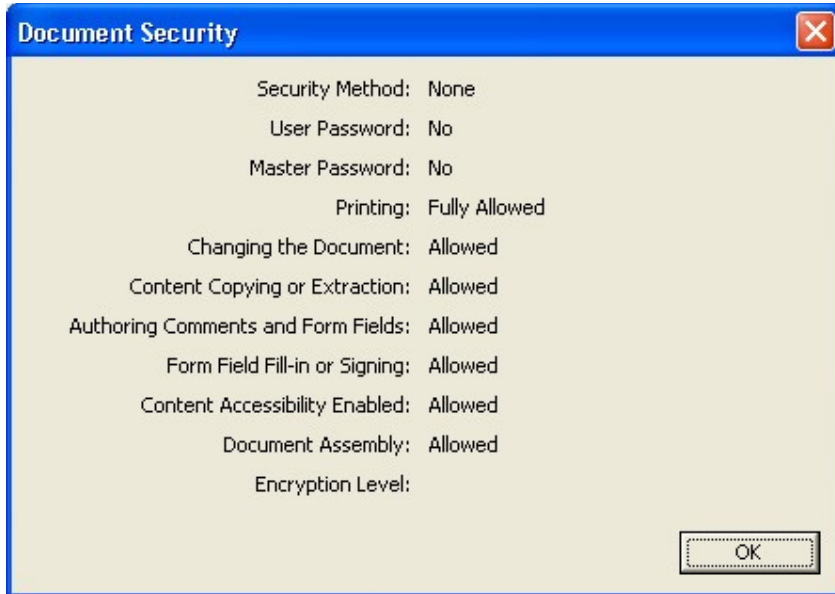*Illustration 59 Document Security dialog*

Illustration 60 Display Settings Dialog

Illustration 61 Document security dialog – list box call dialog when entry has been selected
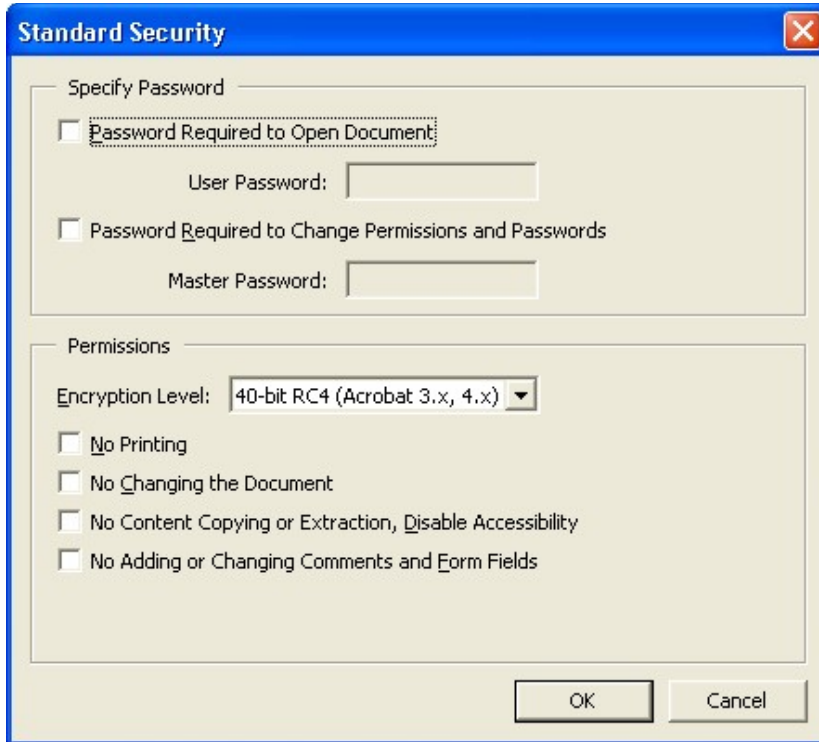
Illustration 62 Dialog called via Acrobat Standard Security entry in security options list box
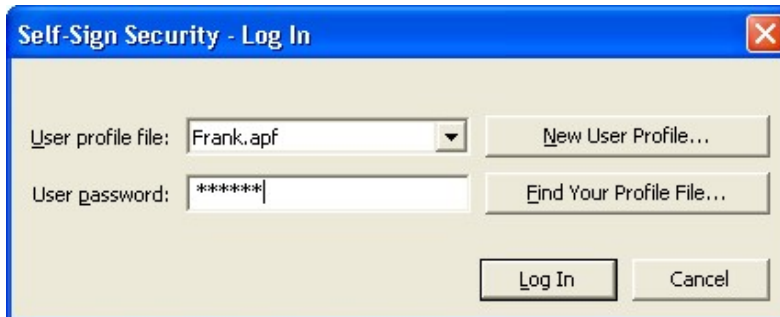

Illustration 63 Login Dialog

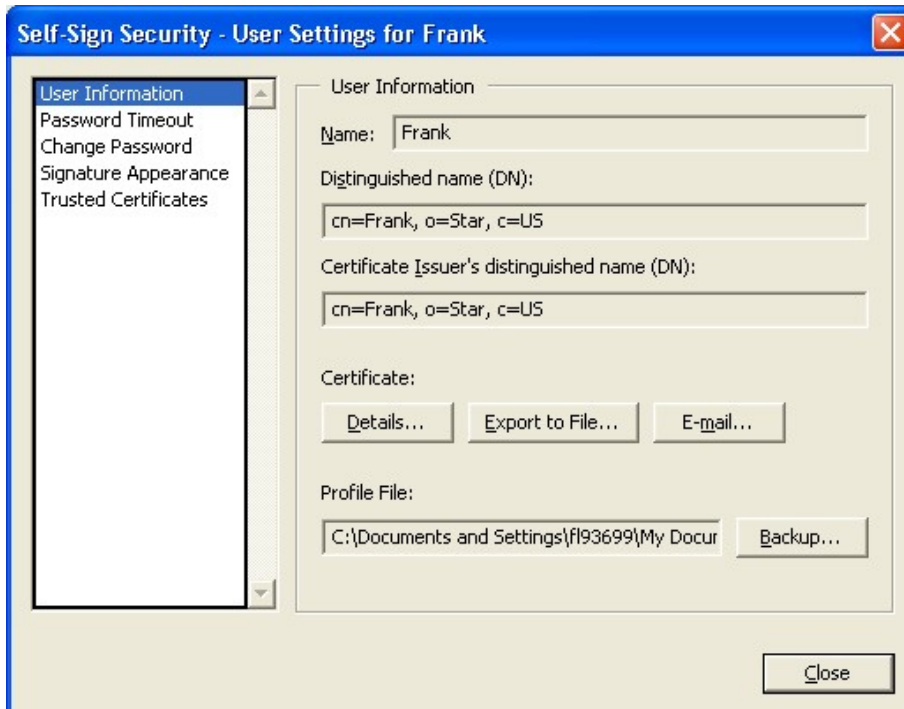*Illustration 64 Create a new user*

Illustration 65 Self signing security dialog
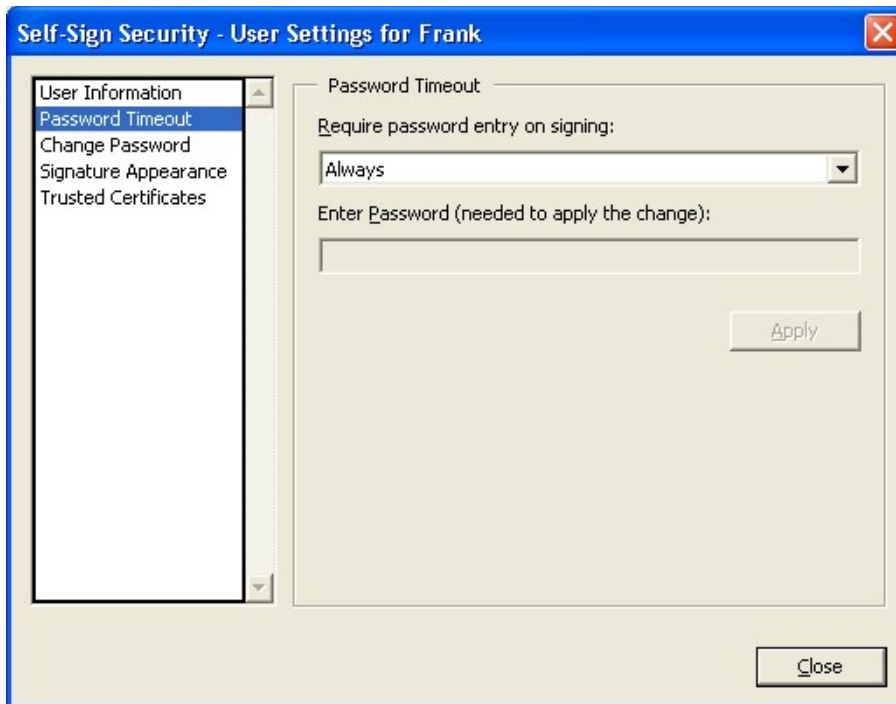
Illustration 66 Self signing security dialog
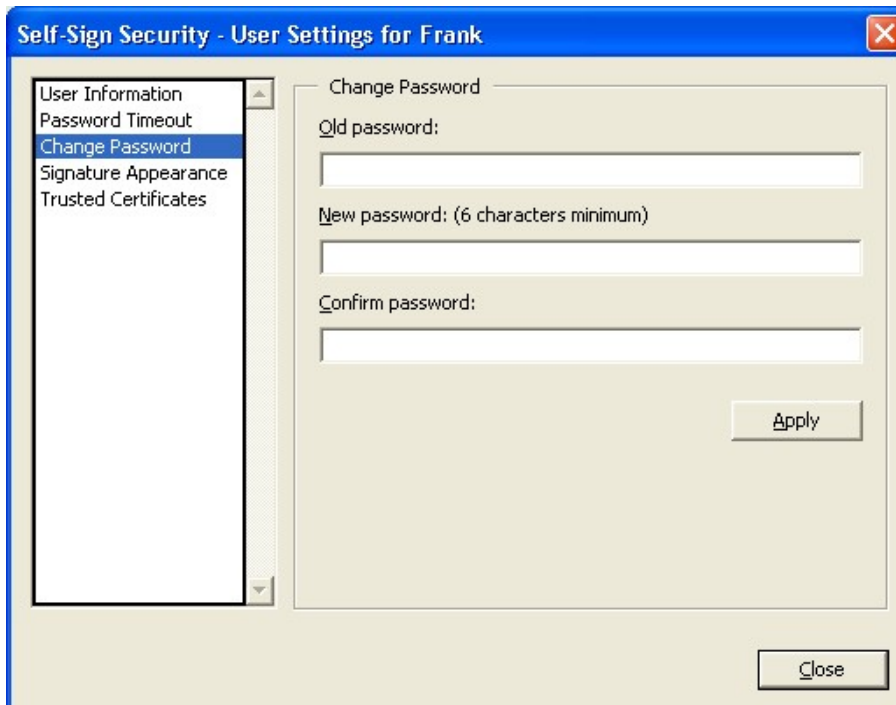
Illustration 67 Self signing security dialog
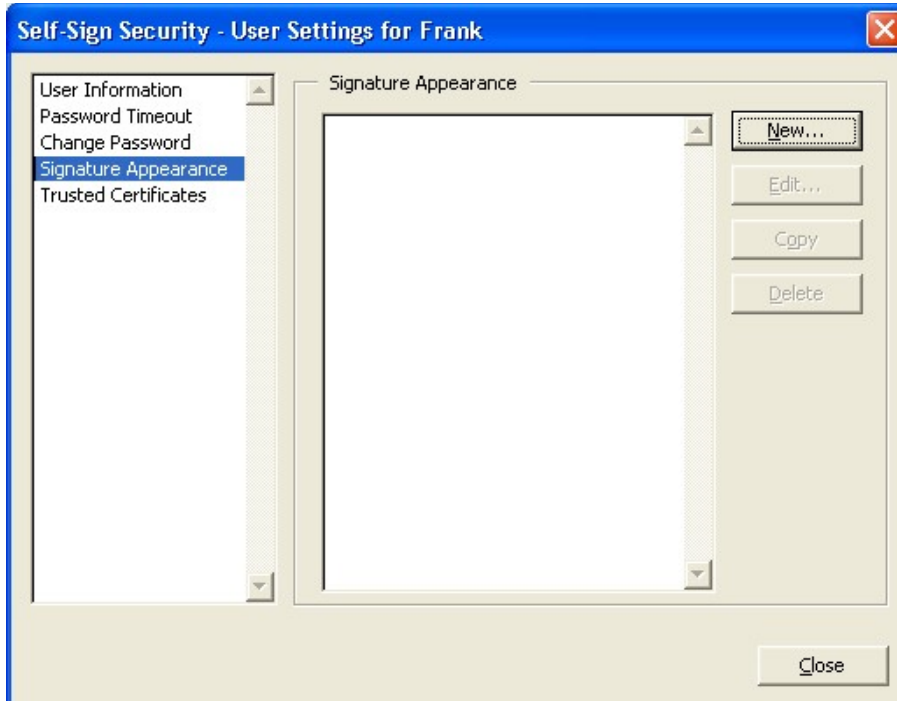
Illustration 68 Self signing security dialog
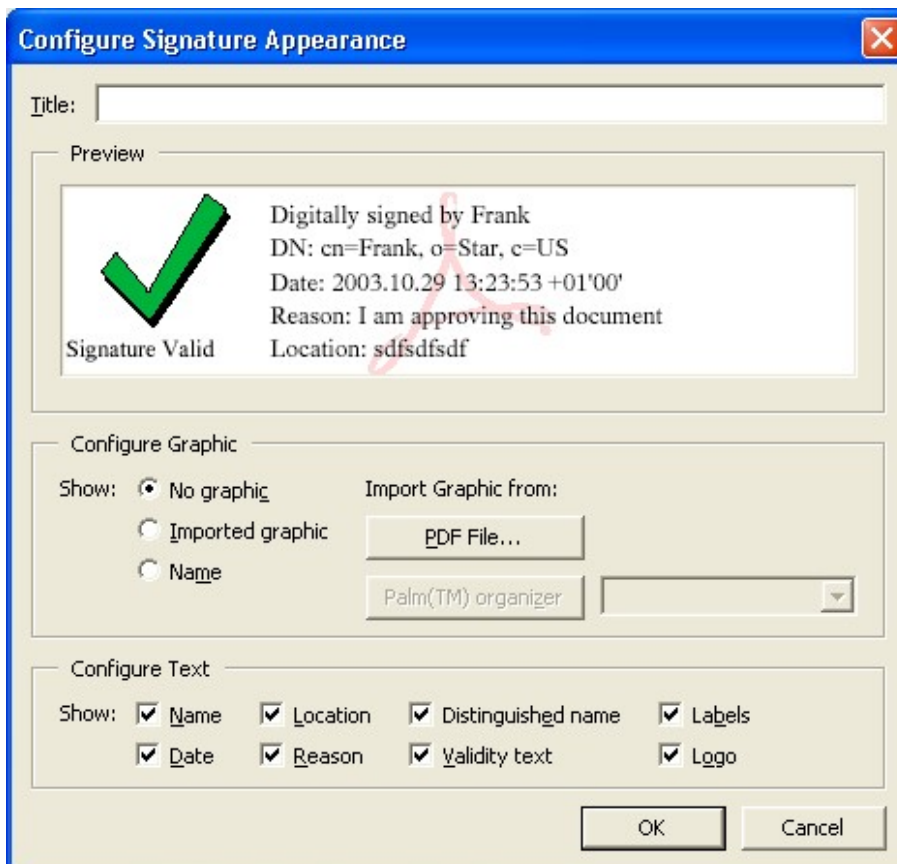
Illustration 69 Called via New (appearance) button
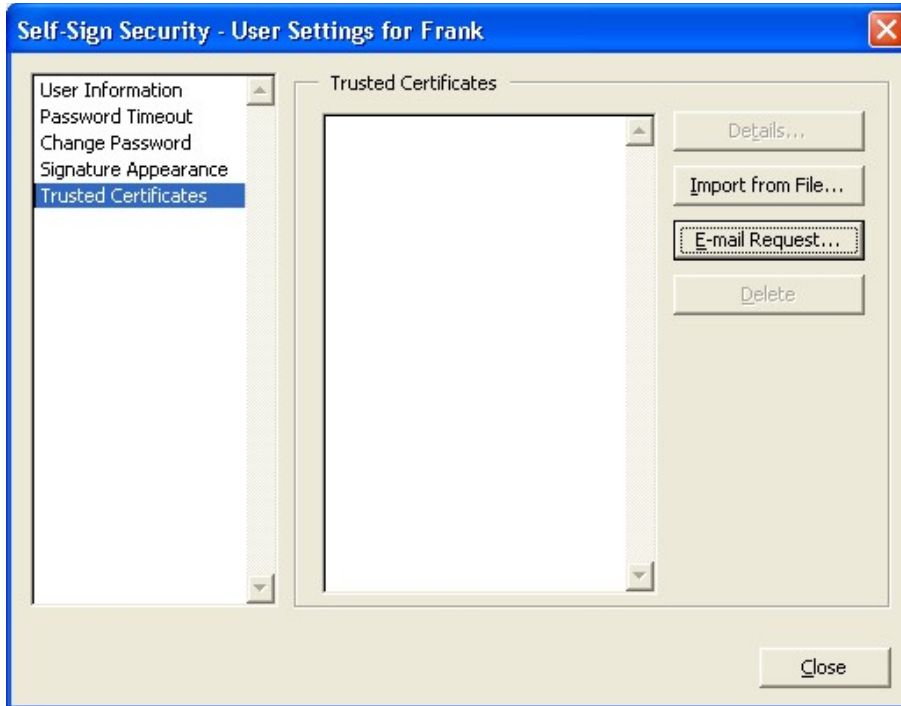
Illustration 70 Trust a certificate

Illustration 71 E-mail a certificate
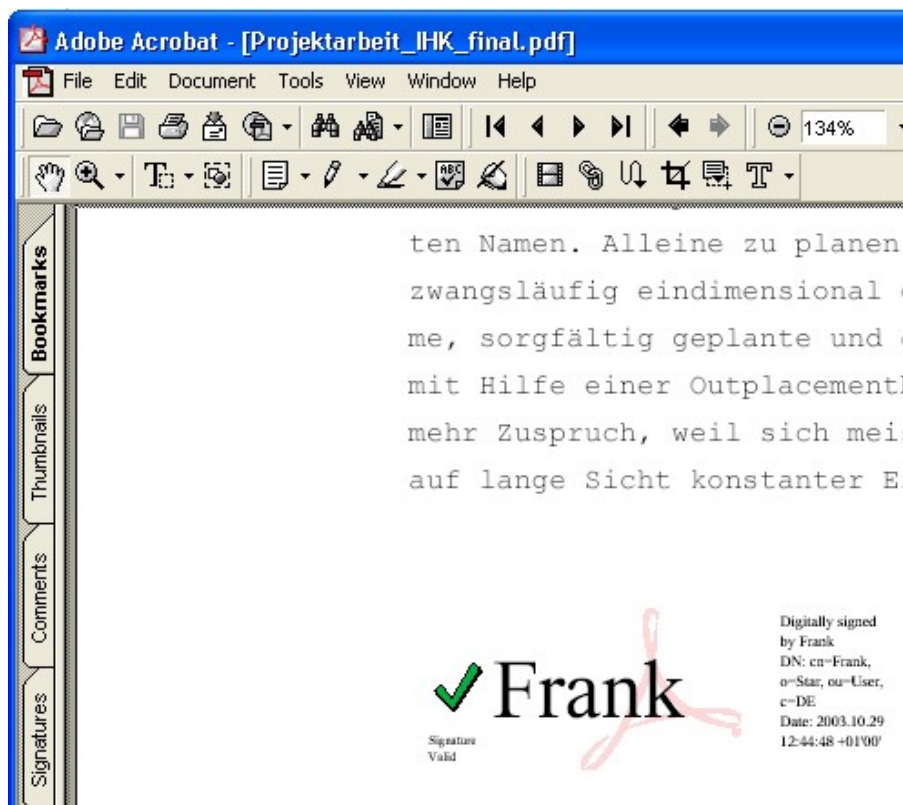
Illustration 72 Signature with default representation in the document
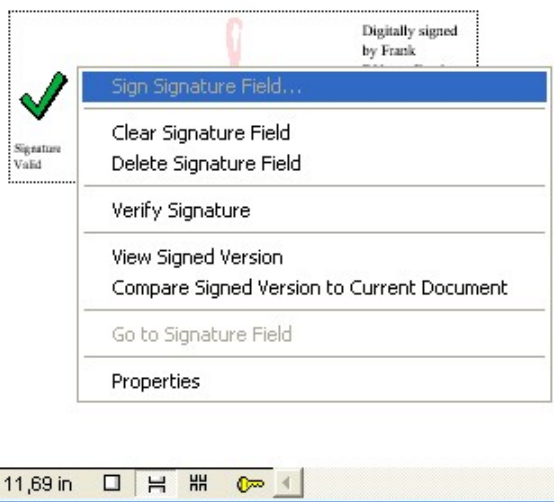
Illustration 73 Context menu on signature
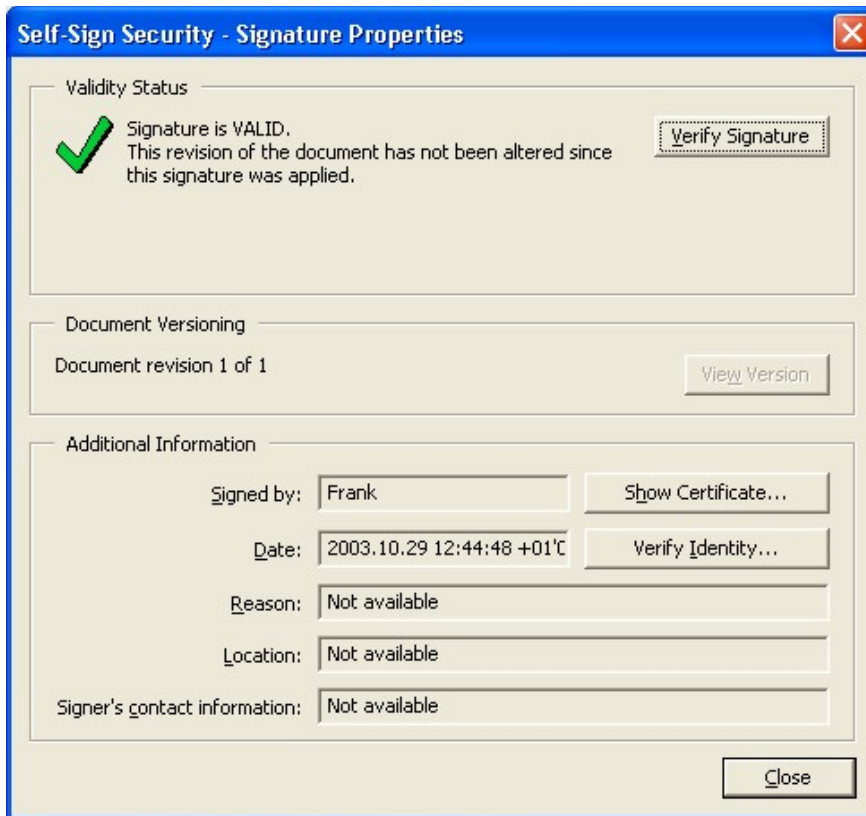
Illustration 74 Signature properties
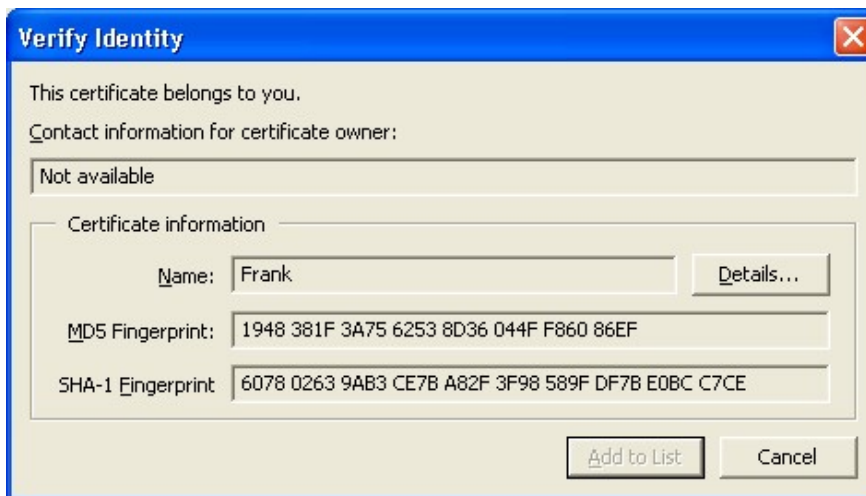
Illustration 75 Verify identity
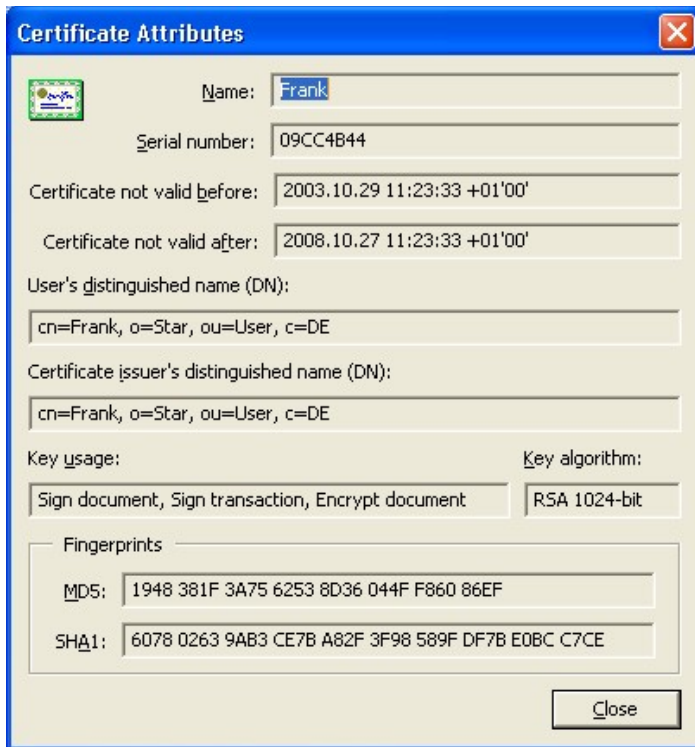
Illustration 76 Certificate Attributes

5.6   Signatures Related UI of Microsoft Visual Basic Editor
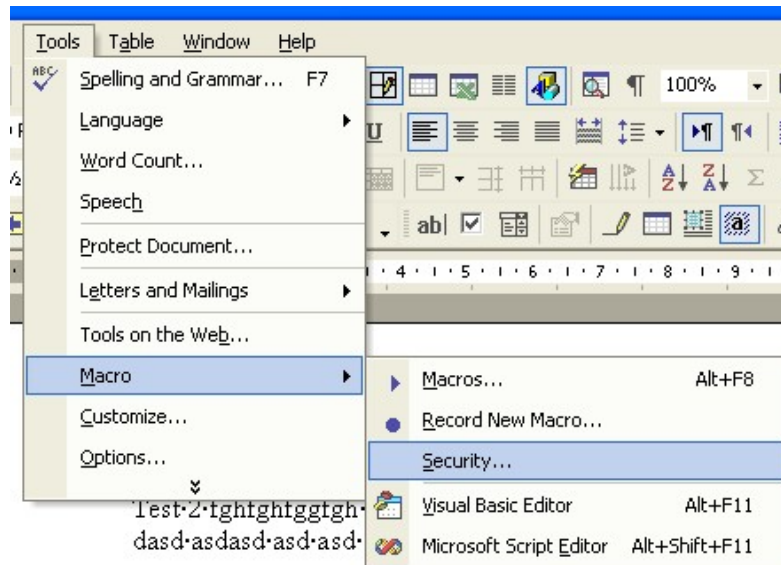
Illustration 77 Macro Security in Word XP

Illustration 78 Tools - Digital Signature Dialog in Visual Basic Editor

Illustration 79 Select Certificate dialog (called by Choose... button)

Illustration 80 MS Office XP Security Warning Dialog
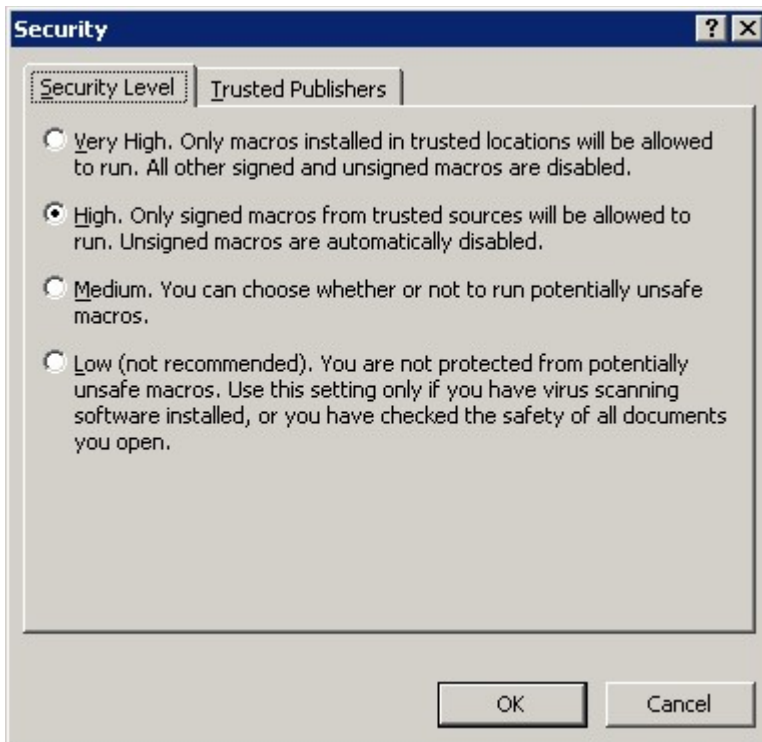
Illustration 81 Macro security dialog of MS Office 2003- Tab 1
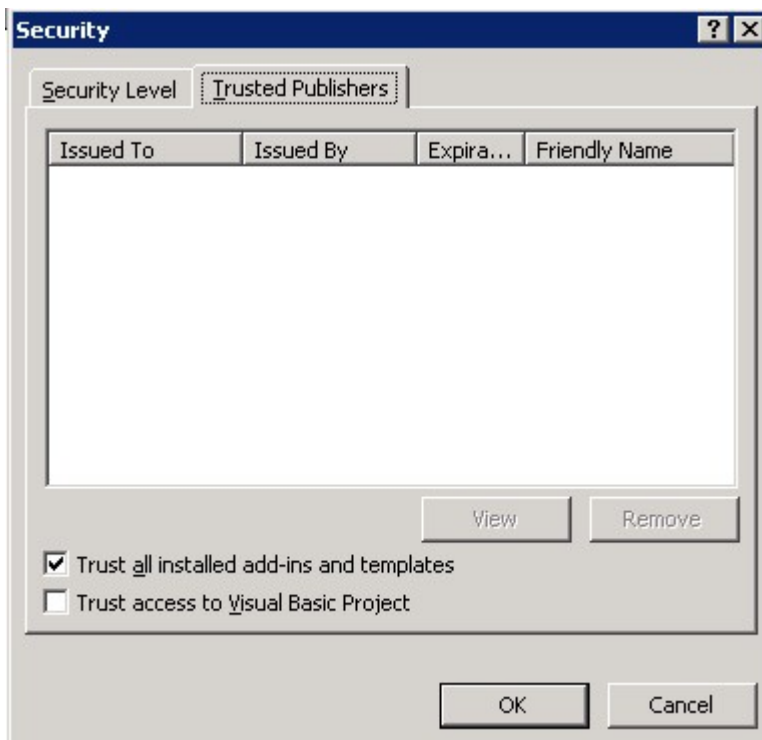
Illustration 82 Macro security dialog of MS Office 2003 - Tab 2
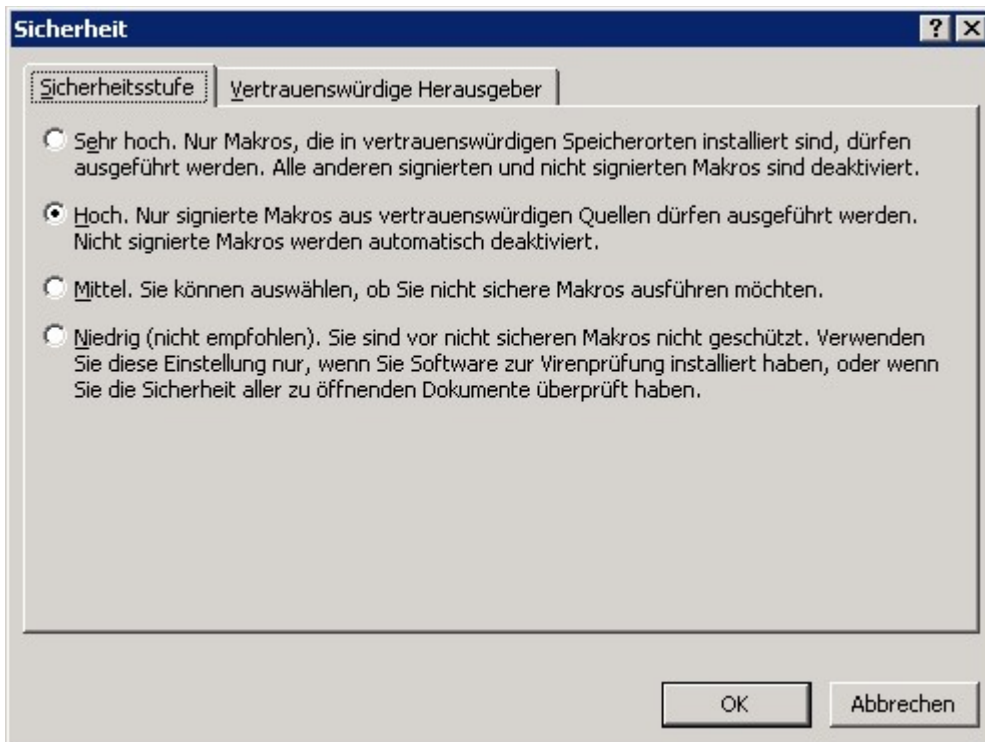
Illustration 83 MS Office 2003 - Security Dialog Tab 1 (German)
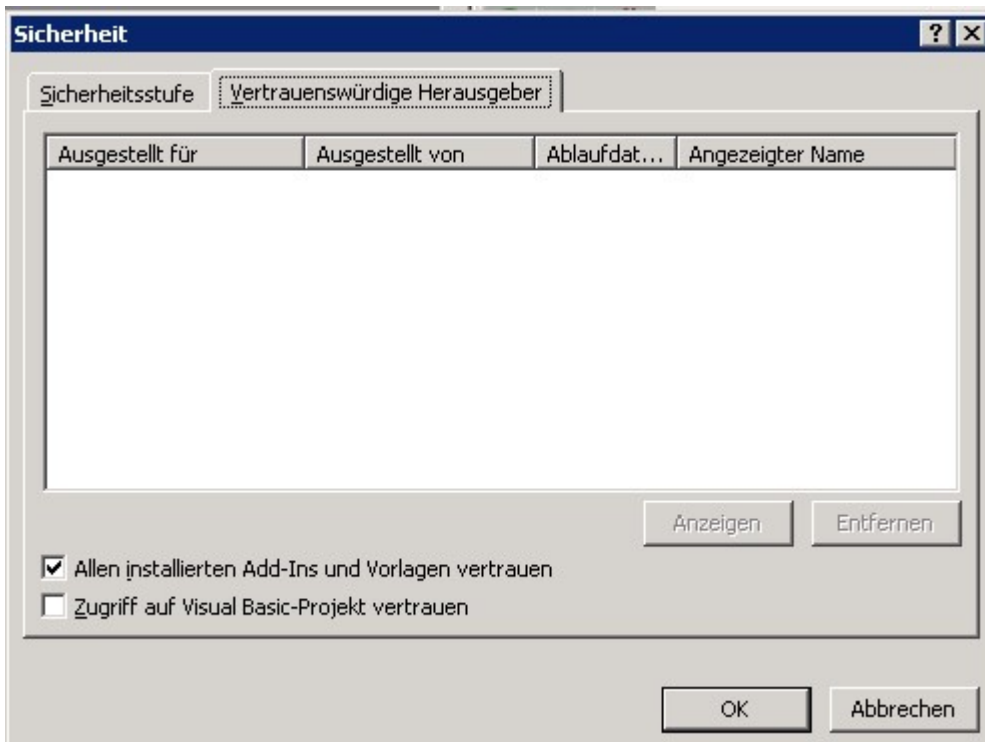
Illustration 84 MS Office 2003 - Security Dialog Tab 2 (German)

http://office.microsoft.com/assistance/preview.aspx?AssetID=HP052495611033&CTT=98

6   Detailed Specification

330   This specification defines the basic feature set for encryption and signing document for OpenOffice.org (OO.org) 2.0.

6.1   Security Options
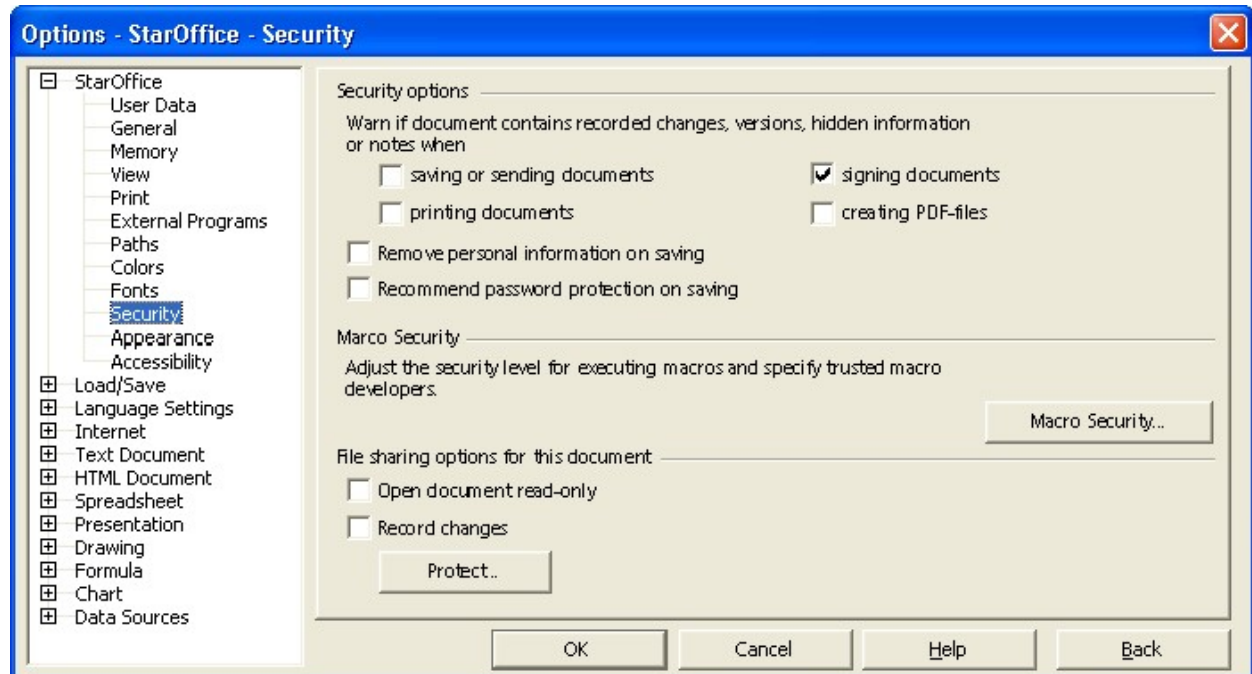
The following dialog replaces the Security tab page in tools options.
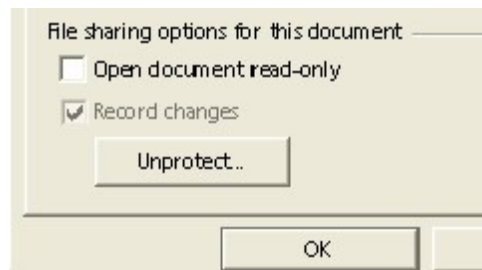
Illustration 85 The state of the "Record changes" check box will be enabled and disabled as long as a the state is protected.

Apoc Settings (Issue #118519)

335   The Security tab page could be protected7 via a setting in the Apoc configuration manager. Each value and status (protected) of a control, except the enable/disable status for buttons, could be configured by Apoc. When protected a lock symbol is shown and the control itself is disabled.

Item	English	German	Comments
Label	Security options	Sicherheitsoptionen	
Label	Warn if document contains	Wenn ein Dokument	

7   Protected means that those controls are disabled and a lock symbol is shown in front of the control. Please see http://so-doc.germany.sun.com/Projects/StarOffice/SO_6.x/Proposals/Drafts/ManagementConsole/Spec/Config _Items_rev8.sxw following behaviour was observered in SO8:

Item	English	German	Comments
	recorded changes, versions, hidden information or notes:	aufgezeichnete Änderungen, Versionen, versteckte Informationen oder Notizen enthält, warnen beim:	
Label	When saving or sending	Speichern oder Senden	
Label	When printing	Drucken	
Label	When signing	Signieren	
Label	When creating PDF files	PDF-Dateien erzeugen	
Label	Remove personal information on saving	Persönliche Informationen beim Speichern aus Dateien entfernen	
Label	Recommend password protection on saving	Kennwortschutz beim Speichern empfehlen	
Label	Adjust the security level for executing macros and specify trusted macro authors.	Anpassen des Sicherheitsstufe für das Ausführen von Makros und Definieren der vertrauenswürdigen Makro-Autoren.	
Button	Macro Security...	Makrosicherheit...	
Label	File sharing options for this document	Optionen für gemeinsame Benutzung dieses Dokumentes	
Label	Open this document in read-only mode	Dieses Dokument schreibgeschützt öffnen	
Label	Record changes	Änderungen Aufzeichnen	
Button	Protect...	Schützen...	
Button	Unprotect...	Schutz aufheben...	**TRANSLATORS! "Unprotect" means remove protection – it is not a real word but exists in computer software**

6.1.1 Show warning dialogs if the document contains recorded changes, versions or notices when

340
- **"Saving or sending documents" Option (default off)**

The following warning dialog appears if one of the following is contained in a document and the document will be saved (or send as an email). Furthermore the "saving or sending documents warning" on the security tab page has to be turned on:

- recorded changes

345
- notices

- document file contains versions

Warning Dialog String List

Item	English	German	Comments
Dialog text	This document contains:	Das zu speichernde Dokument enthält:	

Item	English	German	Comments
Dialog text	* Recorded changes	* Aufgezeichnete Änderungen	**Displayed are only those things contained in the current doc.**
Dialog text	* Notes	* Notizen	**Displayed are only those things contained in the current doc.**
Dialog text	* Document versions	* Dokumentversionen	**Displayed are only those things contained in the current doc.**
Dialog text	Do you want to continue saving the document?	Möchten Sie mit dem Speichern des Dokumentes fortfahren?	
Button	Yes	Ja	
Button	No	Nein	

- **"Printing documents" Option (default off)**

The following warning appears when printing a document, if one of the following is a visible part of the document and the warning function itself is turned on in Tools-Options-StarOffice/OOo-Security:

- shown recorded changes
- shown notices

Warning Dialog String List

Item	English	German	Comments
Dialog text	This document contains:	Das Dokument enthält:	
Dialog text	* Recorded changes	* Aufgezeichnete Änderungen	
Dialog text	* Notes	* Notizen	**Displayed are only those things currently visible/printable in the current doc.**
Dialog text	Do you want to continue printing the document?	Möchten Sie mit dem Drucken des Dokumentes fortfahren?	
Button	Yes	Ja	
Button	No	Nein	

The Printing Options... button calls the Printing Options dialog, were the user can change the behavior for printing notes.

- **"Signing documents" Option (default on)**

The following warning is shown directly before the Digital Signature dialog appears (please see page 62 in chapter 6.4 below for dialog details), if the document contains one of the following and the warning option is turned on in Tools-Options-Security:

- recorded changes
- document file contains versions
- notices in Writer and Calc
- fields

- references to other sources (i.e. linked sections or linked graphics)

365   Warning Dialog String List

Item	English	German	Comments
Dialog text	This document contains:	Das aktuelle Dokument enthält:	
Dialog text	* Recorded changes	* Aufgezeichnete Änderungen	**Displayed are only those things contained in the current doc.**
Dialog text	* Document versions	* Dokumentversionen	**Displayed are only those things contained in the current doc.**
Dialog text	* Notes	* Notizen	
Dialog text	* Fields	* Felder	**Displayed are only those things contained in the current doc.**
Dialog text	* Linked data from other sources (e.g.linked sections or linked graphics)	* Verknüpfte Daten aus anderen Quellen (z.B. verknüpfte Bereiche oder Grafiken)	**Displayed are only those things contained in the current doc.**
Dialog text	Do you want to continue signing the document?	Möchten Sie mit dem Signieren fortfahren?	
Button	Yes	Ja	
Button	No	Nein	

- **"Creating PDF-files" Option** (default off)

  The following warning dialog appears if the PDF export warning in Tools-Options-StarOffice/OOo -Security is turned on and if the document contains one of the following:

  - shown recorded changes in Writer

370   - shown notices in Writer or Calc

  Warning Dialog String List

Item	English	German	Comments
Dialog text	This document contains:	Das aktuelle Dokument enthält:	
Dialog text	* Recorded changes	* Aufgezeichnete Änderungen	
Dialog text	* Document versions	* Dokumentversionen	**Displayed are only those things contained in the current doc.**
Dialog text	* Notes	* Notizen	
Dialog text	* Fields	* Felder	**Displayed are only those things contained in the current doc.**
Dialog text	* Linked data from other sources (e.g. linked section or graphics)	* Verknüpfte Daten aus anderen Quellen (z.B. verknüpfte Bereiche oder Grafiken)	**Displayed are only those things contained in the current doc.**

Item	English	German	Comments
Dialog text	Do you want to continue creating a PDF file?	Möchten Sie mit dem Erstellen der PDF-Datei fortfahren?	
Button	Yes	Ja	
Button	No	Nein	

- **"Remove personal information on saving" Option**

  ➢ Today these information could only be deleted manually in File – Properties – General by pressing the delete button. This new feature removes exactly the same information automatically on save.

- **"Recommend password protection on saving" option** presets the Save with password option in the Save as dialog.

  ➢ The user can un-check this pre-checked setting to save a file explicit without a password.

- **Record Changes**

  This setting activates the changes tracking function for the current document. Furthermore the records could be protected by pressing the Protect... button. If the records are protected, the button label changes to Unprotect.. If the button is pressed in this state the Enter Password dialog (see illustration on page) appears. If the password is entered correctly, the button changes back to the initial label "Protect..." and the Record checkbox is enabled again.

  FST: Illustration ID and page Number is MIA

  Furthermore the Changes submenu in the Edit menu will change as follows:

  - The "Record" menu entry is checked and disabled if "Protect Records" is active

  - The check box and button are only enabled if the current document is a Writer or Calc one.

  - The document modify status is set

    - if the record mode has been protected in Tools-Options

    - if state of record mode has changed

- **Open document read-only**

  This setting will be saved with the current document. The document will be loaded in the already known read-only mode if this options is set and the document is opened. Option is only enabled if current module is a Writer, Calc, Draw or Impress.

6.2 The Menu Entries for Signing

6.2.1 Entry in the File Menu

The following entries will be added to the menu of Writer, Impress, Draw, Calc and the basic IDE to sign the current document content or document macro (in the basic IDE). It is placed directly behind the properties section. In Basic IDE the entry creates a new group since no properties are available.

Item	English	German	Comments
Main Menu entry	Digital Signature...	Digitale Signatur...	Digital Signature dialog is called.

6.2.2 Entry in the Tools-Macros Sub Menu

The following entry will be added to the Tools-Macros sub menu of Writer, Impress, Draw, Calc and the basic IDE to sign the current document's macros. It is placed within the menu as follows:

Item	**English**	**German**	**Comments**
Tools-Macros menu entry	Digital Signature...	Digitale Signatur...	Digital Signature dialog for macros is called.

6.2.3 Digital signature info dialog

The following dialog appears, if the current document is modified and the document has not been saved to a file.

The following dialog is shown, if the document is modified and contains a digital signature:

Item	**English**	**German**	**Comments**
Dialog text	The document has to be saved before it can be signed. Saving the document removes all present signatures.	Das Dokument muss gespeichert werden bevor es signiert werden kann. Das Speichern des Dokumentes entfernt alle vorhandenen Signaturen.	
Dialog text	Do you want to save the document?	Möchten Sie das Dokument jetzt speichern?	
Button	Yes	Ja	**The Yes button is defaulted**
Button	No	Nein	

415 After confirming the Digital Signature dialog , the Save as dialog appears. After saving the document, the Digital Signature dialog (please see page 62 in chapter 6.4 below for dialog details) appears to sign the document.

If the document is **modified and unsigned**, the following dialog appears:

Item	**English**	**German**	**Comments**
Dialog text	The document has to be saved before it can be signed.	Das Dokument muss gespeichert werden bevor es signiert werden kann.	
Dialog text	Do you want to save the document?	Möchten Sie das Dokument jetzt speichern?	
Button	Yes	Ja	**The Yes button is defaulted**
Button	No	Nein	

If the document is **not modified and already signed**, the Digital Signature dialog (please see page 62 in chapter 6.4 below for dialog details) appears to add/remove signatures of the document.

6.2.4 Open a Signed Document with an Invalid Signature

If a document's signature is invalid, the following dialog is shown: For Document Content/Macros

Item	English	German	Comments
Dialog ~~T~~title	Invalid Document Signature	Ungültige Dokumentsignatur	
Dialog text	The digitally signed document content and/or macros do not match the current document signature.	Der digital signierte Dokumentinhalt und/oder die Makros stimmen nicht mit der aktuellen Dokumentsignatur überein.	
Dialog text	This could be the result of document manipulation or of structural document damage due to data transmission.	Dieses deutet auf eine Dokumentmanipulation oder einen Übertragungsfehler hin.	
Dialog text	We recommend that you do not trust the content of the current document. Execution of macros is disabled for this document.	Wir empfehlen Ihnen, dem aktuellen Dokumentinhalt nicht zu trauen. Das Ausführen von Makros ist für dieses Dokument deaktiviert.	
Button	OK	OK	

For Program Packages:

Item	English	German	Comments
Dialog ~~t~~Title	Invalid Package Signature	Ungültige Paket Signatur	
Dialog text	The digitally signed package does not match the current package signature.	Das digital signierte Programmpaket stimmt nicht mit der aktuellen Paketsignatur überein.	
Dialog text	This could be the result of package manipulation or of structural document damage due to data transmission.	Dieses deutet auf eine Dokumentmanipulation oder einen Übertragungsfehler hin.	
Dialog text	We strongly recommend that you do not trust the current package.	Wir empfehlen Ihnen dringend, dem aktuellen Paket nicht zu trauen.	
Dialog text	Do you want to continue adding the package?	Möchten Sie das Hinzufügen des Paketes fortsetzen?	
Button	Yes	Ja	
Button	No	Nein	**The "No" button is defaulted.**

6.3 Digital Signatures

Document content and document macros can be digitally signed independently. .

6.3.1 General behavior when signing a document:

- If a signed document is loaded, OO.org shows a little seal on the right side of the modified field. The seal will be withdrawn, if the document gets changed.

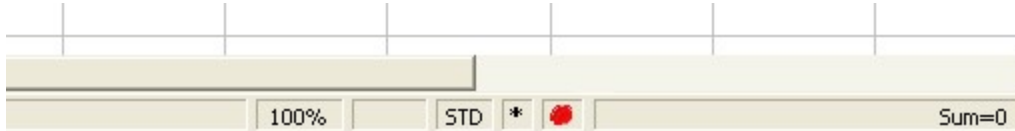*Illustration 86 Signed seal in Writer status bar*

Illustration 87 Signed seal in Calc status bar

Illustration 88 Signed seal in Draw and Impress status bar

Illustration 89 Signed Marco library is loaded in the integrated development environment.

- The following icons have been designed by Stella Schulze (original Files will be provided by Stella as PNG files):

26*26 pixel:

26*26 pixel (high contrast):

16*16 pixel:

16*16 pixel (high contrast):

11*16 pixel:

11*16 pixel (high contrast):

- Tip help of icon in status bar

  Tip Help String List

Item	English	German	Comments
Tip help	Digital signature	Digitale Signatur	

- The following icon is shown in the status bar in the same field were the signature icon is shown. It appears only, if the signature does not match the content or macro.

11*16 pixel:

11*16 pixel (high contrast):

- A double click on the icon shows the dialog with signing information of current document.

- Tip help of icon in status bar (see above)**Context Menu Signature Sign in Status bar**

- The sign in the status bar has a context menu with the following entries:

Item	English	German	Comments
Context Menu	Digital Signature...	Digitale Signaturen...	**Calls the Digital Signature Dialog**

- Furthermore the application title shows a note (Signed) or (Signed document macros) right behind the documents or basic libraries file name in the title bar.
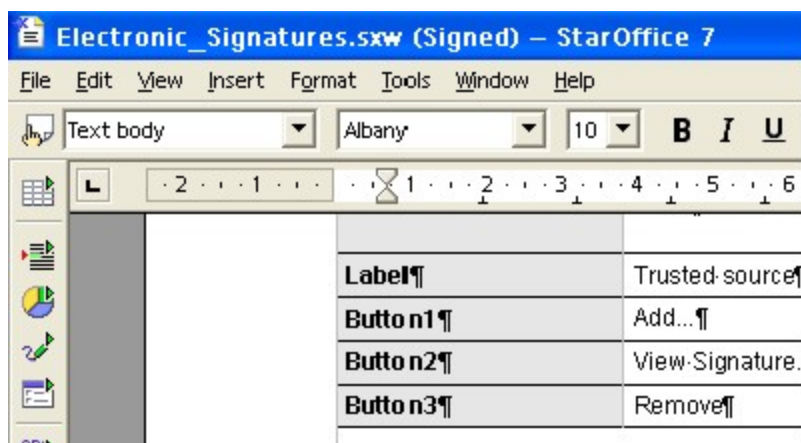

Illustration 90 New note "(signed)" in the title bar of an application

Item	English	German	Comments
Text	(Signed)	(Signiert)	**for document content**
Text	(Signed Macro)	(Signiertes Makro)	**for basic macros**

- Signing requires the OOo or Open Office (OASIS) Format file format.

The following warning dialog appears when a document is already signed and will be saved in **whatever** (including OpenOffice) format :

Warning Dialog String List

Item	English	German	Comments
Dialog text	Saving will remove all existing signatures.	Speichern in diesem Format entfernt alle existierenden Signaturen.	
Dialog text	Do you want to continue saving the document?	Möchten Sie mit dem Speichern fortfahren?	
Button	Yes	Ja	[Yes] button saves the document in the chosen format.
Button	No	Nein	[No] button aborts the saving and goes back to the Save dialog.

The following warning dialog appears when the document is saved in a non OpenOffice.org format and should be signed ("Save and Sign" functionality):

Warning Dialog String List

Item	English	German	Comments
Dialog text	This document must be saved in Open~~Document~~ ~~Office~~ file format before it can be digitally signed.	Dieses Dokument muss im Open ~~Office~~Document Dokumentformat gespeichert werden, bevor es digital signiert werden kann.	[~~Yes] button saves the document in the OO.org format using~~

450

Item	English	German	Comments
			~~the current filename and location.~~
			~~[No] button aborts the signing process.~~
Button	OK	OK	

455   •   If a document has already been saved with a signature, OO.org raises a dialog when the user saves the document again.

6.4 Digital Signatures Dialog

The following dialogs are called when a document has to be signed.

6.4.1 Digital Signature Dialog For Documents

Illustration 91 Digital Signatures - document content

460   The list box shows all currently assigned signatures of the current document. Furthermore a row shows the signature icon and a note is shown below the list box to explain the icon. If the signatures are not valid for the current document, the yellow exclamation sign is shown instead. Then notice 2 is shown in the dialog instead.

Warning Dialog String List

Item	English	German	Comments
Dialog text	The following have signed the document content:	Die Folgenden haben den Dokumentinhalt signiert:	
Dialog text	Signed by	Signiert durch	
Dialog text	Digital ID issued by	Digitale Signatur ausgestellt durch	TRANSLATORS!: note the preposition here. Where necessary in your language, choose a noun to have the same meaning as this phrase.
Dialog text	Date	Datum	
Button	View Certificate...	Zertifikat zeigen...	**Calls the View Certificate dialog described below**
Button	Add...	Hinzufügen...	**Calls the Select Certificate dialog described below**
Button	Remove	Entfernen	
Notice 1	The signatures in this document are valid	Die Signaturen in diesem Dokument sind gültig.	
Notice 2	The signatures in this document are invalid	Die Signaturen in diesem Dokument sind ungültig.	

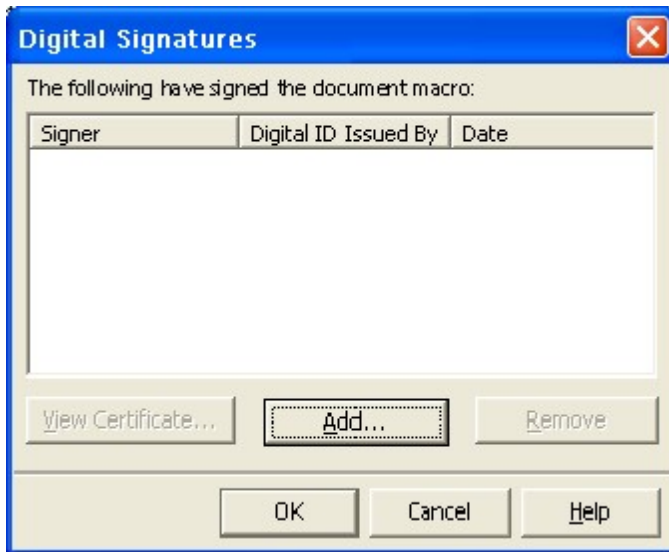### 6.4.2 Digital Signature Dialog For Document Macros

465

Illustration 92 Digital Signatures - document macros

Note: Only the mockup does not show the icon row in the list box and the explanation sentence. It is present as shown above for document content.

String List

Item	English	German	Comments
Dialog text	The following have signed the document macros:	Die Folgenden haben die Dokumentmakros signiert:	

6.4.3 Digital Signature Dialog For Program Packages

Illustration 93 Digital Signatures - for packages

470

Note: Only the mockup does not show the icon row in the list box and the explanation sentence. It is present as shown above for document content.

String List

Item	English	German	Comments
Dialog text	The following have signed this	Die Folgenden haben das	

Item	English	German	Comments
	package:	Paket signiert:	

6.4.4 Select Signature (Add...) Dialog

The following dialog is called if the Add... button is pressed in the Digital Signature Dialog. The view button allows to view at the current selected certificate. If no certificate is selected (default when calling the dialog), the button is disabled.

475
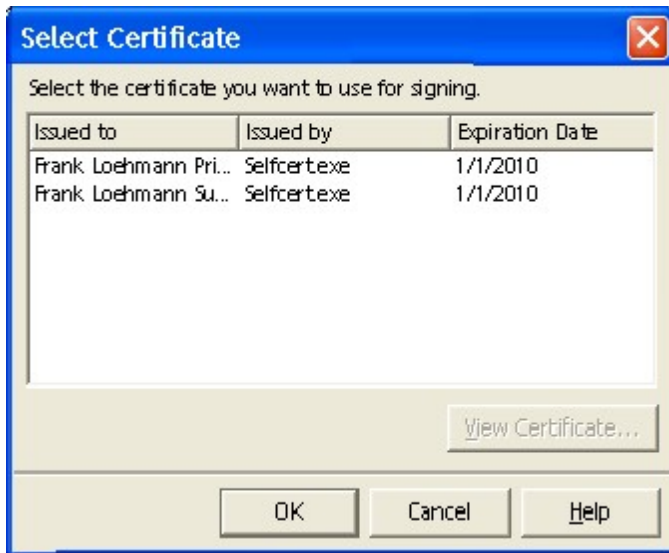
Illustration 94 Select Certificate dialog

String List

Item	English	German	Comments
Dialog text	Select the certificate you want to use for signing.	Wählen Sie das Zertifikat aus, das Sie zum signieren benutzen möchten.	
Button	View Certificate...	Zertifikat zeigen...	

Item	English	German	Comments
Title	Select Certificate	Zertifikat auswählen	
Label	Issued to	Ausgestellt für	TRANSLATORS!: note the preposition here. Where necessary in your language, choose a noun to have the same meaning as this phrase.
Label	Issued by	Ausgestellt durch	TRANSLATORS!: note the preposition here. Where necessary in your language, choose a noun to have the same meaning as this phrase.

Item	English	German	Comments
Label	Expiration date	Ablaufdatum	

6.4.5 View Certificate Dialog

The Certificate dialog is called when the View Certificate button is pressed in the Digital Signatures dialog. The dialog consists of three tab pages.

480
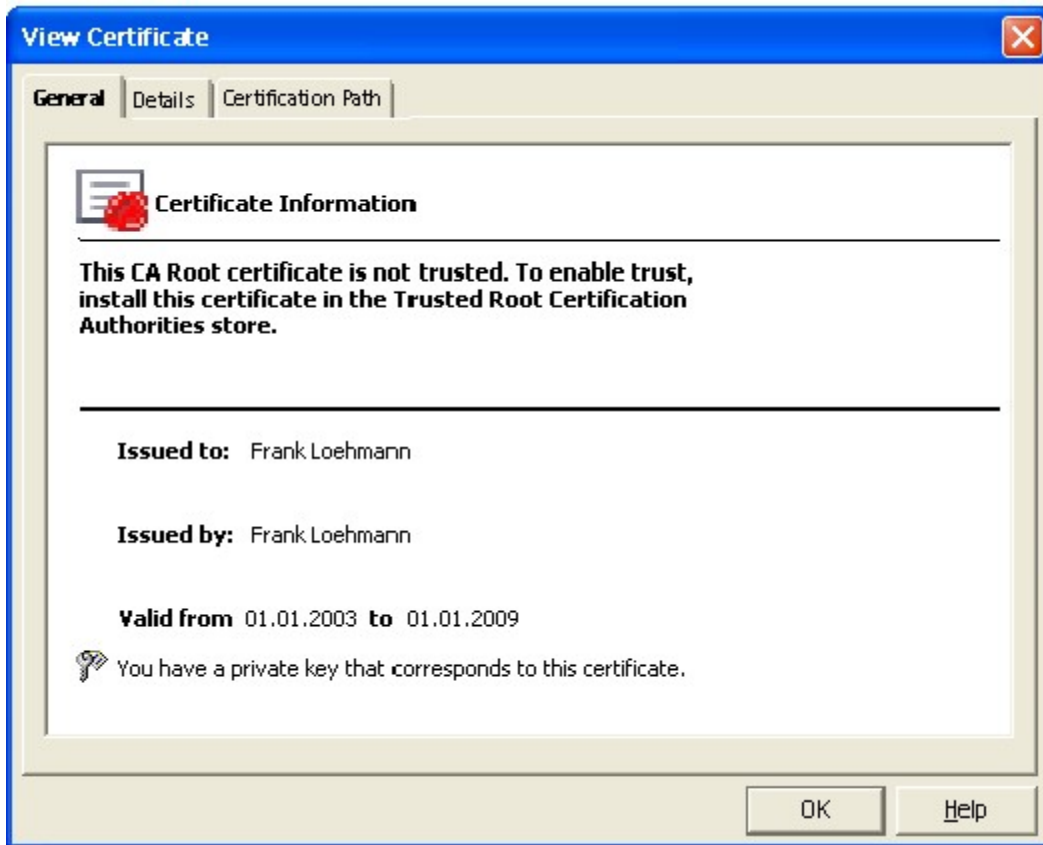
Illustration 95 Certificate Dialog - Tab 1 - General

String List

Item	English	German	Comments
Tab page Label	General	Allgemein	
Tab page Label	Details	Details	
Tab page Label	Certificate Path	Zertifikatspfad	
Label	Certificate Information	Zertifikatsinformationen	
Label	Issued to:	Ausgestellt für:	TRANSLATORS!: note the preposition here. Where necessary in your language, choose a noun to have the same meaning as this phrase.
Label	Issued by:	Ausgestellt durch:	TRANSLATORS!: note the preposition here.

Item	English	German	Comments
			Where necessary in your language, choose a noun to have the same meaning as this phrase.
Label	Valid from %SDATE% to %EDATE%	Gültig von %SDATE% bis %EDATE%	
Label	You have a private key that corresponds to this certificate	Sie haben einen privaten Schlüssel, der mit diesem Zertifikat korrespondiert.	
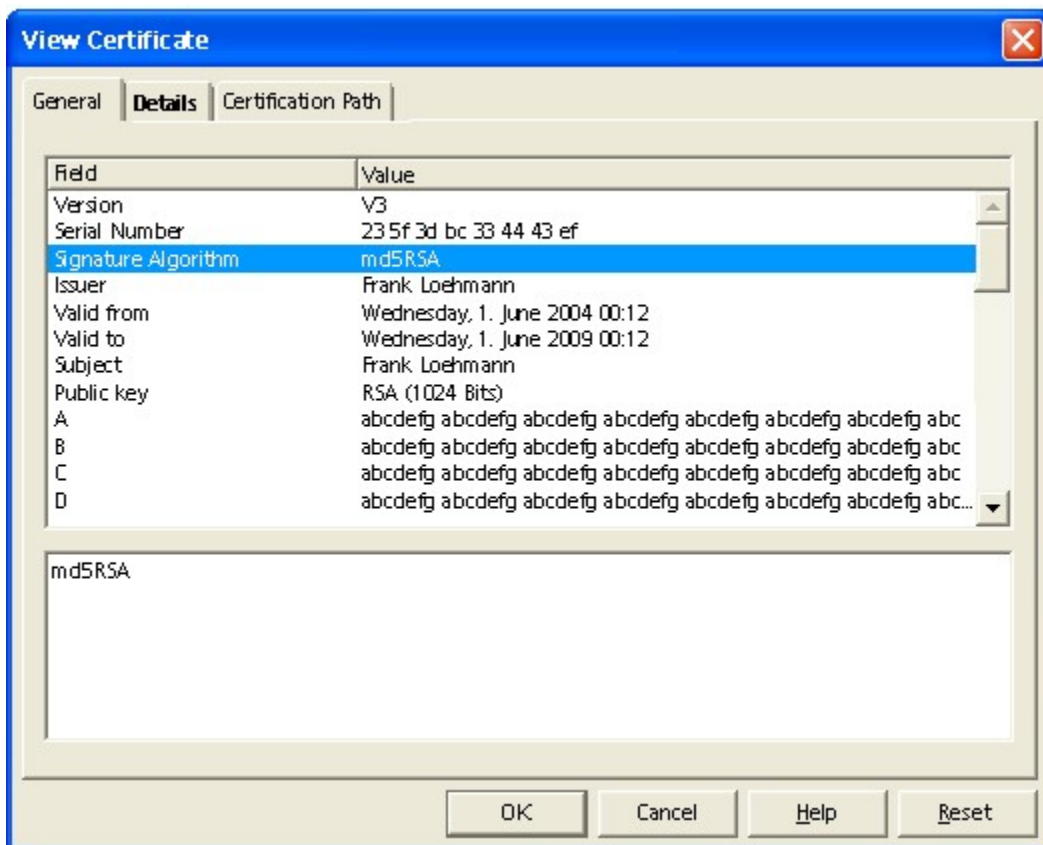
Illustration 96 Certificate Dialog - Tab 2 - Details

String List

Item	English	German	Comments
Column Label	Field	Feld	
Column Label	Value	Wert	
Field label text 1	Version	Version	
Field label text 2	Serial Number	Seriennummer	
Field label text 3	Issuer	Aussteller	
Field label text 4	Valid From	Gültig von	TRANSLATORS!: note the preposition here. Where necessary in your language,

Item	EnglISH	German	Comments
			choose a noun to have the same meaning as this phrase.
Field label text 5	Valid To	Gültig bis	TRANSLATORS!: note the preposition here. Where necessary in your language, choose a noun to have the same meaning as this phrase.
Field label text 6	Subject	Betreff	
Field label text 7	Public Key	Öffentlicher Schlüssel	
Field label text 8	Enhanced Key Usage	Erweiterte Schlüsselverwendung	
Field label text 9	Authority Key Identifier	?Autoritätsschlüsselbezeichner?	PJC/EM->MT/FL: decide on German pls. Suggestions (MSO) for authority depending on which authority you mean "Zertifizierungsstelle" or "Sicherheitsstelle"; It would be good break this big work into a genitive phrase.
Field label text 10	Thumbprint Algorithm	Fingerabdruck-Algorithmus	
Field label text 11	Thumbprint	Fingerabdruck	
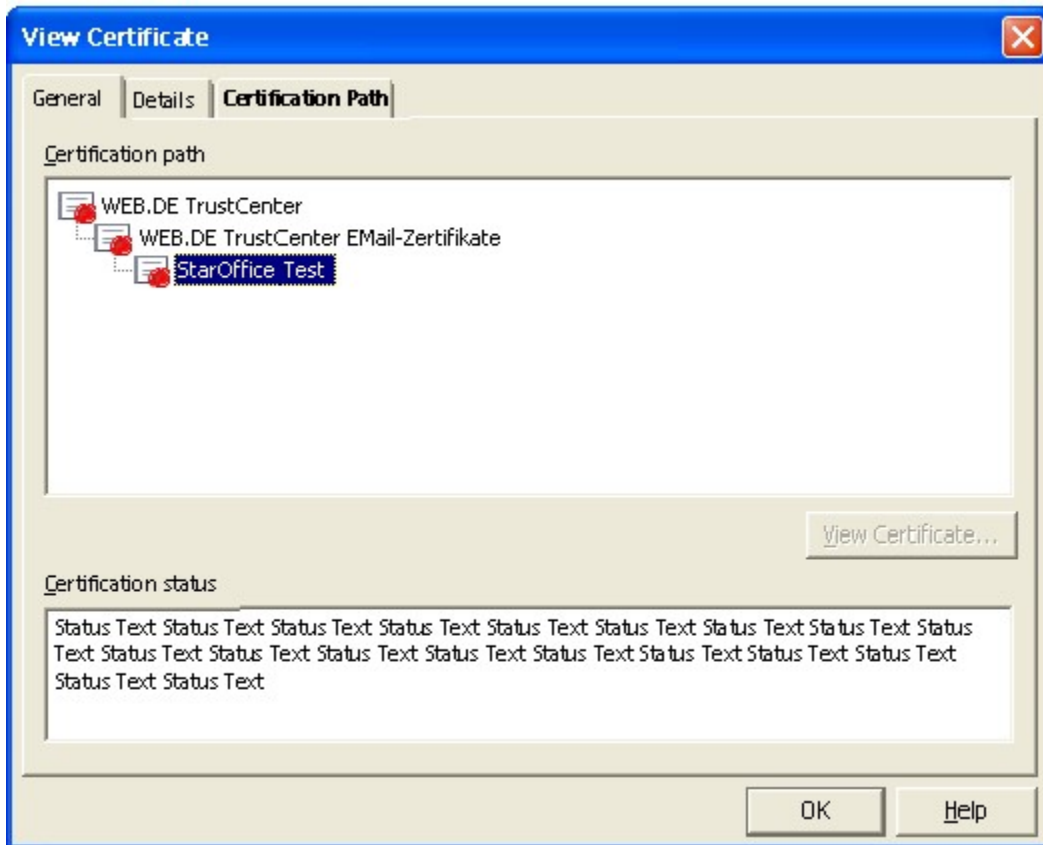
Illustration 97 Certificate Dialog - Tab 3 - Certification Path

String List

Item	English	German	Comments
Label	Certificate path	Zertifikatspfad	
Label	Certificate status	Zertifikatsstatus	

6.5   Document Properties

485   The document properties dialog shows the name, date and time when the document has been signed. If more than one signature is assigned to a document, the dialog shows only "Multiple signed document" instead of name and date of the signer.
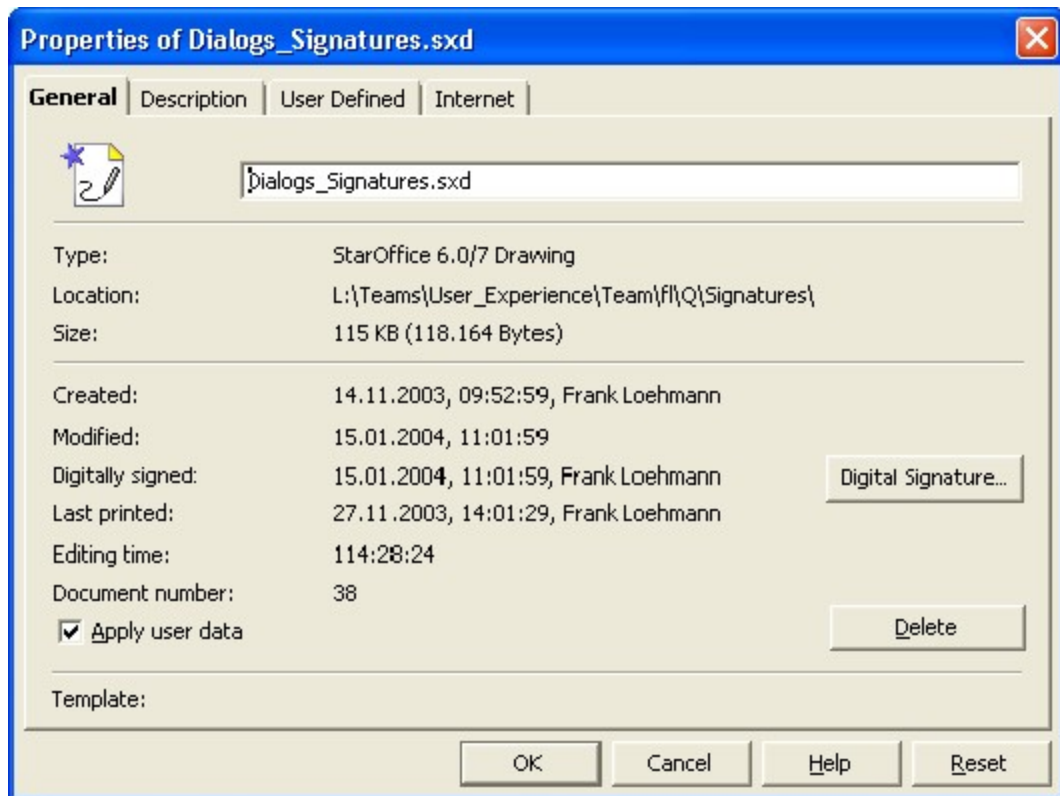
Illustration 98 Document properties dialog with new signature field and View.. button

Item	English	German	Comments
Button	Digital Signature...	Digitale Signatur...	
Label	Digitally signed:	Digital signiert:	
Label	Multiply signed document	Mehrfach signiertes Dokument	

The Digital Signature... button calls a the Digital signature dialog to show all currently assigned signatures. The Digital Signature dialog allows to remove a signature from the document.

490 ### 6.5.1 Changed Default Setting in Tools-Options

In OO.org 1.1 printing sets the document modified status. This could be disabled by a Tools-Option setting, but the default is currently set to on, so that printing modifies the document. This causes a problem, because printing a signed document prompts for saving the document on closing, but saving would remove the assigned signature.

495 Since this is not only a problem when having a signature, the setting '[ ] Printing sets document modified status' in Tools-Options-StarOffice-General will be changed to off by default.

6.6 Macro Security

6.6.1 Security Warning Dialog

The following dialog appears, if a document contains macros.

6.6.2 Macro Security Dialog

500

The Macro dialog is completely redesigned. The old concept of "trusted pathes" for libraries only has been dropped. The new dialog uses a security level concept. The levels Very High, High, Medium and Low are used. Medium is default. The trusted file locations settings from the "Very high" level are valid on all other security levels as well.
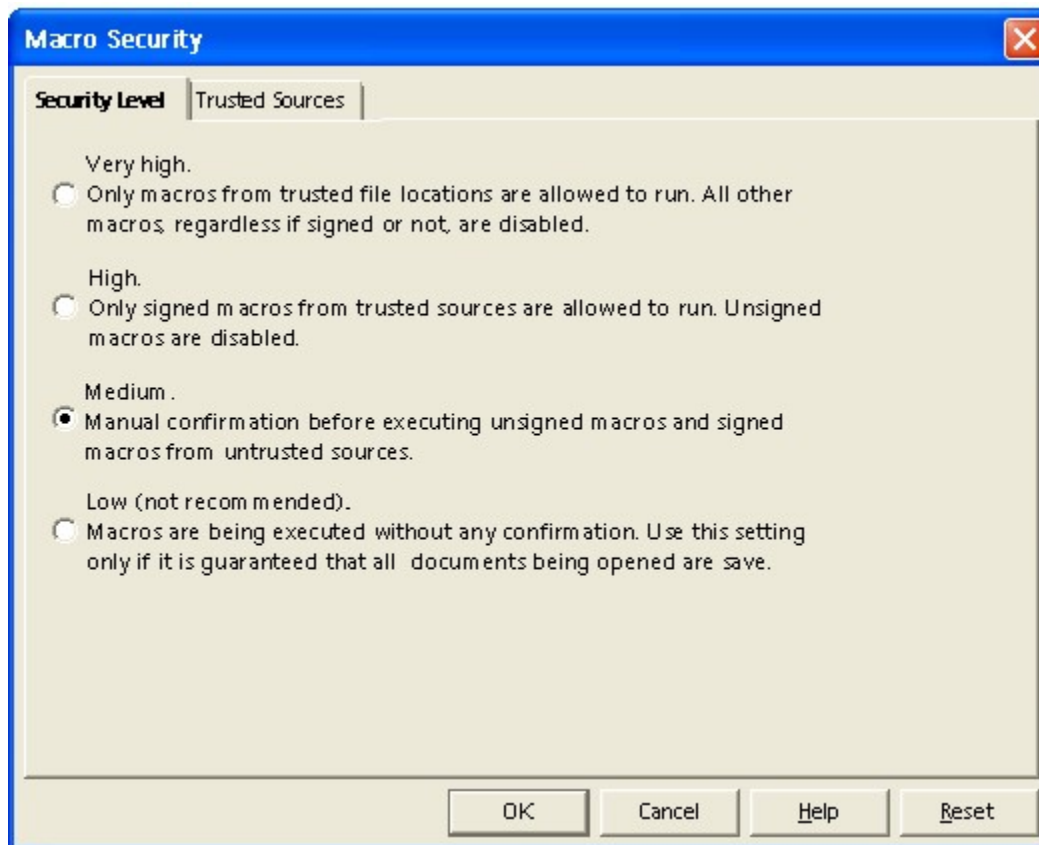
Illustration 99 Macro Security Settings - Security Level tab

505

Apoc Settings (Issue #118519)

The radio button group of the Macro Security tab page could be protected[8] via a setting in the Apoc configuration manager. The value of the radio group is fixed, disabled and a lock symbol is shown.

String List

Item	English	German	Comments
Option0	Very high. Only macros from trusted file locations are allowed to run. All other macros, regardless whether signed or not, are disabled.	Sehr hoch. Nur Makros aus vertrauenswürdigen Dateiquellen werden ausgeführt. Alle anderen Makros, unabhängig ob signiert	

8   Protected means that those controls are disabled and a lock symbol is shown in front of the control. Please see http://so-doc.germany.sun.com/Projects/StarOffice/SO_6.x/Proposals/Drafts/ManagementConsole/Spec/Config _Items_rev8.sxw following behaviour was observed in SO8:

Item	English	German	Comments
		oder nicht, werden automatisch deaktiviert.	
Option1	High. Only signed macros from trusted sources are allowed to run. Unsigned macros are disabled.	Hoch. Nur signierte Makros aus vertrauenswürdigen Quellen werden ausgeführt. Nicht signierte Makros werden automatisch deaktiviert.	
Option2	Medium. Confirmation required before executing macros from untrusted sources.	Mittel. Bestätigung vor dem Ausführen von Makros aus nicht vertrauenswürdigen Quellen.	
Option3	Low (not recommended). all macros will be executed without confirmation. Use this setting only if you are certain that all documents that will be opened are safe.	Niedrig (nicht empfehlenswert). Alle Makros werden ohne Nachfrage ausgeführt. Diese Einstellung sollte nur benutzt werden, wenn sichergestellt werden kann, dass nur sichere Dokumente geöffnet werden.	
Tab Name	Security Level	Sicherheitsstufe	
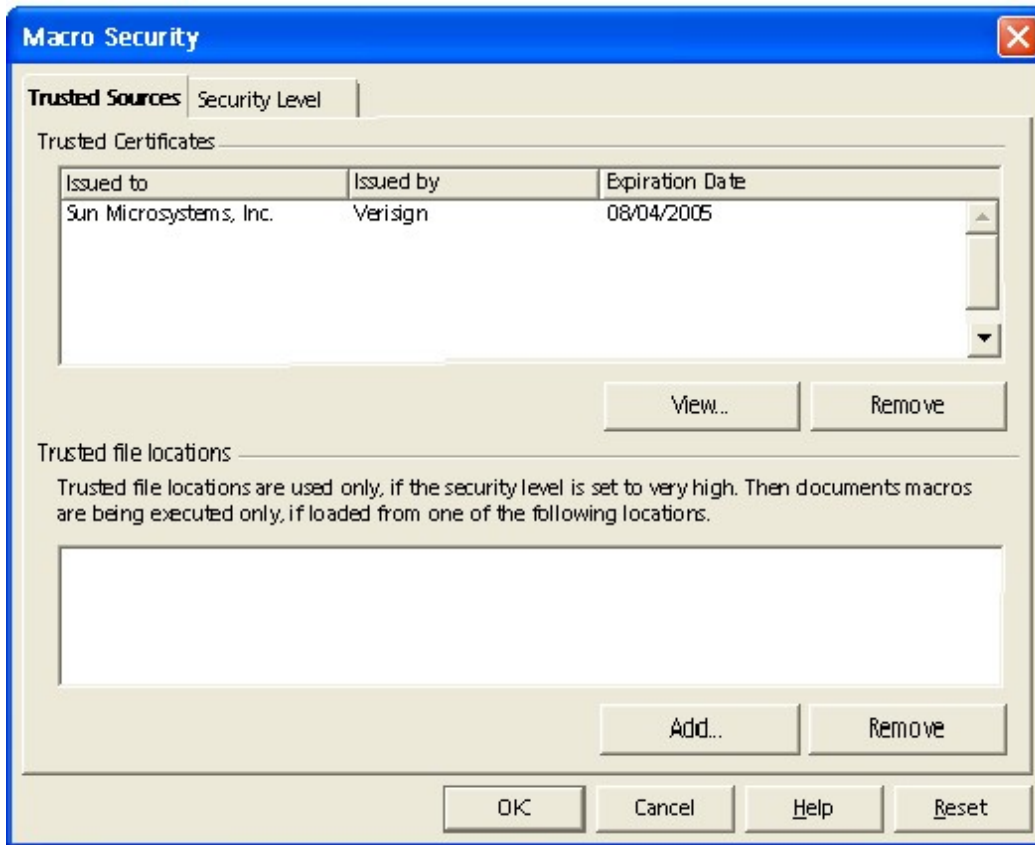
Illustration 100 Macro Security Settings - Security Level tab

Note: Please note that the Trusted Sources and Security Level tab pages are only switched in this mockup to reduce the design effort for this specification. Please also note that text in other languages than English may be much longer, so that a two line text must be able to become a three line text.

The Add**...** button calls a folder picker dialog. The Remove buttons are only enabled, if an entry is selected within the list box. The View button is also only enabled, if a certificate is selected and calls the View Certificate dialog described in chapter 6.4.5 View Certificate Dialog on page 65.

Apoc Settings (Issue #118519)

The trusted file location list box could be protected[9] via a setting in the Apoc configuration manager. The values of the listbox are fixed, disabled and a lock symbol is shown. Furthermore the Add.. and Remove buttons are disabled.

The trusted certificates list box could be administrated by Apoc 1.1 in any way, because Apoc is not capable of loading data (in this case certificates) from a local disk.

Macro Organizer Dialog String - Modules List

Item	English	German	Comments
Label	Trusted certificates	Vertrauenswürdige Zertifikate	
Label	Issued to	Ausgestellt für	TRANSLATORS!: note the preposition here. Where necessary in your language, choose a noun

---

9   Protected means that those controls are disabled and a lock symbol is shown in front of the control. Please see http://so-doc.germany.sun.com/Projects/StarOffice/SO_6.x/Proposals/Drafts/ManagementConsole/Spec/Config_Items_rev8.sxw following behaviour was observered in SO8:

Item	English	German	Comments
			to have the same meaning as this phrase.
Label	Issued by	Ausgestellt durch	TRANSLATORS!: note the preposition here. Where necessary in your language, choose a noun to have the same meaning as this phrase.
Label	Expiration date	Ablaufdatum	

Item	English	German	Comments
Tab Name	Trusted Sources	Vertrauenswürdige Quellen	
Button1	Add...	Hinzufügen...	
Button2	View...	Zeigen...	
Button3	Remove	Entfernen	
Label	Trusted file locations	Vertrauenswürdige Dateiquellen	
Text	Trusted file locations are used only if the security level is set to 'very high'. With this setting, document macros are only executed if they have been opened from one of the following locations.	Vertrauenswürdige Dateiquellen werden nur benutzt, wenn die Sicherheitseinstellungen auf sehr hoch eingestellt sind. Dann werden nur Dokumentmakros aus den folgenden Quellen ausgeführt.	

6.6.3 Trust Source of Macro Dialog for Signed Macros

OO.org raises a dialog if a signed macro will be loaded with the document and it's source has not been trusted before. This dialog allows the user to add the source to trusted sources and execute the macro.
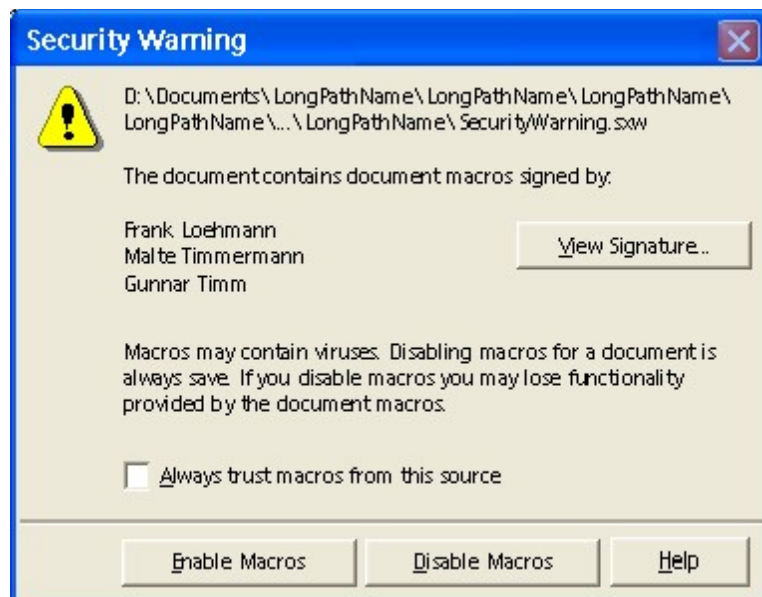
Illustration 101 Security Warning Dialog

525

- The dialog closer (cancel action) is disabled to force the user to decide whether to enable or disable macros.

- The Disable Macros button is defaulted

- The Disable Macros button is disabled if the check box to trust macros is turned on

- The Enable Macros button is disabled if security level is high and the check box to trust macros is not turned on.

String List

Item	English	German	Comments
Title	%PRODUCTNAME Security Warning	%PRODUCTNAME Sicherheitswarnung	
Text	This document contains macros signed by:	Dieses Dokument enthält Makros, die signiert wurden von:	
Button	View Signature...	Signatur zeigen...	
Text	Macros may contain viruses. Disabling macros for a document is always safe. If you disable macros you may lose some functionality.	Makros können Viren enthalten. Es ist immer sicher, Makros zu deaktivieren. Dadurch geht eventuell Funktionalität verloren.	
Text	Always trust macros from this source	Makros aus dieser Quelle immer vertrauen	
Button	Enable Macros	Makros aktivieren	
Button	Disable Macros	Makros deaktivieren	

6.6.4 Enable/Disable Document Macro Dialog for Unsigned Macros

Illustration 102 Security Warning - unsigned macros dialog

- The dialog closer (cancel action) is disabled to force the user to decide whether to enable or disable macros.

- The Disable Macros button is defaulted

String List

Item	English	German	Comments
Title	%PRODUCTNAME - Security Warning	%PRODUCTNAME - Sicherheitswarnung	
Text	This document contains macros.	Dieses Dokument enthält	

Item	English	German	Comments
		Makros.	
Text	Macros may contain viruses. Disabling macros for a document is always safe. If you disable macros you may lose some functionality.	Makros können Viren enthalten. Es ist immer sicher, Makros zu deaktivieren. Dadurch geht eventuell Funktionalität verloren.	

6.6.5 Marco Warning for Security Setting High and Very High.

If a document contains macros and the macro will not be executed due to the macro security is set to high or very high, the following notification dialog appears.

Note: We need to have a configuration entry to suppress this dialog (no GUI needed).

String List

Item	English	German	Comments
Title	%Productname	%Productname	**Should not be translated**
Text	This document contains macros.	Dieses Dokument enthält Makros.	
Button	Execution of this macros is disabled due to the current macro security setting. Therefore, some functionality may not be available.	Das Ausführen dieses Makros wird gemäß der aktuellen Makro-Sicherheitseinstellungen unterbunden. Deshalb könnten einige Funktionen nicht verfügbar sein.	

6.7 Error Conditions

None

7 Future Tasks (not relevant for OO.org 2.0)

The following tasks are not planned to be implemented for OO.org 2.0.

7.1 **Signing of Microsoft Office Documents**

7.2 **Signing on PDF Export**

7.3 Signing of Sections in Writer

OO.org Writer allows to sign sections independently from signing the whole document.

- A signed section is automatically write protected (password is optional).
- The signature of a section gets lost, if the protection of the section gets removed.
- A double click on the signed icon in the status bar shows the signature.
- Only the **content** of the section will be signed. The formatting (i.e. paragraph templates) is not signed. This allows the section to be an active part of the document.

Illustration 103 Signed section if Writer – Version A

Illustration 104 Signed section in Writer - Version B

Illustration 105 Signed section in Writer - Version C
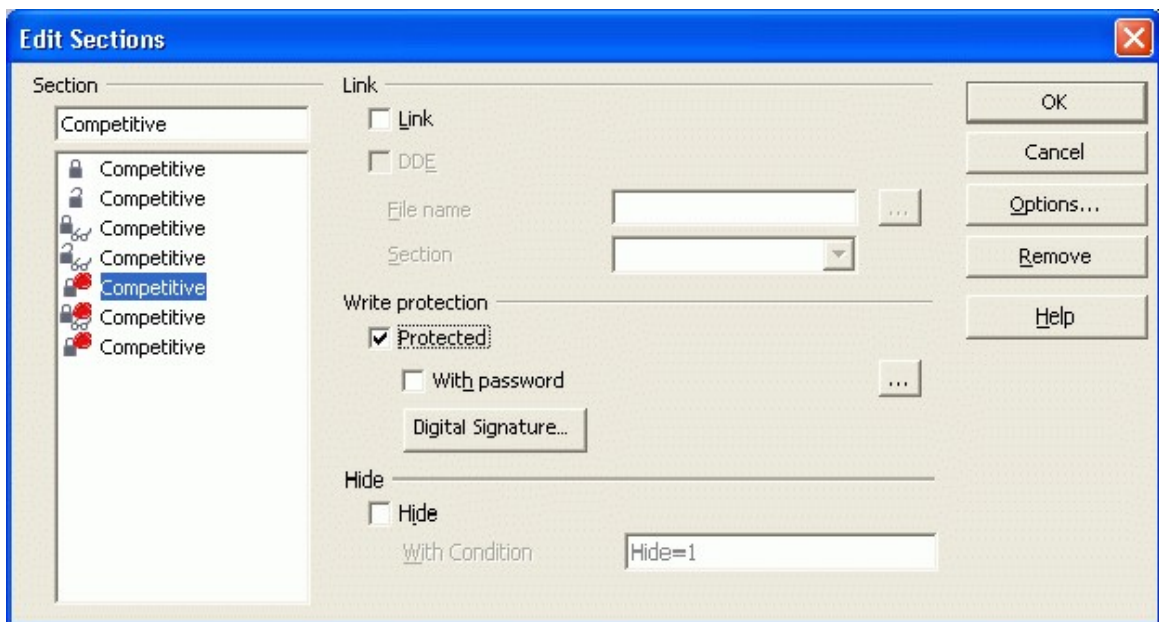
Illustration 106 Sign a section in the section dialog.

555   Icons will be provided directly by Stella Schulze

7.4 Signing of Table Sheets in Calc

OO.org Calc offers the possibility to sign table sheets independently from signing the whole document. The table sheet will be signed as is with references, with fields and formulas.

- A signed table sheet gets protected without password.

560   - The signature of a table sheet gets lost, if the content of the signed sheet will be modified.

- A double click on the signature icon shows the signature.

Illustration 107 A table sheet could be signed in Calc

- The new password dialog layout will be used for protect document and protect table dialog
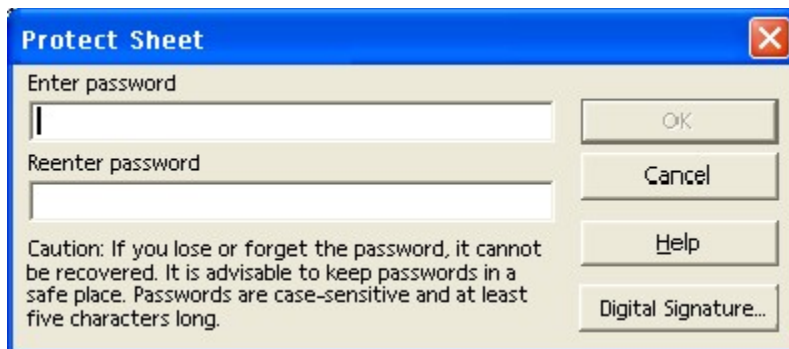
Illustration 108 Protect Sheet dialog in Calc offers a new button Digital Signature... and uses the new dialog layout for assigning passwords.

Protect Sheet Strings

Item	English	German	Comments
Button	Digital Signature...	Digitale Signatur...	

7.5 New Password Dialog

565 MT->i-Team: Change min. password length to 1 ?!

##FL: Notice: The password dialog will not be realized for EA. After that we have to discuss the following: adjust distance between path and dialog text in enter password dialog, think about other solution to cover the min. 5 characters issue, additional password dialogs have to be specified in sfx and svx (see notes section for detailed screenshots.

570 The overworked password dialogs replace the current ones office wide.

The O.K. Button is disabled until the minimum length of 5 characters hasn't been entered. The dialog shows a notice about keeping passwords in a safe place,

- the case-sensitiveness of passwords

- the minimum length of 5 characters.

575 - Note: If we are able to **export (not for OO.org 2.0)** encrypted MS documents, the minimum length of 5 for a password is not valid. This means that the OK button is always enabled and the notice text in the password dialog is displayed as follows.

Changed Warning in Password Dialog for Importing MS Document with passwords

Item	English	German	Comments
Text	WARNING: If you lose or forget the password, it cannot be recovered. It is advisable to keep passwords in a safe place. Passwords are case-sensitive.	ACHTUNG Falls Sie das Kennwort vergessen oder verlieren, kann es nicht wieder hergestellt werden. Es ist ratsam, das Kennwort an einem sicheren Platz aufzubewahren. Kennwörter unterscheiden Groß- / Kleinschreibung.	.

The password has to be retyped correctly in the "Reenter Password" field.

Illustration 109 Set a new password

580 **Password Dialog Strings**

Item	English	German	Comments
Text	WARNING: If you lose or forget the password, it cannot be recovered. It is advisable to keep passwords in a safe place. Passwords are case-sensitive and at least five characters long.	ACHTUNG: Falls Sie das Kennwort vergessen oder verlieren, kann es nicht wieder hergestellt werden. Es ist ratsam, das Kennwort an einem sicheren Platz aufzubewahren. Kennwörter unterscheiden Groß- / Kleinschreibung und sind mindestens fünf Zeichen lang.	.
Label	Enter password	Kennwort eingeben	
Label	Retype password	Kennwort wiederholen	
Label	Enter password to open file:	Kennwort zum Öffnen der Datei eingeben:	

Item	English	German	Comments
Dialog title	Enter Password	Kennwort eingeben	Capitalization different for dialog title

If the reentered password does not match to the original one, the following notice dialog appears:

Error **Dialog:**

Item	English	German	Comments
Notice Dialog	The password confirmation does not match.	Das neue Kennwort und seine Bestätigung sind nicht identisch.	**Dialog has an OK button.**
Button	OK	OK	

The password dialog is being shown after pressing the OK button. The focus is then set to the Reenter Password field. The field itself is empty.

585 An overworked Enter Password dialog replaces the current (OO.org 1.1) dialog. The notice shown is the same as in the define password dialog above.
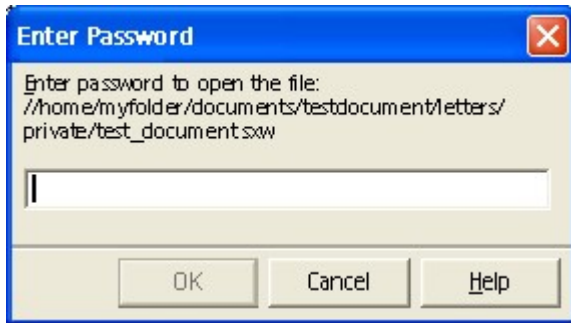
Illustration 110 Overworked enter password dialog

If the password entered does not match to the document password, the following dialog appears:

Warning Dialog:

Item	English	German	Comments
Notice Dialog	The password is incorrect. The document cannot be opened.	Das Kennwort ist ungültig. Das Dokument kann nicht geöffnet werden.	**Dialog has an OK button.**
Text	Enter password to open file: %DOCUMENTPATHANDNAME%	Kennwort für die Datei eingeben:%DOCUMENTPATHA NDNAME%	**TRANSLATORS! %DOCUMENTPA THANDNAME% is a placeholder. Do not translate.**

7.6 **After Beta Tasks**

590

7.6.1 **Warning Dialog if Mozilla Profile is not Found (#i37609)**

The Mozilla crypto engine is needed for using digital signatures in OOo on Unix systems. The following dialog appears, if the Mozilla user profile could not be found, i.e when calling Files - Digital Signatures function.

Warning Dialog String List

Item	English	German	Comments
Dialog text	Digital signatures functionality could not be used, because no Mozilla user profile was found. Please check the Mozilla installation.	Die digitale Signaturen Funktion kann nicht benutzt werden, da kein Mozilla Benutzerprofil gefunden wurde. Bitte überprüfen Sie die Mozilla Installation.	Dialog has OK button

595

Other Future Tasks

- **What's about imported MS documents?**
- **Set permissions restriction for a document (User Rights Management)**
  - Per User
  - Per Group

600

  - Permission types
    - Read/Write access to document
    - Add comments only
    - Read-only access to document

- Load a different version of the document??

- Saving document under a new file name / Send document (i.e. as an e-mail)

- Content copying or extraction via clipboard

- Form field fill-in

- Signing

- Content linking allowed (only possible if content is not encrypted

- Printing / PDF creation

- Problems

- How to deal with MS documents with permissions?

7.7 Normal Writer Edit Mode Behavior

A tip help is shown (see string table below for details) when the mouse is placed on a URL. If the CTRL key is pressed, the i-beam cursor changes to a finger cursor and a click on the link opens the URL in the system's browser.

String list

Tip help	English	German	Comments
Tip help	<URL> CTRL+click to follow link	<URL> Strg+Klick zum Verfolgen der Verknüpfung	**If target is not within the current document.** **The URL tip help is limited to a width of 45 characters, because URLs could become very long.**

7.7.1 Links in Read-Only / Form Use Mode / Help System

In read-only mode/Form use mode of a document (this includes the Writer help viewer), all links are live and the finger cursor is used by default.

7.7.2 Smart Card Support for Signing Documents

Has to be implemented to support government initiatives for digital documents within administration departments.

8 Legal Issues

None

9 Notes

Old Dialog:

Item	English	German	Comments
Dialog Tile	%PRODUCTNAME %PRODUCTVERSION	%PRODUCTNAME %PRODUCTVERSION	
Dialog text	The document is already signed.	Das Dokument ist bereits signiert.	

Item	English	German	Comments
Dialog text	Do you want to add another signature or remove current signature(s) and sign again?	Möchten Sie eine weitere Signatur hinzufügen oder möchten Sie die vorhandenen Signatur(en) entfernen und das Dokument neu signieren?	
Button	Add Signature...	Signatur hinzufügen...	**Add signature button calls the Digital Signature dialog.**
Button	New Signature...	Neue Signatur...	
Button	Cancel	Abbrechen	

2. , the following dialog appears and recommends to open the current document in read-only mode:

Item	English	German	Comments
Dialog text	$PATHANDFILENAME should be opened in read-only mode unless changes to it need to be saved.	$PATHANDFILENAME sollte schreibgeschützt geöffnet werden, solange keine Änderungen an diesem Dokument gespeichert werden müssen.	**TRANSLATORS! $PATHANDFILENAME is a placeholder. Do not translate it.**
Dialog text	Do you want to open the document in read-only mode?	Soll das Dokument mit Schreibschutz geöffnet werden?	
Button1	Yes	Ja	
Button2	No	Nein	
Button3	Cancel	Abbrechen	

630 **For Document Macros**
If present, document macro are teste before testing the signed document content. So if the user continues loading the document with a broken macro signature, he gets no separate warning for the broken document content, because this status could be seen in the status bar.

Item	English	German	Comments
Dialog Tile	Invalid Macro Signature	Ungültige Makro Signatur	
Dialog text	The digitally signed document macros do not match the current document macro signature.	Die digital signierten Dokumentmakros stimmen nicht mit der aktuellen Dokumentsignatur überein.	
Dialog text	This could be the result of document manipulation or of structural document damage due to data transmission.	Dieses deutet auf eine Dokumentmanipulation oder einen Übertragungsfehler hin.	
Dialog text	We strongly recommend that you do not trust the current macro.	Wir empfehlen Ihnen dringend, dem aktuellen Dokumentmakros nicht zu trauen.	
Dialog text	Do you want to continue opening the document?	Möchten Sie das Öffnen des Dokumentes fortsetzen?	
Button	Yes	Ja	
Button	No	Nein	**The "No" button is defaulted. The "No" button is defaulted.**

635 Additional password dialogs:
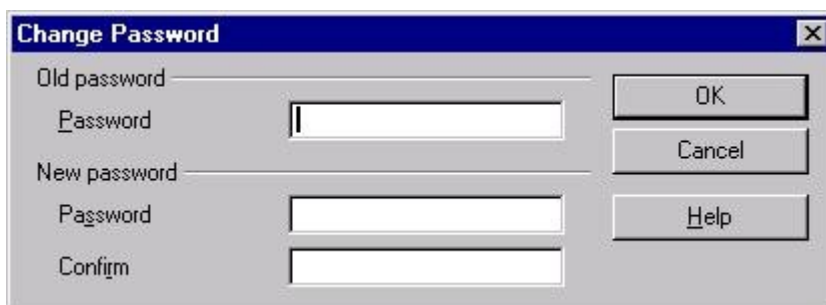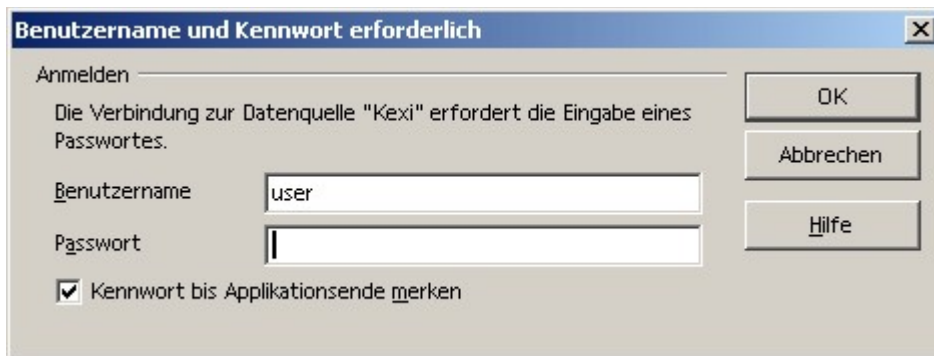
10   References and Links

Signatures:

http://www.w3.org/Signature/

Here is a list of rules and regulations that have special security requirements:

640
- Government Paperwork Elimination Act (GPEA)

- Health Insurance Portability and Accountability Act (HIPAA)

- 21 CFR Part 11 (pharmaceutical industry)

- German Act regarding Digital Signatures (German: "Signaturgesetz" - http://www.bsi.de/esig/basics/legalbas/sigg2001.pdf)

645
- Electronic Signatures Directive by the EC (http://www-personal.umich.edu/~rmann/Statutes/Electronic%20Signatures%20Directive.PDF)

- European Electronic Signature Standardization Initiative (EESSI)

- www.osci.de , http://www.bund.de/BundOnline-2005-.6164.htm

Illustration Index