Das Handbuch zu Kleopatra

Marc Mutz
Entwickler: David Faure
Entwickler: Steffen Hansen
Entwickler: Matthias Kalle Dalheimer
Entwickler: Jesper Pedersen
Entwickler: Daniel Molkentin
Deutsche Übersetzung: Matthias Kalle Dalheimer
Deutsche Übersetzung: Torbjörn Klatt

Inhaltsverzeichnis

Tabellenverzeichnis

Zusammenfassung

Kleopatra ist ein Hilfsprogramm zum Verwalten von X.509- und OpenPGP-Zertifikaten.

Kapitel 1

Einführung

Kleopatra ist das KDE-Programm zum Verwalten von X.509- und OpenPGP-Zertifikaten in GpgSM- und GPG-Schlüsselspeichern, und zum Abfragen von Zertifikaten von LDAP- und anderen Zertifikats-Servern.

Kleopatra kann sowohl aus dem Menü **Extras** → **Zertifikatsverwaltung** von KMail als auch von der Befehlszeile aus gestartet werden. Das ausführbare Programm von Kleopatra heißt **`kleopatra`**.

> ANMERKUNG
> Dieses Programm ist nach Kleopatra benannt, einer berühmten ägyptischen Pharaonin, die zur Zeit Julius Cäsars gelebt hat, mit dem sie ein Kind namens Caesarion hatte, das nicht als sein Erbe anerkannt wurde.
> Der Name wurde gewählt, weil dieses Programm aus dem Ägypten-Projekten stammt.

Kapitel 2

Die wichtigsten Funktionen

2.1 Anzeige des lokalen Schlüsselspeichers

Die wichtigste Funktion von Kleopatra ist das Anzeigen und Editieren des Inhalts des lokalen Schlüsselspeichers, der dem Schlüsselring-Konzept von GPG ähnelt, auch wenn man diesen Vergleich nicht zu sehr bemühen sollte.

Das Hauptfenster besteht aus mehreren Unterfenstern mit Listen von Zertifikaten, der Menüleiste und der Suchleiste am oberen Rand, sowie der Statuszeile am unteren Rand.

Jede Zeile in der Schlüsselliste entspricht einem Zertifikat, das durch den sogenannten **Betreff-DN** identifiziert wird. DN ist ein Akronym für den englischen Ausdruck „Distinguished Name", ein hierarchischer Bezeichner, der einem Dateisystempfad mit ungewöhnlicher Syntax ähnelt und ein bestimmtes Zertifikat eindeutig global identifizieren soll.

Um gültig und damit verwendbar zu sein, müssen (öffentliche) Schlüssel von einer CA (Certification Authority; Zertifizierungsinstanz) signiert sein. Diese Signaturen werden Zertifikate genannt, aber normalerweise werden die Ausdrücke „Zertifikat" und „(öffentlicher) Schlüssel" austauschbar verwendet, sofern das nicht ausdrücklich anders angegeben ist.

CAs müssen ebenfalls wiederum von anderen CAs signiert sein, um gültig zu sein. Natürlich muss diese Kette irgendwo enden, deshalb signiert die oberste CA (die Wurzel-CA) ihren Schlüssel mit sich selbst (dies wird eine Selbst-Signatur genannt). Wurzel-Zertifikaten muss daher die Gültigkeit (meistens Vertrauenswürdigkeit genannt) manuell zugewiesen werden, z. B. durch Vergleichen des Fingerabdrucks mit dem auf der Website der CA. Dies wird normalerweise vom Systemverwalter oder dem Hersteller des Produkts, das Zertifikate verwendet, vorgenommen, kann aber über die Befehlszeilenschnittstelle von GpgSM auch vom Benutzer durchgeführt werden.

Um zu sehen, welche Zertifikate Wurzel-Zertifikate sind, können Sie mit **Ansicht → Hierarchische Zertifikatsliste** in den hierarchischen Anzeigemodus wechseln.

Sie können sich die Details eines beliebigen Zertifikats durch Doppelklick auf das Zertifikat oder durch Verwendung von **Ansicht → Zertifikatsdetails** ansehen. Dabei wird ein Dialog geöffnet, in dem die gängigsten Eigenschaften des Zertifikats, dessen Zertifikatskette (d. h. die Kette der Aussteller bis zur Wurzel-CA) und alle Informationen, die das Backend über das Zertifikat ermitteln kann, angezeigt werden.

Wenn Sie den Inhalt des Schlüsselspeichers außerhalb von Kleopatra verändern (z. B. über die Befehlszeilenschnittstelle von GpgSM), dann können Sie die Anzeige mit **Ansicht → Aktualisieren (F5)** aktualisieren.

2.2 Zertifikate suchen und importieren

Normalerweise bekommen Sie neue Zertifikate durch Überprüfen von Signaturen in E-Mail-Nachrichten, weil die Zertifikate normalerweise in die Signaturen, die damit vorgenommen wurden, eingebettet werden. Wenn Sie aber jemandem eine Nachricht senden wollen, mit dem Sie bisher noch keinen Kontakt hatten, dann müssen Sie das Zertifikat aus einem LDAP-Ordner (GpgSM kann das aber auch automatisch für Sie tun) oder einer Datei holen. Außerdem müssen Sie Ihr eigenes Zertifikat importieren, nachdem Sie die Antwort der CA auf Ihre Zertifizierungsanfrage bekommen haben.

Um ein Zertifikat in einem LDAP-Ordner zu suchen, wählen Sie **Datei** → **Zertifikate auf Server suchen ...** und geben einen Text, wie z. B. den Namen der Person, deren Zertifikat Sie suchen, in das Eingabefeld des Dialogs **Zertifikatssuche auf Schlüsselserver** ein. Drücken Sie dann den Knopf **Suchen**. Gefundene Zertifikate werden dann in der Schlüsselliste unter der Suchleiste angezeigt. Wählen Sie ein Zertifikat aus, um sich mit **Details** zusätzliche Informationen anzeigen zu lassen oder klicken Sie auf **Importieren**, um das Zertifikat in den lokalen Schlüsselspeicher herunterzuladen.

Sie können die Liste der zu durchsuchenden LDAP-Server auf der Seite **Verzeichnisdienste** des Einrichtungsdialogs von Kleopatra einstellen.

Wenn Sie die Zertifikate als eine Datei bekommen haben, versuchen Sie es mit **Datei** → **Zertifikate importieren ... (Strg+I)** . GpgSM muss dazu das Format der Zertifikatsdatei unterstützen; im GpgSM-Handbuch finden Sie eine Liste der unterstützten Dateiformate.

Wenn Sie Ihr Schlüsselpaar nicht mit GpgSM erzeugt haben, müssen Sie auch den öffentlichen und den geheimen Schlüssel aus der PKCS#12-Datei importieren, die Sie von der CA bekommen haben. Dies können Sie von der Befehlszeile aus mit **`kleopatra --import-certificate dateiname`** oder in Kleopatra mit **Datei** → **Zertifikate importieren ... (Strg+I)** durchführen, genauso, wie Sie es auch für „normale" Zertifikate tun würden.

2.3 Neue Schlüsselpaare erzeugen

Der Menüeintrag **Datei** → **Neues Zertifikat ... (Strg+N)** startet den **Assistenten zur Erstellung eines Schlüsselpaars**, der Sie durch die notwendigen Schritte zur Erzeugung einer Zertifikatsanfrage führt.

Wenn Sie mit dem Ausfüllen einer Seite im Assistenten fertig sind, klicken Sie auf **Weiter**, um zum nächsten Schritt zu kommen (mit **Zurück** können Sie bereits durchgeführte Schritte noch einmal anschauen). Die Erzeugung der Zertifikatsanfrage kann jederzeit mit der Schaltfläche **Abbrechen** abgebrochen werden.

Auf der ersten Seite des Assistenten wird die Art des Zertifikats ausgewählt, das erstellt werden soll.

Persönliches OpenPGP-Schlüsselpaar erzeugen

OpenPGP-Schlüsselpaare werden lokal auf Ihrem Rechner erstellt und von Ihren Freunden und Bekannten beglaubigt. Es gibt keine zentrale Beglaubigungsinstanz; jeder Anwender erstellt ein persönliches Netz des Vertrauens durch die Beglaubigung der Schlüsselpaare anderer durch sein eigenes Zertifikat.

Es muss ein **Name**, eine **E-Mail**-Adresse und wahlweise ein **Kommentar** eingegeben werden.

Persönliches X.509-Schlüsselpaar und Beglaubigungs-Anfrage erstellen

X.509-Schlüsselpaare werden lokal erstellt, aber zentral durch eine Beglaubigungsinstanz (Certificate Authority, CA) beglaubigt. CAs können andere CAs beglaubigen, dadurch entsteht eine hierarchische Vertrauenskette.
Der nächste Schritt im Assistenten besteht darin, Ihre persönlichen Daten für das Zertifikat einzutragen. Die auszufüllenden Felder lauten:

- **Allgemeiner Name (CN):** Ihr Name;
- **E-Mail-Adresse (EMAIL):** Ihre E-Mail-Adresse; geben Sie diese sorgfältig ein, denn an diese Adresse werden Nachrichten verschickt, wenn Ihr Zertifikat verwendet wird.
- **Ort (L):** Die Stadt oder der Ort, wo Sie leben;
- **Abteilung (OU):** Die Organisationseinheit, zu der Sie gehören (etwa „Logistik");
- **Organisation (O):** Die Organisation, die Sie repräsentieren (etwa Ihr Arbeitgeber);
- **Ländercode (C):** Der zweibuchstabige Code, der das Land bezeichnet, in dem Sie leben (z. B. „DE");

Im nächsten Schritt des Assistenten wählen Sie aus, ob das Zertifikat in einer Datei gespeichert oder direkt an eine CA geschickt werden soll. Sie müssen entweder den Dateinamen oder die E-Mail-Adresse, an die die Zertifikatsanfrage geschickt werden soll, angeben.

2.3.1 Einen Schlüssel widerrufen

Solange Sie den privaten Schlüssel und die Passphrase besitzen, können Sie einen abgelaufenen Schlüssel wieder benutzbar machen. Wenn Sie einen Schlüssel endgültig unbenutzbar machen möchten, müssen Sie ihn sperren. Das wird mittels einer speziellen Sperrsignatur erreicht, die zum Schlüssel hinzugefügt wird.

Eine Widerrufssignatur in einer gesonderten Datei gespeichert. Diese kann später in den Schlüsselbund importiert werden und wird dann an den Schlüssel angehängt und macht ihn damit unbrauchbar. Bitte beachten Sie, dass dazu das Passwort des Schlüssels nicht erforderlich ist. Deshalb sollten Sie die Datei mit der Sperrsignatur sicher aufbewahren, am besten getrennt von Ihrem privaten Schlüssel. Es ist ratsam, dazu einen Ort zu wählen, der nicht mit einem Computer verbunden ist, z. B. können Sie die Datei auf ein externes Speichermedium wie einen USB-Stick übertragen oder Sie drucken sie einfach aus.

In Kleopatra gibt es keine Funktion, um so eine Widerrufssignatur zu einem beliebigen Zeitpunkt zu erzeugen. Sie können dazu jedoch das KDE-Programm KGpg verwenden und in diesem Programm **Schlüssel** → **Schlüssel sperren** im Menü wählen und dann gegebenenfalls diese Signatur sofort in Ihren Schlüsselring importieren.

Als andere Möglichkeit um ein Widerrufs-Zertifikat können Sie GPG direkt auf der Befehlszeile verwenden:**`gpg --output revocation_certificate.asc --gen-revoke ihr_schlüssel`**. Als Argument für *`ihr_schlüssel`* muss die Kennung eines Schlüssels, entweder die Schlüsselkennung Ihres primären Schlüsselpaars oder ein beliebiger Teil einer Benutzerkennung, die Ihr Schlüsselpaar identifiziert.

Kapitel 3

Menüreferenz

3.1 Das Menü Datei

Datei → Neues Zertifikat ... (Strg+N)

Erzeugt ein neues Schlüsselpaar (aus öffentlichem und privatem Schlüssel) und ermöglicht das Verschicken des öffentlichen Teils an eine Zertifizierungsinstanz (CA) zur Signierung. Das resultierende Zertifikat wird an Sie zurückgeschickt oder in einem LDAP-Server gespeichert, von wo Sie es in Ihren lokalen Schlüsselspeicher herunterladen können, wo es zum Signieren und Entschlüsseln von Nachrichten dient.

Dieser Betriebsmodus wird „dezentrale Schlüsselerzeugung" genannt, weil alle Schlüssel lokal erzeugt werden. Kleopatra (und GpgSM) unterstützt die „zentrale Schlüsselerzeugung" nicht direkt, aber Sie können das Bündel aus öffentlichem und geheimen Schlüssel, das Sie von der CA im PKCS#12-Format bekommen, mit **Datei → Zertifikate importieren ... (Strg+I)** importieren.

Datei → Zertifikate auf Server suchen ... (Strg+Umschalt+I)

Sucht Zertifikate auf Zertifikatsservern und importiert sie in den lokalen Schlüsselspeicher. Weitere Informationen finden Sie unter Abschnitt 2.2.

Um diese Funktion verwenden zu können, müssen Schlüsselserver eingerichtet sein. Weitere Informationen finden Sie unter Abschnitt 5.1.

Datei → Zertifikate importieren ... (Strg+I)

Importiert Zertifikate und/oder geheime Schlüssel aus Dateien in den lokalen Schlüsselspeicher. Weitere Informationen finden Sie unter Abschnitt 2.2.

Das Format der Zertifikatsdatei muss von GpgSM/GPG unterstützt werden. In den Handbüchern von GpgSM und GPG finden Sie eine Liste der unterstützten Formate.

Datei → Zertifikate exportieren ... (Strg+E)

Exportiert die ausgewählten Zertifikate in eine Datei.

Die ausgewählte Dateierweiterung für den Namen der Exportdatei bestimmt gleichzeitig deren Format:

- Bei OpenPGP-Zertifikaten wird mit der Dateierweiterung `gpg` und `pgp` eine binäre Datei, mit der Erweiterung `asc` eine Datei im ASCII-Format erstellt.
- Bei S/MIME-Zertifikaten wird mit der Dateierweiterung `der` eine binäre Datei, mit der Erweiterung `pem` eine Datei im ASCII-Format erstellt.

Sofern nicht mehrere Zertifikate ausgewählt sind, wird Kleopatra `Fingerabdruck.{asc,pem}` als Namen der Exportdatei vorschlagen.

Diese Funktion steht nur zur Verfügung, wenn ein oder mehrere Zertifikate ausgewählt sind.

> ANMERKUNG
> Diese Funktion exportiert nur die öffentlichen Schlüssel; auch wenn geheime Schlüssel verfügbar sind. Mit **Datei → Geheime Schlüssel exportieren ...** können Sie die geheimen Schlüssel in eine Datei exportieren.

Datei → Geheime Schlüssel exportieren ...

Exportiert den geheimen Schlüssel in eine Datei.

Im Dialog können Sie entscheiden, ob Sie in eine binäre Datei oder eine im ASCII-Format (**ASCII-Mantel**) exportieren möchten. Klicken Sie dann auf das Ordnersymbol rechts neben dem Textfeld **Ausgabedatei** und wählen den Ordner und den Namen für die Exportdatei. Beim Export von geheimen S/MIME-Schlüsseln können Sie zudem den **Zeichensatz der Passphrase** wählen. Hierfür sei auf die Erläuterungen der `--p12-charset Zeichensatz`-Option im Handbuch zu GpgSM verwiesen.

Diese Funktion steht nur zur Verfügung, wenn genau ein Zertifikat ausgewählt ist und der zugehörige geheime Schlüssel verfügbar ist.

> WARNUNG
> Diese Funktion benötigt man nur sehr selten, und wenn das doch einmal der Fall sein sollte, dann sollte dies sorgfältig geplant werden. Zur Planung der Migration eines geheimen Schlüssels gehört neben vielen anderen Dingen die Wahl des Transportmediums und das sichere Löschen der Schlüsseldaten auf dem alten Rechner sowie auf dem Transportmedium.

Datei → Zertifikate zu einem Server exportieren ... (Strg+Umschalt+E)

Exportiert die ausgewählten Zertifikate zu einem Schlüsselserver. Diese Funktion steht nur für OpenPGP zu Verfügung.

Falls eingestellt, wird das Zertifikat auf den für OpenPGP konfigurierten Zertifikatserver hochgeladen (siehe Abschnitt 5.1), anderenfalls auf `keys.gnupg.net`.

Diese Funktion steht nur zur Verfügung, wenn mindestens ein OpenPGP-Zertifikat und kein S/MIME-Zertifikat ausgewählt ist.

> ANMERKUNG
> Wenn ein OpenPGP-Zertifikat bei einem öffentlichen Verzeichnisdienst registriert wurde, kann es in der Regel von dort nicht mehr entfernt werden. Stellen Sie daher vor der Registrierung sicher, dass Sie ein Widerrufszertifikat erstellt haben, sodass Sie das Zertifikat bei Bedarf zurückziehen können.

> ANMERKUNG
> Die meisten öffentlichen OpenPGP-Zertifikatserver werden untereinander abgeglichen, so dass es wenig Sinn macht das Zertifikat zu mehr als einen Server hochzuladen.
> Es mag vorkommen, dass eine Suche nach einem Zertifikat keine Treffer ergibt, auch wenn es gerade erst hochgeladen wurde. Dies erklärt sich dadurch, dass die meisten öffentlichen Schlüsselserver zur Verteilung der Last DNS-Ringverteilung nutzen. Diese Server synchronisieren sich untereinander, jedoch in der Regel nur etwa alle 24 Stunden.

Datei → Dateien entschlüsseln/überprüfen ...

Entschlüsselt Dateien und/oder überprüft Signaturen von Dateien.

Datei → Dateien signieren/verschlüsseln ...

Signiert und/oder verschlüsselt Dateien.

Datei → Schließen (Strg+W)

Schließt Kleopatras Hauptfenster. Es kann jederzeit durch Klicken auf das Symbol in der Kontrollleiste wieder hergestellt werden.

Datei → Beenden (Strg+Q)

Beendet Kleopatra.

3.2 Das Menü Ansicht

Ansicht → Aktualisieren (F5)

Aktualisiert die Zertifikatsliste.
Diese Funktion ist im Normalfall nicht erforderlich, da Kleopatra das Dateisystem überwacht und die Zertifikatsliste bei Bedarf automatisch aktualisiert.

Ansicht → Vorgang abbrechen (Esc)

Bricht alle schwebenden Operationen ab, etwa eine Suche, Anzeige einer Schlüsselliste oder ein Herunterladen.
Diese Funktion steht nur zur Verfügung, wenn mindestens eine Operation ausgeführt wird.

> ANMERKUNG
> Es kann vorkommen, dass diese Funktion nicht in der Lage ist Operationen direkt abzubrechen, wenn überhaupt. Dies ist in Einschränkungen der Treiber begründet.
> Um unter diesen Umständen die Funktionsfähigkeit wiederherzustellen, müssen die Prozesse SCDaemon, DirMngr, GpgSM und GPG (in dieser Reihenfolge) mit den Werkzeugen des Betriebssystems (**top**, Systemüberwachung usw.) gestoppt werden, bis die Blockade der Operation aufgehoben ist.

Ansicht → Zertifikatsdetails

Zeigt die Details des derzeit ausgewählten Zertifikats an.

Diese Funktion steht nur zur Verfügung, wenn genau ein Zertifikat ausgewählt ist.

Diese Funktion kann auch direkt durch Doppelklicken des entsprechenden Eintrags in der Zertifikatsliste aufgerufen werden.

Ansicht → Hierarchische Zertifikatsliste

Schaltet zwischen der hierarchischen und der flachen Anzeige der Zertifikatsliste um.

Im hierarchischen Modus werden die Zertifikate nach Aussteller und Subjekt angeordnet, sodass man einfach sehen kann, zu welcher Zertifikationshierarchie ein bestimmtes Zertifikat gehört; ein bestimmtes Zertifikat kann aber anfangs schwerer zu finden sein (zum Suchen können Sie aber natürlich die Suchleiste verwenden).

In der flachen Ansicht werden alle Zertifikate alphabetisch sortiert in einer flachen Liste angezeigt. In diesem Modus kann man ein bestimmtes Zertifikat leicht finden, aber es ist nicht direkt ersichtlich zu welchem Wurzel-Zertifikat es gehört.

Diese Funktion wechselt zwischen der hierarchischen und flachen Ansicht auf einer Karteikarte, d. h. jede Karteikarte hat ihre eigene hierarchische Ansicht. Dies ermöglicht es zur gleichen Zeit sowohl eine hierarchische und eine flache Ansicht der gleichen Liste griffbereit zu haben.

> ANMERKUNG
> Derzeit steht die hierarchische Ansicht nur für S/MIME-Zertifikate zur Verfügung. Es besteht noch Uneinigkeit unter den Entwicklern, wie die hierarchische Ansicht für OpenPGP-Zertifikate auszusehen hat (also: „Elternelement = Unterzeichner" oder „Elternelement = Unterzeichneter").

Ansicht → Alle aufklappen (Strg+.)

Klappt alle Listeneinträge in der Zertifikatsliste auf, macht also die untergeordneten Einträge sichtbar.

Dies ist die Standardeinstellung, wenn in die hierarchische Ansicht umgeschaltet wird.

Natürlich können Sie auch weiterhin jeden Eintrag einzeln ein- und ausklappen.

Diese Funktion steht nur zur Verfügung, wenn **Ansicht → Hierarchische Zertifikatsliste** aktiviert ist.

Ansicht → Alle einklappen (Strg+,)

Klappt alle Listeneinträge in der Zertifikatsliste ein, macht also alle Einträge außer denen auf der obersten Ebene unsichtbar.
Natürlich können Sie auch weiterhin jeden Eintrag einzeln ein- und ausklappen.

Diese Funktion steht nur zur Verfügung, wenn **Ansicht → Hierarchische Zertifikatsliste** aktiviert ist.

3.3 Das Menü Zertifikate

Zertifikate → Inhaber-Vertrauenswürdigkeit ändern ...

Ändert die Vertrauenswürdigkeit des Inhabers des ausgewählten OpenPGP-Zertifikats.

Diese Funktion steht nur zur Verfügung, wenn genau ein OpenPGP-Zertifikat ausgewählt ist.

Zertifikate → Wurzelzertifikat vertrauen

Markiert dieses (S/MIME-)Wurzelzertifikat als vertrauenswürdig.

Gewissermaßen ist dies gleichbedeutend mit **Zertifikate → Inhaber-Vertrauenswürdigkeit ändern ...** für S/MIME-Wurzelzertifikate. Allerdings können Sie nur zwischen — in OpenPGP-Begriffen gesprochen — „uneingeschränktem" Vertrauen und „niemals vertrauen" wählen.

> ANMERKUNG
> Beim Import eines Wurzelzertifikats wird der Treiber (also GpgAgent) fragen, ob dem importierten Wurzelzertifikat vertraut werden soll. Allerdings muss diese Funktion in den Treibereinstellungen ausdrücklich aktiviert werden (`allow-mark-trusted` in `gpg-agent.conf`, oder entweder **GnuPG System → GPG Agent → Klienten erlauben Schlüssel als ˝vertrauenswürdig˝ zu markieren** oder **S/MIME Validierung → Erlauben, Wurzelzertifikate als vertrauenswürdig zu markieren** in Kapitel 5).
> Diese Funktion in den Treibereinstellungen zu aktivieren kann zu sich öffnenden Fenstern durch PinEntry zu unliebsamen Zeitpunkten führen (z. B. beim Überprüfen von Signaturen) und kann dadurch unbeaufsichtigte E-Mail-Bearbeitung blockieren. Aus diesem Grund und weil es wünschenswert sein kann einem vertrauten Wurzelzertifikat wieder zu *misstrauen*, erlaubt Kleopatra das manuelle Setzen des Vertrauens.

> **WARNUNG**
> Auf Grund von fehlender Treiberunterstützung dieser Funktion ist Kleopatra gezwungen die GpgSM-Vertrauensdatenbank (`trustlist.txt`) direkt zu bearbeiten. Stellen Sie sicher, dass beim Verwenden dieser Funktion keine andere Kryptografieanwendung neben Kleopatra Veränderungen an dieser Datenbank vornimmt.

Diese Funktion steht nur zur Verfügung, wenn genau ein S/MIME-Wurzelzertifikat ausgewählt ist und das Zertifikat noch nicht vertrauenswürdig ist.

Benutzen Sie **Zertifikate → Wurzelzertifikat nicht vertrauen** , um diese Funktion wieder rückgängig zu machen.

Zertifikate → Wurzelzertifikat nicht vertrauen

Markiert dieses (S/MIME-)Wurzelzertifikat als nicht vertrauenswürdig.

Diese Funktion steht nur zur Verfügung, wenn genau ein S/MIME-Wurzelzertifikat ausgewählt ist und das Zertifikat vertrauenswürdig ist.

Diese Funktion wird benutzt, um **Zertifikate → Wurzelzertifikat vertrauen** rückgängig zu machen. Näheres finden Sie in dieser Verknüpfung.

Zertifikate → Zertifikat beglaubigen ...

Ermöglicht es, ein anderes OpenPGP-Zertifikat zu beglaubigen.

Diese Funktion steht nur zur Verfügung, wenn genau ein OpenPGP-Zertifikat ausgewählt ist.

Zertifikate → Ablaufdatum ändern ...

Ermöglicht die Änderung des Ablaufdatums Ihres OpenPGP-Zertifikats.

Benutzen Sie diese Funktion, um die Verfallszeit Ihrer OpenPGP-Zertifikate zu verlängern, als eine Alternative zum Erstellen eines neuen Zertifikats oder eines unbegrenzten Ablaufdatums („verfällt nie").

Diese Funktion steht nur zur Verfügung, wenn genau ein OpenPGP-Zertifikat ausgewählt ist und der zugehörige geheime Schlüssel verfügbar ist.

Zertifikate → Passphrase ändern ...

Ermöglicht die Änderung der Passphrase des geheimes Schlüssels.

Diese Funktion ist nur dann verwendbar, wenn genau ein Zertifikat ausgewählt ist und der geheime Schlüssel für dieses vorhanden ist. Sie erfordert sehr aktuelle Treiber, da in der Implementierung nicht mehr GPG und GpgSM direkt aufgerufen wird, sondern auf eine auf GpgME basierende Lösung umgestiegen wurde.

> **ANMERKUNG**
> Aus Sicherheitsgründen ist die Frage durch PinEntry nach sowohl der alten als auch der neuen Passphrase ein separater Prozess. Abhängig von Ihrem System und der Güte der PinEntry-Implementierung auf Ihrem System kann es passieren, dass das PinEntry-Fenster im Hintergrund erscheint. Wenn Sie also diese Funktion gewählt haben und nichts passiert, überprüfen Sie in der Fensterleiste Ihres Betriebssystems, ob ein PinEntry-Fenster im Hintergrund geöffnet ist.

Zertifikate → Benutzerkennung hinzufügen ...

Erlaubt es Ihrem OpenPGP-Zertifikat eine neue Benutzer-ID hinzuzufügen.

Nutzen Sie diese Funktion, um neue Identitäten einem bestehendem Zertifikat hinzuzufügen, alternativ zum Erstellen eines neuen Schlüsselpaares. Eine OpenPGP-Benutzer-ID hat die folgende Form:

```
Wirklicher Name (Kommentar) <E-Mail>
```

In dem Fenster, das beim Auswählen dieser Funktion erscheint, fragt Kleopatra Sie nach den drei Parametern (*Wirklicher Name*, *Kommentar* und *E-Mail*) getrennt und zeigt das Ergebnis in einer Vorschau an.

> ANMERKUNG
> Diese Parameter unterliegen den selben Administrationsrichtlinie wie bei neuen Zertifikaten. Sehen Sie Abschnitt 2.3 und Abschnitt 6.1 für Details.

Diese Funktion steht nur zur Verfügung, wenn genau ein OpenPGP-Zertifikat ausgewählt ist und der zugehörige geheime Schlüssel verfügbar ist.

Zertifikate → Löschen (Entf)

Löscht die ausgewählten Zertifikate aus dem lokalen Schlüsselspeicher.

Verwenden Sie diese Funktion, um unbenutzte Schlüssel aus Ihrem lokalen Schlüsselspeicher zu entfernen. Weil Zertifikate aber normalerweise an signierte E-Mail-Nachrichten angehängt sind, kann das Überprüfen einer Nachricht dazu führen, dass ein Schlüssel, den Sie gerade entfernt haben, wieder im lokalen Schlüsselspeicher auftaucht. Daher sollte man dies Funktion weitgehend vermeiden. Wenn Sie sich in den Zertifikaten nicht mehr zurechtfinden, verwenden Sie die Suchleiste oder die Funktion **Ansicht → Hierarchische Zertifikatsliste**, um wieder klar zu sehen.

> WARNUNG
> Zum obigen gibt es eine Ausnahme: Wenn Sie eines Ihrer eigenen Zertifikate löschen, entfernen Sie ebenfalls den geheimen Schlüssel. Dies hat zur Folge, dass Sie nicht mehr in der Lage sind ältere Korrespondenzen, die mit diesem Zertifikat verschlüsselt sind, zu lesen sofern Sie nicht irgendwo eine Sicherungskopie Ihres geheimen Schlüssels haben.
> Kleopatra warnt Sie beim Versuch, einen geheimen Schlüssel zu löschen.

Auf Grund der hierarchischen Struktur von S/MIME-Zertifikaten werden beim Löschen eines S/MIME-Ausstellerzertifikates (CA-Zertifikat) auch alle Verwendungen gelöscht.[1]

Natürlich steht diese Funktion steht nur zur Verfügung, wenn mindestens ein Zertifikat ausgewählt ist.

Zertifikate → Zertifikat ausgeben

Zeigt alle Informationen eines ausgewählten (S/MIME-)Zertifikates an, die GpgSM über dieses hat.
Für nähere Details über die Ausgabe sei auf den Abschnitt `--dump-key Schlüssel` des Handbuchs von GpgSM verwiesen.

3.4 Das Menü Extras

Extras → GnuPG-Protokollanzeige ...

Startet KWatchGnuPG, ein Hilfsprogramm, mit dem Sie die Ausgaben des Programms GnuPG verfolgen können. Wenn das Signieren, Verschlüsseln oder Überprüfen auf einmal mysteriöserweise nicht mehr funktioniert, können Sie so möglicherweise den Grund dafür herausfinden.

Da die zugrundeliegenden Mechanismen dieser Funktion unter Windows® nicht implementiert sind, ist sie dort nicht verfügbar.

[1] Das ist wie bei einem Dateisystem. Wenn Sie einen Ordner löschen, dann werden auch alle darin enthaltenen Dateien und Ordner gelöscht.

Extras → OpenPGP-Zertifikate aktualisieren

Aktualisiert alle OpenPGP-Zertifikate durch Ausführung von

```
gpg --refresh-keys
```

. Nach der erfolgreichen Ausführung des Befehls ist der lokale Schlüsselspeicher unter Berücksichtigung der Gültigkeit der OpenPGP-Zertifikate aktualisiert worden.

Beachten sie die Hinweise zu Warnungen in **Extras → X.509-Zertifikate aktualisieren** .

Extras → X.509-Zertifikate aktualisieren

Aktualisiert alle S/MIME-Zertifikate durch Ausführung von

```
gpgsm -k --with-validation --force-crl-refresh --enable-crl-checks
```

. Nach der erfolgreichen Ausführung des Befehls ist der lokale Schlüsselspeicher unter Berücksichtigung der Gültigkeit der S/MIME-Zertifikate aktualisiert worden.

> ANMERKUNG
> Das Aktualisieren von X.509- oder OpenPGP-Zertifikaten beinhaltet das erneute Herunterladen aller Zertifikate und Sperrlisten (CRLs), um zu überprüfen, ob sie in der Zwischenzeit zurückgezogen wurden.
> Dies kann Ihre Netzwerkverbindung stark belasten und kann bis zu einer Stunde oder länger andauern, abhängig von der Geschwindigkeit Ihrer Netzwerkanbindung sowie der Anzahl der zu überprüfenden Zertifikate.

Datei → Sperrliste aus Datei importieren ...

Importiert Sperrlisten (CRL) manuell aus Dateien.

Normalerweise werden Sperrlisten (Zertifikatswiderrufslisten, Certificate Revocation Lists, CRLs) vom Backend transparent verarbeitet, aber manchmal kann es trotzdem nützlich sein, eine CRL manuell in den lokalen CRL-Cache zu importieren.

> ANMERKUNG
> Damit der Import von CRLs funktionieren kann, muss das Hilfsprogramm DirMngr im Suchpfad `PATH` enthalten sein. Wenn dieser Menüeintrag inaktiv ist, dann sollten Sie mit Ihrem Systemverwalter Kontakt aufnehmen und um die Installation von DirMngr bitten.

Extras → Sperrlisten-Zwischenspeicher leeren ...

Leert den Sperrlisten-Zwischenspeicher von GpgSM.

Diese Funktion benötigen Sie wahrscheinlich nie. Sie können das Aktualisieren des Sperrlisten-Zwischenspeichers erzwingen, indem Sie alle Zertifikate auswählen und **Extras → X.509-Zertifikate aktualisieren** aufrufen.

Extras → Sperrlisten-Zwischenspeicher ausgeben ....

Zeigt den genauen Inhalt des Sperrlisten-Zwischenspeichers von GpgSM an.

3.5 Das Menü Einstellungen

Kleopatra hat das bekannten KDE-Menü **Einstellungen** aus den KDE-Grundlagen mit einem zusätzlichen Eintrag:

Einstellungen → Selbsttest durchführen

Führt alle Selbsttests durch und zeigt deren Ergebnisse.

Dies sind die gleichen Tests, die beim Starten ausgeführt werden. Sollten Sie die Selbsttests beim Starten ausgeschaltet haben, können Sie diese hier wieder einschalten.

3.6 Das Menü Fenster

Im Menü **Fenster** können die Unterfenster verwaltet werden. Mit den Einträgen können Unterfenster umbenannt, hinzugefügt, dupliziert, geschlossen und nach rechts oder links verschoben werden.

Wenn Sie mit der rechten Maustaste auf einen Karteireiter klicken, wird ein Kontextmenü mit denselben Aktion geöffnet.

3.7 Das Menü Hilfe

Kleopatra hat das bekannten KDE-Menü **Hilfe** das in den KDE-Grundlagen erläutert wird.

Kapitel 4

Referenz der Befehlszeilenoptionen

Hier werden nur die Kleopatra-spezifischen Optionen aufgezählt. Wie bei allen KDE-Applikationen können Sie durch Aufrufen von **`kleopatra --help`** eine vollständige Liste aller Optionen bekommen.

`--uiserver-socket` ***`argument`***
: Adresse der Socket-Datei, an der der Benutzerschnittstellen-Server auf Befehle wartet

`--daemon`
: Nur Benutzerschnittstellen-Server starten, Hauptfenster nicht anzeigen

`-p --openpgp`
: Für die folgende Operation OpenPGP verwenden

`-c --cms`
: Für die folgende Operation CMS (X.509, S/MIME) verwenden

`-i --import-certificate`
: Gibt eine Datei oder URL an, aus der Zertifikate (oder geheime Schlüssel) importiert werden sollen.
Dies ist das Befehlszeilen-Gegenstück zu **Datei → Zertifikate importieren ... (Strg+I)** .

`-e --encrypt`
: Datei(en) verschlüsseln

`-s --sign`
: Datei(en) unterschreiben

`-E --encrypt-sign`
: Verschlüsseln und/oder Signieren von Datei(en). Analog zu `--sign-encrypt`, nicht benutzen

`-d --decrypt`
: Datei(en) entschlüsseln

`-V --verify`
: Datei/Signatur überprüfen

`-D --decrypt-verify`
: Dateien entschlüsseln/überprüfen

Kapitel 5

Kleopatra einrichten

Den Einrichtungsdialog von Kleopatra öffnen Sie mit **Einstellungen** → **Kleopatra einrichten ...**.

Sämtliche Seiten dieses Dialogs werden in den folgenden Abschnitten beschrieben.

5.1 Einrichtung von Zertifikatsservern

Auf dieser Seite können Sie einstellen welche LDAP-Server für die Suche nach S/MIME-Zertifikaten genutzt werden sollen und welche Schlüsselserver für die Suche nach OpenPGP-Zertifikaten.

> ANMERKUNG
> Dies ist eine benutzerfreundlichere Version der gleichen Einstellungen, wie sie unter Abschnitt 5.5 zu finden sind. Alles, was Sie hier einstellen können, ist auch dort möglich.

> EIN HINWEIS ZU DEN PROXY-EINSTELLUNGEN
> Die Proxy-Einstellungen für HTTP und LDAP können in Abschnitt 5.4 eingestellt werden, allerdings nur für GpgSM. Auf Grund der Komplexität der GPG-Schlüsselserveroptionen und fehlender Unterstützung dieser in GpgConf müssen Sie die Proxyeinstellungen für GPG in der Konfigurationsdatei `gpg.conf` selbst vornehmen. Bitte sehen Sie im Handbuch von GPG für Details hierüber nach. Kleopatra wird die dort vorgenommenen Einstellungen beibehalten aber erlaubt es noch nicht diese in der GUI zu ändern.

Die **Verzeichnisdienste**-Tabelle zeigt an, welche Server derzeit eingerichtet sind. Mit einem Doppelklick in eine Zelle lassen sich die Parameter bestehender Einträge bearbeiten.

Die Spalten in dieser Tabelle bedeuten:

Protokoll

Bestimmt das Netzwerkprotokoll, welches benutzt wird, um den Server zu erreichen. Häufig genutzte Schemata sind **ldap** (und das SSL-gesicherte Pendant **ldaps**) für LDAP-Server (übliches Protokoll für S/MIME; das einzige von GpgSM unterstütze), und **hkp**, das Horowitz Keyserver Protocol („Horowitz-Schlüsselserver-Protokoll“), heute in der Regel HTTP-Schlüsselserver-Protokoll, einem auf HTTP basierendem Protokoll das wirklich alle öffentlichen OpenPGP-Schlüsselserver unterstützen.

In den Handbüchern von GPG und GpgSM finden Sie eine Liste der unterstützten Formate.

Servername
: Der Domain-Name des Servers, z. B. `keys.gnupg.net`.

Server-Port
: Der Netzwerk-Port, auf dem der Server auf Anfragen wartet.

  Dieser ändert sich automatisch zum Standard-Port, wenn Sie das **Protokoll** ändern — sofern es anfangs kein Standard-Port war. Sollten Sie den Standard-Port verändert haben und schaffen es nicht mehr, die Standardwerte einzustellen, versuchen Sie **Protokoll** auf **`http`** und **Server-Port** auf **`80`** (Standard für HTTP) zu setzen und fahren von dort fort.

Basis-DN
: Die Basis-DN (nur für LDAP und LDAPS), d. h. die Wurzel der LDAP-Hierarchie, von der aus gestartet werden soll. Oft wird dies auch als „Such-Wurzel" oder „Such-Basis" bezeichnet.
  In der Regel sieht dies aus wie **`c=de,o=Foo`** und ist Teil der LDAP-URL.

Benutzername
: Der Benutzername, wenn vorhanden, der für die Anmeldung am Server genutzt wird.

  Diese Spalte wird nur angezeigt, wenn **Benutzername und Passwort anzeigen** unter der Tabelle ausgewählt ist.

Passwort
: Das Passwort, wenn vorhanden, das für die Anmeldung am Server genutzt wird.

  Diese Spalte wird nur angezeigt, wenn **Benutzername und Passwort anzeigen** unter der Tabelle ausgewählt ist.

X.509
: Markieren Sie diese Spalte, wenn dieser Eintrag für die Suche nach X.509-Zertifikaten (S/-MIME) genutzt werden soll.

  Es werden nur LDAP- und LDAPS-Server für S/MIME unterstützt.

OpenPGP
: Markieren Sie diese Spalte, wenn dieser Eintrag für die Suche nach OpenPGP-Zertifikaten genutzt werden soll.

Sie können so viele S/MIME-Server (X.509) einrichten, wie Sie wollen. Jedoch ist nur ein OpenPGP-Server erlaubt. Die GUI stellt dies sicher.

Um einen neuen Server hinzuzufügen, klicken Sie auf den Knopf **Neu**. Ist ein bestehender Eintrag ausgewählt, wird dieser dupliziert. Anderenfalls wird ein Standard-OpenPGP-Server eingefügt. Anschließend können Sie den **Servername**, den **Server-Port**, die **Basis-DN**, sowie das übliche **Passwort** und **Benutzername** einstellen. Letztere beiden werden benötigt, wenn der Server eine Authentifizierung erfordert.

Um einen neuen Eintrag für X.509-Zertifikate einzufügen, nutzen Sie **Neu** → **X.509**. Für OpenPGP nutzen Sie analog **Neu** → **OpenPGP**.

Um einen Server aus der Suchliste zu entfernen, wählen Sie ihn in der Liste aus und betätigen dann den Knopf **Löschen**.

Mit dem Eingabefeld **LDAP-Zeitüberschreitung (Minuten:Sekunden)** können Sie die LDAP-Zeitüberschreitung einstellen, also die maximale Zeit, die das Hintergrundprogramm auf die Antwort eines Servers warten soll.

Wenn einer Ihrer Server eine so große Datenbank enthält, dass selbst sinnvolle Suchanfragen wie **`Schmidt`** die **Maximale Anzahl Treffer bei Anfragen** überschreiten, dann können Sie diese Begrenzung heraufsetzen. Sie können leicht feststellen, wenn das der Fall ist, weil ein Dialog erscheinen wird, der Ihnen mitteilt, dass die Suchergebnisse verkürzt worden sind.

> ANMERKUNG
> Einige Server haben eigene Beschränkungen, wieviele Einträge sie in einer Abfrage zurückgeben. In diesem Fall führt das Heraufsetzen der Begrenzung in diesem Dialog natürlich zu keiner Änderung.

5.2 Erscheinungsbild einrichten

5.2.1 Kurzinfos einrichten

In der Hauptliste der Zertifikate kann Kleopatra Details eines Zertifikats als Kurzinfos anzeigen. Die angezeigten Informationen sind die selben wie in der Karteikarte **Übersicht** des Fensters **Zertifikatsdetails**. Allerdings können Kurzinfos nur einige Informationen anzeigen.

> ANMERKUNG
> Die **Schlüssel-ID** wird *immer* angezeigt. Dies stellt sicher, dass die Kurzinfos unterschiedlicher Zertifikate sich voneinander unterschieden (dies ist besonders dann wichtig, wenn nur **Gültigkeit anzeigen** ausgewählt wurde).

Sie können unabhängig voneinander die folgenden Informationen ein- oder ausschalten:

Gültigkeit anzeigen

Zeigt Informationen über die Gültigkeit eines Zertifikats an: seinen derzeitigen Status, Aussteller-DN (nur bei S/MIME), Verfallsdatum (wenn vorhanden) und Markierung zur Nutzung des Zertifikats.

Beispiel:

```
Dieses Zertifikat ist derzeit gültig.
Ausgestellt durch:            CN=Test-ZS7,O=Intevation GmbH,C=DE
Gültigkeit:                   von 25.08.2009 10:42 bis 19.10.2010 10:42
Verwendung des Zertifikats:   Signieren von E-Mails und Dateien, ↩
    Verschlüsseln von E-Mails und Dateien
Schlüssel-Kennung:            DC9D9E43
```

Inhaber-Informationen anzeigen

Zeigt Informationen über den Besitzer des Zertifikats: Verwendungs-DN (nur bei S/MIME), Benutzer-ID (einschließlich E-Mail-Adressen) und Besitzervertrauen (nur bei OpenPGP).

Beispiel für OpenPGP:

```
Benutzer-ID:           Gpg4winUserA <gpg4winusera@test.hq>
Schlüssel-Kennung:     C6BF6664
Eigentümer-Vertrauen:  vollständiges Vertrauen
```

Beispiel für S/MIME:

```
Verwendung:         CN=Gpg4winTestuserA,OU=Testlab,O=Gpg4win Project,C= ↩
    DE
Auch bekannt als:   Gpg4winUserA@test.hq
Schlüssel-Kennung:  DC9D9E43
```

Technische Details anzeigen

Zeigt technische Informationen über das Zertifikat an: Seriennummer (nur bei S/MIME), Typ, Fingerabdruck und Speicherort.

Beispiel:

```
Seriennummer:        27
Zertifikatstyp:      1,024-bit RSA (geheimer Schlüssel vorhanden)
Schlüssel-Kennung:   DC9D9E43
Fingerabdruck:       854F62EEEBB41BFDD3BE05D124971E09DC9D9E43
Gespeichert:         auf diesem Rechner
```

5.2.2 Zertifikats-Kategorien einrichten

Sie können in Kleopatra die Darstellung der Schlüssel in der Schlüsselliste einstellen. Dazu gehören die Anzeige kleiner Symbole aber auch die Vordergrund- (Text-) und Hintergrundfarbe sowie der Zeichensatz.

Jeder Schlüsselkategorie in der Liste ist ein Satz von Farben, ein optionales Symbol und ein Zeichensatz zugeordnet, in denen die Schlüssel, die zu dieser Kategorie gehören, dargestellt werden. Die Kategorieliste dient auch als Vorschau für die Einstellungen. Der Systemverwalter oder erfahrene Benutzer können die Kategorien frei definieren; siehe dazu Abschnitt 6.2 in Kapitel 6.

Um das Symbol einer Kategorie zu ändern, wählen Sie die Kategorie in der Liste aus und klicken auf **Symbol einstellen...**. Der Standard-Symboldialog von KDE erscheint, in dem Sie ein Symbol aus der KDE-Sammlung auswählen oder ein eigenes einstellen können.

Um ein Symbol wieder zu löschen, verwenden Sie die Schaltfläche **Voreingestelltes Erscheinungsbild**.

Um die Textfarbe, d. h. den Vordergrund einer Kategorie zu ändern, wählen Sie die Kategorie in der Liste aus und klicken auf **Textfarbe einstellen ...** Der Standard-Farbdialog von KDE erscheint, indem Sie eine Farbe auswählen oder eine neue erstellen können.

Die Hintergrundfarbe wird auf die gleiche Weise geändert, verwenden Sie hier die Schaltfläche **Hintergrundfarbe einstellen ...**.

Sie haben zwei Möglichkeiten, den Zeichensatz einzustellen:

1. Verändern Sie den Standard-Zeichensatz, der für alle Listenanzeigen in KDE verwendet wird.
2. Verwenden Sie einen benutzerdefinierten Zeichensatz.

Die erste Option hat den Vorteil, dass der Zeichensatz Ihren KDE-weiten Stileinstellungen folgen wird, während Sie bei der letzteren Möglichkeit die volle Kontrolle über den zu verwendenden Zeichensatz haben. Die Wahl liegt bei Ihnen.

Um den Standard-Zeichensatz zu verändern, wählen Sie die Kategorie in der Liste und ändern Sie die Modifikatoren **Kursiv**, **Fett** und/oder **Durchgestrichen**. Sie können den Effekt auf den Zeichensatz in der Kategorienliste unmittelbar sehen.

Um einen benutzerdefinierten Zeichensatz einzustellen, klicken Sie auf die Schaltfläche **Zeichensatz einstellen ...**. Der Standard-Zeichensatzdialog von KDE erscheint, in dem Sie den neuen Zeichensatz einstellen können.

> ANMERKUNG
> Beachten Sie, dass Sie die Zeichensatz-Modifikatoren weiterhin für den eigenen Zeichensatz verwenden können; genau wie beim Verändern des Standard-Zeichensatz.

Um auf den Standard-Zeichensatz zurückzuschalten, verwenden Sie die Schaltfläche **Voreingestelltes Erscheinungsbild**.

5.2.3 Die DN-Attributreihenfolge einstellen

DNs sind zwar hierarchisch, aber die Reihenfolge der einzelnen Komponenten (auch relative DNs (RDNs) oder DN-Attribute genannt) ist nicht definiert. Die Reihenfolge, in der die Attribute angezeigt werden, ist daher eine Frage des persönlichen Geschmacks oder von Firmenvorgaben, weswegen Sie diese Reihenfolge in Kleopatra konfigurieren können.

> ANMERKUNG
> Diese Einstellung gilt nicht nur für Kleopatra, sondern für alle Anwendungen, die Kleopatra-Technologie verwenden. Dazu gehören derzeit KMail, KAddressBook und natürlich Kleopatra selbst.

Diese Konfigurationsseite besteht im wesentlichen aus zwei Listen, eine für die bekannten Attribute (**Verfügbare Attribute**) und eine, die die **Aktuelle Attributreihenfolge** beschreibt.

Beide Listen enthalten Einträge, die sowohl durch die Kurzform des Attributs (z. B. **CN**) als auch durch die ausgeschriebene Form (**Allgemeiner Name**) beschrieben werden.

Die Einträge in der Liste **Verfügbare Attribute** sind immer alphabetisch sortiert, während die Reihenfolge in der Liste **Aktuelle Attributreihenfolge** die eingestellte Reihenfolge der DN-Attribute widerspiegelt; das erste Attribut in dieser Liste wird auch als erstes angezeigt.

Nur Attribute, die explizit in der Liste **Aktuelle Attributreihenfolge:** aufgeführt sind, werden überhaupt angezeigt. Der Rest ist in der Voreinstellung ausgeblendet.

Wenn aber der Platzhalter **_X_** (**Alle anderen**) in der „aktuellen" Liste steht, dann werden alle nicht aufgeführten Attribute (ob bekannt oder nicht) an der Position des **_X_** in ihrer ursprünglichen relativen Reihenfolge eingefügt.

Ein kleines Beispiel soll dies deutlicher machen:

Im DN

> O=KDE, C=US, CN=Dave Devel, X-BAR=foo, OU=Kleopatra, X-FOO=bar,

die Standardreihenfolge der Attribute „CN, L, _X_, OU, O, C" ergibt folgenden formatierten DN.

> CN=Dave Devel, X-BAR=foo, X-FOO=bar, OU=Kleopatra, O=KDE, C=US

„CN, L, OU, O, C" dagegen ergibt

> CN=Dave Devel, OU=Kleopatra, O=KDE, C=US

Um ein Attribut zur Anzeigeliste hinzuzufügen, wählen Sie es in der Liste der verfügbaren Attribute aus und klicken auf die Schaltfläche **Zur aktuellen Attributreihenfolge hinzufügen**.

Um ein Attribut aus der Anzeigeliste zu entfernen, wählen Sie es in dieser aus und klicken auf die Schaltfläche **Von der aktuellen Attributreihenfolge entfernen**.

Um ein Attribut an den Anfang oder das Ende zu verschieben, wählen Sie es in der Liste **Aktuelle Attributreihenfolge** aus und klicken auf eine der Schaltflächen **Nach ganz oben** oder **Nach ganz unten**.

Um ein Attribut um eine Position nach oben oder unten zu verschieben, wählen Sie es in der Anzeigeliste aus und klicken auf eine der Schaltflächen **Nach oben** oder **Nach unten**.

5.3 Kryptografie-Aktionen einrichten

5.3.1 E-Mail-Aktionen einrichten

Hier können Sie einige Dinge der E-Mail-Operationen des Kleopatra-UiServers einstellen. Derzeit lässt sich nur einstellen, ob Sie den „Schnell-Modus" für das Signieren und Verschlüsseln von E-Mails nutzen wollen.

Wenn der „Schnell-Modus" aktiviert ist, werden zum Signieren (Verschlüsseln) von E-Mails keine Dialoge erscheinen, solange keine Konflikte auftreten, die eine manuelle Auflösung erfordern.

5.3.2 Datei-Aktionen einrichten

Hier lassen sich einige Dinge der Datei-Operation des Kleopatra-UiServers einstellen. Derzeit können Sie nur das Programm zum Erstellen der Prüfsummen durch **CHECKSUM_CREATE_FILES** festlegen.

Verwenden Sie **Prüfsummen-Programm**, um festzulegen, welches der eingestellten Prüfsummen-Programme für das Erstellen von Prüfsummendateien verwendet werden soll.

Zum Verifizieren wird das erforderliche Prüfsummen-Programm automatisch aus den Namen der Prüfsummen-Datei ermittelt.

> ANMERKUNG
> Systemverwalter und erfahrene Benutzer können die Prüfsummen-Programme, die Kleopatra zur Verfügung stehen sollen, völlig frei in den sogenannten „Checksum Definitions" der Einrichtungsdatei definieren. Für Details sei auf Abschnitt 6.4 in Kapitel 6 verwiesen.

5.4 S/MIME-Prüfung einrichten

Auf dieser Seite können Sie einige Aspekte der Validierung von S/MIME-Zertifikaten einstellen.

> ANMERKUNG
> In der Regel ist dies eine einfachere und benutzerfreundlichere Version der gleichen Einstellungen, wie sie unter Abschnitt 5.5 zu finden sind. Alles, was Sie hier einstellen können, ist auch dort möglich. Einzige Ausnahme bildet **Zertifikatsgültigkeit überprüfen alle *N* Stunden**, welches spezifisch für Kleopatra ist.

Diese Optionen haben folgende Bedeutung:

5.4.1 Einstellen des Intervalls zur Zertifikatüberprüfung

Zertifikatsgültigkeit überprüfen alle *N* Stunden

Diese Option aktiviert regelmäßiges Überprüfen der Zertifikatgültigkeit. Sie können außerdem das Intervall in Stunden wählen. Der Effekt der hier eingestellten regelmäßigen Überprüfung ist der gleiche wie der von **Ansicht** → **Aktualisieren (F5)** . Es gibt keine Vorbedingungen für die Intervallplanung von **Extras** → **OpenPGP-Zertifikate aktualisieren** oder **Extras** → **X.509-Zertifikate aktualisieren** .

> ANMERKUNG
> Die Überprüfung wird vorbehaltlos immer dann ausgeführt, wenn wichtige Dateien in `~/.gnupg` verändert werden. Diese Option, wie auch **Extras** → **OpenPGP-Zertifikate aktualisieren** und **Extras** → **X.509-Zertifikate aktualisieren** , betrifft daher nur äußere Faktoren der Zertifikatgültigkeit.

5.4.2 Einstellung der Überprüfungsmethode

Zertifikate unter Verwendung von Sperrlisten prüfen

Falls diese Einstellung aktiviert ist, werden S/MIME-Zertifikate mit Hilfe von Zertifikatsperrlisten (CRLs) überprüft.

Siehe **Zertifikate online überprüfen (OCSP)** für eine alternative Methode zur Überprüfung der Zertifikatgültigkeit.

Zertifikate online überprüfen (OCSP)

Wenn diese Einstellung ausgewählt ist, werden S/MIME-Zertifikate mittels des Online Certificates Status Protocol (OCSP) überprüft.

> WARNUNG
> Wenn diese Methode gewählt ist, wird eine Anfrage an den Server des CA eigentlich immer dann gestellt, wenn Sie eine verschlüsselte Nachricht empfangen oder senden. Daher ist es dem Zertifikataussteller theoretisch möglich nachzuverfolgen mit wem Sie (z. B.) E-Mails austauschen.

Um diese Methode nutzen zu können müssen Sie die URL des OCSP-Antwortservers in **Adresse der OCSP-Gegenstelle** eingeben.

Sehen Sie **Zertifikate online überprüfen (OCSP)** für eine traditionellere Methode zur Überprüfung der Zertifikatgültigkeit, die keine Informationen darüber verrät, mit wem sie Nachrichten austauschen.

Adresse der OCSP-Gegenstelle

Geben Sie hier die Adresse des Servers für die Online-Überprüfung von Zertifikaten ein (OCSP-Antwortserver). Die Adresse (URL) beginnt üblicherweise mit `http://` .

Signatur der OCSP-Gegenstelle

Wählen Sie hier das Zertifikat mit dem der OCSP-Server seine Antworten signiert.

Dienst-Adresse in Zertifikaten ignorieren

Normalerweise enthält jedes S/MIME-Zertifikat die URL des OCSP-Antwortservers des zugehörigen Ausstellers (**Zertifikate → Zertifikat ausgeben** gibt aus, ob ein bestimmtes Zertifikat diese enthält).

Auswählen dieser Option lässt GpgSM diese URLs ignorieren und nutzt nur die oben eingestellten.

Benutzen Sie dies um z. B. die Verwendung eines firmenweiten OCSP-Proxys zu erzwingen.

5.4.3 Überprüfungseinstellungen einrichten

Zertifikats-Richtlinien nicht überprüfen

Standardmäßig verwendet GpgSM die Datei `~/.gnupg/policies.txt` zur Überprüfung, ob ein bestimmter Umgang mit einem Zertifikat erlaubt ist. Falls diese Einstellung aktiviert ist, wird die Überprüfung nicht durchgeführt.

Nie Sperrlisten zu Rate ziehen

Wenn diese Option ausgewählt ist, werden Zertifikat-Widerrufslisten (Certificate Revocation Lists, CRLs) nie zur Überprüfung von S/MIME-Zertifikaten verwendet.

Das Markieren von Wurzelzertifikaten als vertrauenswürdig zulassen

Falls diese Einstellung beim Importieren eines Wurzel-CA-Zertifikates aktiviert ist, werden Sie um Bestätigung des Fingerabdrucks und des Status gebeten, egal ob Sie dem Zertifikat vertrauen oder nicht.
Sie müssen einem Wurzelzertifikat vertrauen, damit die damit signierten Zertifikate ebenfalls vertrauenswürdig werden können. Durch leichtfertiges Importieren und Vertrauen von Wurzelzertifikaten können Sie die Sicherheit des gesamten Systems gefährden.

> ANMERKUNG
> Diese Funktion in den Treibereinstellungen zu aktivieren kann zu sich öffnenden Fenstern durch PinEntry zu unliebsamen Zeitpunkten führen (z. B. beim Überprüfen von Signaturen) und kann dadurch unbeaufsichtigte E-Mail-Bearbeitung blockieren. Aus diesem Grund und weil es wünschenswert sein kann einem vertrauten Wurzelzertifikat wieder zu *misstrauen*, erlaubt Kleopatra das manuelle Setzen des Vertrauens mit Hilfe von **Zertifikate → Wurzelzertifikat vertrauen** und **Zertifikate → Wurzelzertifikat nicht vertrauen** .
> Diese Einstellung hier beeinträchtigt die Kleopatra-Funktion nicht.

Fehlende Aussteller-Zertifikatsketten einholen

Falls diese Einstellung aktiviert ist, werden fehlende Ausstellerzertifikate heruntergeladen (das gilt für beide Überprüfungsmethoden, CRLs und OCSP).

5.4.4 Einrichten der Optionen für HTTP-Anfragen

Keine HTTP-Anfragen durchführen

Schaltet die Verwendung von HTTP für S/MIME gänzlich ab.

HTTP-Quellen für Sperrlisten von Zertifikaten ignorieren

Für die Suche der Adresse einer Sperrliste (CRL) enthält das fragliche Zertifikat häufig die Angabe eines CRL-Verteilers („Distribution Point": DP), der die Angabe von Adressen (URLs) zur Beschreibung des Zugriffs auf die CRL enthält. Der erste DP-Eintrag wird verwendet.
Bei dieser Einstellung werden alle Einträge, die das LDAP-Schema verwenden, bei der Suche nach einem passenden DP-Eintrag ignoriert.

Systemweiten HTTP-Proxy-Server verwenden

Falls diese Einstellung aktiviert ist, wird der rechts angezeigte HTTP-Proxyserver (die Einstellung stammt aus der Umgebungsvariable `http_proxy`) für alle HTTP-Anfragen verwendet.

Diesen Proxy für HTTP-Anfragen verwenden

Sollte kein systemweiter Proxy vorgegeben sein oder Sie einen anderen Proxy für GpgSM nutzen wollen, können Sie diesen hier angeben.

Dieser wird für alle HTTP-Anfragen, die S/MIME betreffen, genutzt.

Als Syntax wird **`Host:Port`**, z. B. **`meinproxy.nirgendwo.de:3128`** benutzt.

5.4.5 Einrichten der Optionen für LDAP-Anfragen

Keine Verzeichnisdienstanfragen durchführen

Die Verwendung von LDAP für S/MIME gänzlich abschalten.

Verzeichnisdienst-Quellen für Sperrlisten von Zertifikaten ignorieren

Für die Suche der Adresse einer Sperrliste (CRL) enthält das fragliche Zertifikat häufig die Angabe eines CRL-Verteilers („Distribution Point": DP), der die Angabe von Adressen (URLs) zur Beschreibung des Zugriffs auf die CRL enthält. Der erste DP-Eintrag wird verwendet.

Bei dieser Einstellung werden alle Einträge, die das LDAP-Schema verwenden, bei der Suche nach einem passenden DP-Eintrag ignoriert.

Primäre Adresse für Anfragen an den Verzeichnisdienst:

Ist hier ein LDAP-Server angegeben, werden alle LDAP-Anfragen zuerst zu diesem Server gesendet. Genauer gesagt überschreibt diese Einstellung hier sämtliche *Host*- und *Port*-Teile in einer LDAP-URL und wird auch dann genutzt wenn *Host* und *Port* in der URL nicht auftauchen.

Andere LDAP-Server werden nur dann genutzt, wenn die Verbindung „Proxy" nicht aufgebaut werden konnte. Die Syntax hierfür ist **Host** oder **Host:Port**. Ist *Port* ausgelassen, wird Port 389 (der Standard-Port für LDAP) genutzt.

5.5 Einrichtung des GnuPG-Systems

Dieser Teil des Fensters wird automatisch aus den Ausgaben von **gpgconf --list-option *Komponente*** generiert, wobei dieser für jede von **gpgconf --list-components** zurückgegebener *Komponente* ausgeführt wird.

> ANMERKUNG
> Die nützlichsten dieser Optionen wurden als eigenständige Seiten im Einstellungsdialog von Kleopatra dupliziert. Sehen Sie Abschnitt 5.1 und Abschnitt 5.4, um mehr über diese beiden Seiten und die in diesem Teil dieses Fensters enthaltenen Optionen zu erfahren.

Der genaue Inhalt dieses Teils des Fensters hängt von der Version des GnuPG-Treibers ab, den Sie installiert haben. Zudem vermutlich ebenfalls vom Betriebssystem, das Sie nutzen. Daher wird hier nur der allgemeine Aufbau des Fensters einschließlich der Abbildung der GpgConf-Optionen auf die GUI-Bedienelemente von Kleopatra erläutert.

GpgConf gibt Informationen über die Einstellungen zahlreicher Optionen. Innerhalb jeder Komponente sind individuelle Optionen zu Gruppen zusammengestellt.

Kleopatra zeigt eine Registerkarte pro von GpgConf zurückgegebener Komponente. Gruppen sind durch horizontale Linien und den Namen der Gruppe, so wie der von GpgConf zurückgegeben wird, voneinander getrennt.

Jede GpgConf-Option hat einen Typen. Mit Ausnahme einiger gut bekannter Optionen, die Kleopatra mit besonderen Bedienelementen für eine bessere Benutzbarkeit gesondert handhabt, ist die Abbildung der GpgConf-Typen auf die GUI-Bedienelemente wie folgt:

GpgConf-Typ	Kleopatra-Bedienelement	
	für Listen	für nicht-Listen
`none`	Drehfeld (bezogen auf eine „Anzahl")	Ankreuzfeld
`string`	N/A	Eingabefeld
`int32`	Eingabefeld (unformatiert)	Drehfeld
`uint32`		
`pathname`	N/A	spezialisiertes Bedienelement

`ldap server`	spezialisiertes Bedienelement	N/A
`key fingerprint`	N/A	
`pub key`		
`sec key`		
`alias list`		

Tabelle 5.1: Abbilden der GpgConf-Typen auf die GUI-Bedienelemente

Im Handbuch von GpgConf finden Sie weitere Informationen über die Einstellungsmöglichkeiten.

Kapitel 6

Handbuch für den Systemverwalter

Dieses Handbuch für den Systemverwalter beschreibt Möglichkeiten, Kleopatra zu konfigurieren, die nicht über die grafische Benutzerschnittstelle, sondern nur über Konfigurationsdateien erreichbar sind.

Wir gehen hier davon aus, dass der Leser mit der Technologie zum Konfigurieren von KDE-Applikationen vertraut ist. Dazu gehören das Format, die Lage im Dateisystem und das Kaskadieren von KDE-Konfigurationsdateien, sowie das KIOSK-System.

6.1 Anpassung des Assistenten zum Erzeugen von Zertifikaten

6.1.1 Anpassung der DN-Felder

Sie können in Kleopatra die Felder anpassen, die der Benutzer ausfüllen muss, um ein Zertifikat zu erzeugen.

Legen Sie eine Gruppe namens `CertificateCreationWizard` in der systemweiten `kleopatrarc`-Datei an. Wenn Sie die Reihenfolge der Attribute verändern wollen, oder nur bestimmte Elemente anzeigen wollen, dann definieren Sie einen Schlüssel namens `DNAttributeOrder`. Das Argument besteht aus einem oder mehreren der Elementen `CN`,`SN`,`GN`,`L`,`T`,`OU`,`O`,`PC`,`C`,`SP`,`DC`,`BC`,`EMAIL`. Wenn Sie Felder mit einem bestimmten Wert initialisieren wollen, dann schreiben Sie Attribut=Wert. Wenn das Attribut obligatorisch sein soll, dann fügen Sie ihm ein Ausrufungszeichen an (wie in `CN!`,`L`,`OU`,`O!`,`C!`,`EMAIL!`, der Standardeinstellung).

Mit dem KIOSK-Modus-Modifikator `$e` können Sie Werte aus Umgebungsvariablen oder einem ausgewerteten Skript oder Binärprogramm verwenden. Wenn Sie außerdem noch das Editieren des entsprechenden Feldes verhindern wollen, verwenden Sie den Modifikator `$i`. Wenn Sie die Benutzung der Schaltfläche **Meine Adresse einfügen** verbieten wollen, dann setzen Sie `ShowSetWhoAmI` auf false.

> TIP
> Aufgrund der Funktionsweise des KIOSK-Systems von KDE, ist es für den Benutzer unmöglich, den Schalter `$i` zu überschreiben. Das ist das beabsichtigte Verhalten. `$i` und `$e` können auch bei allen anderen Konfigurationsschlüsseln in KDE-Applikationen verwendet werden.

Das folgende Beispiel zeigt mögliche Anpassungen:

```
[CertificateCreationWizard]
;Persönliche Daten dürfen nicht aus dem Adressbuch kopiert werden;
;lokales Überschreiben ist verboten
```

```
ShowSetWhoAmI[$i]=false

;Benutzername mit $USER vordefinieren
CN[$e]=$USER

;Firmenname mit "Meine Firma" vordefinieren; editieren verbieten
O[$i]=Meine Firma

;Den Abteilungsnamen mit dem Rückgabewert eines Skripts vordefinieren
OU[$ei]=$(lookup_dept_from_ip)

; das Land mit DE vordefinieren, aber Änderungen durch den Benutzer ↩
    zulassen
C=DE
```

6.1.2 Beschränkung der Schlüsselarten, die ein Benutzer erzeugen darf

In Kleopatra kann auch die Art der Zertifikate beschränkt werden, die ein Benutzer erzeugen darf. Beachten Sie aber, das diese Einschränkungen leicht umgangen werden können, indem das Zertifikat in einer Konsole auf der Befehlszeile generiert wird.

6.1.2.1 Algorithmen für öffentliche Schlüssel

Um den verwendeten Algorithmus für öffentliche Schlüssel zu beschränken, fügen Sie den Einrichtungsschlüssel `PGPKeyType` und `CMSKeyType` (für CMS-Typen wird nur RSA unterstützt) zum Abschnitt `CertificateCreationWizard` in der Datei `kleopatrarc` ein.

Die erlaubten Werte sind `RSA` für RSA-Schlüssel, `DSA` für DSA-Schlüssel (nur zur Signierung) und `DSA+ELG` für einen DSA-Schlüssel (nur zur Signierung) mit einem Elgamal-Unterschlüssel zum Verschlüsseln.

Der Standardwert wird aus der Datei GpgConf eingelesen. Ist hier kein Standard eingetragen, wird `RSA` verwendet.

6.1.2.2 Größe des öffentlichen Schlüssels

Um die mögliche Schlüsselgröße für einen öffentlichen Algorithmus zu beschränken, fügen Sie den Einrichtungsschlüssel `<ALG>KeySizes` (erlaubte Werte für *ALG* `RSA`, `DSA` oder `ELG`) zum Abschnitt `CertificateCreationWizard` der Datei `kleopatrarc` ein. Tragen Sie als Wert eine durch Kommata getrennte Liste von Schlüsselgrößen in Bit ein. Der Standardwert wird durch das Voranstellen eines Bindestrichs (`-`) gekennzeichnet.

```
RSAKeySizes = 1536,-2048,3072
```

In diesem Beispiel sind nur RSA-Schlüsselgrößen von 1536, 2048 und 3072 Bit erlaubt, der Standardwert ist 2048 Bit.

Zusätzlich zur Größe selbst können Sie auch Marken für jede Größe bestimmen. Geben Sie dazu für den Einrichtungsschlüssel `ALGKeySizeLabels` ein durch Kommata getrennte Liste von Marken ein.

```
RSAKeySizeLabels = weak,normal,strong
```

Zusammen ergeben die beiden oben genannten Beispiele die folgende Möglichkeit zur Auswahl:

```
weak (1536 bits)
              normal (2048 bits)
              strong (3072 bits)
```

Die Standardwerte entsprechen der folgenden Vorgabe:

```
RSAKeySizes = 1536,-2048,3072,4096
              RSAKeySizeLabels =
              DSAKeySizes = -1024,2048
              DSAKeySizeLabels = v1,v2
              ELGKeySizes = 1536,-2048,3072,4096
```

6.2 Schlüsselkategorien erzeugen und editieren

Sie können in Kleopatra das Aussehen von Schlüsseln auf der Basis eines Konzepts namens **Schlüsselkategorien** verändern. **Schlüsselkategorien** werden auch benutzt, um die Liste der Zertifikate zu filtern. In diesem Abschnitt beschreiben wir, wie Sie die verfügbaren Kategorien editieren und neue hinzufügen können.

Um herauszufinden, zu welcher Kategorie ein Schlüssel gehört, versucht Kleopatra, den Schlüssel mit einer Folge von Schlüsselfiltern abzugleichen, die in der Datei `libkleopatrarc` konfiguriert sind. Der erste passende Filter definiert die Kategorie, basierend auf dem später erläuterten Konzept der *Genauigkeit*.

Jeder Schlüsselfilter ist in einer Konfigurationsgruppe namens `Key Filter #n` definiert, wobei *n* eine Zahl ist, beginnend bei `0`.

Die einzigen obligatorischen Schlüssel in einer solchen `Key Filter #n`-Gruppe sind der `Name`, der den Namen der Kategorie enthält, wie er im Einrichtungsdialog angezeigt wird und `id`, die als Verweis auf Filter in anderen Abschnitten der Einrichtungsdatei dient, wie zum Beispiel `View #n`.

Tabelle 6.1 führt alle Schlüssel auf, die die Anzeigeeigenschaften von Schlüsseln dieser Kategorie definieren (d. h. die Schlüssel, die im Einrichtungsdialog editiert werden können), wohingegen Tabelle 6.2 alle Schlüssel auflistet, die die Kriterien definieren, anhand denen Filter mit Schlüsseln verglichen werden.

Konfigurationsschlüssel	Typ	Beschreibung
`background-color`	Farbe	Die zu verwendende Hintergrundfarbe. Wenn dieser Schlüssel nicht vorhanden ist, wird als Vorgabe die global definierte Hintergrundfarbe für Listenansichten verwendet.
`foreground-color`	Farbe	Die zu verwendende Vordergrundfarbe. Wenn dieser Schlüssel nicht vorhanden ist, wird als Vorgabe die global definierte Vordergrundfarbe für Listenansichten verwendet.

font	Zeichensatz	Der zu verwendende benutzerdefinierte Zeichensatz. Der Zeichensatz wird auf die für Listenansichten konfigurierte Größe skaliert, und mit Zeichensatzattributen (siehe unten) versehen.
font-bold	Boolescher Wert	Wenn dieser Schlüssel den Wert true hat und font nicht gesetzt ist, dann wird der Standard-Listen-Zeichensatz in Fettschrift (so verfügbar) verwendet. Wenn auch font vorhanden ist, wird dieser Schlüssel ignoriert.
font-italic	Boolescher Wert	Analog zu font-bold, aber für kursiven Schriftstil anstelle von fettem.
font-strikeout	Boolescher Wert	Wenn dieser Schlüssel den Wert true hat, dann wird eine zentrierte Linie durch den Zeichensatz gezogen. Wird auch dann verwendet, wenn font gesetzt ist.
icon	Text	Der Name eines Icons, das in der ersten Spalte angezeigt wird. Noch nicht implementiert.

Tabelle 6.1: Schlüsselfilter-Konfigurationsschlüssel, die Anzeigeeigenschaften definieren

Konfigurationsschlüssel	**Typ**	**Wenn dieser Schlüssel angegeben ist, passt der Filter, wenn ...**
is-revoked	Boolescher Wert	der Schlüssel widerrufen worden ist.
match-context	Kontext[1]	der Kontext der auf diesen Filter passt.
is-expired	Boolescher Wert	der Schlüssel abgelaufen ist.
is-disabled	Boolescher Wert	der Schlüssel vom Benutzer deaktiviert worden ist (nicht mehr benutzt werden soll). Wird bei S/MIME-Schlüsseln ignoriert.

[1] Kontext besteht aus einer Aufzählung der folgenden zulässigen Werte: appearance, filtering und any.

`is-root-certificate`	Boolescher Wert	der Schlüssel ein Wurzelzertifikat ist. Wird bei OpenPGP-Schlüsseln ignoriert.
`can-encrypt`	Boolescher Wert	der Schlüssel zum Verschlüsseln verwendet werden kann.
`can-sign`	Boolescher Wert	der Schlüssel zum Signieren verwendet werden kann.
`can-certify`	Boolescher Wert	der Schlüssel zum Signieren (Zertifizieren) anderer Schlüssel verwendet werden kann.
`can-authenticate`	Boolescher Wert	der Schlüssel zur Authentifikation (etwa als TLS-Client-Zertifikat) verwendet werden kann.
`is-qualified`	Boolescher Wert	der Schlüssel kann benutzt werden, um qualifizierte Signaturen zu erzeugen, wie sie im deutschen Signaturgesetz ((Gesetz über Rahmenbedingungen für elektronische Signaturen) definiert sind.
`is-cardkey`	Boolescher Wert	der Schlüssel wird auf einer Chipkarte und nicht auf dem Rechner gespeichert.
`has-secret-key`	Boolescher Wert	der geheime Schlüssel zu diesem Schlüsselpaar zur Verfügung steht.
`is-openpgp-key`	Boolescher Wert	der Schlüssel ein OpenPGP-Schlüssel (`true`) oder ein S/MIME-Schlüssel (`false`) ist.
`was-validated`	Boolescher Wert	der Schlüssel überprüft worden ist.

präfix-ownertrust	Gültigkeit[2]	der Schlüssel hat genau (*präfix* = is), hat alle außer (*präfix* = is-not), hat mindestens (*präfix* = is-at-least), oder hat höchstens (*präfix* = is-at-most) das Eigentümer-Vertrauen, das als Wert des Konfigurationsschlüssels angegeben ist. Wenn mehr als ein präfix-ownertrust-Schlüssel (mit unterschiedlichen *präfix*-Werten) in einer einzigen Gruppe steht, ist das Verhalten undefiniert.
präfix-validity	Gültigkeit	Entsprechend präfix-ownertrust, aber für die Gültigkeit von Schlüsseln anstelle vom Eigentümer-Vertrauen.

Tabelle 6.2: Schlüsselfilter-Konfigurationsschlüssel, die Filterkriterien definieren

ANMERKUNG

Einige der interessanteren Kriterien wie is-revoked oder is-expired funktionieren nur bei *validierten* Schlüsseln, weswegen standardmäßig nur überprüfte Schlüssel auf Widerruf oder Ablauf geprüft werden, auch wenn es Ihnen frei steht, diese zusätzlichen Abfragen zu entfernen.

Zusätzlich zu den oben genannten Konfigurationsschlüsseln kann ein Schlüsselfilter auch noch die Attribute id und match-contexts haben.

Mit der id des Filters ist überall in der Konfiguration der Zugriff auf den Schlüsselfilter möglich, z. B. in Kleopatras Konfiguration des Erscheinungsbilds. Der Standardwert der id ist der Name der Gruppe in der Konfigurationsdatei, falls nicht anders angegeben. Der Wert darf auch nicht gesetzt sein. Die id wird durch Kleopatra nicht verarbeitet und kann daher einen beliebigen Text enthalten, der aber eindeutig sein muss.

Das Attribut match-contexts begrenzt die Anwendungsmöglichkeit des Filters. Es sind zurzeit zwei Kontexte definiert: appearance wird benutzt zur Definition von Farben und Schriften für die Anzeige. Mit filtering werden Zertifikate in der Ansicht ein- oder ausgeblendet. any kann zur Kennzeichnung aller aktuell definierten Kontexte verwendet werden. Dies ist die Voreinstellung, wenn match-contexts nicht definiert ist oder sich ansonsten kein Kontext ergibt. Damit wird sichergestellt, dass es keinen Filter ohne Kontext gibt.

Ein Eintrag besteht aus einer Liste von Zeichengruppen, getrennt durch Leerzeichen. Jeder Zeichengruppe kann ein Ausrufungszeichen (!) vorangestellt werden, damit wird der Ausdruck verneint. Die Zeichengruppen werden der Reihe nach auf eine interne Liste von Kontexten angewendet, die zu Beginn leer ist. Das lässt sich am Besten an einem Beispiel erklären: any !appearance entspricht filtering, und appearance !appearance ebenso wie !any ergeben eine leere

[2] Die Gültigkeit ist eine (geordnete) Aufzählung mit den folgenden zulässigen Werten: unknown, undefined, never, marginal, full und ultimate. Eine vollständige Beschreibung finden Sie in den Handbüchern zu GPG und GpgSM.

Menge. Die letzten beiden Ergebnisse werden intern durch `any` ersetzt, da sie keinerlei Kontext ergeben.

Nicht angegebene Kriterien (Kriterien, deren Konfigurationsschlüssel nicht angegeben ist), werden nicht abgefragt. Wenn ein Kriterium angegeben ist, dann wird es abgefragt und muss zutreffen, damit der Filter als Ganzes zutrifft; die einzelnen Kriterien werden also UND-verknüpft.

Jeder Filter beinhaltet eine „Genauigkeit", die alle passenden Filter bewertet. Der genauere Filter wird dem weniger genauen vorgezogen. Haben zwei Filter die gleiche Genauigkeit, wird der zuerst in der Konfigurationsdatei aufgeführte benutzt. Die Genauigkeit entspricht der Anzahl der Kriterien des Filters.

Beispiel 6.1 Beispiele für Schlüsselfilter

Um alle abgelaufenen, aber nicht widerrufenen Wurzel-Zertifikate abzufragen, würden Sie den folgenden Schlüsselfilter verwenden:

```
[Key Filter #n]
Name=abgelaufen, aber nicht widerrufen
was-validated=true
is-expired=true
is-revoked=false
is-root-certificate=true
; ( specificity 4 )
```

Um alle deaktivierten OpenPGP-Schlüssel (derzeit noch nicht von Kleopatra unterstützt) mit einem Eigentümer-Vertrauen von mindestens „marginal" abzudecken, verwenden Sie:

```
[Key Filter #n]
Name=deaktivierte OpenPGP-Schlüssel mit einem Ownertrust von marginal oder ↩
    besser
is-openpgp=true
is-disabled=true
is-at-least-ownertrust=marginal
; ( specificity 3 )
```

6.3 Einstellung von Archivierungs-Programmen für die Benutzung mit „Dateien signieren/verschlüsseln ..."

Kleopatra ermöglicht dem Systemverwalter (und erfahrenen Benutzer) die Liste der Archivierungs-Programme, die im „Dateien signieren/verschlüsseln ..."-Dialog wählbar sind, einzustellen.

Jedes Archivierungs-Programm wird in `libkleopatrarc` als eigenständige `Archive Definition #n`-Gruppe mit den folgenden verbindlichen Schlüsseln definiert:

`extensions`
: Eine durch Komma getrennte Liste von Dateierweiterung, die normalerweise eine Archivdatei kennzeichnen.

`id`
: Eine eindeutige Kennung, um dieses Archivierungs-Programm intern zu identifizieren. Falls Sie Zweifel haben, nutzen Sie den Namen des Befehls.

`Name` (übersetzt)
: Der Name des Archivierungs-Programms, so wie er dem Benutzer im entsprechenden Aufklappmenü des „Dateien signieren/verschlüsseln ..."-Dialogs angezeigt wird.

pack-command

Der eigentliche Befehl zum Archivieren von Dateien. Sie können hier jeden Befehl verwenden, so lange es nicht erforderlich ist eine Shell auszuführen. Sofern Sie keinen absoluten Pfad angeben, wird die Programmdatei wird mit Hilfe der PATH-Umgebungsvariable nachgeschlagen. Anführungszeichen werden so unterstützt, als wenn eine Shell verwendet wird:

```
pack-command="/opt/ZIP v2.32/bin/zip" -r -
```

ANMERKUNG

Da umgedrehte Schrägstriche (\) ein Steuerzeichen in KDE-Einrichtungsdateien sind, müssen Sie diese doppelt verwenden, wenn sie in Pfadnamen auftauchen:

```
pack-command=C:\\Programme\\GNU\\tar\\gtar.exe ...
```

Für den Befehl selbst (im Gegensatz zu seinen Argumenten) sollten Sie nur normale Schrägstriche (/) als Trennzeichen für Pfade auf allen Plattformen nutzen.

```
pack-command=C:/Programme/GNU/tar/gtar.exe ...
```

In den Argumenten des Befehls wird dies nicht unterstützt, da zumindest Windows®-Programme den Schrägstrich für Optionen nutzen. Zum Beispiel funktioniert das folgende nicht, da `C:/meinearchivierung.bat` ein Argument für **cmd.exe** ist und / in Argumenten nicht in \ umgewandelt wird, sondern nur in Befehlen:

```
pack-command=cmd.exe C:/meinearchivierung.bat
```

Dies muss wie folgt umgeschrieben werden.

```
pack-command=cmd.exe C:\\meinearchivierung.bat
```

6.3.1 Dateiname der zu archivierenden Datei, wie er dem **pack-command** übergeben wird

Es gibt drei Möglichkeiten Dateinamen dem Archivierungs-Befehl zu übergeben.

1. Als Befehlszeilen-Argumente.
   Beispiel (GNU-tar):

   ```
   pack-command=tar cf -
   ```

   Beispiel (ZIP):

   ```
   pack-command=zip -r - %f
   ```

   In diesem Fall werden die Dateinamen über die Befehlszeile übergeben, genau so, als wenn die Befehlszeileneingabe genutzt würde. Kleopatra benutzt keine Shell um den Befehl auszuführen. Daher ist die sicherste Methode Dateinamen zu übergeben, auch wenn dies auf einigen Systemen an Begrenzungen der Befehlszeilenlänge stoßen kann. Sofern das Literal `%f` angegeben ist, wird es durch die Namen der zu archivierenden Dateien ersetzt. Anderenfalls werden diese Dateinamen an das Ende der Befehlszeile abgehängt. Daher kann das ZIP-Beispiel wie folgt gleichbedeutend umgeschrieben werden:

   ```
   pack-command=zip -r -
   ```

2. Über die Standard-Eingabe und durch Zeilenumbrüche getrennt: `|` voranstellen.
   Beispiel (GNU-tar):

```
pack-command=|gtar cf - -T-
```

   Beispiel (ZIP):

```
pack-command=|zip -@ -
```

   In diesem Fall werden die Dateinamen dem Archivierungs-Programm über stdin zeilenweise übergeben. Dies umgeht Probleme auf Systemen, die eine niedrige Begrenzung für die Anzahl an erlaubten Befehlszeilenzeilenparametern setzen, schlägt jedoch fehl, wenn Dateinamen Zeilenumbrüche enthalten.

> ANMERKUNG
> Derzeit unterstützt Kleopatra nur LF als Steuerzeichen für einen Zeilenumbruch und nicht CRLF. Abhängig von Rückmeldungen der Benutzer kann sich dies in Zukunft ändern.

3. Über die Standard-Eingabe und durch NUL-Bytes getrennt: `0|` voranstellen.
   Beispiel (GNU-tar):

```
pack-command=0|gtar cg - -T- --null
```

   Dies ist das gleiche wie oben, außer, dass NUL-Bytes für die Trennung der Dateinamen genutzt wurde. Da NUL-Bytes in Dateinamen verboten sind, ist dies die robusteste Methode um Dateinamen zu übergeben. Allerdings wird sie nicht von allen Archivierungs-Programmen unterstützt.

6.4 Einrichtung der Prüfsummen-Programme zur Benutzung mit „Prüfsummen erstellen/verifizieren”

Kleopatra ermöglicht es dem Systemverwalter (und erfahrenen Benutzer) die Liste der Prüfsummen-Programme, aus denen der Benutzer im Einstellungs-Fenster wählen kann, einzustellen. Zudem ist Kleopatra dann in der Lage bei Bedarf eines für die Überprüfung der Prüfsumme einer gegebenen Datei automatisch zu wählen.

ANMERKUNG

Um von Kleopatra benutzbar zu sein muss die Ausgabe eines Prüfsummen-Programms (sowohl die gespeicherte Prüfsummendatei als auch die Ausgabe auf stdout) kompatibel mit GNU **md5sum** und **sha1sum** sein.
Insbesondere muss die Prüfsummendatei zeilenbasiert sein, wobei jede Zeile das folgende Format erfüllen muss:

```
PRÜFSUMME ' ' ( ' ' | '*' ) DATEINAME
```

, wobei *PRÜFSUMME* nur aus hexadezimal-Zeichen besteht. Sollte *DATEINAME* ein Zeilenumbruchzeichen enthalten, muss die Zeile wie folgt formatiert sein:

```
\PRÜFSUMME ' ' ( ' ' | '*' ) MASKIERTER-DATEINAME
```

, wobei *MASKIERTER-DATEINAME* der Dateiname ist, in dem Zeilenumbrüche durch `\n` und umgedrehte Schrägstriche gedoppelt sind (\↦\\).
Vergleichbar muss die Ausgabe von `verify-command` die Form

```
DATEINAME ( ': OK' | ': FAILED')
```

haben, wobei Zeilenumbrüche wieder als Trennzeichen dienen. Allerdings werden Zeilenumbrüche und andere Steuerzeichen der Ausgabe hier *nicht* maskiert.[a]

[a] Diese Programme wurden nicht für eine graphische Benutzeroberfläche geschrieben und Kleopatra wird beim analysieren von irrsinnigen Dateinamen, die „: OK“ und einen Zeilenumbruch enthalten, versagen.

Jedes Prüfsummen-Programm ist in `libkleopatrarc` als eigenständige `Checksum Definition #n`-Gruppe mit den folgenden verbindlichen Schlüsseln definiert:

`file-patterns`

Eine Liste regulärer Ausdrücke, die beschreiben welche Dateien als Prüfsummendateien für diese Prüfsummen-Programm gehalten werden sollen. Die Syntax ist die gleiche, die auch für Zeichen-Listen in KDE-Einrichtungsdateien verwendet wird.

ANMERKUNG

Da reguläre Ausdrücke normalerweise umgedrehte Schrägstriche enthalten, muss Vorsicht gewaltet werden, um diese in der Einrichtungsdatei richtig zu maskieren. Die Verwendung von Werkzeugen zur Bearbeitung von Einrichtungsdateien wird empfohlen.

Ausschlaggebend dafür, ob die Muster Groß-/Kleinschreibung unterscheiden, ist das System.

`output-file`

Der typische Name der Ausgabedatei dieses Prüfsummen-Programms (sollte natürlich einem der `file-patterns` entsprechend). Diesen verwendet Kleopatra als Name der Ausgabedatei beim Erstellen von Prüfsummendateien dieses Typs.

`id`

Eine eindeutige Kennung, um dieses Prüfsummen-Programm intern zu identifizieren. Falls Sie Zweifel haben, nutzen Sie den Namen des Befehls.

`Name` (übersetzt)

Der Name des Archivierungs-Programms, so wie er dem Benutzer in Kleopatras Einrichtungsdialog angezeigt wird.

create-command

Der eigentliche Befehl mit dem Prüfsummendateien erzeugt werden. Die Syntax sowie Begrenzungen und Optionen der Argument-Übergabe sind die gleichen wie für pack-command in Abschnitt 6.3 beschrieben.

verify-command

Genau wie create-command, allerdings für Prüfsummen-Verifizierung.

Hier sehen Sie ein vollständiges Beispiel:

```
[Checksum Definition #1]
          file-patterns=sha1sum.txt
          output-file=sha1sum.txt
          id=sha1sum-gnu
          Name=sha1sum (GNU)
          Name[de]=sha1sum (GNU)
          ...
          create-command=sha1sum -- %f
          verify-command=sha1sum -c -- %f
```

Kapitel 7

Danksagungen und Lizenz

MITWIRKENDE

- Marc Mutz mutz@kde.org
- David Faure faure@kde.org
- Steffen Hansen hansen@kde.org
- Matthias Kalle Dalheimer kalle@kde.org
- Jesper Pedersen blackie@kde.org
- Daniel Molkentin molkentin@kde.org

Übersetzung Matthias Kalle Dalheimerkalle@kdab.net und Torbjörn Klatttorbjoern.k@googlemail.com