FileSeq™

Produktbeschreibung

White Paper

Einleitung

Diese Dokumentation beschreibt die Eigenschaften und die Funktionsweise der File-Seq Dateiverschlüsselungstechnologie.

Die Aufgabe von FileSeq ist die Sicherung eines Netzwerkes gegen unbefugte Zugriffe auf sensible Daten.

Die Netze werden nach außen (Internet) durch Firewall Systeme geschützt. Unberechtigte Zugriffe innerhalb des Intranet können dadurch jedoch nicht verhindert werden.

Die internen Schutzmöglichkeiten in der Office Umgebung lassen sich in den meisten Fällen nur unbefriedigend umsetzen. Sensible Daten z.B. aus dem Forschungs-, Personal- oder Finanzbereich, sind somit leicht zugänglich. Hier bietet die Zugriffs- und Verschlüsselungs- Technologie von FileSeq eine einzigartige und anwenderfreundliche Lösung, um Daten- Diebstahl und Missbrauch zu verhindern.

Daten werden mit einer eigenen Zugriffsberechtigung versehen und mit einer sicheren Verschlüsselungstechnologie in der Office Umgebung abgelegt. Auch ein Abhören / Einsehen der gespeicherten Daten während der Übertragung ist nicht möglich, da nur verschlüsselte Daten übertragen werden.

Durch die einzigartige Architektur von FileSeq wird ein Höchstmaß an interner Sicherheit im Netzwerk erreicht.

1. Überblick

In großen Organisationen und Netzwerken wird der Datenschutz zunehmend wichtiger. Immer mehr Daten werden auf zugänglichen Netzwerkdatenservern gespeichert. Eine der größten Herausforderungen, denen Organisationen heute gegenüberstehen, ist das Zugangsmanagement zu den verschiedenen Datenquellen. Traditionell wurde diese Aufgabe vom Betriebssystem übernommen. Aber durch das Entstehen von Netzwerken sind neue Herausforderungen an die traditionellen Datenschutzmodelle hinzugekommen.

FileSeq ermöglicht es den Unternehmen, sensible Informationen, die in Dateien gespeichert wurden, zu verwalten ohne sich ausschließlich auf die Sicherheit des Betriebssystems der Workstations oder des angeschlossenen Servers zu verlassen.

FileSeq nutzt das Konzept eines Key-Server, um sensible Informationen verbunden mit einem geschützten Dateischlüssel abzuspeichern.

Der FileSeq Client, der auf der Workstation installiert wird, arbeitet mit dem Key-Server zusammen, der die Schlüssel zu Verfügung stellt.

Diese Schlüssel werden vom FileSeq Client Treiber benutzt, um die Dateninhalte aus Standardanwendungen transparent zu ver- oder entschlüsseln. Dieser Vorgang verläuft vom User unbemerkt im Hintergrund, so dass eine hohe Anwenderakzeptanz erreicht wird.

2. Produktkomponenten

2.1 FileSeq Key Server

Der Key Server ist normalerweise in einer gesicherten Umgebung wie z.B. in Rechenzentren oder anders gesicherten Räumlichkeiten untergebracht. Die Key Server stellen erweiter- und skalierbare, sichere Speicherung von Dateiattributen, Zugangskontrollinformationen und kryptographische Schlüssel zur Verfügung. Dateiinhalte werden auf dem Key Server nicht gespeichert.

Jeder Key Server kann von einem Administrator über SSL sicher konfiguriert werden und ermöglicht so die sichere (remote) Verwaltung des Systems.

Die Key Server können zu einem Cluster zusammengefasst werden, um ihre Datenbanken gegenseitig zu replizieren und stellen so ein redundantes System zur Verfügung.

Ein digitales Zertifikat authentisiert den Key Server beim Client.

2.2 FileSeq Client Software

FileSeq Client ist eine Anwendung auf der Workstation. Sie stellt benutzeraktivierte Dateiverschlüsselung und -entschlüsselung zur Verfügung. Wenn der Benutzer auf eine verschlüsselte Datei zugreift, fordert die FileSeq Client Software einen symmetrischen Schlüssel über eine gesicherte SSL Verbindung vom Key Server an.

FileSeq Client wird sowohl für die Erstverschlüsselung von Daten als auch für die Verwaltung der Zugangsrechte von Verzeichnissen verwendet. Der FileSeq Klient meldet sich am Key Server an.

2.3 FileSeq Client Treiber

Der FileSeq Client Treiber ist ein Dateisystemfiltertreiber, der auf der Workstation installiert wird. Er bewirkt permanente Ent- und Verschlüsselungen, ohne dass der Anwender diesen Vorgang auslösen muss.

Der FileSeq Client Treiber initiiert die Zugangskontrolle zu gesicherten Dateien, die vom Key Server verwaltet werden. Das bewirkt einen Access control layer, der zusätzlich zum Netzwerkbetriebssystem arbeitet.

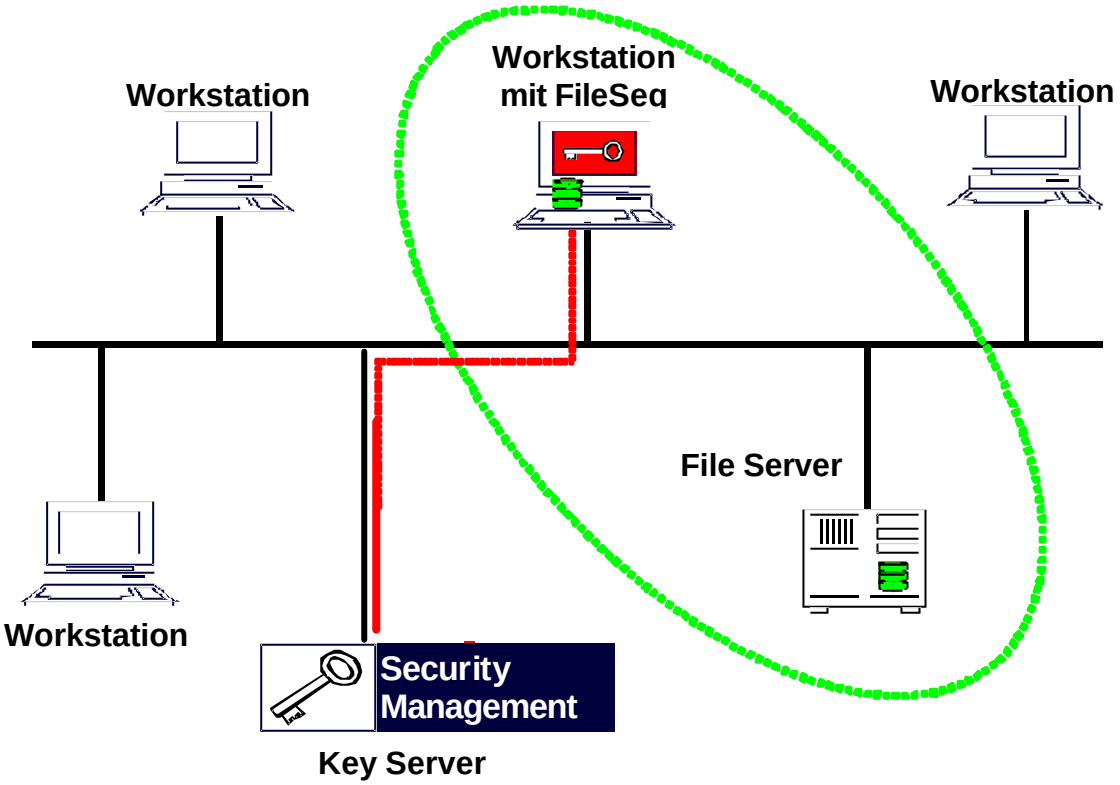

Abbildung 1 Typische Büroumgebung mit FileSeq

3. Funktionsweise

In einer typischen Officeumgebung (dargestellt in Abbildung 1) verbinden sich die Workstations über den FileSeq Client mit dem Key Server, um Verschlüsselungen auszulösen. Der Key Server verifiziert den Zugang und liefert die Schlüssel, die benötigt werden, um Daten auf der Workstation und auf den Servern zu entschlüsseln.

Ein typischer Datenaustausch läuft wie folgt ab:

Schritt 1: Sobald die Verbindung mit dem Key Server hergestellt ist, erscheint ein Login Fenster, in das der Anwender die User ID und sein Kennwort eingibt. Nach erfolgreicher Anmeldung durch den Client steht nun eine gesicherte Verbindung zum Key Server zur Verfügung, über die alle Schlüsselanfragen abgewickelt werden. Alle Anfragen laufen über eine sichere SSL Verbindung zum Key Server unter Verwendung eines HTTP Protokolls.

Schritt 2: Der Benutzer greift über eine Applikation wie z.B. Word oder Excel auf die verschlüsselten Dateien zu. Zur Verschlüsselung ist lediglich die Abspeicherung in einem verschlüsselten Verzeichnis nötig, die Verschlüsselung erfolgt automatisch.

Schritt 3: Der FileSeq Client Treiber fordert Schlüssel vom Key Server an, um Dateien zu lesen oder zu erstellen.

Schritt 4: Der Key Server vergleicht die Anfrage mit den Zugangsrechten ACL, die in der Datenbank hinterlegt sind. Der Zugriff wird automatisch in einer Audit Datenbank aufgezeichnet.

Schritt 5: Der Key Server liefert den Dateischlüssel zusammen mit den Zugriffsrechten. Die Lese- und Schreibrechte werden vom Key Server in einer Maske an den Client übergeben. Der Client entscheidet anhand dieser Maske, ob er Lesen oder Lesen und Schreiben darf, andere Rechte wie z.B. Erstellen von Dateien werden direkt vom Key Server verwaltet. Greift der Client auf eine Datei zu, für die er keine Rechte besitzt, wird vom Key Server eine Meldung an den Client gesendet. Alle anderen Zugriffsrechte wie Erstellen, Löschen, Audit und Verwalten werden vom Key Server authentisiert.

Schritt 6: Der FileSeq Client Treiber cached den Schlüssel und die dazugehörige Zugriffsmaske in einem non paged memory innerhalb des Kernel um ein Höchstmass an Sicherheit zu gewährleisten.

Schritt 7: Der FileSeq Client Treiber vervollständigt die geöffnete Datei und cached den Schlüssel im non paged memory, um nicht permanent auf den Key Server zuzugreifen, oder startet eine erneute Anfrage, wenn der Schlüssel nicht mehr im cache vorliegt.

Die oben beschriebenen Prozesse laufen für den User unbemerkt im Hintergrund. Der gesamte Vorgang dauert durchschnittlich weniger als 50 ms. Die Performance des Netzes bleibt davon unberührt.

4. FileSeq Architektur

4.1. FileSeq System Architektur

Die Architektur von FileSeq ist in der Abbildung 2 dargestellt. Wie aus diesem Diagramm ersichtlich, sind die beiden Hauptkomponenten der FileSeq Client und der Key Server. Diese Komponenten kommunizieren über SSL in HTTP. Die gesicherte Verbindung wird zu Beginn der Session mit dem Key Server hergestellt. Daraufhin kann der Benutzer sich am Key Server authentisieren.

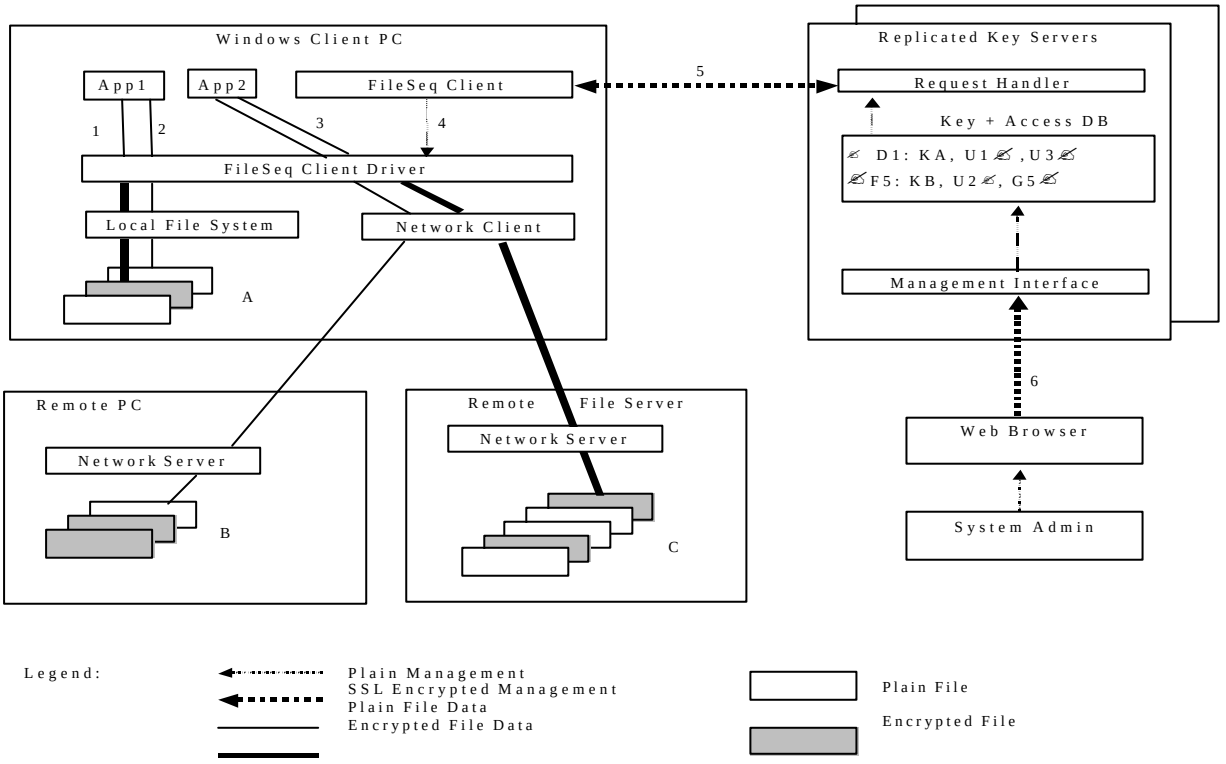

Abbildung 2: FileSeq Architektur

Sobald der User sich angemeldet hat, werden alle Anfragen nach Dateischlüsseln vom Client durch den Key Server beantwortet. Diese Anfragen beinhalten das File Tag, das das Dateiobjekt in der Datenbank identifiziert.
Das File Tag enthält genügend Informationen über das Dateiobjekt, um dem Key Server zu ermöglichen, alle Access Control bezogenen Einträge für Dateiobjekte in der Datenbank aufzufinden. Die Policy Engine beurteilt die Informationen und trifft die Entscheidung über den Zugang (Allow/Deny).

4.2. FileSeq Client Architektur

Die Arbeitsweise des FileSeq Clients, der Windows System Architektur und der Interaktion beider Komponenten wird in Abbildung 3 gezeigt. Der FileSeq Client besteht aus zwei Komponenten, die bei der Verschlüsselung zusammenwirken. Die FileSeq Client Anwendung stellt das User- Interface und das Kommunikations- Interface zum Key Server zur Verfügung. Die FileSeq Treiber Komponente bewirkt eine transparente Ver- und Entschlüsselung für alle Standard Applikationen, die auf das Dateisystem zugreifen.

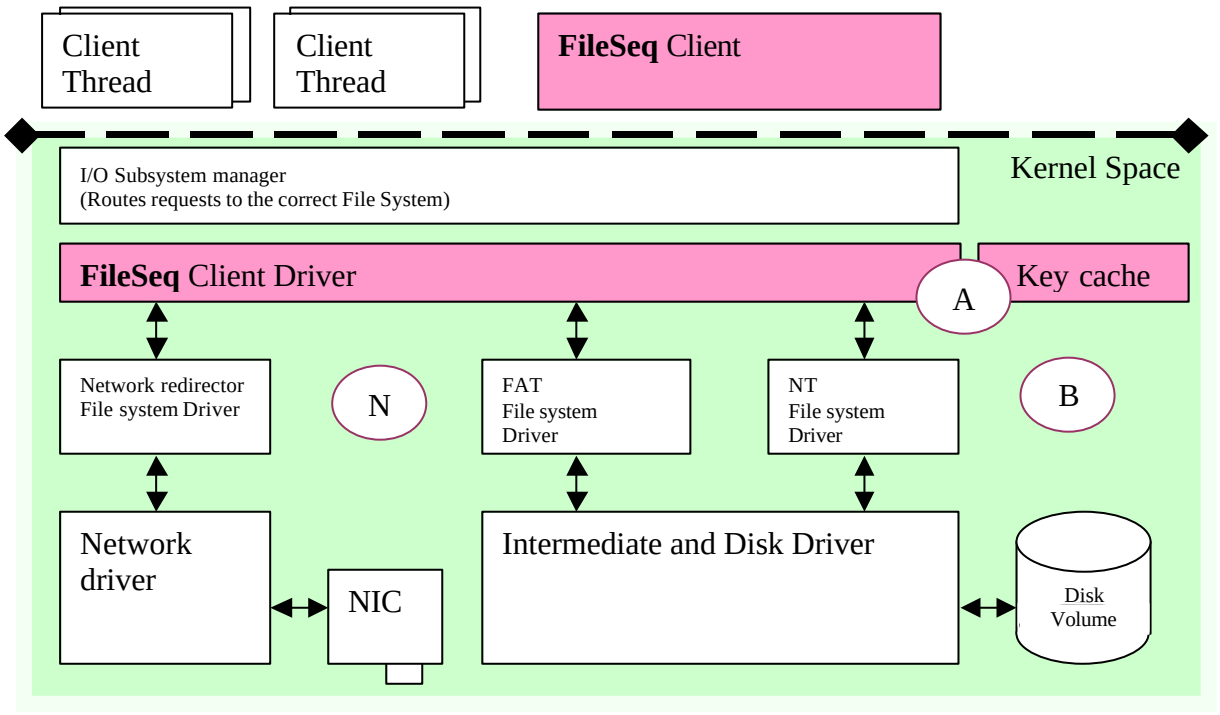

Abbildung 3 FileSeq Client Architektur

Das FileSeq Client Treiber Interface, über dem Netzwerk Redirector, entschlüsselt Dateien bevor sie die Applikationen erreichen und verschlüsselt die Dateien bevor sie in das Netzwerk geschickt werden, was zur Folge hat, dass Daten ausschließlich verschlüsselt im Netzwerk übertragen werden. Dies ist ein wichtiger Vorteil gegenüber anderen Verschlüsselungssystemen.

Der FileSeq Client Treiber behält eine Kopie des Schlüssels in seinem Non Swapped Memory. Dieser Schlüssel ist nur für die im Key Server festgelegte Zeit verfügbar.

4.3. Key Server Architektur

Der Key Server bietet eine sichere Umgebung, in der alle Schlüssel gespeichert sind und der Zugang über Access Control Listen verwaltet wird. Die Architektur des Key Servers ist in Abbildung 4 dargestellt.

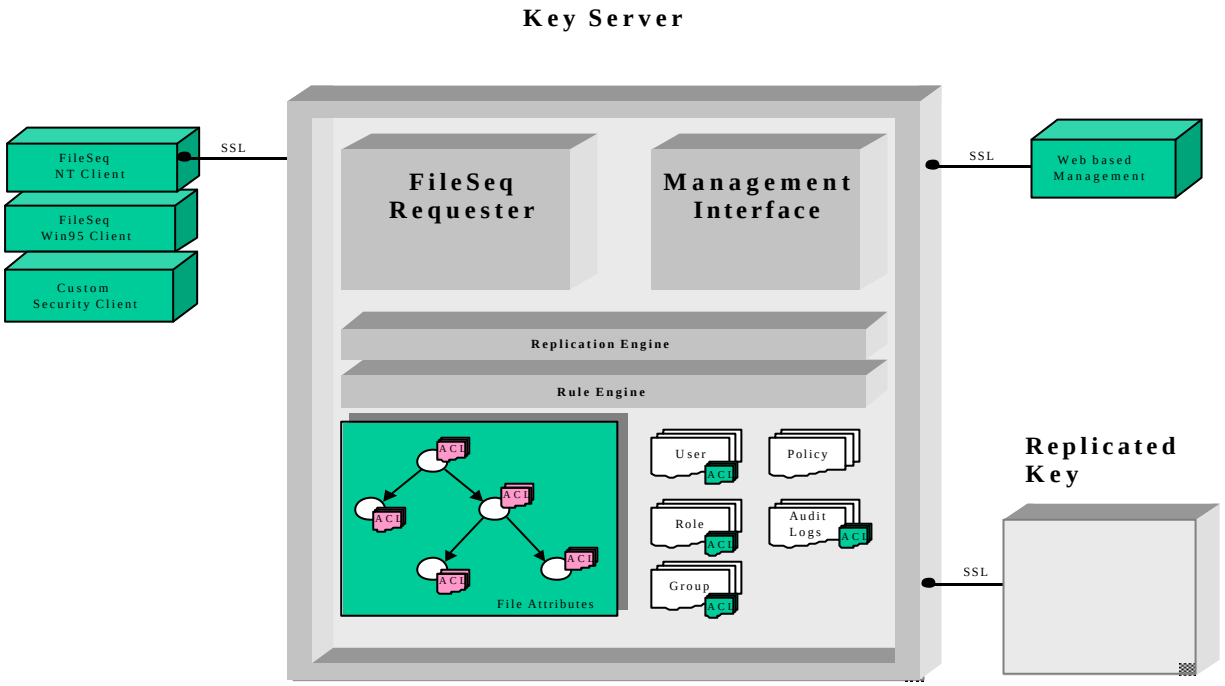

Abbildung 4 Key Server Architektur

Das Key Server Design besteht aus mehreren Ebenen (Layer), mit einer sicheren Rule Engine. Ein Teil dieser Rule Engine bewirkt eine Replication des Transfers vom Original Server zu Partner Servern. Diese Replication wird über eine SSL Verbindung, die mit einem x509 Zertifikat versehen ist, hergestellt. Diese Software ermöglicht das Clustern von mehreren Servern.

Die Key Server Datenbank basiert auf einer SQL Datenbank. Diese Datenbank stellt dem Management Interface und dem FileSeq Requester alle Daten zur Verfügung. Die Datenbank besteht aus folgenden Objekten:

Benutzer (User), Benutzergruppen (User Groups), Benutzer Rollen (User Roles), Dateien (Files) and Verzeichnisse (Directories).

Jedes Objekt in der Datenbank ist verknüpft mit einer Access Control List. Anhand der Access Control List wird von der Rule Engine der Zugriff auf die Datenbank geregelt.

Eine weitere Beziehung besteht zwischen den Objektklassen, die eine Rollenbasierende ACL zur Verfügung stellen. Dieser Mechanismus erlaubt Security Administratoren, Rollen zu definieren, die bestimmte Objektklassen einschränken z.B. Dateiobjekte. Diese Standard ACL´s werden mit Rollen verbunden und so aufgebaut, dass sie die Security Policy des End-Users abbilden. Hiermit lassen sich Organisationsstrukturen komplett nachbilden.

4.4. Key Server Authentication Protokoll

Der Key Server authentisiert den FileSeq Client Benutzer durch eine User ID, Rolle und Passwort. Diese Informationen werden mittels HTTP Protokoll über eine sichere SSL Verbindung über TCP/IP geschickt.

4.5. Key Request / Response Protocol

Das Key Kommunikationsprotokoll nutzt die bestehende SSL Verbindung. Der FileSeq Client sendet eine HTTP Anfrage über diese SSL Verbindung und wartet auf eine Antwort vom Key Server. Der Key Server sendet im HTTP Header einen Bestätigungscode mit den Key- und Privilegien- Informationen.

Wenn der Key Server weitere Informationen benötigt, können diese über einen HTML Request angefordert werden. Beispielsweise ist dies beim Check In und Check Out der Fall.

4.6. Security Management

Der Key Server wird mittels eines Web Interfaces administriert. Die unterstützten Web Browser beginnen ab den Versionen IE 4.02 und Netscape 4.x. Folgende Einstellungen im Browser werden benötigt:
Java, Java Script und Cookies

Das Management Interface nutzt die gleichen Authentifikationsmechanismen wie der FileSeq Client. Sobald der User seine Zugangsdaten eingegeben hat, wird eine Verbindung aufgebaut und ein Cookie auf dem Client abgelegt. Der Cookie wird benötigt um die Browser Verbindung aufrecht zu halten. Der Cookie läuft nach einer konfigurierbaren Zeit ab und der User muss sich neu identifizieren; damit wird vermieden, dass ältere Verbindungen missbräuchlich benutzt werden.

Zusätzlich zu den menübasierenden Optionen, um User, Gruppen, Rollen und Datenobjekte zu administrieren, lässt das Management Interface auch einen Batch Mode zu. Eine objektbasierende Script Sprache in Form einer Textdatei kann über das Management Interface an den Key Server übertragen und dort ausgeführt werden.

Diese Möglichkeit wird genutzt, um große Usermengen und Gruppen in kurzer Zeit anzulegen. Es lassen sich z.B. Daten aus einer NT Domain Datenbank automatisiert in ein Script umwandeln, um die entsprechenden Benutzer im System schnell anzulegen.

5. Replikation zwischen den Key Servern

Eine wichtige Eigenschaft der Key Server ist die permanente Replikation untereinander. Der Replikationsmechanismus schickt alle Transaktionen über SSL zu den anderen Servern. Die Partner Key Server aktualisieren so Ihre Datenbank mit den neuen Informationen, so dass jeder Client auf die gleiche Datenbank zugreift, unabhängig mit welchem Server er gerade verbunden ist.

Der Replikaktionsmechanismus nutzt eine Kombination aus Zeitstempel und einer netzwerkbasierenden Replikationsdatenbank. In allen Vorgängen, zum Beispiel wenn verschlüsselte Dateien erstellt werden, generiert der Quell Key Server einen Schlüssel, trägt diesen in die Datenbank ein und repliziert diese Information zu allen anderen Key Servern ohne eine Bestätigung zu verlangen. Da Anforderungen parallel bedient werden während im Hintergrund die Replikation läuft, wird so die maximal mögliche Geschwindigkeit erreicht.

Im Falle einer User- oder Policy- Administration sendet der Master Server ein Objekt Lock Request zu allen anderen. Das verhindert ein Updaten des Objektes durch einen anderen Server zur gleichen Zeit.

Die Kombination zwischen Locking und Zeitstempel sichert eine hohe Datenintegrität und einen maximalen Real-Time Durchsatz.

6. FileSeq Key Management

FileSeq verwendet eine Anzahl kryptographischer Mechanismen. Als erstes generiert der Key Server ein digitales Zertifikat- Request. Dieser Zertifikat- Request wird von einer Certification Authority (Trust Center) unterzeichnet und auf dem Key Server installiert. Ebenso wird ein Root Certificate des Trust Centers auf allen Servern installiert, so das alle Key Server die Bestätigung vom Trust Center lesen können.

Der FileSeq Client und alle Server, wie auch das Management Interface nutzen alle das jeweilige Key Server Certificate, um den Key Server zu identifizieren.

Während einer FileSeq Client Sitzung wird das digitale Certificate nur benutzt um den Session Key für die SSL Verbindung zu erzeugen. Nach dem Aufbau der Verbindung und dem Schlüsselaustausch wird der Session Key verwendet um den Datenaustausch zwischen Client und Key Server zu entschlüsseln.

Wenn der FileSeq Client eine verschlüsselte Datei entschlüsseln will, wird der File-Tag (ein Anhang im Dateinamen) zum Key Server gesendet. Der File-Tag enthält folgende wichtige Informationen:

File identifier:	Kurzversion des Dateinamens.
Object identifier:	einmalige Datenbank ID für das Dateiobjekt.
Master Key ID:	einmalige Identifikation für den Master Key, der benutzt wurde, um den Dateischlüssel zu verschlüsseln.
Key material:	Der Dateischlüssel, der mit dem Master-Key verschlüsselt ist.

Ein Anwendungszweck des Master Key besteht darin, dass er benötigt wird, um eine von der Datenbank gelöschte Datei wiederherzustellen (z.B. wenn die Datei gelöscht wurde und jetzt vom Backup wiederhergestellt wird). Für diesen Zweck wird eine Reihe von Master Keys in periodischen Intervallen erzeugt. Diese Schlüssel werden in der Datenbank gespeichert und können nicht gelöscht werden. Der Sicherheits- Administrator hat die Möglichkeit, die Intervalleinstellungen für die Master Key Erzeugung festzulegen.

7. Zusammenfassung der FileSeq Eigenschaften

7.1. Kryptographische Sicherheit

7.1.1 **FileSeq arbeitet auf einem sehr hohen Sicherheitsstandard.** FileSeq verwendet einen IDEA Algorithmus, der mit einem 128 Bit Schlüssel arbeitet.

7.1.2 **Unabhängigkeit vom Sicherheitsstandard des Netzwerkbetriebssystems.** Die Systemarchitektur erfordert nur ein Minimum an sicherheitsrelevanten Daten auf dem Client. Die Workstation enthält keine Schlüssel außer dem Dateischlüssel im RAM während der Verarbeitung.

7.1.3 **Es wird keine sichere Speichermöglichkeit auf der Workstation benötigt.** Der Key Server speichert alle Dateischlüssel. Diese Schlüssel werden nur an Clients übergeben, nachdem eine Authentisierung und eine Zugangsprüfung erfolgt ist.

7.2. Benutzerfreundlichkeit

7.2.1 **Automatische Verschlüsselung der Dateien basierend auf der Speicherplatzzuordnung.** Die bestmögliche Security Policy wäre, wenn es gelänge, das Bewusstsein der Anwender permanent auf den Sicherheitsgedanken zu lenken. In der Realität wird jedoch die Verschlüsselung von sensiblen Daten häufig vergessen. Diese Schwachstelle löst FileSeq dadurch, dass bestimmte von der Administration festgelegte Speicherplätze automatisch verschlüsselt werden.

7.2.2 **Applikationsunabhängige Verschlüsselung im Hintergrund.** Unabhängig von der gerade eingesetzten Standardanwendung verschlüsselt FileSeq automatisch im Hintergrund.

7.2.3 **Wenig Overhead beim Zugriff auf verschlüsselte Dateien.** Der FileSeq Key Server wurde dahingehend optimiert, schnellstmögliche Schlüsselzugriffe zu realisieren. Dies erlaubt Real time Anfragen an den Key Server, wodurch sich die allgemeine Reaktionszeit nur minimal erhöht, was aber für den User nicht wahrnehmbar ist.

7.2.4 **Transparentes File Sharing.** FileSeq erlaubt die gemeinsame Nutzung verschlüsselter Dateien durch mehrere Anwender. Dies ist wichtig für bestimmte Applikationen wie z.B. Datenbanken, die gleichzeitig auf verschlüsselte Daten zugreifen müssen.

7.3. Management

7.3.1 **Zentrales Management.** Sowohl zentrale als auch dezentrale Verwaltung der Datei- Privilegien ist möglich. Aufgrund des Management Interface Design kann die Verwaltung der Dateiattribute leicht von irgend einem Ort innerhalb der Organisation ausgeführt werden. Alles was dazu benötigt wird ist eine Workstation mit einem Browser, der einen starken Verschlüsselungs- Algorithmus unterstützt.

7.3.2 Der Zugang zu verschlüsselten Quellen ist sowohl für den **täglichen Betrieb** als auch für **Notfallzugriffe** ausgelegt. In Ausnahmesituationen ist der Benutzerkreis leicht veränderbar. Wenn z.B. ein Mitarbeiter das Unternehmen oder die Abteilung verlässt oder wenn ein Vorgesetzter während seiner Abwesenheit Zugriffsmöglichkeiten für seine Vertreter anfordert.

7.3.3 Die sehr **flexible Systemverwaltung** ermöglicht die Nachbildung jeglicher Organisationsstrukturen und die Einbindung spezieller Organisations- Hierarchien ohne bestimmte Strukturen vorauszusetzen.

7.3.4 Es existieren Mechanismen, um die **Installation und die Einrichtung** des Systems über ein Batch Tool zu erleichtern. Dies ermöglicht eine große Anzahl von Benutzern mit geringem Aufwand aus der NT Datenbank in das FileSeq Key Server System zu implementieren.

7.3.5 **Real time Online Management.** Da FileSeq den Zugang zu Datenobjekten in Echtzeit kontrolliert, erfolgt der Widerruf von Privilegien unmittelbar. Die einzige Ausnahme ist, wenn das Datenobjekt gerade bearbeitet wird und der Schlüssel sich noch im Zwischenspeicher (Non Paged Memory) befindet.

7.3.6 **Reduzierter Management Overhead unter Benutzung von Templates.** Ein sehr wichtiges Leistungsmerkmal ist das „Klonen“ von Datenbankobjekten. Damit lassen sich zum Beispiel Benutzer anlegen, die später nur noch geklont werden müssen. Da die ACL Struktur von FileSeq eine extra Berechtigung (Create Child) beinhaltet, ist es hierdurch auch möglich, Sicherheitslücken zu schließen. Administratoren lassen sich somit von Dateiobjekten und Inhalten ausschließen.

7.3.7 **FileSeq reduziert den Managementaufwand unter Benutzung von rollenbasierenden Standards.** Viele einfache Policies können auf Objektklassen basieren, statt auf einzelnen Objektbeispielen. FileSeq kann einen flexiblen Default Zugang zu Objekten ermöglichen. (z.B. Es lassen sich alle Benutzer administrieren, aber keine Daten lesen). Auch hierduch wird erreicht, dass die Administration keine Einsicht in verschlüsselte Daten erhält.

7.4. Verfügbarkeit und Skalierbarkeit des Systems.

7.4.1 **Replikation:** Der Key Server kann so konfiguriert werden, dass er alle Änderungen, die auf ihm gespeichert werden an alle anderen Partnerserver im Cluster weitergibt. Dies erlaubt einen adressierbaren Fail-Over, wenn einer der Server nicht mehr erreichbar ist. Der FileSeq Client verbindet sich automatisch mit dem nächsten konfigurierten Server, ohne dass ein Eingriff vom Benutzer notwendig ist. In den meisten Fällen synchronisieren sich die Server bei Wiederverfügbarkeit automatisch. Wird ein Server komplett ausgetauscht, lässt sich die gesamte Datenbank von einem anderen Server spiegeln. Diesen Befehl nennt man „Mirror“.

7.4.2 **Hohe Skalierbarkeit:** Das System ist durch Einsatz von zusätzlichen Key Servern erweiterbar und kann somit jederzeit ohne großen Aufwand ausgebaut werden. Ebenso kann der Server im On-Demand Verfahren konfiguriert werden, damit lässt sich eine sehr große Anzahl von Benutzern auf einem System vereinen, ohne weitere Server einsetzen zu müssen.

7.5. Audit

Aufzeichnungen von Zugriffen auf die Datenbank. FileSeq dokumentiert automatisch jeden Zugriff auf alle Objekte (Dateien, User, Gruppen, Rollen). So kann jederzeit nachvollzogen werden, wer, wann, wie oft auf welche Objekte zugegriffen hat. Beispielsweise ist ersichtlich, wenn Rechte eines Users erweitert wurden und auf welche Dateien zugegriffen wurde. Darüber hinaus ist es möglich einzusehen, wer welche Gruppen verändert hat. FileSeq bietet dafür 2 Mechanismen 1. Objektbezogener Audit, (Objektbezogen können alle Zugriffe überprüft werden), 2. Audit Informationen lassen sich mittels einer Suchmaschine aus der gesamten Objektdatenbank herausfiltern.

Berechtigungen für Audit. Nicht jeder Benutzer hat das Recht Audit Informationen einzusehen. Dieses Recht kann anhand der ACL vergeben werden. Die FileSeq ACL bietet hierfür ein eigenes Attribut.

7.6. 4 Augen Prinzip

Für wesentliche Eingriffe in die System Administration von FileSeq sind umfassende Benutzerrechte notwendig. Für die Vergabe dieser Rechte bietet FileSeq ein rollenbezogenes 4 oder 6 Augenprinzip. Meldet sich z.B. ein User als Security Administrator an und ist mit seinen Userdaten authentifiziert, bietet das System eine Liste mit weiteren Usern an, die sich ebenfalls authentisieren müssen. Erst dann ist ein Zugriff auf diese Berechtigung möglich.

8. Zusammenfassung

FileSeq liefert umfassende Datensicherheit für LAN basierte Datei-Server wie auch für lokale Festplatten innerhalb einer Organisation, um die gewünschte Security Policy umzusetzen.

FileSeq bietet eine umfassend skalierbare Architektur mit einer hohen Fehlertoleranz durch die netzwerkbasierende Redundanz, in der sich die Server permanent replizieren.

FileSeq ist ideal für Organisationen, die einen höheren Sicherheitsbedarf haben und es sich nicht leisten können, dass Benutzer, die das Unternehmen verlassen oder die Abteilung wechseln, weiterhin Zugang zu sensiblen Daten erhalten. Genauso ist die Freischaltung von neuen Zugriffsberechtigungen sehr einfach und schnell möglich.

Die Bedienbarkeit von FileSeq ist sehr flexibel und beinhaltet alles, was zur Implementation für große oder kleinere Organisationen nötig ist. Ebenso kann ein zentrales und ein dezentrales Management implementiert werden.

Die Administration ist durch Delegation auf verschiedenen Ebenen möglich.

Die Auditfunktion bietet einen lückenlosen Nachweis und das userspezifische 4-Augen Prinzip verhindert ein Missbrauch der Administrationsoberfläche.

Mit diesen vielfältigen Security Features bietet FileSeq einen einmalig hohen Grad an Datensicherheit.