Inhaltsverzeichnis

1. File Transfer, Access and Management 1
1.1 Funktionalität von FTAM 1
1.2 Einsatzszenarien von FTAM 2
1.3 Abgrenzung zu Alternativen 4
2. Technische Aspekte 5
2.1 Vorbemerkungen 5
2.2 Dateiformate (Document Types) 5
2.3 Hinweise zum Einsatz von FTAM 7
2.4 Ende der Nutzungsdauer von FTAM 8
3. Organisatorische Aspekte 8
3.1 Administration der FTAM-Partner 8
3.2 Absprachen über die Dateiinhalte 9
3.3 Sicherheitsmechanismen 11
4. Anforderungen an Produkte 13
5. Erläuterung zu den Sicherheitsmechanismen 14
5.1 Datenschutz-Maßnahmen 14
5.1.1 Login, Account und Passwort 14
5.1.2 File-Management 15
5.1.3 Die Attribute-Group "Security" 15
5.1.4 Datensicherheitsmaßnahmen 16
5.1.5 Recovery bei FTAM (Quality of Service) 16
5.1.6 Concurrency Control 16

1. File Transfer, Access and Management

1.1 Funktionalität von FTAM

FTAM dient sowohl der Unterstützung des Austauschs vollständiger Dateien als auch dem Lesen und Ändern von Dateiausschnitten, Dateiattributen und Inhaltsverzeichnissen. Um dies unabhängig von der jeweilig im System implementierten Dateiorganisation zu gewährleisten, verwendet FTAM ein logisches Dateisystem, den Virtual Filestore. Dieser Virtual Filestore wird durch die jeweilige Herstellerimplementierung auf das reale System abgebildet. Der Zugang zu den entfernten Dateien erfolgt dabei nicht un-

mittelbar, sondern über Dienste der dort installierten FTAM Software, ist also nicht mit einem allgemeinen Zugang zum entfernten System gleichzusetzen.

FTAM wird in folgenden drei Anwendungsarten eingesetzt:

- **FTAM in automatisierten Verfahren zur Dateiübermittlung**

  FTAM-Implementationen bieten eine Aufrufschnittstelle, so dass die Übermittlung von Dateien bedienerlos in automatisierten Verfahren durchgeführt werden kann. Dadurch ist z.B. die Nutzung von kostengünstigen Tarifen der Telekommunikationsdienste möglich. Die Kommandos für die Übertragung werden in einer Steuerdatei hinterlegt. Auch die Übertragung mehrerer Dateien hintereinander zu festgesetzten Zeitpunkten ist somit erreichbar.

- **FTAM als Unterstützung zur interaktiven Dateibehandlung**

  In der Regel bieten FTAM-Produkte interaktive Schnittstellen mit benutzerfreundlichen Oberflächen. Der Nutzer wird hierdurch in die Lage versetzt, FTAM als Dienstprogramm zu nutzen und mit ihm Dateien auf entfernten Systemen zu bearbeiten.

- **FTAM für die Kommunikation zwischen Anwendungsprogrammen**

  FTAM ermöglicht den Austausch von Dateien zwischen Anwendungsprogrammen in voneinander entfernten Rechnersystemen. Dabei liegt eine Orientierung an dem Client/Server-Modell nahe. Dies kann immer darin Vorteile bringen, wenn marktgängige Standardprogramme an entfernte Systeme angebunden oder in bereits existierende IT-Lösungen integriert werden müssen. Die Anpassung bereits existierender Programme erfordert dabei meist nur einen vergleichsweise geringen Aufwand, wenn ein geeignetes FTAM-Produkt zur Verfügung steht.

Eine ausführliche Darstellung der Funktionalität und Normbezüge zu FTAM befindet sich im FTAM-Modul.

1.2 Einsatzszenarien von FTAM

Einsatzszenarien von FTAM können aus dem Arbeitsalltag der öffentlichen Verwaltung entwickelt werden. Dies erstreckt sich auf praktisch alle Verwaltungsbereiche, wie z. B. Umwelt, Finanzen, Soziales, Verkehr, Statistik.

Ein wichtiges Anwendungsfeld, in dem FTAM zum Einsatz kommt, ist die Dateiübertragung zwischen verschiedenen Gebietskörperschaften:

- Dateiübertragung zwischen Bund und Ländern,

  z. B. Straßenwetterzustands- und Informationssystem (SWIS),

Übermittlung von Umsatzsteuerdaten zwischen Bundesamt für Finanzen und Finanzrechenzentren der Länder;

- Dateiübermittlung zwischen Ländern und Kommunen,

  z. B. Austausch von Gewerbesteuerdaten zwischen nordrhein-westfälischen Kommunen und dem Rechenzentrum für Finanzen NRW.

Im Folgenden werden Beispiele für Einsatzszenarien von FTAM gegeben.

Beispiel 1: Datenaustausch zwischen zwei Systemen

Ein Anwender auf ein Partnersystem A will

- eine Datei von seinem System zu einem Partnersystem transferieren (Senden),
- eine Datei auf dem Partnersystem zum eigenen System transferieren (Holen) oder
- eine Datei auf dem Partnersystem bearbeiten, z. B. Löschen oder Attribute ändern.

Dies kann sowohl interaktiv als auch automatisiert mit Hilfe von Steuerungsdateien (Stapelverarbeitung) erfolgen.

Realisierung

Auf den beteiligten Systemen sind hierzu drei Softwarekomponenten notwendig:

(1) Eine **Steuerungsdatei** (oder eine Benutzeroberfläche bei interaktivem Arbeiten) steuert auf dem System, das die Initiative ergreift (hier System A), die gewünschte Dateibehandlung, legt das gewünschte Partnersystem fest (hier B) und bestimmt die Verarbeitung (Senden, Holen, Manipulieren ...)

(2) Der **Initiator,** eine FTAM-Software auf dem System, das die Initiative ergreift, leitet die Anforderung der Dienstleistung,- (Senden, Holen, Manipulieren von Dateien ...) an das Partnersystem weiter und behandelt ggf. Dateien im eigenen Dateisystem (Ablegen von geholten Dateien, Übertragen von Dateien zum Partnersystem). Der Initiator entspricht in einem Client/Server-Modell dem Client.

(3) Der **Responder,** eine FTAM-Software auf ein System, das als Diensterbringer angesprochen wird, nimmt die Anforderung vom initiierenden System entgegen und führt die gewünschte Dateioperation durch. Der Responder entspricht in einem Client/Server-Modell dem Server.

Beispiel 2: Dezentrale Recherchen in zentralen Datenbanken

Durch Recherchen in zentralen Datenbanken sollen Informationen zu Listen und Tabellen zusammengestellt werden. Diese Informationen sollen dann ohne wesentlichen Zeitverzug vor Ort ausgedruckt oder in der lokal vorhandenen Bürokommunikationsumgebung weiterverarbeitet werden.

Realisierung

Die Recherche selbst erfolgt auf dem zentralen Rechner in einer dezentral nutzbaren Anwendung. Der Anwender erhält Zugang zu dieser zentralen Anwendung über das auf seinem System (dem lokalen Rechner) implementierte virtuelle Terminal. Die Ergebnisse der Datenbankrecherche werden über FTAM vom zentralen zum lokalen Rechner transferiert und automatisch von dort aus in die BK-Umgebung eingebunden.

Die Recherche kann auch automatisiert durchgeführt werden. Die entsprechenden Prozeduren können von der lokalen BK-Umgebung durch Übertragung einer Abfragedatei zum zentralen Rechner angestoßen werden.

Beispiel 3: Zentrale Auswertung dezentral erfasster Daten

In periodischen Abständen (z. B. vierteljährlich) sollen dezentral erfasste Daten zum Zwecke einer Auswertung zentral zusammengefasst werden. Dabei steht im Vordergrund, dass sehr viele dezentrale Erfassungsstellen kostengünstig an die zentrale Stelle angebunden werden.

Realisierung

Um die Grundkosten gering zu halten, ist eine Anbindung der dezentralen Stellen über ein preiswertes Wählnetz vorzusehen. Hier besteht zusätzlich die Möglichkeit, viele Anschlüsse mit ein und derselben Sammelnummer zu versehen und somit die Administration der Datenlieferanten zu vereinfachen.

Zur Leistungssteigerung wird dem zentralen Rechner ein Knotenrechner vorgelagert. Neben dem kontrollierten Senden der Daten nach einer Aufforderung durch den zentralen Rechner ist ebenso auch ein freilaufendes Senden der Datenlieferanten möglich.

1.3 Abgrenzung zu Alternativen

Der Nachrichtenübermittlungsdienst (Message Handling System [MHS}) nach X.400 ist ein etablierter Dienst mit Funktionen für den Nachrichtenaustausch. Er kann sinnvoll auch zum Austausch kleinerer Dateien genutzt werden. FTAM hat Funktionalitäten für andere Anforderungen an Dateiübermittlung, -zugriff und -verwaltung. Es handelt sich damit nicht um konkurrierende Systeme, sondern um einander ergänzende Funktionalitäten.

- FTAM zeichnet sich im Vergleich zu anderen etablierten Datenübermittlungsverfahren insbesondere durch folgende Eigenschaften aus:

- FTAM bietet weitgehende Sicherheitsvorkehrungen sowohl für den Transport von Daten durch Wiederanlaufmechanismen nach Verbindungsunterbrechungen (Restart/Recovery) als auch für den Schutz der Datenbestände selbst durch einstellbare Zugriffsbeschränkungen.

- FTAM erlaubt den gesicherten Transfer von Dateien beliebiger Größe.

- FTAM kann nicht nur Daten an einen entfernten Empfänger versenden, sondern auch entfernte Dateien in kontrollierbarem Umfang lesen oder bearbeiten. Zu berücksichtigen ist, dass der Initiator normalerweise die Übertragungskosten übernimmt.

- FTAM arbeitet zeitlich schritthaltend (synchron). Der Nutzer weiß, wann eine Datei ihren Zielort erreicht hat.

Ergänzend wird auf den Vergleich von MHS und FTAM in der ersten Fassung von EPHOS, S.12 f., verwiesen (vgl. Anhang C).

2. Technische Aspekte

2.1 Vorbemerkungen

Alle Klauseln aus EPHOS, in denen FTAM-Funktionen obligatorisch gefordert werden, sind bei der Beschaffung von Produkten zu berücksichtigen. Zu optional wählbaren Funktionen werden nachfolgend - soweit möglich - Empfehlungen gegeben.

Wegen der umfangreichen Möglichkeiten von FTAM können sich die Empfehlungen nur auf wesentliche Funktionen beschränken. Soweit nicht technische oder organisatorische Gründe ein anderes Vorgehen nahelegen, sollen sie vor allem helfen, den Ersteinsatz von FTAM zu erleichtern.

2.2 Dateiformate (Document Types)

Generell unterscheidet FTAM zwischen verschiedenen Typen von Dateien. Die Festlegung von Dateitypen ist für unterschiedliche Einsatzarten wie z. B. Übertragung von Textdateien oder Transport von Binärdateien erforderlich. So kann die Darstellung von Zeichen auf den verschiedenen Systemen differieren und muss konvertiert werden. Wenn z. B. in EBCDIC-Format erstellte tabellarische Daten in einer Datei per Dateitransfer zu einem Unix-System übermittelt und auf dem Bildschirm ausgegeben werden sollen, leistet FTAM eine Umsetzung der Umlaute.

Auf eine Erläuterung aller durch FTAM festgelegten Dateiformate wird an dieser Stelle verzichtet. Eine vollständige Auflistung kann dem FTAM-Modul, Abschnitt II.1.2., entnommen werden.

Nachfolgend werden zu einigen Dateiformaten Anmerkungen gemacht und Empfehlungen ausgesprochen.

Im Regelfall wird der Dateitransfer mit den Dateiformaten FTAM-1 und FTAM-3 erfolgen können, da sie den größten Teil der Anforderungen abdecken:

FTAM-1
Textdatei ohne weitere Struktur, Zeichen werden in die jeweilige lokale Datendarstellung umgesetzt.

FTAM-3
Binärdatei ohne weitere Struktur, wird transparent von einem System zum anderen übermittelt.

Empfehlung 1:

Für Dateien, die nur druckbare Zeichen enthalten (z.B. ohne Formatierungselemente), sollte FTAM- 1 genutzt werden. Siehe hierzu auch Empfehlung 7.

"FTAM-1" sollte angewendet werden für alle Dateien, die durch IA5 darstellbar sind (einfache Textdateien, SQL-Strings, PostScript Dateien etc.).

"FTAM-3" sollte eingesetzt werden für alle nicht durch FTAM-1 übertragbare Dateien (Dokumente aus Textsystemen mit herstellerspezifischen Steuerzeichen, Grafiken, Binärprogramme).

Für die Dateiformate INTAP-1 und NBS-9 gilt:

INTAP-1
Geeignet für die Übertragung von sehr großen Binärdateien. Es wird eine Datenkompression/ -dekompression durchgeführt. Dieser erhebliche Aufwand lohnt sich nur bei Massendaten wie z. B. der Pixelübertragung von Fernerkundungsbildern.

NBS-9
Lesen von Dateiverzeichnissen in anderen Systemen

Empfehlung 2:

Beim Einsatz der Dateiformate INTAP-1 und NBS-9 ist bereits bei Beschaffung zusätzlich zur Klausel 13 der Interoperabilitätsnachweis für die vorgesehenen IT-Systeme zu fordern.

2.3 Hinweise zum Einsatz von FTAM

Die Handhabung von FTAM in Fällen einfachen Dateitransfers lässt sich für den Neuanwender durch die Beachtung der nachstehenden Empfehlungen deutlich erleichtern.

In FTAM können diverse Passwörter wie Filestore-Password, Create- und Access-Password vergeben werden. Die Eingabe dieser Passwörter kann in verschiedenen Formen erfolgen (siehe Klausel 7).

Empfehlung 3:

Für Passwörter sollte ausschließlich GraphicString verwendet werden.

Der Virtual Filestore lässt eine stark strukturierte Namensgebung zu. Dies kann bei der Abbildung auf reale Dateisysteme (z.B. DOS) auf Schwierigkeiten stoßen.

Empfehlung 4:

In Ergänzung zu Klausel 7 des FTAM-Moduls sollte bei Anwendungen die Beschränkung des Dateinamens auf 12 Zeichen gemäß DOS-Konvention eingehalten werden, wenn PC-Einsatz vorgesehen ist. Klausel 10, die Hinweise im FTAM-Modul, Abschnitt II.3.7. und Empfehlung sollte berücksichtigt werden.

FTAM bietet als Sicherungsfunktion die Möglichkeit, bei fehlerhafter Übertragung eine Teilwiederholung zu starten, anstatt die gesamte Datei neu zu versenden.

Empfehlung 5:

Für die Übertragung von Dateien mit einer Größe ab 50OkB ist der Einsatz von Restart/Recovery empfehlenswert. Bei kleineren Dateien ist der Einsatz von Restart/Recovery unter Durchsatzgesichtspunkten zu prüfen.

FTAM bietet weiterhin die Möglichkeit, konkurrierende Zugriffe auf Dateien zu steuern. Auch ist es möglich, das Inhaltsverzeichnis eines entfernten Systems zu lesen oder die Verfügbarkeit von Dateien zu überprüfen. Diese Zugriffsmechanismen sind aber stark vom realen Dateisystem und der Implemen-

tierung von FTAM durch den Hersteller abhängig, so dass hier die Interoperabilität nicht immer gegeben ist.

Empfehlung 6:

Die zusätzlichen Optionen Concurrency Control und File Availability) sollten nur für homogene Systeme oder für Systeme mit Interoperabilitätsnachweis eingesetzt werden.

Der Dokumententyp FTAM-1 setzt verschiedene Zeichensätze (EBCDIC, ISO 8 Bit etc.) beim Transfer ineinander um. Diese Umsetzung ist i.d.R. nur mit Einschränkungen möglich. Weiterhin können Escape-Sequenzen durch die jeweilige Herstellerimplementierung unterschiedlich interpretiert werden.

Empfehlung 7:

Für die Übertragung mittels FTAM-1 sollte senderseitig nur der Zeichensatz IA5 eingesetzt werden. Sind deutsche Umlaute notwendig, sollte GraphigString verwendet werden. Escape-Sequenzen sind zu vermeiden.

2.4 Ende der Nutzungsdauer von FTAM

In der technischen Arbeitsgruppe für den elektronischen Datenaustausch für das Gesundheits- und Sozialwesen wurde in der Sitzung vom 30.10.2014 beschlossen, die Nutzungsdauer von FTAM per ISDN zum

31.12.2017

einzustellen.
Die Gründe für das Einstellen der Verfügbarkeit sind unter anderem darin begründet, dass die Deutsche Telekom den ISDN Dienst zum gleichen Zeitraum einstellen wird.

3. Organisatorische Aspekte

3.1 Administration der FTAM-Partner

In FTAM implementierte Schutzmechanismen sind in organisatorische Konzepte einzubinden. User-Id und Passwörter sind zu verwalten. Je nach Anforderung (Holen oder Senden) kann dies erheblichen Auf-

wand verursachen. Eine zentrale Stelle muss z.B. für den Dateitransfer zu verschiedenen Partnern eine Vielzahl von Passwörtern verwalten, dezentrale Stellen nur das zentrale Passwort.

Der Initiator übernimmt normalerweise die Kommunikationskosten.

Empfehlung 8:

Für den Fall, dass eine zentrale Stelle Dateien zu vielen dezentralen Stellen transferieren muss, sollte geprüft werden, ob diese Dateien nicht verschickt werden (zentrale Stelle ist Initiator), sondern statt dessen von den Partnern geholt werden können (dezentraler Partner ist Initiator).

3.2 Absprachen über die Dateiinhalte

FTAM legt die Inhalte der Dateien im Detail nicht fest. Die hohe Flexibilität von FTAM kann bei fehlenden Absprachen zwischen Absender und Empfänger zu Problemen führen.

Grundsätzlich sollten die folgenden Punkte zwischen Empfänger und Sender entsprechend den Anregungen des EPHOS-Handbuches berücksichtigt werden.

Bei Dateien vom Typ FTAM-1 ist das Zeichen bzw. die Zeichenkette für den Zeilenabschluss und Beginn einer neue Zeile nicht eindeutig, da es betriebssystemabhängige Implementationen gibt. So können die Zeichen für den Rücksprung an den Zeilenanfang (carriage return <cr>) oder für den Zeilenvorschub (line feed <lf>) einzeln, in Kombination oder auch andere Zeichen verwendet werden. Im FTAM-Modul wird vorgeschlagen, grundsätzlich sowohl auf Sender- als auch auf Empfängerseite zur Zeilenbegrenzung immer die Kombination <CR><LF> zur Zeilenbegrenzung zu verwenden (Klausel 12, Absatz 11.3.9.)

Empfehlung 9:

Zur Zeilenbegrenzung sollte in Textdateien <CR><LF> verwendet werden.

Wird diese Empfehlung beim Einsatz von FTAM berücksichtigt, ist für einfache, zeichenorientierte Dateien mit 1A5 Zeichensatz keine weitere Absprache zu den Inhalten erforderlich,

Die Möglichkeiten von FTAM lassen jedoch auch Informationstausch zu, bei dem eine Absprache zwingend ist. So können sich fragende und antwortende Stellen z. B. darauf einigen, dass eine FTAM-1-

Datei SQL-Abfragen an eine bestimmte Datenbank enthält, die mit einer FTAM-3-Datei als Recherche-Ergebnis beantwortet wird.

Der Stand des Normungsprozesses bei EDI/EDIFACT und ODA/ODIF macht einen Einsatz des entsprechenden Dokumentenaustausches auch in der öffentlichen Verwaltung möglich. Hier wird in EPHOS angeregt. den Dateityp FTAM-3 zur Übertragung zu nutzen.

Empfehlung 10:

Wenn möglich, sollten Inhalte von Dateien in genormten Formaten gestaltet werden:

- EDI/EDIFACT für "formularhafte" Dateien wie Rechnungen, Bestellungen, Statistiken usw.
- ODA/ODIF für formatierte/formatierbare, komplexe Textdokumente
- SQL für Datenbank-Abfrage-Statements

Da FTAM nur den Transportmechanismus beschreibt, besteht keine Möglichkeit, den Inhalt von Dateien beim Versand durch FTAM über die Dienstelemente mitzuteilen. Es ist jedoch über den Dateinamen eine einfache Inhaltszuordnung möglich.

Empfehlung 11:

Angaben über die Weiterverarbeitung sollten im Dateinamen enthalten sein. Folgende Suffixe sind zur Beschreibung des Inhaltes zu verwenden:

- ".EDI" für EDI/EDIFACT-Nachrichten
- ".ODA" für ODA-Dokumente
- ".SQL" für Datenbank-Abfragen
- ".IA5"für einfache Textdateien (IA5 - Dokumente)
- ".TIF" für Grafikdaten im TIF-Format
- ".PS1" für Postscript, Level 1

- ".PS2" für Postscript, Level 2

Weitere Suffixe sind bei Bedarf zwischen den Parteien zu vereinbaren.

Hinweis:

Ausführbare Dateien sollten aus Sicherheitsgründen (Viren etc.) nicht ausgetauscht werden.

Für weitere Details wird auf die EPHOS-Module EDI und Dokumentenaustausch verwiesen.

In einer Vielzahl von Fällen sind hierüber hinaus Absprachen über FTAM-Eigenschaften unerlässlich, da sie bei einer "Regelbeschaffung" nicht berücksichtigt werden, sondern unmittelbar vom zu realisierenden IT-Vorhaben abhängen. Als Beispiele seien die Unterstützung des griechischen Alphabets bei FTAM-1 entsprechend ISO-IR 126, INTAP-1 für binäre strukturierte Massendaten sowie Datenreduktionsverfahren erwähnt.

3.3 Sicherheitsmechanismen

Die heutige IT-Landschaft zeichnet sich vielfach durch heterogene dezentrale Systeme aus. Datenschutz- und Sicherheitseinrichtungen werden entsprechend proprietär vorgehalten.

Jedes dezentrale System verwaltet seine eigenen Zugriffsrechte, um Fremdeinwirkungen möglichst zu vermeiden, indem durch organisatorische Vorkehrungen sichergestellt wird, dass

- nur Berechtigte eingetragen werden,
- abgelaufene Berechtigungen rechtzeitig gelöscht werden und
- Eintragungen von anderen dezentralen Systemen nicht automatisch erfolgen können.

Im Zusammenspiel mit anderen dezentralen System ist es ratsam, je nach Bedrohungslage geeignete Sicherheitssysteme zu nutzen. Für FTAM kann beispielhaft genannt werden:

- Sichere Gestaltung der Übertragung (etwa durch X.25 oder ISDN) Ggf. Bildung von Teilnehmerklassen
- Absicherung auf FTAM-Ebene mit User-Id und Passwort
- Zugriffskontrolle auf Anwendungsebene

- Bei Bedarf Erhöhung der Sicherheit durch Verschlüsselung auf der Leitungs- und Anwendungsebene

Die Dateiübermittlung gemäß FTAM zu anderen IT-Systemen über WAN und LAN/WAN kann auf der Basis von X.25 erfolgen. Hierbei können die angebotenen Sicherheitsfunktionen in X.25 je nach Bedarf aktiviert werden. Dazu gehören:

- Zulassung von Wählleitungen nur für geschlossene Benutzergruppen
- Eindeutige X.121-Adressierung
- Bildung von geschlossenen Benutzergruppen innerhalb der X.121-Adressierung
- Evtl. zusätzlicher Schutz durch Einsatz von leitungsbezogenen Verschlüsselungssystemen

FTAM hat eine File-Zugriffskontrolle. Diese Absicherung wird durch User-Id und Passwort erreicht. So kann etwa bei der Verarbeitung sensibler Daten (z.B. Personalaktendaten) durch eine File-Zugriffskontrolle den Anforderungen des Datenschutzes Rechnung getragen werden.

Empfehlung 12:

Die Zugriffskontrolle auf Anwendungsebene ist ein zusätzlicher Sicherheitsfilter und sollte nach Möglichkeit genutzt werden.

Eine weitere Erhöhung der Sicherheit ist durch eine Verschlüsselung auf Anwendungsebene zu erreichen. Hierbei ist die Organisation der Schlüsselverwaltung eindeutig festzulegen, was häufig einen großen Aufwand bedeutet.

Empfehlung 13:

Nur bei zwingenden Anforderungen wie z. B. bei der Verarbeitung sensibler personenbezogener Daten sollte der Dateiinhalt verschlüsselt werden. Die verschlüsselten Dateien sollten mit FTAM-3 übertragen werden.

4. Anforderungen an Produkte

Bei den FTAM-Produkten ist mittlerweile eine Auswahlmöglichkeit gegeben. Die Anforderungen an die Produkte werden entsprechend dem IT-Vorhaben festgelegt. Geboten wird ein weites Spektrum an Möglichkeiten, die in EPHOS dargestellt werden und je nach Anforderungen zusammengefasst werden können.

EPHOS bietet hierzu unterschiedliche Profile an. Sie reichen von kleinen Anwendungen, bei denen die Initiator-Funktion bei den Datenlieferanten ausreicht, bis zu großen Gesamtsystemen, die die FTAM-Funktionen in ihrer Gesamtheit benötigen. Nach einem "Bausteinverfahren" werden entsprechend den Anforderungen die einzelnen Klauseln für ein Leistungsverzeichnis zusammengefügt. Dieses Verfahren kann zur Folge haben, dass die beschaffende Stelle einen Anbieter auswählt, der nur eine Untermenge der FTAM-Funktionen anbietet.

Empfehlung 14 :

Bei der Beschaffung soll über die benötigten Klauseln hinaus die Verfügbarkeit der übrigen FTAM-Funktionen vertraglich zugesichert werden.

Im Betrieb sollten hingegen nur, die unbedingt notwendigen Funktionen eingesetzt werden.

In EPHOS enthaltene Klauseln zu den Themen

→ unzureichender Standard bei unstrukturierten Textdateien [Klausel 21]

→ Normkonformität und Interoperabilität [Klauseln 22 und 23] und

→ Nutzerfreundlichkeit [Klauseln 17, 19, 20a (mindestens), 20b, 20c (nach Erfordernis)]

sind immer in Leistungsverzeichnissen aufzunehmen.

Dabei sollte darauf geachtet werden, dass die Interoperabilität mit FTAM-Produkten Dritter auf den bereits vorhandenen Systemen sichergestellt ist. Dadurch werden auch bei einer späteren Anforderung, auf diesen Systemen FTAM einzusetzen, die Investitionen gesichert.

Hinsichtlich einer ergonomischen Oberfläche für Nutzer und Systemverwalter wird folgende Empfehlung ausgesprochen.

Empfehlung 15 :

Eine menügesteuerte, möglichst grafische Oberfläche sollte gefordert werden.

Anwendungen erfordern u. U. die Verwaltung einer Vielzahl von Adressinformationen. Hier bietet sich, statt eigenständiger Implementierungen, der Rückgriff auf normgerechte Verzeichnisdienste zur Verwaltung solcher Adressbestände an. Adressänderungen sollten während des Betriebes durchgeführt werden können. Damit ist es möglich, Adressen zu löschen, zu ändern und hinzuzufügen, ohne dass die laufenden FTAM-Anwendungen hiervon betroffen werden.

Ein normgerechter Verzeichnisdienst ist X.500. Ein Profil zur Nutzung von X.500 aus FTAM heraus ist noch in Entwicklung (FDI3). Hierzu werden im FTAM-Modul, Abschnitt 1.2.4.3. und EPHOS-Modul Directory Services nähere Angaben gemacht.

Empfehlung 16 :

Es sollte gefordert werden, dass die Verwaltung von Adresssinformationen normgerecht (X.500 basiert) erfolgen kann. Ggf. sollte eine Ablösung der herstellereigenen Lösung vertraglich zugesichert werden.

5. Erläuterung zu den Sicherheitsmechanismen

Die gegenwärtig auf dem Markt verfügbaren FTAM-Produkte unterscheiden sich hinsichtlich des implementierten Funktionsumfanges und bieten somit auch auf dem Gebiet des Datenschutzes und der Datensicherheit unterschiedliche Funktionalität. Vor dem Einsatz von FTAM sollte das einzusetzende Produkt intensiv auf die geforderte Funktionalität hin untersucht werden.

Im Folgenden soll auf die in den FTAM-Normen definierten Festlegungen zu den Bereichen Datenschutz und Datensicherheit eingegangen werden.

Unter Datenschutz werden technische und organisatorische Maßnahmen bei der automatisierten Verarbeitung personenbezogener Daten zusammengefasst (i.S.d. BDSG oder vergleichbarer Regelungen)

5.1 Datenschutz-Maßnahmen

5.1.1 Login, Account und Passwort

Die erste Möglichkeit zum Schutz der Daten ergibt sich bei der Verbindungsaufnahme zwischen FTAM-Initiator und Responder. Dabei wird entschieden, ob der Nutzer berechtigt ist, Zugriff auf das System zu erhalten. Dieser Verbindungsaufbau erfolgt beim Einsatz von FTAM mittels der PDU (protocol-data-unit). Die PDU enthält die Parameter

- initiator-identity
- account
- filestore-password

Der Parameter initiator-identity ist mit dem weithin bekannten login gleichzusetzen und spezifiziert den Namen des Nutzers, der den Aufbau einer FTAM-Verbindung verlangt. Das filestore-password berechtigt den Nutzer zum Zugriff auf das Zielsystem. Der Parameter account dient üblicherweise zu Abrechnungszwecken. Alle drei genannten Parameter sind optional. Der FTAM-Responder legt fest, welche von diesen 3 Parametern benötigt werden, um dem Nutzer den Zugang zum System zu ermöglichen.

5.1.2 File-Management

Auf den Files im Filestore des FTAM-Responders können verschiedene Aktionen ausgeführt werden. Diese Aktionen werden über eine Steuerungsvariable erlaubt oder verboten. Diese Steuerungsvariable heißt permitted actions. Sie wird vom FTAM-Initiator gesendet und beim Anlegen eines Files im Responder-Filestore diesem File zugeordnet. Die geforderten Aktionen des Initiators werden vorn Responder entgegengenommen, können dort aber auch nur partiell unterstützt werden, d.h. nicht alle geforderten Aktionen werden erlaubt. Dieser Zugriffsschutz ist mit den Zugriffsrechten im Unix-Filesystem vergleichbar, jedoch wesentlich umfangreicher. Das Permitted-Actions-Attribut gestattet das Erlauben bzw. Verbieten folgender Aktionen

- read
- insert
- replace
- extend
- erase
- read-attribute
- change-attribute
- delete-file

5.1.3 Die Attribute-Group "Security"

Beim Verbindungsaufbau werden innerhalb der PDU (protocoll-data-unit) die für die aufzubauende Verbindung gültigen Parameter ausgehandelt (vgl. Login, Account und Passwort). Im Responder-Filestore wird jedem dort abgespeicherten File eine Menge von Attributen zugeordnet. Die Anzahl der in dieser Menge enthaltenen Attribute wird mit dem Parameter Attribute-Group beim Verbindungsaufbau ausgehandelt. Bezüglich Datenschutz steht hier die Attribute-Group "security" zur Verfügung. Diese gestattet die Verwendung der beiden Parameter

- access-control
- legal-qualifications

zur Verwaltung von File-Zugriffen.

Der Parameter Access-Control gestattet die Vergabe von Passwörtern für die Ausführung einzelner Aktionen (vgl. "File Management") über einen File.

5.1.4 Datensicherheitsmaßnahmen

Im Folgenden soll die Funktionalität von FTAM hinsichtlich der Sicherheit bei der Datenübertragung und der Arbeit mit Dateien im FTAM-Filestore beschrieben werden. Die im Folgenden dargestellten Funktionen sind unter den Begriffen aufgeführt, die in der FTAM-Norm verwendet werden.

5.1.5 Recovery bei FTAM (Quality of Service)

Beim Verbindungsaufbau kann der Parameter FTAM-Quality-of-Service innerhalb der PDU ausgehandelt werden. Der ausgehandelte Parameter gibt an, welche Recovery-Maßnahmen, wenn nötig, eingeleitet werden sollen. Es stehen für diesen Parameter die Werte

- no-recovery
- class-1-recovery
- class-2-recovery
- class-3-recovery

Class 1 bis Class 3 gibt an, um welche Fehler es sich handelt. Diese werden genau in der FTAM-Norm spezifiziert.

5.1.6 Concurrency Control

Der optionale Parameter Concurrency Control verwaltet den parallelen Zugriff auf den Datenbestand. Mit Hilfe des Parameters wird festgelegt, wer eine bestimmte Aktion in einem File ausführen darf.

Für jede Aktion kann dabei einer der folgenden Werte gesetzt werden:

- not required Für den Initiator gesperrt. Alle anderen dürfen.
- shared Der Initiator darf. Alle anderen auch.
- exclusive Der Initiator darf. Alle anderen nicht.
- no access Diese Aktion ist für alle gesperrt.

Der Concurrency-Parameter bezieht sich auf die bereits erwähnten Aktionen.