PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 :		(11) Internationale Veröffentlichungsnummer: **WO 00/51288**
H04L 12/00	**A2**	(43) Internationales Veröffentlichungsdatum: 31. August 2000 (31.08.00)

(21) **Internationales Aktenzeichen:** PCT/DE00/00517

(22) **Internationales Anmeldedatum:** 24. Februar 2000 (24.02.00)

(30) **Prioritätsdaten:**
199 08 429.7 26. Februar 1999 (26.02.99) DE

(71) **Anmelder** *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) **Erfinder; und**
(75) **Erfinder/Anmelder** *(nur für US)*: KITTL, Herwig [AT/AT]; Schönfelderstr. 13/1/3, A–2284 Untersiebenbrunn (AT). LAUER, Maria [DE/DE]; Ludwig–Weiss–Str. 45, D–82275 Emmering (DE). MÜLLER, Klaus–Dieter [DE/DE]; Wilbrechtstr. 85, D–81477 München (DE). NAUER, Bernhard [DE/DE]; Fuggerstr. 4, D–81373 München (DE). GLÖSMANN, Josef [AT/AT]; Gerichtsgasse 1C/6/12, A–1210 Wien (AT).

(74) **Gemeinsamer Vertreter:** SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D–80506 München (DE).

(81) **Bestimmungsstaaten:** CN, DE, US.

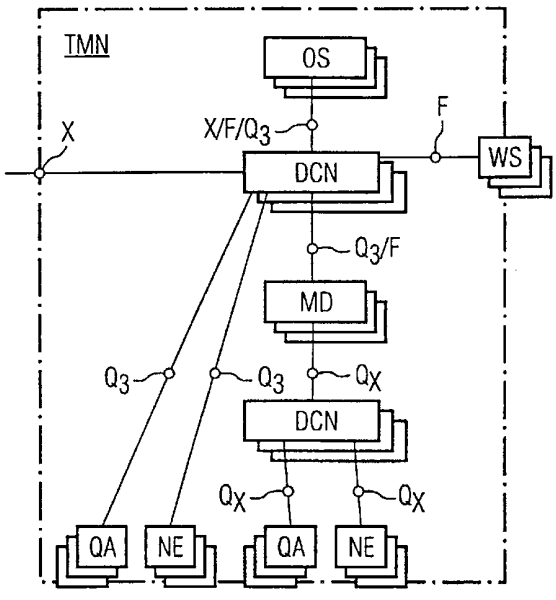
Veröffentlicht
Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) **Title:** MODIFICATION OF THE ITU–T RECOMMENDATION X.741 FOR A UNIFORM ACCESS PROTECTION OF MANAGED OBJECTS AND FILES

(54) **Bezeichnung:** MODIFIZIERUNG DER ITU–T RECOMMENDATION X.741 FÜR EINEN EINHEITLICHEN ZUGRIFFSSCHUTZ AUF MANAGED OBJECTS UND DATEIEN

(57) **Abstract**

The ITU–I recommendation X.741 is provided for access protection of managed objects. According to the invention, said recommendation is modified in such a way that it can also be used for access protection of files. This results in a uniform access protection with uniform handling and uniform management. Particular embodiments of the invention can be obtained by completing the existing object model for access protection of managed objects by an additional object model for access protection of files, by enlarging the existing object model for access protection of managed objects by subclasses for access protection of files and by enlarging the existing object model to form a novel object model for managed objects and files. The inventive model can be realised as an independent model for file protection.



(57) **Zusammenfassung**

Die bislang nur für einen Zugriffsschutz auf Managed Objects vorgesehene ITU–T recommendation X.741 wird derart modifiziert, daß sie auch für einen Zugriffsschutz auf Dateien geeignet ist, womit sich ein einheitlicher Zugriffsschutz mit einheitlicher Handhabung und einheitlichem Management bietet. Besondere Ausführungsformen des Anmeldungsgegenstandes sind durch Ergänzung des bestehenden Objektmodells für einen Zugriffsschutz auf Managed Objects um ein weiteres Objektmodell für einen Zugriffsschutz auf Dateien, Erweiterung des bestehenden Objektmodells für einen Zugriffsschutz auf Managed Objects um Subclasses für einen Zugriffsschutz auf Dateien und Erweiterung des existierenden Objektmodells zu einem neuen Objektmodell für Managed Objects und Dateien gegeben. Der Anmeldungsgegenstand ist als eigenständiges Modell für den Dateischutz ausführbar.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Beschreibung

Modifizierung der ITU-T recommendation X.741 für einen einheitlichen Zugriffsschutz auf Managed Objects und Dateien

Die ITU-T (International Telecommunication Union, Telecommunication Standardization Sector) recommendation X.741 ist derzeit nur für einen Zugriffsschutz von Managed Objects vorgesehen.

Der Anmeldungsgegenstand betrifft ein Verfahren zur Realisierung eines einheitlichen Zugriffsschutzes auf Managed Objects und Dateien basierend auf der ITU-T recommendation X.741 umfassend die Merkmale des Oberbegriffs des Anspruchs 1, 4 oder 5.

Die ITU-T recommendation M.3010 beschreibt die Architektur und die Schnittstellen eines Telecommunication Management Network TMN. Die Schnittstelle zwischen Operations Systems und Network Elements wird mit Q_3, diejenige zwischen den Operations Systems mit X bezeichnet. Um diese beiden TMN-Schnittstellen zu realisieren, wurden das in der ITU-T rec. X.710/X.711 beschriebene Common Management Information Protocol (CMIP) entwickelt und Managed Objects eingeführt, in denen die Management-Informationen gespeichert sind. Mit CMIP werden die Managed Objects administriert. Die Managed Objects werden entsprechend der ITU-T rec. X.720 bis X.722 mit GDMO (Guidelines for the Definition of Managed Objects) beschrieben. In der Praxis reicht diese Realisierung der Q_3- und X-Schnittstelle nicht aus. Für die Speicherung von Massendaten (z.B. Accounting-Daten) werden Files verwendet, auf die mittels File Transfer (z.B. per File Transfer Access Method FTAM oder File Transfer Protocol FTP) zugegriffen wird. In der TMN Standardisierung (z.B. bei ETSI) wurden für die Realisierung der Q_3- und X-Schnittstelle sowohl CMIP als auch FTAM betrachtet.

Der Zugriffsschutz auf die Managed Objects ist in der ITU-T rec. X.741 beschrieben. Die ITU-T rec. X.741 interpretiert und wendet das in der ITU-T X.812 beschriebene Modell für eine Zugriffskontrolle auf Management-Applikationen an, die CMIP als Management-Protokoll nutzen. Sie definiert ein Objektmodell mit dem Zugriffsrechte auf Objektklassen-, Objektinstanzen-, Attribut- und Attributwertebene verwaltet werden können. Eine direkte Anwendung der ITU-T rec. X.741 auf Dateizugriffe ist nicht möglich.

Bisher wurde die Zugriffskontrolle auf Managed Objects und auf Dateien auf unterschiedliche Art und Weise gelöst. Beispielsweise wird in dem herstellerspezifischen Telekommunikationsvermittlungssystem EWSD (Elektronisches Wählsystem Digital) die Zugriffskontrolle auf Managed Objects auf Basis der ITU-T rec. X.741 ausgeführt, wohingegen für die Dateizugriffskontrolle eine proprietäre Lösung eingesetzt wird.

Dem Anmeldungsgegenstand liegt das Problem zugrunde, das in der ITU-T rec. X.741 beschriebene Objektmodell so anzupassen, daß es einheitlich sowohl für einen Zugriffschutz von Managed Objects als auch für einen Zugriffsschutz von Dateien verwendet werden kann.

Das Problem wird bei einem durch die Merkmale des Oberbegriffs umrissenen Gegenstand gemäß Anspruch 1, 4 oder 5 durch die Merkmale des kennzeichnenden Teils des Anspruchs 1, 4 bzw. 5 gelöst.

Der Anmeldungsgegenstand macht sich die Erkenntnis zu nutze, daß die in der ITU-T rec. X.741 beschriebenen Schemata (Access Control List Schemata, Label based Schemata, Context based Schemata oder Capacity based Schemata) für eine Zugriffskontrolle auf die Managed Objects auf eine Dateizugriffskontrolle übertragen werden können. Der Anmeldungsgegenstand bildet die ITU-T rec. X.741 derart weiter, daß sie für einen Zugriffsschutz von Dateien, auf die per File Trans-

fer (z.B. mit FTAM oder FTP) zugegriffen wird, brauchbar gemacht wird. Der Zugriffschutz auf Managed Object Classes und auf Dateien wird in einheitlicher Form realisiert, womit sich einem Operator für den Zugriffsschutz eine einheitliche Handhabung (Look and Feel) und ein einheitliches Management bietet. Bei der Realisierung des einheitlichen Zugriffsschutzes sind Synergieeffekte erzielbar. Der durch den Anmeldungsgegenstand gegebene Dateizugriffsschutz ist unabhängig vom Datei-Management-System und von der Zugriffsmethode. Er ist beispielsweise für FTAM (ISO 8571) und für FTP (RFC (Request for Comments)959 und 1123) verwendbar. Der Anmeldungsgegenstand ist als eigenständiges Modell für den Dateischutz ausführbar.

Vorteilhafte Weiterbildungen des Anmeldungsgegenstandes sind in den Unteransprüchen angegeben.

Gemäß einer besonderen Ausführungsform des Anmeldungsgegenstandes bleibt das in der ITU-T rec. X.741 definierte Objektmodell unverändert und wird allomorph um die für den Dateizugriffsschutz benötigten Subclasses erweitert. Dabei bleibt das Originalmodell unverändert, wodurch eine Änderung der Implementierung nicht notwendig ist.

Der Anmeldungsgegenstand wird im folgenden als Ausführungsbeispiel in einem zum Verständnis erforderlichen Umfang anhand von Figuren näher erläutert. Dabei zeigen:

Fig 1 eine prinzipielle Darstellung der allgemeinen Beziehung eines Telekommunication Management Netz zu einem Telekommunikationsnetz

Fig 2 ein Ausführungsbeispiel für die vereinfachte physikalische Architektur eines Telekommunication Management Netz' und

Fig 3 Beziehungen in einem Objektmodell.

In den Figuren bezeichnen gleiche Bezeichnungen gleiche Elemente.

ITU-T rec. M.3010 beschreibt die Architektur und die Schnittstellen eines Telecommunication Management Network TMN. Die Schnittstelle zwischen Operations Systems und Network Elements wird mit Q_3, diejenige zwischen den Operations Systems mit X bezeichnet.

Fig 1 zeigt allgemeine Beziehungen eines Telekommunication Management Netz TMN zu einem Telekommunikationsnetz TN. Ein Data Communication Network DCN ist mit mehreren Operating Systems OS, einer Workstation WS, einem anderen Telekommunication Management Netz oTMN (für: other Telekommunication Management Netz) und mehreren Vermittlungs-Einrichtungen EX (für: Exchange) sowie mehreren Übertragungs- Einrichtungen TR (für: Transmission) verbunden. Die Vermittlungs-Einrichtungen EX und die Übertragungs- Einrichtungen TR, die einander abwechselnd miteinander verbunden sind, sind dem Telekommunikationsnetz TN zugehörig. Im übrigen sind mit dem Telekommunikationsnetz stellvertretend für eine Vielzahl von Telekommunikationsendeinrichtungen eine Datenverarbeitungseinrichtung TEPC (für: Telekommunikationsendeinrichtung Personal Computer) und eine Fernsprecheinrichtung TEF (für: Telekommunikationsendeinrichtung Fernsprecher) verbunden.

Bei der in Fig 2 dargestellten Architektur des Telekommunication Management Netz' TMN ist das Datenkommunikationsnetz DCN über eine Schnittstelle X, eine Schnittstelle F bzw. eine Schnittstelle Q_3mit einem oder mehreren Operating Systems OS, über eine Schnittstelle F mit einer oder mehreren Workstations WS, über eine Schnittstelle Q_3 bzw. eine Schnittstelle F mit einem oder mehreren Einrichtungen MD (für: Mediation Device), über eine Schnittstelle Q_3 mit einem oder mehreren Network Elements NE, über eine Schnittstelle Q_3 mit einem oder mehreren QA verbunden und ist über eine Schnittstelle X mit einem nicht näher dargestellten anderen Telekommunication Management Netz verbindbar. Die Einrichtung MD ist über eine Schnittstelle Q_x mit einem oder mehreren Einrichtungen QA

(für: Q Adaptor) sowie eine Schnittstelle Q_x mit einem oder mehreren Network Elements NE verbunden.

Die in der ITU-T rec. X.741 beschriebenen Schemata (Access Control List Schemata, Label based Schemata, Context based Schemata oder Capacity based Schemata) für eine Zugriffskontrolle auf die Managed Objects werden anmeldungsgemäß auf eine Dateizugriffskontrolle übertragen. Dafür müssen die im Objektmodell der ITU-T rec. X.741 beschriebenen CMIP-Operationen auf die Dateizugriffe angepaßt werden. Diese Anpassungen basieren im Wesentlichen auf einer Erweiterung des Behaviour, einer Erweiterung der Attribut-Syntax und der Definition neuer Attribute und Actions. Im Einzelnen werden folgende Änderungen vorgenommen:

Access control rules object class
defaultAccess Attribut: die Attribut-Syntax wird erweitert auf die Dateizugriffsmethoden wie "create", "delete", "read", "write", "readAttributes", "execute", "noOperation" ... denialGranularity Attribut: die Attribut-Syntax wird erweitert um Werte, die sich auf die Granularität des Dateizugriffs beziehen, wie z.B. "fileOperation" und "singleFile". Das Behaviour des Attributs wird entsprechend angepaßt.

Rule object class
Behaviour: Das Behaviour wird erweitert um folgenden Satz: "Wenn das targets list Attribut Dateien identifiziert, dann muß das initiators list Attribute Initiatoren im Kontext eines Dateizugriffsschemas identifizieren."

Targets object class
Behaviour: "managed objects" sollte erweitert werden auf "managed objects or files".Die Objektklasse wird erweitert um Attribute zur Datei-Auswahl (wie z.B. fileType, fileName) und durch optionale Attribute, in denen Bedingungen für die Dateiauswahl formuliert werden können (wie z.B. fileFilter, fi-

lePatternList zur Identifizierung von Dateinamen gemäß eines definierten Musters).
OperationsListPackage:
operationsList Attribut: die Attribut-Syntax bezieht sich auf den ASN.1 (Abstract Syntax Notation No 1) Typ "operationType". Dieser Typ wird erweitert um Werte für Dateizugriffsmethoden wie "create", "delete", "read", "write", "readAttributes", "execute", "noOperation" ... Zu jeder Methode kann optional ein Zugriffsschutzpaßwort definiert werden. Das Behaviour des Attributs wird entsprechend angepaßt.
Das Package sollte um die Aktionen "resetPassword" (Rücksetzen eines Zugriffsschutzpaßwortes auf einen vordefinierten Wert) und "cancelPassword" (Entfernen eines Zugriffsschutzpaßwortes) erweitert werden.

Operations object class
Behaviour: "managed objects" sollte erweitert werden auf "managed objects or files".
operationType Attribut: die Attribut-Syntax wird erweitert um Werte für Dateizugriffsmethoden wie "create", "delete", "read", "write", "readAttributes", "execute", "noOperation" ... Zu jeder Methode kann optional ein Zugriffsschutzpaßwort definiert werden. Das Behaviour des Attributs wird entsprechend angepaßt.
Es sollten die Aktionen "resetPassword" (Rücksetzen eines Zugriffsschutzpaßwortes auf einen vordefinierten Wert) und "cancelPassword" (Entfernen eines Zugriffsschutzpaßwortes) hinzugefügt werden.

Initiator object class
Behaviour: "management operations" sollte erweitert werden auf "management operations or file access methods".

Capability initiators object class
capabilityIdentitiesList Attribut: die Attribut-Syntax bezieht sich auf den ASN.1 Typ "operationType". Dieser Typ wird erweitert um Werte für Dateizugriffsmethoden wie "create",

"delete", "read", "write", "readAttributes", "execute", "no-Operation" ... Zu jeder Methode kann optional ein Zugriffsschutzpaßwort definiert werden. Das Behaviour des Attributs wird entsprechend angepaßt.

Die beschriebenen Änderungen können auf folgende Art und Weise in den Network Elements und Operations Systems realisiert werden.

1. Eigenständige Objektmodelle für den Zugriffsschutz von Managed Objects und von Dateien:
Für den Dateizugriffsschutz wird basierend auf dem in der ITU-T rec. X.741 beschriebenen Objektmodell und den oben beschriebenen notwendigen Änderungen für den Dateischutz ein eigenständiges Objektmodell beschrieben.

2. Allomorphe Erweiterung des in ITU-T rec. X.741 definierten Objektmodells:
Das bisher in der ITU-T rec. X.741 definierte Objektmodell bleibt unverändert und wird allomorph um die für den Dateizugriffsschutz benötigten Subclasses erweitert. Unter der allomorphen Erweiterung des Objektmodells wird dabei verstanden, daß ein von einem gegebenen Objektmodell abgeleitetes Objektmodell als Instanz eines Objektmodells gehandhabt wird. Ziel bei dieser Art von Realisierung ist es, bereits definierte Objektklassen, die unverändert auch für den Dateizugriffsschutz genutzt werden können, nur einmal zu definieren und wiederzuverwenden. Fig 3 zeigt am Beispiel Beziehungen in einem Objektmodell, bei dem aus einer Objektklasse Zugriffskontrolle AC (für: accessControl) im Zuge von Vererbung IH (für: inheritance) eine Objektklasse Zugriffskontroll-Schema ACR (für: accessControlRules) und eine Objektklasse Datei-Zugriffskontroll-Schema FACR (für: fileAccessControlRules) gebildet werden.

3. Erweiterung des existierenden Objektmodells zu einem neuen Objektmodell für Managed Objects und Dateien

Das in der ITU-T rec. X.741 definierte Objektmodell kann so erweitert werden, daß in den bestehenden Objektklassen

- das Behaviour wie oben beschrieben angepaßt wird und
- für den Dateizugriffsschutz notwendige neue Attribute und Actions optional (als conditional packages) hinzugefügt werden,
- die spezifisch für den Zugriffsschutz von Managed Objects notwendigen Attribute und Actions in conditional packages eingefügt werden.

Die Änderung der Attributsyntax kann

- entweder durch die Definition neuer Attribute (in conditional packages)
- oder durch die Erweiterung des ASN.1 (Abstract Syntax Notation No 1)-Typen

erfolgen. Werden für den Dateizugriffsschutz eigene Attribute definiert, dann müssen in diesem Fall auch die spezifisch für den Zugriffsschutz von Managed Objects notwendigen Attribute in conditional packages eingefügt werden.

Patentansprüche

1. Verfahren zur Realisierung einen einheitlichen Zugriffsschutzes auf Managed Objects und Dateien basierend auf der ITU-T recommendation X.741
demzufolge
ein erstes Zugriffskontroll-Schema (Objektmodell) auf Managed Objects gegeben ist
dadurch gekennzeichnet, dass
- ein zweites eigenständiges Zugriffskontroll-Schema (Objektmodell) auf Dateien gegeben ist,
- das zweite Zugriffskontroll-Schema sämtliche Eigenschaften, insbesondere Objektklassen, Attribute, der recommendation X.741 aufweist,
- das zweite Zugriffskontroll-Schema um neue Attribute und / oder Actions für den Dateizugriff erweitert wird,
- für den Dateischutz die Attributsyntax eines in der recommendation X.741 definierten Attributes erweitert wird,
- für den Dateischutz die Eigenschaften (Behaviour) einer in der recommendation X.741 definierten Objektklasse erweitert werden und
- das zweite Zugriffskontroll-Schema gleichartig wie für Managed Objects auf Dateien anwendbar ist.

2. Verfahren nach Anspruch 1
dadurch gekennzeichnet, dass
- sämtliche Attribute / Actions, die sich ausschließlich auf Managed Objects beziehen, als Teil von conditional packages ausgebildet werden.
-

3. Verfahren nach Anspruch 1
dadurch gekennzeichnet, dass
- das zweite eigenständige Zugriffskontroll-Schema (Objektmodell) frei ist von sämtlichen Eigenschaften, insbesondere Attributen, syntaktischen Beschreibungen, die sich ausschließlich auf Managed Objects beziehen.

4. Verfahren zur Realisierung eines einheitlichen Zugriffsschutzes auf Managed Objects und Dateien mittels allomorpher Erweiterung der ITU-T recommendation X.741
demzufolge
ein Zugriffskontroll-Schema (Objektmodell) auf Managed Objects gegeben ist
dadurch gekennzeichnet, dass
das Objektmodell um die für den Dateizugriffsschutz benötigten Subclasses erweitert wird.

5. Verfahren zur Realisierung eines einheitlichen Zugriffsschutzes auf Managed Objects und Dateien basierend auf der ITU-T recommendation X.741
demzufolge
ein Zugriffskontroll-Schema (Objektmodell) auf Managed Objects gegeben ist
dadurch gekennzeichnet, dass
- das Zugriffskontroll-Schema sämtliche Eigenschaften, insbesondere Objektklassen, Attribute, der recommendation X.741 aufweist,
- das Zugriffskontroll-Schema um neue Attribute und / oder Actions für den Dateizugriff erweitert wird,
- für den Dateischutz die Attributsyntax eines in der recommendation X.741 definierten Attributes erweitert wird,
- für den Dateischutz die Eigenschaften (Behaviour) einer in der recommendation X.741 definierten Objektklasse erweitert wird und
- das Zugriffskontroll-Schema sowohl für Managed Objects als auch auf Dateien anwendbar ist.

6. Verfahren nach Anspruch 5
dadurch gekennzeichnet, dass
- die für den Dateischutz neu definierten Attribute und / oder Actions als Teil von conditional packages ausgewiesen werden,

- existierende Attribute und Actions, die sich ausschließlich auf Managed Objects beziehen, als Teil von conditional packages definiert werden, und
- die Attributsyntax eines in der recommendation X.741 definierten Attributes durch eine Erweiterung der ASN.1 Syntax erweitert wird.

7. Verfahren nach Anspruch 5
dadurch gekennzeichnet, dass
- die für den Dateischutz neu definierten Attribute und / oder Actions als Teil von conditional packages ausgewiesen werden,
- existierende Attribute und Actions, die sich ausschließlich auf Managed Objects beziehen, als Teil von conditional packages definiert werden und
- für den Dateischutz die Attributsyntax eines in der recommendation X.741 definierten Attributes dadurch erweitert wird, daß das Attribut als Teil eines conditional package definiert wird und zusätzlich ein Attribut als Teil eines conditional package mit der Erweiterung der Attributsyntax definiert wird,

8. Verfahren nach einem der vorstehenden Ansprüche
dadurch gekennzeichnet, dass
für den Dateizugriff FTP (File Transfer Protocol) - Standard (RFC 959 und/oder 1123) verwendet wird.

9. Verfahren nach einem der vorstehenden Ansprüche
dadurch gekennzeichnet, dass
für den Dateizugriff FTAM (File Transfer Access Method) - Standard (ISO 8571) verwendet wird.

10. Verfahren nach einem der vorstehenden Ansprüche
dadurch gekennzeichnet, dass
es in einem Network Element (NE) realisiert wird.

11. Verfahren nach einem der vorstehenden Ansprüche

dadurch gekennzeichnet, dass
es in einem Operations System (OS) realisiert wird.

FIG 1

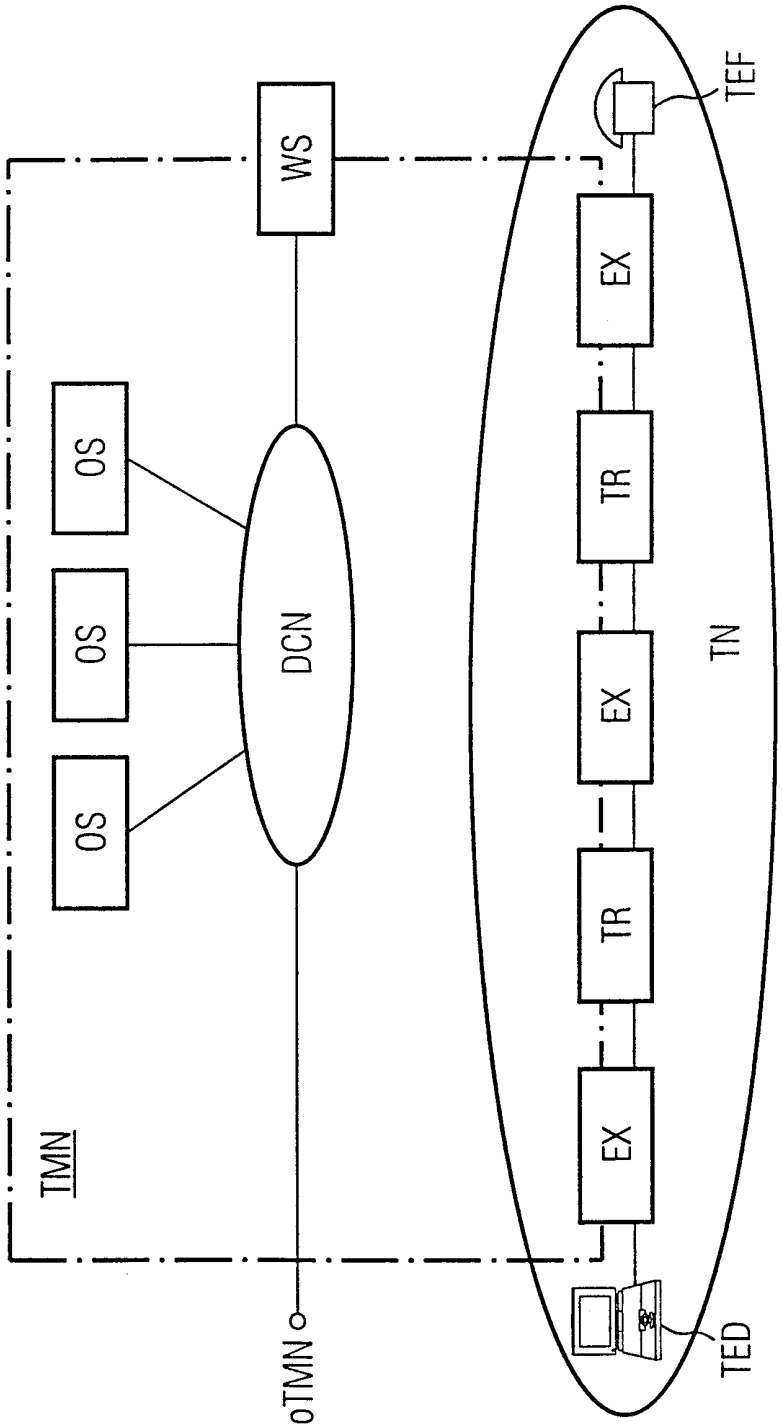


FIG 2

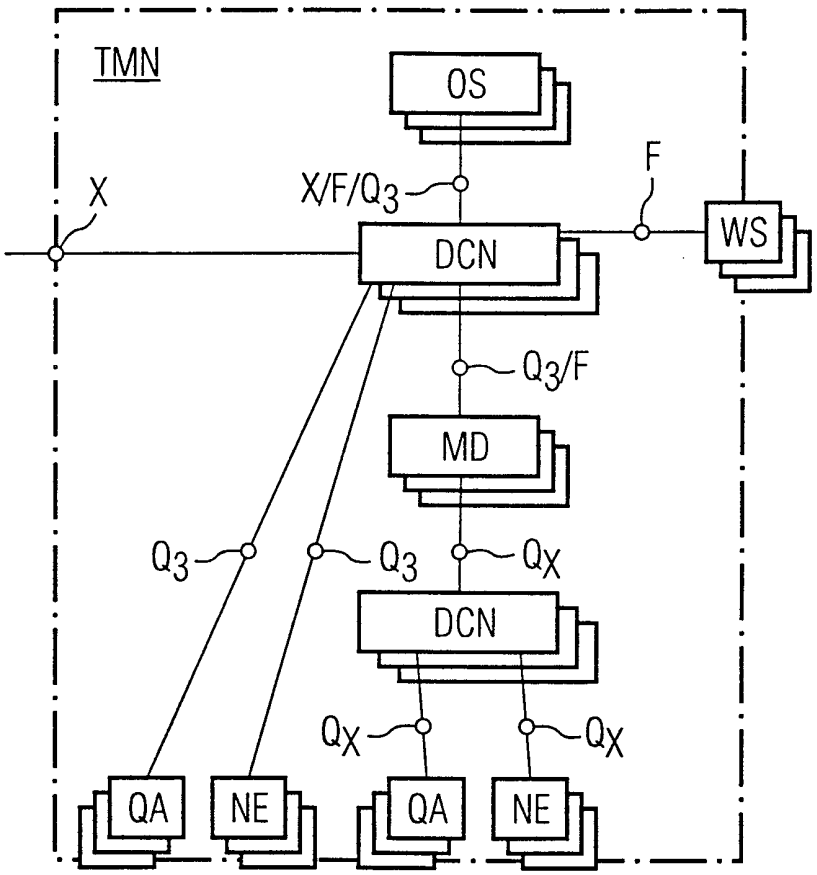
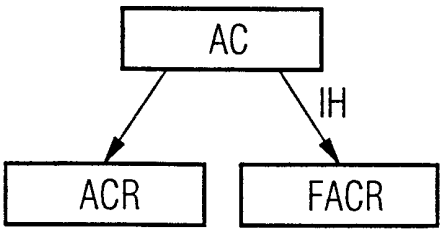

TMN
OS
X
X/F/Q3
F
WS
DCN
Q3/F
MD
Q3
Q3
QX
DCN
QX
QX
QA
NE
QA
NE

FIG 3


AC
IH
ACR
FACR