APPENDIX 1

(to Recommendation Z.331)

User-system access control administration

I.1 General

This appendix has been developed in accordance to the methodology defined in Recommendations Z.332 and Z.333.

The main part of this appendix deals with the model of User- System Access Control Administration. A glossary of the terms used is also included.

The list of functions to be controlled and the list of jobs are contained in Annex A.

For each function to be controlled by means of MML, one or more functions can be derived and each of them can be described using the metalanguage defined in Recommendation Z.333 in order to detail the relevant information structure.

Annex B contains a list of MML functions and information structure diagrams associated to each of them to be used as guidelines.

I.2 Introduction

User-system access control (here and after access control) is provided within a system to restrict the input allowed to be entered in order to prevent unauthorized system modification and or viewing of information.

Access control is the system function which performs the control of the access to systems and their functions by the users.

Access control administration is defined as the administration of the access rights of the users.

This Recommendation mainly covers human beings as users.

Machine to machine access control administration is not covered by this appendix.

It is therefore recognized that this appendix will require further study within a wider scenario including the various aspects of access control (man-machine, machine-machine, etc.).

I.3 Access control model

I.3.1 Introduction

Access criteria are defined to be the attributes that characterize the access to the system.

Permissions are defined to be the rights granted to the user. Authority is defined to be the relationship between the access criteria and the permissions.

The inputs submitted are accepted by the system, provided that the system has verified the authority to enter them.

I.3.2 Model

The main attributes (see Figure I-1/Z.331) which have been adopted to identify access criteria and permissions are the following (other attributes of the two categories can be adopted depending on the administration's needs):

a) for access criteria

- user identity
- terminal identity
- time interval

b) for permissions

- command class
- command parameters

- system identity

- time interval

Some of the attributes listed above may not be implemented according to administration requirements.

In order to facilitate access control administration, groups may be formed in terms of single access control attributes (e.g. group of user identities can form a maintenance group).

An example of implementation is represented n Figure I2/Z.331.

```
+------------------------------------------------------------------ -----------+
¦                                    Authority
         ¦ +------------------------------------------------------------------ -----------¦
¦                                     Access
criteria          ¦          Permissions       ¦
+------------------------------------+--------------------------- -----------¦
¦  User    ¦ Terminal ¦   Time   ¦  System  ¦  Command ¦
Command                                          ¦
¦ identity  ¦  identity ¦  interval ¦  identity ¦    class   ¦ p arameters              ¦
+------------+------------+------------+------------+------------+-- -----------¦
¦                                                                    User
```

```
1             ¦ Terminal ¦   Any    ¦     Any    ¦ Any    ¦     Any
            ¦ ¦           ¦          1          ¦                      ¦            ¦
¦                                                                                          ¦
+------------+------------+------------+------------+------------+-- -----------¦
¦   User  1    ¦ Terminal ¦  8   -   17h    ¦   System
1                                ¦      Subscrib.     ¦              Direct          ¦      ¦
¦                          2      ¦  Monday   ¦                     ¦ Administr. ¦    numb.    ¦
¦                                      ¦                        ¦    through     ¦           ¦
¦   81000  -    ¦ ¦             ¦          ¦    Friday   ¦
¦                                              ¦                           82000              ¦
+------------+------------+------------+------------+------------+-- -----------¦
¦   User  2    ¦ Terminal ¦  20   -   8h    ¦   System
1             ¦ Junction  ¦  Junction     ¦ ¦                     ¦      3     ¦
¦           ¦ maintenance¦   identity    ¦  ¦             ¦
¦                                     ¦                        ¦                       ¦       1A23   1800        ¦
+------------+------------+------------+------------+------------+-- -----------¦
¦   User  3    ¦    Any       ¦  8   -   17h    ¦   System
2             ¦ Subscrib.  ¦   Direct       ¦ ¦                      ¦            ¦
¦           ¦ maintenance¦     numb.     ¦  ¦             ¦
¦                                     ¦                       ¦                      ¦   73000  -     ¦¦
¦                                    ¦                      ¦                     ¦             ¦   87000    ¦
+------------+------------+------------+------------+------------+-- -----------¦
¦                                   Any          ¦      Terminal       ¦         8            -
17h                       ¦       Any                     ¦    Subscrib.   ¦    -         ¦  ¦
¦                          4      ¦                 ¦                      ¦  administr.¦          ¦
+------------+------------+------------+------------+------------+-- -----------¦
¦                          -      ¦    -                       ¦          -             ¦          -       ¦    -
                           ¦     -       ¦¦                    ¦                    ¦           ¦
                     ¦                                    ¦                                    ¦
+------------------------------------------------------------ -----------+
```

FIGURE I-2/Z.331

Example of application

I.3.3 Attributes of access control

In the following the meaning of the main attributes which are likely to be used in the access control administration, is described.

a) User identity

The user identity results from the identification procedure (see Recommendation Z.317) and uniquely identifies the user to the system.

In the identification procedure usually the identity of the individual user is used.

b) Terminal identity

The terminal identity is the identity of the I/O device as known to the system, via its hardwar logical connection.

c) Time interval

The access control may depend on the time when the input is entered and/or executed.

d) Command class

A command class can be either a single command code (see Recommendation Z.315) o identifiable set of command codes.

e) System identity

System identity is the identity of the system or an application in which the command is allowe be performed. In a centralized support system, individual systems connected to it may have their own access control. Alternatively, centralized control may be used based on the identity of the system addressed.

f) Command parameters

Access control may depend on a parameter (see

Recommendation Z.315) or a combination of parameters.

The control may be based on either the parameter name

or the parameter name and its values.

If a parameter is considered, it may be desirable to limit such use to major objects in the system relevant

to specific

O&M Administration needs.

I.4 Glossary of terms

Access criteria

The set of attributes that characterize the access to the

system. Example attributes are user identity and terminal identity. Permissions

The rights granted to the user.

Authority

The relationship between access criteria and permissions. Terminal identity

Identifies a physical terminal, a channel or a port to an SPC system.

I.5 List of functions and jobs

I.5.1 List of system independent Class B functions

I.5.1.1Administering authority

I.5.1.2Retrieving authority information

I.5.2 List of jobs

I.5.2.1To create/change authority

- the purpose of the job is to create/change a specific authority by means of managing the relevant attributes;

- the system is supposed to record the data and check their correctness;
- the operator is supposed to input all needed data;
- the complexity of the job may be high depending on the amount of the data to be input;
- the frequency of the job is low.

I.5.2.2To delete a specific authority

- the purpose of the job is to delete all the data related to the specific authority;
- the system is supposed to delete the data related to the authority;
- the operator is supposed to input the identity of the

  authority to be deleted;
- the complexity of the job is low;
- the frequency of the job is low.

I.5.2.3To interrogate the authority information

- the purpose of the job is to retrieve authority information;
- the system is supposed to output the requested information on the selected device;
- the operator is supposed to input the identity of the access control attributes;
- the complexity of the job is low;

- the frequency of the job is low.

I.5.2.4To activate/deactivate an authority

- the purpose of the job is to activate/deactive a specific authority previously created/changed; this job

may be implied in the creation/changing job;

- the system is supposed to activate/deactivate the authority;

- the operator is supposed to input the date and the time for the activation/deactivation and the identity of the authority;

- the complexity of the job may be medium;

- the frequency of the job is low.

I.6 Guidelines for the list of MML Functions and associated information structure diagrams

I.6.1 Introduction

This section contains guidelines for the list of MML functions and associated structure diagrams related to the access control administration model defined in section 3 of this Recommendation.

I.6.2 List of MML functions

This list contains possible MML functions for the Access Control Administration.

This list is not mandatory nor complete; it may vary according to administration needs, telecommunication network levels,

regulatory needs, etc.

I.6.2.1Creation

- create authority

I.6.2.2Changing

- change authority

I.6.2.3Deletion

- delete authority

I.6.2.4Interrogation

- interrogate authority

I.6.2.5Activation/deactivate

- activate/deactive authority

I.6.3 Information structure diagrams

(to be developed)