ETSI TECHNICAL REPORT

ETR 097

March 1994

Source: ETSI TC-TE

Reference: DTR/TE-06012
EWOS ETG 027

ICS: 33.020, 33.040.40

Key words: Terminal Equipment and Security

Terminal Equipment (TE); Security architecture for the directory

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

Contents

Foreword

ETSI Technical Reports (ETRs) are informative documents resulting from ETSI studies which are not yet appropriate for European Telecommunication Standard (ETS) or Interim European Telecommunication Standard (I-ETS) status. An ETR may be used to publish material which is either of an informative nature, relating to the use or application of ETSs or I-ETSs, or which is immature and not yet suitable for formal adoption as an ETS or I-ETS.

This ETR has been produced by the Terminal Equipment (TE) Technical Committee of the European Telecommunications Standards Institute (ETSI). More specifically, it is the result of a joint effort of experts from the European Workshop for Open Systems (EWOS) EGDIR and ETSI STC-TE6 (Directory Systems). Due to the similarity of objectives, EWOS and ETSI have agreed to issue common texts. The EWOS equivalent to this ETR is known as EWOS Technical Guide (ETG) 027.

NOTE: Since common texts are to be issued, this ETR does not necessarily follow the conventions for the normal ETSI presentation of texts.

The Directory standards provide many facilities that help implementors and service suppliers to provide a secure service. However, the actual use of these facilities to define a secure service is not defined within these standards and some extensions are required to make them perform adequately.

This ETR reviews security issues and identifies some of the specific measures required to achieve security.

Blank page

1 Introduction

The Directory standards define mechanisms whereby security requirements can be expressed in protocol and in the behaviour of the Directory. This ETR indicates some of the provisions that are recommended for the actual achievement of security.

The ETR primarily covers the use of "simple authentication" - verification of a named identity by use of a password - as the foundation of a scheme for security. Access control is assumed to be present but is not currently constrained (e.g. to be compatible with the 1992 edition of the Directory standards).

Strong authentication is outside the scope of the ETR.

2 References

ISO 7498-2 (1992): Security Architecture.

CCITT X.500 Series / ISO 9594: Information Processing Systems - Open Systems Interconnection - the Directory (1988).

Directory Implementer's Guide: Version 6 - June 1992.

ISO TR 10000-2 (1992): Taxonomy.

3 Scope

This ETR is concerned with the establishment of a consistent security architecture, within the scope of DSAs that use the 1988 edition of DAP/DSP and that do not have a strong authentication capability. These DSAs are presumed to have means of protection of the data within themselves (e.g. by application of access control).

The architecture remains consistent with the introduction of "basic access control" (and "simplified access control") in accordance with the 1992 edition of the standards, but it does not rely on compliance with the access control mechanisms to be provided as part of the 1992 edition. Requirements on access control (as defined in subclause 6.9) are intended to be minimal.

The ETR does not describe any requirements on DUAs, while recognising that security requirements may exist in a practical system.

The ETR does not define the means whereby security can be provided against "insider" access; that is, against access by a trusted individual who is, in fact, malicious or against a trusted DSA that is in fact suborned (i.e. capable of providing protocol intended to provide unauthorised access to Directory information). It also provides no confidentiality features (e.g. such as would be provided by encryption).

It does, however, provide the means for comprehensive (if limited) read protection against unauthorised users given proper procedures for password maintenance and physical protection of equipment (screens, DSAs and communications links). It also provides the means for comprehensive (if limited) protection of information within DSAs from unauthorised update.

The ETR recognises the low quality of security that can be achieved using simple authentication, even within a single Directory Management Domain (DMD), but provides rules which, if followed, give the maximum capability available from this technique.

However, for completeness of scenario descriptions, references are made to strong authentication. These references are informative.

4 Scenario

The ETR is intended to cover two main scenarios (clearly, there are many variations possible of each of these):

A) ADDMD Service, including "Rental" Service

A service provider has an Administration Directory Management Domain (ADDMD) which is used to provide a commercial Directory service. Entries within the Directory Information Tree (DIT) may be allocated and maintained on behalf of customers; subtrees of the DIT may be allocated and maintained as a service to corporate customers. The service provider is concerned to maintain the integrity of the parts of the DIT which it maintains, and is also concerned to maintain confidentiality of information that is related to its own internal operations. It may also be concerned to implement specific security rules for corporate customers with regard to their own parts of the DIT. The service provider may also support access to private DMDs, for example via subordinate references backed up by suitable authentication.

B) Protection of use of resources by unauthorised persons

A company maintains a Private Directory Management Domain (PRDMD) which is used to supply internal needs. In this scenario, the DIT Domain (i.e. the part of the DIT mastered by the DMD) is partly private and partly public, i.e. available for access by persons unknown to the DMD (e.g. persons from another organisation); however, information mastered by other DMDs may be accessed from within the first DMD, subject to access controls applied by those other DMDs. A major concern of the company is to protect not only its information but also its Directory resources against access by persons not known to and authorised by the DMD. (For example, an unauthorised person may be prevented not only from binding but also from successfully presenting chained operations).

NOTE 1: DMDs contain potentially many DSAs; some DSAs may hold information which is to be publicly accessible by users from outside the DMD; others may hold information which is to be kept private within the whole or part of the DMD; others may have some combination of private or public information.

NOTE 2: Another scenario, outside the scope of the ETS, relates to secret DSAs: some DSAs may not be accessible at all from outside the DMD, and even their presence (and contents) is potentially secret.

Many aspects of security rest ultimately on physical security (i.e. preventing unauthorised persons from being physically in a place where they can access or attempt to access information or services or equipment without having the right to do so). However, guidance on the achievement of physical security is outside the scope of this ETR.

5 Conformance requirements

This ETR lays down conformance requirements for DSAs that are to make use of the provisions described within it (e.g. subclauses 7.2.1 to 7.2.4, 7.2.6, 7.3.1, 7.3.3, 7.4.1, 7.4.2, 7.5 and 7.6). It is necessary to define such requirements, since differences in security policies may jeopardise the security of the Directory and its components. There are no conformance requirements in respect of strong authentication.

6 Principles

6.1 The Directory Security Model

The security model of the Directory describes the service in terms of authentication and authorisation. An authentication policy is used to identify both providers and users of the Directory service. An authorisation policy is used to specify access rights, primarily to Directory information.

6.2 Overview

This ETR describes Security Architecture in terms that cover four aspects of security policy:

- authentication;
- access to DSA services (service access);
- access to Directory objects (access control);
- trust.

The objective is to describe basic requirements which can be employed to provide protection of DSAs and their contents while still being part of the global Directory.

The basic requirement of a security policy, within the present scope, is to provide this protection, in such a way that an authorised user can carry out a specified operation or part of an operation, while an unauthorised user is prevented from doing so.

6.3 Threats

6.3.1 Directory resistance to security threats

There are many possible threats to security. The following subclauses outline some of these threats and indicate briefly how the Directory copes with them. These terms and definitions are taken from Annex A of CCITT Recommendation X.509 (1988) but are equally applicable to the 1992 Recommendations. Note that signed Directory traffic provides a data integrity service only for the data exchanged by DSAs and DUAs and does not guarantee the integrity (i.e. correctness) of the data on the originating system. Of course, depending on the environment in which the Directory operates, additional security capabilities (i.e. over and above standardized Directory features) may be available to enhance the integrity of the data.

6.3.2 Identity interception

The identity of one or more of the users involved in communications with the Directory may be intercepted and recorded for later misuse.

The Directory provides no inherent protection to this threat. In particular, note that as use of the Directory may involve chaining, it is difficult to even bound the end-points of the communications.

6.3.3 Masquerade

A user pretends to be a different user in order to gain access to information or to acquire additional privileges.

Use of simple protected or strong credentials, or signed Directory traffic, provides some protection.

6.3.4 Replay

This is the recording and subsequent replay of a communication at some later date (with the intent of masquerade). The use of simple protected or strong credentials, combined with signed Directory traffic provides some protection.

6.3.5 Data interception

This is the observation of user data during a communication by an unauthorised user.

The Directory provides no inherent protection. However, a data confidentiality service could be used to provide this (e.g. by link-level encryption within a DMD, or by otherwise restricting data interchange to be wholly contained in a secure network). Further, if strong credentials are used, then a session key may be exchanged for use with the data confidentiality service. Note that in the absence of a data confidentiality service, a DSA may refuse to disclose information or allow security-related information to be modified.

6.3.6 Manipulation

This is the replacement, insertion, deletion or misordering of user data during a communication by an authorised user.

Use of credentials combined with signed Directory traffic provides protection.

6.3.7 Repudiation

This is the denial by a user of having participated in part or all of a communication.

Use of strong credentials with signed Directory traffic provides some protection.

6.3.8 Denial of service

This is the prevention or interruption of a communication or the delay of time-critical operations. The threat may perhaps be presumed to be associated with inadequately-trusted DSAs in other domains, or with lower level communications elements.

6.3.9 Mis-routeing

This is the mis-routeing of a communications path intended for one user to another.

The Directory provides no inherent protection. However, the use of credentials coupled with signed Directory traffic sometimes permits detection of this threat at the receiving end.

6.3.10 Traffic analysis

This is the observation of information about a communication between users (e.g. absence/presence, frequency, direction, sequence, type, amount, etc.).

The Directory provides no inherent protection. This topic is outside the scope of this ETR. However, lower-layer encryption (e.g. at the data-link layer) may provide adequate protection in some environments.

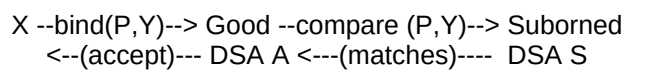
6.4 Countering masquerade

The primary threat considered in this ETR is presumed to be that of masquerade. This threat is presumed to arise when a protocol access is made to a DSA which purports to come from an authorised user, but in fact does not do so.

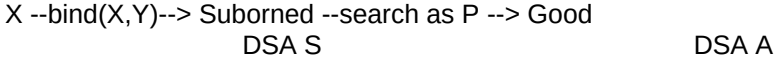
The following are some masquerade scenarios which need to be considered by a security policy:

a) a user X determines the credentials of a user P, and is then able to "log in" as if X were P; X thereby illicitly gains P's access rights to information;

b) a user X uses a suborned (i.e. corrupt) DSA S to hold credentials Y that purport to be those of P, but are in fact bogus credentials known to X. X may thereby be able to pose as P.



c) A user X uses a suborned DSA S to access information, which is capable of falsely supplying user P's name as an originator on the chaining arguments. X may thereby be able to pose as P.



6.5 Practical realisation of directory security

Prior to the availability of implementations conforming to appropriate parts of the 1992 edition of the Directory standards, practical realisation of Directory security must be largely based on the 1988 standard. In this subclause, the ETR considers how the Directory standard - with some modest additional mechanisms - can be used to maximise the protection with which the Directory can operate, using simple authentication.

This analysis is made in the context of the requirements for the Public Directory service. Administrators of some domains will view these policies and mechanisms as insufficient, whilst others will view them as more than adequate. These recommendations do not (nor are they intended to) substitute for a thorough analysis conducted in the context of a particular administrative domain.

The Directory is considered to comprise DSAs (and DUAs) which are grouped together to form Directory Management Domains (DMDs). Each DMD is presumed to be managed by an organisation termed a Domain Management Organisation (DMO).

A DMO is modelled as an entity that can apply a consistent security policy to the DSAs and DUAs within the DMD.

Collections of objects subject to such a consistent security policy are termed Security Domains. A DMD is thus a Security Domain.

By definition, a Security Domain can contain inner, nested, Security Domains. Conversely, a Security Domain may be enclosed within a larger Security Domain. Security Domains can thus be nested, but do not otherwise overlap.

Within each Security Domain a security policy applies which covers the protection of data by means of:

authentication;

service access - that is, the granting or denying of rights to use the services and resources of a DSA;

access control - that is, the granting or denying of rights to access Directory information;

trust - that is making use of known relationships between DSAs.

Security policies within the Directory must be consistent with present and future mechanisms provided by the Directory, and, in particular, must not make use of new elements of protocol.

Security policies must take into account the fact that information within the Directory is distributed, and that potential exists for insecurity at knowledge references and other places where there are transitions in the location of information.

Security policies must also take into account the fact that information within the Directory may be "shadowed" (i.e. replicated) to other DSAs; however, the shadowing may be limited by security policies:

- a security policy may permit shadowing only to DSAs which can be relied upon to maintain the necessary level of protection (e.g. access control) on shadowed information;

- a security policy may restrict shadowed information to that which is appropriate to the level of trust accorded by the shadow "supplier" to the shadow "consumer" (or the converse).

The precise form of a security policy (and its expression within DSAs within a DMD) is a local matter.

6.6 Trust

Since the Directory is a distributed service, there needs to be a certain level of trust between co-operating entities. Hence, it is important for a given DSA to identify the level to which it trusts other DSAs in carrying out Directory operations. Further, because confidentiality is not a part of the Directory service, it must be taken into account that intermediate entities may examine data being chained through them.

6.7 Authentication

6.7.1 Directory authentication

A practical authentication policy balances the need to provide adequate operational confidence within available technology and at realistic cost. As strong authentication is at present constrained in its application by a number of factors, including the lack of a widespread certification-infrastructure, in the first instance, only simple unprotected authentication (name and password) is considered in depth. The improved performance of simple protected authentication is considered briefly below.

6.7.2 Authentication possibilities

Directory authentication occurs when an entity binds to a DSA; the entity may be a DUA or another DSA (the responder is always a DSA). In either case, there are four different types of credential which may be presented:

- the initiator may present no credentials, in effect asking for anonymous access to the Directory;

- the initiator may present simple credentials, in which case the initiator's Distinguished Name (DN) and (optionally) a (plain text) password are provided. Optionally, a time-stamp, a "random number" and the password are passed through a predefined message digest algorithm. The collection of DN, time-stamp, random number and resulting message digest are termed simple protected credentials;

- the initiator may present strong credentials, in which a security token and, optionally, a certification path are provided;

- the initiator may present credentials based on an externally-defined and bilaterally-agreed-upon scheme.

The last two possibilities are not within the scope of this ETR.

Authentication is said to be corroborated when the user has supplied a name and additional credentials (e.g. a password) which have permitted verification of the name.

The responder must respond with the same type of credentials, except that a DSA may respond with its name, even when the initiator supplies no credentials.

NOTE: A defect has been raised to resolve the contradictory statements in the 1988 standard on the credentials to be returned by a DSA if no credentials are supplied by the bind request.

6.7.3 Authenticating users

According to the 1988 standards, user authentication using simple authentication is carried out only at the first DSA, even when the distributed nature of Directory requires an operation to be chained. It is thus only the DAP association which is positively authenticated.

Secure simple authentication via DAP requires that the information upon which the credentials are based be:

- secure against unauthorised read access and alteration;

- contained within a DSA subject to the same security policy, and lying within the same security domain;

- accessed, when chaining is required for access, only via DSAs that lie within the same security domain.

6.8 Service access

A DSA is permitted to select, as a matter of policy, that form or those forms of DAP authentication which it is prepared to accept:

- none (not really a form of authentication);
- name-only (not really a form of authentication);
- name-and-password;
- name-and-protected-password;
- strong-authentication;
- external-authentication.

A DSA is thereby entitled to refuse to give service to any user who is inadequately authenticated. This can be done, for example, by:

- refusing to accept the bind when authentication is carried out in an unacceptable way (e.g. no password supplied);
- refusing to provide service to a user via DSP when the invoking DSA either provides no "originator" element in chaining arguments or is itself untrusted.

The presumption is made that the use of the "originator" element is controlled by an agreed convention. In particular, this element should not be used by a DSA when no authentication took place, or took place to an unacceptable level of confidence.

6.9 Access control

6.9.1 Introduction

User Access Control (UAC) is the granting or denying of permission to Directory users, or classes of such users, to carry out Directory operations or elements of Directory operations in respect of Directory entries and their contents.

Whenever a Directory operation is to be performed, an authorisation policy is consulted. The 1988 Directory standards provide guidance, but not a mechanism, in this area. The consequences of this situation are far-reaching; e.g. it is not possible to implement a caching policy in an intermediate DSA unless the authorisation policy of the source DSA is understood. The 1992 edition of the Directory standards defines standard mechanisms for access control. A summary is given in Annex A.

Information in a DSA is minimally secure if it cannot be created or updated by unauthorised users. Other limited forms of security are provided, for example, by denying read access to any but suitably authenticated and authorised users.

6.9.2 Administrative Access Control

Administrative Access Control is concerned with the protection of operational information within a DSA (i.e. affecting its behaviour or configuration) whose administration is entrusted to the administrative authority for the DSA and its agents. Administrative Access Control provisions may be based on User Access Control, but they may also be based (in whole or in part) on forms of access to the DSA that are not based on Directory protocols.

Where Administrative Access Control does use Directory operations, it implies a preceding process of Administrative Authentication, which establishes the credentials of an administrator in an appropriate way.

6.9.3 Administrative limits

Regardless of the presence of an access control mechanism, each DSA may implement local administrative limits for each operation.

NOTE: Examples of such limits include: maximum time to process a request, maximum size of search or list results, minimum depth from the root before a whole-subtree search is allowed, and the minimum complexity of a search filter. The first two are analogous to available service controls in the Directory standard.

The lower limit on search complexity implies that users may be required to specify at least one strongly limiting filter item (e.g. at least an equality match on a name) to obtain service.

6.10 Use of "trust"

The term "trust" is used in a specific and mechanistic sense for an individual DSA:

- one DSA "trusts" another DSA for some particular purpose (e.g. authentication) if it contains information placed there by its administrative authority which advises that the other DSA is trustworthy for this purpose;

- the consequence of having this "trust" in this other DSA is that certain information (e.g. "originator" in chaining arguments) is considered reliable, enabling actions to be taken (e.g. providing access to information) which could not be taken on security grounds in respect of DSAs not enjoying this trust.

A DSA may be trusted for a particular purpose by another DSA, while not being trusted for some other purpose by the same DSA. However, for the present purpose trust relates only to the reliable authentication of users, and, by implication, of DSAs themselves.

The mechanisms of trust are most effective under two conditions:

- a collection of DSAs mutually trust each other for some purpose, but a DSA inside the collection does not trust any DSA outside this collection;

- the procedures for making use of this trustedness are uniformly applied within the collection.

A collection of mutually trusting DSAs can be considered to be a security domain.

In the limit, a DSA may consider that each other DSA is adequately trusted. A DSA that only implements this trivial level of trust, however, does not fall within the scope of this ETR.

7 Additional Security Mechanisms

7.1 Introduction

The subclauses below indicate requirements, over and above those implied by the standards, which must apply if the security architecture outlined is to work.

7.2 Authentication

7.2.1 Adequacy of Authentication

A DSA shall consider that authentication in respect of a particular user has adequately been carried out only if:

a) the DSA holds master entry information in respect of the user to be authenticated which is secure (viz. NOTE 1 below) and contains matching credentials;

or

b) the DSA holds shadow entry information in respect of the user to be authenticated which is known to be secure because it is supplied as secure by an adequately trusted DSA and contains matching credentials;

NOTE 1: This approach is potentially sensitive to replay for simple protected authentication in that credentials observed for a successful bind can immediately be used to access another DSA that contains the duplicated credential information. Without protection, replay is always possible (viz. subclause 7.2.6).

or

c) the DSA can carry out an adequately trusted compare operation in respect of the credentials (viz. subclause 7.3.4 below) (reading passwords would be insecure, and so may well be prohibited by a security policy);

or

d) the DSA receives a DSP invoke for which the user is quoted as originator in chaining arguments and the DSA originating the invoke is trusted to supply the originator element only when the user is considered to be adequately authenticated (viz subclause 7.2.3 below).

Authentication carried out in any of ways a, b, c or d is termed "adequate authentication". Other authentication is termed "inadequate authentication".

NOTE 2: Directory Information can only be considered to be minimally secure if it is protected against unauthorised update.

7.2.2 Trusted associations

A DSP association supplying a DSP invoke shall be considered trusted only if the DSA bind that initiated it has used either simple (protected or unprotected) or strong credentials. Associations not complying with this requirement are considered inadequately authenticated.

The following requirements apply if only simple authentication is available.

A DSA shall maintain a private table listing the DSAs which it potentially trusts, as defined in subclause 7.5.

Over an inadequately authenticated association, if the chaining arguments of a DSP invoke contain an originator element, the originator element shall be considered inadequately authenticated.

NOTE: This element shall, in particular, be considered untrusted for associations with DSAs that have not supplied corroborative authentication (e.g. by password or better).

If the authenticity of a DSP request is in doubt, or not of a sufficiently high level, the DSA receiving the request could reject the operation with a "referral error" referring to itself. (This capability becomes "official" in the 1992 standards.) The supplying DSA will need to realise that the access point given in the referral is the DSA it has just contacted and pass the referral back to its requester. (In the 1992 standards there is a flag, "return-to-DUA" which simplifies the implementation of this requirement). When the referral arrives back at a DUA, it may attempt a DAP connection to the relevant DSA, which may then result in authentication in the usual DAP manner. However, care should be taken if the DUA and remote DSA are in different domains; first, the remote DSA may not be able to authenticate the DUA, and second, a network path between the two entities may not exist.

7.2.3 Passing on the originator element

DSAs shall not pass the originator element in Chaining Arguments on to any further DSA to which the operation may be chained unless the element, as received, was trusted (e.g. in accordance with subclauses 6.8 and 7.2.2).

This provision permits DSAs to distinguish clearly between chained operations with trusted and untrusted user authentication. A chaining DSA simply omits the element when it cannot identify or mistrusts the supplier of the operation, or, if desired, any DSA previously involved in handling it.

7.2.4 Directory Bind and Chained Compare Operations

A DSA receiving a Directory Bind request using simple unprotected authentication in respect of credentials held in another DSA may optionally test the authentication by generating a chained compare operation.

The DSA shall not generate this operation unless it can establish a trusted DSP association with the DSA to which it chains the operation.

To prevent such operations "escaping" beyond the scope of a trusted set of DSAs, it shall be possible to select one of the following provisions:

1) DSAs within the set shall not chain compare operations (at the least for those referring to password attributes) over an untrusted association, unless the supplying association was untrusted;

or

2) The DSA shall mark each compare operation used to authenticate a bind with the option "chaining-prohibited" (in which case it may establish, if necessary and possible, a trusted association with a DSA whose access point is supplied by a referral).

DSAs compliant with this ETR shall support both options, since either option is legal, but the options cannot be mixed within a domain policy.

7.2.5 Effects of authentication on service

Note that, based on the authentication mechanism used by an initiating entity, a responding entity may unilaterally impose additional restrictions on the operations allowed over the association, without regard to the access rights of the initiating entity (viz. subclause 7.3.1).

7.2.6 Handling user password

Confidentiality of Directory operations is not assured. Hence, a DSA should return an "unwilling-to-perform" service error for any request which would disclose stored credentials (e.g. the value of a password). This restricts read and search operations but not compare operations.

Similarly, a DSA should also return an "unwilling-to-perform" service error for any authorised request which would modify stored credentials, unless the DSA has some a priori mechanism for verifying that the modification request originated inside the same security domain (typically the same DMD).

When a DSA is constrained to use simple protected authentication, the shadowing of credentials is discouraged, since a successful bind to one DSA provides credentials that can be immediately replayed in a bind to a second DSA that contains duplicates of those credentials.

For these reasons, a chained compare operation generated by a DSA receiving a simple-authentication bind request should have the dont Use Copy service control set.

DSAs that generate a compare operation as a result of an internal Directory Bind request shall use their own name in the originator element of the chaining arguments. This requires that (to carry out successful authentication) the DSA must have adequate access control permissions within the DSA that holds the credentials.

7.3 Service Access

Whereas DSAs are obliged on conformance grounds to be capable of carrying out Directory operations, they may optionally be configured in such a way that they restrict user access to DSA services.

For example, a particular class of users may be denied the right to bind to the DSA. Another class of users may be denied the right to use the DSA for update operations (whether local or chained).

If access to information with access-control restrictions is allowed from network addresses outside the Domain, then care must be taken in the choice of credentials allowed. Of course, since the Directory provides no inherent mechanism for confidentiality of Directory traffic, allowing access to sensitive information from outside the Domain may result in unanticipated disclosure of that information.

7.3.1 Access based on authentication method

A DSA may decline to accept an association on the basis of the authentication method without consideration of the access rights of the user. For example, a DSA may refuse any association for which a name was supplied without password. If a DSA does accept an association, it shall support read operations (read, compare, list and search) subject to access control restrictions. (It may place further restrictions on update operations). Here "support" is taken to include the possibility of chaining on the operation, and thus acting as a sentinel for the DMD of which the DSA is a part.

A DSA that has accepted an association may decline to provide update services on the basis of the method of authentication without consideration of the update access rights of the user.

7.3.2 Access for Chained Operations

A DSA may decline to carry out any chained operation, or to carry out a chained update operation, without consideration of the access rights of the user.

A DSA may decline to carry out any untrusted chained operation, or to carry out a chained update operation, without consideration of the access rights of the user.

7.3.3 Access based on identity

A DSA may decline to carry out any operation, or to carry out an update operation, in each case chained or otherwise, in respect of users or user classes, as selected by management action.

If this facility is provided, then each such DSA shall be able to prevent similar access to all users subject to inadequate authentication.

7.3.4 Distributed Simple Protected Authentication

In principle, a DSA receiving a DAP Directory Bind request using either simple or simple protected authentication with respect to credentials held in another DSA tests the authentication by generating a chained compare operation (with the dontUseCopy service control set).

Unfortunately, in the simple protected case, this technique does not work given the existing standards, since the compare operation presumes that a purported password has been provided. Thus, if remote simple protected authentication is required, non-standardized methods must be employed. One such method was proposed as a defect (but not accepted) for DR:064 (viz Directory Implementer's Guide Version 6, subclause 3.3 item C1, DR:064, and also DR:032). This redefined the syntax of UserPassword for the purpose of compare operations to be:

```
UserPassword ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX
                CHOICE {
                        OCTET STRING ((SIZE(0..ub-user-password))
                        SEQUENCE {
                                Validity,
                                PROTECTED OCTET STRING }
                        -- only for use as a value to be compared
                        -- by a compare operation
```

This extension was rejected in defect resolution balloting by an ISO member body as a "defect" on the grounds that it represented an extension of the intent of the simple protected authentication mechanism. (This was indeed what it was intended to do, on the grounds that the original intent was itself defective). In deference to the member body, the extension was rejected as a whole. It remains, therefore, only suitable for use between DSAs within a single DMD.

In making use of this extension, the first element of the choice within UserPassword should be used everywhere except, optionally, when a value is presented within a compare operation. The second element may optionally be used in this case; elements within the choice are as provided by the bind.

7.4 Access Control

7.4.1 User Access Control

DSAs shall be capable of exercising Access Control in terms of granting or denying permissions to ordinary Directory users, or classes of such users, to carry out Directory operations or elements of Directory operations in respect of Directory entries and their contents. This facility is termed User Access Control, or simply Access Control.

No specific requirements are placed on the form of Access Control, except in the following respects:

It shall be possible to arrange that users whose authentication is untrusted shall have fewer access rights than if the authentication had been trusted.

NOTE: The 1992 Directory Standards will contain comprehensive provisions for Basic Access Control (see Annex A).

7.4.2 Administrative Access Control

Administrative Access Control is concerned with the protection of operational attributes and other information concerned with the operation of specific DSAs. There are two significant differences between the requirements of access control (e.g. as defined in 1992 Basic Access Control) and Administrative Access Control:

- Administrative Access Control protects sensitive information in the Directory model, even in the absence of access control information for Basic Access Control, prior to the establishment of access control information;

- Administrative Access Control protects all information within the DSA Model (i.e. from the viewpoint of a single DSA), such as knowledge information; Basic Access Control provides no protection for this kind of information.

Administrative Access Control may make appropriate use of Basic Access Control, or other such standardized access control provisions, to protect information of appropriate classes.

DSAs shall be able to identify administrators and the facilities that they may exercise as distinct from ordinary users and the normal Directory operations and facilities to which they may have access.

Only administrators should be permitted to have update access to the DSA's operational information that affects one or more of:

- access control for more than one entry;
- distributed operations.

The exercising of protection of this information is termed Administrative Access Control. It may (but need not) be distinct from User Access Control (e.g. using Basic Access Control).

Information that can only be updated by an administrative user is considered secure. No protection is provided against suborned (i.e. corrupt or treacherous) administrative users.

7.4.3 Browsing areas

A refinement on this policy is to define browsing areas. (See also earlier discussion on administrative limits.)

A browsing area is one where publicly-available information is found, but with access-controls on the size of the results which may be returned for any one operation. If the request comes from outside the DMD (or from a DSA not known to a DSA at the boundary of the DMD), the size limit may be quite small. In contrast, if the request comes from inside the DMD, then it may be permitted that only a much larger size limit may be enforced. Again, determination of behaviour in respect of intra-DMD requests may be made on the basis of:

- network address of remote entity, and/or
- AE-Title of the remote entity.

Such a policy allows "outsiders" to perform read operations along with searches that have a "tight" filter (i.e. restrictive, with few matches). Otherwise, if an outsider performs a search with a "loose" filter (i.e. with a high chance of a hit), the size limit will be quickly exceeded.

7.4.4 User groups

Organisations may find it useful to restrict Directory traffic to only a small collection of network addresses outside of the DMD. In this case a closed user group facility, available from a lower-layer service could be used. Note that the "users" in such a facility are the application entities communicating, neither of which need be the entity which originated a particular request.

7.5 Trust lists

DSAs compliant with this ETR shall support, as a minimum:

- a list of DSAs (the Trusted DSA List) which are to be considered trusted from the viewpoint of authentication and chaining;
- for each such DSA, the secure holding of credentials information which may be used to establish a trusted association;
- the capability of analysing Trace Information within chaining arguments to determine whether or not the DSAs involved in handling a chained operation are all trusted (i.e. have their names within the Trusted DSA List), and thus, of determining whether the operation itself is trusted.

Such DSAs shall also carry out trust-related procedures, as defined above.

7.6 Directory audit

DSAs complying with this ETR shall have the capability of providing audit information describing activity on both a per-association and per-operation basis. At a minimum, an audit record should include:

- a time-stamp;
- the operation requested, along with important parameters associated with the operation:
    - bind: initiator-name, type of authentication and possibly network address;
    - read: object-name;
    - compare: object-name, and attribute-name;
    - abandon: invocation-identifier;
    - list: object-name;

      search base-object, subset, and filter;
    - add-entry: object-name;
    - remove-entry: object-name;

  - modify-entry: object-name;
  - modify-rdn: object-name, and new-rdn;
  - unbind: abort-indicator;
- the originator element (if chaining arguments were present in the operation);
- the association-identifier and invocation-identifier (if applicable); and
- the invocation outcome.

The control of audit information and the use made of it must remain a local matter, and could be subject to local privacy legislation.

7.7 Physical security

Physical security is outside the scope of this ETR. However, it must be noted that no matter how much "protocol" trust is placed in a remote site, if physical security at that site is compromised, then protocol security is also at risk.

8 Additional recommendations

8.1 Use of the Requester Element in CommonArguments

This element (whose main use is to indicate the original requester for a signed operation) should only be acceptable when it matches precisely with the identity of the user that was authenticated at bind-time.

Conversely, it should not be used when there was no such authenticated identity; otherwise there is a potential conflict between the bound identity and the CommonArgument identity. This might indicate a potential security breach.

8.2 Use of non-specific subordinate references

If a DSA has a non-specific subordinate reference which points to a number of untrusted DSAs, or DSAs which are mutually untrusted, there is a possibility of a "denial of service" threat. (If the NSSR points only to DSAs that are mutually trusted, this threat may be presumed not to apply.)

If the multicast is conducted sequentially, a DSA can claim to be able to resolve the presented name either by returning a result or by returning certain errors (viz. A/DI32). This response has the effect of terminating the multicast prematurely - so that a DSA holding the desired information will have not even been asked to respond.

If the multicast is conducted in parallel, the effect of a false positive response is to generate either an error or return of information which could be itself false.

These factors should be considered before non-specific subordinate references are used.

8.3 Pairwise-distinct passwords for DSP authentication

In the case of DSP authentication, additional security is achieved if passwords are distinct depending on the DSA to which the bind takes place.

Annex A: Summary of 1992 Access Control

In the 1992 CCITT recommendations, Basic Access Control is realised using enhanced access control lists (ACLs), whose elements are called access control information items (ACI Items). A particular element of information may be protected by access control policy or by access controls specific to the entry itself.

Access control policies for users are expressed by ACI Items associated with particular administrative entries. Administrative entries partition the DIT into subtrees of common authority termed administrative areas in accordance with the Authority Model. An access control policy attribute is held within a special entry, termed a subentry of the administrative entry, which enables the policy to apply only to entries within some subset of the administrative area and meeting specific object class requirements.

Access control policy attributes for users are termed prescriptive-ACI attributes, in contrast to those held in entries, which are termed entry-ACI attributes. In addition, there are two further policy attributes: access-control-scheme (which defines in this case that basic access control is being used), and subentry-ACI (which controls access to sub entries themselves). Both of these last are held in administrative entries.

An individual ACIItem contains a set of users, a set of protected objects and a set of permissions or denials relative to these. The basis protected objects are entries, attributes and attribute values, and an individual permission is defined for individual sub functions within the directory operations (e.g. adding an entry, attribute or value, or testing an attribute or value for compliance with a search filter). There are 12 pairs of distinct permissions/denials.

Permissions are potentially relevant to a user within the defined set only if the locally-assessed quality of authentication is adequate. Denials similarly apply to all users that cannot prove themselves exempt, again based on the locally-assessed quality of authentication.

In assessing access to a particular protected item, a combination of entry and policy access controls can apply. The evaluation of these is termed the Access Control Decision Function and results in a grant or denial. Some access controls apply at a background or default level, while others carry a higher level of authority. To model this, each ACIItem component carries a precedence value. For any item, only the relevant ACIItems of highest precedence are considered.

Special provisions are implemented to ensure that access control protection applies uniformly, even with chaining.

The 1992 Recommendations also define Simplified Access Control which is the same as Basic Access Control, except that it forbids entryACIItems and ACIItems within inner administrative areas (i.e. entries that represent delegation of authority within a larger administrative area).

History

Document history	
March 1994	First Edition
March 1996	Converted into Adobe Acrobat Portable Document Format (PDF)