

Title: Final Proposed Draft Amendment of ISO/IEC 9579, Amendment 1
Information technology – Secure RDA

Date: 14 March 1998

Status Recommended for FPDAM Ballot and Comment by the RDA RG meeting,
February 1998 as authorised by SC21

Requested Action: Issue for FPDAM ballot and comment

Editor's Preface:

This text was initially prepared under the BSI/DTI Consultancy Drafting Scheme project 'Remote Database Access to cover Secure RDA' in September 1997 following the direction agreed at a meeting of ISO/IEC JTC1 / SC21 / WG3 / RDA in London in July 1997, and subsequently revised as a result of a meeting of ISO/IEC JTC1 / SC21 / WG3 / RDA in London in February 1998.

The background for this work is in:

RDA-KAN-23 (WG3 N2012)	Remote Database Access – Strategic Directions
RDA-MAD-16	Secure RDA
RDA-LGW-12	Secure RDA

Material that was in the first version of this document has been modified and moved to FDIS 9579 to resolve ballot comments received by the FCD 9579 editing meeting in February 1998.

Document Conventions

Informative Paragraphs

This document contains informative paragraphs that serve to clarify aspects of this International Standard, or which provide information about flexibility open to implementers of the protocol defined by this International Standard. Such paragraphs are introduced by the word "NOTE" followed by a number identifying the paragraph and are set out as in the following example:

NOTE 1 – This is an example of an informative note.

Discussion Paragraphs

This document contains informative paragraphs that serve to explain why certain design decisions have been taken to facilitate review by experts involved in the development of this International Standard. Such paragraphs are introduced by the word "DISCUSSION" followed by a number identifying the paragraph and are set out as in the following example:

DISCUSSION 1 – This is an example of a discussion note.

Discussion paragraphs will be deleted from this document prior to publication as an International Standard.

Incomplete Marker

This document contains markers that indicate that additional text is required, or existing text may need to be modified, prior to completion of this document.

Such markers appear with a surrounding box and a grey background as in the example below:

Example of Incomplete Marker

Incomplete markers will be satisfied and removed from this document prior to publication.

Editor:

*John Hadjioannou
Blue Star Information Systems Ltd
197 Grasmere Way
Linslade
Leighton Buzzard
LU7 7QB*

Office: +44 1525 374667

Email: john@minster.co.uk

Design Criteria

In preparing this document, the following design criteria were observed:

- 1) The document has been prepared as an amendment to ISO/IEC 9579 – Information Technology – Remote Database Access.
- 2) It is a stated aim of the RG to make RDA standards as self-contained as possible by reducing references to other standards to a minimum, particularly where reference to other standards requires a high degree of expertise in a non-database field.

FPDAM
INTERNATIONAL
STANDARD

ISO/IEC
9579

Third Edition
199y-xx-xx

Amendment 1
199x-xx-xx

**Information Technology —
Secure RDA**

Version: FPDAM
Date: 14 March 1998



Reference number
ISO/IEC 9579/Am1:199x(E)

Contents

Contents	ii
Foreword	iv
Introduction	v
1 Scope	1
2 Normative References	2
3 Interoperability	3
3.1 Interoperability with conforming RDA implementations	3
3.2 Interoperability with future editions	3
4 Amendments	4
4.1 Change Clause 1, Scope.....	4
4.2 Change Subclause 2.1, International Standards	4
4.3 Change Subclause 3.1, Interoperability between implementations	4
4.4 Change Subclause 4.1, Definitions	5
4.5 Change Subclause 5.4.4, SQL User Name and Password.....	5
4.6 Change Subclause 5.8, RDA Facilities for Security	5
4.7 Add Subclause 5.8.1, RDA Security Services.....	5
4.8 Add Subclause 5.8.2, Use of Transport Provider security facilities	6
4.9 Add Subclause 5.8.3, Use of Authentication in RDAConnect.....	6
4.10 Add Subclause 5.8.4, Use of MessageAuthentication in RDAMessage.....	7
4.11 Change Subclause 6.2, RDAMessage protocol element	7
4.12 Add Subclause 7.3.5, MessageAuthentication encoding element	8
4.13 Change Subclause 6.4.1, Invocation of the Request in the RDA-client environment	10
4.14 Change Subclause 6.4.2, Evaluation of the Request in the RDA-server environment	10
4.15 Change Subclause 6.4.3, Invocation of the Response in the RDA-server environment	10
4.16 Change Subclause 6.4.4, Evaluation of the Response in the RDA-client environment.....	10
4.17 Change Subclause 7.1, RDAConnect Operation	11
4.18 Change Subclause 7.14, RDAAttribute encoding element	12
4.19 Add Subclause 10.2.4, Provision of mandatory security facilities	12

FPDAM (14 March 1998) of ISO/IEC 9579/Am1:199x (E)

4.20	Add Subclause 10.2.5, Provision of optional security facilities.....	12
4.21	Change Annex A.5, Optional facilities for RDA-clients only.....	13
4.22	Change Annex A.6, Optional facilities for RDA-servers only.....	13
4.23	Change Annex G, ASN.1 Module for RDA.....	14
4.24	Add Annex I, Security Service Requirements.....	14
4.25	Add Subclause I.1, Potential Vulnerabilities.....	15
4.26	Add Subclause I.2, Authentication.....	15
4.27	Add Subclause I.3, Access Control.....	16
4.28	Add Subclause I.4, Transfer Integrity.....	17
4.29	Add Subclause I.5, Transfer Confidentiality.....	17
4.30	Add Subclause I.6, Storage Integrity.....	18
4.31	Add Subclause I.7, Storage Confidentiality.....	18
4.32	Add Subclause I.8, Non-repudiation.....	19
4.33	Add Annex J, Security Profiles.....	20
5	Conformance.....	22

Foreword

ISO (the International Organisation for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

International Standard ISO/IEC 9579/Am1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 32, *Data Management and Interchange*.

Introduction

Remote Database Access for SQL (RDA/SQL) International Standard is a member of a set of International Standards produced to facilitate the interworking of computer systems. This International Standard conforms to the model defined in ISO/IEC 10032, *Information Technology – Reference Model of Data Management*.

Remote Database Access for SQL can be used to provide remote data access to a database management system conforming to ISO/IEC 9075 (Database Language SQL).

The goal of Remote Database Access for SQL is to allow, with a minimum of technical agreement outside this standard, the interconnection of applications and database systems:

- from different manufacturers;
- under different managements;
- of different levels of complexity;
- exploiting different technologies.

An application may itself be a database system and therefore this International standard can be used to support multi-database system interworking.

This International Standard amends ISO/IEC 9579:199y so as to provide secure remote database access.

Information Technology — Secure RDA

1 Scope

This International Standard is an amendment to ISO/IEC 9579:199y, *Information Technology – Remote Database Access for SQL* (RDA).

When used in conjunction with ISO/IEC 9579:199y this International Standard:

- identifies potential security vulnerabilities in remote database access using RDA
- defines RDA facilities which protect against the potential vulnerabilities
- a set of security profiles that identify which RDA facilities and other security facilities are required for different levels of protection against potential vulnerabilities
- an amended Conformance Proforma.

This International Standard refers to but does not define:

- protocols and security mechanisms for communication confidentiality, integrity and authentication of communicating peers
- digital signature and authentication mechanisms supported by protocol elements of RDA

This International Standard does not define:

- recovery mechanisms in the event that transaction co-ordination fails
- support for storage integrity and confidentiality using cryptographic mechanisms
- mechanisms to counter Denial of Service attacks

2 Normative References

The following standards contain provisions, which through reference in this text constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below.

ISO/IEC 9579:199y *Information technology – Remote Database Access for SQL*

Members of ISO and IEC maintain registers of currently valid International Standards.

3 Interoperability

This clause defines the compatibility of RDA-client or RDA-server implementations of the Service and Protocol defined by ISO/IEC 9579:199y as amended by this International Standard with RDA-server or RDA-client implementations respectively of the Service and Protocol defined by ISO/IEC 9579:199y.

3.1 Interoperability with conforming RDA implementations

Conforming implementations of ISO/IEC 9579:199y (base implementation) are fully compatible with conforming implementations of ISO/IEC 9579:199y as amended by this International Standard (secure implementation) when:

- the Secure Implementation uses the same Transport Mapping as the Base Implementation, and
- the Secure Implementation operates with Security Profile 1

3.2 Interoperability with future editions

Features have been included in the Service and Protocol to permit server implementations to detect which version of the protocol a client has implemented and to behave appropriately.

Future editions of this Service and Protocol will be compatible with this edition to the extent that:

- Security features this International Standard will be retained in future editions using the same encodings.
- Changes to the encodings in future editions will be extensions that are recognised by implementations of this edition and discarded after raising an exception.

4 Amendments

4.1 Change Clause 1, Scope

After the sentence “This International Standard relies upon the facilities provided by ISO/IEC 9075 (SQL) and ISO/IEC 9075-3 (SQL/CLI).” add:

This International Standard also:

- identifies potential security vulnerabilities in remote database access using RDA
- defines RDA facilities which protect against the potential vulnerabilities

At the end of the bulleted list starting “Normative annexes provide:” add the bulleted item:

- a set of security profiles that identify which RDA facilities and other security facilities are required for different levels of protection against potential vulnerabilities

After the bulleted list starting “This International Standard does not constrain:” add:

This International Standard refers to but does not define:

- protocols and security mechanisms for communication confidentiality, integrity and authentication of communicating peers
- digital signature and authentication mechanisms supported by protocol elements of RDA

At the end of the bulleted list starting “This International Standard does not define:” add the bulleted items:

- support for storage integrity and confidentiality using cryptographic mechanisms
- mechanisms to counter Denial of Service attacks

4.2 Change Subclause 2.1, International Standards

Before the reference to ISO/IEC 8824-1 add:

ISO/IEC 7498-2:1989 *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*

After the reference to ISO/IEC 9075-4 add:

ISO/IEC 9594-8:1997 | ITU-T Recommendation X.509 (1997)
Information processing systems – Open Systems Interconnection – The Directory: Authentication Framework.

4.3 Change Subclause 3.1, Interoperability between implementations

Replace the paragraph “Where protected access is required, the RDA-client and RDA-server need to share common authentication mechanisms to inter-operate.” with:

Where protected access is required, the RDA-client and RDA-server need to share common cryptographic algorithms and authentication mechanisms to inter-operate.

4.4 Change Subclause 4.1, Definitions

Following the definition of “RDA Protocol” add the definition:

RDA Relay: a system that receives RDA protocol elements as defined in this International Standard for the purpose of forwarding them to the intended recipient.

4.5 Change Subclause 5.4.4, SQL User Name and Password

To the end of the paragraph beginning “ISO/IEC 9075-3 (SQL/CLI) provides for a User to identify themselves” add the sentence:

Additionally, the User Name may be authenticated by other forms of authentication token.

4.6 Change Subclause 5.8, RDA Facilities for Security

Remove the text from subclause 5.8.

4.7 Add Subclause 5.8.1, RDA Security Services

Add a new subclause headed 5.8.1 entitled “RDA Security Services” containing the text:

The requirements for security services are discussed in Annex I. These services are:

RDA Service User Authentication: corroboration of the identity of the Service User.

RDA-client Authentication: corroboration of the identity of the RDA-client.

RDA-server Authentication: corroboration of the identity of the RDA-server.

RDA Outgoing Access Control: access control enforced by the RDA-client Environment.

RDA Firewall Access Control: access control enforced by the RDA relay system

RDA Incoming Access Control: access control enforced by the RDA-server Environment.

SQL Access Control: access control enforced by the SQL-server.

RDA Transfer Integrity: protection of communication against unauthorised modification.

RDA Transfer Confidentiality: protection of communication against unauthorised disclosure.

RDA Request Non-repudiation: protection against the RDA-client denying having requested a specific RDA Operation.

RDA Response Non-repudiation: protection against the RDA-server denying having responded to a specific request for an RDA Operation.

The following subclauses describe how facilities defined or identified by this International Standard may be used to provide the security services. Profiles of combinations of services to achieve defined levels of security are defined in Annex J.

4.8 Add Subclause 5.8.2, Use of Transport Provider security facilities

Add a new subclause headed 5.8.2 entitled “Use of Transport Provider security facilities” containing the text:

The Transport Provider may have facilities for providing RDA Transfer Integrity, RDA Transfer Confidentiality, RDA-client Authentication and RDA-server Authentication.

A Transport Mapping is defined in 10.2 that can be used to provide RDA Transfer Integrity, RDA Transfer Confidentiality, RDA-client Authentication and RDA-server Authentication.

In cases where the RDA Client represents a single Service User then RDA Client Authentication may be used to support RDA Service User Authentication as described in 5.8.3.

4.9 Add Subclause 5.8.3, Use of Authentication in RDAConnect

Add a new subclause headed 5.8.3 entitled “Use of Authentication in RDAConnect” containing the text:

The RDAConnect operation fields AuthenticationType and Authentication can be used to authenticate the name of the RDA Service User as identified by the UserName field.

Four types of RDA Service User Authentication, identified by the AuthenticationType, are supported:

- *password*, the User Name is authenticated using a password carried in the Authentication field.
- *transfer*, the UserName is matched against the RDA-client identity authenticated by RDA-client Authentication (for example using a local equivalence table or mapping algorithm). This mechanism requires that the RDA-client represents a single Service User.

NOTE 18 – The Service User may, however, use several User Names to represent different privileges and may be represented by several RDA-clients.

- *attributeCertificate*, the User Name is related to the identity of an RDA-client by an Attribute Certificate (as defined in ISO/IEC 9598-8 | X.509 1997) carried in the Authentication field. This mechanism requires that the RDA-client represents a single Service User.

NOTE 19 – The Service User may, however, use several User Names to represent different privileges and may be represented by several RDA-clients. Also, if Service Users share common privileges, and do not need to be separately identified for other reasons (for example, accountability), then they can be treated as the same Service User for the purposes of authentication, sharing a common UserName authenticated through the same RDA-client.

- *other*, the Authentication field is used to carry authentication information to support an externally defined mechanism.

The AuthenticationType may also be set to *none* to indicate that no support is provided for RDA User Authentication.

An Attribute is provided to permit an RDA-client to request a particular type of RDA Service User Authentication:

AUTHENTICATION TYPE: a value defining the type of RDA Service User Authentication requested by the RDA-client Environment.

4.10 Add Subclause 5.8.4, Use of MessageAuthentication in RDAMessage

Add a new subclause headed 5.8.4 entitled “Use of MessageAuthentication in RDAMessage” containing the text:

Each RDAMessage protocol element has a field MessageAuthentication that provides a means of communicating information required for RDA Request Non-repudiation and RDA Response Non-repudiation.

Three levels of RDA Request Non-repudiation and RDA Response Non-repudiation are supported:

- *none*, no support is provided
- *originatorSigned*, RDA Non-repudiation is supported by a timestamp and signature produced by the originator of the message
- *ttpSigned*, RDA Non-repudiation is supported by a timestamp and signature produced by the originator of the message, together with a timestamp and signature produced by a trusted third party (TTP).

Attributes are provided to permit an RDA-client and an RDA-server to negotiate the RDA Request Non-repudiation level and the RDA Response Non-repudiation level, and for a Service User to request a particular level of RDA Request Non-repudiation and RDA Response Non-repudiation.

REQUEST NON-REPUDIATION PROVIDED: a value defining the level of RDA Request Non-repudiation provided by the RDA-client Environment.

REQUEST NON-REPUDIATION REQUIRED: a value defining the level of RDA Request Non-repudiation required by the RDA-server Environment.

RESPONSE NON-REPUDIATION SUPPORTED: a value defining the level of RDA Response Non-repudiation supported by the RDA-client Environment.

RESPONSE NON-REPUDIATION REQUIRED: a value defining the level of RDA Response Non-repudiation required by the RDA-client Environment.

4.11 Change Subclause 6.2, RDAMessage protocol element

Replace the definition of “MessageAuthentication” with:

MessageAuthentication: an RDAOctetString whose Encoded Value is a MessageAuthentication encoding element as defined in clause 7.3.5, or an empty string if communication is taking place without RDA Request non-repudiation and without RDA Response non-repudiation.

4.12 Add Subclause 7.3.5, MessageAuthentication encoding element

Add a subclause 7.3.5 entitled “MessageAuthentication encoding element” with text:

Function

Encode a MessageAuthentication parameter

Encoding

```
MessageAuthentication ::= SEQUENCE
{
  MessageNonRepLevel      INTEGER
  MessageResponseLevel   INTEGER OPTIONAL,
  MessageTimestamp       GeneralisedTime,
  OriginatorSignature    MessageAndTimeSig,
  OriginatorCertificate   CertificatePath,
  TtpSignature            MessageAndTimeSig OPTIONAL,
  TtpCertificate          CertificatePath OPTIONAL
}

MessageAndTimeSig ::= SIGNATURE
{
  SEQUENCE
  {
    MessageProtocol      RDAInt32,
    MessageVersion       RDAInt8,
    MessageEncoding      RDAInt8,
    MessageLength        RDAInt32,
    MessageRequestIdent  RDAInt64,
    MessageType          RDAInt16,
    MessageContext       RDAOctetString,
    MessageData          RDAOctetString,
    MessageNonRepLevel   INTEGER
    MessageResponseLevel INTEGER OPTIONAL,
    MessageTimestamp     GeneralisedTime
  }
}
```

Syntax and Encoding

DISCUSSION 9 – An implementation that makes use of Attribute Certificates will in general have the facilities to encode and decode ASN.1, so there is no need to provide a simplified encoding for MessageAuthentication.

The syntax of GeneralisedTime is defined in ISO/IEC 8824-1.

The syntax of CertificatePath and SIGNATURE are defined in ISO/IEC 9594-8 | ITU-T X.509.

The encoding of MessageAuthentication and its subfields is according to the Distinguished Encoding Rules (DER) of ISO/IEC 8825-1:1995.

NOTE 24 – This encoding is independent of the encoding chosen for the Transport Mapping

The Encoded Value of MessageAndTimeSig is the syntax of SIGNATURE applied to message fields encoded using the Default Encoding for RDA specific data types.

Encoding Parameters

MessageNonRepLevel: the non-repudiation level of this message. This is encoded as the value for a non-repudiation Attribute in Table 11.

MessageResponseLevel: if this message is a request for an RDA Operation then the value of the RESPONSE NON-REPUDIATION REQUIRED Attribute.

Other encoding parameters may be not present depending on the value of MessageNonRepudiateLevel according to Table 4.

Table 4 – Use of MessageAuthenticateParameters

Parameter	MessageNonRepudiate Level		
	<i>none</i>	<i>originatorSigned</i>	<i>ttpSigned</i>
MessageTimestamp	not present	present	present
OriginatorSignature	not present	present	present
OriginatorCertificate	not present	present	present
TtpSignature	not present	not present	present
TtpCertificate	not present	not present	present

Those encoding elements which are defined to be present by MessageNonRepudiateLevel have a value defined below (which may be null):

MessageTimestamp: the Timestamp for this message

OriginatorSignature: a signature calculated by the originator of the message.

OriginatorCertificate: the certificate for the originator's public key, the syntax of CertificatePath is as defined in ISO/IEC 9594-8 | ITU-T X.509.

TtpSignature: a signature calculated by a Trusted Third Party.

TtpCertificate: the certificate for the Trusted Third Party's public key, the syntax of CertificatePath is as defined in ISO/IEC 9594-8 | ITU-T X.509

4.13 Change Subclause 6.4.1, Invocation of the Request in the RDA-client environment

Replace the General Rule numbered 8) with:

- 8) If required, the MessageAuthentication field is computed and encoded into *E*, with MessageNonRepLevel set to the level being applied to this message, and MessageResponseLevel set to the level required in the response.

4.14 Change Subclause 6.4.2, Evaluation of the Request in the RDA-server environment

Renumber the General Rule 11) as 12) and after the General Rule 10) add:

- 11) If required, the MessageAuthentication field is checked. If the OriginatorSignature or TtpSignature verification fails then the exception is raised: RDA-specific condition: authentication failure. *M* may be archived for later protection against repudiation.

4.15 Change Subclause 6.4.3, Invocation of the Response in the RDA-server environment

Renumber the General Rules 4), 5) 6) and 7) as 8), 9), 10) and 11) respectively, and after the General Rule 3) add:

- 4) Let *RL* be the MessageResponseLevel of *RO*.
- 5) If the RDA-server does not support the RDA Response Non-Repudiation Level *RL* then the exception is raised RDA-specific condition: authentication failure.
- 6) If *RL* is not none then the MessageAuthentication field is computed and encoded into *E* according to *RL*.
- 7) MessageNonRepLevel is set to *RL*.

4.16 Change Subclause 6.4.4, Evaluation of the Response in the RDA-client environment

Renumber the General Rule 8) as 9) and after the General Rule 7) add:

- 8) If required, the MessageAuthentication field is checked. If the OriginatorSignature or TtpSignature verification fails then the exception is raised: *RDA-specific condition: Message Authentication failure*. *M* may be archived for later protection against repudiation.

4.17 Change Subclause 7.1, RDAConnect Operation

In the definition of “Authentication”, at the end of the bulleted list, add:

- *transfer*, the transport mapping is to a Transport Provider that authenticates the RDA-client. The RDA-server can validate that the RDA-client can rightfully use UserName (for example using a local equivalence table or mapping algorithm). The value of Authentication is ignored
- *attributeCertificate*, Authentication carries an Attribute Certificate as defined in ISO/IEC 9594-8 | ITU-T X.509, with the subject field set to the RDA-client name (that is the identity of the RDA-client authenticated by the transport mapping) and the attribute field set to UserName. The Transport Mapping is to a Transport Provider that authenticates the RDA-client.
 NOTE 26 – This field is encoded according to the Distinguished Encoding Rules (DER) of ISO/IEC 8825-1.
- *other*, Authentication carries a field of type SEQUENCE { OBJECT IDENTIFIER, AuthenticationInformation } where the syntax and semantics of AuthenticationInformation is as identified by the OBJECT IDENTIFIER

In the “RDA-server Evaluation Rules”, replace General Rule 8) with:

- 8) Case:
- a) If *AT* is *transfer*:
 - i) If *RC* has not been authenticated by the Transport Provider then the exception is raised: *RDA-specific condition: authentication failure.*
 - ii) If *RC* cannot rightfully use *UN*, then the exception is raised: *RDA-specific condition: authentication failure.*
 - b) If *AT* is *password* and the security policy indicates that password checks are to be carried out by the RDA-server rather than the SQL-server and the password check fails, then the exception is raised: *RDA-specific condition: authentication failure.*
 - c) If *AT* is *attributeCertificate*:
 - i) If the Attribute Certificate *AU* fails to be validated, then the exception is raised: *RDA-specific condition: authentication failure.*
 - ii) If *RC* has not been authenticated by the Transport Provider then the exception is raised: *RDA-specific condition: authentication failure.*
 - iii) If the subject of Attribute Certificate *AU* is not *RC* then the exception is raised: *RDA-specific condition: authentication failure.*
 - iv) If the attribute of Attribute Certificate *AU* is not *UN* then the exception is raised: *RDA-specific condition: authentication failure.*

4.18 Change Subclause 7.14, RDAAttribute encoding element

Replace the last row of Table 9 – Extension of Table 19 of ISO/IEC 9075-3 with the rows:

AUTHENTICATION TYPE	INTEGER	0 (<i>none</i>); 1 (<i>password</i>); 2 (<i>transfer</i>); 3 (<i>attributeCertificate</i>); 4 (<i>other</i>)
REQUEST NON-REPUDIATION PROVIDED	INTEGER	0 (<i>none</i>); 1 (<i>originatorSigned</i>); 2 (<i>ttpSigned</i>)
REQUEST NON-REPUDIATION REQUIRED	INTEGER	0 (<i>none</i>); 1 (<i>originatorSigned</i>); 2 (<i>ttpSigned</i>)
RESPONSE NON-REPUDIATION SUPPORTED	INTEGER	0 (<i>none</i>); 1 (<i>originatorSigned</i>); 2 (<i>ttpSigned</i>)
RESPONSE NON-REPUDIATION REQUIRED	INTEGER	0 (<i>none</i>); 1 (<i>originatorSigned</i>); 2 (<i>ttpSigned</i>)

4.19 Add Subclause 10.2.4, Provision of mandatory security facilities

Add a new subclause 10.2.4 entitled “Provision of mandatory security facilities” with text:

RDA Transfer Integrity shall be provided by applying Integrity Protection, at least, to all TLS Records carrying RDA Protocol elements.

4.20 Add Subclause 10.2.5, Provision of optional security facilities

Add a new subclause 10.2.5 entitled “Provision of optional security facilities” with text:

If required, optional security facilities shall be supported as follows:

RDA-server Authentication shall be supported using certificates defined in ISO/IEC 9594-8.

RDA-client Authentication shall be supported using certificates defined in ISO/IEC 9594-8.

Transport RDA Service User Authentication shall be supported by placing the UserName field of RDAConnect in the subjectDirectoryAttributes certificate extension field of the RDA-client certificate.

RDA Transport Confidentiality shall be supported by using the TLS Record protocol with encryption.

4.21 Change Annex A.5, Optional facilities for RDA-clients only

Replace entry A.5.8 with:

A.5.8	Which RDA Service User Authentication types are provided (check all that apply): None ? , Password ? , Transfer ? , AttributeCertificate ?
A.5.9	Specify Other RDA Service User Authentication types that are provided (or none):
A.5.10	What levels of RDA Request Non-repudiation are provided (check all that apply): None ? , OriginatorSigned ? , TtpSigned ?
A.5.11	What levels of RDA Response Non-repudiation are supported (check all that apply): None ? , OriginatorSigned ? , TtpSigned ?

4.22 Change Annex A.6, Optional facilities for RDA-servers only

Replace entry A.6.9 with:

A.6.9	Which RDA Service User Authentication types are provided (check all that apply): None ? , Password ? , Transfer ? , AttributeCertificate ?
A.6.10	Specify Other RDA Service User Authentication types that are provided (or none):
A.6.11	What levels of RDA Request Non-repudiation are provided (check all that apply): None ? , OriginatorSigned ? , TtpSigned ?
A.6.12	What levels of RDA Response Non-repudiation are supported (check all that apply): None ? , OriginatorSigned ? , TtpSigned ?

4.23 Change Annex G, ASN.1 Module for RDA

Before the line beginning “RDAConnect” add:

```
MessageAuthentication ::= SEQUENCE
{
  MessageNonRepLevel      INTEGER
  MessageResponseLevel   INTEGER OPTIONAL,
  MessageTimestamp       GeneralisedTime,
  OriginatorSignature    MessageAndTimeSig,
  OriginatorCertificate   CertificatePath,
  TtpSignature            MessageAndTimeSig OPTIONAL,
  TtpCertificate          CertificatePath OPTIONAL
}

MessageAndTimeSig ::= SIGNATURE
{ SEQUENCE
{
  MessageProtocol      RDAInt32,
  MessageVersion       RDAInt32,
  MessageEncoding      RDAInt32,
  MessageLength        RDAInt32,
  MessageRequestIdent  RDAInt64,
  MessageType          RDAInt32,
  MessageContext       RDAOctetString,
  MessageData          RDAOctetString,
  MessageNonRepLevel   RDAInteger
  MessageResponseLevel RDAInteger OPTIONAL,
  MessageTimestamp    GeneralisedTime
}
}
```

4.24 Add Annex I, Security Service Requirements

Add a new Informative Annex I entitled “Security Service Requirements” with text:

This Annex presents the requirements for protecting remote database access against potential violations of security. These requirements are described in terms of:

- an identification of the potential violations of security
- requirements for each of: Authentication, Access Control, Transfer Integrity, Transfer Confidentiality, Storage Integrity, Storage Confidentiality and Non-repudiation

Three distinct entities are identified in clause 5.1: Service User, RDA Client, RDA Server. The security service requirements are expressed with reference to these entities in terms of security services similar to those defined in ISO/IEC 7498-2 but adapted to the RDA protocol.

4.25 Add Subclause I.1, Potential Vulnerabilities

Add a new subclause I.1 entitled “Potential Vulnerabilities” with text:

Communications defined by this International Standard may be vulnerable to the following threats:

Denial of Service: the prevention of authorised access to SQL-data or the delaying of time-critical RDA Operations.

RDA Request Repudiation: the denial by an RDA-client of having sent an RDAMessage requesting an RDA Operation.

RDA Response Repudiation: the denial by an RDA-server of having sent an RDAMessage with the results of an RDA Operation.

RDA-client Masquerade: the pretence by an RDA-client to be some other RDA-client.

RDA-server Masquerade: the pretence by an RDA-server to be some other RDA-server.

Service User Masquerade: the pretence a Service User to be some other Service User.

Transfer Modification: the unauthorised altering or destruction of an RDAMessage.

Transfer Monitoring: the unauthorised disclosure of the contents of an RDAMessage.

Replay: the unauthorised recording and repetition of an RDAMessage.

The provisions of this International Standard address all these potential violations of security, with the exception of Denial of Service, which is beyond the scope of this International Standard.

4.26 Add Subclause I.2, Authentication

Add a new subclause I.2 entitled “Authentication” with text:

The Service User identity may need to be known by the RDA-client environment or the RDA-server environment for the application of identity based access control, for audit purposes, for identification of the “owner” (creator) of data objects or for charging.

To counter Service User masquerade *RDA Service User Authentication* is required.

In situations where the Service User can connect to an RDA-server Environment using different RDA clients, or an RDA-client Environment includes several Service Users, it may be necessary for the RDA-server Environment to identify the RDA-client independently of the Service User identity. For example, the RDA-server may enforce access control based on RDA-client identity to ensure that access to data private to an organisation is not accessible from a system on an external public network, or the RDA-client identity may need to be known for accountability and auditing.

To counter RDA-client masquerade *RDA-client Authentication* is required. To counter RDA-client masquerade *RDA-client Authentication* is required.

In some cases, such as single user workstations, it may not be necessary to distinguish between the Service User identity and RDA-client identity. In such situations, RDA-client Authentication may be used as the basis for RDA Service User Authentication.

FPDAM (14 March 1998) of ISO/IEC 9579/Am1:199x (E)

NOTE 48 – Because of the layering of the security mechanisms and protocol it is not generally possible for SQL Authentication to be used for RDA-client Authentication.

The identity of the RDA-server may need to be confirmed for the Service User to have confidence in the source of data and the effect of other operations. The RDA-server identity may need to be confirmed for the RDA-client Environment to apply outgoing access control to inhibit unauthorised access to certain remote SQL-servers.

To counter RDA-server masquerade *RDA-server Authentication* is required.

RDA-client Authentication and *RDA-server Authentication* are forms of Peer Entity Authentication as defined in ISO/IEC 7498-2.

RDA Service User Authentication is corroboration of the Service User identity.

All these forms of authentication can be based on passwords (if there is no risk of monitoring or replaying passwords), cryptographic based authentication tokens, or digital signature mechanisms. These mechanisms can be supported either directly by the RDA Protocol (*RDA Service User Authentication*) or by the Transport Provider (*RDA-client Authentication* and *RDA Server Authentication*).

4.27 Add Subclause I.3, Access Control

Add a new subclause I.3 entitled “Access Control” with text:

Protection against attempted unauthorised access to SQL-data may be provided by enforcing access control either:

- at an RDA-client – this generally grants or denies access to an entire SQL-server. This form of access control is termed *RDA Outgoing Access Control*.
- in an intermediate (firewall) system between an RDA-client and an RDA-server – this generally grants or denies specific RDA Operations for a given RDA-server or SQL-server. This form of access control is termed *RDA Firewall Access Control*.
- at an RDA-server – this generally grants or denies access to an entire SQL-server. This form of access control is termed *RDA Incoming Access Control*.
- within an SQL-server – this generally grants or denies access to particular parts of the SQL-data associated with the SQL-server for particular types of operation. This form of access control is termed *SQL Access Control* and is defined in ISO/IEC 9075.

The access control services identified above are forms of access control as defined in ISO/IEC 7498-2.

Access control may be provided using:

- Identity based access control where the entity enforcing the access control uses information on access rights associated with identified entities. The identification generally requires authentication to corroborate the identity.
- Label based access control where access is granted or denied based on the matching of labels associated with protected objects against clearances associated with the accessor.
- Capability based access control where a capability is used to represent right of access.
- Context based access control where contextual information, such as time of day, is used in deciding whether to grant or deny access.

This standard currently only specifies use of identity based access control.

RDA Outgoing Access Control applied in an RDA-client Environment uses the identity of the Service User to decide whether to grant or deny access to a specific RDA-server. Authentication of the Service User is a local matter. The RDA-server may be authenticated using *RDA Server Authentication*.

RDA Firewall Access Control applied within a Transport Provider uses either the identity of the Service User, optionally authenticated using *RDA User Authentication*, or the identity of the RDA-client, optionally authenticated using *RDA Client Authentication*, to grant or deny a specific RDA Operation to pass through to a specific RDA-server.

RDA Incoming Access Control applied within an RDA-server Environment uses the identity of the RDA-client, optionally authenticated using *RDA Client Authentication*, to grant or deny access to an SQL-server within the RDA-server Environment.

SQL Access Control applied within an SQL-server uses the identity of the Service User, optionally authenticated using *RDA User Authentication*, to grant or deny access to the SQL-server as defined by ISO/IEC 9075.

The management of access control information (e.g. access control lists) is outside the scope of this International Standard.

4.28 Add Subclause I.4, Transfer Integrity

Add a new subclause I.4 entitled “Transfer Integrity” with text:

The RDA protocol and SQL data may be subject to Transfer Modification or Transfer Replay attacks when passing over vulnerable data networks.

To protect the integrity of SQL-data against such attacks *RDA Transfer Integrity* is required.

RDA Transfer Integrity is a form of connection integrity with recovery as defined in ISO/IEC 7498-2. Recovery is effected by the protocol rules of 6.4.5 which prescribe that a transaction is rolled-back in the event of communication failure in any component part of the transaction.

RDA Transfer Integrity can be provided using cryptographic check codes or digital signatures applied by the Transport Provider.

4.29 Add Subclause I.5, Transfer Confidentiality

Add a new subclause I.5 entitled “Transfer Confidentiality” with text:

RDA Operations and results may be subject to monitoring by unauthorised parties when passing over vulnerable networks.

To protect the confidentiality of RDA Operations and results against such attacks *RDA Transfer Confidentiality* is required.

RDA Transfer Confidentiality is a form of connection confidentiality as defined in ISO/IEC 7498-2.

RDA Transfer Confidentiality can be provided by encipherment mechanisms within the Transport Provider.

4.30 Add Subclause I.6, Storage Integrity

Add a new subclause I.6 entitled “Storage Integrity” with text:

The SQL-data associated with an SQL-server may be subject to attempted unauthorised modification.

Access control as described in I.3 may be applied by the SQL-server to protect the integrity of the SQL-data against such attacks. If SQL access control is not sufficiently trusted for integrity, cryptographic mechanisms, such as digital signatures can be used to protect the data or sensitive portions of the data. This protection can be applied by the SQL-client or by the Service User.

NOTE 49 – The use of cryptographic mechanisms for protecting data may require modification to the schemas of the SQL-data to include the digital signatures.

The use of cryptographic mechanisms for storage integrity is not currently addressed by this International Standard.

Within an SQL transaction a Service User may explicitly connect to several SQL-servers, the RDA-client environment may decompose an SQL-query into fragments that are applied to different SQL-servers or an SQL-server may decompose an SQL-query into fragments that are applied to different SQL-servers. Where data manipulated by a Service User is distributed across several SQL-servers incomplete or inconsistent changes to SQL-data may occur due to the nature of the SQL operations, system or network failures, or malicious attacks on the integrity of the updates by unauthorised parties.

To protect against such incomplete or inconsistent changes *RDA Transaction Co-ordination* is required.

RDA Transaction Co-ordination can be provided by facilities within the RDA Protocol and RDA Operations, or by other external facilities.

4.31 Add Subclause I.7, Storage Confidentiality

Add a new subclause I.7 entitled “Storage Confidentiality” with text:

The SQL-data associated with an SQL-server may be subject to attempted unauthorised disclosure.

Access control may be applied by the SQL-server to protect the confidentiality of SQL-data against such attacks. If SQL access control is not sufficiently trusted for confidentiality, encipherment, applied by the SQL Client or Service User, can be used to protect the data or sensitive portions of the data.

NOTE 50 – The use of encipherment may limit the operations that can be performed on the data, in particular with regard to integrity constraints, keys, and selection.

The use of encipherment for storage confidentiality is not currently addressed by this International Standard.

4.32 Add Subclause I.8, Non-repudiation

Add a new subclause I.8 entitled “Non-repudiation” with text:

This Annex presents profiles that combine the facilities provided by this International Standard in a coherent way to provide four Security Profiles. All but the first provide security services to protect against all threats to RDA security identified in Annex F, other than denial of service and repudiation. The four security profiles differ in the management overhead placed on the Service User and the RDA-server Environment.

A Service User may deny (repudiate) having initiated use of an SQL server through an RDA operation (or sequence of operations) or an SQL server may repudiate carrying out that operation.

To protect against such attacks *RDA request non-repudiation* and *RDA response non-repudiation* are required.

RDA request non-repudiation and *RDA response non-repudiation* are forms of non-repudiation as defined in ISO/IEC 7498-2.

Non-repudiation can be provided using digital signatures and time-stamping. In some situations, an additional digital signature, provided by a trusted third party against the time-stamped data, may be necessary. This trusted third party signature is only provided if the time-stamp is current.

4.33 Add Annex J, Security Profiles

Add a new Informative Annex J entitled “Security Profiles” with text:

RDA Transaction Co-ordination, RDA Suspend and Resume, Access Control security services and RDA Non-repudiation security services can be applied as an adjunct to any of the security profiles listed below. Access control security services can reduce the risk of Denial of Service attacks.

Security Profile 1: the TCP/IP transport mapping is used with password authentication. This offers a basic level of security without Transfer Integrity or Confidentiality. The RDA-server Environment maintains user name and password tables. The Service User maintains a password for each RDA-server Environment.

Security Profile 2: the TLS transport mapping is used with password authentication. This offers Transfer Integrity, Transfer Confidentiality and Server Authentication. The RDA-server Environment maintains user name and password tables. The Service User maintains a password for each RDA-server Environment.

Security Profile 3: the TLS transport mapping is used with Transfer RDA Service User Authentication. The RDA-server Environment maintains RDA-client to User Name mapping tables.

Security Profile 4: the TLS transport mapping is used with Attribute Certificate RDA Service User Authentication. Information required for RDA Security is managed on a network basis.

For each Security Profile, Table G.1 indicates the facilities used to achieve that Security Profile and Table G.2 indicates the services provided by that Security Profile.

Table G.1 – Security Profiles – Facilities Used

<i>Facility</i>	<i>Profile 1</i>	<i>Profile 2</i>	<i>Profile 3</i>	<i>Profile 4</i>
Transport Mapping	TCP/IP	TLS	TLS	TLS
Authentication	Password	Password	Transfer	Attribute Certificate

Table G.2 – Security Profile – Services Provided

<i>Service</i>	<i>Profile 1</i>	<i>Profile 2</i>	<i>Profile 3</i>	<i>Profile 4</i>
RDA Firewall Access Control	Optional	Optional	Optional	Optional
RDA Incoming Access Control	Yes	Yes	Yes	Yes
RDA Outgoing Access Control	Optional	Optional	Optional	Optional
RDA Request Non-repudiation	No	Optional	Optional	Optional
RDA Response Non-repudiation	No	Optional	Optional	Optional
RDA Service User Authentication	Password	Password	Transfer	X.509

FPDAM (14 March 1998) of ISO/IEC 9579/Am1:199x (E)

RDA Suspend and Resume	Optional	Optional	Optional	Optional
RDA Transaction Co-ordination	Optional	Optional	Optional	Optional
RDA Transfer Confidentiality	No	Yes	Yes	Yes
RDA Transfer Integrity	No	Yes	Yes	Yes
RDA-client Authentication	No	Optional	Optional	Optional
RDA-server Authentication	No	Yes	Yes	Yes
SQL Access Control	Yes	Yes	Yes	Yes

5 Conformance

An implementation may not claim conformance to this International Standard.

An implementation may claim conformance to ISO/IEC 9579-199y as amended by the provisions contained within this International Standard. Claims of such conformance shall be accompanied by a completed proforma for the information listed in Annex A of ISO/IEC 9579:199y as amended by the provisions contained within this International Standard.