IEEE

IEEE Standards
PROJECT AUTHORIZATION REQUEST (PAR)

1. Date of Request: 16 March 1990

2. Assigned Project #: P802.10

3. Does this PAR revise a previously approved PAR? ☒ YES ☐ NO

4. Description of Proposed Document:
Standard ☒ Recommended Practice ☐ Guide ☐
New ☐ Revision ☒ of Std. P802.10/D6 12 September 1989
Trial Use ☐ Full Use ☒

5. Project Title:
Standard for Interoperable LAN Security (SILS) Part B - Secure Data Exchange (P802.10B)

6. Scope of Proposed Standard: *(Use attachment sheet if necessary.)*

See Attachment.

7. Purpose of Proposed Standard: *(Use attachment sheet if necessary.)*

See Attachment.

8. SPONSOR: Society: Computer Society
Committee: Computer Communications, Security and Privacy

9. Name of group that will write the standard: The LAN Security Working Group

10. Target Completion Date: August 1990

11. Proposed Coordination: *(See instructions.)* Method of Coordination:

SCC10 (IEEE Dictionary)

See Attachment.

12. Are you aware of any patent, copyright, or trademark issues? ☒ YES ☐ NO
(If yes, attach a sheet with an explanation.)

Are you aware of any standards or projects with a similiar scope? ☒ YES ☐ NO
(If yes, attach a sheet with a complete description of the impact of the similarities.)

TEAR HERE

Attachments to Standards Project Authorization (PAR)

Scope

The scope of the Standard for Interoperable LAN Security (SILS) is to define a standard for services, protocols, data formats, and interfaces that will allow secure IEEE 802 LAN products to interoperate. IEEE 802.10 has specified three areas for standardization: Secure Data Exchange, Key Management, and Security Management, and the objects necessary to manage each protocol. The goals of each of these areas of SILS are to be as independent as possible of any particular encryption algorithm, such as DES or RSA, and of the transmission media. The work in each area is based on the OSI Seven Layer model (IS 7498) and on the OSI Security Architecture (IS 7498/2).

The Secure Data Exchange (SDE) Standard specifies a Layer 2 security protocol that will provide security services using encryption, so that data on an 802 LAN will not be compromised. This protocol resides between the Logical Link Control (LLC) sublayer and the Media Access Control (MAC) sublayer in the 802 architecture. The security services that the standard provides are: data confidentiality and connectionless data integrity. Support to Key Management, if Key Management is present, can be provided by SDE for the services of data origin authentication, and access control.

The appendices to the SILS SDE standard provide explanatory information for the standard. The Rationale for Layer 2 Security Services Appendix explains why the services that SDE provides are appropriate for LANs and how those services address the threats to LAN security. The Examples of Algorithms Appendix gives an example of the use of SDE with particular algorithms. The Objectives of SILS Appendix lists the objectives that the SDE was designed to meet. The Rationale for Placement Appendix explains the reasons for putting the SDE between the MAC and the LLC 802 sublayers. The Fragmentation Appendix recognizes that vendors are planning to provide fragmentation at Layer 2 and provides a standard fragmentation method so that SDE devices will interoperate.

Purpose

The purpose of the Standard for Interoperable LAN Security (SILS) is threefold. First, the standard must specify the minimally acceptable security services to be supported primarily by encryption for IEEE 802 LANs. Second, the standard must define logical and physical mechanisms for achieving these services; this includes the managed objects required to support the processing to provide the services. Finally and most important, the standard must maximize interoperability of products in an open systems interconnection architecture.

Modern LANs provide users connectivity to network resources. Distributed applications and shared resources allow users easy access to the network data. The intended result is that data is

readily available to all users. However, as use of LAN resources increases in commercial and military environments, the data security threat increases. Manufacturing design data, financial analysis data, and health data cannot be protected from modification, disclosure, or unauthorized access without LAN security. The communication required between these systems cannot be achieved without interoperability of the security mechanisms protecting these systems.

To provide interoperable security mechanisms, the SILS Secure Data Exchange standard must consider the issues of cryptography, of IEEE 802 LAN compatibility, and of OSI compatibility. The cryptography issue is to define the SDE to be as independent of any particular algorithm as possible. Thus an appendix is included to show an example of the use of SDE with different algorithms.

The issue of IEEE 802 LAN compatibility is that the security mechanisms of the SDE should not require changes to the existing IEEE 802 LAN standards. For example, when the 802.2 PDUs are encrypted, there should not be any modification to the 802.2 protocol operation. Thus the SDE has a requirement of transparency to 802 protocols.

For SDE to be compatible with OSI, in particular, the OSI Security Architecture, it is required to support data confidentiality. In fact, SDE offers three extra services of data integrity, data origin authentication, and access control. The rationale for these services is supplied in an appendix and discussions with ISO about these services are ongoing. As ISO did not take LANs into account, nor consider that they are more vulnerable than Wide Area Networks, the extra services required to protect a LAN are not surprising.

Sponsor

There are two technical committees who co-sponsor the LAN Security Working Group. These committees are the Technical Committee on Computer Communications and the Technical Committee on Security and Privacy. The primary sponsor of the LAN Security Working Group will be the 802 Standards Subcommittee of the Technical Committee on Computer Communications. The LAN Security Working Group meets in conjunction with 802, participates in the 802 Executive Committee, and adheres to the 802 Operating Rules.

The Technical Committee on Security and Privacy provides the security expertise by participating in the ballot process. In addition, the Technical Committee on Security and Privacy will provide a representative to the Standards Coordinating Committee and the Standards Activities Board.

Proposed Coordination

The following is a list of groups with whom the LAN Security Working Group will coordinate on the Standard for Interoperable LAN Security (SILS) Secure Data Exchange and the type of coordination planned.

Group	Type of Coordination
SCC10 (IEEE Dictionary)	Circulation of Drafts
ANSI X3S3 Data Communications	Circulation of Drafts
ANSI X3T5 OSI	Circulation of Drafts
ISO-IEC/JTC1/SC21 Information Retrieval,Transfer, and Management of OSI, ISO-IEC/JTC1/SC27 Information Processing Systems Data Cryptographic Techniques, ISO-IEC/JTC1/SC6 Telecommunications and Information Exchange Between Systems (WG1 and WG3)	Circulation of Drafts
ECMA TC32/TG9 Security in Open Systems	Circulation of Drafts

Patent Issues

1. Data Encryption Standard (DES)

There are two patents for DES, both held by IBM. IBM made DES available under these patents as stated in the Federal Register Notice of March 17, 1975: "IBM stated they would grant requested, non-exclusive, royalty-free licences for certain patents that could not be avoided when implementing and using DES."

2. RSA Algorithm

RSA is named for its inventors, Ronald Rivest, Adi Shamir, and Leonard Adelman. The patent for RSA is held by MIT as U.S. patent 4405829. This patent which may cover part of the use of SILS, may be used as described in the attached letter from RSA Incorporated.

3. SEEK Algorithm

SEEK is a public key cryptography algorithm for key management. The patents which cover the algorithm are held by Stanford University as U.S. patents 42007700, 4218582, and 4424414. These patents which may cover part of the use of SILS, may be used as described in the attached letter from Stanford University.

Note: In January 1990, Cylink and RSA announced at an ANSI meeting that they are forming a new company to be called Public Key Partners (PKP). Stanford and MIT will be

beneficiaries of this consortium. PKP will be the exclusive licensing representative for all public key patents, thus facilitating the choice and use of public key algorithms. In preliminary discussions, PKP intends to licence their public key algorithms for fair, equitable, and non-onerous fees. Once PKP is formed, 802.10 will request a letter from PKP addressing the licensing of public key algorithms appropriate for use with Secure Data Exchange, with Key Management, and with Security Management. If PKP does not agree to reasonable licensing fees, then references and technology that may depend on public key will be withdrawn from the 802.10 standards.

Projects with Similar Scope

1. Secure Data Network System (SDNS).

The SDNS project has goals which in many ways are complementary to those of the Standard for Interoperable LAN Security (SILS) project in that both projects intend to develop architectures and protocols that can be used to secure networks. However, to date the SDNS project primarily has addressed long haul communications and has concentrated on protocols for Layers 3 and 4 with Key Management to support those protocols. The SDNS recently has forwarded copies of their secure protocol definitions to ANSI for consideration as ISO standards.

In contrast, the SILS standard effort is concentrating on LANs and is intended for the commercial market. The SILS project already has established technical liaisons with the SDNS effort to ensure that when feasible work is done by either project, that work is shared and/or used by both projects where possible.

2. ANSI X3.105, Data Link Encryption 1983.

ANSI X3.105 is a standard which was created by X3T1 and published in 1983. The scope of the standard is to specify the encrypting and decrypting of data on a single data link using DES in a one bit Cypher Feedback mode. This standard is not applicable to LANs and thus is not a duplicate effort of the SILS project.

3. ISO 9160, Link Encryption Standard 1988.

ISO 9160 is a standard which was created by ISO-IEC/JTC1/SC20. The scope of the standard is to specify a protocol which externally is algorithm independent. The standard does not address the management or distribution of encryption keys. In addition, this standard is not applicable to LANs and thus does not duplicate the efforts of the SILS project.