Project Proposal For A New INCITS Standard
Fibre Channel Security Protocols Second Generation

(FC-SP-2)

T11/06-010v1

1 Source of the Proposed Project

1.1 Title

Fibre Channel Security Protocols 2 (FC-SP-2)

1.2 Date Submitted

05 January 2006

1.3 Proposer(s)

INCITS TC T11, with a current membership of 50.

2 Process Description for Proposed Project

2.1 Project Type (Development or Revision)

Type D (Development done within INCITS T11)

2.2 Type of Document

Standard

2.3 Definition of Concepts and Special Terms

None

2.4 Expected Relationship with Approved Reference Models, Frameworks, Architectures, etc.

All Fibre Channel standards are intended for use in closed systems.

2.5 Recommended INCITS Development Technical Committee (Existing or New)

It is recommended that this project be assigned to TC T11, in order that the project be coordinated with work on other Fibre Channel standards.

2.6 Anticipated Frequency and Duration of Meetings

This project will make use of the regularly-scheduled bimonthly T11 plenary meetings. Informal Working Groups will be organized on an ad-hoc basis to discuss specific subjects where appropriate.

2.7 Target Date for Initial Public Review (Milestone 4)

December 2007

2.8 Estimated Useful Life of Standard or Technical Report

It is anticipated that this standard will have a useful life of over 10 years.

3 Business Case for Developing the Proposed Standard or Technical Report

3.1 Description

This project proposal recommends the development of a set of additional and enhanced services that will be used to support the security of Fibre Channel configurations.

Included within this scope are:

a) Consideration of Fabric Loop Security issues

b) Authentication Material Distribution and Management

c) Fabric (as a whole) Credential Definition and Management

d) Additional management interface to support SA Management policy

e) FC-IFR Security support

f) Secure hash algorithm changes (e.g. use of SHA-256), and

g) Any other item as deemed necessary during the development.

Where they exist, the protocols, formats and definitions contained in existing standards will be considered for use in FC-SP-2.

3.2 Existing Practice and the Need for a Standard

Development of the first generation Fibre Channel Security Protocol (FC-SP) draft began in 2002. The FC-SP project addressed the basic Fibre Channel security protocols required to provide the security of Fibre Channel environments. The FC-SP project developed a set of methods that allow security techniques to be implemented in a Fibre Channel fabric and among the fabric elements and N_ports in a Fibre Channel fabric. The Fibre Channel security protocols defined in FC-SP include Security Association (SA) management (supporting encryption and integrity techniques), Fabric Policy (authorization), and authentication services. These protocols provide means to guard against malicious attacks, accidental configuration changes, and to ensure tighter control of deployed configurations.

Today, commonly deployed security techniques are centered about zoning and FC-SP techniques. FC-GS-5 provides an upper layer protocol called CT Authentication and Confidentiality to protect Common Transport (CT) traffic. FC-FS-2 defines lower layer ESP_Header Authentication and Confidentiality headers related to Fibre traffic. There are no standards for specifying policies for Fibre Channel N_ports and no interoperable methods for authentication and distribution of secrets needed to maintain the security of a fabric, its elements, and N_ports in a Fibre Channel fabric. There is no defined management interface to support SA management policy. Loop connections may pose additional unresolved issues.

The FC-IFR project also provides for an infrastructure to extend Fibre Channel storage protocol routing functions. The FC-IFR project is defining methods to manage Fibre Channel routing functions with references to FC-SP where possible. It is anticipated that additional protocols or data structures may be needed as the FC-IFR standard is developed.

In addition, the IETF continues to add and extend protocols. It would be beneficial to end users to continue to align security mechanisms and algorithms where possible between IP and FC interconnects.

Security is an important part of a Fibre Channel Infrastructure, and this requires additional and extended specifications of interoperable methods of providing the necessary techniques for securing the Fibre Channel Infrastructure.

3.3 Implementation Impacts of the Proposed Standard

3.3.1 Development Costs

This standard will be developed through the voluntary and cooperative efforts of T11 Task Committee members. No significant development costs are anticipated.

3.3.2 Impact on Existing or Potential Markets

The proposed standard will provide an upward growth path that complements and enhances existing supplier products and support schemes. The proposed standard will result in expanded applications for existing and conceived products in both the channel and network markets. It is likely that isolated adverse effects would occur in any case through non-standard evolution or revolution.

3.3.3 Costs and Methods for Conformity Assessment

The committee will consider the results of testing provided to the committee through the voluntary efforts of the participants in T11. With this method all costs are borne by the organizations of the various participants and have for the most part been mainly an adjunct of their normal development costs.

3.3.4 Return on Investment

The return on investment for this development is expected to be high, due to the commonality of effort directed to a singular method of providing the services covered by the proposed standard. Additionally, the investment made in products developed under FC-SP-2 will be preserved by providing services within the existing infrastructure.

3.4 Legal Considerations

3.4.1 Patent Assertions

Calls will be made to identify assertions of patent rights in accordance with the relevant INCITS, ANSI and ISO/IEC policies and procedures. T11 is aware of any patent assertions that may be made.

3.4.2 Dissemination of the Standard or Technical Report

Drafts of this document will be disseminated electronically. Dissemination of the final standard will be restricted as the document becomes the property of INCITS, ANSI, or ISO/IEC.

4 Related Standards Activities

4.1 Existing Standards

(1) INCITS 373:2003 Fibre Channel - Framing and Signaling (FC-FS)

(2) INCITS 332:1999, Fibre Channel Arbitrated Loop (FC-AL-2).

(3) INCITS 387:2004, Fibre Channel Generic Services - 4 (FC-GS-4).

(4) INCITS 384:2004, Fibre Channel Switch Fabric - 3 (FC-SW-3).

(5) INCITS 414:2006, Fibre Channel - Backbone (FC-BB-3).

(6) INCITS TR:36:2004, Fibre Channel - Device Attach (FC-DA).

(7) INCITS TR:39:2005, Fibre Channel Methodologies for Interconnects - 2 (FC-MI-2).

4.2 Standards in development

(1) Project 1570-D, Fibre Channel Security Protocols (FC-SP).

(2) Project 1677-D, Fibre Channel Generic Services - 5 (FC-GS-5).

(3) Project 1674-D, Fibre Channel Switch Fabric - 4 (FC-SW-4).

(4) Project 1796-D, Fibre Channel - Backbone 3 (FC-BB-4).

(5) Project 1619-D, Fibre Channel Framing and Signaling - 2 (FC-FS-2).

(6) Project 1620-D, Fibre Channel Link Services (FC-LS).

(7) Project 1745-D, Fibre Channel - Inter-Fabric Routing (FC-IFR).

4.3 Recommendations for Close Liaison

IETF Security Area

SNIA Security Technical Work Group

SNIA FC Technical Work Group

5 Units of Measurement used in the Standard

Système Internationale d'Unités (International System of Units).