SONY

VIDEO COMMUNICATION SYSTEM-TECHNICAL DOCUMENTATION

Encryption

PCS-1/1P	Ver3.20 or later
PCS-11/11P	Ver3.20 or later
PCS-G50/G50P	Ver2.21 or later
PCS-G70/G70P	Ver2.21 or later
PCS-TL30	Ver1.04 or later
PCS-TL50	Ver2.21 or later

IPELA

Introduction

Sony's videoconferencing products (PCS series) encrypt video and audio data. Encryption provides secure connections and protects data from unexpected modification by hackers or other outsiders.

Sony uses two types of encryption technologies. One is an ITU-T standard-based format. This format allows Sony products, as well as other manufacturer's products, to communicate with each other, provided they support ITU-T encryption.

The other format is a Sony proprietary encryption standard, which is supported only over IP connections. A common password is required for all attendees to participate in the same conference, which creates a more secure connection.

All Sony's videoconferencing products provide both encryption formats as standard functions, rather than as options.

Encryption Scheme

Encryption Algorithm

Both ITU-T standard and Sony proprietary formats use Advanced Encryption Standard (AES). AES is an encryption standard based on the Rijndael algorithm for secret key cryptography which was developed by Belgian mathematicians, Joan Daemon and Vincent Rijmen.

AES was finally chosen by the (US) National Institute of Standards and Technology (NIST), as the most advanced encryption method from among the many proposals submitted from around the world.

The intention was to replace the former standard, Data Encryption Standard (DES); therefore, AES is far more reliable than DES.

AES employs a common encryption key for both encoding and decoding.

From the sending end, the digital data stream is divided into multiple blocks of 128 bits each, which are then encoded by a key. At the receiving end, the data blocks are decoded by the same key and the original data is restored.

The key length of AES can be chosen from among 128bits, 192bits, and 256bits. With a key length of 128bits, a hacker would require 2128 (2 to the power of 128) trials to find the correct key. This key length is relatively secure, considering the security of the computer used.

Key Exchange System

If encryption keys are not shared securely, encryption may fail, no matter how advanced AES is; therefore the key exchange system is very important.

The method for exchanging keys is different between ITU-T standard and Sony proprietary formats. ITU-T uses a method called Diffie-Hellman key exchange protocol, and Sony uses a Sony original protocol.

The Diffie-Hellman key exchange protocol, which was invented by Whitfield Diffie and Martin E. Hellman, uses a mathematical difficulty that is not inherent in exchanging the key itself but is inherent in exchanging data and random numbers generated from the key. Thanks to this difficulty, common keys are shared securely at each end, and managing the key is not an issue.

Sony's proprietary format uses a unique Sony-invented key exchange protocol.

A key is generated based on a password entered by the user. Because the password is scrambled, it is sent securely to the far end. The participant of the encrypted conference uses the password in common, which helps to prevent spoofing.

Two Encryption Protocols used for PCS Series

ITU-T International Standard Protocol

ITU-T (International Telecommunication Union-Telecommunication Standardization Sector) defined security and encryption as recommendations of H.233, H.234, and H.235. Both H.233 and H.234 define encryption key management and the authentication system for connections over ISDN (H.320) connections. H.233 defines the encryption system for media, and H.234 defines the total signaling protocol for encrypted communication, including key exchange. The H.235 recommendation describes encryption protocols over IP (H.323) connections. AES is supported under H.235 version 3.

Sony's PCS series videoconferencing products follow these international standards when ITU-T mode is selected at the start of an encrypted conference. Sony PCS videoconference systems support the H.235 recommendation version 3. The data media encrypted are: Audio, video, far-end camera control data,

PC screen images via DSB (Data Solution Box), data drawn on an electric white board, and the second video stream during Dual Video mode.

Encryption is supported in both point-to-point and multipoint connections.

Encryption is also supported in mixed IP (H.323) and ISDN (H.320) connections.

Sony Proprietary Protocol

Sony's proprietary encryption protocol is supported in all IP connections, including H.323 and SIP protocols. ISDN connections (which are more secure than IP connections) are not supported. The data media encrypted are: Audio, video, PC screen images via DSB, and the second video stream during Dual Video mode. Encryption is supported in both point-to-point and multipoint connections, regardless of mixed H.323 and SIP connections.

Relationship Between Configuration And Encryption Support

(Table 1) During point-to-point connection

	IP	ISDN	SIP
SONY encryption	●	N/A	●
Standard encryption	●	●	N/A

(Table 2) During multipoint connection

	IP Only	ISDN Only	SIP Only	IP&SIP	IP&ISDN	SIP&ISDN	IP&ISDN&SIP
SONY encryption	●	N/A	●	●	N/A	N/A	N/A
Standard encryption	●	●	N/A	N/A	●	N/A	N/A

SONY