

TANDBERG Advantage: SECURITY

- Unparalleled protection of videoconferencing content via embedded encryption
- Videoconferencing systems designed specifically to restrict access to only authorized users

Videoconferencing communication encodes audio and video into electronically transmitted data.

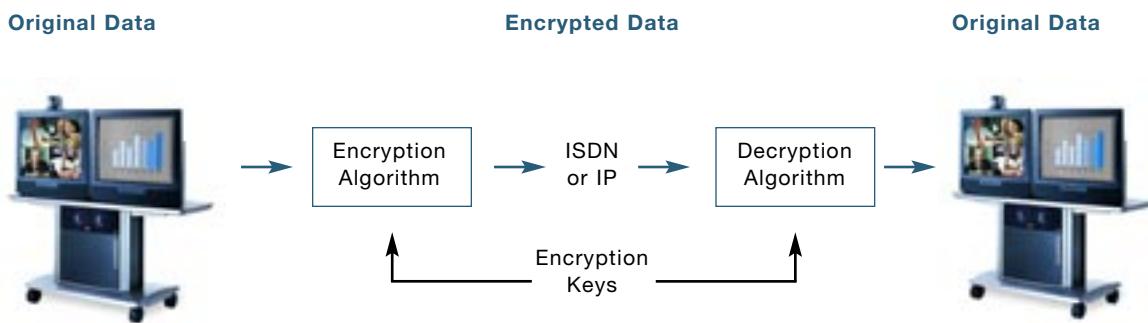
Electronic data transmission over public and private networks requires security measures that ensure privacy, confidentiality, and appropriate access control. TANDBERG equipment has been designed specifically with these security needs in mind.

Secure ConferenceTM Embedded Encryption

Encryption is a way of scrambling data so that only those who know how to unscramble the data get access to it. With encryption, you can rest assured that all your videoconferencing communication is private and confidential. Embedded encryption also allows you to enjoy the full array of videoconferencing features without any degradation in performance, unlike third-party, non-embedded encryption solutions.

The Key to Encryption

All encryption methods use common algorithms. The details of the algorithms themselves are well known. Security comes from the key, which is passed to the algorithm to tell it how to encrypt the data. A key is simply a number or a set of numbers.



Standards Used by TANDBERG

A commonly employed communications encryption method is the “Data Encryption Standard” (DES). DES works by encrypting data with a 56-bit long key. Triple DES (3DES) is an enhancement to DES that effectively runs 112-bit long keys. DES and 3DES are both widely used in commercial and non-defense government communications today.

To provide a higher degree of security than both DES and 3DES, a new standard called Advanced Encryption Standard (AES) has been developed. The new AES standard with 128-bit keys has been approved by the U.S. Government to protect sensitive, unclassified data and will replace the use of 3DES.

TANDBERG supports the following encryption standards: AES, DES, H.233, H.234 and H.235 with an extended Diffie-Hellman key distribution on H.323, H.320 and leased lines.

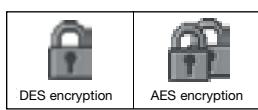
Levels of Encryption

Encryption Level	Standard	Encryption Level	Necessary equipment
High		Military	Custom made external boxes
Medium		Medium-risk enterprises	Full TANDBERG product line with Secure Conference TM AES ¹
None	AES DES Unsecure	Commercial and non-commercial enterprises	Full TANDBERG product line with latest software with embedded Secure Conference TM DES
			Other videoconferencing equipment



¹ Available as a software option on all TANDBERG endpoints, and included in the TANDBERG MCU.

TANDBERG Offers Standards-Based, Easy to Use Encryption



TANDBERG Secure Conference provides embedded, user-friendly, standard-based encryption. Secure Conference is “on” by default. This automatically generates an encrypted call, which is indicated with an on-screen lock symbol. A single lock symbol is displayed for DES. A double lock symbol is displayed for AES.

Secure Conference DES and AES are both available in point-to-point calls and multipoint calls on ISDN and IP up to 768 kbps on the full TANDBERG product line. TANDBERG’s implementation of the AES- and DES cryptographic algorithms has been validated as conforming to Federal Information Processing Standards (FIPS) by a laboratory accredited by The National Institute of Standards and Technology (NIST).

Videoconferencing System Access Control

Videoconferencing Endpoint Access Security

TANDBERG has enhanced the security of its endpoints by allowing users to disable IP services like Telnet, FTP, HTTP, SNMP, H.323 and remote software upgrades to prevent unauthorized access to the systems. In addition, passwords to the internal web server on the endpoint codec are encrypted and secured. Furthermore, the Telnet port allows use of an encrypted password.

Multipoint Control Unit Access Security

As with TANDBERG endpoints, administrators may disable services such as Telnet, FTP, HTTP, SNMP, H.323 and remote software upgrades on the TANDBERG MCU. Furthermore, connections between the TANDBERG MCU and the administrator's PC are encrypted via HTTPS. TANDBERG MCU passwords are encrypted and authenticated via HTTP Digest.

SNMP-Security Alert

A Management Application is notified when an intruder tries to remotely access an endpoint with an illegal password. The alert provides information about the IP address and the service being used, i.e. web, telnet or FTP, which the intruder is using. For example, an alert will be received by the TANDBERG Management Suite, which can then be set to deliver a relevant alert message to a pager or via e-mail. Once the message is received, the administrator can respond immediately with the appropriate action.

User Security

TANDBERG systems employ codes and passwords in order to control access to menu settings, conferences, call settings, and administration. To further protect the security of customers' communications, a "Do Not Disturb" option prevents unwanted interruptions.

To learn more about TANDBERG products and services,
please visit our website at www.TANDBERG.net or contact our global headquarters:

New York: +1 212 692 6500 tandberg@tandbergusa.com

Oslo: +47 67 125 125 tandberg@tandberg.net