Dante Media Encryption

A Device Manufacturer Introduction

v1.0

5th March 2025

Dante®

Copyright

Legal Notice and Disclaimer

Audinate retains ownership of all intellectual property in this document.

The information and materials presented in this document are provided as an information source only. While effort has been made to ensure the accuracy and completeness of the information, no guarantee is given nor responsibility taken by Audinate for errors or omissions in the data.

Audinate is not liable for any loss or damage that may be suffered or incurred in any way as a result of acting on information in this document. The information is provided solely on the basis that readers will be responsible for making their own assessment, and are advised to verify all relevant representation, statements and information with their own professional advisers.

Software Licensing Notice

Audinate distributes products which are covered by Audinate license agreements and third-party license agreements.

For further information and to access copies of each of these licenses, please visit our website: www.audinate.com/software-licensing-notice

Contacts

Audinate Pty Ltd

Level 7/64 Kippax Street

Surry Hills NSW 2010

AUSTRALIA

Tel. +61 2 8090 1000

info@audinate.com

www.audinate.com

Audinate Inc

4380 S Macadam Avenue

Suite 255

Portland, OR 97239

USA

Tel: +1 503 224 2998

European Office

Audinate Ltd

Future Business Centre

Kings Hedges Rd

Cambridge CB4 2HY

United Kingdom

Tel. +44 (0) 1273 921695

Asia Pacific Office

Audinate Limited

Suite 1106-08, 11/F Tai Yau Building

No 181 Johnston Road

Wanchai, Hong Kong

澳迪耐特有限公司

香港灣仔莊士敦道181號

大有大廈11樓1106-8室

Tel. +(852)-3588 0030

+(852)-3588 0031

Fax. +(852)-2975 8042

Contents

Introduction

AVoIP has become the de-facto means of installing large scale enterprise audio and video systems, and these days it is commonly used across corporate, financial and government institutions. Networked systems provide the means to scale an organisation's needs for audio and video endpoints whilst maintaining a high degree of control through management, control and monitoring tools. The management of AVoIP devices increasingly resembles the management of traditional IT assets within an organisation, and this resemblance is a leading factor in the convergence of AV and IT systems.

Over the last decade, users, administrators and installers of connected digital equipment have grown increasingly aware of the threats that are posed by breaches of cybersecurity. The AV industry is no different, and the trend towards converged AV and IT systems is bringing into spotlight the need for AV equipment to deliver best-in-class protections for devices, networks and users of AV equipment. At the same time, regional regulation across the globe is catching up with technology to ensure that all users and systems are protected from cyber threats. Many governments are in the process of drafting - or have recently published - new product security guidelines and regulations to protect their citizens when using connected devices. Examples of these include the EU's Cyber Resilience Act (CRA), UK's Product Security and Telecommunications Infrastructure (PSTI) bill, EU's Radio Emissions Directive (RED) and EU's new Product Liability Directive.

As AV equipment has evolved to capture content in ever higher quality, to embed increasing levels of advanced signal processing, and to provide the means to remotely adjust configurations, these devices are exposed to a broad range of threats from malicious actors in a system. The types of threats that may be of concern for network administrators include:

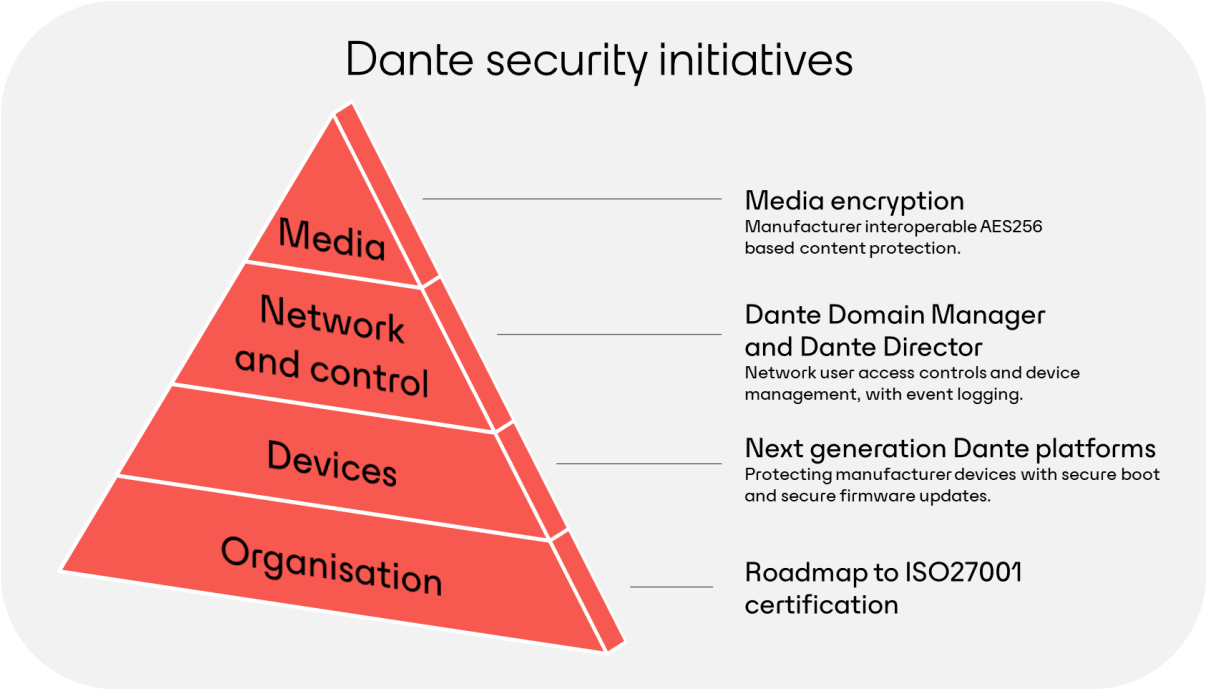
- Eavesdropping - during which audio and video on the network is intercepted or redirected to an unintended recipient
- System disablement - whereby a network or devices are disrupted through unauthorised changes to the configuration of a system
- Client impersonation - through which a rogue actor pretends to be a legitimate device on the network

As the leading provider of AVoIP solutions for manufacturers, Dante from Audinate is the only AVoIP solution enabling protection for devices, networks and user's data.

Dante's Pillars of Security

Devices and networks cannot be made secure by any single act or process however the collective provision of many elements increases the overall system security for the network and the user.

Dante is the only AVoIP solution that implements a multi-layered approach to security to increase protection to devices, networks and the user.



Device Security

Regardless of whether a product incorporates Dante using a chip or module manufactured by Audinate, or through the integration of embedded software or firmware, the device level security performs a key foundation role in protecting the system.

In critical infrastructure, it is essential that administrators trust the authenticity of firmware running in their network. Dante Updater provides administrators a secure method of updating the device firmware (for the latest Dante solutions) in their network, and ensures that the device firmware is coming from a trusted source. Audinate-manufactured chips and modules support Dante Updater today, and support for products integrating Dante embedded software and firmware is coming soon.

The latest Audinate chips and modules take the additional precaution of using a secure boot procedure. Secure boot prevents unauthorised or malicious firmware from being loaded on the embedded processor, shutting down threats before they can occur. Audinate recommends that secure boot is implemented by all device manufacturers integrating Dante embedded software and firmware solutions.

For manufacturers leveraging Dante embedded software and firmware, understanding inherited vulnerabilities of third-party software is essential to taking appropriate corrective actions. As a key supply chain partner to hundreds of manufacturers, Audinate is introducing Software Bill of Materials (SBOM) and Vulnerability Exploitability eXchange (VEX) files to provide transparency into how third-party software is used within Dante solution. This process increases transparency throughout the software supply chain, enabling manufacturers to meet legislative requirements, and ensuring that vulnerabilities are addressed appropriately and in a timely manner through Dante updates as they emerge.

Network Security

The security of a Dante network is enhanced by restricting the devices that can join, and restricting the users that can modify the configuration of the network. Device and user access controls can be implemented across an AV network with a Dante manager. Dante Director is a scalable SaaS environment that provides a suite of network security features for networks of all sizes. A managed network requires that devices are enrolled before they are discoverable to other Dante endpoints. This process prevents Dante signals from being routed to non-authorised devices. Once enrolled, all device control traffic is encrypted to prevent outside patching.

Enrolment and any other changes to the managed Dante network require user authentication and authorisation. Authentication allows role-based access to devices and network settings and prevents unauthorised users from disrupting or rerouting media traffic in the network.

In a managed network, user roles can restrict which parts of a network can be accessed and who can modify security policies.

Site network segmentation ensures that a balance can be made between broad usability and focused security for the most sensitive parts of a network.

Inevitably, changes will happen on a network and this can sometimes have unintended consequences. Detailed event logging can help identify which change affected a system, when it occurred, and who actioned the change.

Media Security

Even when a device is secured and the network configuration is locked down, media traffic must still travel across the network. With the convergence of AV and IT networks and the flexibility of Dante to run as a Layer 3 protocol, media traffic may hop between many devices and network switches. Dante media encryption can be utilised by the network administrator to ensure that media content remains confidential regardless of the underlying Ethernet network.

Interoperable and Simple Encryption of Media

Audinate has introduced media encryption to extend the ecosystem of security to all Dante device manufacturers. Media encryption will be included in all future endpoint firmware for chips, modules and embedded software at no additional licensing cost to manufacturers.

Media encryption supports adherence to IoT requirements and the evolving AV system requirements of government, financial and corporate installations.

Industry leading protection without sacrificing audio performance

Dante media encryption utilises the Advanced Encryption Standard (AES) with a 256-bit key to protect media in transport between devices. AES-256 was chosen due the broad support of implementations across software and hardware, especially within the microcontrollers, microprocessors and FPGA families that are frequently used within professional AV products. AES is considered a fast algorithm that facilitates low latency deciphering of real-time media. A 256-bit cryptographic key is employed to protect against brute forcing of the network security - for this reason, AES-256 is already an industry and government standard for data protection.

Through the management of the AV network with Dante Director or Dante Domain Manager, Dante media encryption provides a centrally-managed key management system (KMS) to generate and distribute the cryptographic keys. Dante's KMS ensures that only devices connected via a media flow have access to the relevant keys, and that keys are regularly rotated to reduce the amount of content that could be exposed when a single key is compromised.

Dante's KMS avoids the need for users and network administrators to manually manage keys or passwords across devices - thus removing the human factor from a critical piece of network AV security.

The speed of the cryptographic algorithm was also critical in the design decision for Dante. Latency is a crucial factor in AV networks, and Dante media encryption has been implemented such that there is no direct impact to media latency. Dante achieves this by encrypting media within the flow and utilizing the wait time while network packets are sorted. In contrast, encryption of digital audio before it is transported over a network directly adds latency through the copying, encryption and decryption of the audio buffer.

Centrally managed security policies in Dante Director

By building upon the user roles that are established in a managed network, Dante media encryption introduces the concept of media security policies that can be configured only by a network administrator to restrict the use of unencrypted traffic on a network. Media security policy is defined on a transmitting channel, and the policy allows a transmitting channel to operate in a 'compatible' or 'strict' policy, thus giving a network administrator the control to balance legacy interoperability with system protection.

When 'strict' policy is applied to a transmit channel, a new subscription will only be successfully created if the receiving device also supports Dante media encryption. If the receiving device is not capable of media encryption, the subscription will fail to be created, and Dante Controller will present an error message to the user.

A transmit channel operating within a 'compatible' policy will first attempt to create a subscription in an encrypted flow – however, if the receiving device is incapable of encryption the subscription will resolve in an unencrypted flow. 'Compatible' policies ensure that networks continue to operate with millions of Dante devices already out in the market whilst allowing the network to become incrementally more secure as newer devices are added and device firmware is upgraded.

Manufacturer interoperable

Media encryption will be a standard feature for new Dante endpoint solutions, starting in 2025.

As a standard feature, Audinate is making encryption freely available as part of existing licensing arrangements so that all Dante device manufacturers can deliver enhanced security to their customers, their users and their networks.

As the most widely used and interoperable AV standard, Dante's media encryption is able to deliver a unique multi-layered and vendor agnostic solution, ensuring that users get the best choice of hardware and software for their AV applications.

Integrating Dante Media Encryption

Coming to Dante endpoints from 2025, Dante media encryption will be available to device manufacturers through firmware updates. Media encryption will be available to device manufacturers for Dante Embedded Platform, Dante Brooklyn 3, Dante IP Core and Dante Pro S1, with updates to the Dante AV solutions to follow.

Dante media encryption will not be available on older Dante solutions.

Manufacturer devices will be supported with software updates to Dante desktop applications, for complete AV network support.

Dante Brooklyn 3 and Dante Pro S1

Media encryption is implemented within the Dante chip or module. Following a device upgrade to the latest firmware, no additional configuration of the device is required by the manufacturer to enable Dante media encryption.

Dante Embedded Platform and Dante IP Core for Zynq-7000 & Zynq UltraScale+

There are additional processing, code memory and/or FPGA resources required as part of the firmware updates that enable Dante media encryption. Audinate recommends that manufacturers upgrade to the latest firmware, once available, and re-evaluate the CPU benchmarks to verify that media quality is maintained.

Expected resource requirements are documented in the Dante Embedded Programmer's Guide and the Dante IP Core Technical Datasheet.