



Cryptographic Streaming (Telecast)

Anonemis Research
Símenona Martínez
AnonemisResearch.com

Cryptographic Streaming

(Telecasting)

Overview

Cryptographic Streaming is the second generation of encryption and decryption methodology used in teleconferencing.

Instead of utilizing a primary shared encryption key, this method requires software which is engineered for rapid and continuous encryption looping within a system for the purpose of cryptographic checks during government telecast, financial transactions, and anti-terrorism protocol, assuring the integrity of security system enterprise.

Cryptographic Streaming would assist in isolating possible attacks, intrusions, fraud, terrorism detection and eavesdropping by early detection and swift retrieval of information regarding attacks as seen in the [Integrated Sensory Constructure Unit](#), within the financial industry.

This procedure would also incorporate the enforcement of digital encryption security screen, inscribed with unique and phantom coding specific to enterprise, thus, making the biometric information requiring a specific matching key for decryption in the same steaming methodology, analysis, and confirmation, thus, in the case of hacking, this information cannot be compromised nor accessed.

It would be required of employees working in high-risk industries, such as The Department of Homeland Security and The Department of Defense to register biometric data to participate future telecast etc.; as an essential part of policy and procedures within enterprise.

The collection of biometric data and the security controls in place would be to protect data and privacy, most notably suggested with, [Secure Biometrics Boarding](#) at Boarder Control.

The disadvantage with using symmetric encryption is always interception. The use of Cryptographic streaming and shuffling encryption makes it impossible to hack a code which is rapidly changing the series of temporary encryption without pattern or sequence.

This methodology would also be utilized in Next Generation Cryptographic regarding text messaging and e-mail, it is a critical baseline in protecting the confidentiality, integrity, and availability in the framework of the overall Nation Security.

Cryptographic Streaming constantly resetting the encryption output, ensures that there are no sequences and codes, which historically were essential but now arbitrarily obsolete to possible intrusion.

Anonemis Research
Símenona Martínez
AnonemisResearch.com