C4L Intelligence Systems

AIS

An Introductory Overview to Aegis Information Securities, a division within C4L Intelligence Systems

AIS Completo

The full and complete data haven for digital media, providing private information securities bank and trust services for Clients.

AIS Compacto

A service that provides secure private encrypted dialogs, exchanges, and transactions for Clients.

AIS Completo

(diagram is in preparation)

The process begins with a Client who has some special information in digital form that must be saved, securely and privately, with no risk of tampering or capture of this information, which is known as the CMOS.

CMOS (Client Media Original Source). This is digital media (any type or format) that is delivered to an AIS representative.

AIS receives the CMOS.

EP (Encryption Process). This is a complex and individuated multi-stage process that is individually managed by an AIS agent. It results in multiple, discrete fully and variably encrypted data objects produced from the CMOS. This result is the pair of datasets, the ETOS and the EPAS.

ETOS (Encryption Transform Object Set)

EPAS (Encryption Process Algebra Set)

The EPAS holds essential parameters for any future reversal of the EP and restoration of the CMOS.

CASAnet (Concurrent Asynchronous Stochastic Allocation Network). This is the system employed by which the elements of the ETOS are distributed, dynamically, repeatedly, virtually ad infinitum for the lifetime of AIS maintenance and storage of all CMOS from all Clients. The CASAnet is global, mobile, and can be considered to be effectively and securely indeterminate, undefined, and

unlocalizable with respect to actions by any agent or force attempting to locate and retrieve or seize any single object from the ETOS (much less the complete ETOS for a given CMOS). All of the complete ETOS is required, along with the EPAS, for the successful reconstructive decryption of the CMOS or any portion of the CMOS. Thus, through AIS, a Client can be assured with absolute confidence that any digital media entrusted, stored, and banked within the AIS data haven vault system is safe and will remain private and secure and untouchable.

Certain Clients will choose to engage in private trading and AIS serves as the broker. For a given CMOS, AIS will produce a special set of information known as the MTAS.

MTAS (Media Trade Attribute Set). This consists of information extracts, summaries, or other forms of textual or graphic representation, approved by the Client for an AIS broker to use in marketing the Client's CMOS for sale or trade according to specified contractual terms (barter, sale for currency, conventional financial securities, real property, or commodities, or in other forms of trade, according to the Client's choice and disposition.

AIS broker engages in specific marketing and if a deal is satisfactory to the Client, then ownership and all rights and information are transferred accordingly to the new owner.

Confidentiality, privacy and anonymity are preserved completed for the benefit of all Clients.

AIS Compacto

(diagram is in preparation)

This is a service for Clients who do not need the extensive, deep, rigorous encryption and storage of specific digital media, but who require and desire private anonymized data management, primarily involving communications and sharing of data in any digital media format, with other persons, organizations or other entities.

This involves a strongly encrypted VPN and the use of diverse encryption algorithms that are not available to the general market and which are computationally intensive and not suitable for typical web-based chat systems, emails, and other forms of "standard" encryption for messaging or transactions. What AIS provides is not for real-time but for "half-duplex" communication exchanges where there may be significant periods of time (generally, in minutes) between sending and receiving.

A major emphasis is placed upon anonymity of senders and receivers. This is accomplished through independent encryption and data pathways, and through OTP and OTP-like forms of encryption, and a variety of other forms which, again, are not conducive to real-time exchanges between multiple parties.