AMHS Security

Isode

This white paper describes AMHS Security Services and how they are provided in the Isode product set. AMHS (ATS (Air Traffic Services)) Message Handling Services is used worldwide for provision of ground-to-ground communication services. Isode products are used in a high percentage of deployed AMHS systems.

The key security services described are:

- Message Digital Signature.
- Two way Strong Authentication for the protocols used.

Background

AMHS is specified in "ICAO Doc 9880 — Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols; Part II – Ground-Ground Applications – Air Traffic Services Message Handling Services (ATSMHS)".

The AMHS specifications have always included security services from the X.400 protocols on which AMHS is based, but these have been optional. Isode has provided some of these services for many years, but there has been minimal interest and uptake.

This changed in 2024 when edition 3 of Doc 9880 was published, which made the security services mandatory. This in turn, has led to AMHS networks looking to deploy AMHS security.

To support this, Isode has implemented all of the AMHS Security Services in its product set. These capabilities are described here. They are available now as pre-release to Isode partners and will ship in the first half of 2026 as the 19.2 release of the products used for AMHS.

Message Digital Signature

AMHS specifies how to digitally sign ATS messages using X.509 Public Key Infrastructure (PKI), which is widely available.

Services Provided

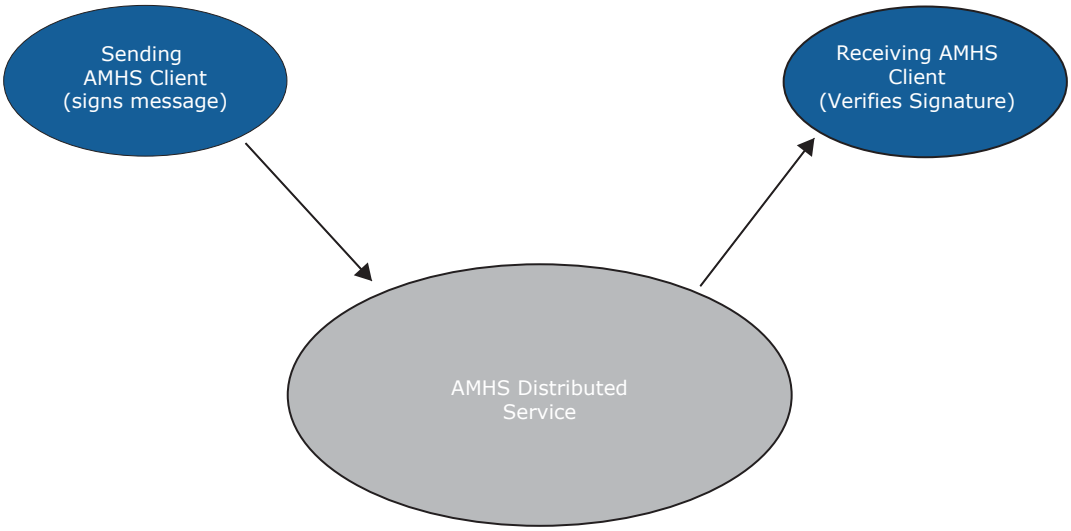
There are two key services provided by message digital signature:

1. Message Origin Authentication. This provides evidence to the recipient that the message was created by the message originator. This check avoids message forgery.
2. Content Integrity. This provides evidence that the message has not been modified in transit. This check is to guard against messages being tampered with.

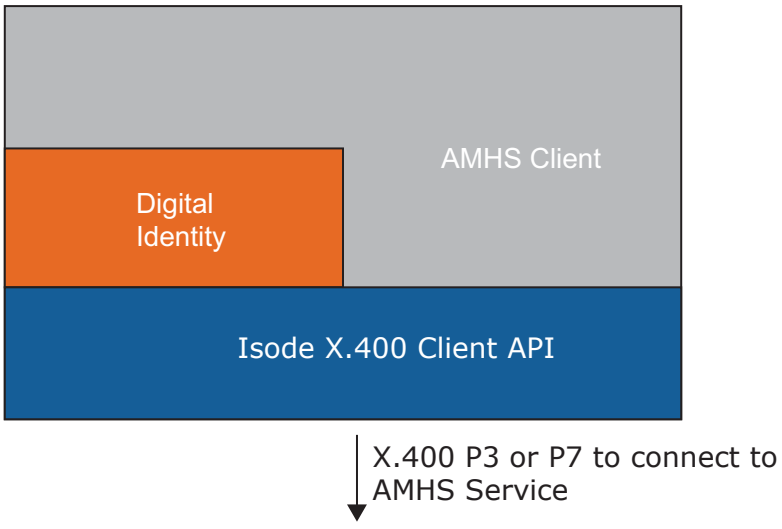
Both of these services are important to provide security.

AMHS provides these services using the per-recipient Message Token capability of X.400, rather than the per-message MOAC (Message Origin Authentication Check) that might have been used. MOAC is supported in the Isode products and APIs. The reason for use of Message Token is that Ed1 also allowed for Client Sequence Integrity, which enables a message receiver to securely determine message order and missed messages. Client Sequence Integrity is not a part of Ed3. Isode sees this as a valuable additional service, and the Isode client API described in the next section supports provision of this service.

Client End to End operation



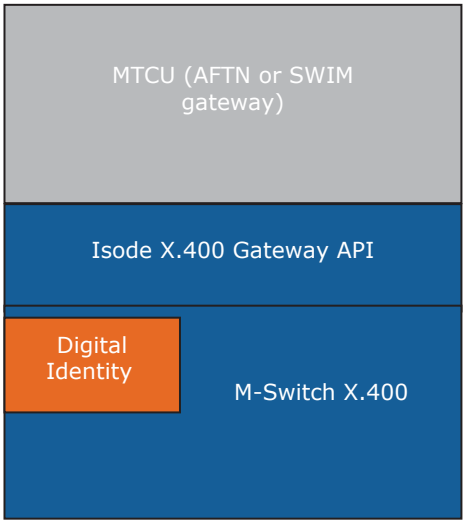
The preferred model for message signature is that the originating AMHS client signs the message, and a receiving client verifies the signature. The signature will bind the O/R Address of the sender to the message using an X.500 Subject Alternate Name (SAN). This enables the receiver to validate the message.



Isode does not provide an AMHS Client but provides a client library (Isode X.400 Client Library product) to enable Isode partners to build AMHS clients.

To generate a digital signature, the AMHS Client will use an X.509 digital identity provided by a Certification Authority (CA), such as the EACP (European Aviation Common PKI). This identity can be referenced in calls to the Isode X.400 Client API to generate the AMHS message signature. The API can also be used to verify the signature of received messages.

AMHS Gateway Operation



Many AMHS messages do not originate in AMHS but are gatewayed from services such as AFTN (a legacy service) or SWIM (a planned future service). In this scenario, the AMHS message is terminated at a gateway known as an MTCU (Message Transfer and Control Unit). Isode provides support for Isode partners to build MTCU using the Isode X.400 Gateway API product, which integrates directly with the Isode M-Switch X.400 product that provides the core AMHS services by interacting with other MTAs (Message Transfer Agents).

M-Switch X.400 manages the digital signatures for MTCU signing as part of its security management capability. This means that an MTCU built with Isode's X.400 Gateway API can simply turn on digital signature without any MTCU code changes.

Isode's X.400 Gateway API allows control of whether messages being sent to AMHS are signed or not, and for received messages, signature verification information is made available to the MTCU.

Note that when a message is signed by the MTCU, the SAN in the PKI certificate associated with the signature is that of the MTCU rather than the initiating client. This value is also used in the first element of X.400 trace. When signatures are verified by Isode X.400 Gateway API or X.400 Client API, the API is aware of this signature option and checks the value of an MTCU signature against the first trace element. Client signatures are checked against the originator address. Results of validation are made available to the API user to use as desired.

Two Way Strong Authentication

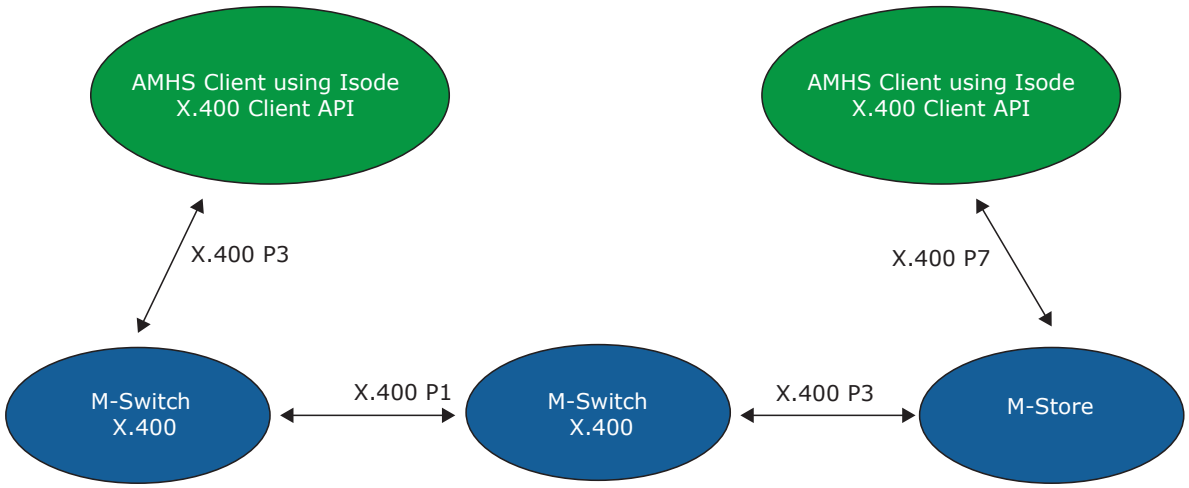
Two Way Strong authentication uses X.509 PKI verification between two entities, so that both entities strongly validate the other one.

Why Strong Authentication?

The X.400 protocols offer simple authentication which is password-based and strong authentication. There is no data security such as TLS provided as standard, although Isode does offer this as a non-standard option.

Use of passwords "in the clear" is very poor security and shifting to strong authentication is highly desirable.

Protocols Supported



The diagram above shows all of the protocols for which Isode has strong authentication support in its product set;

1. M-Switch X.400
    a. X.400 P1 for communicating with other MTAs.
    b. X.400 P3 for communicating with M-Store and AMHS Clients
2. M-Store
    a. X.400 P3 for communicating with M-Switch X.400
    b. X.400 P7 for communicating with AMHS Clients
3. X.400 Client API
    a. X.400 P3 for communicating with M-Switch X.400
    b. X.400 P7 for communicating with M-Store

Note that although this diagram shows Isode products, that this authentication follows open standards and will interoperate with any other products supporting these standards.

Configuration and Provisioning

Configuration of strong authentication is provided in Isode's MConsole management UI. This enables convenient setup of strong authentication, including secure setup of identities with Certificate Signing Request (CSR) support to enable configuration with thirdparty Certification Authorities.

The UI for adding P3 and P7 clients is extended to enable management of client secure identity.

Isode Products

X.400 P1 support in M-Switch X.400 has been available for many years. All of the other capabilities will be in R19.2 version of each product.

- X.400 Client API. Adds digital signature and two way strong authentication for X.400 P3 and X.400 P7.
- X.400 Gateway API. Adds control of digital signature to be used in conjunction with new M-Switch X.400 add-on.
- M-Store. Adds two way strong authentication for X.400 P3 and X.400 P7.
- M-Switch X.400. Retains support for X.400 P1 two way strong authentication.
- New M-Switch X.400 Security add-on (additional price). This adds support for MTCU-driven digital signature and X.400 P3 two way strong authentication.

Isode

www.isode.com

14 Castle Mews, Hampton
Middlesex, TW12 2NP

Secure, Seamless Communication Solutions