

Ciberseguridad para plataformas de eNavigation

Nota técnica de la presentación realizada por Prof. Dr.-Ing. Axel Hahn Nov 15th 2021

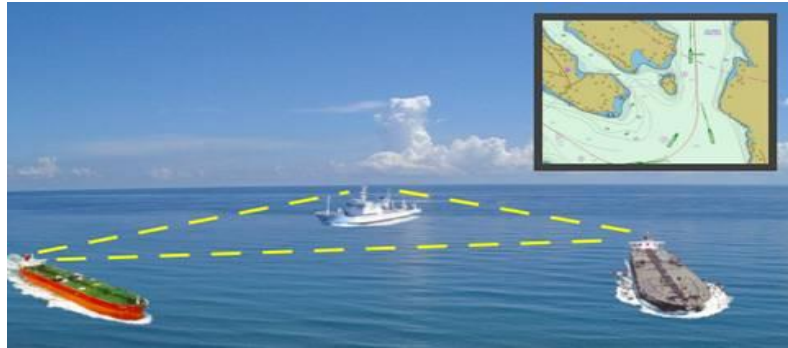
Knowledge for Tomorrow

Agenda

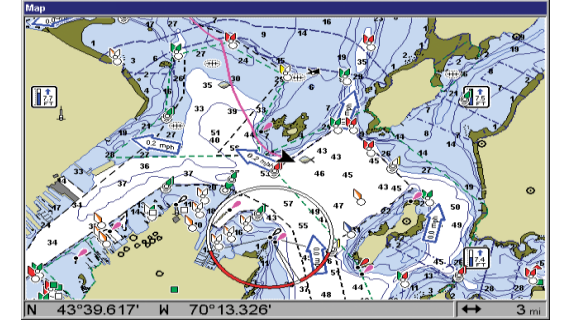
1. Comunicaciones maritimas y ciber-riesgos
2. Principios de ciberseguridad
3. Aplicacion de medidas de ciberseguridad
4. La necesidad de plataformas
5. Criterios para las plataformas de e-Nav
6. Conclusiones



Servicios de Comunicaciones maritimas



Automatic Identification System (AIS)



GNSS / Electronic Nautical Charts (ENC)

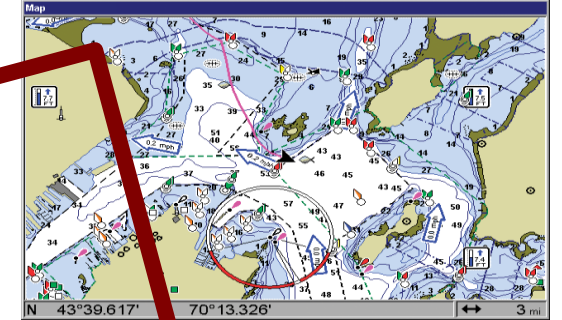


GMDSS



Servicios de trafico maritimo (Vessel Traffic Services) / Logistica

Servicios de Comunicaciones maritimas



Automatic Identification System (AIS)

GMDSS / Electronic Nautical Charts (ENC)

not secured



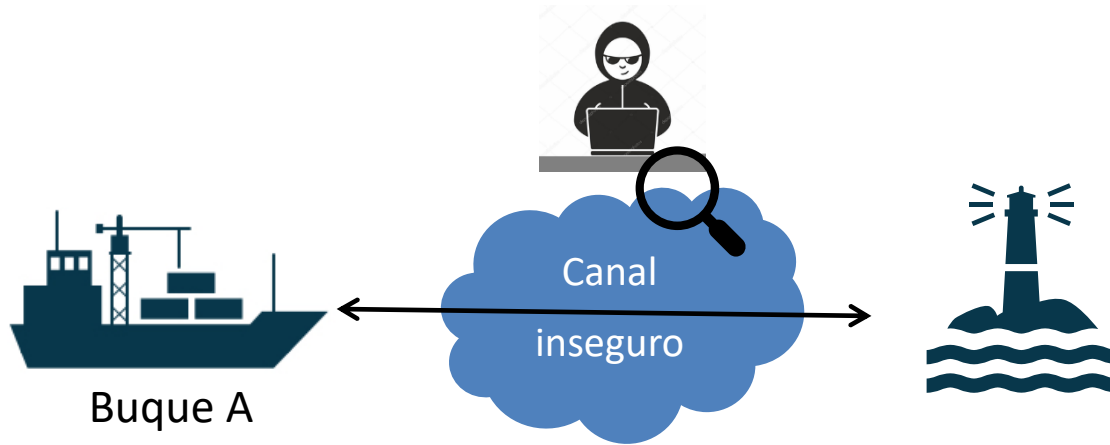
GMDSS



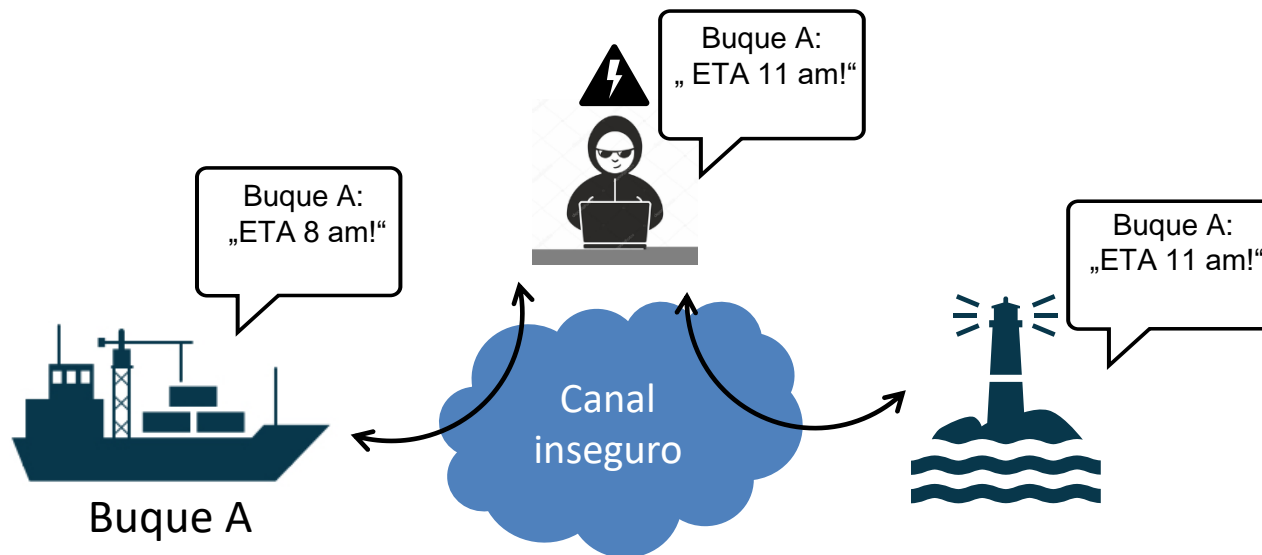
Servicios de trafico maritimo (Vessel Traffic Services) / Logistica



Ciber amenazas



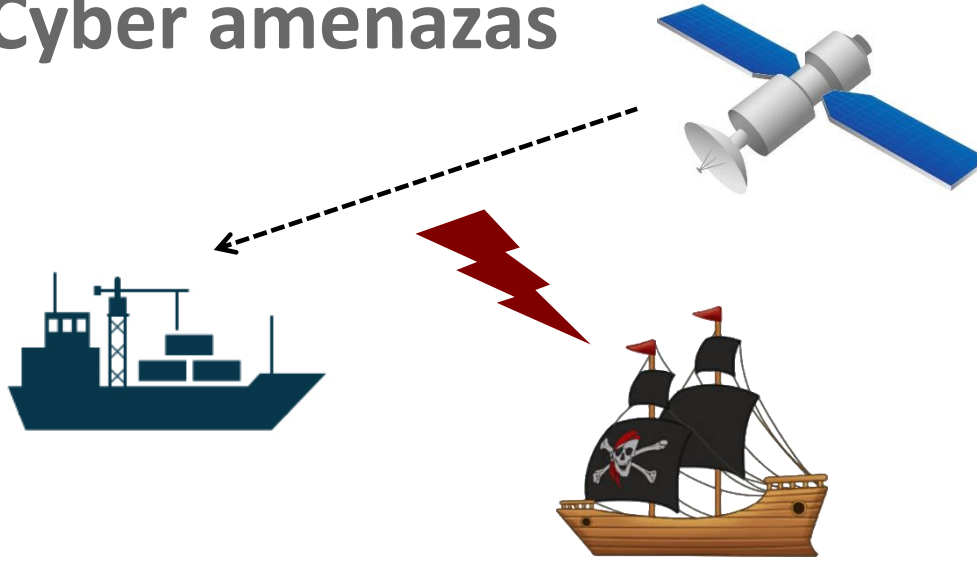
- Escucha / interceptacion
- ej. Informacion en ruta



- „Man in the middle“
- ej. Manipulacion de la negociacion de la ruta durante la prevencion de abordajes



Cyber amenazas



- **Manipulación de datos en el canal físico**
- Ej. Manipulación de la señal GNSS

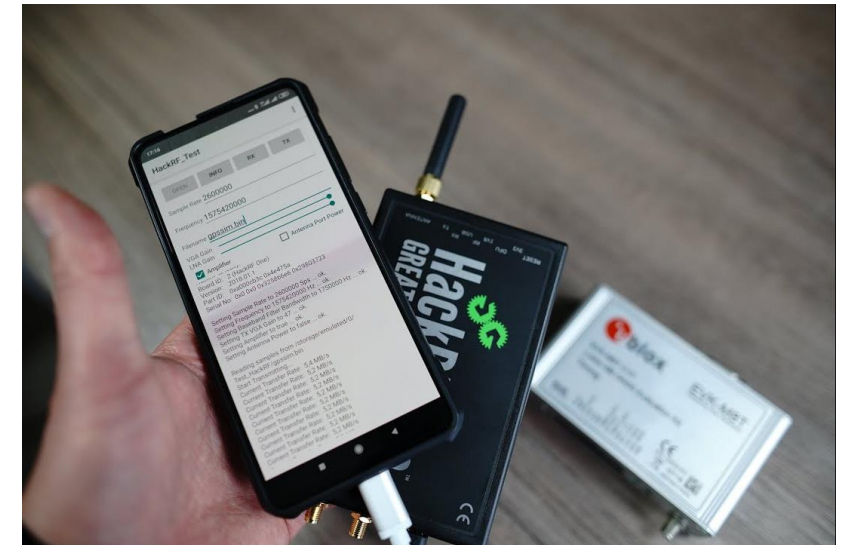
- **Impersonation**
- Ej. Debido a retransmisiones de deliberadamente erróneas de mensaje AIS, el atacante pretende ser un buque de Bandera de un país A causando desencuentros entre las partes



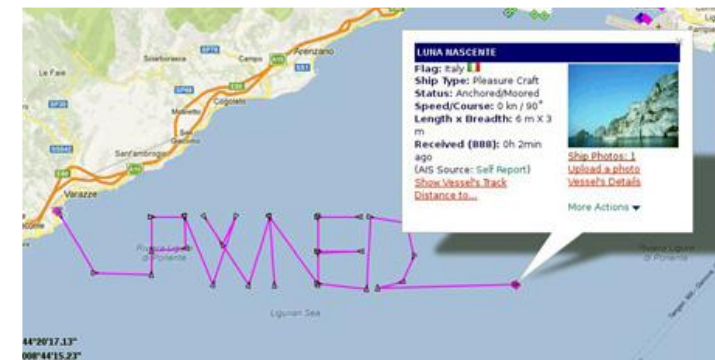
Escenario practico de ataque: Spoofing

Unicamente es necesario un smarthone y un transmisor RF!!

- **Spoofing:** manipulacion de la informacion digital pretendiendo obtener otra identidad.
- Señales en radio frecuencia (RF) desprotegidas pueden ser facilmente spoofeadas.
- Ej. AIS Messages: no encriptados o bajo firma.
- Escenarios de ataque Scenarios:
 - Ship spoofing
 - AtoN spoofing
 - CPA spoofing (prevencion de abordajes)
 - AIS-SART spoofing: generando mensajes distress falsos de radiobalizas
 - ... y muchos otros

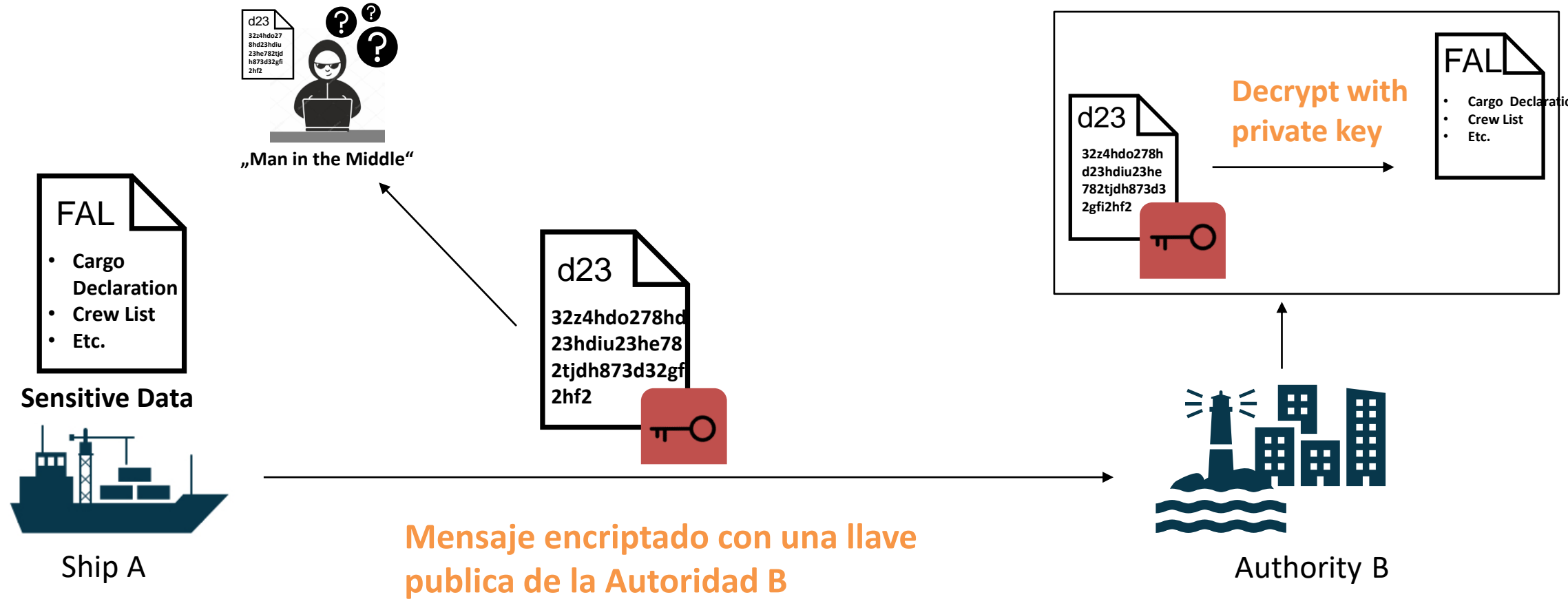


<https://www.youtube.com/watch?v=g-bdK7tRpBI>

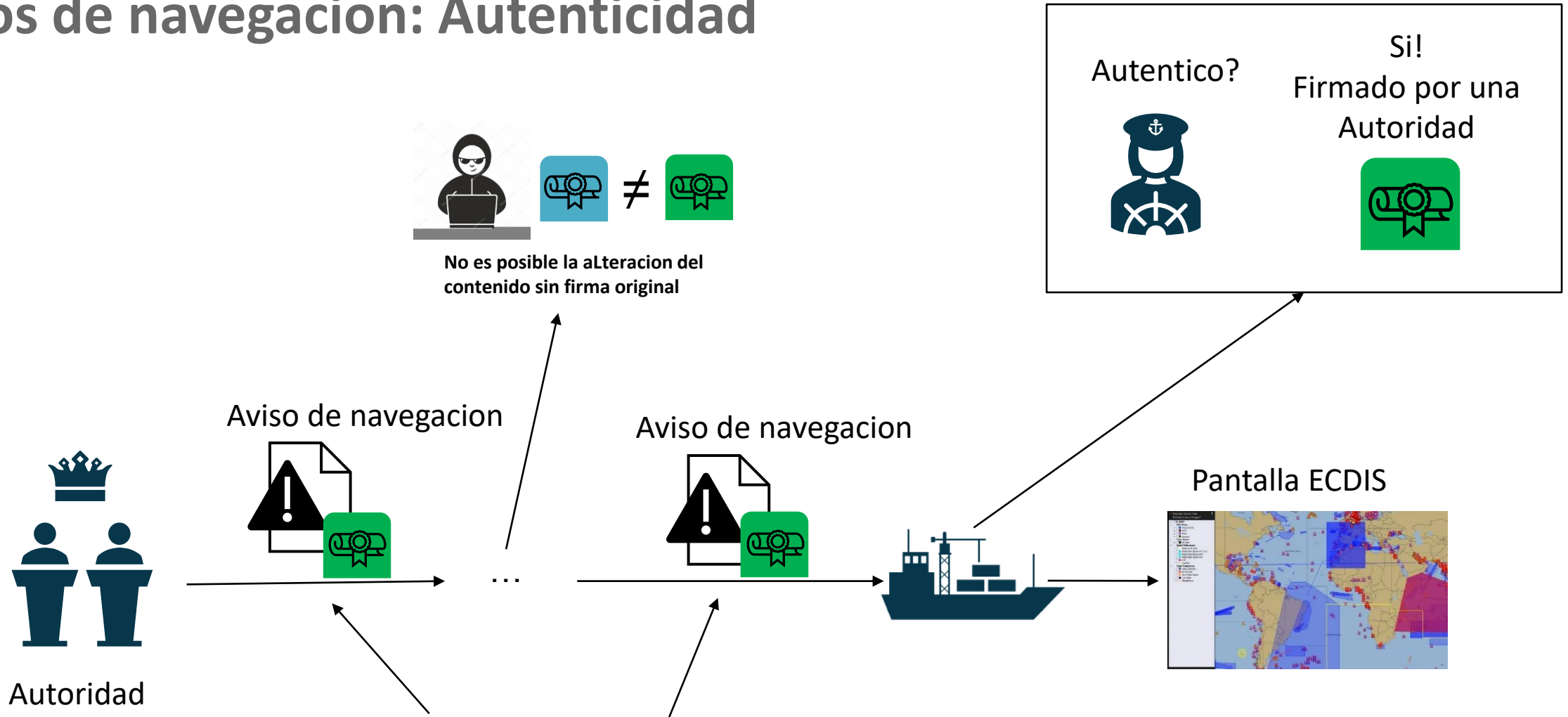


<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf>

Aplicacion FAL: Confidencialidad



Avisos de navegacion: Autenticidad



Firmas digitales utilizando llaves privadas (sin encriptar para informacion publica)



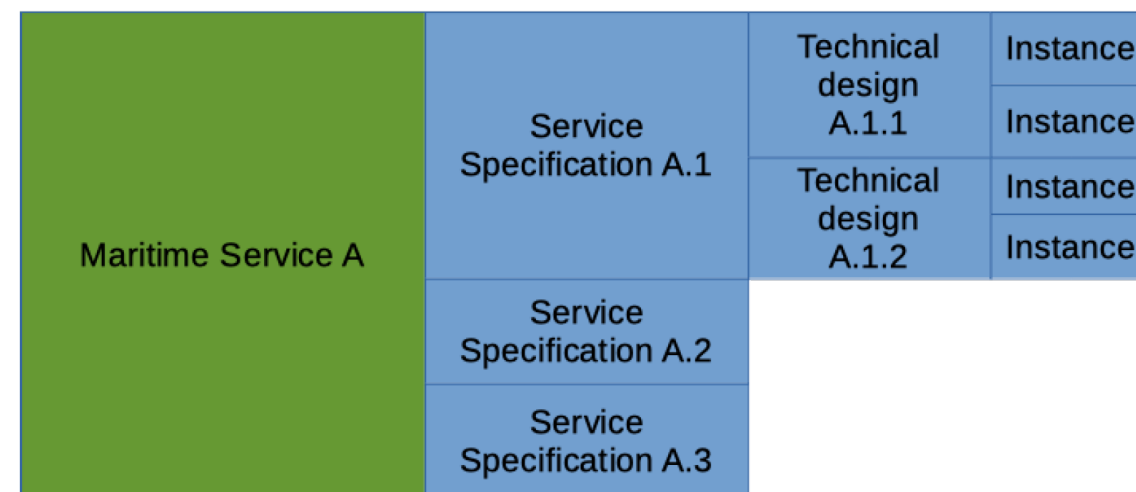
Necesidad de plataformas de e-Navigation

- Se proven comunmente servicios maritimos a través de una **Plataforma de e-Navigation**

„Una Plataforma es un Sistema que facilita el intercambio seguro y veraz de informacion y servicios.“ – IALA G1161

Maritime Services
(defined by IMO
non technical)

Associated technical
services - three
levels
(defined by domain
coordinating bodies)



Managed by platforms



Necesidad de plataformas de e-Navigation

- Digitalización avanza rápidamente
 - Crecimiento de intercambio de información electrónica
 - Visualización de obtención de servicios marítimos
 - Incremento de automatización a bordo y en tierra
- Plataformas proveen características importantes como
 - 🔍 Servicio y capacidad de (Discoverability)
 - 🔒 Gestión segura de identidad
 - 🎵 Servicio de orquestación (Orchestration)



https://dvzpv6x5302g1.cloudfront.net/AcuCustom/Sitename/DAM/073/Fleet_Data_delivers_digitalisation_to_fleets_of_ships_Main.jpg



Criteria for e-Navigation Platforms

- **Architecture of Stable System**

- **Efficient:** performance relative to the amount of resources
- **Robust:** ability to deal with errors and functions in less optimal conditions (e.g. Volatile connectivity at sea)
- **Resilience:** ability to provide an acceptable level of service in daily operation under events of discontinuity

- **Cybersecurity**

- Integrity of information: Protected against modifications
- Information exchange resistant to manipulations



IALA G 1161, IALA G 1157 e IEC SECOM

- Mas detalle:
 - **IALA G1161**: Evaluation of Platforms for the Provision of Maritime Services in the Context of e-Navigation
 - **IALA G1157**: Web Service Based S-100 Data Exchange
 - **IEC 63173-2**: Maritime Navigation and Radiocommunication Equipment and Systems
 - Data Interface – Part 2: Secure communication between ship and shore (SECOM)



Conclusiones

- Las Comunicaciones maritimas tradicionales no son seguras → Uso indebido y manipulacion de la informacion es posible y facil.
- Digitalizacion prove soluciones para un intercambio seguro de informacion.
 - Encryptado, firma digital, certificados, PKIs (infraestructura de claves públicas), etc.
- Se require Plataformas de e-Navigation para facilitar la comunicacion Segura en los servicios maritimos.



<https://mfame.guru/a-digital-twin-to-develop-blue-denmark/>

Tecnologias de Internet y las plataformas digitales de e-Nav
securizan el possible intercambio de informacion – por
primera vez!