Cyber Security in Maritime Shipping Data Exchanges

Authenticity, Integrity and Confidentiality

Summary

Today, maritime shipping undergoes rapid digitalization. This applies to safety and security reporting, mandatory ship documents, electronic port clearance as well as commercial and operational information exchanges. The move from paper and voice based communication to digital and automated information exchanges creates new requirements to authentication of document originator, verifiable integrity of messages as well as confidentiality when this is needed. Papers with stamps and signatures in sealed envelopes currently provide these mechanisms. In the future, new digital solutions are needed to maintain and increase the trust and accountability between parties. These mechanisms provide:

- Exact and secure exchange of mission critical information, e.g. charts and other nautical data. This is important as a counter-measure to cyber-attacks on safety critical information.
- Guarantees that message exchanges have taken place and that the contents of messages have been accepted by recipient. This is important, e.g. to avoid detentions or fines.
- Digitalization of ship certificates, log books and other mandatory ship documents. This dramatically simplifies administrative processes on the ship.
- Protection of operational and commercial messages, such as voyage orders, bills of lading etc., so that business processes can be digitalized and streamlined.

Ships move internationally, and frequently encounter ports or port organisations that they have never met before. New security mechanisms must be internationally applied so that the required trust can be established without prior exchanges of user codes, passwords or similar user authentication data. This paper outlines a possible technical solution that has been adapted from an aerospace application with very similar requirements as the maritime.

1 High level functionality

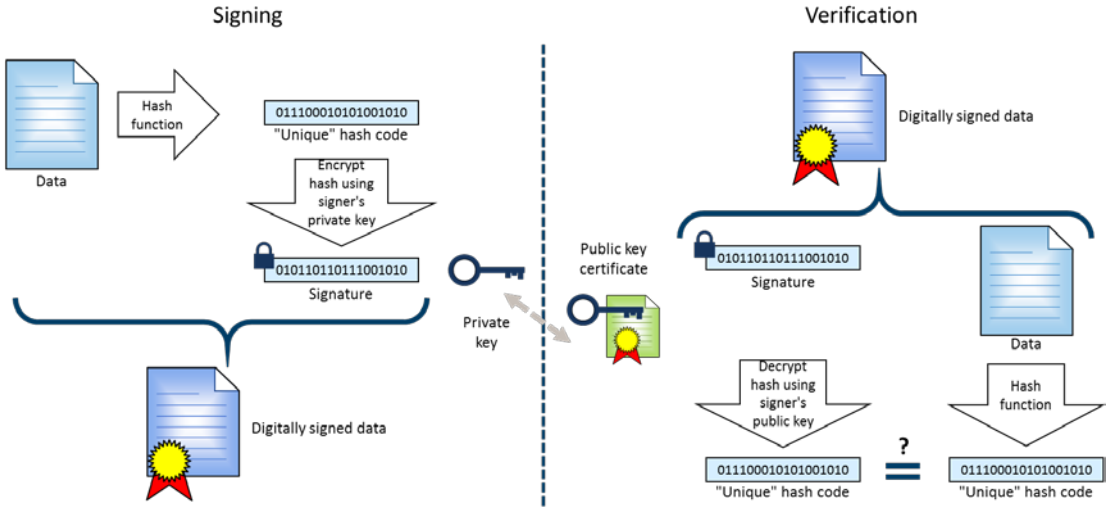
Public-key cryptography is the most common mechanism behind systems that provide digital trust between parties.

The mechanism is illustrated in the figure on the next page, where the combination of a private key and a public key certificate is at the core of the system. The essence of this mechanism is that once the sending party has signed a message (or document) using his *private* key, the signature can be verified by anyone having a copy of the sending party's *public* key certificate.

The system requires a small hierarchy of trusted entities to issue the private key to the signing party and to publish the public key certificate. This enables anyone to verify that documents sent by the private key holder are indeed issued by that party. The same mechanism can be used as basis to support the following:

- **Authentication**: Proving that an issuer of a document or data file is the entity it claims to be. This corresponds to the written signature and official stamp on paper.

- **Integrity**: That the content of the document has not been changed since it was issued. This corresponds to the difficulties in changing printed text on paper.
- **Confidentiality**: That no one else than the intended recipient can read and understand the content of the document. This corresponds to the sealed envelope.



By giving both sender and recipient their own private keys, it is also easy to send acknowledgements on reception that can be verified by the original sender and used as proof that the original message was indeed sent. Likewise, the signature on the original message serves as proof that the sender really sent the message.

The system normally makes use of a hashing or "check-summing" mechanism to avoid having to apply the encryption algorithm to the whole message. This allows the use of open data exchanges where all can read and understand the message without needing to implement the cryptographic system. However, only those that have implemented the system will be able to verify the authenticity and integrity of the data. This is useful for nautical information broadcasted by coastal or port state authorities, where older ships without the newest equipment also must be supported.

Electronic implementations of the trust functions will generally be much more difficult to circumvent than the corresponding mechanisms for paper. The security can be set at arbitrarily high levels, but this is a trade-off between security and operational complexity and cost. The mechanisms described here are the same as those used for Internet banking and shopping. The underlying mathematics are complex, but all this is hidden from the users.

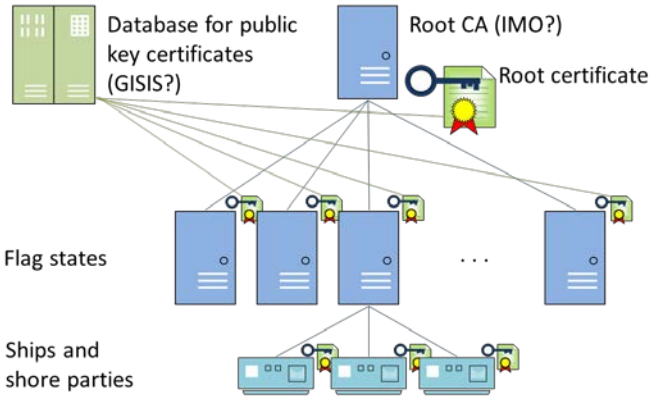
2 A Public Key Infrastructure (PKI) for Shipping

To make the electronic trust system work, the shipping community needs to implement a Public Key Infrastructure (PKI). Many PKIs are already in operation and most have been established by private entities on a commercial basis. However, shipping differs from land based commerce in several important aspects:

- Ships may not always be connected to internet and most established signature system PKIs use on-line exchanges of the public key certificates. Likewise, the standard PKIs use online access to provide any revocation lists and to verify the trust hierarchy anchors.
- Ships operate internationally and need a PKI on an international level and with internationally trusted servers.

- Ships already have a trusted hierarchy based on IMO as international legislator and the flag state authorities as national representatives. This can be used as a starting point to build the hierarchy of trusted entities that are needed in the PKI.
- Ships are bandwidth restricted, for digital VHF communication (VDES), but also to some degree for satellite and mobile data connections. One need to find technical solutions that can be implemented without too high bandwidth requirements for the message signatures themselves or for updates to lists of public key certificates.

A shipping PKI can be set up with IMO as the top trusted entity ("root certificate authority - CA") with flag states directly underneath. Flag states can issue new keys and certificates to its coastal state authorities, ships under their flag, their recognized organisations, ports and others that need an internationally available public key certificate. One can also issue certificates to ship owners or other organisations that have important roles in the international shipping community.



The technical operation could be implemented by IMO or by any other commercial or professional organisation that has the required technical skills. IMO already operates a PKI for Long Range Identification and Tracking (LRIT) that could be extended to general shipping. An official list of public key certificates for international shipping operators could be hosted on GISIS. With 125 000 entities, which covers all ships, all ports and most port and flag state organisations, this would be around 600 mega-bytes. The list will need to be uploaded to the ship when the cryptographic system is installed and only updated with changes each time the ship is in port

Changes in the list will be relatively rare; certificates will be updated at about the same rate as MMSI's are changed. In addition, certificates will be made to expire after some years to keep a good security level. Thus, the update will normally be 1-2 megabytes per week. Doing this in port avoids that ship must use expensive satellite bandwidth to keep the list updated. Missing the updates for several weeks will not be a problem as the system can employ alternative methods for authentication that has a slightly higher cost in terms of bandwidth use.

Ship agents and other commercial operators should be able to operate within national legislation and use whatever certificate mechanism that is used locally. They can use a document signed by the ships certificate to prove their link to specific ships.

3 Implementation on board and on shore

Ships can have one or more private keys that are used to sign outgoing documents. The ship also needs the most common international public key certificates. The latter can be stored in a normal

data-base while the private key requires more extensive security measures to avoid that it is stolen or otherwise compromised.

The additional message size due to the signature will be less than 100 bytes for a single text document or report. For real-time message exchanges, it will be possible to reduce this further by establishing a "communication session" that uses smaller signatures for a limited amount of time.

One possibility for the on-board private certificate is to distribute it on tamper-resistant smart card that can be read by a standard smart card reader. The reader can be accessed from any computer on the same ship data network. Computers or electronic equipment on the ship can then use this smart card to sign any outgoing messages. Incoming messages can be validated by standard software that uses the list of public certificates to do the validation.

The ship can have any number of smart cards and card readers. These can be "activated" one or more at a time and can serve as backup if a card for some reason stops to function.

Messages that are simply signed and not encrypted can be read in clear text even if integrity and authenticity verification is not possible. The content should then be checked by a human operator before actions are taken based on the information in the message. This means that implementation of such a regime can be made gradually with backward compatibility.

This information paper has been provided by the CySiMS (Cyber Security in Merchant Shipping) research and development project. The project is part funded by the Norwegian Research Council through contract number 256508/O80. More information at http://cysims.no/.

Revision 5, Trondheim, 15th September 2019.