Input paper: [1] ENAV19-n.n.n

Input paper for the following Committee(s):	check as appropriate		Purpose of paper:
☐ ARM	☐ ENG	☐ PAP	☐ Input
X ENAV	☐ VTS		**X** Information

Agenda item [2]	n.n
Technical Domain / Task Number [2]	……
Author(s) / Submitter(s)	Maritime Cloud Development Forum: Viktoria Swedish ICT (Sweden) KRISO (Republic of Korea) ETRI (Republic of Korea) Frequentis (Austria) OFFIS (Germany) Danish Maritime Authority (Denmark)

Identity Management and Cyber Security

1 SUMMARY

This paper is an attempt to explain the current status of the part of the Maritime Cloud that is related to identity management and security. Hereunder the Identity Registry and its various parts. It will not go into any details about other Maritime Cloud infrastructure services such as the Service Registry and the Maritime Messaging Service.

For clarity it should be stressed that 'services' in the context of this document are 'technical services'. This could for instance be a service that provides the digital information about weather forecasts in a specific geographical area. It would not be the provision of pilotage in an area, which is also a service, but this would be considered an operational service.

1.1 Purpose of the document

Giving the Committee a broader understanding of the Maritime Cloud Identity Management and Security. This topic was discussed at eNav18, and many wanted a further elaboration of the topic, which hereby is provided.

1.2 Related documents

- Specification guideline for Technical Services (also submitted to eNav 19)
- Maritime Cloud – Conceptual Model (also submitted to eNav 19)

2 BACKGROUND

The Maritime Cloud is an initiative towards providing infrastructural functions such as supporting the concept of a digital maritime identity. Three multi-partner projects, the EfficienSea2 project, the STM validation project (co-funded by the European Commission) and the Korean SMART navigation project – aim to establish and operate such infrastructure functions in the timeframe 2016 - 2018, to demonstrate their value and validate specific services concepts within E-navigation and Sea Traffic Management (the

1 Input document number, to be assigned by the Committee Secretary
2 Leave open if uncertain

SeaSWIM concept). The strategic aim is to use these projects to validate the Maritime Cloud concept, while functioning as the breeding ground for establishing a sustainable operational community for the future. Although the initial aim is support within the projects, the infrastructure can be used by any maritime project that needs a similar setup.

3 INTRODUCTION

A key part in service-oriented economy is the concept of network-based, automated transactions. These transactions almost always need to identify the source, receiver and resources that participates in the transaction. Not only are these transactions central to businesses, but organizations have an ever increasing need to identify employees, resources, systems, and services in a systematic way to ensure the agility of their business as well as securing their business assets. In short, in the digitally service-oriented economy that the maritime industry (and many other industries) are moving towards, digital identity is something that matters.

The lack of a global digital identity of users/vessels/systems is a serious bottleneck in starting a digital maritime revolution across different companies and individuals. Just like human to human communication on a worldwide scale would be impossible without global unique telephone numbers/email addresses. So is trying to integrate a maritime system on a global scale without some concept of a digital maritime identity for the various actors that participate.

4 IDENTITY MANAGEMENT

Identity management refers to the process of employing emerging technologies to manage information about the identity of users and control access to company resources. The goal of identity management is to improve productivity and security while lowering costs associated with managing users and their identities, attributes, and credentials.

The goal of the Maritime Clouds Identity Registry is to create a solution that satisfies the most common identification needs for the entire maritime industry on a global scale.

This is not a simple task as any solution must support every possible user scenario from small leisure sailors to multinational companies. The complexity of this task is why the functionality will be delivered over multiple milestones in the coming years. With the most important things such as support for authentication being implemented first. Additional functionality being added based on user needs in the projects supported by the Maritime Cloud.

5 THE MARITIME CLOUD IDENTITY REGISTRY

In most of the documents that describe the Maritime Cloud there is the concept of an Identity Registry. In reality there are numerous systems both internal to the Maritime Cloud as well as external to the Maritime Cloud that makes up the Identity Registry. Not only are there multiple registries but the interaction with them can also depend on, for example, the type of authentication used. Something like digital certificates can be used offline for authentication, that is, there is no need to contact the Identity Registry to validate a digital certificate. But if a username/password combination is used, both the Identity Registry and an external Identity Registry server belonging to a trusted organization needs to be contacted. Hence a better description of the Identity Registry would probably be an Identity Platform.

Within the scope of the EfficienSea2 and STM validation projects, the digital identities of actors of organizations can be registered in a project Identity Register, thereby giving trusted organizations access without requiring access to the organizations Identity Registry.

This will enable the participants in the projects to easily register actors to validate specific service concepts in testbed trials or utilize the operational services established by the projects, as well as validate the identity management concept of the Maritime Cloud. Beyond the scope of the project, it is foreseen that several identity registries will collaborate to form the global federated Maritime Cloud Identity Registry.

6 KEY ACTOR CONCEPTS

In order to be able to describe some of the concepts we are working with, here is a short introduction of the various actors we envision will interact with the identity registry.

Identity management and security is a very complex and comprehensive field. So wherever possible we must limit non-essential functionality. Clearly, there are some maritime entities that should not be a part of the Identity Registry. Therefore, the Identity Registry should not be:

- Managing information about entities that does not need to have access rights. For example, route or container information. While information about routes can be accessed by various users and systems, routes by them self does not need access rights to access other information. It is only users and systems/devices that need access right.
- Maintaining information about entities that are not security related. For example, business addresses of users, or location information about entities that can be used, for example, for routing messages to the right location.

The main reason for excluding all but non-essential security related information is that it opens up the never ending discussion about what exactly should be maintained in the Identity Registry. If we make a generalized information store that maintains and provides query capabilities for all kinds of information about users and systems/devices, for example, business addresses and geographical location, we might as well use this functionality for storing other queryable information such as, maintaining information about routes or cargo.

This does not prohibit a later revisiting of these goals, or prohibit including work from other groups into a general framework at a later time. But for time being the Identity Registry will revolve about the 5 entities listed below.

6.1 Organization

In the Maritime Cloud an *organization* is an entity, such as an institution, company or an association, that has a collective goal and is linked to an external environment. Examples, include international organizations such as IMO, IALA, IHO. National authorities such as US Coastguard, Swedish Maritime Administration. Local authorities such as VTS-Oeresund, Port of Rotterdam, Hong Kong SAR. Or commercial companies such as Transas or Maris.

In order to be able to use the functionality of the Maritime Cloud in any way, an organization needs to be signed up to the Maritime Cloud. In the context of the EfficienSea2 and STM projects, this is currently done by filling out a form on the Maritime Cloud Portal, and the Maritime Cloud testbed administrator then decides whether the organization should be added.

In the future a process involving a validation workflow by some governing organization may validate the relationship between an organization in the real world, and the issued maritime digital identity. How this validation is to take place is still up for discussion. However, one possible solution would be for the maritime authorities in which a given organization is registered to put the stamp of approval on the signup application.

Once an organization has been registered (and validated), an identity administrator of that organization will be able to create and manage maritime identities that belong to this organization, such as Users, Vessels or Services. This administration is typically done via the Maritime Cloud Portal which is a web based client. For some larger organizations it might make sense to integrate directly via the underlying APIs.

6.2 Vessels

Vessels describes any floating object used for the carriage of people or goods.

The main need for registering vessels in the Maritime Cloud is so that digital certificates can be issued for them. Thereby enabling secure communication between vessels as well as digitally signing of documents. Users might also use these certificates for other purposes. The important thing is that the functionality is there.

As part of the certificate of a vessel, its name, MMSI number, IMO number, callsign and possible other attributes is included in the header of the certificate.

6.3 Services

Services refers to digital services. For example, a weather service that is available to other services for machine to machine communication. Services needs to be registered in such a way that it can successfully authenticate users, but they can also have a need themselves to be able to communicate with other services, and therefore have to be able to authenticate to other services.

6.4 Users

Users mainly refers to human users. Human users differ from other actors in that they typically use a username/password to login which implies a different interaction pattern with the Identity Registry than say communication between vessels.

6.5 Devices

Devices refers to any entity that needs to authenticate using the Maritime Cloud, but does not fall in any of the other entity categories mentioned above.

7 AUTHENTICATION

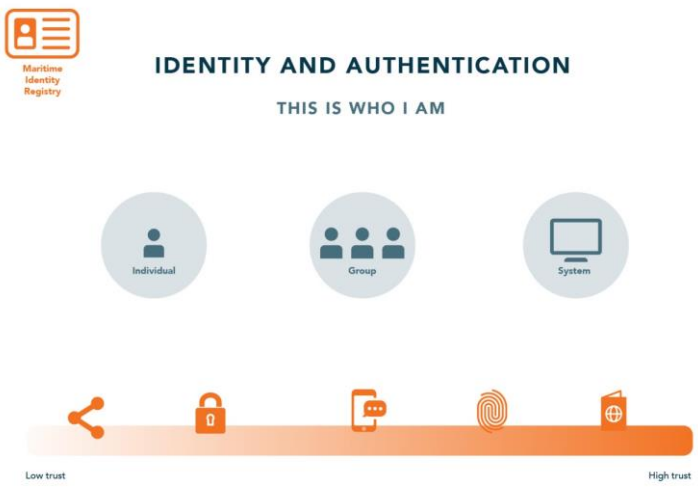

Figure 1 Identity and Authentication

Authentication is any process by which a system verifies the identity of a user (human or machine) who wishes to access it. Since access control is normally based on the identity of the user who requests access to a resource, authentication is essential to effective security. In contrast to identification which refers to the act of stating a person or thing's identity, authentication is the process of actually confirming that stated identity. It might involve verifying the authenticity of a website by a digital certificate that it provides, or validating a person's identity documents.

The way in which a human user or machine may be authenticated typically falls into three different categories, based on what is commonly known as the factors of authentication: something the user knows, something the user has, and something the user is. Each authentication factor covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority.

- **Knowledge factors:** Passwords, passphrases, pins, challenge response, …
- **Ownership factors:** ID card, Cell phone, certificates, …
- **Inheritance factors:** Fingerprint, retinal patterns, face, voice, …

Currently the implementation effort in the Maritime Cloud is concentrating on *knowledge factors (typically username/password)* for human users and *ownership factors (certificates)* for machine users.

While the difference of the factors might seem minor from a user perspective the underlying implementation is radically different which is why it has been split into two different sections.

7.1 Certificates, PKI and M2M Communication

A **public key infrastructure** (**PKI**) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. Thereby helping an organization establish and maintain a trustworthy networking environment. There is no inherent requirement for using a PKI based solution for enabling secure machine to machine (M2M) communication. But it is the most commonly used solution and lots of software, standards and best practices exists for utilizing it. The choice of using PKI based on the X.509 standard for M2M communication in the Maritime Cloud was thus straightforward.

The key piece in a PKI architecture is a PKI CA (Certificate Authority) which is an entity that issues digital certificates. A digital certificate that certifies the ownership of a public key by the named subject of the certificate. An obvious example would be creating a certificate for a vessel, which can serve to certify that a given document was indeed signed by someone in possession of the certificate issued to that vessel.

One of the most important aspects of designing a PKI based architecture is the certificate hierarchy planning, because the design will affect how certificates are validated and used by PKI-enabled actors. Normally a PKI based architecture is arranged in a tree like hierarchy with a single root entity in the top and with numerous leaves called sub CAs. Each sub CA can have their own sub CA thereby forming a tree with a single entity at the top. Each leave in the tree is responsible for creating certificates, for example, ships or organizations. The reason for doing this is to be able to delegate the responsibility to different parties. For example, in the case of the Maritime Cloud one could envision that at some point in the future every flag state would be their own sub CA. Having the sole responsibility of issuing certificates for vessels registered under their own flag.

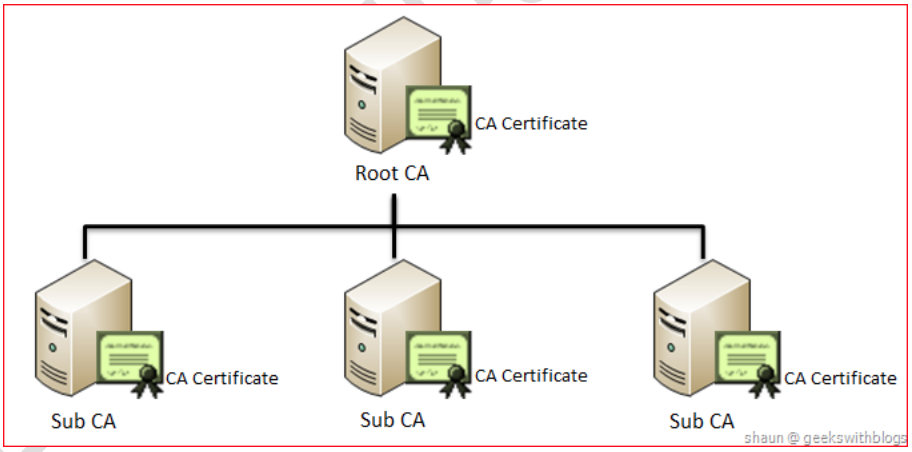

Figure 2 Certificate hierarchy

In the current version of the Maritime Cloud we are working with a single sub CA that has the responsibility for issuing all certificates. This sub CA is located at the Maritime Cloud Identity Registry. However, this can gradually be changed to support another PKI hierarchy design.

The most important functionality of a CA is issuing digital certificates. A digital certificate, certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. In this model of trust relationships, a CA is a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. In the case of the Maritime Cloud these certificates are typically used to make secure connections between maritime actors over the Internet. A certificate is required in order to avoid the case that a malicious party which happens to be on the path to the target server pretends to be the actual target. Such a scenario is commonly referred to as a man-in-the-middle

attack. The client uses the CA certificate to verify the CA signature on the server certificate, as part of the checks before establishing a secure connection. Likewise, the server has the option of inspecting the clients certificate before allowing it to connect.

To issue a new certificate for, for example, a vessel, the administrator of the organization who owns the ship will need to log in to the Maritime Cloud Portal and use its functionality for issuing new certificates. The certificate being issued will contain information about the name of the ship, the owner, the flag state and other attributes such as MMSI and IMO number. In the current implementation there is no validation of this information other than that the organization must have been accepted when signing up. We do not expect this to be a problem for the foreseeable future as the number of participating parties is still relatively small. In the future where a lot of more organizations has been added it might, for example, be possible to integrate with national registries, so an automated check of these information can be made.

After having issued a certificate the administrator can now install it on the ship in some way. The actual logistics about how and where to install it is outside of the scope of the Identity Registry as this might vary a lot between organizations and projects. This also reduces the functionality of the Identity Registry to just provide the core functionality of identity management. Allowing users to be able to build innovative solutions on top of it. This also applies directly to machine to machine communication. The Identity Registry places no restrictions for what kind of machine to machine communication protocols that should be used. It just provides the basic infrastructure to allow for each machine to authenticate the host in the other end. Letting each project select their protocols if needed.

7.2 Human based login

In the previous section we discussed digital certificates for use in machine to machine communication. There are no technical issues to why human users should not be able to use digital certificates to authenticate themselves as well. However, there are some serious practical ones that make it difficult to see them as a general solution for human user authentication. The first issue being that it requires, that the certificate must always be present on the computer or mobile phone from which access is made. This is normally not a problem for machine to machine communication. Because, once installed the hardware configuration almost never changes. Unlike human users that uses their computer during the day to access information, their mobile phone on the way back from work and their tablet in the evening from home. Making sure that certificates are all installed on these devices and refreshing them once they expire is a lot of effort to require of users. We believe having such a complicated setup would be a major barrier towards successful adoption of the Maritime Cloud. So for now, username and passwords are the main technology used for human authentication in the Maritime Cloud.

7.2.1 Federation

Federation is the means of linking distinct identity management systems to a person's electronic identity and attributes. For example, a shipping company might expose all their users via LDAP or Active Directory to the Maritime Cloud in such a way as they appear as Maritime Cloud users. Thereby bypassing the need to manage their users directly in the Maritime Cloud.

7.2.2 OpenID Connect

There exists several standards for exchanging authentication and authorization data between security domains. OpenID Connect is a fairly new standard, but it is built on top of the proven OAuth2 standard and has backing from several large industry players such as Google and Microsoft. OpenID Connect has a number of features that makes it useful for user federation in the Maritime Cloud:

- It is built on already existing open standards (OAuth2, JWT).
- It can be used to authenticate for both websites, web services and native smartphone apps.
- There already exist a number available implementations, both open source and commercial.

An example on how OpenID Connect works can be seen in the diagram below:

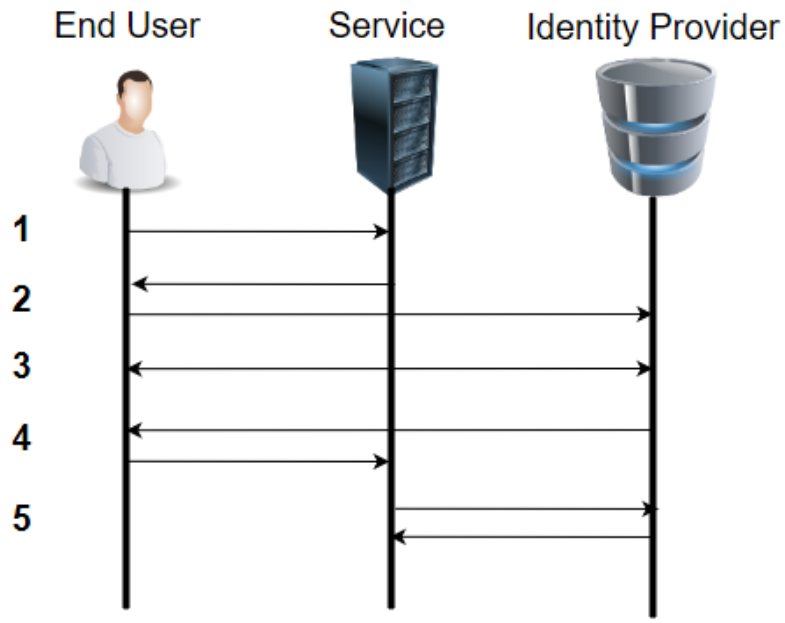

Figure 3 OpenID Connect Authentication flow

1 User opens up a Web based Service (Relying Party), clicks “log in with Maritime ID”.

2 Service redirects the user to an Identity Provider in which the user has registered his login information. For example, an Identity Provider setup by the organization he works for.

3 The user logs in using his company username/password, and gives consent to transferring his information back to the relying party. Notice it is only the Identity Provider setup by his company that receives his password.

4 Identity Provider redirects the user (browser) back to the relying party, with an authentication code.

5 The relying party ask the Identity Provider to validate the authentication code. The Identity Provider replies with a set of JWT tokens, that contains information about the user.

Since OpenID Connect delegates the actual login to the organization of the user, the organization can itself control how to verify if the user really is who the user claims to be. This means that not only username/password can be used but also 2-factor authentication or even biometrics.

7.2.3 Keycloak

Keycloak is one of many products that includes support for OpenID Connect. It is an open source product developed by RedHat. Keycloak can be set up to work in different ways. It can be set up to work as an Identity Provider, using either a database or LDAP/AD as a backend. Or it can be set up as an Identity Broker in which case it will link to other Identity Providers. When acting as an Identity Broker the diagram for authentication as seen above becomes a bit more complicated since another step is added where the service first redirects to the Identity Broker where the user has to choose which Identity Provider he wants to use. Before being redirected to the Identity Provides login page.

The functionality of the Identity Broker is the cornerstone in the Maritime Cloud user federation. Enabling outside organizations to act as Identity Provides via the Identity Broker.

8 AUTHORISATION

Figure 4 Authorisation

Another central aspect of Identity Management is the concept of authorisation which is the process of determining a set of permissions that is granted to a specific trusted identity. In all practical senses, authorization follows authentication. Once a system knows who you are, the system can determine what is appropriate for you to be able to see or do. Authorisation can be determined based on the user identity alone, but in most cases requires additional attributes about the user, such as role, title, flag state, etc.

Authorisation can typically be handled in two ways.

- Locally by the application or service that is being accessed.
- Centralizing the authorization policy decisions regardless of the location of the user or the application/service

Authorisation can always be done locally by the application that is being accessed, for example by storing user rights in a local database. Therefore, we have decided that the Maritime Cloud will not prioritize central support for authorisation for the next milestones. Instead focusing on getting authentication right.

Before implementation of centralized support for authorisation can begin there are some obstacles that lie ahead. Mainly because there, unlike authentication, are no good standards for doing authorisation.

Even though there are no real standards there are a number of approaches that are commonly used. The most commonly used probably being *role-based access control* (RBAC). RBAC is an access control mechanism defined around roles and privileges. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to do user assignments of entitlements. However, adopting RBAC for the Maritime Cloud opens some questions. For example, who defines the roles and are they global roles. Or are they local to a particular service or a particular organization. For example, an "administrator" role might entail a list of certain privileges in one organization and another list of privileges in another organization.

Given these issues and many other we have to decide to wait on the various to sub projects to implement authorisation and then, if possible, compile all the different approaches and try and make something generic.

9 OTHER AREAS

There are other areas within identity management and cyber security in general that we hope to work with in the future in such a way as to provide good standards and best practices for participating projects.

9.1 Cryptography

At some point we hope to define standards for encryption and signing of messages. Hereunder asymmetric and symmetric encryption, digital signatures, message authentication codes (MAC), and key distribution. Deciding on encryption algorithms and system architecture are especially important in relation to bandwidth limitation and offline ships. For example, almost all traditional message signing algorithms (RSA, DSA, ECDSA) uses at least 400 bits for a signature. But some never algorithms such as BLS (Boneh–Lynn–Shacham) uses down to 200 bits for a secure signature. Other issues involve offline ships that might have a hard time doing online verification of users and other ships.

9.2 Privacy

The right to privacy plays an increasing bigger role in people's life. And with the increasing digitalization of the maritime industry it is likely to play a bigger role here as well.

For example, many potential services are location based services. It might be necessary to setup guidelines in the way service providers handle information about client's position.

The work on privacy in the Maritime Cloud is mainly intended to result in various forms of recommendations.

10 TERMINOLOGY

Most of the terminology in this section has been taken from ISO/IEC 24760-1:2011 - A framework for identity management - Terminology and concepts

Authentication: The process of verifying the identity claimed by an entity based on its credentials.

Authorization: The process of establishing a specific entitlement that is consistent with authorization policies.

Authorization policies: Declarations that define entitlements of a security principal and any constraints related to that entitlement.

Entitlements: The actions an entity in a network is allowed to perform and the resources to which it is allowed access.

Federated identity: Is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems

Identity: The set of attributes that uniquely identifies a security principal. A security principal can have many different accounts that it uses to access various applications in the network. These accounts can be identified by these applications using different attributes of this entity. For example, a user can be known in the e-mail service by an e-mail ID, whereas that same user can be known in the human resource application by an employee number. The global set of such attributes constitutes the identity of the entity.

Identity administration: The act of managing information associated with the identity of a security principal. The information can be used by the identity management infrastructure itself to determine administrative privileges.

Identity management policies: Policies affecting the management of identities which includes naming policies and security policies.

Realm: A collection of identities and associated policies which is typically used when enterprises want to isolate user populations and enforce different identity management policies for each population.

Security principals: The subjects of authorization policies, such as users, user groups, and roles. A security principal can be a human or any application entity with an identity in the network and credentials to assert the identity.

11 ACTION REQUESTED OF THE COMMITTEE

The Committee is requested to note the information and take appropriate action.