MONALISA 2.0_D2.3.1-1

Target Institutional Description

Co-financed by the European Union
Trans-European Transport Network (TEN-T)
## Document Status

### Authors

<table>
<thead>
<tr>
<th>Name</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lars-Göran Malmberg</td>
<td>Department of Law at School of Business Economics and Law, University of Gothenburg</td>
</tr>
<tr>
<td>Abhinayan Basu Bal</td>
<td>Department of Law at School of Business Economics and Law, University of Gothenburg</td>
</tr>
<tr>
<td>Trisha Rajput</td>
<td>Department of Law at School of Business Economics and Law, University of Gothenburg</td>
</tr>
</tbody>
</table>

### Review

<table>
<thead>
<tr>
<th>Name</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Approval

<table>
<thead>
<tr>
<th>Name</th>
<th>Organisation</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Status</th>
<th>Initials</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TEN-T PROJECT NO:** 2012-EU-21007-S

**DISCLAIMER:** THIS INFORMATION REFLECTS THE VIEW OF THE AUTHOR(S) AND THE EUROPEAN COMMISSION IS NOT LIABLE FOR ANY USE THAT MAY BE MADE OF THE INFORMATION CONTAINED THEREIN.
# Table of contents

1 General information................................................................................................................................. 4

2 Introduction and Background ................................................................................................................... 5
   2.1 Scope and Purpose of Report.............................................................................................................. 6
   2.2 Structure of the Report....................................................................................................................... 6

3 Legal Issues Pertaining to Identity Management in the Context of SeaSWIM ........................................ 7
   3.1 Fundamentals of Identity Management............................................................................................. 8
   3.2 Basics of Identity Federation............................................................................................................ 9
   3.3 SeaSWIM as a Provider of Federated Identity Management............................................................ 10
      3.3.1 A Maritime Stakeholder as the Subject ................................................................................... 10
      3.3.2 SeaSWIM as the Identity Provider.......................................................................................... 11
      3.3.3 A Maritime Stakeholder as the Relying Party.......................................................................... 12
   3.4 The Main Challenges for Participants in SeaSWIM......................................................................... 12
      3.4.1 Organizational Challenges.......................................................................................................... 12
      3.4.2 Legal Challenges......................................................................................................................... 14

4 Legal Framework to Meet the Challenges and the SeaSWIM Rulebook ............................................. 17

5 Recent Legislative Efforts on Identity Management and Trust Services ............................................. 19
   5.1 EU eIDAS Regulation ....................................................................................................................... 20
   5.2 The Electronic Identity Management Act of Virginia .................................................................... 21
   5.3 Initiative at UNCITRAL Working Group IV on Electronic Commerce ........................................ 21

6 Concluding Remarks ............................................................................................................................... 22
1 General information

MONALISA 2.0 is a project with 39 private, public and academic partners from 10 different countries. Its overall objective is to strengthen efficiency, safety and environmental performance in maritime transportation. Coordinated by the Swedish Maritime Administration, the project is co-financed by TEN-T under the Motorways of the Sea Programme and is part of the EU’s e-Maritime initiative. MONALISA 2.0 follows on from the MONALISA project (2010-EU-21109-S) and also incorporates results and experiences from the SESAR (Air Traffic Management) programme in the aviation sector. MONALISA 2.0 is divided into four Activities: Activity 1, STM Operations and Tools; Activity 2, STM Definition; Activity 3, Safer Ships; and Activity 4, Operational Safety.

This document is a deliverable from Activity 2 of the MONALISA 2.0 project. The objective of Activity 2 is to outline a framework for Sea Traffic Management (STM), elaborate its target concept, and develop a plan for further development and deployment.
2 Introduction and Background

In recent years, the maritime transport industry has witnessed increased use of information and communication technology from navigation to loading and unloading of cargo at ports. However, lack of process integration between the various stakeholders in the industry leaves room for creating greater situational awareness through innovative services and a common communication infrastructure to increase safety, efficiency and environmental protection. The Sea Traffic Management (STM) concept conceived under the MONALISA Project has the potential to overcome many of the challenges of communication and information sharing between stakeholders in the maritime transport industry.

At the commencement of the project, MONALISA was described as “Motorways and Electronic Navigation by Intelligence at Sea”. At that time the main aim was to contribute in a concrete way to safe, efficient and environmentally protective maritime navigation. However, during phase 2 of the project, the description of MONALISA evolved to “Securing the Chain by Intelligence at Sea”. The vision of the project, as it currently stands, is to shake up and sharpen the whole transport chain by making real-time information available to all interested and authorised parties.

STM has been summarised as sharing secure, relevant and timely maritime information between authorised service providers and users, enabled by a common framework and standards for information and access management, and interoperable services. STM is constituted of four sub-concepts, namely, Strategic Voyage Management (SVM), Dynamic Voyage Management (DVM), Flow Management (FM) and Port Collaborative Decision Making (PCDM), all of which are enabled by a distributed and service based information management system called the Sea System Wide Information Management (SeaSWIM).

STM brings into fore the analytical use and sharing of information in the maritime domain. The first three sub-concepts, namely SVM, DVM and FM, relates to efficient navigation through enhanced interaction of ship-to-ship, ship-to-shore, shore-to-ship and shore-to-shore information sharing between various stakeholders. As identified in an earlier study, the implementation of these sub-concepts will require resolution of certain conflicts with international convention instruments such as UNCLOS, SOLAS, COLREGS, and STCW. The fourth sub-concept, PCDM, focuses on the commercial aspects of shipping and therefore its implementation will mainly require acceptability from commercial actors involved in maritime trade. SeaSWIM is envisaged to allow various actors in the industry to become part of a regulated and federated data sharing and service-provisioning ecosystem. SeaSWIM will enable

---


distribution of and access to data streams (open, proprietary, or hybrid) by various stakeholders in the shipping industry to authorised parties through a discoverability mechanism in accordance with certain defined standards.

2.1 Scope and Purpose of Report

The implementation of the MONALISA Project will not cause a revolutionary change in the maritime transport industry in terms of existing business and navigation related procedures and systems. It will rather bring an evolutionary change based on federated information exchange and service-provisioning ecosystem. Hence the focus of the legal analysis is on the SeaSWIM concept which will enable this information exchange between the various stakeholders in the maritime transport industry.

One of the important functions of SeaSWIM is to provide for an identity management system for both shore based and ship borne actors. SeaSWIM also aims to provide general service portfolio management and access management, which are closely tied to its identity management service. SeaSWIM also intends to provide governance and monitoring to the entire ecosystem, which requires the creation of a suitable trust framework.

Identity management is a key element for the delivery of any e-services.\(^3\) It provides assurance to an actor that no unauthorised use is made of its identity and personal data. Also, the service providers associated with SeaSWIM are able to make sure that the actor is the entity it claims to be and have the right that it claims to have to receive the requested service(s). Currently there are a number of possible technological solutions to provide an identity management service but the main challenge in the implementation of SeaSWIM is a multitude of unresolved legal issues on the subject.

This report identifies and analyses the legal issues that arise in connection with the development, implementation and use of SeaSWIM from an international perspective. This work lays the foundation for possible future studies to identify and evaluate liability models for an appropriate legal framework for SeaSWIM and lead to the development of sample terms and contracts that can be used by the parties.

2.2 Structure of the Report

The remainder of this report is organized as follows. Section 2 of the report highlights the key legal issues pertaining to SeaSWIM. To properly identify and address the legal issues for implementing SeaSWIM, first an outline of the basic concepts of identity management and federated identity management is presented. Then the discussion focuses on the basic roles, functions and duties of participants in SeaSWIM. Finally, this section identifies the major risks for participants in

SeaSWIM, which includes challenges related to technology, process, performance, privacy, data security, liability, enforceability and regulatory compliance.

Section 3 of the report suggests ways in which the risks for participants in SeaSWIM can be addressed by creating a legal framework based on existing publicly created identity management laws supplanted by private law created through contracts. A discussion on various models for trust frameworks is made and creation of a SeaSWIM Rulebook is suggested. Such a Rulebook will comprise of contractual agreements among the parties, standards adopted by the parties, and self-asserted undertakings.

Section 4 of this report discusses the recently adopted European Union (EU) Regulation on identity management and compares the approach taken therein vis-à-vis a newly adopted American legislation on the subject. Also, a reference to the initiative at United Nations Commission on International Trade Law (UNCITRAL) Working Group IV on Electronic Commerce is briefly made. Section 5 presents a summary of possible future legal research related to the Project ends this report with a few concluding remarks.

3 Legal Issues Pertaining to Identity Management in the Context of SeaSWIM

In order to develop the trust necessary to make the SeaSWIM ecosystem work, and understand and assess the risk of participation, all stakeholders in the ecosystem need - (1) to know with certainty the legal and technical rules/obligations, (2) to believe that those rules/obligations are effective, fair, and appropriate, (3) an assurance that others will follow those rules, and (4) the ability to enforce those rules/obligations if needed.

In theory it is possible to implement SeaSWIM using the existing laws of most jurisdictions but many lawyers will not know what that legal framework is, and most importantly the impact of the laws on SeaSWIM may be uncertain. This is because most of the relevant laws were written at a time before the Internet came into being and therefore the rules may not address the precise current needs. The rules are also likely to vary by a number of factors, such as, jurisdiction, nature of the participant, etc.

The existing laws that may provide a legal framework to SeaSWIM can broadly be categorised into two. In the first category are generally applicable statutes, regulations, and common law. This category will also include maritime and transport laws as SeaSWIM is essentially directed towards shipping, ports and logistics industries. The second category includes statutes and regulations specific to the subject of identity management consisting of public key infrastructure laws, certain EU regulations, identity laws, authentication laws, etc.4

4 Several national and regional initiatives in the field of identity management and/or trust services are actively underway. A brief discussion on such initiatives is made in section 5 of this report.
The broad legal spectrum relevant for implementation of SeaSWIM relates to that of contract; warranty; torts including negligent performance, negligent misrepresentation, fraudulent misrepresentation and defamation; third party beneficiary; e-transactions; consumer protection; data security; privacy/data protection; identity theft; antitrust; unfair competition; false endorsement; false advertising; intellectual property including copyright, trade secrets, trademark and patent; statutory/regulatory law governing the identity management process and imposing identity management compliance obligations; liability for the conduct of others; governmental immunity law; etc.

There are various factors which may affect the application of these laws to SeaSWIM. It ranges from issues relating to applicable law, nature of person involved (consumer, business, government entity), expertise of the person involved (unsophisticated or professional in the business), nature of the information involved, nature of the use involved, nature of any resulting harm (economic losses, property damage, personal injury), etc.

The discussion in the remainder of this section is directed to understand what is needed to develop an appropriate legal framework that - provides enforceable rules for a workable and trustworthy SeaSWIM ecosystem that are binding on all participants; adequately protects the rights of the parties; fairly allocates risk and responsibilities among the parties; provides legal certainty and predictability to the participants; complies with/works in conjunction with existing law; and is acceptable across jurisdictions.

### 3.1 Fundamentals of Identity Management

Identity management is defined as “the set of rules, procedures and technical components that implement an organisation’s policy related to the establishment, use and exchange of digital identity information for the purpose of accessing services or resources. Effective identity management policies safeguard digital identity information throughout its life cycle – from enrolment to revocation – while maximising the potential benefits of its use, including across domains to deliver joined-up services over the Internet.”

The concept of identity management is not new and such systems have existed for decades through use of documents such as passports, driver’s licenses, government issued ID cards, etc. These are all examples of credentials issued by an entity for the purpose of identifying individuals, and are often used to validate a person’s identity in order to enter into a transaction with a third party. Analysing the use of such credentials reveal that identity management involves three fundamental processes -

---

1. Identification - To identify a person and issue an identity credential to reflect her/his identity.

2. Authentication - To verify that a particular person presenting that credential and claiming to be that previously identified person is, in fact, such person.

3. Authorization - Once the person’s identity is successfully authenticated, it is used by a business relying on the authenticated identity to determine what rights and privileges are to be accorded to such person.  

It is notable that an important characteristic of some of the identity documents such as passport or driver’s license is that their use is not limited to transactions with the entities that issued them. Third parties often rely on them when a proof of certain aspects of one’s identity is required. It is this characteristic which is critical for the identity credentials needed for e-commerce. Such an approach, whereby a business or government agency relies on an identification process performed, and identity information provided, by one of several possible unrelated third parties is sometimes referred to as a federated identity model.

3.2 Basics of Identity Federation

The essential pre-requisite to build up a federation and to share the user authentication across different security domains is the establishment of trust between collaborating partners. Usually, this is done by setting up complex contracts that describe common policies, obligations and procedures to be followed by each federation member and using a common technology platform. Under a federated model, it is possible to use a single identity credential with numerous organizations that had no involvement with the original issuance of the credential. The challenge is to import a similar approach to the digital online environment, i.e., to create secure, reliable and trustworthy digital identity credentials which can be used across different ecosystems and entities. This allows individuals or businesses to use the same identity credential to sign on to the networks of more than one business in order to conduct transactions.

The basic building block of identity federation is the trusted federation relationship established between an identity provider and service providers. An identity provider holds digital identities of registered users for the purpose of provisioning these identities, or portions of them, to a party willing to rely on this information, called the relying party. A service provider, which is the relying party allows its users to

---


7 Common examples of existing technology platforms are OpenID Connect, Shibboleth, WSFederation and OpenAM.

authenticate themselves at a federated identity provider and then relies on the assertion issued by the identity provider upon successful authentication.

### 3.3 SeaSWIM as a Provider of Federated Identity Management

The objective of the identity management service under SeaSWIM is to manage an identity registry for maritime stakeholders to provide access to, and consumption of, STM services. SeaSWIM follows a federated identity model and acts as the identity provider. As envisaged under STM, a maritime stakeholder can take the position of a subject or a relying party depending on whether it is requesting for a service or providing a service. The relying parties as service providers rely on the identification process performed and identity information provided by SeaSWIM.

An oversimplified summary of the process of federated identity management as envisaged under SeaSWIM is described below to put the legal issues in perspective. SeaSWIM as the ‘identity provider’ identifies the service seeking maritime stakeholder as the ‘subject’ and issues a digital identity credential to facilitate authentication of the subject. Later, when the subject wants a service from another maritime stakeholder, i.e., the ‘relying party’ via a remote access, it uses that identity credential to assert its identity to that service provider as evidence of its right to obtain what it wants. Before the relying party grants the subject’s request, it will want to authenticate the identity of the person claiming to be the subject. In some cases, the relying party will also want to obtain an identity assertion about the subject before allowing access to its system or enter into a proposed business transaction. To provide the required identity information and facilitate the authentication process, SeaSWIM will then be asked to make an identity assertion about the subject that contains the requested information. At the time of the transaction, SeaSWIM first authenticates the subject and then the identity assertion is communicated to the relying party. The relying party validates the identity assertion to ensure that it is authentic and not revoked, and then relies on it to obtain the necessary information in order to grant access to a network or proceed with the proposed transaction.

#### 3.3.1 A Maritime Stakeholder as the Subject

Generally speaking, a maritime stakeholder as the subject may be a human being, business entity, device, software application, or digital object being identified in a particular credential and that can be authenticated and vouched for by SeaSWIM. In legal parlance, the person or thing being identified is often referred to as an “entity.” In the case where the subject is not a legal person such as device, software application, or digital object, then a legal person such as a human being or a legal entity such as corporation must take responsibility for it, in which case it is often referred to as the “responsible person.”

The conduct of the maritime stakeholder as the subject can directly affect the validity of the identification and authentication processes. Thus, to ensure accurate and reliable processes, the subject has certain basic duties. The subject should provide

---

9 See Document No. MONALISA 2.0_D2.3.1-6-SSWIM, circulated internally through Projectplace.
accurate information to the SeaSWIM identity registry during the identification process by not omitting or misrepresenting any material fact, or otherwise engage in any identity fraud. The subject should assume responsibility for transactions where the credential was used by the subject, or by a third party with authorization of the subject. The subject should use the issued credential only for the purposes of transactions for which it was intended and should also take reasonable steps to prevent the unauthorized use of the credential issued or registered to the subject. In the event that the credential is lost or compromised, used without authorization, and/or should otherwise be revoked, the subject should immediately notify SeaSWIM and relying parties about such incident. Such notification will allow SeaSWIM to revoke or invalidate the credential/token and otherwise take steps to prevent someone from successfully using it to commit identity fraud.

3.3.2 SeaSWIM as the Identity Provider

SeaSWIM, as the identity provider, has the overall responsibility for the entire process of registering an applicant for an identity credential and for establishing the applicant’s true identity through the identity proofing process, which involves the collection of identifying information and verification of identity against independent and authoritative sources. The strength of the identity proofing process, and hence the trustworthiness of the resulting identification will depend on four important factors. First, what identification documents or information is sought from the applicant for the verification; second, who is performing the collection and verification on behalf of SeaSWIM; third, how the process of verifying the information and the authenticity of the identification documents is achieved; and finally ensuring that the applicant’s identification documents or information came from a trusted source.

SeaSWIM has the primary responsibility for the validity and integrity of the identification process and the resulting identity credential, the accuracy of the identity assertions, and the privacy and security of the subject’s personal information in its control. As a part of the responsibility, SeaSWIM should be able to properly and accurately identify subjects in accordance with specified procedures, including - collection of data that will allow it to perform the requisite proofing necessary to issue the credential; ensure that all identity assertions are accurately based on current valid information that is properly authenticated; and use reasonable procedures to detect omissions or misrepresentations by the subject.

Moreover, SeaSWIM should properly issue each credential; properly perform all identity assertion and authentication processes; ensure that the transfer of the credential and identity assertion is secure to prevent interception or compromise by unauthorized persons, and to protect credential integrity; provide to the subject a capability to revoke a credential to limit identity theft opportunities in the event that the subject’s token is compromised or the subject no longer wants to participate.

SeaSWIM should also provide to all relying parties a capability to validate each credential so the relying party can determine whether the credential is still valid and can be relied upon. If SeaSWIM retains and holds a subject’s credential, it should take reasonable steps to prevent the unauthorized access or use of the credential and
assume responsibility for third party unauthorized use of such credential. SeaSWIM should protect the privacy and security of subject’s personal information; provide subjects with appropriate notice, choice, access, and control of their personal data; and comply with disclosed policies, practices and procedures for the identification and authentication processes so that relying parties can identify assurance levels and determine the level of trust they should have in the resulting authentication and identity assertions.

3.3.3 A Maritime Stakeholder as the Relying Party

A maritime stakeholder as a relying party may be an individual, business, organization or service that relies on the identity claims made by SeaSWIM about a subject. Such reliance may involve granting access to a service or database, or proceeding with a transaction. The relying party should ensure that its reliance on the identification and authentication processes is reasonable under the circumstances and that its use of the subject’s personal information is appropriate. Before relying on the credential of the subject, the relying party should properly authenticate each credential and identity assertions of the subject and validate the credential with SeaSWIM. The relying party should follow appropriate processes prior to relying on a credential and other information received about the subject, and determine whether there are reasonable measures to reduce risk of inaccurate and fraudulent information. The relying party should also protect the privacy and security of the Subject’s personal data, and restrict its use of that data in accordance with its disclosed privacy policy, practices and procedures, the requirements of contractual arrangements between the parties, and applicable law.

3.4 The Main Challenges for Participants in SeaSWIM

The successful implementation of SeaSWIM will require overcoming three types of challenges. The first type is organizational and is attributed to risks associated with technology, process, and procedure. The second type is economic, and involves dealing with matters, such as cost of deployment, coordination, and use of SeaSWIM by the various maritime and transport stakeholders. The third type is legal which constitutes of potential liability risk of the participants, the privacy and security of the subject’s identity information, and the mutual concerns of all participants in the ecosystem that everyone performs their obligations properly. The legal risks to each participant in the ecosystem, and the significance of the risks will, of course, vary by the role such participant is fulfilling at any particular point in time.

In the following paragraphs, the organizational challenges are discussed briefly but no further discussion on the economic challenges is made as it is beyond the scope of this work. The legal challenges are then discussed in contextual detail to set the pace for section 4.

3.4.1 Organizational Challenges

SeaSWIM relies on a variety of different processes and procedures, some of which are technology-based, and others consist of a series of steps performed by a person. It is the task of the technology team of the MONALISA Project to ensure that the
technologies employed for SeaSWIM functions properly and/or achieve the intended result. Even if a robust technological system is in place, the risk to the participants may arise from the possibility that one or more of the processes implemented for SeaSWIM are not properly designed to yield a secure and trustworthy result. Such processes and procedures might include, for example, the process for identity proofing an individual subject, which might specify which identity documents must be reviewed in person, or how identity might be verified online. Other processes relate to authentication, verification of credentials, revocation of credentials, etc. It is critical to the operation of SeaSWIM that the processes utilized are appropriately designed to achieve the intended result, that they function properly and securely, and that they provide reliable and secure results.

Even if the technologies and processes used for SeaSWIM are properly designed to yield a secure and trustworthy result, they will be of little value if they are not correctly implemented or properly followed by the participants. In fact, mere concern about the performance of a participant may lead to a lack of trust, which may prove fatal to the overall ecosystem. One major risk for all participants in SeaSWIM is the risk that one of the other participants, on whose performance they rely, will not perform their obligations as required for the role in which they are acting. Only when this risk is reduced to an acceptable level will parties participate in SeaSWIM. To mitigate performance risk, it is necessary to clearly define the performance obligations of each role by utilizing a combination of statutory, contractual, and/or technological mechanisms. This will provide a certain degree of assurance that the participants in each role will perform their obligations by conducting performance audits where appropriate, and providing a remedy if someone does not comply.

The key component of SeaSWIM lies in the reliability of the identification of the subjects and also the ability to reliably authenticate identity. While the required identification attributes will vary depending on the circumstances, the reliability of that identification is critical for all parties. Failure of the identification process presents a major risk. Once a subject has been properly identified, participants in an identity ecosystem must also address the risk that the authentication process can be compromised.

The risk of an improper identification can arise in several ways. First, there is the risk that the underlying identity documents and third party sources used by the identity provider are incorrect or fraudulent. Second, there is the possibility that SeaSWIM or its subcontractor will not do the job properly when performing the identity proofing process. And third, there is the possibility that the data collected during the identity proofing process will not be properly transmitted or transcribed when it is embodied in the resulting identity credential. For subjects the identification risk is a combination of business, identity theft and privacy concerns. For SeaSWIM, the identification risk relates to the possibility that a flawed identification process may lead to a faulty identification resulting in harm to the relying party and/or the subject, with the consequence that SeaSWIM may be liable for the damages incurred. For relying parties, identification risk is both a liability concern focused on the losses it will suffer if it relies on an inappropriate authentication or identity assertion, as well as a legal compliance obligation. From a liability perspective, the relying party needs
the assurance or trust necessary to enter into a particular online transaction, as well as some level of confidence that it will be able to prove the identity of the other party in a court of law, if that becomes necessary. At the same time, however, laws and regulations increasingly impose on businesses a duty to identify and authenticate the persons with whom they deal remotely. Thus, for many relying parties the use of identity management has become a legal obligation.

Even if the identification risk has been properly addressed, the parties must also address the possibility that a valid identity will not be properly authenticated. This can involve either the possibility that the identity of a legitimate subject cannot be properly authenticated, or alternatively, that a subject’s identity can be falsely authenticated as applying to someone or something else. Authentication risk can be affected by technology risk or performance risk. It can also arise independently, such as where a third party is able to unlawfully compromise the authentication system. At the end of the day, however, authentication risk refers to the risk that authenticating a claimed identity will yield an incorrect result.

3.4.2 Legal Challenges

1. Privacy
The federated identity management process involves the collection of personal information about a subject by SeaSWIM and the disclosure of that information to a relying party. Thus, the foundational issue in approaching SeaSWIM is personal information – how it is collected, stored, shared, and used. Moreover, by its nature, SeaSWIM presents a new challenge to privacy because transfers of personal information routinely occur between organizations as well as between the individual and an organization, and may frequently cross industry sectors and jurisdictional boundaries in the process.¹⁰

The risk to privacy is based on the possibility that personal data collected as part of the identity proofing process will be misused by SeaSWIM or a subsequent relying party because they have access to such data, or that the personal information will be compromised or otherwise improperly disclosed. Privacy risk in many respects is a function of risks related to technology and performance. However, it may go beyond those two risks in that the use or protection of the personal information in certain ways may not be required by the applicable system rules, or, in addition to the rules, may be regulated by existing law.

The privacy risk for subjects focuses on the protection and use of their personal information by SeaSWIM, relying parties, and other third parties, the resulting possibility of inappropriate use, disclosure, and compromise, and the harms that may result, such as identity theft, unauthorized account access, embarrassment, etc. And this risk relates not only to the information provided by the subjects, but also information about the subjects collected from third parties, as well as metadata and transaction data about subjects generated as a result of their online activities.

For SeaSWIM and relying parties, the privacy risk involves navigating the challenges of compliance obligations and restrictions that might inhibit their ability to achieve their goals. Laws and regulations may regulate or restrict their collection and use of personal information, as well as impose a variety of obligations to protect the information. In addition, restrictions on cross-border transfers and other forms of use or sharing of such information may have an impact. Failure to address these obligations may result in penalties and fines, as well as potential liability for any harm suffered by the subjects themselves.

2. Liability

In simple words, liability is the penalty when a person does something wrong. The issue of liability came up several times during the MONALISA Project meetings and received a lot of attention from the discussants. Liability risk emerged as a primary concern for the discussants that aligned their position with SeaSWIM as the identity provider, and maritime stakeholders as subjects and relying parties. Potential subjects expressed fear that obtaining an identity credential may simply lead to liability for its improper use in the event they are unable to adequately secure it. Thus, the primary concern of all participants in SeaSWIM is to determine who will bear the risks associated with the problems that may arise and their consequences. This concern may be easily addressed if all participants in SeaSWIM address the risk that they will be held liable and for which they are deemed legally responsible.

Things that can go wrong in SeaSWIM may result from faulty identification, faulty authentication, inadequate security for or misuse of personal data, or failure to follow appropriate procedures. They can lead to two primary harms. First, a relying party and/or a subject may suffer damage when the relying party acts (a) in reliance on a false identity credential or identity assertion that it thought was valid (e.g., by granting access to, or entering into an unauthorized transaction with, an imposter), or (b) fails to act in reliance on a valid identity credential that it mistakenly believes to be false. Second, a subject may suffer damage when (a) his or her personal information is misused or compromised by SeaSWIM or a relying party or other third party to whom it has been disclosed, or (b) when the subject is improperly denied access or the ability to conduct a transaction he is otherwise entitled to do.

If it is assumed for the sake of this discussion that an identity assertion is inaccurate and a relying party and/or subject suffers a loss, then the outcome will depend on which kind of law is applicable. If negligence law is applied, then liability depends on fault of SeaSWIM which is relative to the standard that applies by law and depends on nature of loss, the jurisdiction involved, etc. On the contrary, if warranty law is applied, then liability does not depend on fault of SeaSWIM but depends on nature of warranty that applies by contract or by law. If SeaSWIM-specific law is applied through the terms of Rulebook as described in the next section, the contractual terms

11 It is be noted in this context that liability risk refers not only to the possibility that a participant may be required to pay damages to another participant within SeaSWIM. It also includes the possibility that a participant may have a responsibility for damage suffered by third parties outside of SeaSWIM who might not be constrained by the rules of the legal framework governing SeaSWIM.
may supersede negligence rules, warranty rules, etc. depending on the stipulation of the terms.

Numerous statutory, common law, and contract theories have been advanced to identify, define, and clarify the source and scope of the potential liabilities of each of the participants in an identity ecosystem. Yet, in many respects, federated identity management is a business model for which the law has not yet had time to adapt. Various liability models have been specifically designed over the years for an industry or a sector using federated identity management. As exemplified above, the warranty model focus on stated or implied guarantees while the tort model focus on standards of conduct and negligence. It is interesting to note that liability scheme for credit cards, for obvious reasons, have been created with no liability for the subjects as other parties bear the risk. In theory, the contractual model presents an opportunity for parties to negotiate the risk allocation. The strict liability approach, on the other hand, may make one party liable regardless of fault.

The question that still remains pertinent is - what is the liability regime for identity management systems and for trust service providers? When a cross-border liability issues arise, the parties can be confronted with uncertain legal rules or case law. Thus, a key aspect of the liability risk is the legal uncertainty regarding the responsibility that attaches to any given action or failure to act by a participant in an identity ecosystem. This uncertainty only enhances the nature of the liability risk and in many cases has dissuaded companies from participating in an identity ecosystem. It must be recognised that a one-size fits all approach cannot be adopted when discussing a potential liability model for SeaSWIM as liability is a zero-sum game and also a matter of policy choice. A detailed discussion on liability issues is necessary during the next phase of the MONALISA Project to decide which liability model SeaSWIM has to follow to service the maritime industry.

3. Data Security
Data security includes not only the security necessary to protect the personal information collected by SeaSWIM and communicated to relying parties, but also the security of the other data and corresponding processes necessary to create secure identity credentials, communicate accurate identity assertions, and verify the status of identity credentials. Thus, data security risk refers to the risk that an unauthorized party obtains access to personal data or is able to otherwise compromise the overall functioning of the SeaSWIM ecosystem.

Currently, there exist no international standards or regulations that set any legally mandated security obligations for identity management systems or for trust service providers. Nevertheless, SeaSWIM has to address data security to be considered as a trustworthy service by the participants.

4. Enforcement
If one participant in SeaSWIM fails to perform as required, the other participants must consider their ability to (i) identify the fact of such failure of performance, (ii) stop and/or remedy such failure, and (iii) obtain redress and/or compensation for any losses suffered as a result. Concerns regarding each of these three elements are the focus of enforceability risk. This risk applies not only when something goes wrong
and someone seeks compensation, but also in situations where a problem has not yet surfaced, but a failure of performance on the part of one or more participants puts the system at risk. For example, if SeaSWIM fails to properly perform the identity proofing process, even though it has not yet resulted in any inaccurate credentials, is a concern for other participants. In such case, the risk of enforcement refers both to the ability to detect that problem, as well as the ability to require the participant to remedy its performance or withdraw from the system.

5. Compliance with Regulations and Standards
Participation in SeaSWIM may raise various issues relating to compliance with standards and regulations. For example, the manner of collection, use, and storage of personal data by the identity provider, and the subsequent receipt and use of that information by a relying party, must comply with applicable privacy laws. Acting contrary to the requirements of those laws poses a compliance risk to the participant.

4 Legal Framework to Meet the Challenges and the SeaSWIM Rulebook
The goal of SeaSWIM is to provide identity assertions that are sufficiently reliable for the intended purpose, and to do so in a manner such that all of the relevant maritime stakeholders are willing to participate and to rely on the results. Achieving this goal requires building a trust framework for the SeaSWIM ecosystem. Generally speaking, a pre-negotiated trust framework allows a trust relationship to be established among a group of parties that have established a set of rules by which each of the parties agrees to abide. Such rules provide a basis that allows the parties to trust each other. The agreement to abide by the rules occurs before participation in the trust framework by the parties. Such a pre-negotiated trust framework can provide a baseline for security that those parties who agree to abide by the framework can implement.

The trust framework specifically designed for SeaSWIM may be named as “SeaSWIM Rulebook” (Rulebook), which will consist of a set of documents. These documents specifically drafted for SeaSWIM will attribute the operational requirements and governing legal rules of the identity system. Some of the common provisions that has to be addressed in the Rulebook are - identity life cycle management requirements; user credential life cycle management; attribute life cycle management requirements; federation services, identity attribute repositories; authentication of federation participants; claim and token profiles; session lifecycle requirements; facility, management and operational controls; technical security controls; accreditation and certification rules; general provisions of the common operating rules; and warranty, indemnification, and liability.

The major benefit of creating a Rulebook is that it removes the requirement for the maritime stakeholders participating in SeaSWIM to negotiate bilateral legal agreements with each other. The Rulebook as a multilateral contract will bind each participant to every other participants in relation to their use of SeaSWIM services.
The purpose of this contract will be to ensure that every user agrees to be governed by a common set of rules enshrining the key elements of the SeaSWIM service.

The Rulebook will address both the operational requirements and the legal rules necessary to make SeaSWIM a trustworthy identity system. The operational requirements will include technical and functional specifications, processes, standards, policies and rules developed to ensure the proper operation of the system and to provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes. The legal rules that will govern SeaSWIM and make the operational requirements legally binding on and enforceable against the participating maritime stakeholders, regulate the content of the operational requirements, and define and govern the legal rights, responsibilities, and liabilities of the participants of SeaSWIM.

The operational requirements of the Rulebook will likely consist of several different components addressing a variety of key operational and policy issues, such as identity proofing, authentication, credential management, privacy, security and assessment/audit. Each component of the operational requirements will establish the technical specifications, processes, standards, policies, rules and performance requirements necessary to address one or more issues of importance to the operation of SeaSWIM. Taken together they will form the operational requirements necessary to ensure that SeaSWIM operates properly and in a manner that all parties trust will be appropriate for the task.

The legal rules will complete the Rulebook by rendering the various components of the operational requirements binding and enforceable. The legal rules shall consist of both existing statutes and regulations, and agreements between or among the participants. They will affect the Rulebook in three ways. First, the legal rules will make the specifications, standards, and rules comprising the various components of operational requirements legally binding on and enforceable against each of the participants. Second, the legal rules will define the legal rights and responsibilities of the parties, clarify the legal risks parties assume by being a party to the Rulebook, such as warranties, liability for losses, risks to their personal data; and provide remedies in the event of disputes among the parties, including methods of dispute resolution, enforcement mechanisms, termination rights, and measures of damages, penalties and other forms of liability. Finally, in some cases, they also regulate the content of the operational requirements.

The legal rules may be set out in numerous contracts at varying management and execution layers, depending on the governance structure used. In many cases they operate as gap-fillers with respect to issues not addressed by the existing law. Where existing laws address issues in a permissive rather than mandatory manner, the legal rules may also express the choices of the parties among legally permissible alternatives. And in both cases they can have the effect of providing the legal certainty and predictability necessary to encourage participation.

SeaSWIM also aspires to establish itself as a trust framework provider for the maritime transport industry. Such a scenario will be possible if a considerable portion of the maritime transport industry uses the SeaSWIM Rulebook as a legally binding
trust framework. In that case SeaSWIM will provide the Rulebook and also the governance infrastructure needed to support it. Examples of such trust framework providers include IdenTrust Inc. for the financial sector,\(^{12}\) the SAFE-BioPharma Association for the pharmaceutical sector,\(^{13}\) and CertiPath for the aerospace sector.\(^{14}\)

Various models have developed over the past decade in the area of identity federation, such as the centralized model, the consortium model, the collaborative or hub model, and the third-party assurance model (3PAM).\(^{15}\) Each of these models relies on the fact that all parties agree to abide by the same set of rules and governance structures applicable to the identity federation. Thus, the technical interaction between two or more entities is based on a standard set of rules by which the participating entities have all agreed to operate. However, these rules and governance structures can take on a number of different forms depending on the model chosen. A detailed analysis of these various models will be imperative when issues related to governance of SeaSWIM are discussed in the next phase of the MONALISA Project.

5 Recent Legislative Efforts on Identity Management and Trust Services

Several national and regional initiatives in the field of identity management and/or trust services are actively underway. National and regional legislation governing identity management and/or trust services that has recently been adopted or proposed, including the EU Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation),\(^{16}\) the Belgian law on the eID card and the draft Belgian law on trust services,\(^{17}\) the French legislation on electronic signatures,\(^{18}\) as well as on electronic registered mail,\(^{19}\) the Italian regulations on the posta elettronica Certificata,\(^{20}\) and the Electronic Identity Management Act of Virginia from the United States of America (US).\(^{21}\) Also, there are

---

\(^{12}\) See https://www.identrust.com/

\(^{13}\) See http://www.safe-biopharma.org/

\(^{14}\) See https://www.certipath.com/

\(^{15}\) For a detailed discussion, see Jeff Nigriny and Randy V. Sabett, The Third-Party Assurance Model: A Legal Framework For Federated Identity Management, 50 Jurimetrics 509 2009-2010.


\(^{17}\) Available online at www.lachambre.be/FLWB/PDF/53/2745/53K2745006.pdf

\(^{18}\) Available online at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00000003990095&dateTexte=&categorieLien=id

\(^{19}\) Available online at http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023513151

\(^{20}\) Available online at http://qualitapa.gov.it/relazioni-con-i-cittadini/open-government/strumenti-dellapa-digitale/la-posta-elettronica-certificata/

\(^{21}\) The Act took effect on 1 July 2015, available online at https://leg1.state.va.us/cgibin/legp504.exe?151+ful+CHAP0483
several public and private sector national and international initiatives that are currently being taken in various parts of the world.\footnote{22}

5.1 EU eIDAS Regulation

The European Union adopted the eIDAS Regulation on 23 July 2014 to replace the current legislation, which is based on the 1999 Directive on Electronic Signatures.\footnote{23} This legislation provides a legal framework for secure electronic interactions across the EU between businesses, citizens and public authorities. It covers electronic identification and trust services, which are paid-for electronic transaction services. The eIDAS Regulation focuses on identity systems that issue credentials for use in online transactions with public sector bodies. Its key goal is mutual recognition of such credentials in cross-border public sector transactions – i.e., to enable individuals who have an identity credential issued in one EU member state to use that same credential to access online public services in another member state. The eIDAS Regulation does not require that identity systems be government-operated.

Accordingly, credentials issued by a EU member state, under a mandate from the member state, or independently of the member state (which can be SeaSWIM for certain services) but recognized by the member state, are all acceptable. However, they must also comply with the applicable technical specifications, standards, and procedures regarding assurance levels set out in the implementing act currently being developed. The Regulation holds member states and identity providers liable for damage caused by a negligent failure to comply with its obligations under the Regulation.

In relation to trust services, the Regulation defines them as paid-for services that include the creation, verification, validation, handling and preservation of electronic signatures; electronic seals; electronic time stamps; electronic registered delivery services; and website authentication. Trust service providers based in the EU are called ‘qualified’ if they meet the regulation’s applicable requirements. They are legally entitled to provide qualified trust services (e.g. qualified electronic signatures, seals or certificates) in all EU countries. Trust services offered by service providers from non-EU countries can be considered legally equivalent to qualified ones, but only after an agreement between the EU and the non-EU country or international

\footnote{22} The public sector national and international initiatives includes the United States National Strategy for Trusted Identities in Cyberspace (NSTIC), and its Identity Ecosystem Steering Group, see www.ideosystem.org/; two OECD studies on Digital Identity Management, see supra note 3, the European Union STORK projects, see https://www.eid-stork.eu/; and the work of several groups including the ITU, the Digital ID and Authentication Council of Canada (DIACC), see www.diacc.ca/; and the United Kingdom of Great Britain and Northern Ireland Government Digital Service, see http://digital.cabinetoffice.gov.uk/category/id-assurance/. The private sector national and international initiatives, including the ABA Business Law Section’s Identity Management Legal Task Force, see http://apps.americanbar.org/dch/committee.cfm?com=CL320041; the Kantara Initiative, see http://kantarainitiative.org/; the Fast Identity Online (FIDO) Alliance, see https://fidoalliance.org; the Secure Identity Alliance, see https://www.secureidentityalliance.org/; the Open Identity Exchange, see http://openidentityexchange.org/; the Transglobal Secure Collaboration Program (TSCP), see www.tscp.org/; and the Open Group: Identity Management Forum, see www.opengroup.org/.

organisation. Under the Regulation, qualified trust service providers have to provide the supervisory authority with a conformity report before they can provide trust services. After the initial report, qualified trust service providers have to be audited at least every 24 months. The supervisory authority can also impose ad hoc audits. The European Commission is authorised to set standards as to how trust service providers will be audited.

From the above discussion, it is clear that certain activities of SeaSWIM will fall under the purview of this Regulation, which will soon have the force of law in all member states. A detailed legal examination will therefore be necessary once the implementing act under the Regulation is available and the framework of subjects and relying parties are decided as part of the continuing work of the MONALISA Project.

5.2 The Electronic Identity Management Act of Virginia

Another recent legislative initiative, after the EU Regulation was adopted, is the state of Virginia’s Electronic Identity Management Act. It is the first state in the US to adopt rules on electronic identity management by enacting its own legislation, which took effect on 1 July 2015. This legislation adopts a very different approach to that of the EU Regulation. It provides for the creation of Virginia Identity Management Standards Council, which is tasked with developing Identity Management Standards. Unlike the EU approach, the Virginia statute grants immunity from civil liability to trust framework operators and identity providers that comply with the requirements of those Identity Management Standards. It also provides for the regulation of identity management trust marks designed to evidence trustworthy systems.24

5.3 Initiative at UNCITRAL Working Group IV on Electronic Commerce

The legislative initiatives in the EU and the US discussed above represent very divergent approaches. Yet there is a general recognition that identity management is a global issue, and that interoperability across national boundaries is critical. Accordingly, in the spring of 2015, the American Bar Association Identity Management Legal Task Force, and the countries of Austria, Belgium, France, Italy, and Poland with support from the EU Commission, all submitted proposals to UNCITRAL recommending that it undertake a project to develop “a basic legal framework covering identity management transactions, including appropriate provisions designed to facilitate international cross-border interoperability.”25 At its July 2015 meeting UNCITRAL agreed to move forward with such a project.


6 Concluding Remarks

This report has highlighted the various legal challenges that have to be met to implement STM services through SeaSWIM. The report has explained that creation of a Rulebook can facilitate the launch and use of the SeaSWIM system. The exact stipulation of the terms in the Rulebook is dependent on the technical offerings of the STM services that will use SeaSWIM. As discussed in section 3 of this report, the relationship between the operational requirements and legal rules of the Rulebook is similar to the relationship between a contract and several sets of technical specifications attached to the contract as exhibits. Execution of the contract is what creates a legally binding relationship between the parties; the specifications in the exhibits detail the parties’ expectations of how the contract will be performed. Adopting such an approach will enable SeaSWIM to accept any internationally agreed standard by simply incorporating it under the operational requirements of the Rulebook. For example, the International Hydrographic Organization’s S-100 standard can be adopted as the baseline data structure for SeaSWIM through such incorporation. It is submitted that creating a Rulebook to implement STM in general and SeaSWIM in particular will cause the least disruption to the established framework of maritime and commercial laws that govern the navigational and commercial aspects of shipping.

Although the creation of a Rulebook may solve some of the major legal hurdles, the implementation of SVM, DVM, FM and PCDM may require some fine-tuning of trade practices and legislative dictates to embrace modernization. For example, the enhanced information sharing between various stakeholders in STM may allow ports to use such information to organise the incoming traffic in accordance with availability of berths, stevedores, pilots, etc. However, in certain shipping trades the provisions of existing legislation may not allow ports to assign time slots to ships before they arrive within the geographical boundaries of the port. A revision of such port related laws across jurisdictions and relevant standard form contracts will therefore be necessary to allow ports to assign time slots to ships situated even outside the port’s geographical limits. It is envisaged that such revisions will not be difficult to pursue as trade practices evolve with adoption of new technology, and legislators generally respond to market forces. Also, support for such revision may be drawn from the liner shipping industry where ports assign time slots to ships which sail based on a published timetable. It is submitted in the context of the above discussion that when various STM services are made operational, many such legal impediments will be addressed through spontaneous legislative and contractual fine-tuning of relevant instruments.

Since liability and privacy emerged as primary legal concerns during the discussions at MONALISA 2.0 Project meetings, this report has discussed in detail the legal issues relating to the potential liability risk of the participants in SeaSWIM, the privacy and security of a subject’s identity information, and the mutual concerns of all participants in the SeaSWIM ecosystem that everyone performs their obligations properly. It is submitted that the Rulebook will provide clarity, and allow all stakeholders to have certainty as to the rights and obligations of all of the entities
involved in the federation. However, in the next phase of the MONALISA Project it will be critical to determine the acceptable liability model(s) for SeaSWIM and the related STM services. Using this report as the foundation, future studies has to be directed to identify and evaluate existing liability models to find an appropriate liability framework that will be acceptable to the various participants of SeaSWIM. Since SeaSWIM also aspires to establish itself as a trust framework provider for the maritime transport industry, a detailed analysis of various identity federation models is necessary to determine what will be suitable for, and acceptable by the industry.

Identity management law is admittedly still in a state of infancy given that legislative efforts commenced only recently in Europe and in the US. The current spate of legislative activity indicates that identity management technology has come of age and businesses are now keen to harness the benefits. The conceptualisation of SeaSWIM is timely and has the potential to push the conservative maritime industry to embrace modern information and communication technology. SeaSWIM may also play a pioneering role in shaping the identity management legal framework for the maritime transport sector. Having said that, the proponents of SeaSWIM have to be observant of the legislative efforts that are currently underway at the national, regional and international levels. At any rate, a well-informed, current and robust legal framework is crucial in making the MONALISA Project a success.
39 partners from 10 countries
taking maritime transport into the digital age

By designing and demonstrating innovative use of ICT solutions
MONALISA 2.0 will provide the route to improved

SAFEY - ENVIRONMENT - EFFICIENCY

Swedish Maritime Administration • LFV • SSPA • Viktoria Swedish ICT • Transas • Carmenta •
Chalmers University of Technology • World Maritime University • The Swedish Meteorological
and Hydrological Institute • Danish Maritime Authority • Danish Meteorological Institute •
GateHouse • Navicon • Novia University of Applied Sciences • DLR • Fraunhofer • Jeppesen
• Rheinmetall • Carnival Corp. • Italian Ministry of Transport • RINA Services • D’Appolonia •
Port of Livorno • IB SRL • Martec SPA • Ergoproject • University of Genua • VEMARS •
SASEMAR • Ferri Industries • Valencia Port Authority • Valencia Port Foundation • CIMNE •
Corporacion Maritima • Technical University of Madrid • University of Catalonia • Technical
University of Athens • MARSEC-XL • Norwegian Coastal Administration

www.monalisaproject.eu

Co-financed by the European Union
Trans-European Transport Network (TEN-T)