A LINDDUN-Based Privacy Threat Modelling for National Identification Systems

Livinus Obiora Nweke[1,2], Mohamed Abomhara[1], Sule Yildirim Yayilgan[1], Debora Comparin[3], Olivier Heurtier[3], and Calum Bunney[3]
[1]*Department of Information Security and Communication Technology*
Norwegian University of Science and Technology (NTNU), Gjøvik, Norway
[2]*Noroff Accelerate*, Oslo, Norway
[3]*OSIA Working Group*, Paris, France
livinus.nweke@{ntnu.no, noroff.no}, mohamed.abomhara@ntnu.no, sule.yildirim@ntnu.no

***Abstract*—The international focus on attaining identity for all has fostered advances in technological developments that have given rise to changing demands on the architecture and deployment of national identification (NID) systems. In particular, national identity management solutions are now expected to respond to a fully modular architecture and to be flexible in the integration of the various building blocks, including the case where the building blocks are provided by different vendors. Another important demand is linked to the increasing concerns about privacy and the potential for unethical or harmful uses of personally identifiable information (PII). This has forced national identity management infrastructures to be compliant with relevant legislation, regulations as well as best practices. In this paper, we investigate how to integrate privacy principles and requirements into a fully modular national identity management architecture implementing a specific use case that deploys the OSIA standard for seamless integration of its building blocks. We employ the LINDDUN methodology to identify privacy threats to the selected use case, elicit mitigation strategies and suggest appropriate privacy enhancing solutions.**

***Index Terms*—National identification (NID) systems, OSIA initiative, Privacy threat modelling, LINDDUN methodology**

I. Introduction

The provision of legal identification has been recognised by the United Nations (UN) Sustainable Development Goals (SDG 16.9) as a global strategic goal [1]–[3]. As a result of this, the UN set target for SDG 16.9 is to "provide legal identity for all, including birth registration by the year 2030" [4]. The SDG 16.9 target has fostered advances in technological developments that have given rise to changing demands on the architecture and deployment of national identification (NID) systems. In particular, national identity management solutions are now expected to respond to a fully modular architecture and to be flexible in the integration of the various building blocks, including the case where the building blocks are provided by different vendors [5]. To answer this demand, in 2018 the not-for-profit Secure Identity Alliance (SIA) launched the Open Standard Identity APIs (OSIA) initiative [6], an interoperability framework as a public good. OSIA aims at standardising the building blocks for national identity management infrastructures and building open standard interfaces to seamlessly connect them [6].

Another important demand is linked to the increasing concerns about privacy and the potential for unethical or harmful uses of personally identifiable information (PII) [7]. This has forced national identity management infrastructures to be compliant with relevant legislation, regulations as well as international best practices. Several regulations such as the General Data Protection Regulation (GDPR) require the implementation of technical and organisational measures to protect PII that may be collected, processed, stored and shared in any system that handles PII, including NID systems [8]–[10]. The implementation of these measures require the identification of the possible privacy threats the system may be expose to, an understanding of the different mitigation strategies and also, a knowledge of the appropriate privacy enhancing solutions.

In this paper, we investigate how to integrate privacy principles and requirements into a fully modular national identity management architecture implementing a specific use case that deploys the OSIA standard for seamless integration of its building blocks. We employ the LINDDUN (Linkability, Identifiability, Non-repudiation, Detectability, Information Disclosure, Unawareness, Non-compliance) methodology [11] as the privacy threat modelling framework to identify privacy threats to the selected use case, elicit mitigation strategies, and suggest appropriate privacy enhancing solutions. We chose to base this case study analysis on a modular architecture implementing the OSIA standard due to the rapid adoption of the OSIA approach by several countries across the globe (7 to date). Moreover, OSIA specifications are quite mature with the release of v6.0.0 in December 2021 and the work is continuing through an open and collaborative consensus-driven process [6]. Our overall goal is to provide awareness to government policy makers implementing NID systems on the different types of privacy threats they need to consider to ensure that the system is in compliant with the relevant legislation and regulations such as the GDPR (**Note** - there are two levels of privacy threats that can be identified and resolved: one at the OSIA standard specification level and the other at the implementation level. This paper considered privacy threats at the implementation level).

The remaining part of this paper is structured as follows. Section II provides a discussion on NID systems and a

978-1-6654-7978-3/22/$31.00

description of the different building blocks for NID systems that have been standardised by the OSIA initiative. Section III discusses the approach we adopted for conducting the privacy threat modelling for the specific use case presented in this study. Section IV applies the LINDDUN methodology to the selected use case to identify privacy threats, elicit mitigation strategies and suggest appropriate privacy enhancing solutions. Section V concludes the paper and presents future work.

II. National Identification (NID) Systems

NID systems have been defined as foundational identification systems that facilitate the provision of national identifications - often a card or most recently a digital identity - and can also be used to issue other credentials [12]. They provide the basis for citizens to lay claim to their entitlements - right to name, recognition before the law, nationality, civic participation, and enhanced access to services [13]–[15]. These NID systems are usually operated by governments, alternatively by private companies, or by collaboration between the two.

The building blocks of NID systems include foundational identification systems, for example, civil registers and population registers, that are made for the purpose of providing identification to the general population for a wide range of services [16]. There are also functional identification systems created by governments to oversee identification, authentication, and authorization for specific use-cases or sectors, including taxation, voting, social services, social protection, travels, and more [16]. Both the foundational identification systems and functional identification systems have been standardised by the OSIA initiative. OSIA main goal is to provide a set of open standard interfaces (APIs) to connect the building blocks of identity management infrastructures [6]. Figure 1 depicts the building blocks of NID systems that have been standardised by OSIA and they are defined as follows [17]:

- The **Enrolment** (E) is defined as a system to register biographic and biometrics data of individuals and it is composed of two sub-components: the enrollment client to record the citizens' data and the enrollment server to receive and process the collected data.
- The **Population Registry** (PR) is defined as "an individual data system, that is, a mechanism of continuous recording, or of coordinated linkage, of selected information pertaining to each member of the resident population of a country in such a way to provide the possibility of determining up-to-date information concerning the size and characteristics of that population at selected intervals" [18].
- The **Unique Identity Number Generator** (UIN G) is defined as a system to generate and manage unique identifiers.
- The **Automated Biometrics Identification System** (ABIS) is defined as a system to detect the identity of an individual when it is unknown, or to verify the individual's identity when it is provided, through biometrics.
- The **Civil Registry** (CR) is defined as "the continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events pertaining to the population, as provided through decree or regulation is accordance with the legal requirement in each country" [19].
- The **Credential Management System** (CMS) is defined as a system to manage the production and issuance of credentials such as ID Cards, passports, driving licenses, digital ID, etc.
- The **Third Party Services** (TPS) is the component that interfaces with external systems such as identity providers (ID P) to offer services, which include identity verification and attributes verification for different use cases.
- The **Digital Credential Issuance and Distribution System** is the component in charge of the issuance and delivery of the digital credentials built from the identity databases under the control of the CMS.
- The **Identity Provider** (ID P) is defined as a trusted third-party entity that interfaces with TPS to manage a citizens' identity and associated identity attributes.

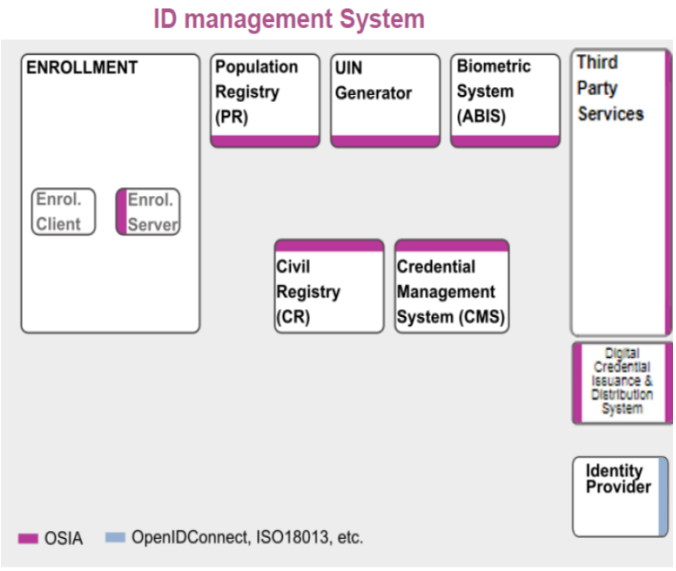

Fig. 1. Components identified as part of the identity ecosystem [17]

III. Methodology

In this study, we adopted a case study approach to explore privacy implications relating to the implementation of NID systems. This is because case study analysis provides concrete, contextual and in-depth knowledge about a real-world subject such as implementing a specific use case of NID systems that deploys the OSIA standard for seamless integration of its building blocks. Thus, the overall processes that was involved in this case study method is depicted in Figure 2.

The case study method involved a collaborative effort between researchers from the **M**ultidisciplinary **R**esearch group on **P**rivacy and data prot**E**c**T**ion (**MR PET**) at the Department

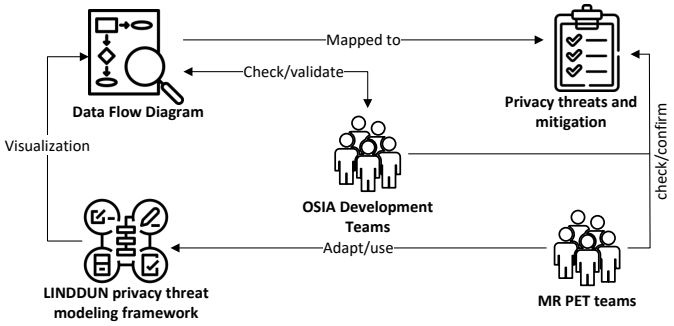

Fig. 2. Case study processes

of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU) and the OSIA development team. Following several interactions between researchers at MR PET and the OSIA development team, a data flow diagram (DFD) – discussed in Section IV – of a specific implementation that uses OSIA for interoperability was created by researchers at MR PET and validated by the OSIA development team. The DFD represents the overall system architecture and the flow of data within the system. It is an important step towards conducting privacy threat modelling for NID systems.

The next phase in the case study processes (Figure 2) was to apply a privacy framework to the developed and validated DFD. Here, the MR PET team adopted the LINDDUN privacy threat modelling framework [11] to identify privacy threats, suggest mitigation strategies and to translate the selected mitigation strategies to appropriate privacy enhancing solutions. LINDDUN takes a model-based approach such that it leverages a DFD as the representation of the system that requires analysis [11]. Using this DFD as the basis for the analysis, the MR PET team then systematically examined each component of the DFD, map privacy threats to the DFD elements and then identify possible threat scenarios. Considering that the LINDDUN methodology usually results in a large number of documented threats [11], the MR PET team had to interact with the OSIA development team to prioritised the identified privacy threats.

After the prioritisation of the identified privacy threats, the final phase of the case study processes is to suggest mitigation strategies and to translate the selected mitigation strategies into appropriate privacy enhancing solutions. In this phase, the MR PET team suggested mitigation strategies for the identified privacy threats and the appropriate privacy enhancing solutions based on the selected mitigation strategies. These were then validated by the OSIA development team.

IV. Privacy Threat Modelling

In this section, first, we present the credential issuance use case as a specific implementation of NID systems that implements OSIA standard for interoperability and then the use of LINDDUN privacy framework for conducting privacy threat modelling for the selected specific use case.

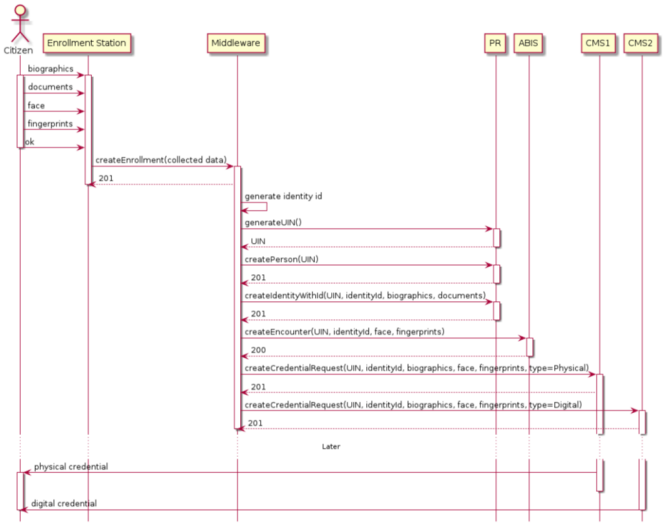

Fig. 3. Sequence diagram of credential issuance use case [17]

A. Credential Issuance Use Case

Credential issuance use case is a typical example of a specific implementation of NID systems that uses OSIA for interoperability to capture identity data, generate a UIN, process the identity data and issue a physical and digital credential. This use case also demonstrates what a middleware could do when connected to multiple OSIA compatible building blocks. The middleware in this example is acting as an enrolment server, scheduling all the processing when the data collection is finalized. The steps involved in this use case are depicted in Figure 3 and as follows [17]:

- The citizen interacts with the enrollment station (ES) to provide the biographic data, the supporting document images, a portrait and a set of fingerprints.
- When all the data is collected, the full data set is pushed to the middleware using the OSIA *createEnrollment* service.
- Backend processing includes interactions with the population registry to generate a UIN and insert the collected data; interaction with the ABIS to insert the face and fingerprints; and interactions with multiple Credential Management System to request the issuance of different types of credentials.

B. Privacy Threat Modelling Using LINDDUN

LINDDUN privacy threat modelling methodology supports the integration of privacy principles and requirements during the development life-cycle of a system and / or can be applied to an existing system [11]. It also facilitates the understanding of privacy principles, which are linked to the set of privacy threat categories embodied in the acronym LINDDUN (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance). This can then be used to define privacy requirements and to suggest

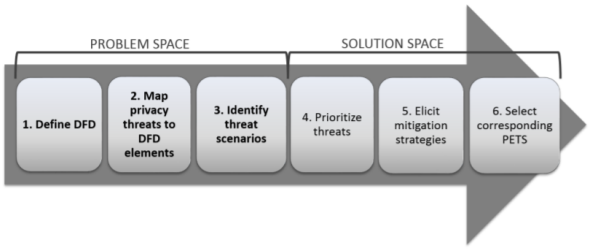

Fig. 4. LIDDUN methodology steps [11]

privacy enhancing solutions. LINDDUN is made up of six steps as depicted in Figure 4. Whilst the first three steps are concerned with the problem space and aim to identify the privacy threats in a system, the remaining three steps are more solution-oriented and aim to translate the identified privacy threats into appropriate privacy strategies and solutions that can mitigate the privacy threats [11].

Consequently, we utilise the six steps involved in LINDDUN methodology for conducting privacy threat modelling for the specific implementation of NID systems that uses OSIA for interoperability. Following these six steps, we define the DFD for the credential issuance use case as shown in Figure 5.

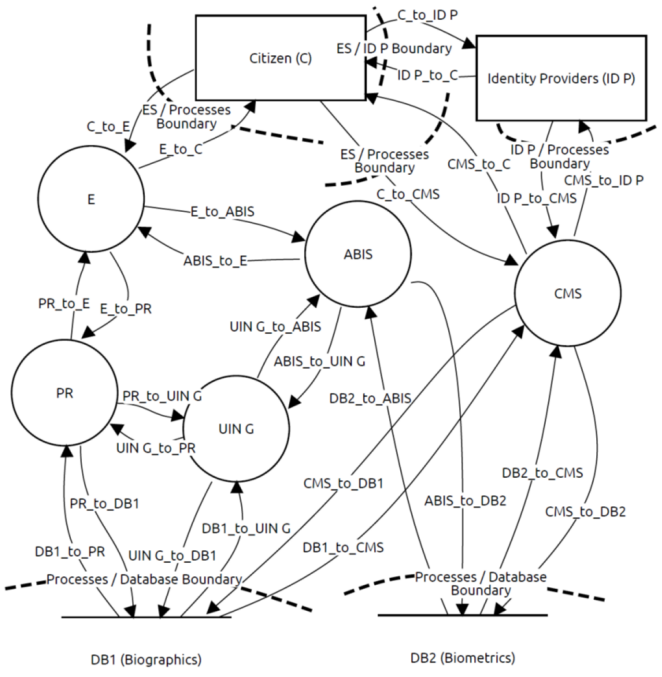

Fig. 5. Data Flow Diagram for Credential Issuance Use Case

The next step in the LINDDUN methodology is to map privacy threat to DFD elements. Based on the LINDDUN mapping template, Table I provides the full mapping for the credential issuance use case example. The "X" in the table indicates a potential privacy threat to the system under consideration, which requires further analysis.

TABLE I
PRIVACY THREATS MAPPING BASED ON LINDDUN MAPPING TEMPLATE

		LINDDUN Privacy Threats						
		L	I	N	D	D	U	N
	DFD elements (Threat targets)							
Entity	C	**X**	**X**				**X**	
	ID P							**X**
Process	E	**X**	**X**	**X**	**X**	**X**		**X**
	PR	**X**	**X**	**X**	**X**	**X**		**X**
	UIN G	**X**	**X**	**X**	**X**	**X**		**X**
	ABIS	**X**	**X**	**X**	**X**	**X**		**X**
	CMS	**X**	**X**	**X**	**X**	**X**		**X**
Data Store	DB1	**X**	**X**	**X**	**X**	**X**		**X**
	DB2	**X**	**X**	**X**	**X**	**X**		**X**
Data Flow	Biographic data stream	**X**	**X**	**X**	**X**	**X**		**X**
	Biometrics data stream	**X**	**X**	**X**	**X**	**X**		**X**
	DB1 data stream	**X**	**X**	**X**	**X**	**X**		**X**
	DB2 data stream	**X**	**X**	**X**	**X**	**X**		**X**

To identify privacy threat scenarios, each of the X's in the mapping table will be considered to ascertain whether they constitute a privacy threat to the system. This step also requires that several assumptions about the system under consideration are made. For the credential issuance use case in this study, we made the following assumptions:

- The processes are vulnerable to insider threats, while we suppose that the backend is sufficiently secured against outsider threats. And considering that process threats are usually similar across different processes, we combine all process threats and examine only one.
- The data stores are not deemed confidential because there is no access control mechanism in place.
- The data flows between processes and between processes and data stores are vulnerable to insider threats, while we suppose that the backend is sufficiently secured against outsider threats. And considering that data flow threats are usually similar across different data flows, we combine all data flow threats and examine only one.
- The data flows between an entity and a process are not deemed trusted because it involves interactions to and from a trusted process over insecure communication channel.
- There is no non-repudiation threats in the systems because the data flows, processes and data stores do not require plausible deniability.
- Detectability is not deemed a threat for the systems because the privacy threats are centred on the data itself and not on the detectability of it.
- Non-compliance is not unique to a single component in the system but relates to the system as a whole. Thus, there is no difference between the different DFD elements for this threat.

- Identifiability of entities is not deemed a threat because all entities have their own unique identifier.
- Linkability of entities is not deemed a threat, as entities have their own unique identifier.
- Linkability and identifiability are not deemed a threat to the data flows between entities processes.
- Linkability and identifiability do not apply to processes.
- Identifiability and linkability are relevant to the data stores.
- Spoofing is a threats to entities.
- Content unawareness only applies to the citizen.
- The data stores are properly secure and also, attacks such as side-channel attacks are not possible.
- Side channel attacks on data flows are not deemed as a threat because they are very unlikely to occur.
- The processes are not susceptible to corruption because they are implemented correctly and input is sufficiently validated, and memory access handled correctly.

Using the above assumptions, we identified the privacy threats to the credential issuance use case based on the LINDDUN threat trees [20]. The identified privacy threats, the threat scenarios, the primary threat actors and the consequences of the identified threats, are described in details in Table II. These first three steps we have described so far, conclude the problem space of the LINNDUN methodology.

The remaining three steps of the LINDDUN methodology are concerned with providing solutions to the privacy threats identified in the first three steps. The first step of these remaining three steps involves the prioritisation of the identified privacy threats. To prioritise the identified privacy threats, we consider the likelihood of the identified threats being realise and the impact that would have on the organisation. We made a differentiation between high, medium, and low risk and then organised the threats in accordance to their risk. Also, we provide a brief explanation on why the identified privacy threats are ordered in that particular manner.

Following our analysis of the credential issuance use case and the subsequent validation with the OSIA team, Information disclosure of data is considered the most important threat because it violates the citizen's privacy the most. Also, the identifiability of the stored biographic data and biometrics data have high priority because citizens should have confidence that only authorised person(s) can access their PII. Information disclosure of the transmitted data also constitutes a high risk as it violates the citizen's privacy. Lastly, spoofing is considered high priority because it can lead to information disclosure of stored data. Thus, the identified privacy threats for the credential issuance use case that we assigned high priority risk are itemized as follows:

- T04 - Information disclosure of citizens' data
- T03 - Identifying a citizen from biographic data and/or biometrics data
- T08 - Disclosure of a user of the systems' transmitted log-in credentials
- T09 - Disclosure of a user of the systems' transmitted session token
- T10 - Disclosure of transmitted citizens' PII
- T05 - Spoofing a user of the system by falsifying credentials
- T06 - Spoofing a user of the system by eavesdropping communication
- T07 - Spoofing a user of the system because of weak credential storage

Moreover, the identified privacy threats for the credential issuance use case, which are deemed medium risk include Non-compliance of the system, missing consents and citizen unawareness. These privacy threats will result in the violation of the citizens' privacy but are considered medium risk. This is because the management are considered knowledgeable and are aware of the consequences of ignoring the relevant legislation and regulations. Non-compliance of employees is also deemed medium risk because employees can be coerced into violating the rules. Therefore, the following summarise the identified privacy threats for the credential issuance use case that we assigned medium priority risk:

- T01 - Profiling citizen data
- T02 - Linking biographic data to biometrics data
- T14 - Non-compliance of employees
- T16 - Non-compliance management
- T15 - Missing citizen consents
- T17 - Citizen unawareness

The identified privacy threats for the credential issuance use case related to internal process and data flow are deemed low priority risk because the system is assumed to be implemented correctly. Thus, the identified privacy threats for the credential issuance use case that we assigned low priority risk are itemized as follows:

- T11 - Disclosure of internally transmitted personal information
- T12 - Information disclosure of process
- T13 - Side channel information disclosure of process

There are also several other risk assessment techniques that could be employed to prioritise the identified privacy threats. For example, the NIST's Special Publication 800-300 [21], OWASP's Risk Rating Methodology [22], Microsoft's DREAD [23], or OCTAVE [24]. These methods exploit the information embodied in the identified privacy threats, for example, the assets, to examine the impact; and the adversary profile including data flows to consider the likelihood.

The next step in the solution space of the LINDDUN methodology is to elicit mitigation strategies. However, organisations may choose to respond differently depending on the potential impact of the identified privacy risk. The other response approaches they may choose to adopt apart from mitigating the risk, include transferring or sharing the risk, avoiding the risk, or accepting the risk [25]. For organisations that decide to mitigate the identified privacy risk, the LINDDUN methodology provides a taxonomy of mitigation strategies which can then be employed to categorise privacy solutions. These mitigation strategies are group into two

TABLE II
IDENTIFIED PRIVACY THREATS, THREAT SCENARIOS, PRIMARY THREAT ACTORS AND CONSEQUENCES

Threats		**Primary Threat Actor**			**Consequences**
Threat	**Threat Scenario**	**Insider**	**Skilled Outsider**	**Management**	
T01- Profiling citizen data	An insider with malicious intent links citizen data	**X**			Threat actor has access to more information about the citizen
T02- Linking biographic data to biometrics data	An insider with access to both the biographic data store and biometrics data store is able to link the data from both databases	**X**			The combined set of data contains personal identifiable information and poses a privacy threat
T03 - Identifying a citizen from biographic data and/or biometrics data	An insider with malicious intent identifies a citizen in a set of biographic data and/or biometrics data	**X**			The threat actor gains access to a citizen's identity that should have remained secret
T04 - Information disclosure of citizen data	An authenticated user can access personal information of all citizens	**X**	**X**		Citizen data or user login details are exposed to unauthorized users or outsiders
T05 - Spoofing a user of the system by falsifying credentials	The threat actor obtains user credentials allowing access to the system		**X**		Citizen data are exposed to outsiders
T06 - Spoofing a user of the system by eavesdropping the communication channel	The threat actor obtains user credentials allowing access to the system		**X**		Citizen data are exposed to outsiders
T07 - Spoofing a user of the system because of weak credential storage	The threat actor obtains user credentials allowing access to the system		**X**		Citizen data are exposed to outsiders
T08 - Disclosure of the transmitted log-in credentials	The threat actor gains access to the data flow that contains the credentials used for log-in		**X**		The threat actor has access to the user's log-in information and can spoof the user
T09 - Disclosure of the transmitted session token	The threat actor gains access to the data flow that contains the session token (which authenticates the user during the entire session)		**X**		The threat actor can use the session token to spoof the user during the current session
T10 - Disclosure of transmitted personal information	The threat actor gains access to the transmitted citizen information		**X**		The threat actor has access to sensitive personal information
T11 - Disclosure of internally transmitted personal information	The threat actor gains access to the transmitted citizen information	**X**			The threat actor has access to personal information
T12 - Information disclosure of process	The threat actor gains access to one of the processes	**X**			The threat actor has access to personal identifiable information
T13 - Side channel information disclosure of process	The threat actor gains access to one of the processes	**X**			The threat actor has access to personal identifiable information
T14 - Non-compliance of employees	The system does not process user data in compliance with legislation or policies	**X**			The citizen's personal information is shared without their knowledge
T15 - Missing citizen consents	The system did not ask the citizen's permission to share part of their personal information			**X**	The citizen's information is shared without permission
T16 - Non-compliance management	The management fails to request a design and implementation of the system in compliance with legislation			**X**	The citizen's personal information is shared without their knowledge
T17 - Citizen unawareness	The citizen is unaware of the consequences of sharing information			**X**	The citizen's personal information is used for other purposes for which it has not been intended

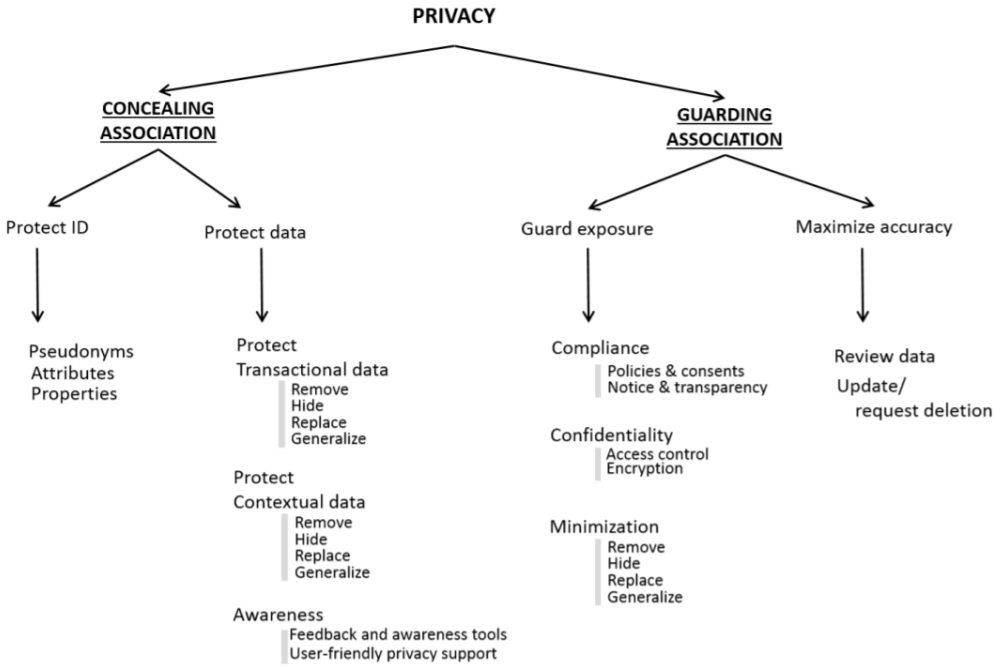

Fig. 6. Taxonomy of mitigation strategies
[26]

TABLE III
MAPPING MITIGATION STRATEGIES TO PRIVACY REQUIREMENTS AND PRIVACY ENHANCING SOLUTIONS

Threat	Mitigation strategy	Privacy requirement	Suggested privacy enhancing solution
T03 - Identifying a citizen from biographic data and/or biometrics data	Anonymity, Confidentiality, Pseudonymity	Provide anonymity of citizen data such that the citizen cannot be identified from biographic and/or biometrics data; Ensure the protection of the data stores; Pseudonymize citizen's data	Apply data anonymization techniques, such as k-anonymity; enforce data protection by means of role-based access control; apply secure pseudonymization
T04 - Information disclosure of citizen data	Confidentiality	Ensure confidentiality of data stores by means of access control and encryption mechanisms	Apply role-based access control at the biographic and biometrics databases; use ISO approved encryption mechanisms to secure both the biographic and biometrics databases
T05 - Spoofing a user of the system by falsifying credentials	Authentication	Provide multifactor authentication method for user access to the system	Use multifactor authentication
T06 - Spoofing a user of the system by eavesdropping communication	Authentication	Provide multifactor authentication method for user access to the system	Use multifactor authentication
T07 - Spoofing a user of the system because of weak credential storage	Authentication	Provide multifactor authentication method for user access to the system	Use multifactor authentication
T08 - Disclosure of the transmitted log-in credentials	Confidentiality	Ensure confidentiality of the transmitted log-in credentials by means of encryption	Use authenticated encryption of TLS (transport layer security)
T09 - Disclosure of the transmitted session token	Confidentiality	Ensure confidentiality of the transmitted session token by means of encryption	Use authenticated encryption of TLS
T10 - Disclosure of transmitted personal information	Confidentiality	Ensure confidentiality of transmitted personal information by means of encryption	Use authenticated encryption of TLS

approaches: proactive approach, where the goal is to conceal associations after disclosure; and reactive approach, where the goal is to guard the exposure of these associations [26]. The LINDDUN methodology's taxonomy of mitigation strategies is shown in Figure 6.

For the credential issuance use case in this study, we consider the mitigation strategies for the identified privacy threats with high priority risk and assume that the organisation would choose to deploy any of the other response approaches for the identified privacy threats with medium and low priority risk (due to the page limitation). Accordingly, the identified privacy threats with high priority risk for the credential issuance use case in this study can also be categorised into the two approaches described in Figure 6.

The final step of the LINDDUN methodology involves the use of the mitigation strategies to define privacy requirements and to suggest privacy enhancing solutions. In this step, we use the mitigation strategies obtained in the preceding paragraph and map them to privacy requirements and privacy enhancing solutions. The results obtained from this mapping is provided in Table III.

V. Conclusion and Future Work

Regulatory requirements have made the integration of privacy principles and requirements to become an integral part of any system that handles PII. To this end, government policy makers implementing NID systems need to also consider the privacy aspects of those particular implementations. In this paper, we have illustrated how to integrate privacy principles and requirements into NID systems using a credential issuance use case that deploys OSIA standard for interoperability. Using the LINDDUN methodology, we identified privacy threats to the selected use case, proposed mitigation strategies that were used to define privacy requirements, and suggested privacy enhancing solutions. It is important to emphasise that OSIA is an open standard specification for interoperability. As a result, the identified privacy threats cannot be fully covered by the OSIA standard specification and they would have to be resolved at the implementation stages by the technology providers. In the future, we hope to expand on this study to include privacy threats with medium and low priority risk, to consider additional use cases in the national identity management ecosystem, and to investigate stakeholders' views on the privacy implications of the deployment of NID systems.

Acknowledgment

We are very grateful to the OSIA Working Group and Advisory Committee for their helpful contributions, feedback and comments.

References

[1] United Nations Legal Identity Expert Group, "United nations strategy for legal identity for all," 2019. [Online]. Available: https://unstats.un.org/legal-identity-agenda/documents/UN-Strategy-for-LIA.pdf

[2] N. Anand, "New principles for governing aadhaar: Improving access and inclusion, privacy, security, and identity management," *Journal of Science Policy & Governance*, vol. 18, no. 01, mar 2021.

[3] B. Manby, "The sustainable development goals and 'legal identity for all': 'first, do no harm'," *World Development*, vol. 139, p. 105343, mar 2021.

[4] United Nations Department of Economic and Social Affairs, "Sustainable development goal 16," 2015. [Online]. Available: https://sdgs.un.org/goals/goal16

[5] J. Clark, "The state of identification systems in africa: A synthesis of country assessments," *World Bank*, 2017. [Online]. Available: http://hdl.handle.net/10986/26504

[6] Secure Identity Alliance, "Osia white paper," 2019. [Online]. Available: https://secureidentityalliance.org/publications-docman/public/osia/158-osia-white-paper-en-june19/file

[7] World Bank's Identification for Development (ID4D) Initiative, "Creating a good id system presents risks and challenges, but there are common success factors," *Practitioner's Guide*, 2022. [Online]. Available: https://id4d.worldbank.org/guide/creating-good-id-system-presents-risks-and-challenges-there-are-common-success-factors

[8] A. Romanou, "The necessity of the implementation of privacy by design in sectors where data protection concerns arise," *Computer Law & Security Review*, vol. 34, no. 1, pp. 99–110, feb 2018.

[9] V. Diamantopoulou, A. Tsohou, and M. Karyda, "General data protection regulation and ISO/IEC 27001:2013: Synergies of activities towards organisations' compliance," in *Trust, Privacy and Security in Digital Business*. Springer International Publishing, 2019, pp. 94–109.

[10] L. O. Nweke and S. Wolthusen, "Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection," in *2020 12th International Conference on Cyber Conflict (CyCon)*. IEEE, may 2020.

[11] K. Wuyts and W. Joosen, "Linddun privacy threat modeling: a tutorial," *Technical Report (CW Reports),volume CW685*, 2015.

[12] World Bank's Identification for Development (ID4D) Initiative, "Glossary," *Practitioner's Guide*, 2022. [Online]. Available: https://id4d.worldbank.org/guide/glossary

[13] A. Roeder, "Benefits, concerns around national identification systems," 2015. [Online]. Available: https://www.hsph.harvard.edu/news/features/benefits-concerns-around-national-identification-systems/

[14] Privacy International, "How national id systems make social protection inaccessible to vulnerable populations," *Free Expression the Law*, 2021.

[15] Harvard FXB, "National identification number project," 2022. [Online]. Available: https://fxb.harvard.edu/national-identification-number-project/

[16] World Bank's Identification for Development (ID4D) Initiative, "Types of id systems," *Practitioner's Guide*, 2022. [Online]. Available: https://id4d.worldbank.org/guide/types-id-systems

[17] Secure Identity Alliance, "Osia doumentation," 2022. [Online]. Available: https://osia.readthedocs.io/en/latest/index.html

[18] United Nations, "Handbook on civil registration and vital-statistics systems: Management, operation and maintenance," 2018. [Online]. Available: https://unstats.un.org/unsd/demographic-social/Standards-and-Methods/files/Handbooks/crvs/crvs-mgt-E.pdf

[19] United Nations Department of Economic and Social Affairs, "Principles andrecommendations for a vitalstatistics system," 2014.

[20] W. J. Kim Wuyts, Riccardo Scandariato, "Lind(d)un privacy threattree catalog," 2014.

[21] National Institute of Standards and Technology, "Guide for conducting risk assessments," National Institute of Standards and Technology, Tech. Rep., 2012.

[22] J. Williams, "Owasp risk rating methodology," *The OWASP Foundation*, 2022. [Online]. Available: https://owasp.org/

[23] T. UcedaVelez and M. M. Morana, *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. John Wiley and Sons, May 2015.

[24] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the octave approach," 2003.

[25] National Institute of Standards and Technology, "Managing information security risk :," National Institute of Standards and Technology, Tech. Rep., 2011.

[26] DistriNet KU Leuven, "Mitigation strategies and solutions," 2020. [Online]. Available: https://www.linddun.org/mitigation-strategies-and-solutions