Kääriäinen, Teemu; Kortesniemi, Yki

Building Trustworthy Twin-based Systems with Self-Sovereign Identities

Published in:
IEEE Access

DOI:
10.1109/ACCESS.2024.3507924

Published: 27/11/2024

Document Version
Publisher's PDF, also known as Version of record

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 October 2024, accepted 10 November 2024, date of publication 27 November 2024,
date of current version 12 December 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3507924

RESEARCH ARTICLE

Building Trustworthy Twin-Based Systems With Self-Sovereign Identities

TEEMU P. KÄÄRIÄINEN AND YKI KORTESNIEMI
Department of Information and Communications Engineering, Aalto University, 02150 Espoo, Finland
Corresponding author: Teemu P. Kääriäinen (teemu.p.kaariainen@aalto.fi)

This work was supported by the European Union (EU) Horizon 2020 Research and Innovation Project Internet of Things-Next Generation Internet (IoT-NGIN) under Grant 957246.

ABSTRACT Semantic Twins are a novel means of describing Digital Twins and their associated real-world entities in human- and machine-readable formats. Together, this (Entity) Triplet facilitates easier development and deployment of Twin-based solutions, but a key challenge in critical applications is ensuring the trustworthiness of the Triplet: that they produce reliable services throughout their lifecycle, particularly in high-risk use cases. This paper studies the trustworthiness requirements of Triplet-based systems and the extent to which they can be addressed with Self-Sovereign identities (SSIs). The results show that there are cross-cutting requirements applicable for different entity types and lifecycle phases, and that SSIs can solve many of the key trustworthiness requirements. However, there is also a need for additional governance methods, such as architectural blueprints and ecosystem governance frameworks, to reach a comprehensive approach to the trustworthiness of Triplets. Finally, the paper provides a list of the essential trustworthiness requirements that even the low-risk Triplets should aim for.

INDEX TERMS Semantic twin, digital twin, entity triplet, self-sovereign identity, trustworthiness.

I. INTRODUCTION

Internet of Things (IoT) devices and their associated Digital Twins (DTs) have enabled many new digital services, e.g. in smart cities [1], and the manufacturing industry [2], but as their numbers grow, manually discovering and managing the devices can become a daunting task. Each device and its associated DT can offer many services [3], use one or more Application Programming Interfaces (APIs) to access them, have different policies for using and paying for the services, and provide different levels of assurance to the veracity of the information they provide etc. To effectively manage this multitude of metadata and efficiently develop and deploy new IoT- and DT-based services, there is a need for an automated and scalable mechanism such as *Semantic Twins (STs)* [4] that provides machine-readable semantic information about the devices and their DTs. Effectively, the addition of a Semantic Twin expands the IoT device (or, more generally, any real-world entity) and its associated DT into an Entity *Triplet*, which addresses the need for solution development and deployment more wholistically.

The Triplets can cover many types of use cases from simple hobby solutions all the way to complex systems that provide high-risk or even life-critical services, which is then reflected on the demands based on the Triplets. A key element in building high-risk and critical solutions, particularly those that utilize multiple Triplets controlled by different actors, is establishing sufficient *trust* for the Triplets. The extent to which entities deserve trust can be assessed with *trustworthiness* [5], which builds on appropriate *assurances / evidence*. *Trustworthiness requirements* can help define which assurances are sufficient to establish trust in a particular situation, and as such, ensure the reliable operation of Triplets under those conditions. However, measuring trustworthiness is difficult [6], especially considering the fact that interactions may occur between different types of entities, such as IoT devices, natural persons, and organizations. Maple et al. [5] defined that the trustworthiness of digital services can be evaluated based on (1) *ethics*, (2) *privacy*, (3) *reliability*, (4) *robustness*, (5) *security*, and (6) *resiliency* criteria, and this categorization is used also in this

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Tsun Cheng.

paper to identify the key trustworthiness requirements for Triplets.

A common technology to address many key trustworthiness requirements in digital services is to use *digital identities* (identifiers, claims, and credentials) [7]. This paper also explores the role of one emerging identity type, the Self-Sovereign Identities (SSIs), in the trustworthiness of Triplets as they offer particularly good privacy-preservation through data minimization[1] and decentralization.

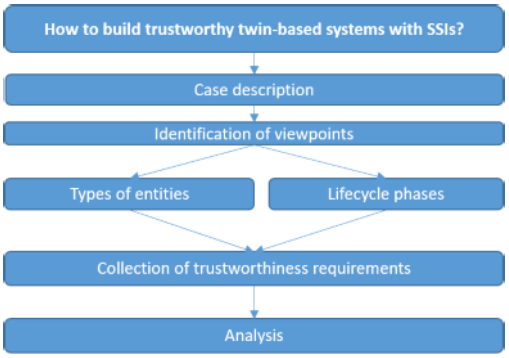

FIGURE 1. Research process to study how to build trustworthy Triplets.

The research process depicted in Fig. 1 was used to study the construction of trustworthy Triplets. The process was initiated by identifying a sufficiently complex case description to extract a comprehensive set of trustworthiness criteria for a high-risk application by utilizing the model of Maple et al. Two complementary viewpoints (*entity types* and *lifecycle phases*) were then used to complete the discovery and assessment of the trustworthiness requirements. The next step was to evaluate SSIs to determine the extent to which they could be utilized to address the requirements and what requirements raise the need for additional approaches. Finally, a list of essential trustworthiness requirements were identified, which are usable in building trustworthy Triplet-based solutions even in low-risk scenarios.

Altogether, the paper addresses the following research questions:

- RQ1: What constitutes a comprehensive set of trustworthiness requirements for Triplets used in high-risk applications?
- RQ2: How does the real-world entity type and different lifecycle phases of the Triplet affect trustworthiness?
- RQ3: Which Triplet trustworthiness requirements are essential even for low-risk Triplet use cases?
- RQ4: Which trustworthiness requirements of the comprehensive list can be effectively addressed using SSIs, and how should that be done?

The results show that Triplets need to balance their trustworthiness requirements against the criticality of the solution, and that SSIs can address many trustworthiness requirements such as data provenance[2] and privacy-preservation.[3] However, a more comprehensive approach to the trustworthiness of Triplets requires the introduction of e.g. additional data governance[4]- and technical-architecture-related activities, such as architectural blueprints, reference architecture frameworks,[5] and ecosystem governance frameworks.[6]

The contributions of the paper include (1) describing the basic characteristics of an entity Triplet, (2) defining a model to identify the essential trustworthiness requirements of a Twin-based system depending on its criticality, and (3) assessing which trustworthiness requirements can be addressed with Self-Sovereign Identities.

The rest of the paper is organized as follows: Section II describes the Triplet, its lifecycle model, and discusses why Triplet trustworthiness is important. Section III provides a background on Self-Sovereign identities, and Section IV presents previous work on trustworthiness requirements. Section V describes the studied real-world IoT use case: a traffic monitoring camera, and Section VI examines the comprehensive list of trustworthiness requirements based on the use case. Section VII explores how different entity types and different lifecycle phases of the Triplet affect the requirements. Section VIII provides the essential Triplet trustworthiness requirements applicable for all Triplets, and analyzes the extent to which SSIs can address the comprehensive list of trustworthiness requirements for high-criticality applications. Section IX provides a discussion along with areas for future work, and Section X presents the conclusions.

II. TRIPLET AND ITS TRUSTWORTHINESS

This section details the Triplet, its lifecycle, and the challenges of ensuring its trustworthiness.

A. THE TRIPLET AND ENTITY TYPES

The Entity *Triplet* [4] as shown in Fig. 2 consists of three things: a real-world entity such as an IoT device, a Digital Twin (DT) that is the digital representation of the entity, and a Semantic Twin (ST) that offers a structured description of the entity and the DT.

A **real-world entity** is the heart of each Triplet. In addition to IoT devices, Triplets can be created for many other *types of entities*, such as companies, private individuals, Artificial Intelligence (AI) systems, and robots. In order to come up with a representative categorization of different types of Triplets, this paper will use three dimensions to assess the

[1] Only processing data that is strictly necessary for a specific purpose.

[2] Trace the origin of a piece of information [8].

[3] Protecting individuals' personal information and maintaining control over the disclosure of their identity-related data.

[4] A set of processes that ensures that data assets are formally managed throughout the enterprise [9].

[5] A structured and standardized set of guidelines, principles, and models that provides a comprehensive blueprint for designing, building, and deploying systems.

[6] Describes the binding, ecosystem-wide rules and specifications (business, legal, technical, social) and defines the ecosystem's borders [10].

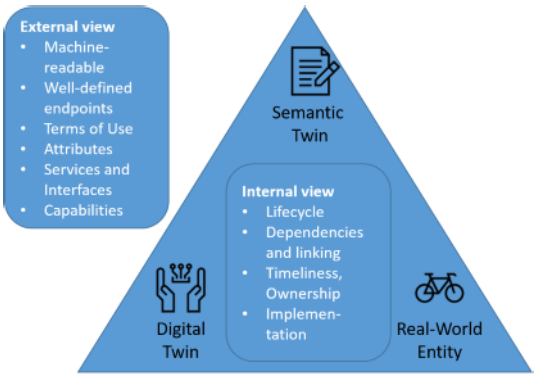

FIGURE 2. Triplet's schematic diagram.

TABLE 1. Entity type categorization.

	Physical	Virtual
Human-centered	Person	Organization
Machine-centered	Device	Service

TABLE 2. Examples of autonomous and dependent entity types.

	Autonomous	Dependent
Person	Adult	Child
Organization	Public Corporation	Franchisee
Device	Robot	Smart Thermostat
Service	AI System	HR Management System

entities for which Triplets can be created: physical vs. virtual, human-centered vs. machine-centered, and autonomous vs. dependent. Table 1 describes the different entity types assessed for the first two dimensions, whereas Table 2 provides examples of autonomous and dependent entities.

Triplets of Person-type entities can describe and allow trustworthy interaction with e.g. their attributes and capabilities, asset ownership, and employment. Similarly, Organizations' Triplets may offer, for example, access to contact points, business processes and workflows, and official representatives of the company. Devices' Triplets may provide metadata about the capabilities of the Device, and facilitate access to the Device and its services. Finally, for Services, the Triplets may e.g. offer details about their ethical and privacy guidelines, and affiliations to companies.

Person-type entities can be divided into autonomous adults and guardian-dependent individuals, such as children. Examples of autonomous Organizations are e.g. autonomous public corporations, whereas franchisees dependent on a franchise are examples of Organizations that can be considered dependent. Devices may be either autonomous (such as robots), or dependent remote-controlled devices, such as smart thermostats. Finally, an example of an autonomous Service could be an AI system, whereas an example of a non-autonomous Service could be an HR management systems which always relies on a natural person managing its functionality.

Digital Twins [11] are the virtual representations of real-world entities that mirror and augment their behavior, characteristics, and interactions. They are used to provide access to the services provided by the entity, but also to e.g. operate, monitor, and make available data of their real-world counterparts, which enables improving decision-making and optimizing their behavior. The versatility of Digital Twins means that they can be applied to entities ranging from individual components to complex systems, but also from physical objects (e.g. humans [12], [13] or cars [14], [15]) to abstract concepts (e.g. organizations [16]).

Finally, the **Semantic Twin** augments the capabilities of the Digital Twin and the entity by providing a means of distributing human- and machine-readable semantic information about the Digital Twin and the associated real-world entity, including their capabilities, services, and other *attributes*.[7] As such, Semantic Twins are used to address e.g. the following types of questions:

- What kinds of services and attributes do the Digital Twin and the associated real-world entity offer?
- Under which terms may the Digital Twin or entity be accessed?
- What costs are involved in using the Digital Twin or entity?
- Who owns and manages the Digital Twin and the associated real-world entity?
- How trustworthy are the Digital Twin's and entity's capabilities and the data they produce?

As a consequence, the main goal of Semantic Twins is to ease the deployment and adoption of Digital-Twin-based solutions by producing human- and machine-readable semantic information in a scalable manner through well-designed API endpoints.[8] Semantic Twins allow e.g. for the discovery of and access to Digital Twins and their associated real-world entities (including their services and attributes). Well-designed API endpoints facilitate a more interoperable and secure manner of accessing DTs, compared to existing solutions (e.g. offering direct access to Digital Twins). Semantic Twins, thus, solve many wide-scale adoption and accessibility problems of Digital Twins [18]: (1) Twins are made accessible through internet platforms only as an afterthought, (2) Digital Twins often contain confidential information, and (3) practitioners do not have the necessary skills to create Internet-accessible Digital Twins. Semantic Twins solve these problems by "providing a shared infrastructure on which other solutions can be built" [18].

Finally, the term **Triplet** refers to the unit made of all three parts. It offers a unified means of discovering and interacting with the entity and its DT to use their services, and to gain access to verifiable semantic information about them via the ST. As such, the three parts of the Triplet complement each

[7] A presentation that defines a property of a Digital Twin or an entity.

[8] A well-designed API is easy to understand, use, and maintain. It should follow consistent style conventions, include built-in security mechanisms for authentication and data encryption, and reliably handle large volumes of traffic [17].

other and offer something more than the sum of its parts, while allowing the parts to act independently of each other or, significantly, be replaced if needed, in which case the triplet can be much longer-lived than its constituent parts.

B. TRIPLET LIFECYCLE

In this paper, *Triplet lifecycle* will refer to the simplified lifecycle model depicted in Fig. 3, which is used to study the implications of Triplet lifecycle to its trustworthiness. This lifecycle model captures the progression of a Triplet from its creation, through ongoing updates, activations, and passivations, until it is deleted. It emphasizes the dynamic nature of the Triplet in actively supporting the development and deployment of twin-based systems.

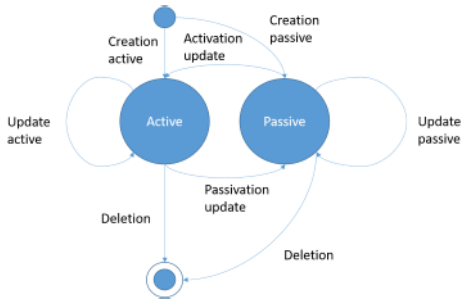

FIGURE 3. Simplified lifecycle model of a Triplet.

Triplets exist in two states: *active* and *passive*. They move between states through three *lifecycle* phases[9]: *creation*, *update*, and *deletion*. Creation operations can create Triplets into active (creation-to-active) or passive (creation-to-passive) states. Update operations can be either *activation updates* (passive-to-active), *passivation updates* (active-to-passive), *updates of active*, or *updates of passive* operations. One special case of a Triplet in passive state is a *tombstone*, where the Digital Twin and the actual Entity may have been removed, but the Semantic Twin remains as a mechanism to refer to the Entity (and DT) that previously existed. As such, a Triplet always requires the presence of an ST, whereas presence of DT or the actual Entity is not necessary.

The Triplet lifecycle starts when it is **created** and the Triplet is moved to either active[10] or passive state. In active state, the ST is discoverable and associated to a DT, and the actual real-world entity (e.g. an IoT device) has been deployed. In passive state, it is possible that only the ST is created, and it is waiting for the deployment and association of the DT and the actual entity.

Changes may be made to the Triplet's setup through **updates** while keeping it in an active or passive state. It is also possible to update the Triplet, for example, in a manner where the entity connected to the Semantic and Digital Twin is changed (for example, in the case of a broken device, or a person acting in certain role changes), so a Triplet can provide *continuity to services* beyond the lifetime of its individual parts. Passive triplet may be brought back to the active state through *activation*, however, this may not be possible for all entity types (e.g. if the ST and DT have been logically and/or physically destroyed). Finally, triplets are removed through **deletion** and, as such, cease to exist.

The effects of different lifecycle phases on the Triplet trustworthiness requirements are studied in detail in Section VII.

C. TRIPLET TRUSTWORTHINESS

Several sectors are taking advantage of IoT and Digital Twin solutions [19]. In many less critical applications, the trustworthiness of the Triplet is not a high priority, but an increasing number of solutions deal with sensitive and high-risk data processing (e.g. in healthcare [20] or critical infrastructure [21]), which makes them susceptible to security breaches such as hacking, data infiltration, and service disruptions. For example, an insulin pump [22] may cause serious repercussions for individuals if its trustworthiness is not properly guaranteed. Taking trustworthiness into consideration from the early phases of Triplet deployments ensures e.g. that Triplets' data can be trusted, they function correctly under varying circumstances, and that they ensure sustainable long-term operations.

As shown in Fig. 2, this paper studies Triplet trustworthiness through external and internal views. The *external view* allows us to consider the trustworthiness of the services and interfaces offered by the Triplet, whereas the *internal view*, which is required to enable the external view, allows us to focus on managing the trust between the parts of the Triplet during normal operations, but also through unusual situation such as replacing a broken device. The internal and external trustworthiness requirements are studied in detail in Section VII through the analysis of different entity types and lifecycle phases.

The systems and services that utilize Triplets may comprise only a single Triplet, but there are examples of complex systems with several inter-connected and interlinked Triplets. In the latter case, the trust between Triplets needs to be factored into the Triplets' trustworthiness requirements. As an example, the large apartment building shown in Fig. 4 has many types of Triplets associated to it: an organization who owns the building, multiple internet-connected sensors monitoring the building, a cloud-based self-service portal, and natural persons as tenants, all of whom need to have sufficient level of trust for each other, i.e. to "believe in the integrity, ability, or character of an entity that they are engaging with" [5].

Maple et al. define trustworthiness as a means to "determine the extent to which the entity deserves trust" and to "obtain confidence that the trust requirements are satisfied" [5]. To this end, they studied the trustworthiness requirements of digital identity management systems and developed a 6 class categorization of trustworthiness requirements, as described below:

[9]Stages that a Triplet undergoes throughout its existence.
[10]The Triplet and its parts are ready, activated, and taken into use.

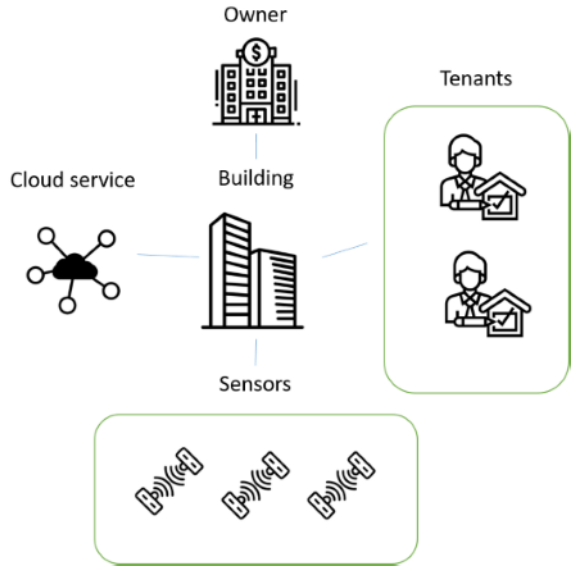

FIGURE 4. Connected and inter-linked Triplets in a large apartment building case.

- (1) Ethics: ensuring transparent, responsible, and auditable operations, whilst enabling user empowerment
- (2) Privacy: ensuring personal and sensitive information is treated privately, with adherence to legal and regulatory restrictions
- (3) Reliability: ability of the system to perform in a consistent and expected way
- (4) Robustness: ability of the system to continue functioning in the presence of internal and external challenges without changes to its operations or state
- (5) Security: protection of data, information, and systems against unauthorized access or modifications
- (6) Resiliency: ability of the system to adjust to internal and external conditions to ensure continuation of expected service

This categorization can be easily adapted to identify some trustworthiness factors in the apartment building example:

- (1) Ethics: The ability of the sensor to ensure that the provenance of its ownership information (who owns the device) is correct, and the need for the tenants to ensure that there is human-readable policy documentation and easily accessible contact points towards the owning organization.
- (2) Privacy: Ensuring that the sensors do not collect information about the tenants without an appropriate legal basis, such as consent, and that they ensure data minimization.
- (3) Reliability: The need for the cloud-based service to ensure that it is engaging with reputable customer organizations to reduce the possibility of fraud.
- (4) Robustness: The ability of the cloud-service to continue operations also when receiving unexpected input from tenants or sensors, and the ability of the owning organization to keep its tenant information up-to-date.
- (5) Security: Allowing the cloud-service to be managed only by authorized representatives of the owning organizations and the need to ensure that the owning organization has deployed the sensors in a manner that prevents unauthorized tampering of the device.
- (6) Resiliency: the ability of the sensors to recover from unexpected environmental conditions (storms or disruptions in electric supply).

In Section V, this paper uses the 6 class trustworthiness requirements categorization by Maple et al. (discussed above) to identify a comprehensive set of Triplet trustworthiness requirements for high-risk applications. However, some modifications are required, because the trustworthiness features of Maple et al. were defined for Digital Identity Systems, and they are discussed in the section, as well.

III. SELF-SOVEREIGN IDENTITIES

Digital identities have been used for decades to identify users of digital services [23] with suitable *levels of assurance*[11] [24]. Cameron defines digital identities as being able to (1) convey an identifier to uniquely identify an actor, (2) assert that an actor knows a given (private) key, (3) convey personally identifying information, (4) convey information that the actor is part of a group, or (5) state that the actor has a certain capability [25].

Another complementary way to define digital identities is that they are ''a representation of an entity'' and being constructed of ''claims and identifiers'' [26]. *Identifiers* are ''attributes or sets of attributes that uniquely characterize [i.e. identify] an identity in a domain'' [27] such as social security numbers or email addresses, whereas *claims* are defined as ''assertions of the truth of something, typically ones which are disputed or in doubt'' [25], such as one's first name and last name or current employment details. Claims and identifiers are often grouped together as *credentials* to enable their use in digital transactions. Credentials use digital signatures to ensure their integrity, along with the ability to verify the origin of the identifier and claim information. Examples of credentials include e.g. your employment certificate issued by your employer, or a driver's license.

In his paper, Allen [26] discusses how digital identities have developed from centralized identities[12] through federated[13] and user-managed identities[14] into *Self-Sovereign Identities (SSIs)*. SSIs are meant to present a shift in digital transactions so that the identity owner is brought to the center of the transactions to give them control over the way their personal information is being processed. SSI

[11] Degree of confidence and trustworthiness.

[12] Digital identities being controlled and administered in a central system or platform.

[13] Sharing of digital identities across multiple autonomous, yet collaborating, organizations or systems.

[14] Users being given more control over their own identity information, and how it is used across different services and applications.

solutions are often implemented using decentralized identity technologies, in which digital identities do not need to rely on any centralized party. A typical example of such technology is the Decentralized Identifier (DID) defined by the W3C DID specification [28], which offers discoverable and privacy-preserving unique identifier capabilities. Other techniques often used in decentralized identity solutions are the Verifiable Credentials (VC) defined by the W3C Verifiable Credential definition [29] and the Passkeys [30] defined by the FIDO alliance.

Compared to previous identity techniques [7], SSIs offer several benefits in solving trustworthiness requirements, including:

- (1) Ethics: They offer equal and affordable access to end-users.
- (2) Privacy: Users can enforce data minimization through selective data sharing.
- (3) Reliability: Interoperable operations ensure that systems function in a consistent and predictable manner.
- (4) Robustness: Decentralized governance of identity information decreases attack surface and ensures that claims about entities remain accurate and timely.
- (5) Security: Users having the ability to control access to their personal and sensitive information protects from unauthorized access and modification.
- (6) Resiliency: A user's digital identity exists independent of any centralized party.

Section VIII explores the extent to which the trustworthiness requirements can be satisfied with SSIs, and where additional solutions are required.

IV. PREVIOUS WORK

This section summarizes how the trustworthiness of Digital Twin-based systems has been addressed in previous studies. Because Semantic Twins are a novel concept, no previous work exists on solving the trustworthiness of Semantic Twins or Entity Triplets specifically. Semantic Twins have, however, been studied in the context of existing semantic technology frameworks, such as Ontology Modelling Language (OML), Resource Description Framework (RDF), and Web Ontology Language (OWF) [31], [32].

An existing study on trustworthiness requirements includes e.g. a study of IoT device trustworthiness requirements by Tragos et al. [33] who defined *trustworthiness* as "a metric of how much an entity deserves the trust of other entities". Based on their study, IoT device trustworthiness requirements consist of criteria related to *governance*, *security*, *privacy*, *availability*, and *safety* which can then be used to calculate the trustworthiness of IoT devices and services.

A common way to identify trustworthiness requirements for a solution is to study the various threats to the solution in question, and for Digital Twins, particularly security- and privacy-related threats have been studied in several studies. A comprehensive survey by Alcaraz and Lopez [34] discovered multiple security, resiliency, and privacy threats (e.g. privilege escalation, privacy leakage) and effective countermeasures, such as access control, authentication, authorization, pseudonymous identification,[15] and collection of forensic information for security monitoring and security event handling. In addition, Damjanovic-Behrendt [35] discussed the privacy implications of Digital Twins in the automotive industry, including the different cryptographic and non-cryptographic approaches to privacy preservation and how these are used to counter privacy-related threats. The limitation of these studies is that they focus only on three of the six trustworthiness requirements categories by Maple et al. [5], listed in section II: (2) privacy, (5) security, and (6) resiliency; therefore, they lack a holistic view of trustworthiness (i.e. do not take into account (1) ethics, (3) reliability, and (4) robustness).

Governance offers an alternative method to study the trustworthiness of Twin-based systems. NIST's retired draft standard NIST IR 8356 [36] provides a holistic governance approach to the trustworthiness of Digital Twins by discussing various cybersecurity and trustworthiness considerations that are relevant for Digital Twins. The draft standard considers the trustworthiness of Digital Twins on different levels, such as the equivalence of the Digital Twin with the physical object, the need to understand the context of the physical object, and the need to standardize and certify the Digital Twin technology. However, the standard lacks a comprehensive view of Digital Twins of different types of entities, as it focuses only on Digital Twins developed for physical objects and ignores all other entity types.

An alternative viewpoint to governance is given by Wright and Davidson [37], who discussed the need to ensure traceability[16] and reliability of measurements produced by Digital Twins. However, this study focuses only on a subset of trustworthiness categories, namely (1) ethics and (3) reliability.

Some studies, such as Lee et al. [38] studied the capabilities of blockchain-based techniques to improve the governance of Digital Twin-based systems through the blockchain platform's ability to ensure immutability,[17] transparency, and traceability of transactions, along with the ability to ensure compliance of different participants. However, these studies only focused on the capabilities of certain technologies (blockchains and Distributed Ledger Technologies (DLTs)), thus making no attempt to provide a more holistic and technology-agnostic approach to studying trustworthiness.

Finally, a comprehensive study of the trustworthiness requirements of Twin-based systems for industrial application was provided by Trauer et al. [39], who studied *trust in the context of Digital Twins* and *developed a trust framework for Digital Twins*. The elements of the model used in the study include trustworthiness requirements, such as proper

[15] Entities represented by pseudonyms or aliases, rather than their real names or direct personal identifiers.

[16] Ability to trace and document the origin, accuracy, and reliability of the data and measurements.

[17] Data cannot be altered or deleted.

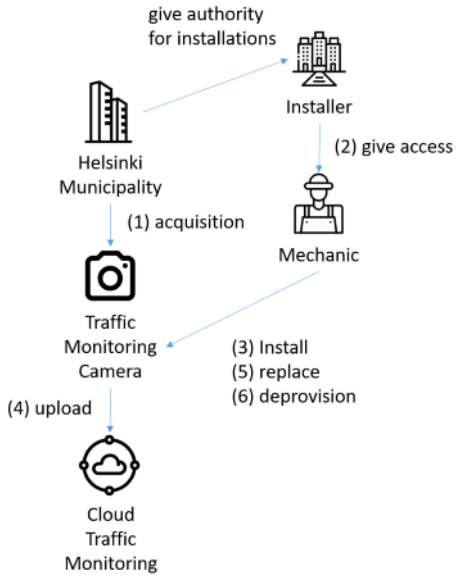

FIGURE 5. The traffic camera use case.

documentation, uniformity of the deployment environment, provable quality, protection of intellectual property, and the need to create common economic incentives. Additional considerations are provided by Khan et al. [40] who argue that the ability to ensure trustworthy Digital Twin ecosystems requires ''joined efforts between manufacturers, maintenance organizations, and regulators in order to mutually design, develop, and control effective and trustworthy systems''. These studies focused on two sectors (manufacturing and industry), whereas Digital Twins can be used in many additional sectors.

A more general approach to address security- and resiliency-related trustworthiness requirements is to adopt a relevant security requirements criteria framework. Commonly used frameworks include e.g. ISO/IEC 27001 [41] and NIST Cybersecurity Framework [42]. Moreover, these standards suffer from focusing only on a few trustworthiness categories: (5) security and (6) resiliency.

The use of digital identities in the context of Digital Twins has been studied in multiple ways. Deng et al. [43] studied the use of digital identities for urban entities (e.g. buildings, sensors, and systems) in the context of building information modeling (BIM) technology, where digital identities are used as the basis for building operations and maintenance and unique identifiers are issued for physical objects in the digital world to enable unique identification, indexing, positioning, and loading of related information about the physical objects to asset databases. This offers the ability to use BIM systems for various activities, such as mapping and surveillance. Several other studies, such as those by Dietz et al. [44] and Putz et al. [45], discuss an approach in which DLTs and their built-in digital identity capabilities are used to offer security capabilities, such as access control, authentication, and authorization, for secure Digital Twin-based data sharing and Digital Twin information management. Other examples of digital identity deployments for digital twins include e.g. the Trusted Twin [46] platform, which supports issuing digital identities for digital twins, and Citopia Self-Sovereign Digital Twins [47], which ''are portable digital twins that can authenticate identity and selectively disclose pertinent data''.

The summary of previous work related to Digital Twin trustworthiness shows that there is a clear research gap due to the lack of a holistic view of trustworthiness, that is, previous studies focus only on certain subsets of trustworthiness areas (e.g. focusing only on (2) privacy, (5) security, and (6) resiliency, thus omitting (1) ethics, (3) reliability, and (4) robustness). Moreover, these studies have been focusing only on a subset of DT types, certain sectors (e.g. manufacturing), or focusing only on a single technology (such as blockchain or DLT). This paper addresses this research gap by providing a holistic and technology-agnostic view of the trustworthiness of twin-based systems that can be applied to any type of entity in any sectors. In addition, this paper provides essential requirements on how to build trustworthiness in twin-based systems that require trust between the actors even in low-risk scenarios.

V. TRAFFIC CAMERA USE CASE

The study of Triplet trustworthiness requires a use case which (1) involves all types of trustworthiness requirements (privacy, ethics, robustness, reliability, security, and resiliency), (2) involves all types of entities listed in Table 1 (Persons, Devices, Organizations, Services), and (3) can be used to analyze the entire lifecycle of associated Triplets. The Jätkäsaari Living Lab[18] provides such a use case with complex interactions between the different types of entities in a Twin-based system.

The use case includes traffic monitoring cameras provided by a supplier, owned by the Helsinki municipality, and maintained by the employees (mechanics) of the Installer (a separate installation firm). Traffic monitoring cameras publish data into a cloud-based traffic-management solution. The use case and relationships of the entity Triplets are shown in Fig. 5.

The use case consists of the following five Triplets:

- Helsinki municipality Triplet and Installer Triplet (Organizations).
- The Triplet of the mechanic (a Person) who is an employee of the Installer and has sufficient privilege to conduct actions on Devices.
- Triplet of the cloud-based traffic monitoring solution (a Service) receiving data from the Devices owned by the Helsinki municipality.
- Traffic monitoring camera Triplet (a Device) publishes data and is operated by the Installer.

Here, the Triplets have differing trustworthiness requirements, e.g.:

[18]The Jätkäsaari Living Lab [48] (part of the EU Horizon 2020 IoT-NGIN project) is a testbed for digital twin deployments in traffic management in the Jätkäsaari area in Helsinki, Finland [49].

- The Helsinki municipality needs to be able to ensure the robustness of the traffic monitoring cameras in varying environmental conditions and to provide sufficient evidence about the maintainability of the setup. The Helsinki municipality and Installer Triplets demonstrate trustworthiness requirements of Organizations, and also the complex trust relationships between Organizations.
- The mechanic (employee of the Installer) needs to be provided a sufficient level of privacy by ensuring e.g. data minimization, data retention, use limitation, and appropriate consent for personal data processing.
- The cloud-based traffic monitoring solution needs to be able to ensure the provenance of the traffic camera data, offer evidence of the ethics of the data processing algorithms, allow traffic monitoring solution users to be empowered to monitor possible misuse of data about them, and to protect the system from unauthorized access and modification.

The lifecycle of the traffic camera use case consists of the following steps: (1) Helsinki municipality acquires a traffic monitoring camera (along with its DT) through a supplier, and the traffic monitoring camera's Semantic Twin is created (= made ready as a passive Triplet for the installation of the rest of the Triplet), (2) Installer firm's mechanic is given access to the traffic monitoring camera's ST and DT by the Installer (who has received the authority from Helsinki municipality), and (3) mechanic installs the traffic monitoring camera, and associates the camera and its Digital Twin with the Semantic Twin to form an active Triplet, (4) data produced by the traffic monitoring camera is uploaded to the cloud-based traffic monitoring solution, (5) traffic monitoring camera may go out of order and needs to be replaced, (6) traffic monitoring camera is taken out of use.

VI. TRUSTWORTHINESS REQUIREMENTS

The trustworthiness features of Maple et al. [5] are used as the basis for the Triplet trustworthiness requirements. However, not all requirements are relevant for all types of processing. Therefore, it is necessary to adjust the requirements depending on the criticality of the data processing, type of entity, and lifecycle phase of the data processing.

The following changes were made to the trustworthiness requirements so that they could be used in the comprehensive analysis of Triplet trustworthiness:

- Generalizing some requirements. For example, the requirement for user consent was generalized so that it applies to personal data processing in general, instead of only focusing on user attribute collection, processing, re-use, and release.
- Removing some requirements that are applicable only to digital identity systems. Examples of removed requirements include e.g. "Remote Identity Proofing and Non-Face-to-face Onboarding", "ID attributes collected fit for scope and purpose", and "Identity Governance and Intelligence".
- Combining some requirements, as they deal with the same topic. E.g. requirements "Evidence of Layered Security" and "Defense-in-depth" were combined to form new requirement "Layered security and defense-in-depth". Also requirements "SSO, MFA" and "Policy enforcement and protection of PII/SPII" were not considered separately, because they were already covered in requirement "Authentication, authorization, and accounting".

TABLE 3. Triplet trustworthiness requirements.

Category	Requirement
Ethics	E1 Data provenance
	E2 Monitor misuse
	E3 Openness
	E4 Audit trail
	E5 Inclusivity and accessibility
Privacy	P1 Data minimization
	P2 User consent
	P3 Data retention
	P4 Use limitation
	P5 Privacy impact assessment
	P6 Privacy risk mitigation plan
	P7 Privacy models and policies
	P8 Use of privacy standards
Reliability	Re1 User contact points
	Re2 Fraud detection and prevention
	Re3 Evidence of government approved audits
	Re4 Evidence of assessments
	Re5 Handling unexpected termination or action
Robustness	Rb1 Expected outcomes from unexpected inputs
	Rb2 Timeliness of information
	Rb3 Tolerance of process variability
	Rb4 Evidence of maintainability
Security	S1 Access control
	S2 Security assessment and auditing
	S3 Authentication, authorization, and accounting
	S4 Evidence of layered security and defense-in-depth
	S5 Regulatory compliance
	S6 Cryptographic protection
	S7 Maturity level of security policies
	S8 Vulnerability management
	S9 Risk response
	S10 Systems and communications protection
Resiliency	Rs1 Internet-face protection
	Rs2 Internal security processes enforced
	Rs3 Backup and disaster recovery plans
	Rs4 Cyber resiliency strategy
	Rs5 Balance between preventive and detective controls
	Rs6 Reaction to security incidents

The adapted, comprehensive set of Triplet trustworthiness requirements for a high-risk application, that addresses RQ1, is provided in Table 3.

A. ETHICS REQUIREMENTS

According to Maple et al. [5], the purpose of ethics requirements is to "ensure transparent, responsible and auditable operations throughout the whole lifecycle of data and information management in systems whilst enabling user empowerment into this process".

1) E1 DATA PROVENANCE

Data provenance (i.e. tracing the origin of a piece of information) is a process to e.g. guarantee the authenticity

of a device [50] by ensuring that the device's claims and attributes (e.g. device model and its unique identifier) have been issued by a trusted issuer. Other practical examples of data provenance are e.g. (1) the need for the cloud service and its end-users to ensure that the images have been produced by an authentic device, (2) the ability of the cloud-service to ensure that the municipality Triplet (the Triplet representing the owning organization) is, in fact, authorized to represent the municipality, or (3) the ability of the device publishing the images to ensure that the cloud service is operated by a trustworthy legal entity whose identity is known.

2) E2 MONITOR MISUSE

Different actors require varying levels of transparency [51] to ensure that the data shared between parties are handled according to a commonly agreed set of rules. This requires tracking and data management tooling, for example, for the mechanics to monitor how their personal data are processed by the device and for users of the cloud-based traffic management solution to track their personal data use. The mechanics may also want to ensure that they can execute their right to be informed about personal data processing activities taking place by their employer. At the same time, the mechanics themselves should be in control of their own personal data, and as such, there should be no way for an external entity to monitor the use of the mechanic's Triplet without the mechanic's own consent.

3) E3 OPENNESS

Users of the cloud-based traffic monitoring solution must be able to ensure that the cloud service's business logic has been implemented in a fair, ethical, and transparent manner [52]. This can be achieved e.g. through offering human-readable policy documentation to provide the necessary evidence and openness about the ethics of the data processing procedures. The same openness may also be required from the device itself as part of the data-processing activities taking place at the device level. The ability of organizations and natural persons to be fully open about their data processing activities may, however, be limited due to data protection or corporate-confidentiality-related requirements, which may then impact their trustworthiness.

4) E4 AUDIT TRAIL

A tamper-proof audit log of essential data[19] must be collected by all the Triplets to ensure an appropriate level of traceability and auditability for the solution in question, and to act as proof for non-repudiation. An example of an audit log to be produced includes e.g. a record of when a user has accessed the DT, including their unique identifier, timestamp, and type of action executed (e.g. read, update, delete). This type of *access log* can be used later, for example, when resolving a possible security incident. Log information must be collected in a manner that ensures privacy-preservation [53] by ensuring data minimization[20] and the presence of necessary controls to reduce the risk of unnecessary correlation.

5) E5 INCLUSIVITY AND ACCESSIBILITY

The solution should consider the varying needs of different user groups, e.g. through promotion of stakeholders' inclusion in city planning [54]. In many cases, this requirement is driven by local regulations that may require inclusivity and accessibility to be considered in the deployment of digital services to ensure equal access [55] for all natural persons. Accessibility requirements are important for the cloud-based traffic monitoring solution, but the requirement is also valid for the Installer firm as an employer, who should not discriminate between its employees.[21] Inclusivity and accessibility governance may be further improved by supporting human-readable documentation that can be made available, for example, to employees or the general public.

B. PRIVACY REQUIREMENTS

Maple et al. [5] defined privacy requirements as ''ensuring that personal and sensitive information transmitted, processed and shared is treated privately, in adherence to legal and regulatory restrictions governing its use.''.

1) P1 DATA MINIMIZATION

The mechanic's Triplet must maintain its claims and attribute information in a trustworthy and tamper-proof manner, while being able to present verifiable information about the mechanic in a privacy-preserving manner. Privacy-preservation is the mechanic's fundamental right [57], and it must be ensured that only a minimal amount of identity information about the mechanic is exposed to the device when assessing whether the mechanic is authorized to operate on it. In addition, it is important to determine the level of privacy of the personal data exposed through the Semantic Twin (e.g. to determine whether the personal data need to be fully anonymous). It is also important to ensure that devices linked to individuals contain the necessary privacy-preservation controls, so that they do not weaken the privacy of the individual. In addition, e.g., if the location information of the device exposes something about the location of its owner, the location information must be presented with sufficient granularity and/or time delay to ensure privacy-preservation in cases where the device is owned or operated by an individual.

Organizations and cloud services must ensure data minimization, so that they only process personal data that is essential for the case and the processing has a valid legal basis. For example, the Installer firm as an organization must only collect and process information about its employees that are directly related to the job at hand. In addition, cloud-based

[19] Who did what and when, and on which asset.

[20] Only collecting information that is needed.

[21] For example, reducing bias and discrimination in hirings or promotions [56].

traffic management solution must not unnecessarily process personal data (e.g. facial images or license plates, that are part of the images, should be removed already on the device-level) that are not essential for the case, but instead should implement measures to prevent the unnecessary processing of personal data.

2) P2 USER CONSENT

User consent (one of the possible legal bases for personal data processing under the EU's General Data Protection Regulation (GDPR) [58]) is often required for personal data processing and "a valid consent must be explicit for data collected and the purpose for the data collection should be stated" [33]. Additionally, "data controllers must be able to collect consent from end-users and consent might be withdrawn" [33]. In this use case, personal data processing occurs within the Installer firm (employees' personal data), in the device (mechanics' personal data), and in the cloud-service (service users' personal data). As such, the only service, where user consent would be the legal basis, is the cloud-service, whereas the legal basis of personal data processing by the Installer firm and within the device is the employment contract of the mechanic. The mechanic's Triplet should offer capabilities for the mechanic to manage his/her own consents by providing consent and allowing revocation of consents.

3) P3 DATA RETENTION

Data retention is a "concept that encompasses all processes for storing and preserving data as well as the specific time periods and policies businesses enforce that determine how and for how long data should be retained" [59]. For natural persons, the data retention processes must ensure individuals' control over their personal data to e.g. remain anonymous when needed, or to control how the individual's personal data can be correlated across digital services (such as the cloud-based traffic monitoring service). The requirements for data retention can be fulfilled, for example, with sufficiently short-lived pseudonymous and anonymous identification of entities.

However, the level of anonymity required in this use case for mechanics is fundamentally a value-based decision. Is there a real need to preserve the actual identity of the mechanic, or would it be enough to ensure that the device was repaired by a certified mechanic? Usually, one major reason for having privacy-preservation in place is to restrict the possibility of large-scale mass surveillance. In the physical world, one may usually meet at most tens or hundreds of people, whereas in the digital world, comprehensive mass surveillance can be easily built if no privacy guarantees are in place. In this use case, it is not necessary to keep the mechanics fully anonymous to mitigate bad maintenance practices. A possible alternative would be to expose anonymous information about the mechanic through the Triplet, while allowing the possibility to reveal, in co-operation with the employer, the identity of the mechanic in exceptional situations (e.g. criminal investigation).

As such, the privacy of the mechanic's identity information should be preserved, while ensuring the ability of the different actors to identify, to a sufficient degree, the counterparts they are interacting with. This requires delicate balancing, and as such, the level of identification is highly contextual considering the need to ensure the anonymity or pseudonymity of individual actors. For instance, the device does not need to be aware of the exact identity of the mechanic, but only of the pseudonymous identification of the mechanic.

4) P4 USE LIMITATION

Personal data processing should be limited to cases in which data are required. For example, the Installer firm should process personal data about its employees only in cases where it is required (i.e. not tracking all movements of the mechanic during the workday). Similarly, the device and cloud-based traffic management service should use the personal data that they process only for implementing the use case in question. Different actors should provide adequate information regarding personal data processing, while ensuring that these limitations are followed in practice.

5) P5 PRIVACY IMPACT ASSESSMENT

When considering compliance with privacy and data protection regulations, the Triplet must be able to provide machine-readable proofs about the existence of an up-to-date and periodically conducted *privacy impact assessment* and the deployment of necessary controls to ensure privacy-preservation. The results of the privacy impact assessment may contain sensitive business-related information, which means that the actual content of the privacy impact assessment must not be published in its entirety.

6) P6 PRIVACY RISK MITIGATION PLAN

Similarly to privacy impact assessments, actors engaging in personal data processing (Installer firm, cloud-service, and camera) need to provide appropriate proof of an existing *privacy risk mitigation plan*. This plan may contain confidential and sensitive information that must be protected appropriately. Privacy risk mitigation plans must be continuously assessed and must ensure that they provide adequate controls to counter threats from the continuously changing privacy threat landscape.

7) P7 PRIVACY MODELS AND POLICIES

End-users engaging in digital transactions with the cloud service, mechanics using the device, and employees of the Installer firm need to be able to understand the privacy models and policies related to personal data processing conducted by these entities. Thus, each entity must be capable of publishing its privacy documentation in a consistent and machine- and human-readable manner through the Semantic Twin. An example of making privacy-policy-related information

available in a standardized and machine-readable manner is the Aries RFC 0430 framework for Machine-Readable Governance Frameworks [60].

8) P8 USE OF PRIVACY STANDARDS

Adherence to privacy standards, such as GDPR [58] and ISO/IEC 27701 [61], is a means for actors to prove e.g. the existence of necessary tools, controls, and processes for privacy-preservation in personal data processing. Compliance usually requires self-assessment or official certification by an independent auditor. An up-to-date self-assessment or an official certification should then be made available by the device, an Installer firm, and a cloud-service through their Semantic Twin.

C. RELIABILITY REQUIREMENTS

Maple et al. [5] defined reliability requirements as ''the ability of the system to perform in a consistent and expected way during a period of time in which it adheres to its performance specifications adequately''.

1) RE1 USER CONTACT POINTS

Triplet users have expectations regarding the sharing of verifiable semantic information about parties engaging in interactions. The ability to identify contact points (e.g. email, reporting portal, or phone number) of e.g. the owner of the traffic monitoring camera or the mechanic, who has conducted device repair, promotes usability and accessibility by allowing users to ensure that the device is in fact one owned by the Helsinki municipality, or maintained by a certified mechanic. Additionally, it would be possible to e.g. report possible incidents, problems, defects, and discrepancies in the traffic monitoring camera or traffic management cloud service to promote e.g. more effective maintenance procedures and quality of service, and reduce downtime.

2) RE2 FRAUD DETECTION AND PREVENTION

Parties engaging in digital interactions expect appropriate measures to be in place to detect and prevent fraud which may lead to e.g. financial loss or identity theft. Fraud prevention may e.g. include mechanisms to ensure that the parties are who they claim to be (e.g. the municipality or the mechanic) and parties to be appropriately notified in cases where fraudulent activity has taken place.[22] Some parties that engage in regulated activities may also have regulatory requirements to counter and detect fraud.

3) RE3 EVIDENCE OF GOVERNMENT APPROVED AUDITS

It must be possible for entities engaging in regulated activities to present proof of certifications that they have undergone to ensure regulatory compliance. This may be enforced, for example, through the need for the camera to undergo regular certifications by an accredited certification body to ensure that the camera produces images with sufficiently high quality. In this use case, the mechanic must undergo a regular certification exam to conduct device repairs. This is especially important considering the trustworthiness of the produced data for end-consumers. Regulatory compliance should also take into account the global scale of Twin-based solutions and their need to support multiple jurisdictions. Based on local regulation, various auditing requirements may also be imposed on the Installer firm (e.g. related to quality or sustainability) or cloud service (e.g. related to financial stability or environmental sustainability).

4) RE4 EVIDENCE OF ASSESSMENTS

Based on regulatory requirements, different entities (e.g. an Installer firm, cloud service, or device) and their Triplets may be required to make available verifiable semantic information e.g. about the security or privacy certifications and assessments of the Triplet. This semantic information should be made available in machine-readable format. Verifiable evidence in question will act as additional regulatory compliance-related proof of the Triplet's trustworthiness.

5) RE5 HANDLING UNEXPECTED TERMINATION OR ACTION

To ensure the reliability and high-availability of the Triplet and the possibility of managing the Semantic and Digital Twins in a scalable manner, the different parts of the Triplet must be loosely coupled.[23] This is needed to e.g. (1) allow replacing a broken device with a new one without the need to provision a new Semantic Twin, (2) to properly manage the situation where the ownership of the device or the cloud service changes, or (3) when the employment contract of the mechanic is terminated.

D. ROBUSTNESS REQUIREMENTS

Maple et al. [5] defined robustness requirements as ''The ability of the system to continue functioning in the presence of internal and external challenges without fundamental or drastic changes to its original operations or state''. Maple et al. also raised the concern that ''There is no globally agreed definition of robustness, and the situation is further blurred by its relationship to resilience and stability''.

1) RB1 EXPECTED OUTCOMES FROM UNEXPECTED INPUTS

While Triplets are expected to be networked, this does not necessarily mean that the Triplets would be open to the Internet; instead, some Triplets (e.g. for industrial IoT devices) may be open only to a local network. However, Triplets of cloud services and organizations (municipality, Installer) are expected to be public, discoverable, and Internet-facing. Since such endpoints have a wider attack surface for possible misuse, it is important to ensure that the Triplets with public and discoverable Internet-facing endpoints continue to operate and provide the expected

[22] Cloud service or municipality can host a contact point to be notified about fraudulent use.

[23] The elements are weakly associated, and changes in one element do not affect the performance of the other elements.

outputs even in exceptional scenarios. This may happen, for example, in cases where the device produces corrupted or invalid information to the traffic-monitoring cloud service, or when an unauthorized person tries to request access from the Installer firm to conduct repairs on the device.

2) RB2 TIMELINESS OF INFORMATION

Triplets must provide a trustworthy and tamper-safe mechanism to present the different claims and attributes of the entities they represent. As such, it must be possible to ensure the timeliness of the claims and attribute information so that they have not been revoked, that they have not expired, and that their information is up-to-date.

The timeliness of claims and attributes is especially important when making authorization decisions about, for example, whether individual entities can perform management activities on the Triplet. Authorization may utilize, for example, ownership-, attribute-, or role-based information in decision-making related to the authorization decision.

Another important situation to consider is the case when the use of the Triplet is impeded, for example, when the device is stolen or lost, or when the traffic monitoring solution is terminated. The decision to revoke claims and attributes associated with the Triplet should be proportional to the associated risk. In some cases (e.g. when using claims for mechanic's access control), it is sufficient to issue claims and attributes with a short lifetime, which restricts their exposure and lowers the risk for misuse [62]. However, in some cases it is important that the claims and attributes are explicitly revoked, for example, in the case that the claims about the municipality contain invalid information that needs to be rectified. One such revocation approach was discussed by Fotiou et al. [63] and can be implemented using e.g. a revocation method described in a W3C draft specification [64].

3) RB3 TOLERANCE OF PROCESS VARIABILITY

Individual parts of the Triplet should be loosely coupled, and therefore, it should be possible to make changes to them independently, without disrupting the overall functioning of the Triplet (e.g. when a physical device is replaced, the mechanic responsible for repairs changes, ownership of the device, or cloud service changes). To observe possible discrepancies in the functioning of the Triplet, it should be possible to monitor their functionality to observe possible errors or malfunctions.

Additionally, it should be possible to observe any unexpected changes in data storage or processing occurring in individual parts of the Triplet. This may be one mechanism for observing possible discrepancies, errors, or malfunctions of the Triplet; for example, in case (1) there is physical failure with the device, (2) the mechanic makes mistakes in the repair, (3) there is a defect in the cloud service business logic, or (4) the Installer firm erroneously grants too wide access to device management.

4) RB4 EVIDENCE OF MAINTAINABILITY

Individual mechanics that conduct maintenance operations may have access to hundreds or thousands of devices and their Triplets. To improve automation and availability of maintenance functionalities, mechanics should be able to effectively discover and have access to machine-readable and well-designed API endpoints through which to e.g. request access to the Triplet management and maintenance functionalities. The same type of automation is also essential for cloud-based services, as automation is essential for ensuring the appropriate security of the service (e.g. through automated installation of software updates).

E. SECURITY REQUIREMENTS

Maple et al. [5] defined security requirements as "The protection of data, information and systems against unauthorized access or modification whether in storage, processing, or transit and against denial of service to authorized entities". Many of the security requirements applicable for Triplets are covered by security requirements criteria frameworks, such as ISO/IEC 27001 [41] or NIST Cybersecurity Framework [42].

1) S1 ACCESS CONTROL

As defined by NIST Cybersecurity Framework [42] requirement *PR.AA*: "Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access". This applies also to Triplets, so that only authorized entities should get access to them.

2) S2 SECURITY ASSESSMENT AND AUDITING

Depending on their risk-posture, the Triplets should demonstrate "evidence on systematic security assessment" [5]. Security assessments and audits are often conducted using standardized tools and methods, such as OSSTMM [65] or OWASP [66]. Triplets should make available machine-readable and verifiable semantic information about the conducted security assessments and audits.

3) S3 AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING

Using authentication, authorization, and accounting (AAA), it should be possible to "Identify all applications and entities in the environment" [5], i.e. to ensure that the entities are who they claim to be. Additionally entities should be assigned access permissions, entitlements, and authorizations following the principles of *least privilege*[24] and *separation of duties*[25] as defined in requirement *PR.AA-05* in NIST Cybersecurity Framework [42].

[24]The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. [67].

[25]No user should be given enough privileges to misuse the system on their own [68].

4) S4 LAYERED SECURITY AND DEFENSE-IN-DEPTH

Requirement for layered security is based on the principle of *defense-in-depth* which integrates ''people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization'' [69]. This means that Triplets can be e.g. protected with layers of administrative, technical, or physical controls [5] to prevent their misuse. Evidence of the use of layered security principles should be part of the security assessments conducted for the Triplets.

5) S5 REGULATORY COMPLIANCE

Regulatory compliance requirements set for different types of Triplets are dependent on the type of Triplet (e.g. Person, Organization), and on the context (e.g. financial sector is more regulated). Generally, Triplets should be able to demonstrate compliance against internal and external requirements, and depending on the type of Triplet, e.g. on ISO/IEC 27001 [41], ISO/IEC 24760 [27], or GDPR [58]. Evidence of compliance should be possible to be presented by the Triplet as verifiable and machine-readable semantic information.

6) S6 CRYPTOGRAPHIC PROTECTION

Cryptographic controls are often used to ensure confidentiality and integrity of data-in-use, data-at-rest, and data-in-transit. They should follow agreed data security policies to ensure that ''data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information'' as defined by requirement *PR.DS* in NIST Cybersecurity Framework [42].

7) S7 MATURITY LEVEL OF SECURITY POLICIES

Entities operating Triplets should be able to assess the maturity of their security policies to continuously improve their security posture. Entities may use security capability maturity models, such as C2M2, to ''evaluate their cybersecurity capabilities and optimize security investments'' [70].

8) S8 VULNERABILITY MANAGEMENT

Entities should consider vulnerabilities in Triplets throughout their entire lifecycle. Vulnerabilities should be ''identified, validated, and recorded'' (requirement *ID.RA-01* [42]), and the ''potential impacts and likelihoods of threats exploiting vulnerabilities'' should be identified and recorded (requirement *ID.RA-04* [42]). Finally, the vulnerabilities should be remediated or mitigated.

9) S9 RISK RESPONSE

Entities operating Triplets should demonstrate ''evidence of security risk management'' and ''compliance with ''relevant standards for cybersecurity risk management'' [5], such as ISO/IEC 27001 [41], NIST Cybersecurity Framework [42]. This requirement is covered e.g. by requirement *GV.OC-01*[26] in NIST Cybersecurity Framework [42].

10) S10 SYSTEMS AND COMMUNICATIONS PROTECTION

Triplets and their communication-means should be protected following a ''protection policy and procedures'' [5]. These policies and procedures may be established e.g. following the principles of requirement *PR.PS* in NIST Cybersecurity Framework [42], which states that ''The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability''.

F. RESILIENCY REQUIREMENTS

Maple et al. [5] defined resiliency requirements as ''The ability of the system to adjust to internal and external conditions by adapting its operations to ensure the continuation of expected service under these new conditions''. Similarly to security requirements, also many of the resiliency requirements applicable for Triplets are covered by security requirements criteria frameworks, such as ISO/IEC 27001 [41] or NIST Cybersecurity Framework [42].

1) RS1 INTERNET-FACE PROTECTION

Triplets exposing publicly-accessible endpoints (e.g. Organizations, Services) should consider applying appropriate measures to protect these endpoints from harmful traffic. Appropriate controls include e.g. network security controls and patch management [5]. The requirement can be fulfilled e.g. following the guidance from NIST Cybersecurity Framework [42] requirement *PR.IR-01*.[27]

2) RS2 INTERNAL SECURITY PROCESSES ENFORCED

Triplets' internal security processes should be understood in order to ensure that appropriate controls and monitoring mechanisms are in place [5]. Monitoring requirements can be adopted e.g. following the guidance from NIST Cybersecurity Framework [42] requirement *DE.CM*.[28] For other controls, guidance from NIST SP 800-53 [71] may be followed.

3) RS3 BACKUP AND DISASTER RECOVERY PLANS

Triplets should consider backups and disaster recovery planning for business-critical data to ensure the continuity of the Triplets' operations. Planning should include defining acceptable downtimes along with the ability to demonstrate verifiable evidence about the necessary actions being taken [5]. Backups are covered by NIST Cybersecurity Framework [42] requirement *PR.DS-11*, whereas disaster

[26] The organizational mission is understood and informs cybersecurity risk management.

[27] Networks and environments are protected from unauthorized logical access and usage.

[28] Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.

recovery planning is covered by an entire section (*RC*) of recovery-related requirements.

4) RS4 CYBER RESILIENCY STRATEGY

NIST SP 800-53 [71] defines resilience as "the ability of an information system to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities, and to recover to an effective operational posture in a time frame consistent with mission needs.". Triplets with strict resiliency requirements should consider defining a cyber-resiliency strategy to ensure that "security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience" (requirement *PR.IR* in NIST Cybersecurity Framework [42]).

5) RS5 BALANCE BETWEEN PREVENTIVE AND DETECTIVE CONTROLS

NIST Cybersecurity Framework [42] sets requirements for both preventive (*PR* - "Safeguards to manage the organization's cybersecurity risks are used") and detective (*DE* - "Possible cybersecurity attacks and compromises are found and analyzed") security controls. Triplets' security should take into account both types of requirements to ensure appropriate level of security for Triplets' functionality.

6) RS6 REACTION TO SECURITY INCIDENTS

Finally, security of Triplets should consider the ability to react to security incidents e.g. by following the requirements from NIST Cybersecurity Framework [42] *RS* requirements category. These requirements ensure the presence of appropriate mechanisms and processes to guarantee that "actions regarding a detected cybersecurity incident are taken".

VII. EFFECT OF DIFFERENT ENTITY TYPES AND LIFECYCLE PHASES

The importance of the studied trustworthiness requirements varies depending on entity type and lifecycle phase of the Triplet. After covering the full list of requirements in the previous section, this section studies how these requirements are applicable to different types of entities and different lifecycle phases. The Triplet's entity type is particularly relevant for the trustworthiness requirements of the Triplet's *external view*, i.e. the services and interfaces exposed by the Triplet, whereas the lifecycle phase affects the *internal view*, i.e. the internal makeup of the Triplet. The two subsections below collectively address RQ2.

A. ENTITY TYPES

The use case discussed in the previous section depicts Triplets for different types of entities:

- Helsinki municipality and Installer (Organizations)
- mechanic (a Person)
- traffic monitoring cloud service (a Service)
- traffic monitoring camera (a Device)

TABLE 4. Trustworthiness requirements pertinent to each entity type.

Req.	Device	Org.	Person	Service
E1	■	■	■	■
E2	■	■		■
E3	■			■
E4	■	■	■	■
E5		■		■
P1	■	■		■
P2			■	■
P3	■		■	■
P4	■	■		■
P5	■			■
P6	■	■		■
P7	■	■		■
P8	■	■		■
Re1	■	■	■	■
Re2		■	■	■
Re3	■	■	■	■
Re4	■	■		■
Re5	■	■	■	■
Rb1		■		■
Rb2	■	■	■	■
Rb3	■	■	■	■
Rb4	■			■
S1	■	■	■	■
S2	■	■	■	■
S3	■	■	■	■
S4	■	■	■	■
S5	■	■	■	■
S6	■	■	■	■
S7	■	■		■
S8	■	■	■	■
S9	■	■		■
S10	■	■	■	■
Rs1		■		■
Rs2	■	■	■	■
Rs3	■	■	■	■
Rs4	■	■		■
Rs5	■	■	■	■
Rs6	■	■	■	■

Table 4 describes the trustworthiness requirements pertinent for each entity type. This section starts by presenting the trustworthiness requirements that are common to all entity types, and then presents the trustworthiness requirements pertinent to the different entity types (Services, Devices, Organizations, Persons). The key requirements for each entity type are summarized in Fig. 6.

1) COMMON REQUIREMENTS

As a general rule, Triplets must have the authority to represent an entity (E1). This capability is needed to counter fraud (Re2) to ensure that the entity is who it claims to be (S3), which may be a mandatory requirement in many regulatory schemes (e.g. Anti-Money Laundering directive [72]). Additionally, it is important to ensure that the entity behind the Triplet is trustworthy, in fact exists, and that it can ensure the timeliness of the provided information (Rb2).

Such assurances should be given by the Triplet by offering access to verifiable evidence about the capabilities of the DT and underlying entity in machine- and human-readable formats. Such evidence may be required e.g. for quality, sustainability, financial stability, and regulatory compliance

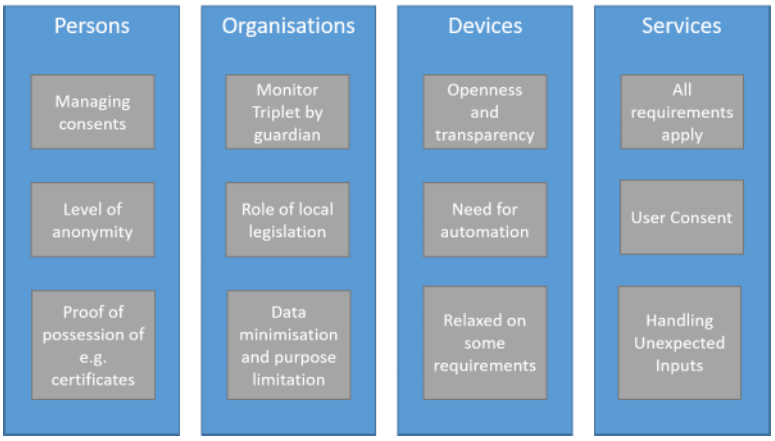

FIGURE 6. Key requirements for each entity type.

(S5). Examples of such verifiable evidence include e.g. semantic information about Privacy Impact Assessments (P5), fulfillment of government approved audits (Re3), or security assessments and audits (S2).

Triplets also require a legal basis for processing personal data. Services are one of the few entity types for which consent (P2) can be considered an appropriate legal basis, and from an individual's point of view, they must have the ability to manage their own consents through their personal Triplet. For Organizations and Devices, the legal basis is usually something other than consent.

Additionally, Triplets must ensure the presence of appropriate preventive and detective controls (Rs5) to protect their data (S6), systems, communications (S10), and internal processing (Rs2). Depending on the case, the controls may be either technical, administrative, or physical (S4), and they should facilitate the continuous identification and remediation of vulnerabilities (S8) posing threats on the Triplets. Finally, the mission-critical data of the Triplets should be protected with necessary backups and ability to restore normal operations in case of a disaster (Rs3).

Moreover, Triplets are the authorized representatives of the entities in the digital realm, and as such, must offer uniform, access-controlled (S1), and well-designed API endpoints for DTs, underlying entities, and their services and capabilities. These are provided by *user contact points* (Re1) that should be used, for example, to report incidents or defects to improve the maintainability and quality of service of the Triplet. User contact points should also be used to notify relevant parties (e.g. device owners as guardians and individuals) about the observed fraudulent activity (Re2). These may, in turn, be used to initiate necessary actions related to security incidents (Rs6).

Finally, to ensure trustworthy operations of the Triplet under unexpected conditions, Triplets should be designed with loose coupling (Re5). Individual parts of the Triplet may be in different states (e.g. due to physical failures, changes in ownership, making mistakes in manual operations), but this should be taken into account in the Triplet design to ensure that it can tolerate this kind of process variability (Rb3).

The coverage of privacy-related requirements is heavily dependent on the type of data processing happening within the Triplet. When personal data is being processed by a third party (such as a Device or a Service), the requirements for privacy are much higher than e.g. in the cases where an individual Person processes his/her own data for own purposes.

2) SERVICES

All the ethics, privacy, reliability, robustness, security, and resiliency requirements listed in Table 4 are applicable to Services. This is understandable as most of the existing trustworthiness requirements categorizations (such as the one by Maple et al. [5]) have been built with digital services and systems in mind.

Moreover, because Services are often exposed through open endpoints, they are susceptible to e.g. hacking and sensitive data leaks. As such, Services' Triplets should be robust enough to be able to handle hacking attempts (Rb1, Rs1) without affecting the normal operations of the Triplet.

3) DEVICES

Types of Devices for which Triplets can be created range, for example, from industrial IoT Devices to personal wearable gadgets. Owing to the wealth of different types of Device setups, it is not relevant for all Devices to offer an appropriate level of inclusivity (E5), be available to all types of user groups, or contain advanced fraud detection capabilities (Re2). Some trustworthiness-related matters can also be relaxed for Devices that are only accessible from local networks that require physical proximity (Rb1, Rs1).

A key factor affecting Device and Service trustworthiness is whether they process personal data, which necessitates openness (E3) and transparency in personal data processing activities. The level of transparency required by Devices and Services differs from Organizations and Persons, as these types of entities are not required to be fully transparent and open about their internal data processing, which might unnecessarily expose confidential information or hinder individuals' privacy.

Finally, considering the key benefit of Triplets in easing the development and deployment of robust Twin-based systems, the need for automation is of particular interest. As the number of Devices increases, the ability to scale automated management of Devices (Rb4) becomes even more important. For this purpose, the Devices must offer an interface for remote management.

4) ORGANIZATIONS

Organizations, similar to Services and Devices, require an actor, who should be able to monitor the Triplet for misuse (E2). This approach differs from Persons' own Triplets where no external monitoring access should be given due to an individual's autonomy and need for privacy (although people with guardians are an exception).

In this use case, the privacy of the mechanic (as an employee of the Installer firm) needs protection. In this case however, the legal basis of employee personal data processing conducted by the Organization Triplet is based on the employment contract and not consent (P2). When dealing with personal data (such as that of employees), Organizations may be forced (due to local regulations) to follow e.g. the principles of non-discrimination, accessibility, and inclusivity (E5).

Privacy and personal data processing in Organizations' Triplets are important because of e.g. the power imbalance between the employer and employee. As such, Organizations should apply data minimization (P1) and use limitation (P4) when processing personal data of their employees to ensure that the privacy needs of the employees are fulfilled. Finally, data retention (P3) is not a major problem, as it is sufficient to assume that in organizations' internal processes, employees can be considered fully correlatable.

Organizations should also consider maturity of their security policies (S7), risk management strategies (S9), and cyber-resiliency strategies (Rs4) to ensure appropriate level of security and resiliency for the data processing activities with the Triplets.

5) PERSONS

Persons should be in control of the personal data processing happening in their own Triplets (again, persons with guardians are the exception). They must be able to control their level of anonymity (pseudonymous or anonymous) (P3) to limit personal data correlation. However, data protection or privacy regulation requirements (P1, P4-P8), and some security-compliance requirements (S7, S9, Rs4) are not applicable in cases where a Person processes personal data for their own personal use (i.e. where the GDPR's household exemption applies [58]). Individuals may, however, need to e.g. take part in regular security trainings (S2) and keep their personal Triplets up-to-date (S8) and backed-up (Rs3) to ensure their secure and resilient operations.

In addition to being in control of their personal Triplets, Persons must be able to manage how they can be discovered. In most cases Persons' Triplets are not expected to host public and discoverable Internet-facing endpoints, and as such, they should be less susceptible to data leaks and hacking by malicious parties (Rb1, Rs1).

Finally, Persons may be working on regulated businesses, and as such, will need the possibility to e.g. prove that they possess certain certifications (Re3, S5). In these cases, it is also important to consider the level of identification (P3) required for the task at hand.

6) SUMMARY

Ethics-related requirements are mostly focused on Devices and Services in the sense that all identified ethics requirements are applicable for these entity types. Persons and Organizations are not required to be fully transparent about their data-processing activities, as they should ensure the appropriate confidentiality and privacy of these activities. However, all entities should be able to produce immutable audit logs and ensure appropriate proofs of the data origin.

Privacy requirements are also fully applicable for Devices and Services; however, the applicability of user consent for Devices depends on the legal basis upon which personal data processing within the Device takes place. For Organizations, some privacy requirements are not seen as applicable, because the legal basis for personal data processing is usually an employment contract. In addition, for Persons, not all privacy requirements are applicable, for example, when individuals process data for personal use.

Reliability is most important for Organizations and Services, because some reliability requirements cannot be imposed on Devices and Persons. This may be due to the limitations of the data processing capabilities of Devices (related to fraud detection and prevention), or to the inability to enforce Persons to conduct security or privacy-related assessments about themselves. All entities should be able to make available contact information about themselves, prove certifications and audits being conducted, and handle unexpected lifecycle events (e.g. terminations or changes in setup).

Robustness is especially relevant for entity types that expose public and discoverable internet-facing endpoints (Organizations and Services), whereas entity types that do not have these types of endpoints can have more relaxed requirements in terms of the ability to process unexpected inputs. Automation is most important for Devices and Services, but also Organizations and Persons can benefit from it. However, all types of entities should be able to ensure the timeliness of the information that they process and their ability to tolerate variability in data processing activities.

Finally, all security and resiliency requirements apply fully to Organizations and Services. Devices and Persons may not need to consider public and discoverable Internet-facing endpoints, if they do not expose such, but need to anyway consider especially the security and resiliency of their internal data processing, storage, and communications. All Triplets should ensure that only authorized entities can access their

functionalities, and that appropriate preventive and detective controls are in place to counter threats against them.

B. LIFECYCLE PHASES

Whereas the previous subsection presented trustworthiness requirements specific to individual entity types, this subsection covers trustworthiness requirements during the different lifecycle phases of the Triplet as summarized in Table 5. Lifecycle is related to the internal characteristics of the Triplet, that is, how different parts of the Triplet are tied to each other. This subsection begins by presenting the common trustworthiness requirements, pertinent to all lifecycle phases. It will then continue to study the requirements of the creation phase (for which all trustworthiness requirements apply), and finally, trustworthiness requirements pertinent to the update and deletion phases are gone through. The key requirements for each lifecycle phase are summarized in Fig. 7.

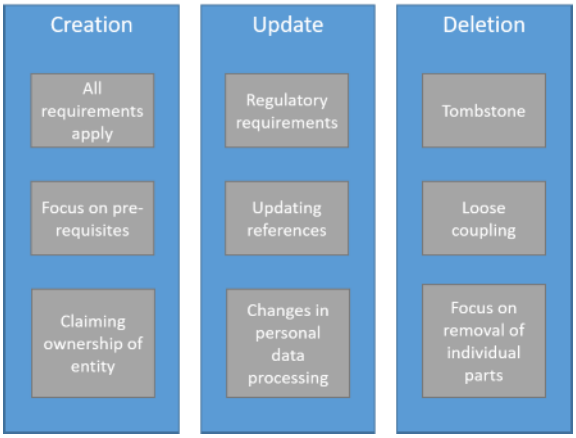

FIGURE 7. Key requirements for each lifecycle phase.

1) COMMON REQUIREMENTS

Triplets change their state through *lifecycle events*, and some requirements need to be considered for all such event types. Cyber attacks or other harmful events may cause issues e.g. related to the integrity or confidentiality of the Triplet, which may lead to the need to conduct investigative operations on the Triplet. For this purpose, an immutable audit trail (E4) must be produced to ensure non-repudiation and traceability. One detective control to mitigate some of the harmful actions is to notify e.g. the guardians of the Triplet through user contact points (Re1) about Triplet lifecycle events (as it might have been initiated by a malicious party) to prevent misuse (E2) and fraud (Re2), and to react to possible security incidents (Rs6).

Keeping Triplet setup up-to-date across lifecycle events may become a daunting task, if done manually. Inconsistencies may also lead to the Triplet going into incoherent state. As such, lifecycle events of Triplets should be conducted in an automated manner (Rb4) to reduce the need for manual operations. This promotes the timeliness of Triplet semantic information (Rb2) along with the ability to tolerate possible variability in processes (Rb3) and to appropriately handle unexpected actions (Re5). Additional resiliency can be achieved through automated backups (Rs3), which ensure the ability to recover e.g. from accidental unwanted changes.

Therefore, it is important that Triplets end up in a stable state as a result of every lifecycle event. This can be achieved by promoting loose coupling between individual Triplet elements, so that discrepancies in individual elements would not make the other parts of the Triplet unusable.

TABLE 5. Trustworthiness requirements pertinent for each lifecycle phase.

Requirement	Creation	Update	Deletion
E1	■	■	
E2	■	■	■
E3	■		
E4	■	■	■
E5	■		
P1	■		
P2	■	■	
P3	■		■
P4	■		
P5	■	■	
P6	■	■	
P7	■	■	
P8	■	■	
Re1	■	■	■
Re2	■	■	■
Re3	■	■	
Re4	■	■	
Re5	■	■	■
Rb1	■	■	
Rb2	■	■	■
Rb3	■	■	■
Rb4	■	■	■
S1	■	■	■
S2	■	■	■
S3	■	■	■
S4	■	■	■
S5	■	■	■
S6	■	■	■
S7	■		
S8	■	■	
S9	■	■	■
S10	■	■	
Rs1	■	■	
Rs2	■	■	
Rs3	■	■	■
Rs4	■		
Rs5	■	■	■
Rs6	■	■	■

2) CREATION

All trustworthiness requirements must be covered in the creation phase of the Triplet lifecycle, while keeping in mind the criticality of the data processing happening in the Triplet. Special emphasis should be given to the possible pre-requisites of Triplet creation, which are dependent on the type of data processing taking place within the Triplet. Most of the requirements related to the pre-requisites are applicable to the entire lifecycle of the Triplet, but they are most important when the Triplet is taken into use. In practice, however, it is possible that Triplets are created in phases, which may mean that not all pre-requisites are fulfilled in the initial phases of the Triplet creation, which impacts the overall trustworthiness of the Triplet.

Triplets that represent entities in high criticality domains may have strict regulatory requirements to ensure their security, privacy-protection, reliability, and resilience. This may require the Triplet to be able to demonstrate the presence of adequate security controls (S4, S6, S10, Rs1), proof of necessary audits (Re3) and assessments (Re4), and the ability to conform to local privacy, data protection, and other regulations (P1-P8, S5).

Proving ownership of the entity is an integral part of the Triplet creation process in order to ensure that the Triplet can, in fact, represent the entity in question. This can be achieved e.g. based on possession of a strong register-based identifier, and as such, to ensure appropriate data provenance (E1) and timeliness of information (Rb2).

3) UPDATE

Significant changes in the internal makeup of the Triplet may lead to a situation, where regulatory requirements force, for example, a re-certification or audit (Re3, S5), or a privacy or security assessment to be conducted (Re4, S2). Updates and changes may also trigger the need to reassess security policies (S7), risk management strategies (S9), or cyber-resiliency strategies (Rs4). Major changes in personal data processing activities also require e.g. that the privacy impact assessment (P5), privacy risk mitigation plans (P6), privacy documentation (P7), and privacy models and standards (P8) are updated. Moreover, user consents (P2) may need to be re-asked.

In addition, updating the internal setup of the Triplet requires updating references in different parts of the Triplet (Semantic Twin, Digital Twin, and entity). It may also be the case that e.g. the newly associated Digital Twin does not have access to the same information that the previous Digital Twin used to have, so it is important that the new Digital Twin is able to claim the necessary information from trusted sources (E1).

Finally, to avoid data leaks and hacking, it is important to detect (E2, Rs5) and prevent (Rb1, Rs5) update events by unauthorized parties (S1, S3), and to ensure that updates to the Triplet setup will not cause problems for the normal operations of the Triplet (Rb3, Re5) e.g. through the introduction of new vulnerabilities (S8).

4) DELETION

The final phase in the lifecycle of the Triplet is the deletion of the associated resources. This may happen so that individual parts of the system are removed or the whole Triplet is removed altogether. Therefore, it is important to discuss how removing individual parts of the Triplet affects its trustworthiness requirements and how the timeliness of its semantic information (Rb2) is guaranteed.

Removing only the Digital Twin would be an appropriate option, for example, in the case that the entity itself continues to function and the Semantic Twin serves the purpose of a *tombstone* for the Digital Twin after it has been removed. It should also be ensured that the entity continues to function even though it has no Digital Twin associated with it. The Triplet functions similarly when the entity itself is removed (with or without the DT being removed). In this case, the ST would act as a tombstone for the entity (and possibly also for the DT).

Removal of the Semantic Twin, which leads to the disappearance of the entire Triplet, must not affect the availability of the consuming services. As such, the Semantic Twin requires loose coupling with the *consuming services* (i.e. services, Triplets, or other entities that use the services and interfaces offered by the Semantic Twin).

Finally, if the entire Triplet is removed in a single operation, the most important point is to ensure that sensitive information that does not need to be retained is removed appropriately to prevent misuse (P3). Appropriate backup and disaster recovery plans (Rs3) are needed to ensure data restoration in case that deletion happens unintentionally.

5) SUMMARY

The creation phase of Triplets is the most critical, as all trustworthiness requirements apply to it. In the update phase it is important to ensure that Triplet data remain up-to-date and are read from trusted sources, and appropriate measures are taken to assess the need for possible re-certifications, audits, or re-assessments of the Triplet due to the change. During the deletion phase, it is important to ensure data cleanup. Common to all phases is the need to detect, track, and act upon authorized changes to ensure robustness and reliability in varying operational conditions, and to implement automation to ensure the maintainability of the Triplets.

VIII. ANALYSIS

This section provides an analysis of the comprehensive set of Triplet trustworthiness requirements for high-risk applications, which are based on a real-world use case, with entity type and lifecycle phase viewpoints. It then provides eleven essential trustworthiness requirements (derived from the analysis) that should be fulfilled by any type of Triplets, even ones used in low-risk use cases. These essential requirements take into account the criticality of the data processing happening in the Triplet, and answer the research question RQ3. This section also studies how individual requirements from the comprehensive list may be solved with Self-Sovereign identities, and which requirements raise a need for additional measures, thus providing an answer to research question RQ4.

A. ANALYSIS OF ENTITY TYPES AND LIFECYCLE PHASES

The analysis revealed that there is no one-size-fits-all approach for Triplet trustworthiness. The Triplet's entity type has a significant impact on trustworthiness requirements and, as such, some requirements become less relevant for some entity types, which allows focusing on trustworthiness requirements that are most relevant to the entity type in question. In addition, analysis of lifecycle phases revealed that trustworthiness should not be treated as an afterthought; instead, it should be ensured that necessary actions have been taken to achieve the correct level of trustworthiness

before the Triplet is created. However, these actions should be balanced based on the criticality of the solution. Altogether, these actions ensure that trustworthiness is not a hindrance for the effective development and deployment of twin-based solutions, but can instead ensure that an appropriate level of trustworthiness is built-in to the solutions.

Furthermore, analyzing trustworthiness requirements reveals several cross-cutting issues across all lifecycle phases and entity types, mostly due to the fact that some capabilities to demonstrate trustworthiness need to be covered throughout the entire lifecycle of Triplets, and some concepts related to security and resiliency are not limited to any particular entity type or domain. These types of requirements include the ability to generate an immutable audit trail (E4), to offer contact points towards the Triplet (Re1), to ensure reliability (Re5) and robustness (Rb3) under varying operational conditions, and to ensure timeliness of the semantic information managed by the Triplet (Rb2). Additionally, several security (S1-S6) and resiliency (Rs3, Rs5-Rs6) requirements also apply to all entity types and lifecycle phases.

Special emphasis should be placed on the creation phase of the Triplet, as all trustworthiness requirements are applicable for this, mostly because it is assumed that capabilities to promote trustworthiness are assumed to be built-in to the Triplets and not incorporated to the solution afterwards. All trustworthiness requirements also apply to Services' Triplets which reflects the notion that existing trustworthiness requirement frameworks have been developed mostly with digital services in mind.

Monitoring capabilities built for Triplets should carefully consider privacy implications, when using them to monitor Triplets for misuse (E2) and fraud (Rb2) in all lifecycle phases. For instance, no external monitoring access should be given to the Triplets of Persons (except those with guardians) to ensure that the individuals are in control of their own Triplets. In addition, the type of data processing taking place within the Triplet and the legal basis on which data processing takes place (e.g. employee data processing is based on employment contract) have a significant impact on the requirements related to transparency and openness (E3), protecting open endpoints (Rs1), inclusivity and accessibility (E5), and privacy (P1-P8).

Moreover, Devices and Services can benefit from a scalable and risk-resilient means for maintainability through automation (Rb4) and presence of an appropriate risk management strategy (S9) in all lifecycle phases.

Finally, Triplet owners are responsible for the necessary actions to demonstrate the trustworthiness of their Triplet, so that third parties can take advantage of them in their own services. Decision-making on trustworthiness can be made easier by offering verifiable proofs to back the claims related to trustworthiness of the Triplet. These verifiable proofs can include e.g. proof of required privacy impact assessments (P5), existence of privacy risk mitigation plans (P6) and privacy documentation (P7), proof of privacy self-assessments or certification (P8), proof of necessary government-approved audits (Re3) and security assessments (Re4), and ensuring the presence of appropriate vulnerability management (S8) and systems and communications protection (S10) practices, and internal security processes (Rs2).

B. ESSENTIAL TRUSTWORTHINESS REQUIREMENTS

The comprehensive trustworthiness requirements list for high-risk applications provided in Section VI allows the study of Triplet trustworthiness from different angles. Within the covered requirements there are, however, some recurring themes that can be summarized to an eleven-point list of *essential trustworthiness requirements* (provided in Table 6) that should be fulfilled by any Triplet-based system requiring at least some level of trustworthiness, thus answering the research question RQ3. This list combines common themes and requirements into a concise set of new and more focused essential requirements that also cover the most important trustworthiness needs of less-critical solutions. For more elaborate trustworthiness requirements handling required by high-critical solutions, it is still necessary to go through the comprehensive trustworthiness requirements listed in Table 3.

C. HOW FAR CAN SSIS SOLVE TRUSTWORTHINESS?

Ensuring the trustworthiness of Triplets is an important aspect to consider when discussing their wide-scale adoption. SSIs offer one way to solve many of the discussed trustworthiness requirements. This subsection presents the extent to which SSIs can be used to solve the comprehensive trustworthiness requirements of Triplets for high-criticality applications, as shown in Table 7, thus addressing RQ4.

SSIs are useful e.g. for identification and ensuring data integrity, but they do not offer other general-purpose IT capabilities, such as monitoring, logging, governance, maintenance, risk management, incident response, or security policy management operations. As such, the following trustworthiness requirements cannot be fulfilled by the deployment of SSIs: monitoring misuse (E2), audit trail (E4), fraud detection and prevention (Re2), handling unexpected termination or action (Re5), expected outcomes from unexpected inputs (Rb1), tolerance of process variability (Rb3), evidence of maintainability (Rb4), risk response (S9), maturity level of security policies (S7), and reaction to security incidents (Rs6). Therefore, dedicated systems should be used instead.

Further, some requirements raise the need for additional measures, such as common monitoring and reporting solutions (E2, E4, Re2), architecture blueprints to ensure robustness (Rb1, Rb3) and reliability (Re5), cyber resilience strategies (Rs4), tooling for automated maintenance, backups, and vulnerability management (Rb4, Rs3, S8); and deployment of dedicated security solutions, controls, and processes (S4, S10, Rs1, Rs2, Rs6). However, through the capabilities of Decentralized Identifiers [28] and Verifiable Credentials [29], it is possible to express identifiers and claims about individual entities such that they are e.g. guaranteed to be issued by a

TABLE 6. Eleven essential trustworthiness requirements for Triplets.

#	Requirement
1	Triplets must be able to produce verifiable, machine- and human-readable proofs and evidence about data processing activities and about the fulfillment of various regulatory (or other) requirements related to e.g. privacy and data protection regulations, security and privacy assessments, government-approved audits, and regulatory compliance.
2	Triplets must track their lifecycle events and produce appropriate immutable audit log for non-repudiation and traceability, along with the ability to monitor lifecycle events for possible misuse.
3	Triplets must offer uniform and well-designed API endpoints as contact points to report to the entity or its guardian about possible defects, malfunctions, or misuse of the Triplet.
4	Triplets must be designed with loose coupling in mind to ensure reliable operations under varying operational conditions and to guarantee that individual parts of the Triplet stay operational irrespective of the state of the parts.
5	Entities must be equipped with tools to influence the level of identification that is deemed necessary in different situations to e.g. have control over correlation and data retention activities.
6	Triplets must strive for automation to keep their internal setup up-to-date and to ensure timeliness of Triplet data.
7	In case the Triplet is tied to a guardian, they should have access to the necessary tooling to monitor and observe the status of the Triplet for any discrepancies, or possible misuse.
8	Triplets must take into account the legal basis on which the data processing is taking place, and in case consents are used, the Persons must be equipped with appropriate tooling to manage the consents that they have given.
9	Triplet creation must carefully consider any possible pre-requisites that may be in place for Triplet creation.
10	Triplet updates must be monitored for unauthorized changes and to ensure that significant changes consider the possible need for re-assessments (e.g. for privacy or security) or re-certifications.
11	Triplets should consider employing appropriate security-criteria frameworks to ensure appropriate level of security and resiliency, depending on the level of criticality of the Triplet.

TABLE 7. Trustworthiness requirements solvable with SSIs.

Requirement	Solvable with SSIs?
E1	x
E2	
E3	x
E4	
E5	x
P1	x
P2	x
P3	x
P4	x
P5	x
P6	x
P7	x
P8	x
Re1	x
Re2	
Re3	x
Re4	x
Re5	
Rb1	
Rb2	x
Rb3	
Rb4	
S1	x
S2	x
S3	x
S4	
S5	x
S6	x
S7	
S8	
S9	
S10	
Rs1	
Rs2	
Rs3	
Rs4	
Rs5	
Rs6	

trusted issuer (E1), are up-to-date and not revoked or expired (Rb2), and offer controls to ensure effective access control (S1) and authentication, authorization, and accounting (S3). Self-Sovereign Identities also take advantage of effective cryptographic measures, and can thus ensure appropriate cryptographic data protection (S6).

Verifiable credentials can also be used as references for documentation of data processing openness and transparency (E3), adherence to inclusivity and accessibility regulations (E5), user contact points (Re1), and evidence of government approved audits (Re3), security assessments (Re4, S2), and regulatory compliance (S5). In addition, most privacy-related documentation required by data protection regulations can be made available in a verifiable manner through verifiable credentials. This documentation includes e.g. details regarding personal data processing use limitations (P4), privacy impact assessments (P5), privacy risk mitigation plans (P6), privacy documentation (P7), and privacy self-assessments and certifications (P8), respectively. Additionally, verifiable credentials can be used to manage user consents and offer consent management capabilities through the ability to give and revoke consents (P2).

Although verifiable credentials are an effective means to ensure the origin and timeliness of the presented claims, they require an additional governance layer to determine e.g. the roles and responsibilities, processes, and common rules that are applicable to the claims in question. Therefore, there is a need for additional *ecosystem governance frameworks* to determine the actual contents and policies associated with verifiable credentials. The key requirements of these ecosystem governance frameworks, compiled from [10] and [73], are listed in Table 8.

Even though SSI concepts are mostly usable for Persons, it is also possible to ensure privacy-preservation for Person-affiliated Devices. Identifiers associated with SSIs also offer the ability to provide anonymous or pseudonymous identification, which is useful for fulfilling e.g. data retention requirements (P3). The entities participating in digital transactions should ensure that they are capable of handling interactions with anonymous or pseudonymous identification to guarantee privacy-preservation of the persons participating in the interactions. Selective disclosure and Zero-Knowledge Proofs[29] (ZKPs) enable data minimization (P1), which has

[29]Protocols allowing one party to demonstrate to another party that a particular statement is true, without revealing any information about the statement itself.

TABLE 8. Key requirements of ecosystem governance frameworks.

#	Requirement
1	Define and adopt interoperability standards to ensure that different solutions can seamlessly interact with each other.
2	Ensure privacy-by-design by mandating the use of privacy-preserving technologies.
3	Establish guidelines to obtain user consent, and to offer granular control over users' data.
4	Enforce strong security measures.
5	Promote decentralization to eliminate central points of control and to enhance resilience against attacks.
6	Specify standards for the use of Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs).
7	Require minimization of personal data collection and emphasize purpose limitation for personal data processing.
8	Ensure compliance to relevant regulations.
9	Define governance structures for decision-making, dispute resolution, and community involvement.
10	Integrate ethical considerations related to the principles of fairness, transparency, and accountability.

been enforced as a guiding principle in many data protection regulations, such as the European General Data Protection Regulation (GDPR) [58].

The benefits of using SSI identities are primarily related to the ability to use a single and well-defined implementation to address multiple trustworthiness requirements. These include, for example, proof-of-origin, timeliness of information, and privacy-preservation. Additionally, SSIs offer a cost-efficient and scalable solution that does not rely on centralized parties. However, in a complex environment with a large number of parties issuing different types of credentials, it may become difficult for cloud providers and other entities to stay up-to-date about who are the parties that produce trustworthy data, which may lead to dependencies on centralized providers of trustworthiness information.

In addition, SSIs cannot anonymize parties if the identifying information is leaked via other channels. Therefore, even though (short-lived) anonymous and pseudonymous identification practically eliminates the ability to correlate individuals' activities, there may still exist additional means for correlation especially when individuals have complex relationships with multiple entities. This may happen, e.g., when a device owner uses multiple devices and correlation occurs, for example, by deducing patterns from device usage.

Altogether, SSIs cover many areas of trustworthiness, and as anonymous identification technology, they have several benefits in ensuring privacy-preservation when comparing against other digital identity technologies. However, SSIs do not solve Triplet trustworthiness by themselves, as additional tools such as architectural blueprints, reference architecture frameworks, and ecosystem governance frameworks are needed to comprehensively address Triplet trustworthiness, and to fulfill the full set of requirements.

IX. DISCUSSION AND FUTURE WORK

Technically, it would be possible to build Triplets without any trustworthiness considerations. However, it is probable that their adoption and use would not expand, as it would not be possible for actors to trust one another when planning to integrate third-party offered Triplets to their solutions. Through the availability of essential trustworthiness requirements, trustworthiness can be offered also for low-risk use cases, which makes it easier to ensure trustworthiness in all types of scenarios and further promote the adoption of Triplet-based technologies as the basis for twin-based solutions.

Trustworthiness is a complex topic that needs to be studied from multiple angles. The comprehensive trustworthiness requirements list in this paper shows that there are at least tens of requirements that need to be considered in a high-risk scenario. Assessing and evaluating even an individual trustworthiness requirement may be a laborious task. Triplets promote automation at the very best, but automation is needed also in the evaluation and assessment of Triplet trustworthiness. This would be an interesting area for future research, i.e. to study the capabilities to automate the trustworthiness evaluations of Triplets.

SSI technologies can still be seen as a viable technology to demonstrate many aspects of trustworthiness. Study of Triplet trustworthiness has shown that there is a need to publish a vast amount of structured and unstructured information about Triplet trustworthiness, which necessitates improved ability to semantically model this information. Therefore, it would be important to study the possibilities of utilizing existing semantic technologies to model Triplet trustworthiness information in an effective manner.

Future work on Triplet trustworthiness will include studies on the effective use of attestation of verifiable data about different entities, such as accreditations by certification bodies about the trustworthiness of device measurements, or credentials issued to a mechanic to perform certain installations or configurations. In addition, discovery mechanisms, such as GS1 links and QR codes, could make accessing the correct twins more convenient, but assuring that the linkage is trustworthy requires further work. Finally, an interesting area for future research would be to study how licensing, payments, and other types of access restrictions should be managed in a complex Twin-based environment.

A key limitation of this paper is that it does not attempt to provide a thorough empirical validation of the proposed model, but instead uses a representative use case to study Triplet trustworthiness. Evaluating the model with additional use cases of different types provides an opportunity for future research.

X. CONCLUSION

This study has provided us with a comprehensive baseline of trustworthiness requirements for Triplets, which ensures trustworthiness for high-risk applications through a holistic approach. This solves the shortcomings of previous studies covered in Section IV by providing multiple trustworthiness categories, viewpoints for different types of entities, and being technology-agnostic. The original set of requirements by Maple et al. [5] needed to be adapted to meet the requirements of Triplets, and a closer study of the requirements revealed that some requirements become irrelevant for some types of Triplets and lifecycle phases. There is

also redundancy and overlap between the requirements; as such, it is useful to primarily focus on the most essential ones first, especially when dealing with low-risk Triplet use cases. These eleven essential trustworthiness requirements for Triplets were presented in Section VIII.

In addition, the paper has shown that it is possible to use a real-world use case as a basis to analyze trustworthiness requirements pertinent to critical Triplet-based systems of different entity types and lifecycle phases. The result of the analysis identified some cross-cutting trustworthiness requirements applicable for all entity types and lifecycle phases, such as audit logging, reliability and robustness under varying operational conditions, and the need to ensure timeliness of the data managed by the Triplet. Differences were identified in terms of entity type and lifecycle phase, particularly considering privacy requirements, support for automation, monitoring for misuse and fraud, and the need to publish verifiable semantic information through the Semantic Twin.

SSIs solve many of the trustworthiness requirements, particularly related to data provenance and timeliness, privacy-preservation, and the ability to present verifiable proofs about the capabilities of the Triplet, but in addition to SSIs, there is a need for architectural blueprints, reference architecture frameworks, ecosystem governance frameworks, and other governance methods to comprehensively cover the trustworthiness requirements of Triplets.

ACKNOWLEDGMENT

The authors would like to thank Juuso Autiosalo for his valuable comments during the writing process.

REFERENCES

[1] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-Khah, and P. Siano, "IoT-based smart cities: A survey," in *Proc. IEEE 16th Int. Conf. Environ. Electr. Eng. (EEEIC)*, Jun. 2016, pp. 1–6.

[2] S. Funabashi, A. Schmitz, S. Ogasa, and S. Sugano, "Morphology specific stepwise learning of in-hand manipulation with a four-fingered hand," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 433–441, Jan. 2020.

[3] Q. Qi, F. Tao, T. Hu, N. Anwer, A. Liu, Y. Wei, L. Wang, and A. Y. C. Nee, "Enabling technologies and tools for digital twin," *J. Manuf. Syst.*, vol. 58, pp. 3–21, Jan. 2021.

[4] J. Autiosalo. (2022). *Guide to Semantic Twins*. [Online]. Available: https://docs.google.com/document/d/e/2PACX-1vQOR2BJj2J_SpFQjNlAFqlGI7lIKiNzs_JkgINweuhIxTtez82LcBSyvnU65Akf5JAbBDPgrifYCppi/pub

[5] C. Maple, G. Epiphaniou, and N. Gurukumar, "Facets of trustworthiness in digital identity systems," Tech. Briefing, Alan Turing Inst., London, U.K., Tech. Rep., 2021. [Online]. Available: https://www.turing.ac.uk/sites/default/files/2021-05/technical_briefing-facets_of_trustworthiness_in_digital_identity_systems.pdf

[6] J.-H. Cho, S. Xu, P. M. Hurley, M. Mackay, T. Benjamin, and M. Beaumont, "STRAM: Measuring the trustworthiness of computer-based systems," *ACM Comput. Surveys*, vol. 51, no. 6, pp. 1–47, Nov. 2019.

[7] U. Der, S. Jähnichen, and J. Sürmeli, "Self-sovereign identity—Opportunities and challenges for the digital revolution," 2017, *arXiv:1712.01767*.

[8] *CSRC Glossary, Data Provenance*. Accessed: 2024. [Online]. Available: https://csrc.nist.gov/glossary/term/data_provenance

[9] *CSRC Glossary, Data Governance*. Accessed: 2024. [Online]. Available: https://csrc.nist.gov/glossary/term/data_governance

[10] J. Langford, A. Poikola, W. Janssen, V. Lähteenoja, and M. Rikken, "Understanding MyData operators," MyData Global, Helsinki, Finland, Tech. Rep., 2020. [Online]. Available: https://www.mydata.org/wp-content/uploads/2022/07/Understanding-MyData-Operators-2022-1.pdf

[11] M. Grieves, "Digital twin: Manufacturing excellence through virtual factory replication," Zenodo, CERN, White Paper, vol. 1, no. 2014, pp. 1–7, 2014.

[12] B. R. Barricelli, E. Casiraghi, J. Gliozzo, A. Petrini, and S. Valtolina, "Human digital twin for fitness management," *IEEE Access*, vol. 8, pp. 26637–26664, 2020.

[13] R. Saracco, J. Autiosalo, D. de Kerckhove, F. Flammini, and L. Nisiotis, "Personal digital twins and their role in epidemics control," Inst. Elect. Electron. Eng. (IEEE), USA, An IEEE Digital Reality White Paper, Apr. 2020.

[14] G. Pappas, J. Siegel, and K. Politopoulos, "VirtualCar: Virtual mirroring of IoT-enabled avacars in AR, VR and desktop applications," in *Proc. Eurographics Symp. Virtual Environments*. The Netherlands: The Eurographics Association, 2018.

[15] J. E. Siegel, "CloudThink and the Avacar: Embedded design to create virtual vehicles for cloud-based informatics, telematics, and infotainment," Ph.D. dissertation, Massachusetts Inst. Technol., Cambridge, MA, USA, 2013.

[16] R. Parmar, A. Leiponen, and L. D. W. Thomas, "Building an organizational digital twin," *Bus. Horizons*, vol. 63, no. 6, pp. 725–736, Nov. 2020.

[17] *API Design*. Accessed: 2024. [Online]. Available: https://www.postman.com/api-platform/api-design/

[18] J. Autiosalo, J. Siegel, and K. Tammi, "Twinbase: Open-source server software for the digital twin Web," *IEEE Access*, vol. 9, pp. 140779–140798, 2021.

[19] D. Yang, H. R. Karimi, O. Kaynak, and S. Yin, "Developments of digital twin technologies in industrial, smart city and healthcare sectors: A survey," *Complex Eng. Syst.*, vol. 1, no. 1, p. 3, 2021.

[20] H. Hassani, X. Huang, and S. MacFeely, "Impactful digital twin in the healthcare revolution," *Big Data Cognit. Comput.*, vol. 6, no. 3, p. 83, Aug. 2022.

[21] G. P. Sellitto, M. Masi, T. Pavleska, and H. Aranha, "A cyber security digital twin for critical infrastructure protection: The intelligent transport system use case," in *Proc. IFIP Work. Conf. Pract. Enterprise Modeling*. Cham, Switzerland: Springer, 2021, pp. 230–244.

[22] G. Zachos, G. Mantas, I. Essop, K. Porfyrakis, J. M. C. S. Bastos, and J. Rodriguez, "An IoT/IoMT security testbed for anomaly-based intrusion detection systems," in *Proc. IFIP Netw. Conf. (IFIP Netw.)*, Jun. 2023, pp. 1–6.

[23] S. Masiero and S. Bailur, "Digital identity for development: The quest for justice and a research agenda," *Inf. Technol. Develop.*, vol. 27, no. 1, pp. 1–12, Jan. 2021.

[24] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines," *NIST Special Publication*, vol. 800, pp. 3–63, Jun. 2017.

[25] K. Cameron, "The laws of identity," *Microsoft Corp*, vol. 12, pp. 8–11, May 2005.

[26] C. Allen, "The path to self-sovereign identity," *Life Alacrity*, Apr. 2016. [Online]. Available: https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/

[27] *It Security and Privacy—A Framework for Identity Management—Part 1: Terminology and Concepts*, Standard ISO/IEC 24760-1:2019, 2019.

[28] M. Sporny, D. Longley, M. Sabadello, R. Drummond, O. Steelie, and C. Allen, "Decentralized identifiers (dids)-core architecture, data model, and representations v1. 0. 2021," W3C, Tech. Rep. Decentralized Identifiers (DIDs)v1.0, W3C Recommendation, Jul. 2022.

[29] M. Sporny, G. Noble, D. Longley, D. C. Burnett, B. Zundel, and K. Den Hartog. (2022). *Verifiable Credentials Data Model 1.1: Expressing Verifiable Information on the Web*. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[30] *Passkeys (Passkey Authentication)*. Accessed: 2024. [Online]. Available: https://fidoalliance.org/passkeys/

[31] A. Vasilyev, G. Bullegas, O. Nachawati, M. Elaasar, and S. Jenkins, "Developing an open platform for democratised MBSE," Eur. Spage Agency, France, Tech. Rep., 2022.

[32] E. Eckstädt, K. Menzel, H. Pruvost, and D. Mayer, "Representing modelica models as knowledge graphs using the MoOnt ontology," in *Proc. Eur. Council Comput. Construct. Conf.*, vol. 4, Jul. 2023, pp. 1–8.

[33] E. Z. Tragos, J. B. Bernabe, R. C. Staudemeyer, J. L. H. Ramos, A. Fragkiadakis, A. Skarmeta, M. Nati, and A. Gluhak, "Trusted IoT in the complex landscape of governance, security, privacy, availability and safety," in *Digitising the Industry Internet of Things Connecting the Physical, Digital and VirtualWorlds*. Denmark, Europe: River Publishers, 2022, pp. 185–214.

[34] C. Alcaraz and J. Lopez, "Digital twin: A comprehensive survey of security threats," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 1475–1503, 3rd Quart., 2022.
[35] V. Damjanovic-Behrendt, "A digital twin-based privacy enhancement mechanism for the automotive industry," in *Proc. Int. Conf. Intell. Syst. (IS)*, Sep. 2018, pp. 272–279.
[36] J. Voas, P. Mell, and V. Piroumian, "Considerations for digital twin technology and emerging standards," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 8356, 2021.
[37] L. Wright and S. Davidson, "How to tell the difference between a model and a digital twin," *Adv. Model. Simul. Eng. Sci.*, vol. 7, no. 1, pp. 1–13, Dec. 2020.
[38] D. Lee, S. H. Lee, N. Masoud, M. S. Krishnan, and V. C. Li, "Integrated digital twin and blockchain framework to support accountable information sharing in construction projects," *Autom. Construct.*, vol. 127, Jul. 2021, Art. no. 103688.
[39] J. Trauer, S. Schweigert-Recksiek, T. Schenk, T. Baudisch, M. Mörtl, and M. Zimmermann, "A digital twin trust framework for industrial application," *Proc. Design Soc.*, vol. 2, pp. 293–302, May 2022.
[40] S. Khan, M. Farnsworth, R. McWilliam, and J. Erkoyuncu, "On the requirements of digital twin-driven autonomous maintenance," *Annu. Rev. Control*, vol. 50, pp. 13–28, Jan. 2020.
[41] *Information Security Management Systems*, Standard ISO/IEC 27001, 2022.
[42] *NIST Cybersecurity Framework*, Nat. Inst. Standards Technol., USA, 2018.
[43] T. Deng, K. Zhang, and Z.-J. Shen, "A systematic review of a digital twin city: A new pattern of urban governance toward smart cities," *J. Manage. Sci. Eng.*, vol. 6, no. 2, pp. 125–134, Jun. 2021.
[44] M. Dietz, B. Putz, and G. Pernul, "A distributed ledger approach to digital twin secure data sharing," in *Proc. IFIP Annu. Conf. Data Appl. Secur. Privacy*. Cham, Switzerland: Springer, 2019, pp. 281–300.
[45] B. Putz, M. Dietz, P. Empl, and G. Pernul, "EtherTwin: Blockchain-based secure digital twin information management," *Inf. Process. Manage.*, vol. 58, no. 1, Jan. 2021, Art. no. 102425.
[46] *Trusted Twin*. Accessed: Sep. 2023. [Online]. Available: https://trustedtwin.com/
[47] *Citopia Self-Sovereign Digital Twins*. Accessed: Sep. 2023. [Online]. Available: https://dlt.mobi/self-sovereign-digital-twins/
[48] *Testbed for Smart Mobility*. Accessed: 2022. [Online]. Available: https://mobilitylab.hel.fi/
[49] *Urban Digital Twin Supports Living Lab Activities*. Accessed: Feb. 2022. [Online]. Available: https://iot-ngin.eu/index.php/2022/02/16/urban-digital-twin-supports-living-lab-activities/
[50] I. Makhdoom, M. Abolhasan, D. Franklin, J. Lipman, C. Zimmermann, M. Piccardi, and N. Shariati, "Detecting compromised IoT devices: Existing techniques, challenges, and a way forward," *Comput. Secur.*, vol. 132, Sep. 2023, Art. no. 103384.
[51] T. A. Coleti, M. Morandini, L. V. L. Filgueiras, P. L. P. Correa, I. G. de Oliveira, and C. R. S. C. de Barbosa, "Design patterns to support personal data transparency visualization in mobile applications," in *Proc. 21st HCI Int. Conf. Hum.-Comput. Interact. Perspect. Design, Thematic Area (HCI HCII)*, Orlando, FL, USA. Cham, Switzerland: Springer, Jul. 2019, pp. 46–62.
[52] N. Antunes, L. Balby, F. Figueiredo, N. Lourenco, W. Meira, and W. Santos, "Fairness and transparency of machine learning for trustworthy cloud services," in *Proc. 48th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, Jun. 2018, pp. 188–193.
[53] A. Lehmann. *Privacy-Enhancing Technologies: DAA, Anonymous Credentials & Pseudonym Systems*. Accessed: 2017. [Online]. Available: https://www.cosic.esat.kuleuven.be/ecrypt/csa/bristol/Complex/Anja Lehmann.pdf
[54] E. Shahat, C. T. Hyun, and C. Yeom, "City digital twin potentials: A review and research agenda," *Sustainability*, vol. 13, no. 6, p. 3386, Mar. 2021.
[55] S. Giorgi, R. Hueting, A. Capaccioli, F. di Ciommo, G. Rondinella, A. Kilstein, I. Keseru, S. Basu, H. Delaere, W. Vanobberghen, and M. Bánfi, "Improving accessibility and inclusiveness of digital mobility solutions: A European approach," in *Proc. Congr. Int. Ergonom. Assoc.* Cham, Switzerland: Springer, 2021, pp. 263–270.
[56] H. Pascual, X. M. Bruin, A. Alonso, and J. Cerdà, "A systematic review on human modeling: Digging into human digital twin implementations," 2023, *arXiv:2302.03593*.
[57] J. S. Davis and O. Osoba, "Improving privacy preservation policy in the modern information age," *Health Technol.*, vol. 9, no. 1, pp. 65–75, Jan. 2019.
[58] *Regulation (EU) 2016/679 of the European Parliament and of the Council*, Eur. Parliament Council, vol. 679, 2016, p. 2016.
[59] *Techtarget Data Backup, Data Retention Policy*. Accessed: 2024. [Online]. Available: https://www.techtarget.com/searchdatabackup/definition/data-retention-policy
[60] D. Hardman *Machine-Readable Governance Frameworks*, document Aries RFC 0430, Feb. 2020.
[61] *Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management—Requirements and Guidelines*, Standard ISO/IEC 27701:2019, 2019.
[62] K. Karvonen, Y. Kortesniemi, and A. Latva-Koivisto, "Evaluating revocation management in SPKI from a user's point of view," in *Proc. Hum. Factors Telecommun.*, Bergen, Norway, 2001, pp. 1–9.
[63] N. Fotiou, V. A. Siris, G. C. Polyzos, Y. Kortesniemi, and D. Lagutin, "Capabilities-based access control for IoT devices using verifiable credentials," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2022, pp. 222–228.
[64] D. Longley and M. Sporny, "Revocation list 2020, a privacy-preserving mechanism for revoking verifiable credentials," Revocation list 2020, W3C, Tech. Rep. Revocation List 2020, Draft Community Group Report, Apr. 2021.
[65] P. Herzog, "OSSTMM 3—The open source security testing methodology manual," Inst. Secur. Open Methodol. Announces, Spain, Tech. Rep. OSSTMM 3, 2010, p. 15.
[66] A. Müller and M. Meucci, "OWASP testing guide," OWASP, USA, Tech. Rep. OWASP Testing Guide 4.0, 2014.
[67] *CSRC Glossary, Least Privilege*. Accessed: 2024. [Online]. Available: https://csrc.nist.gov/glossary/term/least_privilege
[68] *CSRC Glossary, Separation of Duty (SOD)*. Accessed: 2024. [Online]. Available: https://csrc.nist.gov/glossary/term/separation_of_duty
[69] *CSRC Glossary, Defense-in-Depth*. Accessed: 2024. [Online]. Available: https://csrc.nist.gov/glossary/term/defense_in_depth
[70] *Cybersecurity Capability Maturity Model (C2M2)*. Accessed: 2022. [Online]. Available: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
[71] *NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations*, Nat. Inst. Standards Technol., USA, 2020.
[72] *Directive (EU) 2015/849 of the European Parliament and of the Council*, Directive, Eur. Parliament Council, vol. 849, 2015, p. 2015.
[73] A. Badirova, B. Alangot, T. Dimitrakos, and R. Yahyapour, "Towards robust trust frameworks for data exchange: A multidisciplinary inquiry," in *Open Identity Summit 2024*. Bonn, Germany: Gesellschaft für Informatik, 2024, pp. 15–26.

TEEMU P. KÄÄRIÄINEN received the M.Sc. (Tech.) degree from Aalto University, in 2010, where he is currently pursuing the Ph.D. degree. He was a Ph.D. Researcher with Aalto University in the EU H2020 IoT-NGIN project. His research interests include decentralized digital identity methods, privacy-preserving technologies, and their governance models.

YKI KORTESNIEMI received the M.Sc. (Tech.) degree in industrial management and the Lic.Sc. (Tech.) degree in computer science from Helsinki University of Technology, Finland, in 1998 and 2003, respectively, and the D.Sc. (Tech.) degree in networking technology from Aalto University, Finland, in 2015.

He has worked on numerous research projects with Helsinki University of Technology and Aalto University, including the EU H2020 projects SOFIE, PHOENIX, and IoT-NGIN. His research interests include information security and privacy, MyData and legal design, the Internet of Things, distributed ledgers and blockchains, and decentralized identifiers and verifiable credentials.