Published in final edited form as:

J Comput Inf Sci Eng. 2019 ; 19(4): . doi:10.1115/1.4042839.

Method for enabling a root of trust in support of product-data certification and traceability

Thomas D. Hedberg Jr.*,

National Institute of Standards and Technology Gaithersburg, Maryland 20899

Sylvere Krima,

Engisis LLC Bethesda, Maryland 20817

Jaime A. Camelio

Grado Department of Industrial and Systems Engineering Virginia Tech Blacksburg, Virginia 24061

Abstract

Trust in product-data quality (PDQ) is critical to successful implementation of model-based enterprise (MBE). Such trust does not extend to the exchange and reuse of three-dimensional (3D)-product models across the product lifecycle because verifiable traceability in product data is lacking. This assurance is especially crucial when “siloe” manufacturing functions produce product data that is not fully interoperable and thus requires frequent reworking to enable reuse. Previous research showed how Public Key Infrastructure (X.509-PKI) from the X.509 standard could be used to embed digital signatures into product data for the purposes of certification and traceability. This paper first provides an overview and review of technologies that could be integrated to support trust throughout the product lifecycle. The paper then proposes a trust structure that supports several data-transaction types. Next, the paper presents a case study for common configuration management (CM) workflows that are typically found in regulated industries. Finally, the paper draws conclusions and provides recommendations for further research for enabling the product lifecycle of trust (PLOT).

Keywords

Trustworthiness; Authentication; Authorization; Product-Data Quality (PQD); CAD/CAM/CAE; Model-Based Enterprise (MBE); Private Key Infrastructure (PKI)

*Corresponding Author, tdh1@nist.gov.

Publisher's Disclaimer: Disclaimers

The work presented in this paper is an official contribution of the National Institute of Standards and Technology (NIST) and not subject to copyright in the United States. Certain commercial systems are identified in this paper. Such identification does not imply recommendation or endorsement by NIST. Nor does it imply that the products identified are necessarily the best available for the purpose.

1. Introduction

Several software markets in the manufacturing sector, computer-aided design (CAD) in particular, are undergoing rapid evolution with the introduction of cloud, social, and mobile technology [1]. Evolving software technologies coupled with the trend [2, 3, 4] of digital and globally distributed manufacturing systems makes ensuring effective, efficient, and trusted product-data traceability an increasing challenge. Processes across the product lifecycle domains (e.g., engineering, manufacturing, quality assurance, sustainment) are often independent and disconnected – resulting in product-data traceability requiring a significant amount of human resources. Industry is shifting operations towards the concept of model-based enterprise (MBE) by changing the communication of product definitions and specifications from two-dimensional (2D) drawings (i.e., paper) to three-dimensional (3D) product representations (i.e., CAD models) [5].

The trends and challenges associated with the digital transformation of manufacturing increase the importance of product-data traceability and trustworthiness. Ensuring the necessary data is used by the correct function / role at the appropriate time is paramount, especially in regulated industries. This requires the ability to know that data being used is the correct type and version, is authorized for the intended usage, and came from the expected data owner / sender. In 2014, GrabCAD¹ surveyed [6] their current user base (at the time, over one-million users) to determine the most frustrating time-wasters in CAD collaboration. 75 percent of the survey respondents said they wasted time fabricating a prototype or production part using the wrong version of data. Other shocking statistics from the survey are: 80 percent of respondents spend time each month reconciling data versions because users were unaware of changes and 39 percent of respondents missed delivery dates waiting on data verification from their customer. It is the authors' opinion that the survey results point to a practical breakdown in the configuration management (CM) process.

Industry needs a dynamic way to trace and trust product data effectively and efficiently. Previous research [7] shows how Public Key Infrastructure (X.509-PKI) from the X.509 standard [8] could be used to embed digital signatures into product data for the purposes of data certification and traceability. This paper will provide a review of technology that could be integrated to build trust throughout the product lifecycle. Then, the paper will propose a trust methodology supported by a structure and governance policy. Next, the paper will present a reference implementation and case study for common CM workflows typically found in regulated industries. Finally, the paper will draw conclusions and provide recommendations for further research to enable the product lifecycle of trust.

2. Background

2.1. Trustworthiness and Traceability

Data trustworthiness is important to managing relationships across the product lifecycle because poor data quality, out-dated data, or incorrect data causes disruptions and waste in manufacturing operations. To operate effectively, customers and suppliers must trust the data

¹An online community of professional engineers, designers, manufacturers, and STEM students, <https://grabcad.com/>

they exchange. Trustworthiness includes security, privacy, safety, reliability, and resilience [9].

Tracing dependency links across the product lifecycle and in supply chains supports establishing trusted relationships between those entities [10]. Data traceability is a critical quality attribute intended to ensure system outputs conform to stakeholder requirements [11, 12]. Traceability is defined as the ability to discover the history of decisions in the lifecycle, to control the quality of data, products, and processes, and to understand the relationship between assets [13, 10, 11, 12, 14]. Manufacturers in both regulated and non-regulated industries value data authentication (e.g., what is the data, what is the provenance of the data) and authorization (e.g., who can use the data, how the data can be used) as pillars to traceability in their effort to reduce product-liability exposure within supply chains and in the public realm [7].

2.2. Regulatory Needs

Regulated industries are those that must comply with a government mandate and/or law. Examples of regulated industries are Aerospace (regulated by the Federal Aviation Administration (FAA)), Medical (regulated by the Food and Drug Administration (FDA)), and Consumer Products (regulated by the Consumer Product Safety Commission (CPSC)). Although, non-regulated industries do not have such mandates, they often voluntarily self-regulate through the use of consensus-based standards and testing methods. Examples of standards and testing methods are those produced by American Society of Mechanical Engineers (ASME) and Underwriters Laboratory.

The traceability process is often done with significant human capital and minimal-to-no automation [7]. For example, in the regulated U.S. aerospace industry, the FAA requires that aerospace manufacturers define a plan and receive FAA approval for managing and maintaining electronic design data (e.g., 3D CAD models, digital parts lists) used in the certification process [15]. Then, a parts manufacturer must, “[determine] the quality, eligibility, and traceability of aeronautical parts and materials intended for installation on U.S. type-certificated products and articles,” to ensure compliance with applicable regulations [16]. If the manufacturer cannot provide traceable evidence that the applicable requirements were followed, then the FAA has the authority to halt production operations and to ground affected aircraft. Therefore, industry must remain cognizant of the steep consequences of poor traceability.

While industry must focus on traceability and deploy processes to manage their operations in accordance to requirements, the significant human capital burden can no longer remain the generally accepted practice. Industry, whether regulated or not, needs methods and technology to supplement the human resources assigned to ensuring effective and efficient management of data trustworthiness and traceability.

2.3 Lifecycle Information Framework and Technology

Hedberg et al. [17] proposed the conceptual lifecycle information framework and technology (LIFT) to address industry’s problem of connecting the disparate systems, data, and information repositories that exist across the product lifecycle. The goal is to support

cultivating information for decision support and to enable the application of control mechanisms to the lifecycle. The framework consists of three layers: (1) product-lifecycle data, (2) data certification and traceability, and (3) data-driven applications.

The first layer of the framework, product lifecycle, comprises (for purposes of this paper) design, analysis, manufacturing, quality assurance, and customer and product support. Design data must be approved by a person with the appropriate authority, certified by confirming the data is what it is declared to be, and accompanied by authorization specifying how the data may be used. The analysis phase of the lifecycle assesses a product specification using computer-aided engineering (CAE) tools (e.g., simulation-based finite-element analysis (FEA) and computational fluid dynamics (CFD)). The manufacturing phase is where a product is fabricated. The quality assurance phase deals with the inspection and measurement of a product. Lastly, the customer and product support phase manages the end-user support through maintenance services, technical publications, and other support activities. Each of these phases has its own set of data that it maintains for recording-keeping, but the data would benefit other phases of the lifecycle, too. However, linking the data today is difficult and requires significant human capital because the data is created in disparate systems, uses different formats, and is stored in different locations.

In the middle of the framework is the Data Certification and Traceability layer, which supports building trust throughout the product lifecycle. As products progress through lifecycle phases, different requirements move in and out of focus. Because these requirements from different phases often contradict or compete with each other, it can be challenging for organizations to manage and understand them, and to apply them effectively. Misunderstanding and/or not complying with all the requirements leads to distrust of the data.

The last layer of the framework is the data-driven applications layer, which supports integrating applications using plug-and-play like methods. Initially, the framework would include applications to support domain-specific knowledge management, decision support, requirements management, diagnosis, prognosis, and control.

2.4. Digital Manufacturing Certificates

This subsection describes previous work [7, 18] to develop a digital manufacturing certificates (DMC) toolkit. The toolkit supports digital signing and embedding X.509-PKI certificates [19] into several open-data formats used in manufacturing: (1) ISO 10303–242:2014 (STEP AP24) [20], (2) ISO 6983–1:2009 (G-Code) [21], (3) American National Standards Institute (ANSI) / Dimensional Metrology Standards Consortium (DMSC) Quality Information Framework (QIF) [22], and the combined standards of Portable Document Format (PDF) [23] and Product Representation Compact (PRC) [24] to form a 3D PDF. People and systems can use the toolkit to digitally sign data using either a single- or multi-path signature hierarchy (see Figure 1).

In single-path hierarchies, each signer must vouch for all the previous signatures. Mandatory vouching raises legal issues and sets contradictory constraints when data must be legally signed and endorsed by multiple actors from different organizations along the product

lifecycle. In multi-path hierarchical signing, a new signature does not have to vouch for the previous signature in the file and multiple organizations can sign the same data while vouching only for signatures they choose. Signatories may also choose to vouch only for the data, and not for other signatures.

Our previous work [7, 18] provided a foundation for using existing digital-certificate standards and technology in manufacturing to support authentication, authorization, and traceability. However, the work did not provide a recommendation for what metadata should be required to be embedded in the product data during the signing process, nor did the work provide recommendations on trust structures, hierarchies, and governance policies. The goal of this paper is to supplement the previous work with recommendations for the required structures and governance to enable trustworthy exchange of product data.

3. Trust Methodology

Trust is built on relationships. While federating trust forms more of a graph than a tree when visualized, trust still requires some structure and hierarchy to be effective and efficient. We recommend the three-tier hierarchy shown in Figure 2 to support explicit and implicit trust relationships. The top level of the trust structure is an authority level, the second is a service level, and the third is a data level. Using this type of structure would enable a trust environment based on authorization, authentication, and traceability as discussed in [7].

The authority level should not be considered the root certificate authority (CA). Instead, the authority level is an inter-mediate CA that has its certificates signed by a root CA and has the authority to sign certificates for entities the authority level chooses to trust. This approach aligns with X.509-PKI practices used today with digital signatures and Transport Layer Security (TLS) / Secure Sockets Layer (SSL) on the Internet. Visualized in Figure 3, a chain of trust begins with a root CA and links to the authority level, then to the service level, and finally to the data level.

Entities in the authority level act as an audit service – reviewing and certifying the service level entities. The ISO 9001 [25] audit process is a type of authority that could use digital certificates to create a chain of trust to provide evidence that an organization is ISO 9001 certified and to trace back to who certified the organization. Authority-level entities also include regulatory agencies (e.g., FAA, FDA), standards-accreditation organizations (e.g., International Standards Organization (ISO), ANSI), standards-development organizations (e.g., ASME, American Society for Testing and Materials (ASTM)), and manufacturers (e.g., Boeing Company certifying suppliers to their D6–51991 [26] quality specification). Regardless of the type of entity, the authority level should sign certificates of entities from only the service level.

Whereas ISO 9001 is a standard for quality management systems, ISO 16363 [27] is a standard that defines requirements for assessing the trustworthiness of digital repositories. The Primary Trustworthy Digital Repository Authorization Body Ltd. (PTAB) [28] is the first accredited organization to carry out audits in accordance with ISO 16363 and following procedures defined by ISO/IEC 17021–1:2015 [29], which defines requirements for bodies

providing audit and certification of management systems. Authority level certificates could be used to build trust among organizations (e.g., PTAB) carrying out audits in accordance with ISO 16363 and ISO/IEC 17021. However, a long-term vision of any audit service should also include methods for auditing and certifying organizations, people, and products, too.

The authority level signs the service-level certificates, signaling that those service-level entities can be trusted if the authority is trusted. We recommend three types of service-level actors: validation services, approval services, and intellectual property (IP) access services. The validation services audit or vet native and derivative data in the data level. The approval services audit or vet people and systems in the data level. Lastly, the access services set authorization permissions (e.g., who can use data, how data can be used) on the data. Section 3.1 through Section 3.3 provide more details and examples for interactions between the service level and data level.

3.1. Data Trust

Knowing where data came from and the quality of that data are key components to trustworthy communications and data exchange. There are several types of data (e.g., CAD models, analysis models, documents) that could be vetted by actors in the service level and signed with digital certificates. In the context of this paper, we will focus our example on the vetting of native CAD models (i.e., 3D models that come from an authoring CAD system) and derivative CAD models (e.g., 3D models that are translated from the native CAD system to a standard-based format such as Standard for the Exchange of Product Model Data (STEP) [20], Jupiter Tessellation (JT) [30], or PDF [23] / PRC [24]).

Figure 4 shows an example chain of trust for a fictitious aerospace company using a fictitious verification and validation system to digitally sign data with digital certificates. In this scenario, a root CA signs a certificate issued to the FAA. The FAA vets a third-party verification and validation (V&V) solution from ACME Validation Company. ACME sells licenses of its V&V solution to customers who need to complete V&V workflows. AeroStructures Company licenses the software from ACME and uses V&V product-data quality (PDQ) criteria as declared requirements to check the quality of native and derivative CAD models produced by AeroStructures.

Further, consider a wing-rib produced by the AeroStructures Company. AeroStructures outsourced the fabrication of the wing rib. AeroStructures' supplier cannot use the native CAD model because the supplier uses a different CAD system than AeroStructures. Therefore, a derivative CAD model using the STEP standard is sent to the supplier. AeroStructures uses ACME's V&V software to verify and validate the CAD models before sending the STEP file to the supplier.

Figure 5 shows the verification and validation workflows that AeroStructures uses to complete the V&V tasks. In Figure 5(a), AeroStructures runs the ACME software on the native CAD model for the wing rib. Verification criteria that include data-quality rules and tolerances are used to configure the verification settings. After the quality of the model is confirmed, the results of the verification check are captured and AeroStructures is asked to

sign the native model. The digital certificate attached to the native model includes the verification results and AeroStructures' digital signature. The same process is followed to complete the validation check on the derivative STEP data shown in Figure 5(b).

3.2. Person and System Trust

As shown in Figure 5, a person or system can digitally sign data. That signature could represent an approval of data or a confirmation that a task was completed. Examples of approvers are FAA designated-engineering representatives (DERs), company employees, and CM systems. Figure 6 presents a chain of trust for a person with a FAA DER certification who approves data in accordance to FAA requirements.

The FAA Aviation Safety Division appoints DERs. Under our trust structure, the FAA signs the certificate of John Doe, who is an employee of AeroStructures Company and has met the DER requirements. John Doe then uses his X.509-PKI-based certificate to digitally approve data with a digital signature. John Doe's digital signature is verifiable to prove that John Doe has the authority to approve the data in accordance with FAA requirements. The full chain of trust is available to show that the FAA vetted John Doe and appointed him as a DER for the AeroStructures Company. Further, the chain of trust helps to determine that John Doe has the authority to approve the data that has his digital signature attached.

Thus, trust, in cases like the one shown in Figure 6, is represented semantically in data. Semantic representation of trust does not require interpretation of authorization like a handwritten signature. With digital signatures, the chain of trust either provides evidence of trust or it does not. The interpretation is binary.

3.3. Usage Trust

The concept of controlling the usage of digital files is not new. The use of digital rights management (DRM) became popular in the late-1990s and early-2000s as the music, movie, and publishing industries tried to curb pirating of their digital assets. Today, commercial solutions are becoming available in the manufacturing sector because of two main drivers. The first is the significant increasing focus on additive manufacturing. The second is IP protection of digital datasets as manufacturers increase usage of model-based definitions.

However, the current commercial applications are proprietary systems that require additional software and significant cost to deploy across the supply chain. In addition, the commercial solutions are not interoperable. Proprietary software must be installed for each commercial solution. This is problematic for the small-to-medium enterprise (SME) manufacturers who have to support multiple customers that may be using different DRM solutions.

The proposed approach described in this paper reduces the burden on the supply chain by deploying an interoperable solution based on open-standards-based technologies. Data-usage authorization meta-data would be embedded in the X.509-PKI-based digital signature of a file. Should the authorization meta-data be changed or tampered with, the digital signature would become invalid. Figure 7 presents a use case showing how the data-usage rights could be controlled in a computer-aided manufacturing (CAM) system.

In the scenario depicted in Figure 7, the data owner decides to restrict a model to be used only for production purposes. When the manufacturing planner imports the model into the CAM system, he accidentally sets up the job as a development run (Figure 7, Step 1). When the manufacturing planner clicks the accept button to move to the next planning step (Figure 7, Step 2), the CAM system checks the authorization meta-data and determines that the model cannot be used as selected (Figure 7, Step 3). This is a basic example of managing the usage of data with X.509-PKI. However, the same approach could be deployed to other use cases, such as, but not limited to, controlling the number of times a part can be 3D printed, controlling who can access the file, and setting an expiration date for the model.

4. Tracing Transactions

As mentioned in Section 2.1, data traceability is paramount to enabling trustworthiness throughout the product lifecycle. While our previous work in Section 2 focuses on embedding traceability information in the file (Section 2.4), that solution is not completely sufficient or feasible due to the complexity of the supply chain and the heterogeneity of the data exchanged. This gap was realized through further validation of our previous work.

In a complex environment composed of numerous partners and exchanges, embedding traceability data in only files can bloat the product data with information not required by every actor. A complete traceability can not be guaranteed due to the heterogeneity of the data and the need for every file format to support a traceability mechanism. Proprietary and/or binary files are heavily used and do not offer an efficient transparent way of auditing the traceability information. Moreover, numerous open-formats may not support such a mechanism either. Lastly, embedding traceability information in files makes the audit process cumbersome, requiring access to and processing of all the files, which is an enormous amount of data. Therefore, to overcome these challenges and to address efficient audit needs, we suggest to combine our previous work with recording traceability information externally in a safe and shared repository such as a blockchain-based [31] ledger that offers a shared, trusted, and virtually tamper-resistant source of information.

Built on X.509-PKI and blockchain technologies, we have defined two use cases for tracing data transactions throughout the lifecycle. A data transaction occurs anytime data ownership is declared or when data is exchanged between two actors. The first use case is file-only transactions, discussed in Section 4.1. The second use case is blockchain-registered transactions, discussed in Section 4.2.

Listing 1. Embedded *Verification, Release, and Revision* traceability information in a STEP document for an aerospace part

```
1 ISO-10303-21;
2 HEADER;
3 FILE_DESCRIPTION(('WingRib-001 for demonstration of trust and traceability
in
the product lifecycle'),'2:1');
```



```

4 FILE_NAME( 'WingRib-001_rev01.stp','2017-07-17T13:21:18',(''),
(''),'',',',',',',');
5 FILE_SCHEMA(('AP242_MANAGED_MODEL_BASED_3D_ENGINEERING_MIM_LF { 1 0 10303
442
1 1 4 }'));
6 ENDSEC;
7 DATA;
8 #1=APPLICATION_CONTEXT('Managed model based 3d engineering');
9 .
10 .
11 .
12 TRACE:#3415
13 #3416 = PKCS_TRACE({source:'URI:20.500.11993\734.13.wingrib',
date:'2017-06-14T11:39:54', operation:'verification',
usage:'production',
result:'pass with warnings',
report:'URI:15.1115\734.13.wingrib.verification'})
14 #3417 = PKCS('pkcs7_signature_1',N,[])
15 ENDSEC;
16 TRACE:#3418
17 #3419 = PKCS_TRACE({source:'URI:20.500.11993\734.13.wingrib',
destination:'URI:15.1115\734.13.wingrib.release', usage:'production',
date:'2017-06-20T15:18:36', operation:'release'})
18 #3420 = PKCS('pkcs7_signature_2',Y,[#3415])
19 ENDSEC;
20 TRACE:#3421
21 #3422 = PKCS_TRACE({source:'URI:20.500.11993\734.13.wingrib.release',
destination:'URI:15.1115\734.13.wingrib.change01', usage:'production',
date:'2017-07-17T13:21:18', operation:'revision'})
22 #3423 = PKCS('pkcs7_signature_3',Y,[#3418])
23 ENDSEC;
24 END-ISO-10303-21;

```

4.1 File-Only Transactions

File-only transactions are asynchronous, require significant leveraging of X.509-PKI certificates, and require trust of the other actors with whom data is exchanged. Traceability is managed with metadata stored within the data files (See Listing 1). Figure 8 presents a use-case diagram for digitally signing a design specification and exchanging the file with another data user, using the DMC toolkit described in Section 2.4.

The PKCS_TRACE element on lines 13, 17, and 21 of Listing 1 contains metadata that describes the context under which the data was digitally signed. At a minimum, the following attributes should be included in the PKCS_TRACE.

- `source`: identifies the source data that was reviewed and digitally signed, may be a circular reference to data containing the `PKCS_TRACE` element
- `destination`: identifies the actual signed data, which may be a circular reference to data containing the `PKCS_TRACE` element
- `usage`: the purpose(s) / use(s) for which the signed data is authorized
- `operation`: the reason why the data was signed (e.g., release, revision, validated)
- `date`: the date the operation was completed

The `source` and `destination` elements should contain Uniform Resource Identifiers (URIs) to enable link-data approaches [32]. The `usage` and `operation` elements are proposed currently as strings, but `usage` and `operations` types should be added to a standardized data dictionary. The `date` element should be included use the ISO 8601 [33].

The proposed minimum set of metadata should be included using a JavaScript Object Notation (JSON) structure. This enables efficient processing of the metadata by both humans and machines. Using a JSON structure also allows for extending the minimum set of metadata, but the set proposed here should be the required minimum elements of the metadata. Additional and/or metadata can be included from standardized data dictionaries, such as ISO/IEC 11179 [34] and Open Applications Group Integration Specification (OAGIS) [35, 36]. The need for extending the metadata and what additional metadata must be included should be determined by negotiations between the data owners, signers, and consumers. For example, `result` and `report` elements are added to the `PKCS_TRACE` element on line 13 of Listing 1.

Three actors are depicted in the file-only transactions use case: 1) data owner, 2) data user, and 3) bad actor. The data owner (herein owner) and data user (herein user) are the normal roles that would typically share data while executing tasks. When the owner is prepared to release the data to the user, the owner would review and sign the data using the DMC toolkit. Then, the owner would send the data to the user. The owner and user would store that signed data in their respective data repositories. The user would use the data to complete all agreed-upon tasks for the owner (e.g., supplier fabricates a part for a customer). This portion of the use case represents typical manufacturing-related business relationships.

Data could be compromised and/or stolen from owners and users by bad actors. In the file-only transactions use case, a bad actor could steal data from the user by compromising (e.g., gaining unauthorized access) to the user's data repository. The bad actor would have access to the signed data. If the owner somehow then found the signed data in the possession of an unauthorized actor, the owner could go back to his/her repository and determine all the users the data was sent to by querying and reviewing the certificate and metadata. This would provide the owner the ability to discover who received the data and request those users to investigate their systems for breaches. In this case, the owner would simply discover that he/she has a data problem, but the owner would not immediately know the root cause of that problem without further investigation.

However, the file-only transactions use case represents a solid foundation with which to build data-traceability principals and methods. Having the ability to quickly impart additional metadata into a file and then later be able to trace where the data came from, its purpose, and potential uses would reduce the risk of errors being introduced due to the wrong data being used or because of changes that went unnoticed.

4.2 Blockchain-Registered Transactions

Blockchain-registered transactions are synchronous and require leveraging X.509-PKI certificates and a blockchain (i.e., a distributed ledger). Traceability is managed with transactions registered in a blockchain. Figure 9 presents a use-case diagram for digitally signing a design specification, using the DMC toolkit described in Section 2.4, and registering data-ownership and data-exchange transactions in a blockchain.

The same three actors depicted in the file-only transactions use case are also depicted in the blockchain-registered transaction use case. The owner and user are still the normal roles that would typically share data between each other for the purposes of executing tasks. However, in this case, when the owner is prepared to release and send the data to the user, the owner would review and sign the data using the DMC toolkit and register the signature fingerprint in a blockchain to prove ownership of the data. Krma et al. [37] recommend storing only the signature fingerprint in the blockchain, registering the signature fingerprint in a transaction sent by the owner to him/herself for proving ownership, and then registering the signature fingerprint in transactions whenever the data is sent to a user. The owner and user would still store signed data in their respective data repositories. The user would also still use the data to complete all agreed-upon tasks for the owner (e.g., supplier fabricates a part for a customer). This portion of the use case, like the file-only transactions, represents typical manufacturing-related business relationships with the only difference being that each action on the data is registered in a blockchain.

The strength of the blockchain-registered transactions use case is in dealing with bad actors. If the owner found signed data in possession of an bad actor, the owner could query the blockchain and determine the exact transaction that was related to the compromised data. This provides the owner the ability to discover exactly who was authorized to receive the data originally and request that user to investigate his/her systems for breaches. In this case, the blockchain-registered transactions use case is differentiated from the file-only transactions use case because the owner would discover that he/she has a data problem and immediately know the root cause of the problem without further investigation.

5. Configuration Management Use Cases

Ensuring the correct data is used when required by the needed functions and roles in the lifecycle depends on trusting the processes for making a product and managing the workflow. CM is key to managing the workflow and using the data. CM is a methodology for ensuring that a product's performance, function, and physical attributes are consistent with the requirements, design, and operational information of the product [38]. CM is especially crucial at the points data will be released, changed, and/or exchanged. Each phase of the lifecycle must be cognizant of the CM of products because releases, changes, and

process execution often happen in parallel as product specifications mature. Recall from the introduction that 75 percent of respondent manufacturers reported they have wasted time making a prototype or doing a production run using the wrong version of a CAD file [6]. Industry constantly struggles with using outdated version and product configurations. Ensuring the data configuration for a product specification is correct and being used appropriately is difficult today because manufacturing has become decentralized and distributed across the globe.

Using the method presented in this paper would address several CM issues facing industry. For example, the trust structure presented in Section 3 would assure that the right data came from an authorized person or system and that the data is used correctly. Metadata embedded in data would prove ownership, and certificate metadata and authorized digital signatures would allow determination of the validity of that data. Should software and tool providers adopt and implement this approach, industry would enjoy better control of data usage and could ensure that only data authorized for production is used in production processes.

Figure 10 presents three CM workflows that would benefit from the usage of digital certificates. Further, the description of Figure 7 is one example of how the usage of data versions could be controlled. The need is to control how the data could be used – e.g., is data meant for development being used for production? We recognize that the risk remains for two versions of “production” data being available, and an outdated version could be selected. To overcome this challenge, proper configuration-management processes are required, but this topic is outside the scope of the work presented in this paper. Further investigation into distributed ledgers and revocation lists applied to manufacturing use cases could assist with the remaining challenges.

5.1. Release Process

Figure 10(a) presents a typical release process workflow defined in a product-data management (PDM) or CM system. The purpose of the workflow is to manage the multi-stage review cycle of data that is ready to be authorized for use outside the owning organization. The data is considered “released” once the data has been “signed off” by the proper authority. In the context of this paper, the release process is defined as an engineering review, manufacturing review, quality review, and then a final program-management review. The data would be digitally signed by the functional role after each review and approval or rejection.

Listing 2 provides an example of the traceability metadata and digital signature that would be embedded in the data. The traceability data for the engineering review starts on line 12 of Listing 2, the manufacturing review on line 16, the quality review on line 20, and the program review on line 24. After the last approval, the CM system would sign the data. The traceability data for the CM system starts on line 28 of Listing 2. Also, notice the value of the destination attribute changed on line 29 after the CM system completed its task. This is because the status of the data changed in the system and was marked as “released.” Finally, the CM system should cross-sign the data – essentially vouching for the digital signatures of the engineering, manufacturing, quality, and program reviewers. This is why

#3677, #3680, #3683, #3686 are included in square brackets at the end of the signature entry on line 30 of Listing 2.

Now that the data is marked “released,” it is available to be exchanged with users who need the data to complete some tasks. Those users can use the digital certificates to verify the data is in fact released and is intended for production use. This workflow prototype shows how digital certificates could be implemented to ensure the correct data is used in processes across the lifecycle such as the example described in Section 3.3.

5.2. Change Process

Figure 10(b) presents a typical change process workflow defined in a PDM or CM system. The purpose of the workflow is to manage the multi-stage review cycle of proposed data changes. The change to the data is described by an “Engineering Change Request,” which goes through a series of reviews for approval. In the context of this paper, the change request would be a package of data that includes the actual data being changed and supporting documentation for the change (e.g., problem reports, revision history).

The workflow shown in Figure 10(b) includes two opportunities for signatures. The first signature is applied by the change submitter and the second signature is applied by the change approver. In either signature, the actor could be a system or person. For each review, traceability metadata and a digital signature would be embedded in the data similar to the method described for the release process. Lines 32 to 35 of Listing 2 provide an example of the traceability metadata and the digital signature for the change-request submission. The traceability metadata informs the data user that the signature operation was for the purpose of changing the source data to the destination data. The change submitter should also cross-sign the data if release signatures exist to signify that the change has validated the previous version prior to recommending the change. The cross-signing is shown on line 34 of Listing 2. The change approver should also cross-sign the data and reference the change submission signature when the change is approved. The “Engineering Change Order” to initiate the requested change should only be issued after both the change submission and approval signatures are applied to the data.

Listing 2. Embedded traceability information in a STEP document after going through configuration-management processes

```

1 ISO-10303-21;
2 HEADER;
3 FILE_DESCRIPTION(('WingRib-001 for demonstration of trust and traceability
in
the product lifecycle'),'2:1');
4 FILE_NAME('WingRib-001_rev03.stp','2017-07-20T16:21:18',(''),
(''),'','');
5 FILE_SCHEMA(('AP242_MANAGED_MODEL_BASED_3D_ENGINEERING_MIM_LF { 1 0 10303
442
1 1 4 }'));

```

```

6 ENDSEC;
7 DATA;
8 #1=APPLICATION_CONTEXT('Managed model based 3d engineering');
9 •
10 •
11 •
12 TRACE:#3677
13 #3678 = PKCS_TRACE({source:'URI:20.500.11993\734.13.wingrib',
    destination:'URI:15.1115\734.13.wingrib', usage:'production',
    date:'2017-06-20T15:18:36', operation:'release approval'})
14 #3679 = PKCS('engineering_signature',N,[])
15 ENDSEC;
16 TRACE:#3680
17 #3681 = PKCS_TRACE({source:'URI:20.500.11993\734.13.wingrib',
    destination:'URI:15.1115\734.13.wingrib', usage:'production',
    date:'2017-06-20T15:20:03', operation:'release approval'})
18 #3682 = PKCS('manufacturing_signature',N,[])
19 ENDSEC;
20 TRACE:#3683
21 #3684 = PKCS_TRACE({source:'URI:20.500.11993\734.13.wingrib',
    destination:'URI:15.1115\734.13.wingrib', usage:'production',
    date:'2017-06-20T15:23:18', operation:'release approval'})
22 #3685 = PKCS('quality_signature',N,[])
23 ENDSEC;
24 TRACE:#3686
25 #3687 = PKCS_TRACE({source:'URI:20.500.11993\734.13.wingrib',
    destination:'URI:15.1115\734.13.wingrib', usage:'production',
    date:'2017-06-20T15:35:34', operation:'release approval'})
26 #3688 = PKCS('program_signature',N,[])
27 ENDSEC;
28 TRACE:#3689
29 #3690 = PKCS_TRACE({source:'URI:20.500.11993\734.13.wingrib',
    destination:'URI:15.1115\734.13.wingrib.release', usage:'production',
    date:'2017-06-20T15:35:52', operation:'release'})
30 #3691 = PKCS('CM-system_signature',Y,[#3677,#3680,#3683,#3686])
31 ENDSEC;
32 TRACE:#3692
33 #3693 = PKCS_TRACE({source:'URI:20.500.11993\734.13.wingrib.release',
    destination:'URI:15.1115\734.13.wingrib.change01', usage:'production',
    date:'2017-07-20T16:21:18', operation:'change submission'})
34 #3694 = PKCS('change_signature',Y,[#3689])
35 ENDSEC;
36 END-ISO-10303-21;

```

5.3 Import and Verify File

Figure 10(c) presents a data “import and verify” process. Data should be verified before being storing the data in a repository. This is to ensure only verified data is stored. In the “import and verify” process, the user would select data to import into a system. The system would then check any digital signatures present in the data and verify the signatures are valid. If the signatures are valid, then the system would store the data in the repository. If the signatures are not valid, then the system would reject the data and not store it in the repository.

6. Discussion

In this paper, data traceability using X.509-PKI is shown to be a viable option for supporting trustworthiness across the product lifecycle. Further, the proposed trust structure and hierarchy described in Section 3 establishes a governance policy for managing the traceability of data. A trades analysis of solutions was presented in our previous work [7].

We utilized a literature review to identify a method for measuring the quality of our proposed solution. Gol Mohammadi, et al. [39] conducted a survey of the literature to determine trustworthiness attributes to develop metrics for measuring trust. The authors determined 12 high-level attribute categories and further decomposed some of the categories with sub-categories. After careful consideration, we decided to use the attributes to measure the completeness of the work presented in this paper. Table 1 analyzes the completeness and maps the method and governance policy described in this paper to the trustworthiness attributes presented by [39]. We do not claim that Table 1 is a performance measure, but rather a measure of the completeness of our work in addressing trustworthiness. We recognize the measure presented here is a qualitative approach and the need remains for key metrics that can be used for fair evaluations across multiple solutions. Developing such key metrics and/or a measure remains an open area for research.

Overall, the work presented in this paper addresses the Gol Mohammadi, et al. [39] attributes for trustworthiness well. Five of the 32 metrics are considered out of scope, which leaves 27 metrics remaining for assessing this work. The method in the paper fully (black filled circle in the table) or partially (white filled circle in the table) addresses 97 percent (15 full, 11 partial) of the 27 metrics with only one metric not addressed.

7 Conclusion

The method presented in this paper shows promise for enabling a root of trust in support of product-data certification and traceability, thus supporting trustworthiness across the product lifecycle. The trust structure was designed to enable traceability of data; people and systems; and the usage and interactions between data, people, and systems. In addition, the presented method was studied using two types of use cases: 1) transaction tracing, and 2) common CM workflows. The method addresses all the use cases sufficiently. Lastly, the method was analyzed using a set of metrics for measuring trust-worthiness. Overall, the method performed well in addressing most of the trustworthiness metrics, but additional required work was also identified.

7.1 Future Work

Needed future work includes three areas of technical study. The first area is a complete metadata schema for defining all stakeholder-needed traceability information in the digital certificates. The second area is recommendations for extending the widely adopted data formats and standards to enable embedding digital signatures in a normalized manner. The third area is further investigation of how distributed ledgers (e.g., blockchain) would be managed across various industries and would assist with audit trails.

Addressing the future work would ensure the method fully satisfies the needs for data certification and traceability layer of the LIFT concept as described in Section 2.3. Further, Helu et al. [40] proposes a reference architecture for integrating heterogeneous manufacturing systems, in which the authors recommend using STEP Application Protocol (AP) 242 [20], ISO 6983 (G code) [21], MTConnect [41], and QIF [22]. The method in this paper provides the ability to embed digital certificates in each of the domain-specific standards-based data discussed in [40]. Further, a complete metadata schema would also contribute to developing the Minimum Information Model [42, 43], which is the common and domain-specific information elements combined to represent the complete set of information required to effectively communicate to all functions and roles in the product lifecycle.

In addition, future work should be conducted in the management domain to understand what kind of organizational and systematic change is needed to deploy more automated traceability methods. Businesses, especially in regulated industries, make traceability work through significant manual intervention. Understanding how best to deploy the solution proposed in this paper would minimize disruption to businesses while reducing their traceability burdens and challenges. We suspect there is a considerable return-on-investment opportunity in moving to automated traceability methods, but quantifiable data is currently not available.

7.2 Realized Impacts

A goal for any project should be to provide value to the stakeholders. This would ensure the stakeholders can leverage the project outputs to be more competitive and improve quality of life. Impact can be defined here as making a substantial, positive external change directly enabled by project outcomes, resulting from adoption or use by external entities (e.g., industry, government agencies, society). Some impact has already been realized as the result of the work described in this paper.

Two standards development organizations (SDOs) adopted the DMC approach described in Section 2. ISO 10303–21:2016 [44] is the STEP standard that defines the EXPRESS language. The DMC approach for STEP described by our previous work is normalized in ISO 10303–21:2016. An amendment to ISO 10303–21:2016 is currently in work to add the additional traceability elements described in this paper. The QIF standard [22] also adopted and normalized the proposed extensions to that standard. Further, a large CAD vendor, based in Boston Massachusetts, added the DMC approach to their development roadmap for

embedding digital certificates in the vendor's proprietary native file format. The vendor made this decision based on the urging of two large Aerospace companies.

In closing, the contribution of this research is a novel method for using existing technologies to enable data certification and traceability in manufacturing. The method provides the infrastructure and guidance for transmitting the information (e.g., provenance, metadata) required to enable trustworthiness in the product lifecycle. The method would extend the standards-based use of X.509-PKI to enable trustworthy storage and exchange of data in manufacturing. The extension would support industry's needs in meeting traceability requirements from regulatory agencies such as FAA and FDA. A data user must know who did what to whom and when it was done. Therefore, product data must be guaranteed by an authority to a predefined level of data quality and trustworthiness if that information is to be used throughout the product lifecycle.

Acknowledgements

The authors wish to thank Allison Barnard Feeney, Mark Carlisle, Michael Brundage, Brian A. Weiss, and Vijay Srinivasan from NIST and the peer-reviewers for their comments and input to this paper.

Acronyms

2D	two-dimensional
3D	three-dimensional
ANSI	American National Standards Institute
AP	Application Protocol
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
CA	certificate authority
CAD	computer-aided design
CAE	computer-aided engineering
CAM	computer-aided manufacturing
CFD	computational fluid dynamics
CM	configuration management
CPSC	Consumer Product Safety Commission
DER	designated-engineering representative
DMC	digital manufacturing certificates
DMSC	Dimensional Metrology Standards Consortium

DRM	digital rights management
FAA	Federal Aviation Administration
FDA	Food and Drug Administration
FEA	finite-element analysis
IP	intellectual property
ISO	International Standards Organization
JSON	JavaScript Object Notation
JT	Jupiter Tessellation
LIFT	lifecycle information framework and technology
MBE	model-based enterprise
OAGIS	Open Applications Group Integration Specification
PDF	Portable Document Format
PDM	product-data management
PDQ	product-data quality
PLOT	product lifecycle of trust
PRC	Product Representation Compact
PTAB	Primary Trustworthy Digital Repository Authorization Body Ltd
QIF	Quality Information Framework
SDO	standards development organization
SME	small-to-medium enterprise
SSL	Secure Sockets Layer
STEP	Standard for the Exchange of Product Model Data
TLS	Transport Layer Security
URI	Uniform Resource Identifier
V&V	verification and validation
X.509-PKI	Public Key Infrastructure

References

- [1]. Sharma R, 2013 “The problems with reinventing CAD software” Forbes.
- [2]. Wu D, Greer MJ, Rosen DW, and Schaefer D, 2013 “Cloud manufacturing: Strategic vision and state-of-the-art”. *Journal of Manufacturing Systems*, 32(4), pp. 564–579.

- [3]. Xu X, 2012 “From cloud computing to cloud manufacturing”. *Robotics and Computer-Integrated Manufacturing*, 28(1), pp. 75–86.
- [4]. Wu D, Rosen DW, Wang L, and Schaefer D, 2015 “Cloud-based design and manufacturing: A new paradigm in digital manufacturing and design innovation”. *Computer-Aided Design*, 59(0), pp. 1–14.
- [5]. Trainer A, Hedberg T Jr, Barnard Feeney A, Fischer K, and Rosche P, 2016 “Gaps analysis of integrating product design, manufacturing, and quality data in the supply chain using model-based definition”. In 2016 Manufacturing Science and Engineering Conference, American Society of Mechanical Engineers.
- [6]. GrabCAD, 2014 Where did the time go? Report, GrabCAD URL: <https://resources.grabcad.com/time-go/>.
- [7]. Hedberg TD Jr, Krma S, and Camelio JA, 2016 “Embedding x.509 digital certificates in three-dimensional models for authentication, authorization, and traceability of product data”. *Journal of Computing and Information Science in Engineering*, 17(1), pp. 011008–011008–11. [PubMed: 27840596]
- [8]. Telecommunication Standardization Sector of ITU, 2014 Information technology – open systems interconnection – the directory – part 8: Public-key and attribute certificate frameworks. ISO/IEC 9594–8:2014.
- [9]. Cyber Physical Systems Public Working Group, 2016 Framework for cyber-physical systems, release 1.0. Report, National Institute of Standards and Technology, May. URL: <https://pages.nist.gov/cpspwg/library/>.
- [10]. Ramesh B, 2002 “Process knowledge management with traceability”. *IEEE Transactions on Software Engineering*, 19(3), pp. 50–52.
- [11]. Mohan K, and Ramesh B, 2007 “Traceability-based knowledge integration in group decision and negotiation activities”. *Decision Support Systems*, 43(3), pp. 968–989.
- [12]. Mohan K, Xu P, Cao L, and Ramesh B, 2008 “Improving change management in software development: Integrating traceability and software configuration management”. *Decision Support Systems*, 45(4), pp. 922–936.
- [13]. Hamilton VL, and Beeby ML, 1991 “Issues of traceability in integrating tools”. In *IEEE Colloquium on Tools and Techniques for Maintaining Traceability During Design*, pp. 4/1–4/3.
- [14]. Ouertani MZ, Băina S, Gzara L, and Morel G, 2011 “Traceability and management of dispersed product knowledge during design and manufacturing”. *Computer-Aided Design*, 43(5), pp. 546–562.
- [15]. Hempe DW., 2010 Advisory Circular 21–48. Report, Federal Aviation Administration, U.S. Department of Transportation URL: http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC
- [16]. Alle JM., 2010 Advisory Circular 20–62E. Report, Federal Aviation Administration, U.S. Department of Transportation URL: http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC
- [17]. Hedberg T Jr, Barnard Feeney A, Helu M, and Camelio JA, 2017 “Towards a lifecycle information framework and technology in manufacturing”. *Journal of Computing and Information Science in Engineering*, 17(2), pp. 021010–021010–13. [PubMed: 28265224]
- [18]. Krma S, and Hedberg T Jr, 2016 “Digital manufacturing certificate toolkit: Adding trust and traceability to product data”. *NIST Journal of Research (NIST JRES)*, 121.
- [19]. The Internet Engineering Task Force, 2013 Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile
- [20]. International Standards Organization, 2014 Industrial automation systems and integration – product data representation and exchange – part 242: Application protocol: Managed model-based 3D engineering ISO/TC 184/SC 4, ISO 10303–242.
- [21]. International Organization for Standardization, 2009 Automation systems and integration – numerical control of machines – program format and definitions of address words – part 1: Data format for positioning, line motion and contouring control systems ISO/TC 184/SC 1, ISO 6983–1:2009.

- [22]. Dimensional Metrology Standards Consortium, 2014 Part 1: Overview and fundamental principles in quality information framework (QIF) an integrated model for manufacturing quality information
- [23]. International Standards Organization, 2008 Document management – portable document format – part 1: PDF 1.7 ISO/TC 171/SC 2, ISO 32000-1.
- [24]. International Standards Organization, 2014 Document management – 3D use of product representation compact (PRC) format – part 1: PRC 10001. ISO/TC 171/SC 2, ISO 14739-1.
- [25]. International Organization for Standardization, 2015 Quality management systems ISO/TC 176/SC 2, ISO 9001:2015.
- [26]. Dougherty R, 2017, Accessed 2017-08-14. Quality assurance standard for digital product definition at Boeing suppliers. Report D6-51991, The Boeing Company Archived by WebCite at <http://www.webcitation.org/6siPUecWG>.
- [27]. International Organization for Standardization, 2012 Space data and information transfer systems – audit and certification of trustworthy digital repositories. ISO/TC 20/SC 13, ISO 16363:2012.
- [28]. PATB Ltd, 2017, Accessed 2017-09-01. Primary trustworthy digital repository authorisation body ltd, audit & certification, overview URL: <http://www.iso16363.org/iso-certification/overview/>.
- [29]. International Organization for Standardization, 2015 Conformity assessment – requirements for bodies providing audit and certification of management systems – part 1: Requirements ISO/CASCO, ISO/IEC 17021-1:2015.
- [30]. International Standards Organization, 2012. Industrial automation systems and integration – JT file format specification for 3D visualization ISO/TC 184/SC 4, ISO 14306.
- [31]. Yaga D, Mell P, Roby N, and Scarfone K, 2018 Blockchain technology overview. Tech. rep, National Institute of Standards and Technology, Gaithersburg, MD, 10.
- [32]. Bajaj M, and Hedberg T, 2018 “System Lifecycle Handler - Spinning a Digital Thread for Manufacturing”. INCOSE International Symposium, 28(1), 7, pp. 1636–1650.
- [33]. International Organization for Standardization, 2018 ISO 8601 Date and time format
- [34]. International Organization for Standardization, 2015 Information technology – Metadata registries (MDR) – Part 1: Framework
- [35]. Open Applications Group, 2018 OAGIS 10.4.
- [36]. Ivezic N, Kulvatunyou B, and Srinivasan V, 2014 “On architecting and composing through-life engineering information services to enable smart manufacturing”. Procedia CIRP, 22(1), jan, pp. 45–52.
- [37]. Krma S, Hedberg T Jr, and Barnard Feeney A, 2018 Securing the digital threat for smart manufacturing: A reference model for blockchain-based product data traceability. Report AMS 300-6, National Institute of Standards and Technology
- [38]. SAE International, 2011 Configuration management standard EIA649.
- [39]. Gol Mohammadi N, Paulus S, Bishr M, Metzger A, Knnecke H, Hartenstein S, Weyer T, and Pohl K, 2014 “Trustworthiness attributes and metrics for engineering trusted internet-based software systems”. In Cloud Computing and Services Science, Springer International Publishing, pp. 19–35.
- [40]. Helu M, Hedberg T Jr, and Barnard Feeney A, 2017 “Reference architecture to integrate heterogeneous manufacturing systems for the digital thread”. CIRP Journal of Manufacturing Science and Technology, 19, pp. 191–195.
- [41]. MTConnect Institute, 2014 Mtconnect standard: Part 1 - overview and protocol
- [42]. Ruemler SP, Zimmerman KE, Hartman NW, Hedberg JT, and Barnard Feeney A, 2016 “Promoting model-based definition to establish a complete product definition”. Journal of Manufacturing Science and Engineering, 139(5), pp. 051008–051008. [PubMed: 28070155]
- [43]. Miller AM, Hartman NW, Hedberg T Jr, Barnard Feeney A, and Zahner J, 2017 “Towards identifying the elements of a minimum information model for use in a model-based definition”. In International Manufacturing Science and Engineering Conference, American Society of Mechanical Engineers, p. V003T04A017.

- [44]. International Organization for Standardization, 2016 Industrial automation systems and integration – product data representation and exchange – part 21: Implementation methods: Clear text encoding of the exchange structure ISO/TC 184/SC 4, ISO 10303–21.

Single-path hierarchical signing

Multi-path hierarchical signing

Fig. 1.

Examples of the single-path and multi-path hierarchical signing employed in the digital manufacturing certificates toolkit (from [7])

Fig. 2.
Hierarchy for chains of trust using X.509-PKI principles.

Fig. 3.

X.509-PKI certificates chain showing the levels of the trust structure.

Fig. 4.

Chain of trust for a verification and validation system signing data with a digital signature

Fig. 5.
Example verification (a) and validation (b) workflows to ensure data meets a predefined level of quality (based on [7])

Fig. 6.
Verifying the chain of trust for a FAA DER signing data with a digital signature

Fig. 7.
Example of data-usage rights controlling how data must be used in a CAM system

Fig. 8.

Use case for digitally signing a design specification (e.g., CAD model) and exchanging the data with another data user

Fig. 9.

Use case for digitally signing a design specification (e.g., CAD model) and registering ownership and data-exchange transactions in a blockchain

(a) Release Process

(b) Change Process

(c) Import and Verify Process

Fig. 10.

Product-data management workflows for signing data during a release cycle, change process, and import verification

Table 1:

The analysis trustworthiness in product data using digital manufacturing certificates, proposed trust structure, and hierarchy

Main Attribute	Sub-category	Addressed	Description of the method's congruence
Security	Accountability	•	The use of X.509-PKI with embedded metadata ensures a person and/or system can be called upon to account for actions performed on data.
	Audit-ability & Traceability	•	The digital signatures generate a reliable and secure audit trail.
	Confidentiality		This sub-category is outside the scope of the data and is the responsibility of the data-managing systems.
	Integrity	•	The digital signatures would become invalid if the data changes or becomes corrupt. The X.509-PKI digital certificate have a high-level of integrity if generated in conformance to the standard. Therefore, both accidental and malicious alterations in the data are discoverable, which ensures the integrity of the data.
	Safety		This sub-category is outside the scope of the data and is the responsibility of the data-managing systems.
	Non-Repudiation		This sub-category is outside the scope of the data and is the responsibility of the data-managing systems.
Compatibility	Openness	•	The method takes advantage of the X.509-PKI standard, which is widely adopted in information technology and systems. Therefore, the method is open and transparent in how it works.
	Re-usability	•	The method is interoperable between information technologies and systems, while also allowing the metadata to be extensible to support multiple use cases and/or domains.
Configuration-related Quality	Change Cycle & Stability	•	The method meets an acceptable level of stability because it utilizes the widely-adopted X.509-PKI standard.
	Completeness		Future work is required to develop a complete standardized metadata schema to assist in defining semantic representation of the metadata such that it can be computer-processable.
Compliance		•	A governance policy that addresses most needs of regulated and non-regulated industries is proposed for using the method. The method also conforms to industry-led consensus-based standards.
Privacy		○	The method and governance policy partially address the ability to control the usage of private information. The method, being built upon X.509-PKI, supports controlling public and private keys. However, the method and governance policy must be used in concert with a properly configured data-management system to fully control the usage of private information.
Cost			Cost is considered out of scope for the work described in this paper. However, the use of standards should help in minimizing cost.
Data-Related Quality	Data Integrity	•	Human errors, malicious attacks, intentional data modifications, transmission errors, system/software bugs or viruses, and hard-ware malfunctions are discoverable because any change in the data would invalidate the digital certificates / signatures embedded in the data.
	Data Reliability	•	The provenance of the data is traceable. Further, usage (authorization) of the data is controlled by embedded metadata. Therefore, the correctness of the data used by the user is controllable.
	Data Timeliness		Timeliness is considered out of scope for the work described in this paper. Timeliness depends on the systems managing, transmitting, and monitoring the data.
	Data Validity	○	The method partially addresses data validity by enabling the capture of verification and validation results in the metadata. However, a trusted verification and/or validation system must be used to perform the analysis.
Dependability	Accuracy	•	The method is highly accurate if the certificates are created and managed in accordance with the X.509-PKI standard.
	Availability	•	The use of X.509-PKI are intended to operate in asynchronous environments. Therefore, the ability to verify and validate the certificates should be highly available.

Main Attribute	Sub-category	Addressed	Description of the method's congruence
	Failure Tolerance	•	X.509-PKI is a well-established and stable technology. There are mechanisms in the standard for handling failures
	Flexibility & Robustness	○	The method and governance policy partially address this subcategory. A standardized metadata schema is required to ensure the method is robust enough to handle changes in context. Further study into all industry sectors the method and governance policy may apply to is required. The method and governance policy are minimally viable for usage in highly regulated industries, such as aerospace, automotive, and medical devices.
	Reliability	○	Uncertainty exists as to how reliable the method can be without a standardized metadata schema that is semantically representable. However, the X.509-PKI technology has been proven to be sufficiently reliable.
	Scalability	○	The method and governance policy is intended to be extensible to enable scalability. However, further work is need in establishing a metadata schema that covers the minimum information required for all desired domains.
	Maintainability	•	Using well-established consensus-based standards ensures the highest level of maintainability as system undergo evolution.
Performance	Transaction Time	○	The method was designed to be as efficient as possible. However, the transaction time will also depend on several variables outside the control of the method.
	Throughput	○	The method was designed to be as efficient as possible. However, the throughput will also depend on several variables outside the control of the method.
	Response Time	○	The method was designed to be as efficient as possible. However, the response time will also depend on several variables outside the control of the method.
Usability	Satisfaction	•	The method takes advantage of standards that are well-establish and widely adopted.
	Learn-ability		This sub-category is outside the scope of the data and is the responsibility of the data-managing systems.
	Effectiveness	○	The method and governance policy were studied in the context of a limited set of use cases. Therefore, further work is required to determine all domains where the method and governance policy would enable users to achieve the specified goals of this work.
	Efficiency of Use	○	The method was designed to be as efficient as possible. However, the efficiency of use will also depend on several variables outside the control of the method.
Correctness		○	The method conforms mostly to the utilized standards and specifications. The method is in full compliance with the X.509-PKI standard. However, extensions and/or modifications to several data-format standards are required to fully take advantage of the method and governance policy. [7] provide several modifications required.
Complexity		•	The complexity sub-category addresses inverse relationships such that more service fragmentation is typically considered less trustworthy than monolithic services. The method and governance policy presented in this paper were designed to take those inverse relationships into account. Using the X.509-PKI standard assists in managing the fragmentation by enabling the traceability of the data. Therefore, as data moves between systems and services, the digital certificates can be verified and validated to support trusting the data.

• = fully addressed.

○ = partially addressed.