PARTNERS FOR ADVANCED TRANSPORTATION TECHNOLOGY
INSTITUTE OF TRANSPORTATION STUDIES
UNIVERSITY OF CALIFORNIA, BERKELEY

Modernization of Center-to-Center Data Communication Standards

Task 3713 (65A0761)

TMDD Standards Update Recommendations – Data and System Security

Version 1.1
January 4, 2022

Partners for Advanced Transportation Technology works with researchers, practitioners, and industry to implement transportation research and innovation, including products and services that improve the efficiency, safety, and security of the transportation system.

This page left blank intentionally

Primary Authors

Brian Peterson
Software Engineering Manager
California PATH
University of California, Berkeley

This page left blank intentionally

TABLE OF CONTENTS

LIST OF TABLES

This page left blank intentionally

1. INTRODUCTION

This document provides a set of recommendations for modernization of the Traffic Management Data Dictionary (TMDD) (1), currently at version 3.1. These recommendations are based upon the following:

- Connected Corridors project experience
- Three previous technical memorandums provided under this project discussing the current and future state of transportation, the state of the supporting technology for information exchange, and a review of the TMDD standard
- A gap analysis based on the three technical memorandums delivered as part of this project.

The intention of this document is to inform the Institute of Transportation Engineers (ITE) committee responsible for TMDD, California Department of Transportation (Caltrans), and users of the standard, of potential improvements in the standard that should improve its ability to serve current and future transportation and traffic management needs.

1.1. PURPOSE OF DOCUMENT

This document provides recommendations for modifications to the current TMDD standard. Its goal is to provide a foundation for modernizing the standard. This document specifically provides recommendations for implementing this project’s gap analysis recommendations related to providing security guidance for each approved transmission protocol. Included in this document are recommendations related to a new volume of the specification dealing with minimum security requirements and security recommendations for each data transmission protocol.

The recommendations contained in this report should be used in conjunction with those contained within the other related reports dealing with data structures and data communication protocols for data exchange. The recommendations should be considered for implementation in California transportation projects with center-to-center (C2C) communications and for adoption by the ITE committee responsible for the TMDD standard.

Information systems security is a complex, broad, and fast evolving topic. As such, it is not recommended that any TMDD standard volume address all possible security elements required for C2C communications. Security of applications and systems is also very specific to the needs, risks, impacts, and other individual characteristics of any implementation project. Certainly, security elements such as network security, server security, operating systems, and other key elements cannot and should not be addressed by the TMDD standard. However, there are well understood basics that are fundamental to any implementation of a SOAP web service, as an example, that are considered minimal industry-standard requirements for securing such services. Other methods of data communication have their own specific minimal security requirements. Having minimal security requirements defined within the standard can provide critical information to project managers and others implementing TMDD capable systems that do not have a deep security background. The set of recommendations in this document provide suggestions for the TMDD committee to consider adding a new volume to define minimum security requirements for standard compliant systems implementations as well as references to industry standards. Given the risk filled environment and threats to our critical infrastructure that we live with today, this is a critical need that should be addressed for TMDD implementations. The result should be a more secure and less vulnerable traffic and transportation management system.

NONE OF THE METHODS PROVIDED WITHIN THIS SPECIFICATION PROVIDE A COMPLETE SECURITY SOLUTION. SECURITY IS A COMPLEX SUBJECT WITH IMPACTS NOT ONLY AT THE LEVEL OF EXCHANGING MESSAGES, BUT AT THE ORGANIZATIONAL, IT SERVICES, OPERATING SYSTEM, SERVER, NETWORK, SOFTWARE, DESIGN, AND OTHERS WITH MANY POTENTIAL REQUIREMENTS AND CONSEQUENCES; OPERATIONAL, LEGAL AND ETHICAL.

1.2. INTENDED AUDIENCE

The primary audience for this document includes:

- The Caltrans Division of Research, Innovation, and System Information.
- TMDD Steering Committee
- Caltrans Operations personnel involved in specifying, procuring, and implementation of systems requiring C2C communications
- Transportation systems vendor community

1.3. DOCUMENT ORGANIZATION

The remainder of this document is organized as follows:

- **Section 2** presents the recommendations resulting from the gap analysis for implementation within TMDD
- **Section 3** provides example recommendations regarding the general security needs of a TMDD implementation.
- **Section 4** provides example recommendations for a SOAP implementation of TMDD.
- **Section 5** provides example recommendations for a Kafka messaging implementation of TMDD.

2. HIGH-LEVEL RECOMMENDATIONS

2.1. OBJECTIVES

The objective of these recommendations can be simply stated as follows:

Improve the Traffic Management Data Dictionary to achieve:

a. Reduced future traffic and transportation management system deployment effort and integration costs
b. Support high availability, high volume, real-time communications required for support of future transportation advances
c. Achieve off-the-shelf system integration across jurisdictions and between multiple vendor systems with minimal implementation effort
d. Allow the standard to be flexible enough to adapt to future technology advances and remain relevant in an environment dominated by advances in transportation technology

2.2. DATA STRUCTURE RELATED RECOMMENDATIONS

Within the gap analysis, high-level recommendations were developed within the three areas detailed in the previous technical memorandums, including:

- Technology
- Transportation
- TMDD specification and its implementation

These priorities assume a strategy of first separating the standard into additional volumes as suggested throughout this project to include:

Volume 1 – Concept of Operations and Requirements
Volume 2 – Data Structures and Semantics
Volume 3 – Communication Protocols
Volume 4 – Security Requirements and Recommendations
Guide to the Traffic Management Data Dictionary

Some of these recommendations were related to the user needs and concept of operations as well as the data structures defined within the TMDD specification. In addition, recommendations regarding the need to provide guidance for their implementation in center-to-center communications were included. These recommendations and the priority assigned for implementation within the standard include:

Table 2-1 Recommendations

	Recommendation	Priority
1	Change the TMDD standard to allow additional data transmission formats beyond XML. Create a list of recommended data formats and implementation guidance for each format.	High
2	Change the TMDD standard to allow for additional data transmission methods beyond SOAP. Create a list of recommended data transmission methods and implementation guidance for each.	High
3	Select appropriate technologies that will allow for scalable real-time, high volume communications for use with the standard.	High
4	Allow for the data transmission technology to be selected appropriate for each individual data exchange. Separate the technology selections available from the data structure standards to allow choice and flexibility within the standard.	High
5	For the data exchange technology requirements or recommendations within the standard, provide recommendations or minimum requirements for security implementation, along with references to external security standards appropriate for implementation.	High
6	Increase the release cycle of the TMDD standard, incorporating experience of implementations that require new information sources and more advanced devices. Provide a more active method of review and incorporation of implementation specific extensions within the standard with the goal of adding them to the standard. Actively review the current standard requirements and advances in transportation technology, with the specific purpose of identifying and incorporating new user needs and requirements to prepare the standard for the future.	Medium
7	Add dialogs, messages, dataframes, and data elements for exchange of public messaging activities.	Medium
8	Add the dialogs and associated data structures developed by the I-210 Connected Corridors implementation for use in coordination of response plan and response plan approval activities. Review TMDD for additional needs related to other coordinating activities. Review TMDD for applicability within a multi-jurisdictional, multi-party environment.	High
9	Provide new methods of data exchange capable of scaling to real-time date exchange across large geographic areas and a large number of devices.	High

	Recommendation	Priority
10	Select multi-point broadcast communication technologies, along with updates to the data structure to support multi-party communications. Alternatively, hub/spoke system architectures should be recommended within the standard.	Medium
11	Develop a central registry of authorized and standardized TMCs and other party systems that communicate at a State level within the state transportation community. Provide standardized, unique identifiers for each participant, along with other requirements for participation.	Medium
12	Add additional connection management dialogs to the standard such as: 1. Current subscription list query 2. Subscription status 3. Message status and count information 4. System subscription limitations 5. Data content available within a subscription 6. Subscription discovery Add guidance regarding how systems manage subscriptions for both senders and receivers.	High
13	Provide additional implementation guidance for extensions, along with an improved process for migrating extensions into the base standard. Provide a repository for shared extensions, if not at the national level, at minimum at the state level to minimize engineering and implementation costs of new installations.	High
14	Add guidance and requirements for each dialog for dialog behavior. This should take into account the temporal behavior of the dialog as well as ensuring compatibility with the type of data being transmitted and its temporal characteristics.	High
15	Add guidance for the selection of dialogs and methods to limit dialog behavior to match time-domain behavior of field equipment.	High
16	Provide dialog start-up behavior requirements within the standard.	High
17	Add to the TMDD standard, data trigger standards for each on-change dialog.	Medium
18	Provide additional guidance in how messages, dataframes, and data elements are populated. Provide guidance on enumerations usage.	High
19	Update TMDD to provide guidance in resolving temporal dissonance issues to ensure a common implementation standard.	Medium
20	Standardize the usage of command messages.	High
21	Add clear time field definitions and examples to the standard.	High
22	Provide technology options for implementation of the standard.	High

	Recommendation	Priority
23	Add action elements to inventory messages to provide CRUD operations – Create, read, update, delete Allow additional formats and serializations, including JSON, binary, or others for data messages	High
24	While maintaining SOAP as a protocol, add additional data communication protocols/technologies as options in TMDD implementations. Review, update, and add, as necessary, additional dialogs, messages, dataframes and data elements to the standard. While maintaining the current methods within the standard, with some improvements, add parallel methods of information exchange suited for larger, real-time implementations of the standard. Implementation guidance for minimum system performance should be provided.	High
25	Update the standard to comply with the latest SOAP standard and WS-I. Ensure that future technology updates are implemented in future standard updates.	Medium

In the following sections we will provide specific recommendations for adoption within a new volume 4 (Security Requirements and Recommendations) dedicated to security of communications utilizing the TMDD standard.

3. GENERAL TMDD IMPLEMENTATION MINIMUM SECURITY REQUIREMENTS AND RECOMMENDATIONS

3.1. GOALS AND LIMITATIONS

These recommendations are not provided as a prescriptive for securing systems that implement the Traffic Management Data Dictionary. Rather they are a limited set of minimum requirements for any system implementing the standard. Each project should conduct its own security review and design activities to determine its security needs and requirements. Project owners and managers should implement a secure solution that meets all of the security, availability, and functional requirements of their program.

The recommendations are provided for consideration by the committee and implementers of the standard as a set of minimum requirements for projects to be considered compliant with the standard. The recommendations are based on well-defined industry standard information readily available to developers and implementers of information systems.

3.1.1. GOALS

The goals of these recommendations are:

- Provide those unfamiliar with information systems security who are responsible for contracting, developing, implementing, or maintaining traffic and transportation systems a set of basic information for securing their systems
- Provide minimal security requirements for systems that implement TMDD
- Improve the security of traffic and transportation management systems

3.1.2. LIMITATIONS

These requirements and recommendations within this report, and if adopted by the committee, the standard, do not replace the need for addressing security within a project’s user needs, requirements, design, implementation, and/or maintenance. They do not attempt to address the overall system implementation needs, but rather deal only with basic security implementation recommendations for the communication protocols implemented within the standard. Users of the standard are fully responsible for the security of the systems and their infrastructure of their projects.

This document and the information provided do not address all aspects of security for projects that implement TMDD. Specifically, it does not address security elements such as:

- Data center operations and operating procedures such as incident response, physical access control, or others
- Operating system security, patches, and procedures to Operating System (OS) security
- Software security
- Anti-virus and malware protection
- Network security, firewalls, and related protection elements
- IT organization policies, procedures, and standards such as the Information Technology Infrastructure Library (ITIL) (2) or others
- Other elements not related to the specifics of the data transmission method

3.2. MINIMUM GENERAL REQUIREMENTS

General security requirements for implementers of the standard include the following elements:

- Confidentiality of information in transit
- Owner center authentication
- External center authentication
- Message integrity
- Message confidentiality
- Authorization
- Data schema validation
- Data content validation
- Message size limitations
- Resource limitations
- Message throughput limitations

3.2.1. MINIMUM REQUIREMENTS

The minimum requirements for any implementation of TMDD, regardless of the data transmission technology selected should include the following (most of this is based on the OWASP Web Service Cheat Sheet (3)):

3.2.1.1.Confidentiality of Information in Transit

All information exchanged between centers must be encrypted. Encryption methods may vary depending upon the communication protocol. Transport Layer Security (TLS) is a common method for encrypting information between endpoints, especially for transmission control protocol (TCP) traffic. TLS or some other method, such as Secure Sockets Layer (SSL), a predecessor to TLS, is required for TMDD communications.

3.2.1.2. Owner Center Authentication

Owner center authentication must use digital certificates in order to authenticate. TLS or SSL can be used for authentication. Certificates must be valid and invalid certificates should not be accepted. To be valid, a certificate must:

- Not be expired
- Not be revoked
- Match the domain name of the service
- Issued by a trusted provider

3.2.1.3. External Center Authentication

External centers must authenticate using digital certificates. TLS or SSL can be used for authentication. Certificates must be valid and invalid certificates should not be accepted. To be valid, a certificate must:

- Not be expired
- Not be revoked
- Match the domain name of the service
- Issued by a trusted provider

Note that external center authentication and owner center authentication are two separate authentication processes. In general, they will use the same authentication method. Basic authentication should not be utilized.

3.2.1.4. Message integrity

Centers may consider implementing message specific or message element specific signatures (such as Web Service Security (WS-Security) for SOAP implementations) but should consider the additional overhead and the need for an end-to-end security solution.

3.2.1.5. Message confidentiality

Centers may consider implementing message specific or message element specific encryption (such as WS-Security for SOAP implementations) but should consider the additional overhead and the need for in-message encryption.

3.2.1.6. Authorization

Centers should implement a solution to verify that a requestor, once authenticated, has access to the specific information being requested.

3.2.1.7. Data Schema Validation

TMDD implementations must validate all messages against a known TMDD versioned data schema. Any custom extensions included must also have a schema and messages must be validated against their schema definition. Validation should include all defined elements and the specifics of their definition (data type, length, restrictions/enumerations, count, etc.).

3.2.1.8. Message Content Validation

Data contents must be validated to identify malformed content, data content bomb attacks, and various injection attacks. Attachments such as files to messages are not allowed within TMDD.

3.2.1.9. Message Size Limitations

TMDD implementations must impose message size limitations specific to the project. TMDD provides mechanisms to break up large messages and instead utilize smaller, more frequent smaller messages to send the information. Common methods include incremental updates to inventory and related messages and breaking up messages to a limited number of devices.

3.2.1.10. Resource Limitations

TMDD implementations must limit the computational resources available and usage of resources by individual clients for C2C message processing to that required for maximum expected computational loads. For distributed systems, each node should be limited appropriately, and the scalability (number of nodes) should be limited to that expected under maximum service conditions. Limitations on CPU cycles, memory, open files, database connections, and OS processes should be implemented based on maximum expected load. Active monitoring of load with alarms to warn of abnormal load conditions should be implemented.

3.2.1.11. Message Throughput Limitations

TMDD implementations must be configured to optimize for maximum message throughput. Message throughput should be monitored with alarms to warn of abnormal message throughput conditions.

3.3. GENERAL IMPLEMENTATION RECOMMENDATIONS

Beyond the minimum requirements, implementers of TMDD should consider the following recommendations when implementing TMDD communications. Again, these recommendations are limited to the data transmission and are not expected to cover all aspects of a secure system design.

3.3.1. RECOMMENDATION ELEMENTS

General implementation recommendations address the following topics:

- Other message content validation
- Client authentication
- Fine-grained permissions
- Deployment and design considerations

3.3.1.1.Other Message Content Validation

TMDD implementations should validate message contents against defined validation patterns, especially for fixed data formats such as postal codes, enumerated lists, IP addresses, domain names, email addresses, phone numbers, etc. Project specific enumerated validation values are strongly encouraged (such as a list of allowed IP addresses or domain names). Validation against white-listed values is also strongly encouraged.

3.3.1.2.Client Authentication

Client applications that use TMDD for data communication (not server-to-server but rather client-server) should utilize two-factor authentication or certificate based mutual authentication mechanisms when sending and receiving TMDD message traffic.

3.3.1.3.Fine-grained Permissions

TMDD implementations should consider fine-grained permissions for each service/dialog implemented. As an example, a center that provides only intersection signal data should not be provided permissions to services that capture ramp-meter data. The center instead should only be allowed to access services with which it is capable of interacting.

3.3.1.4.Deployment and Design Considerations

TMDD implementations should consider system design elements that help to provide secure communications. While not exhaustive, these recommendations are key elements to ensure communication between centers remain secure. These design elements include:

- Automate system deployments – modern systems often incorporate deployment automation. Automated deployments can improve resilience to failure, reduce human deployment errors and misconfiguration and allow for systemic correction when issues are discovered, improve configuration management, improve security, and reduce time between patches and system updates.
- Automate implementation of security elements and components

- Include monitoring and alert mechanisms to detect system anomalies, performance incidents, and potential security incidents. If feasible, automate basic security actions to improve incident response.
- Design systems with secret protection, such as encryption of credentials and system configuration elements.
- Utilize zero-trust security principles to limit potential for security incidents and limit the scope of security incidents when they occur.

3.4. OTHER REFERENCES

As owners and operators of critical infrastructure, implementers of TMDD should implement robust security programs within their organizations. The recommendations presented here are a small part of a complete security program.

Information security is a specialized discipline with several different formal frameworks or methods of practice and standards. Each of these frameworks, while they have their own processes and procedures, have common elements. A partial list of modern security frameworks includes:

- Control Objectives for Information and Related Technology (COBIT) (4)
- ISO 27000 series standards (5)
- National Institute of Standards and Technology (NIST) Special Publication 800-53 (6)
- NIST Cybersecurity Framework (7)

Some common elements found in most security frameworks include:

- Secure Organization Practice, including
    - Defining IT management processes and governance practices that support secure organizations
    - Personnel training and support regarding secure practices
    - Organizational resiliency
    - Business continuity
    - Security resource identification and provisioning
    - Organization security policy definition and practice
    - Defining information access and required controls
    - Legal and regulatory implications and controls
    - Privacy controls
    - Critical services analysis and identification
    - Defining organizational risk tolerance
- Secure Information Systems and Data, including
    - Risk assessment, management, and reduction
    - Vulnerability assessment and management
    - Detection, monitoring, auditing, and logging practices

    - Data management and assessment
    - Defining and managing trust relationships
    - Secure systems architecture and design
    - Security incident criticality and impact assessment planning
    - System resiliency and recovery
    - IT operations, maintenance, and management for security
    - Security incident management, operations, and response
    - Access control implementation and maintenance
    - Physical device management and controls
    - External systems identification, management, and controls
    - Encryption practices
    - Networking practices
- Threat Assessment, including
    - Threat actor identification and assessment
    - Threat intelligence
    - Threat likelihood analysis

While the vast majority of this is beyond the scope of the TMDD standard, many of these elements have direct impact on securing data communications based on the TMDD standard.

TMDD information exchange between organizations must comply with the information security practices of each organization. Each of the elements above, as well as others identified by the organizations involved, should be considered within the implementation of a TMDD C2C information exchange.

Other references that can provide guidance in this area include the following:

Cybersecurity and Infrastructure Security Agency Transportation Systems Sector Cybersecurity Framework Implementation Guide
https://www.cisa.gov/publication/tss-cybersecurity-framework-implementation-guide

NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

ISO 27000 series of security standards
https://www.iso.org/standard/73906.html
https://www.iso.org/isoiec-27001-information-security.html
https://www.iso.org/standard/54533.html

NIST Special Publication 800-53
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NIST Special Publication 800-171
https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

CIS Controls
https://www.cisecurity.org/controls/

Control Objectives for Information and Related Technology (COBIT)
https://www.isaca.org/resources/cobit

4. SOAP WEB SERVICE SECURITY

SOAP services are generally secured with many of the same methods as other web services. Implementers of TMDD should comply with the minimum security requirements specified in Section 3. This section will discuss specific SOAP security mechanisms available and when they should be utilized within a C2C communication using TMDD.

4.1. WS-SECURITY

In addition to basic security mechanisms available to system communications discussed in Section 3, SOAP services have a specific security mechanism developed for their use, WS-Security. WS-Security does have an advantage over point-to-point security mechanisms such as TLS. WS-Security provides end-to-end security, having the credentials information for authentication and encryption within the message header itself. For implementations with network proxies at the boundary of a center which provide the TLS implementation, WS-Security ensures that the endpoint behind the proxy can authenticate the sender and can ensure the confidentiality of the message behind the proxy.

However, WS-Security adds significant overhead to message processing and message size, since the security information must be embedded into the message itself as opposed to the transport layer, as in TLS. As a result, performance of TMDD implementations utilizing WS-Security will be negatively impacted when using it. WS-Security also adds complexity at the application layer since the security is directly added to each message.

As a result of this tradeoff, it is not specified as a minimum requirement for TMDD implementations, but should be considered when intermediaries such as a proxy are required and the information is deemed particularly sensitive or the proxy is not fully trusted. Projects implementing TMDD communications should consider the advantages and negative performance impacts within their design process.

If WS-Security is utilized, the following mechanisms are available for implementation of a WS-Security solution:

- Basic authentication with a username/password combination (prohibited for TMDD implementations)
- X.509 certificate with public/private key pair. An optional message expiration time can be provided as well
- Kerberos
- Digital signature
- XML encryption

4.2. MINIMUM REQUIREMENTS IMPLEMENTATION FOR SOAP

Details for the minimum requirements for TMDD implementations utilizing SOAP include the following:

4.2.1.1.Confidentiality of Information in Transit

All information between centers must be encrypted. Transport Layer Security (TLS) must be utilized for encrypting information between endpoints.

4.2.1.2.Owner Center Authentication

Owner center authentication must use digital certificates in order to authenticate. TLS must be used for authentication. Certificates must be valid and invalid certificates should not be accepted. To be valid, a certificate must:

- Not be expired
- Not be revoked
- Match the domain name of the service
- Issued by a trusted provider

4.2.1.3.External Center Authentication

External centers must authenticate using digital certificates. TLS must be used for authentication. Certificates must be valid and invalid certificates should not be accepted. To be valid, a certificate must:

- Not be expired
- Not be revoked
- Match the domain name of the service
- Issued by a trusted provider

Note that external center authentication and owner center authentication are two separate authentication processes.

4.2.1.4.Message integrity

Centers may consider implementing message specific or message element specific signatures utilizing WS-Security for SOAP implementations but should consider the additional overhead and the need for an end-to-end security solution.

4.2.1.5. Message confidentiality

Centers may consider implementing message specific or message element specific encryption utilizing WS-Security for SOAP implementations but should consider the additional overhead and the need for in-message encryption.

4.2.1.6. Authorization

Centers should implement a solution to verify that a requestor, once authenticated, has access to the specific information being requested.

4.2.1.7. Data Schema Validation

TMDD implementations must validate all messages against a known TMDD versioned data schema (XSD). Full coverage of the XSD schema and any referenced XSDs is required. Any custom extensions included must also have a schema. Validation should include all defined elements and the specifics of their definition (data type, length, restrictions/enumerations, count, etc.).

4.2.1.8. Message Content Validation

Data contents must be validated to identify malformed content, data content bomb attacks, and various injection attacks. Attachments such as files to SOAP messages should be avoided within TMDD messages and if allowed, should be validated and scanned for malicious content.

4.2.1.9. Message Size Limitations

SOAP message size limitations should be imposed for TMDD implementations. This ensures that an attacker or inadvertent send of large SOAP messages cannot disrupt or cause failure of a TMDD message exchange service.

4.2.1.10. Resource Limitations

Applies to SOAP messaging. See paragraph 3.2.1.10.

4.2.1.11. Message throughput limitations

Applies to SOAP messaging. See paragraph 3.2.1.11.

4.3. GENERAL IMPLEMENTATION RECOMMENDATIONS FOR SOAP

Beyond the minimum requirements, implementers of SOAP-based TMDD services should consider the following recommendations when implementing TMDD communications. Again, these recommendations are limited to the data transmission and are not expected to cover all aspects of a secure system design.

4.3.1. IMPLEMENTATION RECOMMENDATION ELEMENTS

General SOAP-based implementation recommendations address the following topics:

- Other Message Content Validation
- Client Authentication
- Fine-grained permissions

4.3.1.1. Other Message Content Validation

Recommended for SOAP messaging. See paragraph 3.3.1.1.

4.3.1.2. Client Authentication

Recommended for client to server authentication utilizing SOAP messaging. This is not a common use case. See paragraph 3.3.1.2.

4.3.1.3. Fine-grained Permissions

Recommended for SOAP messaging. See paragraph 3.3.1.3.

5. KAFKA MESSAGING WITH JSON OR AVRO MESSAGE DELIVERY

Implementations using Kafka, whether using JSON or Avro message serialization, should consult both the Apache Kafka (8) and Confluent Kafka (9) documentation for security recommendations. These two sources provide extensive information and recommendations to securely implement Kafka within Intelligent Transportation Systems (ITS) environments.

Some general recommendations regarding using Kafka as a data transport between traffic management centers, include:

- Each organization should utilize their own Kafka installation, providing full control of their own systems environment, connected traffic management systems/centers, networking, encryption, authorization and authentication, and ensuring internal responsibility for securing their own environments. Smaller centers with simple connectivity requirements to another center may opt for direct connection of client systems to another center’s Kafka instance, but this is not recommended.
- Creating zero-trust environments, treating both internal and external integrations equally, with full encryption, authentication, authorization, networking, and other security elements is highly recommended. Ensuring that this level of security is in place, even within components of a Kafka implementation is critical to a secure environment.
- Authentication and authorization for Kafka should fully implement a principle of least privilege
- Organizations should consider security requirements when selecting the version of Kafka and Kafka components. Different versions of Kafka and its components have varying security features, and in general, regardless of source (open-source, commercial community version, or commercial enterprise version), the latest stable version should be selected. Commercial versions have increased security features such as configuration file and secret encryption, additional logging capabilities, and role-based security.
- Network security should isolate Zookeeper from any organizationally external connection or public internet. Network security should restrict access to Kafka components to only endpoints and ports required for operation.

5.1. MINIMUM REQUIREMENTS IMPLEMENTATION USING KAFKA

Details for the minimum requirements for TMDD implementations utilizing Kafka include the following:

5.1.1. CONFIDENTIALITY OF INFORMATION IN TRANSIT

All information exchange between centers must be encrypted. Kafka provides for SSL encryption. In addition to information between centers, it is highly recommended to encrypt all internal Kafka connections as well, including communications between Kafka components and between Zookeeper and the broker. Connections between broker nodes should be encrypted. SSL shall use TLS 1.2. SSL implementations shall use an SSL truststore password. HTTP connections such as the Kafka REST proxy shall also use mTLS for authentication and encryption.

5.1.2. OWNER CENTER AND EXTERNAL CENTER AUTHENTICATION

Kafka provides for authentication via SSL or Simple Authentication Security Layer (SASL). Use of SSL provides the benefit of encryption as well. Hostname verification must be used within SSL. Owner and external centers shall mutually authenticate.

It is highly recommended that authentication also be enabled between Kafka components.

Certificates must be valid and invalid certificates should not be accepted. To be valid, a certificate must:

- Not be expired
- Not be revoked
- Match the domain name of the service
- Issued by a trusted provider

5.1.3. CLIENT AUTHORIZATION

Each Kafka broker, external or owner center, shall implement client authorization, specifying read, write permissions via Access Control List (ACL) definition. Authorizations shall be specific to the user, operation, host, and resource.

5.1.4. DATA SCHEMA VALIDATION

TMDD implementations must validate all Kafka events/messages against a known TMDD versioned JSON or Avro data schema. Full coverage of the schema and any referenced schemas is required. Any custom extensions included must also have a schema. Validation should include all defined elements and the specifics of their definition (data type, length, restrictions/enumerations, count, etc.).

5.1.5. MESSAGE CONTENT VALIDATION

Data contents must be validated to identify malformed content, data content bomb attacks, and various injection attacks.

5.1.6. MESSAGE SIZE LIMITATIONS

Kafka event/message size limitations shall be imposed for TMDD implementations. This ensures that an attacker or inadvertent send of large events/messages cannot disrupt or cause failure of a TMDD message exchange service.

5.1.7. MESSAGE THROUGHPUT LIMITATIONS

Kafka implementations shall enforce client quotas. Kafka provides for both producer and consumer byte rate quotas.

This page left blank intentionally

6. REFERENCES

1. **Engineers, Institute of Transportation.** Traffic Management Data Dictionary (TMDD) Standard for the Center-to-Center Communications. *Insitute of Transportation Engineers.* [Online] 2020. https://www.ite.org/technical-resources/standards/tmdd/.
2. **Axelos.** ITIL Certifications. *Axelos.com.* [Online] 2021. https://www.axelos.com/certifications/itil-service-management.
3. **Open Web Application Security Project.** OWASP Web Service Security Cheat Sheet. *OWASP Cheat Sheet Series.* [Online] 2021. https://cheatsheetseries.owasp.org/cheatsheets/Web_Service_Security_Cheat_Sheet.html.
4. **Association, Information Systems Audit and Control.** COBIT. *ISACA.* [Online] 2021. https://www.isaca.org/resources/cobit.
5. **Standardization, International Organization for.** ISO 27001. *ISO.* [Online] 2021. https://www.iso.org/isoiec-27001-information-security.html.
6. **National Institute of Standards and Technology.** Computer Security Resource Center SP 800-53 Rev. 5. *NIST.* [Online] 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
7. —. NIST Cybersecurity Framework. *NIST.* [Online] 2021. https://www.nist.gov/cyberframework.
8. **Apache Software Foundation.** Apache Kafka. *Apache.* [Online] 2021. https://kafka.apache.org/.
9. **Confluent.** Confluent Platform. *Confluent.* [Online] 2021. https://www.confluent.io/product/confluent-platform/.

This page left blank intentionally