

# Kansas TRCC

## Kansas eCitation Security Model Design

Detailed Design Document

Version 1.1.1

## Table of Contents

|       |                                  |    |
|-------|----------------------------------|----|
| 1     | Intent.....                      | 3  |
| 2     | Overview .....                   | 3  |
| 3     | Scope and Limitations .....      | 3  |
| 4     | Security Requirements.....       | 4  |
| 4.1   | Security Risks.....              | 4  |
| 4.2   | System Requirements .....        | 4  |
| 5     | Security Architecture .....      | 4  |
| 5.1   | User Interface Security.....     | 5  |
| 5.1.1 | User Authentication .....        | 6  |
| 5.1.2 | Access Control.....              | 6  |
| 5.1.3 | Audit Trail.....                 | 6  |
| 5.2   | Web Service-Level Security ..... | 6  |
| 5.2.1 | Submission Service.....          | 8  |
| 5.2.2 | Inquiry Service.....             | 8  |
| 5.3   | Database Security .....          | 9  |
| 6     | Appendix A – References .....    | 10 |
| 7     | Appendix B – Definitions.....    | 10 |

## 1 Intent

This document will define in detail the design of the security model that will be used in the eCitation system.

This document is intended to serve as technical documentation of the Kansas eCitation Security model.

This is a technical document and is intended for technical audience.

## 2 Overview

The Traffic Records Coordinating Council (TRCC) commissioned a Strategic Plan for the development and implementation of a statewide electronic traffic citation (eCitation) system, with a central traffic citation information repository (central repository) accessible by state, local, and federal agencies, and the public. This eCitation system is an integral part of the statewide Traffic Records System (TRS) program initiated in 2005 and will integrate with the Kansas Criminal Justice Information System (KCJIS). The TRS will be a virtual data warehouse that will provide state and local agencies with the ability to efficiently access traffic data to increase the safety of the motoring public. It will bring together information that is currently housed in separate, isolated repositories at KDOT, KHP, KDOR, KBI, KDHE, KBEMS and other agencies.

As a vital component of the TRS system, the eCitation project has been initiated with the goal of implementing a statewide eCitation system through which traffic citation data can be collected, analyzed, and distributed accurately, quickly, and cost effectively for the benefit of the public and state, local, and federal agencies.

To accomplish its goals, the architecture for this project needs to allow data sharing among the participating agencies. However, as with any system that allows data sharing come security risks. This Security Model Design document will detail out the security model for eCitation System that will mitigate the identified risks which the system will be exposed to.

## 3 Scope and Limitations

The scope of this Security Model Design covers security design that is applicable to eCitation System and its components including:

- eCitation Submission Service
- eCitation Inquiry Service
- eCitation Repository

It will not cover security requirements or design for other systems outside of eCitation.

## 4 Security Requirements

The CJIS Security Policy is considered to be Sensitive But Unclassified (SBU) material. This policy may not be posted to a public website and discretion must be exercised in sharing the contents of the policy with individuals and entities who are not engaged in law enforcement or the administration of criminal justice. A copy may be obtained by contacting the state’s CJIS Systems Officer (CSO).

### 4.1 Security Risks

Given the system architecture described in the High Level Design document, the following are potential risks that can be mitigated by the security model design for eCitation System:

- Unauthenticated access
- Unauthorized access
- Misuse of user or network profiles
- Malicious XML injection

### 4.2 System Requirements

To be able to implement the security model in this document, the following system requirements must be met:

- All submitting agencies must operate within an authenticated KCJIS network VPN.
- Systems must connect via a firewall-to-firewall VPN or username / password authenticated client VPN connection.

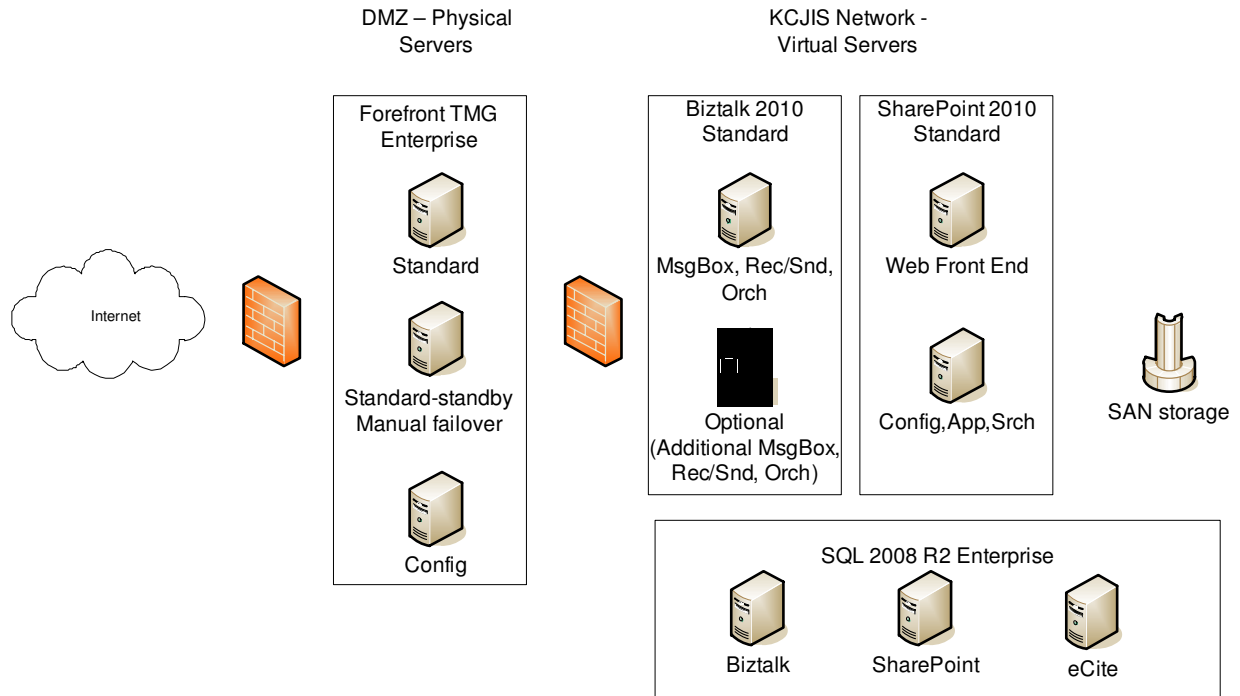
## 5 Security Architecture

The following table summarizes the security aspects leveraged for each of the eCitation components.

| Component          | Consumer                            | Transport Protocol         | Authentication Method  |
|--------------------|-------------------------------------|----------------------------|--|
| Submission Service | External KCJIS Authorized User      | HTTP over KCJIS Secure VPN | None   |
| Inquiry Service    | Internal Protected KBI network only | HTTP                       | None   |
| User Access        | External KCJIS Authorized User      | HTTPS or Secure VPN        | username/password/one time token(Strong Two-Factor Authentication) |
| Database           | Internal Protected KBI network only | Unsecured                  | Trusted DB credentials   |

The following security architecture is designed to mitigate security risks identified for the designed system architecture.

A diagram of the eCitation system security architecture is depicted in Figure 1.



**Figure 1. eCitation System Security Architecture.**

The major entities that will be sharing and consuming information to and from the eCitation System include the following:

- Submitting Agencies – KHP/KLER, and other agencies providing Citation data to the eCitation system.
- Law Enforcement Agencies / Officers
- Other authorized agencies

## **5.1 User Interface Security**

Any direct user interface to eCitation System components (for inquiry or access to eCitation records) will only be available through existing secured KCJIS applications such as the KCJIS Web Portal or the Central Message Switch (CMS) and therefore is subject to the same policies employed by the KCJIS security. This section describes how the security model is applied to direct user interaction with eCitation components.

In particular, the KCJIS Portal is developed as .Net web-based applications, includes the two factor RSA authentication, the KCJIS authorization model and will be configured as a secure web site using SSL with support for 128 bit or higher server encryption. Client certificates are not required.

### 5.1.1 User Authentication

End users directly accessing eCitation components for data inquiry will authenticate using application-level security mechanisms, which utilize a login screen where they will be required to provide their username and password. Because the users authenticate within a trusted application by validating their username, password and RSA token passphrase against an existing user authentication repository, the eCitation services will not require additional authentication. This security model represents a *trusted sub-system* model.

### 5.1.2 Access Control

Once a user is authenticated, authorized users will have access to eCitation components through the identical access control mechanism that currently protects other aspects of the KCJIS portal and using the existing KCJIS user authorization repository. This approach allows the KCJIS user administrators to make use of the familiar administrative tools to grant (or deny) access to eCitation features to agencies and users.

### 5.1.3 Audit Trail

All user actions within the eCitation System will be audited, recording the user, date/time, purpose (for inquiry only) and the action being performed. The auditable actions within the application include citation submission, inquiry, and report generation. Access to individual detail records will be audited to level of the record being accessed. Users with administrative privileges will be able to view the audit log.

The audit log information may be used to investigate any potential misuse of the access to the data.

## 5.2 Web Service-Level Security

Two major components of the eCitation System are the eCitation Submission Service and the eCitation Inquiry Service which are implemented as a Web services. The security architecture for the eCitation services can be separated into two components, the submission service and the inquiry service. The submission service, which accepts and houses citation records from eCitation applications within the state of Kansas, has different security requirements from the inquiry service which processes search queries from end users and returns matching citation records. The security requirements for each of the two services are summarized in the following table:

**Table 1. Web Service Requirement Summary.**

| System Component   | Requirement Summary   |
|--------------------|---|
| Submission Service | <ul style="list-style-type: none"> <li>Purpose – The acceptance of one or more citation records, in a batch,</li> </ul> |

|                 |   |
|-----------------|---|
|                 | <p>submitted to the eCitation repository for indexing</p> <ul style="list-style-type: none"> <li>• Scope – Trusted applications that create and format batch files in the required eCitation format</li> <li>• System Authentication – Devices are authenticated by their network source (IP address or VPN source).</li> <li>• User Authentication – User authentication is problematic because there is no mechanism to authenticate either the user that created the citation or the user that submitted the batch of citations for processing. No user authentication will be performed in the submission service.</li> <li>• Encryption – Citation data will be encrypted while being transmitted over unsecured and private networks. Citation data is not required to be encrypted while being processed and housed in the repository.</li> <li>• Logging – The identifying characteristics of the device that submits the data (IP address) with the status and timestamp of the submission will be logged with the submission.</li> </ul>  |
| Inquiry Service | <ul style="list-style-type: none"> <li>• Purpose – Provide the ability to search the citation repository for relevant records based on a search query.</li> <li>• Scope – Authenticated users logging into KCJIS web portal application. No other applications are expected to be system level consumers of the Inquiry Service.</li> <li>• System Authentication – Devices are authenticated by their network source (IP address).</li> <li>• User Authentication – End users are authenticated at the application level using username / password / RSA token. By assuring that end user actions originate via trusted applications, user authentication need not be performed within the Inquiry Service.</li> <li>• Encryption – Citation queries and search results will be encrypted while being transmitted over unsecured and private networks. Citation data is not required to be encrypted while being processed.</li> <li>• Logging – The identifying characteristics of the end user performing the query (username, agency ORI) will be logged with the query that was performed, timestamp of the query request and the records that were returned with a detailed query.</li> </ul> |

The following section describes the design and how it meets the security requirements.

## 5.2.1 Submission Service

The submission service will be implemented as a Basic HTTP Web service. Per the current industry convention, a Basic HTTP Web service does not require any form of authentication, nor does it provide for any manner of encryption at the message level. This approach will meet the requirements and will provide the low barrier-to-entry solution that the participating agencies seek.

It should be noted that the lack of user authentication and encryption at the message level will prevent the submission service from exhibiting the following features:

- Message Level Privacy – Because the message itself cannot be encrypted, the confidentiality of the message must be protected in other ways (via HTTPS transport protection, ensuring the message is stored in a secure repository and not logged in unprotected location). The Submission Service relies on the KCJIS Network security architecture to provide this capability.
- Integrity – Without any way to provide an encrypted digital signature, no mechanism is available to ensure that the contents of the message were not modified between systems. The Submission Service relies on the KCJIS Network security architecture to provide this capability.
- Originator – Without authenticating the user creating or submitting the citation, there is no verifiable record as to who created or submitted a citation.
- Non-repudiation – A similar cause for concern is that without user authentication, a user could make a valid claim that they did not create or submit a citation that is in their name.

Of the four features named above, the ability to identify the originator should be considered the most commonly required feature. The lack of this feature does not invalidate the ability to meet the KCJIS security policy as long as the device can be authenticated by the network source (IP address or VPN). At a later phase of the project, if the GFIPM security model is implemented, information about a logged-in user would be passed with the submission. The external systems would be able to pass the user GFIPM token to the service, allowing the service to have the full context of the user performing the action.

The following information will be logged to meet the audit requirements of the eCitation submission service.

- Received date/time
- Status of transaction (success, failure)
- IP address (in the firewall log – add to the audit database)

To provide the other system capabilities, some level of user / client digital certificate support would be required. It is beyond the scope of this design to provide those capabilities, but they are noted for completeness.

## 5.2.2 Inquiry Service

The inquiry service will be implemented as a Basic HTTP Web service. Per the current industry convention, a Basic HTTP Web service does not require any form of authentication, nor does it provide

for any manner of encryption at the message level. This approach will meet the requirements and will provide the low barrier-to-entry solution that the participating agencies seek. The service is assured that the request originates from a trusted application and therefore the service can trust that the user has successfully authenticated and that the user assertions (username, agency ORI) provided in the request are valid. During the current phase of the project, the client applications (KCJIS Portal and CMS) will be required to explicitly add the user assertions to the request, while at a later phase, if the GFIPM security model is implemented, the portal would pass the user GFIPM token to the service as a means of providing the user assertions.

The following features are not expected to be implemented:

- Message Level Privacy – Because the message itself will not be encrypted, the confidentiality of the message must be protected in other ways (via HTTPS transport protection, ensuring the message is stored in a secure repository and not logged in unprotected location). The Inquiry Service relies on the KCJIS Network security architecture to provide this capability.
- Integrity – Without any way to provide an encrypted digital signature, no mechanism is available to ensure that the contents of the message were not modified between systems. The Inquiry Service relies on the KCJIS Network security architecture to provide this capability.

The following information will be logged to meet the audit requirements of the eCitation Inquiry service.

- User ID
- Date and Time of Request
- Search Parameters
- Search Response (only for a detail request)

To provide these system capabilities, some level of user / client digital certificate support would be required. It is beyond the scope of this design to provide those capabilities, but they are noted for completeness.

### ***5.3 Database Security***

The eCitation System will be using Microsoft SQL Server 2008 as its database system. The database server will be secured behind firewalls and access to system and application databases will be restricted to authorized administrative users only. Access to SQL Server ports will be restricted to within the KCJIS intranet. All access to data from the various sub-systems of the eCitation system will be using stored procedures. Every sub-system within the eCitation System will have separate user database accounts to access the database from the application. The permissions to execute the stored procedures will be provided only to these database accounts.

## 6 Appendix A – References

|   |   |
|---|---|
| Kansas eCitation High-level Design Document | <a href="https://projects.analysts.com/kansasecitation/internal/Shared%20Documents/Phase%201B%20Deliverables/KS%20E-Cite%20High-level%20Design%20V1.2.docx">https://projects.analysts.com/kansasecitation/internal/Shared%20Documents/Phase%201B%20Deliverables/KS%20E-Cite%20High-level%20Design%20V1.2.docx</a> |
| Statement of Work                           | <a href="https://projects.analysts.com/kansasecitation/SignedDocuments/Kansas%20eCitation%20Project%20Phase%201C%20SOW%2012.28.2010.pdf">https://projects.analysts.com/kansasecitation/SignedDocuments/Kansas%20eCitation%20Project%20Phase%201C%20SOW%2012.28.2010.pdf</a>                                       |

## 7 Appendix B – Definitions

| Acronym/Term | Definition   |
|--------------|--|
| SBU          | Sensitive But Unclassified                         |
| CSO          | CJIS Systems Officer                               |
| XML          | eXtensible Markup Language                         |
| KLER         | Kansas Law Enforcement Reporting System            |
| HTTPS        | Hypertext Transfer Protocol Secure                 |
| ORI          | Originating Agency ORI                             |
| VPN          | Virtual Private Network                            |
| GFIPM        | Global Federated Identity and Privilege Management |