Defence Research and Development Canada | Recherche et développement pour la défense Canada

Canada Border Services Agency (CBSA) National Information Exchange Model (NIEM)-Based Information Exchange

Daniel Charlebois
DRDC – Centre for Security Science

Defence Research and Development Canada
Scientific Letter
DRDC-RDDC-2017-L416
November 2017

Canada

IMPORTANT INFORMATIVE STATEMENTS

The information contained herein is proprietary to Her Majesty and is provided to the recipient on the understanding that it will be used for information and evaluation purposes only. Any commercial use including use for manufacture is prohibited.

Disclaimer: Her Majesty the Queen in right of Canada, as represented by the Minister of National Defence ("Canada"), makes no representations or warranties, expressed or implied, of any kind whatsoever, and assumes no liability for the accuracy, reliability, completeness, currency or usefulness of any information, product, process or material included in this document. Nothing in this document should be interpreted as an endorsement for the specific use of any tool, technique or process examined in it. Any reliance on, or use of, any information, product, process or material included in this document is at the sole risk of the person so using it or relying on it. Canada does not assume any liability in respect of any damages or losses arising out of or in connection with the use of, or reliance on, any information, product, process or material included in this document.

This document was reviewed for Controlled Goods by Defence Research and Development Canada (DRDC) using the Schedule to the *Defence Production Act*.

Defence Research and Development Canada | Recherche et développement pour la défense Canada

DRDC | RDDC
technologysciencetechnologie

November 2017

DRDC-RDDC-2017-L416

Prepared for: Mark Williamson, Director General, Centre for Security Science

Scientific Letter

Canada Border Services Agency (CBSA) National Information Exchange Model (NIEM)-Based Information Exchange

Introduction

This paper is intended to inform DG DRDC CSS and Canada Border Services Agency (CBSA) information management services regarding the outcomes of the CSSP-2013-TI-1046 CBSA Secure Data Exchange project. The project implemented a standards-based approach to securely exchange sensitive information between CBSA, the Canadian Nuclear Safety Commission (CNSC) and Health Canada.

Background

CBSA shares information with other organizations in order to ensure proper decision making for Canadian safety and security. In particular, when cargo reaches a Canadian entry point, information is collected and shared only with the appropriate government departments, law enforcement, health agencies, etc. Current capabilities do not allow them to ensure proper information handling in an effective and efficient manner. This project demonstrated the ability to improve effectiveness and efficiency by packaging information based on National Information Exchange Model (NIEM) [1] specifications as well as improve the confidentiality and integrity by applying cryptographic solutions.

CBSA's mandate is to manage the nation's borders at ports of entry by administering and enforcing the domestic laws that govern trade and travel, as well as international agreements and conventions. The work of the Canada Border Services Agency includes identifying and interdicting high-risk individuals and goods, working with law enforcement agencies to maintain border integrity and engaging in enforcement activities, including seizure of goods, arrests, detentions, investigations, hearings and removals [2].

Supported by DRDC CSS, CBSA has conducted a proof-of-concept for its SensorNet information architecture. Specifically, the Secure Access Management for Secure Operational Networks (SAMSON) [3] technology demonstrator was used to show how the protection of SensorNet data could be enhanced within the CBSA network environment through the application of Data-Centric SecurityCom principles. This proof-of-concept was originally described in Data-Centric SecurityCom for CBSA Operations – SAMSON Database Protection for the CBSA SensorNet [4].

Under the auspices of this research CBSA also conducted an examination of the NIEM as a potential standard to enable information exchange. Specifically, the investigation assessed how data-centric security is supported through NIEM and how it could enable inter-domain exchanges using trust infrastructures such as SAMSON. It was the position of that report that a data-centric security approach to

information protection both leverages the standardization of information exchange transactions based on NIEM and also enhances the protection of, access to and auditing of information assets that are exchanged via NIEM. This investigation was documented in Data-Centric SecurityCom and Information Sharing via NIEM [5].

Since the completion of these two reports, CBSA has produced an Information Interoperability – Architecture Vision [6] document that includes the following vision statement: "*Harmonize and optimize information exchanges between CBSA and its partners through adoption of standards*." Furthermore, it recommends as a strategic approach that CBSA projects adopt NIEM and the Government of Canada (GC) Interoperability Framework standards.

This Scientific Letter documents the efforts to prototype a NIEM exchange based on a CBSA radiation scanning scenario. The prototype will leverage the Data-Centric SecurityCom Services (DCSS) information protection architecture[1] to secure, and control access to, sensitive radiation scan data both within CBSA and when exchanged with Other Government Departments (OGDs).

CBSA Marine Ports

Radiation detection equipment is located at Marine Ports in order to prevent dangerous goods from entering the country. Radiation detection portals (illustrated in Figure 1), which are the primary scanning devices, are used to non-intrusively scan all shipping containers arriving at Canadian marine ports. Any shipping containers with an elevated reading, above normal background levels, generate an alarm and undergo a risk assessment and further radiation examination to determine the cause and extent of the radiation. This is done at the National Targeting Centre (NTC). It is worth mentioning that less than 1% of containers trigger an alarm, and, of this 1%, 80% will be cleared quickly as the radiation is naturally occurring. The remaining alarms require a more detailed secondary scan. A secondary scan typically relies on a carborne unit or a Heiman Cargo Vision Mobile (HCVM) / Vehicle and Cargo Inspection System (VACIS) unit. As the name implies, a carborne unit is one in which the radiation monitoring system is affixed to the roof of a vehicle. Both HCVM/VACIS units are mobile scanners.

Figure 1: Radiation Detection Portal [4].

[1] The Data Centric Security Services (DCSS) architecture is based on the DRDC TDP project SAMSON (Charlebois, Daniel; Henderson, Glen; Simmelink, Darcy; Carruthers, Bruce, 2013) architecture.

National Targeting Centre

CBSA Targeters and NTC Supervisors are responsible for reviewing alarms generated by the radiation detection portal (primary scan). The alerts are received on the Radiation Alarm Viewer (RAV) and compared against the manifest in order to determine whether the radiation is naturally occurring or if further investigation is required. Personnel within the NTC also review advance cargo information prior to the shipment arriving on Canadian soil, or in some cases, prior to leaving the foreign port. Shipments that have been identified as high risk are referred for examination at the first point of arrival or intervention.

Science & Engineering Directorate

Research Safety Officers (RSOs) within the Science & Engineering Directorate (SED) are responsible for deciding whether a secondary scan is warranted and whether the shipping container should be quarantined. The scan and manifest information is entered in the Incident Reporting Tool (IRT). RSOs are also responsible for notifying OGDs, if warranted.

Other Government Departments

When shipments with high levels of radiation are detected, CBSA informs both the Canadian Nuclear Safety Commission (CNSC) and Health Canada in order to prevent radioactive goods from entering Canada and causing health/safety problems to the general public. The CNSC regulates the use of nuclear energy and materials to protect health, safety, security and the environment and to implement Canada's international commitments on the peaceful use of nuclear energy; and to disseminate objective scientific, technical and regulatory information to the public (Government of Canada - Canada Nuclear Safety Commission). Specifically, the CNSC has developed detailed procedures and identified service standards for the treatment of containers that trigger alarms for man-made radiation. Health Canada is the lead department responsible for coordinating the nuclear emergency response of more than eighteen federal organizations in support of impacted provinces and territories.

CBSA Radiation Scenario

The CBSA radiation scenario is based on the RADNet Response Chart found in Ref [4] and follow-up discussion with CBSA subject matter experts. The CBSA radiation scenario, as illustrated in Figure , consists of the following twelve steps:

1. The Radiation Detection Portal (primary scanning device) scans a shipping container at a marine port. The Radiation Portal Monitor (RPM), which records the primary scan in a database and in a file share, identifies that a reading in the scan exceeds a predetermined threshold;
2. The RPM automatically pushes the portal alert event to a database (database-to-database transfer) in the National Targeting Centre (NTC);
3. The CBSA Targeter (3a) views the Portal Alert Event in the Radiation Alarm Viewer (RAV) and compares it with the e-manifest for the shipping container. If the CBSA Targeter does not respond in a predetermined period of time then the Portal Alert Event is automatically sent to the NTC Supervisor (3b) for action;
4. If the Portal Alert Event is at odds with the e-manifest then the CBSA Targeter calls the Radiation Safety Officer (RSO) in the CBSA SED;

5. The RSO makes a determination as to whether secondary scanning is warranted for the shipping container. Note that the NTC Targeter also has the authority to request a carborne exam independent of the RSO. In this case the RSO will still need to be contacted to review the spectrum;
6. The CBSA Targeter calls the Local CBSA at the marine port and requests a secondary scan. The Carborne Radiation Detection System (CRDS) is used to perform the secondary scan. As part of the scanning process, the CBSA NTC targeter will contact the Terminal Operator to place a hold on the shipping container;

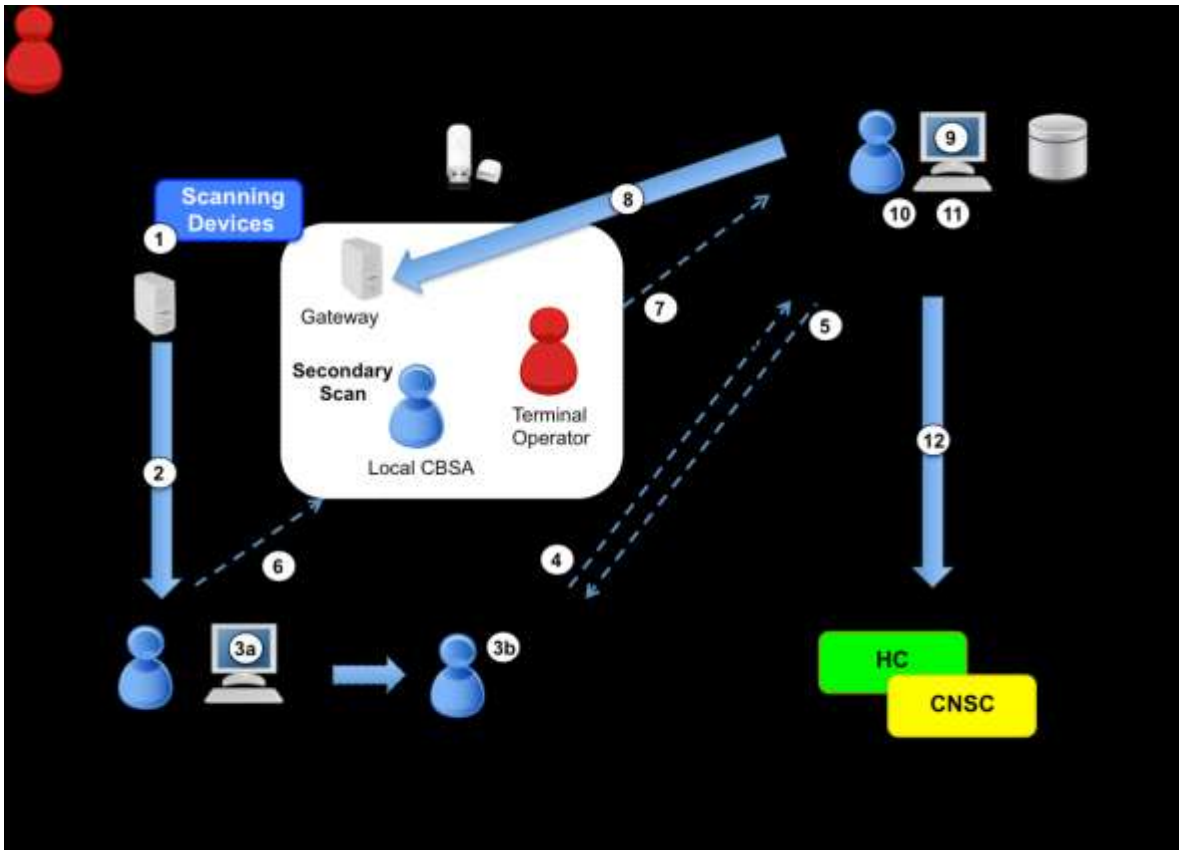

Figure 2: CBSA Radiation Scenario [4].

7. Once the secondary scan has been completed, the Local CBSA will call the RSO and provide notification that the secondary scan results are available for download;
8. The RSO will acquire the secondary scan results. In the case of the carborne scan, the RSO will download the scan from a gateway. In the case of the HCVM/VACIS, scan data is transferred to a workstation via a USB stick. From there it is emailed to the RSO;
9. The RSO, who stores the scan results and images in the Incident Reporting Tool, will examine the secondary scan results and make a determination as to the type of response required;
10. If the carborne scan results are still not conclusive the CBSA RSO will escalate the file to a senior CBSA RSO who will then review the carborne exam results and the manifest data. The senior RSO may then request that an HCVM/VACIS exam is performed;

11. If an HCVM/VACIS exam is requested the results will be reviewed by the Senior RSO and a determination made as to whether the container needs to be forwarded to an OGD; and
12. The RSO will send the scan results (primary scan, secondary scan, image files (HCVM) and templates) via email to the OGDs (CNSC and Health Canada) for incident response.

The sample data provided by CBSA is from alarm #184863 which occurred in Halifax in September 2014. This alarm[2] was selected because the shipping container contained stainless steel contaminated with Co-60 during the recycling process. This alarm was eventually sent for a secondary exam using the mobile carborne unit, an HCVM exam to examine the contents, and then referred on to the CNSC for enforcement. The sample data consists of the following:

- Radiation Detection Portal Scan (Primary Scan);
- Alert Data;
- RAV Alert Page;
- Carborne Scan (Secondary Scan);
- HCVM/VACIS Image; and
- Template.

Experimental Approach

The intent of the prototype is not to re-create the CBSA environment in its entirety. Rather, the objective is to prototype a subset of the CBSA environment in order to be able to satisfy the two Data-Centric SecurityCom objectives.

The primary objective of this CBSA prototype is the secure exchange of standardized radiation scan data with OGDs. The meaning of "secure" in this context has several implications. Not only will the standardized scan data have an appropriate security label denoting the sensitivity of its content, but the security label will be cryptographically bound to the data using a digital signature. In addition, the digitally signed data will be encrypted to prevent unauthorized disclosure during transit. Lastly, the releasability of the data will be ascertained according to a central security policy.

The secondary objective of the CBSA prototype is to secure scan data, including access to applications containing scan data, within the CBSA prototype environment. Consequently, all scan data will be assigned a security label that will be cryptographically bound to the data using a digital signature. In addition, the digitally signed data will be encrypted in order to prevent compromise in the event that the gateway at the marine port was to be stolen. Lastly, access to an application containing sensitive scan data will be mediated so that only authorized users with the appropriate clearance and need-to-know are able to access the sensitive scan data stored within the application.

To that end, it was decided that in order to mitigate risk, the project would be sub-divided into three phases:

- Phase 1: NIEM Exchange – this phase demonstrated the ability to repackage information based on NIEM specifications in order to ensure interoperability between agencies using different applications;
- Phase 2: Secure NIEM Exchange – this phase demonstrated the ability to protect information while stored on CBSA infrastructure as well as in transit towards other organizations; and

[2] It should be noted that none of the sample files contain actual numerical data. That data has been either replaced with simulated data or removed.

- Phase 3: Policy Mediated NIEM Exchange – this phase demonstrated the ability to automatically make release decision for information based on organizational policies.

Statement of Results

The following sections contain a brief description of the testing that was carried out. For a full discussion of the architecture, test plan, test design and test results see [5].

Phase 1 – NIEM Exchange

The following steps were carried out to establish connectivity prior to commencement of the NIEM tests. Specifically, the actual NIEM testing was performed under the following conditions:

- A series of simple CBSA to OGD connectivity tests were carried out to establish that the network for the domains is operational and ready for the experiment;
    - An email without attachments was transmitted from the CBSA to the OGDs;
    - A simulated OGD without the NIEM Policy Enforcement Point (PEP) ran NIEM conformance tests; and
    - A simulated OGD with a NIEM PEP ran NIEM conformance tests;
- A suite of XML transformational and Email functional tests were successfully conducted.

Phase 2 – Secure NIEM Exchange

The testing during Phase II extended the Phase 1 testing through the introduction of the DCSS and the addition of a NIEM PEP in the Health Canada domain, into the prototype and evaluation environment. Phase I provided the capability to support a NIEM CBRN information exchange between the CBSA and a Health Canada domain. The principal target of the experiment in Phase II was, using CBSA CBRN data, to address the ability of a CBSA RSO user sourcing DCSS protected documents/files from the Scan Gateway file server, and sending an email with file attachments, to Health Canada and the CNSC, using a NIEM PEP to successfully apply the NIEM transformation. There were two types of receiving domains; Health Canada had a NIEM transformation and translation capability, while CNSC only had the ability to receive and interpret NIEM translations (no transformation capability).

Phase 3 – Policy Mediated NIEM Exchange

The testing during Phase III extended the testing of Phase II with the introduction of the full DCSS into the Health Canada prototype and evaluation environment and the addition of the IRT application, which has been added to the CBSA domain. An automatic security labelling capability was introduced, whereby N.42 xml files, and Security Incident files were assigned a security label depending on the files contents. Phase I provided the capability to support a NIEM CBRN Information Exchange between the CBSA and a Health Canada domain. The principal target of the experiment in Phase II was, using CBSA CBRN data, to address the ability of a CBSA RSO user sourcing DCS protected documents/files from the Scan Gateway file server, and sending an email with file attachments, to Health Canada and the CNSC, using a NIEM PEP to apply the NIEM transformation. In Phase III the DCS component have been added to the Health Canada domain. There are two types of receiving OGDs; Health Canada had a NIEM transformation and translation capability, and a full DCSS access control capability. The CNSC only had the ability to receive and interpret NIEM translations (no re-transformation capability). The IRT database has been added in the CBSA domain.

Conclusion/Recommendations

The CBSA Data-Centric Security NIEM Prototype demonstrated how the approach can facilitate the secure exchange of standardized information with other organizations while respecting policy. Specifically, it achieved the following three project objectives; standardized exchange of radiation scan data with OGDs, securing this exchange, and securing scan data, including access to applications containing scan data, within the CBSA prototype domain environment.

It is important to note that while NIEM provides an information exchange framework with which to facilitate data transformation, it does not provide the complete set of standards required for immediate implementation. Consequently, even with NIEM, data transformation initiatives are not trivial and will necessitate significant involvement from a variety of stakeholders within the organization.

In order to capitalize on the capability demonstrated within this prototype, it is recommended that CBSA pilot this capability within a production environment. Specifically, the intent would be to provide a standardized container with which to transport any type of scan data within the CBSA production environment. The DCSS information protection architecture would be used to secure the container, and the sensitive scan data embedded within, regardless of where it is stored or transits within the production environment.

Prepared by: Daniel Charlebois (DRDC – Centre for Security Science).

References

[1] US Government, "National Information Exchange Model," 2016. [Online]. Available: https://www.niem.gov/Pages/default.aspx. [Accessed: 2016-10-01].

[2] Government of Canada, "Transport Canada Marine Security," 29 May 2015. [Online]. Available: https://www.tc.gc.ca/eng/corporate-services/planning-dpr-2013-14-1188.html. [Accessed 2016.]

[3] D. Charlebois, G. Henderson, D. Simmelink and B. Carruthers, "Secure Access Management for a Secure Operational Network - DRDC-CSS-TR 2013-037," Government of Canada, Ottawa, 2013.

[4] G. Henderson, A. Magar and A. Clason, 2016. "CBSA Data-Centric Security NIEM System Architecture Document & Prototype Report", Defence Research and Development Canada, Contract Report, DRDC-RDDC-2017-C120.

[5] A. Magar and G. Henderson, 2016, "SAMSON Data Centric Security for the CBSA SensorNet," Defence Research and Development Canada, Contract Report, DRDC-RDDC-2016-C096.

[6] G. Henderson, 2015. "Information Interoperability – Architecture Vision," Cord3, Ottawa.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Centre for Security Science
Defence Research and Development Canada
60 Moodie Dr.
Ottawa, ON
CANDAD K1A 0K2

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Canada Border Services Agency (CBSA) National Information Exchange Model (NIEM)-Based Information Exchange

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

Charlebois, D.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
November 2017	7	6

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Scientific Letter

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Centre for Security Science
Defence Research and Development Canada
60 Moodie Dr.
Ottawa, ON
CANADA K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2017-L416	

11a. FUTURE DISTRIBUTION (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Any limitations on further dissemination of the document, other than those imposed by security classification.)

12. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

13. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Information Sharing, Information Assurance, Public Safety, CBSA, Canada Border Services Agency