Recommendations for Increased Security in Data Exchange Systems

Authors: Edwin Mein, Tobias Beckman, Technolution; Rodrigue Al Fahel, CLOSER

Deliverable: D4.2

Published: December 2024

This report is part of the Smart Urban Traffic Zones project that seeks to develop intelligent solutions within the city to enhance flexibility in urban space utilisation, optimise transportation efficiency, and enhance traffic safety. This involves testing and evaluation of digital tools like geofencing, sensors, and digital signage within the city. The project is conducted in three steps, with the ongoing third step initiated in February 2023. It involves the participation of 24 project partners, including public entities such as cities, technology providers, OEMs, transport companies, and academia. The project is partially funded by the Swedish Innovation Agency, Vinnova.

VINNOVA
Sweden's Innovation Agency

Document elaborated with the support of the Smart Urban Traffic Zones project, 2022-02805, has received funding from Vinnova

Table of content

Sammanfattning **3**

Summary **4**

Introduction **5**

Method **5**

Results **5**

EU Network and Information Security Directive (CER/NIS-2) *5*
Make a Risk Analysis 6
Take Measures 6
Establish Procedures 7

Smart Urban Traffic Zones security architecture *7*
Data integrity and authenticity 8
Secure communication 8
Authentication and authorization 8
Firmware and Software Security 9
Physical security 9
Monitoring and logging 9
Data privacy 9
Resilience and redundancy 9
Compliance and Standards 9
Incident response 9

Security Workshop Results *9*

Generic Recommendations *11*
System architecture level 11
System development level 12
System operation 13

Sammanfattning

I dagens sammankopplade värld fungerar datautbytesnoder som centrala knutpunkter där flera aktörer kan dela och få tillgång till data. Dessa noder möjliggör säker informationsöverföring mellan offentliga och privata aktörer, vilket säkerställer att data finns tillgänglig där och när den behövs. På grund av den känsliga karaktären hos informationen och nodernas kritiska roll utgör de dock attraktiva mål för cyberhot, såsom obehörig åtkomst, dataintrång och skadliga attacker.

Den här rapporten innehåller rekommendationer för ökad säkerhet i systemet genom tre metoder: befintlig lagstiftning, lärdomar från pilotprojekt och en redan existerande lista med rekommendationer.

Målgruppen för detta dokument är representanter från organisationer och intressenter med kompetenser som bidrar till att upphandla och upprätthålla ett säkert system. Att integrera säkerhetsaspekterna tidigt i processen säkerställer ett *safety-by-design*-tillvägagångssätt.

Summary

In today's interconnected world, data exchange nodes serve as crucial hubs that allow multiple stakeholders to share and access data. These nodes facilitate the secure transfer of information between public and private entities, ensuring data is available where and when it is needed. However, due to the sensitive nature of the data and the critical role these nodes play, they are prime targets for cyber threats, including unauthorised access, data breaches, and malicious attacks.

This report describes the recommendations for increased security in the system using three methods: existing legislation, lessons learned from pilots and an existing list of recommendations.

Intended readers of this document are representatives of organizations and stakeholders that have competencies contributing to procuring and maintaining a secure system. Involving the security aspects at an early stage in the process ensures a safety-by-design approach.

Introduction

A Data Exchange Node (DEN) is a critical component in the infrastructure for data sharing and communication. It acts as a central hub for secure and efficient data sharing between various entities such as systems, organisations, and devices. It ensures interoperability, data encryption, robust authentication, supporting high throughput and scalability.

Improving security for a data exchange node means implementing advanced security measures to protect the confidentiality, integrity, and availability of the data being exchanged, following established frameworks such as the European Union's cybersecurity principles. These principles, rooted in the EU Cybersecurity Act and the NIS Directive, promote a unified approach to security for critical infrastructure, emphasizing resilience, proactive threat detection, and data protection compliance.

This report gives a list of recommendations for different aspects of increased security in the system. The methods we used reflect the existing legislation, lessons learned from the pilots and stakeholders and the recommendations from large enterprise deployments.

Method

The results in this report are based on three sources:

- *An inventorial study of existing regulations*.

  The European Union has defined a standardized set of principles, regulations and recommendations for developing enterprise systems and how to embed (cyber) security measures in developing and deploying such systems.

- *A workshop with the pilot stakeholders on September 4, 2024, in Stockholm*.

  During the workshop, commonly known security aspects were discussed, and each stakeholder reflected their organization's view. The information from this workshop gave good insights into the security lessons learned.

- *A list of lessons learned from deployments of enterprise solutions*.

  In the deployment of a larger enterprise system, Technolution developed a standardized list of recommendations to take into account. These recommendations fulfil the requirements of the European regulations.

Results

EU Network and Information Security Directive (CER/NIS-2)

The European Directive (EU) 2022/2557, defined in CER/NIS-2, states that an organisation should implement measures to comply with the NIS-2 directive. In general, the following aspects are also applicable to the implementation of a Data Exchange Node and define generic recommendations:

1. Make a risk analysis of the physical and digital threats that could disrupt your organisation's services.

2. Where possible, take measures that (better) protect your organisation against these risks.
3. Establish procedures that enable your organisation to detect, monitor, resolve and report incidents that (may) disrupt business processes.

The following paragraphs give a short description of the three items mentioned above.

Make a Risk Analysis
Digital and physical threats can pose significant risks to the continuity of services that an organisation provides. Therefore, it is important to have resilience in place. That starts with knowing which physical and digital threats pose a risk to an organisation and to what extent they could disrupt business processes. Gaining that insight requires a risk analysis.

Once the risks have been identified, an assessment of the risks is needed so that an organisation can take appropriate action.

An assessment can be made by asking the following questions:

- *Which physical and digital risks are relevant to your organisation because they could disrupt service continuity?* One way to identify risks is to use a government-wide risk analysis guideline, showing which threats could disrupt our society.

- *What are the organisation's crown jewels or interests to be protected?* By identifying which issues are of great or lesser importance to your organisation and services, you can weigh up which risks require measures to be taken to protect those interests.

- *What measures has your organisation (already) taken to protect interests from the risks?* By answering this question, you identify your organisation's resilience. Resilience is your organisation's ability to prevent, anticipate, adapt to, quickly recover from and learn from disruptions.

Take Measures
Once the risks have been identified, an organisation can, where possible, take appropriate measures to strengthen resilience.

The answer to what measures your organisation should take is, of course, tailor-made and depends on the analysis and assessment of the risks an organisation faces. Organisations can at least consider the following measures:

- *Drafting business continuity plans and crisis management protocols:* The presence of risk and crisis management procedures and alert routines is necessary to mitigate the impact of incidents.

- *Identifying alternative suppliers:* An organisation may be dependent on other organisations for its services. It is therefore important to identify alternative suppliers in the chain so that service continuity isn't disrupted if a supplier fails (temporarily).

- *Raising awareness among staff:* Organisations can already identify which staff members perform critical functions within the and then make them aware of the risks and security measures.

Establish Procedures
Organisations soon to be covered by the CER/NI2-legislation will be obliged to report incidents. Factors that make an incident notifiable include, for example, the duration of an incident or the number of people affected by the incident.

The requirements of the reporting obligation will have to be embedded in business processes. Drawing up an incident response plan can help with this.

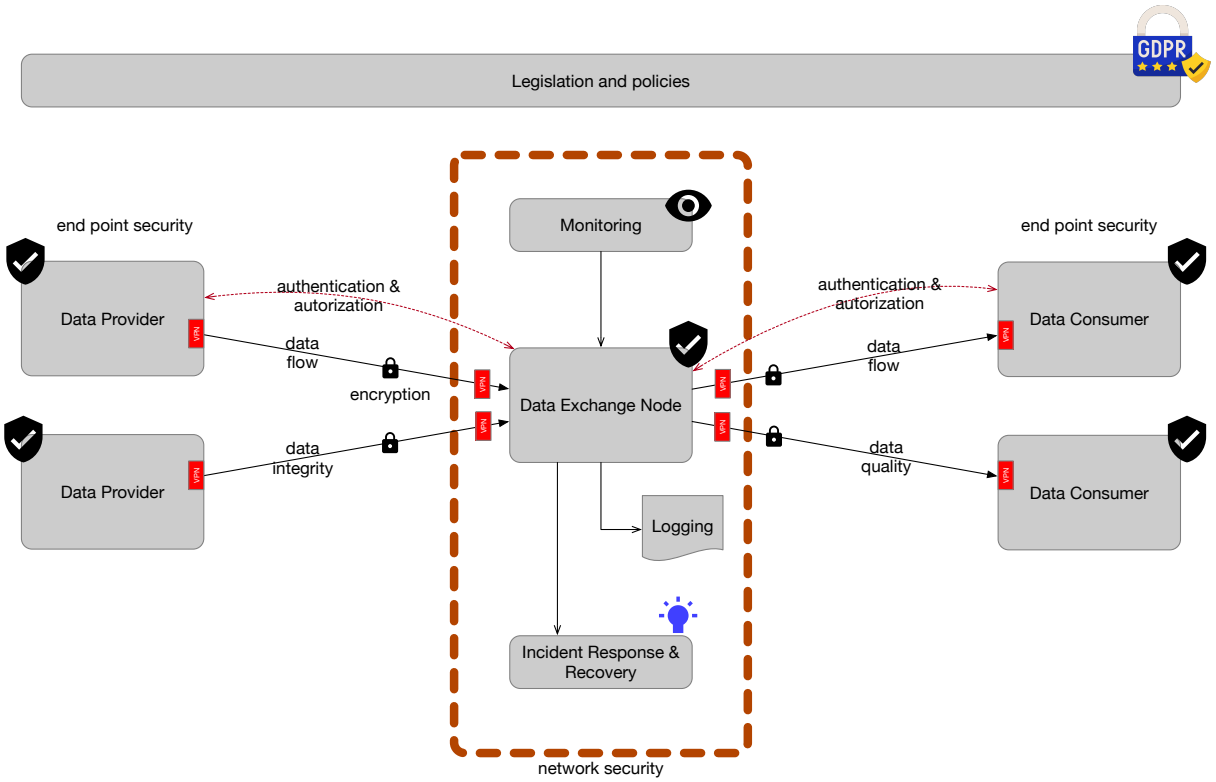
Detection is the approach of using technical means to gain insight into the threats resulting from these activities. Detection creates a clear picture of an incident. Security measures can also be tightened via detection.

Smart Urban Traffic Zones security architecture

The more generic elements of system security, as mentioned in the previous chapter, can be applied to the Data Exchange Node perspective. We have listed the key elements in the list below. In this document, the focus will mainly be on the most relevant of these for the Smart Urban Traffic Zones project context.

1. **Data Integrity and Authenticity**: Ensuring the data is genuine and has not been altered.
2. **Secure Communication**: Protecting data in transit from interception and tampering.
3. **Authentication and Authorization**: Verifying identities and controlling access to data.
4. **Firmware and Software Security**: Ensuring the integrity and security of firmware and software on devices.
5. **Physical Security**: Protecting devices from physical tampering and unauthorized access.
6. **Monitoring and Logging**: Tracking and analyzing device activity for security purposes.
7. **Data Privacy**: Ensuring the privacy of collected data and minimizing exposure.
8. **Resilience and Redundancy**: Ensuring continuous availability and reliability of data sources.
9. **Compliance and Standards**: Adhering to relevant industry standards and legal requirements.
10. **Incident Response**: Preparing for and responding to security incidents effectively.

To show how the different systems in the security chain work together, we will be using the picture below:



The picture above illustrates system security aspects in the process between Data Providers, The Data Exchange Node, and Data Consumers.

Data integrity and authenticity

Data Flows from the Providers to the Consumers, and Consumers should be able to trust that the data is authentic. A common solution is using a digital signage approach, (Public Key Infrastructure (PKI)-based. The Producer signs the data with a secret digital key, and the Consumer can decrypt the data with a public sign. If these match, then the data is authentic from the Provider.

Secure communication

In general, this can be realised with common safe data connections, e.g., Transport Layer Security (TLS) encrypted or Virtual Private Networks (VPN) tunnels. These technologies guarantee that data can't be read between the systems by a man-in-the-middle that 'sniff' on the data streams.

Authentication and authorization

Systems like the Data Exchange Node support a means of authentication and authorisation. The authentication enables the DEN to certify that the right system or person is connecting to the DEN. The authorisation ensures that the authentic system/person can only access data streams it/he/she is entitled to access. A strong group, user, and role-based system enables this with a password or token access layer.

Where possible authorizations shall be restricted to the actor's geographical jurisdictional boundaries, belong to an organization and every user and/or system is related to an organization.

Firmware and Software Security
At the level of firmware and software in general it's important to keep up to date with the latest threats on cyber security level. Most systems can be automated to do so, but also a response script for unexpected threats has to be implemented. Firmware and Software changes should be regulated and monitored to ensure that the new system remains safe.

Physical security
Part of implementing security is physical security, blocking people/systems from access to the internal systems. Usually, this is implemented with access cards that authenticate and authorize personnel with the right access rights.

Monitoring and logging
Even with all layers of security in place, still attacks can happen. Monitoring and logging events can show that systems are under attack or have been breached. Unusual network traffic, strange login attempts, etc. can be indications of something wrong or being attacked from the outside world and require a closer look.

Data privacy
This is commonly related to GDPR and other privacy-regulated rules around data. ISO27001, ISO27002, GDPR, etc. are ways to mitigate risks around data privacy issues.

Resilience and redundancy
Resilience and redundancy are part of the contingency approach to ensure that systems keep working with a high availability. This holds also for a security system that has to have a backup in place in case the first system fails, a second system can step up.

Compliance and Standards
Data- and Cybersecurity is highly regulated at a European and national level. These standards should be implemented by all parties and checked on a regular basis.

Incident response
If something happens that breaches the security, privacy or contingency of the system, a response plan should be available with countermeasures. Depending on possibilities, systems and connections can be blocked to minimise the impact. After careful evaluation of the event, systems or software need to be upgraded or changed and the system can be activated again.

We used a workshop to identify how these key aspects relate to the different stakeholders in the Smart Urban Traffic Zones project. The results from this workshop are shown in the next chapter.

Security Workshop Results

The workshop engaged all project partners, including those involved in the three project pilots. During the workshop, project partners commented on the before-mentioned cybersecurity aspects in the practical cases of the individual pilots and their interaction with the Data Exchange Node in place. This workshop was held on September 4, 2024, in Stockholm.

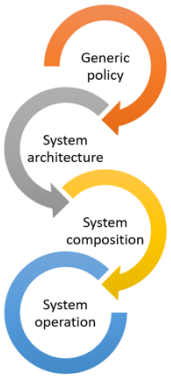
Aspect	Observations, risks and mitigations from pilots and stakeholders
Data integrity and authenticity	• In general, all actors find this very important. If not complied with, this will lead to less trust from the users otherwise.
Secure communication	• This is key to all connections between sensors, actuators, back-ends, front-end, data exchange nodes, etc. • The data provider (e.g., sensors, actuators and other hardware related data) has to support secure communication, otherwise, you need to make sure that you choose providers that can guarantee security.
Authentication and authorization	• When controlling automated systems, like signs, it is important to keep track and who has what authority.
Firmware and Software security	• Sensor, actuator and component level data is not always updated. • Firmware updates for indirectly connected devices are challenging. • Increased demand for cloud-based updates from procurement teams.
Physical security	• Risk of vandalism and damage of signs, actuators and sensors. • Need for detection and prevention measures. • Low risk of damage, due to height of actuators and sensors, usually accidental. • Concerns about data privacy and security compliance (ISO, GDPR). • Potential public resistance to speed cameras. • Importance of clear communication about actuator and sensor purpose and benefits to the public.

Monitoring and logging	• Anomaly Detection:
	  ○ Emphasize the importance of anomaly detection for tracking, logging, and alerting.
	  ○ Highlight the need to identify the source of anomalies to prevent cascading failures.
	  ○ Stresses the importance of collaboration and responsibility sharing among partners.
	  ○ Use processes and systems for anomaly detection solutions.
	  ○ Automated systems to detect anomalies detection are crucial in scaling operations to more users, larger areas, etc.

Data privacy	• Data privacy data classifications are defined in ISO standards and supported by the different actors in the project. • The data shared through the DEN becomes a responsibility of both parties if sensitive data is shared. • The producer of data has to classify the data to ensure it can be shared to everyone or just an authorized group of actors.
Resilience and redundancy	• All actors agree that redundancy should be implemented at every level of the security architecture
Compliance and Standards	• All stakeholders are following the required compliance and standards.
Incident response	• Contingency plans have to be defined for the situation when an unexpected event occurs and might compromise the system's safety. • The level of risk impact is important here. Based on a risk assessment it might be important to inform the other participants in the pilots.
Other	• In general, also think about where e.g., servers are hosted. Should the hosting be within the country, within Europe or somewhere else? This is part of the security aspect. For example, personal data shall never be stored outside the EU or EES.

Generic Recommendations

This chapter iterates a list of common security aspects at different levels in a system. These recommendations come from previous experiences in the development of systems like Data Exchange Nodes. This list is not exhaustive but gives a good guideline to include. These experiences also come from the European NIS2 Directive as described in that chapter.



System architecture level

At the **system architecture,** the principles that the Data Exchange Node must adhere to in terms of system security follow the principles defined and established in a quality system. These include:

- **Applying security by design principles, think of:**
    - Isolation – limiting access to sensitive information
    - Authentication/authorization – think of role-based access, two-factor authentication
    - Open design – no closed or unreadable design, use of common open components
    - Separation of functions – enforcing 'four eyes' in critical actions
    - Access and other functional limitations – 'need to know, need to be' is our guiding principle
    - Ergonomics – ease of use to ensure that the correct procedure is followed
    - Diversity of measures – ensuring that different layers using different approaches

- **Design for remote management and remote monitoring, think of:**
    - Adding agents that provide system health information.
    - Using APIs to allow for remote maintenance.
    - Enable secure access to infrastructure to enable critical response actions.

- **Use of containerized architectures think of:**
    - Applications are running in contained environments, with no spill-over of security breaches
    - Allows for fast service recovery, through quicker deployment and fast start-up of Apps.
    - Portability to move Apps easily between environments without any changes to the App.
    - Simplified maintenance prevents errors and reduces time spent on debugging.
    - Test and production environments are similar ensuring that threads are found quickly.

System development level

At the **system development** level, the focus is on how the software is composed by using managed processes, development according to defined models, and continuous vulnerability monitoring. Focus is on:

- **Application of standards during software development**
    - Proper use of software code guidelines, good programming practices, and code reviews.
    - Automated verification of the proper application of coding standards.
    - Tools used are periodically re-evaluated, also as a result of general usage within other applications.

- **Verification of compliance with developed software**
    - Tracing requirements to code for ease of testing and tracing of security threads to code.
    - Third-party dependency checking, static code analysis, third-party analysis, dynamic code analysis.
    - Software development and delivery according to defined test and deployment procedures.

- **Testing and verifying software for correct functional behaviour**
    - Test management approach based on e.g., TMap.
    - High level of test automation (unit testing) for easy and consistent (regression) testing.
    - Security testing (AAA: access control, authentication, and auditing) is an integral part of the test approach.

- **Checking software for vulnerabilities**
    - For Data Exchange Node a vulnerability scanner in place that periodically scans the suite as a whole for vulnerabilities.
    - Formal processes in place for responding to vulnerabilities.
    - Incident management with immediate action in case of critical vulnerabilities.
    - Automated tools for code quality analysis, based on ISO25010 standard for software quality.

- **Maintaining the quality and integrity of our developers**
    - Use of tools for trend analysis to make code quality measurable and verifiable over time
    - Continuous training of developers and staff on code quality
    - Screening of staff according to the national code of conduct
    - All employees endorse our integrity statement
    - Frequent quality and security reviews and audits
    - A security officer is always available as the primary contact point for security-related matters

System operation

At system operation the focus is on operational security, how we can access the system security to monitor the operational state and to intervene in case of (security-related) critical incidents. It is important that users with remote access to their IT infrastructure can be monitored and managed. By remote access, i.e. access to the (parts of) the relevant infrastructure, to those parts that are strictly necessary (need to know, need to be'):

- **Applying specific measures for the highest level of security when accessing third-party systems**
    - Ensure to follow user access policies.
    - Adequate authentication methods (e.g., 2FA).
    - Secure connections and encrypted communication only.
    - Log all system access.
    - Only authorized personnel with proper clearance have access to passwords and systems.

- **Continuous monitoring of production deployments**
    - Safe deployment (security) patches and updates as soon as they become available.
    - Automated check of system health, disk space, and other system metrics.
    - Monitoring suspicious behavior in the Data Exchange Node.

- **Workflows are elaborated for system operation, system maintenance, and incident response**

    - A step-by-step process for sensitive operations to prevent errors where possible.
    - Stored in a secure environment for easy access by authorized personnel only.
    - Have procedures and work instructions in place.

- **Perform penetration testing regularly of representative system environments**
    - This is done by third parties: provide the URL, and they do the pen-test.
    - Outcomes are reported and thus verifiable and measurable, on at least a yearly basis.

- **Audit all processes with the service and project organization annually**
    - A security officer should be available for operational questions and carrying out ad-hoc checks.
    - A company's ISO27001 certification is audited every three years.