Administration and reliability of X-Road

Have necessary measures been taken to ensure the reliability of X-Road?

Summary of audit results

The performance of public functions, including information exchange between authorities or provision of services, has inevitably become largely digital. This means that the need to exchange large amounts of electronic data increases every year.

The number of users of the secure data exchange layer for information systems developed in the early 2000s and the number of queries made using it is still growing. At the same time, the software and operating principles necessary for the operation of X-Road have started to be exported to foreign countries, and development of software jointly with Finnish colleagues has also commenced.

What did we audit?

The National Audit Office audited whether the Information System Authority responsible for the management of the X-Road Centre has taken into account the major risks to X-Road and implemented measures to mitigate them. It was also examined whether the Authority together with the users of X-Road has complied with the requirements established by the state for the management of X-Road to ensure the operation of secure data exchange in a sustainable manner.

Why is this important to taxpayers?

As at 1 December 2020, 200 public sector authorities (incl. local government authorities) and 525 private sector institutions had joined X-Road, and approximately indirectly 52 000 enterprises and institutions indirectly used X-Road services. 1,263 information systems have been interfaced with the secure data exchange layer. The authorities and institutions using X-Road, or members of X-Road, had installed 164 security servers. The number of services available through X-Road was 2,741.

During the audit, nearly 133 million queries were performed through X-Road in one calendar month. Queries made through X-Road can significantly save time for residents, entrepreneurs and officials and simplify administration between parties. Given the number of queries made through X-Road, the provision of the majority of public services would become impossible or at least significantly more difficult should X-Road not be operational. Replacing data exchange carried out via X-Road with non-electronic data exchange would be practically impossible or at least very costly.

What did we find and conclude from the audit?

It became clear as a result of the audit that the Information System Authority and the members of X-Road observed in the audit have generally implemented measures necessary for ensuring the reliability of X-Road. At the same time, the National Audit Office identified unmitigated risks related to the integrity and confidentiality of databases interfaced with X-Road, which are due to the fact that, in several cases, members of X-Road have not entered into data service agreements or checked the information security level of private institutions when they join X-Road.

The most important observations of the National Audit Office regarding the secure data exchange layer X-Road are the following:

- **The Information System Authority has determined the most important risks to the reliability of X-Road and has assessed them. Measures have been developed to mitigate risks, many of which are being implemented.** The central services of the X-Road infrastructure have so far been

relatively reliable: over the last three years, there has been one significant interruption in the X-Road services caused by the central components of X-Road.

- **Several of the requirements established for X-Road by the Government of the Republic Regulation "Data Exchange Layer for Information Systems" are general and allow members of X-Road to interpret them differently in implementation.** For example, authorities implementing X-Road must take the necessary measures to mitigate information security risks, but it has not been determined which security measures and at which level should be implemented.

- **In the course of the audit, the National Audit Office identified a few risks that could endanger the integrity and confidentiality of databases interfaced with X-Road and create opportunities for unauthorised access to data or making unauthorised changes. The two main reasons for these risks are the following:**

    - There is no common practice for entering into data service agreements, and some authorities do not enter into these agreements at all. Compliance with data service agreements is checked up on only by few members of X-Road. These authorities investigate the reasons for using the data by members of X-Road who made the queries primarily from the point of view of data protection, i.e. it is assessed whether data made available through X-Road (particularly personal data) are processed solely for the purposes prescribed by law.

    - None of the audited national authorities make sure before entering into an agreement with a data service user whether an entrepreneur who is a private legal entity implements adequate measures for ensuring the integrity, confidentiality and availability of data to mitigate security risks. Private sector institutions of X-Road warrant that they implement the required measures when entering into a data service contract, but data service providers do not check up on it.

- **Although the Information System Authority has not prepared an operational continuity plan for X-Road, several measures have been implemented for the continued operation of secure data exchange and requirements have been established in other documents to ensure operational continuity.** Irregularity of performing recovery tests and failure to document them may be considered shortcomings. So can the fact that the vitality and sensitivity of information assets related to X-Road have not been assessed separately.

What did we recommend as a result of the audit?

Recommendations of the National Audit Office to the Director General of the Information System Authority:

- Initiate an amendment of the Regulation "Data Exchange Layer for Information Systems" governing the operation of X-Road that would make the requirements established for members of X-Road more precise and unambiguous so that data service providers could implement the requirements and the Information System Authority could check up on the implementation thereof. Necessary guidelines for implementing the requirements arising from the Regulation should also be prepared and necessary training should be organised for members of X-Road.

- Assess the risks to the security of databases arising from the failure to enter into data service contracts and implement activities to mitigate these risks. Also consider adding the functionality of entering into data service contracts and petition management to make opening and using the data services of the X-Road portal less bureaucratic.

- Develop a system for inspecting members of X-Road who are private legal entity entrepreneurs to ensure the control and supervision of the implementation of measures ensuring integrity, confidentiality and availability required by the Regulation "Data Exchange Layer for Information Systems".

- Perform regular recovery tests on the central components of X-Road and document them. In the event of deficiencies, take the necessary corrective actions.

Response from the Director General of Information System Authority: The Authority has examined the report of the National Audit Office and presented its opinions on the recommendations.

The Authority is of the opinion that due to the necessity to ensure the sustainable development, management and use of the X-Road software, it is not expedient to regulate all the details at the level of a Government of the Republic regulation. According to the Authority, the specific requirements applicable to members of X-Road should instead be established by a subscription contract. The Authority did agree, however, with the conclusion drawn by the National Audit Office that the adequacy and comprehensibility of instruction materials may need to be analysed and guidelines should be supplemented and kept up to date if necessary.

If the X-Road software and Information System Authority create preconditions for the development, provision and use of data services, the practical use of data services can rely solely on mutual agreements between members of X-Road. The Authority plans to develop the functionality of entering into data service agreements and petition management in the X-Road self-service environment in the future.

The Information System Authority finds it important to check that X-Road is used in accordance with the requirements set out in the Regulation and in the contract, irrespective of the legal form of the member of X-Road. The Authority recognised that in order to carry out effective control of private legal entities, the adequacy of the existing rights and intervention measures must be assessed and a functioning control system must be developed.

The Information System Authority will start to organise regular recovery tests together with documenting them and will implement the necessary corrective actions.