Human Interaction and Emerging Technologies (IHIET-FS 2025), Vol. 196, 2025, 1–11
https://doi.org/10.54941/ahfe1005949

Enabling the Transfer of Large Files Across Security Domains in a Multinational Environment

Lorraine Hagemann[1], Philipp Klotz[1], and Dennis Gießel[2]

[1]Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB, Fraunhoferstr. 1, 76131 Karlsruhe, Germany
[2]INFODAS GmbH, Rhonestr. 2, 50765 Köln, Germany

ABSTRACT

In an environment in which data has to be transferred between different applications, nations and domains, various risks in terms of data security exist. This has particularly serious consequences if security-relevant data and information are processed. In this paper we focus on the transfer of large files between several applications across security domains in the military sector. The exchange of data in a military multinational environment is particularly challenging because it is regulated by predefined architectures, concepts and technologies. Coalition Shared Data (defined by STANAG (Standardization Agreement) 4559) specifies services, interfaces and data models to exchange ISR (intelligence, surveillance and reconnaissance) information within a coalition. STANAG 4774 and STANAG 4778 as well as STANAG 5636 define essential (security) metadata and the (security) labeling of data to enable role and security-based data management. In this paper the exchange of large files between different security domains that include Coalition Shared Data services linked by a specific labeling service and security gateway based on STANAG 4774 and STANAG 4778 were examined. Accredited security gateways supporting data exchange often come with limitations e.g. on the file size that can be exchanged. Based on the existing systems, processes and requirements, a concept for the transfer of large files has been developed under consideration of the technical and organizational requirements and constraints. Initial tests of the new approach were carried out in a laboratory demonstrator and demonstrated the fundamental functionality.

Keywords: STANAG, Coalition shared data, Interoperability, ISR, Security domains, Data transfer

INTRODUCTION

For the success of a military operation, it is essential to be able to access information and knowledge about the current situation and especially the enemy in order to gain an advantage. Various systems are used to generate surveillance and reconnaissance data. In military operations, several nations may work together in a coalition, using their resources and systems to achieve the mission objective(s). In order to create a common picture of the situation, the mutual exchange of information is important. For this purpose, the systems in use can be connected to each other and exchange data. Systems

in the home country can also be connected to further process information, take over tasks and enable decision-makers to act. It is important that data and information are made available in a timely manner and that relevant information is passed on to the right person. In this way, information superiority can be achieved.

Systems implementing STANAG 4559 (NATO Standardization Office (NSO), 2018a) are used to transmit data in multinational reconnaissance networks in the NATO environment. A CSD server is used for the result of an intelligence, surveillance and reconnaissance (ISR) task, i.e. static data (e.g. messages in XML format, images, videos or Office documents) in accordance with STANAG 4559 AEDP-17. An implementation of the CSD server is the CSD PLUS server from Fraunhofer IOSB, which is used in national projects of the German Federal Armed Forces.

If data shall be transferred across security domain boundaries, special (security) guidelines must be taken into account. In the CSD context, these guidelines are standardized in STANAG 4774 (NATO Standardization Office (NSO), 2017) and 4778 (NATO Standardization Office (NSO), 2018e). An implementation of these STANAGs is the SDoT Labelling Service (SDoT LS) and the SDoT Security Gateway (SDoT SGW) from the company INFODAS.

In this paper we examine how to support the transfer of increasingly large files across security domain boundaries in a multinational military context. In order to achieve this and to determine the necessary adaptations and extensions, an examination of the existing systems and processes based on the STANAG 4559, STANAG 4774 and STANAG 4778 has been done. The technical and organizational requirements and constraints have been considered. A special aspect is the accreditability of the concept, which is important for the future operational use of the systems. Based on the existing systems, processes and requirements, a concept for the transfer of large files has been developed and tested in a laboratory demonstrator.

Our paper is structured as follows: In the chapter *BACKGROUND* we describe the (CSD) concept that defines the framework of our work, possible scenarios, relevant NATO standards and we also describe the components used by the participating companies Fraunhofer and INFODAS. The chapter *CHALLENGES* outlines the vulnerabilities and challenges with the current solution. In the following chapter *APPROACH*, we present an approach we have developed to counteract these challenges. The tests carried out on the adapted approach and the insights gained are described in the chapter *TESTING*. Finally, the paper concludes with a summary and possible next steps.

BACKGROUND

The following chapter will explain the basics and the background of the CSD environment. The considered scenario and specifications, relevant NATO standards and the components used by INFODAS and Fraunhofer IOSB are also explained.

Scenario and Specification

As described in our paper (Kerth et al., 2019) various use cases for information dissemination based on the CSD concept may be of interest

within a coalition. The specific requirements for a system of systems architecture depend on the respective deployment situation and the specific mission. This applies in particular to the involved system, the system assignments, the security domains, the network connection and performance and the entire information flow.

In our work we considered a scenario consisting of two CSD servers located in two different security domains, a high and a low domain. This means that the CSD servers belong to differently classified network segments within the coalition network. It must be ensured that higher classified data (e.g. secret data) does not leave the corresponding high domain. Nonetheless, the data flow from the low domain to the high domain should be possible. Additionally, unclassified data (i.e. open data) should be transferred from the high domain to the low domain. The decision and responsibility whether data according to their security information can flow via the security domain boundaries lies by the INFODAS components, which evaluate and check the data during transmission at the domain boundaries. The security information of data is covered in the CSD concept via certain metadata fields (policy, classification and releasability). In this way, it is determined which data may flow into the other domains and which must be rejected. Thus, it is possible to make confidential and secret data accessible only to a defined group of people.

In the past, various national recommendations were applied in the area of IT security, e.g. by the German Federal Office for Information Security (BSI). The interpretation of the specifications is not always clear and must be examined individually for the considered use cases.

Not only security-related specifications, but also technical specifications, e.g. through standards that are relevant in the CSD environment (STANAG 4559, STANAG 4774, STANAG 4778 and STANAG 5636 (NATO Standardization Office (NSO), 2022)), which ensure interoperability, provide certain framework conditions. The standards are explained in more detail in the following.

Relevant Standards

STANAG 4559

As described in the work of our colleagues (Essendorfer, et al., 2018), the STANAG 4559 is defined for the interoperable data exchange of NATO ISR artefacts (imagery, video, reports, task, etc.). It describes the CSD concept that makes it possible to connect implementations of the standard from different vendors in a network. Consequently, the standard defines common interfaces, use cases and processes to permit the fundamental dissemination of data between the systems. The standard is divided into three documents, known as the Allied Engineering Documentation Publications (AEDP). These documents describe the three principal parts and data types provided by the standard. They comprise AEDP 17 (static data) (NATO Standardization Office (NSO), 2018b), AEDP-18 (streaming data) (NATO Standardization Office (NSO), 2018c) and AEDP-19 (dynamic data) (NATO Standardization Office (NSO), 2018d).

STANAG 4774

This standard defines the metadata syntax for confidentiality labels, detailing how sensitive information should be tagged to indicate its security information, origin, creation and expiration dates, and permissible sharing parameters.

STANAG 4778

This standard outlines methods for binding confidentiality labels to data objects throughout their lifecycle. It specifies cryptographic techniques to maintain the integrity of both the data and its associated labels, ensuring that any tampering is detectable and that the labels remain attached to the data as it is shared or transferred.

STANAG/ADatP-5636

The NCMS (NATO CORE Metadata Specification) defines a core set of metadata that shall be applied "…to all NATO information and to any data object handled or processed by NATO's communications and information systems" (NATO Standardization Office (NSO), 2022). Allies and partners also must use NCMS. Apart from a minimum set of information considering the creator or the creation date time also security information shall be provided according to STANAG 4774. The core set must be bound to the information using STANAG 4778.

Components

Several components from Fraunhofer IOSB and INFODAS are required to connect two differently classified domains to enable data exchange.

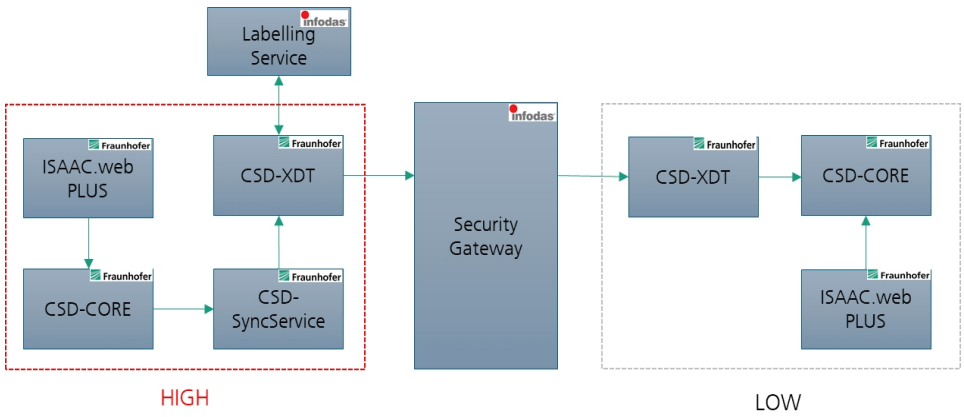

Figure 1: Components involved in the transfer of data across a security domain boundary.

From Fraunhofer IOSB the following components are involved:
CSD-Client:

- ISAAC.web PLUS: Browser-based client for ingesting, retrieving and geo-referenced displaying of CSD data.

CSD PLUS Server:

- CSD-CORE: Component for data storage and data provision in accordance with AEDP-17, STANAG 4559 Edition 4.
- CSD-SyncService: Component for data distribution according to AEDP-17, STANAG 4559 Edition 4 (via Common Object Request Broker Architecture (CORBA)).
- CSD-XDT: (CSD Cross Domain Transceiver) Component to connect Fraunhofer components to INFODAS SDoT components. Contains logic for domain transition.

From INFODAS the following components are involved:

SDoT Security Gateway: System for bidirectional data exchange and filtering of structured and unstructured data between different security domains. For the data transfer a fixed set of rules (e.g. allowed data formats, label required) is defined and used.

SDoT Labelling Service: System for data classification using tamper-proof XML security labels based on NATO STANAG 4774 and STANAG 4778.

As INFODAS components are security products, they must comply with German IT security regulations. Accreditation by the BSI is therefore required. The versions considered in this paper have been tested and approved by the BSI. Any changes to the components must always be agreed with the BSI and would result in the need for re-accreditation. Otherwise a security-compliant production use is not allowed.

CHALLENGES

In the past, various tests in projects including multiple security domains have shown that the current versions of the software components involved do not allow the transfer of large files via the SDoT SGW. Depending on the project environment, the underlying resources and the hardening measures already implemented, different file size limits were identified when transferring data from the high to the low domain. The transfer of data that exceeded these observed limits failed due to the long transfer time. Satellite images and larger videos could therefore currently not be transferred.

In our work, each software component involved was analyzed for limiting factors and optimization potential. As stated above, the SDoT SGW is a security software authorized by the BSI. As a consequence, some of the security functions have an impact on the performance of the device. In the case of the transfer of large files this specifically means that the security check of the Hardware Security Module (HSM) currently limits the maximum file size to 400 MB. Therefore, a new approach for the transfer of large files was necessary. For the changes the technical and organizational restrictions still must be fulfilled. This implies, among other things, that the conditions of the

respective standards must still be met and the solutions must be accreditable for operational use. This results in requirements for the file format and data structure that cannot be changed. Regarding the accreditability, the data integrity must be ensured, a virus scanner in process retrieval must be established and the new solution should change the existing software and its interfaces as little as possible.

APPROACH

In our work different possibilities of transferring large files were discussed. This ranged from optimizing the transmission time, over splitting the file, to compressing the file. In addition, approaches that optimize the organizational file transfer process itself were considered. Due to the technical and organizational specifications mentioned above (in particular the maximum file size limit given by the HSM), we collaboratively decided for an approach to split the file. Files, that exceed the size limit, shall be split into transferable chunks and transferred sequentially. We further ensure that the chunks are composed to the original file at the end of the process and that the approach is acceptable from a security perspective. An appropriate value for the timeout of the transfer duration and for the chunk size must be selected individually for different project environments (depending on the project environment itself, underlying resources and hardening measures).

Adjusted Data Dissemination Process

Our approach results in an adjustment of the process flow for the transfer of files via the security domain boundaries.

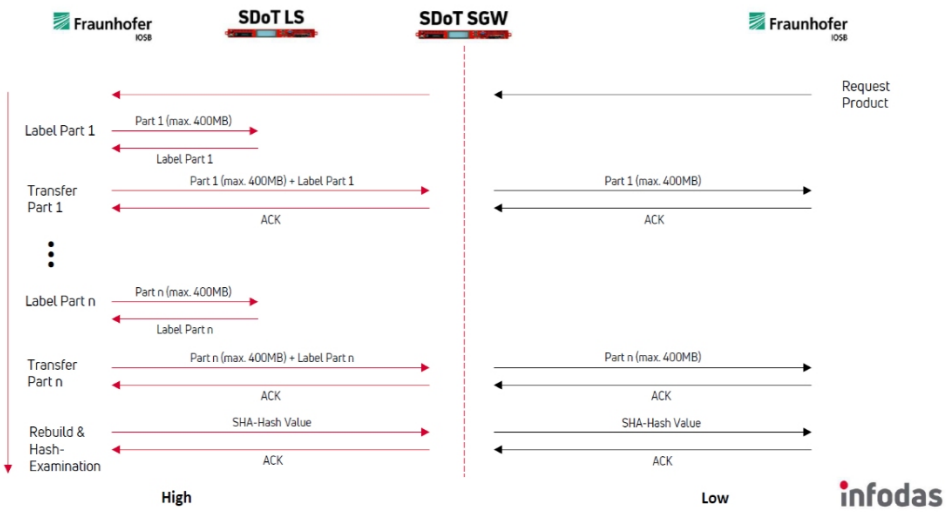

Figure 2: Adjusted approach with partwise data dissemination.

New adapted process:

1. Splitting the file into chunks of 400 MB or smaller.
2. Transfer of the chunks via the security domain boundary into the other domain.
3. Reassembly of the chunks to recreate the original file.
4. Validate the correct and complete transmission with SHA hash value.

To validate that the file has been transferred completely, correctly and consistently, an integrity check must be performed. The standard SHA hash verification was used for this purpose. The SHA hash value of the entire file must be calculated in the CSD PLUS Server in the high domain. Once all parts have been successfully transferred, the CSD-XDT in the high domain sends the SHA hash value to the CSD-XDT in the low domain via the SDoT SGW. The CSD-XDT in the low domain calculates the SHA hash value for the file reassembled from the received chunks and compares it with the SHA hash value received from the CSD-XDT in the high domain. The file is only forwarded to the CSD-CORE in the low domain if both values match. If the hash values do not match, the file (and all parts) is discarded and not forwarded to the CSD-CORE in the low domain. In addition, the detected discrepancy is logged in the log messages of the CSD-XDT in the low domain.

Accreditation of the Approach

As accreditation is the basis for the operational use of the systems, we have already presented the proposed solution to the German authorities. According to the German authorities, the conceptual solution for the transfer of large files appears to be generally acceptable from the current point of view.

TESTING

To determine whether the adapted approach leads to the desired result, a laboratory demonstrator was developed and tested for functionality in a project-relevant setup. For the laboratory demonstrator a high and a low domain were configured to perform the tests. Only those software components were considered that were affected by the changes of the new approach. The CSD-SyncService was therefore omitted.

Test Environment and Test Execution

The high domain was set up with the following components (see Figure 3):

- CSD PLUS Server
  - CSD-CORE
  - CSD-XDT
- SDoT LS
- SDoT SGW

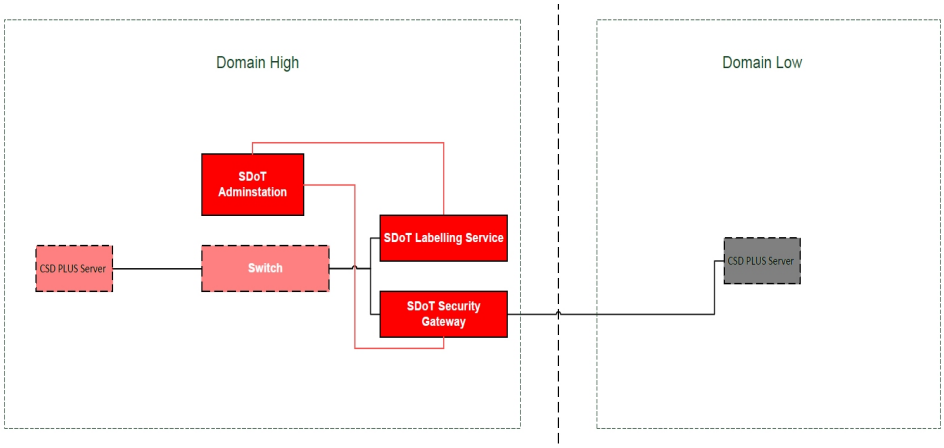

Figure 3: Network diagram of the test setup.

Additionally, the following components were integrated into the test setup for network connections and the configuration of the SDoT components:

- High Domain Switch
- SDoT Administration

The low domain was set up with the following components:

- CSD PLUS Server
  - CSD-CORE
  - CSD-XDT

The objective of the test was to verify the successful transfer of a large file from a high domain to a low domain. For this purpose, multiple test files were uploaded to the ISAAC.web PLUS client in the high domain. Subsequently it was checked whether the file could be sent to the low domain. The intermediate steps (transfer between components) are fully automated. To evaluate performance, corresponding log messages with timestamps were embedded in the CSD-XDT and monitored during the test execution.

During the test execution, the factor "chunk size", that refers to the predefined size of the individual segments of the overall test file, was varied. For the different chunk sizes, the total transfer time (from request to completion) was analyzed.

During the test, the High Domain Switch was substituted with different models to rule out the possibility of it serving as a bottleneck and consequently compromising performance.

Test Results

In the first test run, it was not possible to transfer the files with the original configuration of the test setup. The new approach set an additional header field in the request that contains the content range (HTTP Content range). This value defines the position of a chunk within the overall file. During the tests, it was determined that the SDoT SGW cleans up the request headers for

security reasons. Only the header fields provided by INFODAS are retained, others are discarded. The sanitization of the headers was switched off for the rest of the test runs in order to check the basic functionality and performance. This is only possible with developer tools in the laboratory environment. Further conceptual analyses and adjustments are necessary at this point for stable productive operation.

Table 1: Performance when transferring files.

Chunk Size	Transmission Time
25 MB	3:38 min
100 MB	4:30 min
100 MB	4:53 min
400 MB	4:30 min
400 MB	4:32 min
400 MB	4:35 min

For the tests, a file with a size of 660 MB was used. In the individual test runs, this test file was split into chunks of different sizes. The tests have shown that the conceptual solution is applicable (apart from the transfer of the content range in the header).

As you can see in Table 1 the tests were performed with varying chunk sizes multiple times. Some test runs were repeated several times with the same chunk size to determine whether the transmission time was deterministic. As can be seen from the test runs with 100 MB, the observed transmission time are subject to fluctuations. This can be attributed to the network load. The choice of the selected chunk size (100 MB or 400 MB) only has a small influence on the overall duration of the transfer. Only the change to a rather small chunk size (25 MB) led to a significant improvement of the transmission time. However, depending on the project environment, underlying resources and hardening measures, the chunk size must be adjusted accordingly (e.g. regarding network traffic).

Additional Tests

In addition to the primary test of file transfer from the high side to the low side, further tests were also performed:

- Parallel transfer of two large files

  With the current test implementation of the conceptual solution, a simultaneous transfer of two large files is not possible and leads to an error. Therefore, the demonstrator needs to be adapted.

- Switching off the receiving side during transmission

  When switching off the receiving side during transmission, you receive an error on the sending side, that no connection to the receiving side has been established. After restarting the receiving side, the transmission does not continue automatically, but can be restarted.

- Switching off the sending side during transmission:

  When switching off the sending side during transmission, the transmission is no longer continued. No error messages are received on the receiving side. After restarting the sending side, the transmission is not continued automatically, but can be restarted.

CONCLUSION

The key issue with the transfer of large files across a domain boundary in a multinational military context is the technical restriction of the HSM to a maximum file size of 400 MB. Therefore, a conceptual solution was designed to split files into transferable chunks. The tests with the laboratory demonstrator have shown the fundamental functionality. Initial feedback regarding the accreditation of the current version of the conceptual solution from the responsible authorities in Germany was positive. The further development of the laboratory demonstrator is subject of future research and work. The removal of the content range header field remains an open issue. Up to now, the content range has been used to achieve a more robust transmission. For future versions, a different approach must be identified for this. Furthermore, additional aspects require investigation to advance the conceptual approach into a solution suitable for productive use. Among other things, the effects of the project environment, underlying resources and hardening measures on the chunk size and transfer duration need to be analyzed. Special cases, such as the test cases described in the chapter “Additional Tests”, will also be part of future work.

ACKNOWLEDGMENT

Parts of the work of the authors being described in this publication has been funded by the BMVg (Federal Ministry of Defence). The standard STANAG 4559 is developed within the CST of STANAG 4559. The authors acknowledge valuable help and contributions from all partners within the CST.

REFERENCES

Essendorfer, B., Kuwertz, A. & Sander, J. (2018). Distributed Information Management through Coalition Shared Data. NATO Science and Technology Organization (STO) STO-MP-IST-160.

Kerth, C., Klotz, P. & Essendorfer, B. (2019). A new approach for information dissemination in distributed JISR coalitions. Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation.

NATO Standardization Office (NSO) (2017). Confidentiality metadata label syntax - ADatP-4774 Edition A. Available at: https://nso.nato.int/nso/nsdd/main/standards/stanag-details/8612/EN (Accessed: 07 March 2025).

NATO Standardization Office (NSO) (2018a). NATO Standard ISR Library Interfaces and Services - STANAG 4559. Available at: https://nso.nato.int/nso/nsdd/main/standards/stanag-details/8838/EN (Accessed: 07 March 2025).

NATO Standardization Office (NSO) (2018b). NATO Standard ISR Library Interface-AEDP-17. Available at: https://nso.nato.int/nso/nsdd/main/standards/ap-details/2272/EN (Accessed: 07 March 2025).

NATO Standardization Office (NSO) (2018c). NATO Standard ISR Streaming Services-AEDP-18. Available at: https://nso.nato.int/nso/nsdd/main/standards/ap-details/2273/EN (Accessed: 07 March 2025).

NATO Standardization Office (NSO) (2018d). NATO Standard ISR Workflow Architecture-AEDP-19. Available at: https://nso.nato.int/nso/nsdd/main/standards/ap-details/2274/EN (Accessed: 07 March 2025).

NATO Standardization Office (NSO) (2018e). Metadata Binding Mechanism - ADatP-4778 Edition A. Available at: https://nso.nato.int/nso/nsdd/main/standards/stanag-details/8613/EN (Accessed: 07 March 2025).

NATO Standardization Office (NSO) (2022). NATO Core Metadata Specification (NCMS) - ADatP-5636 Edition A. Available at: https://nso.nato.int/nso/nsdd/main/standards/stanag-details/8879/EN (Accessed: 07 March 2025).