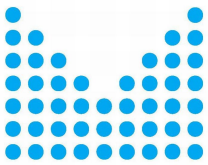
Materiál Ministerstva vnitra



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Export z Národní architektury eGovernmentu ČR

Obsah

Document Management Systems

Document Management System Description

General information about the filing service

According to Act No. 499/2004 Coll., the file service is performed by the so-called designated originators, while the Act also stipulates for which entities the obligation to perform the file service in electronic form in electronic file service systems is imposed. The performance of the filing service is understood as 'ensuring the professional management of documents arising from the activities of the originator or its predecessors, including their proper receipt, registration, distribution, circulation, handling, execution, signing, dispatch, storage and disposal in the shredding procedure, including the control of these activities'. The Archives and Records Management Act defines the term 'document' as any written, visual, audio or other recorded information, whether in analogue or digital form, which has been created by the originator or delivered to the originator. The Archives and Records Management Act also defines the term 'metadata' as data describing the context, content and structure of documents and their management over time.

Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ('eIDAS') defines the term 'electronic document' as any content stored in electronic form, in particular as text or as an audio, visual or audiovisual recording.

The legislative framework for the performance of the filing service is determined by Law No 499/2004 Coll., on archiving and filing service and the implementing Decree No 259/2012 Coll., on details of the performance of the filing service. The National Standard for eSSL issued by the Ministry of the Interior sets out detailed technical requirements for the application and business functions of eSSL and other document management systems (ISSD).

In terms of 'medium', documents can then be divided into an analogue group (typically a paper-based document) and an electronic group (see eIDAS regulation).

The Law on Archives and Records Management introduces the concept of 'output document data formats', i.e. formats that must be accepted by public originators. The definition of these formats is set out in Article 23 of Decree No 259/2012 Coll.

Section 3(5) of the Archives and Records Act sets out the conditions for documents in digital form, where preservation also means ensuring the authenticity of the origin of documents, the integrity of their content and their legibility, the creation and management of metadata relating to these documents in accordance with this Act and the attachment of data proving the existence of the document over time. These characteristics must be maintained until the selection of the archives is made.

The Archives and Records Management Act also lays down specific conditions for dealing with documents in digital form, such as conversion between analogue and digital form or change of data format.

The Act also takes into account situations where public law originators may fulfil their obligations by recording documents outside the filing service systems in so-called separate document registers, where these registers, like electronic filing service systems, must meet the requirements of the National Standard.

To summarise the basic requirements, obliged entities must:

1. Perform the filing service by recording documents in an electronic filing system or in a separate document filing system.
2. Ensure that the eSSL and any separate records of documents held electronically comply with the

requirements of the NSESSS.
3. Have one electronic filing system.
4. Ensure that other information systems are integrated with the eSSL or separate document filing systems as required by the National Standard.
5. Maintain a name register, assign meaningless identifiers to subjects, and create and manage linkages of all documents containing personal information to persons in the name register.
6. Properly store and manage digital documents and their components in eSSL or a separate document repository.
7. Maintain metadata records on files, documents and other entities and ensure that all transactions and defined operations are recorded in the eSSL or in a separate record in accordance with the requirements of the National Standard
8. Ensure that documents are received, recorded, distributed, circulated, processed, produced, signed, sent, stored and disposed of in the shredding process in accordance with the Archives Act, the Filing Ordinance and the National Standard
9. Ensure proper verification of the authenticity and integrity of the digital documents received in accordance with the eIDAS Regulation and Act No 297/2016 Coll. and ensure proper attachment of authentication and authorisation elements to the digital documents produced by the originator in accordance with these regulations
10. Preserve the documents and enable the selection of archives, transferring the selected archives in analogue form to the relevant State archives and the archives in digital form to the relevant digital archive.

Digital Continuity

Digital continuity is the set of processes, measures and resources necessary for the originator to be able to ensure the long-term reliability of information and documents. Given the different nature of the activities of private document originators and public originators, the situation is simpler for public originators. For both groups of originators, however, the basic principles contained in ISO standards, in particular ISO 30300 Document Management Systems, ISO 15489 Document Management, ISO 16363 Audit and Certification of Trusted Digital Repositories, can be used as a basis. The aforementioned standards cover the links between business processes and documents, the assurance of evidential value, the concepts and principles of document management from birth to storage and the assurance of long-term trustworthiness.

Document authenticity refers to the question of whether a document is original: a document is authentic if it has not been altered. In the case of electronic documents, all types of cryptographic electronic signatures, seals and time stamps can ensure their immutability (also known as integrity). That is to say, a guaranteed electronic signature, as well as all higher types of electronic signatures (both a guaranteed electronic signature based on a qualified certificate and a qualified electronic signature), a guaranteed electronic seal, as well as all higher types of electronic seals, and an electronic time stamp.

Document **authenticity** refers to the question of whether a document originates from who we consider to be its originator, and is generally inferred from the authentication elements that the document bears. In the case of electronic documents, these are electronic signatures, electronic seals and electronic time stamps. These are first examined (verified) for their validity, which is a technical concept and depends on the fulfilment of certain technical conditions (described in more detail in Articles 32 and 40 respectively of the eIDAS Regulation). Only if their validity is proven, depending on the type of electronic signature or seal, can the legal authenticity of the relevant authentication elements (signatures and seals) be inferred from the technical validity and, consequently, the authenticity of the electronic document as such.

In this context, it should be stressed that the possibility of verifying the (technical) validity of electronic signatures and seals, as well as time stamps, disappears with the passage of time. This is a fundamental feature, a kind of time safety, characteristic of all guaranteed (and higher) types of electronic signatures, seals and stamps. Its purpose is to protect already created electronic documents from obsolescence and weakening of the cryptographic procedures and algorithms used in their signatures (as well as seals and timestamps). Without this temporal insurance, after a certain period of time, it would no longer be possible to infer the legal

authenticity of signatures, and thus of entire documents, from their technical validity: due to the weakening of the cryptographic algorithms used in the originally signed document, it would no longer be possible to realistically find (calculate) another document that is so-called collision-proof with the originally signed document. That is, a document that has different content but the same electronic signature. It would then be possible to transfer the electronic signature from the originally signed document to the later created conflicting document, and in both cases such a signature would be verified as (technically) valid - and it would no longer be possible to reliably prove which document is genuine (which was originally signed).

On the other hand, the issue of digital continuity of electronic documents does not include the question of their authenticity, or the correctness of the content of these electronic documents. In practice, the requirement to ensure or maintain the digital continuity of electronic documents in the long term applies only to those electronic documents for which there is some reason to maintain the possibility of proving their authenticity and genuineness.

Governing Documents

In the context of the performance of the filing service, the controlling documents are in particular:

- Legislation
    1. Act No 499/2004 Coll., on archiving and filing services
    2. Decree No. 259/2012 Coll., on the details of the filing service
- Technical and architectural requirements
    1. National standard for electronic filing systems
    2. National architectural plan
- Internal governing documents of the Office
    1. File Rules
    2. Filing plan
    3. Information concept of the Office
- Documentation on the electronic filing system
    1. ESSL documentation
    2. Documentation on ESSL integrations
    3. Documentation related to the performance of the filing service

Other resources

There are a number of other sources of information and methodological documents related to the filing service published mainly by the Department of Archives and Filing Service (OAS) of the Ministry of the Interior and the National Archives of the Czech Republic.

View of the document management system

Document Management System Rules

We consider the Records Service to be a common office-level capability (capability) where most of the principles are the same across the entire office (motivation layer, ESSL application layer and integration, business process layer, and functions and interactions) and there is minimal variation at the individual agency level based on the performance of the agency. The architecture of the performance of the file service should therefore be included in the capability map of the office.

In the development of the Enterprise Architecture of the Authority and in the development and implementation of individual architectures, whether related to agencies or capabilities or their solutions, it is necessary to include the file service as a generic capability and to address its implementation in the right way. In doing so, consideration must be given to the extent to which the actual and technical performance of the file service is common across the organisation and whether and how it will vary from one agency or solution to another. The clear recommendation is to have one electronic filing system and for other information systems, including agency information systems and operational information systems, to ensure the tasks related to the management of documents (attachments to transactions) and the performance of the filing service by integrating with the electronic filing system through a prescribed interface.

The following elements, at least, should therefore always be part of the architecture of the office from the point of view of the filing service:

- An electronic filing system (meeting the requirements of the National Standard), including mailroom and mailroom modules enabling the receipt and dispatch of digital documents through the correct communication channels
- A name register (may be a separate component), preferably integrated with the office's client master data register, notified from the basic registers.
- A filing cabinet to preserve closed files and processed digital documents for the duration of the shredding period
- ESSL interface providing document-related tasks and processes of document registration and metadata management in ESSL in the form of application services for other information systems of the Office (agency, operational)
- Information systems managing documents integrated on the ESSL interface

Since the legislation generally assumes that one ESSL is always operated within the authority and other agency and operational information systems are integrated to it and that document-related tasks are performed via the ESSL interface, the integration of all document management information systems (unless they are not themselves a separate electronic record of documents) with the ESSL should be implemented in the authority and the ESSL itself linked to the repository for storing digital document components. The figure below shows the general state of understanding of the integration of an electronic filing system using one central repository for digital documents.

When we talk about the integration of an information system with an electronic filing system and the management of document-related tasks, this integration can be handled at the level of business objects and their metadata according to the following rules:

1. The digital document, or its components and data files, are stored in a digital document repository that provides care for the digital files
2. The metadata about the document is managed by a record-keeping tool, i.e.:
    - An electronic filing system, or
    - an information system which acts as a separate record-keeping system
3. The following are authorised to work with the files in the repository:
    - the electronic filing system, or
    - an information system serving as a separate register, or
    - an information system integrated at the ESSL through the ESSL
4. The Name Register shall keep a record of the data on the subjects to which the documents registered in the filing system relate

Links to the architecture of the agency information system

Within the architecture of any public administration information system used to support the performance of public administration agenda activities, it is necessary to think also about the performance of the file service. Since virtually every public administration agency either creates, processes, sends or records documents, or records a record in a file (from the point of view of legislation on the file service), it is necessary to provide for

file and document-related operations. In general, there are two ways of ensuring that the file service obligations in relation to a given AIS are met, as follows:

1. Integrate the AIS with the ESSL through a prescribed interface and ensure that the document-related tasks are performed by the AIS through that interface.
2. Ensure that the AIS complies with the requirements of the National Standard for ESSL for 'stand-alone filing' and that document-related operations and all processes related to the performance of the filing service are performed in stand-alone filing by this system.

Links to operational systems architecture

It is very often forgotten that the performance of the filing service applies to all documents, and therefore not only to official documents such as submissions and decisions in the performance of public administration agendas. In the case of public authorities, it concerns the registration and management of all documents (except those which the authority has reasonably exempted from registration in its filing system) and therefore the electronic execution of the filing service must also be ensured for working, operational and non-official documents. This applies to documents of a working nature (minutes of meetings, organisational and management documents, management acts, internal communications), but also to all documents of an economic and operational nature (invoices, orders, contracts, economic documents, personnel files, requisitions, accounts and reports, etc.).

In the case of operational information systems, we clearly recommend their integration into the electronic filing system. Especially in the case of economic information systems, HR and payroll management systems and other management information systems related to various applications, records and workflow processes, the performance of the file service is often forgotten. Integration to ESSL is appropriate here, as ensuring that all the National Standard requirements for separate records for these systems are met would entail disproportionate financial costs associated with the acquisition and development of these operational IS. Integration with the ESSL will also ensure the proper implementation of shredding procedures for these types of documents.

Background to the entity data architecture

Pursuant to § 64(4) to (8) of Act No 499/2004 Coll., on archiving and filing services, designated originators who carry out the filing service in electronic form must operate a so-called 'Name Register' as a separate component, in which they enter specified minimum data on all the subjects to which the documents they hold relate.

The implementation of the interconnection of the Name Register and the other components, or the implementation of the processes of registration of subjects, is as follows:

- In the Office, each ESSL has a Name Register as a logical component. Subject to all other conditions being met, the Name Register may also serve as the entity registration resource.
- The Name Register records data on all subjects to whom the recorded documents relate, using the AIFO of the natural persons in the agenda of the file service, not in the agendas in which the persons are registered. The internal identifier, not the AIFO, should be used for linking the name register to the eSSL and other document registers.
- The registration of subjects in the Names Register and the registration of subjects for the purpose of serving an agenda are two separate things, so care must be taken to follow the correct procedures, see the related sections on subject registration and identifiers.

Possible ways to ensure digital continuity of documents

It is very important to keep the issue of digital continuity in mind and to actively take care of your electronic

documents. Public originators must ensure that documents are recorded either in a filing system or in separate document registers. Both of the above mentioned methods must then meet the requirements of the National Standard for Electronic Filing Systems in accordance with Act No 499/2004 Coll. If we focus on electronic documents in the sense of the eIDAS Regulation, then we will talk about electronic filing systems and electronic document registers. One of the key requirements of the National Standard is the existence of a so-called transaction log - a record of operations carried out within the electronic filing system or within a separate electronic document register. In the case of electronic documents, the transaction log ensures that from the moment a document is registered until it is transferred to an archive or is discarded and destroyed, any operation relating to the document being registered is systematically recorded. This ensures that certain characteristics of the electronic document, in particular the authenticity of its origin and the integrity of its content, can be guaranteed within the filing system throughout the life cycle of the document. The readability of each electronic document must also be ensured throughout its life cycle, both in a technical sense and in terms of its user-perceivable form.

For public originators, in view of the above-mentioned requirement to demonstrate the authenticity of the origin and the integrity of the content of the document, there is a legal obligation to verify electronic signatures, electronic seals and electronic time stamps if the incoming electronic document contains them. Those originators are legally obliged to record the results of the verification in their record-keeping systems, which, as mentioned above, must comply with the statutory requirements, including the requirement to maintain a transaction log. Therefore, after the initial verification, it is not necessary for public originators to use methods such as those commonly used to ensure 'trustworthiness of origin' for private originators - for example, it is not necessary to re-stamp electronic documents with time stamps before their expiry, etc. - the trustworthiness of origin of electronic documents is ensured for public originators by the proper systematic recording of documents in designated systems, where, in addition, it is possible to prove all operations that have taken place with the recorded document throughout the life cycle of the document by means of a transaction log - i.e. The systematic recording and transaction protocol are sufficient to prove the authenticity of the origin.

The above can also be easily verified for public originators - auditing of filing systems can be carried out over time and every public originator has a statutory obligation to audit these activities. Electronic filing systems, as well as some significant stand-alone document filing systems (typically agenda information systems), meet the characteristics of a 'significant information system' from the perspective of the Cybersecurity Act, as in the event of their failure or malfunctioning, public law originators would not be able to carry out their activities properly and continuously. In view of this, they should be identified as significant information systems and notified to the National Cyber and Information Society Authority through the procedure under the Cyber Law. This will also bring these systems under the regular scrutiny of the cyber security services.

Electronic filing systems and separate document filing systems also process personal data of natural persons, therefore public authorities have a number of obligations over these systems with regard to the obligations under the General Data Protection Regulation and the Personal Data Processing Act, which also increase the overall credibility of the systems in which public authorities record their documents.

The above measures allow public originators to demonstrate the authenticity of the origin in a completely reliable manner, including for documents received containing electronic signatures, electronic seals and electronic time stamps, without the need to re-stamp them with time stamps or other authentication or authorisation elements.

Potential problems

A potential risk of ensuring digital continuity based on eSSL transaction protocols is the issue of document collisions. This is a situation where a fingerprint (called a hash) of a document is noted in the NSeSSS-compliant transaction log along with the hash algorithm used, but the same hash may correspond to other documents. Consequently, especially for received documents, it is not possible to deduce which document (via its hash) the transaction log refers to, which significantly complicates any possible testimony of legal validity.

To eliminate this risk, procedures can be used to extend the verifiability according to the ETSI (The European

Telecommunications Standards Institute) standard, which corresponds to the eIDAS regulations. This involves the repeated addition of qualified electronic time stamps and validation information to extend the validity of signatures and seals on electronic documents. Simply put, these measures are in the nature of a new electronic signature, a new sealing or a new qualified electronic time stamp measure. These options mean that currently sufficiently strong cryptographic procedures and algorithms (in particular sufficiently robust hashing functions and sufficiently large keys) are used to authenticate the original document, making it - again for a certain period of time - sufficiently difficult to find conflicting documents. Due to the different legal effects of electronic signatures (representing an expression of will), electronic seals (representing a statement of origin) and time stamps (representing a 'fixation in time'), it is qualified electronic time stamps that are used in practice to extend the validity of original signatures and seals. It is important that every single step of this long-term process is carried out in a timely manner. That is to say, the next time stamp must be added before the so-called "time lock" takes effect (before the time-limited ability to verify the original signature or seal expires). Alternatively, missing the deadline will cause the late added timestamp to no longer have a prolonging effect.

In practice, it is not necessary to add (timely) time stamps to individual documents. It is possible to minimize the consumption of timestamps by, for example, placing multiple documents (or only their impressions) together in a suitable container (ASiC) and only timestamping the container as such. The grouping into containers is appropriate according to the logical association of documents, for example at the file level. Similarly, it is irrelevant who takes the measures outlined above, which are necessary to ensure the digital continuity of documents.

However, **it must be noted that, although the risk of document conflicts exists, the current legislative environment does not give public originators sufficient room to decide and weigh up the risks for themselves, and the additional attachment of electronic seals or time stamps could be contrary to good management, as the cost of ensuring such a procedure could be a waste of public budget resources.**

eSSL, File Service, Functional Unit, File Service