Guidelines for digital signatures

Ref. no 1-638/2022

In effect from 2022-06-14

Karolinska Institutet

Guidelines for digital signatures

Ref. no 1-638/2022

CONTENT

Diarienummer: 1-638/2022	**Dnr föregående version:** -	**Beslutsdatum:** 2022-06-14	**Giltighetstid:** Fr.o.m. 2022-06-14 och tills vidare
Beslut: Universitetsdirektören		**Dokumenttyp:** Riktlinjer	
Handläggs av avdelning/enhet: Juridiska avdelningen		**Beredning med:** It-avdelningen, enheten arkiv och registratur, juridiska enheten	
Revidering med avseende på: Nytt styrdokument			

Introduction

Karolinska Institutet (KI) is committed to transitioning, to the greatest extent possible, to digital administration. Part of this move is the use of digital signatures (e-signatures). There are numerous signing services available, but none that has been produced for the specific and common use of public administration in Sweden or the EU. Common EU rules have, however, been set out in eIDAS regulation[1], which includes solutions for e-signatures ("trust services").

KI and other higher education institutions offer a service called eduSign, which has been produced by Sunet (Swedish University Computer Network) and which complies with the Agency for Digital Government's (DIGG) framework for digital signatures for public authorities. Some administrative systems (e.g. Agresso and Primula) have integrated e-signature solutions.

When you receive a document that contains an e-signature, you must decide if it is trustworthy, i.e. that the signature is genuine and that the document has not been altered since signing. This is referred to as validating the signature. You must also assess if the form of the document meets the needs of your department and decide how the document is to be archived.

An e-signature generally takes the form of a service that gives the user a verification code or requests e-identification. An e-signature is legally binding in the same way a handwritten signature is.

Inserting a scanned signature into a document as an image file or verifying a document by email is not the same as an e-signature. Such methods are easy to forge and cannot be tied to the signatory and must therefore not be used at KI.

Purpose

These guidelines are for all KI employees and are intended to be a support in the choice of digital signature service and for the validation of a digital signature in a document.

General information of the regulation of signatures

Information on which documents require a handwritten signature is available in law and regulations. No such requirements are contained in the ordinances that govern activities at KI. There is however requirements that the document must state who has made a decision.

If internal rules at KI require a handwritten signature or set specific requirements for a signature, these rules apply.

The right to make decisions and act as an official KI signatory (i.e. to represent the university) is provided in the President's Decision-making Procedures and

[1] The EU Parliament and Council Regulation 910/2014 on electronic Identification, Authentication and Trust Services for electronic transactions in the EU single market (eIDAS).

Delegation Rules for Karolinska Institutet or in specific delegation decisions.

Specific information on contracts

Agreements can be signed digitally if the service complies with KI's Decision-making Procedures and Delegation Rules or specific delegation decisions in that all signatories have access to the service and that the signatures are supplied in the correct order.

Everyone signing an agreement must use the same type of e-signature service. A combination of e-signature services or of digital and manual signatures in the same document is prohibited.

The significance of an e-signature

An e-signature is personal and connected to an individual. When you sign a document with an e-signature, your identity is tied to the electronic document. The signatory verifies that the document and its content is correct and confirms or accepts what is contained in the document.

Signature service requirements

The signing service used in the EU must meet the requirements of an *advanced* or *qualified* electronic signature as defined by the eIDAS.

An *advanced e-signature* requires the user to identify itself and that the user can be linked to the signatory.

A *qualified e-signature* is essentially the same as an advanced signature but also meets the requirements for qualified trust services. The Swedish Post and Telecom Authority (PTS) has supervisory responsibility for e-signature services and other trust services as set out in the eIDAS regulation. Support for the choice of signature service can be found on the PTS website, which has lists of qualified providers and trust services.

An advanced or qualified e-signature service can be used to check if the document has been changed after having been signed.

If the counterparty's signature service has been used, you must make sure that KI can subsequently determine that the signature has been supplied by a certain person for a certain document.

Archiving requirements

Digitally signed documents must be archived in exactly the same manner as physical documents in accordance with KI's document management plan. Before a document is electronically signed, there must be a long-term means in place of archiving both the document and its signature(s). It should be possible to ensure the document's authenticity and reliability over time.