Memo

1 December 2016
Classification:
C – For public use

Description of the partnership between the Danish Agency for Digitisation and the banks in Denmark for the procurement and operation of the next generation of NemID

Introduction

The Danish Agency for Digitisation, on behalf of the public sector in Denmark, and FR1 as representative of the banks in Denmark, have, effective from 1 July 2016, entered into a partnership, which will lead to the development and operation of a replacement for the existing NemID.

The partnership has agreed to share the procurement and operation of the core of the coming solution, which includes the identification and authentication of individuals – in a public context understood as citizens and in a bank context typically understood as private customers.

However, for banks as well as the public sector, it is important that the overall solution for the next generation of NemID can handle more demands than just identification and authentication. In parallel with the procurement of the core, it is therefore necessary to establish a number of additional components, both public and private, and the use of NemID in a business context must be addressed. The partnership has agreed to put the core functionality out to tender together with the public sector's additional components for signing and an end user-oriented client.

The sum of the core and additional components is referred to as 'citizen solution' or NDIS, which stands for National Digital Identity and Signing (NDIS) solution.

Lots and contractors
The core and the additional components are offered in separate lots, but in the same tender. Lot No. I, the core, is offered by the banks and the Danish Agency for Digitisation jointly, while Lot No. II, additional components, is offered solely by the Danish Agency for Digitisation. On the customer side, there will thus be two contractors for the core (FR1 and the Danish Agency for Digitisation) and only one for the additional omponents (the Danish Agency for Digitisation). The banks' additional components for the core are not included in the total tender procedure.

1. The core

The core is currently expected to contain three key elements:

- Development and operation of a joint authentication service (the technical solution)
- Set of rules (scheme and code)
- Certification service

Signing and transaction approval is not included in the core.

1.1 Authentication service

The technical solution consists of elements that render the authentication possible as well as a so-called RA portal for registration and enrolment of end users and an end-user portal where end users can manage their digital identities.

1.2 Set of rules (scheme and code)

The partnership will lay down a set of rules consisting of a scheme and a code. The scheme governs the 'graphical' appearance of the solution. Elements in the graphical appearance can be logo, colours, font size etc. The code sets out guidelines for the submission of the various factors in relation to different transaction types, e.g. factors known from the existing NemID solution, i.e. user ID, password and the code from the code card or the code token. Other factors too, are in play, such as biometric data.

The scheme and the code will not only govern the authentication process, but also control parts of the elements outside the core.
All clients must therefore comply with the scheme and the code – not only in relation to authentication – but also in relation to signing.

1.3 Certification service

Clients are developed not only by the public sector in Denmark and the banks, but also by third parties who want to do so. As part of the core, a certification service must be set up to ensure that all clients comply with the scheme and the code.

2. Additional components – signing component and end user-oriented client

In addition to the core, the Danish Agency for Digitisation procures a signing component and an end user-oriented client to enable citizens to authenticate themselves towards public authorities and sign digital documents and data in public services using the NDIS solution.

2.1 Signing component

The expectation is that the signing component will be designed to issue electronic signatures with related certificates based on authentication of end users in the

core. Thus, the signing component is to operate closely with the core. Signing is expected to be based on short-term keys and certificates.

2.2 Client

The Danish Agency for Digitisation procures an end user-oriented client that can communicate with the core and the signing component, thus creating a total authentication and signing solution in the form of NDIS. The intention is that the Danish Agency for Digitisation will make the signing component and the client available to private service providers.