APPOINTMENT OF SECURITY OFFICERS

Danmarks Nationalbank
Corporate Services
Portfolio Management and Central Banks Systems

Copy:
Account holders

Case number: 149935
Document number: 1605037

03 February 2017

Danmarks Nationalbank has chosen to centralise the user administration in Kronos2, which means that in future it will not be possible to obtain local access for individual banks to see their users' access rights to the system. Therefore, please appoint at least two "security officers" within your organisation who will be responsible for e.g. requesting access to/amending user rights in Kronos2.

Appointment of security officers

The appointment of your security officers must be approved and signed by an authorised signatory within your organisation. You must appoint at least two security officers. Please use *one* form for each security officer. See form: "Authorisation to security officer to appoint users in Kronos2 and assign user profiles, etc".

The form must be signed by authorised signatories under the signatory rules that are given to the Danish Commerce and Companies Agency. In addition we ask you to submit a new statement from the Danish Commerce and Companies Agency and updated signature circular.

If the account holder's business activity has not been registered by the Danish Commerce and Companies Agency the account holder shall in a manner which is satisfactory to Danmarks Nationalbank document the legal validity, etc. of the rights of signature and powers of attorney in accordance with the legislation of the home country.

All documents must be returned by 17 February 2017 to:

Danmarks Nationalbank
Att.: Kronos Group
Havnegade 5
DK-1093 Copenhagen K
Denmark

Once the system has gone live, only security officers registered at Danmarks Nationalbank may request access to/amend user rights in Kronos2 for users within their institutions.

Danmarks Nationalbank recommends that the security officers appointed are separate from the operational functions of your organisation. However, this is not a requirement. What matters is that the solution chosen makes sense for your organisation.

Responsibilities security officers
Besides being able to request access to/amend user rights in Kronos2 for users within your institutions, security officers are also responsible for:

- Periodically reviewing the list of users and access rights within your organisations and sending any changes to Danmarks Nationalbank.
- Stating to which extent your institution wishes to apply the 4-eyes principle.
- Stating whether they wish to receive specific, optional SWIFT messages (relevant only for account holders using SWIFT).

As soon as your security officers have been appointed, there will be two tasks which need to be looked at as soon as possible:

1. **Security officers must confirm the already collected production information on your users and bank set-up**
   This will be done via e-mail. When the information is confirmed, subsequent changes to user information and bank setup will follow the future request process. A description of the future request process will be sent directly to the selected security officers.

2. **A primary security officer must be identified by name and postal address**
   This security officer will be responsible for distributing all RSA tokens to their users up to go-live. These tokens will be sent by registered post. Therefore, it is important that we get the right contact information of the primary security officer to ensure that all tokens are received in good condition.