**iQ.Suite Crypt and global key mapping**

Individual keys/certificates belonging to the recipient as well as group or corporate keys can be used for encryption with [iQ.Suite Crypt](#). Key mapping is required when group or corporate keys are used. The following describes how these are set up globally.

**Step by Step:**

- In previous versions of iQ.Suite, key mapping was configured for each iQ.Suite job. From iQ.Suite 8.2, a global key mapping function makes it possible to make the necessary entries centrally in the basic configuration.

- When is key mapping necessary?
  
  Let us take the example of encryption with GnuPG: During encryption, GnuPG searches by default for an appropriate public key using the recipient's email address. So if an email is sent to test@irgendwo.com, for example, GnuPG tries to find a key for test@irgendwo.com on the key ring. However, if a corporate key has been imported for the domain anywhere.com (issued on info@irgendwo.com, for example), GnuPG only initially uses this key if emails are sent to info@irgendwo.com.
  
  Key mapping is required so that the corporate key can be used for all the recipients in the anywhere.com domain.

- From iQ.Suite 8.2 the menu item “Global Mapping” is available for global key mapping under Basic Configuration -> Utility Settings -> Crypt Settings.
Use the right mouse button to select the item New -> Global Mapping.

- Enter three pieces of data here

1. Name of the key mapping function
2. Email address to be used for a certain key. In our example *@irgendwo.com
3. The ID/name of the public key to be used for the configured email address. In our case this is info@irgendwo.com
The last step is to assign the global key mapping function to the relevant iQ.Suite Crypt outbound jobs. Activate the "Use global mappings" function on the "Mapping" tab to do this.
- It is not possible for existing job-based mappings to be copied automatically to the global key mapping.