Access via a generic account (user ID + password)

Some commonly occurring transfers and updates can be carried out automatically using programs. In such cases, a generic account must be used so that information related to the personal account is not disclosed.

Please note: for privacy reasons, the user ID and password cannot be hardcoded into the program.

Generic accounts must be used with the following security precautions:

1. A program (or script, procedure, etc.) that uses a generic account to access a production server must – each time it is executed – extract the user ID and password of that account from a different, protected location within the program. Depending on the technology, that location can be a configuration file, database record, etc.
2. The owner of the generic account must be able to modify the password value. This can be done with a specially created interface, standard editor, etc.
3. The "user ID & password" values may be extracted only for the program concerned and only by the owner in order to modify the password value.
4. The DG Webmaster is the only person authorised to enter a request for a generic account, which means that he or she becomes its sole owner.

   The safety requirements for the generic accounts are the same that apply to personal accounts (confidentiality, responsible use, etc.).