Other Functions of the SmartWeb Platform

The implementation of the SmartWeb server is based on the philosophy to not duplicate functionalities already existing in D2000. That is why the SmartWeb does not even have its own user management but closely integrates with the D2000 functionality in areas where it makes sense. These areas are mentioned in the next chapters.

Authentication

The SmartWeb can authenticate a user in D2000 in the following manner:

1. authentication by the entered D2000 user's name/password (+ additional authentication in an authentication RPC to restrict logins only for chosen users)
2. authentication by entered name/password in one's own authentication RPC + for automatic creation of the D2000 session for communication with D2000, name/password entered in the SmartWeb configuration will be used
3. automatic login with preconfigured name/password (meaning without showing the login display)
4. additional validation to possibilities 1. and 2. using client certificate installed on chosen devices from which one can access applications
    a. authentication can be realized locally on the SmartWeb server,
    b. or remotely from authentication RPC in D2000

Besides the mentioned methods of authentication, the SmartWeb server can call configured logOn/logOut RPC methods for every user who logs in/logs out. It is also possible to change the user's name and password through API.

Currently, we support the following authentication methods. It is possible to broaden the methods according to the clients' requirements in the future.

- HTTP BASIC for REST API
- HTTP FORM for Comet API

Connection to D2000

Connection to D2000 is realized through the JAPI library. That is why it is possible to use all the possibilities provided by JAPI for realizing the connection to D2000 such as:

- reverse connection because of the SmartWeb server in a demilitarized zone
- secured connection
- redundant connection

The Connection of the D2000 Session with the HTTP Session

For every logged in user, there is a unique D2000 created specifically for his session and lasts until the logout (Exception is the authentication through HTTP BASIC where there is one D2000 session shared by all API calls under the same user).
The web HTTP session of the logged in user is linked to the D2000 session and in the case of ending the D2000 Session (externally through a system console for example) or the HTTP Session (by logout for example), also a linked session is automatically ended so there will be no loosening of sources that are not used anymore. The SmartWeb server can end both sessions (D2000 and also HTTP) in the case of non-activity from the client's side in a time defined by the parameter *session timeout* for a user in D2000. Be careful, the session expiration happens when the client's side is non-active and sending data from the server's side by the Publish/Subscribe concept is not considered a client's activity.

Monitoring of users' and system's statistics

The SmartWeb enables to acquire statistics of D2000 RPC methods calling to a particular user also globally for the whole system through API. At the same time, it is possible to acquire system statistics about the status of the SmartWeb server for monitoring and solving of performance problems.