TABLE OF CONTENTS

1. Introduction ........................................................................................................................................... 3
   1.1 VPN Access via AT&T client (certificate based authentication) .................................................. 3
   1.2 HEIRES and WEB-Access: ........................................................................................................... 3
2. Purpose of this document ....................................................................................................................... 3
3. How to ….................................................................................................................................................. 3
   3.1 How to configure and start AT&T global network client ............................................................. 3
      3.1.1 AT&T Global Network Client: ................................................................................................. 3
      3.1.2 Profile: ...................................................................................................................................... 4
      3.1.3 AD-Authentication: ................................................................................................................ 5
      3.1.4 Profile details ........................................................................................................................... 5
   3.2 How to assign the token to your account (= enrollment) for WEB-Access and Web based Remote Service (Heires) ........................................................................................................... 6
      3.2.1 Short Description .................................................................................................................... 6
      3.2.2 Long Description .................................................................................................................... 6
   3.3 How to re-sync the token ............................................................................................................... 9
   3.4 How to reset the PIN .................................................................................................................... 10
      3.4.1 Reset with PIN + token code ................................................................................................ 10
      3.4.2 Reset with e-mail .................................................................................................................. 11
      3.4.3 Reset with SMS .................................................................................................................... 13
   3.5 How to login WEB-Access ............................................................................................................ 15
   3.6 How to login WebBased Remote Service ...................................................................................... 15
4. FAQs ..................................................................................................................................................... 16
   4.1 I don’t know my PIN any more. .................................................................................................... 16
   4.2 My token password is not accepted (any more) ......................................................................... 16
1. **Introduction**

“HEIDELBERG Remote Access” allows the authentication to the following services/applications:

- VPN Access via AT&T- Client on standard HEIDELBERG Notebooks
- Web Access
- HeiRes

1.1 **VPN Access via AT&T client (certificate based authentication)**

Two step authentication:

- User enters AD credentials (Windows logon credentials) (account + password)
- Machine certificate will be checked if credentials are valid.

1.2 **HEIRES and WEB-Access:**

Authentication v2 service by Integralis / Safenet via token

- Authentication procedure:
  - Token provides one time password (OTP) without PIN
  - User has to enter PIN + OTP in prompted field
- User Self Service:
  - User has to create a PIN with WEB based user portal
  - User can reset the PIN if forgotten
  - User can re-sync the token if it is out of sync (e.g. long time not used)

2. **Purpose of this document**

This user manual should enable the user to use features of the HEIDELBERG remote access service without additional help.

This includes how to use the AT&T client for remote access and how to use the selfs service portal for the token.

3. **How to ....**

3.1 **How to configure and start AT&T global network client**

3.1.1 AT&T Global Network Client:

Once you have Internet Access, launch the AT&T software as usual. Now click on “Profiles” in the menu bar, you will see a drop-down selection offering you all available profiles as shown below:
3.1.2 Profile:
Select the **HEIDELBERG Certificate** profile according to your region (The screenshot above displays it for EMEA), and click on "Connect" as you have done it before. The login screen will look slightly different from the one you have seen before:

![Network Login](image)

Please do not modify the Account field; it is filled automatically depending on the chosen profile.
3.1.3 AD-Authentication:
Now enter your 8-digit user-ID and your windows password (as if you were logging in into your windows) and click OK.
Important: The AT&T Global Network Client does not support passwords longer than 16 digits and most of the internationally used special characters (Cyrillic, Asian, Turkish etc.). Confirmed exceptions:

`:~!@#$%&{?`

Once the VPN-Tunnel is established, you will have to confirm the “Security Banner” as usual:

3.1.4 Profile details
Please Note that you can change your authentication method any time by choosing the corresponding profile. The new Token solution is only meant as backup for the certificate solution as well as Web Access and HEIRES Authentication.
Currently the application displays 3 authentication methods with one profile for each region:

- Current token authentication (current solution to be replaced soon):
  - Heidelberg EMEA (Profile name: DEEID)
  - Heidelberg America (Profile name: HEIDK)
  - Heidelberg Asia (profile name: GHBA)

- New Authentication via certificate (new standard solution):
  - Heidelberg EMEA Certificate (profile name: DEEIDCA)
  - Heidelberg America Certificate (profile name: HEIDKCA)
  - Heidelberg Asia Certificate (profile name: GHBACA)

- New token authentication method (only as temporary solution in emergency cases):
  - Heidelberg EMEA Token (Profile name: DEEIDTK)
  - Heidelberg America Token (Profile name: HEIDKTK)
  - Heidelberg Asia Token (profile name: GHBATK)
3.2 How to assign the token to your account (= enrollment)
   for WEB-Access and Web based Remote Service (Heires)

After you have received the new token and the enrollment mail you need to assign the token to your account, before you can start to use it. Below find a description on what to do. The short description is for experienced users. The long description explains each step in detail.

3.2.1 Short Description
1. Click on the link provided in the enrollment mail.
2. Enter the serial number of the token (without the leading “+”) → you will be displayed an initial pin, please note this one since you may need it again.
3. Enter without blank: Initial pin (you got in step 2) and token code (you get when pressing the button on the token)
4. Define a new pin number

3.2.2 Long Description

After you have received the enrollment mail click on the link provided in the mail in order to start the enrollment process.

Title of the Mail: “Enrollment: Heidelberg Remote Authentication Service”

Your self-enrollment account has been created.
If you have not received your token yet, please contact your local IT-Contact.

Please, use the following URL to enroll with the service:

https://se.safenet-ive.com/sefEnrollment/index.aspx?code=0idiaA621rev70Kas/0a932ahq

Enter the serial number from your token (without the leading “+”), you find it on the back of the token.
Now enter your PIN + your token code. **Important: The length of PIN + token code has 12 digits.**

(Press the button on the front side. The display will show a newly generated token code).

**Important: The token display will switch off automatically after thirty (30) seconds which means you have this time to enter the six (6) digit number in your remote Authentication Service.**

Enter a new PIN number (4 to 8 digits).
3.3 How to re-sync the token

Go to the following URL:  [https://ss.safenet-inc.com/blackshieldss/index.aspx?org=JQN8WVE8T1](https://ss.safenet-inc.com/blackshieldss/index.aspx?org=JQN8WVE8T1)

Enter your User ID and the token serial number (looking backside)

![User ID and token serial number input screens](image)

Now enter your token code. **Important: The length of token code has 6 digits.**

After thirty (30) seconds enter the next code.
3.4 How to reset the PIN

Go to the following URL: https://ss.safenet-inc.com/blackshieldss/O/JQN8WVE8T1/index.aspx

3.4.1 Reset with PIN + token code

Enter your PIN + your token code. **Important: The length of PIN + token code has 10 or more digits.**

Enter a new PIN between 4 and 8 characters long.
3.4.2 Reset with e-mail

If you have forgotten your PIN you can request a new PIN via E-Mail or SMS.

Enter your User ID and click send.

Your Security PIN has been successfully reset.
Waiting for a mail with a temporary password enter your User ID and sign in with temporary password.

**Important:** Please use this password to sign in within the next 10 minutes.
3.4.3 Reset with SMS

If you have forgotten your PIN, you can request a new PIN via E-Mail or SMS.

Enter your User ID and click send. (You can only use it if you have a mobile number added in your outlook address book).

Waiting for a SMS with a temporary password enter your User ID and sign in with temporary password.

**Important:** Please use this password to sign in within the next 10 minutes.
Your Security PIN has been successfully reset.
3.5 How to login WEB-Access

Go to www.heidelberg.com

Click on Heidelberg Web Access:

Enter your Windows user account into the field “user name”

Enter your PIN + Token – Code into the field “password”

3.6 How to login WebBased Remote Service

Start your login page.

Enter your Windows user account into the field “user name”

Enter your PIN + Token – Code into the field “password”
4. FAQs

4.1 I don’t know my PIN any more.
   - See: How to reset the PIN -> 3.4

4.2 My token got lost or stolen
   - Please contact the global IT-Helpdesk

4.3 My token password is not accepted (any more)
   - Ensure that you have entered your PIN & one-time password correctly.
   - Check if your password does not exceed 16 digits
   - Check if your password does not contain any special characters → 3.1.3
   - Ensure that your token is in sync. See: How to re-sync the token -> 0