Using Fallback scenario instructions

1. TPP authenticates with a call to **GET /service/TPP/Token**

Accessing the service, hosted on <https://online.tbibank.bg/service/TPP/Token> with web browser, TPP has to provide the certificate which will be used for data encription. The response of the service contains token and its expiration date. The token is encrypted with the public key of the TPP as shown on **Example 1**

*Request:* GET /service/TPP/Token HTTP/1.1

Host: online.tbibank.bg

Accept: application/json

*Response ("Content-Type":"application/json; charset=utf-8"):*

{

 "expirationDate": "2019-02-13T17:11:38.944609+02:00",

 "channel": 17,

 "encryptedKey": "MIICqAYJKoZIhvcNAQcDoIICmTCCApUCAQAxggJBMIICPQIBADAlMBcxFTATBgNVBAMTDHYtYnVsYmFuayBjYQIKWQV9dwAYAAANGzANBgkqhkiG9w0BAQEFAASCAgCtftxLnT4lhfZ3ZIhPz4hCtJEzcN4YVewljy51lGoFroYme+oIW+fxhMddpTI8pLbkSDWuqoCiYUsPNEidw5Rgm4U5LFaxLWNgVkoeFNnb4Av2cDf2yG8IKVYel8TVAGIMVDGbeqoQb161E9wb5i5wQE7nk/OTlIbdSl6rkT8F9UWbYUQ3n2j/ZRTMTAmWMuMFu4kI32/dknmYnpQw8B1Y/hiZLfLAXjLQz+iv+VT+Vqhj7rjjBjNPDY9xTamLsf7ynBcP80qalrIs3UTuTl/vY4mqPHZUfJMdLdvqgKi9l57ukwfBwzmvwD5c7ktjQ43zWz5RRFk08KSqNIIrYRUyXJ66IvVS/ryY/ztk8C1vLONGTi5y0OQ+bCCM9AGDnTFflqDZURPkbxnk3tmulrqweMJ75WHtI4C2i1LfWfgrsUWl7W6ZKLhbE9Zq7BT4frmR3j4EC0VsR4ihtHzH7AxIWme1FAfK+8F5v0FE1KWt8tna+H+ElZK/q5V8pTFyOcExOJR+HK0QWOmYUoWOcE7CIZEZctMaOOH8rMxlzB4+zsvKCIjJf8o7QBU3P73yTJCpwicaJQs7ngnw4MxR+dEwWcsEAVF2YIgfro2nITm99+9bzklWhx6+rgAS+rOywiiCQRipiMcK9T2hJDP90oVphFQqOf49qu2a4kVnhM1KlDBLBgkqhkiG9w0BBwEwFAYIKoZIhvcNAwcECGXfPMLaKD/JgCizyYgcKAjT1cbW6+UEpmHPxV//RgkRJlmyMJzVEUkYQSQP30k0Naw9"

}

**Example 1**

1. TPP decrypts the token with the private key of its certificate
2. TPP forwards the bank user to authentication site of TBI bank. TPP has to fill the encoding segment xml\_id=/<languange>/tpp/ and decrypted token as shown on **Example 2:**

https://online.tbibank.bg/page/?xml\_id=/bg-BG/tpp/&token=bcb0b8696f414e549dae0826aae0d7cb

**Example 2**

1. The user provides its credentials for online banking. After successful authentication, authorised session is created. This session (login URL) is encrypted with the public key of the provided in Step 1 certificate. TPP has to create an encrypted cookie on the browser which will be used for access to the banking portal.
2. TPP retrieve encrypted login URL and cookie data with POST request on followin address **:** [**https://online.tbibank.bg/service/TPP/Token?token=<token**](https://online.tbibank.bg/service/TPP/Token?token=%3ctoken)**>** as shown on **Example 3**

*Request:* POST /service/TPP/Token?token=f0165beefb644ae2957454ab86fda46d HTTP/1.1

Host: online.tbibank.bg

Accept: application/json

*Response ("Content-Type":"application/json; charset=utf-8"):*

{

 "cookies": "MIIB4QYJKoZIhvcNAQcDoIIB0jCCAc4CAQAxggFBMIIBPQIBADAlMBcxFTATBgNVBAMTDHYtYnVsYmFuayBjYQIKF2qb4gAQAAAKnjANBgkqhkiG9w0BAQEFAASCAQBO3ZY/OdEs6ueAnGMU9IKmvghyA8OP3l6CGRpBW+5itMC6RzmVJep08gFPq+jNnLKiOjuK0iBHNqLg/uyd0LdfSafjP+Sufyv1tMKZYCYjAoWQj6ULPfIZKTLDgTc1cXJfo3p0KHhMEotmzhr5XRK8xXPG208lkpz7OAjKzpe4dKweQeAgn6gHVim9kyRsKXlXEyw9m2QkIzO61EmdsrHmlGXeBFpkHLt8tKQDeejveiBEkzx3DEj06VUmQxfoXJefboJwxmzG2F+W+1cOapPO2eqqsRy6iVQumZRSnTT38U/OQMzPUc9UutWbgRL41M+7GnS8AdtaSXo/JjwMF+UXMIGDBgkqhkiG9w0BBwEwFAYIKoZIhvcNAwcECM9Y+wWhVeQTgGB6oWnq7EFYeQurqffHBtnrTzzYqFWBPWfblmiTVKEFwpDrG+Xk2yEMfgfBc9Ugx0cOKcnZBE/1RNzwHjeoej4yAzJ3+pUDu3neqwst4W33n6FjwSfU0MpyF27xD6M++G0=",

 "url": "MIICSgYJKoZIhvcNAQcDoIICOzCCAjcCAQAxggFBMIIBPQIBADAlMBcxFTATBgNVBAMTDHYtYnVsYmFuayBjYQIKF2qb4gAQAAAKnjANBgkqhkiG9w0BAQEFAASCAQAWuf6OeHeO3LdOSQuLJGMSPm9fp/Zjx8hlKxmNo2FDXiUXjURLWaghD7BpXl7uDFk78ujXPfjNmBGSdqvrQJ2FjvWFJPc7iRY+oBKINF+HAuJIk9LXAkGBVJdDvGNsUkcumiOvpj8BFK+5togrLXEaN1XqTUbRv053pBqgmRWHqH0MwHkvF60bWP1CZ/ME2htisIlQudCYsY4A4sYYOWvJ8YDDgD4usQZrWhJpz1M24fV9dCl1/qw5avL1cLa7A5ptG/f0fYM5xBG2Q6FaLU2ziv+wLzZqX27KmnfRnQ3Q6Wx1MPKuiBRRg4xZqXHcaYc5HqOORIkAUM+yI05Vj24PMIHsBgkqhkiG9w0BBwEwFAYIKoZIhvcNAwcECCsaFKMC3pwJgIHINsXlIuxR1GbyO+g+HixSMwpnPgEzAkZp3VKIVyGcnaWPcbeI7uD6XWjqNGuaY74l5Dbs26fnva2EDKrVBqKDaoGhoc4Sjh6e1R9BC6fWxUZwm6EfvgTs4DU19wXz9eWIfcDJlZDwbVjZ9cIUNBS3H0SfNELLCjBXHhZrTxc9JlX1rVkFVE+YF2MOQkhsI1iKv8QwK26ow1CTQWU1Pbma5Iv6y1l/5SMbuCgV/ZBC0/tU8A+z2JUgbJkCgr4H345iMgyvm8Tc2kM="

}

**Example 3**

1. TPP decrypts received data with the private key of its certificate.

**NB!** Authorised session could be terminated by selecting “Logout” on banking portal. Once terminated, the user has to create a new session, completing again Step 3 from this instruction.