altipeak security

Use case of Transaction signature

1. Altipeak Transaction Data Signature Mobile solution

The Transacion Data Signature Mobile solution (TDS) include also the time based OTP functionality for Strong authentication.

It can be used by:

- **Internal users** use Time based OTP Mobile app and physical devices to access (strong authentication) their heldesk portal and for remote access to the organization (VPN)
- **External users** (customers) use the Time based OTP Mobile app
    - To access the client portal
    - To sign online transactions to secure validity of transaction data
    - To sign offline transactions (handwritten material like fax or mail) to secure validity of data and verify that an authorized person requested the transaction

When TDS is enabled on the Safewalk mobile application, the application will have an additional screen with input for data that generates a transaction data signature code that can be used to enable different types of applications.

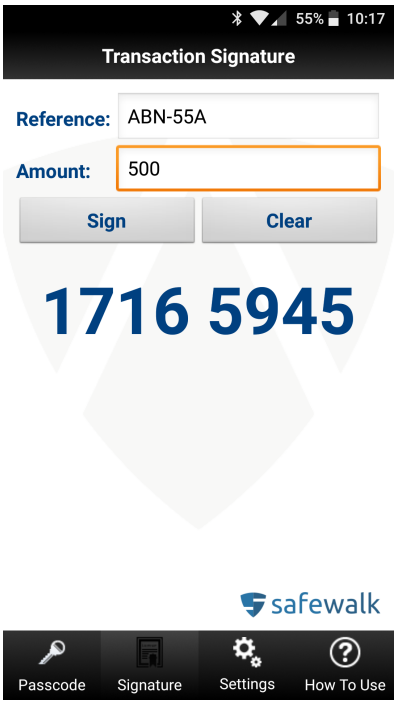
2. Use of Transaction signature for online transactions

The TDS functionality works the same way for online transactions verification and for offline verification. There is little difference on the workflow.

The TDS Mobile app use and workflow for on-line transactions verification is the following:

Assume the user wants to do an online transfer of USD 500:

- User access the Bank portal with the OTP generated on his Mobile app
- User enter transaction data in the Bank portal
- In the portal, the Bank asks the user to enter part of the transaction data (challenge) in the mobile app
- User enter transaction data requested by the bank as shown below :



- User Press « Sign »
- The Mobile app will perform a signature of transaction data entered by the user together with other secrets and generate a transaction signature code (17165945) in the example above)
- User enter the transaction code in the portal
- The Server verify that transaction data has not been modified by, for example, a man in the middle by correlating the transaction signature code with the received data
- If verification ok, transaction is processed

3. Use of Transaction signature for offline transactions

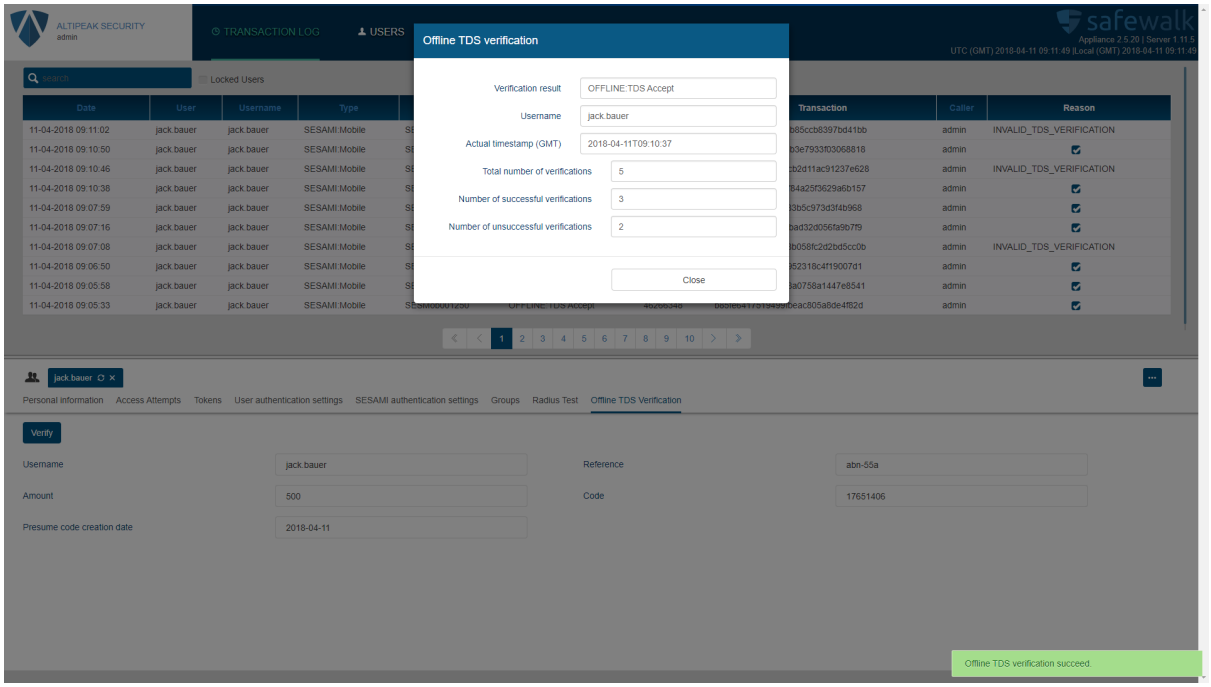
TDS Mobile app for off-line transaction verifies the authenticity of hardcopy documents such as FAX that were sent by customers.

Assume the user wants to send a request for a transfer of USD 500 to the bank by fax.

The TDS Mobile app use and workflow for off-line transactions verification is the following:

- The sender opens the Mobile app
- User enter transaction data the same way as for the online transaction case above
- User press « Sign » and Mobile app generates the transaction signature code
- User writes the code in the paper and send it
- Bank receives the fax
- Operator at the bank checks the fax (hours, days, etc. later)
- Operator goes to the Management console
- Operator select the user, enter trnsaction data and the transaction signature code
- Operator clicks « verify »
- The console confirms validity and gives the exact date and time of the request and it tells how many verifications have been done (can be verified several times in the case several departments need to verify the transaction). The offline signature verification application provides a mechanism to verify transaction data signatures that were created by a user in the past and verify the transaction content along with the time the transaction took place.

The verification of a signature that was performed by a Safewalk user in the past can be done by a help-desk personnel inside the Safewalk management console, similar to what is shown below:



4. Customization possibilities

- The length of transaction data that needs to be entered into the Mobile app by the user for signature can be configured or customized on request
- The Mobile apps can be rebranded on request

5. Technical note

A Transaction Data Signature (TDS) or Challenge-Response is an algorithm for generating a dynamic code that is based on a challenge that is given as an input for the user (in this case is the transaction data asked to be entered by the bank) to enter on its Authenticator device (e.g. a mobile app).

When the dynamic input to the code generation function is a random string (with no special meaning) this method is called challenge-response.

If the dynamic input has a meaning (for example, an amount and account number) the resulting code can be used to verify the user and to get the user approval for the said input – in this case (when the input has a meaning not random) the type of code is often referred to as transaction-data-signature (TDS).

6. Inputless TDS

Mobile TDS can be used using the Push method.

- The user access the portal with the push method by pressing accept when he receives the push message (challenge) for authentication to the Bank portal.
- For the transaction
    - User enter transaction data in the Bank portal and send it
    - User receive a push message on his Mobile device with the transaction information details and is asked to accept
    - If user press accept, the transaction data will be signed (using the user's private key) and sent over-the-air to the server for verification
- This version will not need any input from the user and be based on assimetric (public and private keys) authentication method including two-ways authentication as the server signs the challenge sent to the user Mobile app with his public key