SAFE-T

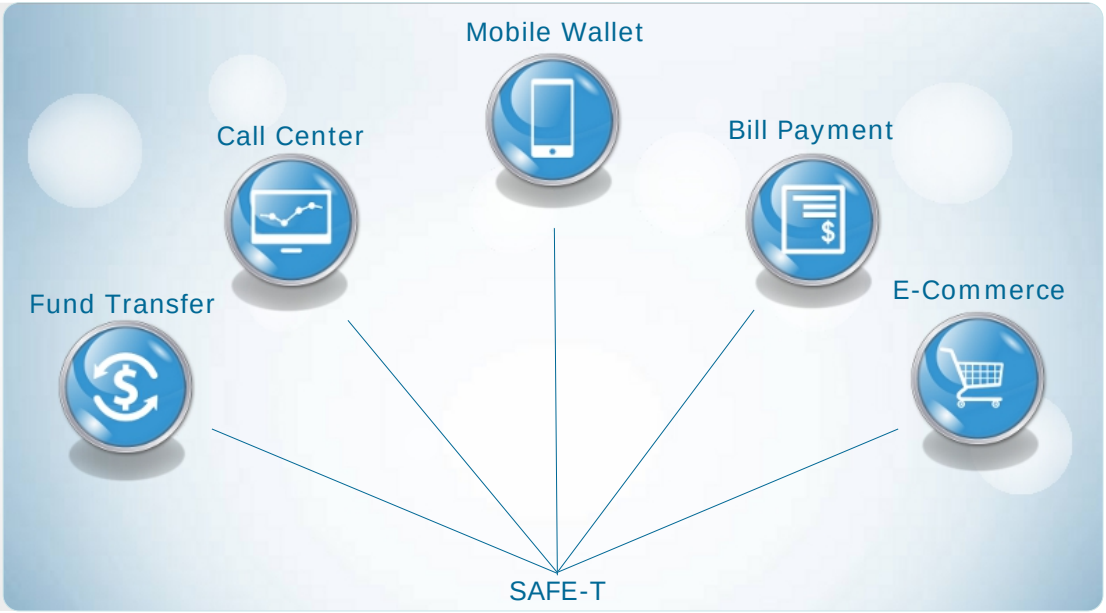
Strong Authentication for Electronic Transactions

Introduction

There is both opportunity and risk for banks in the digital age. The necessary shift in strategic focus from being providers of financial products and services to being solution providers requires sophisticated security applications.

To confront new and non-traditional threats, banks need to focus on:

- Protecting Electronic Data
- Financial Application Security
- Verification of the User Identity
- Verification of Transaction Data Origin



SAFE-T Use Cases

SAFE-T is an indispensible value proposition securing eBanking, ePayment and the expanding informal and impersonal world of eCommerce. It offers multiple use cases, guaranteeing customer authentication thus securing:

1. Service logins - websites, call-centers, mobile apps

2. eSignatures for higher value or critical data transactions

3. eContracts - enabling the useage of variable data parameters to secure user authentication apllicable in various electronic agreements

SAFE-T New Trust Relation

Knowing that the security of financial transactions relies primarily on the robustness of customer authentication and device identification, BGS' SAFE-T puts a strong focus on these security elements. The underlying objectives were:

- Ease of implementation - critical emphasis on ensuring the least intrusive implementation scenario
- No additional HW requirements (readers, dongles) to achieve security levels
- Ease of use - Biometric and/or Pin authentication
- Independent and autonomous authentication processs
- Data/ID Protection - no requirement to save critical or personal data
- Speed - instantaneous process using push notification

Security Concept

The combination of proven industry standards guarantees maximum levels of protection. A multilayer encryption methodology protects the phone and user from threats such as fraud-after-theft, hacking, malware, man-in-the-middle, and all known SSL weaknesses. All solution and data relevant components are processed within the secure crypto-container of the mobile phone - such as iOS "Keychain", or Android "Keystore System" protected at OS hardware and software levels.

The solution consists of an SDK that is implemented on the phone within an app, and our Enrolment and Authentication Host, which generates and encrypts keys via a Hardware Security Module (HSM) thus ensuring the protection of any sensitive data.

Privacy by Design

Strong Customer Authentication is a process based on the use of two or more of the following components categorized as knowledge, ownership and inherence.

- something only the user knows (e.g. a static password, code or personal identification number)
- something only the user possesses (e.g. a token, smart card or mobile device)
- something the user is (e.g. a biometric characteristic, such as a fingerprint)

(Recommendations for the security of mobile payments; European Central Bank 2013)

Device Binding

The ability to assert the trustworthiness of a device is vital for addressing mobile transaction security concerns. Binding a customer account to a mobile device is the first element of the SAFE-T security concept. To establish a firm link, SAFE-T ties the customer's phone number, to hardware specific attributes of the mobile phone used in the registration process. This link is unbreakable.

To activate SAFE-T on the phone after the download of the application, the customer simply inserts his PAN or account number, which is matched with the customer's account registration data. The SAFE-T host server generates the activation code, which is sent by SMS to the phone number specified by the customer in the primary identification at the bank branch. This phone becomes the so called “Trusted Device”.

Customer Verification

The user defines his personal PIN and activates biometric data recognition (fingerprint, face, voice recognition) for secure user identification and transaction authorization. A crucial element in the security concept of SAFE-T is, that PIN and biometric data are created offline on the mobile phone itself. They are not stored on the host server, or on the customer's phone. They are factors only known and inherent to the customer - Nobody else!

The availability of both elements, the PIN - something only the user knows - and the biometric data - something the user is - for customer identification ensures highest flexibility for the bank to define any combination of elements (2F, 3F), as per its risk assessment procedures. RSA Keys are used to establish a secure channel between the SAFE-T Host and the application on the phone.

Unique User Profile

The activation code and the customer's credentials form part of the underlying securitization process of the key cryptograms used for personalization. Once the activation code is entered, and the personal identification criteria are set, the SAFE-T instance is fully personalized and a user profile is created on the host and downloaded through secure data transfer to the mobile phone.

SAFE-T relies on a security concept based on the combination of unique factors to process transcations securely. Transactions are processed via the secure communication chain provided by the unique instance link between a registerred device, the user profile and the SAFE-T host.

Application Use Case

1.

SAFE-T is intended to offer the most secure method of user authentication and transaction signing. The application design allows for user personalization and convenient transaction data entry. Alternatively, the SAFE-T application can be used to authenticate the user (login) or authorize (sign) transcations, being performed on other devices or in other environments.

2.

After the customer initiates the authorization process, the authentication method is automatically invoked in accordance with the security level the bank has set for the specific transaction type.

The inherent versatility of the underlying methodology offers the possibility to include transaction specific information in the computation of the authentication cryptogram. This provides for even greater security and flexibility to the respective stakeholders.

The user may be required to enter or confirm transaction specific information such as value or currency as part of the authentication for specific types of transactions e.g. government related payments. Depending on the transaction securitization level, the bank may prompt the customer to sign by using PIN, or biometric authentication or if deemed necessary with a combination of both.

4.

After entering the required authentication information, the verification is processed in the background. The SAFE-T application retrieves the master key from the crypto-container on the phone and calculates the transaction token. This transaction token is returned back to the SAFE-T host for verification.

5.

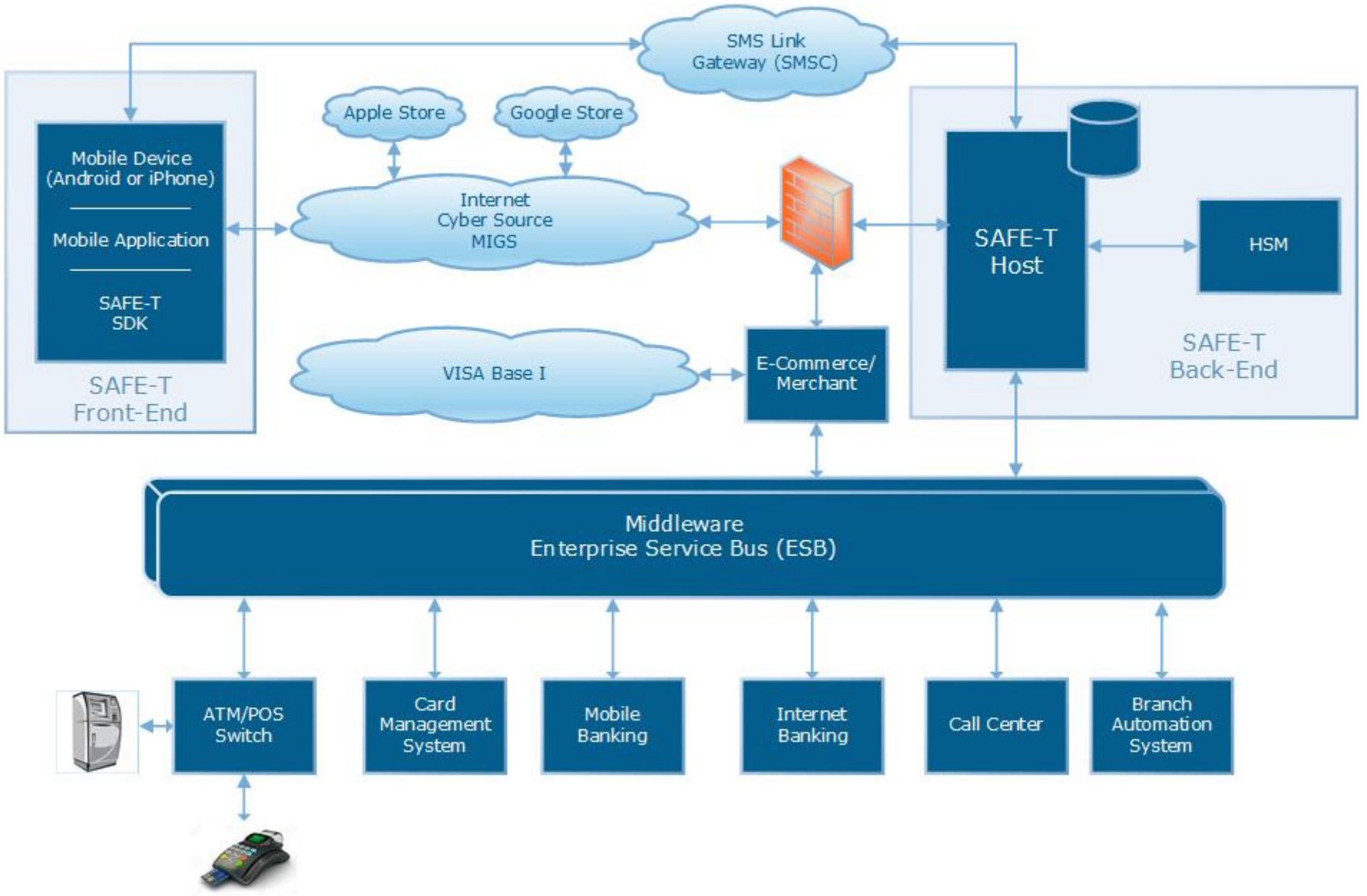
The SAFE-T host verifies the token and returns the authentication result to the bank host. The validated transaction is processed and confirmed to the customer without the need to enter an OTP or other confirmation code.

Process Flow Diagram

1. Customer initiates transaction in respective environment
2. Application requests Bank host to execute the operation
3. Bank host requests transaction verification from SAFE-T host
4. SAFE-T host sends encrypted transaction details to the phone's crypto-container
5. SAFE-T application prompts customer for PIN or biometric authentication
6. SAFE-T application retrieves master key and calculates transaction token
7. The transaction token is returned back to SAFE-T host for verification
8. SAFE-T host verifies the token and returns authentication result to the host

BGS Smartcard Systems

System Architecture



BGS Smartcard Systems

Business Cases

Secure Service Login

Anytime a user attempts to login to a secure online environment such as the eBanking website the final authentication can be performed using the SAFE-T application. There are two key environments for service logins to take place:

- within the mobile device – the user attempts to login into the mobile banking app resident on the mobile phone. In order to complete the login the user either enters the correct PIN and/or uses biometric data (voice, face or finger)

- outside of the mobile device – attempting to login into a website from any PC the user enters his regular access data within the website as usual. Before final access is granted the webservice host requests the SAFE-T host to authenticate the user. In order to do so, the SAFE-T host sends an authentication request to the respective registered secure device (mobile phone). As soon as the user provides the correct PIN/Biometric data the SAFE-T host can validate the response and provide such to the webservice host.

Authenticating ATM transactions – Cardless Cash Withdrawals

A possible business case asks for ATM withdrawals without the use of a plastic card. This could be useful in providing a salary distribution scheme for unbanked segments of the population. An employer could provide the bank with his salary list of his employees. A SAFE-T registered employee could then enter credentials provided by the host and finally authenticate him/herself at the time of the transaction.

SAFE-T

The SAFE-T application always preforms the same technological process designed using latest security concepts to securely authenticate a user. This authentication can be utilized for two key processes – validating and thus ensuring a secure:

- authentication of the user
- authorization by the user

This key underlying concept is then applicable in a variety of different scenarios representing the numerous business cases that the application can be used for. SAFE-T can simply be introduced at any point within existing processes at which the secure authentication of the user is essential to ensure absolute security.

SAFE-T USPs vs. common market solutions:

- additional secure communication channel established between host and device within SSL/TLS link

- secret keys are protected by user passcode which is not stored on the device

- the authentication token is generated by the mobile device and validated at the host

- SAFE-T applies a multi-layer security concept

eCommerce Payment Authorization

The SAFE-T application can be utilized to provide the strongest authentication of a customer in the case of an underlying eCommerce payment transaction. Current solutions such as verified by VISA, MasterCard Secure Code and static or dynamic OTP (One time passwords) cannot absolutely exclude the possibility of fraudulent misuse. At the time of checkout from the respective webshop the user proceeds as per normal and confirms the transaction with the final purchase click. At this time the credit or debit card data is routed to the issuer host using the international network. Prior to final authorization the card management system would request the SAFE-T host for a user authentication and thus authorization. Only once the user is validated by the SAFE-T the card management system is provided with the ok to proceed and authorize the underlying payment card transaction within the network.

eSignature – Authorizing Underlying Transactions/Processes

Online Funds Transfer - In the case of a user processing an account to account transfer, for example to pay for an invoice, the system could be set-up to request an authorization for the transaction via the SAFE-T host. This could be an additional step required to process a transaction even if the user has securely accessed the eBanking environment.

Online ‘signature’ (validation) of a data transfer – It might be required to ensure the authenticity of the user in the process of the person submitting documents or information electronically. In this case the user would be requested to authenticate the respective data transaction/submission using the SAFE-T application.

Summary

SAFE-T can be applied in a wide array of scenarios to increase the security levels of financial services. Be it the basic step of user-authentication for service logins or the more critical and higher risk scenarios associated with high value transactions. SAFE-T can and should be seen as an indispensible omni channel value proposition for eBanking, Call Centers, ATM or POS Transactions, eTrading, ePayments and the expanding informal and impersonal world of eCommerce.

BGS understands that the war on crime through cryptography is an ever-evolving one, which is why a clear and continuous roadmap on innovation plays an important role in our R&D. Due to long standing experience and network with the best security experts in the field, our customers can be assured to always remain at the cutting edge of mobile and cyber protection trends. Speed and time to market are essential in the mobile world, which is why we place great value on developing solutions that adapt to a client's infrastructure, rather than the other way around.

For ease of integration, our solution is available as an SDK that provides APIs for quick and seamless implementation in any new or existing mobile solution. The security mechanisms of our solution mostly run transparently in the background in order to minimize the impact on the user experience of the app.

BGS Smartcard Systems Offices:

Austria:
Heiligenstaedter Strasse 32/202, 1190 Vienna
Phone: +43 676 328 7722
e-mail: info@bgssmartcard.com

Russia:
Bld. 16, 11/10, Letnikovskaya str., Moscow, Russia, 115114
Phone: +7 495 669 23 63
e-mail: info@bgs.ru

Functional Requirements	Technical Solution
- Easy Implementation	- The SAFE-T solution is available as an SDK that provides APIs for quick and seamless implementation in any new or existing solution
- No additional devices for authentication - No OTP received by SMS	- Authentication data is generated by the user on the mobile phone in the SAFE-T application - The customer can use a PIN, which is only known to him, or biometric authentication (Fingerprint, Facial, Voice Recognition) for authentication
- Need for secure authentication mechanism - Strong Authentication	- PIN authentication with randomized secure PIN pad and protected screenforms - Transaction type dependant securitization by combination of authentication methods (PIN, biometric in combination with transaction related information)
- Secure Data Storage/Encryption - Secure Channels	- Any sensitive data (keys, registration details) are kept in a secured crypto container of the mobile device, protected by OS level security. Secret keys are encrypted by the PIN only known to the customer, or his biometric data. Neither PIN, nor biometric characteristics are stored in any component of our solution. The SAFE-T host generates and encrypts via a Hardware Security Module (HSM) - Authentication data is transmitted encrypted with session keys. The SAFE-T application connects to the Bank using TLS connection with SSL pinning. Session keys are generated by the SAFE-T application and the SAFE-T host by common secret (Master Key) to prevent man-in-the-middle attacks
- Advanced Obfuscation - Brute Force - Man-in-the-browser	- The SAFE-T application is obfuscated to prevent reverse-engineering. It generates and encrypts via a Hardware Security Module (HSM) - PIN correctness is checked at the SAFE-T host - URL of the SAFE-T host is hardcoded in the obfuscated SAFE-T application

BGS Smartcard Systems