BGS Smartcard Systems

SAFE-T

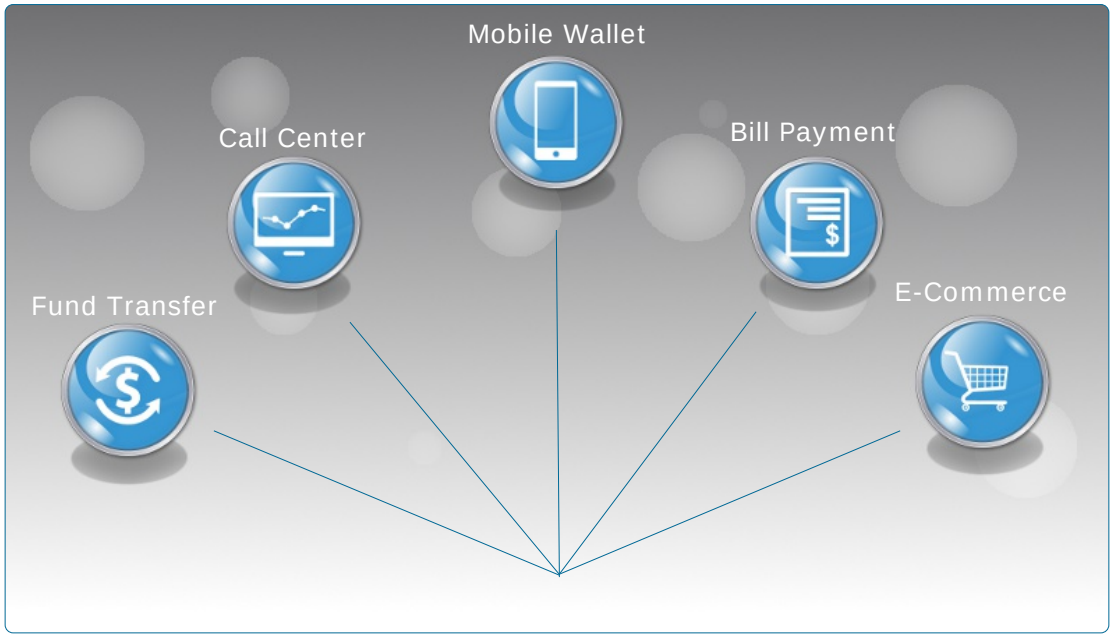
Strong Authentication for Electronic Transactions

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:

- financial application security
- protecting payment data
- 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

2. eSignatures for higher value or critical data transactions

3. Multiple transaction types by applying variable en-cryption parameters (currency, value, ID) to strengthen cryptographic tokens reflecting varying security levels

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/ personal data
- Speed - instantaneous process using push notification

Security Concept

The combination of proven industry standards, such as EMV and BGS' own technology guarantees maximum levels of protection. Our multilayer encryption methodology protects the phone and the user from all threats such as fraud-after-theft, hacking, malware, man-in-the-middle, and all known SSL weaknesses.

All solution and thus 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 application 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 (2 factor, 3 factor), as per its risk assessment procedures. RSA Keys are used to establish a secure channel between the CVS Host and the application on the phone during the initial activation process and for transaction processing.

Card Emulation

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 card profile – a virtual equivalent of the customer’s physical card - is created on the host and downloaded through secure data transfer to the mobile phone.

SAFE-T relies on proven EMV methodology, which invokes algorithms and methods to process secure transactions based on a “call and response” methodology that communicates with the card securely emulated in the unbreakable crypto-container of the phone.

Application Use Case

Transaction type dependant - Bank can define different transaction securitization levels

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.

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.

3.

The user might be required to enter transaction specific information such as value or currency as part of the authentication process. This could be a pre-requisite setting for specific types of transactions e.g. government related payments. Depending on the defined 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 SAFE-T host for verification.

5.

The SAFE-T host verifies the token and returns the authentication result to the bank host. When validated the 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 crypto-container on the phone
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 bank host

BGS Smartcard Systems

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 value proposition for eBanking, 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 64
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 - For authentication the customer uses PIN, which is only known to him, or biometric authentication (Fingerprint, Facial, Voice Recognition)
- 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	- All 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 SAFE-T application and 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