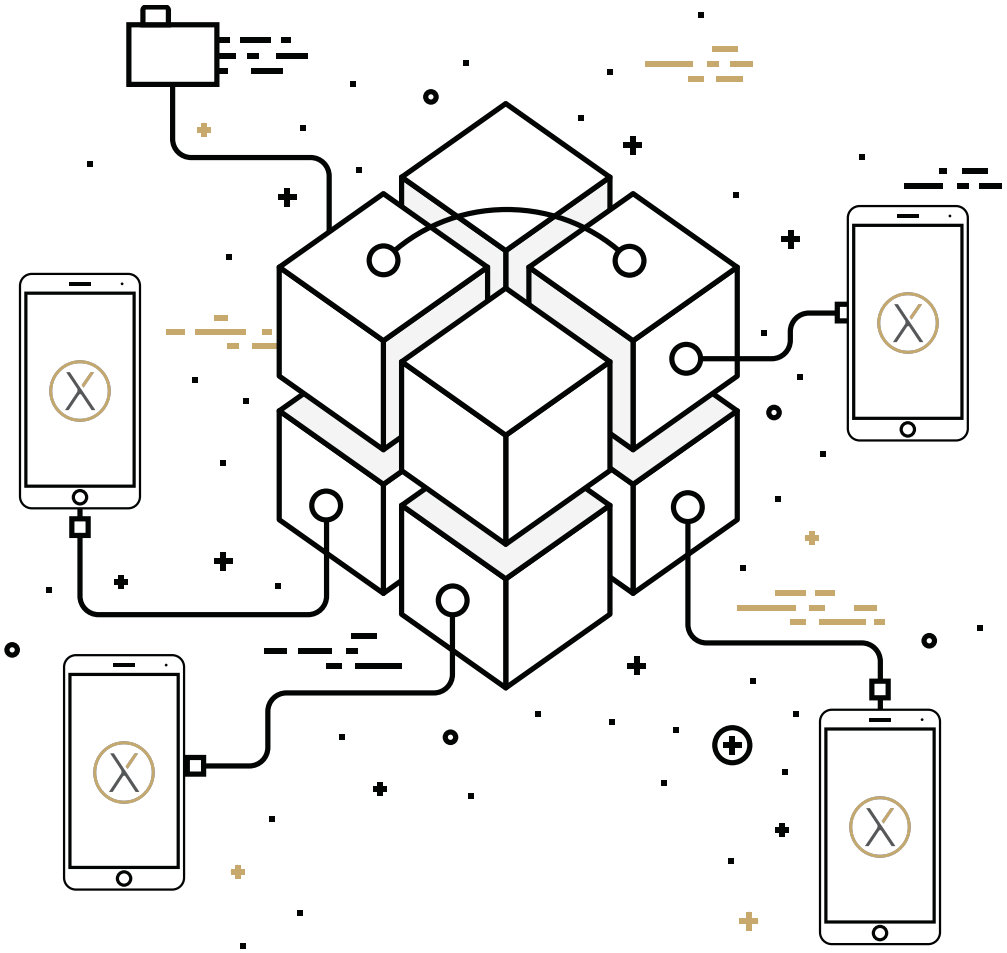
APPLICATION SECURITY OVERVIEW



This document provides an explanation of the technical and policy based measures SmartFinance has taken to ensure maximum security for the XOBI software ecosystem. For more information or concerns please contact us at feedback@XOBI.com.

Privacy of Client Banking Data

The XOBI application allows users to view their aggregated financial data across their existing bank accounts as well as to amend and attach personal notes, images, tags and rankings for improved personal organization. XOBI is, at present, a "read only" application that cannot facilitate money movements of any type either though account transfers, bill pay, credit card payments or P2P. Users can delete their accounts which will immediately and irrevocably remove all of their financial data along with any stored images, notes, tags and rankings. No personal information is left in the SmartFinance ecosystem.

To aid our merchant resolution efforts, we do extract merchant related fields and store them for offline analysis. These fields are limited in number and encompass the original bank record and any address information such as street, city, state, country, postal code, url and telephone # of the merchant. They do not include transaction dates or prices nor do they include any user identification fields. These merchant related fields are the sole exception of data that will persist with SmartFinance in the case of an account deletion and we use this data solely for the purpose of improving our merchant resolution product.

Technical Security

The protection of client data from unwarranted access is a fundamental responsibility that we take very seriously. Traditionally the problem of data protection is addressed by levels and methods of encryption that are appropriate to the perceived risk and whether the data is at rest or being moved. From a technical security perspective, there are several areas for consideration:

A. Protecting communications from the smartphone to XOBI servers
B. Protecting data on the physical mobile device
C. Protecting data between backend applications
D. Protection of any persisted data in the backend
E. XOBI username and password protection
F. Authenticating with 3rd party financial institutions
G. Transmission of records with 3rd party financial institutions
H. User and account deletion

Other Topics:

I. Exception monitoring and alerting
J. Employment background checks

A) Protecting communications from the SmartPhone to XOBI servers

All data that is transmitted between the device and XOBI web-servers is through an SSL/TLS connection with a certificate created with a SHA256 RSA signature. At initial startup the device generates an RSA-256 public/private key pair and sends the public key to the web-server after the secure connection is established. The XOBI backend then generates an AES 128-bit session key and encrypts it with the public key and sends that back to the device. This AES key is now used to further encrypt all other communication thus ensuring a double encryption of all messages. This is important to protect against SSL man-in-the-middle attacks. Only after this process is fully complete are usernames, passwords or any other sensitive data such as personal transactions or images transmitted. In summary, all personal data is encrypted twice before being passed through the public internet.

B) Protecting Data on the Physical Mobile Device

We do not create any log files or use any disk caching technology that could leave a user's data open available for capture. The on-device application stores only the minimum data necessary for identification and managing keys necessary for secure connections. This includes username, a private RSA key for double encryption and a XOBI generated 128 bit secure GUID identifying the device. This data is persisted and managed by the industry standard key chain facilitated by the IOS. All session based information, including the secure 128-bit session GUID resides only in the applications private memory space.

C) Protecting Data between Backend Applications

The backend is broken into 3 tiers with stricter security at each tier.

The 1st tier is the perimeter security tier. It is a perimeter web service layer, which does not store any information and provides a conduit between the external apps and the 2nd tier. The transitive nature of the 1st tier alerts us to a potential issue, but does not compromise the security of the data.

The 2nd tier is the "business logic" tier. It only stores sensitive information temporarily in memory, and is not accessible from the public internet. It can only be accessed from the 1st and 3rd tiers. The 2nd tier is known as a De-Militarized Zone.

The 3rd tier is the "persistence" tier. It is accessible only from the 2nd tier, meaning any intrusion attempting to access this tier would need to penetrate the 1st tier and 2nd tier.

Intra-server communication is secure at every step and requires precomputed access keys, which are only accessible on a dedicated key server that authenticates via a closely controlled and monitored white list. These keys are never stored on local disk.

GUIDS are leveraged to uniquely identify and access transactions, user information and active sessions. GUIDs are generated using a combination of machine, temporal and hardware specific factors, all passed through an MD5 algorithm. The result is shuffled in a separate process to further eliminate any change of pattern.

D) Protection of any Persisted Data in the Backend

Sensitive data is AES encrypted via keys from the key server and then stored on encrypted drives. All physical data storage is doubly encrypted using a separate key for each of the two encryption stages. Flow diagram:

Tier 2 Encrypts data using a key available only to Tier 2 > Transport layer securely transmits to Tier 3 > Tier 3 encrypts data using a key only available to Tier 3 > Data is associated with a secure 128 bit GUID and Stored in database housed on encrypted drive > GUID is returned to Tier 2 for future retrieval.

This means that two different keys from different sources are required to decrypt data. Only the double encrypted data is archived, which means both keys are required to unlock and use data. All Log statements produced have any sensitive information redacted before being written to disk.

Passwords for databases are not stored locally. There are also accessed via the tightly controlled key server. Passwords are machine generated 40 char sequences using an MD5 algorithm.

E) XOBI Username and Password protection

When a user account is created the password is tested for meeting a minimum strength requirement. The user password is then immediately hashed using state-of-the-art scripting methods and then the password is discarded. Scripting prevents against brute force attacks used to reverse engineer access keys. Your XOBI password can never be retrieved, even by SmartFinance, because it's never stored. XOBI servers employ session timeouts to further protect your account and have automated detection of continuous bad password and unusual login attempts. Attempts by a "robot" would result in a phased set of account lockouts with progressively longer timeout periods until the account is fully "locked down." A locked down account can only be unlocked via supervisory controls. Changing passwords, emails or any other security-sensitive information is audited and notifications are sent to the user immediately via the last known confirmed email address.

F) Authenticating with 3rd party financial institutions

When a user enters their online banking credentials (username and password) SmartFinance temporarily uses those credentials only once to establish a secure end-to-end link between the XOBI application running on the personal device and the user's online account. On that initial secure handshake, a secure 128 bit GUID is agreed upon at which point the username and password are immediately discarded. After that, the issued GUID is used for all further communication and account identification.

G) Transmission of records with 3rd party financial institutions

Transmission of data to your financial institutions is strictly governed using multiple systems managed by a dedicated aggregation service. Traffic to said services API uses only the strongest TLS protocols and ciphers and all private data exchanged with banks is transmitted securely over TLS. Within the aggregation service, database and decryption servers are unable to access or be accessed through the internet and can only communicate with specific instances in our private network and server-to-server traffic utilizes asymmetric encryption. Cryptographically hashed headers and timestamps are utilized to ensure message authenticity. All access to the decryption servers is logged, and requests are made through TLS with additional HMAC authentication.

H) User and Account Deletion

Should a user delete there XOBI account all data is "hard deleted" meaning that all records are physically deleted from the database and persistence level. This is in contrast to a soft delete where data is simply "marked" as deleted.

I) Exception Monitoring and Alerting

SmartFinance has deployed a dedicated audit system, which captures machine level, application level and specific user actions across the entire ecosystem. This information is then aggregated and continuously evaluated by machines and humans for anomalies and potential unwanted intrusions. All processes and network connectivity including database access, remote session access is captured and audited. In the case of a significant breach a single "kill switch" can be activated to swiftly and automatically prevent further access by shutting down applications at all 3 tiers.

J) Employment Background Checks

All employees are subject to background checks without exception.

K) Annual Security Penetration Test

VERACODE

November, 2015 Successfully completed without issue.
http://www.veracode.com