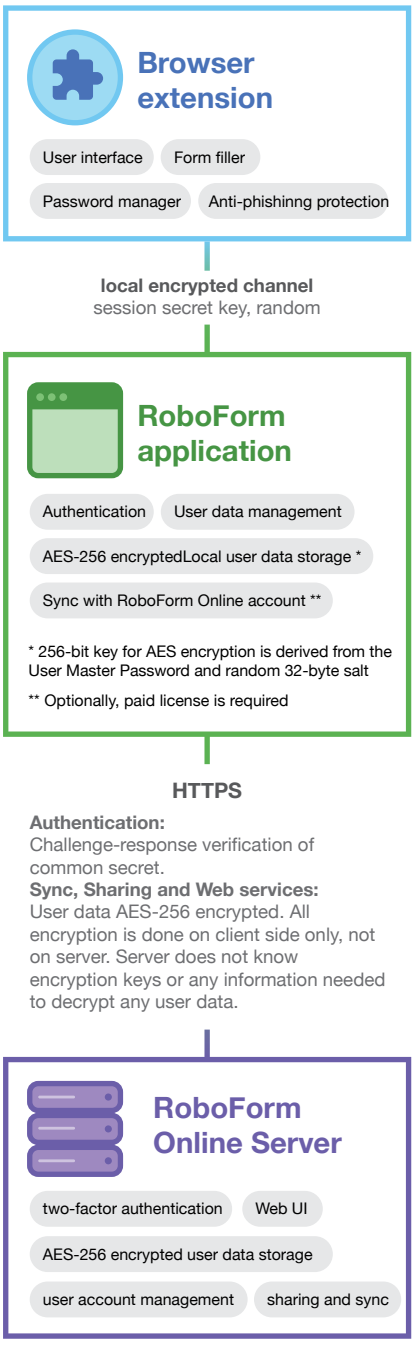
RoboForm

Security Overview Whitepaper

Table of contents

Product Description



Components of RoboForm application and online storage

RoboForm is a password management system that consists of several elements:

- Computer, mobile device or browser based **RoboForm Clients** and
- Central server called **RoboForm Server** that provides licensing, synchronization, storage, administration interface for business users, distribution of RoboForm policies, and form-filling and password management capability though a web-based client.RoboForm user data may contain one or more of the following RoboForm Data Object types:

Logins
for websites and applications

Identities

SafeNotes
plain text files

Bookmarks

Contacts

RoboForm protects user data on user devices, in transit, and on the server. RoboForm uses symmetrical cryptography to protect user data. All RoboForm data items are packed into a single file encrypted with AES-256 algorithm. RoboForm uses a concept of a human-readable Master Password that a user can set, and that is used by RoboForm to generate an AES-256 key for data encryption and decryption.

RoboForm data security depends on the complexity of the user's Master Password. RoboForm enforces minimal complexity of Master Passwords by not allowing users to pick a Master Password that does not meet these minimal requirements. The minimal Master Password requirements are 8 characters long with at least 4 non-numerical characters.

In the RoboForm for Business version, these requirements can be increased (not decreased) by the company admin to include additional conditions. In the Business version, these requirements will be enforced through policies that propagate to the user's clients automatically from the RoboForm Server.

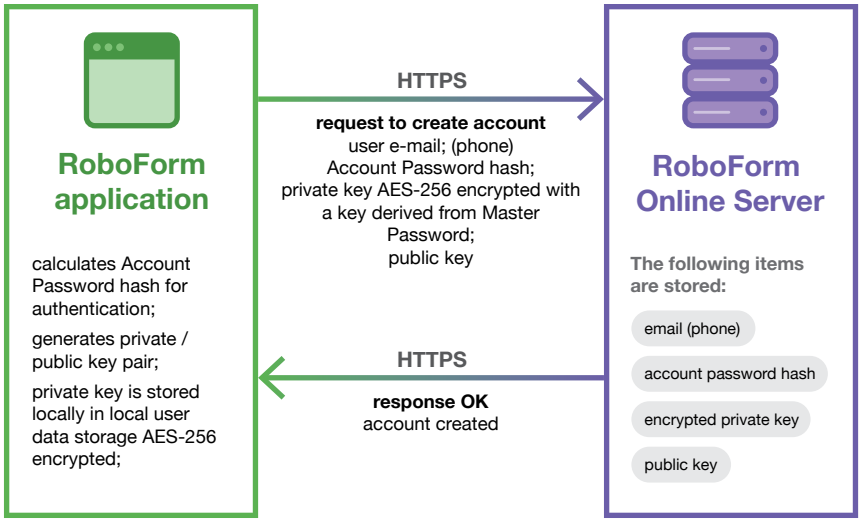
Account Creation and Master Password Generation

All encryption/decryption operations are only performed by RoboForm locally on user's devices and never on the RoboForm Server. RoboForm Data Objects and other user data is never sent to the Server in an unencrypted form. All communication between RoboForm Clients and Server are conducted over encrypted channels only.

When a new user is about to create an account, RoboForm prompts that new user to create his/her Master Password. This is the only password that the user will be required to remember to access all of his/her RoboForm Data Objects locally or online.

RoboForm uses two distinctly different one-way cryptographic functions to generate the symmetrical key for local data encryption/decryption and server-side password. Both algorithms use two different randomly created user-specific "salts".

Generation of AES encryption keys uses PBKDF2 (Password-Based Key Derivation Function 2) algorithm with SHA-256 hash function and long random salt (32-byte). PBKDF2 is an iterative algorithm with a sufficiently large number of iterations (4,000 by default).



Registration

A higher number of iterations provides greater protection against brute force and dictionary attacks by not only slowing them down, but also by making RoboForm Clients proportionally slower, especially on slow devices (Android, iOS) or applications (RoboForm Online web site). Intentionally making a slow algorithm is an accepted practice targeted at preventing dictionary attacks against compromised authentication stores.

This technique is called "key strengthening" or "key stretching". We recommend increasing the length of the Master Password instead of increasing the number of iterations as, according to some researchers, the addition of two characters to the length of the password is roughly equivalent to multiplying the number of

iterations by 1,000 yet it does not slow down the algorithm.

A combination of 10,000 iterations and a 7-letter password is already insecure and it can be brute-forced relatively quickly, as demonstrated some time ago on one of RoboForm's competitor products.

Only the password hash derived from Master Password is shared with the RoboForm Server. It is computationally infeasible to recover the user's Master Password or the AES-256 key from that password hash due to the one-way nature of the algorithm used to generate it.

RoboForm Servers

The Master Password is used for two distinct purposes: to create a cryptographic key that encrypts and decrypts the user's RoboForm data and to authenticate the user to the RoboForm Server (either online or through the local instance of a RoboForm Client for synchronization).

The RoboForm Client periodically connects to the RoboForm Server to perform a set of tasks that are collectively known as synchronization. Synchronization action is always initiated by a RoboForm Client.

Synchronization between RoboForm Client and Server

Synchronization is performed:

- Periodically once an hour.
- On Master Password entry on the RoboForm Client side by the user.
- On change of the user data on the RoboForm Client.
- On RoboForm Data Objects sharing or sending action performed by the local user on RoboForm Client.
- Manually through RoboForm Client graphical user interface.

User Authentication During Synchronization and Web Access

User synchronization is only available when the user successfully enters the Master Password on a local device. The Master Password is verified by successfully decrypting local data storage using the AES-256 key derived from it. When accessing an online account on the RoboForm Server, the Server checks the Master Password using special a challenge-response algorithm by sending only hash codes irreversibly derived from the Master Password and randomly generated numbers.

The Server also monitors both successful and rejected authentication attempts in order to prevent user ID probing and password guessing by limiting the request processing rate and temporarily blocking access from suspected client IPs and to attacked user accounts. RoboForm Server uses a combination of source IP and account blocking to slow down brute force and DoS attacks.

Licensing

One of the essential functions of the RoboForm Server is to provide licensing information to the RoboForm Clients. During each synchronization, the RoboForm Client requests the RoboForm Server to provide licensing information.

RoboForm Data Sharing

Both Consumer (Everywhere) and Business users have an option to share RoboForm Data Objects (including Logins) with other users. Sharing is a process by which one RoboForm user can make one or more of their RoboForm Data Objects available to another one or more RoboForm users. There are three types of sharing: “data sending,” “folder sending,” and “group sharing.” All three sharing types use a very similar delivery mechanism, but different sharing concepts which are described below.

Data Sending (Free, Everywhere, Business)

All users, free and paid, have an option to “send” one of their RoboForm Data Objects to another RoboForm user. When a RoboForm Data Object is sent, a copy of it is delivered though a cryptographic protocol to the receiver’s encrypted RoboForm data storage. Once the object is sent, the sender no longer has any control over it (e.g. access to that object cannot be revoked or changes made to that object on the sender’s side cannot be automatically propagated).

Folder Sending (Everywhere, Business)

Paid users are allowed to share one folder with other RoboForm users. When a sender chooses to share a folder with the receiver, the receiver is notified. After receiving the notification, the receiver has an option to reject or to accept the request and receive a local copy of that shared folder through a cryptographic protocol.

A shared folder can contain an unlimited number of RoboForm Data Objects. A sender can add up to 5 recipients and specify different permission levels for each one of them. These permissions will apply to each RoboForm Data Object within the shared folder.

These levels define permissions to perform operations on RoboForm Data Objects within that folder:

	Folder owner	Folder manager	Regular user	Limited user
Use	✓	✓	✓	✓
Read	✓	✓	✓	
Edit	✓	✓	✓	
Create	✓	✓		
Manage recievers and assign permition levels	✓			

The “**Use**” permission only allows the user to effectively use a RoboForm Data Object with the maximum possible restrictions. “Use” permission allows the user to:

- Login: use the login to automatically log in to an application (Windows) or a website.

- Identity: fill forms with information from Identity.
- Contact: fill forms with information from Contact.
- Bookmark: open a web page defined in the Bookmark.
- SafeNote: same as “Read,” view contents of a SafeNote.

By nature, “**Read**” permission is only different from “Use” permission for the Login RoboForm Data Objects. Without the “Read” permission, the Limited User cannot view the contents of the Login type RoboForm Data Object. Combined with the fact that most applications and websites mask the contents of the password field, this option provides an additional control to conceal passwords from the users.

The “**Edit**” permission allows the user to edit the content of all RoboForm Data Objects within the folder including adding, removing, or changing the content of fields within that RoboForm Data Object.

The “**Create**” permission allows the user to create and delete RoboForm Data Objects in the folder.

The simple addition of a Login or another RoboForm Data Object will automatically make it available to all folder receivers. Any changes to any Login or any other RoboForm Data Object is automatically propagated to all folder receivers during the synchronization process. Only the sender (the owner of the folder) and the folder manager are allowed to add or remove users, and to change user permission.

Group Sharing (Business)

RoboForm for Business users may be allowed to use both “sending” and “folder sharing” functions if the company admin allows them to do so in the RoboForm Policies.

RoboForm for Business offers “Group Sharing” as an additional method of sharing logins and other RoboForm Data Objects specifically designed for company use. A RoboForm Group is an object that provides a logical connection between an unrestricted number of RoboForm users and an unrestricted number of RoboForm Data Objects.

Company Admins can create an unrestricted number of RoboForm Groups. Company Admins can assign an individual permission level to each individual RoboForm user within a RoboForm Group.

These levels define permissions to perform operations on RoboForm Data Objects within that group:

- **Company Admin** can create RoboForm Groups, perform all operations on RoboForm Users and RoboForm Data Objects within a group.
- **Group Managers** (assigned by the Admin or another Group Manager of that particular group) can perform all operations on RoboForm Users and RoboForm Data Objects within a group.
- **Regular Users** can use, read, and edit RoboForm Data Objects.
- **Limited Users** can only use RoboForm Data Objects.

The “Use” permission only allows the RoboForm user to effectively use a RoboForm Data Object with the maximum possible restrictions. “Use” permission allows the user to:

Login: use the login to automatically log in to an application (Windows) or a website

- **Identity**: fill forms with information from an Identity
- **Contact**: fill forms with information from a Contact
- **Bookmark**: open a web page defined in the Bookmark
- **SafeNote**: same as “Read,” view contents of a SafeNote

By nature, “Read” permission is only different from “Use” permission for the Login type RoboForm Data Objects. Without the “Read” permission, the Limited User cannot view the contents of the Login type RoboForm Data Object. Combined with the fact that most applications and websites mask the contents of the password field, this option provides a limited yet effective additional control to conceal passwords from the users.

The “Edit” permission allows the RoboForm User to edit the content of all RoboForm Data Objects within the RoboForm Group including adding, removing, or changing the content of fields within that RoboForm Data Object.

The “Create” permission allows the user to create and delete RoboForm Data Objects within the RoboForm Group.

Simple addition of a Login or another RoboForm Data Object will automatically make it available to all RoboForm Group members. Any changes to any Login or any other RoboForm Data Object is automatically propagated to all RoboForm Group members during the synchronization process.

RoboForm Data Management Categories

RoboForm Data Objects are either managed by the users or are shared with the users and managed by the sender (another RoboForm user or a company). All RoboForm Data Objects created by the user are managed by the same user. All RoboForm Data Objects that were shared with the user with the send function, are managed by the user who is the recipient (sender retains and manages his/her own copy). In this scenario, RoboForm creates a local copy of the sent object in the user’s data repository (One File) and encrypts it with user’s the Master Password.

All RoboForm Data Objects shared with the user with the Folder Sharing function by default are managed by the sender. The sender may designate the receiver to be a Folder Manager. In that case, the receiver will also be able to manage his/her data from the shared folder.

By default, all RoboForm Data Objects shared with the user with the Group Sharing (Business only) function are managed by the Company Admin or Group Manager. The Company Admin or Group Manager may designate the receiver to be a Group Manager. In that case, the receiver will also be able to manage his/her data from the shared group. All Company Admins can manage all RoboForm Data Objects in all shared RoboForm Groups.

Data Synchronization

Data synchronization is only allowed in the Everywhere and Business versions of RoboForm. It is not allowed in the Free version. A limited exception for Free users is the ability to send and receive RoboForm Data Objects via the send function and accept Emergency Access invitations.

Consumer (Everywhere Account type) and Business versions of RoboForm treat user data differently. In the Consumer (Everywhere Account type) version of RoboForm, a copy of the user-managed data is always kept on the device where the RoboForm Client is installed. The decision of whether to synchronize this data with the RoboForm Server and to keep a copy of that data on the Server is made by the user.

In the Business version of RoboForm, an encrypted copy of user-managed data is always kept on the device where the RoboForm Client is installed and by default on the company account hosted on the RoboForm Server.

Company Admin, using RoboForm Policies, can restrict RoboForm users from creating any RoboForm Data Objects (restriction can be enforced by RoboForm Data Object type) thus restricting the RoboForm users only to the RoboForm Data Objects assigned to him/her by the company via the RoboForm Group sharing feature.

RoboForm uses a combination of symmetric (AES-256 by default) and asymmetric aka public-key (RSA with key length is 2048 bits by default) cryptography to provide a cryptographically-secure way for users to share RoboForm Data Objects.

Cryptographic Protocol

When a user creates a RoboForm account, the local RoboForm on that device creates a public/private key pair for that user. The private key is stored in user's OneFile and is encrypted by the users' Master Password at all times. That private key is propagated to other devices that belong to the same user along with Logins, Safenotes, Identities, Bookmarks, Contacts, and other user data.

The user's public key is made accessible to the RoboForm Server. When the sender instructs RoboForm to send a RoboForm Data Object (one or more login, safe note, identity, bookmark, or contact) to the receiver or share a folder with the receiver, the following happens:

1. RoboForm on the sender's side (locally on the device) creates a Temporary Key (a unique randomly generated AES-256 key not known to the RoboForm Server).

2. RoboForm on the sender's side (locally on the device) requests from the server and receives public keys of all receivers.

3. RoboForm on the sender's side (locally on the device) encrypts the Temporary Key with each of the receivers' public key.

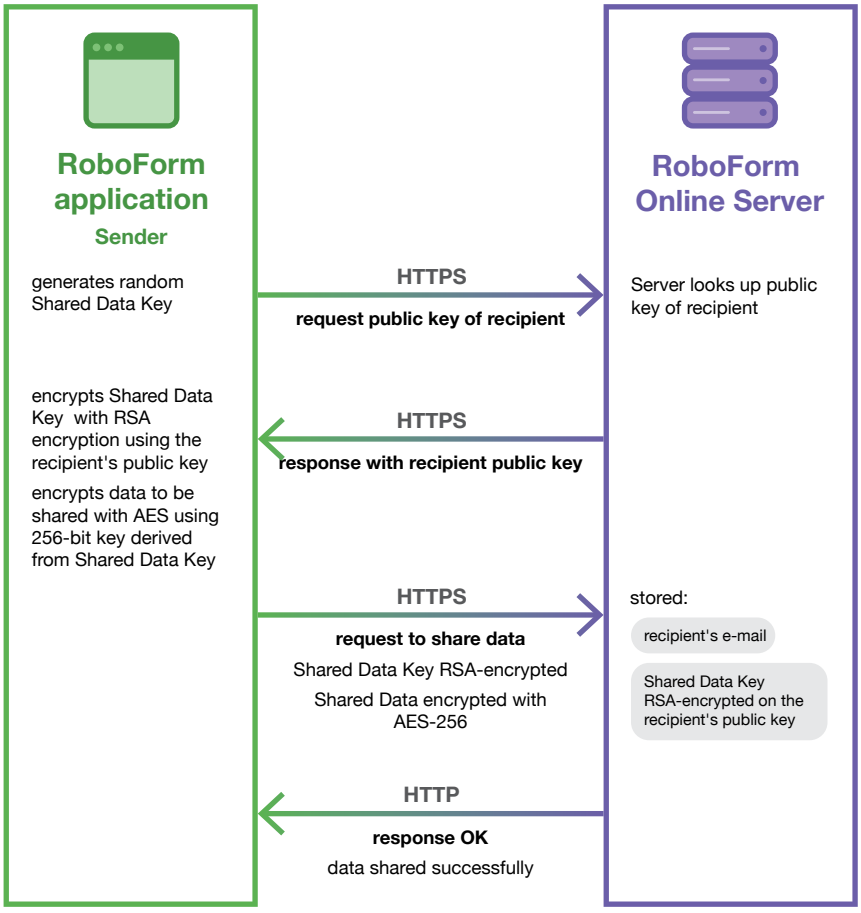
4. The receiver gets the Temporary Key (that was previously encrypted with receivers public key) and decrypts it (locally on the device) with own private key from the server through the automatic synchronization process.

5. RoboForm sends the Temporary Key encrypted with each of the receiver's public key along with the sent RoboForm Data Object to the Server; from where each corresponding receiver can automatically request it

via the synchronization process. RoboForm only uses encrypted channels to communicate between the RoboForm Server and RoboForm Clients. All data is sent in an encrypted form between the RoboForm Server and the RoboForm Clients.

6. Receiver gets the shared RoboForm Data Object and decrypts it (locally on the device) with the Temporary Key that was decrypted in the previous step and stores it locally encrypted under the receiver's Master Password.

7. Now the receiver is able to perform operations with the received RoboForm Data Object or Objects. RoboForm will only perform decryption operations locally on the receiver's device.



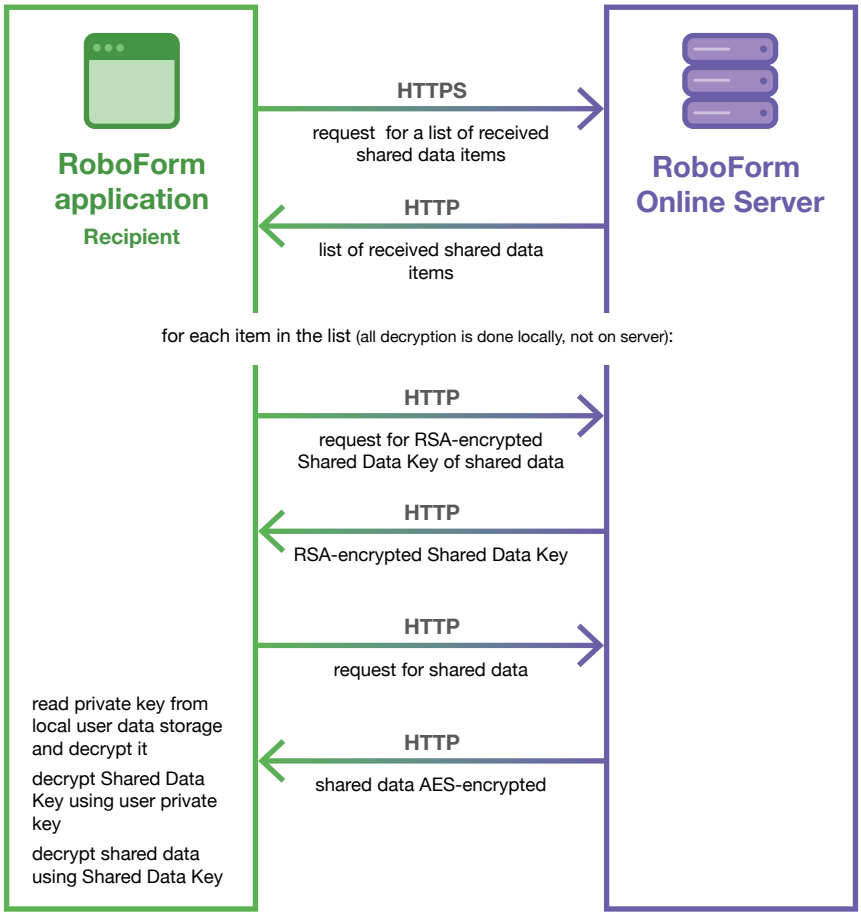
Sharing (part 1)

It is important to note that using that schema, only the receiver can decrypt his/her copy of the Temporary Key encrypted with his/her public key. That decrypted Temporary Key can be used to decrypt the shared data, and subsequently use the shared RoboForm Data Object (e.g., use the login to fill in credentials on a website). No one else can decrypt encrypted copies of the Temporary Key.

The only major difference in the way RoboForm deals with Groups is in the fact that a Group Key is created instead of a Temporary Key, and it is created at the time when that particular group is created. Using the Group Key, the Admin

performs all the operations the sender does in the description above using the Temporary Key.

The Admin's copy of the Group Key is kept encrypted with his/her public key. Only the Admin's actions can cause RoboForm (locally on the admin's device) to decrypt it and re-encrypt with public keys of other group members. If there are multiple Admins within a group, each Admin can use his or her personal encrypted copy of the Group Key to provide access to data to other group members.



Sharing (part 2)