Third Party Secure Key Communication

SAKUA2Random, produces around some 150 Million 108 character long random strings. This is just a test program, not perfect in anyway.

There are three parties involved.

- SAKUA2Random String generated site (The third party KeyServer)
- The End-User
- The Website or Service Provider the End-User wishes to work with.

The End-User installs an app from the random strings generator site (KeyServer), the app downloads 150Million+ 108 character long random strings. The random strings file content can change over time but the ID remains the same.

The 150Million+ 108 character long random strings file is then shuffled so as to generate around 8 Billion+ combinations or more for various other users.

Each user registers with a website and uses their username along with the random strings file ID. An Id is used to represent the random strings file.

The End-User accesses the site, Let's say Gmail.com (server). Gmail.com sends the string index along with a list of indices. These indices represent the offset of characters amongst the random strings (offsets amongst the 150Million+ strings). The values together in these indices represents the shared key. Which could optionally be mixed in with the password to create an even more secure shared key.

The End-User then sends his username and uses the encrypted key to create a secure connection. This would authenticate and authorize the user.

At the server-end which is Gmail in this case, it contacts SAKUA2Random Strings Site (KeyServer) sends the random strings file ID, string index and offsets and retrieves the shared key. Which is then used to decrypt the data from the End-User and send encrypted messages to the End-User.

The random strings file can be regenerated every week or so to improve the security.

5. The Website contacts the KeyServer with the random strings file id ,string index and offsets to get the encrypted key for secure communication.

1. End user registers with the KeyServer, obtains an app and gets the random strings file.

2. End user registers with a service provider like gmail.com with the random strings file ID.

3. When the end user tries to login, the server sends a random string index number and some offsets.

4. The end user uses his or her app, and inputs the string index, the offsets and his or her password to create an encrypted string. Which is then used for secure communication.