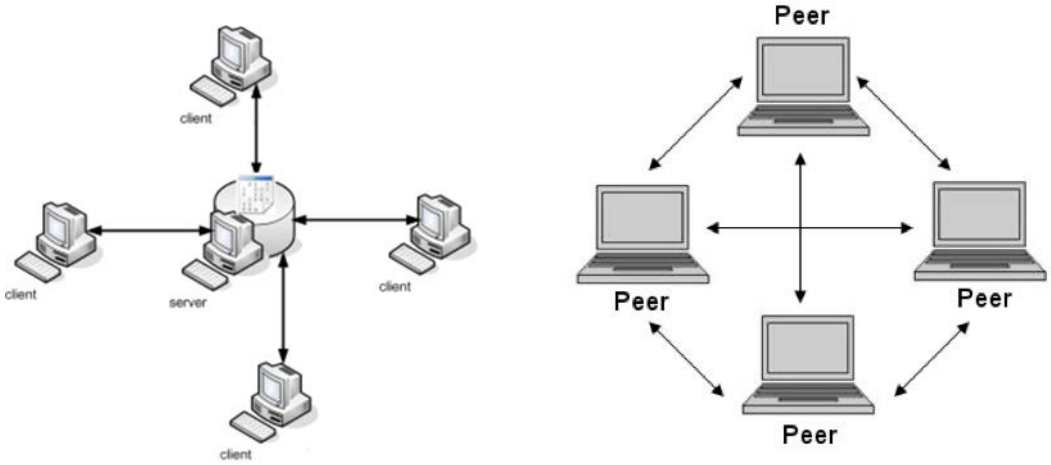
Private Messenger Security Overview

from

Secure Digital Communications

This document is intended for those who have already downloaded and installed a copy of the **SDC Private Messenger** (PM) to explain functionality unique to it needed to meet the requirements for security. Such functionality is absent in ordinary plain text (non-secure) instant messenger clients.

I. Operational Overview for Secure Instant Messaging



These are two common types of network topology. The network on the left is called Client Server. All of the users are connected by a common server, where all of the information needed to connect is stored. The server stores contact information, and also knows when a user is online and where he is. The server also orchestrates the two way chat communications between users.

The network on the right is called Peer To Peer. Instead of using a server to delegate and store information, the peers are responsible for resolving all the groups' addresses themselves. They are also responsible for making multiple outbound connections and accepting multiple inbound connections.

PM utilizes a mechanism called the **Resolver** which is used by any one peer in a group to receive the addresses of each group member and then makes them available to the group. Every peer must have the ability to receive connections from multiple nodes (peers) with a mechanism called the **Listener**. The PM also has a two person only direct point to point **Quick Chat** mode that only requires the entry of a Key and destination IP Address and Port number to operate.

II. Security Starts with Planning

A group of people (Participants) desiring to commence a Group Chat session must first decide on the manner of **Key Distribution** to be used. There are three methods to choose from. Each Participant must have a secure flash drive or other means to secure the **Session Keys** (SK)

because PM does not persist any user data or message content to the database. This makes PM something like the old wooden telephone booth with the folding door. Upon approaching the phone booth with dime in hand a person has no idea of, nor is it discoverable, the identity of the person(s) who made or received any calls as well as the identity of the party on the other end.

Each Participant other than the **Resolver Operator** (RO) should store the RO's IP Address and Port Number on the secure flash drive with the current SK's. A runtime scratchpad table is used to store Network Information such as internal and external IP Address and port number in use and available network connections. This table is deleted at shutdown and the data is encrypted with a 256 bit AES encryption key randomly created at startup and discarded at shutdown.

The PM utilizes this scratchpad table because PM is designed to be operable almost indefinitely as there are no open connections unless and until a Participant actually sends a chat. PM schedules the **Refresh** calls to the Resolver every 9 minutes and the Resolver discards **Registrants** after 12 minutes. This allows network connections to fluctuate with a high probability of not affecting a current chat session. The PM nodes are all point to point connected when actually messaging. No registered servers or DNS is involved. The PM sits in its silo on the Dark Net highly undiscoverable if the user's router and its settings are capable. PM never announces it presence on the Internet and discards connection attempts from 'strangers'. The maintenance of the chat session and it participants is protected by a separate 256 bit encryption key.

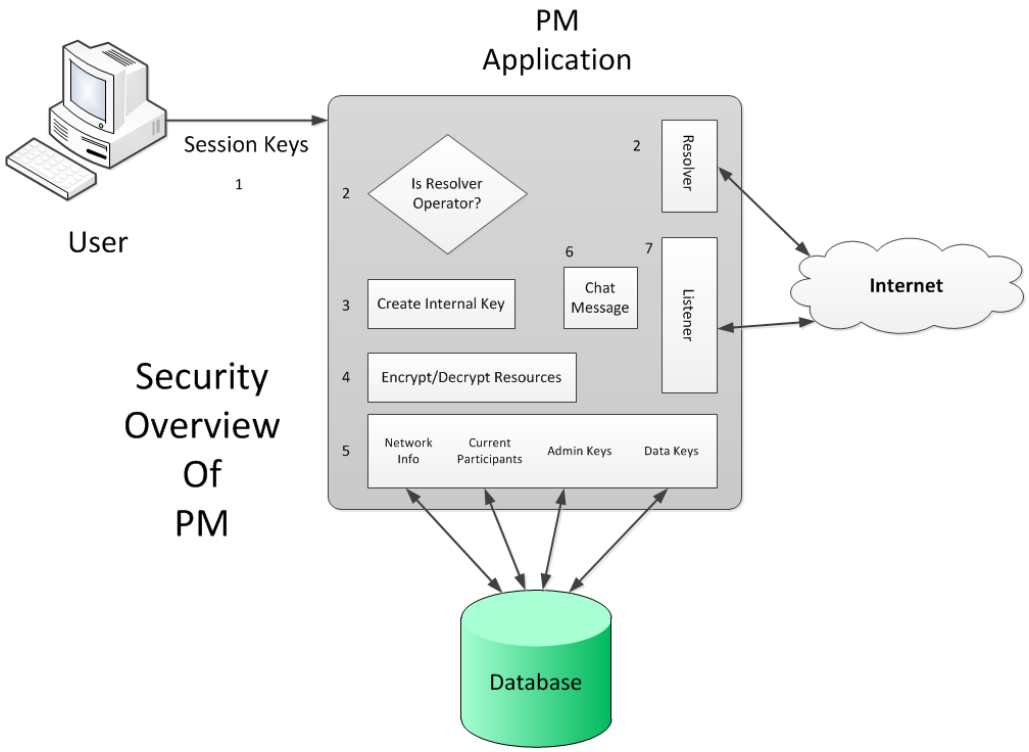


Figure 2. PM Security Functionality

A. Typical User Workflow Security Measures:

1. Data (Session), Admin Key and Resolver Status (1 & 2)

The user inputs his previously obtained **Data** (Session) and **Admin Keys**. The Participant who is the RO must initialize the Resolver and his Listener then communicate to the remainder of the Group that the Resolver is available. The remainder of the Participants also input their previously distributed Data (Session) and Admin Keys and wait for the RO to signal ready before starting their Listeners. All Resolver functionality has its data protected by the Admin Key. The chat message content is protected by the Data (Session) Key.

2. Internal Key Operations (3, 4 & 5)

The Internal Key is also a 256 bit AES encryption key. This key is used for protecting all of the run time data collected and used by PM. It is a random cryptographically strong key created at startup and discarded at shut down. All data encrypted by the Internal Key is specifically deleted at shut down even though encrypted.

3. Chat Message Operations (6 & 7)

Once PM is running and all Participants are **Registered** to the Resolver, chatting from this point forward is much like with plaintext non-secure messengers except every chat message is encrypted with the Data (SK) Key.

4. Key Management (5)

To maintain secrecy of the Session and Admin Keys used between Participants there must be secure protocols that the users agree upon and follow. All of the methods available to PM users have stood the test of time and are in use today by governments, militaries, banks, corporations and others.

The first and most traditional is the physical exchange of key values by any desired means or combinations or means. The values thus exchanged may be encrypted by a **One Time Pad** for added security. The second and third methods available to PM users both use the **Elliptic Curve Diffie-Hellman** (ECDH) key exchange protocol although in slightly different ways. The ECDH protocol allows to users to create a public-secret key pair (not to be confused with RSA) and exchange their public keys safely as they are useless to an adversary. Then the exchanged public keys are combined with the secret keys to produce the very same key value on all Participants computers. This key is also secret from the world and used only once and is known as a **Key Encryption Key** (KEK).

The Key Master exchanging Session Keys enters or creates a new Session and Admin Keys for himself and the all of the Participants. The new Session and Admin Keys are communicated to the Remote User Participants encrypted with the exclusive and mutually derived KEK.

If the Participant Group is exchanging keys for the very first time the **Distribute First Time Keys** functionality employing ECDH is used. The users exchange public keys and then the created or entered new Session Key is encrypted by the KEK and delivered

to the Remote User via any means including ordinary email.

When the Group already has a Key Relationship established the Participants may employ the **On The Fly Key Exchange** functionality in PM. This method also utilizes ECDH the main difference being is the Key Master and Remote User have the option of using built in messaging of the exchanged values encrypted with the current Data Key.

Support: stephen.tassio@topsecretcommunications.com