Design for E2E Secure Chat Application

**Security is not an after thought and it starts at Design level!**

|  |  |
| --- | --- |
| Asset(s) | 1. Database 2. Messages 3. Application Software 4. User verification link sent while registration |
| Stakeholder(s) | 1. Developers 2. Users |
| Adversary model(s) | 1. Eavesdropping adversary 2. Compromise of database 3. Compromise of exchange of keys |
| Attack Surface(s) | 1. User account details 2. Database 3. Configuration 4. Executables 5. DLL’s 6. Email/SMS Service 7. Server 8. HTTPS Protocol 9. JWT |