

The three applications will have three levels of security, the AI chatbot being the lowest and most accessible, while the RPA system will be the strictest to access. This is due to the data the applications have access to, and the functionality they have on said data. By applying the principles ‘assume breach’, ‘use least privilege access’ and ‘verify explicitly’, this architecture ensures robust security.

The users are split into 3 primary sections. Mobile customers, non-mobile customers and non-customers, and thirdly Employees. The Mobile customers will be able to access the mobile app and can have increased security through passwordless verification (such as fingerprint and face authentication). All users would have access to the chatbot, employees, customers and non-customers. The devices they use is irrelevant therefore the authentication required for access to this application is the least critical. The third type of user (Employee) would be the only user to be able to access the RPA system. This would be through levels of authentication. Such as multi-factor authentication, their identity being granted though the IAM, and additionally device authentication. It is standard practice for companies to have authorised devices that employees must have to access higher graded applications.

The Policy Enforcement point (PEP) and the Policy Decision Point (PDP) are standard sections of any Zero Trust Diagram (ZTD). The PDP evaluates the access requests, while the PEP applies the access controls. The PEP grants the user level of access to the applications.

The data that is inserted in the Mobile Banking App should be encrypted for increased security. This is in case of a data breach to the database, however if the data is encrypted, it would be no use to the perpetrator(s).

The diagram also has a ‘Security control zone’ where in the network, zero trust principles are withheld and enacted upon the rest of the network, for example the Role-base access control (RBAC) will be crucial for the RPA. It will allow the system access to specific datasets, not the entire database. This is a key principle in the Zero Trust philosophy. To minimise access as must as possible at all times.