Banking Cloud Application and Infrastructure Scenario

Merrilton Bank is developing a cloud application to provide a wide range of its banking services to its customers and is considering a cloud-based infrastructure to support it. The bank has a clear vision about the application and its function, as well as the supporting infrastructure.

You have been hired to design and develop the cloud infrastructure that will support the application. The notes in this document were compiled by the bank's personnel in various meetings and outline the business and infrastructure requirements, specifications, and recommendations made to date. You will use them to inform your design of a cloud-based solution that meets the needs of the bank.

Purpose

The Merrilton Banking Application is a cloud application that will provide a wide range of banking services to the customers of Merrilton Bank. The app is being developed for Android and iOS systems and will be available in Google Play and the Apple App Store.

Security Aspects

Device Security

- The application will use the International Mobile Equipment Identity (IMEI) or another unique telephony number (e.g., IMSI, MEID, or ESN) for device authentication so a determination can be made if the user is logging in from a known or a new device.
- The system should map one account with a maximum of 10 devices and/or browsers.
- When the log-in is being attempted from a new device or browser, a push alert should be sent to another two-factor authentication system for validation of the device or the browser.

User Security

- Users should be authenticated by a unique number that is not their bank account or their email address.
- Two-factor authentication should be pushed to an email or pushed to text an authenticated device.
- At the time of log-in, device authentication should occur before user authentication.

Push Notifications

- The push notifications are considered worker threads within a queuing structure provided by the cloud background.

- A relational database tied into a queueing system for outbound text, email, and application alerts (if enabled by the user) should be in place.
- Internal fraud alerts should also be a part of the queue when unusual activity is detected by the application or the account.

End-to-End Security

- The Merrilton banking cloud application should implement the end-to-end security model from the application by using encoding/decoding and serialization from within the app to the receiving computing system.
- The communications channel will be set up as port 4599 and will be provided custom gateway software for a Windows Server 2012 that would handle the decryption, deserialization, and then encryption/serialization back to the application. The setup will reside in a cloud environment with defined firewall rules.

Backend Architecture

- The developer has recommended that there be at least four SMS or equivalent queues, two of which are high priority and two medium priority. High-priority queues should be updated immediately and handle transactions and fraud-prevention activities. The medium-priority queues should be used for email, push, and in-app push notifications of transactions.
- Customers can choose to be notified when transactions are higher than a set amount. The supporting medium-priority queues should alert only when a customer's threshold amount is stored in a database.
- The system interacts with at least five other systems via application programming interfaces (APIs), three of which are of the major credit reporting agencies, one for fraudulent activities, and one for credit card activities. All these interactions will result in transactions, logs, and requirements for data security based on the Payment Card Industry Data Security Standard (PCI DSS).
- Single sign-on (SSO) services will be provided by an SSO gateway.
- The implementation will include a public-private architecture; public gateway services on port 4599; a private architecture that provides queues; an email gateway; a text gateway; a push gateway to the app; databases; API interconnections; worker queues (SMS queues); connections back to deep-banking information for risk management including fraud; a balance; and credit information that meets Federal Deposit Insurance Corporation (FDIC), PCI DSS, Sarbanes-Oxley Act (SOX), and other applicable laws, regulations, and standards.

In-House Data Center

- The cloud architecture must tie into the bank's data center located in Atlanta, Georgia, via a virtual private network (VPN) system.
- The cloud architecture must implement appropriate redundancy to allow for disaster recovery and business continuity.
- The cloud architecture should allow for international access based on geographic information system (GIS) information and be accessible by banking personnel from the home office only. All Merrilton Bank branches already feed through the Atlanta data center. There will be no local access by branches to the cloud architecture unless they are customers using the application. Branches must show the same balance and other customer information as the customer sees; therefore, tight integration between the home data center and the cloud is critical.

Disaster Recovery and Business Continuity

- The disaster recovery plan should use at least three geographically dispersed cloud data centers.
- In case of a disaster affecting the Atlanta data center, a hot copy will be available in the cloud, and a cloud-based VPN router will support the branches of the bank.

App Management Requirements

The bank's chief information security officer (CISO) and the chief information officer (CIO) need a project timeline, an estimate of maintenance costs, and a risk management assessment, as well as redevelopment costs based on the cyclic nature of the app stores.

- Both app stores recommend updating frequently, and the management team has decided on a rolling 30-day update cycle for bugs or new functionality. On average, it takes seven days to review and put an updated app in the store, so this lead time must be built into the monthly management plan. If the app requires any change to the backend, the CISO and CIO would like to see an updated change management plan based on the rolling 30-day update cycle, including any changes to operations or management of the cloud backend. The CISO and CIO would like to see any suggestions on compliance and management of the cloud system and how it aligns to the in-house data center in Atlanta, GA.

- The CISO would like to see the following included in the plan:
  - patch management
  - access management
  - new account creation management and integration with the help desk
  - change management and how fraud management and integration with the Fraud Department will be accomplished

- The CIO would like to see the following included in the plan:
  - disaster recovery/business continuity considerations
  - daily operations expectations or concerns
  - integration with overall bank regulations that need attention, especially data center accreditation