RSA Adaptive Authentication On-Premise Implementation Guide

Last Modified: June 12, 2013

Partner Information

Product Information	
Partner Name	Monitise
Web Site	www.monitise.com
Product Name	Monitise Mobile Banking Solution
Version & Platform	5.0
Product Description	Monitise's Bank Anywhere product provides complete account management services, including account balances, statements, transfers and alerts. Bank Anywhere supports major mobile operating systems, ensuring availability on the widest range of device models, including tablets.

monitise ™

Solution Summary

The Monitise Mobile Banking Solution platform's key banking services include balance enquiry, personal financial management, account transfer and business banking. The platform also offers strong security options that protect access to sensitive financial data with RSA Adaptive Authentication On-Premise (AAOP) risk-based authentication.

AAOP works behind the scenes to authenticate Monitise end-users based on individual user and device profiles. It relies on the RSA Risk Engine to estimate the level of risk associated with each login attempt. Customer policy determines whether to admit, deny or challenge the user based on the engine's risk score and a host of additional parameters.

All Bank Anywhere clients support login authentication, but only the iPhone and Android mobile applications support user-enrollment. Before enrolling with AAOP, end-users must create a mobile banking account. They can do so with either the iPhone or Android mobile applications or by contacting their bank.

RSA Adapted Authentication On-Premise Supported Features	
Monitise Mobile Banking Solution 5.0	
RSA Adaptive Authentication User Enrollment	Yes[1]
RSA Adaptive Authentication Login Monitoring	Yes
RSA Adaptive Authentication Login Authentication	Yes
RSA Adaptive Authentication Transaction Monitoring	No
RSA Adaptive Authentication Transaction Authentication	No
RSA Adaptive Authentication Web Channel Data Collection	Yes
RSA Adaptive Authentication Mobile Channel Data Collection	No
Challenge Question Authentication	Yes
Out-of-Band Phone Authentication	No
Out-of-Band Email Authentication	No
Out-of-Band SMS Authentication	No

The Monitise – AAOP integration consists of two key components:

- **Bank Anywhere Client** – Bank Anywhere clients provide a mobile interface to a banking customer's website. Monitise offers a mobile browser client and a variety of mobile application clients. Monitise Professional Services configures these clients to collect device profile information and pass it to a Monitise Server.

- **AAOP Connector** – An AAOP connector sits on a Monitise server and enables bidirectional communication between Bank Anywhere clients and an AAOP server. Connectors are implemented and by Professional Services.

---

[1] User enrollment is only supported on the Bank Anywhere iPhone and Android mobile applications. Users must pre-enroll with Adaptive Authentication before they can use a mobile browser client.

Each Bank Anywhere client includes JavaScript code that collects data from an end-user's device and passes it to a connector deployed on a Monitise server. The connector forwards this data to the customer's AAOP server for analysis. The server uses the data to identify potential fraud and recommends further action based on the customer's policies. The connector then instructs the client to take the appropriate action.
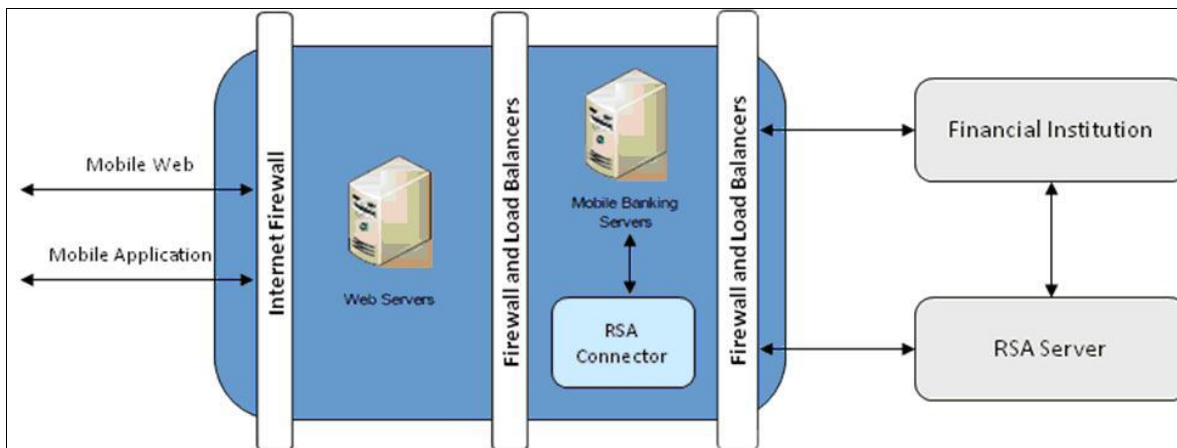
Partner Product Configuration

Monitise Professional Services is responsible for:

- delivering AAOP connectors and Bank Anywhere clients
- customizing Bank Anywhere clients to meet the customer's branding requirements
- deploying a connector on the Monitise server
- configuring the connector to communicate with the AAOP server and the mobile clients.
- customizing Bank Anywhere clients to meet the customer's branding requirements
- customizing the connector according to the customer's requirements
- making the iPhone and Android mobile applications availible to end users
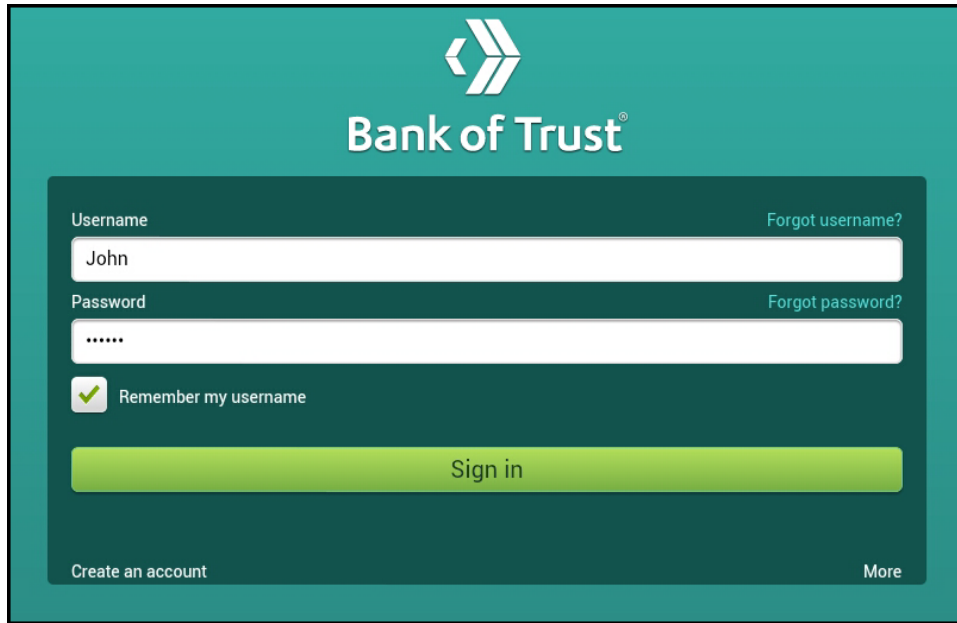
Note: The customizations mentioned above require collaboration between the Monitise implementation team and the customer's security experts (typically the IT Security team and/or RSA).

Software Requirements

- Monitise Server 5.0.
- RSA AAOP 6.0.2.1 SP3.
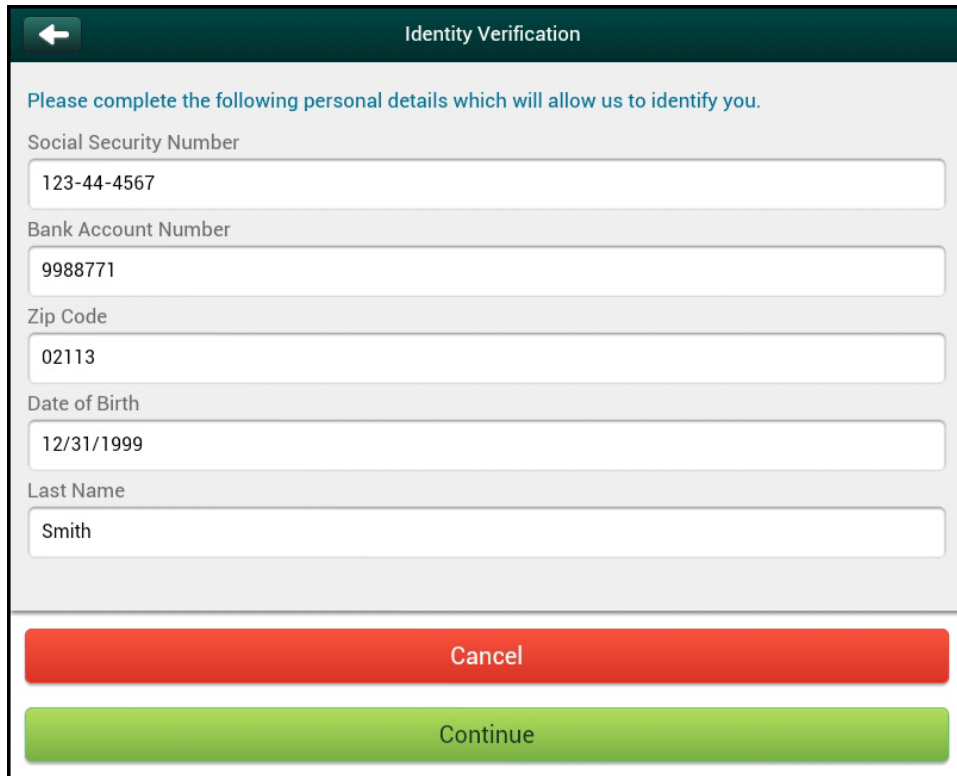
Android Client Application Screenshots[2]

Standard Logon Prompt (Create an Account link)[3]

---
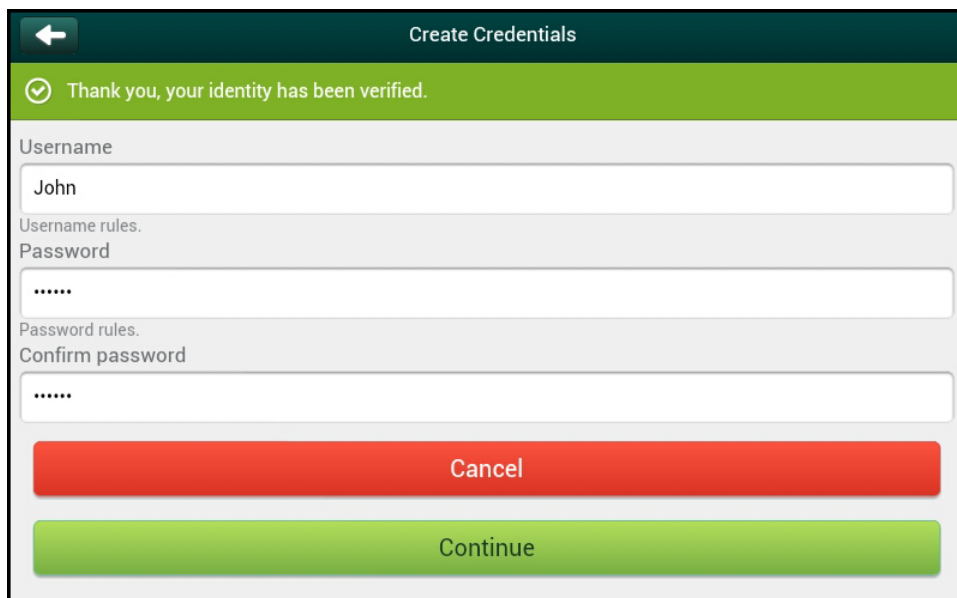
[2] The iPhone client and Android client have very similar GUIs. Screenshots of the iPhone client have been omitted.
[3] The *Create Account* link allows an existing bank user to create a mobile profile for the account and to enroll with AAOP.

Identity Verification Form

Mobile Account Credentials Enrollment Form
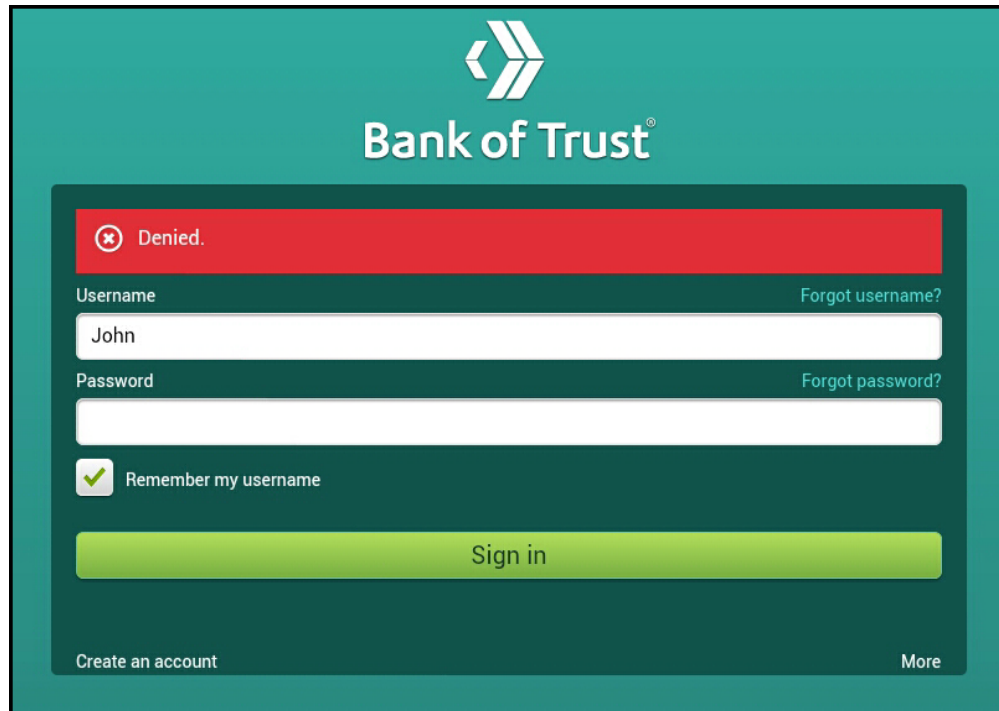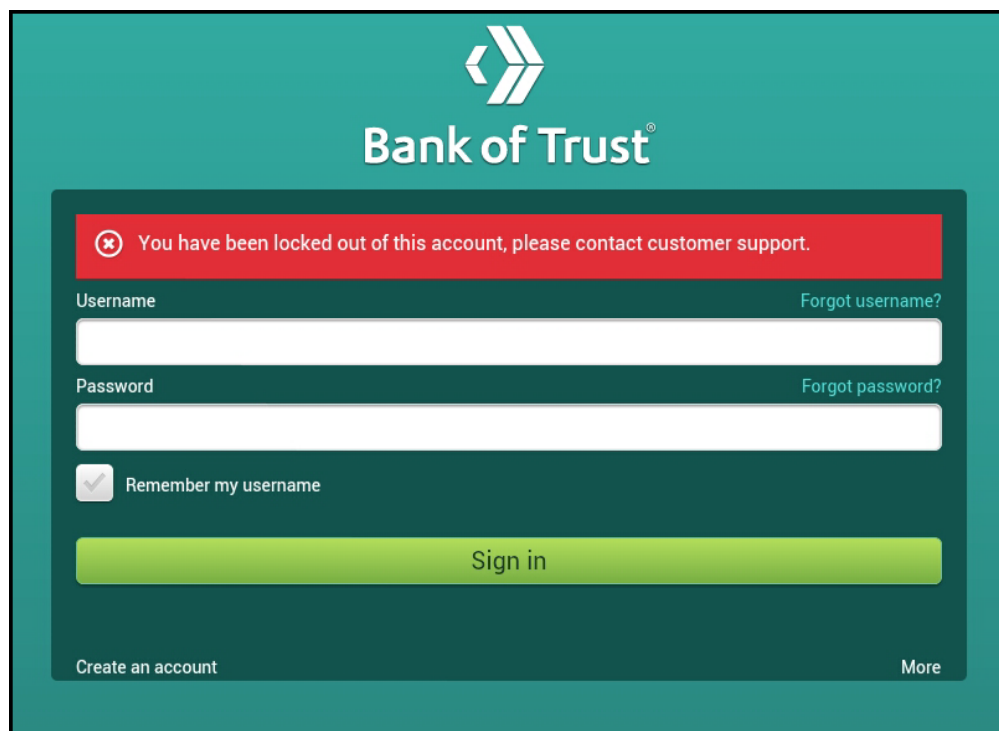
Challenge Question Enrollment Form

Access Denied Message

Lockout Message

Challenge Question Prompt

Main Menu Page

Account Summary Page

Change Security Questions Form

Mobile Browser Enrollment and Login Screenshots

Standard Logon Prompt

Access Denied Page

Lockout Page

Challenge Question Prompt

Challenge Authentication Failure Page

Main Menu Page

Preferences Page

Account Summary Page

Change Password Page

Certification Checklist for RSA Adaptive Authentication Login

Date Tested: June 18, 2013

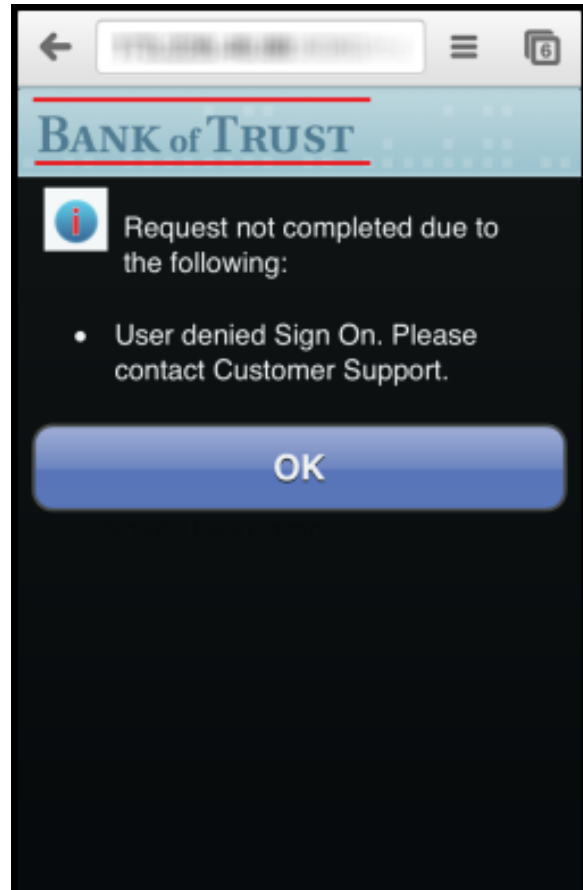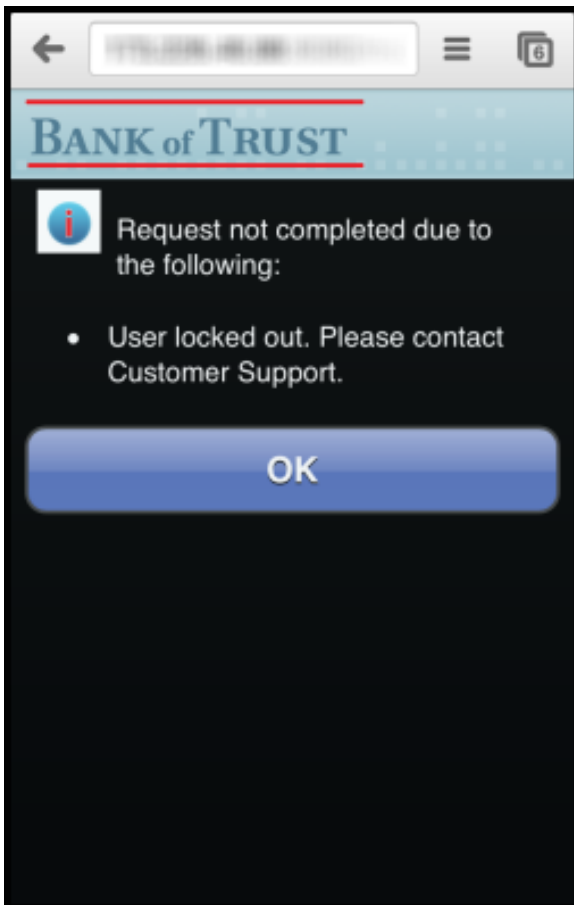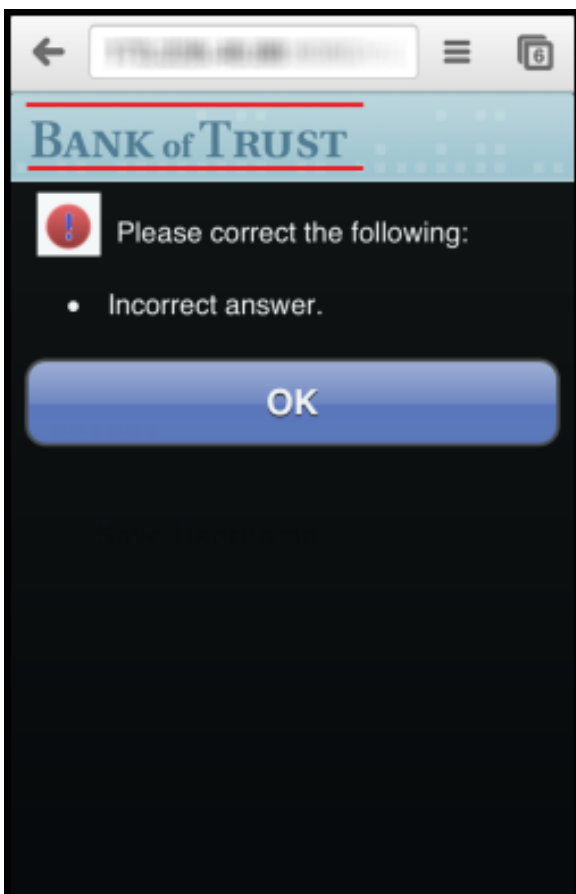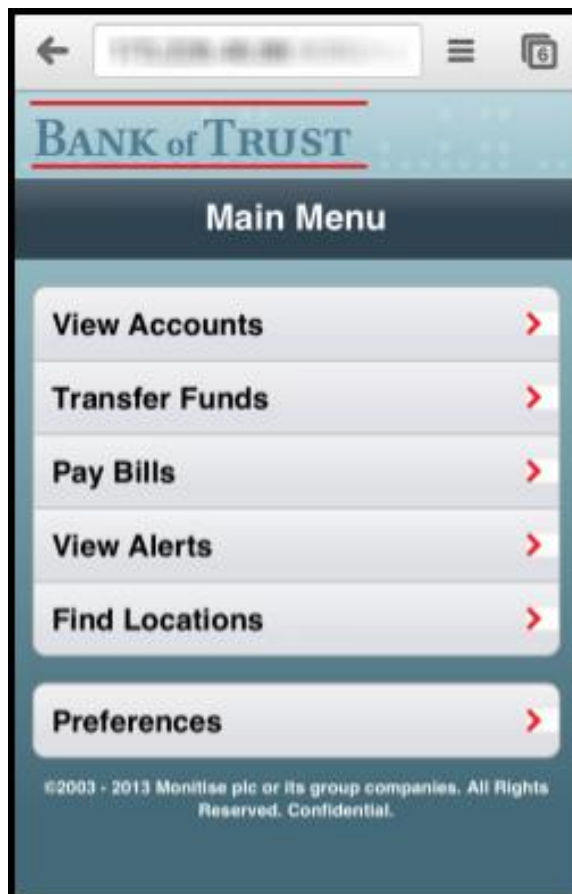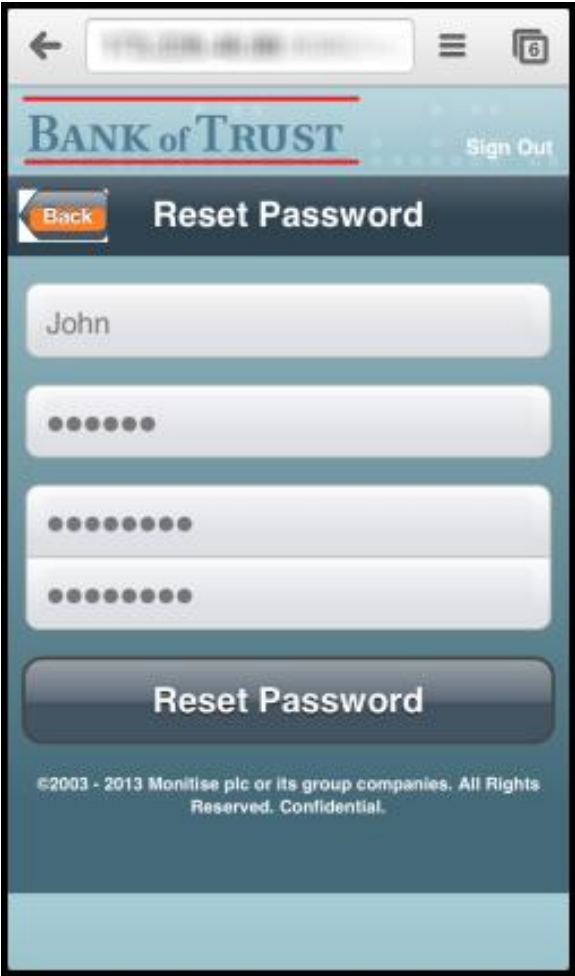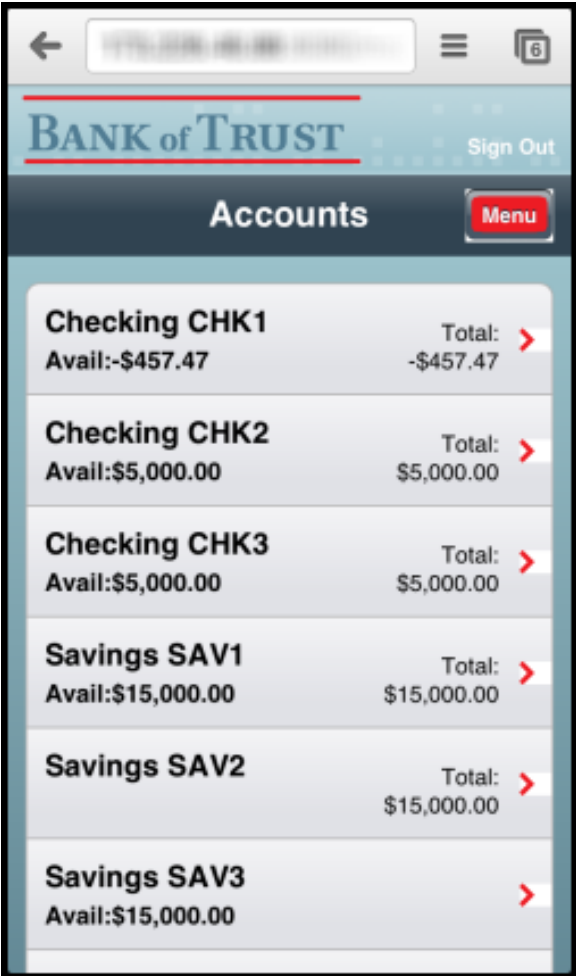| Certification Environment		
Product Name	**Version**	**Operating System**
AAOP	6.0.2.1 SP3 P2	CENTOS 6
Monitise Server	5.0	NA
Mobile Browser	Safari	iOS 6.0.1
Android Bank Anywhere Application	5.0	Android 4.0.4
iPhone Bank Anywhere Application	5.0	iOS 6.0.1

Login Authentication			
	Mobile Browser	**Android**	**iOS**
User Status			
Unknown Bank Users	✓	✓	✓
Un-enrolled Users	✓	✓	✓
Unverified Users	✓	✓	✓
Deleted Users	✓	✓	✓
Locked Users	✓	✓	✓
Unlocked Users	✓	✓	✓
Verified Users	✓	✓	✓
Analysis Response Actions			
Allow	✓	✓	✓
Review	✓	✓	✓
Challenge	✓	✓	✓
Deny	✓	✓	✓
Authentication Methods			
Challenge Questions	✓	✓	✓
Out-of-Band Phone	NA	NA	NA
Out-of-Band Email	NA	NA	NA
Out-of-Band SMS	NA	NA	NA

User Enrollment and Profile Maintenance			
	Mobile Browser	**Android**	**iOS**
User Enrollment			
Enroll User with AAOP	NA	✓	✓
Profile Maintenance			
Change Challenge Questions	NA	✓	✓
Change Phone Number(s)	NA	✓	✓
Change Email Address	NA	✓	✓

JGS/PAR   ✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

Checklist for RSA Adaptive Authentication Device Data Collection

Web Channel Data Collection			
	Mobile Browser	**Android**	**iOS**
Device Data			
Device Fingerprint	✓	✓	✓
HTTP Accept	✓	✓	✓
HTTP Accept Character Set	✓	✓	✓
HTTP Accept Encoding	✓	✓	✓
HTTP Accept language	✓	✓	✓
HTTP Referrer	✓	✓	✓
IP Address	✓	✓	✓
Device Token Cookie	✓	✓	✓
Device Token FSO	✓	NA	✓
User Identification Data			
Username	✓	✓	✓
User Login Name	✓	✓	✓
Org Name	✓	✓	✓

Mobile Channel Data Collection			
	Android		**iOS**
Device Data			
SIM ID	NA	SIM ID	NA
Hardware ID	NA	Hardware ID	NA
Other ID	NA	Other ID	NA
Phone Data		**Phone Data**	
Phone Number	NA	Phone Number	NA
Country Code	NA	Country Code	NA
Area Code	NA	Area Code	NA

JGS/PAR   ✓ = Pass ✗ = Fail N/A = Not Applicable to Integration