## Multifactor Authentication Solution

**Requirements:**

* Secure enterprise authenticator solution.
* Secures internal and remote network access.
* “zero footprint” options.
* Available in multiple form factors including hardware and software authenticators as well as Risk-Based and On-Demand (SMS) authenticators.
* Strong network security: hardware or software authenticator with a unique symmetric key that is combined with a proven algorithm to generate a new one-time password (OTP) every 60 seconds.
* High quality and reliable authentication: from temperature cycling to mechanical shocks to being immersed in water, hardware tokens are subjected to rigorous tests to ensure that user organizations to not face hidden costs due to token failures.
* Convenient solution for end users: hardware and software tokens, ach end -user is assigned an authenticator that generates a one-time-use code. Risk-Based and On-Demand (SMS) authenticators, convenient options for zero-footprint authenticators enable organizations the flexibility of extending applications to a greater population of users while at the same time maintaining the security posture of the organization.
* Hardware token model that generate and display new codes every 60 seconds.
* PINpad feature, that enables user to encrypt their passcode for a higher level of security.
* The one-time password functionality of the other hardware authenticators and can be sed for storage of Windows username/password credentials and digital certificates – creating a master key for multiple authentication methods.
* Software authenticators: software tokens use the same algorithm as hardware tokens. Instead of being stored in hardware, the symmetric key is safeguarded securely on the user’s PC, smart phone or USB device. Software tokens can be revoked and recovered when someone leaves the company or loses a device, eliminating the need to replace tokens.
* Software tokens supported smart phone platforms: BlackBerry, iOS, Android and Microsoft Windows Phone.
* Token for Windows and MAC OSX are convenient form factors that reside on a PC or MAC and enable automatic integration with leading remote access clients.
* Toolbar Token combines the convenience of auto-fill capabilities for web applications with the security of anti-phishing mechanisms.
* Risk-Based multi-factor authentication solution, that strengthens traditional password-based systems by transparently assigning a risk level to each login request. A powerful risk engine evaluates each attempted login and activity in real time by tracking hundreds of risk indicators and determining the risk associated with each access request.
* Authentication Manager deployment on a single platform alongside hardware and software authenticators.
* On-Demand authenticator enables users to receive a one-time password as an SMS message delivered to their cell phone or via e-mail. Users are sent a one-time password to use as a login to their SMS-enabled mobile device. The On-Demand authenticator is a true zero footprint authenticator and requires no hardware or software token to be deployed.
* With tested, documented, certified and fully supported interoperability with 500+ technology partners and standards-based interoperability with thousands more.
* The broadest range of MFA options, including mobile push authentication, biometrics (fingerprint, eyeprint), SMS, voice, email, risk-based, FIDO, proximity-based authentication and soft tokens—and, of course, hardware tokens.
* Integration with native authentication on leading mobile devices (Apple Touch ID, Samsung Fingerprint, Android Fingerprint and Windows Hello).
* Software token application available in major app stores and should be user-activated.
* Using the Cryptographic Token Key Initialization Protocol (CT-KIP) for secure seeding of hardware tokens, and Ocode for software token seeding/activation.
* Interprets large amounts of data for machine learning to detect patterns of abnormal user behavior and recognize individual users’ interaction patterns, ultimately making security frictionless and smarter at the same time.
* Interoperability with leading Privileged Access Management (PAM) solutions.
* Working together with SIEM solutions allowing not only share log information with the SIEM solution but also to ingest threat intelligence from the SIEM for real-time response that adjusts access policies based on the level of risk shared.
* Working with VMware Workspace One to provide enterprise-grade security to digital workspaces for a frictionless access experience.
* Interoperable with third-party SSO solutions.
* Deployment options: Cloud hosted (AWS), On premises, SaaS, Hybrid.
* Multi-factor authentication technology to a wide range of web-based applications.
* Enabling authentication based transparent analysis of end user device and behavior.
* Offering convenient username and password login experience.
* Mix and match hardware tokens, software tokens, and Risk-Based authentication to support varying end user needs.
* Machine-learning risk engine.
* Device profiling.
* Behavior profiling.
* Identity confirmation.
* Hardware tokens that leverage the AES-128 algorithm and are time synchronous.
* Certifications: Cloud Security Alliance (CSA) STAR Certification, FIPS Compliance, Skyhigh Enterprise-Ready™, SOC 2 Compliance.

**Supported authentication agents:**

* Standard agents (IIS/Apache, Windows, PAM)
* RADIUS agents with token support
* Authentication API - deployed on-premises
* RADIUS agents with push and biometrics support
* Cloud SAML authentication
* Authentication API - cloud deployed
* SSO Agent for SaaS and web (SAML, proxy, and password vault)

**Authentication Methods:**

* Hardware and software tokens, on-demand authentication (ODA/SMS)
* Authenticate App: Tokencode, Approve, or Device Biometrics (such as Fingerprint, FaceID, or Windows Hello)
* FIDO Token
* Integrated SMS Tokencode and Voice

**VTB Bank infrastructure**

|  |  |
| --- | --- |
| **Systems** | **Quantity** |
| Virtualization (vmware) | 20 |
| Windows servers | 100 |
| Linux servers | 30 |
| Antispam (Barracuda Email Security Gateway) | 1 |
| Mail Archiver (Barracuda Message Archiver) | 1 |
| RADIUS server (Cisco Identity Services Engine (ISE)) | 2 |
| Telephone system servers | 15 |
| Backup copying device (HPE StoreOnce) | 3 |
| Data storage systems (Storage HPE Eva) | 2 |
| Data storage systems (Storage HPE 3PAR) | 1 |
| Routers | 98 |
| Switches | 107 |
| Firewalls | 6 |
| FibreChannel switches | 4 |
| WIFi network controllers | 2 |
| Data center UPS (APC) | 4 |

**Terms and Conditions of Warranty And Support Services:**

* License must be perpetual.
* 2 year support for hardware tokens.

**Documentation and API:**

Should have user documentation and API documentation available for integration with custom/in-house business applications.

Preference will be given to those who have experience in implementation of offered solution in our Region or CIS.