CENTAGATE® BOX Solution Technical Data

1. Physical Hardware Data

Branded Server Appliance with specifications best fitted into the deployment in line with performance expectation.

Form Factor	Industrial grade 2U Server
CPU	Intel Xeon 4-core
RAM	Standard: 32 GB; upgradeable up to 64 GB
Storage	Standard: 2x 512 GB storage; upgradeable and field replaceable, total of 4 slots
Power Supply	Redundant, 2x field replaceable power supplies
Network	4x Gigabit Ethernet
Management	Multi-touch screen
	Out-of-band management
Environmental Temperature	In operation: +10 °C to +40 °C
	In warehouse: -10 °C to +55 °C
Humidity	10 to 95% relative humidity, non-condensing

2. Hardware Security Architecture

Security Certification	FIPS 140-2 Level 3 compliant and ongoing validation
Security measures	No low-level access to hardware and software

	Controlled Interfaces, only Ethernet or serial line communication available outside
	Signed and Encrypted Software Packages
	Secure reset cycle deleting all secrets (zeroization)
	Prevent extraction of data and application
Secure Boot	Independent ARM based SOC validates OS images before boot and controls the status of the server mainboard
Operating System	Small footprint Linux based OS as hypervisor
Physical Shield	FIPS 140-2 Level 3 compliant physical shield

3. Software Architecture

Security Certification	• Common Criteria EAL 4+
Compliance Standards	• FFIEC • MAS IBTRM
Development Platform	• J2EE
Web and Application Server Support	• Jboss / Wildfly
Database Support	• MySQL (version 5 or higher) • Maria DB (version 10 or higher)
Supported Authentication Mechanisms	• OATH: ○ HOTP (RFC 4226) ○ TOTP (RFC 6238) ○ OCRA (RFC 6287) • Dynamic Signature

	• Public key infrastructure with X.509 certificates • FIDO U2F • Biometrics • Challenge Questions and Answers • Static password with policy
Supported Integration Interfaces	• WebSSO using SAML 2.0 • Web service RESTful API • LDAP and Active Directory • RADIUS Protocol
Supported Channels	• PC, Out-Of-Band Mobile Push, QR Code Scanning and SMS
Supported Risk Scoring Methods	Whitebox configurable policy Not limited to number or transactions Policy and Case base analysis based on factors: • OS • Browser • Time • IP address • Location • Transaction behavior (customized project)

4. System Architecture

Time synchronization	NTP Support
High-availability clustering	Active-active and active-passive configurations for production environment and disaster recovery with support from external load balancers
	Real-time database replication
Connectivity	SSL/TLS support
	Encapsulation – 2nd layer of end-to-end encryption for all sensitive data transferred between server and mobile token: seed code

	distribution, encryption passwords, transaction signing OTP, etc.

5. Software Features Summary

Features	On-premise
User Management	
Self-Registration	✓
User Life-Cycle Management	✓
Bulk User Import	✓
Group Management	
Group Life-Cycle Management	✓
Role and Permission Management	✓
Company Management	
Company Life-Cycle Management	✓
Token Management	
Token Life-Cycle Management	✓
OTP synchronization	✓
Support for Mobile Security Token (Mobile Application)	✓
Device Management	
Device Provisioning, encrypted seed code distribution	✓
Device Life-Cycle Management	✓
Certificate Management	
User Certificate Management	✓
Trusted Certificate Management	✓
CRL Management	✓
Advanced Signature Verification	✓
Authentication Options	
Username/Password	✓

Challenge Question & Answer	✓
SMS OTP	✓
OTP (Hardware Token/Mobile Application)	✓
Challenge Response OTP (CR OTP)	✓
QR Code	✓
Mobile Push	✓
PKI	✓
Mobile PKI	✓
Mobile AudioPass	✓
Fast ID Online (FIDO) U2F	✓
SecuGen Biometrics	✓
Security Image	✓
Security Management	
Hybrid Risk Scoring Engine – Security Policy Management	✓
Cases Management	✓
Trust Level Management	✓
Password Policy Management	✓
Session Management	✓
IP Address restriction for integrated applications	✓
Geo-Fencing	✓
Seed code encryption	✓
Integration	
Application Management	✓
SAML 2.0	✓
Web service RESTful API	✓
LDAP and Active Directory	✓
RADIUS Protocol (Support Radius Client, VPN system)	✓
Key Management	
Server Encryption and Signing Key Life-Cycle	✓

HSM Integration	✓
Reporting	
Dashboard, Console overview: Real time monitoring • SNMP status • Load-balancing status • Hardware status • Application status • Connectivity	✓
Authentication Usage	✓
World Map of Authentication	✓
Certificate Expiry	✓
Company license Expiry	✓
User Usage	✓
Activities Log	✓
Authentication Log	✓
Device Usage	✓
Comprehensive Notification	✓
Configuration Management	
Email Template Management	✓
SMTP Management	✓
SMS Template Management	✓
SMS Gateway Configuration	✓
OTP Configuration	✓
License Management	✓
Rsyslog service with function to forward logs to centralized log management system (SIEM)	✓
Monitoring: SNMP Setting	✓
Backup scheduler	✓
Maintenance	
Email Template Management	✓
SMTP Management	✓

SMS Template Management	✓
SMS Gateway Configuration	✓
OTP Configuration	✓
License Management	✓
Backup & Restore	✓
Factory reset	✓
Update patch, version, functions	✓
Customization	
Professional services to provide additional/customized APIs	✓

6. System Integration Resources

Use case	Programming Language	Functions
Web API Page	JAVA, .Net, Webservice	Username/Password Authentication
		Adaptive Authentication
		OTP Authentication
		Request SMS OTP
		SMS OTP Authentication
		User registration
		Update user status
		Unbind and delete user
		Unlock user
		Update user profile

		Sync User from other system
		Token Registration (One-Time PIN)
		Update token status
		Unlock OTP Token
		Unregister Token
		Sync Token
		Request Random String
		PKI Authentication
		Simple PKI Authentication
		PKCS#7 PKI Authentication
		Request QR Code
		QR Code Authentication
		Request OTP Challenge
		CR OTP Authentication
		Request Challenge Question
		Security Question Authentication
		Request Mobile Push CR OTP Authentication
		Check Authentication State
Transaction Form		CR OTP Authentication

	JAVA, .Net, Webservice	Request Mobile Push CR OTP Authentication

7. Workstation requirements

User interface	• Web user interface for administration and self-service
Operating system	• Windows XP Professional (SP 2) and above • Mac OS X version 10.7 and above • GNU/Linux kernel 3.6 and above
Web browsers	• Microsoft® Internet Explorer version 7.0 or later • Firefox version 30 or later • Google Chrome version 38 or later
Minimum hardware requirements	• Intel Pentium 1 GHz or equivalent • 512 MB memory • Colored monitor with display resolution of 1024x768 • 2GB hard disk free space • Network card • Keyboard and mouse

8. Mobile Token (Soft Token)

Mobile Token is a software (application), that can be installed on mobile devices, and can replace Hardware tokens

Supported devices	Wide range of Android and iOS devices (tablet, mobile phone…) • Android 4.1 and above • iOS 8.0 and above

Supported Authentication Mechanisms	OATH OTP Tokens (HOTP RFC 4226, TOTP RFC 6238, OCRA RFC 6287): • SMS OTP (Event based HOTP) • Mobile OTP (Time based TOTP) • Mobile Challenge Response (OCRA) • Mobile OTP transaction signing (OCRA) • QR Code with OTP transaction signing (OCRA) • Push Mobile with OTP transaction signing (OCRA) • Mobile PKI
Access protection	• Username, Password, PIN and biometrics login authentication • Auto log-off • Lock account after 3 failed attempts (customizable) • Logout Application after x time (customizable)
Connectivity	• SSL/TLS and Certificate pinning
Synchronization (server and mobile app)	• Manually • Automatically
Encryption	Encapsulation – 2nd layer of end-to-end encryption for all sensitive data transferred between server and mobile token: seed code distribution, encryption passwords, transaction signing OTP, etc.
Seed code protection	• Cryptography strength: 320-bits • Secure mobile device provisioning using encapsulation for seed code distribution • Seed codes are cryptographically bound to the device ID and user PIN (prevent clone to other devices)
RASP configuration	• Anti-repacking • Anti-debugging • Prevent access data in memory • Jailbreak / Root detection and prevention • Anti-cloning (Device Binding)

	• Emulator Detection • Code Obfuscation • Overlay detection and prevention API • Prevention code injection • Hook detection and prevention • Anti-Keylogger • Prevent screen reader • Screenshot detection and prevention • External Screen Blocker • Secure storage (Centagate Mobile user keys and seeds)
Language	• Available by default: English • Additional languages are available as project customization: Bahasa Melayu, Bahasa Indonesia, Vietnamese, etc…
Project customizations available	• Look and feel with customer's UI, Logo, etc. • UI support for wide range of device screens: mobile phones, tablets, iPads, iPhone X notch, etc… • OTP length 6 or 8 digits (configurable) • OTP validity time: default 60s (configurable)
Mobile SDK	Available for • Android 4.1 and above • iOS 8.0 and above • Support customize UI

9. Performance

Benchmark	195 OTP/s
Concurrent sessions	Unlimited
Number of user / Box	1.5 million users per Box with ability to expand