



Technical Data Sheet

November 2021
Document Version 1.4

Overview

Torus is a complete IoT solution for key management. It is built using Microsoft Azure technology stack with embedded Linux device firmware. Torus cabinets can be managed from any computer over secure internet services, with **no software installation** required.

Hardware specifications

AC Power supply	Input: 110VAC – 240VAC 2.5A, 47 ~ 63Hz Output: 14VDC
Power over Ethernet	POE / POE+ / POE++ <i>Battery backup must be connected</i>
Battery Backup	DC12v 7.2AH lead rechargeable
Certifications	 ICES-003 RoHS
Operation System	Embedded Linux
Flash memory	8GB (eMMC)
RAM	512 Mb
Max user capacity	10,000
Max event capacity	100,000
User management	From Torus software <i>(or third party using Torus Exchange or Torus Rest API)</i>
Communication Options	LAN (10/100Mbps Ethernet) 4G/LTE <i>Customer to provide SIM</i>
Other interface	USB

Physical construction

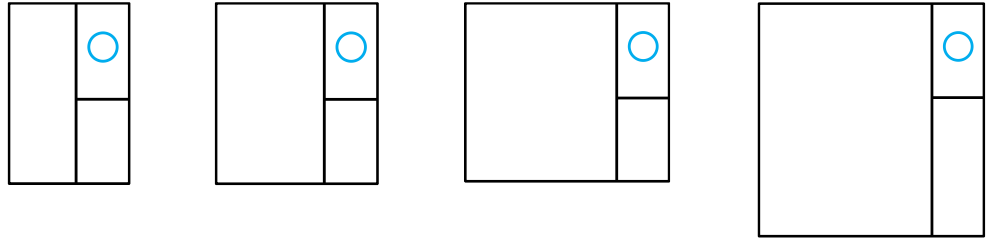
Cabinet body	Powder Coated Mild Steel 1.6mm
Door	4mm Polycarbonate
Inner Key panel	1.6mm Anodized Aluminum
Screen	Capacitive Touch Screen Size: 6.5-inch Resolution: 800x1024
Area for reader	Dimensions: Height 200mm X Width 100mm Material: Mild Steel
Operating Environment	0°C to 55°C
Application Situation	Indoors <i>No direct exposure to sunlight or water</i>
Mounting	Wall
Cable entry point	Through back of cabinet <i>See page 4</i>
Mechanical override	Bi-Lock key <i>on underside of cabinet</i>

Authentication options

Authentication devices	Card & Fingerprint Readers using Wiegand & RS485/OSDP <i>up to 256bits binary string</i>
Authentication options <i>(applies to every user on cabinet)</i>	User ID + PIN Card Card + PIN <i>User ID: 1 – 12 digits PIN: 6-digit default</i>

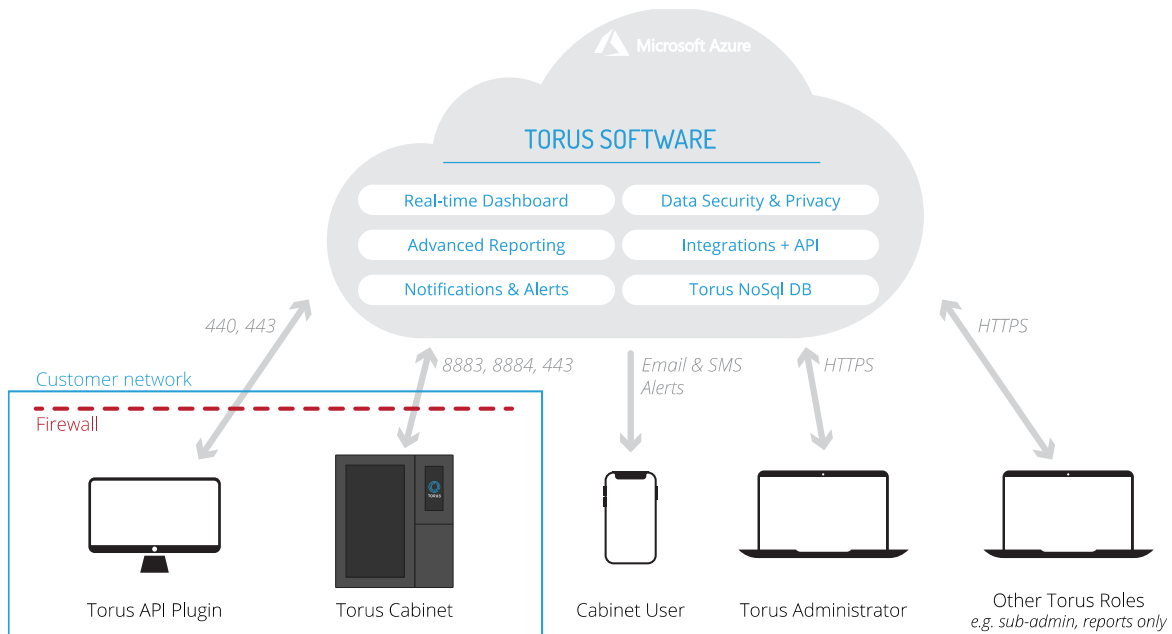
Cabinet security

Local data storage	Hashed using SHA-256
USB Port	Default: disabled <i>User must be granted permission through their Role in Torus software</i>
Traffic	End-to-end encrypted. TLS1.2, X509 certificates



		Torus 15	Torus 25	Torus 50	Torus 100
Overall Cabinet	Capacity	15 Bunch	25 Bunch	50 Bunch	100 Bunch
	Weight	35.2Kg	39.1Kg	54.1Kg	89Kg
	Height	674.8mm	674.8mm	674.8mm	941.8mm
	Width	532mm	620mm	840mm	1036mm
	Depth (including mounting bracket)	212.6mm			
	Depth (Between door & cabinet rear surface)	182mm			
	Depth (Between door & key panel surface)	84mm			
	Spacing of the key position	Horizontal: 88mm Vertical: 110mm Depth: 84mm			
Mounting bracket	Height	670.6mm	670.6mm	670.6mm	937.6mm
	Width	442.4mm	530.4mm	750.4mm	946.4mm
	Depth	30mm	30mm	30mm	30mm

Architecture



Data	
Storage	20GB per customer software data 20GB per cabinet for events data 20GB per customer for reporting and analytics data
Retention policy	365 days <i>After this time reporting data will be overwritten using first in first out (FIFO) method</i> <i>Customer can download or subscribe to reports to store log data in an offline manner</i>
Location	Australia Canada USA <i>Other locations available depending on customer requirements and availability of Microsoft Azure Datacenter.</i>
Backup and recovery	Every 4 hours. Locally Redundant Storage (LRS) <i>2 copies of data replicated across 2 locations in the primary region</i>
Certifications	 Torus is designed and manufactured by CIC Technology Pty Ltd, an ISO27001 certified organization.

Microsoft Azure

Torus Software inherits Azure's multi-layered security, deployed across physical data centers, infrastructure, and operations.

Certifications	Tier 4 ISO/IEC 27001 ISO/IEC 27018	CSA SOC 1 SOC 2	PCI DSS HIPPA
Application security	Azure Application Gateway Azure Web Application Firewall (WAF) IOT hub <i>(highly secure communication between Cabinet and backend services)</i> API security <i>(Application Gateway and WAF only allows API calls with secure cookies for Torus Web and per-device security tokens for Torus cabinets)</i>		
Network security	Torus instance resides in dedicated, segmented network. Multiple layers of firewall and denial-of-service (DDOS) hardware-based protection Azure WAF policies prevent OWASP top 10 vulnerabilities. Policies continuously upgraded by Microsoft		
Data security	Enterprise level security policies including data storage, data transit and infrastructure Customer account information encryption. Strong password enforcement Azure Key Vault used to store credentials. Critical data hashed using SHA-256 HTTPS & TLS 1.2 protocols for communication with Cabinet, Torus Exchange & Torus REST API <i>Torus software integrated application security architecture prevents anyone but the customer from accessing their data. This security model is reapplied with every request and enforced for the entire duration of a user session.</i>		
Systems security	Regular vulnerability testing of Torus software. DevOps and engineers in regular contact with security consultants and tech vendors Frequent scans of infrastructure to detect potential risks		