Information Security Paper

Torus Electronic Key Management System

Version 1.9



Legal Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of CIC Technology Pty Ltd. This document and the data herein shall not be duplicated, used or disclosed to others for procurement or manufacturing, except as authorized with the written permission of CIC Technology Pty Ltd. The information contained within this document or within the product itself is considered the exclusive property of CIC Technology Pty Ltd. All information in this document or within the hardware and software products themselves is protected by the copyright and/or other intellectual property laws of Australia.

© 2022 CIC Technology Pty Ltd. All trademarks are property of their respective owners. All rights reserved.

Table of Contents

Information Security Paper 1
Legal Disclaimer 2
Table of Contents 3
Introduction 4
Torus Architecture 5
Account Management 6
Torus cabinets 6
Torus Process Flow 7
API Services 7
Purdue Model 8
Cloud Computing Security 9
Data at rest 9
Resilient Design 9
Continuous Monitoring 9
Vulnerability Scanning 9
System Maintenance/Patching 9
Multi-Tenancy 10
Network Security 10
Web Application Firewall (WAF) 10
Intrusion Detection System (IDS) 10
Office Network 10
Remote Work 10
Torus cabinet Security 10
Data at rest 11
Networking 11
Bot Detection 11
Data in motion 11
Cabinet Administration Interface 11
Cabinet User Access 11
System Data Flows 12
Torus System Components and Support Processes 12
Torus Security Features 13
Administrator Authentication 13
Logging & Reporting 14
TLS 14
Cookies & Sessions 14
Software Development Life Cycle (SDLC) Security 14
Secure Development 14
Change Control Process 14
Application Vulnerability Scanning 15
Penetration Testing 15
Security Policies 15
Risk Management 15
Access Control 15
Security Training 16
Physical Security 16
Visitors 16
Privacy 16
Privacy Contact Information 16
Certifications 16
Data Ownership & Retention 17
Revision Table 18

© CIC Technology Pty Ltd. All rights reserved.

Introduction

Torus is a sophisticated IoT solution for securely managing physical keys and other items. Information Security is a fundamental element of integrity for our products.

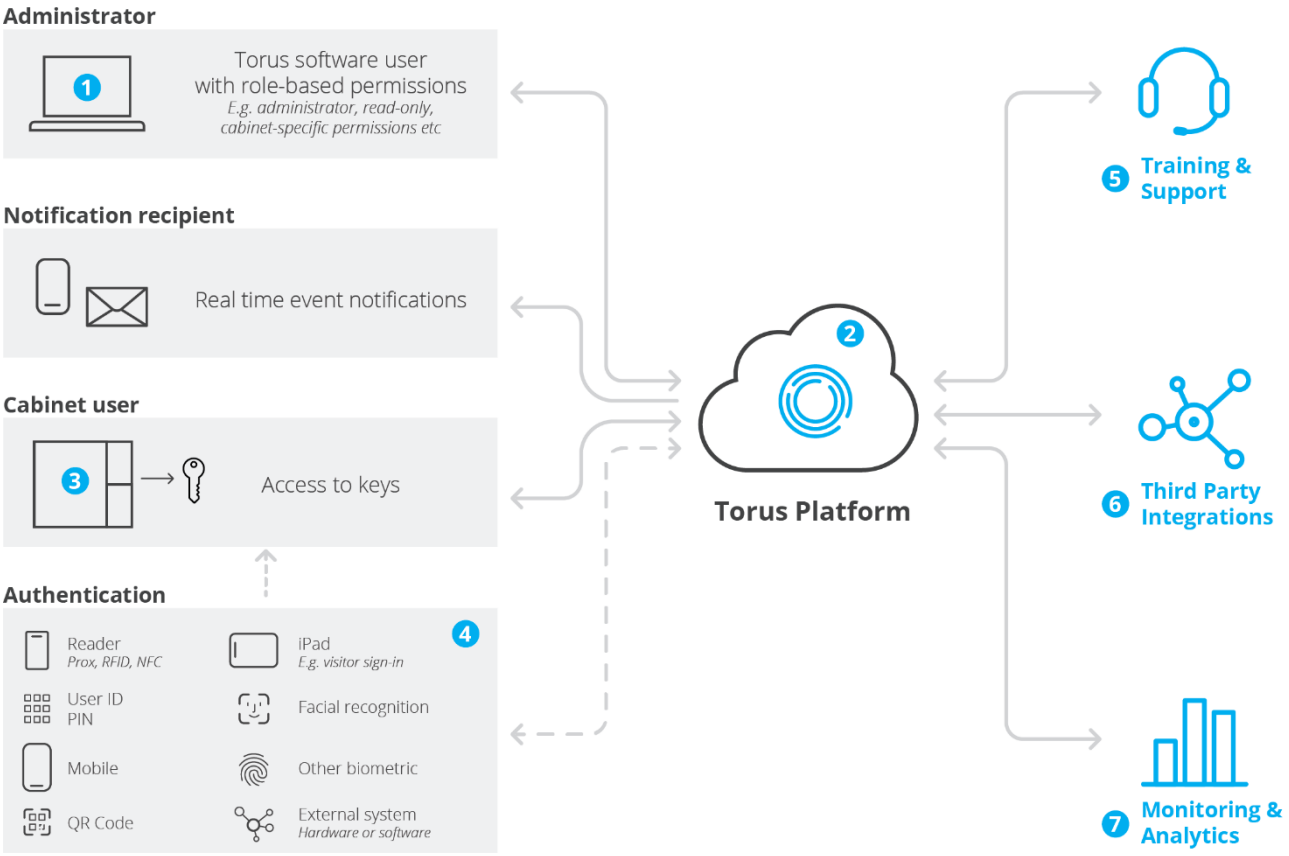
We use guidance from industry best practices and international regulatory requirements to employ a strategy for the controls in our security framework.

© CIC Technology Pty Ltd. All rights reserved.

Torus Architecture

Torus software is a physical security Software as a Service (SaaS) targeted at commercial and government enterprise workplaces with employee, resident, and visitor populations for whom Torus to keys (& other items) needs to be regulated and recorded. A cloud hosted system is an excellent fit for geographically distributed applications that span multiple properties.

Figure 1: Torus System Overview



As shown above in Figure 1, there are seven major components to the Torus solution:

1. Torus software (available via web browser)
2. Torus services are hosted with Microsoft Azure
3. Torus cabinet installed at customer premises using customer network (LAN) or Mobile connection (SIM)
4. Authentication of credentials via other devices and IT systems
5. Torus service & support, maintenance, and continuous monitoring.
6. Third-party API integrations
7. Continuous monitoring & analytics

These components share data across multiple platforms and networks in order to manage Torus control privileges, deliver alarm and event records and to provide other services such as software updates to Torus cabinets.

© CIC Technology Pty Ltd. All rights reserved.

Torus cabinets are networked to the cloud through wired or wireless connection. Wired options include an Ethernet port for connection to a corporate LAN, or broadband modem, or any other IP-based networking technology with connectivity to the Internet. Wireless networking options include a cellular modem that comes integrated with the Torus cabinet.

Account Management

The Torus key control life cycle begins with an administrator logging into the Torus software and setting up users, groups, credentials, schedules, and other security policy elements that dictate who has permission to which keys at which times. Any activity in an account performed by an administrator is logged in the journal report.

User credentials can be populated via a high-level integration (HLI) with third party systems (eg access control, credential management, contractor management, visitor management). Torus HLI ingests all required user credentials and associated access rights from the third-party system. Torus exports events and alarms, in real time to the third-party system. Depending upon the capability of the third-party software, the administrator will be able to manage and monitor access to keys and their current status via the third-party system, avoiding unnecessary duplication of effort.

Torus does not collect or store any personal identifiable information (PII) other than name, email address and phone number. There are no personal details such as home address, identification documents, banking or financial details.

Torus cabinets

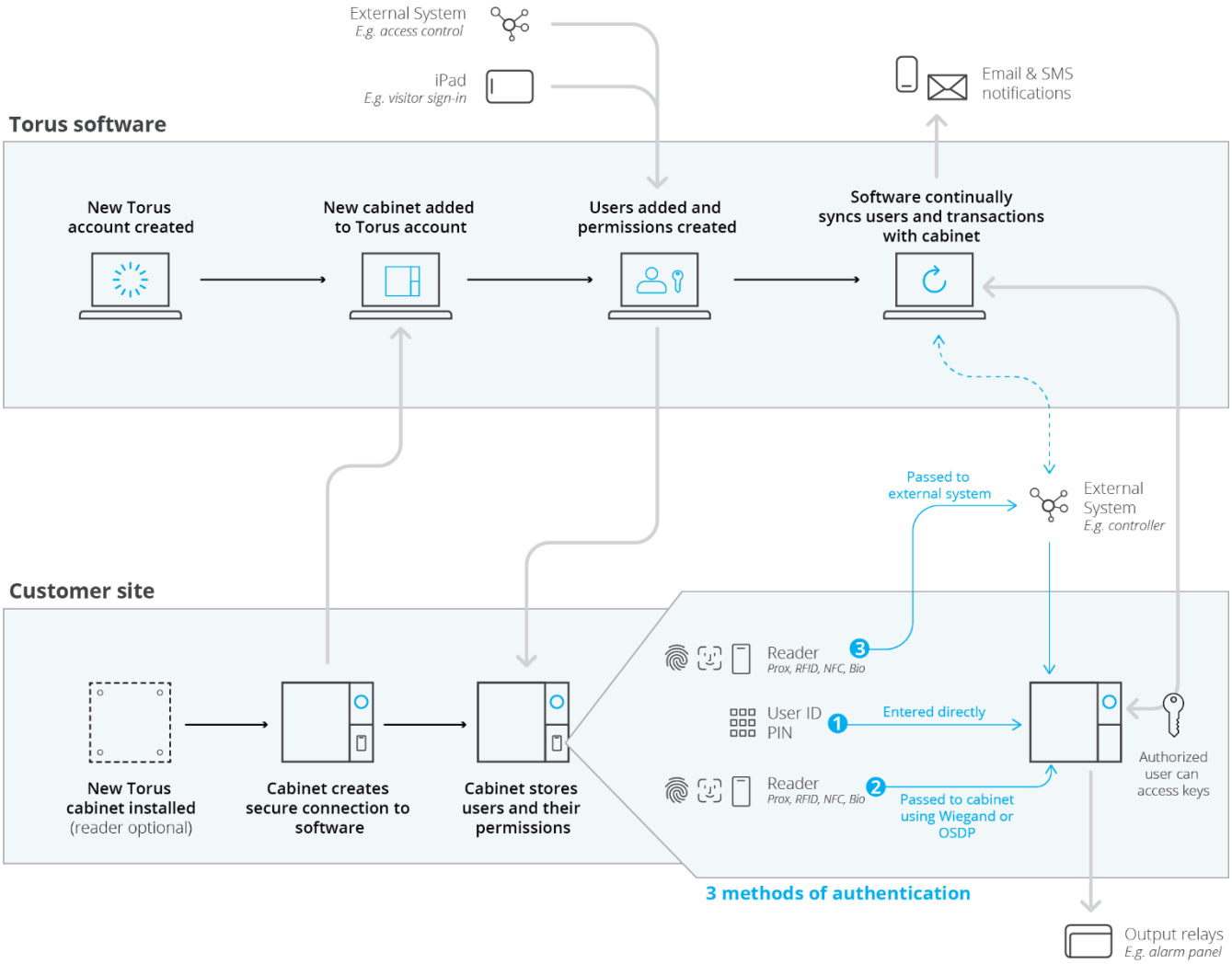
A Torus cabinet is installed by a Torus authorized reseller on the customer's premises. This cabinet is the interface between Torus cloud platform and third-party Torus devices such as credential readers. The cabinet's primary function is to secure keys until a user presents an authorized credential at the touch screen interface or at a credential reader and to monitor for any unauthorized openings of the cabinet.

The account and user data is stored in the Torus cloud platform. The cabinet, upon initial connection, will download the data files to approve or deny users access to the cabinet and the securely stored keys. The cabinet will establish a connection with the server and check regularly for new account data. If changes are made to users in the Torus account, an update is pushed to the cabinet from the server.

© CIC Technology Pty Ltd. All rights reserved.

Torus Process Flow

Figure 2: Data Flow for Torus Events



When a credential is presented to a reader, the reader will send the card data as a binary value to the Torus cabinet. The cabinet can make a local decision to unlock the door and will check with the Torus software if the credential is not stored in the cabinet database. If the request is not valid, access is denied and the cabinet door will not unlock. The cabinet will update the activity log with the event whether approved or denied.

In the event that the Torus cabinet loses an Internet connection, it will use a local cache of the account data that will allow the cabinet to operate based on its last configuration. When connectivity is restored, the cabinet will request and download any changes to the account and synchronize the events with Torus cloud platform.

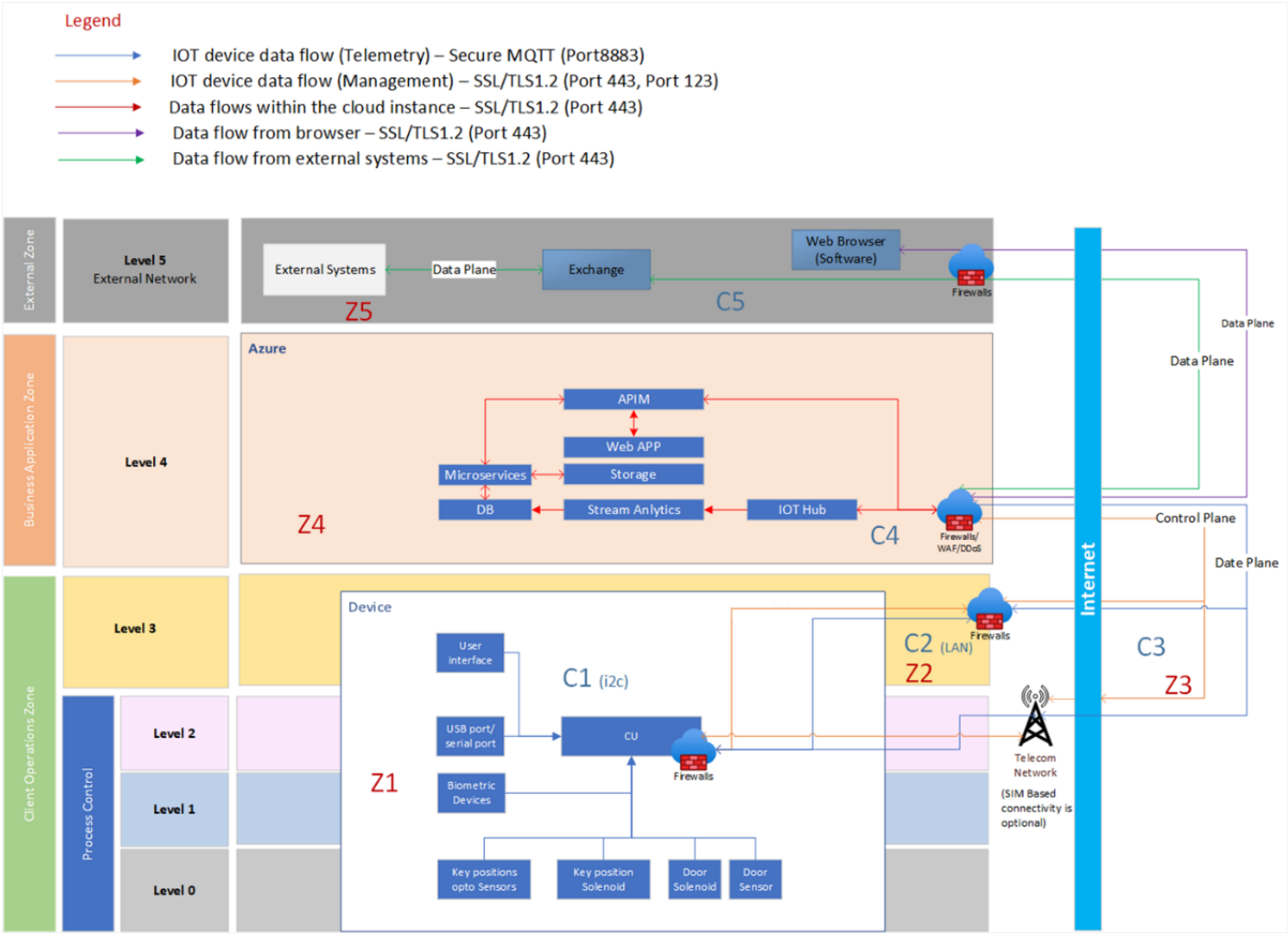
API Services

Torus offers API services for third-party integrations. Torus API uses multiple authentication methods including OAuth2.0 with cookie, REST API for external systems - Header authentication and Single Sign On with AD - OAuth2.0 with JWT. Administrators are provided the ability to selectively enable/disable API connections to their Torus account. All communications via APIs are encrypted using SSL/ TLS 1.2.

© CIC Technology Pty Ltd. All rights reserved.

Purdue Model

Figure 3: Data Segmentation of physical processes, sensors, supervisory controls & operations



© CIC Technology Pty Ltd. All rights reserved.

Cloud Computing Security

Torus is delivered as a multi-tenant model using secure logical controls to separate customer data. Torus leverages Microsoft Azure hosting services and other third-party solutions for a secure and resilient solution. Microsoft Azure has a comprehensive security program that Torus evaluates continually as part of its supply chain risk management program. Microsoft publicly provides details on their security program and data centers which you can find on their website https://learn.microsoft.com/en-au/azure/security/ including:

Data at rest

All Torus cloud data stores are encrypted at rest. Torus uses the industry standard AES-256 encryption algorithm to encrypt the data at rest for our databases. Data stored at rest in the underlying storage is encrypted, as are its automated backups, read replicas, and snapshots. Microsoft Azure Key Vault is used to store credentials.

Resilient Design

To provide high availability of our services, Torus uses a modern, resilient design for applications and services. Torus utilizes serverless functionality. Torus inherits multiple layers of resilience from the infrastructure provided by Microsoft Azure. Torus is run on highly available, fault-tolerant infrastructure spread across availability zones. Microsoft Azure manages all the administration, maintenance, and patches of the infrastructure without any impact to Torus availability. Serverless architecture enables Torus to have continuous scaling of our application by running event triggered code in parallel and processing each event individually.

Torus API and utility services are built as micro-services which are to be replicated across Microsoft Azure data centres and regions. This enables Torus to seamlessly release updates to services and provide services in the event of an Azure zone outage. Backup snapshots of our database are performed every 4 hours. Torus annually updates and tests our processes and backup restoration to ensure efficient incident response and disaster recovery is available.

Torus cabinets will cache up to 100,000 events (using first in first out method) that occur during a disruption of communication to Torus servers and will upload that data once the connection is restored. The cabinets will use this cache to continue to make control decisions while disconnected.

Continuous Monitoring

Torus has a suite of tools used by our operations staff to monitor critical systems. These tools create baselines for system performance and alert staff when performance is abnormal. These alerts could signal an upcoming service disruption, or a potential security event. We have 24/7 alerting and ability to respond to these alerts with procedures for activating incident response and disaster recovery plans.

Vulnerability Scanning

Torus uses vulnerability scanning tools, including Microsoft Defender for Cloud, to assess the environment. These tools automatically update their signatures and scans systems daily to potentially identify any flaws in their configuration or installed operating system and services. The tool alerts our security and operations teams on new vulnerabilities for investigation and remediation.

System Maintenance/Patching

Microsoft Azure manages all the administration, maintenance, and patches of the infrastructure without any impact to Torus availability.

© CIC Technology Pty Ltd. All rights reserved.

For the rest of Torus's architecture, Torus performs patching in order to keep systems up to date and minimize vulnerabilities. In the event of a high-risk patch identified by a security advisory or vulnerability scan, we create a mitigation plan, test the proposed mitigation in a non-production environment and, if no issues arise, deploy those updates to production with no downtime.

Multi-Tenancy

Torus logically separates customer accounts within the database. When an account is created, it is tied to a unique identifier that is hidden to the end-user. When any action is done on an account, the unique identifier and valid credentials are needed. Torus administrators can be granted different levels of privileges for reading, modifying, or deleting user groups or sites within the account.

Network Security

Torus configures logical networks in Azure using built-in security features. Environments are logically separated through the use of different Azure accounts and services are interconnected through private APIs within Azure... Torus leverages Azure's secure network, hardware, and automatic encryption of all traffic on the global and regional networks between Torus instances.

Web Application Firewall (WAF)

Torus uses a Microsoft Azure Web Application Firewall (WAF) in addition to the built in network security features to monitor and restrict traffic flowing to Azure resources. The WAF is set up with rules to deny traffic that is from known bad reputation IP addresses. The Azure WAF policies are continually updated to prevent known risks.

Intrusion Detection System (IDS)

For our serverless architecture, Torus uses a runtime protection tool that can block code/SQL injection attempts and unauthorized executables, as well as detect indications of compromise (IoCs). The architecture is based on microservices heavily relying on Azure APIM which has WAF protection against common web attacks, such as SQL injection, cross-site scripting (XSS), and other known vulnerabilities. These WAF rules are customized, configured, and monitored to deliver a secure microservices based application.

Office Network

Torus's office networks use logical separation of departments through subnetting. Network firewalls only authorize the ports necessary to provide services. In the event of a disaster, employees are able to work from home to continue maintaining services and providing support to end users.

Remote Work

Torus employees and contractors must use a Torus-managed VPN to access network resources when remote and some sensitive systems when on location. Use of this VPN allows another layer of Torus control, logging, and encryption for employee network traffic.

Torus cabinet Security

A Torus cabinet contains a microprocessor, memory, and I/O interfaces that allow it to interconnect to credential input devices such as readers. There are various sizes of Torus cabinets which possess the same electronics, firmware and security credentials.

© CIC Technology Pty Ltd. All rights reserved.

Data at rest

Data at rest in the Torus cabinet is encrypted. The encryption method used is AES256 encryption algorithm.

Networking

The Torus cabinet initiates all communication sessions with the Torus server. The IP address assigned to the cabinet does not need to be a static or routable IP address. This means that the Torus cabinets will operate with routers and firewalls configured to use Network Address Translation (NAT).

Cabinets require outbound HTTPS traffic (TCP port 443) open to connect to Torus servers. Cabinets will not accept inbound connections, they will only listen to network traffic within the HTTPS session which was initiated by the Torus cabinet itself. For networks with a proxy server, cabinets have built in support for the SOCKS 5 and HTTP proxy protocols.

Bot Detection

Torus cabinets monitor their connections and are only permitted to connect to specific listed URLs using specific service protocols. If at any time the cabinet is redirected to a non-Torus server, the cabinet would not allow the connection and would alert the Torus server. This is to prevent a process (bot), which was planted on a cabinet to create a cyber-attack such as denial-of-service (DoS attack).

Data in motion

All Torus cabinets exchange credential and event information with the Torus data center. Torus uses digital certificates described by the ANSI X.509 specification for public key infrastructure (PKI) systems. For Torus cabinets, Torus acts as its own CA because it can guarantee a physical chain of custody during the installation of certificates into Torus cabinets during our manufacturing process, and because there are no third parties communicating with those cabinets who need to be part of the authentication process.

Torus cabinets communicate via TLS1.2 with AES 256-bit encryption and Digital Signature Algorithm (DSA) verified SHA256 digital certificate signed with a key length of either 1,024 or 4,096 bits, depending on the device. Cabinets establish a TLS session with Torus before exchanging information. When establishing a TLS session, the cabinet and the server validate each others' certificate to authenticate their identity.

Cabinet Administration Interface

The cabinet administration interface in Torus software is only accessible by a direct connection to the cabinet. Cabinets provide a high level of physical security but should be installed in a secure location to prevent tampering with the hardware. The Torus software requires a username and complex password which can also be integrated with Microsoft Active Directory credential management (or other such systems). This interface does not allow for opening of a cabinet door. The data available in the interface includes device settings such as networking configuration and logs of all activity.

Cabinet User Access

The cabinet is able to be accessed via a USERID (numeric with a minimum of 6 characters and up to 20) and is associated with a numeric PIN which is configurable up to 6 digits. Other options include access control proximity card and a any biometric devices which are able to connect using OSDP, Wiegand or via IP/software.

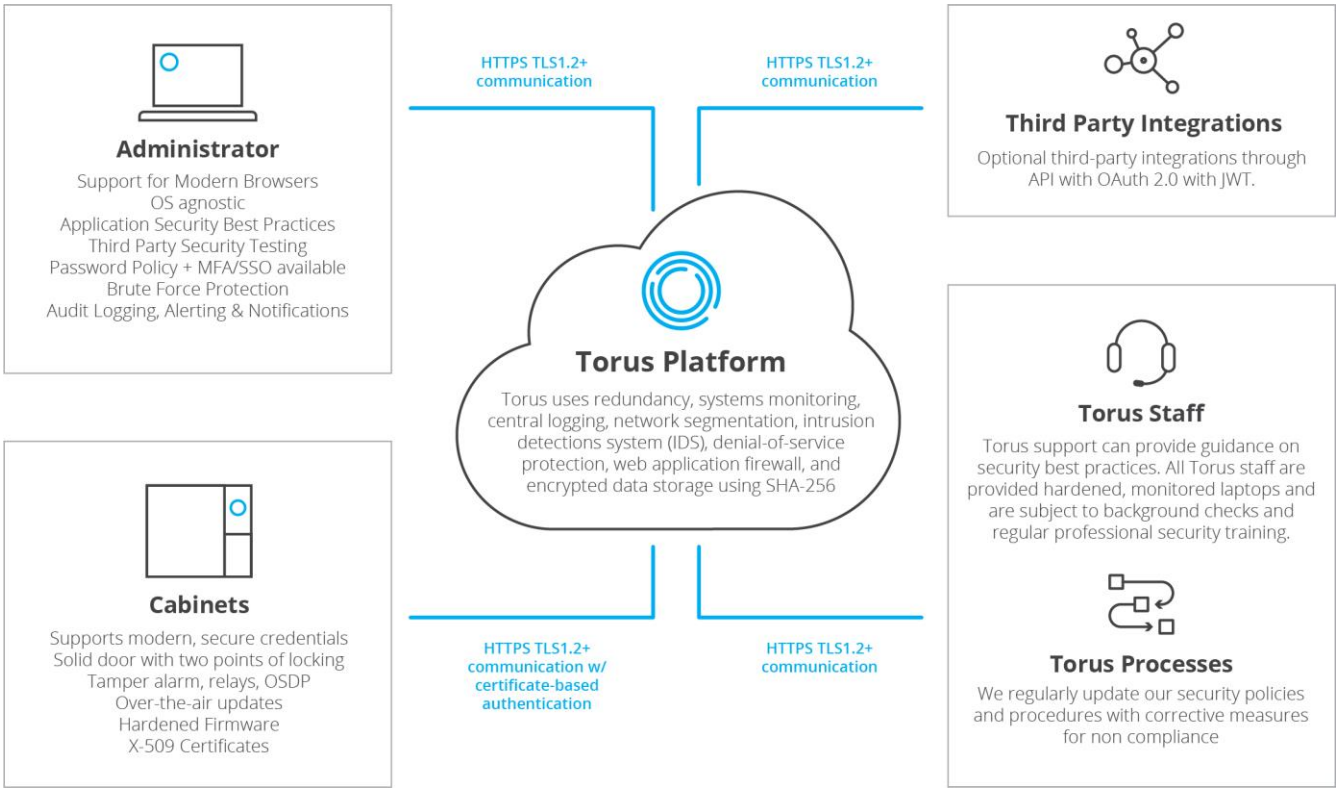
© CIC Technology Pty Ltd. All rights reserved.

System Data Flows

Torus System Components and Support Processes

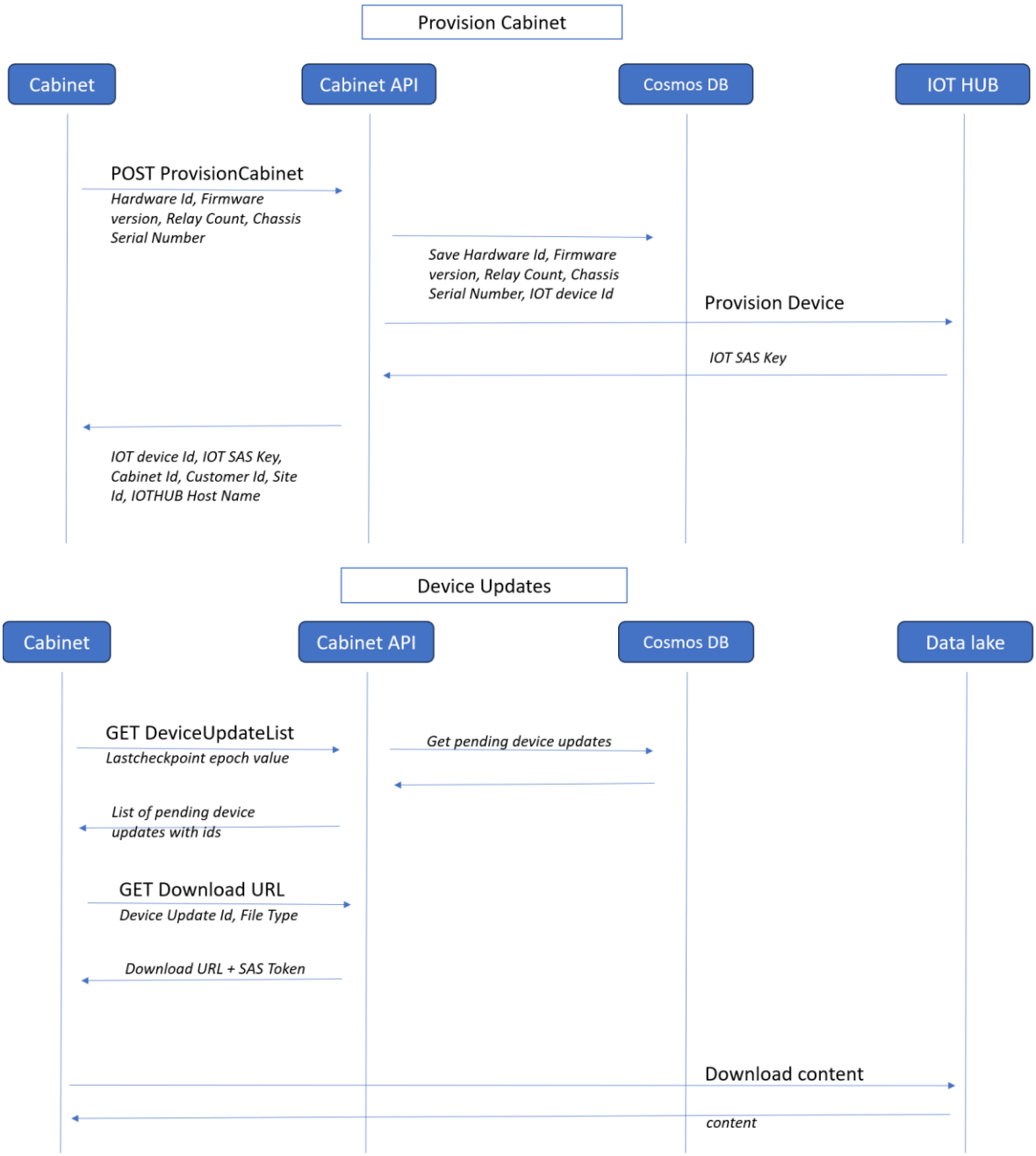
The following diagram depicts the data flows between major system components and the layered protections provided for each element.

Figure 3. Torus System Components and Support Processes



© CIC Technology Pty Ltd. All rights reserved.

Figure 4. Torus API Sequence Flows



Torus Security Features

Administrator Authentication

An administrator is a Torus user with privileges to sign into the Torus software and observe or make changes to an account that controls one or more cabinets. Torus authenticates administrators by an email address and password. These are entered on separate pages to avoid 'brute force' attacks. The password policy is the following:

© CIC Technology Pty Ltd. All rights reserved.

- Passwords may be between 8 and 128 characters in length and must contain Lower case (a-z), upper case (A-Z) and numbers (0-9)
- Passwords cannot be compromised credentials from a third-party data breach. Users will be notified if their credentials were breached and asked to change their password before logging in.
- Passwords may not be reused

Torus offers and recommends administrators to enable two-factor authentication on their account. This feature requires all administrators within an account to set up two factor authentication. Torus two-factor authentication uses one-time passwords (OTPs) as an authentication factor.

Torus authentication services have two types of brute-force protection. The first blocks an IP address when it makes a high number of login attempts targeting too many different accounts. The second occurs if a user attempts to log in consecutively fails 10 times, future login attempts for the username will be blocked and an email will be sent to the administrator to unlock themselves.

Logging & Reporting

All administrator activity is logged and available for reporting. All Torus cabinet events are logged and available for reporting. Torus administrators with sufficient permissions can download their data by running reports. All data is retained per the Terms of Use for Torus Services https://torus-technology.com/us/terms/

TLS

Torus supports TLS 1.2 connections, and we recommend users to keep their browsers updated to get the best possible TLS encryption options.

Cookies & Sessions

Torus uses sticky sessions to maintain state information and provide a continuous experience to clients. To use sticky sessions, the clients must support cookies. Cookies have the secure flag enabled so they are transmitted via HTTPS. Session's timeout after two hours of inactivity. Regardless of activity, users must log back in every 14 days.

Software Development Life Cycle (SDLC) Security

Torus uses security best practices throughout the Software Development Life Cycle (SDLC). This means that security is included throughout phases of development and deployment.

Secure Development

Torus engineers are required to develop according to the OWASP Top 10 vulnerabilities and how to mitigate them through secure coding practices. Engineers have a plugin in their integrated development environment (IDE) to highlight security best practices or vulnerabilities that need to be remediated inline as they are writing code. Engineers can also create a sandbox on their machine to perform static application security scans on files they are working on so they can remediate any flaws before submitting a release for QA. The security team and management track the progress of training and results of sandbox scans.

Change Control Process

The development, QA and production environments are logically separated in the cloud. In order to submit any releases to QA or production environments, Torus has a change control process to ensure that every release meets the criteria as set forth by management. This process requires every release to be documented with changes before submitting to the QA environment. Once in the QA environment, the release is tested through

© CIC Technology Pty Ltd. All rights reserved.

automated tools and manual input. Those results and the documentation must be approved by an engineering manager & Chief Operating Officer prior to being released to production and the approval is documented.

Releasing to production generally does not cause any outage of services due to the resilient design of our environment. Once deployed, regression testing is performed and any issues are resolved by either roll back or roll forward as determined by the engineering team.

Application Vulnerability Scanning

Torus uses static analysis and source component analysis to identify any vulnerabilities within Torus software and our supporting services. Microsoft Defender for Cloud is used to continually assess the potential vulnerabilities which may arise.

Static analysis scans are done automatically with every build of our applications. Static analysis tests the application's source code for any vulnerabilities including OWASP Top 10, CVEs, etc.

Source component analysis is built into our static analysis scans and reviews the usage of third-party libraries to check their version and licensing which it checks against a constantly updated vulnerability database to determine if the libraries have any known vulnerabilities.

Penetration Testing

Torus continually utilises Microsoft Defender for Cloud to conduct vulnerability and penetration testing. We also periodically use external third-party provider to conduct penetration tests for major platform updates. These tests aim to discover vulnerabilities and exploit these vulnerabilities to gain unauthorized Torus to data or systems. Any results received are prioritized according to risk-rating for remediation and follow-up testing. The goal is to have no critical, high or medium risk vulnerabilities after remediation.

Security Policies

Torus has security policies as approved by an internal Information Security Team (IST) including

members of senior management. These security policies are based on best practices and are audited by a third party annually as part of our ISO 27001 assessments.

Risk Management

The IST reports risks to the Risk Management Committee (RMC) at least half yearly. The RMC is composed of the executive leadership team and is responsible for making any business decisions with regards to risk. Annually, the RMC reviews an organization risk assessment together and creates an action plan to mitigate risk where needed.

Access Control

The Torus policy around access control requires access to be granted using role based and least privilege principles. Prior to granting access, Torus employees are screened in an interview process, undergo a background check, sign confidentiality clauses, acknowledge the employee handbook, and complete security awareness training. Sensitive systems access is reviewed quarterly. Access is revoked immediately upon termination. Torus requires the use of two-factor authentication and single-sign on (SSO) using Microsoft Azure Active Directory.

The password policy requires passwords to be at least 8 characters in length and must contain at least 2 of the following 4 categories: Lower Case, Upper Case, Digit, Non-Alphanumeric. Password hygiene training is available

© CIC Technology Pty Ltd. All rights reserved.

for all employees and included in security awareness training. Torus system administrators are required to change default passwords on all systems to passwords that meet the requirements in this policy.

Customer support teams perform authentication for callers using probing questions and/or an email from the account on file to verify the caller identity prior to divulging any information or performing any actions on an account.

Security Training

Torus provides security training for employees including a security awareness program for all employees that is attended during onboarding and annually thereafter. The Security Awareness program includes, but is not limited to, physical security, safety, account management, social engineering attacks, data classification and information handling, security policies, and how to report security events. The training is updated annually and delivered annually via a training system with a test to assess comprehension.

Physical Security

Torus offices are secured at the building and office level with access control systems. Torus employees are granted Torus access cards with the minimum access needed to perform their duties.

Visitors

Visitors are required to sign in using an electronic visitor management system and are not granted access to office areas unless escorted by an authorized Torus employee.

Privacy

Torus does not collect or store any personal identifiable information (PII) other than name, email address and phone number. There are no personal details such as home address, identification documents, banking or financial details.

Torus values the privacy of our end users and we are transparent with our privacy policy. For our privacy policy in regards to business practices and the use of the Torus website, please review our Privacy Policy as found on our website (https://torus-technology.com/us/privacy-policy/). For the specific privacy policy surrounding the use of Torus services, please see our Privacy Statement as found on our website (https://torus-technology.com/us/terms).

Privacy Contact Information

If you have questions regarding Torus Privacy Policies or if you need to request Torus to or update, change or remove personal information that we control, you can do so by contacting the Torus Privacy Officer privacy@torus-technology.com

Certifications

Torus is designed and produced by CIC Technology Pty Ltd, which is a ISO9001 and ISO27001 certified organization. Torus has been certified by Global Risk Exchange (Cyber GRX) and approved by Telstra Corporation Ltd

© CIC Technology Pty Ltd. All rights reserved.

Torus inherits the following certifications from using Microsoft Azure development stack and server infrastructure:-

- Tier 4 data center
- ISO/IEC 27001 & ISO/IEC 27018
- SOC1&2
- HIPPA

Microsoft Azure provides certification for Australia IRAP. An IRAP assessment has been completed for the Azure in-scope services for the processing of government data in Australian regions up to and including the PROTECTED level. Extra compensating controls are to be implemented on a risk-managed basis by individual agencies prior to agency authorization and subsequent use of these cloud services.

Through the previous Australian Government certification process, Azure was IRAP assessed and certified by the ACSC at both the Unclassified Dissemination Limiting Marker (DLM), now OFFICIAL: Sensitive, and PROTECTED levels. This process resulted in Azure being included on the CCSL, which was used to identify cloud services that had successfully completed an IRAP assessment and were awarded certification by the ACSC. Following the closure of CCSL in July 2020, Microsoft will continue to have Azure cloud services assessed by an IRAP assessor, while agencies can continue to self-assess or procure the services of an IRAP assessor to assess their own systems deployed on Azure. Commonwealth entities remain responsible for their own assurance and risk management activities. Agencies can engage the ACSC through their normal channels for assistance with this process.

Data Ownership & Retention

The data is owned by the customer. The customer is able to download all of the data in their account at any time by using the Reports feature and downloading as xls files.

Data is accessible for reporting for 12 months. It is then archived for up to 5 years.

For customers who use Torus as an integrated solution with their access control or other third party system, the transactional and events data from Torus will also be reportable and retained in those systems.

© CIC Technology Pty Ltd. All rights reserved.

Revision Table

Version	Date	Author	Content
1.0	02/02/2023	SA	Original Final Draft
1.1	11/08/2023	AA	Purdue Model
1.2	04/12/2023	AA	Password updates
1.3	20/02/2024	TL	Cabinet access
1.4	05/03/2024	SA	Security Training
1.5	15/03/2024	SA	Data retention
1.6	12/07/2024	TL	VAPT
1.7	31/08/2024	TL	Cyber GRX
1.8	17/11/2024	TL	Password updates
1.9	29/11/2024	AA	API sequence flows

© CIC Technology Pty Ltd. All rights reserved.