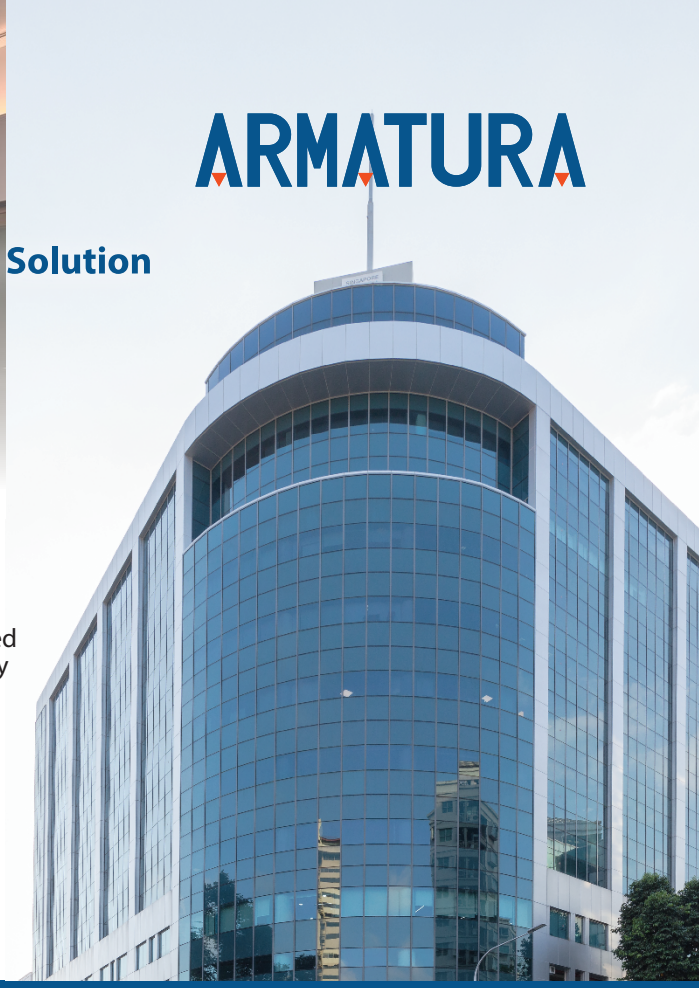


Internal Use Only

ARMATURA

Ultimately Advanced and Integrated Security Solution for Singapore Pools



About Client

Established in 1968, Singapore Pools is a world-class, state-owned lottery and gaming operator in Singapore. As the country's only legally authorized provider of lotteries and sports betting, it manages a vast network of retail outlets and advanced digital platforms. Operating under strict government supervision, Singapore Pools acts as a crucial financial contributor to local community, charity, and sports development. Serving an organization of this national scale requires an absolute commitment to regulatory compliance and the highest standards of physical and digital security.

Requirements

As a highly sensitive public lottery and gaming organization, Singapore Pools handles massive financial transactions and public data on a daily basis. With the enforcement of Singapore's Personal Data Protection Act (PDPA), regulatory bodies have imposed exceptionally strict compliance standards regarding the collection and protection of sensitive personal data, such as biometric traits (facial and palm templates). Any data breach could subject the organization to staggering fines of up to millions of SGD, along with irreversible damage to its corporate reputation.

Faced with the dual pressures of physical security threats and stringent legal regulations, the client urgently needed to upgrade the security architecture of its headquarters. Their core concerns were centered on the following four dimensions:

Eliminating Vulnerabilities to Physical Intrusions

Traditional access control terminals are installed outdoors or in public corridors. The client was deeply concerned that intruders might leverage brute force to vandalize the terminals and short-circuit the internal wiring to gain unauthorized entry into restricted zones. Therefore, the new system had to completely eradicate this physical vulnerability—where a destroyed device results in an unlocked door—ensuring that high-security areas remain airtight.

Mitigating Regulatory Non-Compliance and Data Leakage Risks (Core PDPA Concerns)

To satisfy rigorous PDPA compliance audits, the client's biggest anxiety was: How do we ensure that employee and visitor biometrics remain absolutely secure across every single stage of collection, transmission, and storage? The system required top-tier cybersecurity encryption. Furthermore, terminals accessible to the public must not store any user databases locally, eliminating the risk of a massive compliance disaster should a device be stolen. The visitor registration workflow also needed an explicit, legally sound mechanism for capturing informed consent.

Preventing Operational Disruptions Caused by System Downtime

As an organization operating on a 24/7 basis, even a single second of system failure or server crash could paralyze access control across the entire building, bringing operations to a standstill. The client could not afford the security blind spots and commercial losses associated with a single point of failure. Consequently, the system demanded extreme stability and near-instantaneous disaster recovery capabilities.

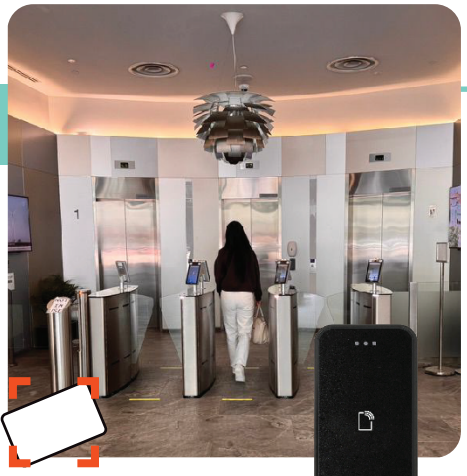
Dissolving Information Silos to Drive Automated Operational Efficiency

The building's internal Office Automation (OA) system, legacy video surveillance, and card printing equipment operated completely independently. The client wanted to prevent employees from spending valuable time manually re-entering data across multiple, disjointed systems. This manual overhead was not only inefficient but also heightened the risk of accidental privacy data exposure. They required an intelligent platform capable of maximizing their prior infrastructure investments while achieving seamless, automated orchestration.

Internal Use Only

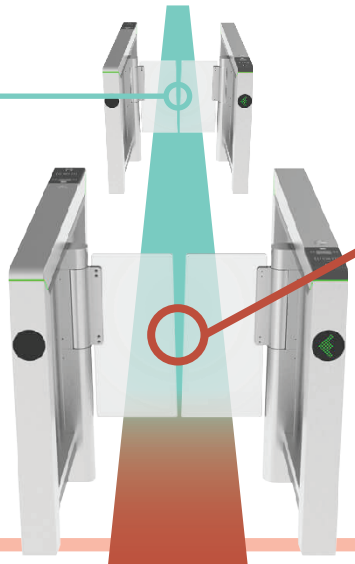
Access Control

Solution Details



Card Verification

EP10





FT10CMQ



OmniAC30



To better fit the access control system into the ambience of Singapore Pools's ambience, All OmniAC30 terminals' display have been fully customize to reflect the visual identity of Singapore Pools, including the background color, organization logo, and greeting messages.

General Area

For general access control of the lobby and each floor of Singapore Pools's office building, Armatura deployed EP10 multi-tech smart card readers, which are integrated with ZKTeco's Mars-S1000 swing barriers, and together centrally managed by Armatura One comprehensive security management platform. On Armatura One, all employees are registered with their personnel profiles, including employee information and specific biometric data for identity authentication, and are issued RFID cards as their staff cards. To access or exit the building and the floors, employees are required to swipe their cards on the EP10 card reader for identity authentication. Also, upon passing through ZKTeco's Mars-S1000 swing barriers, the built-in infrared sensors also prevent tailgating intrusions actively.



Facial Recognition or Palm Recognition

Restricted Area

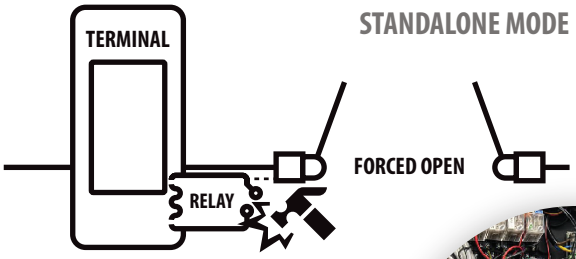
For specific zones on each floor requiring high-intensity security, OmniAC30 or FM10CMQ biometric standalone terminals are deployed for biometric verification. When employees register on Armatura One, their profiles include facial and palm recognition data in addition to basic information. Only employees with the corresponding access privileges can enter or exit using palm or facial recognition.

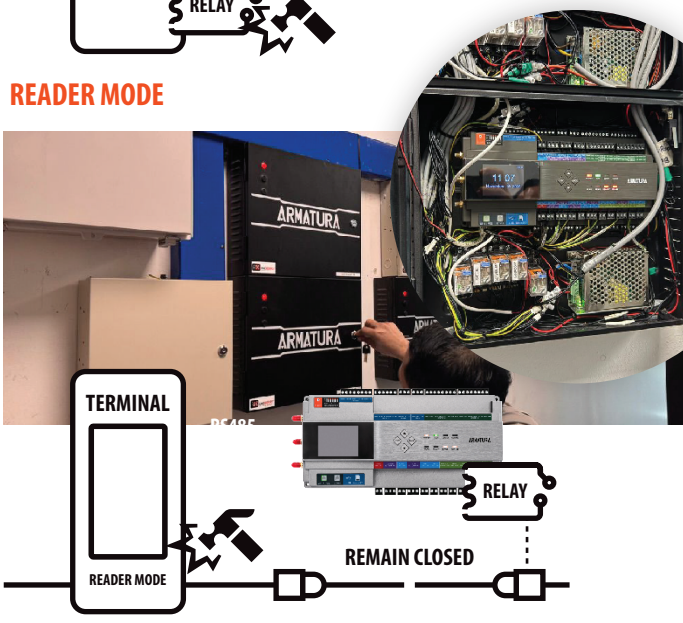
Customized Reader Mode Conversion

By default, both OmniAC30 and FT10CMQ are fully featured, independently operating standalone terminals capable of performing identity matching, recognition, privilege determination, and door lock/unlock control on their own. As high-specification access control equipment, both the OmniAC30 and FT10CMQ feature tamper alarm functionalities; if subjected to violent disassembly or vandalism in an attempt to gain illegal entry, they will instantly sound an alarm and dispatch notifications to security personnel.

However, given the highly sensitive nature of Singapore Pools' business, the probability of attracting illegal intrusion is significantly higher. Even if security personnel receive immediate notifications, they might still fail to intercept intruders in time, resulting in assets loss that can only be followed up after the fact. To guarantee strict compliance with PDPA security regulations and minimize security risks, Armatura configured both models into "reader mode."

Through RS485 communication, the terminals connect to AHSC-1000 controllers, which then link back to Armatura One. Consequently, the mechanism responsible for controlling the opening and closing of the swing barriers shifts from the built-in relay inside the standalone terminal to the relay inside the AHSC-1000 controllers. These controllers are housed in highly secure locations that are not exposed to physical tampering, such as protective enclosures inside the security room. Therefore, even if intruders break the OmniAC30 or FT10CMQ terminals at the cost of being immediately detected, they cannot successfully trigger the barriers to open by forcing the terminal's internal relay, because the lock-controlling relay is completely absent from the terminal itself.





Internal Use Only

Visitor Management

Visitor Self-Service Registration

To enhance the efficiency of visitor management, Armatura integrated ZKTeco's FaceKiosk-H13C biometric smart kiosks and HID FARGO HDP6600 card printers with Armatura One, to enable quick and convenient visitors' self-service enrolment. Visitors are enabled to quickly self-register their visitor profiles and biometric data in the FaceKiosk-H13C, and upon successful completion of registration, Armatura One automatically transmits the data to the HID FARGO HDP6600 to instantly print the physical access cards of the visitors.

Customization
Consent of Biometric Feature Collection



To ensure PDPA compliance, the ZKTeco FaceKiosk-H13C requires visitors to provide their explicit consent prior to registration, ensuring the lawful collection of their biometric features used for identity verification.



AHSC-1000



Self Enrolment

ZKTeco
FaceKiosk-H13C



ARMATURA



HID
FARGO HPD6600



Card Printing

Visitor Profile

Integration and Data Interconnection with Existing OA System

Visitor arrivals must first be requested by employees via their internal office automation system. Within this solution, although the visit request and the automated visitor registration are completed by two separate systems, Armatura One is seamlessly integrated with the office automation system. Due to this data interconnection, employees do not need to log into Armatura One separately to handle visitor registration; Armatura One can automatically match profiles during visitor check-in, successfully streamlining the entire visit registration and access credential provisioning workflow.

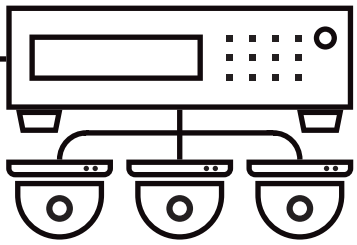
Singapore Pool
Office Automation System



Visit Booking

Video Surveillance

Third-party Network Video Recorder

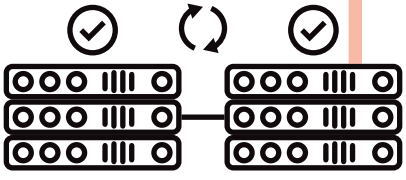


Third-party Camera | Third-party Camera | Third-party Camera

Given that the building already possessed a complete and well-functioning pre-existing third-party video surveillance system—including cameras and network video recorders (NVRs) installed throughout the premises – Armatura integrated the entire surveillance system into Armatura One, enabling real-time data interconnection between the two systems. All live video feeds can be monitored in real time on the video surveillance interface of Armatura One, and all historical surveillance logs can be audited within Armatura One at any time.

Furthermore, Armatura leverages the native facial recognition capability of the third-party video surveillance system to enhance protection against potential illegal intrusions. If a visitor is identified within a zone where they do not possess access privileges, the system instantly dispatches an alarm notification to management personnel.

High-Availability



ZKTeco ZKBio HA

To maintain continuous and seamless operation of the system, Amratura On is integrated with ZKBio HA – a high-availability cluster with dual servers running in parallel. All data between the servers is continuously synchronized, and each server monitors the other's health status. If one server fails, a failover is triggered immediately, and all operations are transferred to the healthy server, ensuring uninterrupted system operation, minimizes downtime, and reduces the risk of data loss or service interruption.

Internal Use Only

Functions & Advantages

Comprehensive Security Protection

High-Security and High-Efficiency Access Control

AES-128 Encrypted Card Access Control

Armatura's solutions are highly flexible, enabling composition and integration of different devices and systems to accommodate diversified needs of the clients' scenarios. For the general access of Singapore Pools's office building with comparatively larger daily people flow and lighter security risks, EP10 multi-tech smart card readers can be utilized. With AES-128 encrypted card data to prevent illegal duplication, and card reading speed as quick as below 0.1 second, both security and efficiency of access are well balanced.

Advanced Biometric Access Control

For the restricted areas with high security needs, advanced biometric authentications are deployed. Both the OmniAC30 and FT10CMQ are contactless biometric security standalone terminals equipped with facial and palm recognition capabilities. Boasting powerful recognition functionalities, both terminals can complete facial recognition within 0.3 seconds (with a recognition distance and angle up to 10 feet and 30°) and palm recognition within 0.35 seconds (with a recognition distance and angle up to 1.6 feet and 60°). Concurrently, both machines feature Liveness Detection; their infrared light sensors verify whether the presented face or palm belongs to a real living person rather than a fake artifact, completely closing the loophole of spoofing vulnerabilities.

Ultimate Situational Awareness with Flexible and Feature-rich Access Control Management

As a web-based and all-in-one security platform, Armatura integrates multiple systems and devices including access control, video surveillance and office automation. Security personnel can manage the system anytime and anywhere, with support for over 100 global linkages across hardware and software, as well as real-time monitoring of all access events. Thus, Armatura One can interlink and integrate with various subsystems and hardware via multiple methods, including native SDKs, ONVIF, and TCP/IP. This orchestrates powerful security workflows such as Global Anti-Passback, Global Interlocking, and proactive monitoring & alerting, effectively and significantly enhancing the overall situational awareness of the security ecosystem.



Integrating Existing Equipment and Systems to Enhance System Efficiency

Beyond delivering robust security protection, the powerful integration capabilities of the Armatura solution unlock the latent potential of pre-existing equipment. For example, integrating the high-performance HID FARGO HDP6600 card printer with Armatura One and the ZKTeco FaceKiosk-H13C visitor self-service registration kiosk further automates the visitor registration and credential issuance process. In addition to accelerating the overall workflow, this automation reduces errors that may result from manual data entry. Furthermore, data exposure caused by manual visitor profile handling by staff is minimized, effectively safeguarding visitors' personal privacy.

Moreover, Armatura One's formidable ability to integrate with third-party systems allows it to link with Singapore Pools' office automation system and video surveillance system. Through APIs, real-time data interconnection across systems is achieved, eliminating the need for employees to constantly switch between or log into different systems. Instead, they can carry out simple and highly efficient management from a single, fully featured interface.

Strong Cybersecurity for Privacy Protection

Armatura treats data as a critical asset that demands stringent protection, particularly given the sensitive nature of identity, biometric, and access-pattern information.

TLS 1.2 encryption

All communication between OmniAC30, FT10CMQ terminals and servers is protected using TLS 1.2, creating a secure tunnel that resists eavesdropping and man-in-the-middle attacks.

EAL6+ secure crypto chip

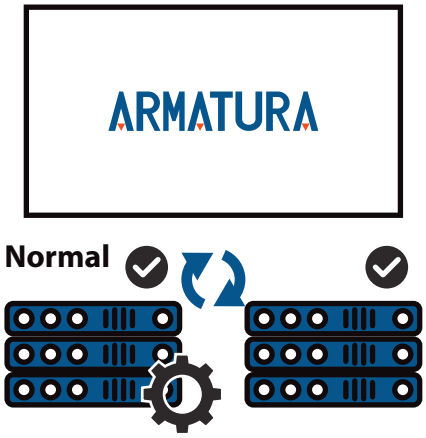
Devices are equipped with EAL6+rated cryptographic chips that provide a high-assurance environment for key management and critical cryptographic operations, guarding against physical tampering.

AES-128 and AES-256 biometric data encryption

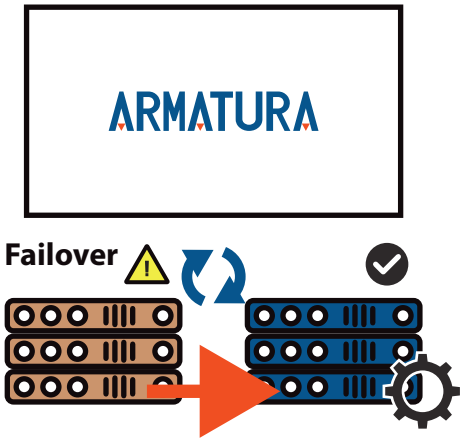
All card data and biometric data transmissions are secured with AES-128 and AES-256 encryption specifically. Data is segmented into small chunks, each encrypted and transmitted through a secure channel with pre-negotiated keys, ensuring that only authorized recipients can decrypt and access the information. This architecture protects user privacy and the integrity of biometric data.

Internal Use Only

Robust Redundant System Architecture



Designed with high availability in mind, Armatura One supports clustering so that multiple servers work together, continuously monitoring one another's status. In the event of a server failure, automatic failover transfers the workload to another server with synchronized data and configuration, minimizing downtime and ensuring that the security system remains available. This reduces the risk of data loss and system crashes, which is critical in regulated environments like data centers and pharmaceutical facilities.



Flexibility of System Expansion and Integration for Optimal Cost Efficiency

Armatura's products possess strong integration capabilities and can seamlessly integrate with different equipment and systems. If scale expansion is needed, there is no need of a replacement of new system. Instead, simple connection of the newly added devices to Armatura One for integration is enabled. Armatura One, using an MQTT-based communication protocol, can communicate with more than 10,000 edge devices (controllers, door units, readers, sensors, etc.) and manage over one million users within a straightforward network environment. This ensures that future requirements—such as new authentication methods, additional devices, or expanded facilities—can be accommodated without fundamental redesign of the security architecture.

Furthermore, Armatura's solutions are built for seamless integration with third-party systems, enabling seamless data synchronization with Armatura's access control and other modules without extensive manual re-entry. Where needed, Armatura One integrates existing systems via RESTful APIs, SDKs, or other suitable mechanisms, preserving prior investments and adding new functionality. For example, integration with a third-party video surveillance system allows access-control events or security anomalies to automatically trigger live monitoring and recording on associated cameras. Integration with an office automation system (OA) enables real-time access data to support more efficient operations. Value-adding enhancement of the existing system is thus enabled without total replacement of hardware and system to optimize cost effectiveness.

Address:190 Bluegrass Valley Parkway, Alpharetta, GA 30005
Phone: + 1 (470) 816-1970
Email: sales@armatura.us
Website: www.armatura.us
Copyright ©2026 Armatura LLC @ARMATURA, the ARMATURA logo, are trademarks of Armatura