Access Control System - Vendor Specification Document

The Tennery Condominium

Prepared for: Managing Agent
Date: February 2026
Document Version: 1.0

---

1. Executive Summary

The Tennery condominium is seeking to replace the existing outdated Fermax intercom system with a modern, API-enabled access control solution. This document outlines the technical specifications and requirements for vendors to provide quotations.

Project Scope

- **5 access points** (glass door entrances)
- Integration with existing resident web/mobile application
- Remote unlock capability via smartphone app
- Visitor management with temporary access codes
- Video intercom functionality
- Comprehensive audit logging

---

2. Site Information

Property Details

- **Property Name:** The Tennery
- **Address:** Woodlands Road, Singapore 677727
- **Total Units:** 338 residential units
- **Blocks:** Multiple blocks
- **Completion Year:** 2013

Current System

- **Existing System:** Fermax Intercom (to be replaced)
- **Condition:** Outdated, limited functionality, no API integration

---

3. Access Points Specification

3.1 Access Point Locations

ID	Location	Type	Door Type	Notes
1	Main Lobby (Tower B Ground Floor)	Main Entrance	Glass Door	Primary entrance, highest traffic
2	Entrance A (Tower A Side)	Secondary Entrance	Glass Door	Pedestrian access
3	Entrance B (Tower B Side)	Secondary Entrance	Glass Door	Pedestrian access
4	Entrance C (Tower C Side)	Secondary Entrance	Glass Door	Pedestrian access
5	Entrance D (Tower D Side)	Secondary Entrance	Glass Door	Pedestrian access

3.2 Hardware Requirements Per Access Point

Each access point must include:

1. **Door Controller/Intercom Panel**
    - Outdoor-rated (IP65 minimum for external units)
    - Vandal-resistant housing (IK08 minimum)
    - Built-in camera (minimum 2MP, wide-angle lens)
    - Two-way audio with noise cancellation
    - Touchscreen or keypad for code entry
    - RFID/NFC card reader (optional, for future expansion)
    - LED status indicators
2. **Electric Lock Integration**
    - Compatible with existing or new electric strikes/magnetic locks
    - Fail-safe or fail-secure options (specify recommendation)
    - Door position sensor
    - Request-to-exit (REX) button support
3. **Network Connectivity**
    - Ethernet (PoE preferred for simplified cabling)
    - Wi-Fi backup (optional)
    - Support for VLAN segregation

---

4. Software & Integration Requirements

4.1 API Requirements (CRITICAL)

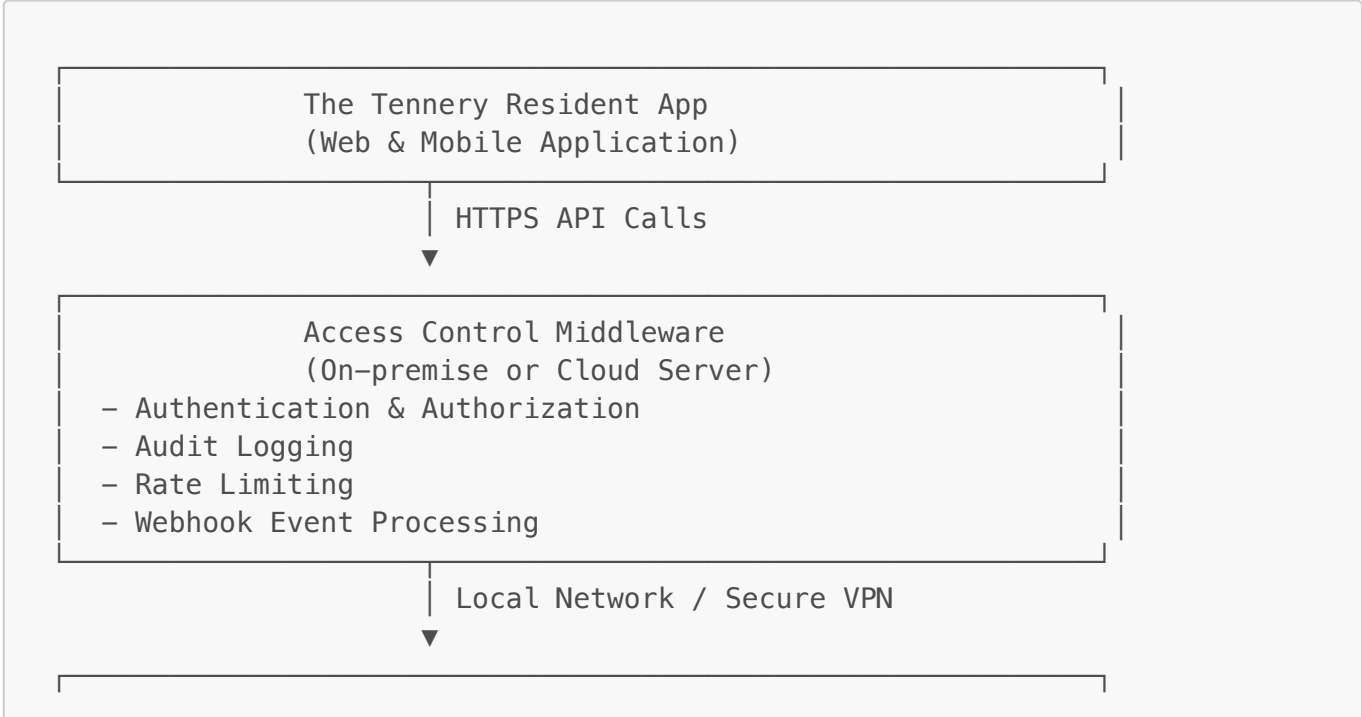
The system **MUST** provide a well-documented REST API or SDK that supports:

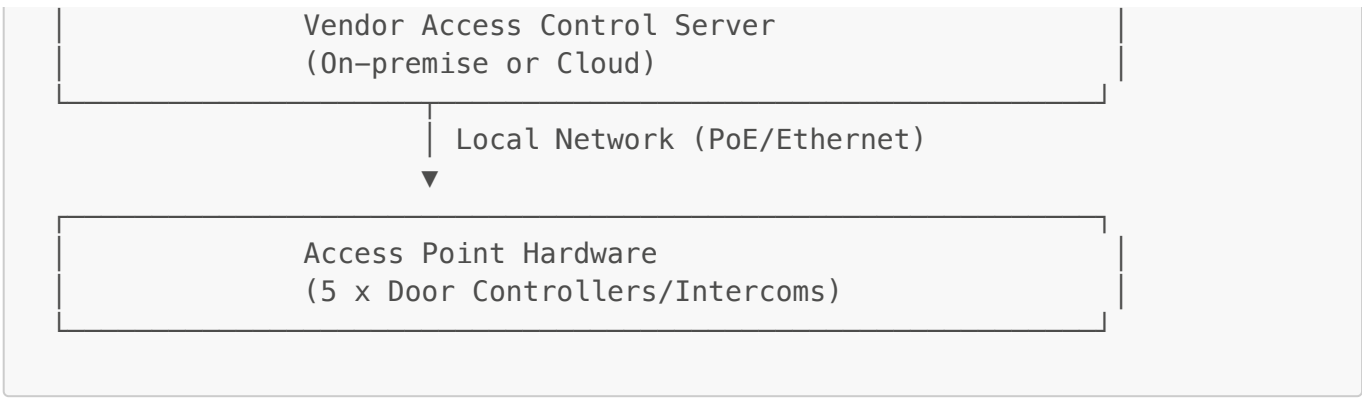
Feature	Required	Priority
Remote door unlock command	✅ Yes	Critical
Door status query (locked/unlocked/open/closed)	✅ Yes	Critical
Device health/heartbeat monitoring	✅ Yes	Critical
Visitor access code generation	✅ Yes	Critical
Visitor access code validation	✅ Yes	Critical
Visitor access code revocation	✅ Yes	Critical
Access log retrieval	✅ Yes	Critical
Live video stream access	✅ Yes	High
Video snapshot capture	✅ Yes	High
Push notifications/webhooks	✅ Yes	High
User/resident management	⚪ Optional	Medium
Firmware update via API	⚪ Optional	Low

4.2 API Technical Specifications

- **Protocol:** HTTPS (TLS 1.2 minimum)
- **Authentication:** OAuth 2.0 or API Key with HMAC
- **Data Format:** JSON
- **Rate Limiting:** Minimum 100 requests/minute per client
- **Latency:** Maximum 500ms response time for unlock commands
- **Availability:** 99.9% uptime SLA

4.3 Integration Architecture





---

5. Functional Requirements

5.1 Resident Features

Feature	Description
Remote Unlock	Residents can unlock any authorized door via smartphone app
Video Preview	View live camera feed before unlocking
Visitor Invites	Generate temporary access codes for visitors
Time-Limited Access	Set validity period for visitor codes (date/time range)
Entry Limits	Limit number of times a visitor code can be used
Access Point Selection	Specify which doors a visitor can access
Arrival Notifications	Push notification when visitor uses their code
Access History	View personal unlock and visitor activity history

5.2 Management Features

Feature	Description
Centralized Dashboard	Monitor all access points in real-time
Emergency Unlock	Unlock all doors simultaneously (fire/emergency)
Emergency Lockdown	Lock all doors and disable all codes
Audit Logs	Comprehensive logs with timestamps, user IDs, IP addresses
Failed Attempt Alerts	Notifications for repeated failed access attempts
Device Health Monitoring	Status of all devices, firmware versions, connectivity
Visitor Management	View/revoke all active visitor codes across property
Report Generation	Export access logs for specified date ranges
User Management	Add/remove/modify resident access permissions

5.3 Visitor Access Flow

```
1. Resident creates visitor invite via app
   ├── Enters visitor name, contact, purpose
   ├── Selects valid date/time range
   ├── Selects authorized access points
   └── System generates 6-digit access code

2. Resident shares code with visitor (WhatsApp/SMS/Email)

3. Visitor arrives at access point
   ├── Enters 6-digit code on keypad
   ├── System validates code (time, entry count, access point)
   ├── If valid: Door unlocks, resident notified
   └── If invalid: Access denied, logged

4. Code expires or reaches entry limit
   └── Code automatically deactivated
```

---

6. Security Requirements

6.1 Network Security

- [ ] All API communications over HTTPS/TLS 1.2+
- [ ] Support for network segmentation (VLAN)
- [ ] No direct internet exposure of door controllers
- [ ] Encrypted storage of access credentials
- [ ] Regular security patches and firmware updates

6.2 Access Control Security

- [ ] Brute-force protection (lockout after failed attempts)
- [ ] Audit trail for all access events (tamper-proof)
- [ ] Role-based access control for management functions
- [ ] Two-factor authentication for admin functions
- [ ] Automatic code expiration

6.3 Physical Security

- [ ] Tamper detection on door controllers
- [ ] Backup power (UPS) for minimum 4 hours operation
- [ ] Fail-safe/fail-secure configuration options
- [ ] Physical key override capability

---

7. Recommended Vendors

Based on our requirements, the following vendors are recommended for evaluation:

Tier 1 (Preferred - Full API Support)

Vendor	Product Line	API	Video	Est. Cost/Point	Notes
Akuvox	R29 Series	REST API	Yes	$800-1,200	Good API docs, cloud option
2N (Axis)	IP Verso	HTTP API	Yes	$1,500-2,500	Enterprise-grade, reliable
ButterflyMX	Smart Intercom	Full API	Yes	$2,000-3,000	Cloud-native, excellent UX
Doorbird	D2101V	REST API	Yes	$1,200-1,800	Good for residential

Tier 2 (Budget Options)

Vendor	Product Line	API	Video	Est. Cost/Point	Notes
Hikvision	DS-KV Series	ISAPI	Yes	$400-800	Budget-friendly
Dahua	VTO Series	CGI/API	Yes	$400-700	Budget option

Evaluation Criteria

When evaluating vendors, please score on:

1. **API Quality (30%)** - Documentation, reliability, feature completeness
2. **Hardware Quality (25%)** - Build quality, durability, camera quality
3. **Total Cost (20%)** - Hardware + installation + annual fees
4. **Local Support (15%)** - Singapore-based support availability
5. **Ease of Integration (10%)** - Time to integrate with our app

---

8. Installation Requirements

8.1 Cabling

- CAT6 Ethernet cabling to each access point
- PoE switch with sufficient ports and power budget
- Backup power connection to building UPS

8.2 Server Infrastructure

Option A: On-Premise Server

- Dedicated server or VM for access control software
- Minimum specs: 4 CPU cores, 8GB RAM, 500GB storage
- Network connectivity to all access points
- Backup and disaster recovery plan

Option B: Cloud-Hosted

- Vendor-provided cloud infrastructure
- Secure VPN connection to local network

- Data residency considerations (Singapore preferred)

8.3 Integration Support

Vendor must provide:

- API documentation and sample code
- Technical support during integration (minimum 40 hours)
- Test environment for development
- Training for management staff (minimum 4 hours)

---

9. Quotation Requirements

Please provide quotations including:

9.1 Hardware Costs

Item	Quantity	Unit Price	Total
Door Controller/Intercom Unit	5	$	$
Electric Strike/Lock (if needed)	5	$	$
PoE Switch	1	$	$
Server Hardware (if on-premise)	1	$	$
Cabling and Accessories	1 lot	$	$
Hardware Subtotal			**$**

9.2 Software & Licensing

Item	Term	Price
Access Control Software License	Annual	$
Cloud Hosting (if applicable)	Annual	$
API Access License	Annual	$
Software Subtotal (Annual)		**$**

9.3 Services

Item	Price
Installation & Commissioning	$
Integration Support (40 hours)	$
Training (4 hours)	$
Services Subtotal	**$**

9.4 Ongoing Costs

Item	Annual Cost
Maintenance & Support	$
Software Updates	$
Cloud Services (if applicable)	$
Annual Recurring Total	**$**

---

10. Project Timeline

Phase	Duration	Activities
Vendor Selection	2 weeks	Evaluate quotations, site visits
Procurement	2-4 weeks	Order hardware, prepare contracts
Installation	1-2 weeks	Hardware installation, cabling
Configuration	1 week	System setup, network configuration
Integration	2-3 weeks	API integration with resident app
Testing	1 week	End-to-end testing, UAT
Training & Handover	1 week	Staff training, documentation
Total Estimated Duration	**10-14 weeks**	

---

11. Contact Information

For quotations and technical queries, please contact:

The Tennery Management Office
Email: thetennery.cm@gmail.com
Phone: +65 6763 8978

Submission Deadline

Please submit quotations by: **[To be filled by Managing Agent]**

Site Visit

Site visits can be arranged by appointment. Please contact the management office to schedule.

Appendix A: API Integration Examples

A.1 Remote Unlock Request

```
POST /api/v1/doors/{door_id}/unlock
Authorization: Bearer {access_token}
Content-Type: application/json

{
  "duration_seconds": 10,
  "reason": "resident_remote_unlock",
  "user_id": "resident_12345"
}
```

A.2 Create Visitor Access Code

```
POST /api/v1/visitor-codes
Authorization: Bearer {access_token}
Content-Type: application/json

{
  "visitor_name": "John Delivery",
  "valid_from": "2026-02-07T09:00:00+08:00",
  "valid_until": "2026-02-07T18:00:00+08:00",
  "max_entries": 1,
  "authorized_doors": ["door_1", "door_4"],
  "host_unit": "#05-12",
  "host_user_id": "resident_12345"
}
```

A.3 Webhook Event (Visitor Check-in)

```
{
  "event_type": "visitor_checkin",
  "timestamp": "2026-02-07T10:32:45+08:00",
  "door_id": "door_1",
  "door_name": "Main Lobby",
  "visitor_code": "847291",
  "visitor_name": "John Delivery",
  "host_user_id": "resident_12345",
  "host_unit": "#05-12"
}
```

Appendix B: Compliance Checklist

Vendors must confirm compliance with:

- [ ] PDPA (Personal Data Protection Act) - Singapore
- [ ] Fire Safety regulations (SCDF)

- [ ] BCA building codes
- [ ] Cybersecurity best practices (CSA guidelines)

Document prepared by The Tennery Management Council
For internal use and vendor quotation purposes only