RETA
REAL ESTATE TECHNOLOGY ALLIANCE

1775 Eye Street, N.W., Suite 1100
Washington, D.C. 20006
reta@nmhc.org | www.retall.org

A RETA REPORT | OCTOBER 2023

ACCESS CONTROL AND CREDENTIALS

BY: THE RETA ACCESS CONTROL AND CREDENTIALS WORKGROUP

About RETA

Through collaboration and partnership, the Real Estate Technology Alliance (RETA) fosters the development of next-generation systems and solutions that will enable real estate companies and their technology partners to do business globally in the 21st century. RETA creates resources that facilitate the development of technology models for the real estate community that will foster innovation, improve the resident experience, increase the effectiveness and efficiency of property operations, and create a healthy ecosystem of technology suppliers.

Note: This document does not provide legal advice or guidance. RETA always recommends consulting legal counsel before entering into any agreement.

Contents

Executive Summary

Access control and credential management solutions have become essential to the multifamily housing industry. In today's world, traditional access control systems are no longer adequate for facilitating new and emerging technologies, like self-guided tours, or for providing sufficient security controls. And unlike single-family homes, multifamily communities have shared spaces, such as lobbies, elevators, gyms, and pools, which require different access levels. Managing access to these spaces and individual units requires a balance between convenience for residents and security measures that protect them and their belongings.

Also, unlike single-family homes, we have three major groups of people accessing our communities: staff, residents, and visitors, including vendors, resident service providers (such as dogwalkers), and guests of existing residents. For staff, solutions can streamline access management, reduce the administrative burden of managing keys and locks, and provide a secure and transparent audit trail of all access activity. For residents, solutions can enhance the resident experience, enabling keyless and touchless entry and provide a more seamless and convenient access process. For visitors, access control solutions can improve operational efficiency, enabling remote access permissions and reducing the need for on-site supervision.

Anyone seeking a comprehensive access control and credentialing solution should start with mapping the journey of those three groups through their community. That will lead to an assessment of all their common access points, which most likely will highlight current limitations and gaps. When seeking a solution, some guiding principles should include assuring the option is technologically advanced and secure, cost-effective, operationally efficient, and ultimately, a solution that promotes staff and resident satisfaction.

Before and after a solution is implemented, metrics for success should be created. Your Key Performance Indicators (KPIs) for staff and residents will likely be a little different for each. All the steps outlined above, including example KPIs, are outlined in more detail throughout this report.

Some common challenges faced by property owner-operators include managing visitor access, controlling key distribution, monitoring access to shared spaces and ensuring the security of individual units. Best practices for addressing the challenges include conducting regular security assessments, implementing comprehensive electronic access control systems, using mobile credentials and adopting a visitor management system.

As property owner-operators consider investing in advanced access control and credential management solutions, taking an informed, thoughtful and strategic approach will help manage the risks always inherent with access control and will set owner-operators up for good outcomes. As always, RETA seeks to be a trusted source of information to help with the implementation of this new technology.

Note: This document does not provide legal advice or guidance. RETA always recommends consulting legal counsel before entering into any agreement.

Multifamily Access Control Overview

This report was created by the RETA Access Control and Credentials Working Group and explores access control and credential management in multifamily communities. As industry and technology peers, we understand the importance of providing reliable, user-friendly, secure access control and credential solutions to our staff and residents. We recognize that legacy access controls and credentials must be updated as they pose significant risks to property security and resident safety.

To address these challenges, next-generation access control solutions, including smart locks, keyless entry systems, biometric authentication, and cloud-based access management platforms, can provide greater flexibility and control over access permissions. These solutions can streamline access management, reduce the administrative burden of managing keys and locks and provide a secure and transparent audit trail of all access activity.

We also understand stakeholders have unique needs and challenges relating to access control and credentials. That is why any access control and credentials solutions should be designed to meet the specific requirements of each group. For staff, access control solutions can streamline access management, reduce the administrative burden of managing keys and locks and provide a secure and transparent audit trail of all access activity. For residents, access control solutions can enhance the resident experience, enabling keyless and touchless entry and provide a more seamless and convenient access process. For visitors, including vendors, resident service providers (such as dogwalkers), and guests of existing residents, solutions can improve operational efficiency, enabling remote access permissions and reducing the need for on-site supervision.

RETA is committed to helping the multifamily industry adopt next-generation access control and credential solutions that optimize safety, security and convenience. Solutions can transform the access management landscape, while providing greater flexibility, transparency and control over access permissions. We look forward to collaborating with the industry to drive innovation and provide resources that meet their evolving needs. By sharing our knowledge and expertise, we can empower owner-operators to make informed decisions about their access control and credential solutions.

Access Control Challenges

This report identifies some of the challenges owner-operators, residents, and visitors face in controlling and gaining access to shared spaces and individual units within multifamily communities. By examining the latest technology and industry best practices, this report serves as a resource for implementation of effective access control and credential management systems to enhance the safety and security of residents, their property and common areas.

Multifamily communities present unique access control and credential management challenges. Unlike single-family homes, multifamily communities have shared spaces, such as lobbies, elevators, gyms and

pools, which require different access levels. Managing access to these spaces and individual units requires a balance between convenience for residents and security measures that protect them and their belongings.

Some challenges include:

- Managing visitor access
- Controlling key distribution
- Monitoring access to shared spaces, and
- Ensuring the security of individual units

Additionally, owner-operators must ensure their access control systems comply with relevant regulations and industry standards. Significant due diligence and consultation with legal counsel is recommended on this front, particularly assuring the security of any solution. Failure to do so can result in significant liability and reputational damage.

Best Practices, Principles and KPIs

Best Practices:

To address these challenges, there are a few best practices that property managers can implement. Some practices include:

- Conducting regular security assessments
- Implementing comprehensive electronic access control systems
- Using mobile credentials, and
- Adopting a visitor management system

Additionally, property managers must provide training to staff and residents on the proper use of access control systems and how to report suspicious activity.

Principles of a Good Solution:

When looking at access control and credentials solutions for their community, it's essential that any owner-operator ensure that the access control and credential management system implemented is:

- Technologically advanced and secure
- Cost-effective
- Operationally efficient, and
- Promotes staff and resident satisfaction

Each of these key areas should be addressed to ensure the system's success and an appropriate return on investment (ROI).

First, the access control and credential management system should be technologically advanced and secure and should easily integrate with other building management systems. This includes mobile integration, smart cards and other advanced technologies that can provide a high level of security and convenience for residents. The system should also provide data analytics to inform business intelligence and ensure informed decision making.

Implementation planning is crucial to ensure successful access control and credential management system implementation. Such planning should include the identification of key stakeholders, such as property managers, staff and residents, and their needs and requirements. It should also include creation of a roadmap and timeline for implementation, including system testing, staff training and resident communication. Challenges may arise during implementation, such as system compatibility issues, staff resistance to change, and resident concerns about data privacy and security. Addressing these challenges requires clear communication, staff training, and addressing resident concerns and feedback.

Second, the access control and credential management system should be cost-effective, with a clear ROI and cost savings generated by the system. This includes savings generated by reducing the use of physical keys and access cards, reduced maintenance costs and efficient system operation that can save staff time and increase efficiency.

Third, the access control and credential management system should be easy to implement, operate, and maintain. This includes efficient staff training, maximum system uptime, and easy system integration that can reduce complexity and improve efficiency.

Finally, if you've done a good job following those three principles, resident and staff satisfaction should follow. To summarize, implementing an advanced access control and credential management system in multifamily housing requires a comprehensive solution addressing key areas, including technology, financial, operational efficiency, staff and resident satisfaction. Implementation planning and addressing challenges are also crucial to ensure successful implementation and long-term success.

The benefits of successfully implementing the system can lead to improved resident satisfaction and retention rates. Success can be measured by tracking KPIs, which will likely vary for owner-operators and residents. A few examples of KPIs for each group are listed below.

Examples of Owner-Operator KPIs:

1. Resident satisfaction: High satisfaction leads to resident retention and increased occupancy.
2. Safety: Measures the level of safety provided by the access control and credential management system to ensure resident security and protection.
3. Ease of Use: Measures the user-friendliness of the access control and credential management system to ensure resident convenience and satisfaction.
4. Technology Integration: Measures the level of integration with other building management and security systems to help ensure a safe, seamless living experience for residents.

5. Reduced Waiting Times: Measures the reduction in waiting times for building access to ensure a convenient and efficient living experience for residents.
6. Convenience: Measures the overall convenience of the access control and credential management system to ensure resident satisfaction and retention.
7. Transparency: Measures the level of transparency of the access control and credential management system to ensure resident trust and satisfaction.
8. Data Access: Measures the level of access to data generated by the access control and credential management system to ensure informed resident decision making and satisfaction.
9. Data Security: Protects and allows for the management of resident and property level data to ensure compliance with applicable data security and privacy laws and regulations.
10. Reduced Staff Time: Reduced staff time means more time for other tasks and better resident customer service and improved property operations.

By measuring these KPIs, property owner-operators can ensure the success and ROI of the access control and credential management system. A high occupancy rate, resident satisfaction and cost savings generated by the system can lead to increased Net Operating Income (NOI). An efficient and effective system operation and reduced staff time can save operating costs and increase efficiency.

Examples of Resident KPIs:

1. Safety and Security: High safety and security indicates resident protection and peace of mind.
2. Ease of Use: An easy-to-use system improves resident satisfaction and can lead to resident retention.
3. Technology Integration: Integration with other building management systems provides a seamless living experience.
4. Convenience: High convenience leads to resident satisfaction and can increase occupancy rate.
5. Privacy: Protocols are transparent to safeguard resident access history, biometrics, or other identifiable information.
6. Reduced Waiting Times: Reduced waiting times for building access can increase resident satisfaction.

By measuring these KPIs, residents can determine the safety, convenience and satisfaction of the access control and credential management system. A safe and easy-to-use system, technology integration and reduced waiting times can increase resident satisfaction and retention. High security ensures resident protection and peace of mind, and access to data generated by the system can inform resident decision making and increase satisfaction.

Three Journeys in Access Control

While you will likely want to measure KPIs for staff and residents, there are actually three major groups to consider when creating your access control and credentials solution: staff, residents, and visitors, including vendors, resident service providers (such as dogwalkers), and guests of existing residents. Each has their own journey through your property and each needs to be treated differently. Below we outline the three journeys in access control step-by-step along with a description of each step and its impact on access control and credentialing.

The Staff Journey

For an employee working in a multifamily property setting, daily experiences are deeply intertwined with access control and credential management systems. These systems are essential for maintaining our residents' secure, efficient and comfortable living environment. In their role, they encounter various challenges, such as navigating complex access control technologies, handling lost or stolen credentials and monitoring unauthorized access attempts. Their journey as employees involves continuous learning, adaptation and clear communication with colleagues and residents. The best staff remain vigilant and committed to providing exceptional service, ensuring the safety and well-being of their community, and contributing to a positive living experience for all residents on the property.

The Staff Journey: Steps and Impacts

Journey Step	Description	Access Control & Credential Impact
Access to the employee only doors	Gain access to back-office doors	Employee record must be in the building access control system.
Access to individual resident units	Gain access to resident units when permission to enter granted or within a prescribed time frame	Employee records must be in the building access control system and a separate access control system (if they are not the same system). Real-time notifications for access requests (activity log) from staff to customers may be useful.
Credential issuance to other Stakeholders - Residents	Staff creation and management of access control rules and credentials for access by other stakeholders	Resident records must be in the building access control system and a unit access control system (if they are not the same system). Real-time notifications for access requests (activity log) from staff to customers may be useful.
Credential issuance to other stakeholders - third parties	Third-party access - granted by the resident - housekeeping, health care provider, pet sitters, etc.	Property protocol will need to determine how resident will be able to grant access to third parties. This may be achieved via visitor management systems (intercom), mobile credentials or guest credential fobs.

Journey Step	Description	Access Control & Credential Impact
Credential issuances to emergency services	The ability to grant access or issue credentials as required by state/local code or in emergency situations	Credentials may need to be created with the proper access right as required by state or local code. Knox Box (lockbox) credentials, such as keys/fobs, are a good fire code example. In some circumstances, there may be a specific tie-in to the access control system.
Credential revocation	Revocation, or eliminating credentials to expired authorized users	Ensure safety from unauthorized users who no longer have, or can give, access to the community.
Access to/for guest parking	Giving access to restricted guest parking	Keeps a secured parking area for guests of the community to maintain safety for authorized guests.
Access to/for resident parking	Gated access for residents to keep them safe once on community premises	Limits reserved parking for residents and no real impact.
Access to fire alarm systems	Access for emergency services and third-party monitoring	Check with local fire code for compliance
Fire watch management in case of power outages	Access systems need to function during power outages.	Systems should have backup power (local battery or other power source) and stored memory in case of power outages.

The Resident Journey

The resident journey in using an access control and credential management system begins with the initial move-in process. Residents will be provided with their credentials, such as access cards or mobile app access, and will be given a brief overview of how to use the system.

Once moved in, residents will use their credentials to access the building or community and any common areas or amenities. The system may also be integrated with other building management systems, such as smart home technology, to provide a seamless living experience.

If residents have any issues with the system or need assistance, they can contact the property management staff for support. Staff can help residents troubleshoot any issues with their credentials or the system, as well as provide any necessary updates or changes to access privileges.

Residents can also provide feedback on their experience with the system, such as ease of use, convenience and security. This feedback can help inform any necessary changes or updates to the system to improve the resident experience.

Overall, the resident journey using an access control and credential management system should be seamless, convenient and secure. By prioritizing resident satisfaction and support, owner-operators can increase resident retention rates and ensure the long-term success of their communities.

The Resident Journey: Steps and Impacts

Journey Step	Description	Access Control & Credential Impact
Credential issuance	The method of distribution, type of credential	Typically, a physical fob, brass key, and potentially other new technology solutions utilizing digital issuance like NFC/Bluetooth/PIN/Magstripe, etc. Accessibility considerations may apply.
Access to the main lobby	Resident needs to enter the main lobby	Resident needs a key/fob/mobile phone to gain access. Might require a resident record to be added to a third-party access control solution.
Access to indoor amenities	Resident wants to gain access to an indoor amenity that they have reserved	Resident needs a key/fob/mobile phone to gain access. Might require a resident record to be added to a third-party access control solution.
Access to outdoor amenities	Resident wants to gain access to an outdoor amenity that they have reserved	Resident needs a key/fob/mobile phone to gain access. Might require a resident record to be added to a third-party access control solution. Power, communications, and weather resistance are important considerations for devices and software.
Access to resident unit/home	Resident wants to open the door to their own unit	Resident needs a key/fob/mobile phone to gain access. Might require a resident record to be added to a third-party access control solution.

Journey Step	Description	Access Control & Credential Impact
Access to community parking	Resident wants to open the community gate or access to the community parking structure	Resident records in the system that controls the access gate to the community and parking areas.
Credential issuance by the resident to visitors/third parties	Resident wants to give access to a visitor or third party for services or other purposes	Individual properties should have the ability to enable or disable this feature. The property should institute rules to manage access: time-based (open hours), permanent vs. temporary, the quantity of passes limits, limited access to amenities or other areas of property vs. just resident unit. The ability to request this access by a third party may be helpful and/or required from a regulatory perspective.
Credential revocation by the resident to visitors/third parties	Resident wants to revoke access to a visitor or third party for services or other purposes	The ability to revoke with immediate effect triggers based on move-out and other requirements is important. This is a key issue to consider in an online vs. offline system.
Notifications of credential usage to resident	Resident is notified of access by a visitor or third party	Notifications or real-time alerts of access may be useful for security purposes.

A typical resident in a multifamily community may require access to a wide variety of access points.

The Visitor Journey

Visitors in our communities will include guests of existing residents, third-party vendors, such as mail delivery personnel, and resident service providers, such as housekeeping staff and dog walkers. All play an essential role in the daily lives of staff and residents, and in the access control and credential management system of multifamily housing.

The vendors and resident service providers require access to the community to perform their services but may be treated as temporary employees. Guests of residents can be granted access by the resident through generation of a code, or by being put on an approved guest list. Given that the process for vendors and service providers is more complex, that will be the primary focus for mapping the visitor journey below.

To ensure that third-party vendors and service providers can access the building or community efficiently and safely, property management staff can create temporary credentials or access codes that can be provided to the vendors and service providers as needed. These temporary credentials can be revoked or changed as necessary to ensure the security of the community.

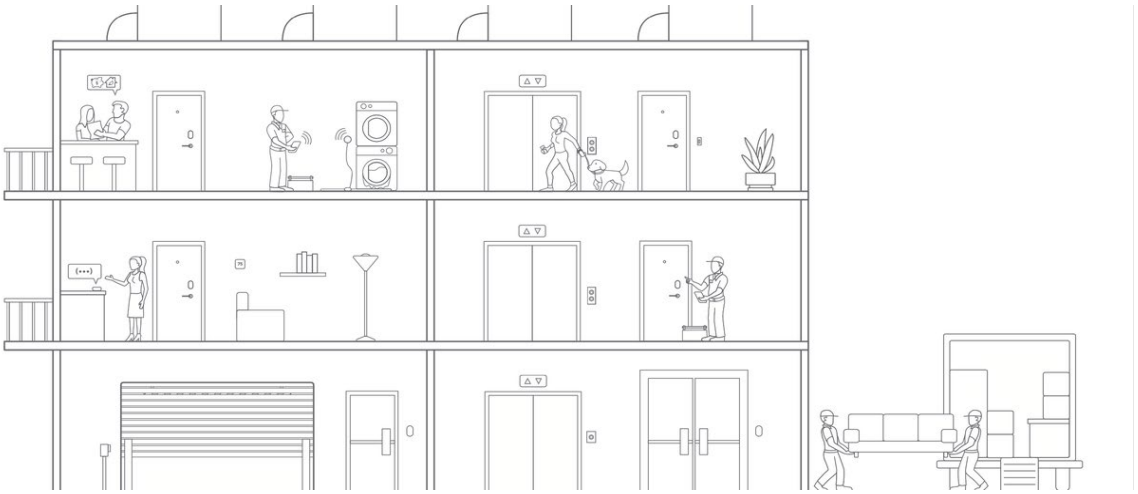
Third-party vendors and service providers must also follow building access policies and procedures, such as checking in with the property management staff before accessing the community. This helps ensure that all vendors and service providers are authorized and accounted for, reducing the risk of security breaches or other issues.

In addition to providing temporary credentials, property management staff can communicate effectively with third-party vendors and service providers about the access control and credential management system and any updates or changes to policies or procedures. This helps ensure that they are informed of any necessary changes or updates.

Overall, third-party vendors and service providers are essential to the access control and credential management system in multifamily housing. By providing temporary credentials and effective communication and support, property management staff can ensure they can access the building or community safely and efficiently while maintaining the system's security and integrity.

The Visitor Journey: Steps and Impacts

Journey Step	Description	Access Control & Credential Impact
Visitor/vendor lobby access	Gain access to lobby when permission to enter has been obtained	Legacy products (non-video) do not allow for verification of guests (guest, prospect, food, parcel, vendor) to the community. Modern video systems allow for additional security based on the verification preview of kiosk users.
Visitor/vendor resident unit access	Gain access to resident units when permission to enter has been obtained	Hard credentials (unrestricted keys, proximity fobs) can be copied or stolen for future unwarranted use, reducing resident security. Advanced key systems and the latest generation of smart credentials (e.g., DesFire EV3) provide more robust security. Digital credentials (PINs, Bio, BLE, App) allow the resident to have total control over the guest's access permissions.
Visitor/vendor amenity access	Gain access to amenities during the appropriate scheduled time	In most cases, they do not need access to amenities.
Visitor/vendor community/parking access	Gain access to the parking area/community when permission to enter has been obtained	If the parking area is restricted, they likely do not need access.
Resident guest/vendor access to the building	Resident wants to be able to grant access to a guest without having to meet the resident in the lobby	Resident needs to send a code or place guest/vendor on an approved guest list.



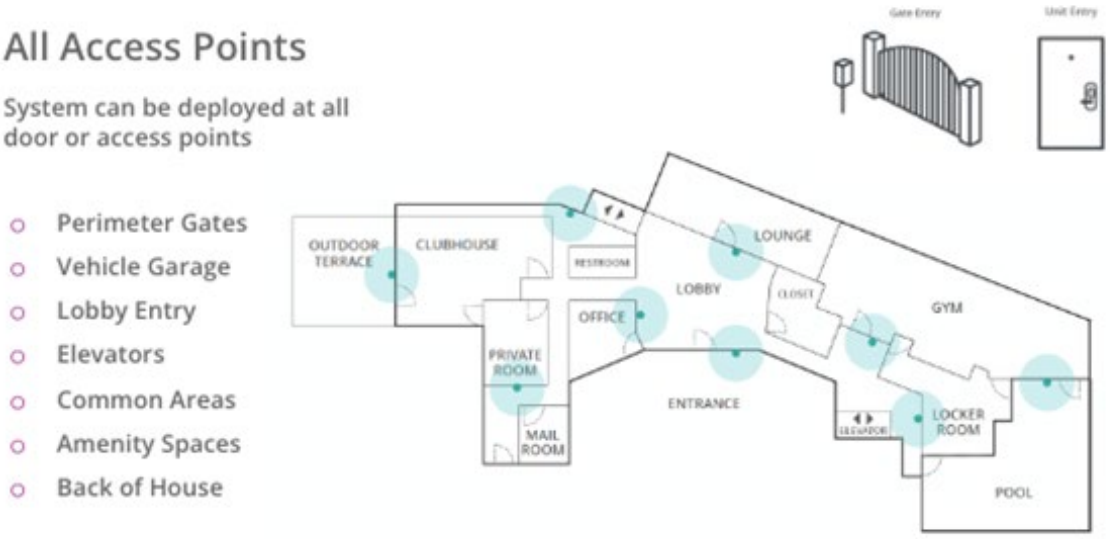
Third-party vendors, visitors and service providers may need access to a typical multifamily community for a wide variety of reasons.

Access Points and Gap Analysis

Mapping your three journeys highlights all the different access points you'll find in a typical multifamily community. Listed below are common access points and some thoughts on assessing your current limitations and gaps and how you can address them.

Common Access Points

Common access points in multifamily properties typically include entrances, exits, elevators, stairwells, parking garages, and common areas such as gyms, pools and laundry rooms. Effective access control and credential management systems should be designed to secure these areas and provide authorized access to residents and staff while preventing unauthorized entry. By prioritizing the security of these common access points, property owner-operators can ensure the safety and well-being of residents and staff and protect the integrity of the property.



Limitations and Gap Analysis of Current Systems

Legacy access control and credential management systems in multifamily housing have several limitations that can pose significant challenges for property owner-operators. These legacy systems often rely on physical keys or access cards, which can be lost or stolen and difficult and time-consuming to manage. These systems also need more integration with other building management systems, such as smart home technology, which can limit their effectiveness and convenience.

To address these limitations, next-generation access control and credential systems offer several key advantages. These systems typically use advanced technology, such as biometric scanning, smart cards or mobile apps, to control access to the community. They can also be integrated with other building management systems to create a seamless and convenient living environment for residents.

To conduct a gap analysis of next-generation access control and credential systems, property owner-operators should consider their current systems and identify areas where improvements can be made. This may include security, convenience, integration with other systems and cost-effectiveness. Next-generation systems can help address these gaps by providing enhanced security, greater convenience and improved integration with other building management systems. They can also offer cost savings over time by reducing the need for physical keys or access cards and streamlining system management.

By conducting a thorough gap analysis and considering the advantages of next-generation access control and credential systems, property owner-operators can make informed decisions about upgrading their systems to improve their properties' safety, security and convenience. This can lead to increased resident satisfaction, higher occupancy rates and enhanced ROI.

The Limitations

Solution Description	Limitation
Matter Protocol-based solutions	Incomplete protocol-level standards. The first products to incorporate the Matter Protocol will focus on single-family homes & consumer experience.
Online vs. offline systems	Online systems generally have little to no delay when updating the access control door. Offline systems may have a delay in updating access control rights at a particular door as required.
Credential security, encryption	(Gathering information for this and the previous section)

Assessment Criteria for Access Control and Credentials

Assessment criteria for credentials and access control should prioritize security, convenience, and ease of use for all stakeholders, including property management staff, residents and third-party vendors. The criteria should also consider cost-effectiveness, system compatibility and scalability to ensure a sustainable, long-term solution.

Additionally, the assessment criteria should be regularly reviewed and updated to reflect changing needs and requirements of the property and stakeholders. By prioritizing these criteria, owner-operators can ensure the successful implementation and operation of the access control and credential management system.

The Criteria

Assessment Criteria	Details
Staff credentials	Access control and serialization needs to be codified with naming structures to maintain easily understood audit trails.
Security criteria for credentials	System should allow administrative user role that has authorization to assign credentials (User Provisioning).
Credential database integration	Reduce the number of databases that need to be managed with sensitive information.
Audit trails	Is access control saved appropriately, and for how long? How does this work for offline vs. online doors? Compliance with applicable data privacy and security regulations.
Communication architecture	What systems and infrastructure does the system rely on? What happens when this system does not work?
Video integration	Is it possible to tie access control to video surveillance? Are the clocks from both systems aligned to track access? What are the regulatory considerations for recording video?
Escalation paths/exception management	What processes and plans are available in case of problems?

The Credentials

Credential Type	Technology	Pro	Con
Card	Magnetic stripe		Legacy technology, contact required, wear on card and reader over time, no encryption
Key fobs, cards and wristbands	Proximity technology	Inexpensive, widely distributed	Can be duplicated easily, no encryption
Key fobs, cards and wristbands	Smart technology - MIFARE Classic	Higher security, harder to duplicate, encrypted	Older technology, will become easier to duplicate over time, may require an upgrade to your card reader
Key fobs, cards and wristbands	Smart technology - MIFARE EV3 DESFire	Newest technology, AES 128-bit encryption (has not been cracked/compromised yet)	May require an upgrade to your card reader
Keypads and PIN	Digital Keypad reader	Very convenient, does not require user to physically carry something with them	PINs can be easily shared and create a potential security risk
Mobile	BLE-Bluetooth Low Energy	Can leverage best practices for security and encryption	Requires user to open a mobile app on a smartphone and show intent (this can be a slower experience than using a card), may require an upgrade to your card reader

In summary, understanding the assessment criteria and types of credentials available is crucial for successfully implementing and operating an access control and credential management system in multifamily housing. By prioritizing security, convenience and cost-effectiveness, property owner-operators can select the right types of credentials and systems that meet the needs and requirements of all stakeholders.

A Journey – Not a Conclusion

The current state of access control and credential management systems in multifamily housing has several limitations and challenges, which can be addressed by adopting next-generation systems. But these systems also have the potential to offer improved security, convenience and integration with other building management systems while reducing the need for physical keys or access cards that can improve the resident experience.

Access control and credential management systems will likely continue to evolve and improve by integrating emerging technologies such as artificial intelligence and the Internet of Things (IoT). These advancements are expected to further enhance the security and convenience of multifamily communities while providing new opportunities for data analysis and insights.

It is important to note that as technology evolves and federal and state regulations change, owner-operators must remain up-to-date with the latest regulations and technological advancements to ensure the effectiveness and compliance of their access control and credential management systems. The information provided in this report is current as of the date listed on the cover.

Overall, access control and credential management systems are critical for the safety and security of multifamily communities, and advancements in technology and regulations will continue to shape their evolution and adoption. As such, owner-operators must stay informed and adapt their systems to meet changing needs and requirements to ensure long-term success and profitability of their communities. RETA will continue to provide resources to reflect the ever-evolving technology landscape.

Workgroup Co-Chairs

Kevin DeMattio
Managing Partner, Co-Founder
InvictusXP

Robert Gaulden
Go to Market Director, Multifamily Access
Allegion

Workgroup Team

Frank McCammon III
Senior Director of Living Technologies
Hines

Mariana Estrada
Chief Strategy Officer
RPM Living

Justin Doran
Technical Product Manager
RPM Living

Gerrit Reinders
Director, Global Business Development
Johnson Controls