The Matter of Choice: Top Considerations for Companies Rethinking Keyholding and Transforming Access Control

4 months ago

Stuart Wheeler, Managing Director of [Keynetics](), shares the most pressing questions and key requirements poised by organisations exploring new and more effective ways of managing property keys and controlling access to premises.

Anyone responsible for facilities management or security is well aware that access control and keyholding are often challenging and, consequentially, can cause a number of operational and even financial issues.

Appetite for Change

Keyholding and access control are dynamic processes that involve daily activity and ongoing management. Keys are frequently stored off-site and exchanged daily. Access cards and fobs require setup. Every lapse creates a chain reaction: replacements, lock changes, risk reporting, all of which consume time, money, and patience.

Against this backdrop, it's not surprising that more and more organisations of various sizes, both in public and private sectors, are actively seeking alternatives to traditional methods of manned keyholding or manual pen-and-paper visitor logs. There is a clear shift towards technology-led solutions that offer greater reliability, visibility and scalability.

The driving force behind this move is not innovation for its own sake but rising service expectations. Things must be done faster, better, more efficiently; FM and security tenders outline stricter requirements for alarm response times and service delivery, with little tolerance for service shortfalls and delays, or

penalties will follow.

Moving Beyond the Traditional Approach

As operational demands evolve, security and FM professionals are beginning to ask the same question: is there a better way?

"Over the past couple of years, we have seen a drastic positive change in attitudes towards new methods of keyholding," says Stuart Wheeler, Managing Director of Keynetics.

Keynetics is one of the companies pioneering change in this space, offering smart key management solutions such as SentriGuard. With this system, keys are stored at the point of need in key safes with commercial grade, certified security. They are accessed either using a temporary code or a mobile app. The incorporated technology enables management of access to hundreds of locations remotely, and provides notifications when keys are not returned or the device battery is running low.

Stuart recalls initial resistance to change in the market. "When we started Keynetics, there was hesitation around adopting new methods. I was told more than once, "No way I am storing keys in a key safe", but that mindset has shifted entirely."

He attributes the change in attitude to a combination of persistent issues with the existing keyholding methods and increased understanding of the benefits that alternative approaches can offer, particularly if they offer adequate security and greater control.

"We're now seeing strong interest from a wide variety of organisations," he says, "including security service providers, FM companies and in-house teams operating in a range of sectors.

"Selecting the right system is often the most complex part," he adds. "Requirements can differ significantly depending on the sector and business model, but there are key areas that tend to come up repeatedly. Over time, we've identified the most common considerations raised by both existing customers and those looking for a change."

Access Traceability: The Top Priority

While security remains central, the most consistently cited requirement is access traceability, or the ability to see who accessed which property, when, and for how long.

"In many cases, the high security rating of the device was accepted without much debate," Stuart notes. "What proved to be more important was the ability to run real-time audit reports without needing to visit premises and upload visit logs, or complete some other action to get hold of that valuable access data."

This growing focus is understandable. Technology is now expected to take on tasks previously carried out by personnel, but unmanned systems must still provide a high level of oversight and accountability. In today's operating environment, access data is seen as a vital resource, not only for day-to-day management, but also for compliance, reporting and service performance evaluation.

Security: The Most Risk-Dependent Factor

Naturally, security is a high-ranking factor when selecting an access control solution. However, the emphasis placed on it varies significantly depending on the sector and the perceived risks.

"For obvious reasons, clients in high-risk sectors, such as banking or government, conduct in-depth evaluations and demand robust certification," Stuart explains. "We've attended countless meetings with some clients, continuously providing proof of both physical and digital security.

"Smaller companies with lower perceived risks, on the other hand, often acknowledged the security rating and focused more on factors like cost."

The takeaway is clear: while security is crucial, the level of scrutiny it receives is relative to the client's sector and operational risk.

Costs: Are We Breaking the Bank Here?

It is in our human nature to want the best and the shiniest, but the implementation costs may become the stopping point. For many decision-makers, the question often isn't whether a solution is ideal, it's whether it aligns with operational needs at a sustainable cost.

FM directors work within fixed budgets, often balancing multiple objectives alongside day-to-day operations. Cost isn't just about the system itself, it is about scale. A high-end solution may be entirely feasible for a business with one manufacturing site, while even a budget-friendly option could prove expensive for someone managing hundreds of retail locations.

In many cases, new systems are implemented not because they are cheap, but because the cost of doing nothing is higher. A serious issue with the current method may justify investment, where the price of failure outweighs the cost of change.

Practical Considerations: Installation, Hardware and Usability

Beyond the top three factors, practicalities such as installation requirements, ease of use and maintenance also influence the decision-making process.

Organisations typically seek systems that can be retrofitted with minimal disruption. Common questions include: Is the unit hardwired? Does it need a power supply or internet connection? How long does installation take?

Where installation is overly complex, or the benefits do not clearly outweigh the effort required, adoption may stall. On the other hand, a quick, straightforward setup is often seen as a major advantage.

Post-purchase support, including maintenance, training and customer service, is usually discussed later in the process, but remains an important factor in long-term satisfaction.

System Integrations: A Logical Next Step

We live in a digital age where doorbells can be answered from miles away and kettles are turned on with a tap on the phone screen. So it is no surprise that the security sector is so tech-orientated.

System integration is fast becoming a top request. The ability to manage multiple systems, including access control, alarms and cameras, through one interface offers a streamlined and time-saving solution that increases control.

Stuart notes, "We're primarily a software development company, so the digital side of our solutions is built with continuous improvement in mind.

"Right now, one of our long-standing clients is trialling an integration between our system and AJAX alarms. Since they actively use both SentriGuard and AJAX, it makes perfect sense to manage alarm controls within the same key management platform."

While system integration is often not the top priority, it does indicate the forward-thinking, customer-centric approach.

No Right or Wrong

Ultimately, choosing the right keyholding or access control solution depends entirely on the end user's needs. Factors such as access traceability, security (physical and digital), and implementation costs all play a part.

There is no one-size-fits-all answer. Some will retain their current methods. Others will go fully keyless. Many will find a golden middle ground.

But the journey doesn't end at purchase. Continuous evaluation, access management refinement, and user feedback are essential to ensure ongoing effectiveness or to justify the search for an even better solution.

After all, the market never stands still.