This 15 page report provides the most in-depth guidance on specifying Access Control systems you will find.

Specifying Access Control correctly can be tricky, because every opening has quirks and are prone to outside factors that impact system performance. Not only this, but what you don't specify can be just as problematic as what you do.

Most access RFPs have serious problems. While they comprehensively spell out contract conditions and business terms, they are typically scant on relevant details about the system. Not only do they tend to be a random smattering of technical points, pulling them together into a cohesive system is often needlessly costly or may even be impossible to build.

The Big Mistakes

Most of the trouble specifying access has a root cause in one of the three areas below:

1. Incomplete details, where things you don't know can ruin your budget and system goals.
2. Difficult to build, where details that sound prudent may actually limit selection and significantly drive complexity to integrate.
3. Proprietary, where even generic boilerplate writes in choices that lock you into one vendor.

In this report, we address the best strategies to avoid these problems.

Doing It Right - 18 Key Specification Areas

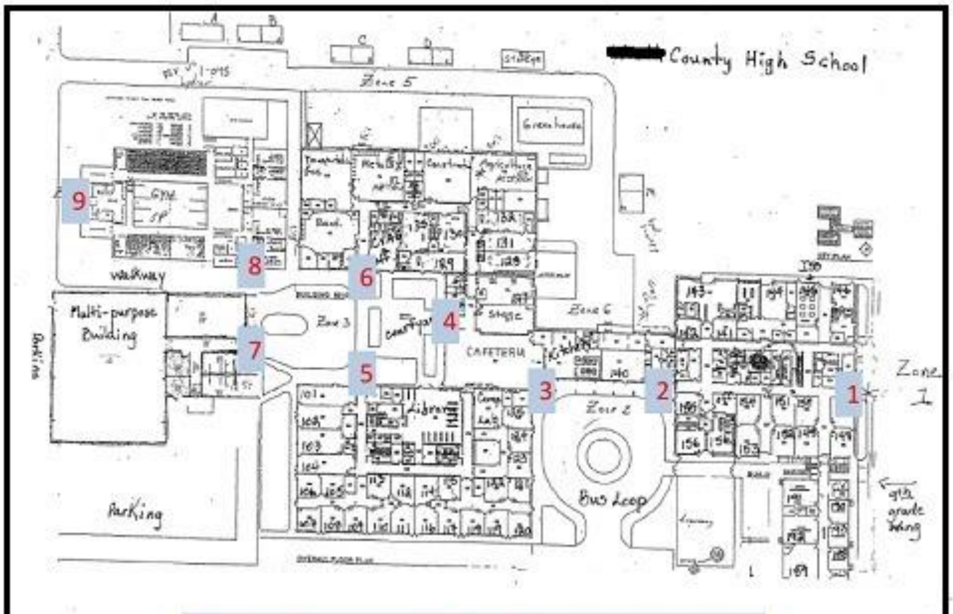
The good news is that you do not need to be an expert to specify great systems. In the sections below, we cover the right details to include, how to include them, and how to avoid common traps through addressing these 18 areas:

- Is This An Expansion or New System?
- Determining Access Security Goals
- Establishing Monitored, Managed, or Forensic Use
- Identifying Other System Integrations
- Which Credentials To Use
- Defining Doors/Opening Detail
- Defining Turnstile Use
- The Importance of Door Position Switches
- Defining Existing Locks/Hardware
- Specifying Readers
- Deciding to Use IP or Serial based Controllers
- How To Use PoE For Powering Systems
- System Edge vs. Centralized Architecture
- Is System Networking Wired or Wireless?
- Considerations For Using Existing Databases
- Evaluating User Management Features
- Using Special Features Like Time and Attendance & Mustering
- Establishing System Maintenance Expectations

First take a look at how common mistakes appear:

Common Examples

RFPs for access control might be well intentioned, but that does not mean they will get the job done. Look at these examples we pulled from recent RFPs:
Not Enough Detail: With any specification, the risk is including too many particulars that potentially drive cost. However with Access Control, the opposite is more typically true. Take this example from the Specifications section of this school's access solicitation:



Attachment B – Door access control locations

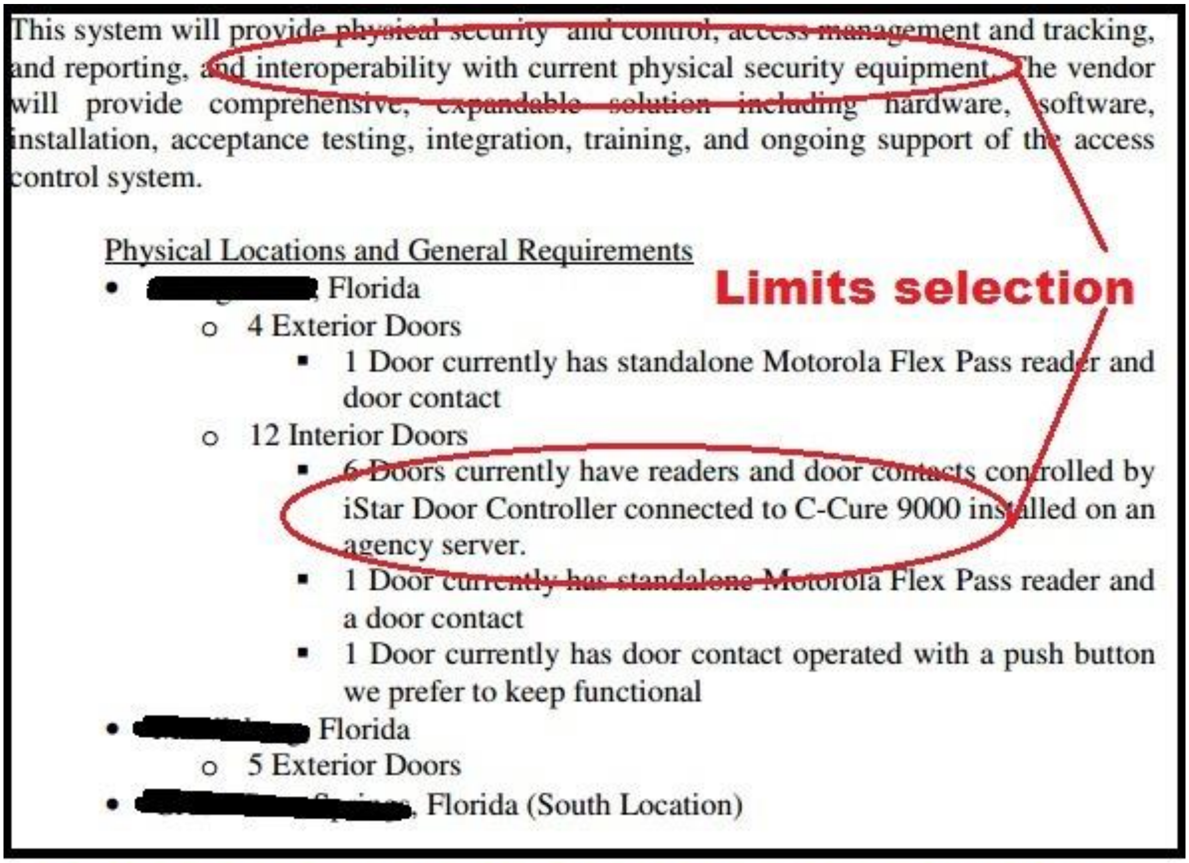
Woeful Specifications

The bulk of details to build a quote from are found in the map above. No details regarding door/opening type, existing hardware, how many people need to have access or what credential types they carry, or when the openings should be unlocked are noted. Not to mention that descriptions of how and who the system will be used, or which other systems will need to integrate with the access platform.

Granted, all these details may be released or discovered after a job walk, but not all respondents may have a fair crack at using them to build a bid.

Careless Specification: Another regrettable trait is the inclusion of specs that sound smart or economical, but prove to essentially limit choices to just one or two bids.

Take the example from a Police Department RFP:


Limits selection

This system will provide physical security and control, access management and tracking, and reporting, and interoperability with current physical security equipment. The vendor will provide comprehensive, expandable solution including hardware, software, installation, acceptance testing, integration, training, and ongoing support of the access control system.

Physical Locations and General Requirements

- [redacted], Florida
  - 4 Exterior Doors
    - 1 Door currently has standalone Motorola Flex Pass reader and door contact
  - 12 Interior Doors
    - 6 Doors currently have readers and door contacts controlled by iStar Door Controller connected to C-Cure 9000 installed on an agency server.
    - 1 Door currently has standalone Motorola Flex Pass reader and a door contact
    - 1 Door currently has door contact operated with a push button we prefer to keep functional
- [redacted] Florida
  - 5 Exterior Doors
- [redacted], Florida (South Location)

One Specification Excludes Most Choices

Overall the spec includes good detail including door descriptions and locations and is non-biased. However, due to the ambiguity in defining 'interoperability' and the listing of a single proprietary type of door controller essentially limits quotes to expansions of that existing system.

Whether this is intended or not is difficult to guess, however it would be much more efficient for both the solicitor and the bidders to state this requirement plainly upfront. The author does not realize the proprietary nature of access systems, they may think they are economically trying to use existing hardware for another system.

However, the lack of detail defining 'interoperability' dooms this option.

Technical Specification

Here are 18 technical aspects to include in every access specification:

Defining Expansion or New Systems

Is this system new, or will it be a scaled addition to an existing system? Divulging this upfront will clarify for all involved what kind of work is being scoped. Due to the proprietary design of most access systems, interoperability is essentially non-existent, and if a system is already in place and satisfactory the best path is likely expanding that platform. This is likely the least expensive option since redundant equipment like servers and software may be avoided and not needed.

Also making this plain potentially avoids mistakenly buying two systems that cannot incorporate each other's equipment. Even if the goal is abandoning an existing system, recovering or reusing some of the existing components is a goal that should be made clear from the start. Special labor or software tools may be needed to transfer existing cardholder information.

Security Goals

Harder to define, but essentially important, is to give a concise explanation of the goals for the access system. Stating "With this system, our facility wants to restrict off-shift staff from entering the premises and keep all but certain individuals from entering <specific areas> at any time" will greatly assist those designing a system in knowing the important features to build around.

Specifically, when access control is confronted by the issue of "Tailgating", knowing where the most sensitive openings are located is key when specifying equipment to offset the risk.

Even when specialty design or equipment is not needed, establishing the rough groups that get access and when/where they need it is the foundation of access control. Making these basic goals clear will help bidders select the right platform with the proper level of assignable features for the stated need.

Restating and examining these goals when expanding an existing system is still essential, as the areas of control and vulnerabilities can change over time. Including a short statement describing 'security goals' can refresh the effectiveness of a system even decades old.

Monitored, Managed, or Forensic

Next is to define how the 'control' aspects of the system will be managed. Is the goal to set everything up initially, and then only access it when absolutely necessary? Will an onsite guard staff actively monitor and respond to events 24/7/365? Or is it better if system oversight and monitoring is active, but farmed out to a central station facility?

Defining just how the system is going to be used and by whom can control costs by avoiding unused features, or by making sure the right people can manage the system at the right time.

Other Systems Integration

Do you want your access control to be combined with video surveillance or intrusion alarms? Do you have a fire alarm system? Making a point to state these goals, complete with the current make/models/versions of the systems to be integrated help drive design and installation labor requirements.

Credentials

If the system is new, important decisions should not be answered by the lowest bid response. If an expansion of an existing system, the answer might already be made. However, in either case, explicitly defining which credential type is desired prevents it from being a purely economic decision. In terms of technology, most access systems use contactless credentials. In the past, 125 kHz credentials have been the mainstay, but due to security concerns (lack of encryption) and limited storage capacity, they have been superseded by 13.56 MHz types. From a cost standpoint, the more advanced credentials are the same price or cheaper than older formats.

If no credentials already exist, deciding the right product is as much security design as an economic one. How many people will be credentialed? Should photo IDs double as badges, or is a more durable option needed? What other systems use credentials, and should they be combined? What about biometrics? Does risk mandate multiple factors are used?

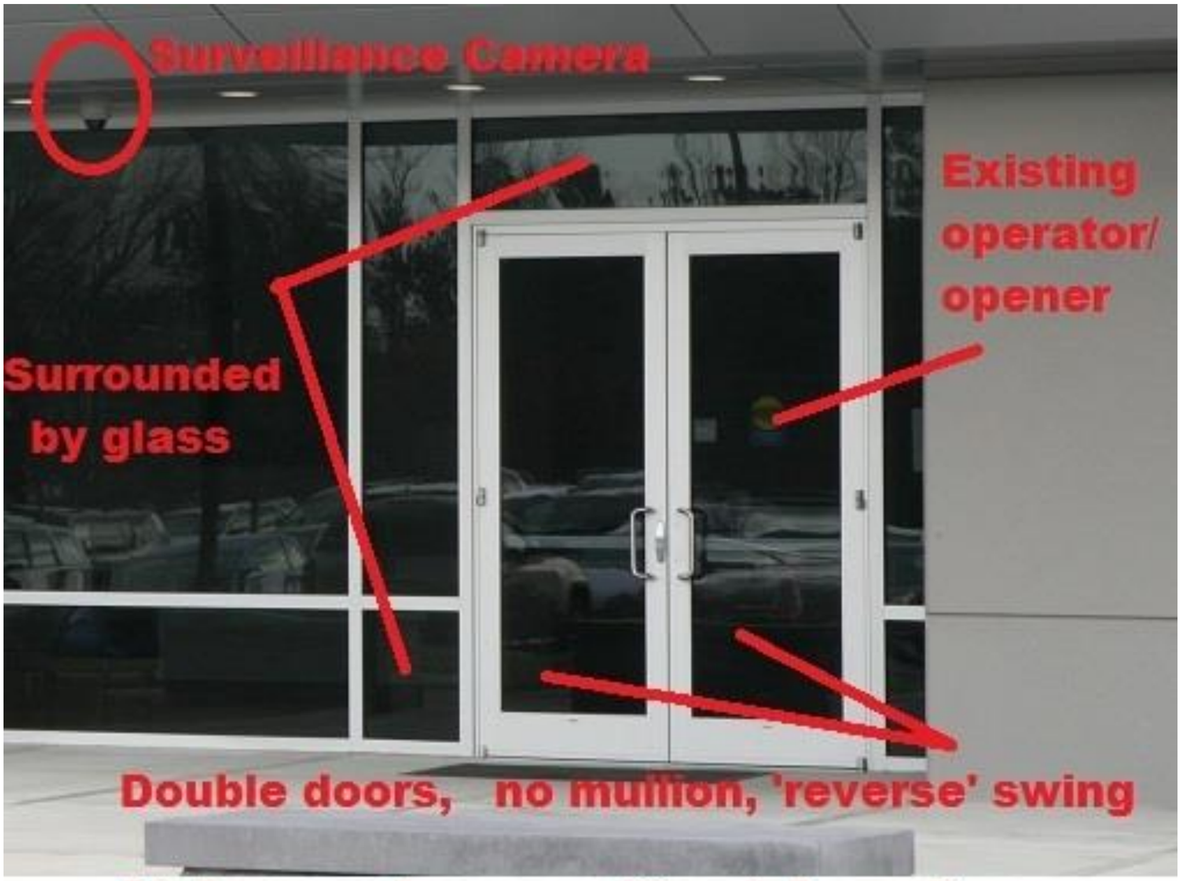
Additionally, if existing facility codes are in use, they should be noted as a specification of the future system. Not all systems are able to work with dynamic codes, and this minor detail may drive significant cost if not made clear.

Doors/Openings Detail

Describing the openings to be controlled is helpful not only from a design perspective but also from potential management changes. No two openings are alike or used the same way, and a short description or picture of the opening and it is used goes far in designing good controls.

For example, the 'main entrance to an office building' is better described as this:

"The main entrance is a set of glass double doors that both swing out. These doors are handicap accessible, and the right side automatically opens and closes when a nearby button is pressed. A nearby security camera should be integrated into the system so that all potential users are recorded as they enter. This entrance is typically used by the public during business hours, but should be locked and only accessible by approved users from 7pm - 6am overnight. Approximately 30 people may need access during a typical night during those hours, including cleaning staff and delivery people. This picture shows the opening:"


Surveillance Camera
Existing operator/ opener
Surrounded by glass
Double doors, no mullion, 'reverse' swing

Pictures enhance written information

Note: Photos need no annotation, just a good clean shot of the opening to be useful.

While not technical, the information provided gives great insight that cannot be observed during a quick job tour and includes door type, door function, security goal, user volumes, and secondary system integration (video). While expert knowledge is not needed, passing on basic details mitigates guesswork.

Door Position Switches

One of the most useful, yet most neglected aspects of access control are the sensors that indicate whether the door is shut or open. While many view DPS as an 'extra', there remains no more effective or inexpensive way to monitor the current state of the opening that these sensors.

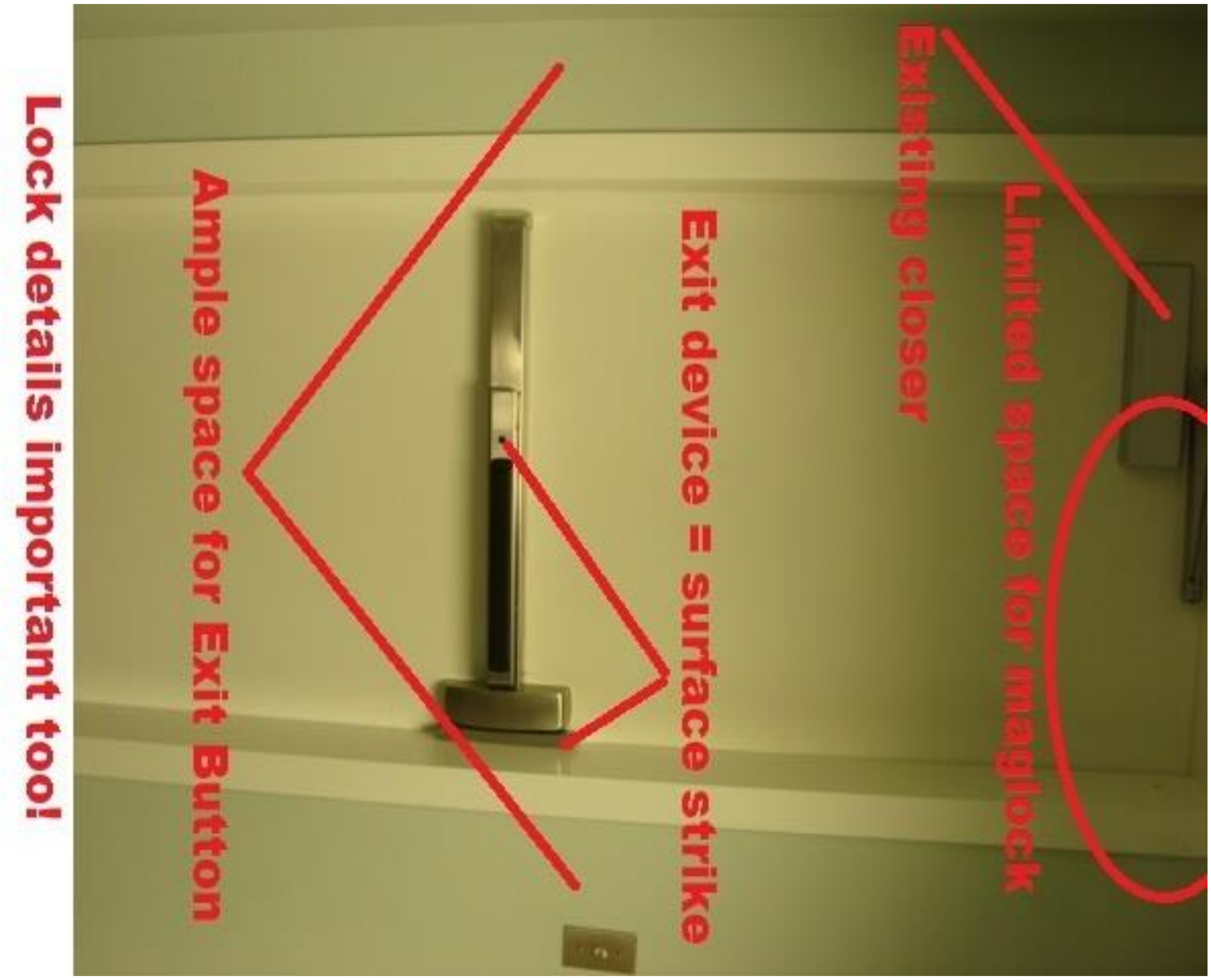
Since they are viewed by some as 'optional', solicitors should explicitly state they want these sensors included. Catch our "Door Position Switches (DPS) For Access Control Tutorial" for more detail. For insights on the biggest barrier to successful use of DPS switches, read "Combating Door Prop Problems" to catch the subtle behavior that totally undermines the access system.

Existing Locks/Hardware

Like doors, expert-level detail is not required, but basic observations are useful. Often access control interoperates with existing mechanical locks, and quick inventory of how each opening is appointed is invaluable to choosing the best method of control.

For each door, a picture or basic written description is useful: "*The back door is a metal (steel) door currently kept closed with a panic bar. The door swings out and has an 'Exit' placard above it. The door can be locked or unlocked from the outside of the door by a key only issued to managers.*

See picture for details:"


Limited space for maglock
Existing closer
Exit device = surface strike
Ample space for Exit Button
Lock details important too!

Choosing Readers

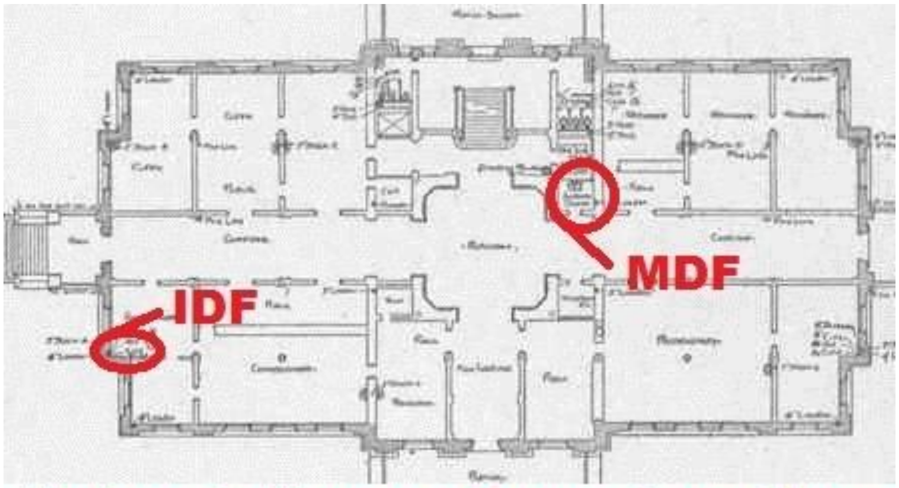
Selecting the right reader is the result of which credentials are used and where the opening is located. From the written descriptions and photos of the doors/locks, good decisions can be made what type to include and where.

Clearly indicating the openings where Multiple Authentication Factors should be used help ensure the right reader is specified to support all credentials needed at that spot.

IP or Serial Networked Systems

The network that ties a system together should be mentioned if existing cabling or LAN should be used. Hard specifying one type over the other can be costly if preference is not strong, although many modern systems use IP networks as the primary option, a trend that will continue.

If existing networks are to be used, making the locations of existing switch rooms clear avoids guesswork or expensive redundancy. Marking a set of floorplans that include these positions part of your specification is vital:



Network /Server Room Locations

If new or dedicated networks are needed, making note of any raceway, main cable trays, or access panels confirms that new cable with run concurrent with existing.

Edge or Centralized Architecture

To a lesser extent, specifying where door control takes place is important. Most modern systems use a form of door controller mounted near the opening, and specifying centralized location of system components could significantly drive cable costs or result in older systems being bid.

Even if 'edge' systems are used, all equipment can be installed behind locked closets or secured enclosures. However, making sure enough space is allocated for those devices is commonly overlooked and can drive costs if not properly considered during spec writing.

Using Power Over Ethernet

In many cases, standard 802.3 af/at PoE can be used to inject power to edge controllers and subsequently connected devices like readers and strikes. Using PoE is generally more convenient and offers online management when separate, stand alone power supplies typically do not.

However, using PoE may limit the range of connected devices based to 'total pass-through' power available, which is usually 750 mA or less, and the max number of doors on a single PoE powered controller are limited to two. Other factors to consider include the rating of the controller contacts, and disclaimers against powering maglocks on a constant basis from a PoE controller are common.

Wired or Wireless

When it comes to controlling cost, hard specification of wired systems can cause prices to skyrocket for remote or hard to reach openings. Especially if those doors are not heavily used, but electronic control and logging is essential, consider using wireless and 'stand-alone' styles of locks.

While the unit cost may be high for a single wireless lock, the overall cost of connecting multiple devices together via a long network run could be more expensive. While the overall price and maintenance associated with wireless locks (ie: replacing batteries) could be prohibitive for entire systems, they could prove an economic fit in lieu of significant wired network expansion.

Using Existing Databases

Especially for larger, multi-site systems, the database can bring significant cost. Assuming the most economical choice will be made is foolish unless the specification explicitly states which database platform may already be available.

User Management

Defining user's needs are a critical aspect of the specification, and one where presuming features will be available is dangerous. Spelling out expected 'Live View' and management control helps designers specify can configure the right platform. If operators need to lock/unlock doors in real time, weekly activity reports are to be created, or if the access system should integrate with the video surveillance system, these requirements should be clear.

Even for systems that are not actively managed, if items like 'remote access' from smartphones or inclusion of 'ID Badge' creation modules, it should not be assumed it will be included unless stated.
Also, if specific workstations are to be used for running clients, description of their location and build specifications should be listed so deploying the system to operators is confirmed.

Special Features: Access control is useful for more than just unlocking doors. Many systems include options for 'Time and Attendance' logging that essentially replaces a time clock, or 'Mustering' that grants you special reporting that that provide a roster of occupants in a particular area.
If these features are desired, or any other integrations falling outside the core access control functions, effort should be spent defining the desired result in specification documents.

Maintenence Costs

Finally, specifications should spell out any ongoing annual software maintenance costs and any additional ongoing expenses required to keep the system current and operational. Some platforms have no ongoing maintenance plan, while others require a yearly plan and may not prioritize service or tech support if not current.

The cost of this maintenance should figure into system selection, as a system may be thousands less when initially installed, but add thousands in unrealized costs in subsequent years.

Access Control Specification Form

The following section provides a summary of each requirement and common options to consider. We recommend you copy and paste this into your own documents and use it as a starting point in defining the requirements for your access systems.

Opening/Door Type: Often best depicted in a picture. If not permitted, a short written description describing: Steel, wood single or double door? Right, left, or swing 'reverse'. Glass opening? Turnstile?

Users per Hour: Average number of users during busy times, so that cycle times of locking hardware can be sized accounting to the busiest period the door permits access.

Opening's Security Goals: The high-level purpose of access control: "Restrict unapproved users from entering during overnight hours" or "Only residents with current rent payments should be allowed to use gym facility."

Other Equipment on the Door: Often best expressed in a picture, a snapshot or written description of the other hardware devices hung on the opening. Examples: "Closer on upper hinge side, vertical rod on upper strike side, and an exit device hung on the inside. Outside keyed access."

Reader Type/Mounting Position: On the door frame (mullion), or on an adjacent wall? Are mounting surfaces suitable? Are they protected/sheltered from ice and snow? Can someone is a wheelchair or with limited range of movement reach the reader, per ADA (or similar)?

Credentials to Use/Multiple Authentication Needed: Common Choices: 125 mHz, 13.56 MHz contactless. HID format, MiFARE/DESFire? 26,33,34,35 bit cards? Facility code needed? Is more than one credential needed at the door to verify the user?

Intercom Needed?: If a user cannot enter the door, or if a visitor request entrance, can they page help or an attendant? Two two-way conversations need to be supported?

Lock Type Needed: Choices- typically electric strikes or maglocks, but dictated by building code, AHJ preference, and type of hardware existing on the door.

System Network Type: TCP/IP, Serial hardwire, wireless, or stand alone locks? If IP, are existing LAN segments available? Are cable pathways and data closets marked? If wireless, the signal strength at doors verified?

Controller Types: Choices- Edge or Centralized? Standalone or host dependent?

Critical User Management Features: What real-time features required? What type of reporting is needed? Will users need access from a browser or mobile devices? Are client workstations available?

Server Space/Preference?: Do you have available resources in the server stack? Are they physical or virtual? Do you need your servers to host access locally or remotely? Including this ensures no ugly incompatibilities happen at the last minute. If a new server is used, will local IT resources be familiar with configuration and support?

Database Platform Needed: Does you enterprise already use a standard database platform like SQL? If so, make note so the access system can plan to make use of existing rather than purchasing new or using a proprietary platform.

Special Features: Do you need Time & Attendance or Mustering? If so, does your hardware design support those features? Make note of the 'other systems' you would like access control to feed into or use like video surveillance or intrusion alarm.