

## Revolutionizing Building Physical Security

If you're a building owner with multiple tenants, you likely have a physical security system from one vendor. It was expensive to deploy because of the high cost for proprietary door panels and their proprietary software. You also probably get requests from tenants wanting to deploy their own security systems and also integrate with their identity management systems. You likely don't allow this or it's a hassle to achieve. Finally, you also probably have identities stored in your physical security system that are not cleansed quickly when the identity leaves one of the tenants. This results in you being left with not only their access rights active BUT it may contain sensitive personal data like their medical condition that makes you liable to personal information infringement after they've gone.

How would you like to drop the cost of the physical security system, easily allow your tenants to take over some management of the security system with you still having over-ride, easily integrate with their identity management systems and also quickly purge identities when they leave a tenant? That's what this article will describe. First, a little about me:

I'm an independent identity management expert who has several times integrated physical and logical security systems in large Fortune 500 enterprises. I was appalled at:

- Proprietary code physical security vendors used
- High cost of door panels and the fact that it tied you, the customer, into the vendor
- Lack of integration capabilities with identity management software

At great cost, I would rip out different vendors products and replace them with one vendor where we could integrate with identity management. Then along came companies like [Quantum Secure](#) and [Alert Enterprise](#) that acted as a bridge between different physical access systems and identity management. While this was good, it didn't address the high proprietary cost of physical security.

There is a problem with identity management systems however. They all use role based access control (RBAC) as their main access model. This only works where the roles map to an entitlement - application access or, in the case of physical security, access to physical area. As many building security people know, there are "oodles" of exceptions for physical access making department or financial roles ineffective. (I reference the reader to a NIST draft paper published last year "[A Survey of Access Control Models](#)" that clearly explains this).

In past white papers I have written I was predicting that one day TCP/IP (i.e. the internet) would commoditize these systems, dramatically lower cost, allow for easy interoperability and easily integrate with identity management systems. That day is now here!

[Viscount Security](#) has very recently introduced TCP/IP door panels that are very inexpensive. This means that you can now not only deploy physical security systems cheaply BUT it also runs over your existing network cabling! No more getting locked into a vendor for a very long time. It will be possible

to then segment the network and in the future have you, the building owner, delegate management of the physical security to the tenant with you still having over-ride capability.

From an enterprise point of view, as a building owner, you need to have maximum flexibility in dealing with your tenants. For example, consider a use case where a client has external auditors and lawyers in to work on a merger. They want to have a series of rooms available to them and have only certain members of the enterprise able to access those rooms. In the past, this would involve numerous calls to the front security desk to get all this set up.

If they had the Viscount system and were going to automatically create the policies for this using their own traditional identity management systems, this wouldn't be easy because of roles. However, there is also a new solution to this.

[Axiomatics](#), is a young company that offer policy based attribute access control using open standards of XACML (eXtensible Access Control Markup Language) and SAML (Secure Assertion Markup Language) which is applicable to both logical and physical access. This allows the tenant to quickly create policies that say "allow anyone with the attribute of MERGER to access room 1, 2 and 3". No special roles have to be created! Note also from the Tenant's point of view that they can as easily also specify access control policies for the lawyer, auditors and special staff for their own network and applications using Axiomatics i.e. their logical layer.

Having a physical security system that easily integrates with your tenants' identity management system, means that you can now transfer some of the liability to your tenant for creating, modifying, removing and archiving identities from the physical access system. For example, let's say that Tennant One has their own identity management system. In the future, you and they will include in your tenancy agreement that they will be responsible for creating, modifying, terminating and archiving access as well as automatically passing these to your master physical identity management system.

Thus when "Guy" is hired by Tennant One, their identity management system will automatically create the identity for Guy, assign him rights to their floors and rooms and then automatically notify your physical identity management system. This way you will know who has access to the floor and rooms in case of an emergency. If Guy has a medical condition, then the tenancy agreement will specify that the tenant's identity management system must notify your physical identity management system. So if Guy has a diabetic attack in your building, the security guard on the scene should know this from the building systems and then assist in notifying the ambulance team that's arriving. When Guy is terminated, Tenant One's identity information will be automatically removed not only from their system but also from your building identity management system, thus reducing your risk.

For your tenants that don't have identity management systems, then you, the building owner, can use your own identity management system one in combination with Axiomatics and easily create policies, delegate administration and have easy flexibility in dealing with your tenants.

Since Viscount is TCP/IP based, this also means that you can quickly add different authentication devices to your physical security system. For example, I am working with them to use cell telephones to access certain facilities (e.g. remote sub-stations, pump houses, etc.).

I want to develop policies in Axiomatics that specify to give access to the facility if the person belongs to certain groups, or have a special access attribute and also have attributes specifying requisite training which then allow them to use their cell phone to open the door. Note that often training certification comes from outside enterprises. So how does the identity management system know this? For example, let's say that Tenant One has a sensitive area in a facility that you own. When "Guy" approaches the door and dials a specific number, here is what could happen.

The cell phone number is reviewed by an Axiomatic security policy that specifies that Guy must have a training attribute from Acme Inc. The Axiomatic server would either go to the Tenant One's LDAP directory, or go to the HR Training database or go to Acme's database/directory and see if Guy has the attribute. If he does, then he is allowed entry. The access to the door record can also be sent to your physical identity server to show who had access to the door historically.

## Summary

It is the early days of a revolution! It is becoming possible to wean yourself off of proprietary physical security vendors and manage this at much lower cost and flexibility. Please email me or call me if you'd like to learn more or participate in this.

## About the Author

Guy Huntington has been in the identity industry for the last 13 years. He has rescued several large Fortune 500 identity projects and written numerous white papers on identity and physical and logical access and integration (<http://www.authenticationworld.com/papers.html>). Guy can be reached at [guy@hvl.net](mailto:guy@hvl.net) or 1- 604-861-6804.