Are you enterprise ready?

Hexicurity
SimpleAccess

Innovation in Access Control Integration

A solution for today's business environment

Mobile workforces of today's global teams work long hours in varied locations. Today they may be working in Dallas. Tomorrow morning will find them in Chicago. Next week they will be working overnight in New York.

Access integration is not just a convenience; it is a necessity for these road warriors. Whether closed building requiring credentialed access twenty-four by seven or open building after-hours access, integration is key to productivity.

Identity theft is forcing company boards to limit access to employee lists. A real solution must keep employee data within the corporate envelope. Confidentiality is critical.

With mobility comes fluidity, Security must not impede new hires. In stark contrast, it is critical to stop separations at the building door. Integration must be accurate.

Any solution must work every time and without maintenance downtime. Reliability is key.

Further, today's hackers and state-sponsored industrial spying look for any way into a company. Any solution must not expose the organization's IT assets to hackers. The best method is called an air gap, eliminating two-way communication. Information security is important.

TransVerify® devices adapt to doors, turnstiles, elevators, and dispatch systems. The back office workflow is identical for the turnstiles in the lobby and the back door into the suite.

Our patented solution works with all contemporary access control systems. The organization can enjoy all the benefits of TransVerify across their enterprise.

We give special consideration to communications. Networks are two-way thoroughfares; our solution uses two dedicated one-way paths. Only Wiegand data, a number, can use the first track into the company. A humble yes or no is the only thing allowed to return. We call this a virtual air gap, a credential number flows in, and only a yes or no flows out.

- Above, client employees present a card to the turnstile (A) to enter the elevator lobby.
- Credential data flows to the Base Building access control panel (B) and the Distributors (C).
- The Distributor encodes and transmits the credential to the Verifiers (D) over an isolated security network.
- The Verifier decodes and presents the credential to the client's access control system (E).
- The client verifies the credential as authorized and gives an indication back.
- The Verifier (D) encodes and transmits that verification back to the originating Distributor (C).
- The Distributor closes a circuit releasing the turnstile (A).

Could you benefit from building access innovation? Contact us for details. A factory trained engineer will respond to your questions.

www.TransVerify.com
sales@hexicurity.com
832-380-4878

A security director considering her options for integrating a new lease space with their current access control system.

InfoSec vetoed sending a complete employee list daily outside the corporate envelope for security. The organization is too large and fluid to carry two cards. Wiegand splitters won't work because the constant alarms of other tenant cards would blind her monitoring to real alerts.

She chose TransVerify® because it gives her the same employee access fidelity of her suite doors at the building perimeter.

Basic System
Distributor - Verifier

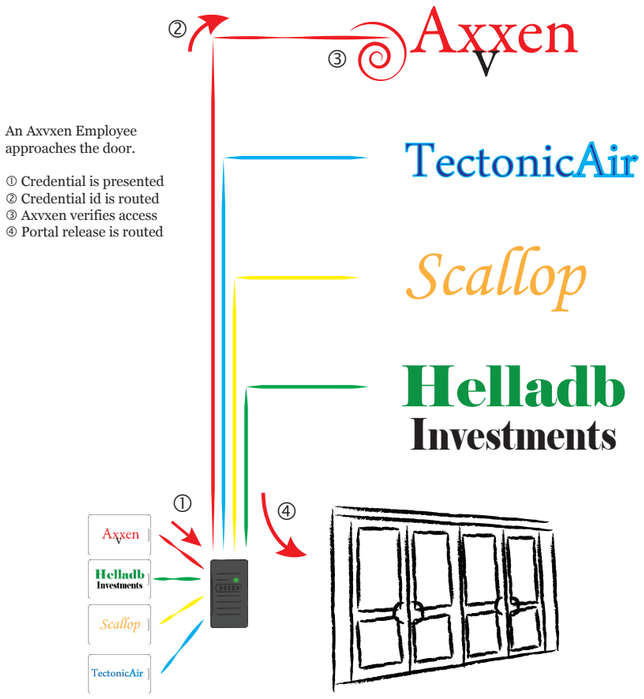
Doors, Gates, and Turnstiles

TransVerify® simplifies tenant access. This system eliminates duplicate data entry, file transfers, and card database synchronization issues. A Distributor monitors each card reader echoing card reads to the tenant via our Verifier. Upon tenant approval, a release signal is directed into the door control panel granting access.

In other words, **Simple***Access*.

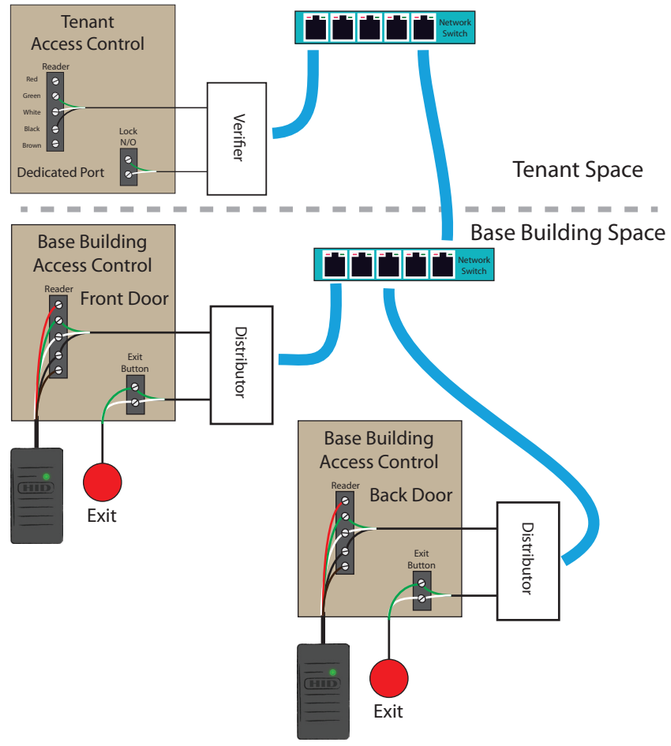
Transverify System Walkthrough

www.transverify.com



Covered under US Patent US8370911B1

Simplified Diagram
Two Doors - One Tenant

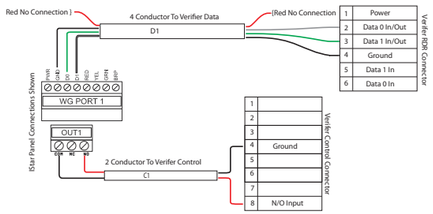


The Distributor shares all card reads with the Verifier. The Verifier relays only the tenant's cards to the tenant's access control system. If the tenant approves the card, a release signal is transmitted to the originating Distributor. The Distributor directs the release into the panel REX circuit. The base building grants access to door.

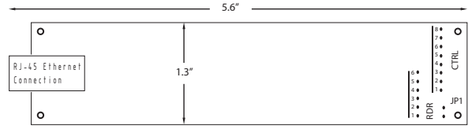
Note:
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Verifier Component

Verifier Connection



Considerations for Verifier Board Layout



RDR Connections
1 - Pwr - Red
2 - Data 0 - Green
3 - Data 1 - White
4 - Gnd - Black
5 - rfu
6 - rfu

CTRL Connections
1 - rfu
2 - rfu
3 - rfu
4 - N/O - Blue
5 - rfu
6 - rfu
7 - rfu
8 - C - Orange

JP1
No Jumper if in parallel with panel

Jumper if pullup required (4.7K to 5vdc)

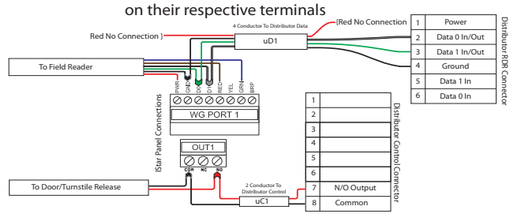
Specifications

Pseudo Reader Output	Industry Standard Wiegand (Data 1 and Data 0)
Card Compatibility	Wiegand 26 - 64 Bits
Contact Monitor Time	.25 to 10 seconds
Communications	10BaseT / 100BaseT Ethernet
Network Cable	Category 5 or better
Tenant Interface Cable	Six Conductor 22 Gauge
Distributors Supported	1024
Facility Codes Relayed	Up to 4 user selectable 32 Bit, one user specified 64 Bits or All
Security	AES 128 CBC PSK
Mating Connector Housings	Molex 22-01-3067, 22-01-3087
Queue Size	7 Card Reads
Power	9 VDC 120 ma
Agency Approvals	FCC Part 15 Sub Part B Class A

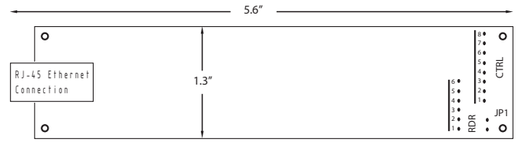
Distributor Component

Typical Distributor Connections

D0 (Grn) , D1(Wht) , and GND (Blk) are connected in parallel on their respective terminals



Considerations for Distributor Board Layout



RDR Connections
1 - Pwr - Red
2 - Data 0 - Green
3 - Data 1 - White
4 - Gnd - Black
5 - rfu
6 - rfu

CTRL Connections
1 - rfu
2 - rfu
3 - rfu
4 - rfu
5 - rfu
6 - rfu
7 - C - Blue
8 - N/O - Orange

JP1
No Jumper if in parallel with panel

Jumper if pullup required (4.7K to 5vdc)

Specifications

Reader Input	Industry Standard Wiegand (Data 1 and Data 0)
Card Compatibility	Wiegand 26 - 64 Bits
Release Time	.25 to 10 seconds
Communications	10BaseT / 100BaseT Ethernet
Network Cable	Category 5 or better
Building Interface Cable	Recommended 22 Gauge
Verifiers Supported	Up to 16
Mating Connector Housings	Molex 22-01-3067, 22-01-3087
Security	AES 128 CBC PSK
Power	9 VDC 120 ma
Agency Approvals	FCC Part 15 Sub-Part B Class A

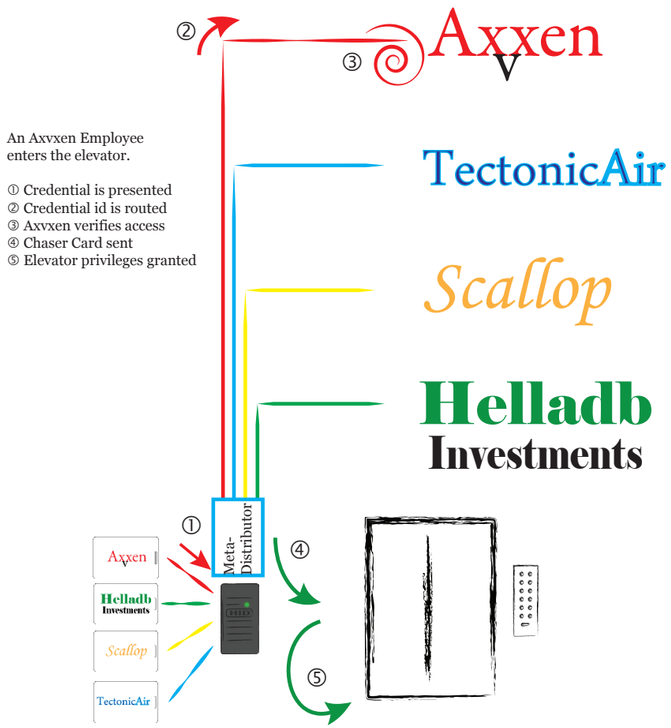
MetaSystem
MetaDistributor - MetaVerifier

Elevators, Dispatch, and HVAC

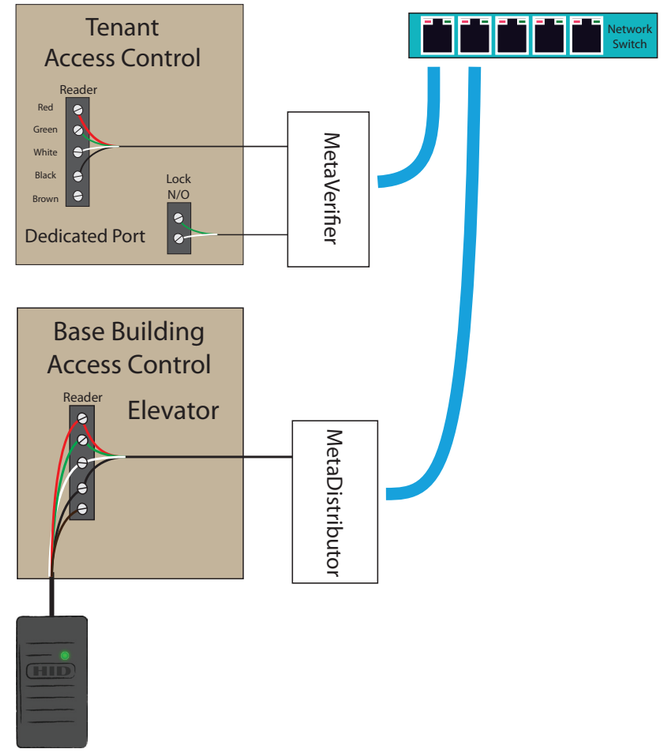
TransVerify® simplifies tenant access. This system eliminates duplicate data entry, file transfers, and card database synchronization issues. A MetaDistributor monitors each elevator card reader echoing card reads to the tenant via our MetaVerifier. Upon tenant approval, a chaser card is directed into the elevator control panel granting access to the floors associated with the chaser card. Also works with HVAC and the new elevator Dispatch systems.

In other words, **Simple***Access*.

MetaDistributor System Walkthrough
www.transverify.com



Simplified Diagram
One Elevator - One Tenant

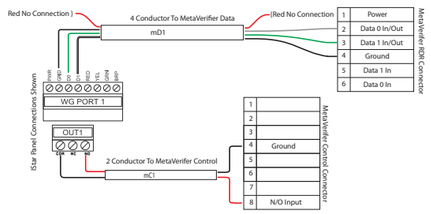


The MetaDistributor shares all elevator card reads with the MetaVerifier. The MetaVerifier relays only the tenant's cards to the tenant's access control system. If the tenant approves the card, a chaser card is transmitted to the originating MetaDistributor. The MetaDistributor directs the chaser card into the elevator's card reader input. The base building grants the access to floors associated with the chaser card.

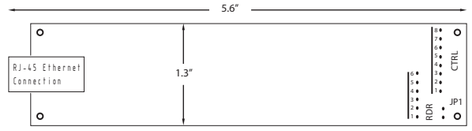
Note:
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

MetaVerifier Component

MetaVerifier Connection



Considerations for MetaVerifier Board Layout



RDR Connections
1 - Pwr - Red
2 - Data 0 - Green
3 - Data 1 - White
4 - Gnd - Black
5 - rfu
6 - rfu

CTRL Connections
1 - rfu
2 - rfu
3 - rfu
4 - N/O - Blue
5 - rfu
6 - rfu
7 - rfu
8 - C - Orange

JP1
No Jumper if in parallel with panel

Jumper if pullup required (4.7K to 5vdc)

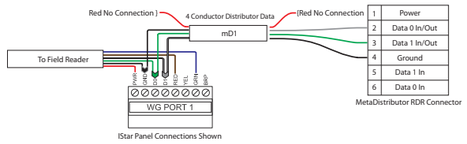
Specifications

Pseudo Reader Output	Industry Standard Wiegand (Data 1 and Data 0)
Card Compatibility	Wiegand 26 - 64 Bits
Contact Monitor Time	.25 to 10 seconds
Communications	10BaseT / 100BaseT Ethernet
Network Cable	Category 5 or better
Tenant Interface Cable	Six Conductor 22 Gauge
MetaDistributors Supported	1024
Facility Codes Relayed	Up to 4 user selectable 32 Bit, one user specified 64 Bits or All
Security	AES 128 CBC PSK
Mating Connector Housings	Molex 22-01-3067, 22-01-3087
Queue Size	7 Card Reads
Power	9 VDC 120 ma
Agency Approvals	FCC Part 15 Sub Part B Class A

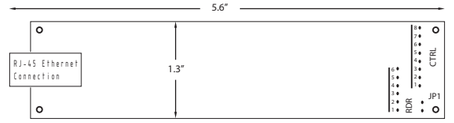
MetaDistributor Component

MetaDistributor Parallel Connection

D0 (Grn) , D1(Wht) , and GND (Blk) are connected in parallel on their respective terminals



Considerations for MetaDistributor Board Layout



RDR Connections
1 - Pwr - Red
2 - Data 0 Out - Green
3 - Data 1 Out - White
4 - Gnd - Black
5 - Data 1 In - White
6 - Data 0 In - Green

CTRL Connections
1 - rfu
2 - rfu
3 - rfu
4 - N/O - Blue
5 - rfu
6 - rfu
7 - rfu
8 - C - Orange

JP1
Jumper if pullup required (4.7K to 5vdc)

Specifications

Pseudo Reader Output	Industry Standard Wiegand (Data 1 and Data 0)
Card Compatibility	Wiegand 26 - 64 Bits
Contact Monitor Time	.25 to 10 seconds
Communications	10BaseT / 100BaseT Ethernet
Network Cable	Category 5 or better
Tenant Interface Cable	Six Conductor 22 Gauge
MetaVerifiers Supported	16
Facility Codes Relayed	Up to 4 user selectable 32 Bit, one user specified 64 Bits or All
Security	AES 128 CBC PSK
Mating Connector Housings	Molex 22-01-3067, 22-01-3087
Power	9 VDC 120 ma
Agency Approvals	FCC Part 15 Sub Part B Class A

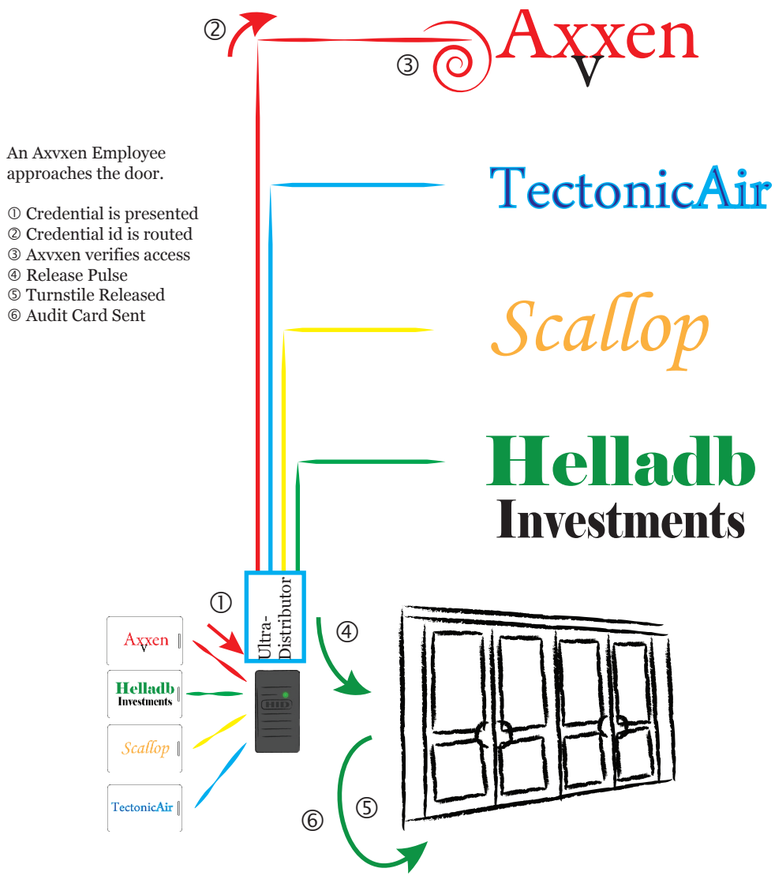
UltraSystem

UltraDistributor - UltraVerifier

Doors, Gates, and Turnstiles

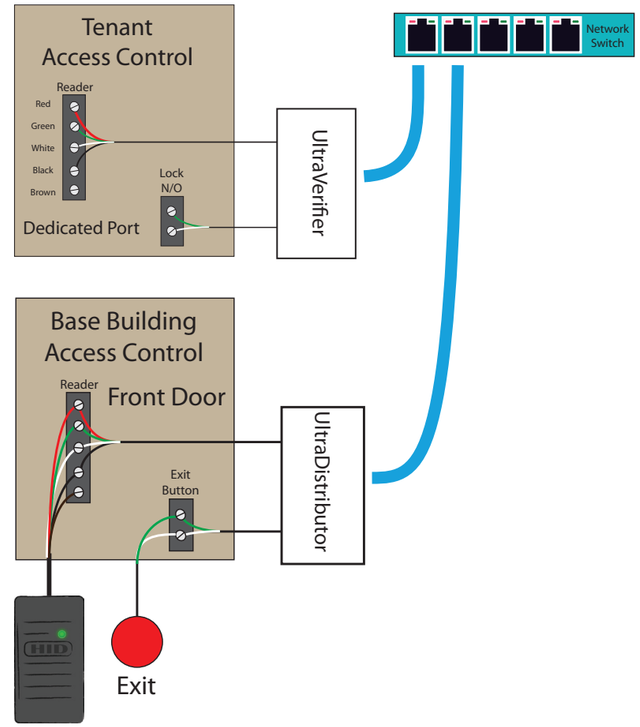
TransVerify® simplifies tenant access. This system eliminates duplicate data entry, file transfers, and card database synchronization issues. Each UltraDistributor monitors a base building card reader, sharing tenant card reads via the UltraVerifier. Upon tenant approval, a quick release is sent to the associated base building door, turnstile or gate followed by an audit card directed to the base building.

In other words, **Simple***Access*.



Covered under US Patent US8370911B1 US9019071B1 & US9165123B1

Simplified Diagram
One Door - One Tenant

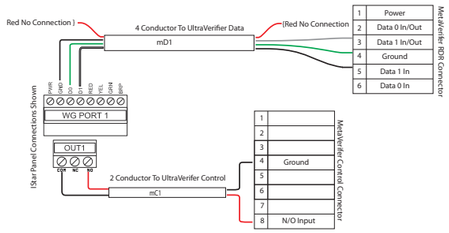


The UltraDistributor shares all front door card reads with the UltraVerifier. The UltraVerifier sends only the tenant's cards to the tenant's access control system. If the tenant approves, quick release is sent to the front door. That release pulse is followed by an audit card directed into the base building's card input. The audit card identifies the access to the base building as authorized by that tenant.

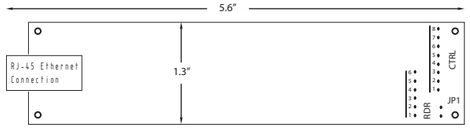
Note:
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

UltraVerifier Component

UltraVerifier Connection



Considerations for UltraVerifier Board Layout



RDR Connections
1 - Pwr - Red
2 - Data 0 - Green
3 - Data 1 - White
4 - Gnd - Black
5 - rfu
6 - rfu

CTRL Connections
1 - rfu
2 - rfu
3 - rfu
4 - N/O - Blue
5 - rfu
6 - rfu
7 - rfu
8 - C - Orange

JP1
No Jumper if in parallel with panel

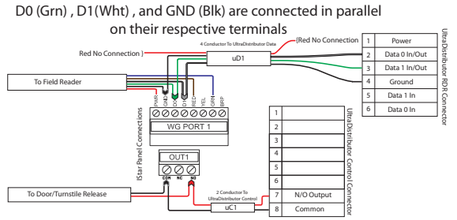
Jumper if pullup required (4.7K to 5vdc)

Specifications

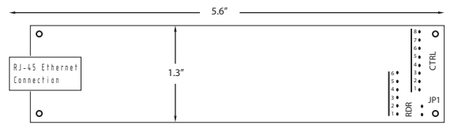
Pseudo Reader Output	Industry Standard Wiegand (Data 1 and Data 0)
Card Compatibility	Wiegand 26 - 64 Bits
Contact Monitor Time	.25 to 10 seconds
Communications	10BaseT / 100BaseT Ethernet
Network Cable	Category 5 or better
Tenant Interface Cable	Six Conductor 22 Gauge
UltraDistributors Supported	1024
Facility Codes Relayed	Up to 4 user selectable 32 Bit, one user specified 64 Bits or All
Security	AES 128 CBC PSK
Mating Connector Housings	Molex 22-01-3067, 22-01-3087
Queue Size	7 Card Reads
Power	9 VDC 120 ma
Agency Approvals	FCC Part 15 Sub Part B Class A

UltraDistributor Component

Typical UltraDistributor Connections



Considerations for UltraDistributor Board Layout



RDR Connections
1 - Pwr - Red
2 - Data 0 - Green
3 - Data 1 - White
4 - Gnd - Black
5 - rfu
6 - rfu

CTRL Connections
1 - rfu
2 - rfu
3 - rfu
4 - rfu
5 - rfu
6 - rfu
7 - C - Blue
8 - N/O - Orange

JP1
No Jumper if in parallel with panel

Jumper if pullup required (4.7K to 5vdc)

Specifications

Pseudo Reader Output	Industry Standard Wiegand (Data 1 and Data 0)
Card Compatibility	Wiegand 26 - 64 Bits
Contact Monitor Time	.25 to 10 seconds
Communications	10BaseT / 100BaseT Ethernet
Network Cable	Category 5 or better
Tenant Interface Cable	Six Conductor 22 Gauge
UltraVerifiers Supported	16
Facility Codes Relayed	Up to 4 user selectable 32 Bit, one user specified 64 Bits or All
Security	AES 128 CBC PSK
Mating Connector Housings	Molex 22-01-3067, 22-01-3087
Power	9 VDC 120 ma
Agency Approvals	FCC Part 15 Sub Part B Class A

14 Channel Enclosure

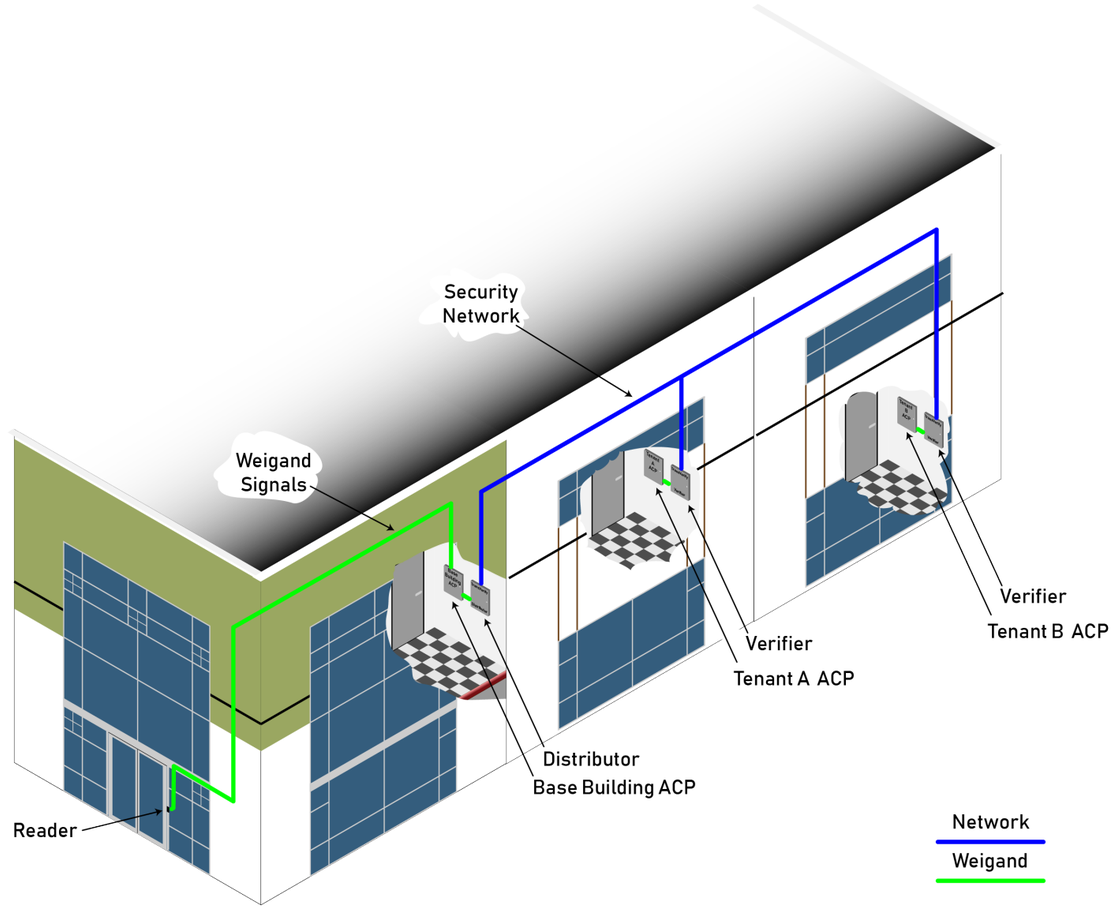
Wall Mount Enclosure

TransVerify® simplifies tenant access. This system eliminates duplicate data entry, file transfers, and tenant complaints about card database problems. The Distributor monitors a base building card reader, relaying tenant card reads to the tenant via our Verifier. Upon tenant approval, access is granted to the associated base building door, turnstile or gate.

In other words, **Simple***Access*.

Door Mounted
Network Switch

Stainless Steel
Backplane with
Power supply and fusing



Specifications

Enclosure Size	24 by 20 by 6.62 Inches
Backplane Size	21 by 18 1/2 by 5 inches
Enclosure Compatibility	Hoffman A24N20ALP
Mounting Height	2 meters maximum
Power Supply	9 Volts @ 2 Amps
Communications	10BaseT / 100BaseT Ethernet
Network Cable	Category 5 or better
Mini-GBIC	2 Ports Avalible
Distributors / Verifiers Supported	Up to 14
Mating Connector Housings	Molex 22-01-3067, 22-01-3087
Agency Approvals	IEC 62368-1:2014 (Second Edition)
Temperature	0 ºC to 30 ºC
Maximum Altitude	2000 meters
A/C Power Requirement	120 Volts at 1.75 Amps

White Papers and Application Notes

Cyber-Risks of Physical Access Control Systems

The Danger of Legacy Procedures

Physical access control systems, card reader systems, use personally identifiable information (PII) to authorize access. For organizations owning all structures they occupy, the cyber-risks associated with physical access control are the same as with any other database holding PII and therefore outside the scope of this paper.

This paper focuses upon the cases where tenant operations occur in leased spaces such as multi-tenant high rise buildings. This scenario presents the most risk to an organization for PII loss and the potential for lawsuits, hacker opportunity, and government sanctions.

Property ownership's doors, turnstiles, gates, and elevators must be accessed to reach the tenant lease space. The most common techniques used by property management utilizes tenant employee PII to enable access through base building card readers. The building access control system uses this data for either after hours (ASIS[1] open buildings) or at all times (ASIS closed buildings) access. These legacy techniques force the tenants to disclose employee PII to the base building.

These techniques were developed in the late 1980s[2] and predated any cyber-risks considerations. Organizations have widely deployed this legacy technique due to the lack of viable alternative solutions.

The focus of this paper is stanching this flow of employee information outside the corporate envelope, improving efficiency, and tightening security.

Conventional Methods

Base buildings commonly use three techniques for tenant access into base buildings; Dual Cards, Dual Entry, and Parallel Control. We will examine these three methods while illuminating the cyber-risks, enterprise considerations, costs, and other factors.

1 American Society for Industrial Security
2 September 1991 Access Control Vol 34 #10 page 1; Future of Access Control tied to Integration by George Mallard

Dual Cards

This first method distributes a separate building credential to every tenant employee. This technique suffers several weaknesses: unauthorized card passing, expense, and employee time. However, the setup is very inexpensive for this method.

Cyber-Risks:

Advesarial Lateral Movement

The risk of a cyber adversary making a lateral move, spreading a computer infection, from the base building to tenant or tenant to tenant is neglible with this method.

Compromise by users

Managers solve problems, and front-line managers often solve one problem only to create a more insidious problem. To address cost and save employee time, managers often resort to a credential cache (or more conventionally a pile of building access cards in their desk), which the manager hands out as needed, but without proper accounting for who has which card. This decoupling of credential from an individual makes any tracking or control impossible which poses a significant cyber risk via physical access by the unauthorized.

Enterprise Considerations:

This technique does not scale well. Enterprises will struggle to implement and maintain proper controls on base building credentials.

Expense:

Startup costs

Minimal, a simple procedure needs to be implemented and communicated to employees.

Ongoing costs

Most base buildings charge either directly on indirectly through the lease for access cards. Typical charges are twenty dollars a credential.

Many implementations require the employee to visit building management for a building credential, wasting what is arguably a valuable asset, employee time.

Other Considerations

Controls on card distribution

Any restrictions on the distribution of building ownership's cards are entirely manual; credentials can remain active for years after employee separation, loss or transfer. Ownership seldom personalizes credentials with the employee photograph, further exasperating control issues.

Dual Entry

This method entails transferring the PII of an employee and their tenant issued credential number either through actual keyboard entry into another system or a periodic file transfer. Weaknesses of this technique include exposing all employee activity to third parties, expense, localized procedures, maintenance, and latency. The setup has some costs associated with it, but lower than methods other than dual cards.

Cyber-Risks

Advesarial Lateral Movement

The risk of an cyber adversary making a lateral move, spreading a computer infection, from the base building to tenant or tenant to tenant is neglible to high with this method, depending upon the implementation details. The highest risk comes with transferring files between organizations, the lowest risk is where the base building manually enters tenant credentials from paper transmittals.

Trustee Security Implications

Building ownership data security may pose a cyber-risk. With only a few exceptions, ownership's data protections do not meet the tenant's standards for handling PII. If the base building systems become compromised, the adversaries have a full updated list of the tenant's employees and their activities.

C-Suite Activity Exposed

All commercial grade access control systems track credential activity, exposing the coming and going of employees by anyone who has access to the base building access logs. This activity can indicate critical business activity (like mergers and acquisitions), by observing activity patterns of c-suite occupants.

Ultimate Phising List

Further, as the employee data list is frequently updated, it is a simple matter to identify both new hires for phishing attacks and employee separations for compromise with database comparison analysis. Targeting new hires for phishing attacks using this data is trivial since organizations typically standardize the mapping between name and email address.

Security Director Investigations

Finally, insider threat investigations requiring building access logs can expose confidential parameters. For example, the investigation subject happens to be romantically involved with the building secretary, who runs the reports.

Enterprise Considerations

Localized Procedures

A large tenant organization leases office space from many different management companies. Since there is no global standard for PII transfer, thus a variety of techniques have flourished. Diversity is a challenge to scaling or securing this solution thwarting any attempt to standardize.

Expense

Startup Costs

The typical costs and risks associated with a small software project coordinated between two entities, the tenant and the building, should be anticipated

Ongoing costs

A security director of a respected financial services company quoted their IT group charges 40K$ per year for file transfers per building serviced.

Proper database practice to assure database synchronization requires periodic audits of any technique that duplicates a database across disparate systems. Auditing is typically a manual or semiautomatic process that is an ongoing expense.

Other Considerations

Latency

The time between a tenant disabling a credential and denying the credential at the base building portals can be up to forty-eight hours depending upon the system configuration. We have seen floppy disks employed as transport media between the tenant and the base building.

Parallel Control

In this method, the base building and tenant access control systems are electronically coupled, sharing credential activity in real time. Each base building reader directly shares its data with the ownership and tenant systems. This coupling enables the tenant to manage their credential holders confidentially.

Wiegand Splitter

Typical weaknesses include expense, data flooding, compatibility, control, and extension of the security network beyond the corporate envelope.

Cyber-Risks

Extension of Security Network

Parallel control typically deploys tenant access control panels (ACP) adjacent to the base building controls. Tenant ACPs require connectivity, usually network connectivity. The connectivity extends the security network beyond the corporate envelope and can expose critical infrastructure to adversaries.

Data Flooding

Wiegand splitters do not filter card reads. Any tenant system will see and record all building activity. Further, access control systems typically mark invalid card reads as critical. The resulting flood of events can create alert fatigue, overwhelming effective alarm monitoring by the tenant.

Surveillance

In addition to extending the network beyond the corporate envelope as addressed above, unauthorized surveillance risks exist. The tenant systems see all credential activity in the building, enabling tenant surveillance of other tenants possibly leaking competitive information.

Advesarial Lateral Movement

The risk of a cyber adversary making a lateral move, spreading a computer infection, from the base building to tenant or tenant to tenant is neglible with this method.

Enterprise Considerations

This technique scales well as the base building becomes an extension to the tenant's security system.

Expense

Conventional parallel controls duplicate the building access controls. Every base building portal has reader ports both on the ownership's system and the tenant system. Duplication is expensive in terms of equipment, installation, and maintenance.

Other considerations

Compatibility

For the modern office tower that integrates elevators into the security plan, parallel control becomes a technical challenge to deploy. Elevator floor select, elevator dispatch, and HVAC controls are now standard building amenities, requiring a nuanced response defining authorized floors for the credential. Nuanced control is beyond the capability of Wiegand splitters.

Further, while the data sharing has a device, the Wiegand splitter, the actual circuits that release the portals are typically developed ad-hoc by installing technicians with varying degrees of skill. We have seen literal rat's nest of wires, relays, and diodes controlling doors in downtown office towers. It is rare to find these ad-hoc implementations documented, making the system difficult to troubleshoot. In addition to being difficult to service, they may introduce life-safety issues in the event of a fire or other emergency conditions.

Proposed Solution, TransVerify

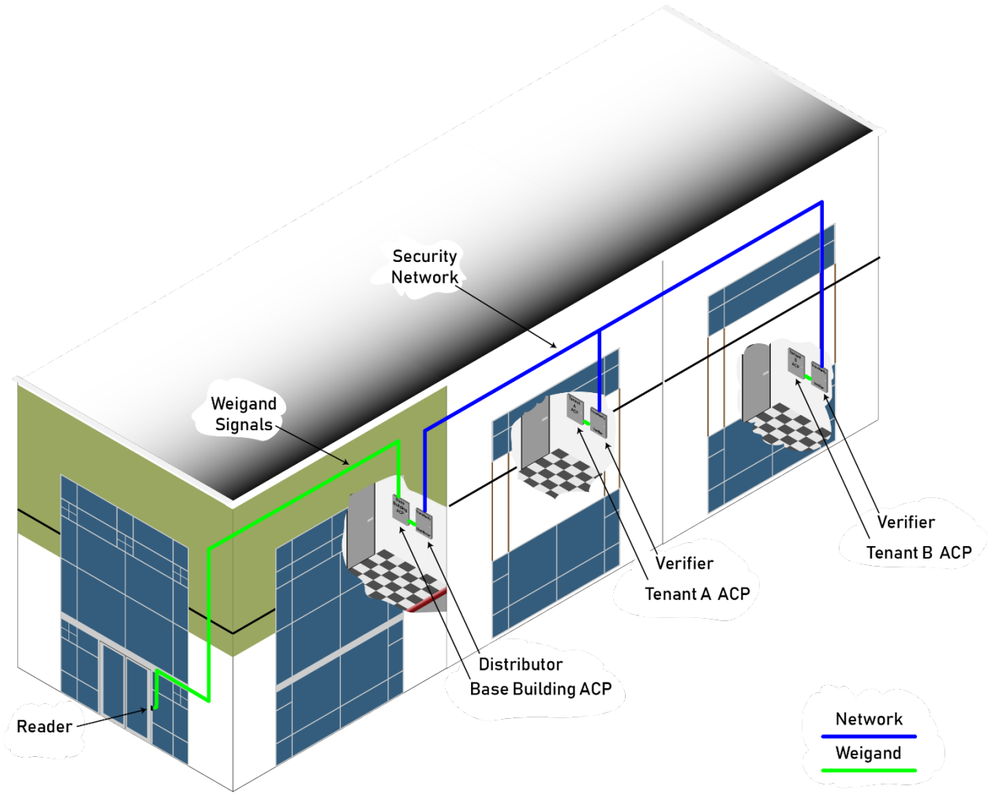
The TransVerify® system addresses the weaknesses of the more conventional methods while keeping or improving upon their strengths. The marriage of network technology with Wiegand interfaces solves confidentiality, latency, and maintenance issues. Further our implementation of the Wiegand interface at the system edge effectively air-gaps the tenants from each other and the base building.

The Distributor and Verifier are the core components of this system. Each Distributor monitors a card reader for tenant card-reads. The Verifier reflects those card-reads to the tenant ACP and upon approval from the tenant echos that approval back to the originating Distributor.

Each tenant needs at least one Verifier device. The granularity requirement of historical data and employee load determine the number of tenant Verifiers. This number can vary from tenant to tenant.

Setup expense is a disadvantage as each building portal requires a Distributor device. However, this one base building mirroring will service sixteen tenants. A Distributor is less expensive than an access control panel further reducing costs. TransVerify devices require connectivity. The proliferation of IP cameras makes security network connectivity a standard building amenity, eliminating this expense in most Class A buildings.

How it works



The diagram above illustrates the TransVerify system connections. Each base building reader has an associated Distributor. The Distributor both monitors the card reader and, upon authorization from the tenant, injects the Meta-Card into the base building access control.

The Verifiers connect with the Tenant Access controls and reflect appropriate credential reads from one or more Distributors. An ordinary ethernet network knits the distributors and verifiers together. Internet access is not required making remote exploits very challenging

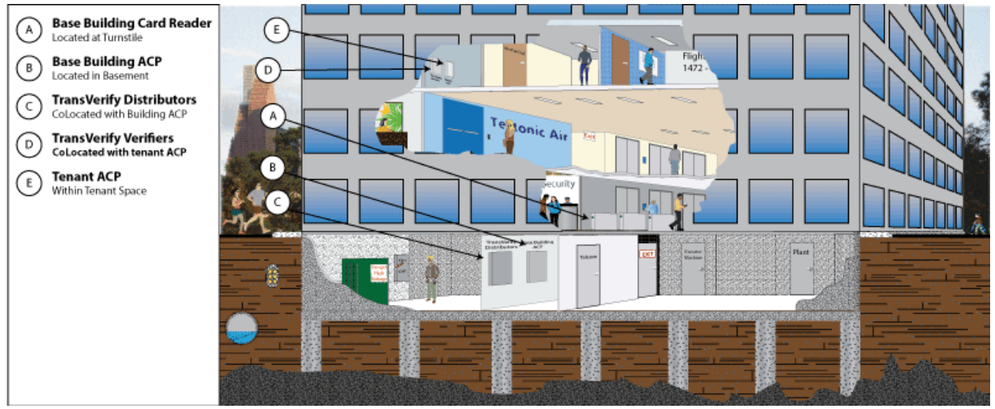
Pictured above are two tenants, Tenant A and Tenant B. TransVerify route the card reads to the appropriate tenants using the card format. Usually, the facility code but any credential bits or combination of bits comprise the filter.

When an employee of Tenant A presents his card to the reader, the reader transmits the credential number via Weigand signals to both the building access control panel (ACP) and the Distributor associated with the door. The Distributor puts the credential on the network and routes it via the Verifier to Tenant A's access control panel (ACP) which authorizes the access. When approved, the Distributor out-pulses Tenant A's virtual card to the base building ACP which in turn releases the door.

The Weigand signals are not network signals; they are unidirectional only transferring a credential's electronic serial number. To simplify the diagram the simple contact closure from the tenant to their Verifier is not shown. This signal authorizes the Verifier to send the Meta-Card. After installation, the tenant is unable to change the Meta-Card's number.

The only connections between the TransVerify equipment, the base building, and the tenants are Weigand signals to their access control equipment. We hold that the TransVerify architecture makes lateral cyber exploit movement between any of these subnetworks, such as tenant to tenant or building to tenant, extremely challenging with the combination of the uni-directional nature of the Weigand interface, the credential data restriction of no more than 64 bits, and the ACP which will only interpret Weigand signals as credential numbers[3]. There are no direct ethernet connections, wired or wireless between the subject networks. We call this feature of the architecture malware isolation.

Equipment Location



The building cutaway above shows another building with the equipment locations. The base building card readers (A) located at the turnstiles connect to the access control panel in the basement (B) with Wiegand signaling. TransVerify distributors co-located in a cabinet (C) connect with the Wiegand signaling from the card readers. The distributors communicate with the verifiers (D) in the tenant space. The tenant access control panel (E) connects both Weigand and authorization signals with the verifiers.

Cyber-Risks

The tenant's employee PII never leaves the tenant's corporate envelope, thus eliminating the risks associated with a third-party disclosure. Further, options exist to block even the employee credential number from the base building, only presenting employee credentials to the tenant for verification and Meta-Card generation upon approval.

---

3 Strictly speaking we are not air-gapped, there is a galvanic connection between TransVerify and the ACP. In terms of cyber security, if this interface could be exploited that would imply the ability to generate a card or sequence of cards that would do bad things to the access control system. The author is not aware of any exploits of this type either academic or in the wild.

TransVerify offers malware isolation for the tenant from the base building and other tenants, mitigating network risks associated with base building access.

The employees use their own company issued and controlled credentials. This single point of control streamlines and enhances safety effectively coupling convenience and security.

Confidentiality

TransVerify acts as a Wiegand splitter with two differences. First, the Distributors are truly networked devices. The Tenant connection, the Verifier, filters card activity. This filtering blocks any cards not administered by the Tenant from being presented to their access control system. Filtering eliminates false errors, tenant to tenant data exposure, and data flooding.

In the basic configuration, the base building sees the tenant cards, but as undefined records. The Distributor can be configured to filter even these events from the base building.

An engineered portal release solution eliminates the problems introduced with the ad-hoc implementation of Wiegand splitter door release systems.

TransVerify sends tenant credential activity at building portal directly to the tenant access control system. Security directors can be confident that their investigations will remain secret. The extension of tenant control to the building perimeter makes perceptible previous unseen activity. This activity could foreshadow events is now available for easy analysis.

Latency

As the tenant access control system directly grants tenant administered credentials eliminating any lag. The tenant manages their employees just like they owned the building.

Enterprise Considerations

TransVerify works with all known access control systems leveraging the de facto Weigand standard for card reader interfaces. The TransVerify system offers a standardization opportunity for large enterprises. This standardization reduces risk when compared with maintaining a plethora of methods, each with their unique hazards.

Expense:

Startup costs

Each building portal to have shared tenant access must have a Distributor associated with it; making the setup investment higher than all other methods except Wiegand splitters.

Ongoing costs

The TransVerify system is hardware based, resulting in minimal continuing expenses.

Other considerations

Reliability/Maintenance

TransVerify has proven itself to be reliable and stable integration system. George Mallard, the VP of Engineering for Hexicurity attributes this the fact that the installations are air-gapped networks.

Deployment

Evaluators ask with anything new; What implementation risks exist? Is this solution unproven?

TransVerify is a proven solution implemented by landmark properties across the United States including Brookfield Properties, The John Buck Company, Boston Properties, Hines, Lerner Enterprises, SJP Properties and Commonwealth Partners all have successfully deployed TransVerify for their tenants.

Compatibility

Previously challenging portal types, elevators, elevator dispatch systems, and HVAC controls, are easily integrated by the employment of what Hexicurity calls a Meta-Card. This card only exists as an electronic representation of a base building credential. Building management endows the Meta-Card with access appropriate to that tenant. Presenting a valid tenant card, say to an elevator dispatch kiosk, a Meta-Card is electronically returned by TransVerify. The dispatch system recognizes the Meta-Card and grants the tenant appropriate access.

Further, the most authoritative database, the tenant access control system, grants or denies the credentials, removes the need for tenant-building audits.

Another advantage for large organizations is the ability for employees to travel from city to city and gain authorized after-hours access enterprise-wide. The tenant directly grants building access eliminating site-specific procedures.

Engineered to prevent the tenant from over-riding building hours TransVerify only allows the tenant to grant access to their cards only within a short window of the credential presentation to the reader.

Summary

The conventional approaches to base building access have many weaknesses. Five characteristics of the methods reviewed are tabulated below for comparison. As usual, red is unfavorable, and green is good.

Base Building Access Methods

Method	Specific Technique	Cyber-Risks	Enterprise	Setup	On-Going
Dual Cards	Building Issues Cards	Very High	No	Low	Expensive
Dual Entry	Building Enters Cards	Very High	No	Low	Expensive
	Data Transfer	Very High	No	Moderate	Expensive
Parallel Control	Wiegand Splitters	Moderate	No	High	Moderate
	TransVerify®	Low	Yes	Moderate	Low

We feel the evidence shows TransVerify offers improved physical and logical security over transferring employee PII to the base building. It is also more convenient, as the tenants administer their employee's building access with the same tools and processes for their own space.

The variety of methods employed by the building management of leased spaces across the enterprise makes access control integration difficult. This environment has resulted in the Balkanization of system integration for global companies bringing problems associated with managing disparate systems. Weigand signaling is the de facto standard for access control systems. By leveraging Weigand signaling with networking, achieving standardized control of base building access across the enterprise is now a reality. Thus, TransVerify is the first Enterprise grade solution to access control integration.

The Author

George Mallard is a Texas Registered Engineer and holds degrees from Rice University and The University of Houston. Mr. Mallard has a financial interest in Hexicurity Inc., which designs and produces the TransVerify® solution. Mr. Mallard has extensive experience in system integration that spans from E911 systems to access controls. This document is his original work.

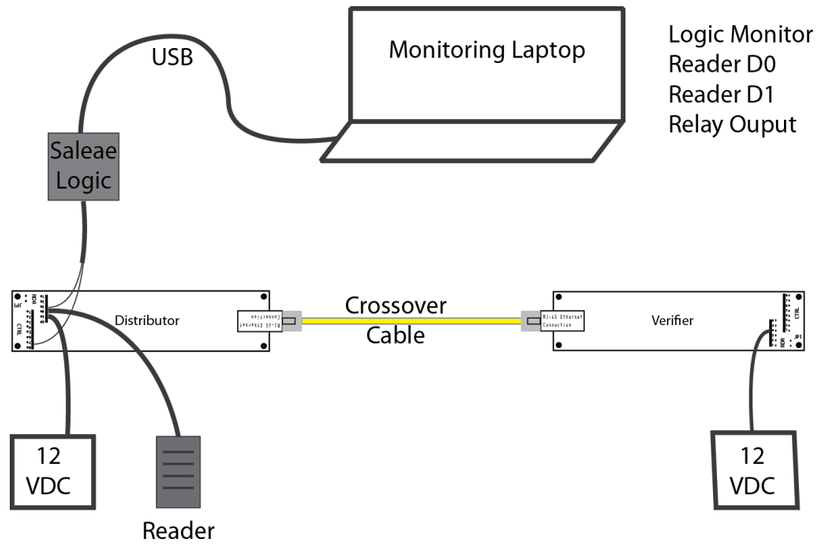
System Timing
AN-03

This application note addresses the performance, timing, of the system response.

Summary:

System response neglecting network or attached tenant system delays is .124 Seconds.

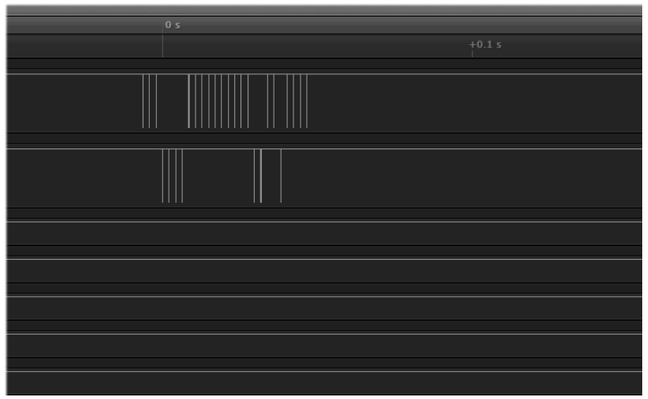
The component setup:



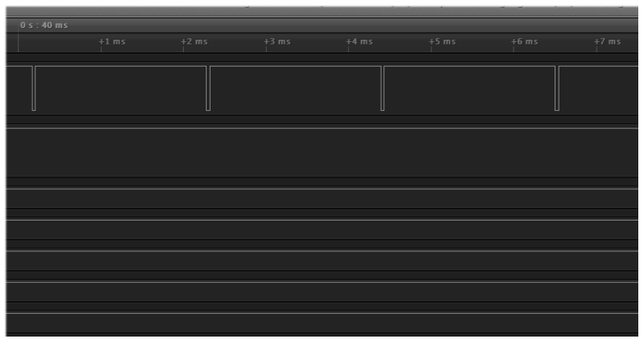
Test Procedure:

1) Start Logic Capture
2) Present a card to the reader.
3) Save Capture

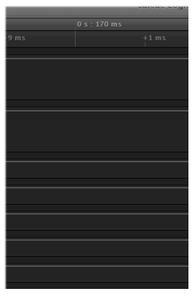
Results:



This first image shows the overall timing of the test. The D1 falling edge triggers the system and shows the first “1s” bit at time zero.



This image shows the last pulse leaving the reader at +46.5 ms



This final image shows the release pulse starting at +170.5 ms.

Calculating 170.5 less 46.5 equals 124 ms.

The response of our system neglecting delays from network propagation and attached tenant system is 124 ms or .124 seconds.

Hexicurity, Inc.
PO Box 7857
The Woodlands TX 77387
832-380-4878
smallard@hexicurity.com

July 2019