Georgia Institute of Technology

The Journey to Re-implementing Physical Access Control Services

Donald Smith
Director Information Technology Security Operations
Campus Services

Jonathan Wimberly
Service Delivery Manager, Low Voltage Projects
Campus Services

Georgia Tech Information Technology Group

A Look Back

- Multiple Stakeholders
  - Campus Card Program ('BuzzCard')
    - Card production
    - Access control system administration (1-Platform)
  - Georgia Tech Police Department
    - Physical security
    - Access control system administration (2-Platforms)
  - Campus Facility Managers
    - Cardholder access privilege administration
    - Door time schedule functions
  - Georgia Tech Research Institute (Applied Research & Development)
    - Card production (Separate Card)
    - Access control system administration (1-Duplicated Platform)
- Primary card credential technology based on HID Proximity II technology (125-kHz) (Corporate 1000)
  - Various bar code and magnetic stripe use cases

#1 - Andover Continuum

- Circa 1999
- Installed in 84 Campus Buildings
- Total Door Count - 2,113

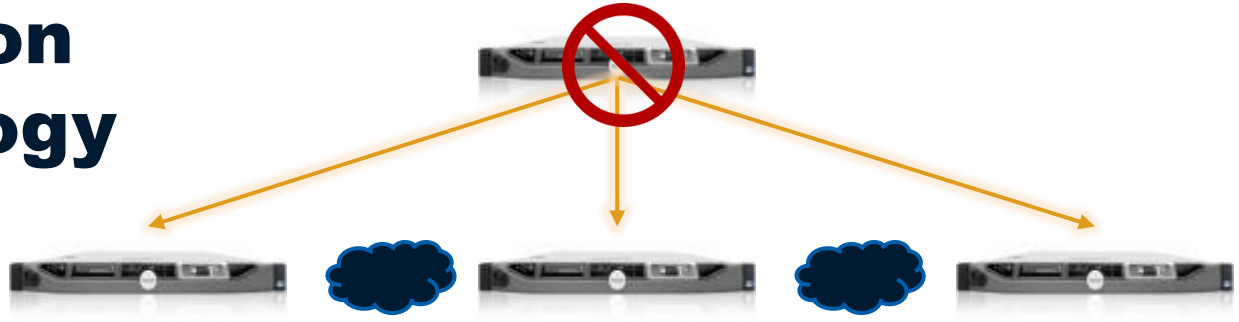
Advantages	Disadvantages
None	No clear product road-map (only 4-7 years of useful life)
	Proprietary hardware
	Security risk (Non-encrypted communications)
	No support for new credentialing technologies (Smart Contactless)
	Inability to easily integrate with other systems
	Multiple demographic records per credential technology
	No ad hoc management reporting

#2 - Avigilon

- Circa 2011
- Installed in 41 Campus Buildings
- Total Door Count - 524 (includes Engineered Biosystems Building-241 Doors)

Advantages	Disadvantages
Open source software (Linux, OpenLDAP)	No global access management
Open source hardware (Mercury Access Controllers)	
Support for new credentialing technologies (Smart contactless, Biometrics)	
Ability to converge video surveillance	

Avigilon Topology



Identities
Roles
Policies
Collaboration
Gateways
Physical AC
Settings

Peer to Peer Automated Synchronization

Identities
Roles
Policies
Collaboration
Gateways
Physical AC
Settings

Peer to Peer Automated Synchronization

Identities
Roles
Policies
Collaboration
Gateways
Physical AC
Settings

Via Subnet to Controllers & Readers

Via Subnet to Controllers & Readers

Via Subnet to Controllers & Readers

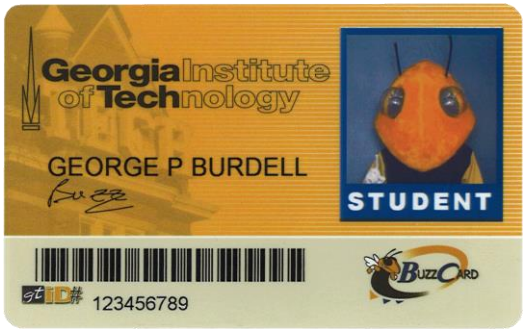
#3 - Blackboard-Transact

- Circa 2007
- Installed in 83 Campus Buildings
- Total Points-of-Use – 900 (Residence Hall Doors, Parking Gates, & Event Turnstiles)

Advantages	Disadvantages
Near real-time integrations (Housing, Parking, EMS)	Proprietary hardware
Integrated with web-based, self-service tool (Middleman)	
Support for new credentialing technologies (Smart contactless)	

Credential Technology

- 44,241 Active Cards
- Bar Code, Magnetic Stripe, & Proximity Technologies
- Financial Purchases – Magnetic Stripe
- Access Control – Proximity Technology



Advantages	Disadvantages
Reliable performance	Security Risk – Magnetic stripe can be easily replicated
	Security Risk – Proximity technology does not offer encryption nor mutual authentication

PROXMARK3

~ $350

Other Points

- System of record according to the Georgia Tech Facilities Management Yellowbook is Avigilon
  - It is a challenge to manage access privileges for a building that contains multiple access control systems
- Access privilege management is manually facilitated – no automated triggers
  - True for all Academic & Administrative Buildings
  - 109-Facility Managers assigned to these tasks
- Lack of standard door fit-out specifications
- No universal lock-down capability exists in the event of an incident or catastrophe
- The physical condition of the door and frame impacts the consistent and reliable operation of the access control solution

The Journey to Re-implement Physical Access Control

Risks

Safety	Time	Accuracy	Institutional Knowledge	Reputation
In the event the Institute does not develop a strategy for campus-wide physical access control, **Georgia Tech may be unable to support controlled access of campus buildings**, potentially resulting in increased instances of trespassing, burglary, and crimes against persons. Moreover, today, there is **no universal lock-down capability**.	The product path of the existing Andover Continuum is not well defined. Through discussions with the vendor, we have learned they want to port the solution to their next generation SmartStruxure platform, albeit there is no established project plan. All things equal, **the maximum useful life of the existing solution is 4 to 7 years**.	Privilege access administration is a manual process that is dependent upon the assignment and revocation of cardholder privileges by an individual. **The practice inherently causes the continued assignment of access privileges for cardholders who should no longer be authorized**.	**There exists one employee who is the resident expert** on the Andover Continuum and Avigilon solutions. The project team will mitigate the risk by formulating a service delivery team that contains multiple technical experts.	**Unfavorable publicity** has previously occurred regarding the potential cloning of BuzzCards by offenders who can employ relatively low cost technology to capture and replay the HID proximity data communication streams to card readers to gain access to campus facilities.
HIGH	HIGH	HIGH	Medium	Low

Objectives

1. Develop a strategy and organized roadmap for the implementation of a single, campus-wide physical access control service that will result in a reliable, scalable, non-proprietary (open architecture), integrated (video surveillance), and supportable solution that will serve to secure the campus community into the foreseeable future
    a. Solution must provide a foundation for the adoption of future advancements in access control (ex. Smart Contactless/NFC, Biometric credentials)
    b. Solution must maximize the investment already made in infrastructure (to the extent possible)

Objectives – Cont.

2. Review and align the service delivery model to support a comprehensive, campus-wide physical access control strategy that ensures effective customer service and safety

3. Formulate an access control policy to effectively manage the timely assignment and revocation of access privileges to ensure campus facilities are safe and secured

4. Seek cost savings opportunities by leveraging bulk quantity discounts of replacement equipment purchases

Physical Access Security Service Re-Implementation Project – Proposed Group Structures and Main Tasks

Executive Team

MEMBERSHIP: Pat McKenna (Legal Affairs and Risk Management), Paul Strouts (Campus Services), Rob Connolly (GTPD), Jim O'Connor (OIT), Chuck Rhodes (Facilities Management)

Main Objective(s):
Decision-making. Secure funding.

Stakeholder Advisory Committee

MEMBERSHIP: Herb Baines (OIT), Al Concord (GTRI), Nick Perez and Jeff Fischer (2 Representatives from the Technical Experts Council to Represent the Campus-At-Large, Cheryl LaFoy (GTAA)

Main Objective(s):
Serves in an advisory capacity to the project. Provides feedback as needed to the project management team. Is kept up-to-date and communicated with frequently and routinely.

Project Management Team

TEAM LEAD: Jim Pete (Campus Services)
MEMBERSHIP: Donald Smith (Campus Services), Cheryl Hunter (Police), Eric Buckhalt (OIT), Jerry Davis (Building Manager), Lindsay Grooms (Campus Services), Ernie Olivares (Housing), Meggan Levitt (Strategic Consulting)

Main Objective(s):
Overall project management. Project Plan for Implementation. STIC presentations. Pilot planning. Site Visits. Determine and collect requirements for hardware and software for the service from campus constituents. Select product.

Working Groups with Specialized Focus

Group Leads are charged with determining the appropriate membership for their group. However, some suggested members are provided.

Policy, Risk, and IT Security

Group Lead:
Jeff Hunnicutt

Main Objective(s): Facilitate Policy Creation for the project. HR processes. Risk Management. Emergency Preparedness.

Other Suggested Member(s):
Jimmy Lummis
Tiffany Watson

Campus Engagement

Group Lead:
Kara Tillman

Main Objective(s):
Change Management and Communication Planning

The Customer Experience

Group Lead:
Lindsay Grooms

Main Objective(s):
Determine customer service practices that will support the new service.

Other Suggested Member(s):
Jerry Davis (Building Manager)
Uwanna Smith (Academic, CoC)

Integrations and Middleware

Group Co-Leads:
Noel Moreno and Greg Phillips (OIT)

Main Objective(s):
Determine how to integrate service with current technical infrastructure

Other Suggested Members:
Eric Buckhalt
Eric Gill
Keith Watson

Infrastructure

Group Co-Leads:
Glen Hickman and Gary Jelin

Main Objective(s):
Evaluate door frames and cabling. Determine retrofitting requirements and planning. Determine evaluation criteria for prioritization of retrofitting.

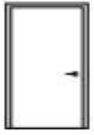
Revised Door Transition Budgetary Estimate

	Expense Range*	
Original Guidance		
Fit-Out Expense Per Door	$7,500	$10,000
Total Fit-Out Expense (Qty. 2,654)	$19,905,000	$26,540,000
Revised Guidance		
Total Fit-Out Expense (Qty. 3,472)	$13,345,360	

* Includes existing cable/equipment demolition, new cable install, and new access electronics. As required, replace failed doors, door frames, & hardware components, procure required network electronics, and accomplish emergency power fit-out.
* Identify and contract with a Construction Manager to affect the door transitions

Service Delivery Model

Proposed Physical Access Security Control Service Delivery Model



Approximately 5 standard doors configurations that are Agreed Upon by Service Owner and SMEs

TO BE IDENTIFIED: A single, open architecture physical access control platform that will scale to appropriately support access program requirements, maximize existing infrastructure investments (to the extent possible), and support new and future end-point technologies.

OUT of SCOPE: GTRI due to their unique needs which include the use of a different card, closed systems for DoD compliance

Subject Matter Experts (SMEs)

GT Police Department

- Security & Safety Experts
- Security Design Consultation & Review
- Investigations
- Emergency Responses
- Policy Owner (via Legal Affairs/Risk Management)

Office of Information Technology

- Structured Cabling Design & Maintenance
- Network Connectivity
- Enterprise Data and Authorizations (i.e. GTED, course enorllment, employment status)

Facilities Management

- New Building Design & Contracting
- Building Renovation Design & Contracting
- Physcial Door Hardware Break-Fix

Communication
Collaboration
Partnership

Service Owner

Campus Services ITG/Buzzcard Team

- Customer Service
- Credential Issuance & Management (Card Production)
- System Administration & Maintenance*
- Application Integrations*
- Programming* (Door/Privilege Configurations)
- Access Control Equipment Break-Fix

*** Indicates responsibilities transferred from Police Department to ITG.**

Access Control Solution

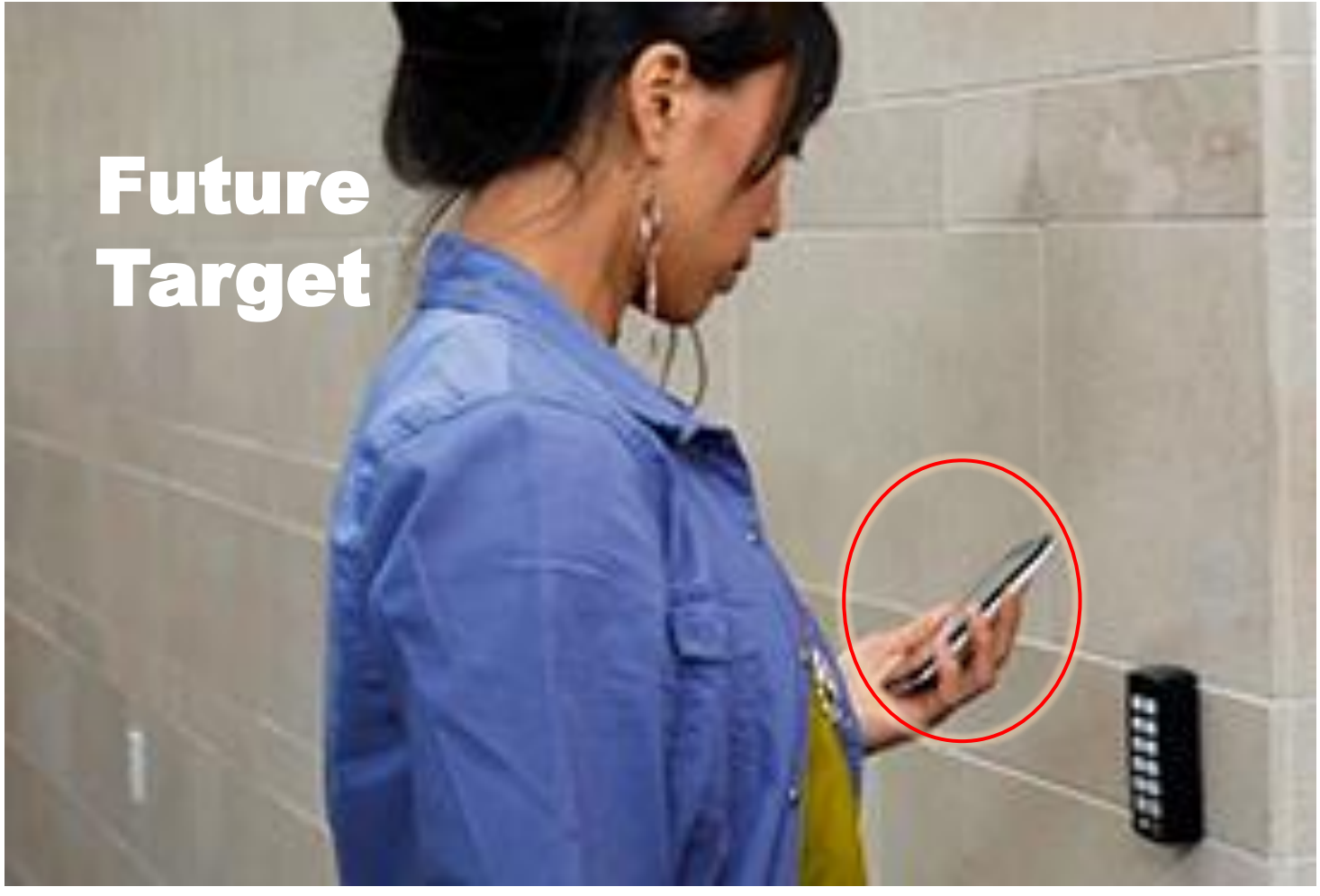
- S2 Systems has formulated a strategic partnership with Blackboard-Transact
- S2 Access Control is similar to Avigilon, but it contains a global management module
  - Interoperability with our current configuration
    - Support for Mercury hardware (Avigilon)
    - Support for Blackboard-Transact proprietary hardware
  - Integration exists between S2 & Blackboard-Transact for demographic records
  - Video surveillance convergence capability
  - Mobile First Approach – including Lock-down application
  - State Contract

Credential Technology

- Identify a transitional credential that:
  - Preserves existing proximity infrastructure (125-kHz)
  - Enables new smart contactless (13.56MHz) applications
- Blackboard has adopted support of the NXP Semiconductors MiFare DESFire EV1 smart contactless protocol that provides for mutual authentication and encryption
- Multiple vendors provide a credential that contains Magnetic Stripe, HID 125-kHz Prox, and MiFare DESFire EV1 technologies


125 kHz Prox
Contact chip-embeddable
13.56 MHz contactless
Magnetic Stripe
hidcorp.com

‘Tried & True’

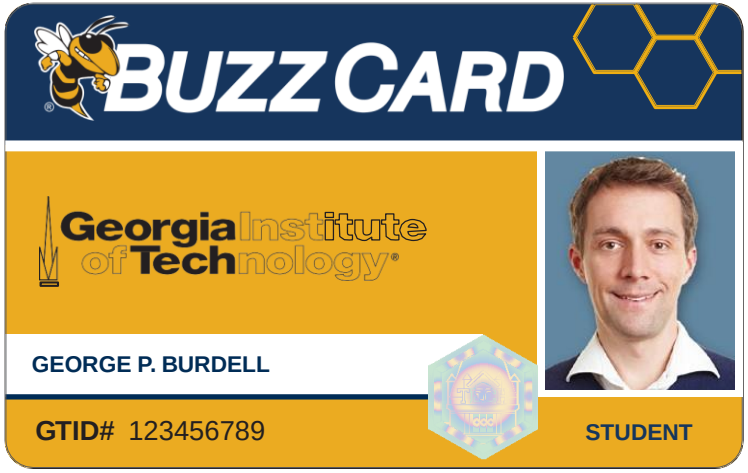

Future
Target

New BuzzCard

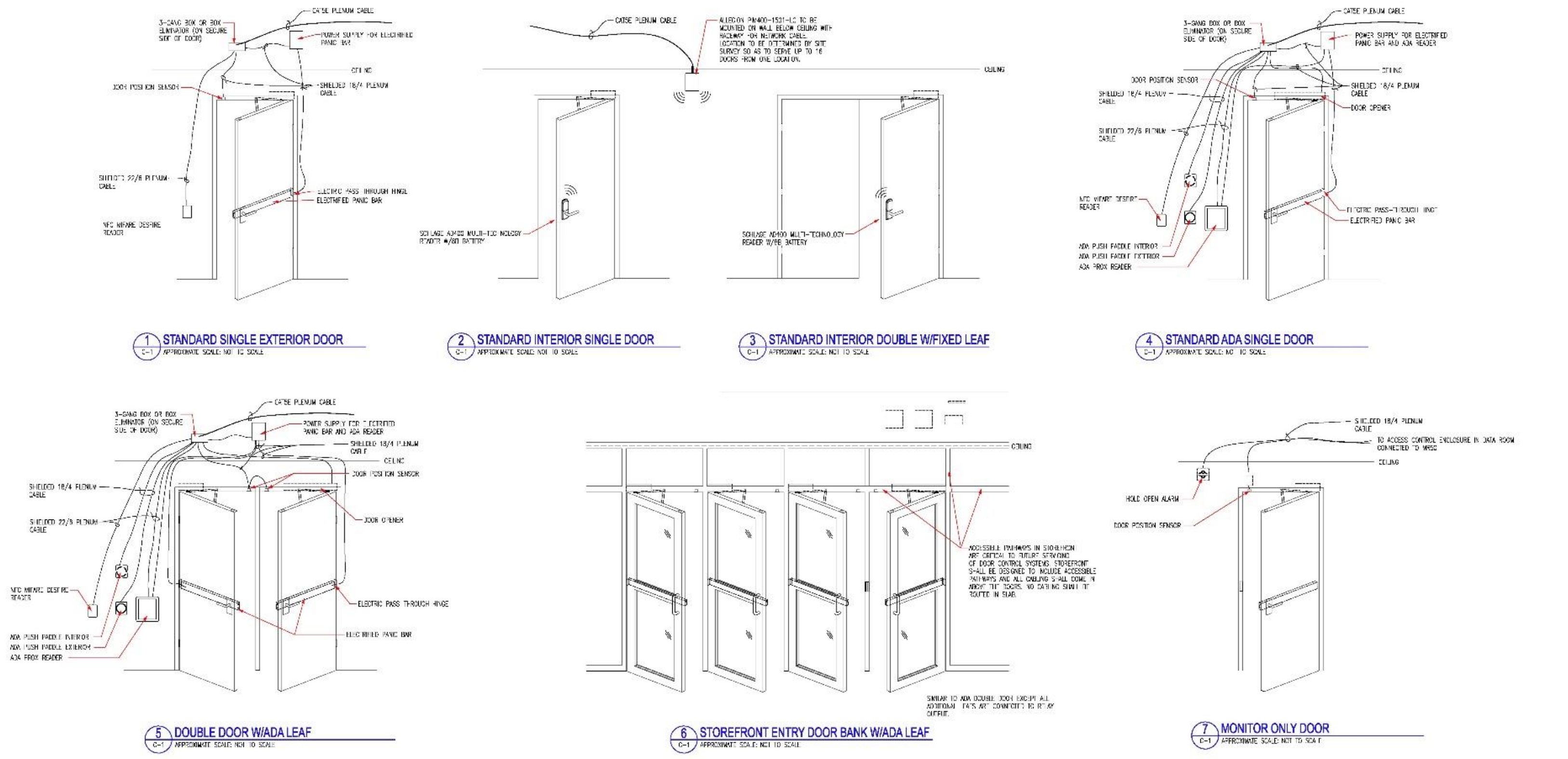
Preferred Name

Legal Name

1 Card Front and Back
SCALE: FULL



2 Card Front - Detail
SCALE: 2:1



GENERAL NOTE:

IN EVERY DOOR INSTALLATION, PATHWAY TO ALL THE WIRED COMPONENTS IS NECESSARY NOT JUST FOR INSTALLATION BUT FUTURE SERVICEABILITY OF ACCESS CONTROL COMPONENTS.

DOOR OPENERS AND POWER SUPPLIES EACH WILL NEED 120v POWER CIRCUITS.

Standard Door Fit-Outs

ACCESS CONTROL ADDITIONAL INFORMATION

Exterior Door – Full Access (w/Card Reader)	• Mercury EP1501 – http://www.mercury-security.com/controllers.html#ep1501 (To be installed locally on the secure side of the door) (PoE) • Non-ADA Card Reader – Allegion Aptiq MT11/MT15 – http://us.allegion.com/Products/readers/Pages/default.aspx • ADA Card Reader – HID MaxiProx 5375 Reader – http://www.hidglobal.com/products/readers/hid-proximity/5375 • If ADA – Activate HID MaxiProx and install Allegion Aptiq for future use (including cable); Mount ADA & Non-ADA reader on stanchion adjacent to controlled door unless otherwise the readers can be mounted to the building based upon the relation of the door to the card reader location one wheelchair access. Non-ADA reader shall be mounted on the front face of the stanchion and the ADA reader shall be mounted on the side of the stanchion. Stanchion (stainless steel 5"x6") shall include an integrated manual opener (paddle) – i.e. http://www.barrier-free.com/916.jpg
Exterior Door – Monitor Only (All Exterior-Perimeter doors w/o a card reader)	• Mercury EP1502 – http://www.mercury-security.com/controllers.html#ep1502 (To be installed in MDF/IDF) (1-EP1502 supports 32-MR50 door controllers) • Mercury MR52 – http://www.mercury-security.com/controllers.html#mr52 (To be installed in MDF/IDF) (1 Per 2 Monitored Doors) • Power Cabinet for EP1502/MR52 Controllers – Sized appropriately based on # of controllers & related power requirements) http://www.lifesafetypower.com/products/access-control-power-systems/unified-power-solutions/modess-mercury
Interior Doors (Limited to Office Suite Doors & High Security Areas (i.e. Research Labs, Data Centers, A/V Control Rooms, Archive Rooms, etc))	• Allegion AD400 – http://us.allegion.com/IRSTDocs/datasheet/104115.pdf (Multi-technology Reader Module w/BE Battery Option) (All other lockset features according to Architect specifications) • Allegion PIM400-1501-LC – http://us.allegion.com/IRSTDocs/InstallInstructions/110436.pdf (PIM placement(s) derived by Building Survey) (1-PIM supports up to 16-AD400 Locksets) • Mercury EP1501 – http://www.mercury-security.com/controllers.html#ep1501 (Mounted inside of the PIM enclosure; PoE)

GEORGIA INSTITUTE OF TECHNOLOGY
OFFICE OF INFORMATION TECHNOLOGY
ADVANCED RESEARCH TECHNOLOGIES GROUP
258 4th St. N.W.
Rich Computer Building
Atlanta, Georgia 30332-0730

REVISIONS | DATE | DRAWN BY

ASBESTOS HAZARD NOTIFICATION

PROJECT TITLE: B835 GENERAL CAMPUS STANDARD ACCESS CONTROL DETAILS

DESIGN: RET | ISSUED
DRAWN: RET | APPROVED: RET

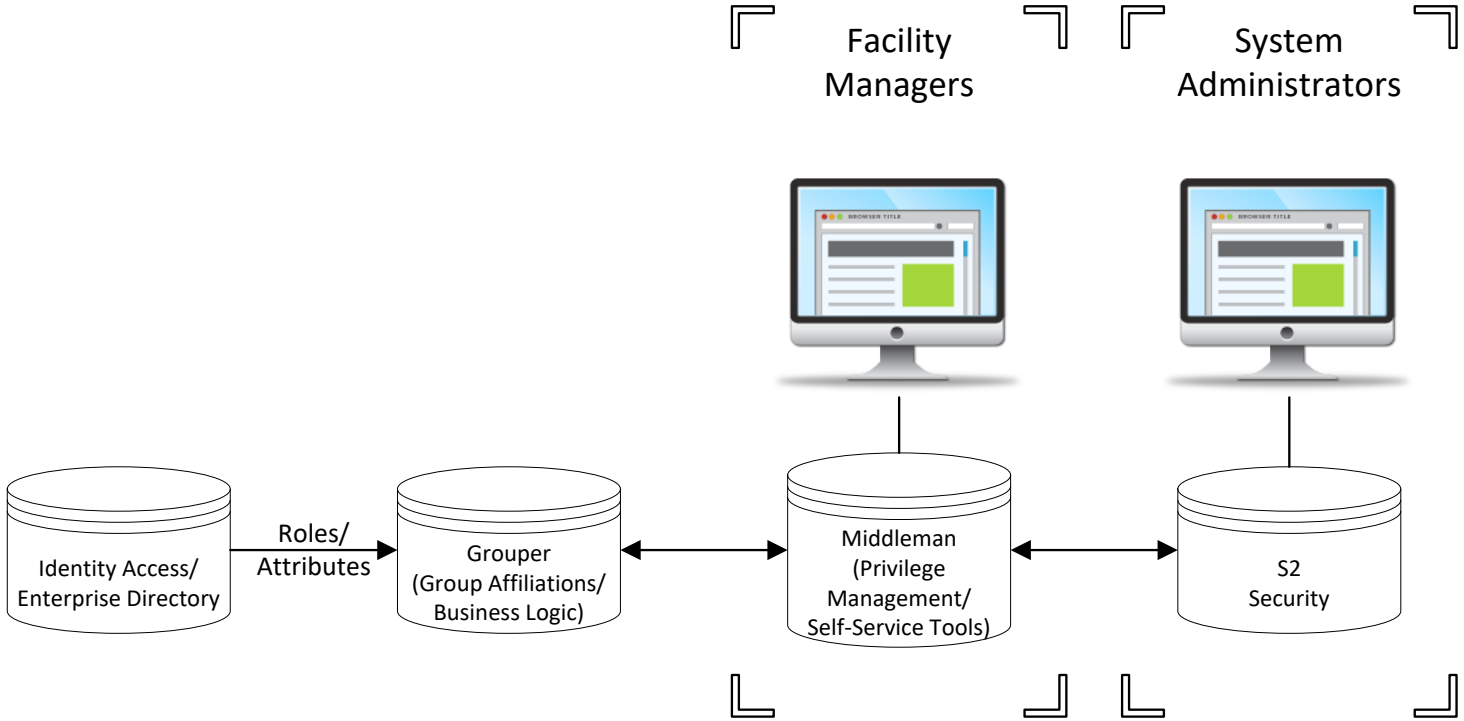
CAD FILE NAME: S2 CONTROLS.dwg

SHEET TITLE: STANDARD DOOR AND STRUCTURE

DESIGN/ESTIMATE NO.: NS3901

SHEET NO.: C-1 OF 1

Privilege Management



Accomplishments-to-Date

- Transitioned support of the existing Andover Continuum and Avigilon Access Control Platforms from the Police Department to ITG
- Began issuance of the new, improved BuzzCard
  - Design & Credentialing Technology (MIFARE DESFire EV1)
  - 9,921 Cards Issued through December 2016
- Procured & Installed the S2 Security System
- Integrated Blackboard-Transact with S2 Security Systems
  - Cardholder Data
- Contracted with Blackboard-Transact to transition three buildings from Andover Continuum to S2 Security
  - Scheller College of Business (80 Doors)
  - Bunger-Henry (24 Doors)
  - Student Services (6 Doors)
- Completed transition of Scheller College of Business prior to Fall Semester

Access Control Standards

- Yogi Berra Project
  - Replacement for current Yellow Book for Low Voltage Standards
    - http://gtlowvoltagestandards.gatech.edu/low-voltage-standards
  - Enables easier updating when standards need to be revised
  - Will be live later this year

Targeted Door Types

- Exterior Doors
- Laboratory Doors
- Office Suites
  - Individual Offices will not be card enabled

Basic Access Control Standards

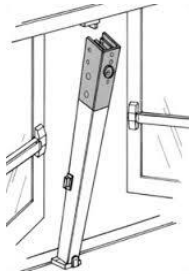
- No Magnetic Locks

- No Vertical Rods

Basic Access Control Standards

- Latch Retraction
  - With QEL
  - Micro Switch built in for Request to Exit

- Electric Strike



- If door is Double Leaf than it should have Keyed Mullion or one locked leaf

Basic Access Control Standards

- Access Controls will be placed in the Data Closet
  - No longer wired to Telecom Network
  - Wired to Data Network
  - Controls will not be placed over doors
  - Use of a composite cable when possible

Basic Access Control Standards

- Reader will be Allegion MT11 if mounted to door frame

- Reader will be Allegion MT15 if mounted to wall

- Maxi Prox will be used in addition to above if ADA opener is required

Basic Access Control Standards

- Wireless Door hardware
  - Schlage AD400
  - Schlage NDE – Possibly in the near future

Q&A Session

- Donald Smith, Director, IT Security Operations
  Donald.Smith@itg.gatech.edu
- Jonathan Wimberly, Service Delivery Manager – Low Voltage
  Jonathan.Wimberly@itg.gatech.edu