QUANTUMSECURE
part of HID Global

SAFE FOR HIGHER EDUCATION

Improve physical and cyber security with physical identity and access management

COLOR ID
Toll Free: 888.682.6567
ph: 704.987.2238
fx: 704.987.2240
www.ColorID.com

QUANTUMSECURE
part of HID Global

CONTENTS

© 2017 Quantum Secure, Inc.

QUANTUMSECURE
part of HID Global

Challenges in Managing Physical Identities and Their Access at Educational Institutions

Colleges and universities present a unique challenge to physical security teams in how they manage people who need physical access to different assets/areas. The profile of these individuals is extremely diverse (e.g. students, faculty, staff, contractors, vendors, visitors) while the campus assets have significant variation in their risk profile (data centers, labs, classrooms, administrative staff, records, library). With the continuous emphasis on cutting operational costs, creating a safe learning environment is difficult to achieve.

The cause of these challenges lies in the inherent complications of the current systems and manual processes for managing physical identities and their access.

Lack of consolidated view into the identity population and their physical access rights – Universities have multiple authoritative systems to enroll and manage identities like student enrollment systems, HRMS, housing, parking systems and the multiple access control systems to manage credential and physical access information for these identities. Unfortunately, none of these systems provide a consolidated view of all these physical identities, their credentials and access, thereby making policy enforcement a futile and risk-prone exercise.

Silos of identity systems – physical, cyber and other authoritative systems with limited or no integration – The complication described above gets aggravated because universities have multiple identity-based systems (see Figure 1), which have multiple stakeholders. These systems

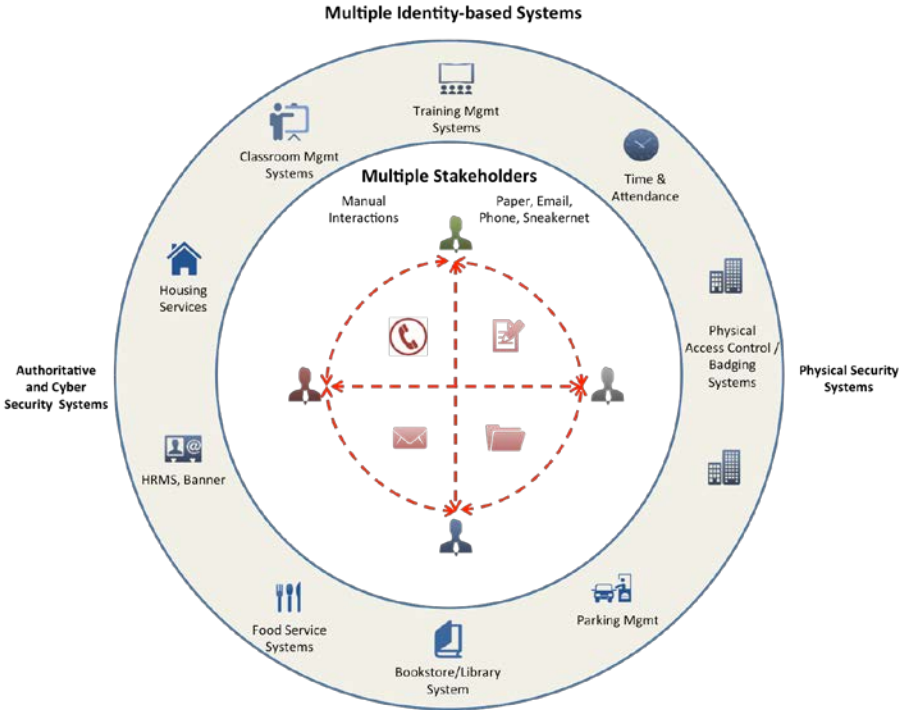

Figure 1: Silos of Identity-Based Systems with Data Exchange through Manual Interactions among Multiple Stakeholders

© 2017 Quantum Secure, Inc.

store data for the same person but due to lack of proper integration, data exchange happens through manual interactions of different stakeholders. Even integrated security solutions for universities (cbord, Blackboard, Banner) don't integrate with other access control systems that may co-exist in the physical security environment (SoftwareHouse, DMP, AMAG). These solutions also have limited or no integration with authoritative and cyber security systems. As a result, there are huge operational inefficiencies, delays and a high state of risk to potential security threats.

Manual enforcement of security policies related to physical access control – Most of the physical security systems for universities manage identity, credential and access data but lack the intelligence required to ensure that the decisions associated with the data are taken in accordance with mandated security policies. As shown in Figure 2 below, physical access to different areas within an education institution has dependencies on various attributes of an identity. For example the start date of access to a classroom/lab area is tied to the enrollment date of the student for the associated course. Similarly, access to housing areas should be immediately reviewed and removed if a student changes or leaves existing housing. Physical security departments manually track this process and given their huge volumes, it leads to errors and oversights causing risk and delays.

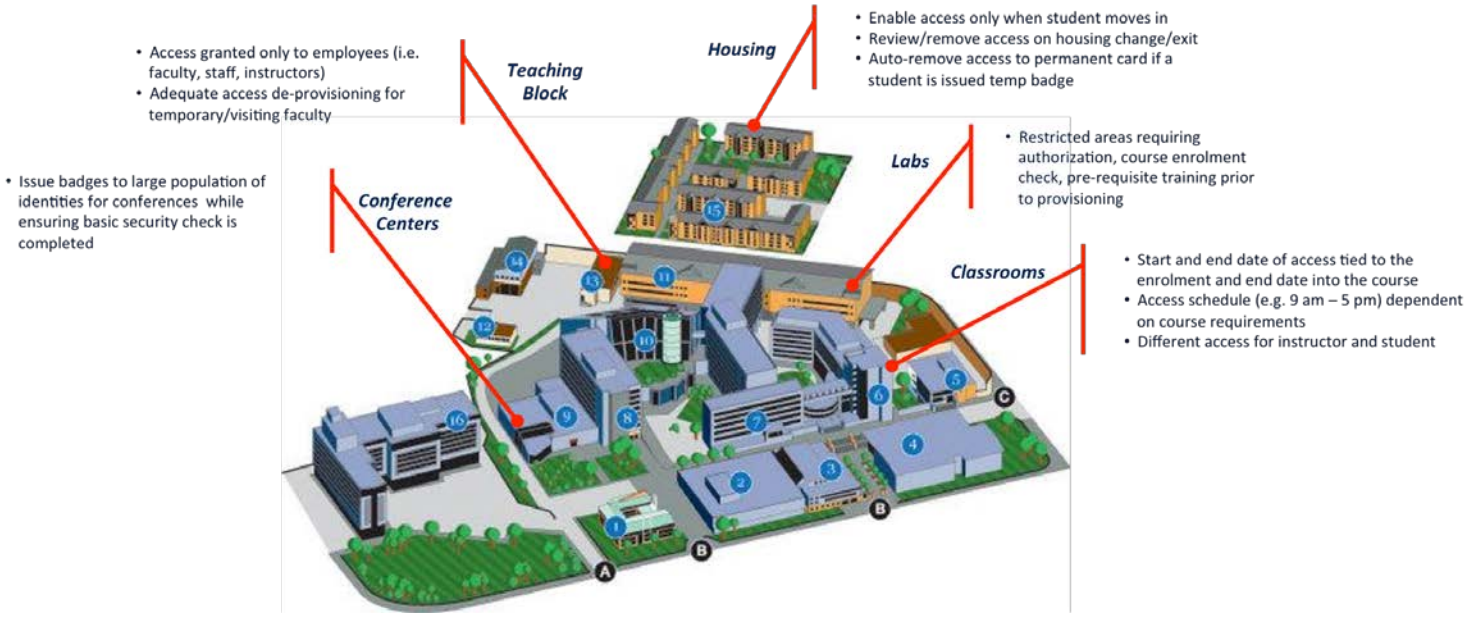

FIGURE 2: SECURITY POLICIES FOR DIFFERENT CAMPUS AREAS

Manual processes for on-/off-boarding and physical access (de-)provisioning/change management – Most physical security departments at universities manually add identity data obtained from different authoritative systems (HR, Housing) into security systems. The processes for handling end user requests like request new card, report lost card are carried out through paper-based forms. This leads to lost productivity and huge amounts of delays.

© 2017 Quantum Secure, Inc.

THE IDEAL SOLUTION: POLICY-DRIVEN SOFTWARE SOLUTION FOR PIAM

Given the challenges with the current state of physical security operations and systems, education institutions should adopt a **policy-driven physical identity, credential and access management software solution**. This not only ensures the interoperability of current and future security and other identity-based systems but also automates physical identity processes and policy enforcement. The illustration below summarizes the key capabilities of an ideal software solution.

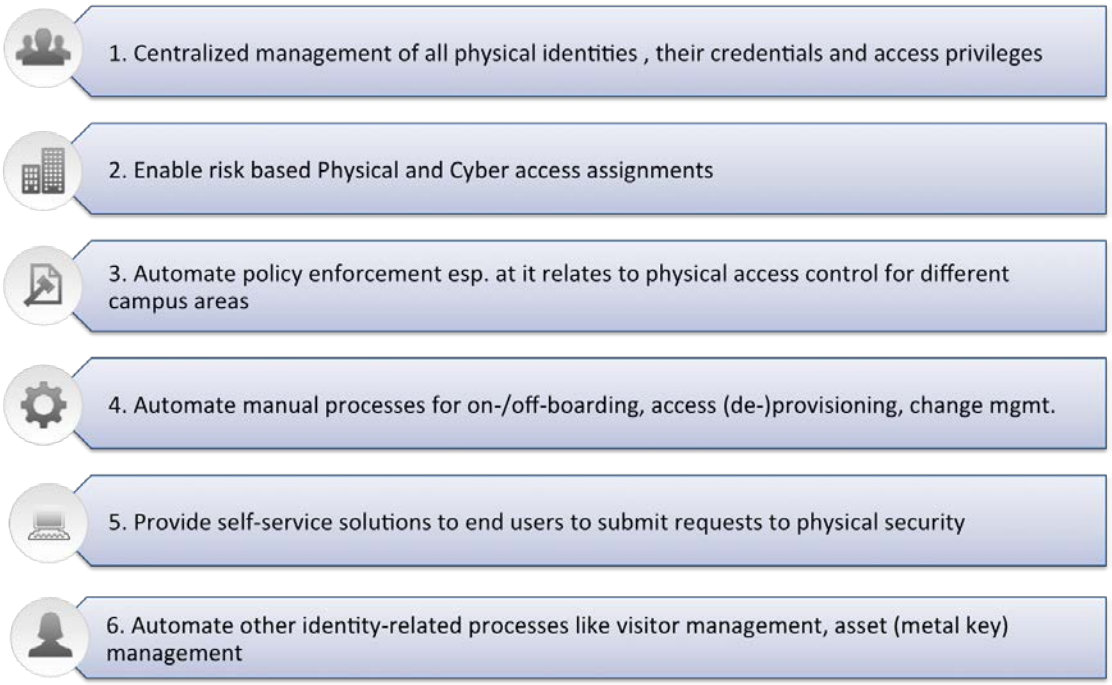

FIGURE 3: KEY CAPABILITIES OF POLICY-DRIVEN SOFTWARE SOLUTION FOR PIAM

© 2017 Quantum Secure, Inc.

THE QUANTUM SECURE SOLUTION: SAFE FOR HIGHER EDUCATION

Quantum Secure has created SAFE, a web-based, policy-driven software solution that includes all the capabilities of an ideal solution for managing the **physical identity and access management needs at education institutions.** Figure 4 shows the logical components of the SAFE Solution.

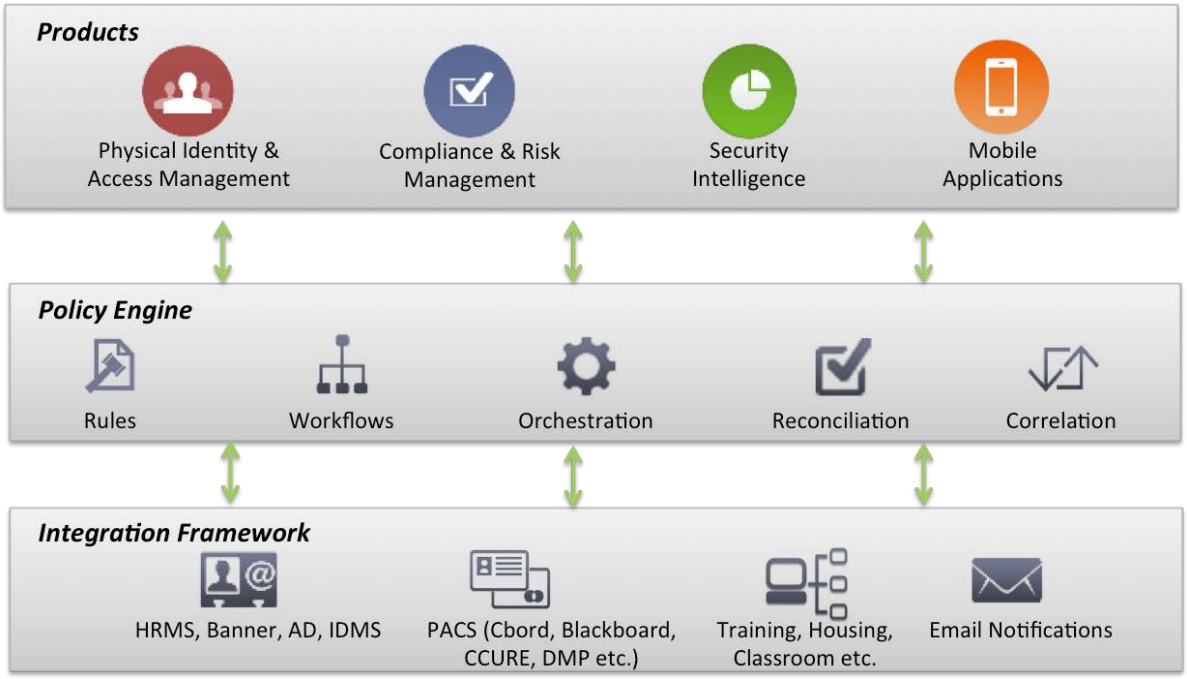

FIGURE 4: THE QUANTUM SECURE SAFE SOLUTION FOR HIGHER EDUCATION

SAFE Integration Framework – Includes out-of-the-box connectors (agents) that provide bi-directional data exchange between SAFE and other systems that need to be integrated for centralized physical identity and access management. This includes connectors for PACS and authoritative data sources like HRMS, IDMS, Housing, Classroom Mgmt., and much more.

SAFE Policy Server – This layer includes pre-defined rules and workflows for acting on the data fed by the integration framework. Key rules include condition-based (de-)provisioning of physical access for students and other identities.

SAFE for Higher Education Applications – These individual web-based applications support the needs of educational institutions to economically enforce rigorous physical identity and access management.

- **Physical Identity and Access Manager** to manage all types of cardholders and their processes for synchronized on-/off-boarding, physical access (de-)provisioning, and change management.
- **Web badging**, which allows authorized users to print and issue badges to the identities and subsequently manage the lifecycle of the credentials.

© 2017 Quantum Secure, Inc.

- **Self-Service Portal**: Allows end users (students) to submit requests for a new badge, report a lost card, upload and submit a photo, request physical access and manage PIN. It also allows area owners and approvers to review and approve/deny requests.
- **Automated Visitor Management Portal**: Allows users to request and manage visits and visitors, as well as the supporting visitor check-in processing by front desk personnel. It also provides the ability to easily process a large number of visitor records associated with conferences through an easy upload function using a spreadsheet and through bulk printing of badges.
- **Watch List Manager:** Manages an internal list of physical identities that are potential threats to the campus facilities. It is used in conjunction with SAFE PIAM and the visitor management solution to verify all types of identities and flag those for whom a match is reported against the watchlist.
- **Asset (Metal Key) Manager:** Allows security personnel to manage the inventory of different assets (metal keys) that are issued to identities.
- **Mobile Tool Suite:** Provides end users and security with anytime/anywhere convenience to complete activities like submit a new access request, report a lost card, approve/deny an access request, check-in/-out visitors during conferences.
- **Security Reporter**: Consists of built-in reports on the data and transactions executed within the SAFE system like identities on-/off-boarded, access provisioning and revocation actions along with supporting reasons.

© 2017 Quantum Secure, Inc.

KEY WORKFLOWS AUTOMATED BY SAFE

PHYSICAL IDENTITY ONBOARDING

Figure 5 below shows the typical on-boarding workflow of different physical identities into SAFE.

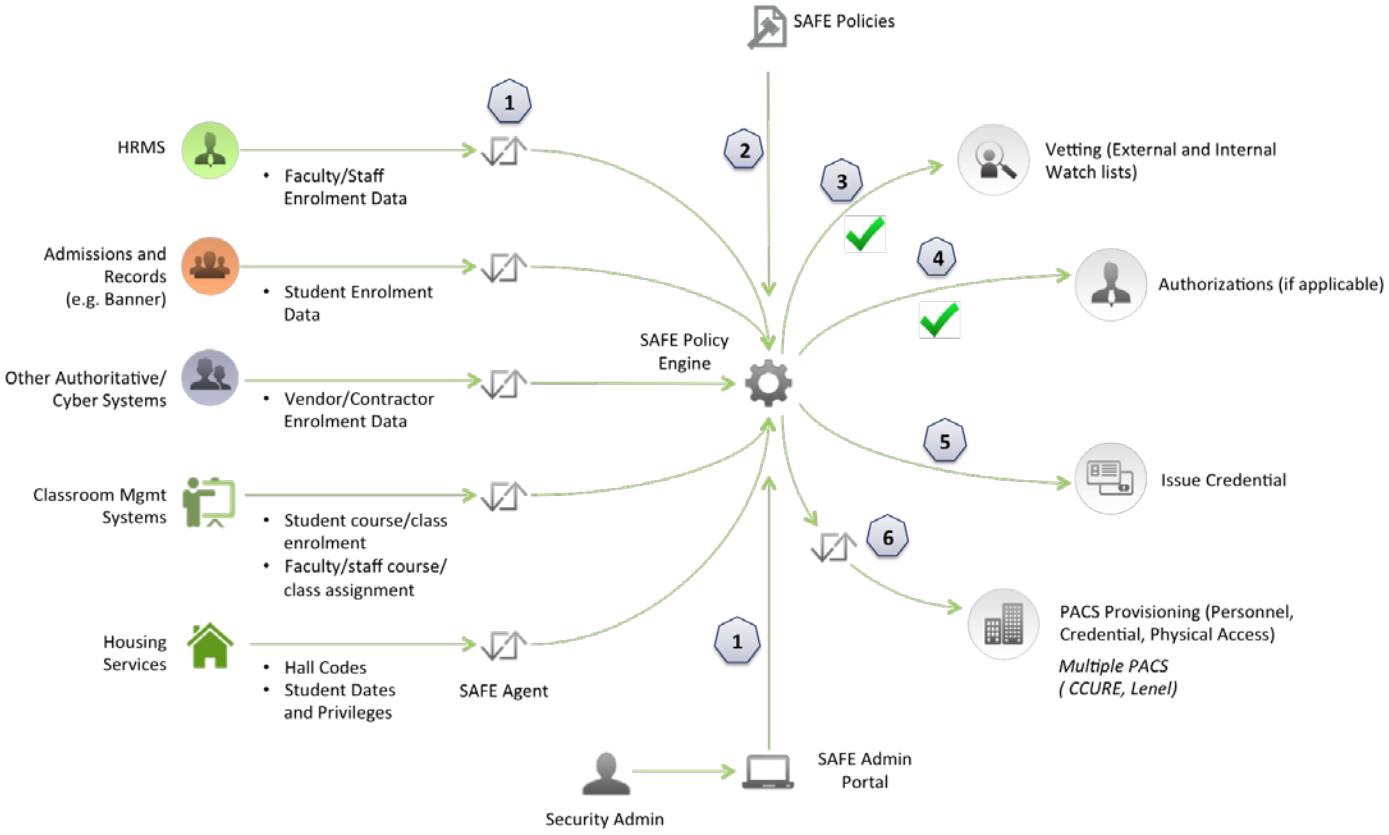

FIGURE 5: PHYSICAL IDENTITY ONBOARDING WORKFLOW

#	Description
1	SAFE agents for various identity authoritative systems like HRMS (for faculty and staff), Admissions and Records system (for students), others (for vendors, service providers) automatically retrieve any new record that gets added in these systems. It should be noted that SAFE can also become an authoritative system to on-board any personnel which isn't maintained in any of the above authoritative systems. In addition, SAFE agents also integrate with other systems, which contain identity-related data that is used for making provisioning decisions. For example, systems containing classroom/course information provide details of student enrolment and that in turn is used within SAFE to provision right physical access schedule to the student.
2	The data aggregated from different SAFE agents in Step 1 above is then processed through the SAFE Policy Engine. SAFE Policy Engine comprises set of policies that are a

#	Description
	combination of rules and workflows. The application comes with built-in policies leveraging best practices from across multiple deployments of SAFE and also provides the flexibility to define custom policies.
3	One such policy, which gets triggered, is to complete security check of the identity against external and internal watch list databases.
4	If the identity passes security check from Step 3 above, then there is an optional step of getting authorizations. SAFE automates workflows for identity and access approval and provides a web-based interface to authorized users to complete the approval process.
5	Post completion of approval above, a security administrator or badging officer can issue a credential
6	SAFE agent for different PACS automates the provisioning of the physical identity, its access and credential in the respective access control systems.

PHYSICAL IDENTITY OFF-BOARDING

Figure 6 below shows the typical off-boarding workflow of different physical identities using SAFE.

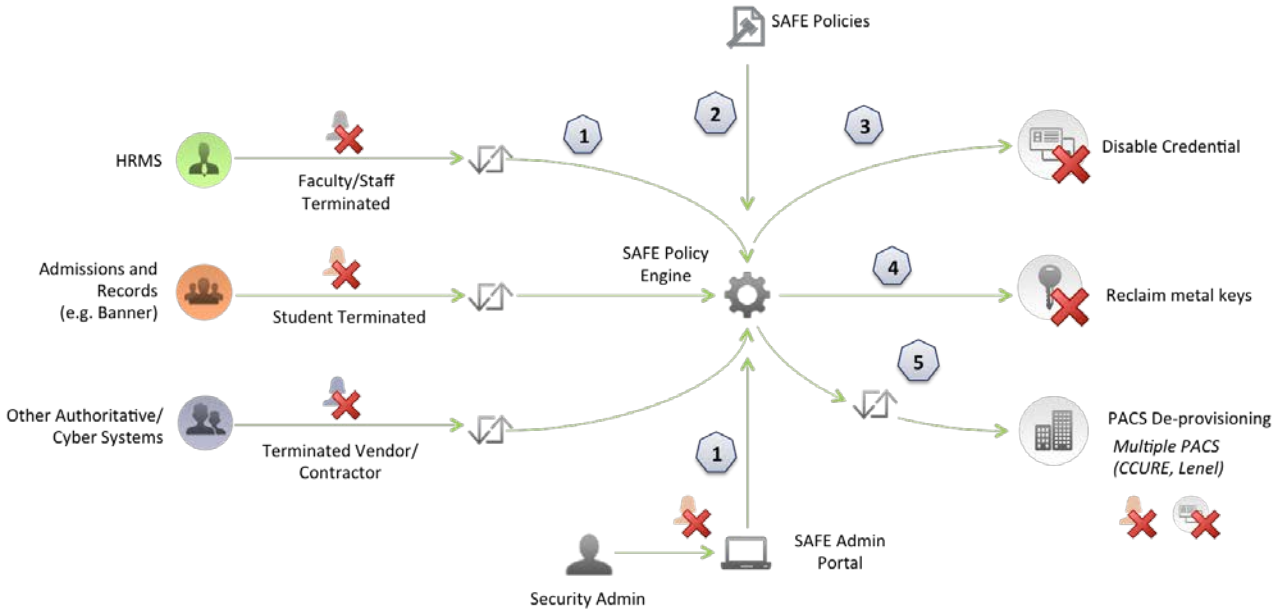

FIGURE 6: PHYSICAL IDENTITY OFF-BOARDING WORKFLOW

#	Description
1	SAFE agents for various identity authoritative systems like HRMS (for faculty and staff), Admissions and Records system (for students), others (for vendors, service providers) automatically retrieve termination of existing record. SAFE also allows security users to complete “urgent termination” of any identity from within SAFE itself.
2	The data aggregated from different SAFE agents in Step 1 above is then processed through the SAFE Policy Engine. SAFE Policy Engine processes policies related to identity and access termination.

© 2017 Quantum Secure, Inc.

#	Description
3	Credential associated with the identity is disabled in real-time.
4	Any assets issued to the identity are set to be "reclaimed"
5	SAFE agent for different PACS automates the de- provisioning of the physical identity, its access and credential in the respective access control systems. In short SAFE ensures that any identity terminated in the different authoritative systems is terminated in real-time in the integrated PACS.

Self-Service Requisition and Approval Workflows

Figure 7 below shows the typical on-boarding workflow of different physical identities using SAFE.

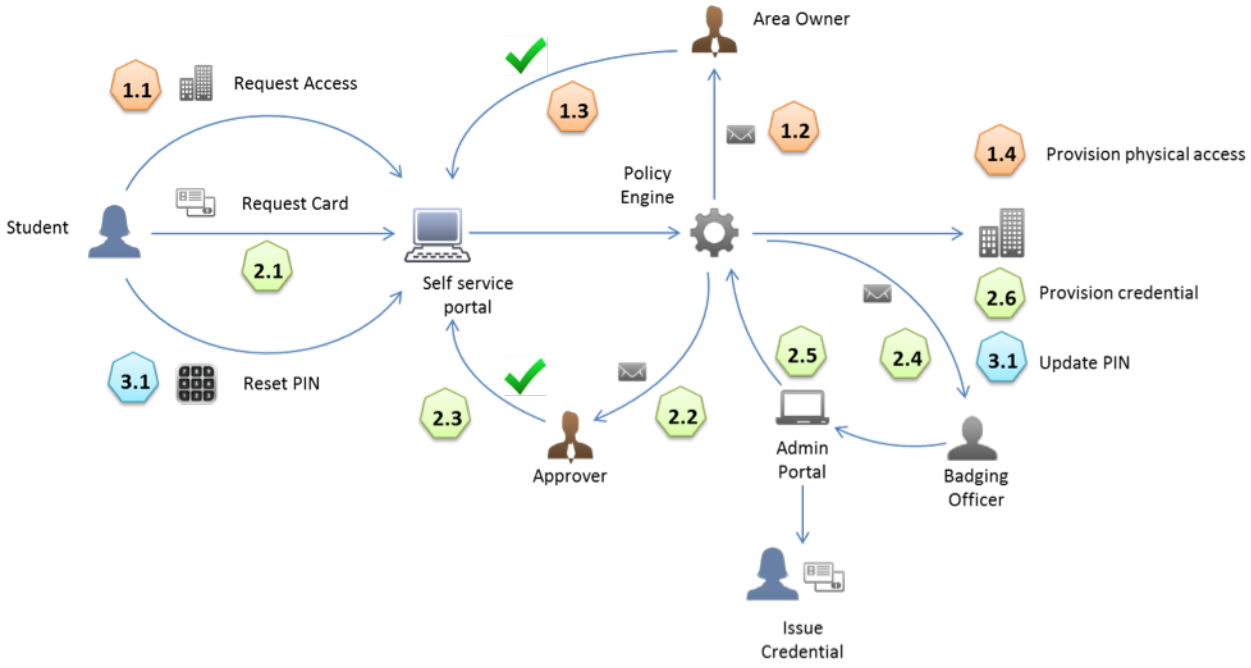

FIGURE 7: SELF-SERVICE WORKFLOWS AUTOMATED IN SAFE

#	Description
1.1	Student submits request for access using web-based self-service portal
1.2	SAFE policy engine creates task for the area owner and sends a notification
1.3	Area owner logs onto its self-service portal, reviews and approves the task
1.4	SAFE policy engine provisions the physical access in the respective PACS and notifies users

#	Description
2.1	Student submits request for new card using web-based self-service portal. Student has the option of uploading its picture
2.2	SAFE policy engine creates task for the authorized user (approver) and sends a notification
2.3	Approver logs onto its self-service portal, reviews and approves the task
2.4	SAFE policy engine notifies the badging officer to issue credential

© 2017 Quantum Secure, Inc.

#	Description
2.5	Badging officer logs onto the SAFE Admin portal, verifies that all the information for student is available and issues a badge
2.6	SAFE policy engine provisions the credential into the respective PACS

#	Description
3.1	Student logs onto self-service portal to reset his/her PIN
3.2	SAFE policy engine updates the PIN in the respective PACS in real-time

© 2017 Quantum Secure, Inc.

QUANTUMSECURE
part of HID Global

WHY SAFE FOR MANAGING PHYSICAL IDENTITIES AND THEIR ACCESS AT EDUCATIONAL INSTITUTIONS?

SAFE is the only Commercial-Off-The-Shelf (COTS) solution, which can ensure that different security systems at universities interoperate, and that various identity related processes are automated as per their unique requirements.

Reduced risks

- Enhanced Security – Automated policy/rules based. Minimal manual intervention
- Automation of more than 90% card management process – Implying zero redundant manual actions
- Elimination of "inaction upon termination" and of "manual" report and auditing cycles
- Reduced operational training; better use of staff for decision-making and strategy processes rather than manual operational processes
- Assurance that physical security access is provisioned correctly and de-provisioned accordingly in a timely and efficient manner

Superior customer service

- Single portal for security interactions and visibility into access control processes including request, approvals, visitor management, etc.
- Increased service levels
- Reduced errors and reactionary events
- Analytics to better forecast and plan operations

Operational costs reduction

- Elimination of duplicate work effort across multiple systems
- Reduced manual processes and data entry, which are error prone and resource intensive.
- Streamlining of the management and access request process for faculty, staff, students, and vendors via one centralized solution.

Future-proofing

- Ensuring that the solution grows and evolves along with a university's dynamic physical/ cyber infrastructure

Quantum Secure subject matter experts in applications for educational institutions can be reached at info@quantumsecure.com. To find more about Quantum Secure and its breakthrough SAFE solution, visit http://www.quantumsecure.com or call +1-408-453-1008.

© 2017 Quantum Secure, Inc.