NIST SPECIAL PUBLICATION 1800-27B

Securing Property Management Systems

Volume B:
Approach, Architecture, and Security Characteristics

William Newhouse
Information Technology Laboratory
National Institute of Standards and Technology

Michael Ekstrom
Jeff Finke
Marisa Harriston
The MITRE Corporation
McLean, Virginia

September 2020

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/use-cases/securing-property-management-systems

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series of practice guides, which map capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices, and they provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe an example implementation of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Hotels have become targets for malicious actors wishing to exfiltrate sensitive data, deliver malware, or profit from undetected fraud. Property management systems (PMSes), which are central to hotel operations, present attractive attack surfaces. This example implementation strives to increase the cybersecurity of the PMS and offer privacy protections for the data in the PMS. The objective of this guide was to build a standards-based example implementation that utilizes readily available commercial off-the-shelf components that enhance the security of a PMS ecosystem.

The NCCoE at NIST built a PMS ecosystem in a laboratory environment to explore methods to improve the cybersecurity of a PMS. The PMS ecosystem included the PMS, a credit card payment platform, and an analogous ancillary hotel system. In this example implementation, a physical access control system was used as the ancillary system.

The principal capabilities include protecting sensitive data, enforcing role-based access control, and monitoring for anomalies. The principal recommendations include implementing cybersecurity concepts such as zero trust, moving target defense, tokenization of credit card data, and role-based authentication.

The PMS environment outlined in this guide encourages hoteliers and similar stakeholders to adopt effective cybersecurity and privacy concepts by using standard components that are composed of open-source and commercially available components.

KEYWORDS

access control, hospitality cybersecurity, moving target defense, PCI DSS, PMS, privacy, property management system, role-based authentication, tokenization, zero trust architecture

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Sapna George	Cryptonite
Hans Ismirnioglou	Cryptonite
Mike Simon	Cryptonite
Rich Walchuck	Cryptonite
Justin Yackoski	Cryptonite
Katherine Gronberg	Forescout
Timothy Jones	Forescout
Scott Morrison	Forescout

Name	Organization
Shane Stephens	Forescout
Oscar Castiblanco	Häfele
Ryan Douglas	Häfele
Chuck Greenspan	Häfele
Sarah Riedl	Häfele
Harald Ruprecht	Häfele
Roy Wilson	Häfele
John Bell	Hospitality Technology Next Generation
Kartikey Desai	MITRE
Eileen Division	MITRE
Karri Meldorf	MITRE
Paul Ward	MITRE
Trevon Williams	MITRE
Kevin Garrett	Remediant
Paul Lanzi	Remediant
Nicole Guernsey	StrongKey
Pushkar Marathe	StrongKey
Arshad Noor	StrongKey

Name	Organization
Bill Johnson	TDi
Pam Johnson	TDi

The technology partners/collaborators who participated in this project submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a CRADA with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Cryptonite	network protection appliance that provides additional layer of protection against cyber attacks
ForeScout	policy-based control enforcement for guest Wi-Fi networks and visualizations of diverse types of network-connected devices
Häfele	Physical access control ecosystem, including door locks, room-key encoding, and management
Remediant	Real-time incident monitoring and detection, privilege escalation management, and reporting functions
StrongKey	payment solution appliance that secures credit card transactions and shrinks the Payment Card Industry compliance enclave
TDi	access control platform that secures connections and provides control mechanisms to enterprise systems for authorized users and authorized devices; also monitors activity down to the keystroke

Contents

115 # List of Figures

124 # List of Tables

1 Summary

Hotel operators rely on a property management system (PMS) for daily administrative tasks such as reservations, availability and occupancy management, check-in/out, guest profiles, report generation, planning, and record keeping. This PMS controls the onsite property activities and connects with other applications such as the hotel point-of-sale (POS) and central reservation system (CRS), which support availability, reservations, and guest profile information.

Additionally, various interfaces are available to create further links from the PMS to internal and external systems such as room-key systems, restaurant and banquet cash registers, minibars, telephone and call centers, revenue management, on-site spas, online travel agents, guest Wi-Fi, and connected rooms.

The value of the data in a PMS and the number of connections to a PMS make it a likely target for bad actors. This guide documents a system that prevents unauthorized access to a PMS and applies both security and privacy protections to the data used in the PMS.

1.1 Challenge

Volume A of this publication described why the National Cybersecurity Center of Excellence (NCCoE) accepted a hospitality cybersecurity challenge as a project. Here, in Volume B, the focus shifts to the challenge of building an example implementation that offers hotel owners and operators some options to secure their property management systems.

Securing Property Management Systems supports the following security and privacy characteristics:

- prevents unauthorized access via role-based authentication
- protects from unauthorized lateral movement and privilege escalation attacks
- prevents theft of credit card and transaction data via data tokenization, explicitly allows only identified entities access (allowlisting), and enables access control enforcement
- increases situational awareness by auditing, system activity logging, and reporting
- prevents unauthorized use of personal information

To build the example implementation, hereafter known as the PMS ecosystem, the project collaborators reached consensus on an architecture that implements aspects of a zero trust architecture (ZTA), moving target defense (MTD), and data tokenization to reduce cybersecurity risk for a hotel's PMS.

1.2 Implementation

The project demonstrates to hospitality organizations how to protect against loss and misuse of customer data and how to provide more cybersecurity and privacy for guest Wi-Fi networks, employee workstations, and electronic door locks.

Best practices for network and enterprise cybersecurity as put forth by the collaborators include role-based access control, allowlisting, and privileged access management. Utilizing data tokenization,

explicitly allowing only identified entities access (allowlisting), and role-based access control enforcement, theft of credit card and transaction data is prevented. Allowlisting is the practice of listing entities that are granted access to a certain system or protocol. When an allowlist is used, all entities are denied access, except those included in the allowlist.

The PMS ecosystem enables and enforces role-based access control to define exactly who or what will be allowed to make connections within the PMS ecosystem. ZTA utilizing dynamic provisioning specifies permitted connections and data transactions. Privileged access management defines, enforces, and monitors the privileges for each user, machine, and data transaction.

The NCCoE PMS ecosystem, three types of authorized users: hotel guests, hotel staff, and back-end administrators; engineers; and system owners. Each user has defined access privileges. Guests can connect to the internet via the Wi-Fi. Staff are allowed authorized access for only the systems and applications needed to perform their work and are not allowed to make any connections outside the scope of their role. Back-end administrators, engineers, and system owners are granted back-end access, but only for the systems and applications they provision, maintain, and troubleshoot.

Best practices for privacy protection include data minimization, transparency, and preference management. The *NIST Privacy Framework* Core [1] is a set of privacy protection activities, desired outcomes, and applicable references that are common across all sectors. The Core presents industry standards, guidelines, and practices in a manner that enables communicating privacy activities and outcomes across the organization from the executive level to the implementation/operations level. The Privacy Framework Core consists of five Functions—Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P. When considered together, these Functions provide a high-level, strategic view of the life cycle of an organization's management of privacy risk arising from data processing. The Framework Core then identifies underlying key Categories and Subcategories–which are discrete outcomes–for each Function and provides example informative references such as existing standards, guidelines, and practices for each Subcategory.

This project demonstrates these best practices in a PMS ecosystem designed to simulate a typical hotel.

1.2.1 PMS Ecosystem

Within the constructed PMS ecosystem, registered hotel guests can connect to the internet via the guest Wi-Fi. Registered guests attempting to connect to the internet will initially be challenged to provide a response, which is validated against information from their reservation. Once validated, the guest is able to connect to the internet and any public-facing hotel websites or guest service portals but is not able to discover other devices using the guest Wi-Fi, which may also be supporting hotel operations and Internet of Things (IoT) devices.

The PMS ecosystem represented in the example implementation constantly changes the internet protocol (IP) addresses of devices, enabling a moving target defense tactic that is transparent to the staff. They can reach the systems that allow them to perform their work while the defense tactic hinders lateral movement of attackers, who will be challenged to achieve and maintain persistent access.

In designing the hotel PMS ecosystem adapting some of the tenets of zero trust resulted in secure, authorized dynamic access to data or resources on a per-transaction, per-user, and per-system basis, based on factors such as device health and hygiene and other cybersecurity considerations.

The PMS ecosystem includes a network protection device and an access control platform to support privileged access management. Adding a wireless protection and visibility platform enables allowlisting, network segmentation, and role-based authentication to the Wi-Fi. All access to resources is granted on a per-connection basis, based on a security policy.

1.2.2 Standards and Guidance

In developing the example implementation, we were influenced by standards and guidance from the following sources, which can also provide an organization with relevant standards and best practices:

- Hotel Technology Next Generation (HTNG): *Secure Payments Framework for Hospitality,* version 1.0, February 2013 [2]
- HTNG: Payment Tokenization Specification, February 21, 2018 [3]
- HTNG: Payment Systems & Data Security Specifications 2010B, October 22, 2010 [4]
- HTNG: *EMV for the US Hospitality Industry,* October 1, 2015 [5]
- PCI Security Standards Council: Understanding the Payment Card Industry Data Security Standard, version 3.2.1, May 2018 [6]
- HTNG: *GDPR for Hospitality,* June 1, 2019 [7]
- National Institute of Standards and Technology (NIST) Cybersecurity Framework, April 2018 [8]
- *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,* Version 1.0, January 16, 2020 [1]
- NIST Special Publication (SP) 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013 [9]
- NIST SP 800-63-3, *Digital Identity Guidelines,* June 22, 2017 [10]
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personably Identifiable Information (PII),* April 2010 [11]
- NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,* August 2017 [12]
- Trustwave Holdings: *2019 Trustwave Global Security Report*, [13]

1.3 Benefits

The NCCoE's practice guide *Securing Property Management Systems* can help an organization:

- reduce the risk of a network intrusion compromising the PMS and preserve core operations if a breach occurs
- provide increased assurance for protecting guest information
- ensure that only personnel with a business need are given access to the PMS
- increase overall PMS security situational awareness and limit exposure of the PMS to incidents in systems that interface with it
- avoid exploitations that decrease consumer confidence of the property owner, chain, or industry
- increase consumer confidence in the protection of their sensitive data

In the hospitality space, cost is a major driving factor for many enterprise decisions, so the example implementation documented in this guide is designed to be modular. The PMS ecosystem documented here offers opportunities for an organization to choose only those components of the implementation that fit its enterprise.

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate a more secure PMS. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST SP 1800-27A: *Executive Summary*
- NIST SP 1800-27B: *Approach, Architecture, and Security Characteristics*–what we built and why **(this document)**
- NIST SP 1800-27C: *How-To Guide* –instructions for building the example implementation

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary* (NIST SP 1800-27A), which describes the:

- challenges that enterprises face in making a PMS more secure and protective of privacy
- example implementation built at the NCCoE
- benefits of adopting the example implementation

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, NIST SP 1800-27B, which describes how the PMS ecosystem mitigates risk.

The following sections may be of interest to users of risk management and privacy frameworks:

- Section 3.4, Risk Assessment, describes the risk analysis performed.
- Section 3.4.3, Cybersecurity Control Map, maps the security characteristics of this example implementation to cybersecurity standards and best practices.

- Section 6.2, Privacy Protections of the Reference Design, describes how we used the *NIST Privacy Framework* Subcategories.

Technical-savvy readers who wish to implement the security offered in this document might benefit by sharing not only this document but also the *Executive Summary,* NIST SP 1800-27A, with leadership to push for resources needed to secure the PMS and reduce risk.

Information technology (IT) professionals who want to implement an approach like this will find the whole practice guide useful and will find the how-to portion of the guide, NIST SP 1800-27C, to have all the details that would allow replicating all or parts of the PMS environment built for this project. The how-to guide provides specific product installation, configuration, and integration instructions for implementing the example implementation—in this case, a functioning PMS environment.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these products. An organization can adopt this example implementation or one that adheres to these guidelines in whole, or this guide can be used as a starting point for tailoring and implementing parts of a more secure PMS. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. The NCCoE encourages organizations to seek products that are congruent with applicable standards and best practices. Section 4.4, Technologies, lists the products in this project's PMS environment and maps them to the cybersecurity controls provided by this example implementation.

Acronyms used in figures are in the List of Acronyms appendix.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/ Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide.*
Bold	names of menus, options, command buttons, and fields	Choose **File > Edit.**
`Monospace`	command-line input, onscreen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**

Typeface/ Symbol	Meaning	Example
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://nccoe.nist.gov.

3 Approach

This practice guide highlights the approach that the NCCoE used to develop the example implementation. The approach includes a risk assessment and analysis, logical design, example build development, testing, and security control mapping.

The NCCoE worked with hospitality organizations, such as the American Hotel & Lodging Association and HTNG, to identify the need for an example implementation that improves the security of connections to and from the POS and PMS and other integrated services and components. These organizations, along with the Retail and Hospitality Information Sharing and Analysis Center, offered opportunities for the NCCoE to discuss this project and solicit input from stakeholders used to shape this effort.

In developing the example implementation, the NCCoE:

- met with hospitality entities and stakeholders such as hotel operators and managers to identify cybersecurity challenges with property management systems
- regularly interacted with members of the NCCoE Hospitality Community of Interest to discuss current cybersecurity trends and challenges
- received input from the collaborators participating in the project documented by this guide
    - The collaborators provided technologies to address the project's requirements and partnered in developing the PMS built for this project.
- implemented stronger security measures within and around the PMS through network segmentation, point-to-point encryption, data tokenization, and business-only usage restrictions
    - We considered including analytics and multifactor authentication, but ultimately we did not include these security measures.

3.1 Audience

This practice guide is intended for any hospitality stakeholder concerned about and/or responsible for securely implementing and operating a PMS. This includes system owners, IT engineers and technicians, hoteliers, and cybersecurity vendors.

The technical components of this guide will appeal to those who are directly involved with or oversee the PMS. Property management systems represent the heart of a hospitality organization's IT system. The example implementation demonstrated by this project will help increase the level of security around a PMS.

3.2 Scope

This project is focused on increasing cybersecurity and privacy of a PMS environment. This includes protecting the data moving between ancillary systems such as a POS, physical access control systems, and hotel guest Wi-Fi as well as data at rest within components of the PMS environment.

After an open call in the Federal Register inviting vendors to become collaborators, the project was scoped to create an on-premise (not cloud) PMS ecosystem that offers the following:

- protection against loss of customer data
- cybersecurity situational awareness within the PMS ecosystem
- cybersecurity for ancillary systems such as customer-facing Wi-Fi networks, employee workstations, and electronic door locks

We considered the following areas determined they are outside the scope of what we documented in this project:

- point-of-sale terminals
- validation of compliance with the Payment Card Industry (PCI) Data Security Standard (DSS)
- securing web servers and web applications
- mobile device security
- penetration testing and vulnerability assessments

3.3 Assumptions

This project is guided by the following assumptions:

- availability of skills–The organization has employees or contractors who can implement a security architecture around its property management system.
- uniqueness of lab environment—The example implementation was developed in a lab environment. It does not reflect the complexity of a production environment, and we did not use production deployment processes. Before production deployment, it should be confirmed that the example implementation capabilities meet the organization's architecture, reliability, and scalability requirements.

3.4 Risk Assessment

For this project, Risk Management Framework Quick Start Guides [14] proved to be invaluable in providing a baseline to assess risks from which we developed the project and the security characteristics of the build. For a deeper dive into the application of a risk management framework, the NCCoE recommends following the guidance in NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*—publicly available material [15].

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence" [16]. This guide defines risk assessment as "the process of identifying, estimating, and

prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

3.4.1 Threats

All organizations face external and internal threats. While not every threat can be eliminated, an architecture can be built to mitigate and/or reduce the potential realization of various threats. The PMS ecosystem mitigates threats related to unauthorized and elevated privileges, data exfiltration, configuration modification, and access to sensitive data.

3.4.1.1 External Threats

One managed security service provider's annual global security report [13] shows that the hospitality industry has the second highest number of incidents being investigated by the author's services. The same report notes that motivation or types of data targeted by malicious actors for hospitality organizations includes, in the author's words, "credit card track data, financial/user credentials, proprietary information, and PII."

Since 2014, a targeted technique labeled *DarkHotel hacking* [17] by security services leverages a hotel's Wi-Fi to selectively target and deliver malicious software to traveling executives. Further, identity theft and *doxing*—searching for and publishing private or identifying information about an individual on the internet, typically with malicious intent—are persistent threats within the hospitality industry.

3.4.1.2 Internal Threats

Hotels also face internal threats, including misuse, inappropriate sharing or disclosure of personal information via employees with malicious intent, and accidental breaches. In fact, it is suggested that more than 50 percent of security incidents are initiated from current or former employees [18]. Mitigating internal threats involves more than just physical concepts, such as locking doors; rather, the process needs to include cybersecurity concepts that help protect against insider threats and unauthorized lateral movement within the enterprise by employees and guests.

3.4.2 Vulnerabilities

A vulnerability is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" [19]. Among this project's goals is to mitigate the ability of an actor to exploit vulnerabilities. Often, vulnerabilities are self-inflicted. For instance, organizations may:

- commit integration and configuration errors due to poor configuration management processes
- delay and/or not perform patching/updating regularly
- mis-deploy assets

Other vulnerabilities are inherent due to the very nature of valuable data. As data is the highest value asset, vulnerabilities to consider include:

- unauthorized modification and unauthorized exfiltration
- fraud, which is one of the largest concerns in the hospitality industry

3.4.3 Cybersecurity Control Map

Visit Appendix A to see the security control mappings that have been identified for this project's PMS ecosystem. A Cybersecurity Framework Components Mapping table (Table A-1) shows the result from examining all the NIST Cybersecurity Framework [8] Core Subcategories and picking the Subcategories supported as a desired outcome of the PMS environment. Each of the Cybersecurity Framework Subcategories shown in the table maps to PCI DSS [6], to controls in NIST SP 800-53 rev 4 [9], and to work roles in the NICE Cybersecurity Workforce Framework [12].

3.4.4 Privacy Control Map

Visit Appendix B to see privacy control mappings that we have identified for this project's PMS ecosystem. A Privacy Framework Mapping table (Table B-1) shows the result from examining all the *NIST Privacy Framework* [1] Core Subcategories and picking the Subcategories supported by components of the PMS ecosystem. This work was done after the collaboration team designed the PMS ecosystem system. We include it to draw attention to NIST's Privacy Framework, a tool for improving privacy through enterprise risk management, to enable better privacy engineering practices that support privacy by design concepts and help organizations protect individuals' privacy.

We did not run a privacy risk assessment methodology during this project on any existing PMS as a first step that would enable an organization to subsequently identify a target privacy profile. Table B-1 simply identifies the Subcategories addressed by the PMS ecosystem and indicates what component is responsible for covering the Subcategory's desired outcome.

4 Architecture

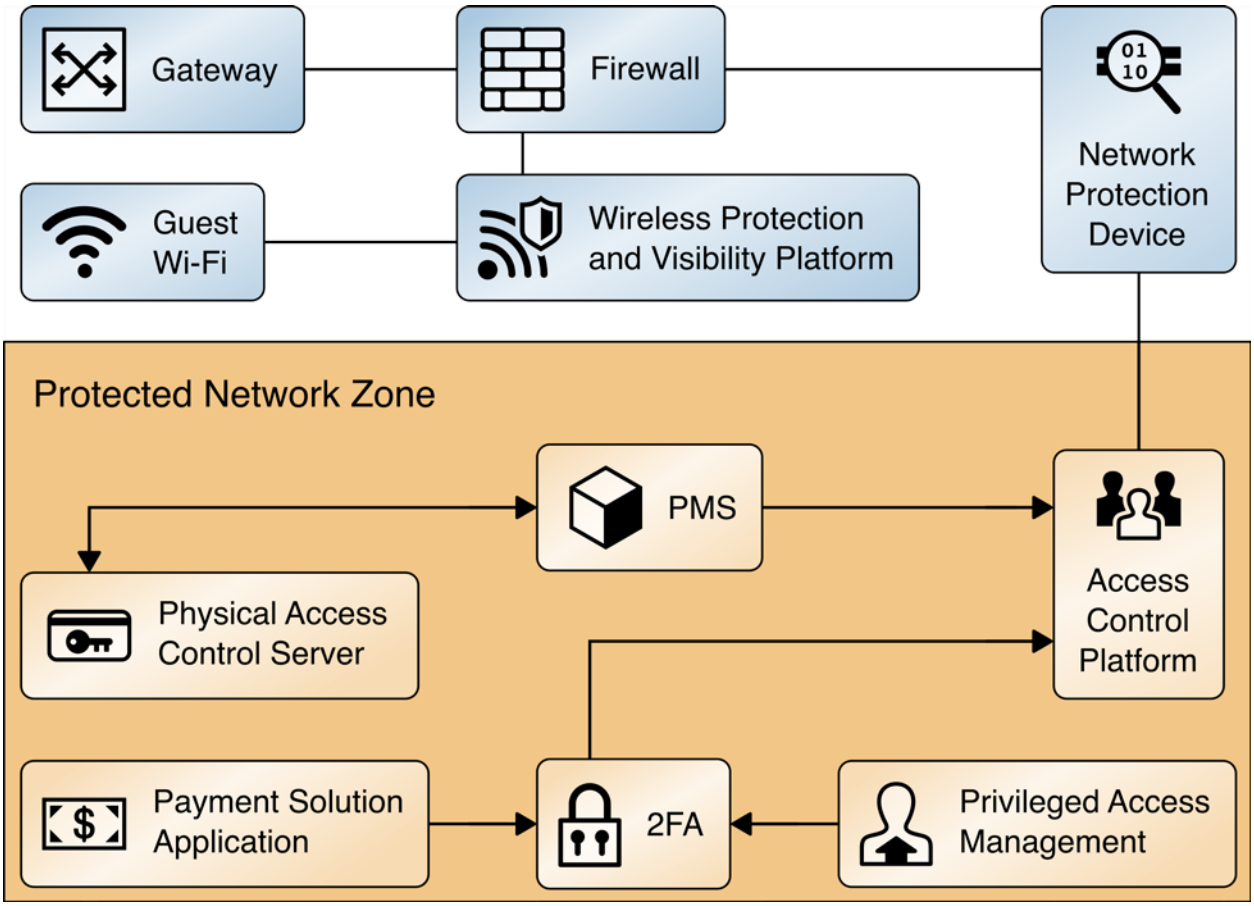
The PMS ecosystem built for this project demonstrates a typical hotel process for reservations, issuing room keys, and check-in and checkout credit card transactions. This section presents a high-level architecture and reference design for enacting such an implementation.

4.1 Architecture Description

4.1.1 High-Level Architecture

The example implementation is designed to address the security Functions and Subcategories described in Table 4-1 and is composed of the capabilities illustrated in the high-level architecture shown in Figure 4-1.

435 **Figure 4-1 Secure PMS High-Level Architecture**



436

437 - **Data protection and encryption** provides the capability to securely store PCI/PII data [11] using
438 additional data protection measures such as data encryption, limiting transmission of payment
439 card data, secure data tokenization, and a secure data vault.

440 - **System protection and authentication** provides the capability to protect the functionality of the
441 PMS, including the POS system and the reservation systems. This function also employs
442 multifactor authentication, eliminates unauthorized access to data and services via dynamic
443 authorization. This also includes making the access control enforcement, on a per connection
444 basis, as granular as possible for internal and third-party users. Finally, it involves the use of
445 network segmentation, and controlling change across multiple system dimensions to increase
446 uncertainty and complexity for attackers, thereby reducing their window of opportunity [20].

447 - **Logging and analytics** give continuous and near real-time auditing, logging, and reporting of
448 user activity, network events, and component interactions.

449 ## 4.2 Use Cases Supported by the Property Management System Ecosystem

450 We designed and built the PMS ecosystem to support the following hotel use cases.

4.2.1 Use Case 1: PMS Accepts Reservation

In Use Case 1, the PMS accepts a reservation, reconciles the bill, and closes out the reservation while never exposing any data to unauthorized access. Further, the reservation data is editable in a secure manner. In this PMS ecosystem, all reservations were manually entered directly into the PMS and not supplied by an external CRS.

4.2.2 Use Case 2: Authorized User Access

In Use Case 2, only authorized users can connect to their authorized devices. They are not able to gain access to devices that might enable them to escalate their privileges within the PMS ecosystem or conduct any unauthorized lateral movements.

The access control platform in the PMS ecosystem allows users only to only connect to the systems for which they are authorized based on their role as a hotel guest; hotel staffer; or back-end administrator, engineer, or system owner [9]. The action of inputting or modifying a reservation requires an authorized staffer to authenticate to gain access to the PMS.

4.2.3 Use Case 3: Secure Credit Card Transaction

In Use Case 3, a credit card transaction is securely conducted. The guest credit card transaction is tokenized before introduction to the PMS.

Credit card data is consumed only by the payment solution application (PSA) and is immediately tokenized. The PSA function to validate the guest credit card data with a third-party payment processor is not included in the PMS ecosystem. The validated credit card data token is sent from the PSA to the PMS. The token is used again at checkout when the bill is paid, with only the token sent from the PMS to the PSA.

4.2.4 Use Case 4: Secure Interaction of Ancillary Hotel System (with PMS)

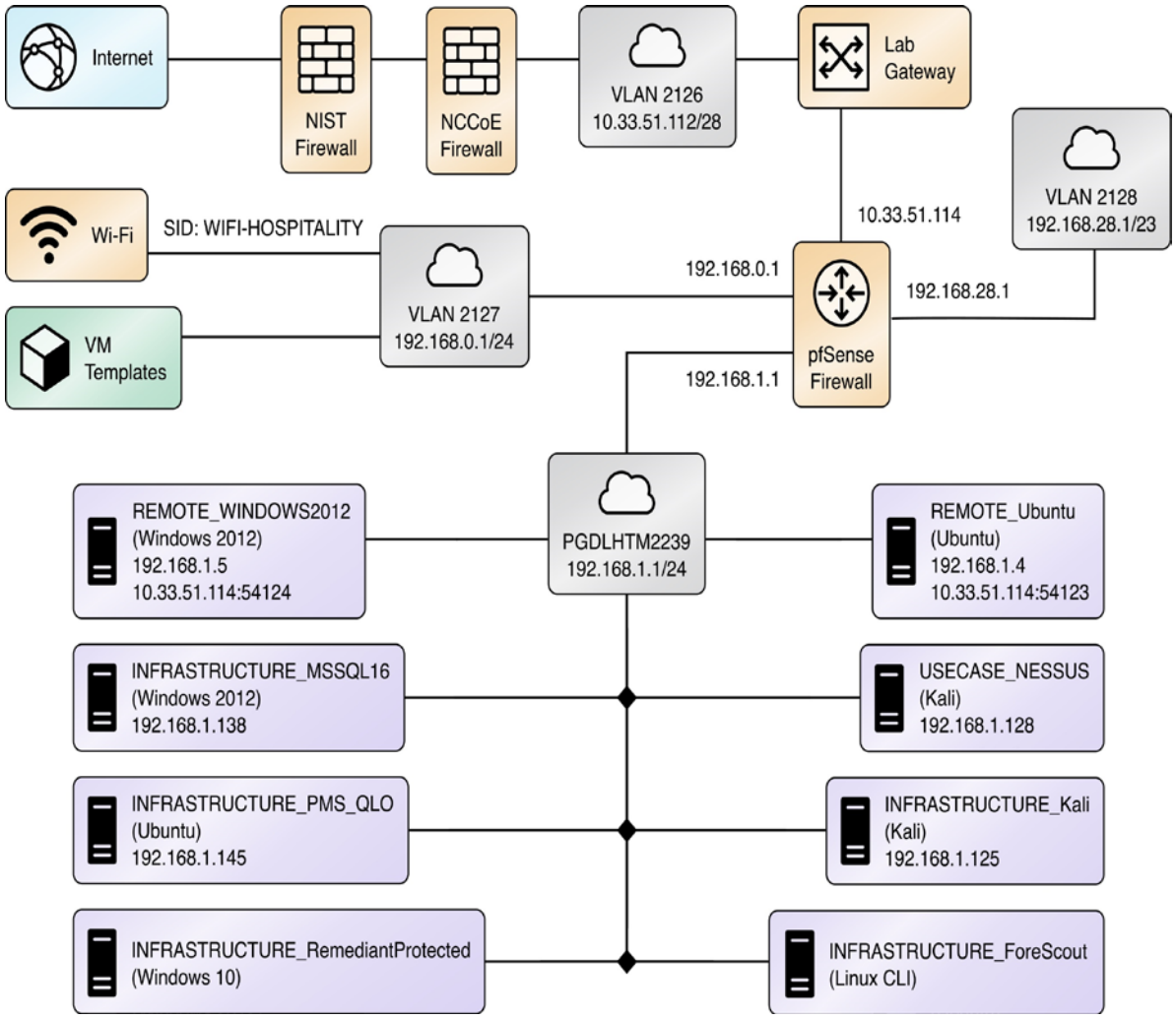
In Use Case 4, the PMS securely interacts with a physical access control system, specifically a door lock and room-key encoder.

The physical access control server is a door lock/room-key system that requires connectivity to the PMS. To encode a room key at check-in, an authorized staffer accesses the PMS to identify the assigned guest room number and provides only the room number to the physical access control server (PACS) to encode a unique room key. In this process, the authorized staff authenticates to the PACS and simply inputs a room number. No guest PII is moved from the PMS to the PACS during key creation.

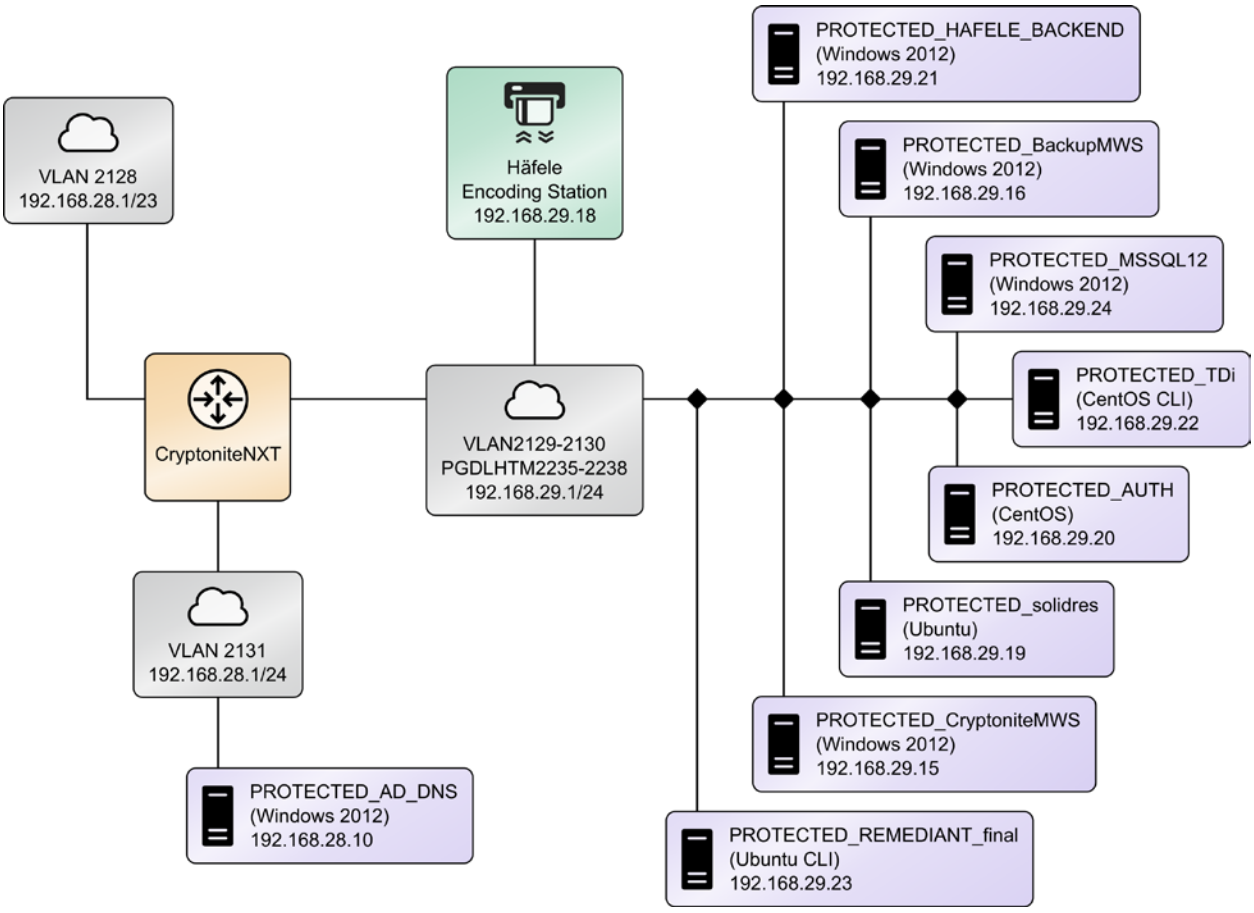
4.3 Detailed Architecture

All devices that operate within the PMS environment for this project are shown in Figure 4-2 and Figure 4-3. The design is separated into two figures for space considerations. The two figures are the two halves of the overall design.

484 **Figure 4-2 Secure PMS Reference Design (part 1 of 2)**



485 **Figure 4-3 Secure PMS Reference Design (part 2 of 2)**



486 The following summarizes the main function of each technology as displayed in Figure 4-2 and Figure 4-
487 3.

488 • The pfSense firewall provides exterior protection and segments the enterprise into the guest
489 portion and the nonguest portion.
490 • Forescout CounterACT protects the guest portion of the Wi-Fi by limiting guest access to only
491 the internet and preventing guest access to hotel back-end systems.
492 • The CryptoniteNXT device provides the secure zone for the enterprise, which includes tenets of
493 zero trust architecture (ZTA) and MTD.
494 • TDi ConsoleWorks facilitates the user authentication security and functionality.
495 • StrongKey SAKA (StrongAuth KeyAppliance) provides the token vault and tokenization along
496 with multifactor authentication.
497 • Remediant SecureONE receives logs and monitors for incidents.
498 • Häfele Dialock's physical access control system encodes and manages room keys.

4.4 Technologies

Table 4-1 lists the technologies used in this project and provides a mapping among the generic application term, the specific product used, the Cybersecurity Framework Subcategories and the Privacy Framework Subcategories that are affected by the product.

Table 4-1 Products and Technologies

Component	Product	Function	NIST Cybersecurity Framework Subcategories Affected	NIST Privacy Framework Subcategory Affected
PMS	Solidres Note: This is the only purchased component in this project.	heart of the hotel enterprise; facilitates the reservations process, checks customers in and out, tracks charges, and reconciles billing	N/A	N/A

Component	Product	Function	NIST Cybersecurity Framework Subcategories Affected	NIST Privacy Framework Subcategory Affected
network protection device	CryptoniteNXT Secure Zone 2.9.1	network protection appliance that works in concert with firewalls; provides additional layer of protection against cyber attacks	**ID.AM-1** Physical devices and systems within the organization are inventoried. **ID.AM-2** Software platforms and applications within the organization are inventoried. **PR.AC-4** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. **PR.AC-5** Network integrity is protected (e.g., network segregation, network segmentation). **PR.DS-2** Data in transit is protected. **PR.DS-5** Protections against data leaks are implemented. **PR.IP-3** Configuration change control processes are in place. **PR.PT-4** Communications and control networks are protected.	**ID.IM-P8** Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.

Component	Product	Function	NIST Cybersecurity Framework Subcategories Affected	NIST Privacy Framework Subcategory Affected
access control platform	TDi ConsoleWorks 5.2-0u1	secures connection and control mechanism to enterprise devices from authorized users and authorized devices; also provides security perimeter monitoring, auditing, and logging activity down to the keystroke	**PR.AC-1** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. **PR.AC-3** Remote access is managed. **PR.AC-4** **PR.AC-6** Identities are proofed and bound to credentials and asserted in interactions. **PR.AC-7** Users, devices, and other assets are authenticated (e.g., single factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks). **PR.PT-3** **DE.CM-3** Personnel activity is monitored to detect potential cybersecurity events.	**CT.PO-P3** Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.
privileged access management	Remediant SecureONE 18.06.3-ce	provides real-time incident monitoring and detection, privilege escalation management, and reporting functions for the IT enterprise	**PR.AC-1** **PR.AC-3** **DE.AE-2** Detected events are analyzed to understand attack targets and methods. **DE.CM-1** The network is monitored to detect potential cybersecurity events. **DE.CM-7** Monitoring for unauthorized personnel, connections, devices, and software is performed. **DE.DP-4** Event detection information is communicated.	**CT.DM-P8** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.

Component	Product	Function	NIST Cybersecurity Framework Subcategories Affected	NIST Privacy Framework Subcategory Affected
wireless protection and visibility platform	Forescout CounterACT 8.1	provides insight into the diverse types of devices connected to the network; enforces policy-based controls to reduce the attack surface	**ID.AM-1** **ID.AM-2** **PR.AC-3** **PR.AC-5** **DE.AE-2** **DE.CM-1**	**ID.IM-P4** Data actions of the systems/products/services are inventoried. **CT.DM-P1** Data elements can be accessed for review.
payment solution appliance	StrongKey Key Appliance	secures credit card transactions and shrinks PCI compliance enclave	**PR.AC-1** **PR.DS-1** Data a rest is protected.	**ID.IM-P8**
physical access control server	Häfele Dialock 2.0	physical access control ecosystem, including door locks, room-key encoding, and management	N/A	N/A
firewall	pfSense	exterior border protection; demarcation	N/A	N/A

4.5 Process Flows

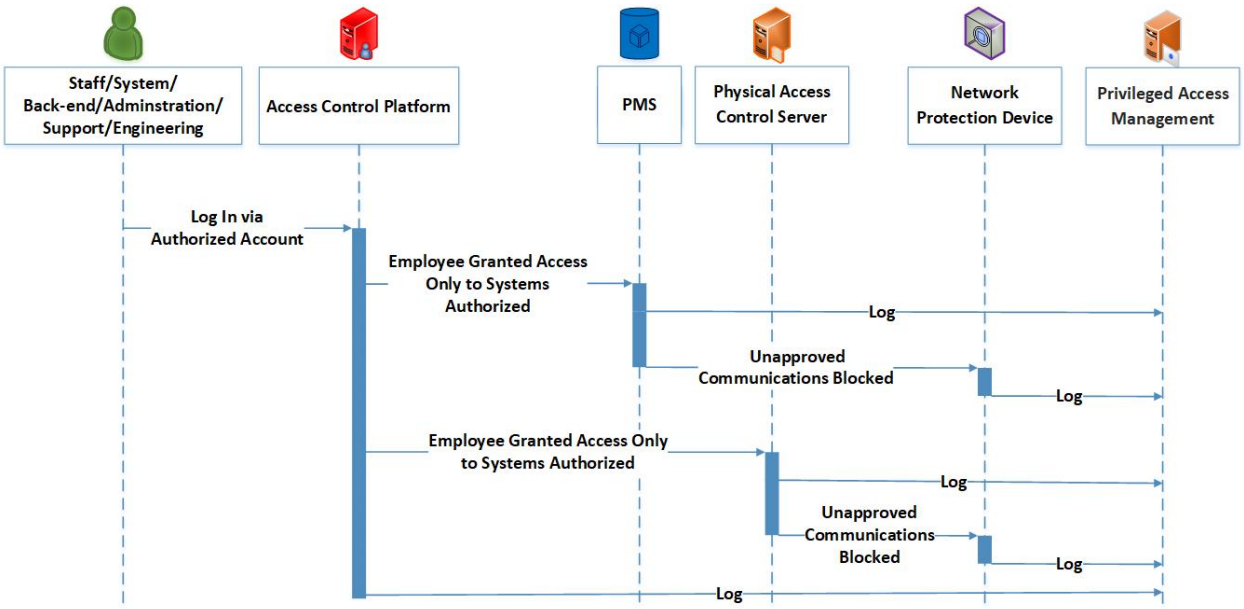
The following process flows show the sequence of events taking place for various hospitality functions in the enterprise.

4.5.1 Authorized Employee Access

Figure 4-3 shows the process flow for an authorized employee connecting to only the systems for which they are authorized. The employee will be challenged by the access control platform and will be required to present whatever credentials are required by policy; further, they will be granted only minimal access based upon their role. The process of Figure 4-4 is described below.

1. From a device or terminal, an authorized employee attempts to log in via the access control platform. All login attempts are directed to the access control platform and logged.
2. The employee who presents valid authentication credentials is granted access to only the system(s) they are allowed based upon their role.
3. The network protection device monitors their activity and maintain logs via the privileged access management system.
4. Any suspicious behavior is noted, logged, and responded to based on policy.
5. Logs are collected by the privileged access management solution.

Figure 4-4 Staff Process Flow

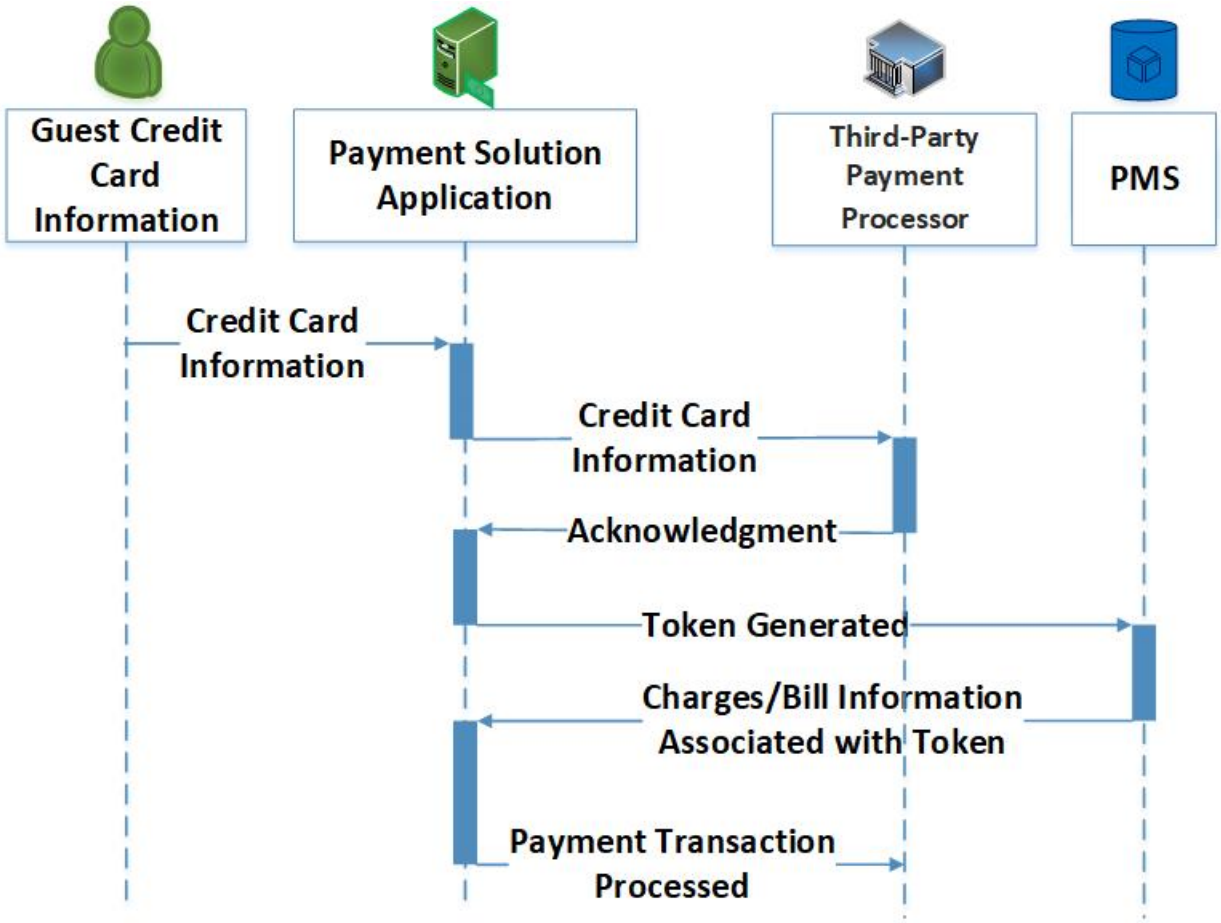


4.5.2 Secure Credit Card Transaction

Figure 4-5 shows the process flow for a credit card transaction [1]. The transaction is protected by the payment solution application via tokenization [2]. The token alone is ineffective as only the payment solution application can decrypt it and associate a credit card with charges. The process of Figure 4-5 is described below.

1. The payment solution application collects the credit card information.
2. The payment solution application secures credit card information via a secure vault.
3. The payment solution application validates with a third-party payment processor.
4. The payment solution application issues a token.
5. Charges/bill are reconciled via the token from the PMS through the payment solution application back to the third-party payment processor when the guest checks out.

532 **Figure 4-5 Secure Credit Card Process Flow**

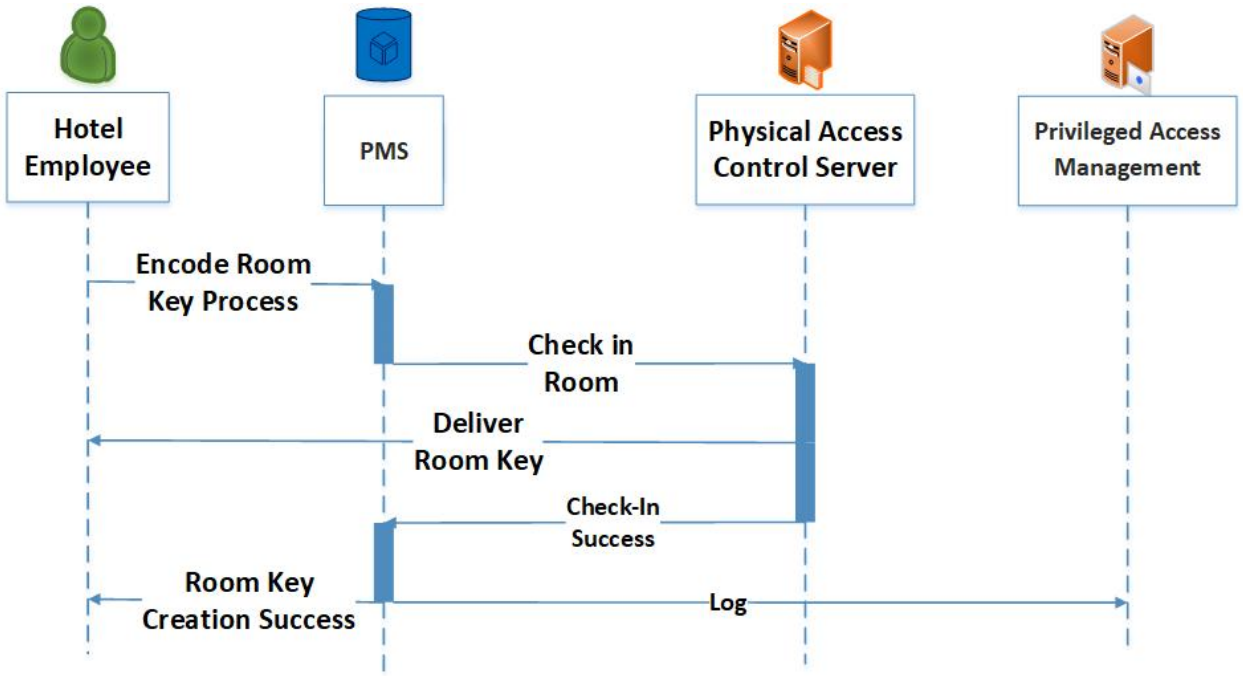


533 ### 4.5.3 Secure Interaction of Ancillary Hotel System (with PMS)

534 Figure 4-6 shows the process flow for the secure interaction of an ancillary system with the PMS. The
535 following demonstrates how a door lock/room-key system is used in this example implementation.

536 1. An authorized employee connects to the PMS.
537 2. The physical access server validates the room-key request against a reservation in the PMS.
538 3. The room key is created and delivered.
539 4. All activity is logged and sent to the privileged access management system.

Figure 4-6 Secure Interaction of Ancillary System with PMS Process Flow

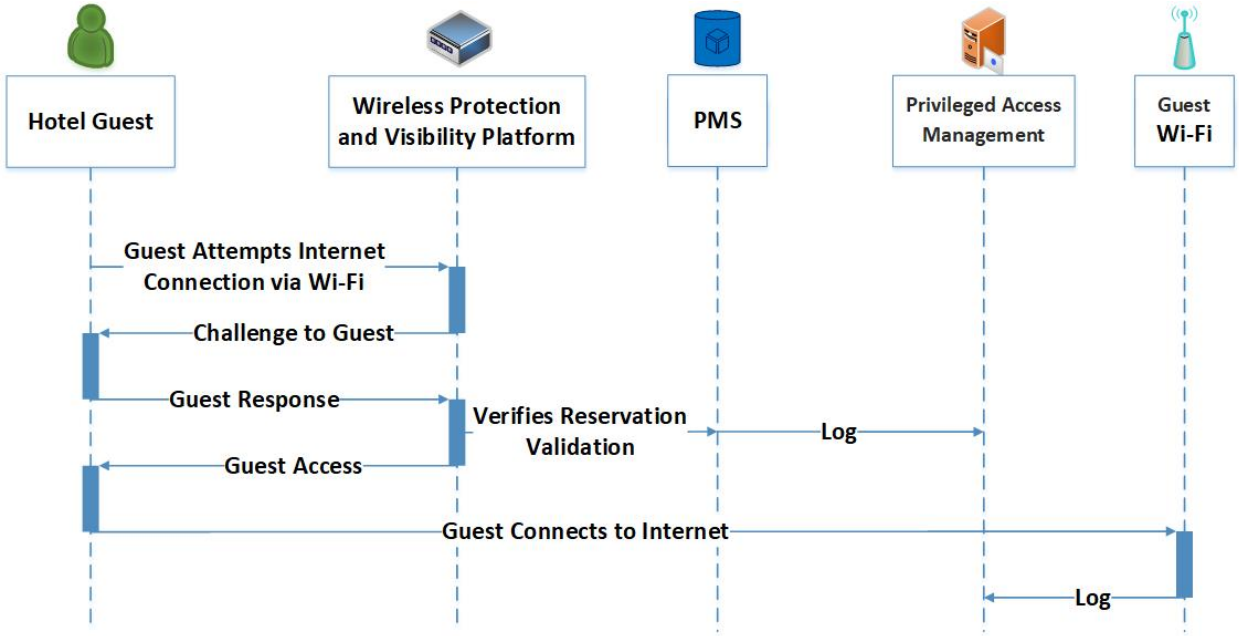


4.5.4 Guest Internet Access via Guest Wi-Fi

Figure 4-7 shows the process flow for a guest accessing the internet via the hotel's guest Wi-Fi, showing how the:

1. guest attempts to connect to the internet via the guest Wi-Fi
2. guest is challenged
3. guest responds with temporary credentials they have been provided, corresponding to their reservation
4. wireless protection and visibility platform validates with the PMS, and the guest is provided internet access
5. guest is provided only access to the internet (is forbidden to move laterally) and any external-facing enterprise hospitality systems; all activity, including surfing and web activity, is logged and sent to the privileged access management system

553 **Figure 4-7 Guest Internet Access via Guest Wi-Fi Process Flow**



554 # 5 Security Characteristic Analysis

555 The purpose of the security characteristic evaluation is to understand the extent to which the project
556 meets its objective of demonstrating improved cybersecurity of a PMS.

557 ## 5.1 Limitations

558 The security characteristic evaluation has the following limitations:

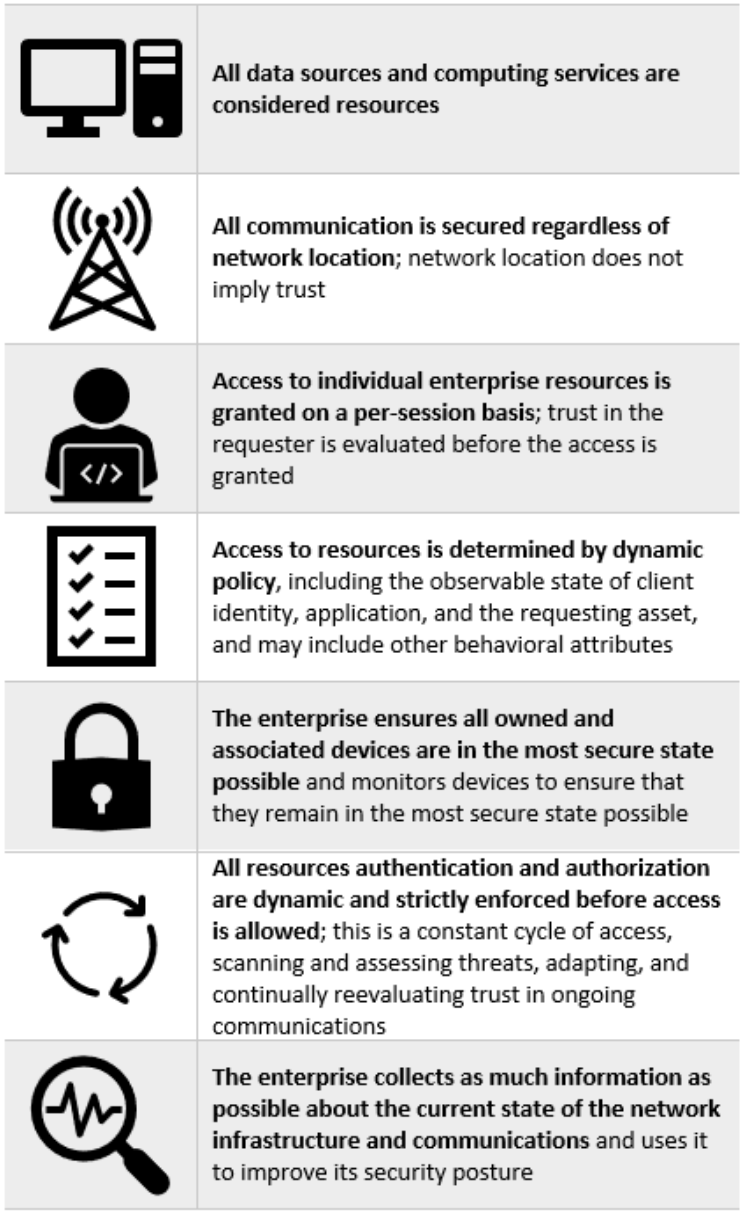
559 - It is not a comprehensive test of individual security components, nor is it a red team exercise.
560 This project did not include a comprehensive test of all security components or "red team"
561 penetration testing or adversarial emulation. Cybersecurity is a rapidly evolving field where new
562 threats and vulnerabilities are continually discovered. Therefore, this security guidance cannot
563 be guaranteed to identify every potential weakness of the build architecture. It is assumed that
564 implementers will follow risk management procedures as outlined in the NIST Risk Management
565 Framework.

566 - Security of the Reference Design

567 The NIST Cybersecurity Framework Subcategories are a basis for organizing our analysis and allowed us
568 to systematically consider how well the reference design supports the intended security characteristics.

569 This project is also designed to show a PMS ecosystem that adheres to some of the tenets of zero trust
570 architecture.

571 **Figure 5-1 Tenets of Zero Trust**



572 Table 5-1 shows zero trust tenets associated with components in the PMS ecosystem and Cybersecurity
573 Framework Subcategories.

574 **Table 5-1 Zero Trust Tenets/Components/Cybersecurity Framework Subcategories**

Zero Trust Tenet	PMS Ecosystem Component	Cybersecurity Framework Subcategories
All data sources and computing services are considered resources.	CryptoniteNXT Secure Zone 2.9.1	**ID.AM-1** Physical devices and systems within the organization are inventoried. **ID.AM-2** Software platforms and applications within the organization are inventoried.
All communication is secured regardless of network location; network location does not imply trust.	CryptoniteNXT Secure Zone 2.9.1 StrongKey's vault	**PR.AC-5** Network integrity is protected. **PR.DS-1** Data at-rest is protected **PR.DS-2** Data in transit is protected. **PR.PT-4** Communications and control networks are protected.
Access to individual enterprise resources is granted on a per-session basis; trust in the requester is evaluated before the access is granted.	TDi ConsoleWorks 5.2-0u1	**PR.AC-1** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. **PR.PT-3** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.

Zero Trust Tenet	PMS Ecosystem Component	Cybersecurity Framework Subcategories
Access to resources is determined by dynamic policy, including the observable state of client identity, application, and the requesting asset, and may include other behavioral attributes.	TDi ConsoleWorks 5.2-0u1	**PR.AC-4** Access permissions and authentications are managed, incorporating the principles of least privilege and separation of duties. **PR.AC-6** Identities are proofed and bound to credentials and asserted in interactions. **DE.CM-3** Personnel activity is monitored to detect potential cybersecurity events.
The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors devices to ensure that they remain in the most secure state possible.		**PR.IP-1** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).
All resources' authentication and authorization are dynamic and strictly enforced before access is allowed; this is a constant cycle of access, scanning and	Remediant SecureONE 18.06.3-ce	**PR.AC-1** Identities and credentials are issued, managed, verified, revoked, and audited for

Zero Trust Tenet	PMS Ecosystem Component	Cybersecurity Framework Subcategories
assessing threats, adapting, and continually reevaluating trust in ongoing communications.	CryptoniteNXT Secure Zone 2.9.1 Forescout CounterACT 8.1	authorized devices, users and processes. **PR.AC-3** Remote access is managed. **PR.AC-4** Access permissions and authentications are managed, incorporating the principles of least privilege and separation of duties. **PR.DS-5** Protections against data leaks are implemented. **PR.IP-3** Configuration change control processes are in place. **DE.CM-7**: Monitoring for unauthorized personnel, connections, devices, and software is performed.
The enterprise collects as much information as possible about the current state of the network infrastructure and communications and uses it to improve its security posture.	Remediant SecureONE 18.06.3-ce	**DE.AE-2** Detected events are analyzed to understand attack targets and methods. **DE.CM-1** The network is monitored to detect potential cybersecurity events. **DE.DP-4** Event detection information is communicated.

6 Privacy Characteristic Analysis

The purpose of a privacy characteristic evaluation is to understand the extent to which a project meets its objective of demonstrating improved privacy protection for a PMS.

6.1 Limitations

For this project, the privacy characteristic evaluation has the following limitations:

- It is not a comprehensive test of individual privacy components, nor does it include a privacy risk assessment methodology in that the design is clean slate.
- It cannot identify all weaknesses.

6.2 Privacy Protections of the Reference Design

The *NIST Privacy Framework* Core Subcategories are a basis to identify privacy characteristics that are supported by our PMS ecosystem. The PMS ecosystem architecture was designed before the *NIST Privacy Framework* [1] was developed. This section is included to draw attention to the Privacy Framework and to highlight that protecting an individual's privacy could become a core value for PMS ecosystems through more thorough use of the Privacy Framework.

See the Privacy Framework Mapping, Table B-1, in Appendix B for the technical privacy characteristics identified as being satisfied by this PMS ecosystem.

7 Functional Evaluation

7.1 Test Cases

This section includes the test cases necessary to conduct the functional evaluation of the PMS example implementation. Refer to Section 4 for descriptions of the tested example implementation.

Each test case consists of multiple fields that collectively identify the goal of the test, the specifics required to implement the test, and how to assess the results of the test. Table 7-1 describes each field in the test case.

Table 7-1 Test Case Fields

Test Case Field	Description
requirement tested	identifies the requirement to be tested and guides the definition of the remainder of the test case fields. specifies the capability to be evaluated
description	describes the objective of the test case
associated Cybersecurity Framework Subcategories	lists the Cybersecurity Framework Subcategories addressed by the test case
sub test cases	In some cases, one or more tests may be part of a larger use-case or functionality.
preconditions	identifies the starting state of the test case. Preconditions indicate various starting state items, such as a specific capability configuration required or specific protocol and content.

procedure	lists the step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple sequences of steps (with delineation) to indicate variations in the test procedure.
expected results	lists the expected results for each variation in the test procedure
actual results	records the observed results
disposition	indicates if the test was passed or failed

7.1.1 PMS Use Case Requirements

Table 7-2 identifies the PMS functional analysis requirements that are addressed in the associated requirements and test cases and mapped to the build components.

Table 7-2 Functional Analysis Requirements

Capability Requirement (CR) ID	Parent Requirement	subrequirement	Test Case	Component
CR 1	guest reservation		PMS-04	property management system
CR 1.a		room key provisioned	PMS-05	physical access control server
CR 2	authorized user can log in		PMS-01	access control platform
CR 2.a		cannot move laterally unless authorized to do so	PMS-03a, PMS-03b	access control platform
CR 2.b		have access only to data they are authorized to access	PMS-03b, PMS-03c	network protection device
CR 2.c		users with partial/compromised credentials are blocked	PMS-02	access control platform
CR 3	secure credit card transaction		PMS-07a	payment solution appliance
CR 3.a		Credit card data was tokenized.	PMS-07a	payment solution appliance

Capability Requirement (CR) ID	Parent Requirement	subrequirement	Test Case	Component
CR 3.b		Eavesdropper cannot see credit card data.	PMS-07b	payment solution appliance
CR 4	Wi-Fi guest connectivity/login		PMS-06a	wireless protection and visibility platform
CR 4.a		Guest cannot access enterprise systems.	PMS-06b	wireless protection and visibility platform
CR 5	Authorized device can connect/ unauthorized device cannot connect.		PMS-08, PMS-09	privileged access management

7.1.2 Test Case PMS-01 (Authorized User Can Log In)

Table 7-3 contains test case requirements, an associated test case, and descriptions of the test scenario for an authorized user logging in to the system(s) for which they are authorized.

Table 7-3 Authorized User Can Log In

Test Case Field	Description
requirement tested	(CR 2) system login capability for authorized users
description	Verify that a new authorized user is provided credentials and can log in to enterprise systems for which they are authorized.
associated Cybersecurity Framework Subcategories	PR.AC-1, PR.AC-4, PR.PT-3
sub test cases	N/A
preconditions	PMS and room-key systems up and running
procedure	Log in to end user workstation/front desk, open TDi in browser, authenticate, open connection to host in console.
expected results	User can log in to the PMS with their issued credentials.
actual results	User can log in to PMS through TDi console. (Other tested machines include front desktop, management workstation.)
disposition	pass

7.1.3 Test Case PMS-02 (PMS Authentication)

Table 7-4 contains test case requirements, associated test case, and descriptions of the test scenario for validating the PMS authentication mechanism and validating that the mechanism protects against compromised accounts/credentials.

Table 7-4 PMS Authentication

Test Case Field	Description

requirement tested	(CR 2.c) users blocked with partial/compromised credentials
description	Validate that authentication to the PMS works as planned, e.g., multifactor authentication, biometric.
associated Cybersecurity Framework Subcategories	DE.AE-2, DE.CM-1, DE.CM-7
sub test cases	If a "user" has only a partial credential or a compromised credential, they cannot access the PMS.
preconditions	PMS configured and running properly
procedure	Log in to end user workstation/front desk, open TDi in browser, authenticate, open connection to Solidres's admin console. Trigger password policy by trying to log in Solidres's admin side 10 times.
expected results	Solidres admin console can be accessed successfully. Locked account cannot be accessed.
actual results	Solidres admin console can be accessed successfully. (Multifactor is enabled and can be used if the user provisions a tokenization device.) Enabled brute force plug-in in PMS that blocks IP for one day when attempting to log in past 10 attempts. The account was locked and could not be accessed after locking.
disposition	pass

7.1.4 Authorized Users Can Access Only Systems and Data They Are Authorized for Test Cases

The following three test cases validate users being granted access only to that for which they are authorized.

7.1.4.1 Test Case PMS-03a (Users Cannot Move Laterally from the PMS Unless Authorized to Do So)

Table 7-5 contains test case requirements, associated test case, and descriptions of the test scenario for preventing lateral movement.

620 **Table 7-5 No Unauthorized Lateral Movement**

Test Case Field	Description
requirement tested	(CR 2.a) cannot move laterally unless authorized to do so
description	Verify that an authorized user cannot go outside their boundary.
associated Cybersecurity Framework Subcategories	PR.AC-5, PR.PT-3, DE.CM-3
sub test cases	If they are authorized to access only the PMS, they cannot move laterally to another enterprise system from the PMS.
preconditions	PMS configured and running properly
procedure	attempted to connect to another system with an account that was authorized only for the PMS
expected results	access denied
actual results	access denied
disposition	pass

621 ### *7.1.4.2 Test Case PMS-03b (Prevent Unauthorized Function)*

622 Table 7-6 contains test case requirements, associated test case, and descriptions of the test scenario for
623 preventing a user from performing a function for which they are not authorized.

624 **Table 7-6 Prevent Unauthorized Function**

Test Case Field	Description
requirement tested	(CR 2.a, CR 2.b) cannot move laterally unless authorized to do so; have access only to data for which they are authorized

description	Verify that an authorized user cannot go outside their "boundary."
associated Cybersecurity Framework Subcategories	PR.PT-3, DE.CM-3
sub test cases	The user cannot perform a function for which they are not authorized, e.g., create a master room key.
preconditions	PMS configured and running properly; Häfele back-end server configured and running properly
procedure	Front desk user created with no write or delete access. Verify the access controls of the Häfele back-end server.
expected results	Häfele permissions do not allow user to create a master room key for all of the created rooms in the back-end server.
actual results	Master key could not be created when the lowest level of privilege was given. The user was not able to add an authorization to create or save MIFARE credentials.
disposition	pass

7.1.4.3 Test Case PMS-03c (Only Authorized Data)

Table 7-7 contains test case requirements, associated test case, and descriptions of the test scenario for ensuring that users have access only to data for which they are authorized.

Table 7-7 Only Authorized Data

Test Case Field	Description
requirement tested	(CR 2.b) have access only to data for which they are authorized
description	Verify that an authorized user cannot go outside their boundary.
associated Cybersecurity Framework Subcategories	PR.AC-5, PR.DS-2, PR.DS-5, PR.PT-3, DE.CM-3

Test Case Field	Description
sub test cases	Verify that the user has access to only the data set(s) for which they are authorized; further, that they can only edit data, download data they are authorized to download, and edit data that they are authorized to edit.
preconditions	PMS configured and running properly
procedure	created a user account that was giving the permission of a "site sponsor." This user account could see only site-specific information, not including guest reservations. After logging in to the account, it was verified that the specified permissions were valid and that the account could not navigate to sensitive data.
expected results	Solidres Access Control List (ACL) controls are functioning, and registered guests or sponsors should not be able to access or view sensitive customer data.
actual results	ACL manages view of permissions of the logged-in users. Users could only view data they were authorized to view within the Solidres PMS.
disposition	pass

7.1.5 Test Case PMS-04 (Guest Reservation Editable)

Table 7-8 contains test case requirements, associated test case, and descriptions of the test scenario for entering a reservation and editing the reservation.

Table 7-8 Guest Reservation Editable

Test Case Field	Description
requirement tested	(CR 1) creating a guest reservation and having the ability of only an authorized user to edit the reservation
description	Enter a guest reservation into the PMS. Verify that it is in the PMS and that it is retrievable and editable.

Test Case Field	Description
associated Cybersecurity Framework Subcategories	N/A
sub test cases	N/A
preconditions	PMS up and running properly
procedure	Navigate to Solidres guest registration from guest machine, and book a room.
expected results	reservation record in the PMS
actual results	The test registration is bookable/retrievable from web interface of Solidres.
disposition	pass

7.1.6 Test Case PMS-05 (Room-Key Provisioning)

Table 7-9 contains test case requirements, associated test case, and descriptions of the test scenario for entering a reservation and editing the reservation.

Table 7-9 Provisioning Room Key

Test Case Field	Description
requirement tested	(CR 1) room key provisioned
description	From the reservation in the PMS, verify that a room key is provisioned for the guest.
associated Cybersecurity Framework Subcategories	N/A
sub test cases	Verify the processing of provisioning, writing, reading.
preconditions	Rooms are defined in Häfele, and PMS is running.

Test Case Field	Description
procedure	Provision a key through the PMS in conjunction with Häfele's back-end server. The provision process includes assigning a key in the PMS, writing a key card with the Häfele back-end server, and making sure that the assigned key-card room number and guest-registered room number are the same.
expected results	Provisioned room key works.
actual results	Room keys were provisioned.
disposition	pass

7.1.7 Provisioning Guest Wi-Fi Access

The following two test cases will validate provisioning guest Wi-Fi access and that guests cannot access the restricted enterprise from the Wi-Fi.

7.1.7.1 Test Case PMS-06a (Guests' Limited Wi-Fi Access)

Table 7-10 contains test case requirements, associated test case, and descriptions of the test scenario for preventing lateral movement.

Table 7-10 Guests' Limited Wi-Fi Access

Test Case Field	Description
requirement tested	(CR 4) Wi-Fi guest connectivity/login
description	Only registered guests will be granted limited Wi-Fi access.
associated Cybersecurity Framework Subcategories	PR.AC-3, PR.IP-3, PR.PT-3, PR.PT-4, DE.CM-3
sub test cases	Verify that the guest can access only authorized resources via the Wi-Fi, e.g., the internet and guest-facing resources such as activities reservations and room charges.
preconditions	PMS up and running properly; guest Wi-Fi up, running, and connected; guest has provisioned Wi-Fi login

Test Case Field	Description
procedure	Attempt to connect a device to the guest Wi-Fi. When the login screen appears, enter the password created for the guest as part of the reservation process to complete the login. Open a browser, and verify internet sites are accessible.
expected results	Guest successfully logs in to Wi-Fi with issued login.
actual results	entered the Wi-Fi key and gained access to the internet
disposition	pass

644 *7.1.7.2 Test Case PMS-06b (Prevent Unauthorized Guest Lateral Movement via Wi-Fi)*

645 Table 7-11 contains test case requirements, associated test case, and descriptions of the test scenario
646 for preventing a guest from accessing any restricted back-end systems.

647 **Table 7-11 Prevent Unauthorized Guest Lateral Movement via Wi-Fi**

Test Case Field	Description
requirement tested	(CR 4.a) Guest cannot access enterprise systems.
description	Only registered guests are granted limited Wi-Fi access.
associated Cybersecurity Framework Subcategories	PR.AC-3, PR.PT-4, DE.CM-3
sub test cases	Verify that the guest via the Wi-Fi cannot jump to any enterprise systems (e.g., PMS).
preconditions	PMS up and running properly; guest Wi-Fi up, running, and connected; guest has provisioned Wi-Fi login

Test Case Field	Description
procedure	Once the guest Wi-Fi is operating and internet access has been established, attempt to ping the IP addresses of the protected hotel systems.
expected results	Guest cannot access unauthorized resources when logged in to the guest Wi-Fi.
actual results	Guest Wi-Fi range is blocked via NGINX ACL implementation, which works with CounterACT protections.
disposition	pass

7.1.8 Secure Credit Card Transaction

The following two test cases validate secure credit card transactions.

7.1.8.1 Test Case PMS-07a (Tokenized Credit Card Data)

Table 7-12 contains test case requirements, associated test case, and descriptions of the test scenario for tokenizing credit card data for a credit card transaction.

Table 7-12 Tokenized Credit Card Data

Test Case Field	Description
requirement tested	(CR 3.a) Credit card data was tokenized.
description	Conduct a credit card transaction, and verify that the credit card data was tokenized and that the transaction went through.
associated Cybersecurity Framework Subcategories	N/A
sub test cases	Validate that credit card data was tokenized; validate that additional charges can be recorded using the token; validate that the token can be reconciled for payment; validate that the token encrypts and/or otherwise obfuscates credit card data; validate that a “captured” or copied or exfiltrated token is worthless.

Test Case Field	Description
preconditions	PMS is up and running properly.
procedure	Log on to end user workstation/front desk, open TDi in browser, authenticate, open connection to Solidres PMS, navigate to reservations, click the test reservation, validate credit card information was tokenized. Open terminal in TDi Virtual Network Computing (VNC) session, authenticate to MySQL Server, view table entries for reservation, validate credit card information was tokenized (database, PMS, over the wire).
expected results	valid credit card transaction. The credit card information can be seen when accessing the guest reservation in the PMS.
actual results	Tokenized credit card information is stored in Solidres and is reading for processing through the offline plug-in. PII for credit card charges is tokenized. Data in database is stored as a token. (The stripe plug-in required a credit card for charges, and the offline plug-in simulates the "on-site payment" solution that charges the cards after the fact or forwards them to a third party securely.)
disposition	pass

7.1.8.2 Test Case PMS-07b (Verify that Credit Card Data Is Hidden)

Table 7-13 contains test case requirements, associated test case, and descriptions of the test scenario for verifying that credit card data is hidden.

Table 7-13 Verify that Credit Card Data Is Hidden

Test Case Field	Description
requirement tested	(CR 3.b) Eavesdropper cannot see credit card data.
description	Conduct a credit card transaction, and verify that the credit card data was tokenized and that the transaction went through.

Test Case Field	Description
associated Cybersecurity Framework Subcategories	PR.AC-5, PR.DS-2, PR.DS-5
sub test cases	Verify that an eavesdropper cannot see any credit card data.
preconditions	PMS is up and running properly.
procedure	Verify that a credit card transaction cannot be determined from captured Wireshark traffic.
expected results	No credit card data is visible to an eavesdropper.
actual results	Wireshark shows Transport Layer Security encrypted traffic where payment information is tokenized, and user is submitting reservation through guest system. Wireshark was run on the host machine that also housed the PMS server.
disposition	pass

7.1.9 Test Case PMS-08 (Authorized Device Provisioning)

Table 7-14 contains test case requirements, associated test case, and descriptions of the test scenario for allowing an authorized device to connect to the enterprise.

Table 7-14 Authorized Device Provisioning

Test Case Field	Description
requirement tested	(CR 5) Authorized device can connect/unauthorized device cannot connect.
description	Verify that an authorized device can be provisioned and added/connected to the enterprise.
associated Cybersecurity Framework Subcategories	ID.AM-1, ID.AM-2, PR.AC-1, PR.IP-3
sub test cases	N/A
preconditions	Various technology is up and running; security mechanisms are in place.

Test Case Field	Description
procedure	Connect an authorized device with valid credentials.
expected results	Device will connect to the enterprise.
actual results	Authorized device could connect.
disposition	pass

7.1.10 Test Case PMS-09 (Prevent Unauthorized Device from Connecting)

Table 7-15 contains test case requirements, associated test case, and descriptions of the test scenario for preventing an authorized device form connecting to the enterprise.

Table 7-15 Prevent Unauthorized Device from Connecting

Test Case Field	Description
requirement tested	(CR 5) Authorized device can connect/unauthorized device cannot connect.
description	Verify that an unknown/unauthorized system that appears on the enterprise cannot access the PMS or establish a connection to any enterprise system.
associated Cybersecurity Framework Subcategories	PR.AC-5, PR.IP-3, DE.CM-1, DE.CM-7
sub test cases	N/A
preconditions	Cryptonite rules are configured to block unverified accounts.
procedure	Add a machine to the secure enclave Virtual Local Area Network (VLAN) (simulates connecting to the network). From the connected machine, try to navigate to the PMS.
expected results	Unverified machine is unable to navigate to PMS.
actual results	Device was not allowed to connect.
disposition	pass

8 Future Build Considerations

We have considered several areas for future or follow-on hospitality projects. These include expanding the physical access control with a connection to mobile devices (mobile device security per NIST SP 1800-4, *Mobile Device Security: Cloud and Hybrid Builds*), smart rooms, and IoT. Subsequent work may

be an amalgamation of these themes grouped into the smart room concept, a focal point in many of these topics. Another possible direction for the follow-on work could be a hotel-centric IoT project.

Appendix A Mapping to Cybersecurity Framework

Table A-1 shows the National Institute of Standards and Technology (NIST) Cybersecurity Framework Subcategories that are addressed by the property management system (PMS) ecosystem built in this practice guide. The first three categories show the Cybersecurity Framework details. The next three categories show how the Cybersecurity Framework Subcategories are related to requirements in Payment Card Industry Data Security Standard (PCI DSS) v3.2.1; security and privacy controls in NIST Special Publication (SP) 800-53r4; and work roles in NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [12]. This table is included to help connect those with expertise in any of these areas and illuminate areas that the PMS ecosystem. Examining the work roles in the NICE Framework may help an organization understand if it has people who can perform tasks and apply the skills described for each work role on its teams. Noting a discrete PCI requirement or NIST SP 800-53 control [9] may match areas of focus within an organization that securing a PMS ecosystem could help address.

Table A-1 Securing Property Management Systems: NIST Cybersecurity Framework Components Mapping

NIST Cybersecurity Framework v1.1			Standards and Best Practices		
Function	**Category**	**Subcategory**	**PCI DSS v3.2.1**	**NIST SP 800-53r4 Security and Privacy Controls [9]**	**NIST SP 800-181, NICE Framework Work Roles (Work Role ID) [12]**
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and man-	**ID.AM-1:** Physical devices and systems within the organization are inventoried.		CM-8, PM-5	Technical Support Specialist (OM-STS-001)
		ID.AM-2: Software platforms and applications within the organization are inventoried.		CM-8, PM-5	Technical Support Specialist (OM-STS-001)

	aged consistent with their relative importance to organizational objectives and the organization's risk strategy.				
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. 3.6.1 Generate strong keys. 3.6.2 Keys are only distributed to authorized recipients. 3.6.3 Stored keys are stored encrypted. 3.6.4 A reasonable crypto period shall be set. 3.6.5 A key life cycle shall be established, denoting when keys should be destroyed and when keys should be securely kept for archived/legacy encrypted data.	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	System Administrator (OM-ADM-001) Product Support Manager (OV-PMA-003)

			3.6.7 Keys shall only be accepted from authorized sources.		
		PR.AC-3: Remote access is managed.	8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • enabled only during the time period needed and disabled when not in use • monitored when in use	AC-1, AC-17, AC-19, AC-20, SC-15	Information Systems Security Developer (SP-SYS-001) System Administrator (OM-ADM-001)
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	Technical Support Specialist (OM-STS-001)
			7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.		Technical Support Specialist (OM-STS-001)

			7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.		
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	1.1 Establish and implement firewall and router configuration standards.	AC-4, AC-10, SC-7	Network Operations Specialist (OM-NET-001)
			1.1.4 requirements for a firewall at each internet connection and between any demilitarized zone (DMZ) and the internal network zone		Network Operations Specialist (OM-NET-001)
			1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.		Network Operations Specialist (OM-NET-001)

			1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.		Network Operations Specialist (OM-NET-001)
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	8.1.6 Limit the number of failed login attempts. 8.1.7 Establish a reasonable "cool down period" for locked-out accounts prior to automatic unlocking processes. 8.1.8 Reasonable idle time prior to workstation lockout shall be established. 8.2 Where appropriate, multifactor authentication (two or more of something you know, something you have, and something you are) shall be implemented. 8.2.1 Authentication transactions and data are encrypted at rest and in transit.	AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	Systems Requirements Planner (SP-SRP-001)

		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).		AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11	Systems Requirements Planner (SP-SRP-001)
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data at rest is protected.	3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.	MP-8, SC-12, SC-28	Information Systems Security Developer (OM-DTA-002)
			3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This		Information Systems Security Developer (OM-DTA-002)

			data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.		
			3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.		Information Systems Security Developer (OM-DTA-002)
			3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.		Information Systems Security Developer (OM-DTA-002)
			3.4 Render Primary Account Number unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:		Information Systems Security Developer (OM-DTA-002)

		PR.DS-2: Data in transit is protected.	1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. 1.3 Prohibit direct public access between the internet and any system component in the cardholder data environment.	SC-8, SC-11, SC-12	Information Systems Security Developer (OM-DTA-002) Cyber Defense Analyst (PR-CDA-001) Information Systems Security Developer (OM-DTA-002) Cyber Defense Analyst (PR-CDA-001)
		PR.DS-5: Protections against data leaks are implemented.		AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4	Information Systems Security Developer (SP-SYS-001)
	Information Protection Processes and Procedures (PR.IP): Security poli-	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and		CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	Enterprise Architect (SP-ARC-001) Cyber Policy and Strategy Planner (OV-SPP-002)

	cies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	maintained, incorporating security principles (e.g., concept of least functionality).			
		PR.IP-3: Configuration change control processes are in place.		CM-3, CM-4, SA-10	Systems Developer (SP-SYS-002) Systems Security Analyst (OM-ANA-001)
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	AC-3, CM-7	Privacy Officer/Privacy Compliance Manager (OV-LGA-002)
		PR.PT-4: Communications and control networks are protected.		AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32,	Security Architect (SP-ARC-002) Communications Security (COMSEC) Manager (OV-MGT-002)

				SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected, and the potential impact of events is understood.	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods.		AU-6, CA-7, IR-4, SI-4	Cyber Defense Analyst (PR-CDA-001)
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of	**DE.CM-1:** The network is monitored to detect potential cybersecurity events.		AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	Cyber Defense Analyst (PR-CDA-001)
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.		CA-7, PE-3, PE-6, PE-20	Network Operations Specialist (OM-NET-001)

	protective measures.	**DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed.		AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	Threat/Warning Analyst (AN-TWA-001)
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-4: Event detection information is communicated.	10.1 Audit logs are generated, documenting user activity. 10.2 Audit events are logged. 10.2.1 User account privileges are documented. 10.2.7 The creation and deletion of system level objects are logged. 10.3 Events are logged so that they are auditable. 10.5 Audit logs are strongly protected, including encryption and strong role-based authentication for authorized log users.	AU-6, CA-2, CA-7, RA-5, SI-4	Cyber Defense Infrastructure Support Specialist (PR-INF-001)

Appendix B Privacy Framework Mapping

Table B-1 shows National Institute of Standards and Technology *(NIST) Privacy Framework* Subcategories as outcomes addressed in this practice guide and mapped to the property management (PMS) ecosystem components.

Table B-1 Securing Property Management Systems: NIST Privacy Framework Components Mapping

Privacy Framework Function	Privacy Framework Category	Privacy Framework Subcategory	PMS Ecosystem Component
Identify-P	Inventory and Mapping (ID.IM-P)	**ID.IM-P4:** Data actions of the systems/products/services are inventoried.	Forescout CounterACT 8.1
		ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components, roles of the component owners/operators, and interactions of individuals or third parties with the systems/products/services.	CryptoniteNXT Secure Zone 2.9.1 StrongKey KeyAppliance
Control-P	Data Processing Management (CT.DM-P)	**CT.DM-P1:** Data elements can be accessed for review.	Solidres PMS Forescout CounterACT 8.1
		CT.DM-P2: Data elements can be accessed for transmission or disclosure.	Solidres PMS
		CT.DM-P3: Data elements can be accessed for alteration.	Solidres PMS
		CT.DM-P4: Data elements can be accessed for deletion.	Solidres PMS
		CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the	Remediant SecureONE 18.06.3-ce

Privacy Framework Function	Privacy Framework Category	Privacy Framework Subcategory	PMS Ecosystem Component
		principle of data minimization.	

Appendix C Deployment Recommendations

When deploying the reference design in a hospitality environment, organizations should follow security best practices to address potential vulnerabilities and ensure that all solution assumptions are valid to minimize any risk to the production network. Organizations leveraging the reference design should adhere to recommended best practices that are designed to reduce risk. Note that the laboratory instantiation of the reference design described in Volume C does not implement every security recommendation on its own.

Organizations should not consider the following list to be comprehensive, as merely following this list will not guarantee a secure environment. Organizations must consider items such as vulnerability and patch management, continuity of operations planning, and environment elements that are not addressed in this document. Planning for design deployment gives an organization the opportunity to audit its existing systems and get a clear view of the controls going into effect.

Appendix D List of Acronyms

2FA	Two Factor Authentication
CNSSI	Committee on National Security Systems Instruction
GDPR	General Data Protection Regulation
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
MTD	Moving Target Defense
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
PMS	Property Management System
POS	Point of Sale
SP	Special Publication
VLAN	Virtual Local Area Network
VM	Virtual Machine
ZTA	Zero Trust Architecture

Appendix E Glossary

Access Control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). SOURCE: Committee on National Security Systems Instruction (CNSSI) 4009-2015
Architecture	The design of the network of the hotel environment and the components that are used to construct it.
Authentication	The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. SOURCE: Federal Information Processing Standards (FIPS) 200
Authorized User	Any appropriately provisioned individual with a requirement to access an information system. SOURCE: CNSSI 4009-2015
Console	A visually oriented input and output device used to interact with a computational resource.
Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. SOURCE: NIST SP 800-150
Firewall	A part of a computer system or network that is designed to block unauthorized access while permitting outward communication. SOURCE: NIST SP 800-152
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. SOURCE: FIPS 200

Multifactor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). SOURCE: CNSSI 4009-2015
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. SOURCE: NIST SP 800-37 Rev. 2
Privilege	A right granted to an individual, a program, or a process. SOURCE: CNSSI 4009-2015
Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. SOURCE: NIST SP 800-161
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. SOURCE: FIPS 200
Wi-Fi	A generic term that refers to a wireless local area network that observes the IEEE 802.11 protocol. SOURCE: NIST Interagency or Internal Report 7250

Appendix F References

[1] National Institute of Standards and Technology. *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management,* Version 1.0. Available: https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf.

[2] Hotel Technology Next Generation (HTNG). *Secure Payments Framework for Hospitality,* version 1.0. Feb. 2013. Available: https://cdn.ymaws.com/htng.site-ym.com/resource/collection/CC1CE2B8-0377-457E-9AB0-27CFDD77E17B/HTNG_Secure_Payments_Framework_v1.0_FINAL.pdf.

[3] HTNG. *Payment Tokenization Specification*. Feb. 21, 2018. Available: https://www.htng.org/page/technical_specs.

[4] HTNG. *Payment Systems & Data Security Specifications 2010B*. Oct. 22, 2010. Available: https://cdn.ymaws.com/www.htng.org/resource/resmgr/Files/Specifications/2010B/HTNG_2010B_PaymentsWG_Paymen.pdf.

[5] HTNG. *EMV for the US Hospitality Industry*. Oct. 1, 2015. Available: https://cdn.ymaws.com/sites/htng.site-ym.com/resource/collection/CC1CE2B8-0377-457E-9AB0-27CFDD77E17B/2015-09-23_EMV_White_Paper.pdf.

[6] Payment Card Industry Data Security Standard version 3.2.1. May 2018. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

[7] HTNG. *GDPR for Hospitality*. June 1, 2019. Available: https://www.hospitalitynet.org/file/152008749.pdf.

[8] NIST. *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1. Apr. 16, 2018. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[9] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations,* NIST Special Publication (SP) 800-53 Rev. 4, NIST, Gaithersburg, Md., Apr. 2013. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[10] P. Grassi et al., Digital Identity Guidelines, NIST SP 800-63-3, NIST, Gaithersburg, Md., June 22, 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[11] E. McCallister et al., *Guide to Protecting the Confidentiality of Personably Identifiable Information (PII),* NIST SP 800-122, NIST, Gaithersburg, Md., Apr. 2010. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

[12] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,* NIST SP 800-181, NIST, Gaithersburg, Md., Aug. 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[13] Abbasi et al., *2019 Trustwave Global Security Report*, 2019 Trustwave Holdings, Inc. Available: https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/.

[14] NIST. *Risk Management Framework: Quick Start Guides*. Available: https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides.

[15] Joint Task Force, *Risk Management Framework for Information Systems and Organizations*, NIST SP 800-37 Revision 2, NIST, Gaithersburg, Md., Dec. 2018. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[16] Joint Task Force, *Guide for Conducting Risk Assessments,* NIST SP 800-30 Revision 1, NIST, Gaithersburg, Md., Sept. 2012. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[17] Social Tables. *Cybersecurity for Hotels: 6 Threats Just Around the Corner from Your Property.* Available: https://www.socialtables.com/blog/hospitality/cyber-security-hotels/.

[18] Calicchio et al, 2018 PwC Hotels outlook: 2018-2022. PWC, Inc. Available: https://www.pwc.co.za/en/assets/pdf/hotels-outlook-18-2022.pdf

[19] C. Paulsen R. Byers, Glossary of Key Information Security Terms, NIST Interagency or Internal Report 7298 Rev. 3, NIST, Gaithersburg, Md., July 2019. Available: https://csrc.nist.gov/glossary/term/vulnerability.

[20] W. Newhouse et al., *Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers,* NIST SP 800-17, NIST, Gaithersburg, Md., Aug. 2018, 253 pp. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/cr-mfa-nist-sp1800-17.pdf.