Implementing a Mobile Identity Application in a Ubiquitous Computing Environment

Christopher R. Byrnes & Tyler V. Rimaldi
Marist College
School of Computer Science and Mathematics
Poughkeepsie, NY 12601
{Christopher.Byrnes, Tyler.Rimaldi1}@Marist.edu

***Abstract*—The proliferation of smartphones and Internet of Things devices has resulted in a range of new applications. Applied and emerging technologies include Bluetooth and Near Field Communications, peer-to-peer networks, and edge-computing, all of which can substantially improve or enhance the experience of end users on college campuses. As these technologies are applied to more areas, there will be a greater need for a single federated digital identity to manage their use. A ubiquitous computing environment emerges when these various components are combined in an increasingly seamless manner, offering a range of benefits to end users and participants. The Marist College Digital Identity Initiative offers proof-of-concept implementation of key components of this emerging network of sensors and devices by demonstrating the ability to issue, change and revoke facility access across campus. There is an opportunity to vastly enhance federated identity end user experience a wide range of activities on Marist College campus, from building access to library resource management and retail payments.**

Keywords*—*Ubiquitous computing, federated identify, mobile application, bluetooth, near field communication, digital identification, peer-to-peer networks, identity and access management

I. Introduction

Smartphones and Internet of Things (IoT) devices are becoming more pervasive in our personal and professional lives [1]. Already these technologies are used to measure our fitness, wirelessly connect to our TVs, and to pay for coffee. As we move from an internet of information to one of value, it becomes necessary to encrypt and provision a variety of identity traits to the many nodes with which we interact across the digital layer. From "Name" and "Date of Birth" to student ID numbers and bank account information, the collection of these identity traits, available for transaction within ubiquitous computing environments, comprise what is called a federated identity. This portfolio of identity traits creates the foundation for a wide range of innovative applications that enhance how we experience the physical-digital interface, and take advantage of an increasingly ubiquitous network of sensors.

There is widespread market acceptance of the technologies that make this architecture possible, which means we can expect the range of applications to grow [2]. Bluetooth Low Energy (BT LE) and Near Field Communication (NFC), pervasive data encryption, smartphone applications, Peer-to-Peer (P2P) computing, and ubiquitous sensors combine to support millions of transactions per day [2]. As these applications scale, the volume of transactions will grow rapidly, so we must develop a means of managing this collection of federated identity traits in the digital layer.

In this paper we provide technical background on several applied and emerging technologies that make up the digital identity ecosystem. We discuss products from IBM and Lenel that have been used to integrate those technologies in an enterprise software platform on the Marist College campus. With this understanding, we provide a detailed discussion of our implementation, outlining our efforts in four areas: requirements, design, execution, and testing & troubleshooting. Finally, we conclude by discussing potential applications that could enhance business processes at Marist College and other institutions.

The opportunities that arise from a scaled implementation of these technologies is significant. Within this proof-of-concept (POC), we demonstrated an enhanced user experience in the form of ease of use and convenience by maintaining credentials in a digital wallet. For administrators, we optimized several business processes involved in the management of identities and access across the campus. At scale, costs would be reduced by relying less on physical, plastic ID cards, and require less labor in the management of new credentials. Finally, by using digital ID cards, we expect that impacts on the environment can be reduced. In addition to the immediate benefits of this network, the capabilities it brings will enable a range of innovations that will enhance user experience across the campus. Examples are improved handicap access to buildings and learning spaces; optimized library resource management that would enable students to seamlessly reserve and access study rooms and other spaces; improved campus security through P2P identity challenge and verification.

Key contributions of this paper include the following:

- In Section II we consider prior work and examine applied and emerging technologies including BT LE, NFC, P2P networks, identity and access management (IAM), and edge computing environments.
- In Section III we discuss the design, architecture, and implementation of our ubiquitous computing network for mobile identity. We also show the application of federated identity traits through our proof-of-concept implementation.
- Section IV describes how federated identity applications in edge-computing environments support the emergence of ubiquitous computing.
- We conclude in Section V with ideas for applying these technologies to enhance the quality of ubiquitous end user experiences.

II. Background

We provide this background to establish core concepts in BT LE, NFC, P2P networks, federated identities, and the industry products used in this implementation. With this understanding, we then describe and demonstrate the performance of the architecture. Throughout this discussion we use the term ”device” to encompass all types of wireless-enabled smartphones and sensors. However, when we describe our implementation, ”device” will refer specifically to an iPhone with BT connectivity.

A. Prior Work

The Marist Digital Identity Initiative builds on an existing body of knowledge and work. Pardo de Vera et al. discuss the need for ”an infrastructure with automatic mechanisms to allow applications to discover and access particular information provided by sensors networks over the Internet” [1]. This is an important assumption in the building of a local, ubiquitous network such as the one offered in this POC. We make this assumption and build on it to envision first, a small network of connected BT sensors tied to identity and access management software, and later, an entire federated identity interfacing with a host of other sensors that allow for the increasingly seamless interaction between the physical world and digital objects.

McWaters et al. lay out a very thorough argument of the need for digital identities in the future [2]. They describe the different types of identity traits that a successful federated identity must provide in order to meet rising user expectations across the range of use cases. We incorporate many of these factors into our own assumptions of the utility that a federated Marist ID card would provide on Marist Campus and beyond.

Chadwick explains succinctly both what comprise an identity in general, those characteristics such as ”hair colour, sound of their voice, height, name, qualifications, past actions, reputation, medical records, etc”. He further explains the characteristics of identity management as ”a set of functions and capabilities...used for assurance of identity information...assurance of the identity of an entity...and enabling business and security applications [3]. The understanding provided by Chadwick is critical for our POC implementation because the traits selected for inclusion must be tied to transactional behavior such as access credentials, payments, or resource management.

Srivastava et. al provide a unique and informative viewpoint on the types of implementations that are possible using ubiquitous sensor networks. They argue that ”[s]mart environments instrumented with sensor- and-wireless-enhanced objects would be able to sense events and conditions about people and objects in the environment, and act upon the sensed information or use it as context when responding to queries and commands. [4]” We agree with this, and show in our implementation that such improvements begin with the elemental applications of our identities, namely for the purpose of access, but extensible to a range of other activities and processes.

Gomez, Oller, and Paradells provide a useful overview and description of the layers involved in BT technology, which is representative of the architecture used in this POC. They introduce the concept of advertising and data channels, which plays a role in our evaluation of this POC, particularly as it relates to latency times for BT synchronization. Though BT LE does provide an incremental improvement over previous methods of access control (e.g. magnetic strip, proxy card), we believe that further improvement will be recognized by the application of NFC, whose benefits over BT LE we describe further [5].

Wang et al. are cited to provide a succinct definition of a P2P network. Some of the more pertinent applications are to act as a distributed network for data exchange that responds to requests for resources, updates performance parameters, and supplies resources to an originator if possible [6]. While we implemented a small-scale model of such a network, we envision a scaled version to contain multiple structured and unstructured networks cooperating to enhance the end users' quality of experience [6], [7].

Bajaj introduces an emerging technology, NFC, and provides a useful overview of the its applications, many of which we argue could be readily implemented on the Marist College campus [4], [8]. He provides a comparison of NFC to BT and infrared (IR), which strengthens the argument for an eventual implementation of a ubiquitous sensor network that takes advantage of NFC [9].

B. Specific Tools

1) Bluetooth Communication: Devices utilizing BT communication are managed using a star topology, in which a master node provides a time division multiple access radio frequency (TDMA RF) for up to 7 other devices [5]. Peripheral nodes synchronize to the frequency of the master node, enabling peripherals to persistently transmit information back and forth [5]. The transmission range for BT technology varies from 10 meters for class 3 devices up to 100 meters for class 1 devices [10]. Both devices used in this implementation were version 4.0 LE or more recent.

2) Near Field Communication: NFC can be split into two modes, active and passive. Devices in active mode generate their own RF for transmission purposes [8]. These devices must contain their own power supply. When two devices are in active mode and are within a proximity of 4cm - 20cm, they can open up two-way, peer-to-peer communications suitable for data transfer [8] [11] [12]. Devices in passive mode do not generate their own RF and do not need to contain their own power supply [8]. Devices in passive mode use Near Field Wireless Power Transfer Technology (NFWPTT), a form of magnetic induction, to send a response back to the active device [8], [13].

3) Peer-to-Peer Networks: P2P networks exist wherever there is more than one computing node, when each node possesses spare processing power, and when each node has the capacity to exchange and store transactional data [6]. Such networks enable smartphones and other IoT devices to connect and transfer data in a persistent and ubiquitous manner, enhancing the network performance and quality of end user experience.

P2P networks can exist in three forms: unstructured, structured, and hybrid. Unstructured networks contain randomly graphed nodes that can choose other nodes with which to pair or interact with [14]. Structured networks, on the other hand, can be thought of as a keyed list of nodes. The placement of data within a node and the placement of the node on a graph both vary depending on specific keys [14]. Each set of data corresponds to a specific key that is represented on the node. Using that key, the node is graphed accordingly, thus representing an organized graph [14]. A hybrid network combines properties of both, such as the node placement found in structured networks, and the data placement and discovery methods found in unstructured networks [14]. This provides efficient data searches throughout a large network nodes.

P2P networking can improve the quality of end user experience by performing a multitude of tasks. By taking advantage of the spare memory and computing power of edge devices, devices can transmit access credentials used to enter a room or a building simply by recognizing known nodes in their proximity and by performing the desired actions. Devices can respond to requests for identity information from unknown nodes if the appropriate credentials are presented, providing only information that is requested and not revealing more than is needed. They can also communicate with retail point-of-sale systems to facilitate cashier-less checkout, making appropriate charges to bank accounts. These federated identity traits are readily transmitted on a P2P network with sufficient speed (e.g. 5G) [15], and demonstrate the wide range of applications that such networks provide.

4) IBM Mobile Identity: IBM Mobile Identity (MI) is a cloud-based cryptographic framework for issuing and managing federated identity documents represented by secure tokens. Its functionality is embedded within the Marist digital student identity card through a Software Development Kit (SDK), and interacts through a Representational State Transfer Application Programming Interface (REST API) between the card acquisition server and IBM's cloud credential server. IBM's MI provides user authentication and authorization for a variety of user identity applications, including one-way transmission of encrypted credentials and two-way transmission of identity challenges and encrypted credentials. [16]

5) Lenel Onguard and BlueDiamond: Lenel's Onguard is an open architecture identity and access management software used by Marist College. It provides a web-browser enabled user interface to issue and manage access credentials and to resolve alarm conditions at buildings throughout campus. Through a REST API, it provisions a one-time authentication code to device users, who in turn use that code to pair their device with a particular identity document. In this implementation, we paired each user device with an encrypted representation of the user's student identity number. In the Onguard terminal interface, when a credential is issued to a particular user, Onguard automatically sends an email to the user, with a link to a credential server, which returns the one-time authorization code.

Lenel's BlueDiamond BT LE readers allow digital credentials to be submitted from a mobile application on a smartphone to the Onguard system for identity verification and access approval. Once submitted, the credentials are vetted against the authorized users' Lightweight Directory Access Protocol (LDAP) server profile and Onguard access credentials. Lenel also provides a mobile application that we used as a performance and stability benchmark. Once the BlueDiamond mobile application was shown to be stable and reliable, we installed and began testing the Marist College Digital Identity application [17].

6) Marist College Digital Identity Initiative: The Marist College Digital Identity Initiative is a proof-of-concept (POC) program to develop, implement, and test a software/hardware architecture that enhances the ways in which Marist College identity cards are used on and around campus. Through the IBM/Marist College Joint Study, and in partnership with IBM and Lenel, this initiative has progressed through two phases of POC implementation, Event Registration and Secure Access.

In the first phase, Event Registration, we demonstrated the ability to issue a digital identity card for use by a smartphone application, and to register students at a Marist activity using a QR code. This showed that college administrators and students could enjoy significant efficiencies in the issuance of identities and registration of students at sanctioned events.

In the second phase, Secure Access, we demonstrated the ability to issue, change, and revoke access to buildings, classrooms, and offices on campus. Using IBM MI, and having installed a BlueDiamond BT LE reader on a server room door, students, faculty, and staff now have the ability to acquire a digital identity, receive and activate credentials, and open bluetooth-enabled locks that are available to them utilizing a smartphone application. The application submits encrypted credentials to the door lock reader, which are compared against an access database, and if the participant is authorized, the lock is activated and the door is opened.

III. Implementation

The technologies we have discussed up to now allow us to digitize student identification cards, enhancing end user experience, and streamlining administrator business processes. In this section we discuss each of the four phases of the Digital Identity Initiative: requirements, design, execution, and testing.

A. Requirements

Requirements for implementing this POC were gathered between January and February of 2018. During this time, regular conference calls among stakeholders from IBM, Lenel, and Marist College were held to identify key resources and integration points, and to offer a venue for participants to communicate directly with one another.

Requirements generally fell within one of three categories: software and hardware resources, administrative and legal, and design and technology integration. Initial software resources included a Docker container environment running on an Ubuntu server on Marist's internal server network [18]. This required 35 GB of storage and 4 GB of RAM.

In order to issue digital student identities from this environment, IBM provided an on-boarding package that provided necessary scripts and HTML files to create and acquire digital identity cards for integration with our smartphone application. We developed a web acquisition page to allow for input of student profile pictures, names, student identity numbers, and other pertinent information. These forms can be tailored to accommodate as much information as institution managers wish to include within their federated identity programs.

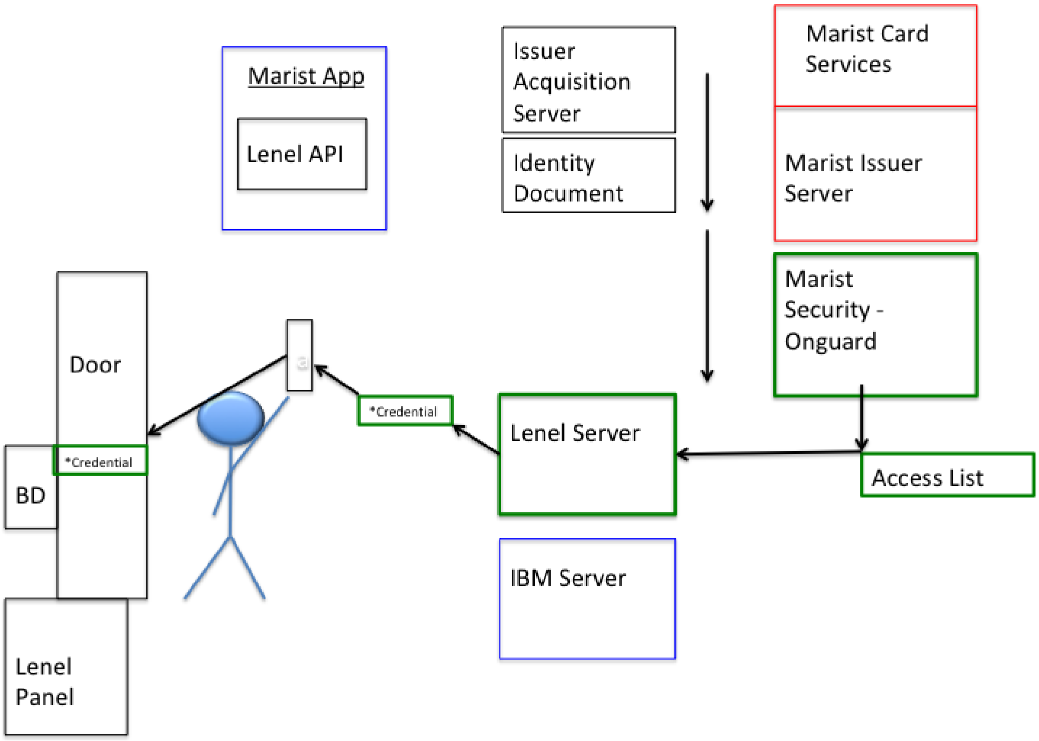


Fig. 1. Digital Identity Architecture

B. Design

Our system design takes advantage of a service-oriented architecture (SOA) to issue Marist identity credentials, to generate encrypted credentials paired to user devices, and to update user credentials as appropriate based on changing access authorization [19]. These actions are performed by REST API's integrated with each main process. The design of the the Marist card acquisition page was largely dictated by the features of the IBM MI product. This included all functionality necessary for hosting web services, creating digital ID cards, and integrating with the smartphone application.

The Onguard workstation located in the Marist Security office is a key component in this process. It connects to a database of all students, faculty, staff, and visitors who can be issued access credentials. We used the Onguard system to generate an email, which was sent to the end user with a link to a credential server. When activated, that link sends an API request to the credential server, which returns a one-time authorization code to the end user. That credential is then uniquely paired with the user's device, offering resistance against unauthorized use or other malicious intent.

We designed our architecture to implement two separate smartphone applications primarily for testing purposes. The first is a mobile application developed by Lenel for use with its Onguard system and BlueDiamond BT readers. The second app was developed by IBM and Marist to integrate with its MI product. We use the BlueDiamond application to set performance and stability benchmarks. Once demonstrated, we began testing the Marist-branded application, which used an embedded SDK provided by Lenel to call on the same services as the BlueDiamond application.

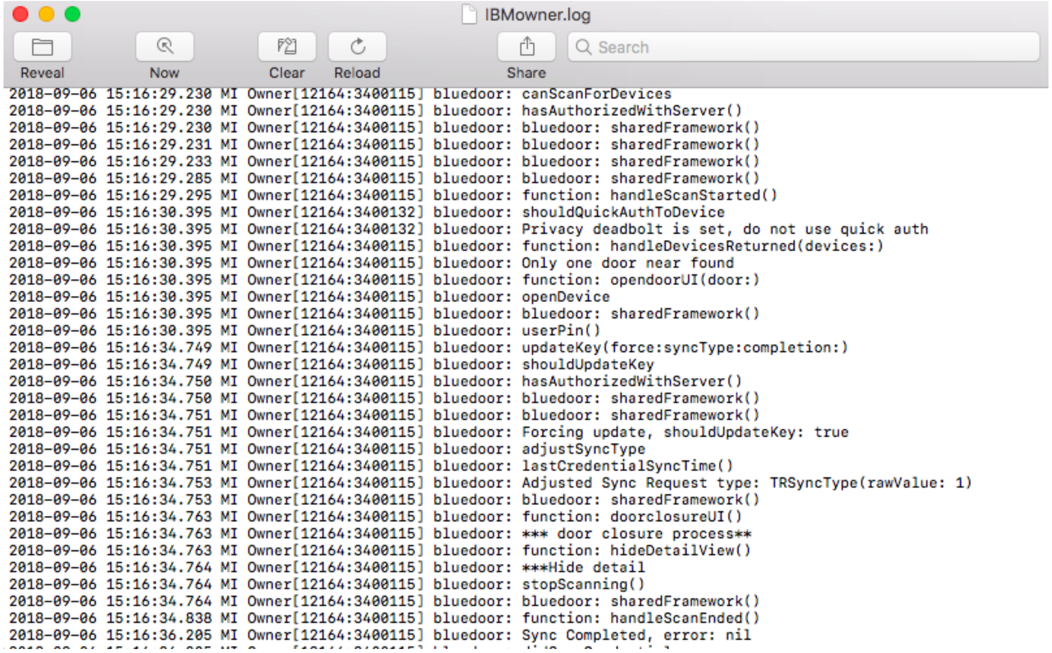
C. Execution

In the implementation at Marist College, we use a wireless sensor network, micro-processors, and wireless communications [10]. The collection of smartphones present on the Marist College campus effectively acts as a wireless sensor network of peer-to-peer devices that provides the ability to award and revoke access, create and execute resource reservations, verify identities, and incentivize behavior across different types of participants within a peer-to-peer, edge computing framework [20].

Using products from IBM and Lenel, we have implemented a wireless sensor network containing peer-to-peer, ubiquitous mobile devices, enabling us to monitor and validate credentials. The first critical milestone within the execution phase was to install the bluetooth reader on the door lock to the Enterprise Computing Research Laboratory (ECRL). In conjunction, we configured Onguard to accommodate the addition of a a digital identity credential, and to be able to send new credentials to end users through Marist's SMTP server.

In order to provide a suitable mobile environment to support testing of the Digital Identity application on iOS devices, we provisioned TestFlight to several participants. TestFlight allows for beta testing of applications on iOS devices without submitting the application to the iTunes store.

Next, we demonstrated successful activation of the bluetooth door lock using Lenel's BlueDiamond application. First, we manually entered the necessary information in URL format



```
2018-09-06 15:16:29.230 MI Owner[12164:3400115] bluedoor: canScanForDevices
2018-09-06 15:16:29.230 MI Owner[12164:3400115] bluedoor: hasAuthorizedWithServer()
2018-09-06 15:16:29.230 MI Owner[12164:3400115] bluedoor: bluedoor: sharedFramework()
2018-09-06 15:16:29.231 MI Owner[12164:3400115] bluedoor: bluedoor: sharedFramework()
2018-09-06 15:16:29.233 MI Owner[12164:3400115] bluedoor: bluedoor: sharedFramework()
2018-09-06 15:16:29.285 MI Owner[12164:3400115] bluedoor: bluedoor: sharedFramework()
2018-09-06 15:16:29.295 MI Owner[12164:3400115] bluedoor: function: handleScanStarted()
2018-09-06 15:16:30.395 MI Owner[12164:3400132] bluedoor: shouldQuickAuthToDevice
2018-09-06 15:16:30.395 MI Owner[12164:3400132] bluedoor: Privacy deadbolt is set, do not use quick auth
2018-09-06 15:16:30.395 MI Owner[12164:3400115] bluedoor: function: handleDevicesReturned(devices:)
2018-09-06 15:16:30.395 MI Owner[12164:3400115] bluedoor: Only one door near found
2018-09-06 15:16:30.395 MI Owner[12164:3400115] bluedoor: function: opendoorUI(door:)
2018-09-06 15:16:30.395 MI Owner[12164:3400115] bluedoor: openDevice
2018-09-06 15:16:30.395 MI Owner[12164:3400115] bluedoor: bluedoor: sharedFramework()
2018-09-06 15:16:30.395 MI Owner[12164:3400115] bluedoor: userPin()
2018-09-06 15:16:34.749 MI Owner[12164:3400115] bluedoor: updateKey(force:syncType:completion:)
2018-09-06 15:16:34.749 MI Owner[12164:3400115] bluedoor: shouldUpdateKey
2018-09-06 15:16:34.750 MI Owner[12164:3400115] bluedoor: hasAuthorizedWithServer()
2018-09-06 15:16:34.750 MI Owner[12164:3400115] bluedoor: bluedoor: sharedFramework()
2018-09-06 15:16:34.751 MI Owner[12164:3400115] bluedoor: bluedoor: sharedFramework()
2018-09-06 15:16:34.751 MI Owner[12164:3400115] bluedoor: Forcing update, shouldUpdateKey: true
2018-09-06 15:16:34.751 MI Owner[12164:3400115] bluedoor: adjustSyncType
2018-09-06 15:16:34.751 MI Owner[12164:3400115] bluedoor: lastCredentialSyncTime()
2018-09-06 15:16:34.753 MI Owner[12164:3400115] bluedoor: Adjusted Sync Request type: TRSyncType(rawValue: 1)
2018-09-06 15:16:34.753 MI Owner[12164:3400115] bluedoor: bluedoor: sharedFramework()
2018-09-06 15:16:34.763 MI Owner[12164:3400115] bluedoor: function: doorclosureUI()
2018-09-06 15:16:34.763 MI Owner[12164:3400115] bluedoor: *** door closure process**
2018-09-06 15:16:34.763 MI Owner[12164:3400115] bluedoor: function: hideDetailView()
2018-09-06 15:16:34.764 MI Owner[12164:3400115] bluedoor: ***Hide detail
2018-09-06 15:16:34.764 MI Owner[12164:3400115] bluedoor: stopScanning()
2018-09-06 15:16:34.764 MI Owner[12164:3400115] bluedoor: bluedoor: sharedFramework()
2018-09-06 15:16:34.838 MI Owner[12164:3400115] bluedoor: function: handleScanEnded()
2018-09-06 15:16:36.205 MI Owner[12164:3400115] bluedoor: Sync Completed, error: nil
```

Fig. 2. User Log File

into the test device browser, which navigated to the BlueDiamond application. We then demonstrated the ability to send an email from Onguard to the user device and authorize the device by clicking on a link to the credential server within that email. This step required two weeks of troubleshooting before we were able to accomplish sending the email and subsequent authorization. A more in depth discussion of the troubleshooting necessary to accomplish this is provided in the next section.

After demonstrating that we could successfully send an activation email and open the bluetooth lock using the BlueDiamond application, we proceeded to show the same capability using the Marist Digital Identity application, using the same procedures that we did for the BlueDiamond application.

As seen in Fig. 1, the platform design allows for Card Services to issue digital identity cards and Security services to separately manage the issuance, changing, and revoking of access credentials. The Lenel Server performs in the same manner that it would under a BlueDiamond configuration, in that it generates an authorization code, which is used to pair the user device with the unique access credential generated by the IBM server. The credential is sent to the user device and stored there until modified or revoked. Once presented to the Bluetooth reader associated with a door, the credential is compared with the access list managed by the Security office.

D. Testing

Testing and troubleshooting began with the installation of the BlueDiamond BT reader on the ECRL door and configuration of Onguard for interoperability with a digital credential. We used the BlueDiamond mobile application to activate the door lock by manually entering the authorization code in the URL of our smartphone browser (Safari). This proved our ability to activate the application and open the door. Following that we sought to demonstrate the ability to send an email to the end user, which contained a link to the credential server. On activation of the link, the user is sent a one-time activation code used to pair the device with the federated identity trait stored in Onguard, in this case the student ID number.

In attempting to provision these credentials using an email, we received an error indicating that the credential had been provisioned, but the email failed to send. In troubleshooting this issue, we examined multiple nodes and logs within the Onguard network, including the Marist user database (SQL Server), network monitors (EMO logs), the Onguard workstation (Lenel debugging logs and IBMOwnerlogs). We eventually traced the issue to the local instance of the McAfee Virus Scanner Service, which was preventing the request from being sent to the SMTP server. The sender account was white-listed by the local administrator, but the scanner service was interrupted when sending the email from the Onguard administrator account.

When we were finally able to properly generate and send the activation credential, we then sought to demonstrate the same ability with the Marist Digital Identity application. This required a small change to the HTML script called by the Onguard .exe file to activate the Marist application instead of BlueDiamond.

We found that high latency results in longer wait times due to bluetooth synchronization requirements. This resulted in an average synchronization time of 5.04 second from submitting the request for access in the application to the lock being activated. The credential encryption process speed is more dependent on the speed by which the email server sends the email from Onguard through the local SMTP server, and received by the end user. This ranged from a minute or two to several depending on local network traffic.

There are some drawbacks to BT LE that could be overcome by the use of NFC instead. In testing, we were able to successfully connect with and activate the BT reader from a distance of over 9 meters, which could be seen as a security drawback. Man-in-the-middle attackers could easily intercept the signal with eavesdropping tools and play it back when the genuine user is not present. The shorter range and higher frequency of NFC would limit the volume of space available to a would-be attacker. The shorter ranges of NFC would also allow for easier signal management by end user smartphones. Currently, the Marist Digital Identity application presents a list of all available BT readers to the end user. This could become difficult to manage if a specific end user had access to several doors in a given geographic area. The shorter transmission ranges of NFC would limit the number of accessible BT readers and improve the quality of experience for the end user. In the next phase of this initiative, we will install additional BT readers to see how the user devices respond to additional BT signals [12].

IV. Benefits

In surveying the landscape of the Marist College ecosystem, we identified several areas where our platform provides significant benefits. These include process optimization and automation, elimination of plastic waste, labor cost savings, streamlined decision making, and ease of use.

Fig. 2 shows the user log file from a successful activation of the ECRL lock using the Marist Digital Identity application. Key events in this log are the ”canScanForDevices”, ”Only one door near found”, ”openDevice”, ”userPin”, ”stopScanning”, and ”Sync Completed, error: nil”. Collectively they represent the process whereby our architecture allows for scanning by the user device, discovery of available BT devices, opening of the lock, and completion of the synchronization. These actions will allow for several follow-on benefits throughout Marist College campus. The user device will be able to scan for other BT devices with which it can interact, such as student computer terminals and library desks.

Processes that could be streamlined or automated include, class attendance and club participation, dining hall and bookstore payments, applying for and receiving financial aid. All of these activities are good candidates for inclusion in the Digital Identity Initiative because they interact with one or more aspects of the federated identity traits they require At each point of interaction between two nodes, one or more identity traits must be transmitted, received, and stored for comparison against a database, as represented in Fig. 2.

In an edge computing framework, technologies such as bluetooth-enabled devices, user-specific credential encryption, and smartphone applications will enable Marist College to streamline its operations with respect to credential monitoring and issuance. Students, faculty, and staff members can be issued credentials digitally. These devices will operate in a peer-to-peer, edge computing framework that offers fast and secure monitoring of credentials. This will enable more trust to the Security office, as these credentials will be sent through a secure network to an application on the users device that requires the user’s fingerprint to access, preventing unauthorized identity use.

In addition to streamlining Marist College operations, these technologies will offer cost and waste reduction. Physical identity cards will no longer be necessary, as identity cards will be digitized and stored locally on a user’s device. Instead of allocating funds to buy plastic and ink to print identity cards, administrators will simply issue and authorize credentials digitall.

V. Future Work

A. *Security Challenge*

Extending the ability demonstrated in the Secure Access Phase to a Security Challenge is a natural next step. The IBM MI session layer currently provides the ability to send a request for an identity trait to any other bluetooth-enable smartphones with the MI framework available for synchronization. An additional node is introduced representing a campus security guard who may decide to challenge the identity of someone on Marist College campus. The security guard could send a request to the unknown person to authenticate their identity, corresponding to their status as a student, faculty, staff member, visitor, or unknown. This status would maintain dependencies on several other user identity traits such as whether they are in good standing with the Financial Aid office, or whether they have graduated or withdrawn with the Registrar’s office. While the security guard could also verify the identity of the person by looking at the picture on the digital ID card, the Digital Identity application provides a more thorough understanding of the unknown person’s identity, without divulging more than is needed.

B. *Library Resource Management Tool*

In the case of a Library Resource Management system, several processes can be streamlined. A critical component in the user’s federated identity is transacted, there is significant cost savings, and it provides ease of use that does not exist today. An application would be developed to interact through a REST API with the legacy system in use within the library. Bluetooth or near-field readers would be installed at the circulation desk, study rooms, and other nodes where the user’s identity is required. On presenting the user’s smartphone to the reader, the appropriate action would then take place, either accessing the library user’s account, or requesting that a study room door be opened.

VI. Conclusion

As organizations implement more technologies that make their user experiences more seamless, ubiquitous networks will naturally emerge. Those networks will necessarily consist of many of the technologies that we describe here: bluetooth sensors, mobile applications, federated identities, and legacy systems. They will also assuredly incorporate other technologies like NFC, which will make these networks more secure and less subject to malicious attacks.

The Digital Identity Initiative demonstrates that such networks are feasible and provide significant benefits to students and administrators. Existing business processes will be streamlined and enhanced through the integration of legacy systems with industry products like Mobile Identity and BlueDiamond. Just as the magnetic strip and proximity chip enhanced the experience of end users accessing buildings and paying for goods, so too will digital credentials provisioned on mobile identity applications improve the interoperability of legacy systems with emerging technologies, while opening other areas to innovation.

Acknowledgments

We would like to thank the team of engineers at IBM and Lenel for their contributions to this project, including Dan Gisolfi, Greg Lacey, Jonathon Kaufman, Aaron Reed, Richard Redpath, and Bryce Curtis from IBM; Mike Green, Greg Berry, Jay Shephard, Yuri Novozhenets, Kumar Praveen, and Maroju Kishore from Lenel; Dave Thomas and Kevin Addington from Open Systems Integrators. We also want to thank several members of the Marist College community, including Peter Wenzel, Kathleen LaBarbera, Pat Goewey, Chris Taylor, Roger Norton. A special thanks to Prof. Alan Labouseur for his help bringing this paper together. We'd also like to thank Daniel Gisolfi, Phaelan Koock, Katerina Tzannes, and Danny Mulick from the Joint Study for their contributions.

References

[1] Pardo de Vero, Izquierdo, Vercher, Gomez, "A Ubiquitous Sensor Network Platform for Integrating Smart Devices into the Semantic Sensor Web," *Sensors*, vol. 14, 2014.

[2] J. McWaters, G. Bruno, M. Drexler, R. Galaski, and C. Robson, "A Blueprint for Digital Identity The Role of Financial Institutions in Building Digital Identity," in *A Blueprint for Digital Identity*, 08 2016, online, Accessed 8/15/2018.

[3] D. W. Chadwick, *Federated Identity Management*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 96–120. [Online]. Available: https://doi.org/10.1007/978-3-642-03829-7_3

[4] M. Srivastava, R. Muntz, and M. Potkonjak, "Smart Kindergarten: Sensor-Based Wireless Networks for Smart Developmental Problem-Solving Environments," University of California, Los Angeles.

[5] C. Gomez, J. Oller, and J. Paradells, "Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology," *Sensors*, pp. 11 734–11 753, August 2012, online, Accessed 8/15/2018.

[6] Fang Wang and Robert A. Ghanea-Hercock and Yaoru Sun, "Peer-to-Peer Networks," Patent US 7,852,786B2, 12 14, 2010. [Online]. Available: http://www.patentlens.net/patentlens/patent/US_7062320/

[7] R. Mahmud, S. N. Sriramana, K. Ramamohanaro, and R. Buyaa, "Quality of Experience (QoE): Aware Placement of Applications in Fog computing Environment," *Journal of Parallel and Distributed Computing*, 2018, https://doi.org/10.1016/j.jpdc.2018.03.004.

[8] C. Bajaj, "Near Field Communication," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, pp. 899–905, August 2014, online, Accessed 8/12/2018.

[9] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on Fog Computing: Architecture, Key Technologies, Applications and Open Issues," *Journal of Network and Computer Applications*, vol. 98, pp. 27–42, June 2017.

[10] S. Krco, "Bluetooth Based Wireless Sensor Networks Implementation Issues and Solutions," *Applied Research Lab, Ericsson Ireland*.

[11] "Near Field Communication - Interface and Protocol (NFCIP-1)," *Standard*, vol. 3, June 2013, ECMA Standard.

[12] E. Haselsteiner and K. Breitfu, "Security in Near Field Communication (NFC)," *Strengths and Weaknesses*, Philips Semiconductors.

[13] M. A. Hassan and A. Elzawawi, "Wireless Power Transfer through Inductive Coupling," *Recent Advances in Circuits*, http://www.inase.org/library/2015/zakynthos/bypaper/CIRCUITS/CIRCUITS-18.pdf.

[14] M. Castro, M. Costa, and A. Rowstron, "Peer-to-peer overlays: structured, unstructured, or both?" *Microsoft Research*, 08, Technical Report, MSR-TR-2004-73.

[15] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile Edge Computing: A key technology towards 5G," *European Telecommunications Standards Institute*, vol. White Paper, September 2015.

[16] "IBM Mobile Identity Documentation," http://pilot.mi-project.org:9282/, 2015-2017, online, Accessed 9/7/2018.

[17] "Onguard," online, Accessed 9/7/2018.

[18] "What is Docker?" *https://www.docker.com/what-docker*, accessed 9/6/2018.

[19] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," *Wireless Communication and Mobile Computing*, vol. 13, pp. 1587–1611, June 2013.

[20] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, Oct 2016, online, Accessed 8/12/2018.