Marist College Digital Identity Initiative

Christopher Byrnes

Partners

- Marist / IBM Joint Study
- Marist IT
- Marist Security
- Marist Card Services

Industry Platforms

- North Carolina
- Poughkeepsie

- Albany

- Albany

Digital Identity Initiative

Design Phases	Applied Technologies
Event Participation, 2016-2017	Digital Credentials
Secure Access, Spring 2018	Credential Encryption
Security Challenge, Summer 2018	Credential Exchange
Priority Points Enhancement, 2019	Tokenization

IBM Mobile Identity

- Cloud-based cryptographic framework for:
    - issuing, managing, and verifying digital identity credentials
- Collection of encrypted identity traits represented by secure tokens
- What exactly is a crypto-blob?
- Provides institutions with the ability to create and manage access

Lenel Onguard and BlueDiamond Readers

- Cloud-access, browser-based alarm and cardholder management
- Integrated with IBM Mobile Identity through embedded SDK
- Hardware/software solution for institutional access management

Agile Development Model

- Welcome change
- Working software over documentation
- Business and developer cooperation
- Motivated individuals → successful projects
- Face-to-face conversations
- Sustainable development
- Team feedback
- Final scrum

Requirements

Marist Joint Study

- Implement Issuer Server
- Create Ubuntu server
- Establish Docker environment
- Install IBM Onboarding package

IBM Industry Platforms

- Provide application design and implementation
- Provide onboarding kit to Joint Study
- Provide cloud server resources as necessary

Lenel/OSI

- Provide SDK
- Install BlueDiamond readers
- Integrate Lenel Onguard with Marist/IBM Mobile Identity Applications

Design Objectives

Joint Study

- Issuer server installed and tested to be able to issue identity document
- User identity documents and profiles

IBM

- Receive document requests from Marist Issuer Server
- Encrypt credentials
- Submit triggerable identity traits through Lenel API

Lenel

- Provide SDK/API for interface with IBM application and BT readers

OSI

- Provide intermediate control panel connection for, BT conversion

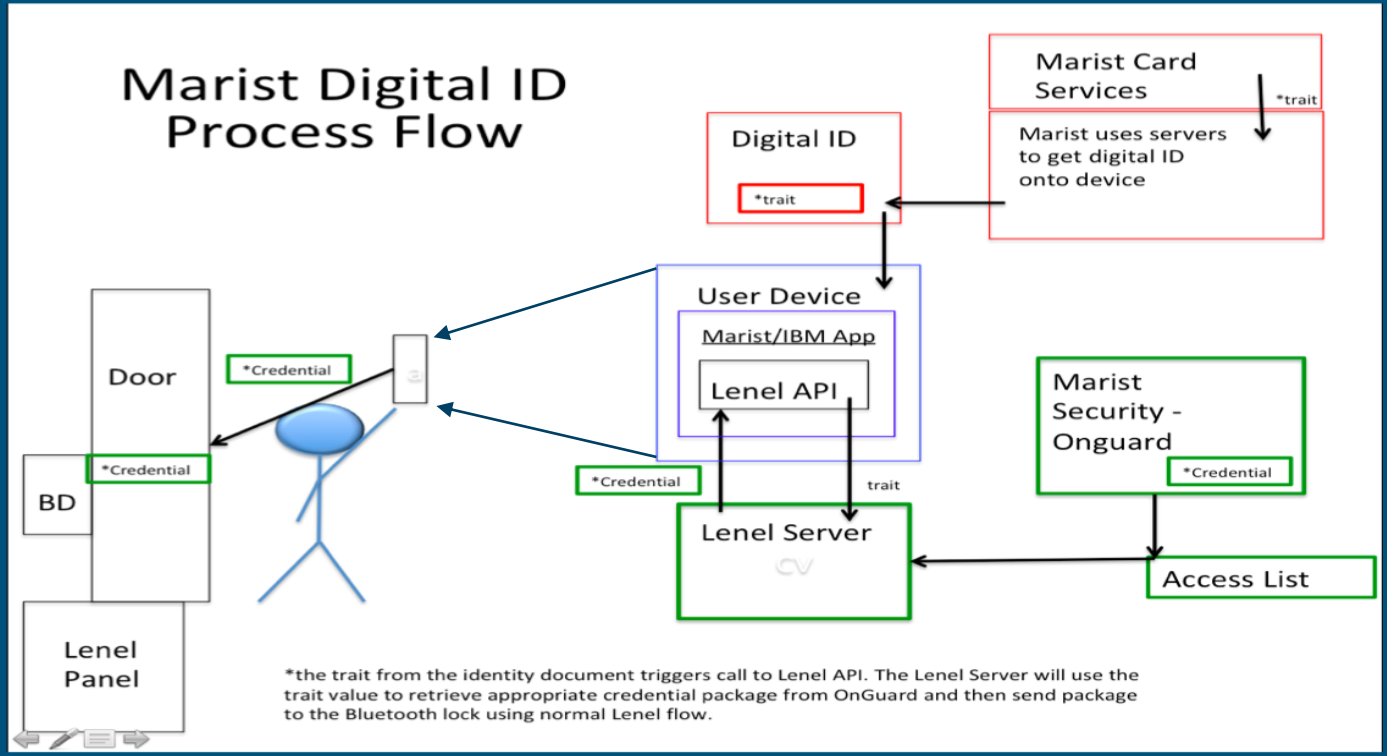
Design Challenges

- Ability to issue, change, and revoke credentials
- Lost phone
  - how to ensure only one set of credentials per user
- Stolen phone
  - how to ensure credentials revoked upon reporting
- Loss of power
  - how to ensure access to controlled spaces in the event of a power outage

Considerations

Milestone Planning Team Identification Artifact Creation	Weekly Phone Conference Local Coordination	Non-disclosure agreement Participant Communication Hardware Installation	Procedure Development Testing Program Feedback and Lessons Learned	Next Phase

Process Flow Artifact



Implementation

Week 1

- Monday
  - Verify legal complete
  - Sandbox setup
  - IBM access API
  - Phone call
    - Aaron, Chris, Greg
- Tuesday
  - IBM dev
- Wednesday
  - Installation
  - Name, email of all participants
  - IBM dev
- Thursday
  - Pete Wenzel on sandbox setup
  - IBM dev
- Friday
  - IBM dev
  - Sandbox setup complete
  - Danny verify setup on all participants phones
    - Document setup procedure
  - Phone Conference

Week 2

- Monday
  - IBM dev
- Tuesday
  - Chris and Danny run sandbox
  - IBM dev
- Wednesday
  - Chris and Danny run sandbox
  - IBM dev
- Thursday
  - Chris and Danny run sandbox
  - IBM dev
- Friday
  - IBM dev
  - Phone Conference

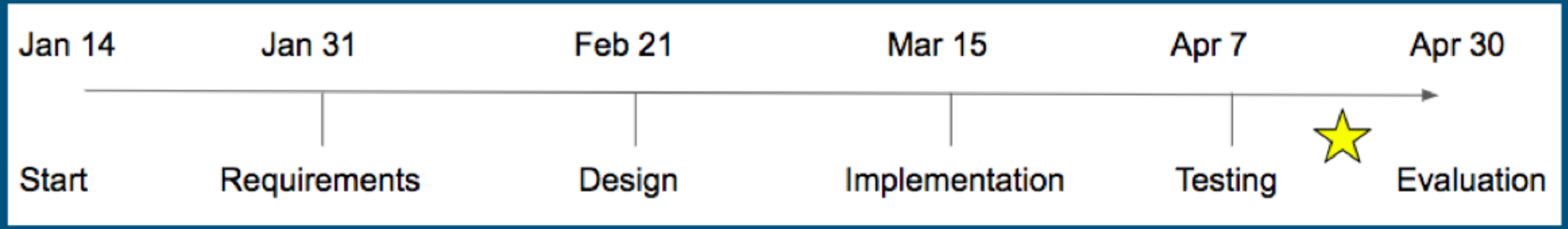
Week 3

- Monday
  - Locks installed and tested
- Tuesday
  - Connection test w/ sandbox
- Wednesday
  - Connection test w/ sandbox
- Thursday
  - Connection test w/ sandbox
- Friday
  - Phone conference

Week 4

- Monday
  - System test
    - Danny and Chris
- Tuesday
  - System test
    - Danny and Chris
- Wednesday
  - Participant test
- Thursday
  - Participant test
- Friday
  - Delivery

Timeline Artifact



Risks

Assumed

- Completion
- Continuity
- Integration

Managed/Mitigated

- Momentum
- Partner Interest
- Legal

Present

- Hardware Integration
- Testing

Testing

Demo

- 20 Participants
- Integration
- 1 Access Point

Test Plan

- Issue
- Change
- Revoke

Overall Benefits

- One Time Software Installation
- Cost Effective
- Secure Credential Exchange
- Versatility

Future Development - Identity Verification

Extends the proof of concept offered in Facility Access phase to Marist College campus

Robust enough to support verification with or without WiFi connectivity

Clear benefits to campus security personnel and administration

Identity Verification - Requirements

- Loss of phone
- Loss of power
- Robust and flexible
- Quick updates to access lis

Identity Verification - Design

- Extend current capability

Priority Points Use Case

Points issued to students for use in housing selection

Points are aggregate value based on GPA, club participation, and Marist-sanctioned events

Tokenization of points would allow Marist to incentivize behavior and extend benefits to more of the student community

Priority Points Implementation

- Blockchain technologies will enable implementation of a Digital Identity and a Marist Token System that would enhance the current Priority Point System.
- Securly keep track of student information and point statistics
- Incentivize students that are and are not affected by campus housing
- Tokenized Priority Points provides versatility of each point value.

Questions?