Implementation of Technology Solution Task 1

Name

Western Governors University

**Table of Contents**

Cover Page ………………………………………………………………………………..1

Table of Contents………………………………………………………………………….2

1. Internal Communication Artifact……………………………………………………...3
2. Fact Sheet Artifact…………………………………………………………………….5
3. Writing Analysis for Each Artifact……………………………………………………6
   1. Planning……………………………………………………………………….6
   2. Drafting……………………………………………………………………….6
   3. Revising………………………………………………………………………7
4. Audience Analysis for Each Artifact………………………………………………..7
5. Internal Communication Artifact

NanoTech, USA

**Memo**

|  |  |
| --- | --- |
| To: | CEO; CFO; CIO |
| From: | Michael Robinson |
| Date: | November 26, 2019 |
| Re: | Implementation of Single Sign-On with Smart Card Technology |
|  |  |

The growth of our company and our work force going more mobile, security of our assets is becoming more of a priority than in the past. With this growing concern, it is time that we implement a Single Sign-On technology using PKI (public key infrastructure) Smart Cards. The smart cards will be utilizing technologies already available on the laptops of our work force in the form of a smart card reader. Combining the already encrypted hard drives on the laptops with the smart cards utilizing certificate-based technology to sign into the laptop it will add an additional layer of security to ensure minimal loss of our secure corporate information.

With the implementation of the PKI cards, security certificates, and single sign-on methodologies there will be significant return on investment in the form of reduced labor costs, increased data security, and efficiency increases in the on-boarding and off-boarding of employees.

The cost effectiveness to corporate and benefits to the end-user are outlined below:

* Benefits to corporate and end users:
  + Secure authentication via pin number created by the end user and does not need to be reset as often by the end user
  + Removes the need for multiple passwords to access the different platforms and applications
  + Increased laptop security by allowing sign in without the card, and immediately logged out when the card is removed
* CEO; CFO; CIO Page2 November 26, 2019
  + All access is terminated for the assigned card if lost or stolen
  + Can dual purpose as corporate id card
  + Dual factor authentication into corporate portals and VPN
* Cost reductions to corporate:
  + Reduced calls to service desk for password resets
  + Increased staff productivity and efficiency
  + Lowered call volume from password resets will reduce the call center staff
  + Increased efficiency in new hire on-boarding process
  + Off boarding efficiency increased by turning off PKI card
* Implementation of the technology:
  + Install PKI server authentication software and certificate manager
  + All portals converted to use PKI certificate authentication
  + A selected group of beta testers will be used to gage end user acceptance
  + All end users trained on use of PKI technologies
  + All end users will be issued a PKI card and a certificate from the certificate server
  + All laptops converted to use PKI certificates for login
  + Install PKI certificates for login to end user laptops and validate access

1. Fact Sheet Artifact

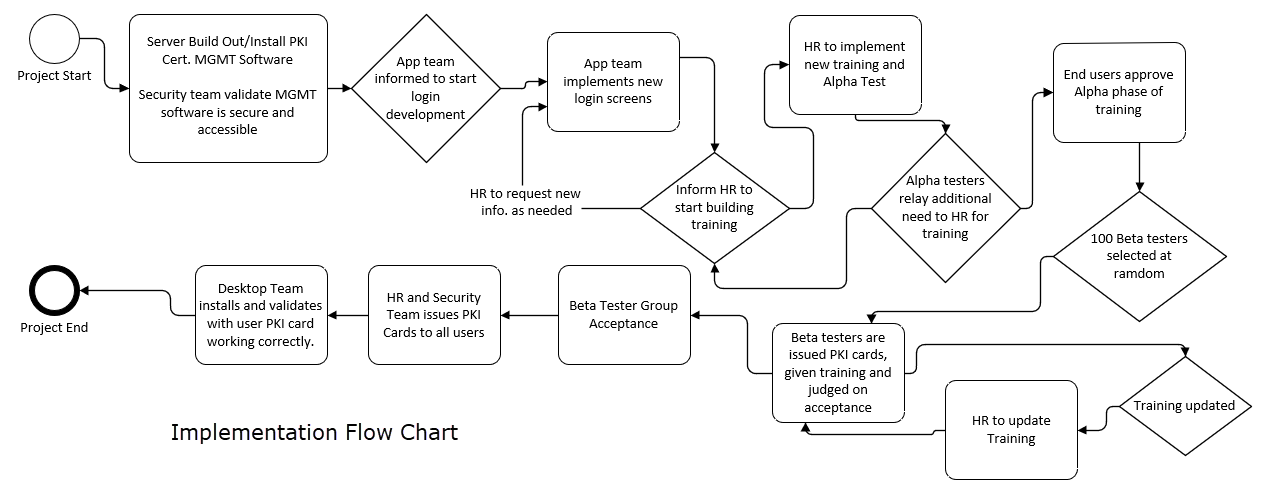
**Description**

The smart card is a technology used to authenticate users to computer systems and applications. The technology combines both physical hardware and network-based software. The physical hardware is in the form of two parts: the PKI Smart Card used by the end user and the server housing the certificate management software. The software aspect of the technology is the virtual certificate itself used by the PKI card and the authentication software on the server used to validate the certificate.

The hardware and software work in conjunction to increase the security and end user ease of access to authorized systems and applications. The security comes in the form of the certificate that must be valid on the authentication server, and the ease of end user use comes from only having to remember your pin instead of various passwords for the different systems.

**Implementation Rationale**

The rationale behind implementing this is multi-fold. With the work force increasingly moving to laptops and gaining the ability to work remotely there is a need for increased security of company assets.



With the smart card technology in place security of the company assets comes to the forefront. The smart card will not only be required to login the mobile laptop, it will also be required to access an array of internal company applications and VPN.

The security will also be increased as the smart card will be required for VPN access and internal network shares. If the smart card is removed from the laptop the end user laptop will immediately lock.

The implementation will also have a cost reduction to the company by reducing calls to the service desk for password resets, reduced staffing needs on the service desk and add efficiency to the work force by reducing the time needed to on-board and off-board employees.

**Implementation Phases**

Phase 1:

The server and securities teams will setup and install the PKI authentication server. HR will begin to design the training material of the technology.

Phase 2:

The applications development team will develop the authentication portal logins to accept both passwords and PKI credentials. The password option will remain until full go live of the new PKI technology. Applications development team will work with HR to ensure the training correctly conveys the process to use the PKI cards.

Phase 3:

This is the beta phase of 100 end users to test the new login process and test for user acceptance. This group will also assist HR in finalizing the training for the new process and address issues in the training to resolve any questions in the process.

Phase 4:

All end users will be required to take a training course on the new process and system used for accessing laptops and company assets

Phase 5:

HR and the security teams will work in conjunction to issue new PKI cards to all end users. Security will assign each end user their PKI card and HR will swap out their PKI card for their current corporate ID card

Phase 6:

This will occur in conjunction with phase 5 as each end user is issued their PKI/Corporate ID card the desktop support team will install the PKI card certificates needed, setup the laptop to use the PKI card and certificate as login credentials, have the end user create their 8 digit pin and desktop support will the validate that the end user is able to login correctly to all assets needed to perform job functions.

C. Writing Analysis for Each Artifact

I. Planning

In the planning phase for the internal communication artifact, I first looked at who my audience was and being the CEO, CFO and CIO I needed to convey the company need, a cost savings and the benefit to the company. In looking at this I was then able to convey why the company would need this new technology to help secure the company assets while in the hands of a mobile work force. Since any new technology implemented into a company will almost always have an upfront cost that will impede the implementation from an executive, I needed to show and explain how this cost will in turn be a long run cost savings to the company. Then I continued to explain how and why the end user would be more willing to accept the solution as it would increase their ease of use of their computer and ease access to company assets.

When writing the fact sheet artifact, I needed to take a more technical aspect to the artifact as the given audience would be the technical IT teams implementing the solution, HR assisting in the training of the new technology and ultimately the end users using the technology. For the IT teams speaking technically to them is straight forward and you only need to give them a break down of the phases of operation. For HR, I explained that their role in creating the training documentation they will need to work with several IT technical teams to ensure that the training material is correct and covers what the end user will need to be able to use this technology. The end users are also referenced in this artifact as they are going to be the primary users of the technology, so their feedback is greatly needed in the beta testing of implementation. They help is needed to ensure that the training meets the needs to address issues and questions with the technology and the beta testing of a large group of end users allows for a good judge of user acceptance.

II. Drafting

When drafting the internal communication memo, I needed to ensure that I would address the concerns and questions that would potentially arise from the executives. With them being charged with the financial impact of the new solution and any security concerns they may have I needed to ensure that I addressed those equally. Since the new technology will cost the company upfront monetary loss, I took the approach to address the financial and security concerns together. Financially there will be a loss to implement the new technology but the cost to implement the solution is offset by the improved security, reduction is work force costs, and the improved efficiency gain by several different work force groups by implementing the solution.

When drafting the fact sheet artifact for HR, the IT technical teams, and end users I took a more forward approach of just the fact about the solution. For the IT teams I broke down what will be implemented, how it will be implemented, and at what phases the different IT teams will be engaged. For HR the approach was much the same since they are charged with training the employees on the new technology and assisting in guiding user acceptance. For the end users, I felt it was important to include them in several steps of implementing the new technology as they will be the users utilizing the new technology the most. Helping them feel empowered in the implementation process of the new technology should help gain user acceptance.

III. Revisioning

When revising the internal communication memo, I needed to ensure that the language used was appropriate for the target audience since they are not as technically inclined at the technical teams I needed to ensure that they understand the technology and the terms used to reference the new technology. I also needed to ensure that I addressed their financial and security concerns as implementing any new technology will have a cost and they will want to be assured that their will be a return on their investment. They will also want to be reassured that the investment will result in end user acceptance of this technology.

When revising the fact sheet memo, I needed to ensure that all groups needed in the implementation were addressed, the terminology used when referencing each group was with in acceptable norms for that group, and that it properly conveyed the phases in the correct order for a successful implementation and user acceptance. While revising I continually asked if the terminology and language used is appreciate for the target group of this step or phase. I included a timeline for these groups this will help facilitate when the different phases start and stop to assist in ensuring a seamless transition into the new technology.

D. Audience Analysis for Each Artifact

* 1. Internal Communication Memo

The primary group for this artifact is the CEO, CFO and CIO. The executive team has some technical knowledge being a manufacturer company and they use technology in the day to day activities of work but are primarily focused on the running on the company and ensuring the company maintains profit.

* The subject knowledge for the new technology is not strong for the executive team as a whole and this adjusted how I presented the information to this team. I needed to ensure that the message of improved security and cost effectiveness of the technology would be a good move for the company.
* The CEO having a minimal technical background is not fully versed in all technical aspects of the technology being implemented and in addressing this I gave the core benefits of the technology to be implemented.
* The CFO also having minimal a minimal technical background I again limited the technical aspect to the core benefits to the company with the added expression of the cost savings to the company.
* The CIO having the most technical background I included more technical information on how the technology is to be implemented in the company and the benefits to the concerns he would have with security and ease of use for the end users.
  1. Fact Sheet Artifact

The primary groups for this artifact are the IT teams implementing the solution, HR training on the solution, and the end users using and accepting the solution. Their technical background in the solution ranges from limited to expert. This creates a unique way that the information is to be disseminated as you need to ensure that each group is addressed correctly, and the information conveyed is on a proper level for that group.

* IT teams implementing the solution are experts in their specific area of the project. This team needs the least amount of technical explaining on the solution as they have the strongest technical background of all groups for this solution.
* HR teams have a strong background in training but minimal to intermediate knowledge in technology. This group although experts in creating training need to rely on the IT teams to ensure that the training conveys the correct information and in knowing this their aspects in the fact sheet are limited to creating the training and communicating with both the IT teams and end users to ensure training is covering the topic adequately.
* The end users, the group that will be using the new technology the most, has the least technical knowledge of all the groups. When addressing them in the fact sheet their role is to work with HR to ensure the training material covers the use and facts around the technology. This group is also the strongest factor in regards to the acceptance of the new technology and the gauge of the overall success of the implementation.

References

Akamai. (2015). *Smart Card and Client Certificate Authentication for Web-Enabled Applications* [PDF file]. Retrieved from <https://www.akamai.com/us/en/multimedia/documents/white-paper/smart-card-and-client-certificate-authentication-for-web-applications-white-paper.pdf>

CardLogix. (2009). *Smart Card and Security Basics* [PDF file]. Retrieved from <http://www.smartcardbasics.com/pdf/7100030_BKL_Smart-Card-&-Security-Basics.pdf>

Kiran, S., Lareau, P., & Lloyd, S. (2002, November). *PKI Basics - A Technical Perspective* [PDF file]. Retrieved from <http://www.oasis-pki.org/pdfs/PKI_Basics-A_technical_perspective.pdf>

Wilson, S. (2005, June 28). *Guidelines on how to determine Return on Investment in PKI* [PDF file]. Retrieved from <http://www.oasis-pki.org/whitepaper/roi.pdf>