UNIVERSITÉ
Concordia
UNIVERSITY

Concordia Institute for Information System Engineering
(CIISE)

Concordia University

INSE 6150 – Security Methodology Evaluations

Assignment -1:

Submitted to:

Professor Jeremy Clark

Submitted By:

Nithish Reddy Yalaka - 40164619

Systems:

Vaccine Passports Recently, Quebec has introduced a system for residents to prove they have been adequately vaccinated against COVID19. Consider a few possible designs for a vaccine passport system used by a customer at a restaurant.

The Quebec System: the Quebec government issues a digital message with: (1) a name, (2) a birthdate, and (3) indication of a fully vaccinated status. This message is signed with the government of Quebec's public key. The signed message is encoded into a QR code which can be displayed on paper or in a smartphone app by the customer, along with a piece of photo ID. The restaurant checks with the assistance of an smartphone app: (1) the photo on the ID matches the person, (2) the name/birthdate on the ID matches the QR code, (3) the QR code indicates the vaccination status, and (4) the QR code contains a digital signature by the Quebec government.

A Physical Card System: the Quebec government will take a photograph and issue a physical card (like a driver's license or health card) with a name, photo, and vaccination status on it. It will be mailed to people vaccinated in Quebec. A customer displays this card to the restaurant. The restaurant checks (1) the photo on the card matches the person, and (2) the card displays the vaccination status.

An Online System: the Quebec government gives each vaccinated person a unique identity number encoded into a QR code which can be displayed on paper or in a smartphone app by the customer. The restaurant scans the code from the back of the card with a smartphone app from the Quebec government that queries a server run by the Quebec government using HTTPS. The server responds with the customer's name, ID, address, photograph, and confirmation of their vaccination status. The restaurant checks with the assistance of an smartphone app: (1) the photo matches the person, and (2) the app displays the vaccination status.

(Question 1)

STRIDE

STRIDE is a Dive in and Threat Model and stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

It is also known as Model of Threats used to help reason and find threats to a system.

Spoofing:

Bob
Security Specialist

Spoofing:

Spoofing is impersonating something or someone else. It violates the Authentication Property.

Quebec System:

As the verification is with QR code, QR can be easily spoofed with various mobile applications by modifying the location parameters in the JSON file which acts as the input for validation and creation of QR. With Cryptography and changing the values of the keys, it is possible to achieve spoofing in this system.

Physical Card System:

This system can be spoofed very easily by modifying or generating the dummy cards as the authorities cannot verify them in any database for validating the information.

Online System:

This system can be easily spoofed by modifying the details in the database by any security experts or hackers instantly by homographic exploits . Eg: Mission Impossible

Tampering:

Bob
Security Specialist

Tampering:

Tampering is modifying the data or code from its original nature. It violates the Integrity Property.

Quebec System:

For so long, we thought it is not easy to process and deploy the malicious code into the source code for QR Code, but not so long ago, Przemek Jaroszewski, the head of Poland's CERT, has done this and tried it on various European airports.

Physical Card System:

The Physical proof card can be tampered by creating a false ID that will look relevant to the original one using a printing press.

Online System:

This system can be easily tampered by modifying the data while authorities wait for the response from the server through sniffing or MoM attacks.

Repudiation:

Repudiation:

Repudiation is claiming to have not performed an action.
It violates the Non-RepudiationProperty.

Quebec System:

Once the system is compromised with Tampering and spoofing, the hackers would've easily entered into the system with all the accesses and it wouldn't be hard for them to delete their logs or cover their tracks or without leaving any digital fingerprint. Quebec System admins wouldn't even understand this until if something goes bad.

Physical Card System:

In the physical system, it's not possible to do the repudiation as it is physical presence of the person.

Online System:

Similar to the Quebec system, it is possible to cover the system logs and no one will notice anything until if something actually bad happens in the system or security audit occurs.

Information Disclosure:

Information Disclosure:

Information Disclosure is exposing the information to someone who is not authorised to see it. It violates the Confidentiality Property.

Quebec System:

All the information of the QR is tokenised into the JSON formats which are key-value pairs where you can easily see the complete information which was present in the passport like name, family name and DOB and visa status. This information is violated confidential property as now all those details are exposed

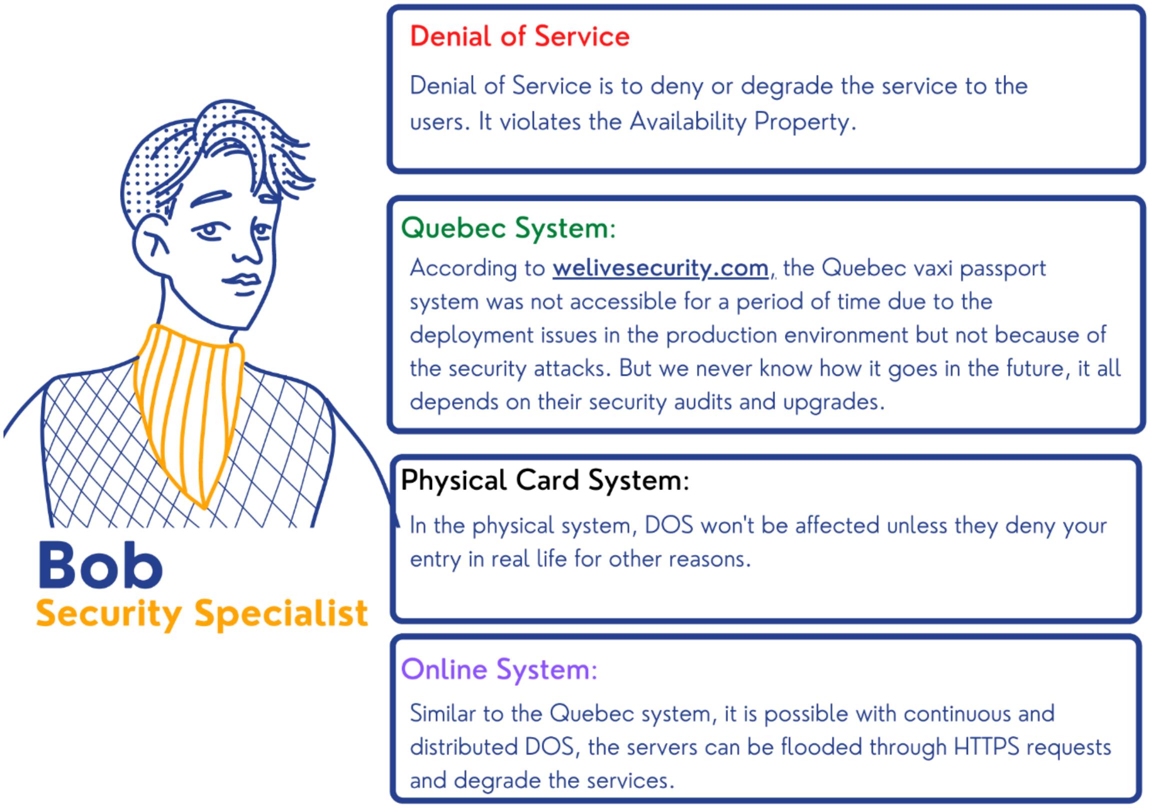
Physical Card System:

In the physical system, it's not possible to do the Information disclosure as it is most likely to have the basic details.

Online System:

Similar to the Quebec system, it is possible for the exposure of confidential information as the customer data can be sniffed easily if the channel is not securely kept .

Denial of Service:


Bob
Security Specialist

Denial of Service

Denial of Service is to deny or degrade the service to the users. It violates the Availability Property.

Quebec System:

According to **welivesecurity.com**, the Quebec vaxi passport system was not accessible for a period of time due to the deployment issues in the production environment but not because of the security attacks. But we never know how it goes in the future, it all depends on their security audits and upgrades.

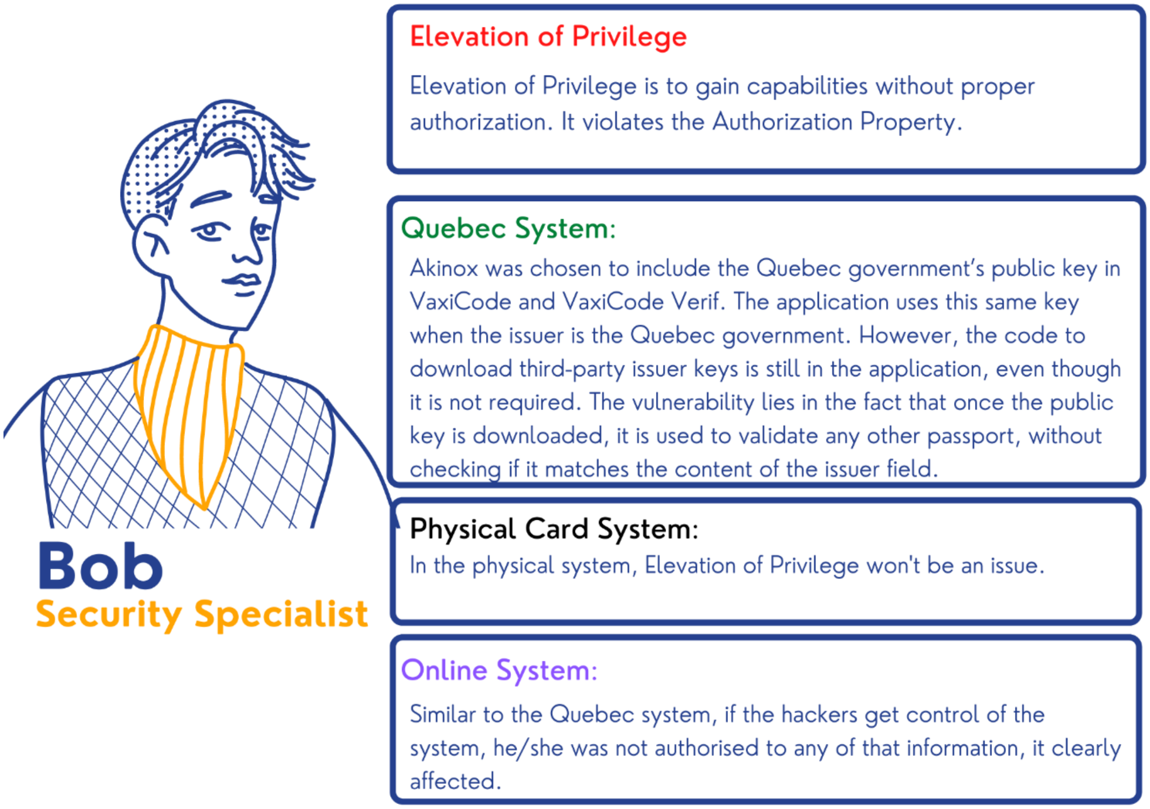
Physical Card System:

In the physical system, DOS won't be affected unless they deny your entry in real life for other reasons.

Online System:

Similar to the Quebec system, it is possible with continuous and distributed DOS, the servers can be flooded through HTTPS requests and degrade the services.

Elevation of Privilege:


Bob
Security Specialist

Elevation of Privilege

Elevation of Privilege is to gain capabilities without proper authorization. It violates the Authorization Property.

Quebec System:

Akinox was chosen to include the Quebec government's public key in VaxiCode and VaxiCode Verif. The application uses this same key when the issuer is the Quebec government. However, the code to download third-party issuer keys is still in the application, even though it is not required. The vulnerability lies in the fact that once the public key is downloaded, it is used to validate any other passport, without checking if it matches the content of the issuer field.

Physical Card System:

In the physical system, Elevation of Privilege won't be an issue.

Online System:

Similar to the Quebec system, if the hackers get control of the system, he/she was not authorised to any of that information, it clearly affected.

(Question 2)

Security Evaluation Criteria:

It is the comparison between the alternatives. Here there are no solutions, only the tradeoffs.

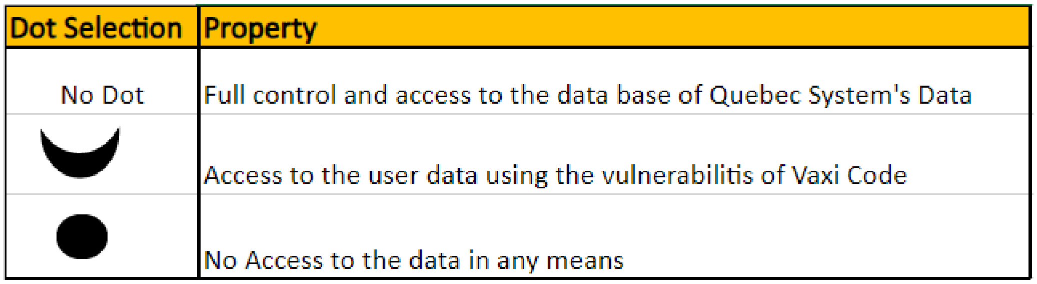
The deliverable is a simple chart , coming up with the criteria is harder than it seems.

Usually, there is more to security than the actual security(security, usability, deploy ability).

UDS Framework.

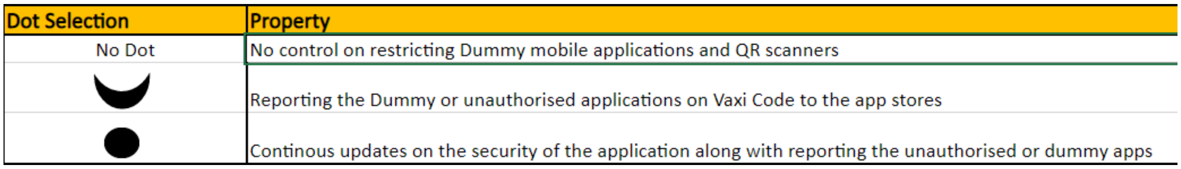
6 Security Evaluation Criteria:

S1:Resilient to Physical Theft



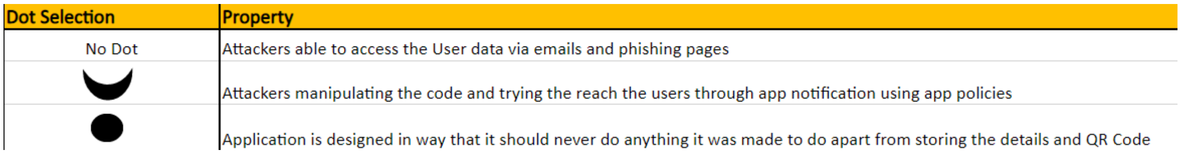
Dot Selection	Property
No Dot	Full control and access to the data base of Quebec System's Data
◡	Access to the user data using the vulnerabilitis of Vaxi Code
●	No Access to the data in any means

S2: Resilient to Spoofing



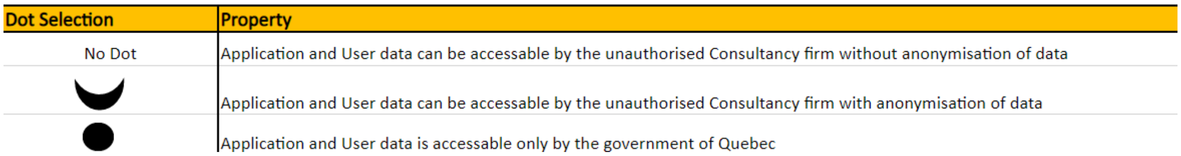
Dot Selection	Property
No Dot	No control on restricting Dummy mobile applications and QR scanners
◡	Reporting the Dummy or unauthorised applications on Vaxi Code to the app stores
●	Continous updates on the security of the application along with reporting the unauthorised or dummy apps

S3: Resilient to Phishing:



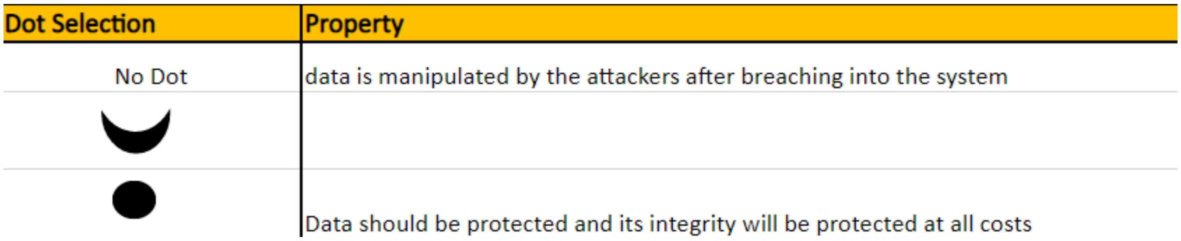
Dot Selection	Property
No Dot	Attackers able to access the User data via emails and phishing pages
◡	Attackers manipulating the code and trying the reach the users through app notification using app policies
●	Application is designed in way that it should never do anything it was made to do apart from storing the details and QR Code

S4: Resilient to Elevation of Privilege



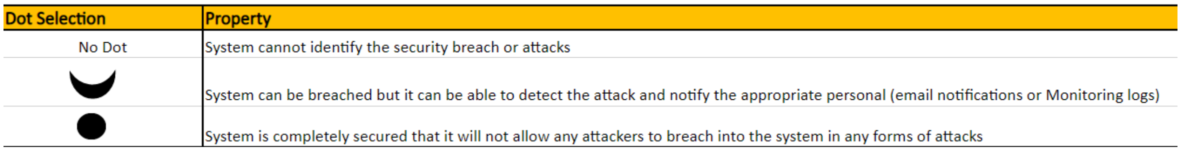
Dot Selection	Property
No Dot	Application and User data can be accessable by the unauthorised Consultancy firm without anonymisation of data
◡	Application and User data can be accessable by the unauthorised Consultancy firm with anonymisation of data
●	Application and User data is accessable only by the government of Quebec

S5: Resilient to Tampering



Dot Selection	Property
No Dot	data is manipulated by the attackers after breaching into the system
◒	
●	Data should be protected and its integrity will be protected at all costs

S6: Resilient to Identify the Threats

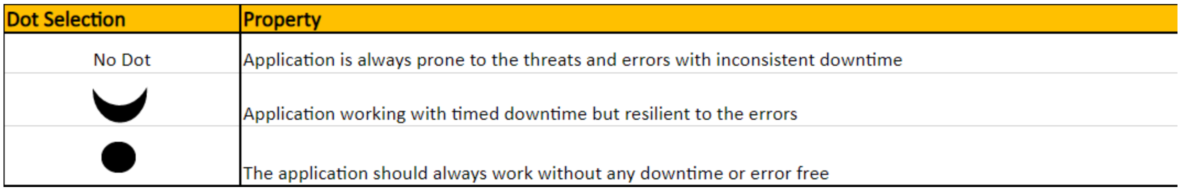


Dot Selection	Property
No Dot	System cannot identify the security breach or attacks
◒	System can be breached but it can be able to detect the attack and notify the appropriate personal (email notifications or Monitoring logs)
●	System is completely secured that it will not allow any attackers to breach into the system in any forms of attacks

(Question 3)

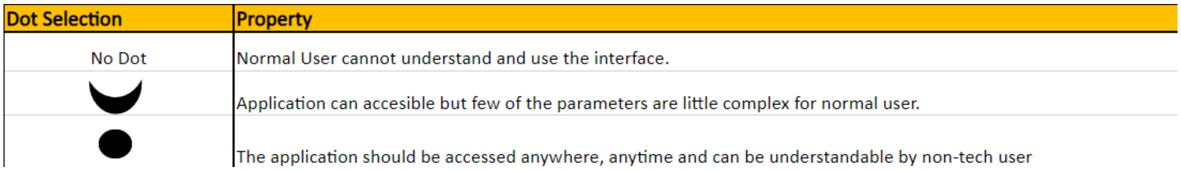
6 Usability Evaluation Criteria:

U1: Error Free



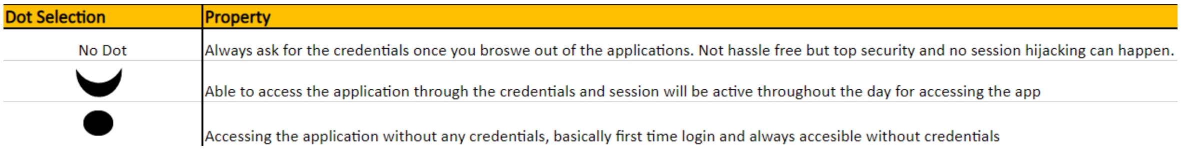
Dot Selection	Property
No Dot	Application is always prone to the threats and errors with inconsistent downtime
◒	Application working with timed downtime but resilient to the errors
●	The application should always work without any downtime or error free

U2: Efficient to Access



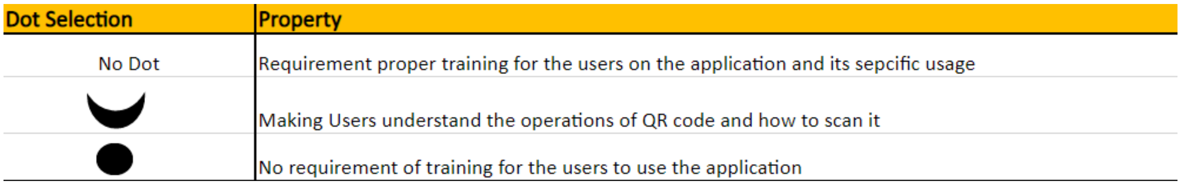
Dot Selection	Property
No Dot	Normal User cannot understand and use the interface.
◒	Application can accesible but few of the parameters are little complex for normal user.
●	The application should be accessed anywhere, anytime and can be understandable by non-tech user

U3: No Password Requirement



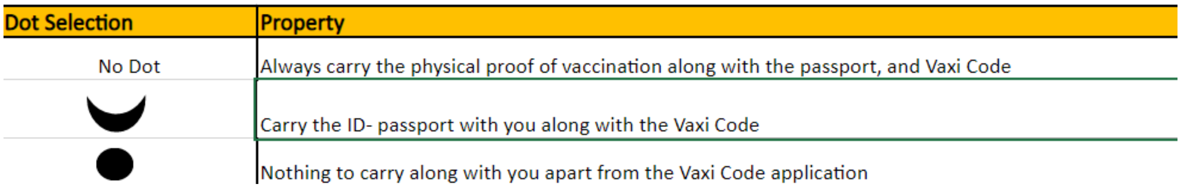
Dot Selection	Property
No Dot	Always ask for the credentials once you broswe out of the applications. Not hassle free but top security and no session hijacking can happen.
◒	Able to access the application through the credentials and session will be active throughout the day for accessing the app
●	Accessing the application without any credentials, basically first time login and always accesible without credentials

U4: Ease of Use for Users



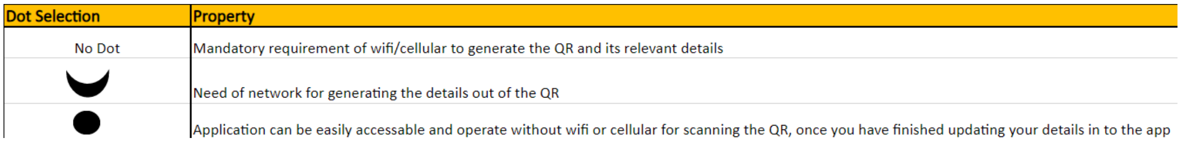
Dot Selection	Property
No Dot	Requirement proper training for the users on the application and its sepcific usage
◡	Making Users understand the operations of QR code and how to scan it
●	No requirement of training for the users to use the application

U5: Nothing to Carry



Dot Selection	Property
No Dot	Always carry the physical proof of vaccination along with the passport, and Vaxi Code
◡	Carry the ID- passport with you along with the Vaxi Code
●	Nothing to carry along with you apart from the Vaxi Code application

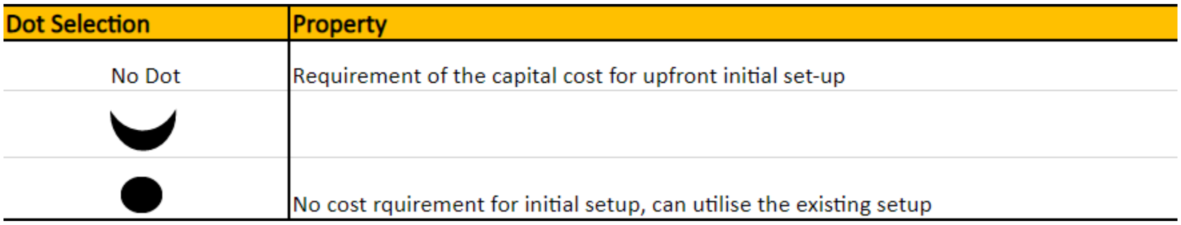
U6: No Dependency on the Internet



Dot Selection	Property
No Dot	Mandatory requirement of wifi/cellular to generate the QR and its relevant details
◡	Need of network for generating the details out of the QR
●	Application can be easily accessable and operate without wifi or cellular for scanning the QR, once you have finished updating your details in to the app

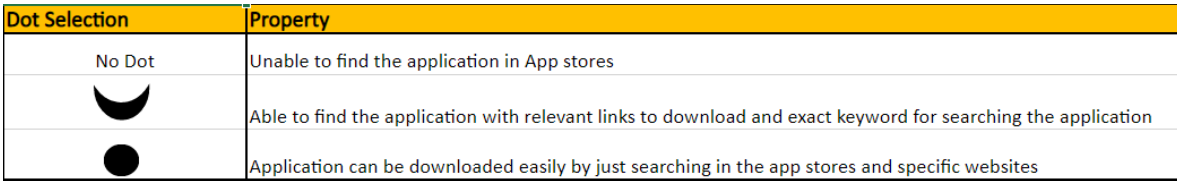
6 Deployability Evaluation Criteria:

D1: Negligible Cost/Cost Effectiveness



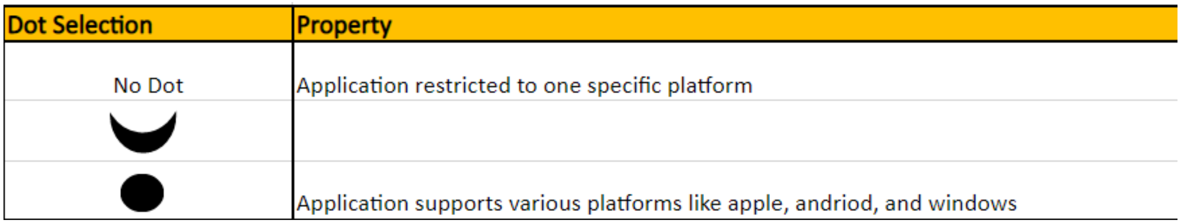
Dot Selection	Property
No Dot	Requirement of the capital cost for upfront initial set-up
◡	
●	No cost rquirement for initial setup, can utilise the existing setup

D2: Ease of Application Download



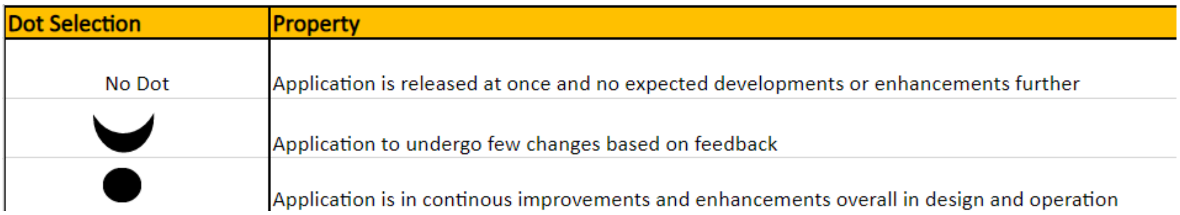
Dot Selection	Property
No Dot	Unable to find the application in App stores
◡	Able to find the application with relevant links to download and exact keyword for searching the application
●	Application can be downloaded easily by just searching in the app stores and specific websites

D3: Cross-Platform Support



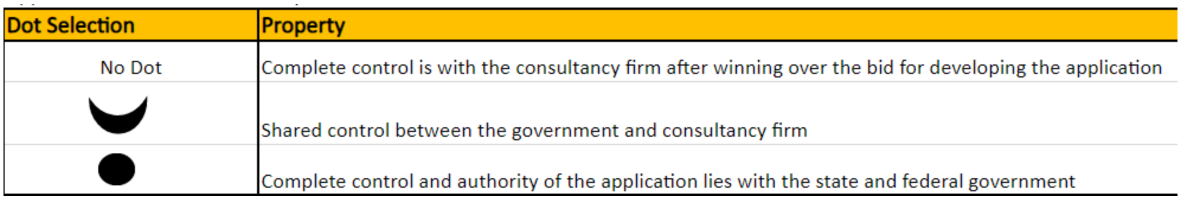
Dot Selection	Property
No Dot	Application restricted to one specific platform
◡	
●	Application supports various platforms like apple, andriod, and windows

D4: Continuous Product Improvements



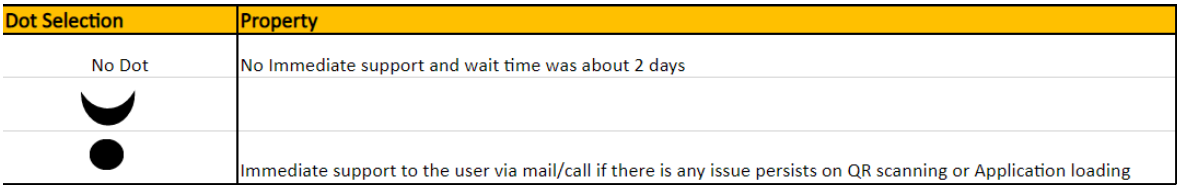
Dot Selection	Property
No Dot	Application is released at once and no expected developments or enhancements further
◡	Application to undergo few changes based on feedback
●	Application is in continous improvements and enhancements overall in design and operation

D5: Application Control and Authority



Dot Selection	Property
No Dot	Complete control is with the consultancy firm after winning over the bid for developing the application
◡	Shared control between the government and consultancy firm
●	Complete control and authority of the application lies with the state and federal government

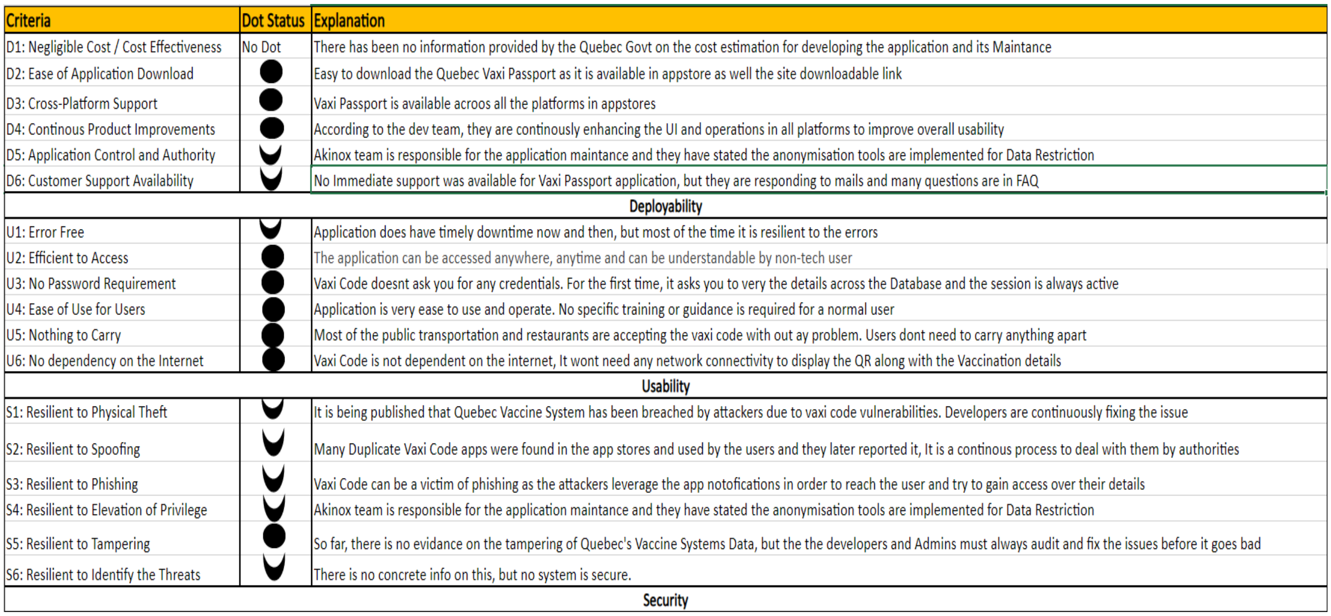
D6: Customer Support Availability



Dot Selection	Property
No Dot	No Immediate support and wait time was about 2 days
◡	
●	Immediate support to the user via mail/call if there is any issue persists on QR scanning or Application loading

(Question 4)

Evaluation of Quebec System:



Criteria	Dot Status	Explanation
D1: Negligible Cost / Cost Effectiveness	No Dot	There has been no information provided by the Quebec Govt on the cost estimation for developing the application and its Maintance
D2: Ease of Application Download	●	Easy to download the Quebec Vaxi Passport as it is available in appstore as well the site downloadable link
D3: Cross-Platform Support	●	Vaxi Passport is available acroos all the platforms in appstores
D4: Continous Product Improvements	●	According to the dev team, they are continously enhancing the UI and operations in all platforms to improve overall usability
D5: Application Control and Authority	◡	Akinox team is responsible for the application maintance and they have stated the anonymisation tools are implemented for Data Restriction
D6: Customer Support Availability	◡	No Immediate support was available for Vaxi Passport application, but they are responding to mails and many questions are in FAQ
Deployability		
U1: Error Free	◡	Application does have timely downtime now and then, but most of the time it is resilient to the errors
U2: Efficient to Access	●	The application can be accessed anywhere, anytime and can be understandable by non-tech user
U3: No Password Requirement	●	Vaxi Code doesnt ask you for any credentials. For the first time, it asks you to very the details across the Database and the session is always active
U4: Ease of Use for Users	●	Application is very ease to use and operate. No specific training or guidance is required for a normal user
U5: Nothing to Carry	●	Most of the public transportation and restaurants are accepting the vaxi code with out ay problem. Users dont need to carry anything apart
U6: No dependency on the Internet	●	Vaxi Code is not dependent on the internet, It wont need any network connectivity to display the QR along with the Vaccination details
Usability		
S1: Resilient to Physical Theft	◡	It is being published that Quebec Vaccine System has been breached by attackers due to vaxi code vulnerabilities. Developers are continuously fixing the issue
S2: Resilient to Spoofing	◡	Many Duplicate Vaxi Code apps were found in the app stores and used by the users and they later reported it, It is a continous process to deal with them by authorities
S3: Resilient to Phishing	◡	Vaxi Code can be a victim of phishing as the attackers leverage the app notofications in order to reach the user and try to gain access over their details
S4: Resilient to Elevation of Privilege	◡	Akinox team is responsible for the application maintance and they have stated the anonymisation tools are implemented for Data Restriction
S5: Resilient to Tampering	●	So far, there is no evidance on the tampering of Quebec's Vaccine Systems Data, but the the developers and Admins must always audit and fix the issues before it goes bad
S6: Resilient to Identify the Threats	◡	There is no concrete info on this, but no system is secure.
Security		

If the Image is not properly Visible, please find the link for the above sheet below:

https://liveconcordia-my.sharepoint.com/:x:/g/personal/n_yalaka_live_concordia_ca/Eew-py-alfhBlPuS1s873-cBPs0wnXnrZVBJVQzQxrik4A?e=qul2Me