Threat Modeling Report

Created on 11/13/2023 7:38:05 PM

Threat Model Name: Traveler-Verifier DFD

Owner: Cole Nardini

Reviewer:

Contributors:

Description: Cardea Mobile Agent is a phone app intended for end-users of Cardea. The app is like a digital wallet that holds legal and medical information of the user. The app's data store is the smartphone itself. All data saved by the app is stored on the phone itself; not external servers. The traveler is the end-user. They interact with Cardea Mobile Agent as an app on their phone. The Verifier user initiates the verification process by sending a communications request by way of QR code to the mobile agent. The mobile agent creates a secure direct channel and passes along it's credentials. The credentials are then passed to HyperLedger Indy Network and the Machine Governance for verification.

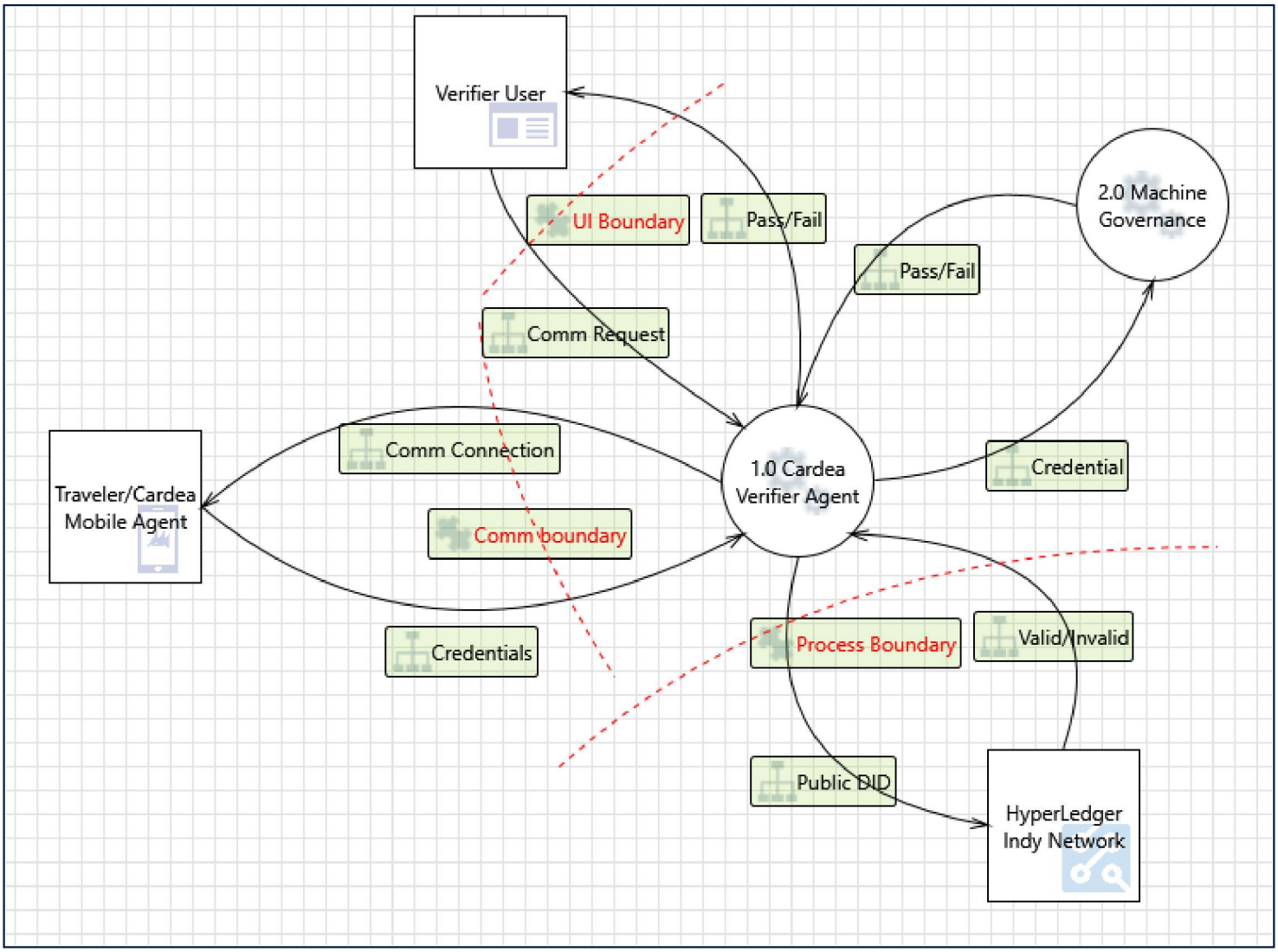
Assumptions: There are two other external entities of Cardea Mobile Agent: a Health Agent and a government enterprise agent. The Health Agent is better described in Logan and Daniel's diagram. The government enterprise agent is only used on the Aruba version of Cardea. Aruba is a pacafic island with a different legal jurisdiction that allows this external interactor. The Cardea team does not expect this entity to apply on a larger scale. In a level 2 DFD then this entity would be included. But it was decided that a level 1 DFD conveyed adequate information on threats for the system-of-interest.

External Dependencies: Cardea Mobile Agent is run on end-user smartphones. As such, the performance of the agent depends on the various software and hardware configurations of smartphones. For instance, a smartphone OS may prevent Cardea Mobile Agent from saving files, causing a DoS for the app. It also depends on the upkeep of the HyperLedger Indy Network for reliability and security purposes.

Threat Model Summary:

Not Started	0
Not Applicable	4
Needs Investigation	2
Mitigation Implemented	1
Total	7
Total Migrated	0

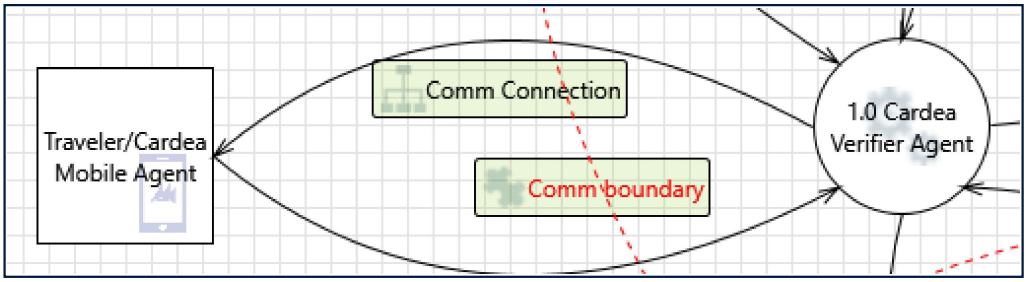
Diagram: Traveler-Verifier DFD



Traveler-Verifier DFD Diagram Summary:

Not Started	0
Not Applicable	4
Needs Investigation	2
Mitigation Implemented	1
Total	7
Total Migrated	0

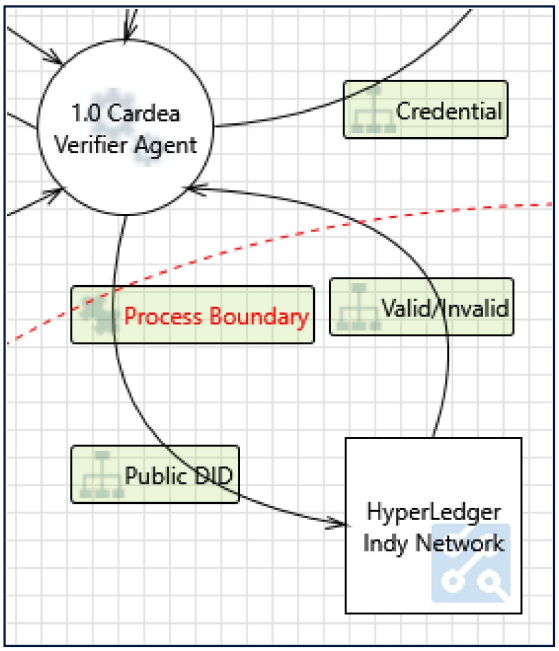
Interaction: Comm Connection



1. If a mobile device containing cached customer data in the CRM Mobile Client is lost the data could be disclosed if the device is not secured [State: Not Applicable] [Priority: Low]

Category:	Information Disclosure
Description:	If a mobile device containing cached customer data in the CRM Mobile Client is lost the data could be disclosed if the device is not secured
Justification:	The QR code sent to make the Comm Connection is not a data transfer and is not meant to be lost. It is only used for communication purposes.
Possible Mitigation(s):	Ensure a device management policy is in place that requires a use PIN and allows remote wiping. Refer: https://aka.ms/tmtcrypto#pin-remote
SDL Phase:	Design

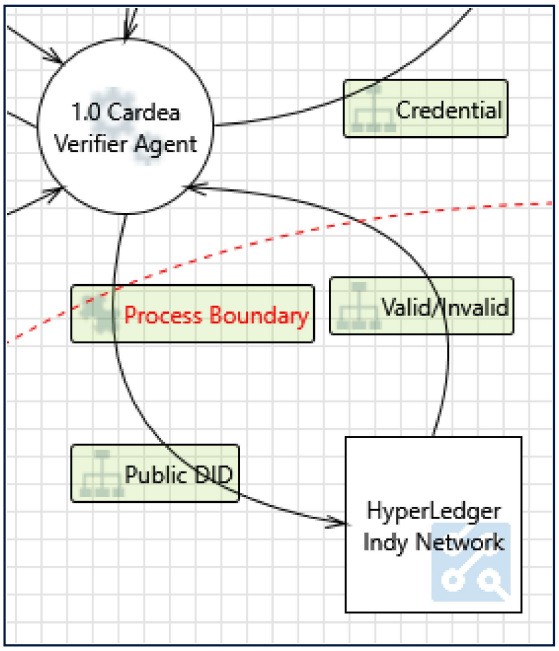
Interaction: Public DID



2. An adversary may execute unknown code on HyperLedger Indy Network [State: Not Applicable] [Priority: Low]

Category:	Tampering
Description:	An adversary may launch malicious code into HyperLedger Indy Network and execute it
Justification:	This is an outgoing transmission from the domain scope. The Verifier Agent should be in control of what goes out
Possible Mitigation(s):	Ensure that unknown code cannot execute on devices. Refer: https://aka.ms/tmtconfigmgmt#unknown-exe
SDL Phase:	Design

Interaction: Valid/Invalid



3. An adversary may tamper the OS of a device and launch offline attacks [State: Not Applicable] [Priority: High]

Category:	Tampering
Description:	An adversary may launch offline attacks made by disabling or circumventing the installed operating system, or made by physically separating the storage media from the device in order to attack the data separately.
Justification:	This isn't really an IoT Device, there just didn't seem to be a good way of describing the blockchain as an external entity.
Possible Mitigation(s):	Encrypt OS and additional partitions of IoT Device with Bitlocker. Refer: https://aka.ms/tmtconfigmgmt#partition-iot
SDL Phase:	Design

4. An adversary may tamper HyperLedger Indy Network and extract cryptographic key material from it [State: Needs Investigation] [Priority: High]

Category:	Tampering
Description:	An adversary may partially or wholly replace the software running on 1.0 Cardea Verifier Agent, potentially allowing the replaced software to leverage the genuine identity of the device if the key material or the cryptographic facilities holding key materials were available to the illicit program. For example an attacker may leverage extracted key material to intercept and suppress data from the device on the communication path and replace it with false data that is authenticated with the stolen key material.
Justification:	The public DID and issued credential could be used if stolen.

Possible Mitigation(s):	Store Cryptographic Keys securely on IoT Device. Refer: https://aka.ms/tmtcrypto#keys-iot
SDL Phase:	Design

5. An adversary may exploit known vulnerabilities in unpatched devices [State: Not Applicable] [Priority: High]

Category:	Tampering
Description:	An adversary may leverage known vulnerabilities and exploit a device if the firmware of the device is not updated
Justification:	Patched firmware is beyond the scope of this application.
Possible Mitigation(s):	Ensure that the Cloud Gateway implements a process to keep the connected devices firmware up to date. Refer: https://aka.ms/tmtconfigmgmt#cloud-firmware
SDL Phase:	Design

6. An adversary may exploit unused services or features in 1.0 Cardea Verifier Agent [State: Needs Investigation] [Priority: Medium]

Category:	Elevation of Privileges
Description:	An adversary may use unused features or services on 1.0 Cardea Verifier Agent such as UI, USB port etc. Unused features increase the attack surface and serve as additional entry points for the adversary
Justification:	I am unsure of what unused code may be in the codebase to be taken advantage of.
Possible Mitigation(s):	Ensure that only the minimum services/features are enabled on devices. Refer: https://aka.ms/tmtconfigmgmt#min-enable
SDL Phase:	Implementation

7. An adversary may gain unauthorized access to privileged features on HyperLedger Indy Network [State: Mitigation Implemented] [Priority: Low]

Category:	Elevation of Privileges
Description:	An adversary may get access to admin interface or privileged services like WiFi, SSH, File shares, FTP etc., on a device
Justification:	This should be a simple true/false. There is not a need for raised privileges.
Possible Mitigation(s):	Ensure that all admin interfaces are secured with strong credentials. Refer: https://aka.ms/tmtconfigmgmt#admin-strong
SDL Phase:	Implementation