Document Purpose: Analyze security requirements of all Matter-Compatible Devices and how they will affect the Door Face Panel System. While Matter can be a smart device standard that would allow devices from different vendors to work together it will also bring some security limitations which will be shown in this document

Overview of Matter Security:

- Device Identity: Each of the Matter Devices will have a unique digital certificate to show it is a legitimate device
- Encrypted Communications: Matter will use encryption so that when data is sent between devices it will not able to be easily intercepted or read
- Secure Updates: All of the software updates have to be verified and signed to make sure there is no malicious software being installed

Matter Security Mapping:

- **Edge Layer**
  - Encrypts data before sending it to other components in the system
  - runs the Matter protocol using Wifi
  - will use secure boot to ensure only trusted software runs

- **Gateway Layer**
  - Will manage the device onboarding and authentication
  - validates the device certificate
  - applying security measures such as firewalls

- **Cloud Layer**
  - stores the encryption keys
  - manages the software updates
  - manages system logs for monitoring and auditing system activity

Security Limitations:

- Limited Security Customization
  - The device uses a rigid, standard security model that limits customization and modification

Vendor and Firmware Limitations

Not all vendors fully support Matter, and some devices require firmware updates or proprietary software.

- Inconsistent security support across vendors may increase system risk.

Mitigation:

Require minimum security and firmware standards

Review vendor documentation before integration

Limit early deployment to trusted and well-supported devices

Final Conclusion:

Matter provides a security foundation for smart device inter-connectioms but it also has limitations that have to be looked at more in depth to make sure it is the right fit