Technical Disclosure Commons

November 2019

Network-connected Locker Kiosk for Device Delivery

Anonymous

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Network-connected Locker Kiosk for Device Delivery

ABSTRACT

Many organizations provide devices to various users. The issuance and tracking of such devices can impose a burden on the organization's information technology group. Further, users may not be able to obtain devices on-demand due to manual processes to issue or return devices. This disclosure provides a smart, network-connected locker kiosk that can identify and authenticate users to issue devices or accept device returns.

KEYWORDS

- Kiosk
- Smart locker
- Device issuance
- Prototype devices
- Information security

BACKGROUND

Many organizations provide devices such as mobile phones, tablets, laptops, etc. to employees, contractors, and others. Assigning a device to a particular individual as well as removing the assignment are typical manual processes. Further, when devices are left on premise, e.g., at the office, there is no systematic solution to ensure the security of such devices. This poses an information security risk to the organization.

DESCRIPTION

This disclosure provides a smart, network-connected locker kiosk that can identify and authenticate users to issue devices or accept device returns.
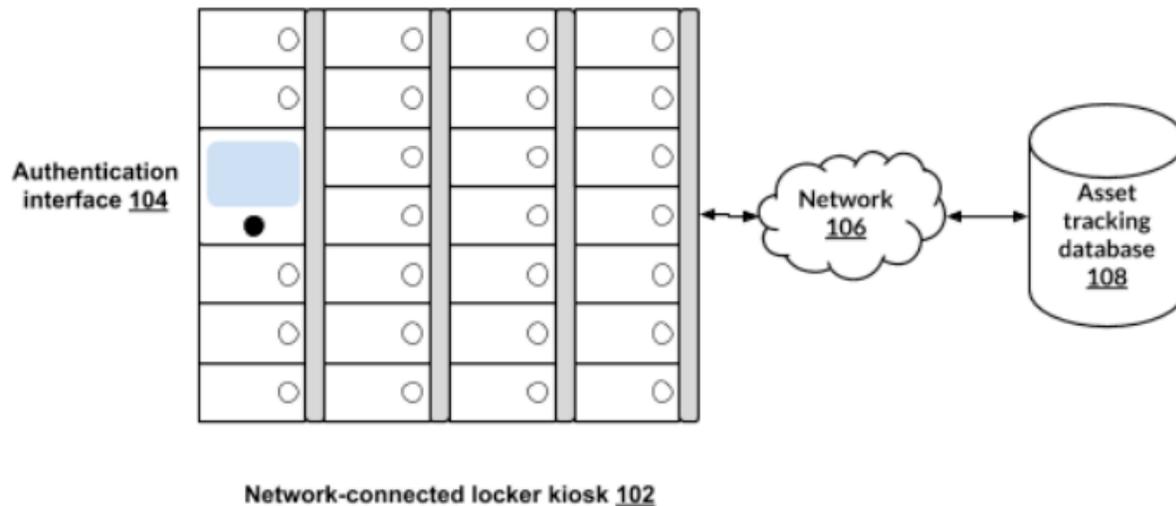
Fig. 1: Network-connected locker kiosk

Fig. 1 illustrates a network-connected locker kiosk. The kiosk (102) includes a configurable set of lockers, as shown in Fig. 1. For example, the number of lockers as well as the type/ size of lockers can be chosen based on the planned use of the locker kiosk. The kiosk can be used to store devices and is configured to communicate over a network (106), e.g., an internal network of an organization, such that the kiosk is not reachable over the internet. The network is secure and controlled by the organization.

Authorized users, e.g., employees, contractors, interns, etc. can approach the lockers, identify and authenticate themselves, e.g., via a badge, using an authentication interface (104) provided at the locker kiosk. Once the user is authenticated, the user can pick up or drop off a device. The lockers provide an interface to request and receive any type of device, e.g., test devices, device prototypes, laboratory equipment, etc. The lockers are also integrated with an asset tracking database (108) that stores information regarding devices and the users that picked up/ dropped of each device at the kiosk.

Providing such kiosks at various locations within the organization's offices can reduce the lead time for a user to obtain a device. Since devices are issued upon secure authentication and the asset tracking database is linked to the lockers, issued devices can be tracked systematically and the issuance of the device is compliant with organizational security policies.

The kiosk can be used to provide loaner laptops or other devices in any setting. The kiosk can also be used for virtual laptop/mobile device imaging. Use of the lockers to deliver prototype devices can improve security and supply chain efficiency.

Providing kiosks at different physical locations within the organization's offices can reduce the number of trips users make to the organization's information technology group and can also reduce tickets/requests for devices that the group needs to process. The kiosk also enables employees and others to store devices on-site in a secure manner.

The network connected kiosk solution, as described herein, can also be deployed outside of an organization for external users to pick-up/drop-off items over a secure network connection while maintaining anonymity. An end-to-end solution, e.g., provided via a mobile phone app, can allow external users to easily pick up or drop off items per their convenience.

CONCLUSION

This disclosure provides a smart, network-connected locker kiosk that can identify and authenticate users to issue devices or accept device returns.