June 2020

Secure Authentication and Provisioning of Hardware Devices

Anonymous

Secure Authentication and Provisioning of Hardware Devices

ABSTRACT

Computing devices such as wearable devices are often used on enterprise settings. Customers benefit from secure purchase, provisioning, and management of devices. This disclosure describes secure mechanisms to track device purchases, to authenticate devices as genuine and in possession of a customer, and to provide tools that enable customers to manage their devices. Per the described techniques, each manufactured device is provisioned with a unique serial number and a key. Devices that are sold to an end customer (e.g., through a distributor) are authenticated using the serial number and the key. A database is maintained that records device status for each manufactured device, where devices that are not associated with a particular customer are marked as pending devices.

KEYWORDS

- Device provisioning
- Device authentication
- Device management
- Device setup
- Genuine device
- Enterprise device

BACKGROUND

Many organizations purchase devices of various types, e.g., smartphones, wearable devices, augmented reality devices, etc. Often, such devices include consumer-class devices that are configured for use in the enterprise. Organizations can use device management software for various purposes such as issuing devices to users, configuring devices in accordance with organizational policies, maintaining device configuration, etc. In some instances, organizations provision devices with organization-specific confidential information or software applications.

DESCRIPTION

It is valuable to have secure mechanisms to track device purchases, to authenticate devices as genuine and in possession of a customer, and to provide tools that enable customers to manage their devices. This disclosure describes a process that provides such features, as described in detail below.

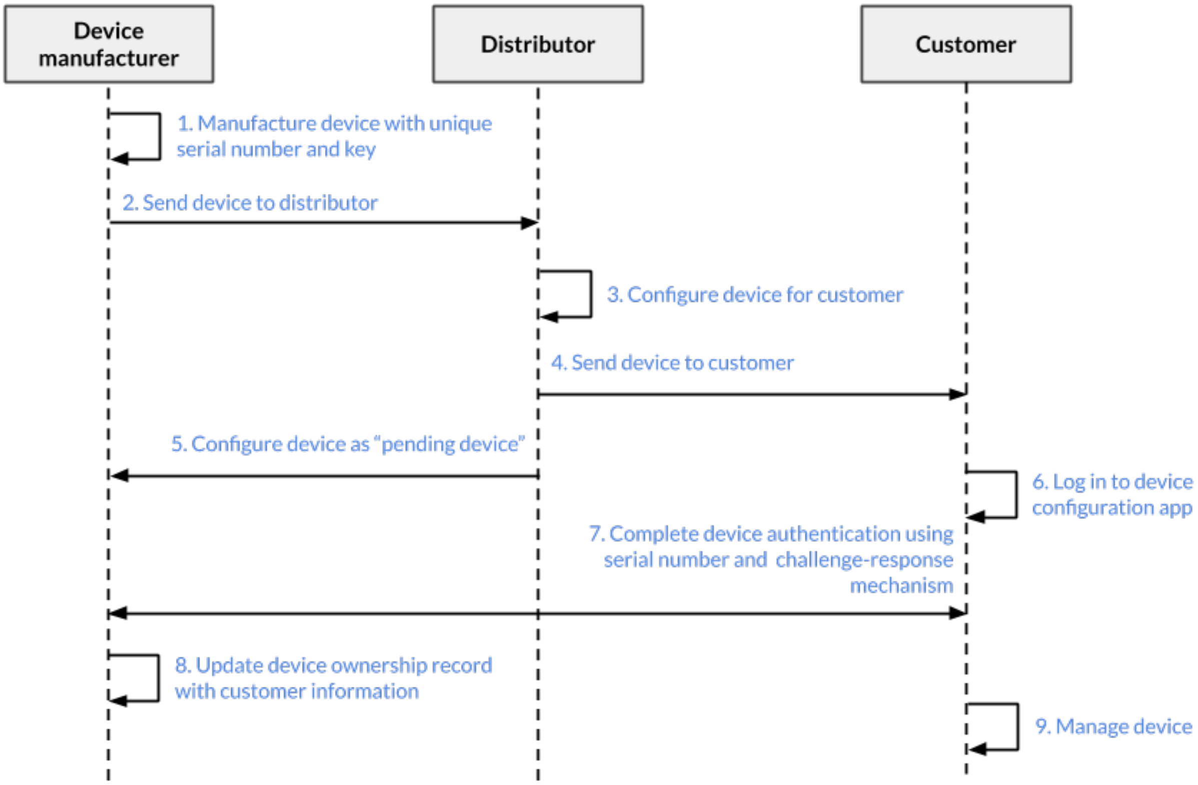
Device manufacturer
Distributor
Customer
1. Manufacture device with unique serial number and key
2. Send device to distributor
3. Configure device for customer
4. Send device to customer
5. Configure device as "pending device"
6. Log in to device configuration app
7. Complete device authentication using serial number and challenge-response mechanism
8. Update device ownership record with customer information
9. Manage device

Fig. 1: Secure device authentication and provisioning

Fig. 1 illustrates an example process to securely provision computing devices that are used in an enterprise setting. For example, such devices can include augmented reality devices. As illustrated in Fig. 1, a device manufacturer manufactures (1) each device with a unique serial number and with a device-specific encryption key that are stored securely on the device, e.g., in a permanent memory of the device. The manufacturer ships (2) the device to various distributors that then handle the sales to different customers.

Distributors are provided with tools that enable them to configure the device for specific orders (3) by entering order details for various customers. For each order, the distributor includes the serial numbers of the specific devices that are part of that order in the order details. The tool is configured to prevent the use of the same device (serial number) in multiple orders. Order data is shared with the manufacturer (not shown), who can map the order to the customer account.

Once the order details have been entered, the distributor ships the devices (4) that are part of the order to a customer, e.g., an enterprise customer. The status of the device is marked as a "pending device" by the manufacturer (5), e.g., by storing a database record for each device that is manufactured, based on the device serial number. The pending device status indicates that the device has been sold to a particular customer, as specified in the order details but has not yet been authenticated and provisioned for use. The pending device status allows the manufacturer to track a device prior to the device being connected to the Internet, e.g., from the factory till a customer activation of the device.

Upon receipt of the device, the customer logs into a device configuration application (6). For example, the customer can log in with their customer account with the device manufacturer that is associated with their orders stored by the manufacturer. The customer can use the application to initiate a device authentication process (7) with the manufacturer.

For example, in the device authentication process, the manufacturer can issue a request to the device, e.g. to sign a challenge. The device generates a response to the challenge by signing the challenge using its device-specific key to generate a response. If the manufacturer is able to match the signed response, the device is determined to be authentic and in possession of the customer associated with the customer account. The challenge-response can be implemented via network communication over the Internet. The mechanism ensures that the customer has physical possession of the device and that the device is genuine.

The manufacturer then updates (8) the device ownership record with the customer information and the device status is changed from pending to active. The customer can then actively manage the device (9), e.g., to add apps to the device, to apply customer-specific settings, to configure or perform a remote wipe on the device, etc. For example, customer specific settings that can be configured can include selecting specific apps to be active on the device, user-specific settings, disabling certain features, etc. Device management can also include viewing device status, grouping devices, etc.

The ownership information associating the device with the particular customer is maintained even if the customer performs a factory reset or returns the device to the manufacturer.

The manufacturer can also provide a device management tool to the customer. For example, the tool can include a device administration portal that can be used to manage all devices that are associated with the customer account.

The process described with reference to Fig. 1 provides a secure mechanism to authenticate a customer as the owner of a particular device and to securely transfer device ownership from a device distributor to a customer. The techniques of provisioning devices with serial numbers and device-specific keys, maintaining a database of pending devices, authenticating devices over the Internet, and enabling customers to manage their devices using a device management tool enables the manufacturer to ensure that there is no accidental onboarding of a device, e.g., a device sold to one customer being inadvertently activated by another customer. This is ensured since each device is assigned a unique serial number and a database is maintained that maps each device to a particular customer.

Further, the described techniques enable provisioning devices in enterprise mode, e.g., to store organization specific, confidential information on the device. Since no device can be associated with the enterprise without passing the challenge, security of such information is maintained. The described techniques also enable locking devices in case of unauthorized access. The described techniques can support multiple different types of devices.

CONCLUSION

This disclosure describes secure mechanisms to track purchases of computing devices, to authenticate devices as genuine and in possession of a customer, and to provide tools that enable customers to manage their devices. Per the described techniques, each manufactured device is provisioned with a unique serial number and a key. Devices that are sold to an end customer (e.g., through a distributor) are authenticated using the serial number and the key. A database is maintained that records device status for each manufactured device, where devices that are not associated with a particular customer are marked as pending devices.