smartlox

A Digital Lockout-Tagout System

A white paper on the use of electronic lockout devices and software-based Lockout-Tagout systems in the control of hazardous energy sources.

SL-WP-3-02-V2
February 2026

This white paper discusses the use of electronic lockout devices and software-based Lockout-Tagout systems in controlling hazardous energy sources during the servicing and maintenance of machines and equipment. In such situations, the unexpected energization or startup of machines or equipment, or the release of stored energy, could cause injury to employees.

The aim is to introduce operators, safety managers, and business owners to the benefits of Digital Lockout-Tagout systems while addressing common concerns and questions.

smartlox

1 Background

Controlling hazardous energy sources through the application of Lockout-Tagout is a critical function for many industrial, mining, and manufacturing businesses. It is paramount in protecting workers from serious injury or death.

Traditional Lockout and Tagout practices have not changed greatly since regulatory standards were adopted in the 1980's; however, the scope and complexity of lockout activities have continued to increase, resulting in service and maintenance procedures that can be:

- Time-consuming and inefficient to operate when large numbers of workers are involved,
- Error-prone and inaccurate when manually written records are used,
- Costly to operate when keys or locks are misplaced, or when locks must be cut,
- Challenging for management to control or oversee, and
- Potentially unstable over time.

Advances in cloud computing and low-power wireless technologies, together with the significant growth of smartphones and smart devices in the workplace, have created new opportunities for businesses to achieve levels of automation, control, and monitoring that were not possible 10 years ago.

Digital Lockout-Tagout systems are designed to strengthen existing safety management protocols by utilizing modern technologies to provide an integrated software and hardware system that brings new levels of efficiency, accountability, and visibility to the lockout process.

Benefits of Digital Lockout-Tagout systems include:

- Enhanced accountability by ensuring that all participants in the process are individually identified and their activities are electronically recorded.
- Greater flexibility by allowing some traditional Lockout-Tagout activities to be performed better to match the service and maintenance needs of the business.
- Improved visibility and control of lockout activities across workgroups by providing all participants with the latest up-to-date information to ensure coordination of safety activities.
- Reduced costs by dramatically improving setup time in large or complex group lockouts, reducing the overall number of locks and group lockout hardware, and eliminating the need to cut or replace locks.

2 The Digital Lockout-Tagout System

2.1 Overview

Digital Lockout-Tagout systems typically comprise four major components: the electronic lockout device, a smartphone or tablet device, a SmartTag, and various cloud-based software services.

The following figure shows a simplified overview of the Digital Lockout-Tagout system and the interconnection between the different components.

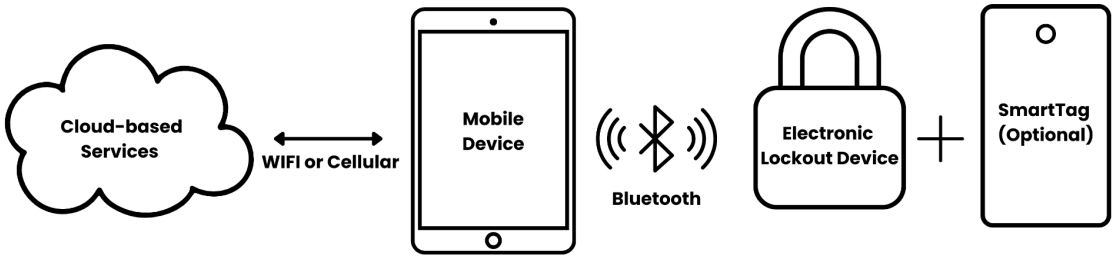

Figure 1: System Architecture and Connectivity — An overview showing how Cloud-based services communicate with Mobile Devices via Wi-Fi/Cellular, while Mobile Devices connect to electronic lockout devices via Bluetooth and have the option to attach a SmartTag for identification purposes.

The mobile device communicates wirelessly with the electronic lockout device (typically over Bluetooth) and communicates with the cloud-based services over Wi-Fi or Cellular data networks. An optional SmartTag, typically including a QR code, allows users to scan to retrieve information about the lockout.

2.2 Physical Components

The physical components of a Digital Lockout-Tagout system typically are:

- A machine, or equipment, requiring isolation for service and/or maintenance.

- An energy isolating device that prevents the unexpected energization or startup of the machines or equipment, or the release of stored energy, could cause injury to employees.
- An electronic lockout device is an electronic padlock used by an authorized employee to lock out a machine's energy isolating device.
- A smartphone or tablet device that runs the digital lockout application used by all employees involved in the lockout process.
- A SmartTag with a QR code that can be scanned by mobile devices to identify who is locked on, when they locked on, and what machine they are locked on to.

2.3 Software Components

The software-based components of a Digital Lockout-Tagout system typically are:

- A Digital Lockout Application that is the user interface to the Digital Lockout-Tagout System used by all employees involved in the lockout process.
- A cloud service that provides the digital keys, virtual lockboxes, and virtual personal locks.
- A digital key is used to open the electronic lockout device.
- A virtual lockbox is a software version of a physical lockbox; it performs the same function as a physical lockbox and contains the digital key required to open the corresponding electronic lockout device.
- A virtual personal lock is a software version of a physical personal lockout lock that can be applied to a virtual lockbox.

2.4 Persons Involved

Typical persons involved in a Digital Lockout-Tagout system include:

- An authorized employee is responsible for applying and removing the electronic lockout device from the machine's energy isolating device.
- A non-authorized employee who is assigned to the service and/or maintenance of the machine but is not responsible for applying or

removing the electronic lockout device from the machine's energy isolating device.

2.5 Digital Key

Each electronic lockout device has a matching encrypted digital key that is securely stored in the cloud service and can be downloaded to the Digital Lockout application to open the corresponding Electronic Lockout Device.

2.6 Electronic Lockout Device

An electronic lockout device is typically a battery-powered Bluetooth Padlock specifically designed for Digital LOTO. The electronic lockout device performs the same function as a traditional lockout device. Still, instead of using a physical key, it uses a digital key that is communicated to the device over Bluetooth from the user's smartphone.

2.7 Virtual Personal Lock

A virtual personal lock is a software version of a physical personal lockout lock. A virtual personal lock performs the same function as a physical lock, and one or more virtual personal locks can be applied to a virtual lockbox.

Each virtual personal lock is associated with an individually authenticated user of the system (the owner), and the identity of that user is attached to the virtual personal lock.

Only the virtual personal lock owner can open or close their corresponding virtual personal locks.

2.8 Virtual Lockbox

A virtual lockbox is a software version of a physical lockbox. A virtual lockbox performs the same function as a physical lockbox in a group lockout activity, but

exists in the cloud service and is accessible to the smartphone app via the internet.

A virtual lockbox can contain none, one, or more digital keys, and each virtual lockbox can have none, one, or more virtual personal locks attached.

A virtual lockbox is ‘open’ when no virtual personal locks are attached. When the virtual lockbox is ‘open’, the contained digital keys can be used to apply and/or remove the corresponding electronic lockout device using the mobile application.

A virtual lockbox is ‘closed’ when one or more virtual personal locks are attached. When the virtual lockbox is ‘closed,’ the contained digital keys cannot be accessed or used, and the corresponding electronic lockout device cannot be opened by any mobile application.

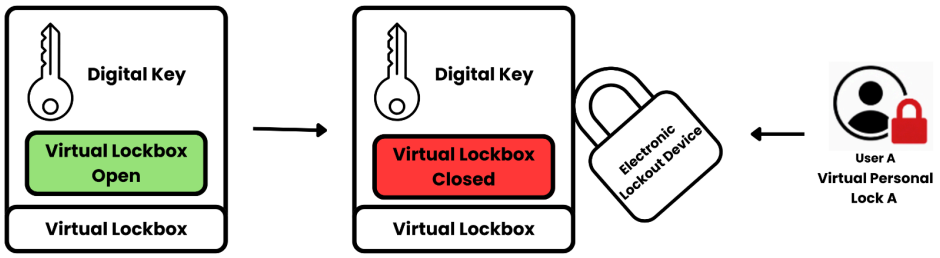

Figure 2: The Virtual Lockbox Mechanism — Visualizing the transition of a Virtual Lockbox from an "Open" state (containing an accessible Digital Key) to a "Closed" state once a user (User A) applies their Virtual Personal Lock.

smartlox

3 An Example Digital Lockout-Tagout Procedure

The following procedure is an example of a typical electronic group lockout procedure involving a single authorized employee and a single non-authorized employee working as a group in the service or maintenance of a machine under the following conditions:

- The single authorized employee shall assume the overall responsibility for the control of hazardous energy for all members of the group while the servicing or maintenance work is in progress.
- The machine has a single energy isolating device that requires a single electronic lockout device.
- All lockout participants are using their personal smartphone devices, have the digital lockout application installed and running, have signed into the mobile application, and have been assigned the correct permissions.

3.1 Notification and shutdown

The authorized employee notifies unauthorized employees and shuts down the machine.

3.2 Isolation and verification

The authorized employee applies the electronic lockout device to the machine's energy isolation device as follows:

1. The authorized employee opens the mobile app and verifies their identity.
2. The authorized employee activates the electronic lockout device
    a. The mobile app detects the activated electronic lockout device and retrieves the corresponding digital key from the cloud service.
3. The authorized employee opens the electronic lockout device
    a. The mobile app transmits the digital key to the electronic lockout device to open it.
4. The authorized employee applies the electronic lockout device to the energy isolating device to lock out the machine.

5. The authorized employee attaches a SmartTag if necessary.

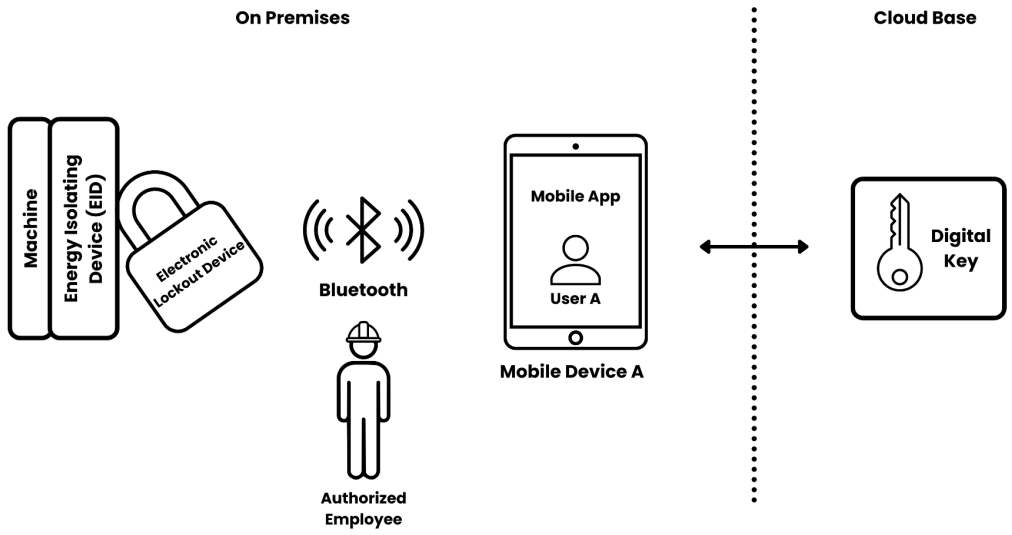

Figure 3: Initiating Isolation — The Authorized Employee uses a mobile device to establish a Bluetooth connection with the electronic lockout device on the machine's energy isolating device.

6. The authorized employee applies a digital lockout using their smartphone app
    a. The mobile app places the digital key in a virtual lockbox.

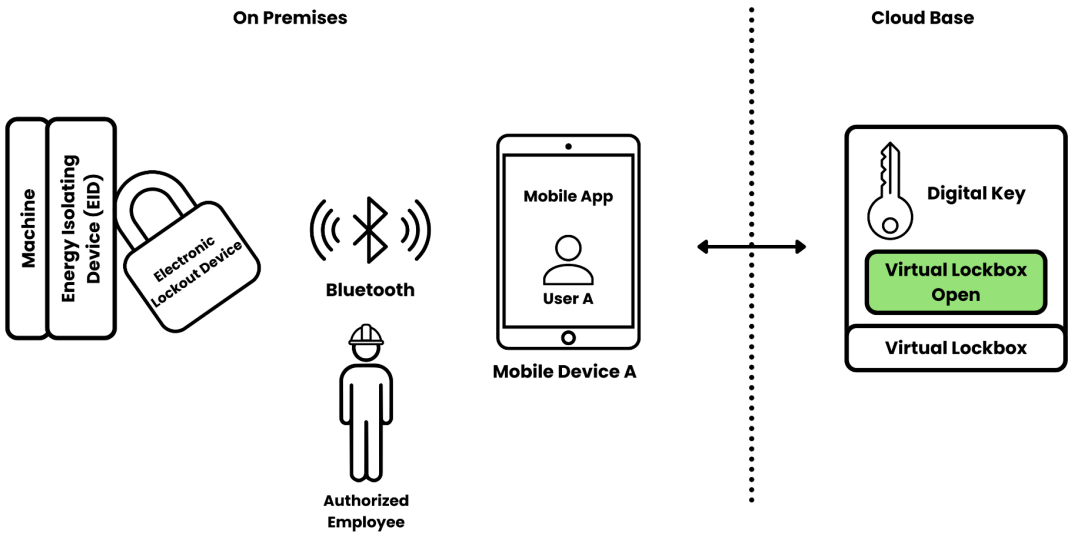

Figure 4: Securing the Digital Key — The process where the mobile app transfers the Digital Key from the physical device into an "Open" Virtual Lockbox residing in the cloud service.

b. The mobile app places the authorized employees' virtual personal lock on the virtual lockbox.
c. The virtual lockbox is now closed, and the digital key is no longer accessible.

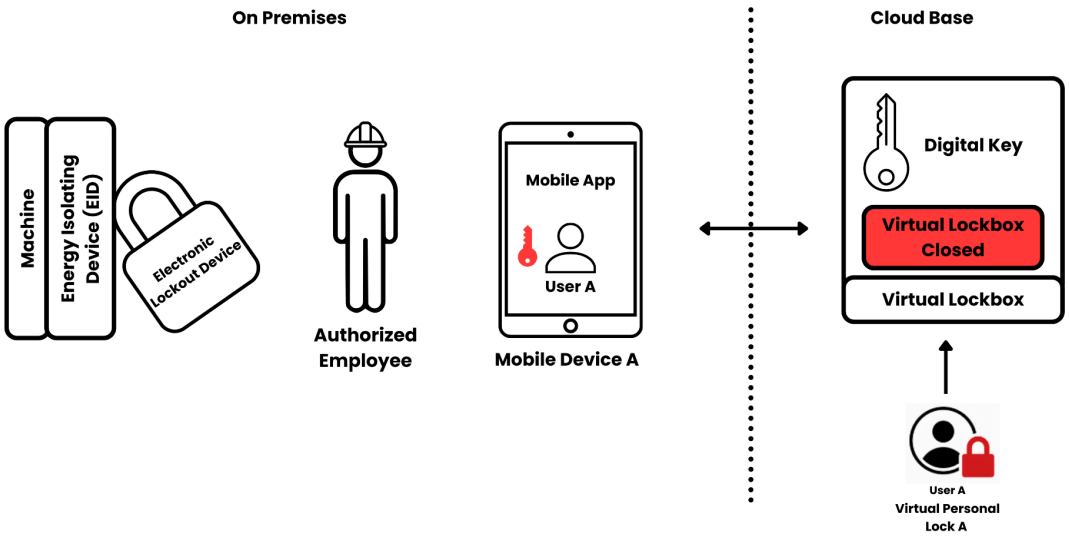

Figure 5: Closing the Virtual Lockbox — The Authorized Employee applies their Virtual Personal Lock to the lockbox, rendering the Digital Key inaccessible and effectively locking out the system.

6. The authorized employee verifies that the machine has no residual or stored energy and notifies the non-authorized employee that servicing can begin.

3.3 Group Lock On

The non-authorized employee locks onto ('joins') the digital lockout by applying their virtual personal lock to the virtual lockbox.

1. The non-authorized employee opens the mobile app and verifies their identity.
2. The unauthorized employee uses the mobile app to find the virtual lockbox created by the authorized employee in 3.2 above.
3. The unauthorized employee uses the mobile app to place a virtual personal lock on the virtual lockbox.
    a. The mobile app places the unauthorized employees' virtual personal lock on the virtual lockbox.
4. The unauthorized employee now has a level of protection equivalent to that provided by the implementation of a personal lockout and can commence work.

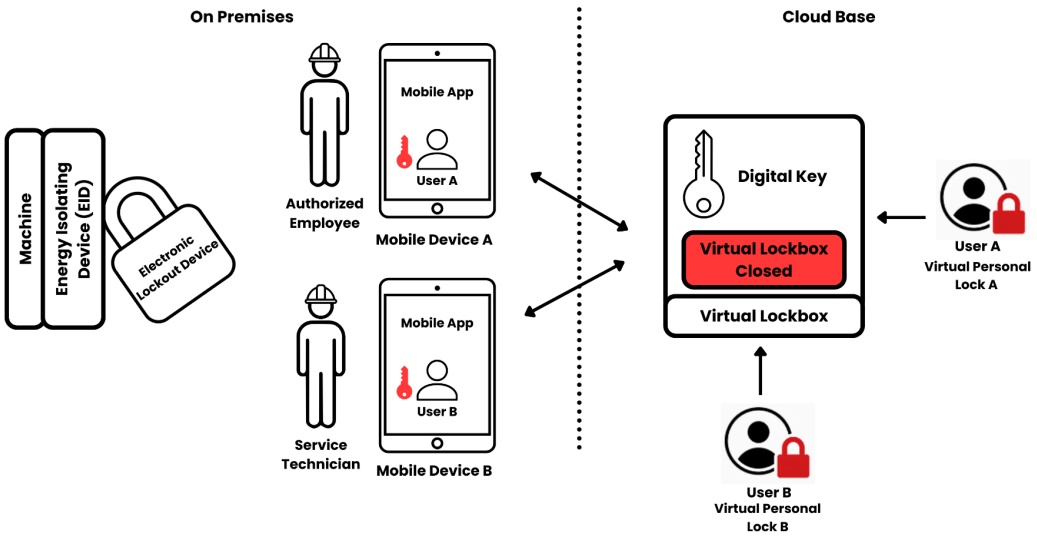

Figure 6: Active Group Lockout — A multi-user lockout state where both an Authorized Employee and a Service Technician have applied their specific Virtual Personal Locks to the single Virtual Lockbox.

A group lockout situation is now in effect, and the electronic lockout device cannot be removed until all participants have removed their virtual personal locks from the virtual lockbox.

3.4 Group Lock Off

The service is completed, and the unauthorized employee removes their virtual personal lock:

1. The unauthorized employee opens the mobile app and verifies their identity.
2. The unauthorized employee uses the mobile app to find the virtual lockbox from 3.2 above.
3. The unauthorized employee uses the mobile app to remove their virtual personal lock on the virtual lockbox.
    a. The mobile app removes the unauthorized employee's virtual personal lock on the virtual lockbox, leaving the authorized employee's virtual personal lock in place.

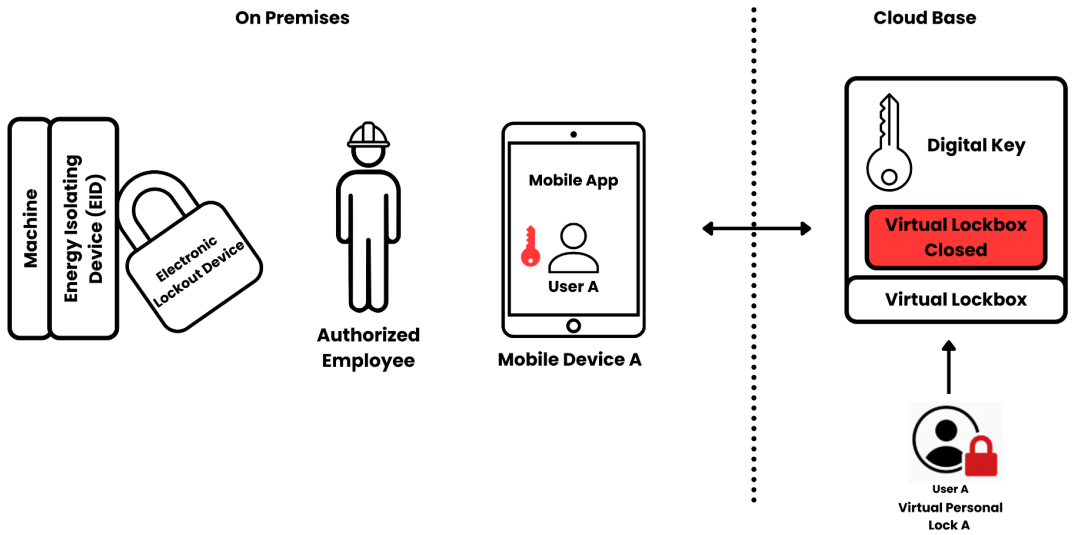

Figure 7: Partial Group Disengagement — The state of the Virtual Lockbox after the Service Technician has finished work and removed their personal lock, while the Authorized Employee remains locked on.

3.5 Remove Lockout and Reenergize

The authorized employee removes the electronic lockout device:

1. The authorized employee checks the machine and the work area to ensure all employees have been safely positioned or removed and verifies that the controls are in neutral.
2. The authorized employee opens the mobile app and verifies their identity.
3. The authorized employee uses the mobile app to remove their personal virtual lock from the virtual lockbox.

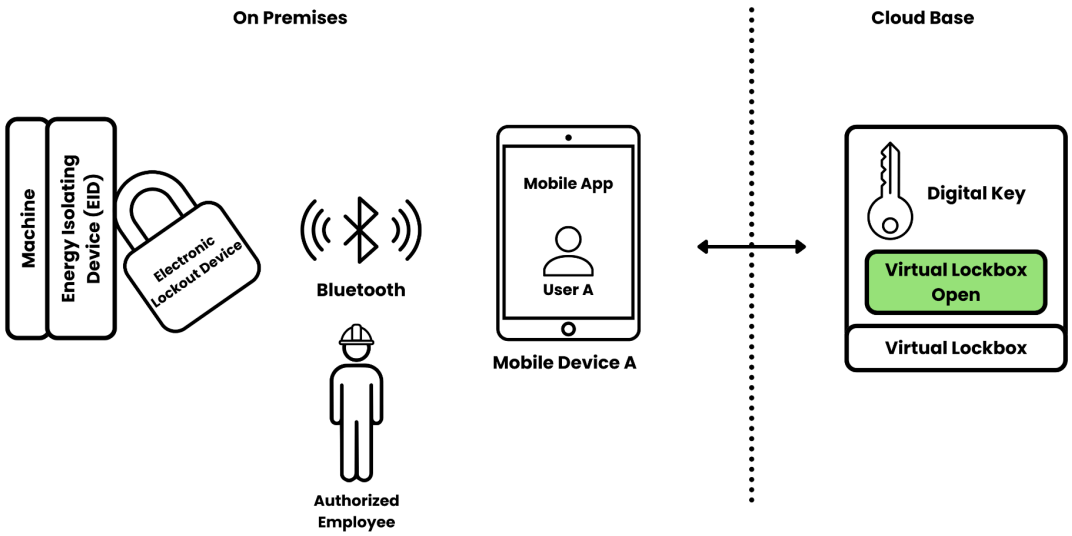

Figure 8: Releasing the Lockout — The Authorized Employee removes the final Virtual Personal Lock, returning the Virtual Lockbox to an "Open" state so the Digital Key can be retrieved.

4. The unauthorized employee now has a level of protection equivalent to that provided by the implementation of a personal lockout, and the unauthorized employee can commence work.
    a. A. The mobile app detects the activated electronic lockout device, finds the corresponding virtual lockbox, and verifies that the virtual lockbox is open.
    b. The mobile app retrieves the digital key that corresponds to the electronic lockout device from the virtual lockbox.
    c. The mobile app transmits the digital key to the electronic lockout device to open it.

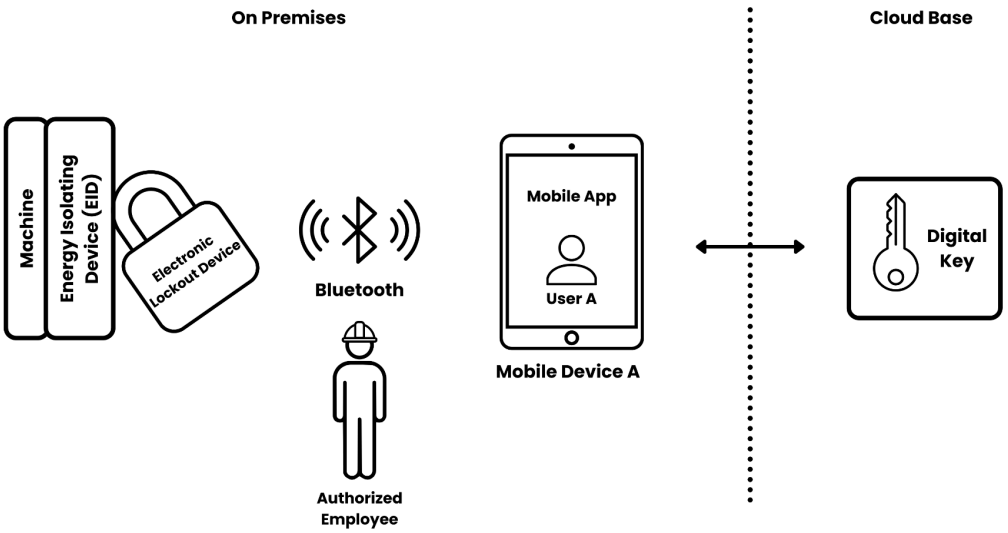

Figure 9: Removing the Electronic Lockout Device — The Authorized Employee uses the mobile app to transmit the retrieved Digital Key to the physical device, allowing them to unlock and remove the electronic lockout device from the energy isolating device.

5. The authorized employee removes the electronic lockout device from the energy isolating device.
6. The authorized employee reenergizes the machine.

smartlox

4 Regulatory Implications

This section outlines the clauses from the United States Department of Labor, Occupational Safety and Health Administration ('OSHA') regulations regarding the control of hazardous energy, reference 29 CFR § 1910.1471 [1], that are relevant to this white paper and the interpretations used in the design of a Digital Lockout-Tagout system.

Definitions

Authorized employee.

> A person who locks out or tags out machines or equipment in order to perform servicing or maintenance on that machine or equipment. An affected employee becomes an authorized employee when that employee's duties include performing servicing or maintenance covered under this section.

Application of control

Lockout or tagout device application.

> Lockout or tagout devices shall be affixed to each energy isolating device by authorized employees

Interpretation: Company lockout procedures and industry best practices should ensure that only authorized employees can apply and remove lockout devices to a machine's energy isolating device. A digital lockout system can enhance these procedures by utilizing individual user authentication, role-based permissions, and encrypted electronic keys to ensure that only authorized users can apply and remove electronic lockout devices to a machine's energy isolating device.

Additional requirements

> **Group Lockout or Tagout**
>
> When servicing and/or maintenance is performed by a crew, craft, department, or other group, they shall utilize a procedure that affords the

employees a level of protection equivalent to that provided by the implementation of a personal Lockout or Tagout device.

Interpretation: Company lockout procedures and industry best practices should ensure all participants in a group Lockout-Tagout process "lock on" to a lockout before commencing work, and "lock off" from a lockout when work is complete. Traditional lockout procedures utilize physical lockboxes to meet this requirement. A Digital Lockout-Tagout system can strengthen and improve on this process by providing a virtual lockbox for all participants to apply a virtual personal lock (as described in the example above). These virtual mechanisms afford the participants a level of protection equivalent to that provided by the implementation of a physical personal lock.

Group lockout or tagout devices shall be used in accordance with the procedures required by paragraph (c)(4) of this section, including, but not necessarily limited to, the following specific requirements:

Primary responsibility is vested in an authorized employee for a set number of employees working under the protection of a group lockout or tagout device.

Interpretation: Company lockout procedures and industry best practices should ensure that a single authorized employee has primary responsibility for a group of employees working under the protection of a group lockout. A Digital Lockout-Tagout system can ensure compliance with this requirement by maintaining an electronic record of the responsible authorized employee, and by providing a robust and predictable function for transferring this responsibility to other authorized employees, and ensuring all participants are notified of the state of the group lockout and the responsible authorized employee.

Each authorized employee shall affix a personal lockout or tagout device to the group lockout device, group lockbox, or comparable mechanism when he or she begins work, and shall remove those devices when he or she stops working on the machine or equipment being serviced or maintained.

Interpretation: Company lockout procedures and industry best practices should ensure all participants in a group Lockout-Tagout process "lock on" to a lockout before commencing work, and "lock off' from a lockout when work is complete. Traditional Lockout-Tagout procedures utilize physical lockboxes to meet this requirement. A Digital Lockout-Tagout system can strengthen and improve this process by providing a virtual lockbox for all participants to apply a virtual personal lock (as described in the example above). These virtual mechanisms afford the participants a level of protection equivalent to that provided by the implementation of a physical personal lock.

5 Summary

Digital Lockout-Tagout systems can strengthen existing safety management protocols while delivering improved operating efficiencies, greater accountability and control, and reducing operating costs.

In summary, the Digital Lockout-Tagout System proposed in this whitepaper meets the intent of OSHA requirements for Lockout-Tagout and affords all participants in the lockout process with a level of protection equal to, or greater than, that provided by the implementation of traditional physical and personal lockout locks.

References

[1] Occupational Safety and Health Administration (OSHA), "Title 29, Subtitle B, Chapter XVII, Part 1910, Subpart J: The control of hazardous energy (lockout/tagout)," *Code of Federal Regulations*, Feb. 18, 2026. [Online]. Available: https://www.ecfr.gov/current/title-29/subtitle-B/chapter-XVII/part-1910/subpart-J#1910.147. [Accessed: Feb. 18, 2026].