

Securing Remote Locations - Reducing Costs of Key/Card Management

Executive Summary

Across northern Canada and elsewhere in the world, there are many remote locations where utilities, oil and gas, water supply and other enterprises have to secure their equipment/premises. Many of the existing solutions require either a lock and key or some kind of smart card access requiring telecommunication between the remote location and the enterprise hubs.

One of the main costs and challenges of operating these facilities is the loss of keys, master keys and cards. Trying to keep track of these and to then de-provision the user or worse, having to rekey the facilities is expensive, time consuming and also creates a weak security system. Further, if the wrong key or pass card is given, then there is lost time in getting back to get the right key or card.

Further, many different people often enter these premises on a temporary basis. For example, an electrician or welder on contract may require access to the facility. Trying to keep track of these people and then to terminate them quickly is often very hard to do.

What if your enterprise could?

- Provision a welder, electrician or employees easily such that they could receive their credentials remotely and then access the facility
- Automatically terminate the access
- Lower your overall operational key and card management costs
- Control this without having to require a communications system to the facility
- Centrally manage this at a very low implementation cost
- Integrate this with existing physical access control and identity management systems

That's what this paper will describe.

Low Cost Solution: Telcred

The solution this paper proposes uses low cost technology from Telcred. They enable remote access control using NFC-capable (Near Field Communication) cell phones smart cards, or dongles, which doesn't require any communication system for the locks

Telcred

[Telcred](#) is a young company whose mission is to replace physical keys with an access control system where previously not thought possible. The solution enables remote distribution of access rights to mobile phones, key-fobs and smart cards. So what do they offer? To illustrate, let's use an example of quickly provisioning Bob Welder, who's a contractor, hired to do some welding work at three of your remote locations in northern Canada (let's call them all in Zone 1). He's going to need access for only three days.

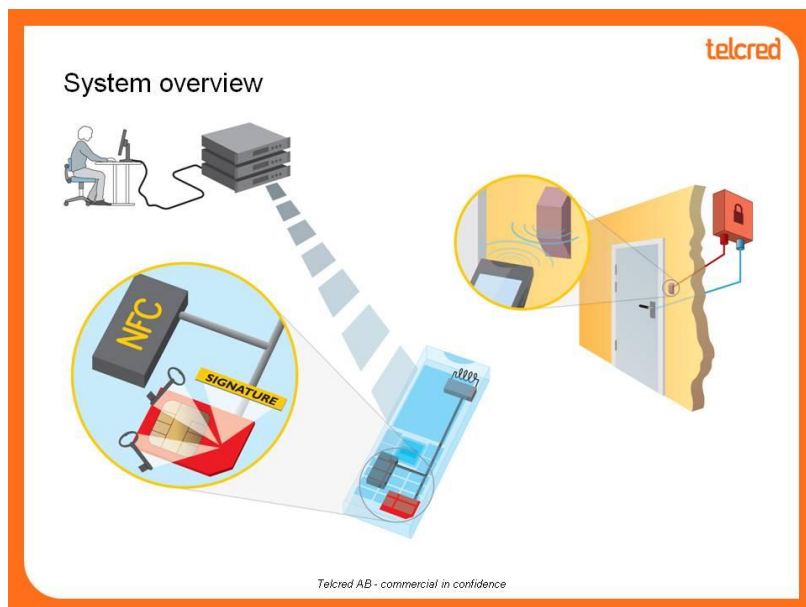
The central security dept, or a regional security administrator, would create an access control policy that says Bob is given access to Zone One facilities for 3 days. This would only take a minute to do. Bob has a cell phone that has NFC (Near Field Communication) capabilities, allowing it to emulate a contactless smart card, and which has already been provisioned with Telcred's application. A few seconds later, Bob's cell phone receives an encrypted file which contains his new access rights.

Bob then drives out or takes a helicopter to the first location. He walks up to the door where there is a card reader (similar to the ones used in traditional access control systems) and presses his cell phone about 1-3 cms away from the reader. In less than a second here's what happens unbeknownst to Bob.

The cell phone securely passes Bob's authentication data and access credentials to the reader which then talks to a door controller located inside the building. The door controller has its own identity or identities which your enterprise has assigned to it. In this example, it is part of a group called Zone 1. The controller also knows the date and time. It then checks Bob's authentication and authorization and determines that Bob's access credentials fall within the current time and date and that his authentication is correct. Therefore, the door controller tells the door to unlock and in walks Bob.

When Bob goes to the other two sites, the same process happens. Unfortunately, Bob realizes he needs to spend an extra day at one of the sites. He calls in to your enterprise and after the supervisor's approval is given, the security administrator extends Bob's access by one day. Bob's cell phone is then updated and Bob continues to work.

If there is no cell phone reception in the remote areas, it is not a problem to open the door because Bob's phone only needs access to receive updated access rights. The access control process at the door is completely offline.



NFC is a new communication technology gradually being introduced in mobile phones, but it is also available as smart cards and key-fobs and Telcred's solution works just as well with such devices. In this case, provisioning of updated access rights is done through an inexpensive NFC-writer connected to a PC with an Internet connection through USB. In our previous example, before leaving his office Bob would place his NFC smart card on the NFC-writer and launch a PC application which connects to the Telcred backend system, checks for updates to Bob's card and writes them to the card.

Gone are all the hassles of key management without having to provide a communication infrastructure for the locks. At a cost well below \$500 per door, the enterprise has a remote access solution that can easily integrate with the rest of the physical access security and logical security as the next sections illustrate.

I am looking for pilot sites to demonstrate this. If you're interested then please contact me.

About the Author

Guy Huntington has been in the identity industry for the last 13 years. He has rescued several large Fortune 500 identity projects and written numerous white papers on identity and physical and logical access and integration (<http://www.authenticationworld.com/papers.html>). Guy can be reached at guy@hvl.net or 1- 604-861-6804.