Tutorials:

Tutorials of Personal Identifier are perhaps the best way to understand its applications and methodology.

Tutorial Scenarios:

There are three tutorial scenarios, two of which are current day authentication situations and the third is one of several new applications of identification verification made possible by Personal Identifier.

First Scenario:

John Doe is addressing a task many of us repeat each day. He's arrived at his desk and is about to log into the corporate networks. In recognizing this, the corporate gatekeeper sends off a request for identification verification to John's smartphone. Gatekeep then connects to the Bluetooth interface of John's smartphone and awaits receipt of the personal identifier code produced as a result of the request. Receiving that the gatekeeper confirms the smartphone is the device belonging to John. It then verifies the smartphone is at that instant in John's possession. Finally gatekeeper verifies the session identifier token is that included with the identification verification request and that it was received within the time limits expected. All conditions being met, John is granted access to the corporate networks and begins his day's work.

Second Scenario:

Jane, John's wife, arrives at the local high where she teaches 10th grade physics. Approaching the main entrance she presents her smartphone to the admission control scanner. Detecting the pending access request, an identification verification request is sent off by the gatekeeper to Jane's smartphone. Following that gatekeeper reads a QR barcode from the smartphone display whereupon it verifies it is Jane's smartphone, that the personal identification code indicates it is in Jane's possession and that the verification response was within the time limits expected. All conditions met, Jane is admitted to the school campus.

Third Scenario:

Johnny junior, in ninth grade this year, arrives at the high school. As he his friends and classmates pass through one of the access portals the campus gatekeeper detects his smartphone and sends off an identification

verification request over the cellular network. Milliseconds later an identification code is received over the Bluetooth channel. As in prior scenarios, the smartphone is confirmed to be Johnnies, possession is confirmed and Johnny is now registered to be present and on campus. Should Johnny decide to leave school the same process plays out in reverse. In this way the gatekeep knows at all time who is on campus, an presumably who is not. Of course, should an unrecognized smartphone or person without smartphone pass through the portal alarms go off and countermeasures taken.

Takeaways:

There are several subtle observations that may have been picked up on. First off, the first two scenarios are similar to activities most Americans experience each day, but with seamless use of Personal Identifier where credentials were once relied upon. The final scenario is a new access management possibility made possible by Personal Identifier. It should have been obvious that in scenarios no one fumbled with passwords, PINs, selfies taken just right or multiple swipes over the finger print scanner. In each case the activity of identity verification was automatic, natural and error free. Also not apparent but a fact, each authentication session was performed completely without risk of successful cybercriminal impersonation attack.

Further information on this and other security related interests and projects can be found at www.ProteqsIt.com.

Contact Information

Rick Hallock
Rick.Hallock@ProteqsIt.COM
Phone: (239) 370-0246