4OI6 Phase 2 – Competitor Research

**Nymi:** [**http://www.biometricupdate.com/201503/nymi-to-test-biometric-wristband-at-uk-based-halifax-bank**](http://www.biometricupdate.com/201503/nymi-to-test-biometric-wristband-at-uk-based-halifax-bank) **($80)**

Description: Itis a small, wearable device that uses electrocardiogram (ECG) to authenticate user identity. In effect, the Nymi turns a person’s own heartbeat into a unique key that can be used to unlock any conceivable device.

How it’s used: You put it on once a day, touch it with your opposite hand for a few seconds, it measures your heartbeats, it confirms that you – the rightful owner are wearing it, and then it’s able to communicate that identity to whatever system or service you use

How is it distinct: The real unique part of what we’re doing with the idea of putting biometrics into a wearable device is this concept of persistent identity. Even with the iPhone with its fingerprint reader, every time I want to access my phone, every time I want to access an application that’s enabled by the touch ID, I have to put my fingerprint down. Whereas with the Nymi, you put it on once and until you take it off you’re still authenticated. And that’s the big difference. We just have to make one match, we can tune the system to be very secure during that one matching process, and then you don’t need to think about it.

**Olea: http://www.oleasys.com/**

Description: Olea HeartSignature is like no other authentication technology in its ability to continuously identify an individual in real time using contact-less, wireless detection of vital signs to create a unique digital "signature" for limitless security applications; a revolutionary authentication technology with precision comparable to existing biometric authentication systems.

How it works: real time detection of vital signals using micro Doppler radar technology

**Researchers at the State University of New York-Binghamton**

Since mobile health devices would have already collected a patient’s electrocardiogram (ECG)—a measurement of the heart’s electrical activity—the heartbeat data can simply be reused for security purposes. This has an advantage over many existing encryption techniques, Jin says, because it's far less computing-intensive and uses less energy, which is important when working with energy-limited devices like small wearable health monitors. Since the data has already been collected, it adds little extra cost to the process as well.

An ECG as a secondary form of ID would remove that issue.

There's only one problem: these unique patterns are also changeable. A person’s ECG can change with physical activity, mental states (like stress), age and other factors.

https://www.smithsonianmag.com/innovation/using-your-heartbeat-password-180961952/

**Korean Government: http://www.biometricupdate.com/201706/korea-internet-security-agency-developing-biometric-authentication-for-mobile-banking**

What are they doing: “We are developing an algorithm for authenticating mobile banking with a combination of a fingerprint, heart rate and (an) electrocardiogram,” said Jason Kim, chief of KISA’s security technology dissemination team. “The technology is expected to be much safer than existing biometrics including iris sensors, fingerprint scanners and facial recognition.”

How it works: The biometric authentication technology reads heart rates and electrocardiograms on an individual’s smartwatch and then sends the information to his or her smartphone.

Investment: The development of the biometrics technology is being led by Kim under the Ministry of Science, ICT and Future Planning with an investment of 1.2 billion won ($1 million).