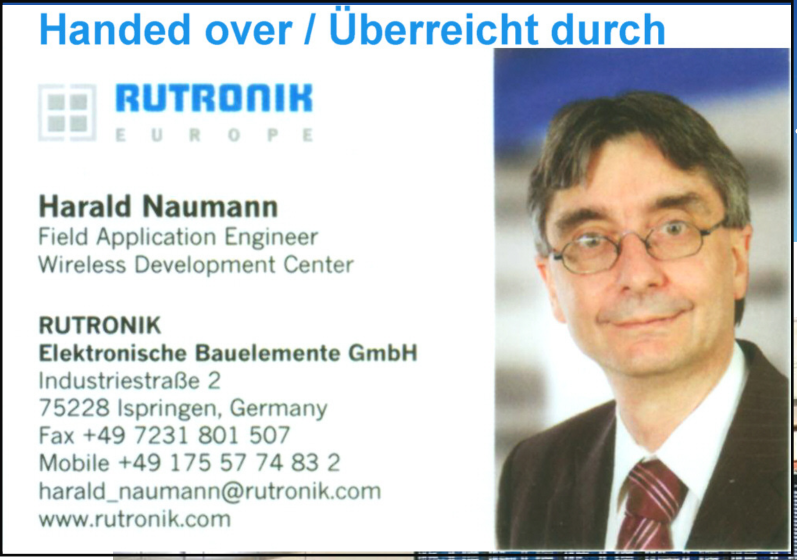

Handed over / Überreicht durch

RUTRONIK
EUROPE

Harald Naumann
Field Application Engineer
Wireless Development Center

RUTRONIK
Elektronische Bauelemente GmbH
Industriestraße 2
75228 Ispringen, Germany
Fax +49 7231 801 507
Mobile +49 175 57 74 83 2
harald_naumann@rutronik.com
www.rutronik.com

Where am I? Inside a large building such as an airport terminal Bluetooth low energy tags could be placed in strategic locations to inform cell phone-equipped passengers of their location

> **“Bluetooth low energy is an ‘always off’ technology. It wakes up now and then but basically stays in the lowest power modes”**
>
> Alf Helge Omre, Business Manager for Bluetooth low energy, Nordic Semiconductor

Because power consumption is so low, coin cells will typically last a year or more.

Bluetooth low energy chips can operate either as slaves or masters and which device takes what role is decided during the initial negotiation. There is no reason for a tag to be the proverbial one-trick pony. Design cycles will be short compared to proprietary solutions because the design team can concentrate its efforts on writing application layer code instead of the entire protocol stack.

Sensing a means of making mobile phones even more indispensable, Nokia and other manufacturers are clearly on the *Bluetooth* low energy bandwagon. “We see it as part of the continued evolution to the *Bluetooth* chip set,” says Mika Sarén, Nokia’s Senior Technology Manager for Connectivity. When the specification is released, it will be supported in time for the first product release on Forum Nokia, the company’s web site for developers.

Security and privacy

In a world populated by sophisticated hackers on one hand and a growing concern among the general population about privacy on the other, any technology that can open doors automatically or help document its user’s location had better provide system designers with tools to protect privacy and assure security.

RFID technology has, for example, been the subject of severe – and not always justified – criticism by privacy advocates. Among the lessons learned is that complete systems must be developed, says Tim Newson, NXP Semiconductors’ RFID director of sales and marketing for the Americas.

Security and/or privacy concerns vary from application to application more than one might first imagine, he says. Although password protection provides a fairly low level of security, in some instances it is sufficient. At the other end of the spectrum, completely disabling a device that senses it is being hacked is appropriate in some instances but not all.

Another consideration, which is outside the technology realm but is nonetheless important, is influencing public perceptions. Attacks on RFID by privacy advocates have been intense, Newson says, and this has prompted the RFID community to spend a good deal of time and energy informing the public about the technology.

Protecting keyless entry systems from hackers is a problem that has already been solved and *Bluetooth* low energy will undoubtedly follow suit. Applications that run on “keyless” key fobs change the code every time they lock or unlock the door. Typically a challenge/response mechanism is added on top of security that exists in the wireless device itself.

Bluetooth low energy has built in a variety of tools for developers. It will run 128-bit DES encryption and it will require authentication before encryption.

Privacy mode

The privacy mode will, generally speaking, prevent people from tracking a key fob or other *Bluetooth*-enabled device. Like most wireless devices, *Bluetooth* chips have a standard 48-bit Ethernet address that does not change. This unique number, however, would allow the tag or phone to be tracked. The privacy mode frustrates this security hole by transmitting a randomized 48-bit address instead of the standard fixed one.

This only happens after the devices are paired. Afterwards they communicate by using a shared security key. The randomized address might change on roughly 15 minute intervals. To any listener that is not aware of the shared keys, the *Bluetooth*-enabled device is anonymous. The engineers who developed the Proximity Profile have tried, says CSR’s Hunn, to supply a robust set of security tools for designers but if the application requires higher security it can be added on an end-to-end basis.

Location services

Using clever techniques and emerging mathematical concepts such as self-organizing topological networks, *Bluetooth* low energy’s ability to determine proximity can be leveraged into finding a person’s location when GPS is not available.

Inside a large, multi-story building, for example, a number of *Bluetooth* low energy tags can be placed in strategic locations with information about where they are located.

Someone carrying a *Bluetooth* low energy-equipped device inside the building can be informed of his or her location by having the *Bluetooth*-equipped devices communicate with others (stationary or mobile). By relaying information back and forth and calculating proximities, a location inside the building (a three-dimensional position, in fact) can be calculated.

Coupled with the imagination of design engineers, *Bluetooth* low energy’s Proximity Profile is virtually certain to ignite a revolution in location applications. Chip companies will smooth the way by providing highly integrated solutions, including in some cases an embedded microcontroller, and development kits, says Nordic’s Omre. ■