# White Paper: IoT wireless pairing proposal

linkedin.com/pulse/white-paper-iot-wireless-pairing-proposal-roberto-a-foglietta


*Published on December 13, 2015*

## ABSTRACT

Internet of Things (IoT) market requires that micro devices like sensors with a limited computational capacity and power source would be able to negotiate with an access point (AP) their entrance in a Personal Area Network (PAN). Adding such devices into a PAN should be an user-friendly action for final customers. Moreover pairing a couple of systems should be a secure enough action for the target market customers.

This pairing concept is based on sharing a cryptographically strong shared secret like a RSA public key (or anything equivalent) between two devices. Shared secret is used to let the two devices identify themselves and establish a trusted connection. A couple of NFC cards are used to inform the access point about incoming device set of permissions required and to acquire its credentials. Using a set of clearance levels, an ACL table and an API set, the configuration procedure could handle any kind of devices that support a standard encrypted connection like SSL or SSH tunnel and VPN setup.

Security is a process, not a product. So far, absolute security does not exist even if deployed by design. Security and simplicity usually do not fit the same bill together but they are at opposite sides in a balance between them. It is quite difficult to imagine something simpler than pressing a button on each devices. Using a set of NFC cards (or any contact-less card with similar data capacity) is possible to attribute to any device a specific level of trust and related capabilities (guest, parent control, IoT device, administration, etc.). Moreover this helps to reduce the range in which the attacker should stay within to be considered a threat.

In order to design an innovative and more secure pairing method for PAN devices, some of well-known assumptions may be challenged or totally abandoned. Designing and delivering a new hardware subsystem may as well contribute to setup a new standard. Combination of existing standards may drive to a faster time to market solution.

NFC cards are cheap to create, easy to read and accessible only locally within 5 cm (without the usage of special and costly devices). Today they could store up to 8.192 bytes of data that are enough to store credentials, device and producer identification, required network permissions and describe a list of features exported by the device.

Each device enabled for this pairing protocol will be delivered by an OEM producer with a NFC card. Its manual will instruct the user about which level of security each feature will require. So far, the end user could decide to have limited features set in order to maximize security or full features

set.

This procedure is the main point of strength which brings the security usually related to enterprise networks to the end user without the pain of dealing with such technologies. However, designing and implementing a secure and user-friendly back compatible procedure is the key of a fast adoption.

## The importance of being Sally

Henry would like to know Sally but he knows that to acquire her trust within a certain degree of confidence, he has to be introduced to her by a common trusted friend. This is the trust-of-chain basic concept and the implementation relays on unique humans ability to recognize faces which is relatively difficult to tamper.

Another typical human characteristic involved in granting trust to someone else is that process is not a single act but a step-by-step path escalating higher level of trust. At any step and at any time the level of trust could be reverted back or completely denied. So far, NFC cards are not the only part of the system that is designed to manage different levels of trust, but the pairing protocol itself. Resilience (elasticity) differs from resistance (hardness) because is does not fail if a single step or component fail but still maintain a certain level of protection.

Forget biometrics because are sensitive data complex to deal and their custody is critical. For personal IoT and SoHo use, they could be replaced with something like contact-less business cards which contains all data to identify and authorize the desired device. The owner present himself to the AP by the chosen card then introduce the new device to the AP presenting the device card and switch-on it.

## White paper

The full paper is available at this link:

- http://www.roberto.foglietta.name/pub/IoT-HaS-pairing-rev076.pdf

These MD5 and SHA1 sum codes will grant you about the document integrity:

- md5sum: 5e5da4835e23956a83f6bbc42b597794
- sha1sum: 4a43e47b0386fd330e8b147988b00271d582397d