

**Subject :** Pathchecker Authentication Scheme

**Keywords :** Computational RFID, Authentication, Lightweight Cryptography, Traceability.

**Abstract :** Authentication requirements for manufactured goods is rapidly extending from “*origin only*” to “*origin & process conformance*” : because of counterfeiting and grey market pressure on the one hand, and regulatory constraints on the other hand, the ability to easily authenticate in the field the context in which the tracked product has evolved is becoming a requirement in many industries (aircraft maintenance, cattle traceability, pharmaceutical goods...). These authentication requirements might cover items as various as distribution stage, authorized party, control performed, physical parameters conformance...

The Pathchecker authentication scheme was designed for that purpose, extending the fields of application of passive RFID by computing and storing this authentication information where required : directly on the tag associated to the tracked object. This allows for light, easy to deploy and operate field authentication applications.

*Pathchecker : an RFID Application for Tracing Products in Supply-Chains*  
Khaled Ouafi & Serge Vaudenay / RFIDSec 2009  
<http://infoscience.epfl.ch/record/139219>

**WISP Development :** The WISP platform will be used for two purposes :

1. Implementation of lightweight hash algorithm and ORIDAO traceability protocol layer for validation of Pathchecker authentication scheme on a sequence of stage ID's only.
2. Extension of the Pathchecker authentication scheme to physical parameters authentication (temperature...) through the use of WISP sensors interface capability.

**Team :** *Yusuf Leblebici, Catherine Dehollain, Nilay Dagtekin*

Microelectronics Systems Laboratory  
Ecole Polytechnique Fédérale de Lausanne (Switzerland)  
<http://lsm.epfl.ch>

**Nicolas Reffé**

ORIDAO (France)  
[www.oridao.com](http://www.oridao.com)

**Contact :** *Nicolas Reffé / [nicolas.reffe@oridao.com](mailto:nicolas.reffe@oridao.com) / +33 467 130 065*