# Revoke and Let Live: A Secure Key Revocation API for Cryptographic Devices*

Véronique Cortier
CNRS, Loria, UMR 7503
F-54506
Vandœuvre-lès-Nancy, France

Graham Steel
INRIA
Paris, France

Cyrille Wiedling
CNRS, Loria, UMR 7503
F-54506
Vandœuvre-lès-Nancy, France

Embedded systems deployed in hostile environments often employ some dedicated tamper-resistant secure hardware to handle cryptographic operations and keep keys secure. Examples include mobile phones (which contain SIM cards), smartphones (recent models include 'Secure Elements'), public transport ticketing systems (such as the Calypso system which employs 'SAM' modules), smart utility meters (that include a smartcard-like chip for cryptography), on-vehicle cryptographic devices to support vehicle-to-vehicle networking *et caetera*. In such systems, it is often necessary to support the possibility of remotely revoking and updating the long-term keys on the device.

While extensive research addresses the problem of establishing session keys through cryptographic protocols (see e.g. [1, 2, 4]), relatively little work has appeared addressing the problem of revocation and update of long term keys [3, 7, 5, 6]. We present an API for symmetric key management on embedded devices that supports revocation and prove security properties in the symbolic model of cryptography. Our API supports several modes of operation depending on the capabilities of the hardware, including time-based revocation and forced revocation with (temporary) blacklisting of key levels.

## References

[1] C. Cachin and N. Chandran. A secure cryptographic token interface. In *Computer Security Foundations (CSF-22)*, pages 141–153, Long Island, New York, 2009. IEEE Computer Society Press.

[2] J. Courant and J.-F. Monin. Defending the bank with a proof assistant. In *Proceedings of the 6th International Workshop on Issues in the Theory of Security (WITS'06)*, pages 87 – 98, Vienna, Austria, March 2006.

[3] Laurent Eschenauer and Virgil D. Gligor. A key management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS)*, pages 41–47, 2002.

[4] S. Fröschle and G. Steel. Analysing PKCS#11 key management APIs with unbounded fresh data. In P. Degano and L. Viganò, editors, *Preliminary Proceedings of the Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS'09)*, volume 5511 of *Lecture Notes in Computer Science*, pages 92–106, York, UK, 2009. Springer. To appear.

[5] F. (Ed) Kargl. Sevecom baseline architecture. Deliverable for EU Project Sevecom, 2009. D2.1-App.A.

[6] Sebastian Mödersheim and Paolo Modesti. Verifying sevecom using set-based abstraction. In *IWCMC*, pages 1164–1169. IEEE, 2011.

[7] Xukai Zouz Yong Wan, Byrav Ramamurthy. Keyrev: An effifcient key revocation scheme for wireless sensor networks. In *IEEE International Conference on Communications (ICC)*, pages 1260 – 1265, 2007.

*The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement no 258865, project ProSecure, and the Direction Générale de l'Armement under contact no 11810242, Secure Interfaces.