



## Summary Report on KINAMIK K-NOTARY PROTOCOL Gap Analysis Universitat Politècnica de Catalunya

### Scope

The scope of the analysis The scope of the analysis includes

- Analysis of the linking timestamp algorithms and requirements of those algorithms of standards ISO 18014-3 and ANS X9.95.
- Analysis of the K-Notary's protocol from the document K-Notary Technical Basis – Security Register Architecture, ver 1.5, November 2008.
- Gap analysis of the protocol of the linking timestamp generation algorithm of K-Notary's, version 1.5.- as documented at “K-Notary Technical Basis – Security Register Architecture, ver 1.5, November 2008**Error! No bookmark name given.**”(herein after “K-Notary”)- against the standards ISO 18014-3 and ANS X9.95 .

This analysis only includes documental revision of the protocol of the linking timestamp generation algorithm of K-Notary's. No further testing was performed.

It is out of the scope of this gap analysis any other type of analysis, evaluation, audit and/or testing against the above mentioned standards or any other whatsoever.

### Reservations

This document is not a certification of compliance and shall be seen as a gap analysis of K-Notary technical specifications as regards ISO 18014-3 and ANS X9.95 technical requirements.

### Conclusion

The results of the analysis indicate that, with some technical modifications to achieve a full alignment, K-Notary could be able to comply with ISO 18014-3 and ANS X9.95.



Barcelona, March 18<sup>th</sup>, 2010

P.A. Juan Carlos Cruellas

**Universitat Politècnica de Catalunya (UPC)**  
Departament de Arquitectura de Computadors (DAC)  
c/ Jordi Girona 1-3, Modul D6.103, Barcelona  
Spain



Departament d'Arquitectura  
de Computadors

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Campus Nord  
Mòdul - D6  
Jordi Girona, 1-3  
08034 Barcelona  
Tel. 93 401 70 01  
Fax 93 401 70 55