Title (en)
METHOD FOR HSM MIGRATION

Title (de)
VERFAHREN ZUR HSM MIGRATION

Title (fr)
PROCÉDÉ DE MIGRATION POUR MODULES MATÉRIELS DE SÉCURITÉ (HSM)

Publication
EP 2454702 A1 20120523 (DE)

Application
EP 10730489 A 20100714

Priority
- EP 2010060107 W 20100714
- DE 102009027747 A 20090715
- DE 102009028064 A 20090729
- DE 102010030167 A 20100616

Abstract (en)
[origin: WO2011006912A1] The invention relates to a method for migrating from a first HSM (140; 101A) to a second HSM (101B), wherein the first HSM is associated with a first asymmetrical cryptographic key pair having a first personal key (142; 142A) and a first public key (147 A) and a first certificate (144; 144A) containing the first public key, comprising the following steps: generating a second asymmetrical cryptographic key pair having a second personal key (142B) and a second public key (191B) and a second certificate (190B), which contains the second public key, by the second HSM, transmitting the second certificate (190B) with the second public key from the second HSM to the first HSM, and generating a third certificate (144B) by the first HSM by signing the second public key using the first personal key, wherein a certificate check of the second certificate can be carried out by way of a certificate chain containing the first and third certificates.

IPC 8 full level
G06F 21/33 (2013.01); **G06F 21/41** (2013.01); **H04L 9/32** (2006.01)

CPC (source: EP)
G06F 21/33 (2013.01); **G06F 21/41** (2013.01); **H04L 9/3247** (2013.01); **H04L 9/3265** (2013.01); **H04L 63/062** (2013.01); **H04L 63/0823** (2013.01); G06F 2221/2153 (2013.01)

Citation (search report)
See references of WO 2011006912A1

Citation (examination)
- SAFENET: "Luna SA with Trusted Path Authentication", 31 December 2004 (2004-12-31), XP055457782, Retrieved from the Internet <URL:https://safenet.gemalto.com/resources/integration-guide/data-protection/luna_sa-_microsoft_rms_integration_guide> [retrieved on 20180308]
- NCIPHER: "NCIPHER netHSM TECHNICAL ARCHITECTURE WHITE PAPER", 31 December 2003 (2003-12-31), XP055457783, Retrieved from the Internet <URL:http://www.asiapeak.com/Download/nethsm_arch_issue_1.pdf> [retrieved on 20180308]

Designated contracting state (EPC)
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

DOCDB simple family (publication)
WO 2011006912 A1 20110120; EP 2454702 A1 20120523; EP 4250636 A2 20230927; EP 4250636 A3 20231227

DOCDB simple family (application)
EP 2010060107 W 20100714; EP 10730489 A 20100714; EP 23170433 A 20100714