

Building a Threshold Cryptographic Distributed HSM with Docker Containers

Caterina Munoz

INRIA Chile
caterina.munoz@inria.cl

Francisco Cifuentes

NIC Labs, Universidad de Chile
francisco@niclabs.cl

Francisco Montoto

NIC Labs, Universidad de Chile
montoto@niclabs.cl

Javier Bustos-Jiménez

NIC Labs, Universidad de Chile
jbustos@niclabs.cl

ABSTRACT

In this work we will present an implementation of the threshold cryptography system theoretically presented by Victor Shoup at EUROCRYPT 2000. Our implementation relies on the implementation of a standard PKCS#11 interface API, ZeroMQ messages over TCP, and Docker containers for the key-shares. Docker allowed us to make deployments simpler, without requiring a deep intervention of the servers. This is very important when we look for the system to be used by worldwide third parties.

Based on work published at [1].

CCS CONCEPTS

• **Security and privacy** → **Key management**;

KEYWORDS

E.3 DATA ENCRYPTION.

ACM Reference Format:

Caterina Munoz, Francisco Montoto, Francisco Cifuentes, and Javier Bustos-Jiménez. 2018. Building a Threshold Cryptographic Distributed HSM with Docker Containers. In *ANRW '18: Applied Networking Research Workshop, July 16, 2018, Montreal, QC, Canada*. ACM, New York, NY, USA, 1 page. <https://doi.org/10.1145/3232755.3232761>

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

ANRW '18, July 16, 2018, Montreal, QC, Canada

© 2018 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-5585-8/18/07.

<https://doi.org/10.1145/3232755.3232761>