Presenting our Distributed HSM and DNS-Tools

Javier Bustos-Jiménez & Hugo Salgado
jbustos@niclabs.cl, hsalgado@nic.cl

Since 2013, we have been working on a distributed HSM using threshold cryptography algorithms, mainly developing the distributed RSA algorithms proposed by Victor Shoup, where the private key is distributed among n key shares and only k (k > n/2) of them are need to generate a valid signature. Our first developments were written in C using ZeroMQ as transport layer. Since 2019 we moved the development to GoLang creating the TCRSA which is composed by DTC (the PKCS#11 compliance library) and DTCNode (the key-share signers). Further information can be found at https://niclabs.cl/tchsm/. Nowadays our distributed threshold cryptography library support also RSA and ECDSA like signatures.

To achieve the support of ECDSA we developed two new libraries: TCPaillier (for homomorphic encryption) and TCEDSA. TCPaillier is an implementation of Threshold Criptography Paillier's Cryptosystem. This code is based on the implementation of "Paillier Threshold Encryption Scheme" from UTDallas, both implementations (NIC labs and UTDallas) are based on the paper from Ivan Damgård et al. "A Generalization of Paillier's Public Key System with Applications to Electronic Voting". TCECDSA is an implementation of Threshold Cryptography Eliptic Curve Digital Signature Algorithm proposed on the paper "Using Level-1 Homomorphic Encryption To Improve Threshold DSA Signatures For Bitcoin Wallet Security". This implementation is loosely based on the extension of "Paillier Toolbox to use Level-2 Homomorphic Encryption" from Princeton CITP. That code is the working example of the work in the paper mentioned earlier. The code also implements the level-2 homomorphic encryption protocol from Dario Catalano et al, "Boosting Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data".

Why is a Distributed HSM important to DNSSEC? besides the fact that now the same level of security can be achieved using legacy hardware (we tested the system using a set of Raspberry Pi), it can be used to sign the root zone, distributing the power of such signature on k > n/2 representatives.

Also, while we were testing our distributed HSM, we developed our DNS-TOOLS https://github.com/niclabs/dns-tools to generate full DNSSEC zone signatures including NSEC or NSEC3 registers. Taking in account some recommendations from ccTLD operators, we added the capabilities of not only signing using our distributed HSM, but also using any SoftHSM that fulfill the PKCS#11 standard. Later, receiving more recommendations from DNS operators we did add the capabilities of DNS signing using file-stored keys. Giving that DNS-TOOLS was intended to generate DNSSEC signatures it is very suitable for third level domains that don't have to update on daily basis. Also, its modularity and documentation makes DNS-TOOLS easy to extend in case of new experimental behaviors want to be tested, for instance, the zone digest ZONEMD (https://tools.ietf.org/id/draft-ietf-dnsop-dns-zone-digest-08.html) was implemented in less than three days.